ULTIMATE POS COMPENDIUM

BETA

1. Základní principy přenosu dat

Podle směru využívání média

Simplex – data se prenášejí pouze jedním směrem, pro přenos stačí jeden přenosový kanál (tv vysílání)
Half duplex – přenos střídavě v obou směrech, pro přenos také stačí jeden přenosový kanál (vysílačky, ethernet s huby)
Full duplex – přenos dat probíhá oběma směry současně, musí být dva nezávislé kanály (přepínaný ethernet)

Podle způsobu přenosu bitů znaků

Paralelní – určitý počet signálových prvků (např. bitů) se přenáší současně, obsahuje typicky další řídící signály jako třeba hodiny
Sériový – signálové prvky téhož datového proudu jsou předávány za sebou, dělí se na asynchronní a synchronní

- v počítačových sítích využíván téměř výhradně sériový přenos (menší náklady na přenosové médium)

Synchronní přenos

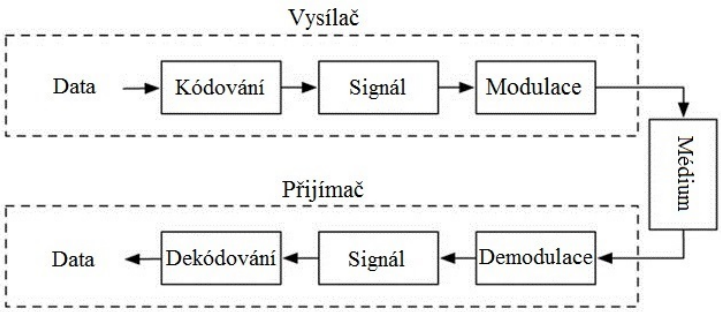
- realizován pomocí izochronního (pravidelného) signálu
- komunikační kanál je taktován společným hodinovým signálem (je veden buď zvlášť nebo je obsažen v datovém signálu)
- hodinový signál vymezuje intervaly platnosti jednotlivých značek
- používán u bitově orientovaných protokolů, kde se informace seskupuje do rámců, ty obsahují hlavičku a data proměnné délky (stovky bajtů až jednotky kB), pro přenos větších objemů dat
- začátky a konce rámců vyznačeny křídlovou značkou
- vysokorychlostní komunikace nebo izochronní linky

Asynchronní přenos (arytmický)

- vysílač a přijímač nemají společný hodinový signál
- obě strany mají své vlastní hodiny, které se po zasynchronizování mohou pro přenos několika bitů považovat za izochronní
- hodiny je třeba pravidelně synchronizovat, synchronizace probíhá fázově před začátkem každého vysílání znaku (startbit - 0)
- na konci znaku paritní bit (zabezpečení), mezi znaky pauza (stop bit - 1)
- používá se nejčastěji pro přenos krátkých bitových posloupností - znaků (5 - 8 bitů)
- terminály, průmyslové automaty, komunikační porty PC (COM)

Fyzikální omezení při přenosu dat

- signál se šíří médiem (prostředím)
  - metalické vedení (koaxiál, kroucená dvojlinka)
  - optické vlákno
  - vzduch, vakuum



Parametry média

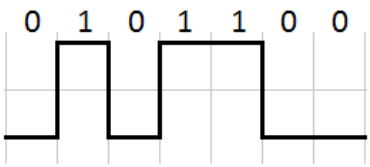
- útlum, rychlost šíření signálu, přeslechy, útlum odrazu (disperze)
- závislé na frekvenci – snaha využívat co nejužší pásmo frekvencí
- médium využíváme v rozsahu frekvencí, kde má výhodné parametry

Přenos v základním pásmu (baseband)

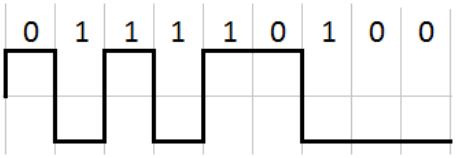
- přenáší se přímo frekvenční spektrum vzniklé zakódováním sekvence jedniček a nul
- digitální signál se přenáší v původním pásmu – nepoužívá se modulace
- pro metalická vedení v LAN, pro optická i ve WAN
- omezení dosahu – nevhodné vlastnosti média v určitých částech pásma
- bez použití nosné frekvence potřebujeme jiný mechanismus fázové synchronizace přijímače s vysílačem

Non Return to Zero (NRZ)

- přímé dvoustavové kódování
- pokud se nepřenáší stejnosměrná složka, nerozlišíme sekvenci nul od sekvence jedniček
- kvůli absenci neutrální hodnoty nelze toto kódování v základním tvaru použít pro synchronní přenosy
- 0: nízká úroveň, 1: vysoká úroveň

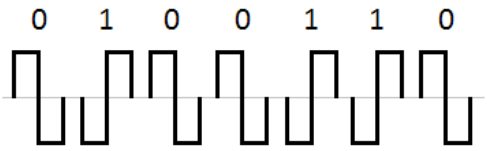


Non Return to Zero Inverted (NRZI)



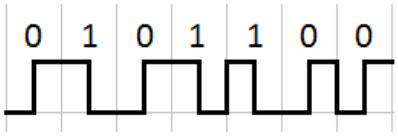
- dvoustavový
- 0: úroveň signálu zůstává, 1: inverze signálu

Return Zero (RZ)



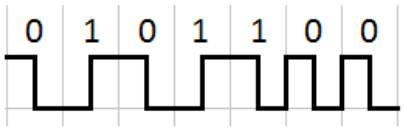
- třístavový (úrovně napětí: 0, -1, +1)
- první polovina bitového intervalu kóduje hodnotu bitu
- ve druhé polovině vždy nulová úroveň
- 0: úroveň signálu zůstává, 1: inverze signálu

Manchester



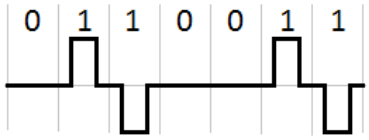
- kódování směrem změny uprostřed bitového intervalu
- na začátku bitového intervalu změna jen je-li potřebná
- 0: sestup signálu, 1: vzestup signálu

Diferenciální Manchester



- kódování změnou nebo absencí změny na začátku intervalu
- uprostřed intervalu změna vždy (směr podle potřeby)
- 0: změna, 1: absence změny

Alternate Mark Inversion (AMI)



- 3 úrovně amplitudy signálu (0, +1, -1)
- problém udržet synchronizaci přijímače při dlouhých posloupnostech nul
- 0: nulová hodnota, 1: střídavě úroveň +1 a -1

HDB3

- řeší problém AMI s dlouhou posloupností nul tak, že po třech nulách vloží jedničku
- vložená jednička se pozná porušením pravidla střídání polarity

Code Mark Inversion (CMI)

- pro přenos AMI/HDB3 přes optická vedení
- u optických vedení nelze vyjádřit dvojí polaritu (3 úrovní), pouze svítí / nesvítí
- jedna ze tří úrovní se vyjádří kombinací dvojice bitů (jedna kombinace zůstane nevyužita)

4B5B (5B6B, atd.)

- čtveřice bitů se mapují na vhodně vybrané bitové kombinace o šířce 5 bitů (nebo 5 na 6)

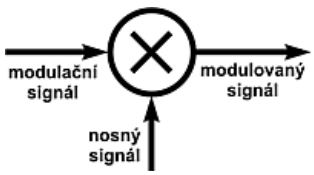
2B1Q

- jedním ze 4 možných stavů (amplitud) se kódují vždy 2 bity současně

Přenos v přeloženém pásmu (broadband)

- frekvenční spektrum zakódované sekvence jedniček a nul se překládá do frekvenčního pásma, kde má médium vhodné charakteristiky, nebo mimo oblast kde již nějaký signál přenášen je, využití média pro více nezávislých přenosů

Modulace



- zvolíme sinusový signál o frekvenci vhodné pro přenos médiem, měníme jeho parametry v závislosti na přenášených datech (frekvenci, amplitudu, fázi, nebo kombinaci těchto parametrů)

Frekvenční

- odolné proti rušení, omezené frekvenční pásmo

Fázová modulace

- 2^n možností změny fáze (úhlového posunutí) zakóduje jednou změnou současně n bitů
- např. Změna o 45, 135 , 225 a 315 stupňů, u fázové modulace se nejlépe rozpoznávají stavy

Kvadraturně-amplitudová modulace (QAM)

- kombinace fázové a amplitudové modulace

Modulační rychlost

- počet změn v signálu za sekundu – Baud[Bd]

Přenosová rychlost

- počet bitů přenesených za sekundu – b/s, bps
- přenosová rychlost může být vyšší než modulační – jednou změnou v signálu můžeme vyjádřit najednou více bitů

