Računarske mreže 1

5. deo: Wireless LAN

Predavač:

Prof. dr Slavko Gajin, slavko.gajin@rcub.bg.ac.rs

Asistent:

Stefan Tubić, stefan.tubic@etf.bg.ac.rs
Marko Mićović, micko@etf.bg.ac.rs
Kristijan Žiza, ziza@etf.bg.ac.rs

http://elearning.rcub.bg.ac.rs

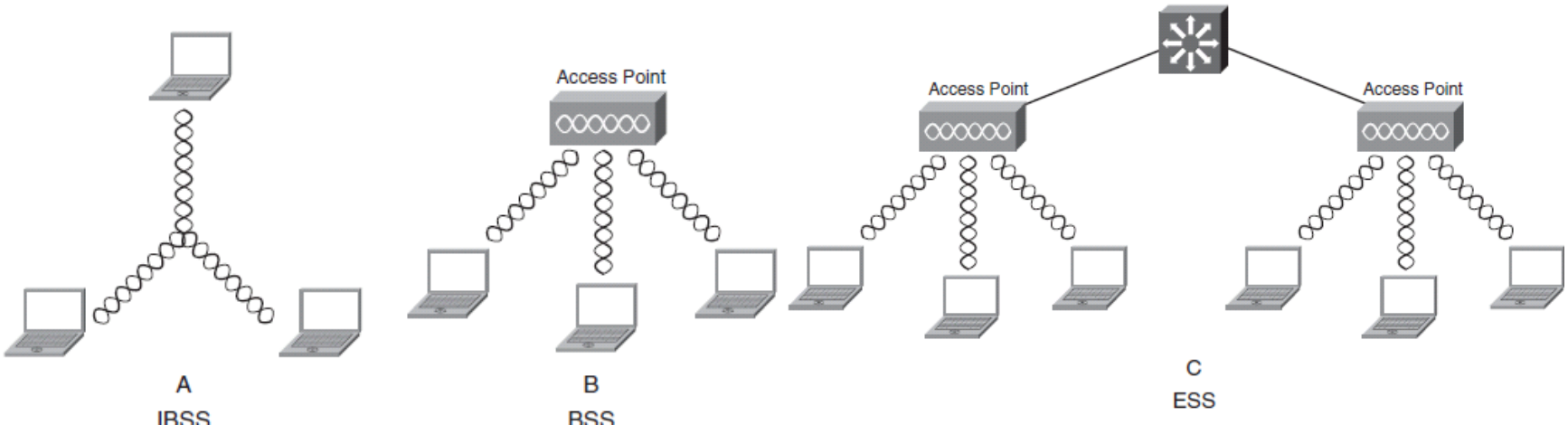
2020. god

WLAN – Wireless LAN

- WLAN (*Wireless LAN*) - Bežične lokalne računarske mreže
- WLAN standard - IEEE 802.11
  - Deljeni medijum – jedna frekvencija
  - *half-duplex* – samo jedna stanica može da šalje podatke u jednom trenutku
  - nije Ethernet !
- Kolizija se ne može detektovati:
  - tokom slanja podataka, prijem podataka je isključen - kolizija se ne može detektovati kao kod “žičanog” Etherneta
  - Zbog slabljenja signala ne može se garantovati da će svi uređaji da detektuju koliziju (tzv. „*hidden station*“)
- Izbegavanje kolizije – *Collision Avoidance* (CSMA/CA)
  - Zahteva se slanje potvrde za uspešan prijem svakog okvira

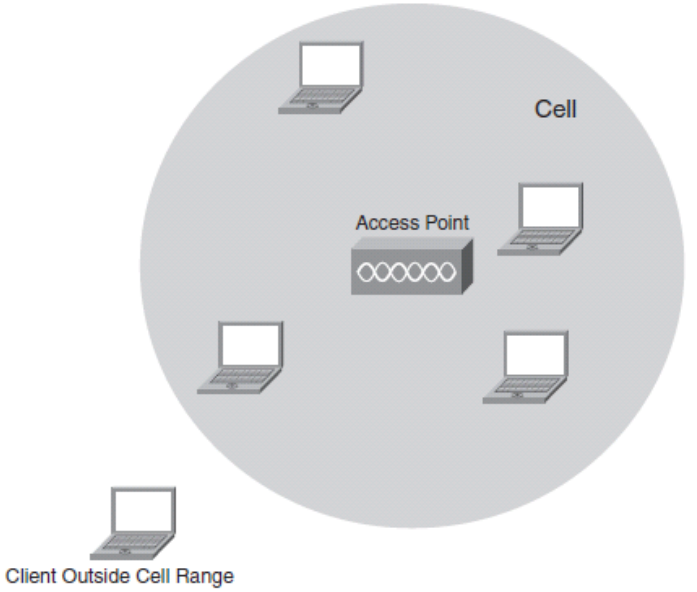
Arhitektura WLAN

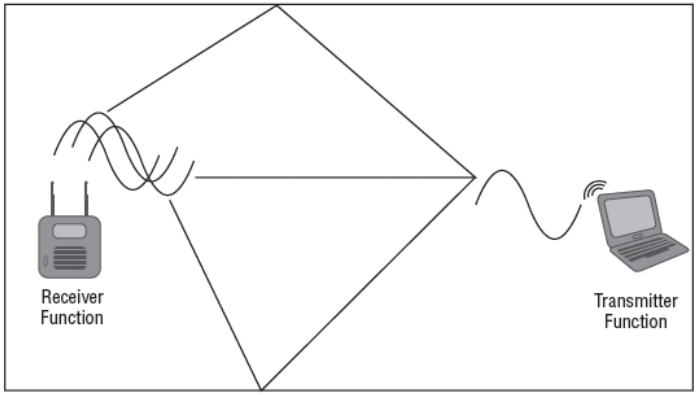
- "Service Set" - grupa povezanih bežičnih uređaja – WLAN mreža
- Ad-hoc mod:
  - **IBSS – *Independent Basic Service Set***
    - svi učesnici ravnopravni
- Infrastrukturni mod**:**
  - **BSS - Basic Service Set**
    - centralni AP uređaj – *Access Point*
    - sva komunikacije se obavlja preko AP-a
  - **ESS – Extended Service Set** – više AP povezanih preko sviča



Arhitektura WLAN

- **AP - Access Point**
  - centralni uređaj u WLAN mreži
- WLAN ćelija (*cell*)
  - oblast dometa signala jednog AP
- Refleksija od objekata u okruženju stvara izobličavanje signala
  - dve antene na AP razmaknute za ½ talasne dužine - kompenzacija izobličenja





