

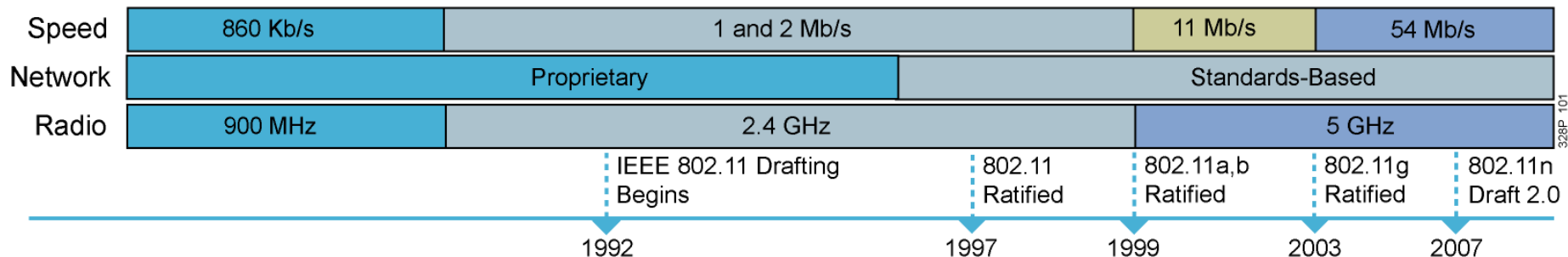
RAČUNARSKE MREŽE

13 – Bežične mreže

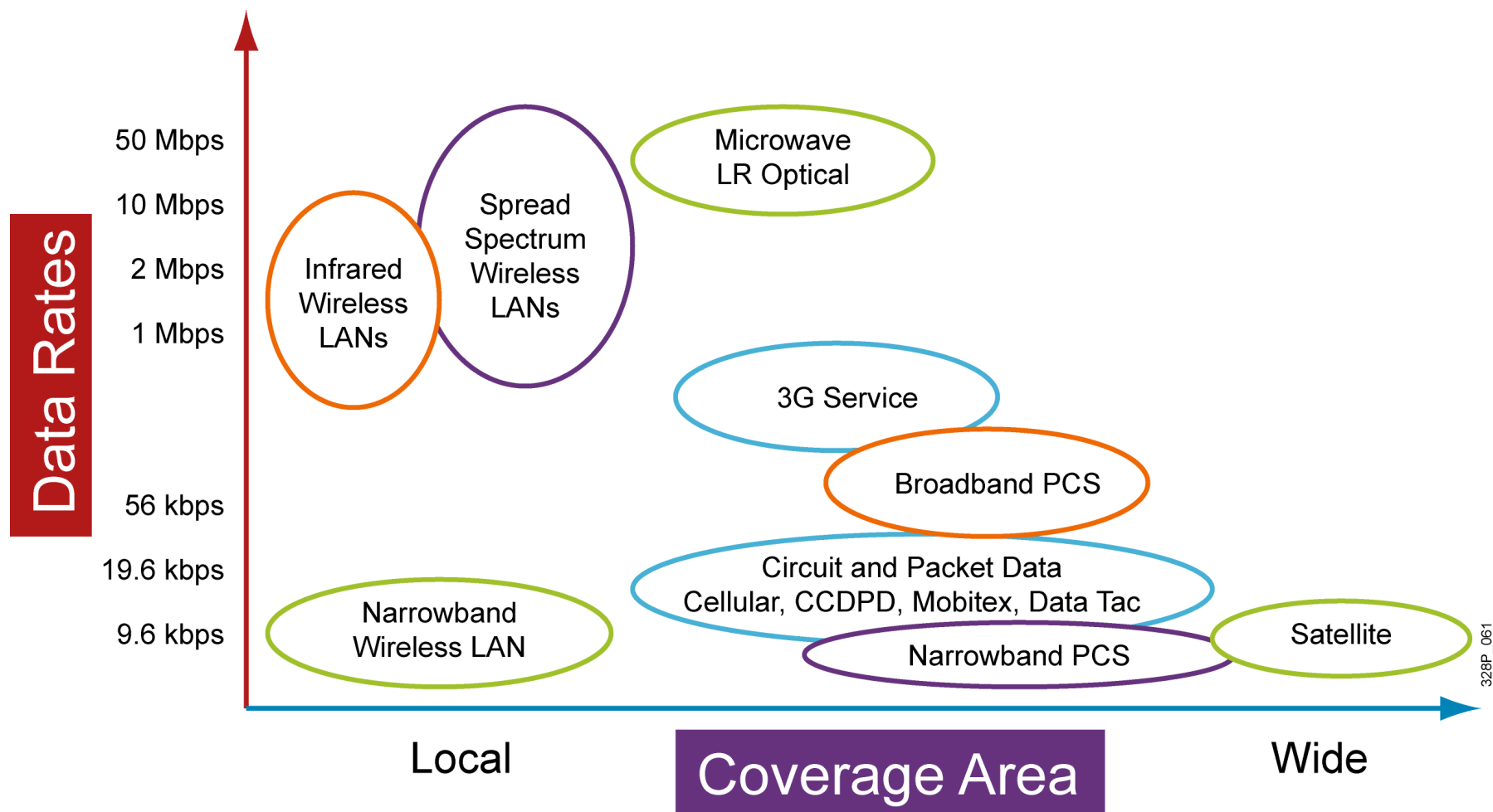
Osnove bežičnih mreža

Osnovni pojmovi

- Prvi bežični prenos: 1870 g.
- Upotreba 900-MHz opsega od 1980 g.
- Upotreba ISM opsega počinje 1990 g.
- Realizacija: u različitim ambijentalnim uslovima



Upotreba bežičnih mreža



WPAN (Wireless Personal Area Network)

- WPAN mreže realizuju konekciju na malom prostoru .
- Linkovi su obično peer to peer ili male mreže.
- WPAN: jednostavne, jeftine, mobilne.
- Bluetooth je tipičan primjer.

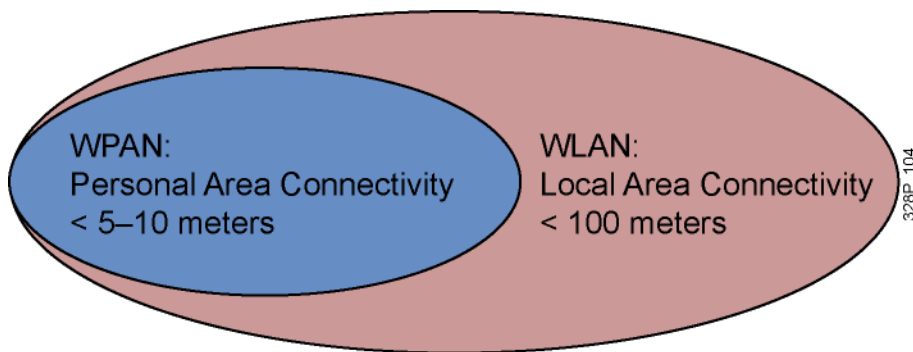


WPAN:
Personal Area Connectivity
< 5–10 meters

328P_103

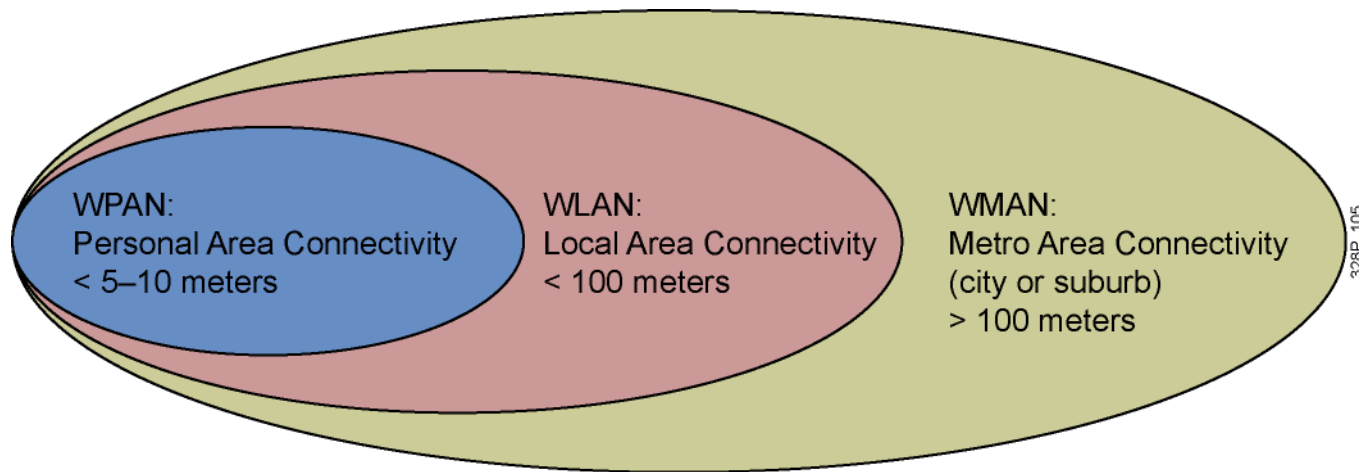
WLAN (Wireless LAN)

- Udaljenosti veće nego PAN, spektar 2.4 GHz i 5 GHz
- Potrebno više energije
- Očekuje se veći broj korisnika u mreži
- Potrebno da je dizajn fleksibilan i skalabilan



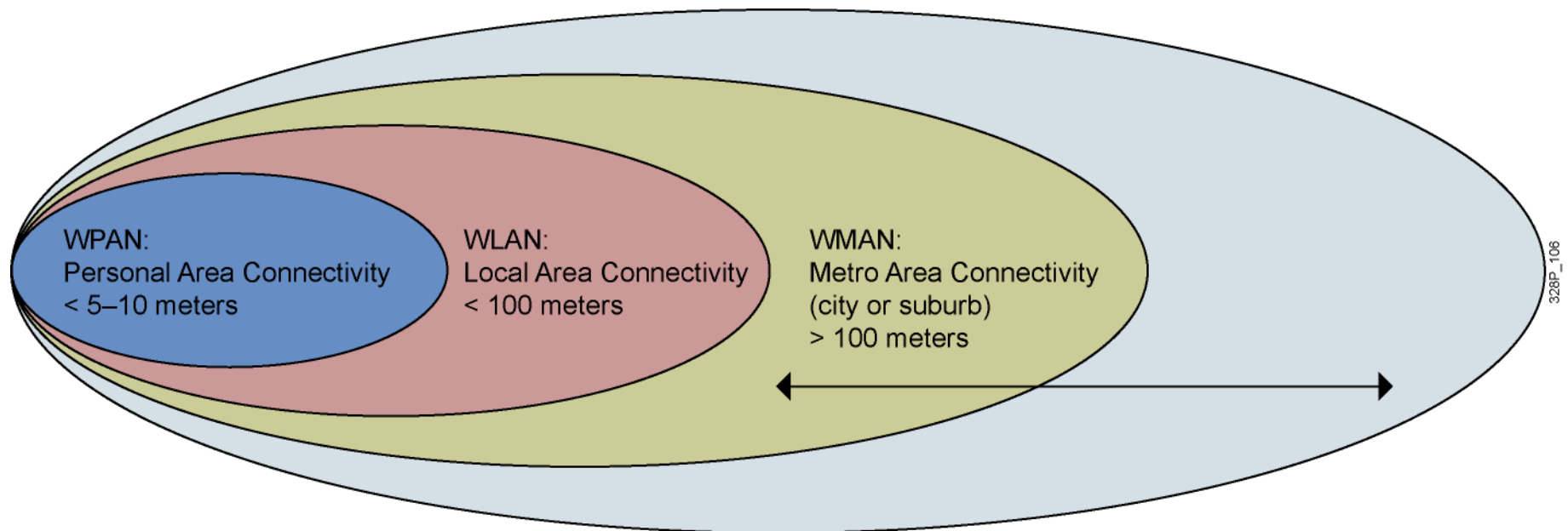
WMAN (Wireless Metro Area Network)