2. Topologie sítí, přenosová média, metody sdílení přenosového média

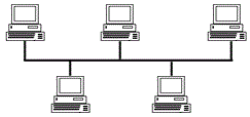
Topologie sítí

- se zabývá spojením různých prvků a zachycením jejich skutečné (reálné) a logické (virtuální) podoby (datové linky, síťové uzly)
- vlastnosti topologií: propustnost, rozšiřitelnost, spolehlivost proti výpadkům a jejich rekonfigurovatelnost

LAN

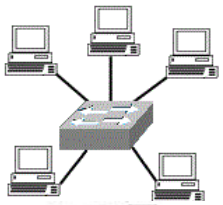
- lokální sítě, sdílený kanál, velké přenosové rychlosti
- v jednom okamžiku se na médiu nachází jen jeden paket

Sběrnice (BUS)



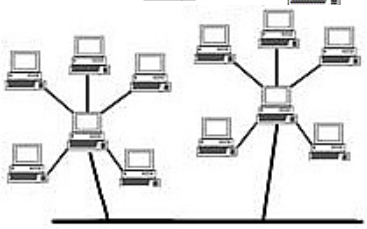
- spojení zprostředkovává jediné přenosové médium, ke kterému jsou připojeny všechny uzly sítě
- když chtějí vysílat dvě stanice ve stejný okamžik, nastává kolize, což je častý jev, proto se používá např. CSMA
- má nízké pořizovací náklady - vhodná pro malé nebo dočasné sítě, které nevyžadují velké rychlosti přenosu
- pokud nastane nějaký problém s kabelem, celá síť přestane fungovat, výkon rapidně klesá při vyšším počtu stanic a provozu

Hvězda (STAR)



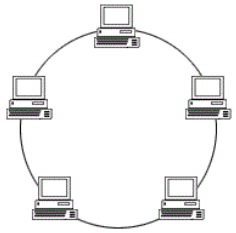
- nejpoužívanější způsob propojování počítačů do počítačové sítě
- centrálním prvkem je hub nebo switch, mezi každými dvěma stanicemi existuje vždy jen jedna cesta
- při zkolabování centrálního prvku zkolabuje celá síť, pokud vypadne jedna stanice, síť to neovlivní
- snadno se nastavuje a rozšiřuje, jednoduše nalezitelné závady

Strom (TREE)



- vychází z hvězdicové topologie spojením aktivních síťových prvků, které jsou v centrech jednotlivých hvězd
- pokud selže jeden aktivní síťový prvek, ostatní podsítě stromu mohou dále pokračovat
- zvýšení bezpečnosti – zvyšuje se obtížnost odposlouchávání síťové komunikace

Kruh (RING)



- stanice tvoří logický kruh (fyzicky hvězda), nevznikají kolize, nejvyšší průchodnost sítě
- stanice si dokola předávají token, který držiteli umožňuje vysílat, jinak pouze naslouchají
- výpadek jednoho uzlu ochromí celou síť, proto se používá např. FDDI – záložní kruh

WAN

- rozlehlé sítě, nižší přenosové rychlosti
- v jednom okamžiku se na médiu nachází více paketů
- polygonální, linky bod – bod mezi routery, k jednotlivým routerům jsou připojeny různé podsítě
- alternativní cesty

Přenosová média

Metalická

- **Koaxiál** – asymetrické, drahé, kvalitní, jeden vnější válcový vodič, jeden drátový nebo trubkový vnitřní vodič
  - Základní pásmo: 0-150 MHz (bez použití modulace)
    - elektrické vlastnosti omezují maximální vzdálenost na stovky metrů, 50 Ohm
  - Přeložené pásmo: 50-750MHz (s použitím modulace)
    - lze překlenout vzdálenosti řádově jednotky km, CATV kabely (75 Ohm)

- **Twisted Pair** – symetrické, levné, méně kvalitní, v kabelu 4 kroucené páry, vzájemně opět zkrouceny
  - parametry výrazně horší než koaxiální kabel, na rozdíl od něj nedokáže dělat odbočky (pouze dvoubodové spoje)
  - použití typicky v základním pásmu v LAN dosah 100m při přenosových rychlostech do 1Gbps
  - přenosová rychlost podle kvality kabelu (kategorie)
    Kategorie 1 – telefonní a modemové linky
    Kategorie 2 – 4 Mhz, starší terminály
    Kategorie 3 – 16 MHz (10 Mbps), většinou telefonní rozvody
    Kategorie 4 – 20 MHz (16 Mbps), málo rozšířené
    Kategorie 5 – 100 MHz (100 Mbps), původně Fast Ethernet
    Kategorie 5+ – dodefinovává parametry (FEXT, ...)

Radiová

- přenos vzduchem či vakuem

Optická

- vysoká přenosová kapacita (desítky Gbps), dosah vyjádřen součinem Mb/s*km
- odolnost proti rušení, odposlechu

- **Multimode (vícevidová)**
  - komunikace na krátké vzdálenosti, jako například uvnitř budovy nebo areálu
  - rychlost přenosu u vícevidových linek se pohybuje okolo 10 Mbit/s až 10 Gbit/s na vzdálenosti do 600 metrů
  - je levnější než singlemode, šířka jádra je 50 - stovky mikrometrů

- **Singlemode (jednovidová)**
  - přenos dat na větší vzdálenosti (mezi městy, státy, kontinenty)
  - singlemode je náchylnější na ohyby, protože dochází k disperzi (rozptylu)
  - je to tím, že vlákno je cca 8-10 mikrometrů široké (to vede k menšímu prodloužení dráhy paprsku)

Multiplexování

- proces, ve kterém je více analogových signálů nebo digitálních datových toků kombinováno do jednoho signálu

- **Frekvenční multiplex**
  - použití v páteřních WAN spojích a sítích FTTC
  - použité frekvence a jejich počet pevně dán
  - obvodovým řešením (analogové obvody) problém neúplného využití pásma vlivem nutnosti odstupu pásem
  - efektivní pro fixní počet uživatelů, z nichž každý kanál pokud možno plně využije

- **Časový multiplex**
  - sloty organizovány do periodicky se opakujících rámců
  - nutnost synchronizace (bitové i rámcové)
  - dnes používanější

- **Statistický multiplex**
  - Většina přenosů počítačového charakteru má shlukový charakter, takže je neekonomické vyhradit konstantní přenosovou kapacitu pouze pro jediný kanál. Poměr zatížení špička-průměr i (1000:1)
  - nevýhodou synchronního TDM je pevné přidělení slotů
  - neodpovídá nárazovému charakteru požadavků stanic
  - řešením statistický časový multiplex (ATM) pomocí inteligentního multiplexeru a označování dat v timeslotech hlavičkami určujícími příslušnost ke kanálu
  - na médiu kontinuální proud buněk (cells)

Strukturovaná kabeláž

- je obecné označení metalických a optických prvků, které umožňují propojení jednotlivých uživatelů v rámci počítačové sítě
- podporuje přenos digitálních i analogových signálů
- u něhož se přípojné body instalují i tam, kde momentálně nejsou potřeba
- používáno UTP a optika, předpokládaná dlouhá technická i morální životnost

3. Metody sdílení přenosového kanálu

Klasifikace přístupových metod

- přístupová metoda má za úkol zamezit kolizím při jednotlivých přístupech stanic k přenosovému kanálu

- **Deterministické (bezkolizní)**
  - je definován jednoznačný algoritmus určující, v jakém pořadí mohou stanice na kanál přistupovat
  - na kanál nebude nikdy přistupovat více stanic současně
- **Nedeterministické (kolizní)**
  - v algoritmu přístupu na kanál hraje roli náhoda – náhodně volené časové prodlevy
  - o přístup na kanál se může pokusit více stanic současně – kolize, přístupová metoda musí kolize řešit

Nedeterministické

- **Kolizní slot**
  - udává, kolik času se nejvýše ztratí na nevyužití kanálu vlivem kolize
- **Aloha**
  - netestuje se obsazenost média, rovnou se vysílá
  - kolize nastane, pokud do časového limitu nepřijde potvrzení -> opakování pokusu po vypršení limitu
  - použití: radiové a družicové sítě
- **Taktovaná aloha**
  - vysílat se smí začít jen v okamžicích začátků časových úseků pro odeslání jednoho rámce
  - kolizní slot je poloviční, dvojnásobná efektivita
- **Řízená aloha**
  - řízená změna intenzity opakování podle okamžitého zatížení sítě
- **CSMA (Carrier Sense Multiple Access)**
  - skupina metod náhodného přístupu s příposlechem nosné vlny
  - podmínky: dokonalá slyšitelnost stanic, malé zpoždění signálu
- **CSMA/CD (CSMA with Collision Detection)**
  - před odesláním rámce se testuje stav kanálu, je-li kanál obsazen, odloží se vysílání na okamžik jeho uvolnění
  - riziko kolize stanic čekajících na uvolnění kanálu - HW musí umožňovat detekci kolize
  - posun SS složky u koax Ethernet, signál na přijímacím páru u TP Ethernet
  - okamžité ukončení vysílání po detekci kolize - kanál se zbytečně nezaplňuje rámcem, který je stejně zkolidován
  - pošle se 32bit kolizní signál (jam) – oznámení kolize všem stanicím
  - po kolizi čekání náhodnou dobu před dalším pokusem (backoff)
- **CSMA/CD v Ethernetu**
  - při detekci kolize stanice vysílá kolizní signál (jam), aby kolizi rozpoznaly všechny kolidující stanice
  - prodleva po kolizi určena algoritmem Binary exponential backoff

