ISO/OSI

Obecný rámec pro návrh protokolů distribuovaných systémů, do nějž jsou zasazována jednotlivá konkrétní řešení, hlavním cílem je umožnit snadné propojování distribuovaných systémů

1) *Fyzická vrstva*
   - Neinterpretuje, co přenáší
   - Ethernet, Wi-Fi
   - Na úrovni fyzické vrstvy se rozlišuje:
     – paralelní a sériový přenos
     – synchronní, asynchronní a arytmický přenos
     – přenos v základním a přeloženém pásmu
2) *Spojová vrstva*
   - Přenáší rámce, Zajišťuje přenos pouze v dosahu přímého spojení
   - Rozdělena na dvě podvrstvy (Spodní MAC, Horní LLC-logical link control)
     - synchronizace na úrovni rámců
     - řízení přístupu ke sdílenému médiu
     - adresace
     - zajištění spolehlivosti
     - řízení datového toku
3) *Síťová vrstva*
   - Přenáší pakety
   - Zajišťuje doručení paketů až ke konečnému adresátovi
   - Je poslední vrstvou, kterou musí mít přenosová infrastruktura
   - Nejrozšířeněji protokol IP
4) *Transportní vrstva*
   - Úkolem transportní vrstvy zajistit potřebné přizpůsobení
   - Protokoly transportní vrstvy jsou implementovány pouze v koncových účastnících
   - Transportní vrstva může měnit:
     – nespolehlivý charakter přenosu na spolehlivější
     – nespojovaný přenos na spojovaný
5) *Relační vrstva*
   - Zajišťuje sestavení, řízení a zrušení relací pro spojovanou komunikaci
   - Dále může zajišťovat synchronizaci, šifrování dat, kompresi dat
6) *Prezentační vrstva*
   - Prezentační vrstva má na starosti potřebné konverze
     - kódování znaků, formát čísel, formát struktur, polí, ukazatele
7) *Aplikační vrstva*
   - aplikační vrstva obsahuje pouze „jádro“ aplikací, které má smysl standardizovat

Transportní vrstva: TCP • UDP
Síťová vrstva : IPv4 • IPv6 • ICMP • adresování • směrování
Linková vrstva: Ethernet • Token ring • Wi-Fi • ARP

CRC

kódové slovo – splňuje definovanou podmínku (bylo takto odesláno)
Hammingova vzdálenost – dvou kódových slov jako počet znaků, v nichž se liší
Hammingova vzdálenost kódu d – jako nejnižší počet znaků, v nichž se liší libovolná dvě kódová slova

- Kód odhaluje t-násobné chyby, pokud je Hammingova vzdálenost kódu d > t
- Kód opravuje t-násobné chyby, pokud je Hammingova vzdálenost kódu d > 2t

CRC – cílem je maximalizovat Hammingovu vzdálenost kódu, minimalizovat velikost redundantních dat

Detekce chyb:
- Pokud je polynom reprezentující chybu beze zbytku dělitelný generujícím polynomem, chybu nepoznáme.
- Lze detekovat všechny jednonásobné chyby, pokud má generující polynom alespoň dva členy
- všechny jednonásobné chyby, pokud má polynom G(x) alespoň 2 členy
- všechny dvojnásobné chyby, pokud generující polynom nedělí ($x^m + 1$) pro všechna m < délka kódového slova a má alespoň 2 členy
- všechny chyby liché násobnosti, pokud je generující polynom G(x) beze zbytku dělitelný (x + 1)
- všechny shlukové chyby délky ≤ k (k je stupeň G(x)), pokud G(x) obsahuje nenulový konstantní člen
- téměř všechny shlukové chyby délky k+1 (k je stupeň G(x)), pokud G(x) obsahuje nenulový konstantní člen
- téměř všechny shlukové chyby délky > k+1 (stejný předpoklad o G(x))

Metalická přenosová cesta

Odrazy na vedení:

$$U_a = U_0 \cdot \frac{Z}{R_0+Z} \qquad U_\infty = U_0 \cdot \frac{R}{R_0+R}$$

$$U_{r1} = U_a \cdot \rho_b \qquad \rho_b = \frac{R-Z}{R+Z} \qquad \rho_a = \frac{R_0-Z}{R_0+Z}$$

$$U_{r_2} = U_{r_1} \cdot \rho_a$$

Optická přenosová cesta

Snellův zákon lomu:

$$n = \frac{c}{v} \qquad n_1 \cdot \sin sin\ \alpha_1 = n_2 \cdot \sin sin\ \alpha_2$$

