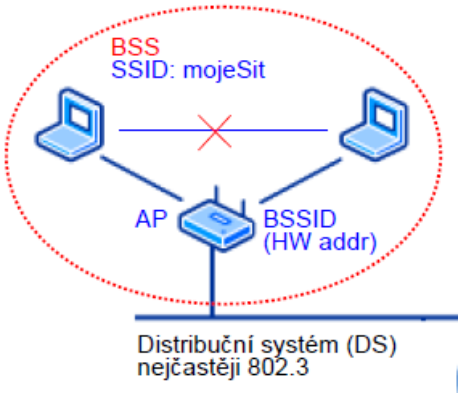
Topologie WiFi

Základním prvkem protokolu rodiny 802.11 je přístupový bod – Access Point (AP) – s BSSID (Basic Service Set Identificator - typicky MAC adresou). Jedná se o analogii k přepínači na metalických sítích. AP pokrývá fyzickou oblast - tzv.: Basic Service Area (BSA).

Uzly asociované k AP dohromady s AP tvoří - Basic Service Set (BSS). Každá takováto síť má vlastní identifikátor – SSID.

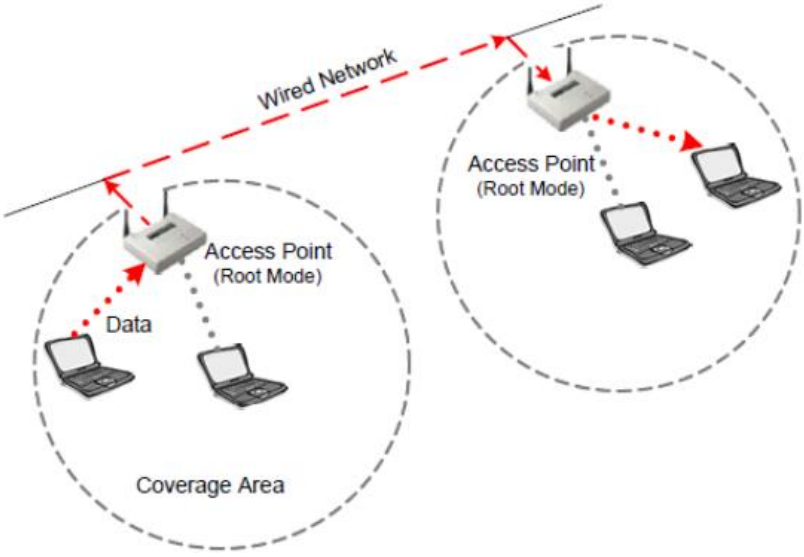
Uzly komunikuji přes AP mezi sebou i do datové sítě. Proto AP většinou tvoři gateway (GW) do datové sítě.

Propustnost - stanice se střídají na AP v časovém multiplexu. Problémem je tzv.: skryty uzel.



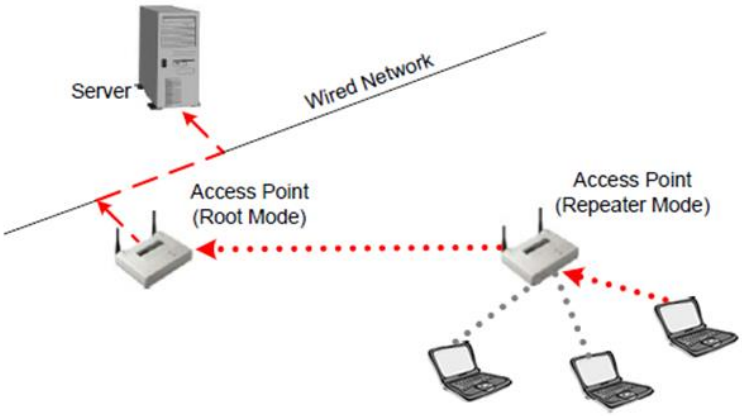
Režimy činnosti Access Pointu – AP Modes