Deterministické

- **Token passing**
  - ve stavu klidu, když žádný uzel nevyžaduje právo na vysílání, cyklicky putuje mezi uzly rámec Token (vysílací právo)
  - libovolný počítač sítě může začít s vysíláním údajů, až když získá toto vysílací právo
  - dvě varianty: metoda se váže k fyzickému kruhu (Token Ring), nebo ke sběrnici (Token Bus)
  - výhodou této metody je, že každý počítač má zaručeno získání vysílacího práva do určitého časového limitu
  - protože údaje jsou přenášeny jen jedním směrem, nedojde ke kolizi jak to je u metody CSMA/CD
  - vhodné pro řízení technologických procesů, kde se vyžaduje řízení v reálném čase.
- **<u>Centralizované řízení</u> (Polling)**
  - jedna stanice je vyhrazena jako řídící a ta přiděluje kapacitu kanálu ostatním
  - část kapacity kanálu obětována na komunikaci s řídící stanicí

    Přidělování na výzvu

    - **s**tanice smí vysílat, jen když je k tomu vyzvána centrálním řídicím prvkem (master)

      Cyklická výzva
      - nabízení práv k vysílání
      - vyzývaná stanice buď zašle data nebo neodpoví

      Binární vyhledávání
      - organizace stanic do stromové struktury - řídící stanice vyzývá jednotlivé skupiny stanic (větve)
      - ve větvi se výzva posouvá směrem dolů od kořene dokud neodpoví některá ze stanic na výzvu a bude moci poté vysílat data

    Přidělování na žádost

    - žádosti přicházejí od stanic k řídící stanici po vyhrazených kanálech
    - použití: rádiové sítě

- **Distribuované řízení**
  - nezávislé na řídící stanici, složitější implementace

- **Rezervační rámec**
  - master periodicky generuje rezervační rámec
  - každá stanice má svůj slot, ve kterém si může požádat o přidělení datového slotu
  - datové sloty následují za rezervačním rámcem
- **Binární vyhledávání**
  - stanice nejprve synchronizovaně vysílají bity své adresy
  - vysílané bity se pomocí OR logicky sčítají na sběrnici
  - jakmile stanice vysílá 0 a čte 1, chce vysílat někdo s vyšší prioritou a stanice musí umlknout
  - kdo úspěšně odešle celou svou adresu, může vyslat jeden rámec
- **Logický kruh**
  - adresy stanic tvoří cyklickou posloupnost
  - každá stanice zná svou adresu a adresu následníka
  - mezi stanicemi se cyklicky předává právo na vysílání (token)
  - stanice vlastnící token smí vysílat, do určité doby však musí předat token následníkovi

4. Zabezpečení dat při přenosech, potvrzovací schémata, linkové protokoly

Zabezpečení dat při přenosech

- **Komunikace bez spojení**
  - vysílač může pakety a rámce zasílat střídavě různým příjemcům
- **Komunikace se spojením**
  - nutnost zřízení spojení mezi vysílačem a přijímačem
  - po dokončení vysílání zrušení spojení
- **Kanál**
  - jednosměrný, popř. half-duplex
- **Okruh**
  - obousměrný, dvojice kanálů
- **Problémy při komunikaci v reálné síti**
  - ztrácení a poškozování paketů (nutnost zpětné vazby)
  - duplikace a změna pořadí paketů v síti (předbíhání, nutnost číslování paketů)
- **Typy zpětné vazby**
  - potvrzovací – zpět ACK/NAK
  - detekční – zpět CRC
  - informační – zpět celý rámec
- **Číslování paketů**
  - zajištění správného pořadí paketů a odbourání duplikace paketů

Potvrzovací schémata

- protokoly pro zajištění spolehlivé komunikace dvou stanic

- **Pozitivní (ACK)**
  - potvrzuje správné přijetí
- **Negativní (NAK)**
  - informuje o přijetí rámce s chybou
  - samo o sobě nestačí
- **Kombinace**
  - používá se ACK i NAK
- **Potvrzování s časovým limitem**
  - volba vhodného timeoutu řeší problém ztráty pozitivního potvrzení
- **Klasifikace potvrzovacích schémat**
  - Stop-and-wait – vysílač pošle jediný rámec a čeká na potvrzení
  - Skupinové potvrzování (pipelining) – vysílač smí vyslat více rámců a až poté čekat na potvrzení
- **Metoda Sliding window**
  - stanice smí vyslat i více rámců bez ACK (počet stanoven šířkou okna)
  - při odeslání se pro každý rámec nastartuje časovač pro potvrzení
  - vysílací okno – buffer na vysílači s vyslanými rámci, které dosud nebyly potvrzeny a možná budou muset být vyslány znovu
  - přijímací okno – buffer na přijímači na přijaté rámce, které ještě nemohly být doručeny vyšší vrstvě přijimače, protože dosud chybí některý z předchozích rámců v řadě

- varianty obsluhy chyb
  - Go-Back-N – přijímač všechny rámce po chybném nebo nedoručeném zahazuje
  - Selective Repeat - rámec s chybou došlý na přijímač se zahodí, ale následující se bufferují
- **Inkluzivní potvrzování**
  - efektivnější – odolnost proti ztrátě ACK
- **Řízení toku dat (flow control)**
  - možnost zbrzdit vysílač, pokud aplikace přijímače nestačí odebírat data
  - úprava vysílacího okna na vysílači

Linkové protokoly

- **Přenos dat mezi přímo propojenými systémy**
  - kom. kanál může sdílet více stanic, je třeba umět v bitovém proudu na kanále vydělit jednotku přenášené informace – rámec
  - rámec obsahuje data i hlavičku, která obsahuje: adresu odesílatele a příjemce, sekvenční číslo, typ přenášených dat (IP, IPX)
- **Multicast**
  - příjemcem rámce je celá skupina
- **Broadcast**
  - příjemcem rámce jsou všechny stanice na sdíleném kanále
- **Rámec**

Křídlová značka	Hlavička	DATA	Checksum	Křídlová značka

Znakově (bajtově) orientované protokoly

- vždy přenášeno 5 – 8 bitů naráz = celý jeden znak
- asynchronní sériový přenos, závislé na použité znakové sadě (ASCII, EBCDIC..), řídicí znaky vyhrazeny
- použití: průmyslové řídicí automaty, terminálové systémy

- **Řídicí znaky**
  - začátek vysílání, konec vysílání, začátek rámce, konec rámce, začátek hlavičky, začátek dat, …

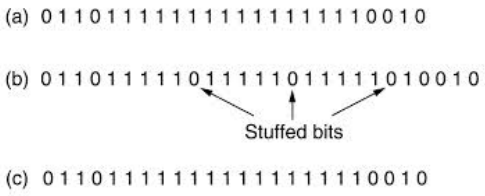
Bitově orientované protokoly

- přenos po jednom bitu, synchronní sériový přenos, běžné v LAN i WAN
- oddělovače rámců: křídlové značky (typicky 01111110), speciální kódová značka

Bit Stuffing

- je způsob, jak vynutit změnu obvykle napěťové úrovně na sériové sběrnici vložením nevýznamového bitu (jednoho či více)
- zajištění synchronizace mezi vysílačem a přijímačem nebo zajištění toho, aby se na sběrnici nevyskytla sekvence bitů se speciálním významem

(a) – původní data před vysláním
(b) – za každých 5 jedniček dodána uměle 0
(c) – nulu po 5 jedničkách přijímač automaticky odstraňuje



Příklady linkových protokolů

- **PPP** – Point to Point Protocol
- **HDLC** – High Level Data Link Control
- **LAPD** – Link Access Procedure – D channel
- **LLC** – Logical Link Control

5. Referenční model ISO-OSI, aktivní prvky a jejich principy

Vrstvená architektura

- výhodami je dekompozice problému komunikace na menší snadněji řešitelné celky
- sousední vrstvy mezi sebou komunikují mezivrstvými protokoly
- každá má svůj vrstvový protokol se kterým komunikuje se stejnou vrstvou na jiném systému

Entity vrstev

- vrstva je tvořena množinou entit, ty (logicky) komunikují s entitami stejnolehlé vrstvy partnerského systému
- entity jsou nositelé funkcí vrstvy a poskytovatelé služeb
- pro vykonávání svých funkcí využívá entita služeb entit v nižší vrstvě

