Sítě standartu IEEE 802.11

Joseph Soukup – P4

Přenosová trasa

- Přenosová trasa může být telefonní linka, koaxiální kabel, rádiový přenos apod.
- V případě bezdrátových sítí je to optické (infračervené, laser) nebo mikrovlnné záření

Metody přístupu k médiu podle 802.11

- Všechny popisované metody definují chování při sdílení přenosové média (u bezdrátového přenosu je tím míněno frekvenční pásmo - kanál) mezi více koncovými uzly a přístupovým bodem (Access Point - AP)

DCF (Distributed Coordination Function)

- Systém, podobný metodě přístupu k médiu u Ethernetu (stanice naslouchají, zda je přenosové médium volné, a okamžiku kdy se tak stane, začnou vysílat)
- Detekce volného média se provádí měřením signálu na anténě

PCF (Port Coordination Function)

- Funguje jako arbitr a centrálně přiděluje přenosové médium registrovaným žadatelům
- Přidělování média funguje buď na principu cyklické obsluhy (round robin) nebo na základě priorit

802.11a

- 5 GHz s přenosovou rychlostí až 54 Mbit/s
- OFDM

802.11b

- 2,4 GHz s přenosovou rychlostí až 11 Mbit/s
- DSSS
- Doplněk specifikuje, že podle momentální rušivosti prostředí se dynamicky mění rychlost na nižší nebo naopak na vyšší:
    - 11 Mbit/s
    - 5,5 Mbit/s
    - 2 Mbit/s
    - 1 Mbit/s

IEEE 802.11g

- 2,4GHz s přenosovou rychlostí až 54 Mbit/s
- Fyzické vrstva OFDM, a navíc se používá DSSS pro zpětnou kompatibilitu
- K modulaci se používá podle kvality přenosového média QPSK, BPSK, 16-QAM či 64-QAM
- 54 Mbit/s (64-QAM), 48, 36 a 24 Mbit/s (16-QAM), 18 a 12 Mbit/s (QPSK), 9 a 6 Mbit/s (BPSK)
- Další rychlosti jsou stejné jako u 802.11b:
    - 11 Mbit/s (CCK)
    - 5,5 Mbit/s (CCK)
    - 2 Mbit/s (DQPSK)
    - 1 Mbit/s (DBPSK)

IEEE 802.11n

- S přenosovou rychlostí až 540 Mbit/s
- Upravit fyzickou vrstvu a pod část linkové vrstvy, takzvanou Media Access Control (MAC) podvrstvu tak, aby se docílilo reálných rychlostí přes 100 Mbit/s
- Maximální fyzická (L1) rychlost může být až 600 Mbit/s při MAC (L2) rychlosti až 400 Mbit, to konfiguraci 4X4 MIMO
- MIMO

IEEE 802.11ac

- Pracuje v pásmu 5GHz
- Má větší šířku pásma, na jednu anténu 433 Mb/s
- MIMO jen 3 antény a přenosová rychlost 3,1 Gb/s

WIFI

- Označení pro několik standartů IEEE 802.11 popisujících bezdrátovou komunikaci v počítačových sítích
- Využívá bezlicenčního frekvenční pásma
- Wi-Fi zajišťuje komunikaci na spojové vrstvě, zbytek je záležitost vyšších protokolů
- Typicky se proto přenášejí zapouzdřené Ethernetové rámce
- Pro bezdrátovou komunikaci na sdílení médiu (šíření elektromagnetického pole prostorem) je používán protokol CSMA/CA
- SSIS (Service Set Indentifier) -> řetězec až 32 ASCII znaků, kterými se jednotlivé sítě rozlišují -> broadcast

Ad-hoc sítě

- Spojují dva klienti, kteří jsou v rovnocenné pozici -> probíhá pomocí SSID
- Musí být v přímém rádiovém rozsahu

Infrastrukturní sítě

- Obsahuje jeden nebo více přístupových bodů
- Klient si podle názvů sítí vybere, ke které se připojí

AP (Access point)