Numerická apertura – maximální úhel, pod kterým mohu vyslat paprsek do optického vlákna, aby došlo k odrazu a paprsek zůstal v jádře

$$NA = n_0 \sin sin\ \theta$$

Optická vlákna – skleněná, plastová, jednovidová (jeden paprsek), mnohovidová (více paprsků)

Bezdrátová přenosová cesta
- Infračervená komunikace (nízký dosah, nízká přenosová rychlost)
- Laserová komunikace (vysoká přenosová rychlost)
- Rádiová $f = \frac{c}{v}$ VLF, LF – nízký útlum, velký dosah, vysoká úroveň rušení
  MF šíření povrchovou vlnou
  HF vlna se odráží od země a od ionosféry
  VHF, UHF šíření přímou vlnou
  SHF blíží se šíření světla

- World Radiocommunications Conference (WRC)
- Český telekomunikační úřad (ČTU)
  - Národní kmitočtová tabulka 9 kHz – 105 GHz

Protokoly rodiny TCP/IP

TCP/IP je starší, neodpovídá ISO/OSI modelu
Aplikační vrstva – aplikační, prezentační, relační
Transportní vrstva – transportní
Síťová vrstva – síťová
Vrstva síťového rozhraní – linková, fyzická
Unicast, Broadcast, Multicast, Anycast

IP adresy:
IPv4 (4 bajty), IPv6 (16 bajtů)
IP adresa = <network number><host number> 3 třídy adres původně A, B,C +D, E
Maska sítě – definuje hranici, která část IP adresy reprezentuje síť a která uzel
Classless InterDomain Routing – CIDR
Vyhrazené adresy:
netid, hostid=0 -> reprezentant sítě jako celku
netid=0, hostid -> myšleno tato síť, ve které jsme
1.1.1.0 -> použije uzel, pokud nezná svou adresu (používána jen pro konfiguraci)
255.255.255.255 -> limited broadcast, (neprochází přes router)
netid, hostid=1 -> directed broadcast, broadcast pouze pro jednu síť
127.x.x.x -> localhost, paket se otočí na síťové vrstvě

Privátní (neveřejné) adresy:
– 10.0.0.0: síť třídy A

– 172.16.0.0 až 172.31.0.0 – 16 sítí třídy B
– 192.168.0.0 až 192.168.255.0: 256 sítí třídy C
– nejsou směrovány ve veřejném internetu

IPv6 – unicast, multicast, anycast
jedno rozhraní uzlu může mít několik adres
Prefix – používá se na určení adresy sítě a uzlu, udává, kolik bitů zleva je adresa sítě

Globální adresa – 2000::/3, globální směrovací prefix (podle něho se směrují pakety v páteřních sítích, je přidělován centrálně), identifikátor podsítě
identifikátor rozhraní – (volen náhodně) nebo:
EUI-64 – 0 celosvětově globální, 1 lokální identifikace – nakopírována a druhý nejméně významný bit nejvyššího bajtu se invertuje (kvůli zkracování zápisu)
MAC adresa – rozpůlí se, vloží se doprostřed 2 bajty (fffe) a provede se stejná inverze jako u EUI
Lokální adresa – může být použita pouze v lokální síti
Lokální linkové
Unikátní lokální
Skupinové adresy

NAT – Network Address Translation
Překlad adres při přechodu z privátní do veřejné části sítě a naopak
Nevýhody: nový výpočet CRC v hlavičkách vyšších vrstev, překlad IP v datovém poli aplikačního paketu
NAT musí být přednastaven pro komunikaci iniciovanou z veřejné sítě

NAPT – Network Address Port Translation
Je překládáno i číslo portu
Privátní síť je vnímána z veřejného pohledu jako jeden uzel s mnoha procesy
Není schopna překládat fragmentované pakety v případě komunikace více uzlů z privátní sítě

ARP – Address Resolution Protocol
Používán v IPv4
Konverze IP adresy na MAC adresu
Uzel sítě si udržuje tabulku IP – MAC (ARP Cache)
Broadcast v síti s požadavkem na MAC adresu daného uzlu s IP adresou