- Uloga: backbone ili da pokriju veće oblasti
- Obično u licenciranom spektru



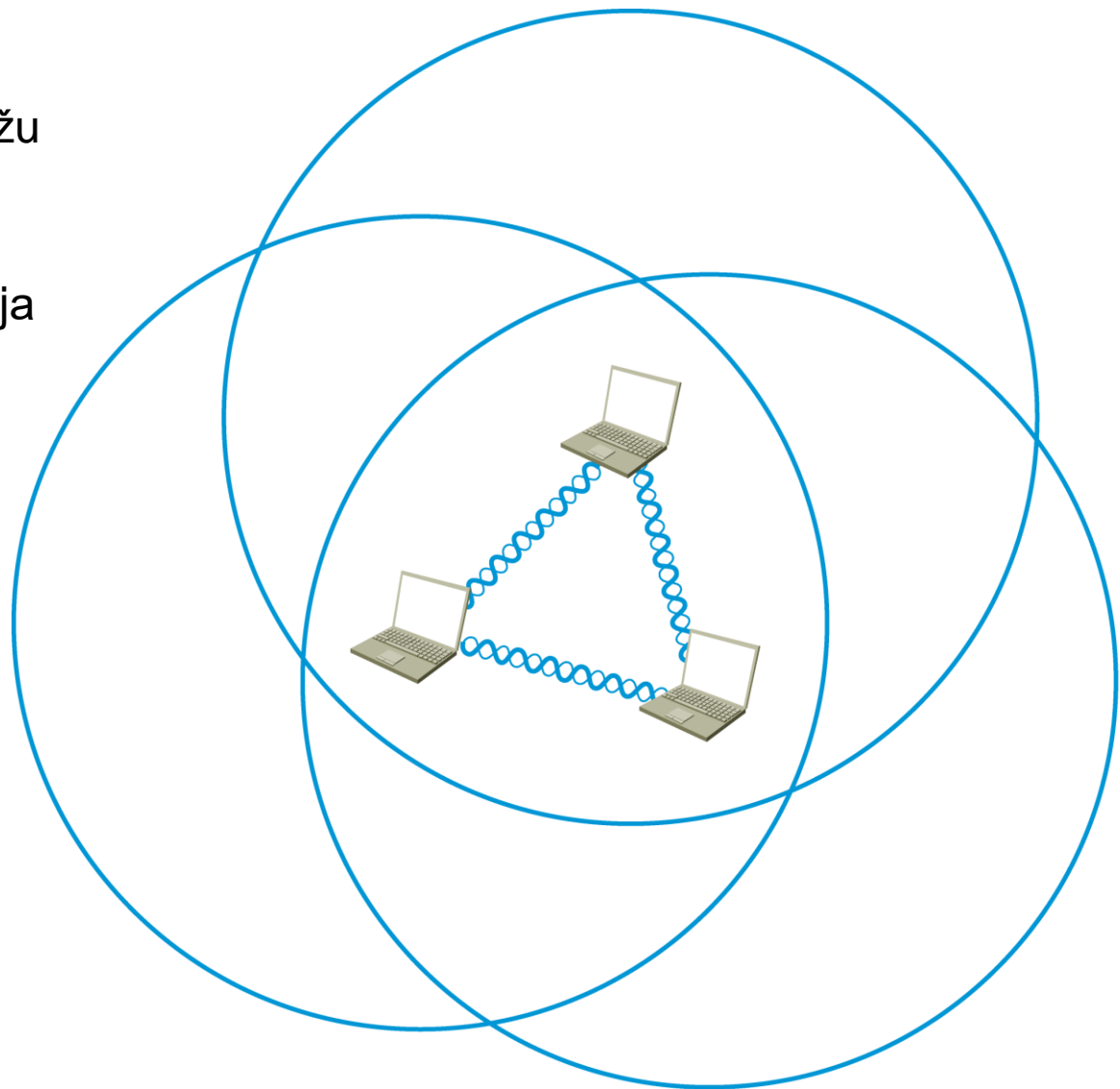
Wireless WAN

- Pokrivaju veće površine



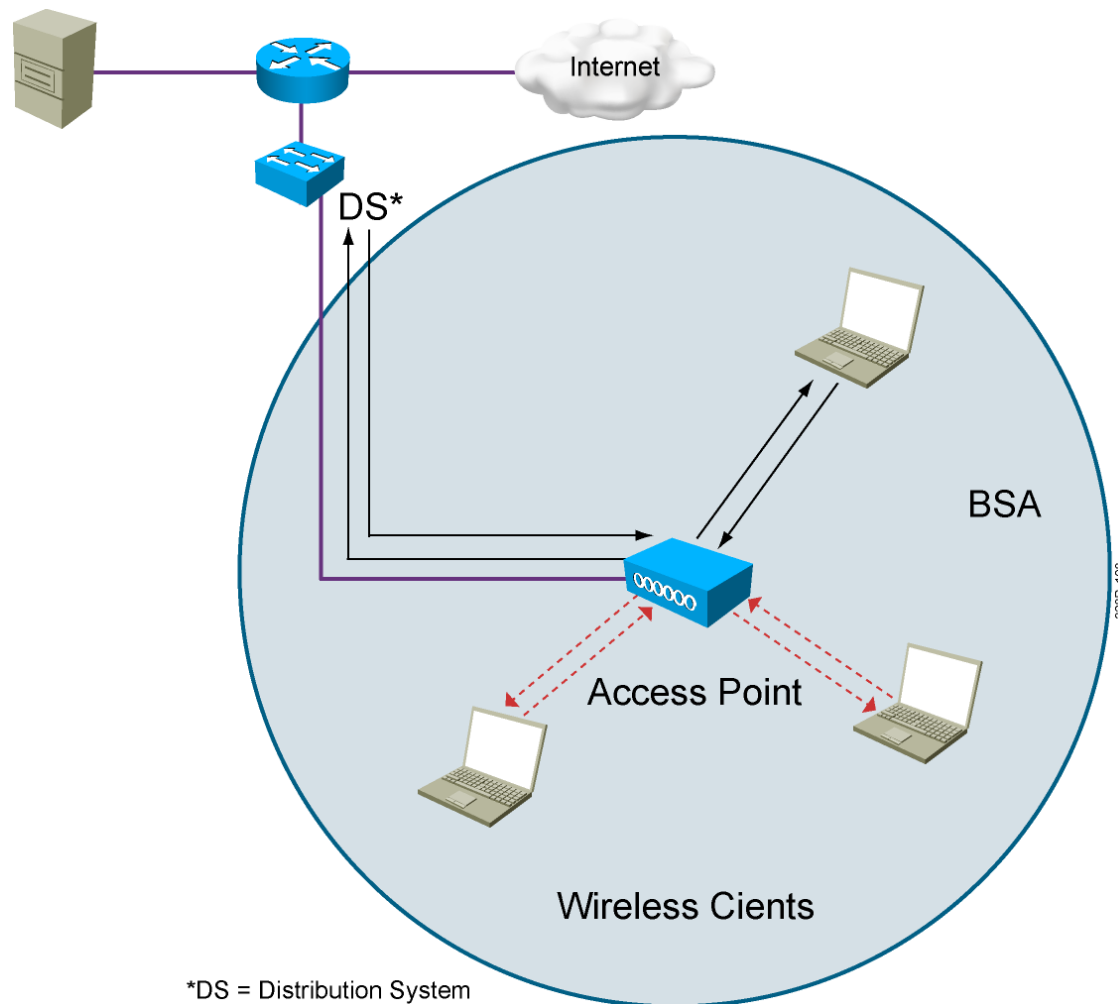
Ad Hoc mreže

- Postoji kada se povežu minimalno dva korisnika
- Ograničen broj uređaja zbog kolizije i organizacionih problema