- Root mode



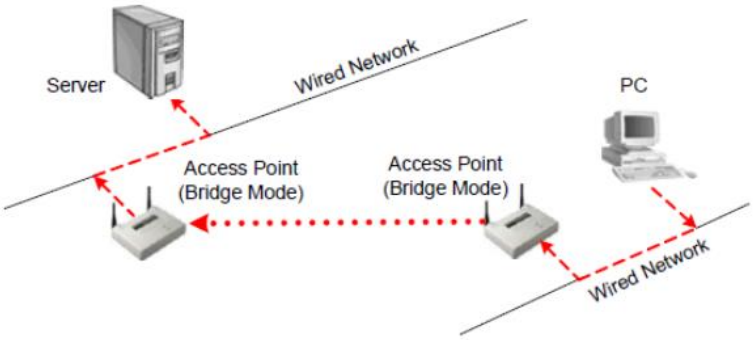
To je základní běžný režim činnosti AP.

- Repeater Mode

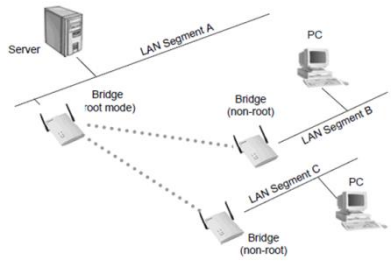


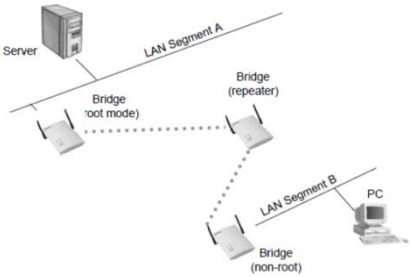
Příjemce je připojen k jinému AP. Jsou potřeba 4 MAC adresy (skutečný odesílatel a příjemce, odesílatel a příjemce na bezdrátovém spoji). Tato situace nastává při bezdrátovém spojení dvou LAN-to je P2P.

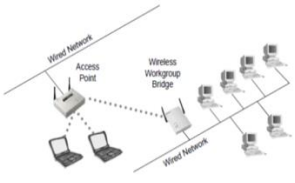
- Bridge Mode



V rámci režimu mostu (Bridge) jsou možné následující možnosti:



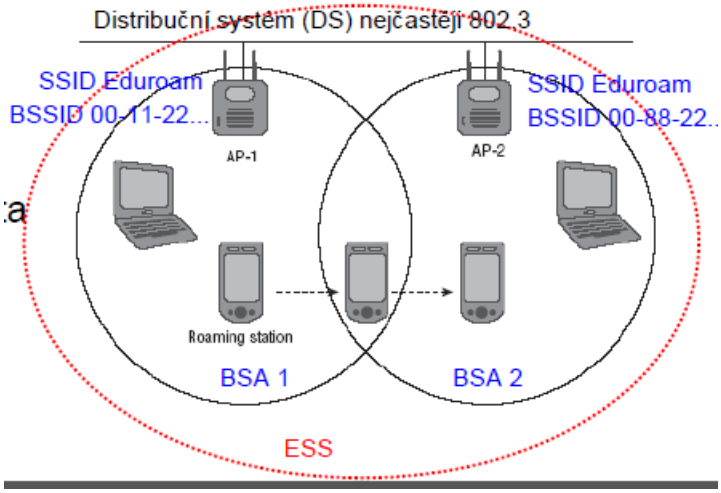




Pozn.: Speciální případ - klient AP, který funguje jako bridge pro více dalších stanic. AP o tomto nic neví a proto komunikuje jednou jeho vlastní MAC add. Jak ti ostatní? Asociace

stanic po jedné za každou (na AP musí být MAC povolené). Jde směrovat, vše se doručuje podle MAC add routeru za bridgem. Další variantou je Proxy ARP. Všechny počítače se „schovají“ za jednu MAC add (NAT na linkové vrstvě). Na bridge je převodní tabulka MAC add (jako arp cache) – podle IP add a AP tabulky je bridge dál přeposílá. Otázka je potom jak dopadne routing.