ICMP - Internet Control Message Protocol
(ping, tracert)
ICMP slouží k hlášení chyb a získání konfiguračních údajů
Time exceeded – paket byl zahozen. protože TTL byl překročen
Destination unreachable – nelze dosáhnout cílového uzlu
ICMPv4 – ICMPv6

NDP – Neighbour Discovery Protocol
Používán v IPv6, používá ICMPv6 multicast, pracuje na linkové vrstvě
- zjistit linkovou adresu z IP adresy
- detekovat změny v linkových adresách
- hledat směrovače
- přesměrování
- zjišťování parametrů sítě (např. prefixů) pro automatickou konfiguraci
- ověření dosažitelnosti sousedů
- detekci duplicitních adres

Skupinové adresy s prefixem ff02:0:0:0:0:1:ff00::/104
Posledních 24 bitů hledané adresy se připojí za tento prefix

Porty a Sockety
Port 16bitové číslo
Socket je struktura definující komunikační kanál pro aplikaci

UDP – User Datagram Protocol
Podporuje podporuje pouze porty, checksum nepovinné (pro IPv6 ano)
Source port, Destination port, Length, CRC, Data

TCP – Transmission Control Protocol
Spolehlivá komunikace, Řízení datového toku, Segmentace dat do paketů, Multiplexování dle čísla portů, Garantuje pořadí přenášení dat

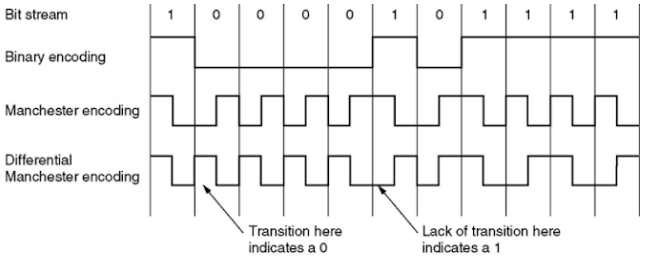
TCP Congestion Control
– snaha identifikovat, jakou rychlostí je možné odesílat, aby se síť nepřehlcovala
Slow start – rychlost odesílání na novém spojení je pomalu navyšována s cílem nalézt limit
Congestion avoidance
Fast retransmit - exponenciální a poté logaritmické navyšování rychlosti

DHCP - Dynamic Host Control Protocol
Protokol poskytující konfigurační informace novému uzlu v síti

DNS – Domain Name Server
Typy
Primární – má autoritu nad zónou, probíhá na něm editace záznamů
Sekundární – přebírá data od primárního serveru
Caching Only – poskytuje neautorizované odpovědi, přebírá informace z primárních a sekundárních serverů

Teorie informace, Přenosové kanály

NRZ (Not Return To Zero): úroveň signálu přímo odpovídá 1/0
RZ (Return To Zero): třístavový, polovina intervalu +1 při bitu 1, -1 při bitu 0, druhá polovina intervalu nulová.
NRZI (Not Return To Zero Inverted): 1-inverze signálu, 0-úroveň zůstává
PSK (Manchester): fázová modulace, uprostřed intervalu: 0-sestup signálu, 1-vzestup signálu *. Každý bitový interval má tedy uprostřed změnu. Dvojnásobné pásmo oproti přímému kódování. Použití v Ethernetu.
DPSK (Diferenciální Manchester): 1-změna na začátku intervalu, 0-absence změny na začátku intervalu *. Uprostřed intervalu změna vždy. Kóduje se změna/zachování úrovně posledního bitu (ne hodnota aktuálního bitu). Použití v Token-Ring.



AWGN kanál – zdroj chyb je aditivní šum, použití modely satelitních komunikací
BSC kanál
Gilbert-Elliott – dvoustavový kanál, Good/Bad

Kódy pro zabezpečení dat:

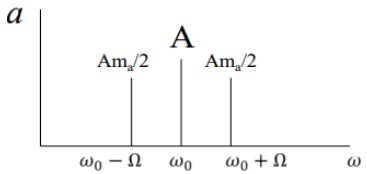
Prefixový kód – žádný symbol jeho kódové abecedy není předponou (začátkem) jiného symbolu abecedy
Kraftova nerovnost: Z n znaků lze sestavit prefixový kód s délkami kódovaných slov
Šifry
obousměrné – lze dešifrovat, když máme správný klíč
jednosměrné – ukládání hesel, digitální podpis
Digitální podpis
výtah zprávy zašifrovaný privátním klíčem autora dokumentu
digitální podpis zajišťuje tři funkce:
– integritu
– autentifikaci (kdo zprávu podepsal)
– nepopiratelnost (autor nemůže v budoucnu zapřít, že zprávu podepsal)

Modulace

Z hlediska modulované veličiny
- – Amplitudová
- – Frekvenční
- – Fázová
- – Šířková

Z hlediska nosného signálu
- – S harmonickým n.s.
- – S impulsním n.s.

