Počítačové sítě r. 2008/2009

materiál ke zkoušce

autor: losperdos

5.1.2009

obsah:

1. základní principy přenosu dat

podle směru využívání média:

- **simplex** – pouze v jednom směru (tv vysílání)
- **half duplex** – v obou směrech střídavě (vysílačky, ethernet s hub)
- **full duplex** – v obou směrech současně (ethernet se switch)

podle způsobu přenosu bitů znaků:

- **paralelní**
- **seriový** –synchr., asynchr.

asynchronní přenos:

- přenos po znacích (8, 7, 6, 5 bitů) – kvůli nebezpečí rozsynchronizování hodin jen jeden znak
- vysílač i přijímač mají vlastní hodiny
- na konci znaku paritní bit – bezpečnost
- mezi znaky stop bit (1) – pauza, start bit (0)
- menší efektivita
- použití: průmyslové automaty, komunikační porty PC

synchronní přenos:

- přenos po rámcích (hlavička, data o proměnné délce, kontrolní součet)
- synchronizace je udržovaná neustále
- křídlová značka – tak jsou označovány začátky a konce rámců
- použití: ISDN kanály

fyzikální omezení při přenosu dat

médium = prostředí (metalická média, optická, vzduch)

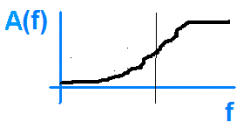
princip přenosu signálu:

vysílač -> data kódována na signál -> signál je modulován -> přenos přes medium ->signál je demodulován -> signál je dekódován na data -> přijímač

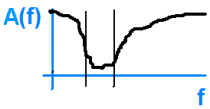
parametry média:

- útlum, rychlost šíření signálu, přeslechy, …
- závislé na frekvenci – proto nejideálnější je použití co nejméně frekvenci měnících prvků

použitelný frekvenční rozsah média:



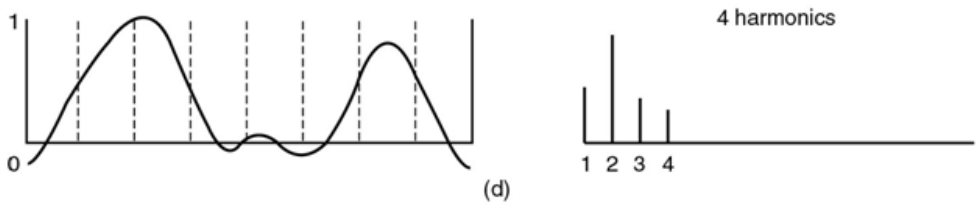
médium se chová jako dolní propust

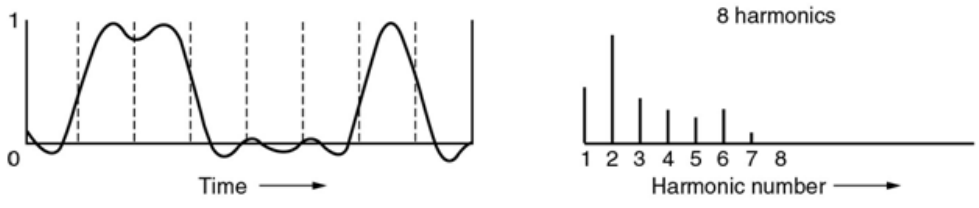


jako pásmová propust

rozklad na harmonické signály:

- harmonický = sinusový





přenos v základním a přeloženém pásmu

a) v základním pásmu:

- baseband
- přenáší se přímo frekvenční spektrum vzniklé zakódováním jedniček a nul
- digitální signál – nepoužívá se modulace
- pro metalická i optická vlákna (omezení dosahu)

kódování:

Non Return to Zero (NRZ):

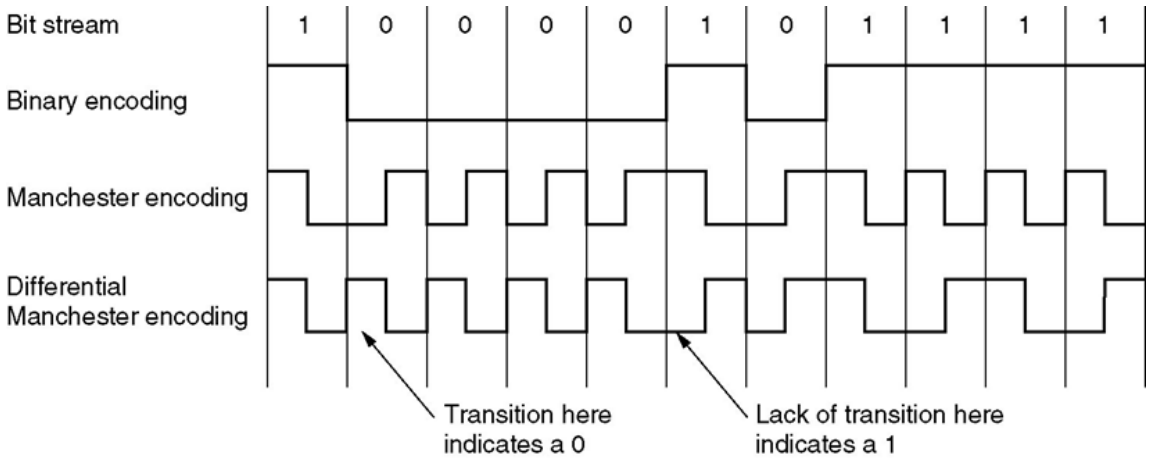
- přímé dvoustavové kódování
- 0 – nízká úroveň, 1 – vysoká úroveň
- pouze stejnosměrná složka

Manchester:

- kódování směrem změny **uprostřed** bitového intervalu
- 0 – sestup signálu, 1 – vzestup signálu
- ethernet, metalické vedení

Diferenciální Manchester:

- kódování změnou nebo absencí změny na **začátku** intervalu
- 0 – změna, 1 – absence změny
- uprostřed intervalu změna vždy



Return to Zero (RZ):
- třístavový
- +1 při kódování binární 1
- -1 při kódování binární 0
- 0 při kódování je vždy uprostřed

Non Return to Zero Inverted (NRZI):
- dvoustavový
- 1 – inverze signálu, 0 – signál zůstává

Alternate Mark Inversion (AMI):
- třístavový
- binární nula je 0
- binární jednička je střídavě +1 a -1
- problém udržet synchronizaci přijímače při dlouhé sekvenci nul

HDB3:
- řeší problém AMI s dlouhou posloupností nul tak, že po dvou nulách vloží jedničku.

Code Mark Inversion (CMI):
- pro přenos AMI/HDB3 přes optiku

4B5B:
- čtyři bity se mapují na bitové kombinace 5 bitů
- použití: Fast Ethernet
- existují i další: **5B6B**, …

---

b) v přeloženém pásmu:
- broadband
- tyto zakódované sekvence jedniček a nul se překládají do frekvenčního pásma kde má médium vhodné charakteristiky
- možnost vícenásobného využití média

<u>modulace:</u>
- zvolíme sinusový signál o frekvenci vhodné pro přenos médiem, měníme jeho parametry v závislosti na přenášených datech (frekvenci, amplitudu, fázi, nebo kombinace)

fázová modulace:
- 2^n možností změny fáze (např. změna o 45, 135, 225, 315 stupňů)

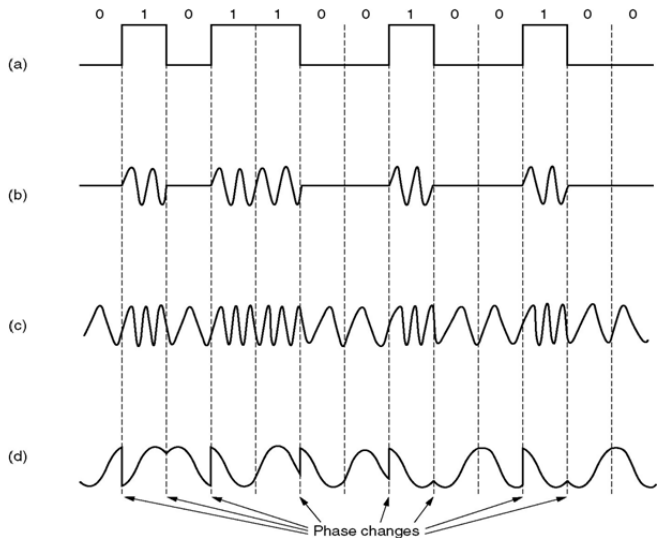
kvadraturně-amplitudová modulace (QAM):
- kombinace fázové a amplitudové modulace

modulační rychlost:
- počet změn v signálu za sekundu[Baud]

přenosová rychlost:
- počet bitů přenesených za sekundu

kontrolní otázky:

- Jaké nepříznivé vlivy působí na signál přenášený médiem ? Jakými fyzikálními vlastnostmi média (metalického, optického) jsou ovlivněny ? Lze je zcela eliminovat ?
- nepříznivě působí např. okolní elektrická zařízení, představují šum v signálu.
- fyzikálně je ovlivněn přenos impedancí metalického média, a optickými zákony v optickém médiu (odraz světla, útlum, …)
- Proč je maximální bitová rychlost přenášených dat u každého reálného přenosového média shora omezena ?
- tato horní rychlost je dána fyzikálními možnostmi daného média. Tzn. např. metalické vedení má svůj strop, na který může navázat optické vedení, které má daleko lepší možnosti
- Proč se při přenosu dat médiem používá modulace ?
- kvůli bezpečnosti (např. kontrolní součty) – abychom zajistili, že se médiem přeneslo vše co jsme chtěli a nic se cestou neztratilo
- Jaké základní typy modulací znáte ? Pro každou z těchto modulací nakreslete nosný signál modulovaný bitovou sekvenci 0101100 (konkrétní parametry modulace si zvolte)
- příklad amplitudové, frekvenční a fázové modulace:



- Proč se při přenosu bitového proudu v základním pásmu používá kódování ? Jaká kódování znáte ? Zakódujte bitovou sekvenci 0101100 v každém z těchto kódování.
- NRZ, NRZI, Manchester, Dif. Manchester, RZ, AMI, CMI, HDB3, 4B5B
- Jaký je rozdíl mezi synchronním a asynchronním sériovém přenosem ?
- asynch. – přenos po znacích, synch. – přenos po rámcích, synchronizace je neustále udržována
- Vysvětlete pojmy simplex, half-duplex a duplex.
- simplex – přenos signálu pouze v jednom směru
- half duplex – v obou směrech střídavě
- full duplex – v obou směrech současně

2. Topologie sítí. Přenosová média. Metody sdílení přenosového média

topologie sítí

sítě LAN a WAN

LAN:
- lokální sítě
- sdílený kanál
- velké přenosové rychlosti
- na médiu v jenom okamžiku jeden paket