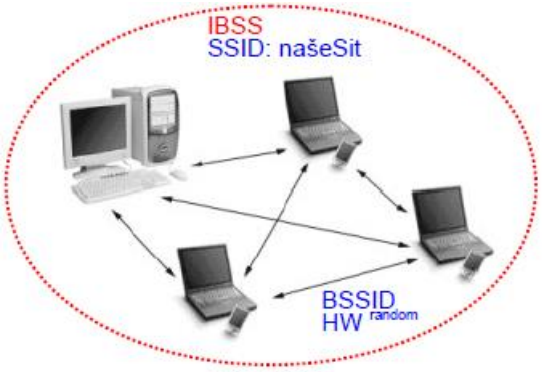
Extended service set - ESSS. Co-chanel Interference (ve 3D!). Při 15 - 20% overlaping (překrytí) se jedná roaming zařízení. Při 100% overlaping (colocation) se zvyšuje kapacita.



https://en.wikipedia.org/wiki/Lightweight_Access_Point_Protocol

Někdy je AP zbytečný a proto je definována topologie – Ad-Hoc.

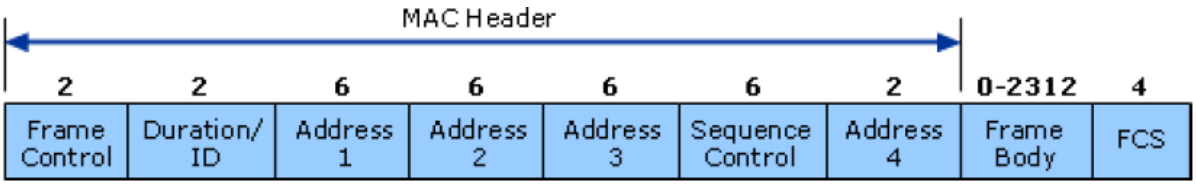
Independent basic service set – IBSS. Neexistuje mezilehlý uzel a klienti komunikují přímo mezi sebou - musejí se „vidět“. Vlastnosti - vyšší globální spolehlivost a obecně nižší dosah. Jedná se většinou pouze jako „optional“.



Asociace a autentizace WiFi – přístup do datové sítě prostřednictvím AP

Na linkové vrstvě jsou realizována tzv. Integration Services např. mezi 802.3-802.11-802.x. Pro koexistenci potřebujeme v rámci WiFi následující identifikace BSSID (BSS) nebo MAC (IBSS), dále DA (destination add) a SA z 802.3, receiver a transmitter add (např. MAC). Závisí také na režimu komunikace (DS – distribuční systém).

→ DS	← DS	AD 1	AD 2	AD 3	AD 4
0	0	Destination	Source	BSSID	N/A
0	1	Destination	BSSID	Source	N/A
1	0	BSSID	Source	Destination	N/A
1	1	Receiver	Transmitter	Destination	Source



Protože WiFi nemá pevné hranice, je potřeba odlišit jednotlivé uživatele příslušející k různým sítím. O to se starají

- vrstva autentizační a asociační
- vrstva zabezpečení přenášených dat

Pozn.:

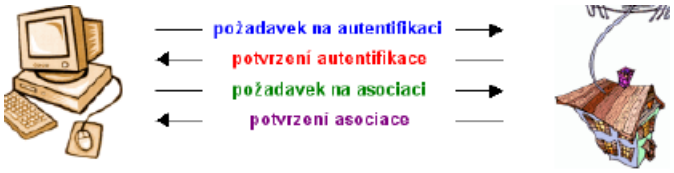
- Autentizace - odpovídá zapojení Ethernetového kabelu
- Asociace - odpovídá rozhodnutí „můžeš začít komunikovat“ (association RQ → AP → association RSPn)

Pro připojení stanice se používají metoda otevřeného systému (Open –system) a metoda sdíleného klíče (Shared Key).

V obou případech se začíná broadcast dotazem na existenci AP – Probe Request. Je-li AP v dosahu odpoví (Probe Response).

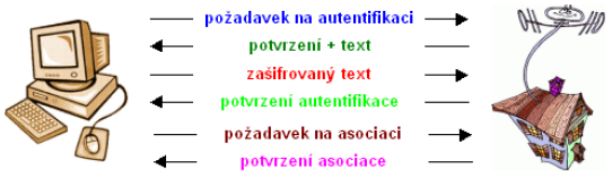
Metoda Open-system

Metoda vyžadována v 802.11. Klient je autentizován na základě informací jim zaslaných, které nejsou nikde ověřovány. AP vždy autentizuje klienta (pokud splní HW předpoklady).