Arhitektura WLAN

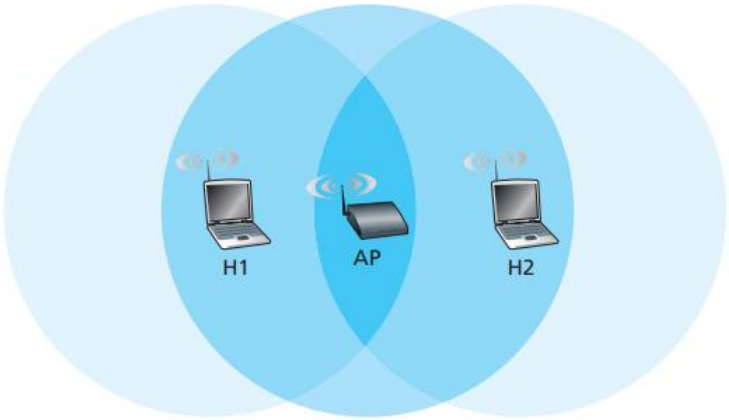
- SSID – *Service Set Identifier*
  - Naziv grupe bežičnih uređaja – naziv WLAN mreže
  - Tekst do 32 karaktera
  - *beacon* okvir
    - Periodično oglašava AP
    - Sadrži SSID i MAC adresu AP
    - Mreža postao vidljiva za ostale uređaje („mreže u dometu“)

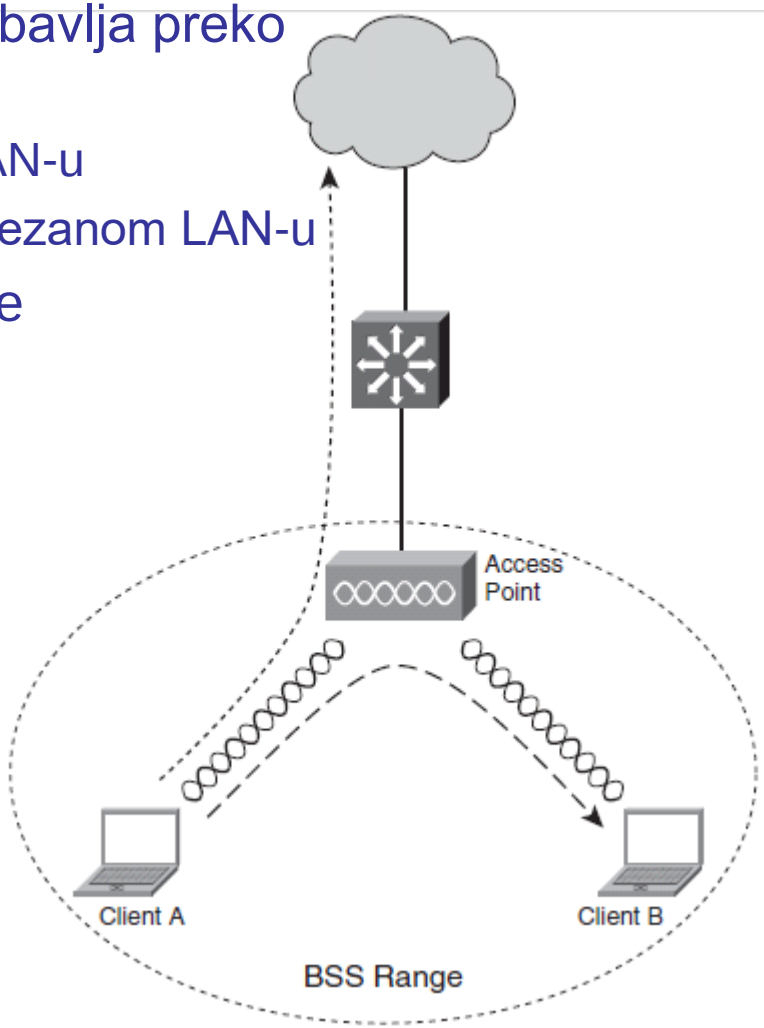
Arhitektura WLAN

- Asocijacija - učlanjenje u bežičnu mrežu
- Osnovni proces učlanjivanja (asocijacije)
  - *association request message* – klijent šalje zahtev AP-u
  - *association reply message* – AP odgovara klijentu - prihvata ili odbija zahtev
- Složeniji proces učlanjenja
  - više poruka, opcija i sigurnosnih parametara
- Uslov za povezivane:
  - Kompatibilnost (podržani standardi, frekvencije itd.)
  - SSID – korisnik se povezuje na izabranu mrežu
  - Autentifikacija korisnika

Arhitektura WLAN

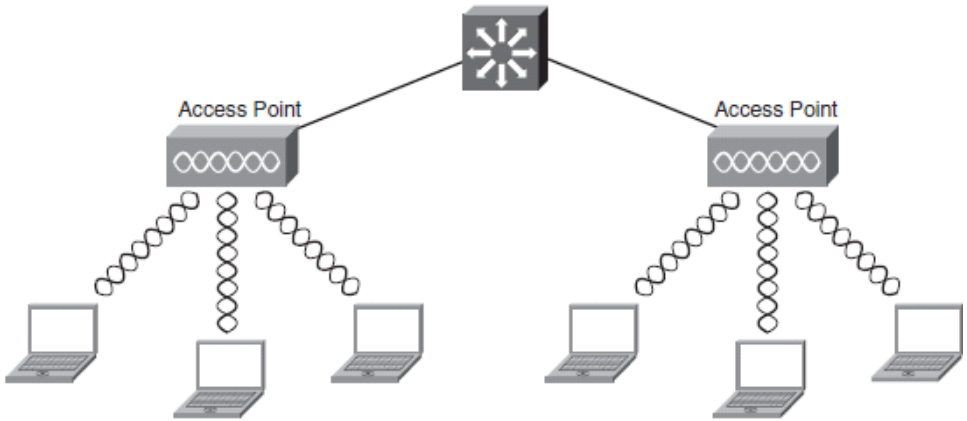
- Sva komunikacije na fizičkom nivou se obavlja preko AP-a:
  - Komunikacija sa drugim klijentima u WLAN-u
  - Komunikacija sa ostalim uređajima u povezanom LAN-u
- AP prenosi i okvire sa podacima i potvrde
- Svi uređaju mogu da detektuju okvire, ali ih prihvataju samo od AP
- Rešenje i za „*hidden station*“