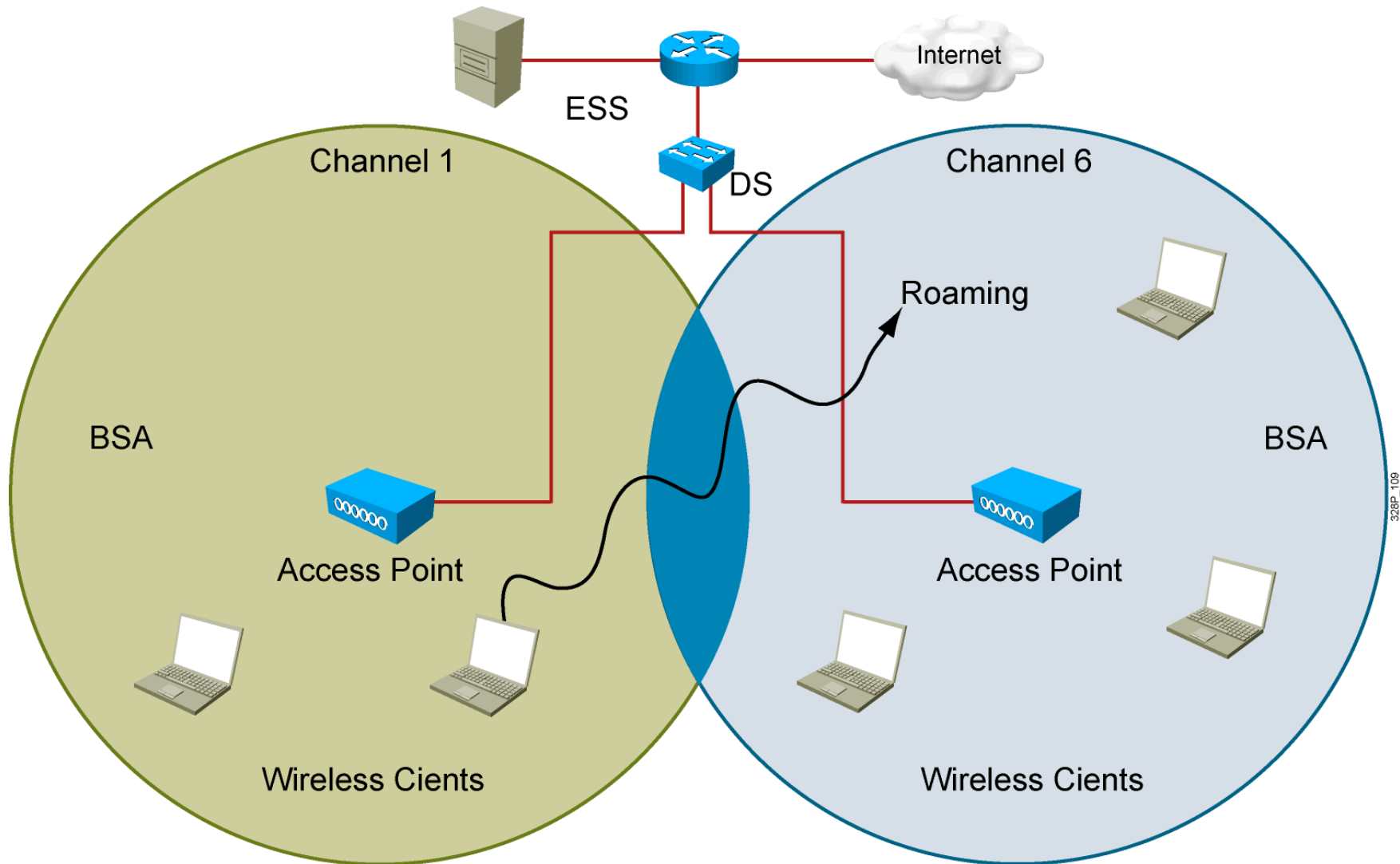


Infrastructure Mode

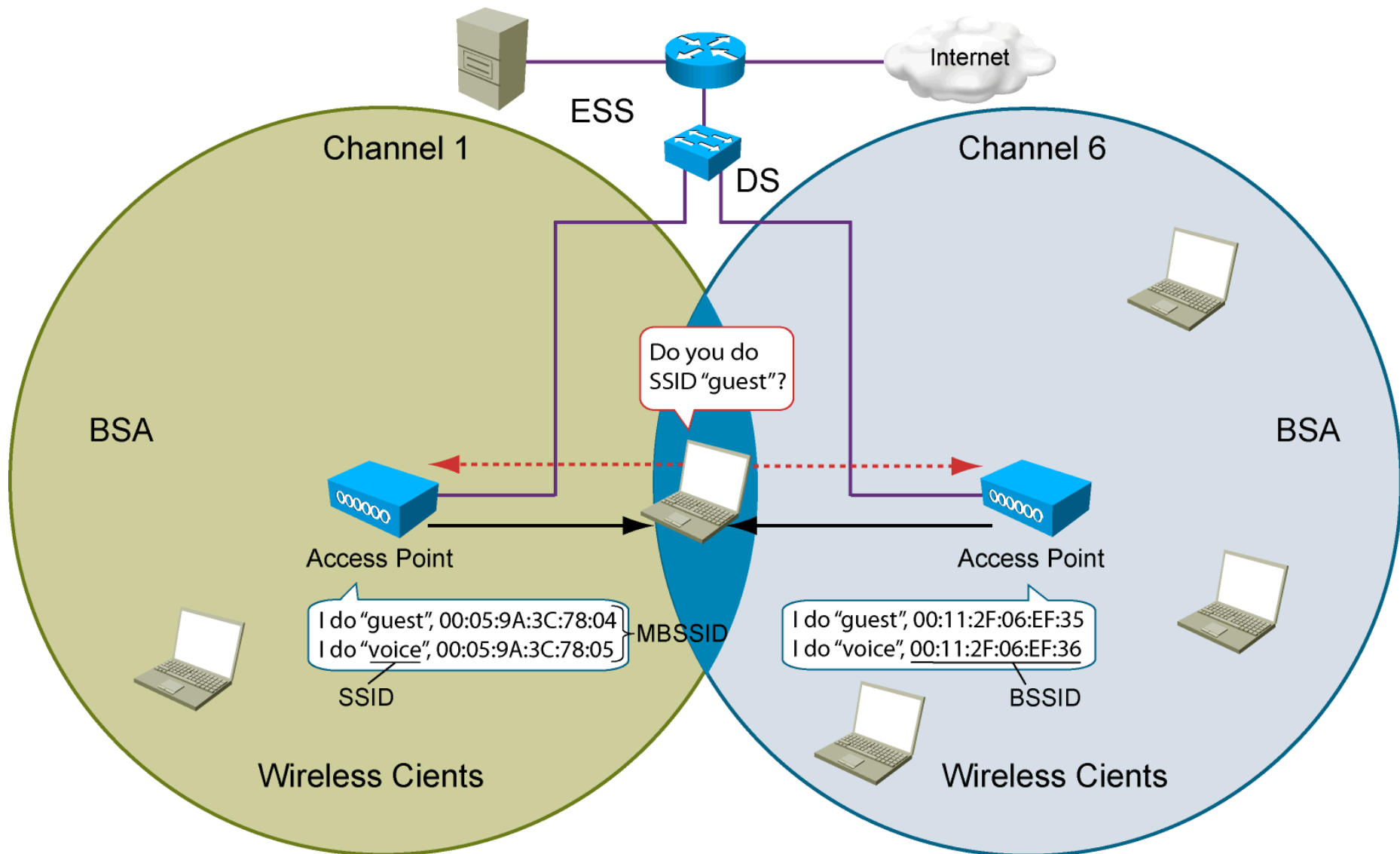
- AP rade kao “translational bridge” između 802.3 žičnih medija i 802.11 bežičnih medija.
- BSA = wireless ćelija.
- BSS =servis obezbijeđen od strane AP.



Infrastructure Mode (Cont.)

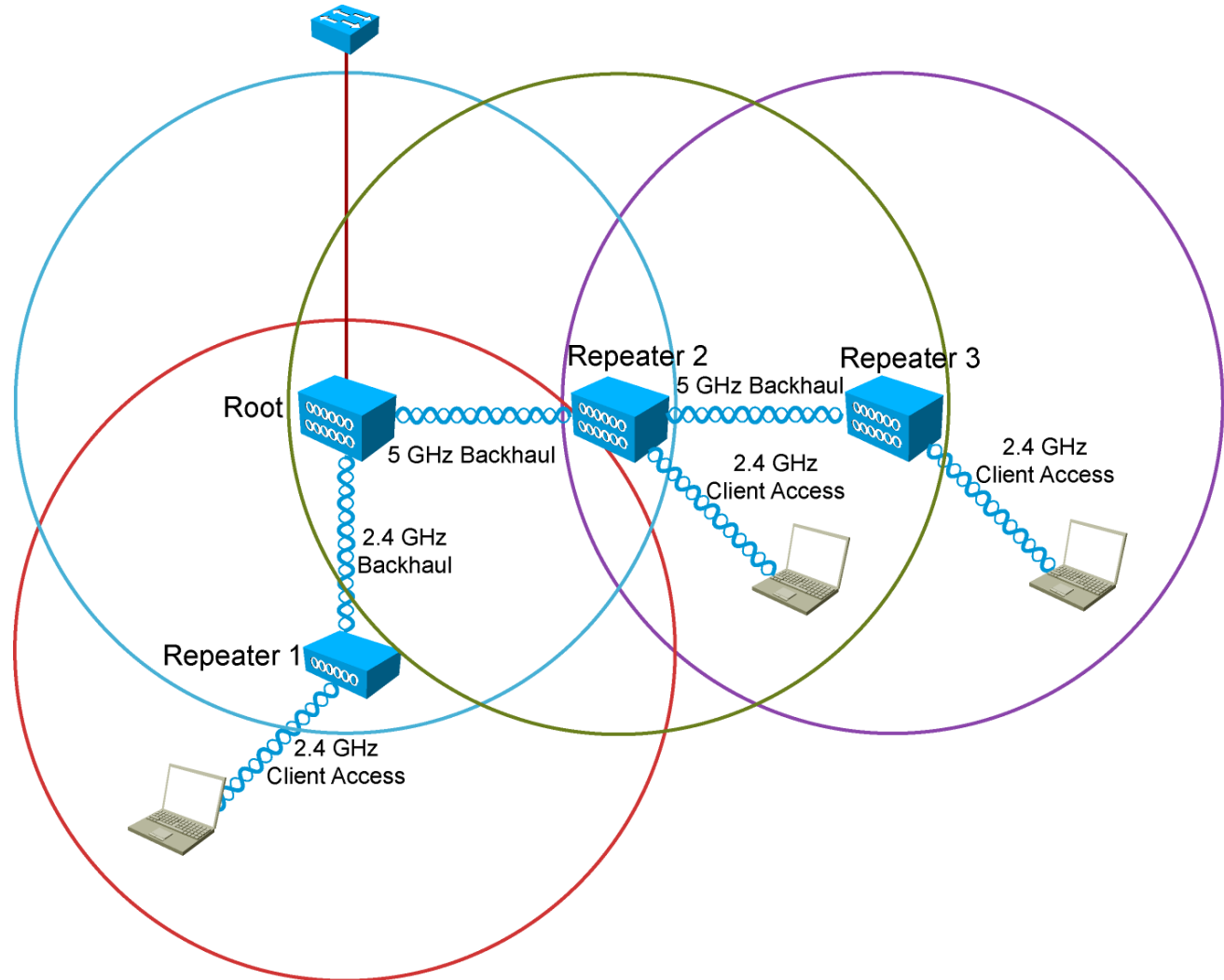


SSID (Service Set Identifier)



Repeater

- Proširuje oblast pokrivenosti AP
- Dual radio- može kreirati dual half-duplex
- Neophodno je prekrivanje ćelija od min 50%



Regulaciona tijela, standardi i sertifikacija u bežičnim komunikacijama

IEEE



- IEEE razvija komunikacione standarde
- Postoji više od 1300 protokola.
- 802.11 komitet analizira aplikacije i okruženje za primjenu bežičnih mreža
- 802.11 familija ima više od 26 subprotokola.

Wi-Fi Alijansa



- Wi-Fi Alijansa sertifikuje interoperabilnost između interoperability WLAN proizvoda.
- Uključuje 802.11a, 802.11b, 802.11g, 802.11n, dual-band proizvode i sigurnosna testiranja.
- Certifikovani proizvodi na stranici : <http://www.wi-fi.com>.

Regulaciona tijela



Svaka zemlja definiše pravila o upotrebi RF prostora uključujući pravila:

- Koje frekvencije su dozvoljene
- Dozvoljena transmitovana snaga zračenja („transmitters and antennae gain“, EIRP)
- Tehnike modulacije i kodovanje

Primjer FCC: 2.4-GHz EIRP Output Rules

Point-to-multipoint

- *Maximum of 36 dBm EIRP*
- *30-dBm maximum transmitter power with 6-dBi maximum gain of antenna and cable combination*
- *A 1:1 ratio between the maximum power and maximum gain*
- *Reduce transmit power below maximum of 30 dBm by 1 dBm and increase maximum antenna and cable system gain by 1dBi*

Point-to-point

- *Maximum of 36 dBm EIRP*
- *30-dBm maximum transmitter power with 6-dBi in gain of antenna and cable combination*
- *FCC allows exceeding the 36 dBm EIRP in point-to-point installations using the 3:1 ratio rule*
- *Reduce transmit power below maximum of 30 dBm by 1 dBm and increase maximum antenna and cable system gain by 3 dBi*

2.4-GHz EIRP Output Rules—FCC Example (Cont.)

Point-to-Multipoint

	Transmitter Power - dBm	Maximum Gain	EIRP
FCC Maximum	30 dBm	6 dBm	36 dBm
Cisco Maximum	20 dBm	16 dBm	36 dBm

The above values reflect the 1:1 rule.

Point-to-Point

	Transmitter Power - dBm	Maximum Gain	EIRP
FCC Maximum	30 dBm	6 dBm	36 dBm
Cisco Maximum	20 dBm	36 dBm	56 dBm

The above values reflect the 3:1 rule.

Wireless Spektar

- 2.4-GHz: ISM opseg je od 2.4 do 2.4835 GHz (2.4970 GHz Japan). Dozvoljeno je 11 kanala u USA, 13 u Evropi, i 14 Japanu.
- 5-GHz: ISM opseg je od 5.725 do 5.875 GHz.
- 5-GHz: ISM opseg se preklapa sa Unlicensed National Information Infrastructure (UNII) opsezima:
 - UNII-1 opseg od 5.15 do 5.25 GHz (4 kanala).
 - UNII-2 opseg od 5.25 do 5.35 GHz (4 kanala).
 - UNII-2 opseg proširuje opseg od 5.470 do 5.725 GHz (do 11 kanala).
 - UNII-3 opseg od 5.725 GHz do 5.825 GHz (4 kanala).