Primitiva interakce mezi uživatelem a poskytovatelem služby

- žádost – žádost o službu nižší vrstvy
- potvrzení – potvrzení poskytovatele služby o dokončení akcí dříve požadovaných primitivou žádost
- oznámení – oznámení poskytovatele služby o vzniklé situaci vedoucí k potřebě vyvolání určité akce na straně uživatele služby
- odpověď – reakce uživatele služby potvrzující ukončení akcí iniciovaných předtím poskytovatelem služby primitivou oznámení

Propojování sítí

- zvětšení rozsahu, propojení jiných oddělených sítí
- oddělení provozu, zmenšení zátěže, bezpečnost

Referenční model ISO-OSI

- obecný vrstvený model
- normy jsou veřejně dostupné
- všechna zařízení vyhovující normám jsou propojitelná

1. **Fyzická**
   - specifikuje fyzickou komunikaci, aktivuje, udržuje a deaktivuje fyzické spoje mezi koncovými systémy
   - definuje všechny elektrické a fyzikální vlastnosti zařízení, kabelů, stanovuje způsob přenosu "jedniček a nul"
   - zařízení pracující na této vrstvě: hub, repeater, modem, síťová karta

   Funkce
   - navazování a ukončování spojení s komunikačním médiem
   - spolupráce na efektivním rozložení všech zdrojů mezi všechny uživatele
   - modulace neboli konverze digitálních dat na signály používané přenosovým médiem (a zpět) (A/D, D/A převodníky)

   Protokoly
   - 10BASE-T, 10BASE2, 10BASE5, 100BASE-TX, 100BASE-FX, 100BASE-T, 1000BASE-T, 1000BASE-SX, radio, Bluetooth, USB, DSL, ISDN

2. **Spojová**
   - poskytuje spojení mezi dvěma sousedními systémy zapojenými na téže lince (switch – PC)
   - topologie fyzické sítě, například síť zapojená jako kruh, sběrnice, hvězda nebo obecný graf
   - podvrstvou jsou MAC (Media Access Control) a LLC (Logical Link Control)
   - zařízení pracující na této vrstvě: NIC- síťová karta, bridge, switch

   Funkce
   - uspořádává data z fyzické vrstvy do logických celků známých jako rámce, formátuje je a opatřuje je fyzickou adresou
   - vytváření, udržování a rušení spojení, rušení toku dat (flow control)

   Protokoly
   - Ethernet, SDLC, HDLC, LAPB

3. **Síťová**
   - stará se o směrování v síti a síťové adresování, poskytuje spojení mezi systémy, které spolu přímo nesousedí
   - cílem je překlenout rozdílné vlastnosti různých síťových technologií a dosáhnout univerzálního rozhraní služby
   - zařízení pracující na této vrstvě: router

   Funkce
   - zahajování a ukončování síťových spojení, síťová služba bez spojení – v internetu (IP)

   Protokoly
   - IP, ICMP, IPX, ARP, RARP, Appletalk, IPSec

4. **Transportní**
   - umožňuje adresovat přímo aplikace (např. V protokolech TCP/IP pomocí čísel portů)
   - poskytuje transparentní, spolehlivý přenos dat s požadovanou kvalitou

Funkce
- vyrovnává různé vlastnosti a kvalitu přenosových sítí
- provádí převod transportních entit v rámci zařízení s jednou síťovou adresou
- mezi dvěma systémy může být několik transportních spojení současně

Protokoly
- TCP, UDP, SCTP, RTP, AMTP, IPX/SPX

5. **Relační**
   - smyslem vrstvy je organizovat a synchronizovat dialog mezi spolupracujícími relačními vrstvami obou systémů a řídit výměnu dat mezi nimi

   Funkce
   - umožňuje vytvoření a ukončení relačního spojení, synchronizaci a obnovení spojení, oznamování výjimečných stavů

   Protokoly
   - SSL, DLC, RPC, NetBIOS, SPDY, SMB, NFS

6. **Prezentační**
   - cílem je sjednotit prezentaci informace, kterou si vyměňují ostatní entity v aplikační vrstvě
   - zabývá se pouze strukturou dat a ne jejich významem, ten je znám pouze vrstvě aplikační

   Funkce
   - transformování dat do tvaru, který využívají aplikace, převod kódů a abeced, modifikace grafického uspořádání
   - přizpůsobení pořadí bajtů a pod.

   Protokoly
   - MIME, XML, TLS, TDI, SMB (Samba)

7. **Aplikační**
   - účelem je poskytnout aplikacím přístup ke komunikačnímu systému a umožnit tak jejich spolupráci
   - předepisuje, v jakém formátu a jak mají být data přebírána/předávána od aplikačních programů

   Funkce
   - logická identifikace komunikujících partnerů, dohoda parametrů funkcí nižších vrstev

   Protokoly
   - SSH, DNS, DHCP, FTP, TFTP, HTTP, IMAP, IRC, POP3, SNMP, SMTP, SIP, LDAP, Telnet, X.400, X.500

- **HUB**
  - 1. vrstva, příchozí paket rozešle na všechny porty vyjma příchozího
- **SWITCH**
  - 2. vrstva, propojuje koncové zařízení, co port, to zařízení
- **ROUTER**
  - 3. vrstva, směruje packet sítí dle cílové IP adresy, ke směrování využívá směrovací tabulky, z nich ví, kudy se k cíli dostane
  - směruje pakety konkrétního síťového protokolu (IP, IPX, ...), pro každy paket najde ve směrovací tabulce, kam jej zaslat

6. Standardy IEEE 802, Ethernet, přepínané sítě, virtuální sítě

IEEE 802
- normalizace aktuálního stavu lokálních sítí, definuje fyzickou a spojovou vrstvu

Vztah IEEE 802 a RM OSI
- spojová vrstva dělená na:
  - MAC – Media Access Control (různá pro různé sítě), sdílení přístupu ke společnému kanálu
  - LLC – Logical Link Control (společná), definuje služby, které síť poskytuje

MAC adresy
- MAC adresa přiřazena každému fyzickému připojení k síti
- délka adresy je 48 bitů
- první bit adresy: 0 – individuální, 1 – skupinová
- druhý bit adresy: 0 – univerzálně, 1 – lokálně
- samé jedničky v adrese = broadcast
- samé nuly v adrese = testovací a prázdné rámce

  Rámce
  - přenášeny po oktetech

LLC vrstva
- definuje služby, které síť poskytuje
- umožňuje adresaci entit, v rámci stanice (SAP – Service Access Points)

Funkce LLC

- error-control, flow-control
- poskytuje společné rozhraní síťové vrstvě

Typy služeb poskytovaných LLC

- nespojovaná služba nepotvrzovaná - nejrozšířenější, není flow control a error control, detekci chyb a zahazování chybných rámců řeší MAC vrstva
- spojovaná služba - služba s navazováním logického spojení mezi SAP, korekce chyb, flow control, sekvencování rámců
- nespojovaná služba s potvrzováním – nejméně využívaná

Obsah hlavičky LLC

- umístěná na začátku datové části rámce MAC vrstvy
- DSAP – Destination Service Access Point (cílová služba, 1B)
- SSAP – Source Service Access Point (zdrojová služba, 1B)
- řízení (1 – 2B)
- uživatelská data

Enkapsulace SNAP (SubNetwork Access Protocol)

- mechanismus pro použití dříve zavedených dvoubajtových kódů protokolů vyšších vrstev
- je-li DSAP=AAh, řízení=AAh, jde o tzv. SNAP enkapsulaci

Doporučení pro nejdůležitější typy sítí

- 802.3 – Sítě CSMA/CD (Ethernet)
- 802.4 – Token Bus
- 802.5 – Token Ring
- 802.6 – MAN DQDB (Dual-queue Data Bus)
- 802.11 – bezdrátové lokální sítě
- 802.14 – sítě HFC (Hybrid Fiber Coax)
- 802.15 – Bluetooth

Doporučení 802.1

- definuje transparentní mosty a mosty s explicitním směrováním
- definice spanning tree (802.1d)
- definice virtuální sítě VLAN (802.1q)
- priorita provozu (802.1p)

Ethernet

- **Dle normy EIA/TIA 568A/B**

Označování podle IEEE 802.3

- Mbps (10, 100, …) [Base, Broad] [délka_segmentu v m | médium] (médium: T – Twisted pair, F – Fiber optic)
- např. 10Base5, 10BaseT, 100BaseF