Dle modulačního signálu
- – Analogový
- – Číslicový
  - • Binární
  - • Vícestavový



Modulace analogová:
Amplitudová modulace (viz obr.)

Modulace číslicová:
ASK – amplitudová modulace ()
FSK – kmitočtová modulace (měním frekvenci)
PSK – fázová modulace
- BPSK – 2logické stavy
- QPSK – 4 logické stavy
- 8-PSK – 8 logických stavů

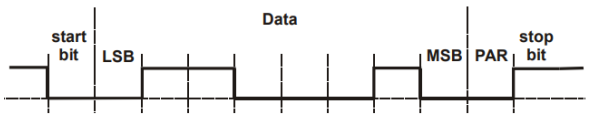
QAM – kombinace amplitudové a fázové modulace 8 – 256 stavů
- EVM – vyjadřuje, jak nepřesná je odchylka od ideálních poloh dané modulace v procentech
  - čím více možných stavů, tím nižší musí být

Modulace s rozprostřeným spektrem – využívá se větší část frekvenčního spektra, k přenášenému toku dat se přidává pseudonáhodný signál
– odolnost vůči (úzkopásmovému) rušení
– možnost sdílení pásma
– obtížná detekce provozu
– odolnost proti odposlechu
– časová synchronizace (GPS –výpočet vzdálenosti družice a přijímače)

Typy datových přenosů
- jednosměrný – simplex
- obousměrný střídavý – half-duplex
- obousměrný současný – full-duplex

- sériový, paralelní

- paralelní synchronní, asynchronní (pomalejší)
- sériový asynchronní (UART), synchronní



přenášen bajt, vyhodnocování uprostřed intervalu -> musí být synchronizováno prvním bitem

Sdílení kapacity kanálu

Multiplexování – metody umožňující rozdělit jeden fyzický kanál na více kanálů logických

Frekvenční multiplex
- rozdělení fyzického kanálu na požadovaný počet subkanálů
- V optických přenosech
  - elektrické (vyžaduje vysokou linearitu, nepoužívá se)
  - optické multiplexování (vlnový multiplex, různý lom při dané frekvenci)

Časový multiplex
- kapacita postupně využívána pro přenos dat jednotlivých kanálů, přiřazení časových slotů

Statistický časový multiplex
- konstantní časové rozdělení slotů je neefektivní -> přiřazuje slot na základě statistiky využití

Kombinovaný časový a frekvenční multiplex

Kódový multiplex
- modifikace vybraného parametru signálu podle předem daného pseudonáhodného kódu
- dekódování – založeno na ortogonalitě pseudonáhodných sekvencí (WiFi, Bluetooth)

Prostorový multiplex

Adresace na linkové vrstvě
- Adresace uzlů – MAC adresa, specifikuje, komu je rámec určen
- Adresace zpráv – broadcast, identifikuje se obsah rámce

Řízení přístupu k médiu

Deterministické – dopředu víme, kdo bude vysílat, kolize zde nenastávají
Stochastické (s náhodným přístupem) – kolize nastávají, protokol s tím počítá

Deterministické:
- Master-Slave – master se dotazuje slavů zda chtějí vysílat, komunikace jde přes mastera
  - + jednoduchá implementace
  - - závislost komunikačního cyklu na počtu uzlů
  - - závislost na výpadku uzlu Master
- Token Passing – uzly rovnocenné, vysílá ten, kdo drží token (předává se v kruhu periodicky)
  - + nezávislost na jednom uzlu
  - - dlouhý čas na zformování kruhu
  - - čekání v případě ztráty tokenu
- TDMA – uzly mají přesně přidělený čas, kdy mohou vysílat
  - využíván v aplikacích, které mají vysoký nárok na bezpečnost
- Delegated Token – vyhrazený uzel (arbitr) vysílá výzvy, umožňující ostatním uzlům vysílat
  - + jednoduché arbitra zálohovat
  - - závislost na arbitrovi