IEEE 802.11 aktivnosti standardizacije

- 802.11a — 5GHz, 54 Mb/s; ratified in 1999
- 802.11b — 2.4 GHz, 11 Mb/s; ratified in 1999
- 802.11d — World Mode; ratified in 2001
- 802.11e — QoS; ratified in 2005
- 802.11g — 2.4GHz, 54 Mb/s; ratified in 2003
- 802.11h — DFS and TPC mechanisms; ratified in 2004
- 802.11i — Authentication and security; ratified in 2004
- 802.11k — Radio resource measurement enhancements (under development)
- 802.11n — Higher throughput improvements using MIMO antennas (under development)
- 802.11t — WPP; test methods and metrics recommendation (under development)
- 802.11w — Protected management frames (under development)

802.11 Standardi za spektre i brzine

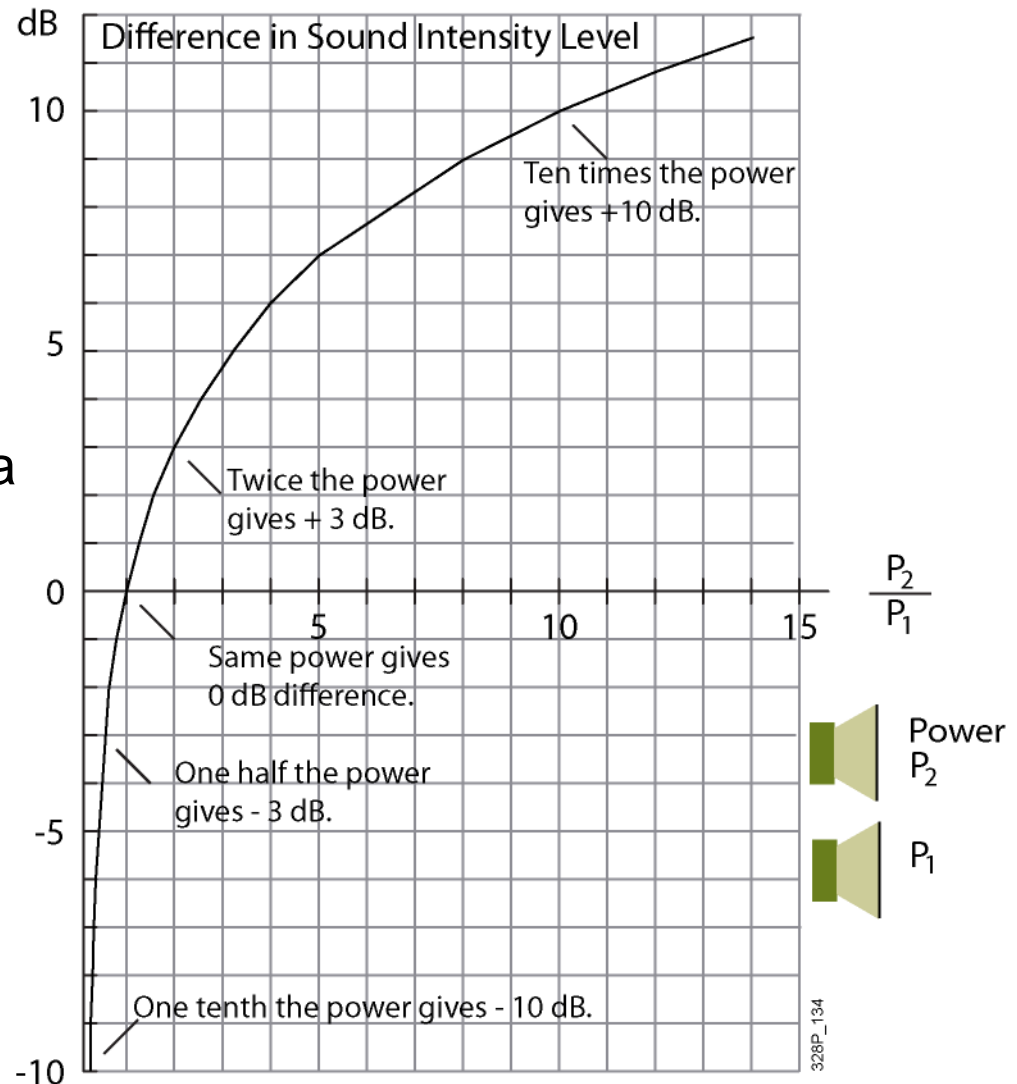
	802.11	802.11b	802.11a	802.11g		802.11n
Ratified	1997	1999	1999	2003		Not Ratified
Frequency Band	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz		2.4 GHz, 5 GHz
No of Channels	3	3	Up to 23	3		varies
Transmission	IR, FHSS, DSSS	DSSS	OFDM	DSSS	OFDM	DSSS, CCK, OFDM
Data Rates (Mb/s)	1, 2	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	100+

Osnove RF matematike

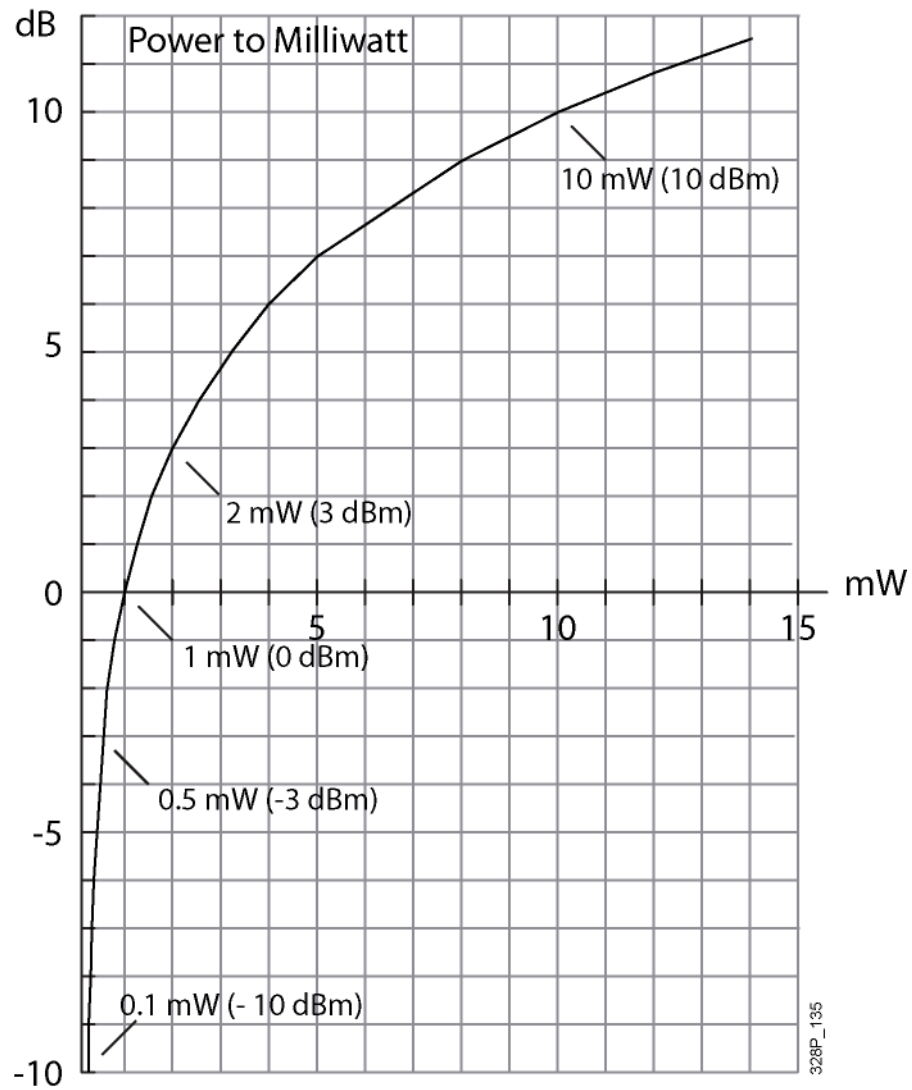
Decibel

Poređenje snaga zračenja:

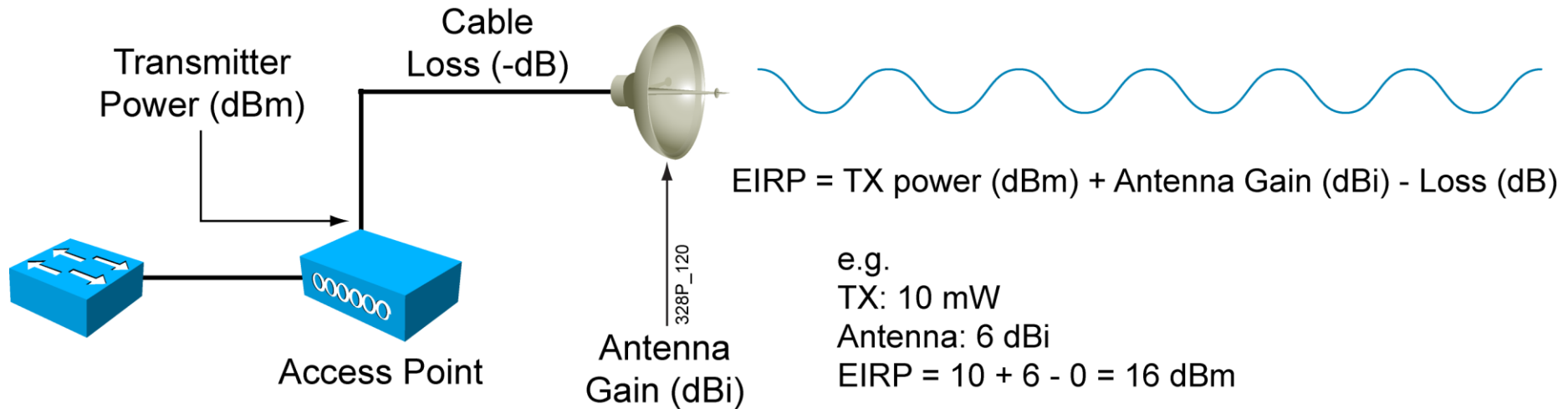
- 0 dB = ista snaga
- 3 dB = dvostruka snaga
- -3 dB = polovina snage
- 10 dB = 10 puta veća snaga
- -10 dB = 1/10 snage



dBm



Efektivna izračena snaga



EIRP: Effective Isotropic Radiated Power

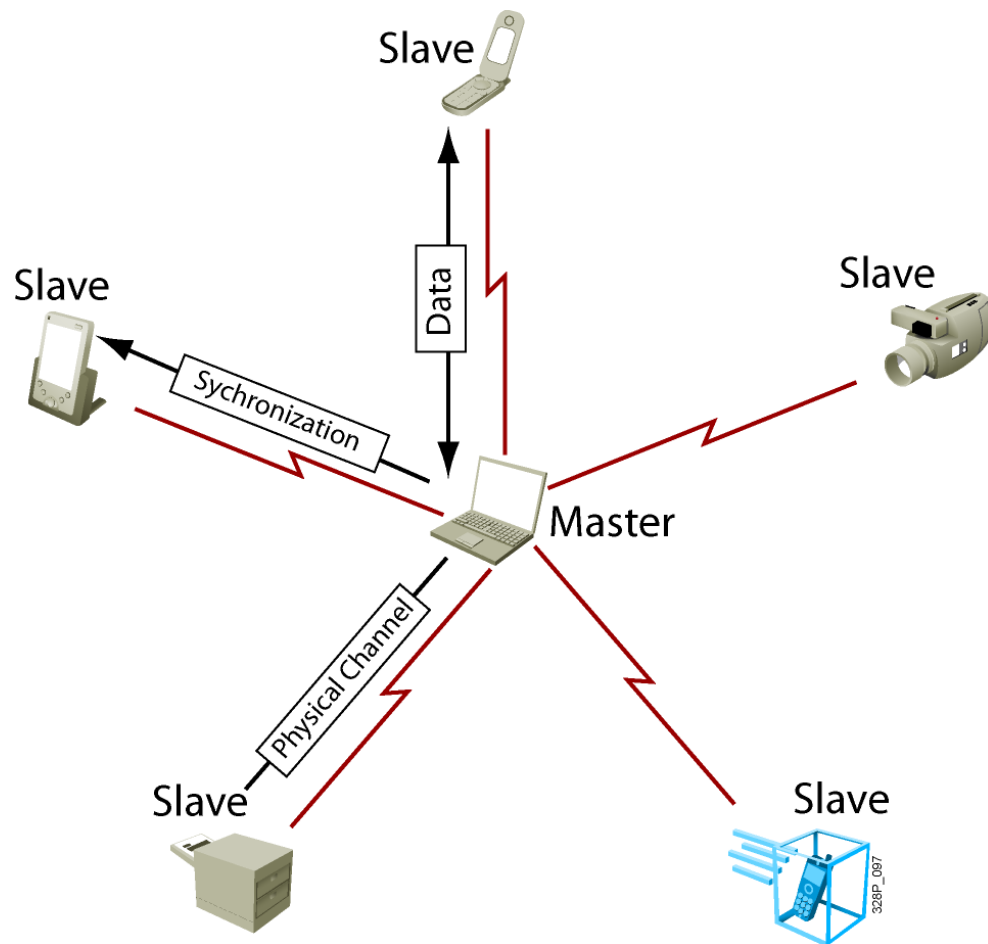
Osnovne Non-802.11 Wireless tehnologije i njihov uticaj na WLAN