Povezivanje u LAN mrežu

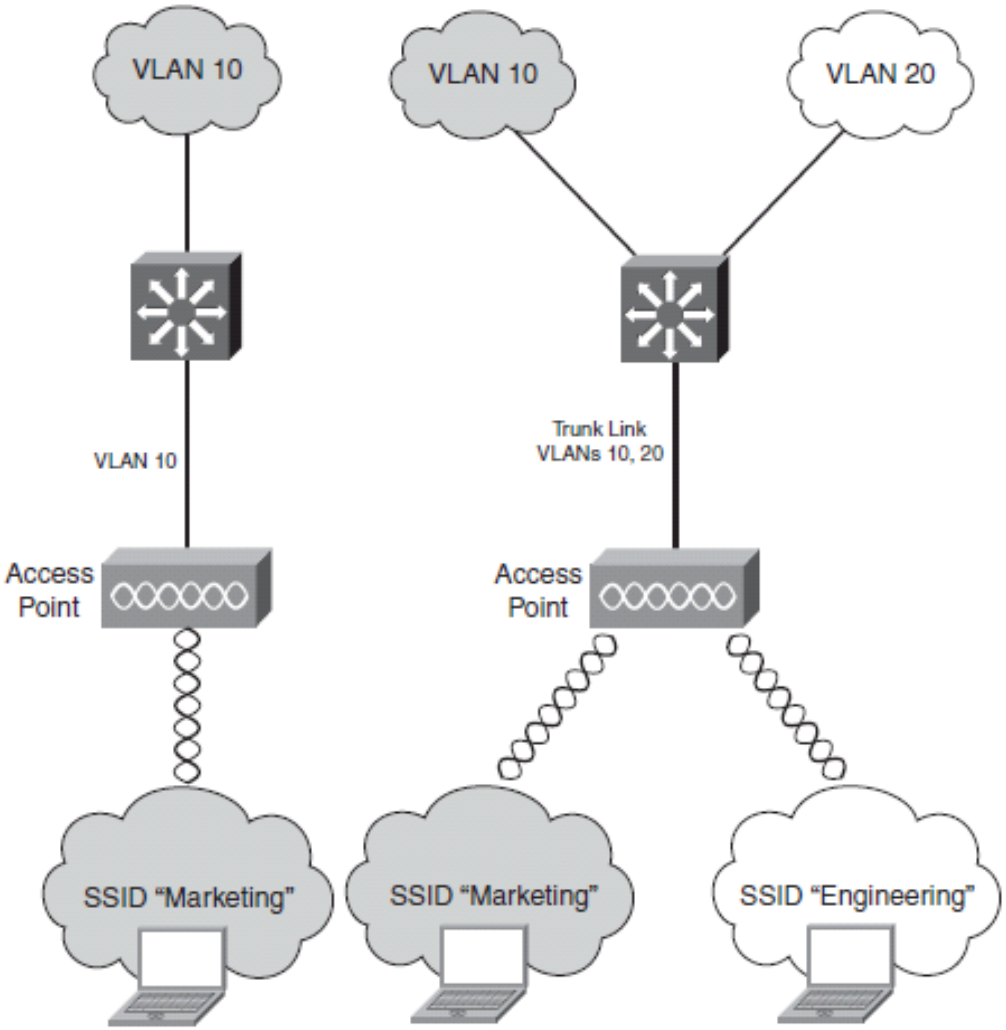
- AP je aktivni uređaj
  - Zahteva napajanje
- AP ima i Ethernet karticu
  - Povezuje se na svič – *bridge mode* između WLAN i LAN
- *Power Over Ethernet* (PoE)
  - Posebni svičevi koji prenose DC napajanje preko UTP kablova
  - AP se može napajati preko PoE



Povezivanje u LAN mrežu

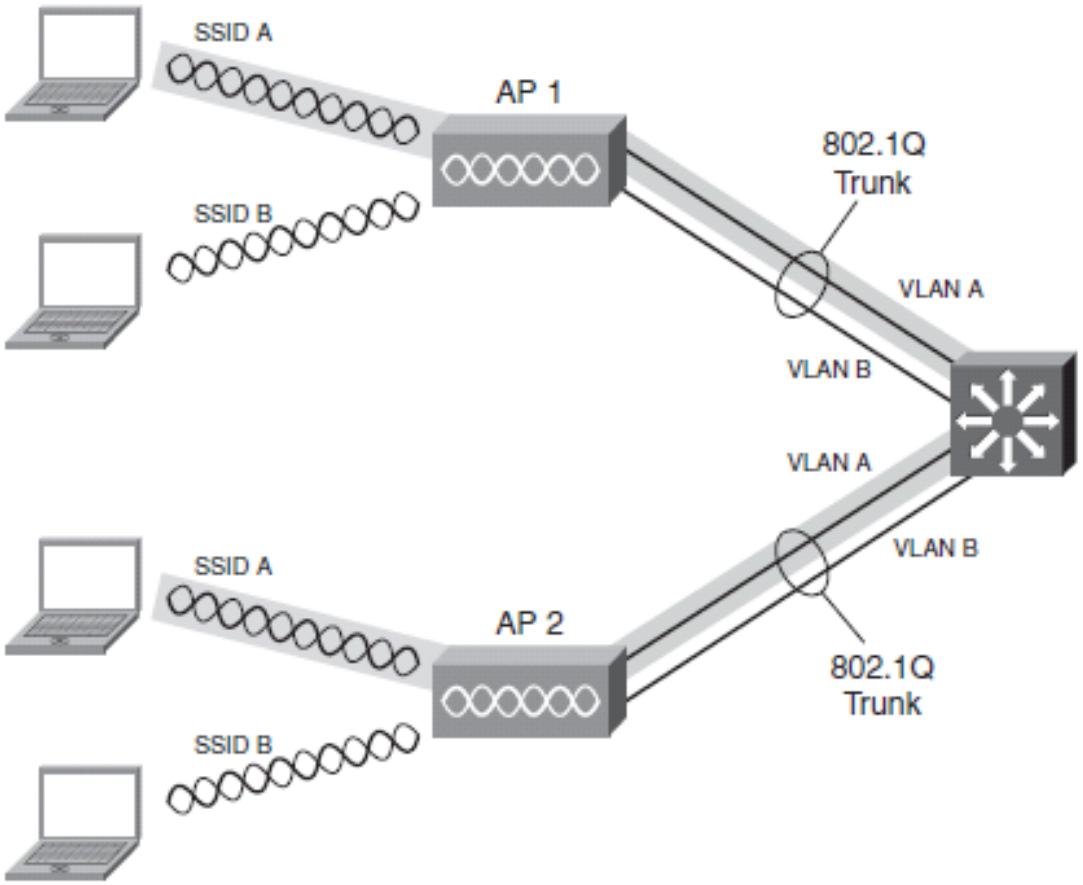
Integracija sa VLAN-ovima

- mapiranje SSID-a u VLAN
- više SSID-a na jednom AP uređaju – u odvojene VLAN-ove
  - trank link sa svičem