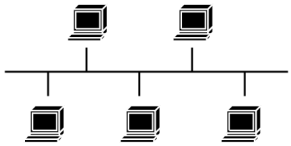
WAN:
- rozlehlé sítě
- nižší přenosové rychlosti
- na jednom médiu současně více paketů

typy sítě:
- token ring – kruhový
- ethernet – stromový, sběrnicový

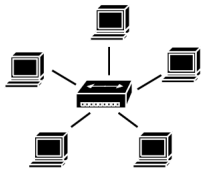
další vlastnosti topologií:
- rozšiřitelnost
- spolehlivost proti výpadkům
- rekonfigurovatelnost při výpadku
- propustnost

a) LAN:

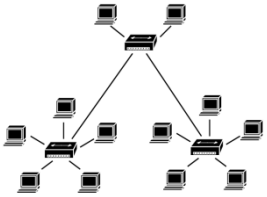
sběrnice (bus):
- pasivní médium
- malézpoždění signálu
- všechny stanice přijímají (špatná bezpečnost)
- T-kusy, terminátory (odpor na konci vedení)



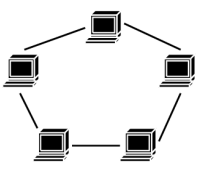
hvězda (star):
- ve středu hub
- odolné proti výpadku stanic



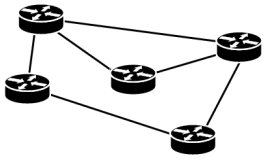
strom (tree):
- rozšíření hvězdy
- nejvyužívanější



kruh (ring):
- jednosměrná dvoubodová propojení stanic
- základní prvek posuvný registr
- citlivé na výpadky
- vysílání se přeposílá přes sousedy



b) WAN



- polygonální
- linky bod – bod mezi routery
- alternativní cesty
- k jednotlivým routerům jsou připojeny různé sítě (viz. výše)

přenosová média

- je využíván sériový přenos z důvodu úspory vedení

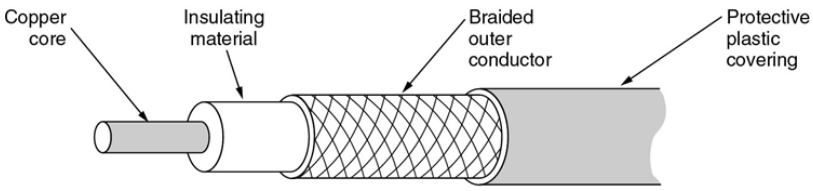
metalická:
- nesymetrická - koax
- symetrická – twist pair

optická:
- jednovidová (singlemode)
- vícevidová (multimode)

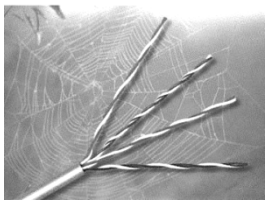
rádiové:
- vzduchem

jednotlivá média:

a) koaxiální kabel:
- pro přenos v zákl. (0 – 150 MHz) i přelož. pásmu (50 – 750 MHz)
- drahé, kvalitní
- 50 Ohm

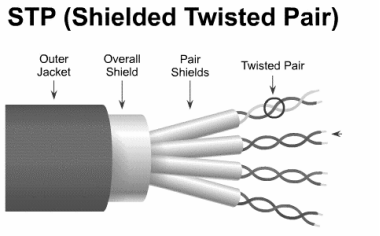


b) kroucená dvojlinka (TP):
- horší parametry než koax, avšak levnější
- 100 metrů při přenosu 1Gbps
- přenosová rychlost podle kategorie TP



UTP:
- nestíněná dvojlinka (unshielded TP)

STP:
- stíněná dvojlinka (shielded TP)



norma EIA/TIA 568:

- kategorie TP

kat. 1 – klasické telefonování
kat. 3 – 16 MHz (10 Mbps)
kat. 5 – 100 MHz (100 Mbps)
kat. 5+ - dodefinovává parametry (FEXT, …)

c) optická vlákna:

- velká přenosová kapacita (desítky Gbps)
- žádné rušení, odposlech

kontrolní otázky:

- Jaké topologie počítačových sítí znáte ? Jaké jsou výhody a nevýhody každé z nich ?
  - hvězda, strom, sběrnice, kruh
- Jaké přenosová média znáte ? Jaké jsou výhody a nevýhody každého z nich ? Jaké médium se dnes nejčastěji používá v lokálních sítích ?
  - metatalické, optické, vzduch
  - koax – drahý, dobré vlastnosti
  - TP – levný, dnes nejvyužívanější v LAN
- Co znamená označení média UTP5 ?
  - nestíněná kroucená dvojlinka kategorie 5
- Jaké dva základní typy optických vláken rozlišujeme ? Jaké jsou výhody a nevýhody každého typu ?
  - jednovidové, vícevidové (singlemode, multimode)
- Vysvětlete pojem "strukturovaná kabeláž".
  - kabeláž je strukturována společně s aktivními prvky podle předem daných pravidel posloupnosti a řazení

3. Metody sdílení přenosového kanálu

klasifikace přístupových metod

deterministické (bezkolizní):
- je definován postup, v jakém pořadí mohou stanice na kanál přistupovat
- v jeden okamžik vždy jen jedna stanice

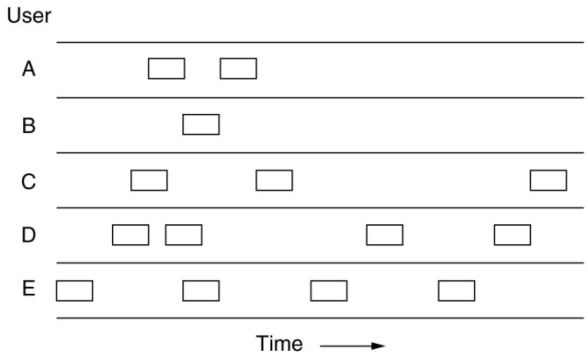
nedeterministické (kolizní):
- náhodný přístup stanice na kanál (náhodné časové prodlevy)
- musí se řešit kolize, pokud na kanál přistoupí naráz více stanic

a) nedeterministické metody

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

prostá Aloha:



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

Carrier Sense Multiple Access (CSMA):
- skupina metod náhodného přístupu s příposlechem nosné
- podmínky: dokonalá slyšitelnost stanic, malé zpoždění signálu

naléhající CSMA (1-persistant CSMA):
- před odesláním rámce se testuje stav kanálu, a je-li obsazen, čeká se na uvolnění
- riziko kolize čekajících stanic

nenaléhající CSMA (non-persistant CSMA):
- při detekci obsazeného kanálu se počká náhodnou dobu, pak opět test obsazení.

řízení metod CSMA:

p – naléhající CSMA (p – persistant CSMA):
- při potřebě vysílání se počká na okamžik uvolnění kanálu (nebo byl volný okamžitě)
- s pravděpodobností p začne vysílat, s pravděpodobností (1-p) se počká 1 timeslot.
- toto se opakuje do úspěšného odeslání rámce
- pokud mezitím začala vysílat jiná stanice, počká se náhodnou dobu (jako při kolizi)
- volbou p lze nastavit optimální využití kanálu pro danou zátěž
- pro p=1 jde o naléhající CSMA
- pro velmi malá p značně narůstá průměrná doba doručení paketu

CSMA/CD:
- CSMA s detekcí kolize
- před vysíláním musí být na médiu klid po dobu kolizního slotu
- další postup je stejný jako u naléhající CSMA

časování CSMA/CD:
- vzájemný vztah mezi: rychlostí šíření signálu na médiu, maximální povolenou délkou segmentu, minimální dobou vysílání rámce

minimální délka rámce:
- Rámec musí být vysílán alespoň takovou dobu, jaká je nejdelší možná doba do zjištění „nejhoršího“ možného případu kolize

maximální délka kabelového segmentu:
- doba šíření mezi nejvzdálenějšími stanicemi je daná délkou segmentu, rychlostí šíření signálu v kabelu
- Tato doba nesmí být delší než doba vysílání nejkratšího možného rámce

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

---

b) deterministické metody

Centralizované řízení
- Přidělování na výzvu
- Přidělování na žádost

Distribuované řízení
- Rezervační rámec
- Binární vyhledávání
- Logický kruh

Centralizované řízení

- jedna stanice je vyhrazena jako řídící a ta přiděluje kapacitu kanálu ostatním
- část kapacity kanálu objetována na komunikaci s řídící stanicí

přidělování na výzvu:

- stanice 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

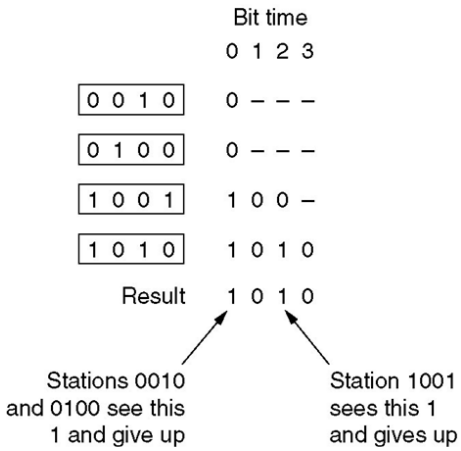
- nezávislé na řídící stanici
- složitější implementace

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 rezeračním 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 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

kontrolní otázky:

- Proč je v lokálních sítích třeba implementovat přístupovou metodu ke společnému kanálu ? Co má přístupová metoda za úkol?
- má za úkol zamezit kolizím při jednotlivých přístupech stanic k přenosovému kanálu
- Vysvětlete rozdíl mezi deterministickými a nedeterministickými přístupovými metodami a jejich výhody a nevýhody.
- nedeterm. – udává časové prodlevy přístupů
- determin. – definuje postup, v jakém pořadí se přistupuje
- Jaké konkrétní deterministické a nedeterministické přístupové metody znáte ?
- Aloha, prostá Aloha, takt. Aloha, …
- centralizované řízení, distrib. řízení
- Vysvětlete princip metod CSMA/CD a Token Passing.
- CSMA/CD - Na rozdíl od čistého CSMA u CSMA/CD stanice při svém vysílání současně kontroluje přenosové médium, zda nezachytí jiné vysílání, které koliduje s jejím. Z této vlastnosti je odvozena přípona „s detekcí kolizí“ (with Collision Detection) v názvu metody. Pokud stanice zjistí kolizi, zastaví vysílání, počká náhodnou dobu a opakuje svůj pokus znovu. CSMA/CD je proto efektivnější než samotné CSMA či CSMA/CA – v nich se kolize nezjišťují a dojde-li k nim, zbytečně se odvysílá celý datový rámec, který bude beztak nutno opakovat.
- Uveďte dvě metody centranizovaného deterministického řízení přístupu na kanál a dvě metody řízení deterministického distribuovaného (nikoli Token Passing)
- centr. – přidělování na výzvu, přidělování na žádost
- distr. – rezervační rámec, binární vyhledávání