Bluetooth

- Radio sistem (radio frekvencijski standard) koji definiše koncept-wireless personal area network (WPAN).
- Nominalna veličina linka do 10m/ 0 dBm (~100m sa 20 dBm)
- Transmituje od 2.402 GHz do 2.480 GHz (79 kanala)
- Brzine do 720 kb/s
- Klase proizvoda: 100 mW, 2.5 mW and 1 mW
- Nema line-of-sight restrikcija
- Visoka sigurnost

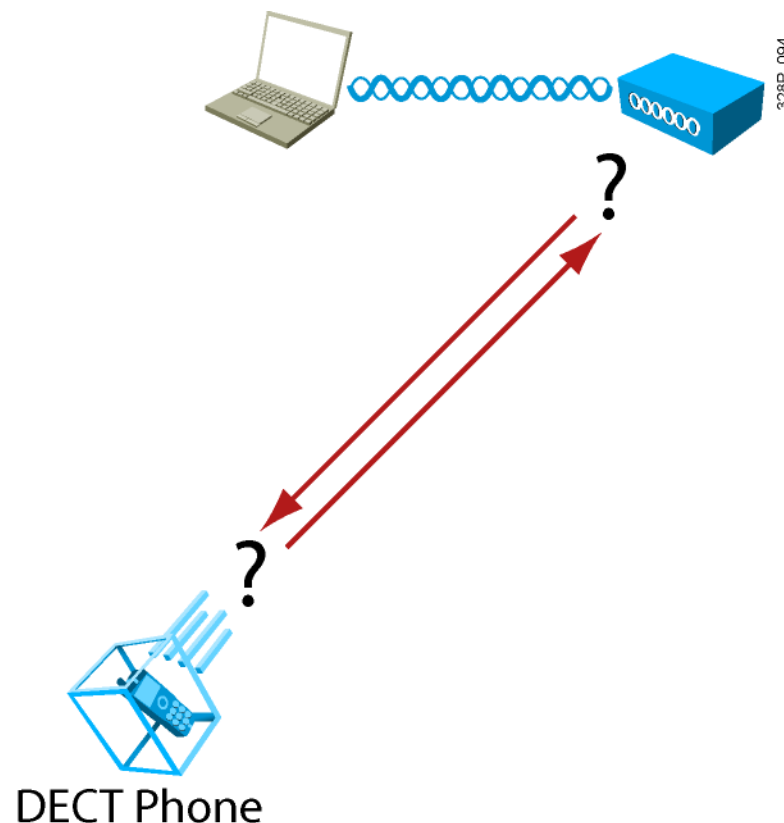
Bluetooth (Cont.)

- Bluetooth mreža: do 7 slave uređaja i jedan master.
- Čelija se zove "piconet."
- Bluetooth omogućuje jednostavnu realizaciju ad-hoc mreže.



Bežični telefon

- Telefon je klijent na baznoj stanici.
- Koristi se TDMA (Time Division Multiple Access) i FDMA (Frequency Division Multiple Access).
- Protokoli dobijeni od ISDN.
- Nisu kompatibilni sa Wi-Fi, ali zbog istog frekvencijskog opsega je moguća interferencija.

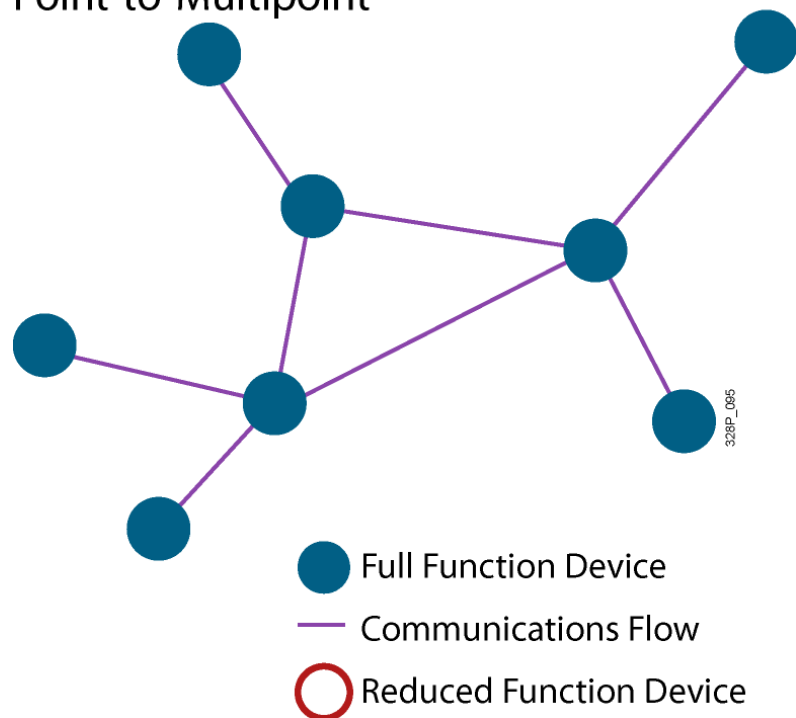


ZigBee

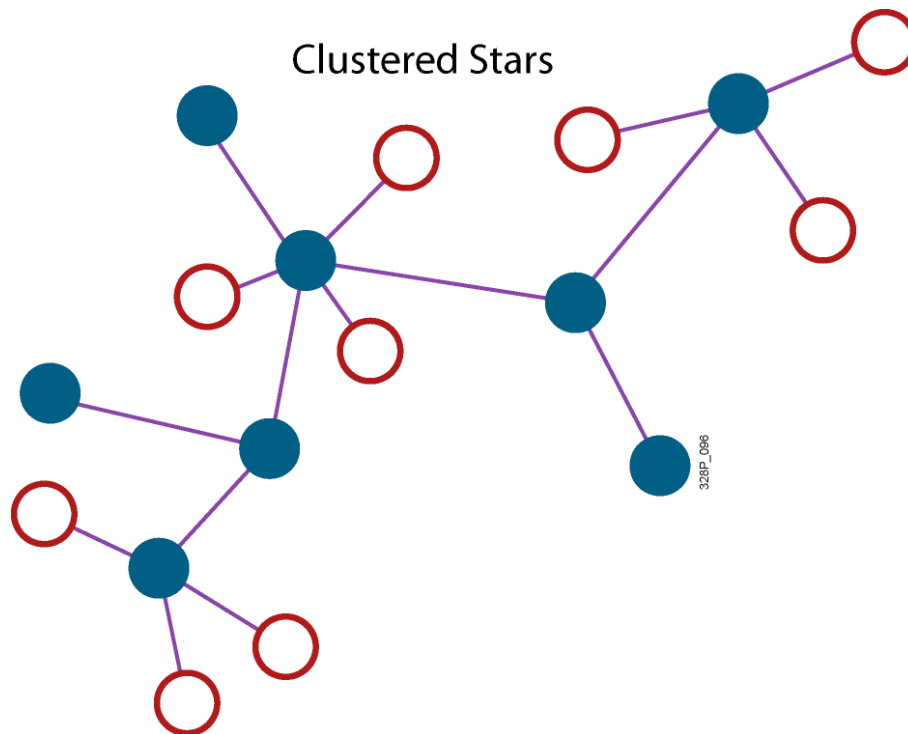
- Novi standard za “short range mesh” umrežavanje
 - Baziran na IEEE 802.15.4 standard
 - Pouzdanost
- Dizajniran za „low-power“ aplikacije
 - Dug vijek baterije
- „Low data rate“
 - 20 do 250 kb/s (zavisi od opsega)
- Sigurnost
 - AES-128 enkripcija
- Samostalna konfiguracija
 - Dozvoljava ad-hoc mreže
 - Jednostavnost instalacije i konfiguracije
- Primjene: daljinsko upravljanje, klimatizacija, automatizacija, i slično.
- Jefinija implementacija od Wi-Fi ili Bluetooth