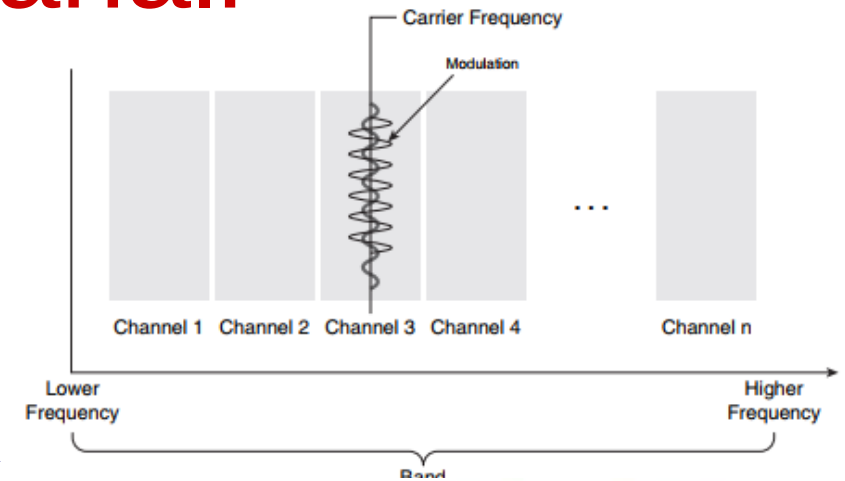
Povezivanje u LAN mrežu

- Proširivanje SSID na više AP uređaja preko LAN mreže
- Svaki SSID jedan VLAN
- trank između AP i sviča

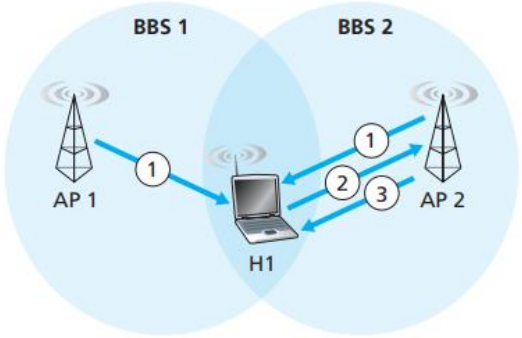


WLAN kanali

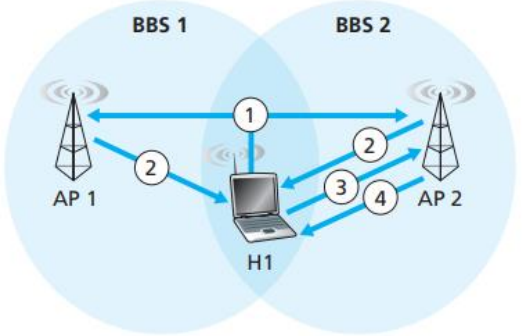
- Kanali, frekvencijski domen širine od 22Mhz
- WLAN podržava više kanala
- AP radi samo na jednom kanalu
- Skeniranje kanala – traži se kanal na kom je signal najjači



  - Pasivno skeniranje
    - Uređaj čeka da AP oglasi *beacon* okvir

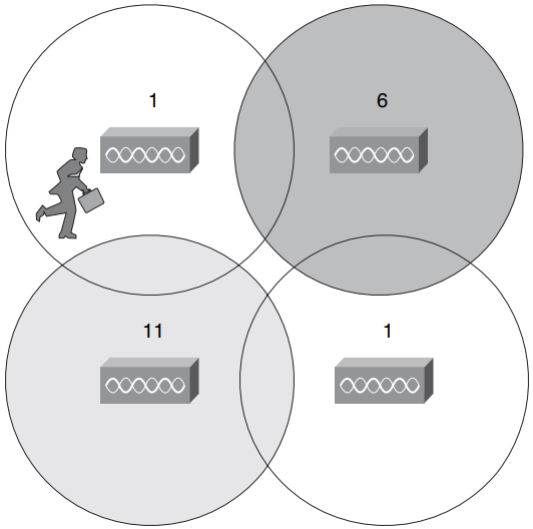


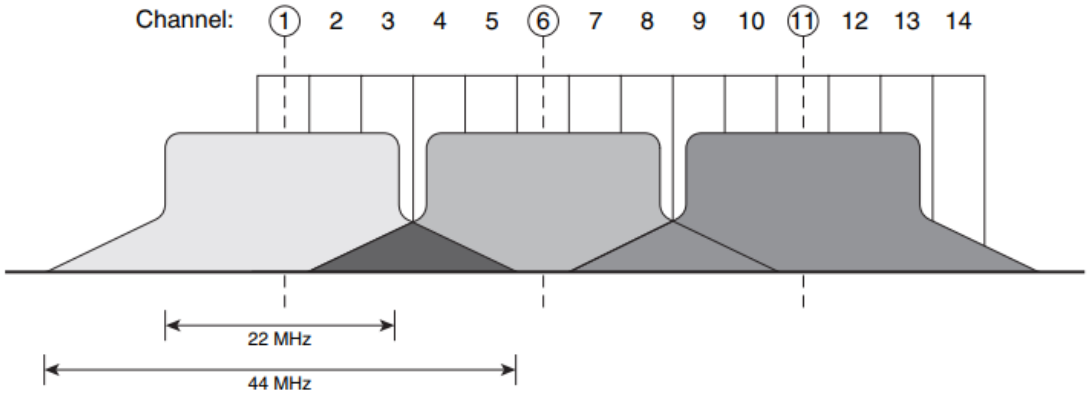
  - Aktivno skeniranje
    - Uređaj šalje se poseban upit za raspoložive kanale – *Request Probe* paket