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 okruhu 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 vysilači s vyslanými rámci, které dosud nebyly potvrzeny a možná budou muset být vyslány znovu
- přijímací okno - buffer na přijimači 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 přijimač 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:
- komunikační 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

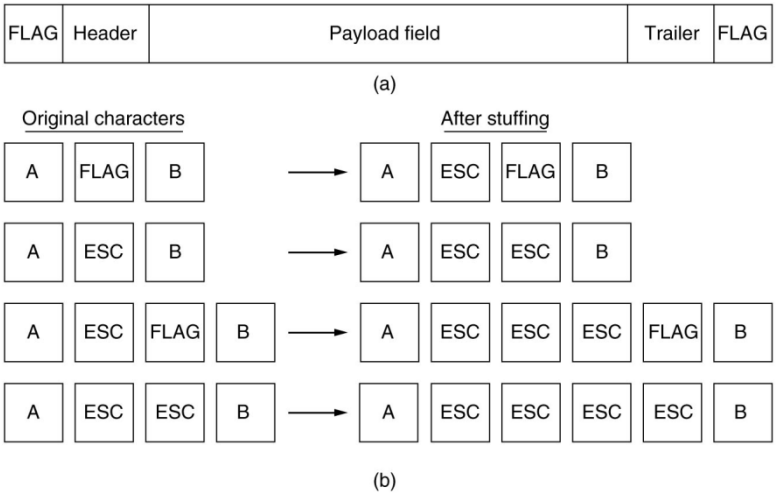
rámec:

křídlová značka	hlavička	DATA	kontrolní součet (checksum)	křídlová značka

a) znakově orientovaně protokoly:
- vždy přenášeno 5, 6, 7, nebo 8 bitů naráz = celý jeden znak
- asynchronní sériový přenos
- použití: průmyslové řídicí automaty

řídicí znaky:
- začátek vysílání, konec vysílání, začátek rámce, konec rámce, začátek hlavičky, začátek dat, …

přenos řídicích znaků v datech:

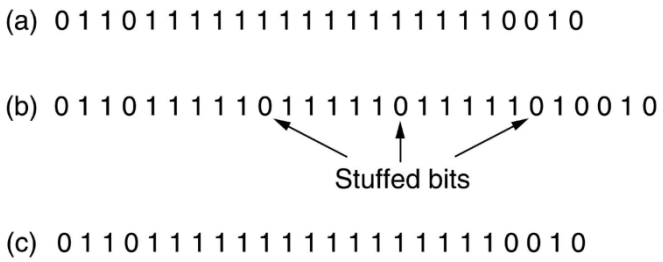


---

b) bitově orientované protokoly:

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

Bit Stuffing:



(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

kontrolní otázky:

- Proč je při přenosu dat v počítačové síti nezbytné potvrzování ? Postačuje samotné pozitivní, resp. negativní potvrzování ?
- kvůli bezpečnosti. Abychom měli jistotu, zda data dorazily v pořádku celá. Negativní potvrzování samo o sobě nestačí.
- Vysvětlete princip potvrzovacích schemat stop-and-wait a skupinového vysílání (pipelining). Za jakých podmínek bude stop-and-wait velmi neefektivnía kdy jej naopak lze použít ?
- 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
- Vysvětlete princip skupinového vysílání s použitím algoritmu klouzavého okénka (Sliding window). Jakou úlohu v něm hrají buffery na straně vysílače a přijímače, potvrzování a časové limity ?

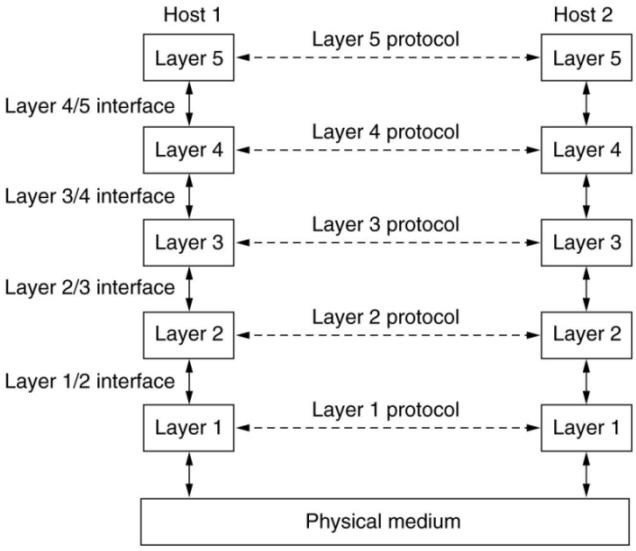
- stanice smí vyslat i více rámců bez ACK (počet stanoven šířkou okna)
- Jaká musí být alespoň velikost vysílacího okna (v počtech paketů) u skupinového potvrzování, pracuje-li se s pakety pevné délky 128B a potvrzeními 8B, bitová rychlost je 64kbps a zpoždění na kanále je 1 ms ?
- velikost vysílacího okna by měla být alespoň 3 pakety
- Proč a kde se používají linkové protokoly ? Jakou obecnou strukturu mívá a jaké údaje zpravidla obsahuje rámec ?
- linkové protokoly se používají na druhé vrstvě k vydělení rámce z bitového toku, obsahuje DATA, hlavičku, kontrolní součet
- Vysvětlete rozdíl mezi bitově a bajtově orientovanými protokoly. Který z těchto typů se používá v sítích LAN ?
- bitově = přenos po jednom bitu, bajtově = přenos po znacích

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

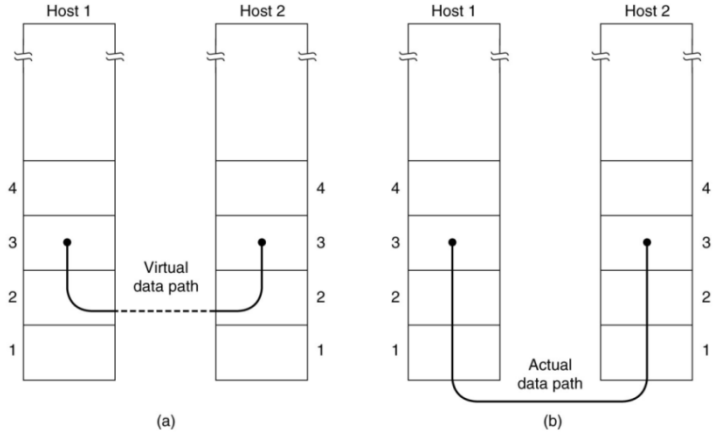
architektury komunikujících systémů

vrstvená architektura:
- cílem dekompozice problému komunikace na menší, snadněji řešitelné celky
- možnost modulární výměny vrstev

vrstvové a mezivrstvové protokoly:



vrstvový protokol:



mezivrstvový protokol:
- pravidla spolupráce sousedních vrstev

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

referenční model ISO OSI:
- obecný vrstvený model

systém:
- samostatný celek schopný vykonávat zpracování a přenos informace

otevřený systém:
- ISO OSI
- normy jsou veřejně dostupné
- všechna zařízení vyhovující normám jsou propojitelná

vrstvy referenčního systému ISO OSI:
1. **fyzická**
2. **spojová**
3. **síťová**
4. **transportní**
5. **relační**
6. **prezentační**
7. **aplikační**

1) fyzická vrstva:
- fyzická komunikace mezi sousedními systémy
- full nebo half duplex

poskytované služby:
- přenos sériového proudu bitů
- oznamování chybových stavů spojové vrstvě
- otevření a uzavření fyzického spojení

---

2) spojová vrstva:
- poskytuje jedno nebo více spojení mezi dvěma entitami síťové vrstvy v sousedících systémech

poskytované služby:
- formátování a rozpoznávání rámců
- detekce a korekce chyb
- vytváření, udržování a rušení spojení
- rušení toku dat (flow control)

3) síťová vrstva:

- cílem překlenout rozdílné vlastnosti různých síťových technologií a dosáhnout univerzální rozhraní služby
- zabezpečuje přenos dat obecně mezi nesousedními uzly sítě přes prostředníky
- adresace systémů

poskytované služby:

- síťová služba se spojením – zahajování a ukončování síťových spojení
- síťová služba bez spojení – v internetu (IP)

---

4) transportní vrstva:

- poskytuje transparentní a ekonomický přenos s požadovanou kvalitou mezi dvojicí transportních adres
- řeší adresaci transportních entit v rámci zařízení s jednou síťovou adresou
- mezi dvěma systémy může být několik transportních spojení současně

---

5) relační vrstva:

- organizace a synchronizace dialogu mezi partnerskými entitami presentační vrstvy

poskytované služby:

- řízení dialogu – komunikace jednosměrná, obousměrná střídavá, obousměrná současná
- normální, urgentní, pozdržený přenos zprávy
- synchronizační body

---

6) prezentační vrstva:

- cílem sjednotit prezentaci informace, kterou si vyměňují entity v aplikační vrstvě
- presentační vrstva se zabývá pouze strukturou zpráv, sémantika zpráv je známa pouze **aplikační** vrstvě

funkce:

- dohoda syntaxi
- přenos zpráv se současnou transformací syntaxe dat

---

7) aplikační vrstva:

- cílem vrstvy je poskytnout aplikacím přístup ke komunikačnímu systému
- předepisuje, v jakém formátu a jak mají být data přebírána/předávána od aplikačních programů

služby vrstvy:

- logická identifikace komunikujících partnerů
- dohoda funkcí parametrů od nižších vrstev

kontrolní otázky:

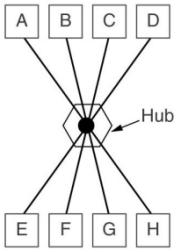
- Vysvětlete výhody vrstvené architektury komunikujících systémů. Jak probíhá komunikace mezi vrstvami ?
- dekompozice problému na snadněji řešitelné vrstvy, modulární výměna systému
- Jaké konkrétní vrstvy definuje referenční model ISO OSI a co je úkolem každé z vrstev ?
- viz. výše
- Vysvětlete pojem "enkapsulace".
- zapouzdření ….
- Vysvětlete rozdíly mezi komunikací se spojením a beze spojení.
- bez spojení – vysílač může rámce, pakety zasílat střídavě různým příjemcům
- se spojením – před zasíláním dat je nutné zbudovat spojení, poté je ukončeno

propojování sítí

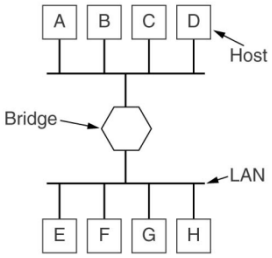
důvody propojování a rozdělování sítí:
- zvětšení rozsahu, propojení jiných oddělených sítí
- oddělení provozu, zmenšení zátěže, bezpečnost