ZigBee mreža

Point-to-Multipoint



Clustered Stars



- Nije kompatibilan sa Wi-Fi
- Koristi ISM band i moguća interferencija

Drugi Non-802.11 uređaji –moguća interferencija



Microwave Ovens



Wireless Video
Cameras



Radar



Motion Detectors



Wireless
Headphones



Outdoor
Microwave Links



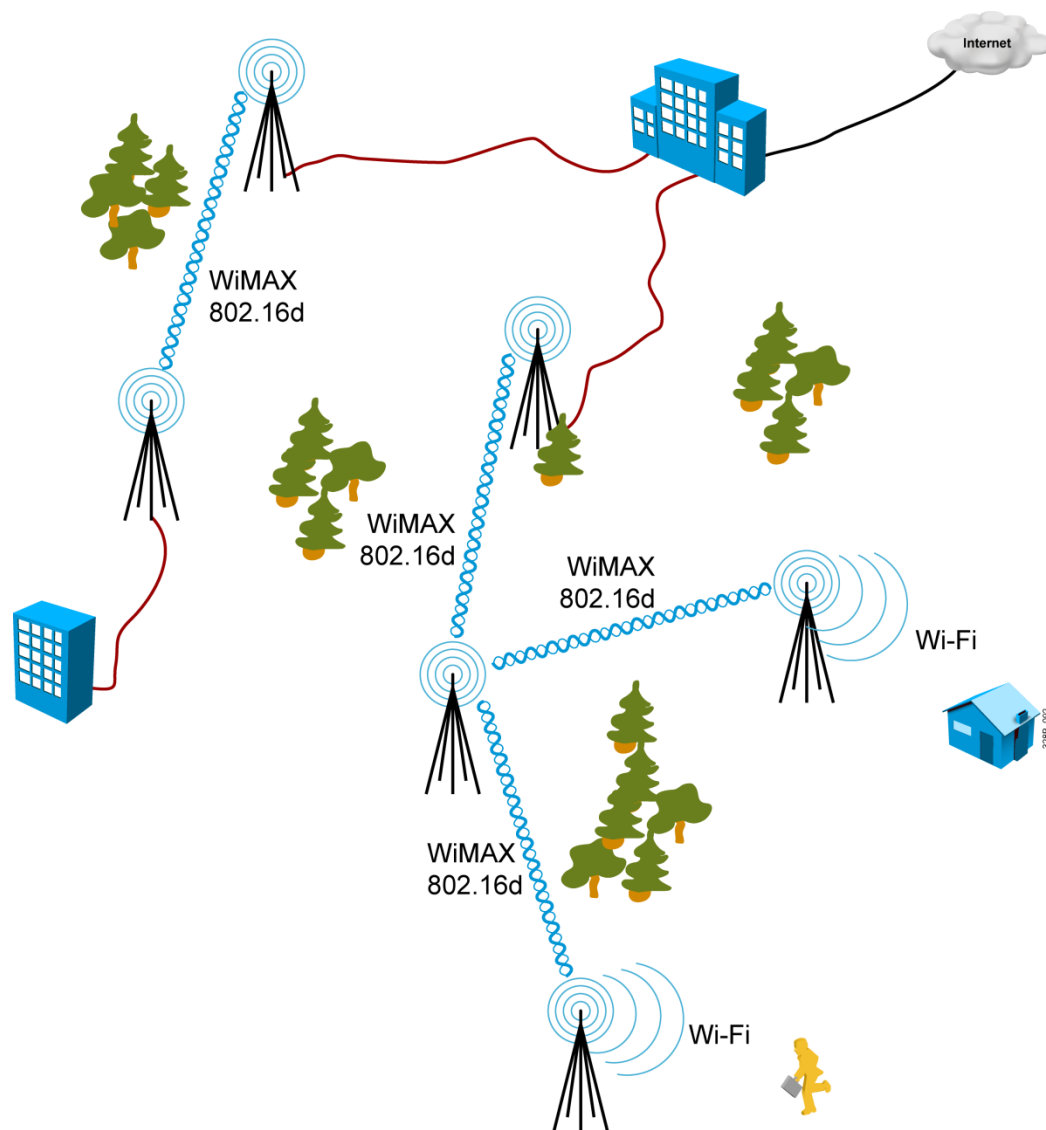
Fluorescent Lights



Wireless
Game Controller

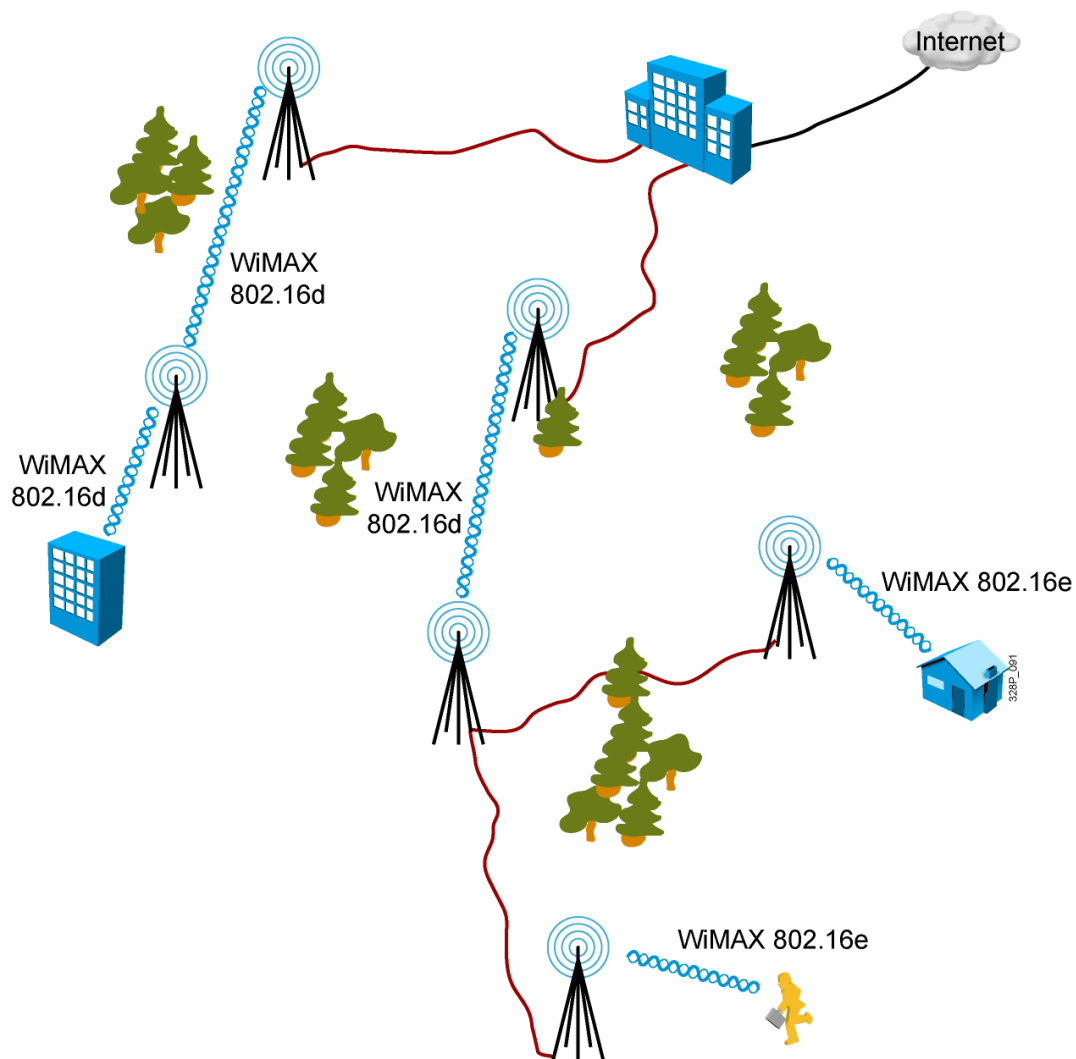
WiMAX tehnologija

- WiMAX -Worldwide Interoperability for Microwave Access.
- IEEE 802.16 podržan od WiMAX Forum.
- Fiksni WiMAX, baziran na 802.16d
- Upotreba kao backbone, T1/E1 linije
- Realizacija „last mile“ konektivnosti pomoću WiFi ili žičanim medijem
- Velike udaljenosti sa velikim brzinama



WiMAX tehnologija

- „Last mile“ konektivnost bazirana na 802.16e
- Mobilni korisnici
- „Line-of-sight“ ograničenja
- Udaljenosti 4 do 6 milja, brzine do 40 Mb/s, ali zavisi od udaljenosti i linije vidljivosti



Wireless LAN

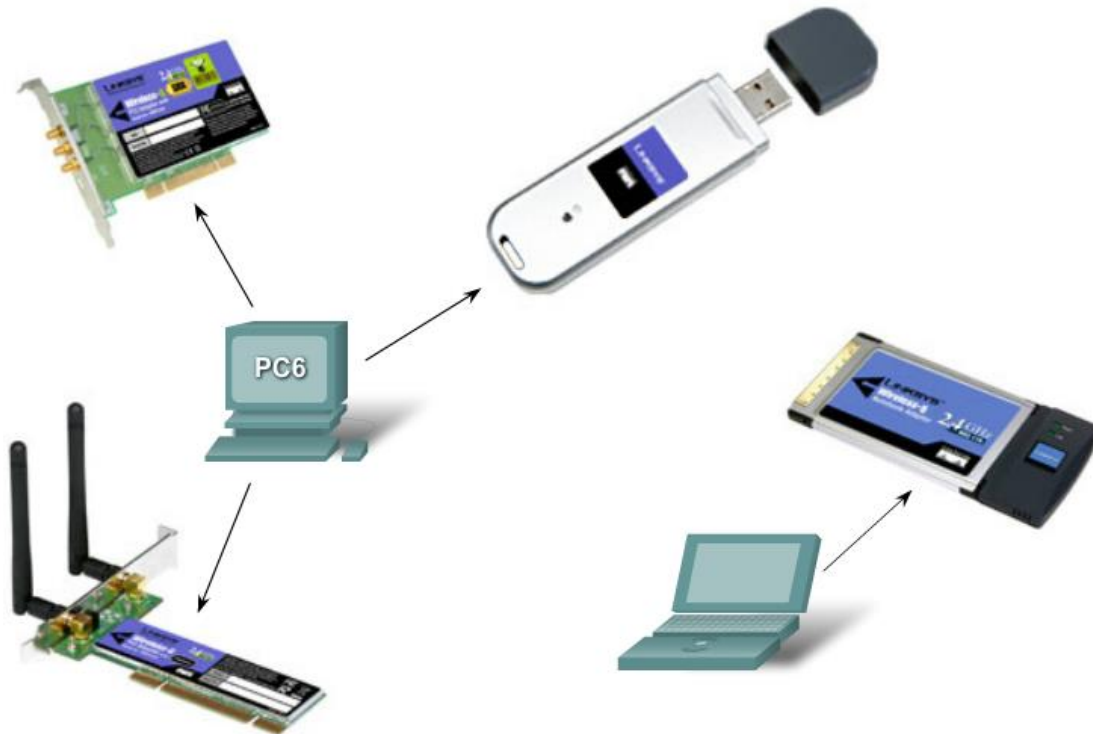
Poređenje WLAN i LAN

- Pregled osnovnih karakteristika WLAN i LAN mreža

Characteristic	802.11 Wireless LAN	802.3 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential
Regulation	Additional regulation by local authorities	IEEE standard dictates

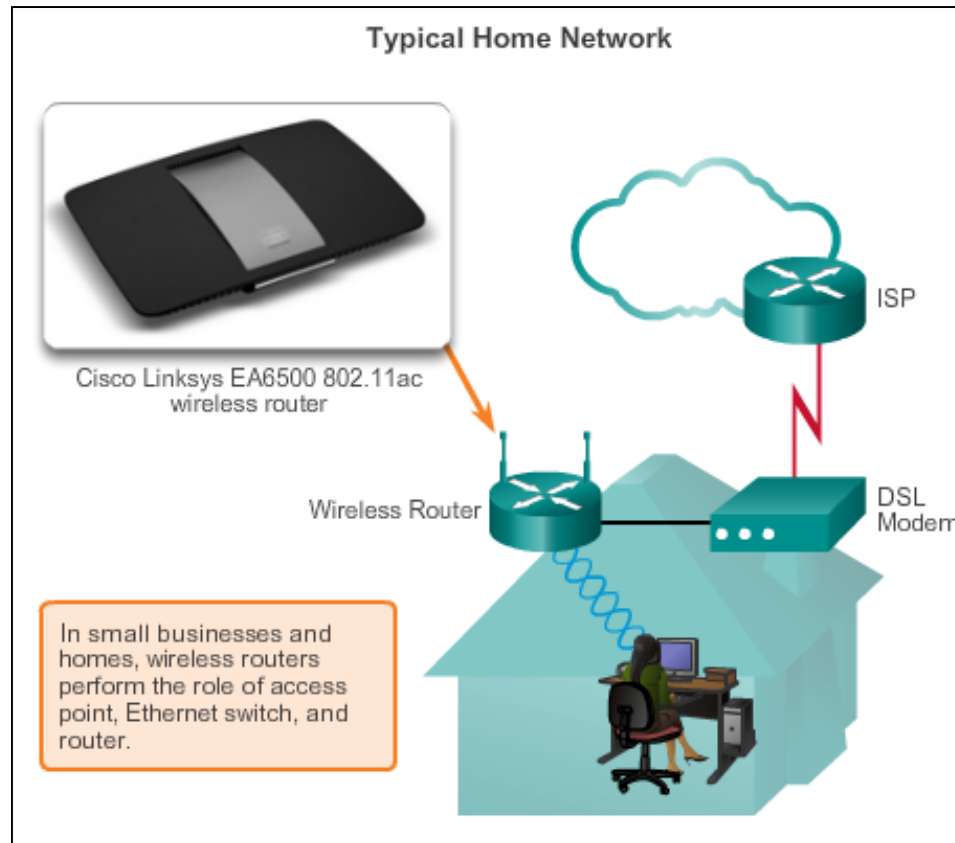
Osnovne WLAN komponente

- Neophodna upotreba bežičnih mrežnih adaptera i uređaja kao što su wireless router ili wireless AP
- Wireless NIC