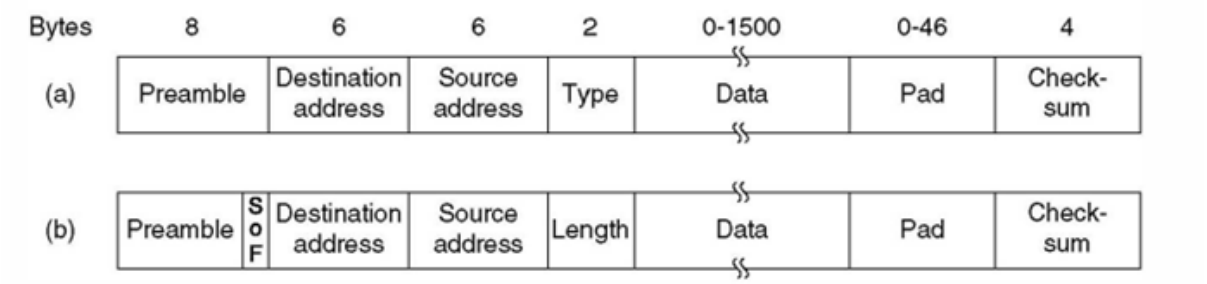
Režimy

- Half-duplex – kolizní prostředí
- Full-duplex – nekolizní přepínané prostředí

Dohoda duplexu a rychlosti

- FLP (Fast Link Pulses) – stanice se mezi sebou dohodnou na rychlosti a na režimu

Formát rámce Ethernetu



a) DIX
b) 802.3

- délka max. 1500B
- povinná mezera mezi rámci dělá 96 bitových intervalů

Preamble

- slouží k synchronizaci hodin příjemce

Type/lenght

- pro Ethernet II je to pole určující typ vyššího protokolu
- pro IEEE 802.3 udává délku pole dat

Data

- pole dlouhé minimálně 46 a maximálně 1500 oktetů (46 – 1500B); minimální délka je nutná pro správnou detekci kolizí v rámci segmentu

Pad

- vyplní zbytek datové části rámce, pokud je přepravovaných dat méně než 46B

Checksum

- kontrolní součet, kontroluje správnost dat, ze všech polí kromě Preamble a FCS

Varianty Ethernetu

10Base5

- Ethernet 2
- sběrnice
- koax – yellow cable
- segment 500m ukončený terminátory (max. 5 segmentů)
- max. 100 stanic/segment
- kódování Manchester

10Base2

- CheaperNet
- sběrnice
- koax – RG58
- segment 185m ukončený terminátory
- max. 30 stanic/segment, oddělené 0.5m
- propojeni BNC konektory

10BaseT

- topologie hvězda (strom)
- 2 páry TP + konektory RJ-45
- použití hubů
- max. 512 stanic/segment
- přípoj k rozbočovači max. 100M
- křížení kabelu přijímače na vysílač

100Mbps (Fast Ethernet)

- IEEE 802.3u
- vychází z 10BaseT
- 2 páry UTP-5, 100m
- kódování 4B5B

Gigabit Ethernet

- 802.3z
- topologie hvězda
- dnes použití pro přepínané páteřní rozvody

  Fyzická vrstva GE
  - přejatý ANSI Fibre Channel – poskytuje rychlosti 133Mbps až 1Gbps
  - 1000Base-SX – short wavelength (850 nm)
  - 1000Base-LX – length wavelength (1300 nm)
  - 1000Base-T

10 Gigabit Ethernet

- optika
- full-duplex
- i ve WAN

VLAN

- na jednom přepínači více vzájemně oddělených sítí (virtuálních)
- může být i přes více přepínačů
- oddělení logické struktury sítě od fyzické topologie
- zvýšení bezpečnosti

  Trunk linka
  - slouží k provozu více VLAN mezi přepínači
  - lze specifikovat, které VLAN smějí linkou trunk procházet
  - VLAN ID je v datové části paketu

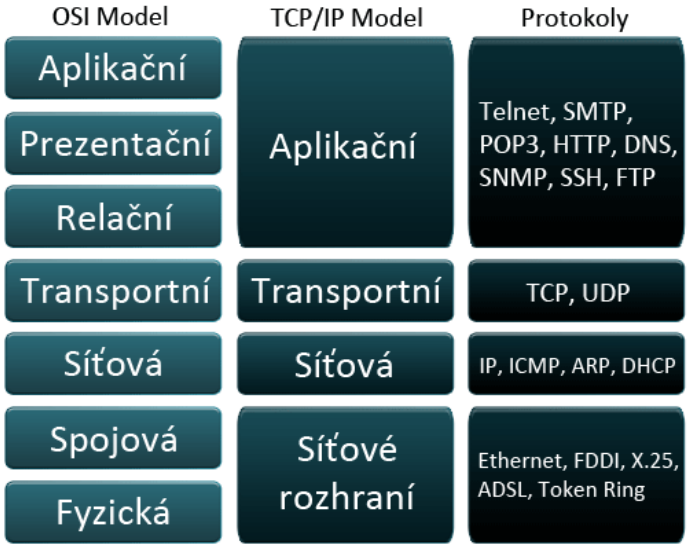
  Členství ve VLAN
  - staticky – podle portu
  - dynamicky – podle MAC adresy

7. Protokoly TCP/IP

TCP/IP

- standard pro komunikaci v internetu a v intranetu
- TCP – protokol 4. vrstvy
- IP – protokol 3. vrstvy

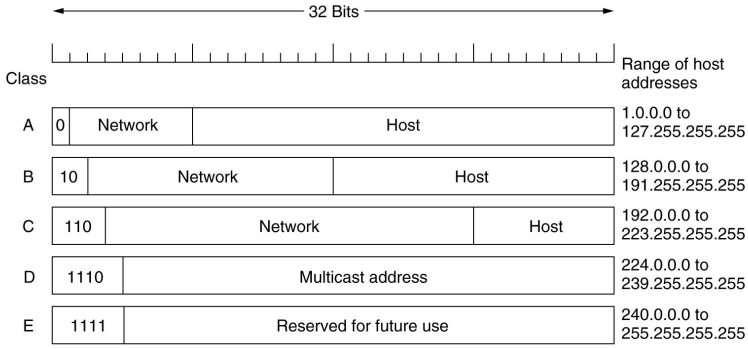
Vrstvený model TCP/IP



Adresace v protokolu IP

- 32 bit adresy (x.x.x.x)
- dělení na adresu sítě + adresa uzlu v rámci sítě
- adresy všech stanic na segmentu LAN mají společnou část IP adresy (adresu sítě, prefix)
- směrovače ukládají pouze adresy sítí

Třídy IP adres



Beztřídní adresy

- délka prefixu sítě je přidělována podle potřeby
- musí být specifikována maska podsítě, která určuje délku prefixu

Přidělování IP adres

- přiděluje oblastní správce (pro Evropu RIPE)
- soukromé izolované sítě mají vyhrazené rozsahy adres použitelné opakovaně, ale nesmějí být připojeny do internetu, jen přes NAT (překlad adres)
- speciální IP adresy:
  - 255.255.255.255 – univerzální broadcast
  - 224.x.x.x, 239.x.x.x – multicast

Podsíťování (subnetting)

- rozdělení přiděleného adresního prostoru mezi více segmentů
- každý segment má svou vlastní adresu podsítě
- část adresy původně určené pro identifikaci uzlu sítě se rozdělí na adresu „podsítě“ a na adresu uzlu v této podsíti
- **Maska podsítě (subnet mask)**
  - pro každou podsíťovanou adresu nutno udat, kolik bitů zleva představuje síť + subsíť a kolik uzel

- **Použití podsíťování**
  - rozdělení prefixu přidělené délky na daný počet podsítí (zadány maximální počty stanic na segmentech)
  - stanovení maximální délky pevně přiděleného prefixu pro požadovaný počet podsítí a požadované počty stanic na jednotlivých segmentech
  - vytvoření adresního plánu sítě WAN

Network Address Translation (NAT)

- překlad zrojové nebo cílové IP adresy, probíhá na routeru nebo firewallu
- překlady buď statické, nebo dynamické
- **Statický NAT**
  - překladová tabulka konfigurována staticky (ručně)
- **Dynamický NAT**
  - překladová tabulka vzniká za provozu automaticky
  - adresy se propůjčují z rezervoáru adres (pool)
- **Časové omezení dynamického NAT**
  - aby mohlo N strojů sdílet M adres, mají dynamicky vytvořené záznamy překladové tabulky časově omezenou platnost (timeout od posledního použití)
  - při odstranění expirované položky se veřejná adresa vrátí zpět do poolu
- **Port Address Translation (PAT)**
  - ukrytí více stanic za jedinou IP adresu, rozlišení podle více zdrojových portů
  - přidělováno dynamicky

Protokol IP

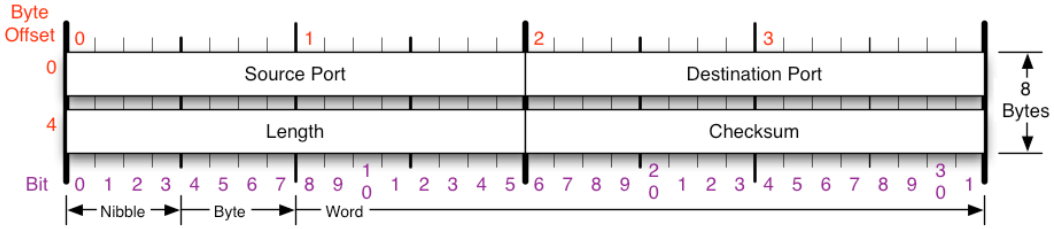
- Internet Protocol
- 3. vrstva, síťová služba posílání nezávisle směrovaných paketů bez vytvořeného spojení