Stochastické:
- ALOHA – kdy chce vysílat, začne
- CSMA (Carrier Sense Multiple Access) – kontroluje, zda je kanál volný
  - CSMA/CD – collision detection
    - kolize jsou detekovány, po kolizi uzly čekají náhodně dlouhou dobu
  - CSMA/CA – collision avoidance
    - v bezdrátových sítích, po detekci volného kanálu se čeká po náhodnou dobu a pokud je kanál ještě volný, uzel smí vysílat
  - CSMA/CR – collision resolution
    - kolize nejsou destruktivní, na začátku vysílání arbitráž, vybrán uzel s nejvyšší prioritou

Nespolehlivá služba
- nezaručuje doručení všech rámců, může provádět kontrolu správnosti obsahu (Ethernet, UDP)

Spolehlivá služba
- zabezpečuje kompletní doručení všech rámců či paketů bez chyb, provádí kontrolu správnosti obsahu, při zjištění chyb se přenos opakuje (USB)

Zpracování chyb při přenosu
- Dopředná korekce (FEC – Forward Error Correction)
  - simplexní kanály (DVB) není možné znovu žádat o data
  - vysoká chybovost (Powerline networking)
  - isochronní datové toky (streamování multimédií)

ARQ – Automatic Repeat reQuest
- Stop and Wait – vyslání paketu až po potvrzení předchozího paketu, nebo při timeoutu
  - - velké zpoždění mezi uzly
  - - potvrzení může být přiřazeno špatnému rámci (řešení číslováním)
- Go-Back-N – vysílající uzel smí odeslat až N rámců bez potvrzení, potvrzení obsahuje pořadové číslo posledního správně přijatého rámce, chybějící rámce jsou ignorovány
  - - všechny rámce odeslané po chybě jsou opakovány
- Selective Repeat – buffery na obou stranách, vysláno N paketů, opakovány jsou pouze chybějící rámce

Přepínání okruhů
- klasická telefonie, rozhlas, TV
- mezi příjemcem a odesílatelem vzniká (fyzicky) přímá, souvislá cesta, komunikace probíhá v reálném čase
- vhodné pro kontinuální přenosy, multimediální formáty, data nemusí být adresována

Přepínání paketů
- nevzniká žádná souvislá vyhrazená cesta
- data musí být adresována

Spojovaná služba – přepínání okruhů
Nespojovaná služba – přepínání paketů -> chceme vhodným protokolem emulovat spojovanou službu (TCP)

Propojování distribuovaných systémů

– fyzická vrstva: opakovač, (repeater), rozbočovač
– linková vrstva: most (bridge), přepínač, (switch)
– síťová vrstva: směrovač (router)
– aplikační vrstva: brána (gateway)

Pro vyšší protokolové vrstvy je jeho funkce transparentní a má na ně pouze nepřímý vliv

Repeater
funguje v reálném čase, zesiluje, znovu tvaruje signál
nevýhoda - může plýtvat dostupnou přenosovou kapacitou, hloupý

Bridge
spojuje dva segmenty sítě, respektuje protokoly spojové vrstvy

Switch
spojuje více segmentů sítě, předává informace jen tam, kam jsou určeny
nepracuje v reálném čase, ukládá data ->
umožňuje spojit segmenty sítě s různými přenosovými rychlostmi
vzniká zpoždění, může dojít ke ztrátě dat

Router
analyzuje obsah paketu síťové vrstvy a směřuje paket k cíli - směrovací tabulka
má povědomí o topologii celé sítě

Gateway
"rozumí" všem přenášeným datům, spojuje různé technologie (i mimo OSI model)

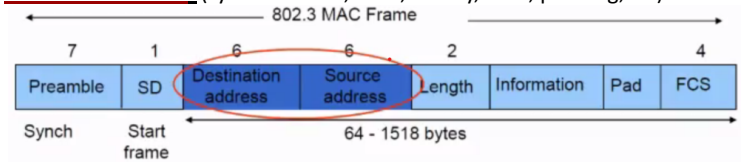
Základní modely přenosu dat:
Klient-Server: klient->žádost-> <-odpověď<-indikace<-server (role se mohou měnit)
Producent-Konzument: producent vysílá data nezávisle, nepotvrzované, (digitální televize)