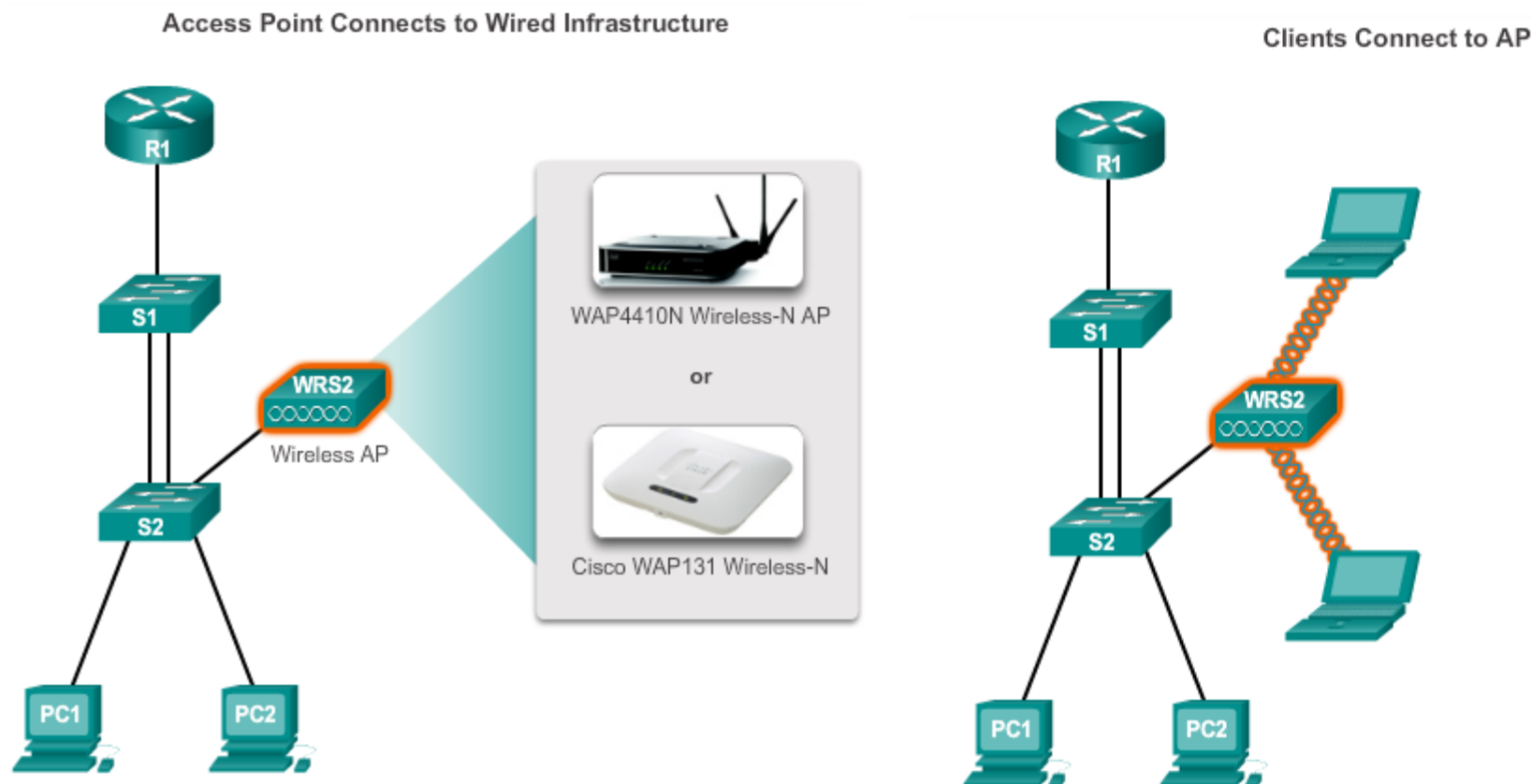
Osnovne WLAN komponente

- Wireless home router
- U manjim kućnim i poslovnim aplikacijama wireless router ima višestruku ulogu i to kao: AP, switch i router.



„Business Wireless Solutions“

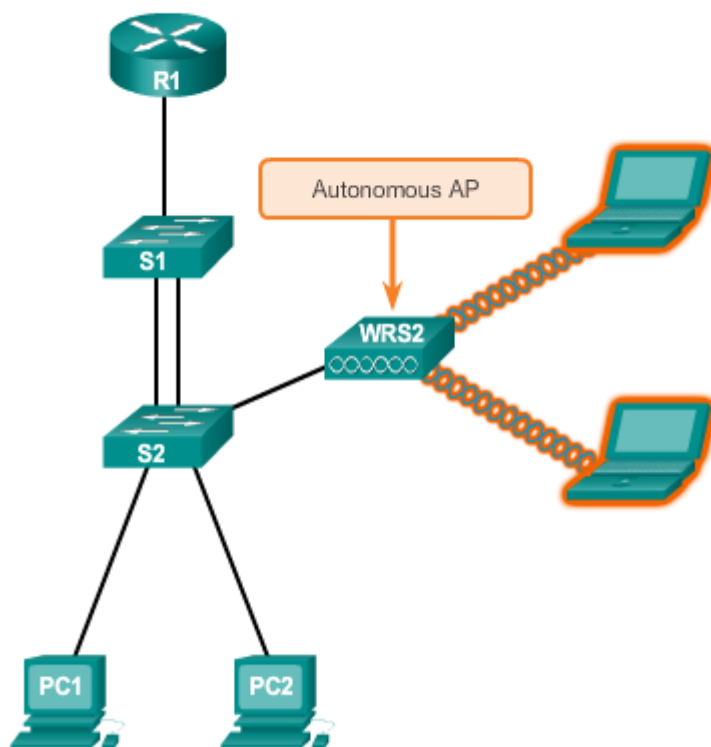
- Primjer proširenje postojeće 802.3 Ethernet LAN infrastrukture upotrebom WLAN-a



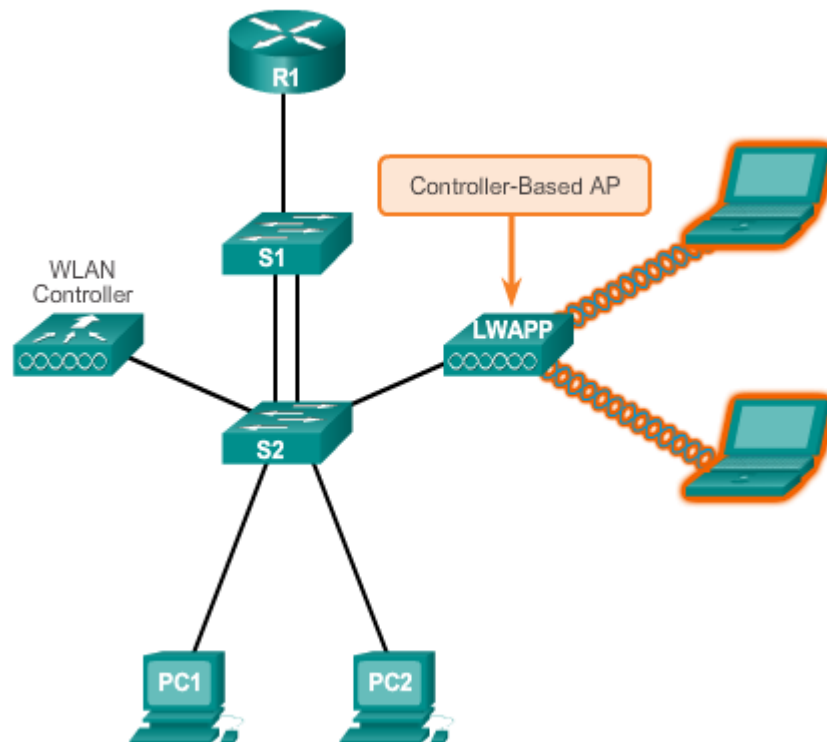
„Business Wireless Solutions“

- Mogućnost konfiguracije i administracije svakog AP („standalone“ AP) pojedinačno ili upotreba kontrolera i „lightweight“ AP uređaja .

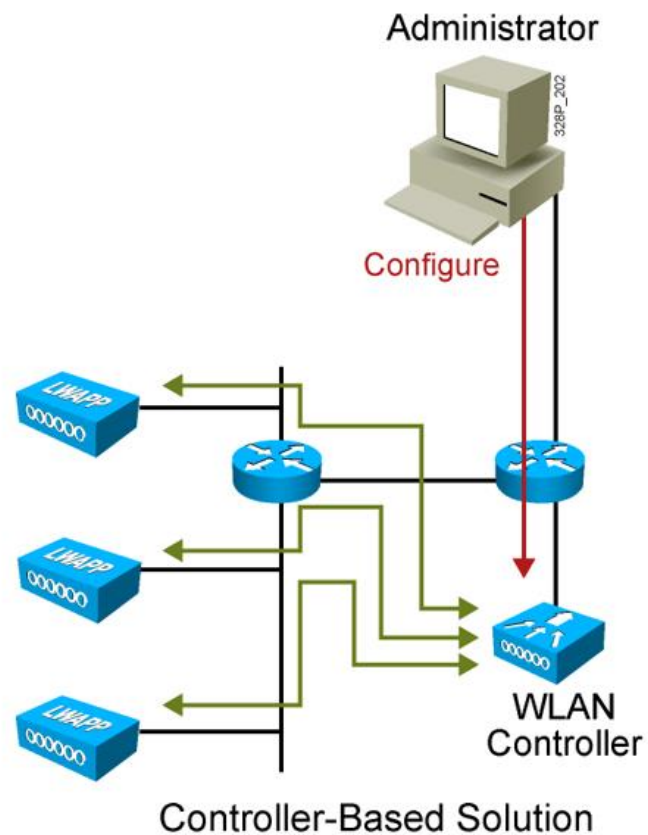
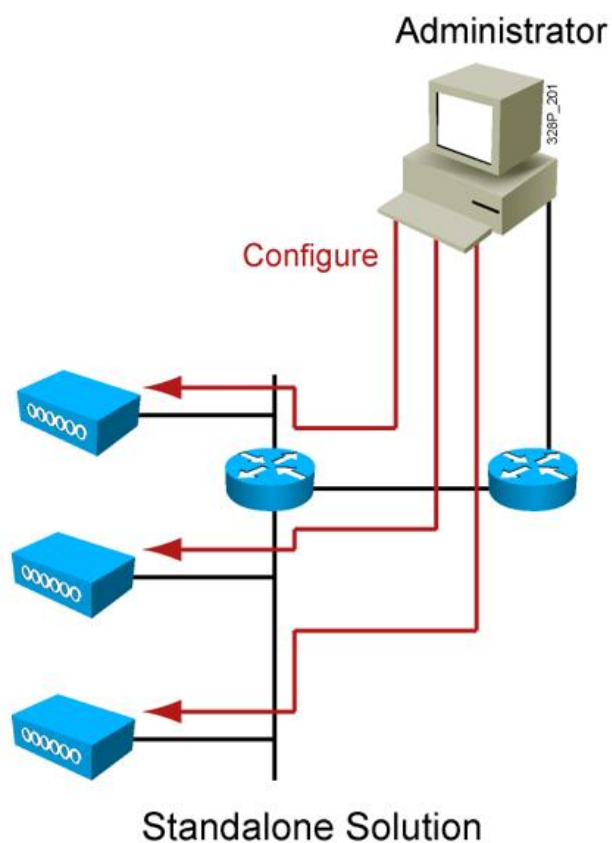
Autonomous AP



Controller-Based AP



„Standalone“ i „Lightweight“ AP



Osnovni konfiguracioni parametri

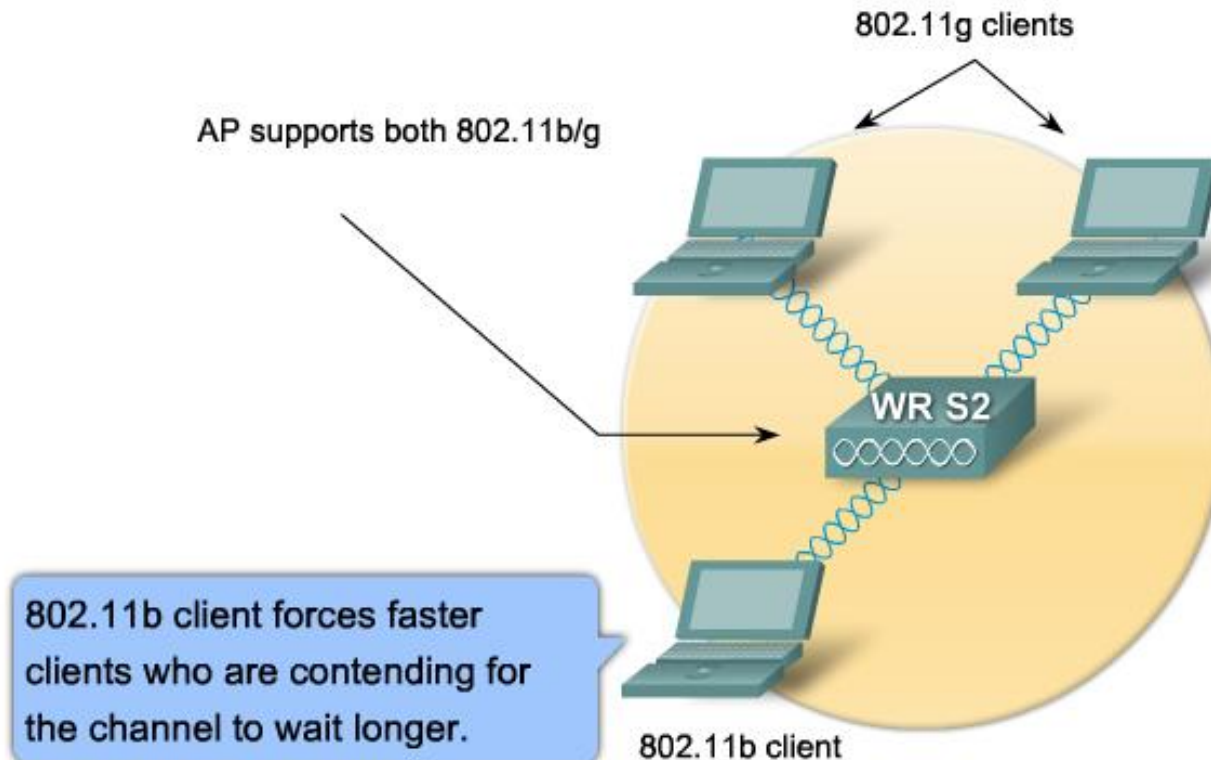
- Osnovni parametri:
SSID, Password, Network Mode, Security Mode, Channel Settings

The screenshot displays the Linksys web interface for configuring a wireless network. The top header features the Linksys logo and the text 'A Division of Cisco Systems, Inc.'. Below this, a navigation bar includes tabs for 'Wireless', 'Setup', 'Wireless', 'Security', 'Access Restrictions', and 'Applications & Gaming'. Under the 'Wireless' tab, there are sub-links for 'Basic Wireless Settings', 'Wireless Security', and 'Wireless Network Access'. The main content area is titled 'Wireless Network' and contains the following configuration options:

- Wireless Network Mode:** A dropdown menu set to 'MIXED'.
- Wireless Network Name (SSID):** A text input field containing 'linksys03'.
- Wireless Channel:** A dropdown menu set to '1 - 2.412GHz'.
- Wireless SSID Broadcast:** Two radio buttons, with 'Enable' selected and 'Disable' unselected.