Metoda sdíleného klíče – Shared Key

Vyžadována pro všechna zařízení s podporou WEP. Shared Key autentizace - klient usilující o připojení musí správně (správným klíčem) zašifrovat (RC4) zaslaný klíč (náhodně vygenerované číslo).



Pozn.: Jedná se o základní autentizační metodu – challenge-reponse. Nevýhodou je zasílání textu v otevřené a následně v zašifrované formě….

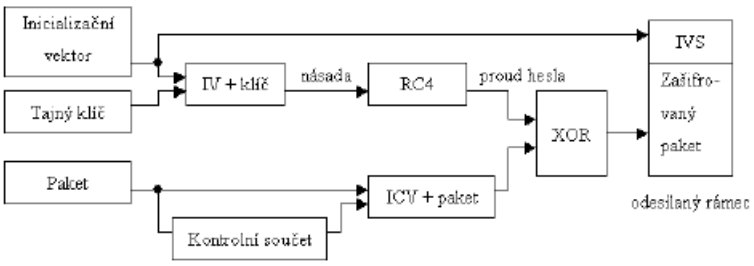
Proběhne-li úspěšně asociace, je klient připojen k síti – asociován.

Předpokladem úspěšné asociace je i znalost SSID. SSID je AP pravidelně v rámci BSA prezentováno. Toto je možné zablokovat, ale v případě dotazu na SSID musí odpovědět…

Dalším asociačním nástrojem je filtr MAC adres a asociovány jsou pouze z platného seznamu. Bohužel MAC adresy se vysílají v nezašifrované podobě i v případě šifrování dat. Problém s asociací filtrem MAC se pozná tak, že proběhla autentizace, ale nepřišlo potvrzení asociace - responze (RSPn).

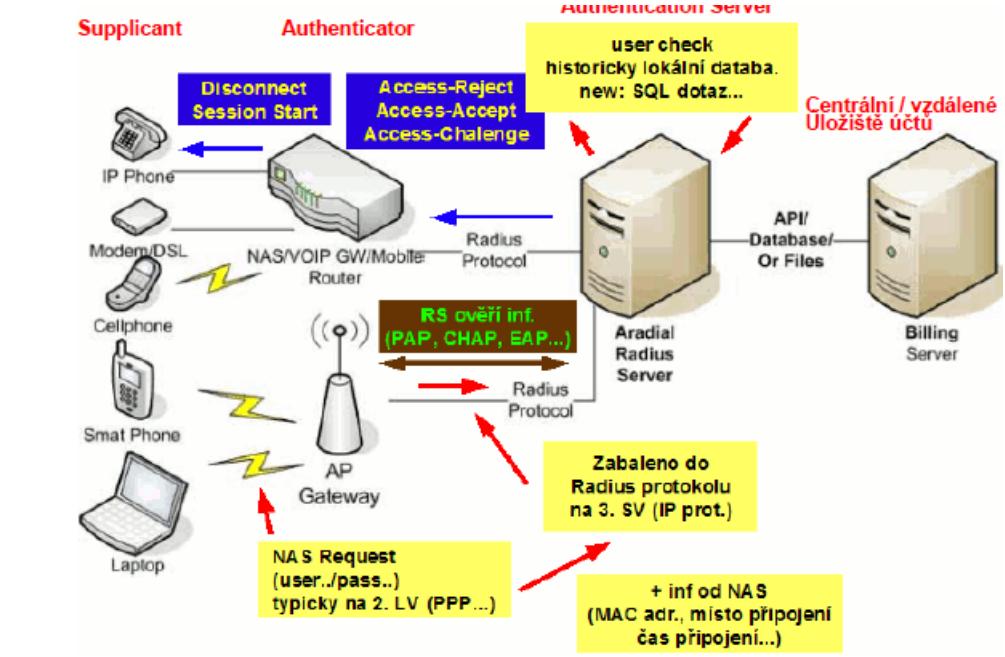
Problémem MAC filtru je manuální správa (administrátor). Tedy bez možnosti dynamické změny klientů.

Dále se používá WEP jakožto volitelný doplněk 802.11 pro řízení přístupu k síti a zabezpečení přenášených dat. Je však potřeba nastavit na klientských stanicích.