- **Fragmentace paketů**
  - rozdělení paketů při průchodu linkami s nedostatečným MTU (Maximum Transmission Unit)
  - podle konvence musí každý segment internetu být schopen přenést paket o délce **576**B pro IPv4 a **1280**B pro IPv6
- **Podpůrné protokoly IP**
  - ARP – Address Resolution Protocol, mapování IP na MAC
  - ICMP – Internet Controll Message Protocol, ohlašování chyb a zvláštních stavů při přenosu paketů
- **Traceroute**
  - zjišťování cesty sítí a zjištění všech směrovačů na cestě k cíli, zvyšování hodnoty TTL

UDP

- nepotvrzovaná datagramová služba, podpora broadcastu a multicastu (na rozdíl od TCP)

Pseudohlavička UDP



Source port

- identifikuje port odesilatele a zároveň port, na který má přijít odpověď, pokud je to potřeba – pokud ne, hodnota je 0

Destination port

- identifikuje port příjemce, povinná hodnota

Length

- specifikuje délku UDP hlavičky v bajtech, minimální délka je 8B (délka hlavičky) + data, povinná hodnota

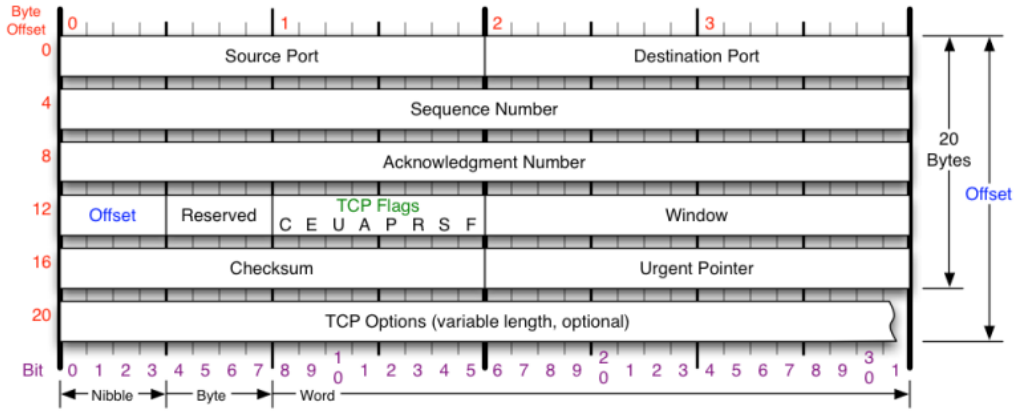
Checksum

- využíváno pro chybovou kontrolu hlavičky a dat, nepovinná hodnota (pouze pro IPv4)

TCP

- duplexní spolehlivý logický kanál, segmentování dat, algoritmus Sliding Window, protokol pro navazování a ukončování spojení

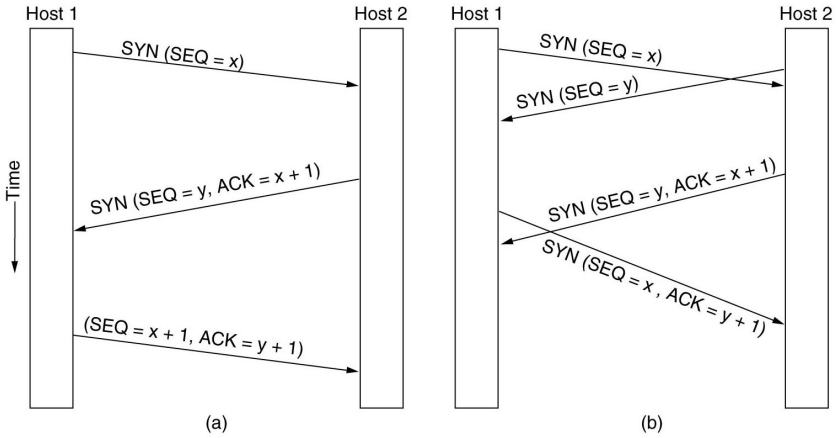
TCP pseudohlavička a její položky



Source Port (4B)
port procesu generujícího datagram
Destination Port (4B)
určuje kterému procesu na cílovém uzlu jsou data určena
Sequence Number (8B)
sekvenční číslo prvního datového oktetu v segmentu
Acklnowledgement Number (16B)
má význam pouze když je nastaven kontrolní bit ACK
Data Offset (16B)
indikuje kde v segmentu začínají data přenášená tímto datagramem
Reserved (3B)
rezervované pole, které by mělo být vždy nulové
Control Bits (13B)
kontrolní bity zajišťující handshaking a ostatní specifické procesy
Window (8B)
množství dat v oktetech, které je potvrzováno najednou
Checksum (8B)
kontrolní součet, není povinný a v tom případě je 0
Urgent Pointer (16B)
údaj je platný pouze pokud je nastaven příznak URG
Options (32B)
pole proměnné délky které je určeno pro volitelné parametry TCP
Padding (32B)
specifické množství nulových bitů doplňujících hlavičku tak, aby měla 32 bitovou hranici (tj. Aby byla beze zbytku dělitelná 32)

Navazování TCP spojení

- tzv. three-way handshake



Uzavírání TCP spojení

- uzavírá se zvlášť z obou stran, **FIN** + **ACK** u obou stran
- příznak **RST** vynucuje ukončení spojení v obou směrech

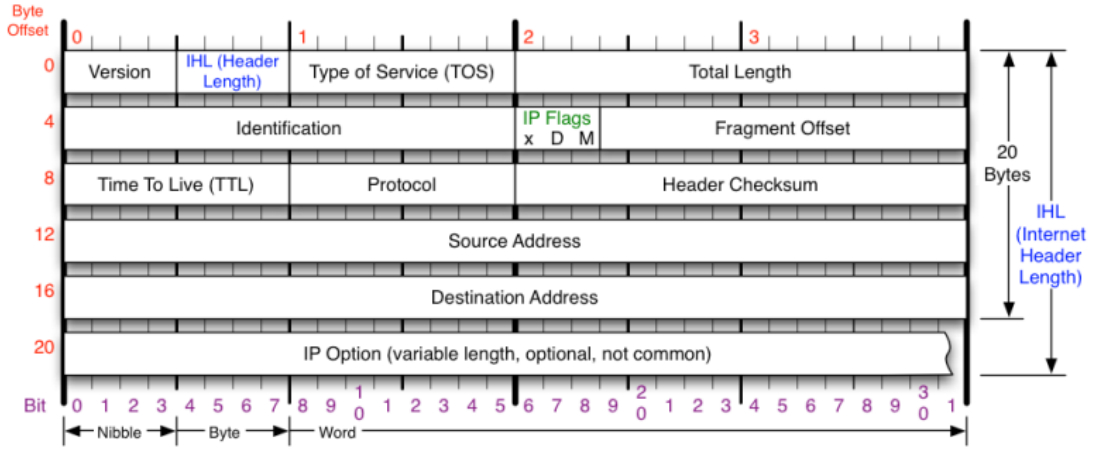
Porty

- spolu s IP adresami identifikují konkrétní proces na konkrétním zařízení v internetu (16 bit)
- uvádíme zdrojový i cílový, aby mohla služba při zpětné komunikaci adresovat na správný port

ICMP zprávy

- echo request, echo reply
- destination unreachable
- time exceeded
- redirect
- parameter problem

Hlavička IPv4



Version (4B)
označující verzi, specifikující, jestli se jedná o IPv4 nebo IPv6 paket
IHL (4B)
označující délku hlavičky vynásobenou 4
Type of Service (8B)
označující typ služby (Type of Service)
Total length (16B)
označující délku paketu v bytech
Identification (16B)
označující identifikační tag pomáhající k rekonstrukci paketu z více fragmentů
DF, MF (3B)
příznak označující zda je možno paket fragmentovat (DF: Don't Fragment, MF: More Fragments)
Fragment offset (13B)
označujících offset fragmentu
Time to live (8B)
označují, přes kolik směrovačů může paket projít, než bude zničen
Protocol (8B)
označující protokol (ICMP, UDP, TCP, …)
Header checksum (16B)
obsahující kontrolní součet CRC
Source address (32B)
obsahující zdrojovou IP adresu
Destination address (32B)
obsahující cílovou IP adresu

Hlavička IPv6

Version (4B)
obsahuje konstantu 6 (bitová sekvence 0110)
Traffic Class (8B)
umožňuje specifikovat požadavky na vlastnosti sítě
Flow Label (20B)
identifikuje tok – proud datagramů od odesilatele k cíli se stejnými vlastnostmi – mělo by usnadňovat směrování
Payload length (16B)
délka přenášených dat
Next Header (8B)
identifikace typu další hlavičky
Hop Limit (8B)
maximální počet směrovačů, kterými datagram smí projít, než bude zničen (analogie TTL z IPv4)
Source Address (128B)
obsahující zdrojovou IP adresu
Destination Address (128B)
obsahující cílovou IP adresu