- Zařízení, ke kterému se klienti připojují
- Klienti spolu nekomunikují přímo, ale prostřednictvím přístupového bodu

AFH (Adaptive Frequency Hopping)

- Využívá dostupných volných kmitočtů a neomezuje tak Bluetooth přenos pouze na sadu frekvencí obsazených jinými bezdrátovými standarty, díky čemuž uživatelům náhlavních souprav Bluetooth zajišťuje nepřerušované čisté spojení
- Všechna zařízení, jež využívá pásmo 2,4 GHz, mohla pracovat současně, aniž by docházelo ke snížení kvality přenosu dat

DS (Distribution System)

- Propojuje na úrovni linkové vrstvy
- DS propouští broadcast
- Může propojovat dvě drátové sítě nebo i dvě bezdrátové sítě

DSSS

- Přímý rozprostření spektra
- Jednotlivý bit určený k přenosu, je nejprve nahrazen určitou početnější sekvencí bitů

FHSS

- Přeskakování mezi několika frekvencemi při přenosu bitu nebo bitů
- Pokud na některém kanálu vysílá jiné zařízení nebo je příliš velký útlum, vysílač ihned přejde na jinou frekvenci

OFDM

- Použití několika desítek až tisíce nosných kmitočtů
- Využívá frekvenčních dělení kanálů
- Pracuje s tzv. rozprostřených spektrem, kdy je signál vysílán na více vzájemně ortogonálních frekvencích, které jsou označovány jako subnosné

QAM

- Kvadraturní amplitudová modulace
- Digitální i analogové modulační schéma, které umožnilo sestrojení modemů pro analogové telefonní linky s přenosovou rychlostí vyšší, než je maximální kmitočet telefonního signálu, a které je používáno pro digitální televizní vysílání

MIMO

- Využívá vícero vysílacích a přijímacích antén a měl by se také zvýšit dosah

BSS (Basic Services Set)

- Nejmenší prvek bezdrátových sítí, několik počítačů, co spolu komunikují
- Jde o analogii buňky v mobilních sítí

Kontrola MAC adres

- Přípojný bod bezdrátové sítě má k dispozici seznam MAC adres klientů, kterým je dovoleno se připojit (tzv. Whitelist)
- Zrovna tak je možné nastavit blokování určitých MAC adres (blacklist)
- Útočník se může vydávat za stanici, která je již do bezdrátové sítě připojena pomocí nastavení stejné MAC adresy (pokud je na AP tato funkce aktivní)

WEP (Wired Equivalent Privacy)

- Šifrování komunikace pomocí statických WEP klíčů symetrické šifry
- Ručně nastaveny na obou stranách bezdrátového spojení
- Jde prolomit

WPA (Wi-Fi Protected Access)

- Využívá WEP klíče, které jsou ale dynamicky bezpečným způsobem měněny
- K tomu slouží speciální doprovodný program, který nazýváme prosebník (suplikant)
- Autentizace přístupu do WPA sítě je prováděna pomocí PSK (Pre-Shared Key – obě strany používají stejnou dostatečně dlouhou heslovou frázi) nebo RADIUS server (ověřování přihlašovacím jménem a heslem)

WPA2

- Novější WPA2 přináší kvalitnější šifrování (šifra AES), která však vyžaduje větší výpočetní výkon a proto nelze WPA2 používat na starších zařízeních

EAP (Extensible Authentication Protocol)

- Autentizační rámec zprostředkující přenos a používání klíčů generovaných podle metod
- EAP není síťový protokol, pouze definuje formáty zpráv
- Každý protokol, který používá EAP definuje způsob zapouzdření v daném protokolu

802.1x

- Přístupový bod vyžaduje autentizaci pomocí protokolu IEEE 802.1x
- Pro ověření je požíván na straně klienta program, který nazýváme prosebník (suplikant), kterému přístupový bod zprostředkuje komunikaci s třetí stranou, které ověření provede (například RADIUS server)
- Za pomoci 802.1X lze odstranit nedostatky zabezpečení pomocí WEP klíču