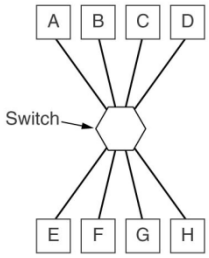
prvky pro propojování sítí:

rozbočovač:

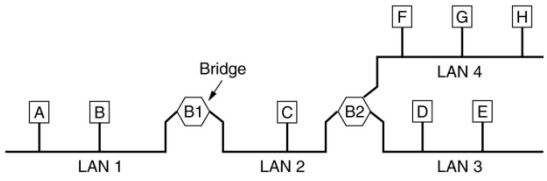


most a přepínač:





most:
- na 2. vrstvě RM OSI
- stejný formát rámce na všech rozhraních
- jsou mosty **zdrojové směrování** a **samoučící**
- možnost konverze média, kódování
- parametry:
    - forwarding rate
    - filtering rate



samoučící most:
- zasílá rámce podle tabulky se záznamy ve tvaru: <MAC_adresa, port>
- tabulku si buduje z příchozích rámců podle MAC a portu
- záznamy v tabulce mají časově omezenou platnost
- rámce, jejichž cílová adresa v tabulce dosud není, se rozesílají na všechny porty – flooding

zdrojové směrování:
- cestu rámce sítí určuje zdrojová stanice
- v rámci je seznam segmentů, kterými projde
- v síti Token ring
- popis funkce:
    - Zdroj cestu získá tak, že před vysláním datového rámce cíli pošle "průzkumný rámec" šířený v síti všemi cestami, který sbírá seznam projitých segmentů. Pro zamezení cirkulace se průzkumný rámec neodesílá se do segmentů sítě, jejichž identifikátor již v seznamu je. Cíl, který průzkumný rámec přijal, seznam segmentů otočí a pošle zpět zdroji (po již známé cestě). Zdroj může získat zpět několik odpovědí, ze kterých vybere.

spanning tree:

- neustálá automatická konstrukce stromu pokrývajícího celý graf sítě
- některý z portů na linkách tvořících smyčky bude zablokován
- v případě výpadku linky/portu se strom automaticky změní – odblokuje se některý doposud zablokovaný port

funkce spanning tree:

- volba kořenu stromu
- vytvoření nejkratších cest ve stromu, z každého mostu ke kořeni (preference linek lze ovlivnit nakonfigurováním cen)

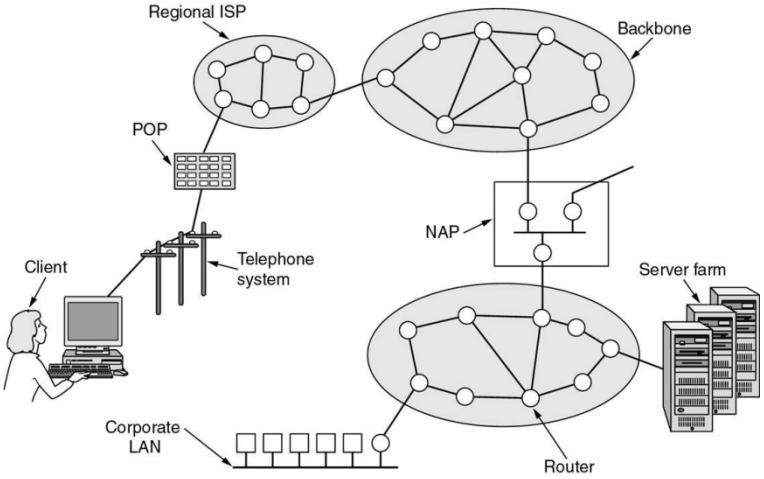
provoz spanning tree:

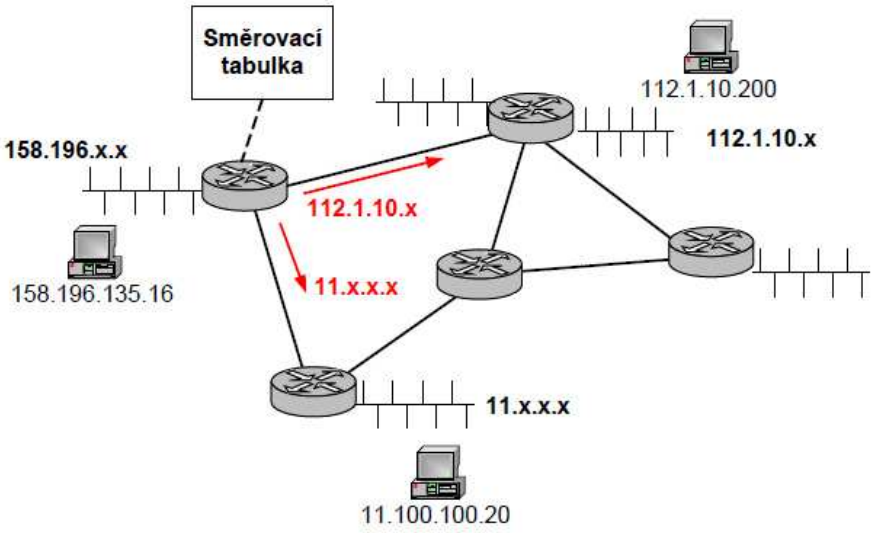
- root generuje každé 2s zprávu BPDU, která postupuje směrem dolů
- každý most kontroluje, zda tuto zprávu na svém portu slyší (přechodné stavy portů learning a listening)
- při výpadku – překonfigurování stromu max. 50s

---

směrovač (router):

- slouží k zasílání paketů nejkratší cestou sítí skok po skoku k cíli





funkce směrovače:

- směruje pakety konkrétního síťového protokolu (IP, IPX, …)
- pro každý paket najde ve směrovací tabulce podle směrovací adresy, kam má paket zaslat

kontrolní otázky:

- Jaké prvky pro propojování sítí znáte ? Kdy použijete který z nich ? Na kterých vrstvách referenčního modelu ISO-OSI pracují ?

- most (2. vrstva), switch (ke koncovému spojení zařízení v jednu síť), router (3. vrstva, při propojení více sítí, WAN), hub (jako opakovač, zesilovač)

- Popište princip funkce rozbočovače (hub), přepínače (switch) a směrovače (router).

- rozbočovač - veškerá data, která přijdou na jeden z portů (zásuvek) zkopíruje na všechny ostatní porty
- přepínač – data pošle jen na určený port
- směrovač – přenášení, přeposílání dat mezi více sítěmi

- V čem spočívá problém se smyčkami při použití transparentních mostů (přepínačů) ? Jak se odstraňuje ? Jakým způsobem může administrátor vzniklou aktivní topologii ovlivnit a proč to může být užitečné ?

- u samoučících mostů, když jsou tři paralelně spojeny. Problém řeší spanning tree

- Proč pro propojování různých typů lokálních sítí nevystačíme s přepínači, ale potřebujeme router ? Proč často potřebujeme router i pro propojení sítí stejného typu ?

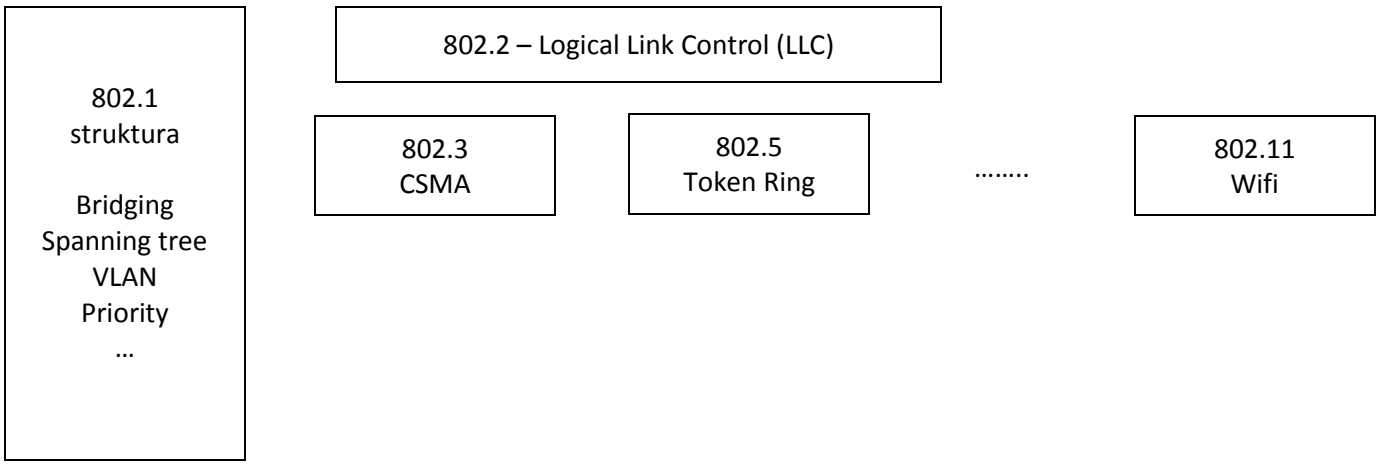
- řešení pomocí routerů je mnohem rychlejší a levnější na případnou kabeláž. která by se jinak musela u switchů použít. Nelze.