WLAN kanali

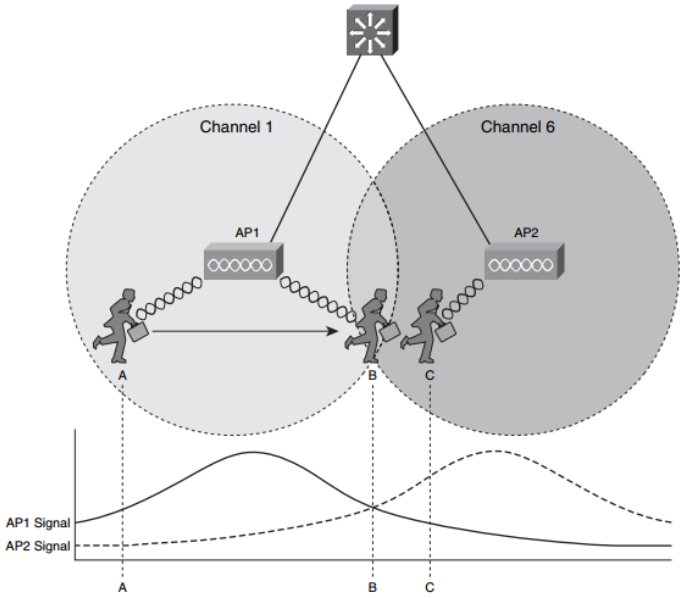
- Pokrivanje većeg prostora – ćelije moraju da se preklope
- Susedni kanali su razdvojeni za 5 MHz
  - međusobno su preklopljeni
- Preklopljene ćelije koriste različite i dovoljno udaljene kanale

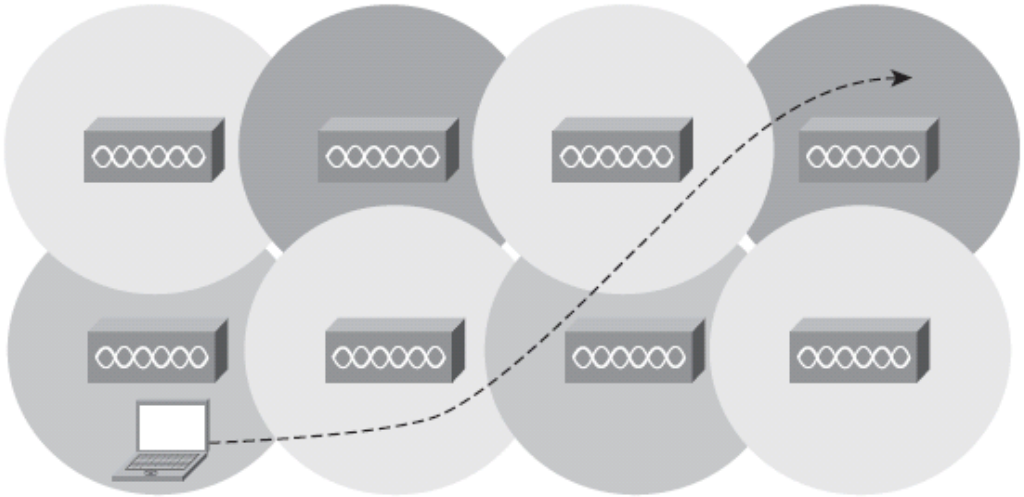




WLAN pokrivenost

- Roming (*roaming*)
  - Prelazak iz jedne ćelije u drugu bez gubitka veze
- Omogućava mobilnost korisnika





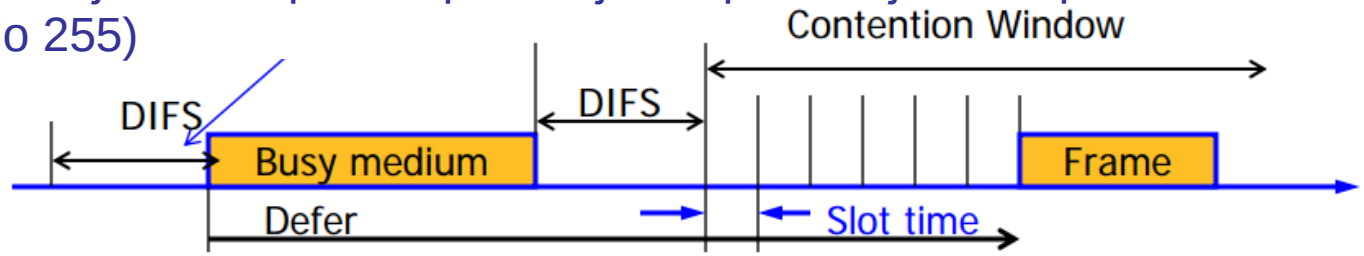
CSMA/CA

Dva pristupa za izbegavanje kolizije na MAC nivou:

- Centralizovana koordinacija
  (*PCF – Point Coordination Function*)
  - Jedan centralni uređaj (AP) „proziva“ ostale uređaje i daje im dozvolu za slanje
  - Samo Infrastrukturne mreže
  - Retko se koristi u praksi
- Distribuirana koordinacija
  (***DCF – Distributed Coordination Function***)
  - Svi uređaji su jednaki (uključujući i AP) i „nadmeću“ se za zauzimanje medijuma
  - Infrastrukturne i ad-hoc mreže
  - Dominantan pristup u praksi