Porovnání IPv4 a IPv6

- délka adresy v IPv4 je **32** bitů, délka adresy v IPv6 je **128** bitů
- IPv4 header obsahuje **12** prvků, IPv6 header pouze **8** prvků, délka IPv4 hlavičky je **20B**, délka headeru IPv6 je **40B**
- IPv6 se snaží, aby nedocházelo k fragmentaci (když už, může fragmentovat pouze zdroj), IPv6 nemá broadcast (pouze multicast)
- součástí IPv6 je protokol pro IP vrstvu šifrování a autentizaci, IPv6 může mít daleko větší velikost paketu, IPv6 nemá checksum
- multicast je součástí základní specifikace IPv6, na rozdíl od IPv4

Koexistence IPv4 a IPv6

- statické a dynamické tunelování, rozsah IPv4 adres je považován za podmnožinu rozsahu IPv6

8. Směrování a směrovací algoritmy

Sítě s přepínáním okruhů

- vyvinuto z telefonních sítí
- přenosová kapacita rezervována po celou dobu existence okruhu
- při výpadku a rozpadu okruhu nutno žádat síť o nové vytvoření okruhu

Sítě s přepínáním paketů

- vyvinuto v rámci vojenského projektu ARPA
- polygonální struktura s redundantními spoji založena na směrovačích
- datová jednotka – paket – se předává mezi směrovači
- předávání paketu skok po skoku („hop by hop“)

Virtuální kanál

- vytvoření logického okruhu nad sítí s přepínáním paketů
- všechny pakety jdou stejnou cestou – nemohou se přeházet do nesprávného pořadí

Směrovací algoritmy

- část software 3. vrstvy OSI RM rozhodující, kterým rozhraním se má odeslat příchozí paket, nebo kudy zřídit požadovaný (virtuální) okruh
- implementován obvykle s použitím směrovací tabulky

  Směrovací tabulka
  - záznamy ve tvaru **< cílová adresa (+maska), výstupní rozhraní / next_hop, metrika >**
  - jako cílová adresa může být uvedena síť, podsíť nebo uzel

Přístupy ke směrování

- **Centralizované směrování**
  - v síti existuje centrální prvek RCC (Routing Control Center), který shromažďuje informace o okolí od všech směrovačů, kombinuje z nich topologii sitě, počítá směrovací tabulky pro všechny směrovače a předává jim je
- **Distribuované směrování**
  - každý směrovač zná "vzdálenost" (ceny linek) ke všem svým sousedům a stav těchto linek
  - každý směrovač si vyměňuje své informace o směrování s jinými směrovači
  - ze získaných informací si směrovač vytvoří směrovací tabulku
- **Izolované směrování**
  - založeno pouze na lokálně dostupné informaci
  - pouze pro speciální účely

Typy směrování

- neadaptivní – statické
- adaptivní – dynamické (mění se podle okamžité topologie sítě, okamžitého zatížení jednotlivých částí sítě)
- **Statické směrování**
  - směrovací tabulky konfigurovány ručně – pracnější, odpadá režie směrovacích protokolů
  - bezpečnější, při výpadku linky nutný ruční zásah
  - použitelné, pokud se topologie sítě často nemění (intranety)
- **Dynamické směrování**
  - automaticky reaguje na poměry v síti
  - nutnost provozu směrovacích protokolů
  - použitelné při častých změnách (typicky internet), příklad DVA a LSA
- **Hiearchické směrování**
  - rozdělení sítě do hierarchicky rozdělených celků
  - směrovače v jednotlivých celcích znají jen topologii svého celku

DVA – Distance Vector Algorithm

- směrovače neznají topologii sítě, pouze rozhraní, přes která mají posílat pakety do jednotlivých sítí a vzdálenosti k těmto sítím
- na začátku směrovací tabulka obsahuje pouze přímo připojené sítě – staticky nakonfigurováno administrátorem
- z došlých směrovacích tabulek sousedů a výběrem nejlepší cesty si směrovač postupně upravuje svou směrovací tabulku
- zátěž od broadcastu celých směrovacích tabulek, pomalá konvergence při změnách topologie
  - **RIP** – Routing Information Protocol, **IGRP** – Interior Gateway Routing Protocol

LSA – Link State Algorithm

- směrování na základě znalosti "stavu" jednotlivých linek sítě (funkčnost, cena)
- směrovače znají topologii celé sítě a ceny jednotlivých linek, neustále sledují stav a funkčnost k nim připojených linek
- každý směrovač počítá strom nejkratších cest ke všem ostatním směrovačům pomocí Dijkstrova algoritmu
- při změně (pouze při ní) okamžitě šíří informaci o aktuálním stavu svého okolí všem ostatním směrovačům
  - **OSPF** – Open Shortest Path First, **IS-IS**, ISO standard koncepčně podobný OSPF

VLSM (Variable-Length Subnet Mask)

- dovoluje v podsítích jedné sítě používat více rozdílných masek podsítí

9. DNS

Domain Name System
- mapování logických jmen na IP adresy

Doménová jména
- hierarchická struktura jmenného prostoru
- doménové jméno vytvořeno spojením jména uzlu stromu se všemi jmény uzlů na cestě ke kořeni
- oddělovačem tečka, délka komponenty max. 63 znaků, celkově max. 256 znaků

Sekundární a primární DNS servery
- sekundární servery periodicky testují u primárního, zda mají aktuální verzi DB, pokud ne, vyžádají transfer databáze od primárního serveru

Resolver
- část SW klienta, který provádí komunikaci s DNS serverem

Záznamy databáze DNS
- mají univerzální formát
  - doménové jméno
  - typ záznamu
  - data proměnné délky
  - time-to-live – doba, po kterou se záznam smí držet v cache klientů

Reverzní domény
- mapování IP na doménová jména

Dynamická DNS
- umožňuje dynamické registrování IP adres k doménovým jménům
- užitečné při DHCP, problém s autentizací

10. Protokoly služeb internetu

Emulace terminálu
- **Telnet**
  - emulátor terminálu přes síť (TCP/23)
- **SSH**
  - obdoba Telnetu, ale provoz je šifrován
  - asymetrická kryptografie
  - postaveno na šifrovací spojově orientované službě vrstvy SSL

Přenos souborů
- **FTP – File Transfer Protocol**
  - obousměrný přenos souborů mezi dvěma systémy s autentizací uživatele
  - přenášená data chápána jako soubor
  - nad TCP
  - vrací 3místný kód – odpovědi na příkazy
    - aktivní režim – datové spojení navazuje server
    - pasivní režim – datové spojení navazuje klient, bezpečnější
- **TFTP – Trivial FTP**
  - nad UDP, používá potvrzovací Stop-And-Wait protokol
  - umožňuje stanicím stáhnout soubor pro start OS ze serveru

Elektronická pošta
- pro odesílání zpráv se používá protokol SMTP, nezávisle na použitém protokolu pro příjem pošty
- bez šifrování, možnost šifrování zabalením do SSL
- textově orientované protokoly
- struktura zprávy – obálka, hlavička, tělo

- **SMTP – Simple Mail Transfer Protocol**
  - pro odesílání elektronické pošty pomocí přímého spojení mezi odesilatelem a adresátem, TCP/25
  - zpráva je doručena do poštovní schránky adresáta, ke které může (i offline) přistupovat
  - může navazovat TCP spojení s jiným SMTP serverem
  - při průchodu zprávy vloží hlavičku Received určující, že zpráva prošla
  - příkazy orientovány textově, nešifrováno, neautentizováno
    - MUA – Mail User Agent, poštovní klient, který zpracovává zprávy u uživatele
    - MTA – Mail Transfer Agent, server, který se stará o doručování zprávy na cílový systém adresáta
    - MDA – Mail Delivery Agent, program pro lokální doručování, který umisťuje zprávy do uživ. schránek, případně je může přímo automaticky zpracovávat
- **MIME – Multimedia Internet Mail Extension**
  - možnost strukturovat tělo zprávy a určení interpretace dat
  - definuje způsob kódování binárních dat
  - podpora zpráv z více částí – multipart
- **POP3 – Post Office Protocol**
  - pro přijímání pošty, ze serveru stahuje všechny zprávy – i ty, které uživatel číst nechce
  - klient – server, port 110
  - nešifrováno, autentizace textem, klient však může šifrovat užitím SSL nebo TLS
- **IMAP – Internet Message Access Protocol**
  - vylepšená verze POP3, práce v online i offline režimu
  - klient – server, port 143
  - podpora složek a přesouvání zpráv mezi nimi, prohledávání na straně serveru
  - stahuje pouze záhlaví zpráv a obsah až v případě, že uživatel chce zprávu přečíst
  - vylepšená autentizace