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

IEEE 802:

- normalizace aktuálního stavu lokálních sítí
- ISO 8802
- definuje fyzickou a spojovou vrstvu

struktura doporučení IEEE 802:



vztah IEEE 802 a RM OSI:

- spojová vrstva dělená na:
  - MAC – Media Access Control (různá pro různé sítě)
  - LLC – Logical Link Control (společná)

MAC vrstva:

- sdílení přístupu ke společnému kanálu
- formáty rámců
- adresace stanic
- zabezpečení proti chybám

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

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 mostys explicitním směrováním
- definice spanning tree (802.1d)
- definice virtuální sítě VLAN (802.1q)
- priorita provozu (802.1p)

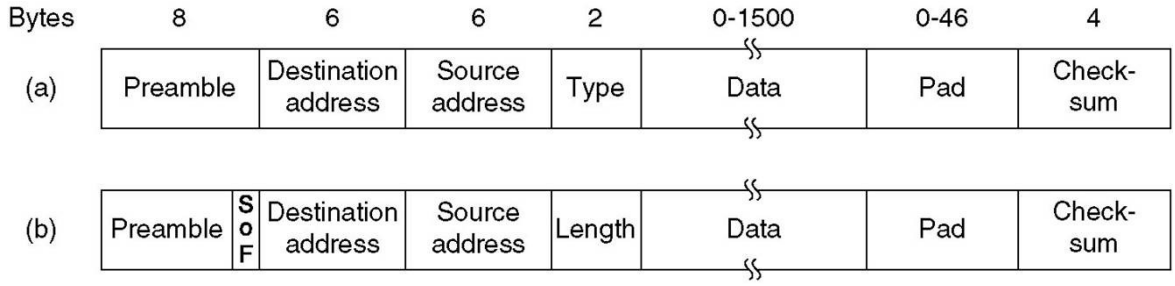
Ethernet

označování podle IEEE 802.3:
- Mbps (10, 100, …) [Base, Broad] [délka_segmentu v m | médium] (médium: T – Twisted pair, F – Fiber opric)
- 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:

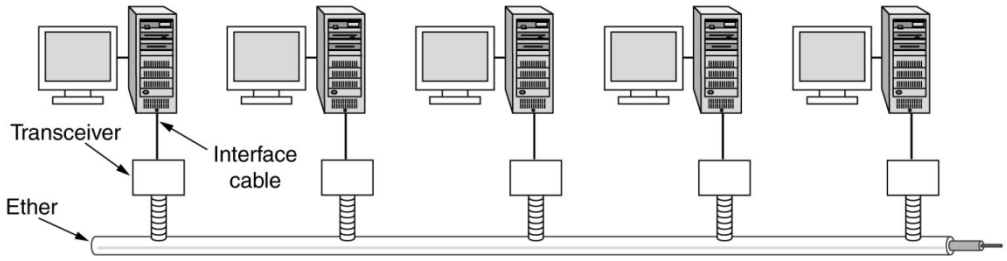


a) DIX
b) 802.3

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

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

přepínaný Ethernet:

přepínače:
- chování jako mosty – v topologii strom
- malé zpoždění
- výhody:
    - bezkolizní
    - vynucení více deterministické chování
    - vyšší bezpečnost
    - lepší udržovatelnost

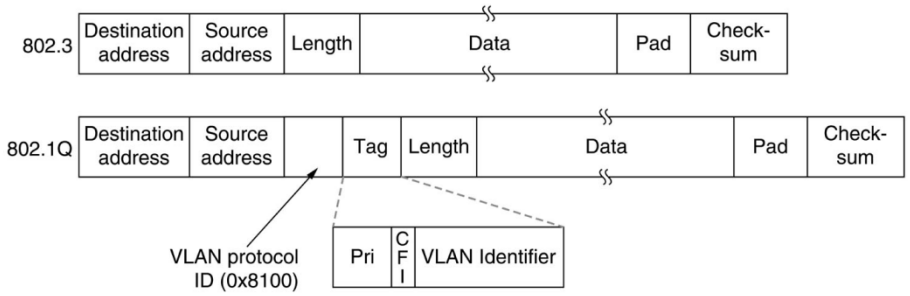
- metody přepínání:
    - Store-and-Forward
    - Cut-through (okamžitě začne vysílat po přečtení cílovéMAC)
    - FragmentFree – kombinace

- parametry:
    - počet MAC adres na port
    - celkový počet MAC adres
    - způsob přiřazení MAC k portům
    - správa a monitorování provozu
    - filtrace provozu

half/full duplex v přepínaných sítích:
- half-duplex – o médium kolizně soupeří switch a síťová karta
- full-duplex – bezkolizní, povoleny delší vzdálenosti

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 LAN mezi přepínači
- lze specifikovat, které VLAN smějí linkou trunk procházet
- VLAN ID je v datové části paketu



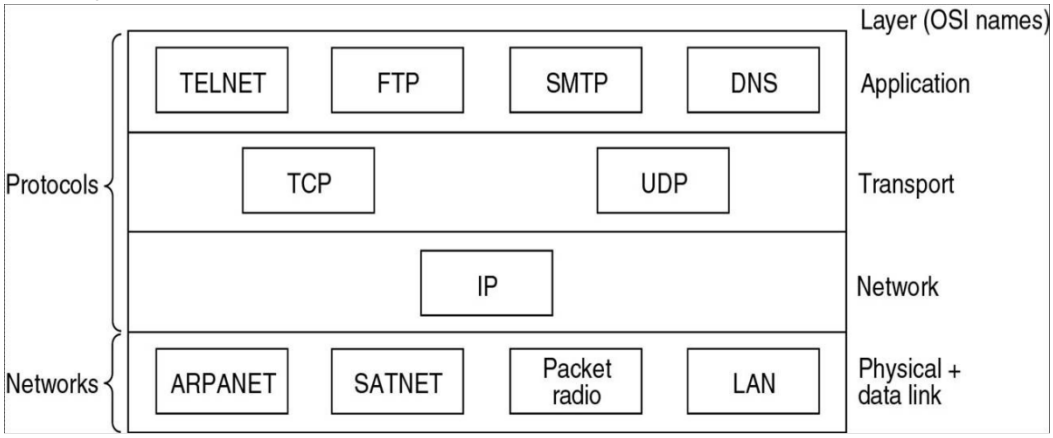
členství ve VLAN:
- staticky – podle portu
- dynamicky – podle MAC adresy

kontrolní otázky:
- Jaké úkoly plní vrstva LLC a MAC z doporučení IEEE 802 ?
- LLC - definuje služby, které síť poskytuje
- MAC – sdílení přístupu ke společnému kanálu
- Jaký je formát MAC adres ? Jak vypadá MAC adresa označující broadcast ?
- 48 bitů, broadcast = samé 1
- Co definují doporučení IEEE 802.3, 802.5 a 802.11 ?
- 802.3 – CSMA
- 802.5 – Token Ring
- 802.11 - Wifi
- Popište základní charakteristiky sítě Ethernet (možné topologie + dosah, používané médium a aktivní prvky, přístupová metoda, přenosové rychlosti).
- viz výše
- Co znamenají zkratky 10BaseF, 100BaseT a 1000BaseSX ?
- udávají typ sítě, rychlost, přenosové médium

7. Protokoly TCP/IP

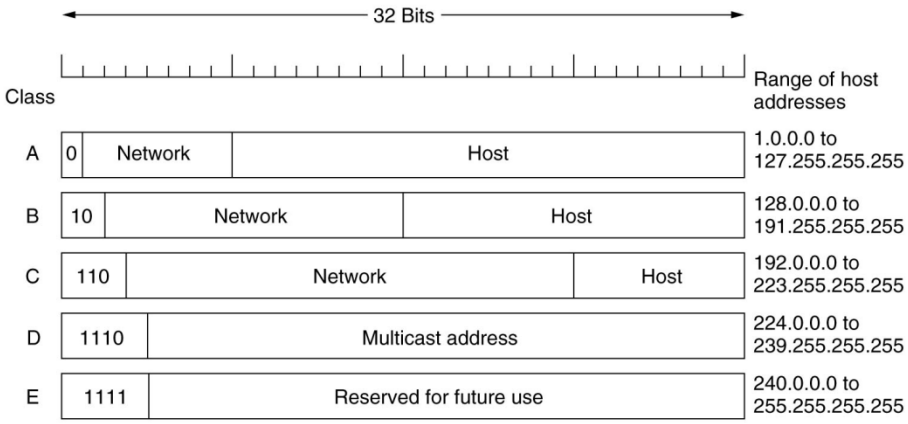
TCP/IP
- standard pro komunikaci v internetu a v intranetu
- TCP – protokol 4. vrstvy
- IP – protokol 3. vrstvy

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:

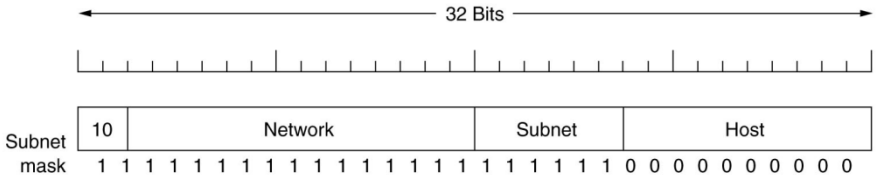


beztřídní adresy:
- délka prefixu sítě je přidělována podle potřeby
- musí být specifikována maska podsítě, která určuje délku prefixu

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

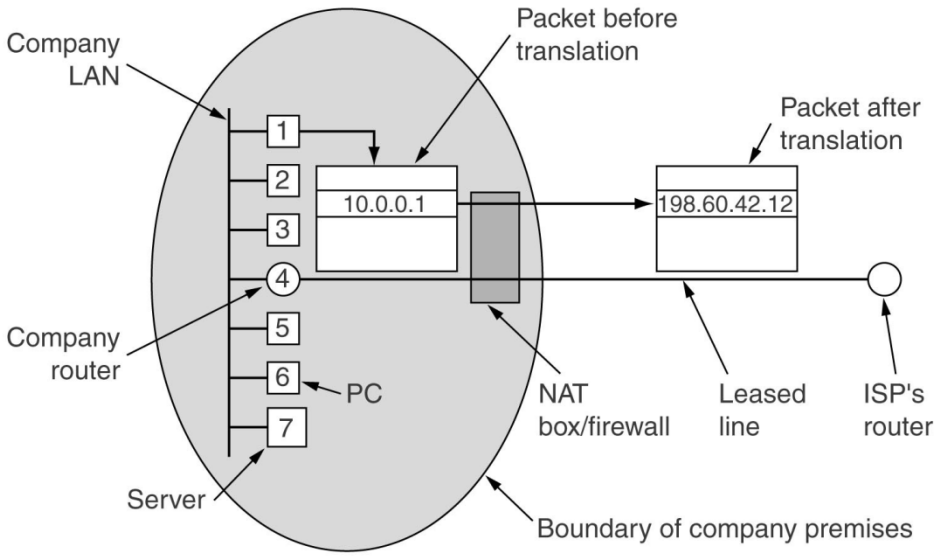
podsíťování (subnetting):
- rozdělení přiděleného adresního prostoru mezi více segmentů
- každý segment má svou vlastní adresu podsítě
- část adresy původně určené pro identifikaci uzlu sítě se rozdělí na adresu „podsítě“ a na adresu uzlu v této podsíti

maska podsítě (subnet mask):
- pro každou podsíťovanou adresu nutno udat, kolik bitů zleva představuje síť+subsíť a kolik uzel