DCF – Distriburirana koordinacija

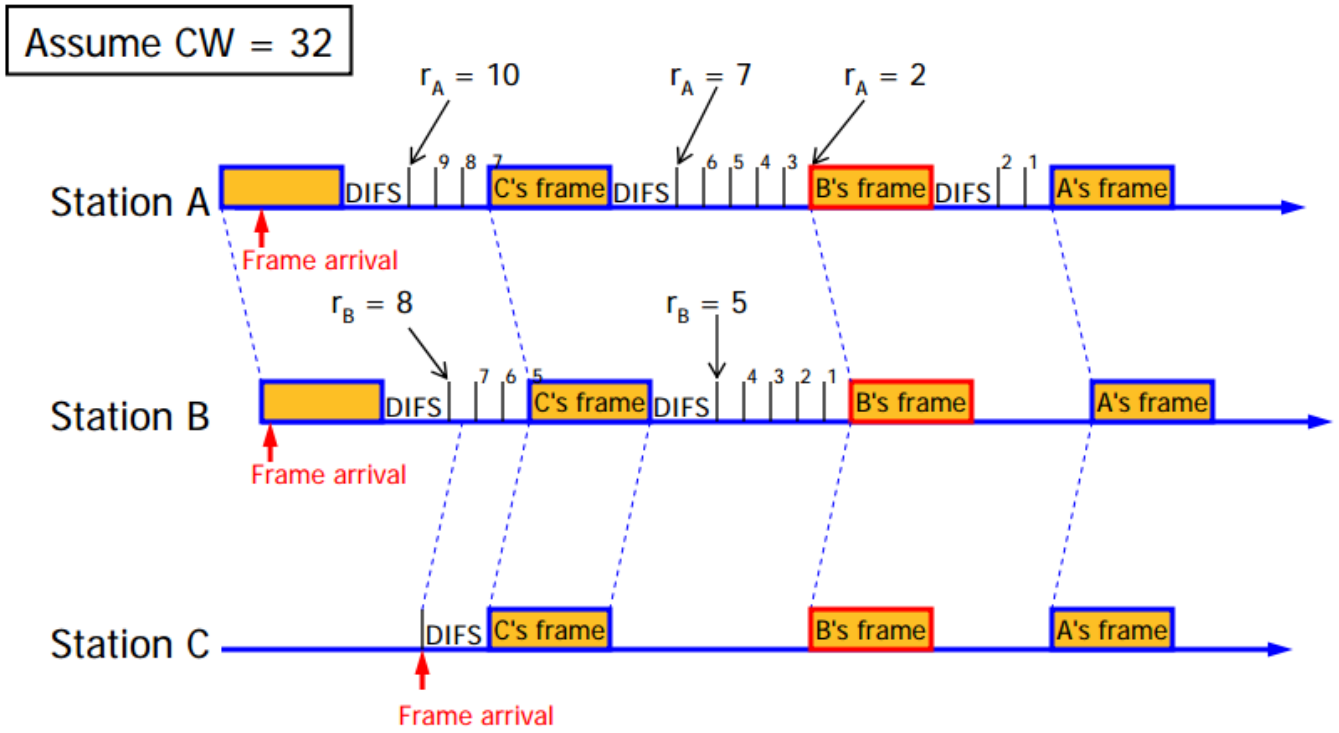
- Kada stanica želi da šalje podatak (okvir), ona “sluša” medijum:
  - Ako je medijum slobodan – okvir se šalje
  - Ako je medijum zauzet
    - čeka se da se medijum oslobodi
    - čeka se fiksni vremenski interval
      DIFS – Distributed Inter Frame Space
    - dodatno se čeka i slučajan vremenski interval – ***back-off***
  - ***Back-off***
    - vreme čekanja, izraženo u broju *slot-time* vremena (npr. ST=20μs)
    - bira se slučajan broj R (od 0 do CW - *Contention Window*)
    - back-off time = R x ST
    - sa brojem neuspešnih pokušaja eksponencijano se povećava CW (do 255)



DCF – Distriburirana koordinacija

Ako medijum postane zauzet tokom čekanja back-off vremena

- back-off vreme se zaustavlja
- back-off vreme nastavlja da teče kada se mediju oslobodi



DCF – Distriburirana koordinacija

- Izbegavanje kolizije - obavezna potvrda prijema
  ***Positive Acknowledgement* (ACK)**
  - Svaki okvir koji se uspešno primi bez kolizije mora da se potvrdi
  - Ako ima kolizije, potvrda izostaje u očekivanom vremenu, okvir se reemituje

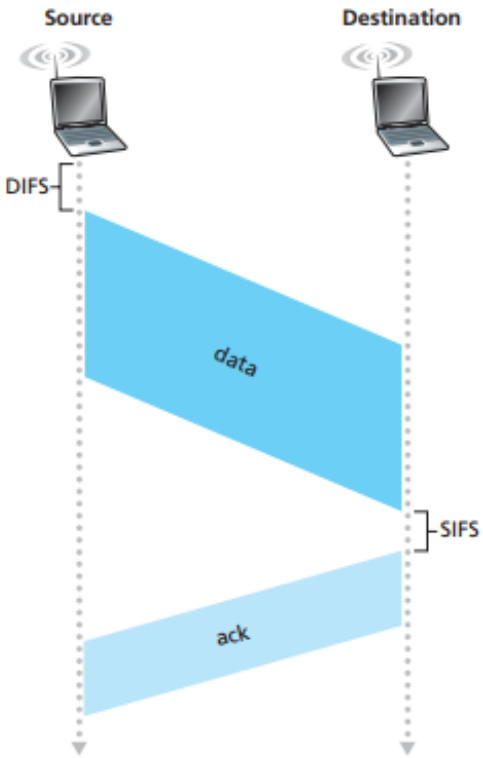
Dva režima prenosa okvira (od A do B)

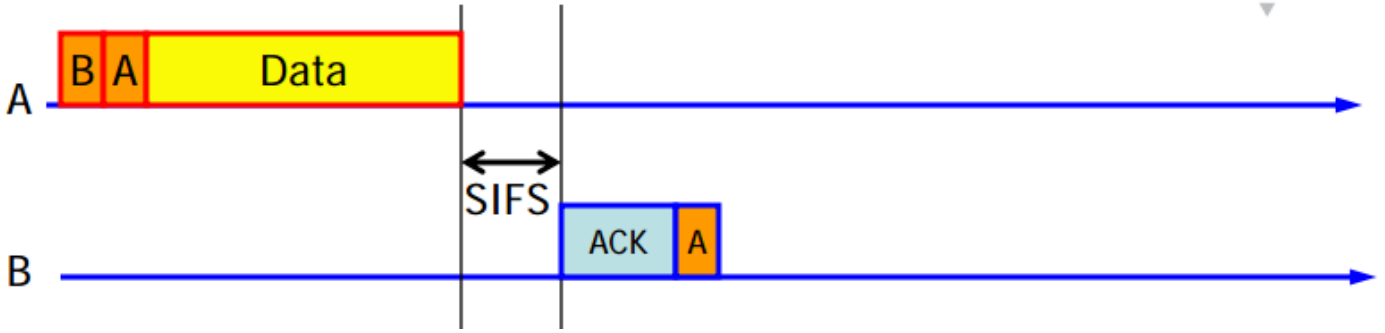
- Prenos u dva koraka (*two-way handshake, Positive Acknowledgement*)
  1. (A -> B) okvira sa podacima (A -> B)
  2. (B -> A) potvrda (*Acknowledgement)*