Ethernet

pokrývá fyzickou a spojovou vrstvu, nespolehlivá služba, žádné ARQ
+ : poměr cena/výkon, prověřená technologie, rostoucí rychlost, vysoké množství uživatelů
- : nižší odolnost vůči prostředí, nedeterminismus z něj vyplývající nevhodnost pro aplikace v reálném čase (lze vyřešit souběžnou komunikací obou stran, potlačení echa)

CSMA/CD
kolizní okénko - 2x doba šíření signálu segmentem
minimální délka rámce 512 bitů
při detekci kolize signál JAM, čeká náhodně dlouho, další pokus o vysílání
16 pokusů na odeslání paketu, poté paket zahodí

a) formát MAC rámce: (synchronizace, start, adresy, data, padding, CR)



MAC adresa - unicast, multicast
broadcast FF..FF
Globální adresa - 1-3 bajt přidělen výrobci autoritou, zbytek definuje výrobce
Lokální adresy - definovány správci sítě

b) LLC (Link Service Access Point)
poskytuje podobnou funkci jako porty u TCP/UDP, přidá hlavičku, destination, source address
různé formáty, Ethernet II., 802.3, 802.2…

Propojování v Ethernetu:

- opakovač - musí opakovat informaci o kolizi,

kolizní doména - všechny segmenty, kam se dostane informace o kolizi
- rozbočovač (hub), jako opakovač, vyšší počet portů, nevýhoda -> vyšší riziko kolize
- bridge, switch (linková vrstva) - lokalizace, filtrování, forwarding - cílové předávání rámců a MAC adres, (asociace MAC adres/portů se vytváří dynamicky, učí se)
nesmí existovat smyčky:

(Rapid) Spanning tree - identifikace smyček v síti, virtuálně smyčku rozpojí
vybere se kořenový prvek (root), ostatní prvky určí cenu propojení k rootu, vybere se ta nejlevnější cesta, ostatní porty jsou pro vysílání deaktivovány, mohou sloužit jako záloha cesty

Auto negotiation - automatické nastavení typu ethernetu (10/100/1000) (full duplex, half duplex)
netestuje kabeláž, ohoda na nejvyšším shodném podporovaném standardu

Power over Ethernet - napájení zařízení přes Ethernet
integrovaný do switche
samostatný
detekce a klasifikace, jaký příkon zařízení požaduje a zda je schopné napájecí zařízení poskytnout

Virtual LAN - realizace virtuálních LAN na sdílené infrastruktuře, realizované tagem v ethernetovém rámci, implementováno aktivními síťovými prvky, Spanning Tree algoritmus
přímo - rámec obsahuje daný tag
nepřímo - tag je doplněn přepínačem dle portu z něhož dorazil

Wi-Fi

na linkové vrstvě
pásmo 2.4 GHz - 14 částečně překrývajících se kanálů, povoleno 100 mW

Ad-hoc síť - přímá komunikace mezi uzly bez síťové infrastruktury
Stacionární sítě - infrastruktura (Access Point)

DCF - Distributed Coordination Function - varianta CSMA/CA pro WiFi
DIFS + CSMA/CA Backoff
volitelné použití virtuálního odposlechu kanálu
PCF - Point Coordination Function - varianta Master-Slave
nadřazená metoda poskytující bezkolizní provoz, je nad DCF, střídá se s ní
PIFS + beacon + SIFS + data
HCF - Hybrid Coordination Function
vylepšená varianta DCF a PCF, dynamicky mění čas DCF a PCF

Virtuální odposlech kanálu - uzel pošle žádost (RTS - Request To Send) o přidělení kanálu s využitím CSMA/CA, AP odpoví po uběhnutí SIFS přidělením vysílacího času (CTS - Clear To Send) ostatní slyší CTS a pokládají kanál za obsazený (snižuje počet kolizí), opět se čeká SIFS a následně se posílají data, SIFS, ACK

potvrzovací mechanismus - ACK, stop-and-wait
Fragmentace - Jsou-li data delší než maximální délka datového pole MAC rámce

Zabezpečení
WEP (Wired Equivalent Privacy) - nepoužívané
WPA (WiFi Protected Access) - nepoužívané
WPA2 - využívá AES (Advanced Encryption Standard)