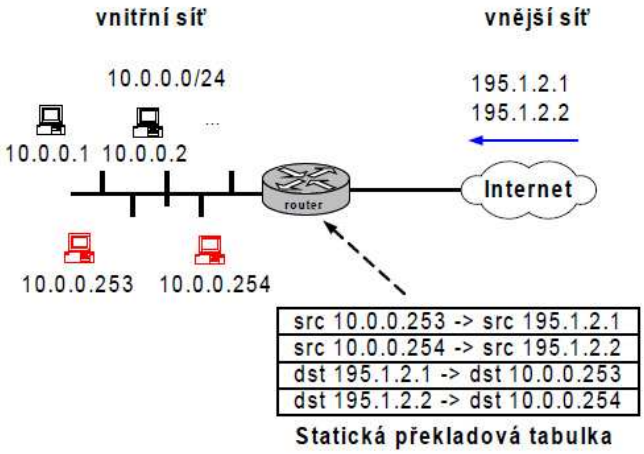
použití podsíťování:
- rozdělení prefixu přidělené délky na daný počet podsítí (zadány maximální počty stanic na segmentech)
- stanovení maximální délky pevně přiděleného prefixu pro požadovaný počet podsítí a požadované počty stanic na jednotlivých segmentech
- vytvoření adresního plánu sítě WAN

překlad adres (NAT):
- Network Address Translation
- překlad zrojové nebo cílové IP adresy
- probíhá na routeru nebo firewallu
- překlady buď statické, nebo dynamické



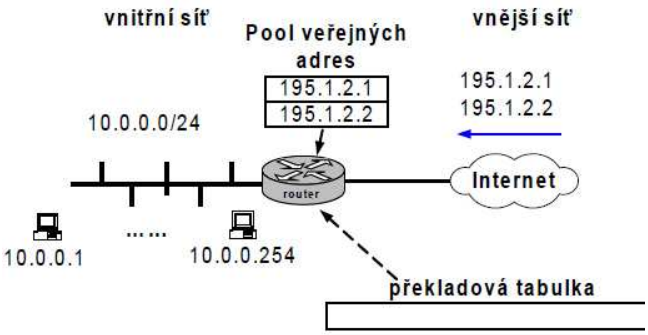
statický NAT:

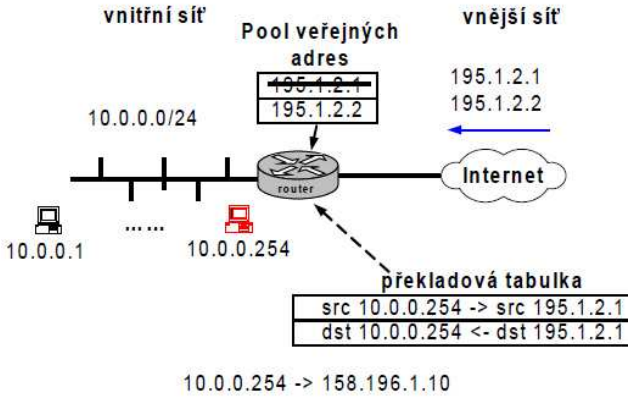
- překladová tabulka konfigurována staticky (ručně)



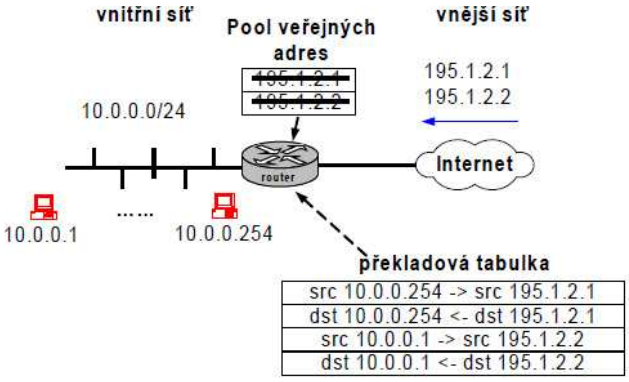
dynamický NAT:

- překladová tabulka vzniká za provozu automaticky
- adresy se propůjčují z rezervoáru adres (pool)





10.0.0.254 -> 158.196.1.10

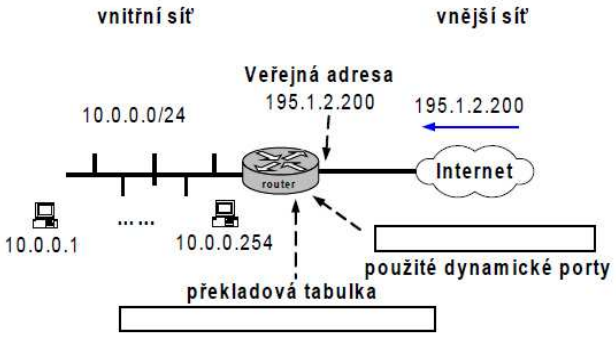


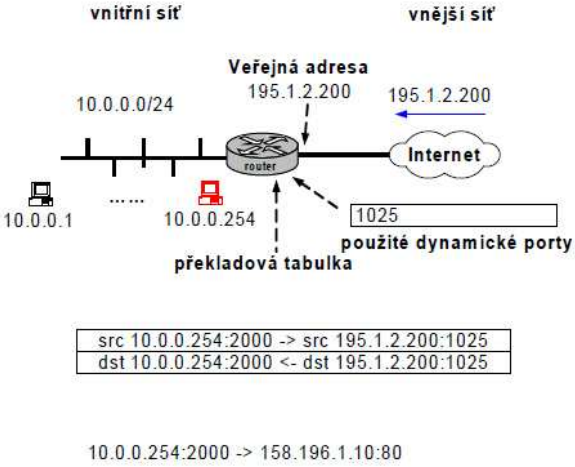
10.0.0.1 -> 158.196.1.10

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

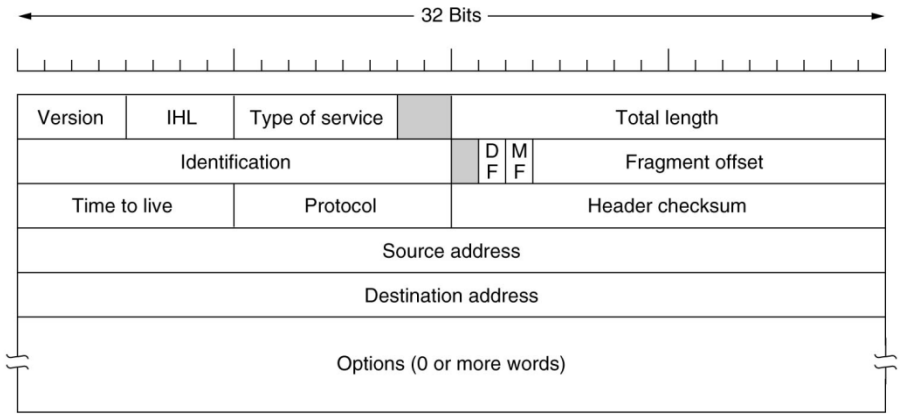
Port Address Translation (PAT)
- ukrytí více stanic za jedinou IP adresu
- rozlišení podle více zdrojových portů
- přidělováno dynamicky





protokol IP:
- Internet Protocol
- 3. vrstva, síťová služba posílání nezávisle směrovaných paketů bez spojení

hlavička IP:

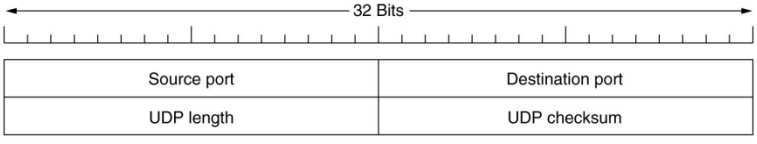


fragmentace paketů:
- rozdělení paketu při průchodu linkami s nedostatečným MTU
- podle konvence musí každý segment Internetu být schopen přenést paket o délce 576 B

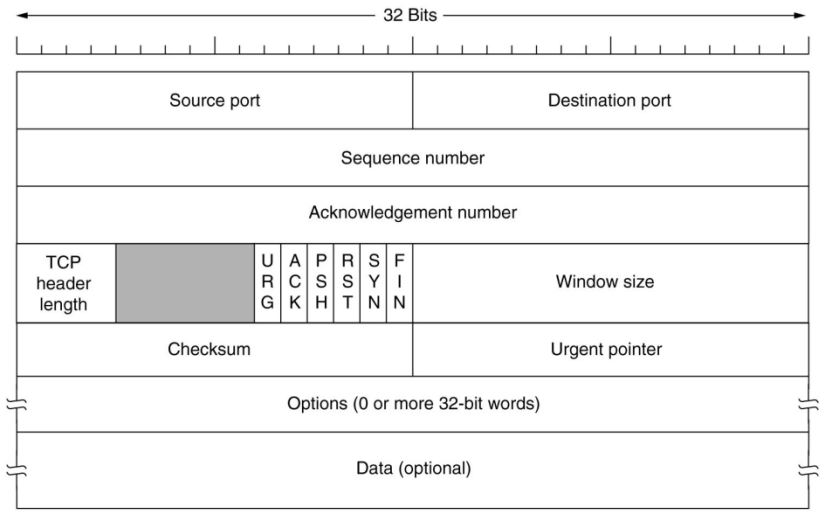
podpůrné protokoly IP:
- **ARP** – Address Resolution Protocol, mapování IP na MAC
- **ICMP** – Internet Control Message Protocol - ohlašování chyb a zvláštních stavů při přenosu paketů

traceroute:
- zjišťování cesty sítí
- zjištění všech směrovačů na cestě k cíli

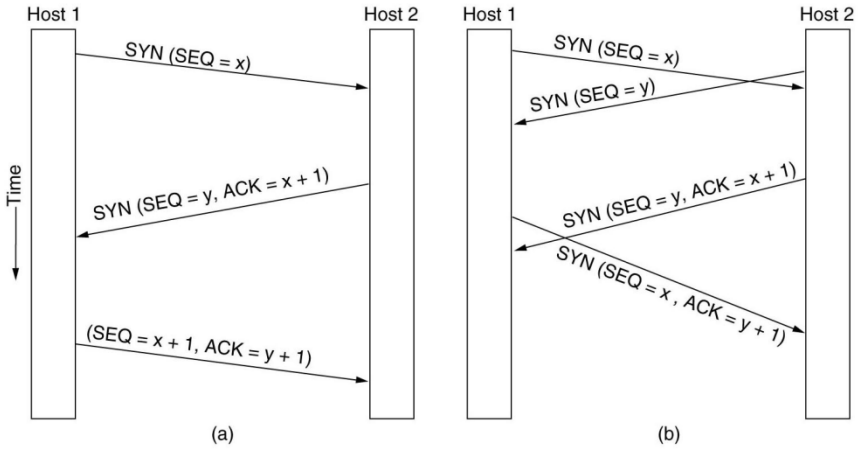
transportní vrstva TCP/IP:
- **UDP** – nepotvrzovaná datagramová služba, podpora všesměrového a skupinového vysílání
  hlavička UDP:



- **TCP** – duplexní spolehlivý logický kanál, segmentování dat, algoritmus Sliding window, protokol pro navazování a ukončování spojení
  hlavička TCP:



navazování TCP spojení:



uzavírání spojení TCP:
- uzavírá se zvlášť z obou stran
- FIN + ACK z obou stran

- **porty** – spolu s IP adresami identifikují konkrétní proces na konkrétním zařízení v internetu (16 bit)

kontrolní otázky:
- Jaké protokoly se v Internetu používají na 3. a 4. vrstvě OSI RM ?
- Srovnejte vrstvený model architektury TCP/IP s ISO OSI RM.
- Jaká je délka a struktura adresy protokolu IP ? Co znamenají třídy adres ? Co jsou beztřídní adresy a k čemu se u nich používá maska podsítě (subnet mask) ?
- Co jsou privátní adresy a k čemu se používají ? Kdo je přiděluje ? Uveďte aspoň jeden z rozsahů, který můžete použít jako privátní adresy.
- Co reprezentují IP adresy 255.255.255.255 a 127.0.0.1 ?
- Jak se formálně označí určitá IP (pod)síť jako celek ?
- Jak vypadá adresa broadcastu pro určitou konkrétní IP (pod)síť ?
- Proč se používá podsíťování (subnetting) a v čem spočívá jeho princip ?
- Naučte se vytvářet podsítě přiděleného adresního rozsahu s konstantní maskou podsítě.
- K čemu slouží překlad adres (NAT) , jaký je jeho princip a na jakém síťovém prvku jej lze realizovat ?
- Jaký je princip dynamického NAT a statického NAT ?
- Na jakém principu lze pomocí NAT za jedinou veřejnou IP adresu "ukrýt" větší množství vnitřních adres ?

- Na které vrstvě pracuje IP protokol ? Co je jeho úkolem ?
- Popište význam všech položek v hlavičce IP paketu (obrázek hlavičky si najděte ve studijních materiálech).
- Protokol IPv4 podporuje fragmentaci přenášených paketů. Proč a za jakých okolností k fragmentaci dochází ? Kdo fragmenty opět skládá a jak pozná, které fragmenty patří stejnému paketu a v jakém pořadí ?
- Vysvětlete úkol a princip činnosti protokolu ARP.
- Vysvětlete, k čemu se používá protokol ICMP. Uvěďte alespoň několik typů ICMP zpráv vždy s příkladem konkrétní situace, za které se generují (vždy rovněž udejte, kdo bude zprávu generovat).
- K čemu se používá příkaz traceroute implementovaný ve většině OS ? Vysvětlete princip jeho funkce.
- Jaké protokoly se v Internetu používají na 4. vrstvě ? Jaký je mezi nimi rozdíl ? K jakým účelům je který z nich výhodnější ?
- Popište význam položek hlavičky UDP.
- Popište význam položek hlavičky TCP.
- K čemu se u protokolů UDP a TCP používají porty ? Proč nestačí cílový port, ale pracuje se i se zdrojovým portem ?
- Popište proceduru navázání a uzavření spojení u protokolu TCP.
- Popište výměnu dat během TCP spojení včetně řízení toku (flow control). Zaměřte se na položky Sequence number, Acknowledgement number a Window v hlavičce TCP segmentu.

8. Směrování a směrovací algoritmy

sítě s přepínáním okruhů a paketů

s přepínáním okruhů:
- vyvinuto z telefonních sítí
- přenosova kapacita rezervovana po celou dobu existence okruhu
- při vypadku a rozpadu okruhu nutno žadat siť o nove vytvořeni okruhu

s přepínáním paketů:
- vyvinuto v ramci vojenskeho projektu ARPA
- polygonalni struktura s redundantnimi spoji založena na směrovačich
- datová jednotka – paket – se předává mezi směrovači
- předávání paketu skok po skoku („hop by hop“)

virtuální kanál:
- vytvořeni logickeho okruhu nad siti s přepinanim paketů
- všechny pakety jdou stejnou cestou – nemohou se přeházet do nesprávného pořadí

směrovací algoritmy:
- část software 3. vrstvy OSI RM rozhodujici, kterým rozhraním se má odeslat přichozí paket nebo kudy zřídit požadovaný (virtuální) okruh
- implementovan obvykle s použitim směrovací tabulky

směrovací tabulka:
- zaznamy ve tvaru *<cílová adresa(+maska), výstupní rozhraní/next_hop, metrika>*
- jako cílová adresa může být uvedena siť, podsiť nebo uzel

přístupy ke směrování:
- centralizované
- distribuované
- izolované

typy směrování:
- neadaptivní – statické
- adaptivní – dynamické (mění se podle okamžité topologie sítě, okamžitého zatížení jednotlivých částí sítě)

---

centralizované směrování:
- v síti existuje centrální prvek RCC (Routing Control Center), který shromažďuje informace o okoli 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

---

statické směrování:
- směrovací tabulky konfigurovány ručně
- bezpečnější
- použitelné, pokud se topologie sítě často nemění

dynamické směrování:
- automaticky reaguje na poměry v síti
- nutnost provozu směrovacích protokolů
- použitelné při častých změnách

hiearchické směrování:
- rozdělení sítě do hierarchicky rozdělených celků
- směrovače v jednotlivých celcích znají jen topologii svého celku

---

<u>směrovací algoritmy:</u>
- čím se liší:
    - použitá metrika
    - úroveň informovanosti směrovačů o topologii sítě
    - mechanismus šíření směrovací informace

algoritmy vektorů vzdáleností:
- 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
- metrikou je počet "přeskoků" (hop count) na cestě mezi zdrojem a cílem
- pomalá konvergence při změnách topologie
- reprezentanti:
    - RIP – Routing Information Protocol
    - IGRP – Interior Gateway Routing Protocol

algoritmy stavů spojů:
- směrování na základě znalosti "stavu" jednotlivých linek sítě
- směrovače znají topologii celé sítě a ceny jednotlivých linek
- každý směrovač počítá strom nejkratších cest ke všem ostatním směrovačům
- každý směrovač neustále sleduje stav a funkčnost k němu připojených linek
- při změně okamžitě šiři informaci o aktuálním stavu svého okolí všem ostatnim směrovačům
- reprezentanti:
    - OSPF – Open Shortest Path First
    - IS-IS

VLSM (Variable-Length Subnet Mask):
- dovoluje v podsítích jedné sítě používat více rozdílných masek podsítí

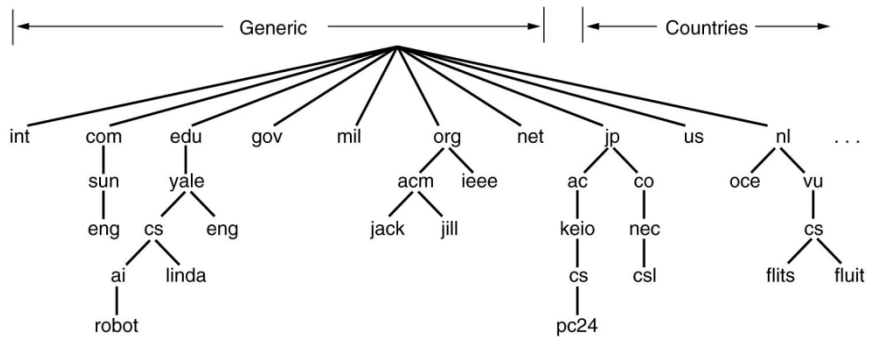
kontrolní otázky:
- Vysvětlete pojem směrování. Které aktivní prvky se směrováním paketů zabývají ?
- Vysvětlete pojem směrovací tabulka. Jaké položky (sloupce) byste očekávali v jejich jednotlivých záznamech (řádcích) ?
- Vysvětlete pojem implicitní cesty (default route).
- Jaký je rozdíl mezi statickým a dynamickým směrováním ?
- Vysvětlete princip, výhody a nevýhody hierarchického směrování.
- Vysvětlete pojem směrovací protokol.
- Do jakých dvou základních kategorií směrovací protokoly (algoritmy) dělíme ?
- Vysvětlete princip směrovacích algoritmů na bázi vektorů vzdáleností (distance vector).
- Vysvětlete princip směrovacích algoritmů na bázi stavů spojů (link state).
- Srovnejte výhody a nevýhody směrovacích algoritmů tříd distance vector a link state.
- Uveďte reprezentanty směrovacích algoritmů tříd distance vector a link state v prostředí TCP/IP.

9. DNS

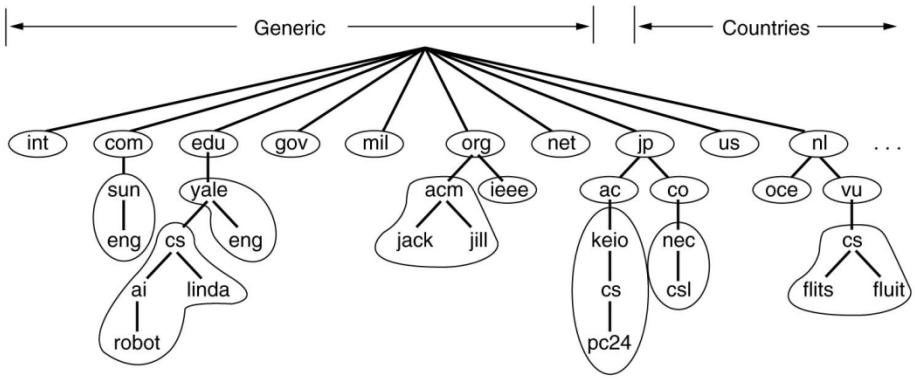
Domain Name System
- mapování logických jmen na IP adresy

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

doménový strom:



zóna:
- část stromu uložená na jednom DNS serveru



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

kontrolní otázky:

- Jaká je struktura doménového jména ? Co znači (obvykle vynechávaná) tečka za jménem vpravo ?
- Uveďte základní generické domény.
- Definujte pojem domény.
- Definujte pojem zóna. Jaký může být vztah domény a zóny ?
- Co je DNS server ? Čím se liší primární a sekundární server domény ? Co je to kořenový (root) DNS server ?
- Vysvětlete, jak probíhá vyhledání záznamu odpovídajícího zadanému doménovému jménu v DNS (postupně od root serveru).
- Jaký protokol transportní vrstvy se používá pro komunikaci s DNS serverem ?
- Jaké typy záznamů databáze DNS znáte ? K čemu se jednotlivé typy používají ?
- Vysvětlete, jak se provazuje hierarchie DNS serverů pomocí NS záznamů.
- Vysvětlete, jak probíhá přemapování známé IP adresy na odpovídající doménové jméno.
- Vysvětlete, k čemu slouží záznam SOA a MX.