- Prenos u četiri koraka (*four-way handshake, RTS/CTS*)
  1. (A -> B) zahtev za prenos (RTS – *Request To Send*)
  2. (B -> A) odobravanje prenosa (CTS – *Clear To Send*)
  3. (A -> B) okvira sa podacima
  4. (B -> A) potvrda (*Acknowledgement)*

DCF - Prenos u dva koraka

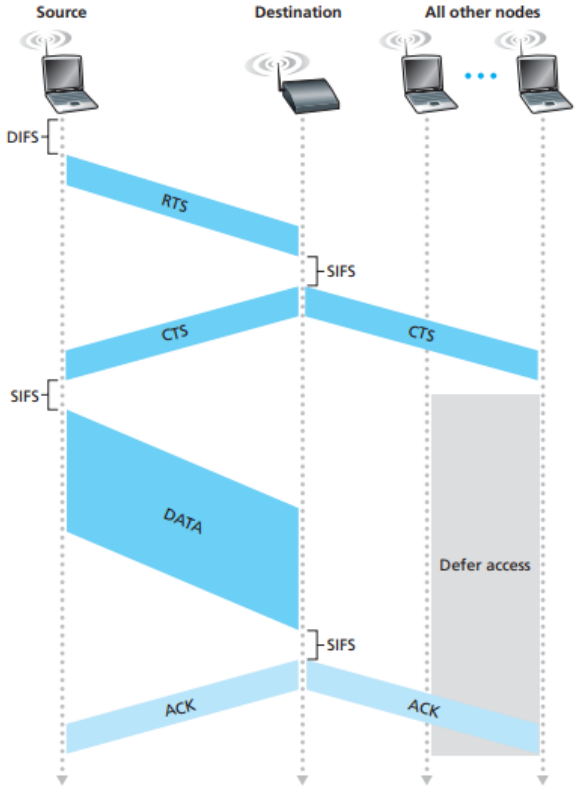
- Prenos u dva koraka (*two-way handshake*)
  1. (A -> B) okvira sa podacima (A -> B)
  2. (B -> A) potvrda (*Acknowledgement)*
- *SIFS – Short Inter Frame Space*
  - kratko vreme čekanja da pristigne ACK okvir



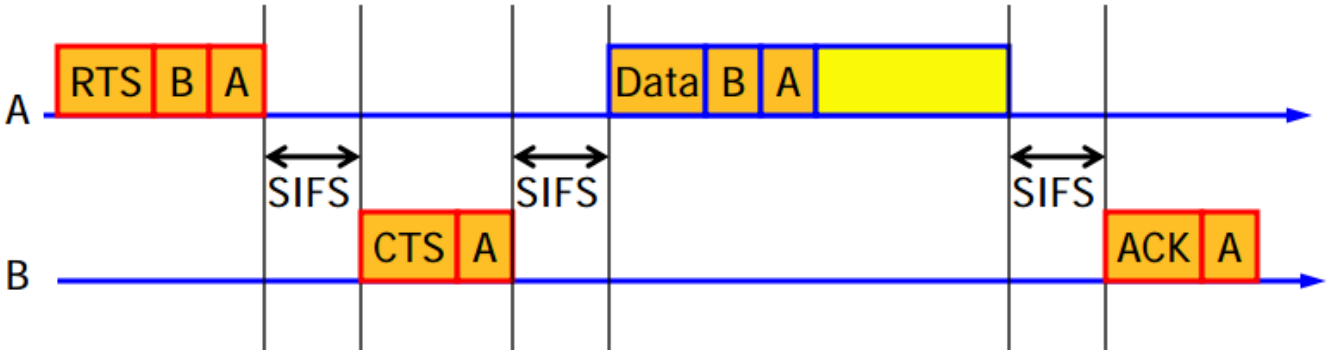


DCF - Prenos u četiri koraka

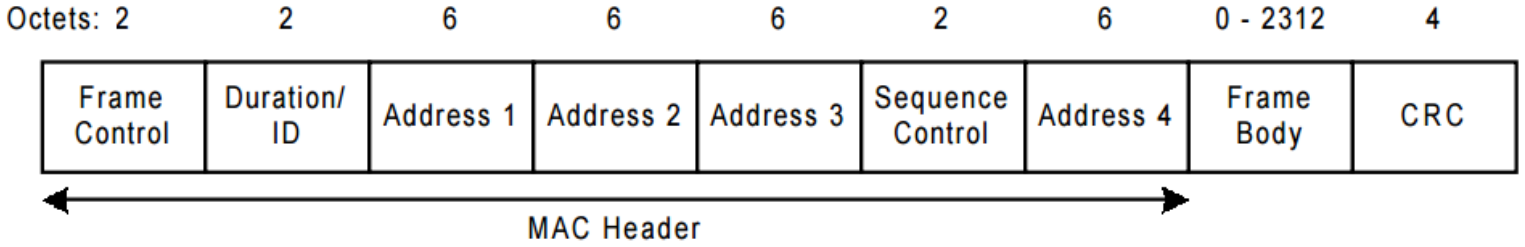
- Prenos u četiri koraka
  (*four-way handshake, RTS/CTS*)
  1. (A -> B) zahtev za prenos (RTS – *Request To Send*)
  2. (B -> A) odobravanje prenosa (CTS – *Clear To Send*)
  3. (A -> B) okvira sa podacima
  4. (B -> A) potvrda (*Acknowledgement)*



- Rezerviše se period za slanje okvira
- Obično se koristi kod slanja velikih okvira



Format okvira



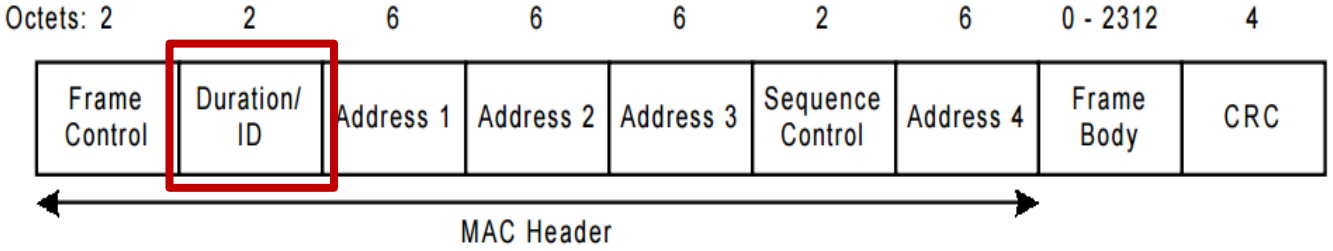
- *Frame Control* – različiti flegovi
- CRC – kontrola greške
- Zbog prenos okvira preko AP, postoji više vrsta adresa:
  - *Source Address* (SA) – izvorišni uređaj
  - *Transmitter Address* (TA) - izvorišni uređaj ili AP
  - *Receiver Address* (RA) – odredišni uređaj ili AP
  - *Destination Address* (DA) – odredišni uređaj
  - SSID - AP
- Korišćenje adresnih polja zavisi od konkretne namene
  - Određeno sa dva flega u kontrolnom polju: „To DS“, „From DS“ (*Distribution System*)