WWW

- **URL – Uniform Resource Locator**
  - protokol://uživatel:heslo@stroj:port/cesta
- **HTTP – Hypertext Transfer Protocol**
  - klient – server, Port 80
  - návaznost na URL adresy, využívá MIME
  - formát požadavku: příkaz, hlavička, prázdný_řádek, data – obsah formuláře
  - formát odpovědi: odpověď – stavový kód, hlavička, prázdný_řádek, data – obsah www stránky
  - příkazy: POST, PUT, GET, HEAD, DELETE, LINK, OPTIONS, TRACE

  HTTP 1.0
    - spojení iniciuje klient, ukončuje server po odeslání odpovědi, pokud má stránka více dokumentů, posílají se zvlášť po samostatných spojeních

  HTTP 1.1
    - klient může požádat o podržení TCP spojení po vyřízení požadavku serverem, podpora Virtual Hosts (více logických serverů se stejnou IP), podpora komprese dat

  HTTPS
    - secure HTTP, skrze SSL
- **BOOTP**
  - konfigurace parametrů protokolu TCP/IP stanice na základě MAC adresy
  - šíří se v UDP broadcastech
- **DHCP**
  - dočasné přiřazování adres IP z poolu volných adres, oproti BOOTP umí přidělit více parametrů
  - pronájem adresy je třeba periodicky obnovovat, lze přidělovat i vždy stejné parametry podle MAC
  - kompatibilita s BOOTP, žádost UDP broadcastem, mimo segment je třeba posílat routerem
    - DHCP Discover – příkaz pro vyhledání DHCP serveru
    - DHCP Request – žádost o adresu

11. Bezpečnost sítí

- **Utajení** – posluchač na kanále datům nerozumí
- **Autentizace** – jistota, že uživatel je tím, za koho se vydává
- **Integrita** – jistota, že data nebyla na cestě zmodifikována
- **Nepopiratelnost** – zdroj dat nemůže popřít jejich odeslání

Symetrický systém

- autentizace – zakódování username klíčem u odesilatele, stejným klíčem dekódování u příjemce + test smysluplnosti jména
- zajištění integrity zpáv – pošle se zpráva + hash

Asymetrický systém

- klíče se generují jako doplňující se pár
- digitální podpisy, odpadá problém s distribucí klíčů
- certifikační autorita – entita, které je důvěřováno vytváří dvojice privátní klíč + veřejný klíč
- mnohem náročnější na výpočty, pomalejší

Zabezpečení na jednotlivých vrstvách OSI

- **L2** – hop-by-hop, neefektivní
- **L3** – nezávislé na médiu/síťové technologii i aplikaci
- **L4** – Secure Sockets Layer (SSL), jen TCP
- **L7** – řeší jednotlivé aplikace

Filtrace provozu

- **bezestavová** – výsledkem vypuštění nebo zahození paketu
- **stavová** – rekontrukce datových toků

Paketové filtry

- **ACL**
  - nejčastěji na rozhraní směrovačů, filtrace podle informací ze síťové a vyšších vrstev
  - reflexivní ACL – automaticky propouští vstupní provoz, který odpovídá povolenému provozu výstupnímu

Stavová inspekce provozu

- **Firewall**
  - oddělují důvěryhodnou a nedůvěryhodnou část sítě
  - hardwarové, softwarové
- **NAT**
  - skrytí vnitřní struktury sítě
- **VPN**
  - virtuální privátní sítě
- **Tunel**
  - virtuální dvoubodové spojení přes sdílenou infrastrukturu
  - nese pakety jednoho protokolu zabalené v jiném protokolu
- **Implementace VPN na 3. vrstvě**
  - Ipsec – architektura pro technickou realizaci tunelů

Útoky na počítačové sítě

- **Denial of Service (DoS)**
  - cílem útočníka je vyčerpání systémových prostředků síťového prvku nebo serveru a jeho zhroucení, nebo změna požadovaného chování
- **Intrusion Detection System**
  - rozpoznává podezřelé vzory komunikace, pracuje na různých vrstvách

12. Vzdálený přístup do počítačových sítí

Možnosti vzdáleného přístupu
- komutované připojení (telefon), trvalé připojení (xDSL, CDMA, GPRS, WIFI)

DCE
- ukončovací zařízení okruhu
- CSU/DSU – pro vyšší rychlosti

DTE – Data Terminal Equipment
- koncové zařízení

Přístup přes POTS
- analogová účastnická přípojka
- přenos v základním pásmu nemožný, potřeba přeloženého pásma
- použití modulace – MODEM – režim komunikace: asynchronní, synchronní

Parametry modemů
- přenosová rychlost, použitelné modulace, podpora komprese, schopnost korekce chyb

MNP – Microcom Network Protocol
- standard pro dnešní asynchronní modemy, pro koncová zařízení neviditelný
- význačné třídy
  - třída 1 – asynchronní, bajtově orientovaný, half-duplex
  - třída 2 – přidává full-duplex
  - třída 3 – synchronní, bitově orientovaný, full-duplex
  - třída 4 – adaptivní změna délky paketu
  - třída 5 – kompresi dat
  - třída 6 – doplňuje Universal Link Negotiation
  - třída 7 – vylepšení kompresního algoritmu
  - třída 9 – vylepšená korekce chyb
  - třída 10 – provoz na nekvalitních linkách

ISDN
- digitální síť s integrovanými službami a přepínáním okruhů
- provoz na původních účastnických vedeních
- **Kanály**
  - B – transparentní bitový tok 64kbps, mezi koncovými zařízeními
  - D – signalizace, mezi koncovým zařízením a ústřednou
- **Typy přípojek**
  - BRI – Basic Rate Interface – 2B+D, zřízení připojení do cca 1 sec
  - PŘI – Primary Rate Interface – 30B+D
- **Vlastnosti ISDN při přenosu dat**
  - orientováno na dočasné okruhy – zpoplatňováno za dobu spojení, výhodné pro krátkodobé spojení
  - možnost rychlého zřízení okruhu
- **Typická použití ISDN**
  - poskytování internetu, propojování geograficky vzdálených LAN pro krátkodobé přenosy dat, záložní cesty

xDSL
- použití stávajících symetrických telefonních metalických kabelů
- jednotlivá účastnická vedení zakončena v ústředně na DSL Access Multiplexeru

ADSL
- rozdělení pásma na subkanály pomocí splitteru
- upstream/downstream frekvenční oblast + oblast pro hlas
- přizpůsobuje skutečnou rychlost kvalitě linky

13. Rádiové sítě

IEEE doporučení

- 802.11 – původní standard, definován pro rychlosti 1 a 2 Mbps
- 802.11a – moc se zde neobjevil (v Evropě) – 5GHz (USA), 6,9,12,18,24,36,48,54 Mbps
- 802.11b – 2,4 GHz (USA, Evropa), rozšiřuje 802.11 DSSS 1,2,5.5 a 11 Mbps
- 802.11g – standardně současně v mobilech atd. 2,4 GHz (USA, Evropa)
- 802.11h – 5 GHz (Evropa dnes), podobně jako u 802.11a, ale vyžaduje dynamické nastavení výkonu a automatický výběr kanálu
- 802.11i – bezpečnost + QoS, QoS přišlo z 802.11e
- 802.11F – rychlý roaming mezi AP, nahrazen 802.11k a 802.11r – rychlý roaming
- 802.11n – 2,4 a 5 Ghz, MIMO, větší šířka pásma (20/40 MHz), rychlost až 144,4 Mbit/s na 20 MHz a 300 Mbit/s na 40 Mhz

ISM – Instrumental Scientific Medicine

- 2,4 GHz, 5GHz
- pro použití uvnitř budov
- odstup kanálů 5 MHz, šířka kanálu pro použití rozprostřeného spektra však je 22 MHz

WIFI

- Ad-hoc – dočasné přímé propojení několika blízkých počítačů
- Infrastruktura – použití přístupového bodu

Architektury realizace bezdrátové sítě

- IBSS – skupina vzájemně komunikujících stanic
- BSS – Basic Service Set – přístupový bod, komunikace přes něj
- ESS – Extended Service Set – propojení přes distribuční systém

Service set

- logická skupina stanic
- SSID – Service Set Identifier, název přístupového bodu

Problémy při šíření signálu

- vícecestné odrazy, problém skrytého uzlu

Autentizace

- následuje po asociaci
- módy
  - open – bez autentizace
  - shared key – se sdíleným klíčem z WEP

Speciální zařízení rádiové infrastruktury

- Repeater – čistě bezdrátový most
- Workgroup bridge – připojuje pracovní skupinu stanic vybavených pouze Ethernetem do WiFi
- Wireless bridge – obdoba workgroup bridge, ale hlavním smyslem je rádiové propojení LAN na větší vzdálenost

Bezpečnost

- autentizace, šifrování
- WEP – sdílený klíč (64, 128 bit)
- WPA, WPA 2 – odstraňuje nedostatky WEP