Pozn.: WEP = 40b(104) klíč + 24b inicializační vektor (40b – 10 hex znaků, 104 – 26 hex znaků)

Pozn.: Zopakovat architekturu EAPOL



Přehled způsobů zabezpečení:

802.11 Standard	*Wi-Fi Aliance certif. program*	*Metoda autentizace*	*Metoda šifrování*	*Šifra*
802.11 (legacy)		Open systém	WEP	RC4
	WPA-Personal	WPA-PSK	TKIP	RC4
	WPA-Enterprise	802.1x/EAP	TKIP	RC4
802.11-2007 (RSN)	WPA2-Personal	WPA2-PSK	CCMP (předepsaný)	AES
			TKIP (možný)	RC4
802.11-2007 (RSN)	WPA2-Enterprise	802.1x/EAP	CCMP (předepsaný)	AES
			TKIP (možný)	RC4

Pozn.: Metoda WPA podporuje jenom infrastrukturní topologii.

Přehled typů datových rámců (frame) používaných WiFi:

- Management Frames
  - Association request frame
  - Association response frame
  - Reassociation request frame
  - Reassociation response frame
  - Probe request frame
  - Probe response frame
  - Beacon frame
  - ATIM frame
  - Disassociation frame
  - Authentication frame
  - Deauthentication frame
- Control Frames
  - Request to send (RTS)
  - Clear to send (CTS)
  - Acknowledgement (ACK)
  - Power-Save Poll (PS Poll)
  - Contention-Free End (CF End)
  - CF End + CF Ack
- Data Frames

O některých bylo zmíněno (control frames či některé management frames). Dále to nebudeme rozebírat ☺.

Zajištění komunikace mezi více AP – viz prezentace CISCO

Přehled nosných standardů WiFi

IEEE 802.11a

Schváleno v r. 1999, ČTÚ povolil k užívání 1.9.2005

- 5,470 – 5,725 GHz (255 MHz)
- 11 nepřekrývajících se kanálů s odstupem 20 MHz
- Max. rychlost 54 Mbit (54,48,36,24,18,12,9,6 Mbit/s)
- Ad-hoc (P2P), Infrastructure
- OFDM (Orthogonal Frequency Division Multiplexing)
- BPSK, QPSK, 16-QAM, 64-QAM

IEEE 802.11b

Schváleno v r. 1999, ČTÚ povolil k užívání v r. 2000

- 2,412 – 2,472 GHz (60 MHz)

- 13 kanálů s odstupem 5 MHz, kanál má šířku cca. 22 MHz
- Max. rychlost 11 Mbit (11, 5,5, 2, 1 Mbit/s)
- Ad-hoc (P2P), Infrastructure
- DSSS (Direct Sequence Spread Spectrum)
- 30 –4% kapacity tvořírežie0

IEEE 802.11g

Schváleno v r. 2003, ČTÚ povolil k užívání v r. 2000

- 2,412 – 2,472 GHz (60 MHz)
- 13 kanálů s odstupem 5 MHz, kanál má šířku cca. 22 MHz
- OFDM a DSSS (pro kompabilitu)
- Max. rychlost 54 Mbit OFDM: 16-QAM (54, 48, 36, 24 Mbit/s) QPSK (18, 12 Mbit/s) BPSK (9, 6 Mbit/s)
- DSSS: (11, 5,5, 2, 1 Mbit/s)

IEEE 802.11p

Schválení v listopadu 2010 ?

- WAVE (Wireless Access for the Vehicular Environment)
- Licencované pásmo 5,9 GHz
- Až pro rychlosti do 200 km/h
- Max. rychlost 27 Mbit/s
- Dosah v řádu km
- Kooperace s CALM, DSRC

IEEE 802.11n

Schváleno 11.9.2009

- 2,4 GHz a 5 GHz s kanálem 40 MHz (dva sdružené 20 MHz kanály)
- Upravené ODFM –52 dílčích datových pásem
- MIMO (Multiple Input Multiple Output)
- Dostupná max. rychlost 300 Mbit (Draft 2.0)
- Teoretická max. rychlost až 600 Mbit (4 nezávislé 40 MHz kanály)
- Kompatibilita s 802.11a/b/g