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:
- obousměrný přenos souborů mezi dvěma systémy
- autentizace uživatele
- přenášená data chápána jako soubor
- vrací 3 místný kód = odpovědi na příkazy
- aktivní režim – datové spojení navazuje server
- pasivní režim – datové spojení navazuje klient

TFTP:
- trivial FTP
- nad UDP, stop-and-wait protokol

elektronická pošta

- bez šifrování
- SMTP bez autentizace
- textově orientované protokoly
- možnost šifrování zabalením do SSL
- struktura zprávy:
    - obálka
    - hlavička
    - tělo

SMTP:
- pro odesílání
- TCP/25
- příkazy orientovány textově
- nešifrováno
- neautentizováno

MIME:
- možnost strukturovat tělo zprávy
- možnost určení interpretace dat
- definuje způsob kódování binárních dat

POP3:
- pro přijímání pošty
- klient – server
- port 110
- nešifrováno
- autentizace textem

IMAP:
- vylepšená verze POP3
- klient-server
- port 143
- podpora složek
- vylepšená autentizace

www

url:
- Uniform Resource Locator
- protokol://uživatel:heslo@stroj:port/cesta

http:
- Hypertext Transef Protocol
- port 80
- klient-server
- 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:
    - GET
    - HEAD
    - POST, PUT
    - DELETE
    - LINK
    - OPTIONS
    - TRACE
- **http 1.0** – spojení iniciuje klient, ukončuje server po odeslání odpovědi. Pokud má stránka více dokumentů, posílají se zvlášť po samotných 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

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
- podle MAC
- DHCP Discover – příkaz pro vyhledání DHCP serveru
- DHCP Request – žádost o adresu

kontrolní otázky:

- K čemu se používá protokol Telnet ? Který port služba používá ? V čem spočívají bezpečnosní rizika Telnetu ? Čím lze službu Telnet nahradit pro omezení těchto rizik ?
- Jak se dá Telnet klient využít k ladění jiných služeb s textově orientovaným protokolem (kterých například) ?
- K čemu slouží protokol FTP ? V čem spočívají jeho bezpečnosní rizika ?
- Jaké dva typy kanálů se při práci FTP vytváří a jaké porty se k tomu používají ? Kterými příkazy protokolu se zajistí přečtení a uložení souboru ? K čemu slouží příkaz PORT ? Jak se přenáší obsah adresáře (příkaz list) ?
- Co obnáší FTP přenos v režimu textovém nebo binárním ?
- Co znamená pasivní režim FTP ?
- K čemu se používá protokol TFTP a jak se technicky liší od FTP ?

- Vysvětlete pojmy User Agent, Message Transfer Agent a Mailbox.
- Jaké protokoly se používají pro odesílání zpráv elektronické pošty a jaké pro vzdálené vyzvedávání zpráv z poštovních přihrádek ? Jaký protokol transportní vrstvy se při tom využívá ?
- Jaká je úroveň autentizace a šifrování v běžných protokolech pro odesílání a stahování pošty ?
- Jaká je struktura zprávy elektronické pošty ? Uveďte příklady údajů v hlavičce zprávy. Kdo smí modifikovat hlavičku zprávy ?
- Jak lze pomocí elektronické pošty posílat zprávu s netextovým (multimediálním) obsahem a zprávy složené z více částí (s "přílohami") ?
- Popište, jak se z poštovního klienta vaší pracovní stanice dostane zpráva k příjemci prostřednictvím Internetu. Předpokládejte, že klient používá server odchozí pošty (proč je to výhodné ?)
- S použitím vašeho poštovního serveru odešlete zprávu se zadaným předmětem (subject) na určitou e-mailovou adresu pouze s použitím Telnet klienta (využijte příkazů protokolu SMTP).

- Přečtěte si pouze pomocí Telnet klienta za použití příkazů POP3 poslední e-mailovou zprávu z vaši poštovní schránky.
- Co je to URL ? Jaká je obecná struktura URL ?
- Jaký protokol se používá pro čtení WWW stránek (HTML) ? Nad jakým transportním protokolem a se kterým číslem portu pracuje ?
- Ověřte si pouze s pomocí Telnet klienta existenci WWW stránky na zadaném URL a vypište si její HTML kód.
- Vysvětlete, k čemu v protokolu HTTP slouží metody GET, POST a HEAD.
- Pomocí programu Ethereal zachyťte komunikaci s WWW serverem, při níž je na server zasílán obsah nějakého formuláře. Prostudujte obsah dat zasílaných na server metodou POST.
- Vysvětlete, proč odpověď WWW serveru na žádost o určité URL obsahuje nejen obsah samotného zdroje, ale i hlavičku. Uveďte příklady údajů, které se mohou v hlavičce vyskytovat.
- Vysvětlete, proč i HTTP požadavek obsahuje hlavičku. Uveďte příklady údajů, které mohou být uvedeny v hlavičce požadavku HTTP.
- Jak se realizuje autentizace uživatelů při přístup na WWW stránky ?
- Co jsou a k čemu lze použít Cookies ?
- Uveďte základní rozdíly mezi HTTP 1.0 a 1.1.
- Jak lze zajistit šifrování a autentizaci při přenosu WWW stránek ?

- Vysvětlete, k čemu se používá protokol DHCP. Jaké parametry lze jeho prostřednictvím předat ? Jaká je výhoda oproti statické konfiguraci stanice ? Popište sekvenci zpráv protokolu během přidělování IP adresy dynamicky konfigurovatelné stanici.
- Proč je problémem,když DHCP server není na stejném segmentu jako klienti ? Jak lze tuto situaci řešit ?

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:
- sdílený klíč
- algoritmy:
    - DES
    - 3DES
    - AES
- autentizace - Zakódování username klíčem u odesílatele, stejným klíčem dekódování u příjemce + test smysluplnosti jména
- zajištění integrity zpráv – pošle se zpráva + hash

asymetrický systém:
- použití – digitální podpisy,
- certifikační autorita – entita, které je důvěřováno. Vytváří dvojice soukromý klíč, veřejný klíč

možnosti zabezpečení přenášených dat:

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 – rekonstrukce 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

<u>útoky na počítačové sítě:</u>

denial of service (DoS):
- cílem útočníka vyčerpání systémových prostředků síťového prvku nebo serveru a jeho zhroucení nebo změna požadovaného chování

intrusion detection systém:
- rozpoznává podezřelé vzory komunikace
- na různých vrstvách

kontrolní otázky:
- Definujte pojmy utajení, autentizace a integrita.
- Čím se liší symetrický a asymetrický kryptografický systém ? Jaké jsou jejich výhody a nevýhody ?
- K čemu lze použít soukromá a veřejný klíč ?
- Jak lze realizovat autentizaci v symetrickém a asymetrickém systému ?
- K čemu slouží certifikační autorita ?
- Jak lze ověřit integritu zprávy ?
- Jaké jsou výhody a nevýhody realizace bezpečnosti na 2., 3. 4. a 7. vrstvě ISO OSI RM ?
- Vysvětlete, v čem spočívá filtrace provozu na základě bezestavové inspekce paketů. Proč se nazývá bezestavová a v čem jsou její omezení oproti plnohodnotnému stavovému firewallu ? V čem je výhodnější ?
- Co jsou reflexivní ACL ?
- Proč se někdy tvrdívá. že NAT zvyšuje bezpečnost vnitřní sítě ?
- Vysvětlete pojem virtuální privátní sítě a tunelu.
- Jaká bezpečnostní rizika plynou z dynamických směrovacích protokolů ?
- Jaká bezpečnostní rizika plynou z protokolu ARP ?
- Jaké bezpečnostní rizika a ochranné mechanismy znáte v souvislosti s přepínači ?
- Jaké bezpečnostní rizika plynoucí z použití DNS znáte ?
- Co jsou DoS a DDoS útoky ? Uveďte konkrétní příklad.
- Co jsou IDS systémy ?

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
- digitální síť s 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
    - PŘI – Primary Rate Interface – 30B+D

vlastnosti ISDN při přenosu dat:
- orientováno na dočasné okruhy – spoplatňováno 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
- upstream/downstream frekvenční oblast + oblast pro hlas – odděluje se splitterem

kontrolní otázky:
- Proč je pro přenos dat přes klasickou telefonní linku nutné použít modem ? Jakou funkci modem vykonává ?
- Jaký je rozdíl mezi asynchronním a synchronním modemem ? Kde se který typ obvykle používá ?
- Co je AT jazyk ? Co jsou S-registry ?

- Vyhledejte sekvenci AT příkazů pro zřízení spojení, přechod do povelového režimu a ukončení spojení. V případě možnosti prakticky ověřte.
- Co je to síť ISDN ?
- Jaké typy přípojek ISDN znáte a jaká je jejich struktura ? Jaké je jejich typické použití ?
- Jak je fyzicky uspořádaná účastnická přípojka BRI ?
- K čemu slouží B a D kanály a jaká je jejich přenosová rychlost ?
- Vysvětlete pojem signalizace.
- Jaká zařízení lze připojit k přípojce BRI a kolik ? Kolik jich může být aktivních současně ?
- Vysvětlete, co je DSL přípojka. Co je to splitter a DSLAM ?
- Podle jakých kritérií můžeme technologie DSL dělit ?
- Co znamená dělení technologií xDSL na symetrické a asymetrické ? Proč se pro přístup k Internetu zpravidla používá asymetrické verze ? Proč asymetrická technologie není vhodná pro poskytovatele služeb ?
- Jak je to s koexistencí xDSL s klasickou telefonní / ISDN linkou ?

13.Rádiové sítě

- IEEE 802.11 (WIFI)

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

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, čifrování
- SSID – název přístupového bodu
- WEP – sdílený klíč (64, 128 bit)
- WPA, WPA 2 – odstraňuje nedostatky WEP

kontrolní otázky:
- Co znamená zkratka WiFi a v jakém doporučení IEEE jsou rádiové sítě ve volném pásmu definovány ?
- V jakých dvou nelicencovaných pásmech mohou sítě WiFi pracovat ?
- Co znamená práce v rozprostřeném spektru ?
- Jaký je rozdíl mezi režimem komunikce ad-hoc a infrastrukturním ? K čemu slouží přístupový bod (AP) ?
- Jaké přenosnové rychlosti lze teoreticky dosáhnout u technologií 802.11b a 802.11g ? Jak je to s reálně dosažitelnými rychlostmi ? V čem je ukryt rozdíl ?
- Vysvětlete problém skrytého uzlu v rádiové síti.
- Vysvětlete princip přístupové metody CSMA/CA.
- Vysvětlete mechanismus rezervace kanálu pomocí RTS-CTS rámců.