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA = DA	TA = SA	BSSID	N/A
0	1	RA = DA	TA = BSSID	SA	N/A
1	0	RA = BSSID	TA = SA	DA	N/A
1	1	RA	TA	DA	SA

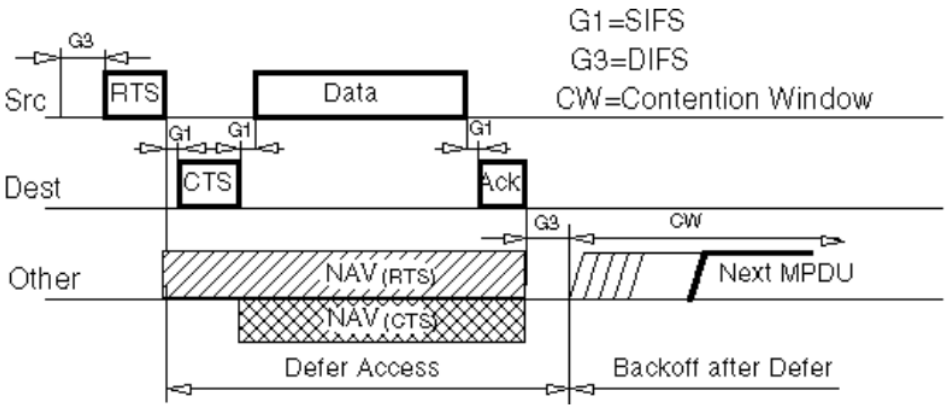
Vreme zauzeća medijuma

Procena vremena zauzeća medijuma - *Network Allocation Vector* (NAV)

- zavisi od veličine okvira i brzine prenosa okvira
- polje u zaglavlju okvira sadrži procenu vremena korišćenja medijuma
- ostali uređaji znaju kada će se medijum osloboditi



- Osluškivanje medijuma (*Carrier Sense*)
  - Fizičko – sluša se da li je medijum slobodan ili zauzet
  - Virtuelno – tokom trajanja NAV vremena



Wireless sigurnost

- Sigurnosni problemi
  - Deljeni medijum – svi članovi mreže mogu da čitaju pakete
  - Kontrola pristupa – povezivanje i bez fizičkog prisustva objektu
- Rešenja
  - WEP – *Wired Equivalent Privacy*
  - WPA – *Wi-Fi Protected Access*
  - *IEEE 802.1i* (WPA2 - *WiFi Protected Access 2*)

Wireless sigurnost

WEP – *Wired Equivalent Privacy*

- Uvodi se šifrovanje paketa statičkim simetričnim ključem
- Problemi:
  - Statičko definisanje ključa – svaki korisnim mora ručno da podešava ključ (komplikovano, nepromenljivo)
  - Ključ je nedovoljne dužine
    - Ukupna dužina 64 bita, ali se za šifrovanje koristi samo 40 bita
    - slaba zaštita, relativno se lako „provali“ automatizovanim variranjem svih vrednosti (*brute force attack*)
- Ad-hoc rešenja proizvođača
  - Sakrivanje SSID naziva – AP ne oglašava SSID
  - Filtriranje po MAC adresama – ručno se dozvoljava pristup samo za određene MAC adrese

Wireless sigurnost

WPA – *Wi-Fi Protected Access*

- Wi-Fi – aliance proizvođača wireless opreme
  - sinonim za WLAN standarde
- Industrijski *de facto* standard
- Prednosti:
  - Dinamička razmena ključeva – mogućnost česte promene ključa
  - Autentifikacija korisnika
    - pristupni ključ
    - username/password (802.1x)
- Posledice
  - Velika podrška proizvođača
  - Sertifikacija od strane Wi-Fi alijanse
  - Nastavljen proces formalne standardizacije

Wireless sigurnost

***IEEE 802.1i* (WPA2 - *WiFi Protected Access 2*)**

- Formalni standard (2005)
- WPA2 – neformalni, ali uobičajeni naziv
- Unapređena sigurnost
  - AES – *Advanced Encryption Standard*
    - Sigurniji algoritam šifrovanja
    - Ključ veće dužine
- Nekompatibilan sa WEP i WAP
- Preporuka za korišćenje u današnjim *wireless* mrežama

Wireless standardi

- IEEE 802.11a (1999)
  - 5Ghz, od 6 Mbps do 54 Mbps
  - skuplji, manja pokrivenost
- IEEE 802.11b (2000)
  - 2.4 GHh, max protok 11Mbps (*Dynamic data rate scaling*-1, 2, 5.5 i 11Mbps)
  - jeftiniji, mala brzina
- IEEE 802.11g (2003)
  - 2.4 GHz, max protok 54 Mbps (6, 9, 12, 18, 36, 48 i 54 Mbps)
  - kompatibilan sa 802.11b – „najmanji“ zajednički standard
    - Ako je jedan uređaj povazan preko 802.11b, AP će automatski da pređe na 802.11b – maksimalna brzina limitirana na 11 Mbps !
- IEEE 802.11n (2007)
  - 2.4 i 5 GHz, do 450Mbps (u realnosti max oko 240Mbps
  - kompatibilan sa 802.11b i 802.11g
- IEEE 802.11ac (2013)
  - Teorijska max protok 1300Mbps, u realnosti oko 700Mbps

Kako koristi WLAN

- WiFi bez ključa su nebezbedne
  - Svako može da pristupi
  - Nema šifrovanja podataka
- Podešavanje WiFi uređaja
  - Birati nepersonalizovani SSID
  - Postaviti WPA2 i „jak“ ključ (lozinka)
  - Izabrati kanal koji je najmanje zauzet
    - WiFi Analyzer
      - besplatna mobilna aplikacije (ali sadrži reklame)