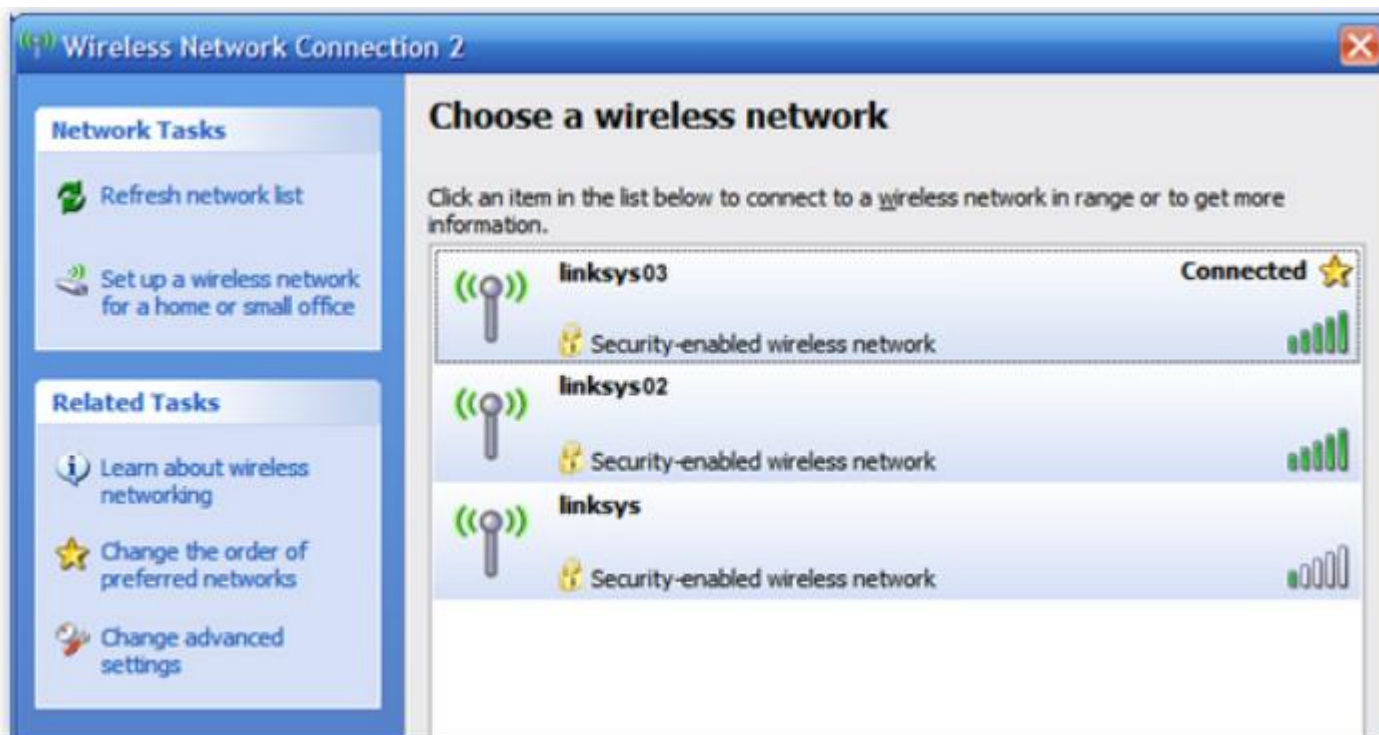
Osnovni konfiguracioni parametri

- Network mode se odnosi na korištene WLAN protokole: 802.11a, b, g, ili n.
- 802.11g je unazad kompatibilan sa 802.11b---access point podržava oba standarda.
- Mixed mode: AP konfigurisan da dozvoljava rad na oba mode



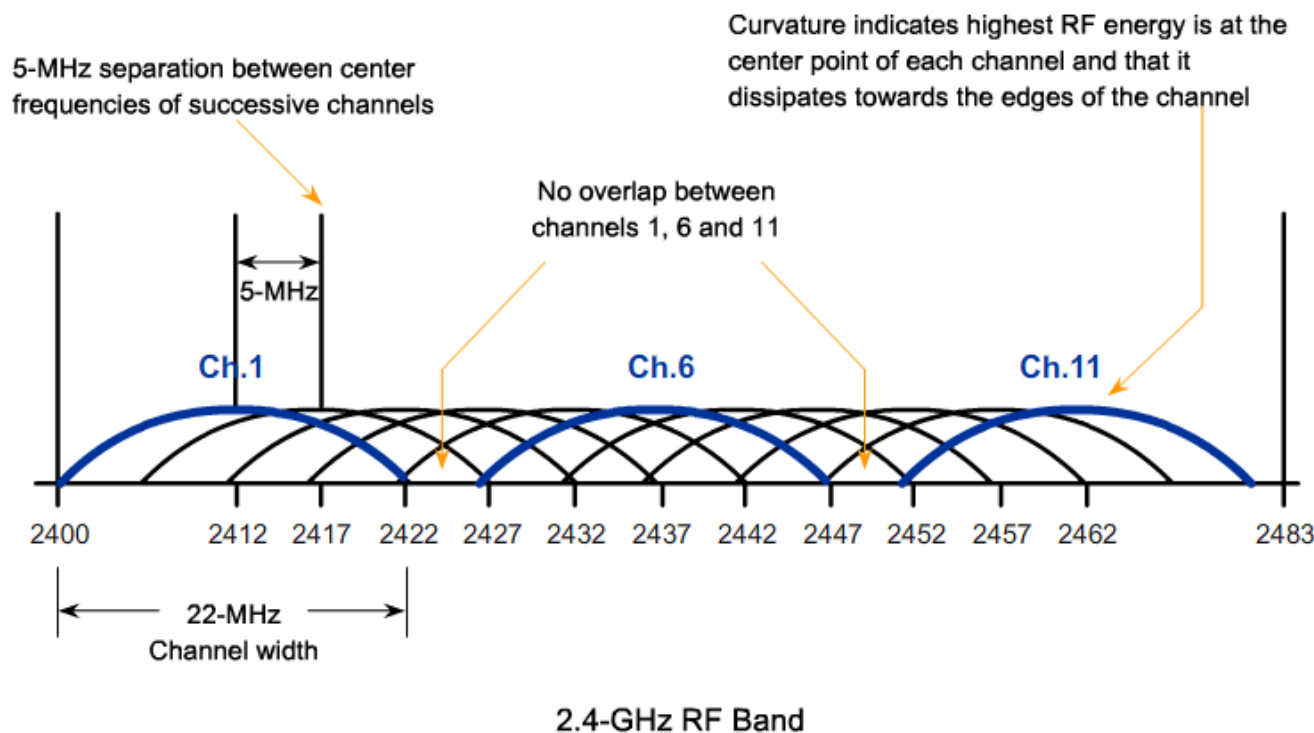
Osnovni konfiguracioni parametri

- SSID je jedinstveni identifikator koji se koristi da se razlikuju bežične mreže
- Nekoliko AP može da dijeli SSID

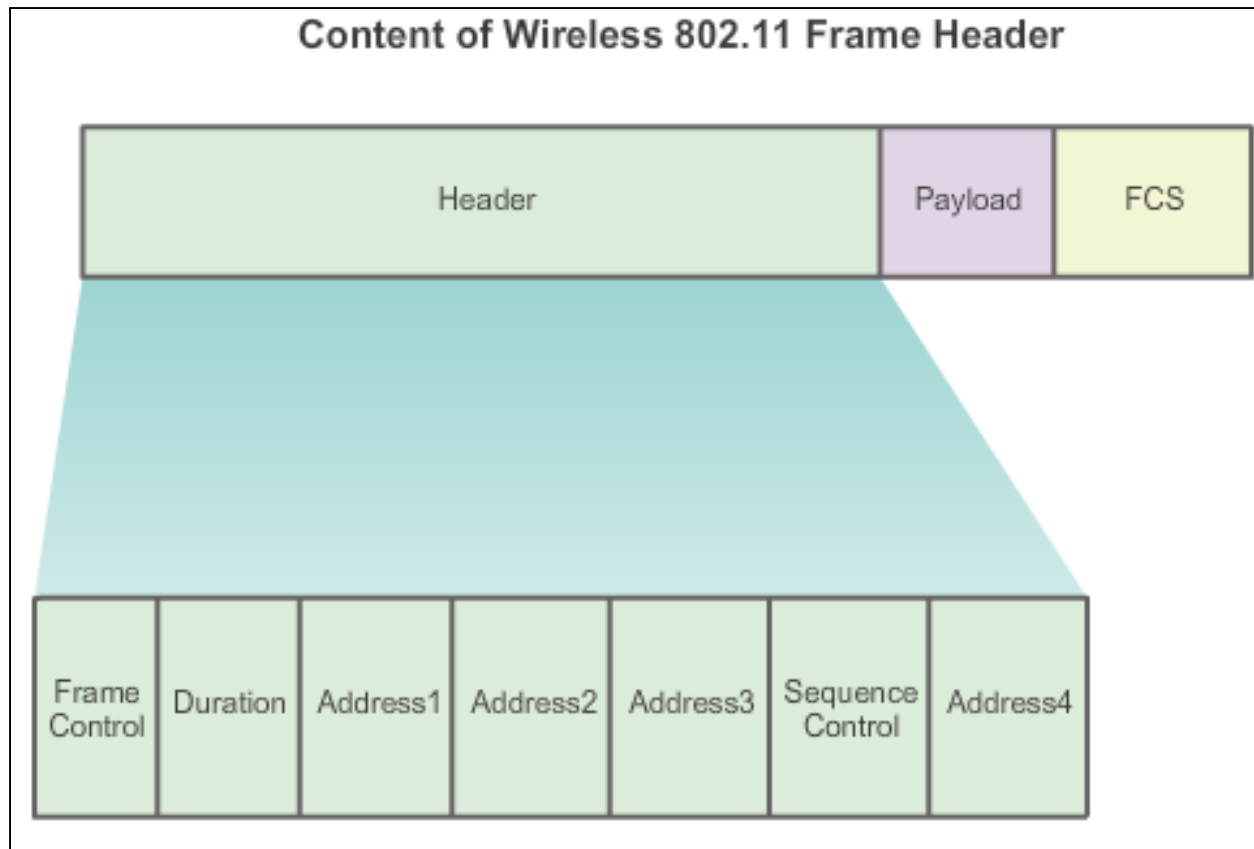


Osnovni konfiguracioni parametri

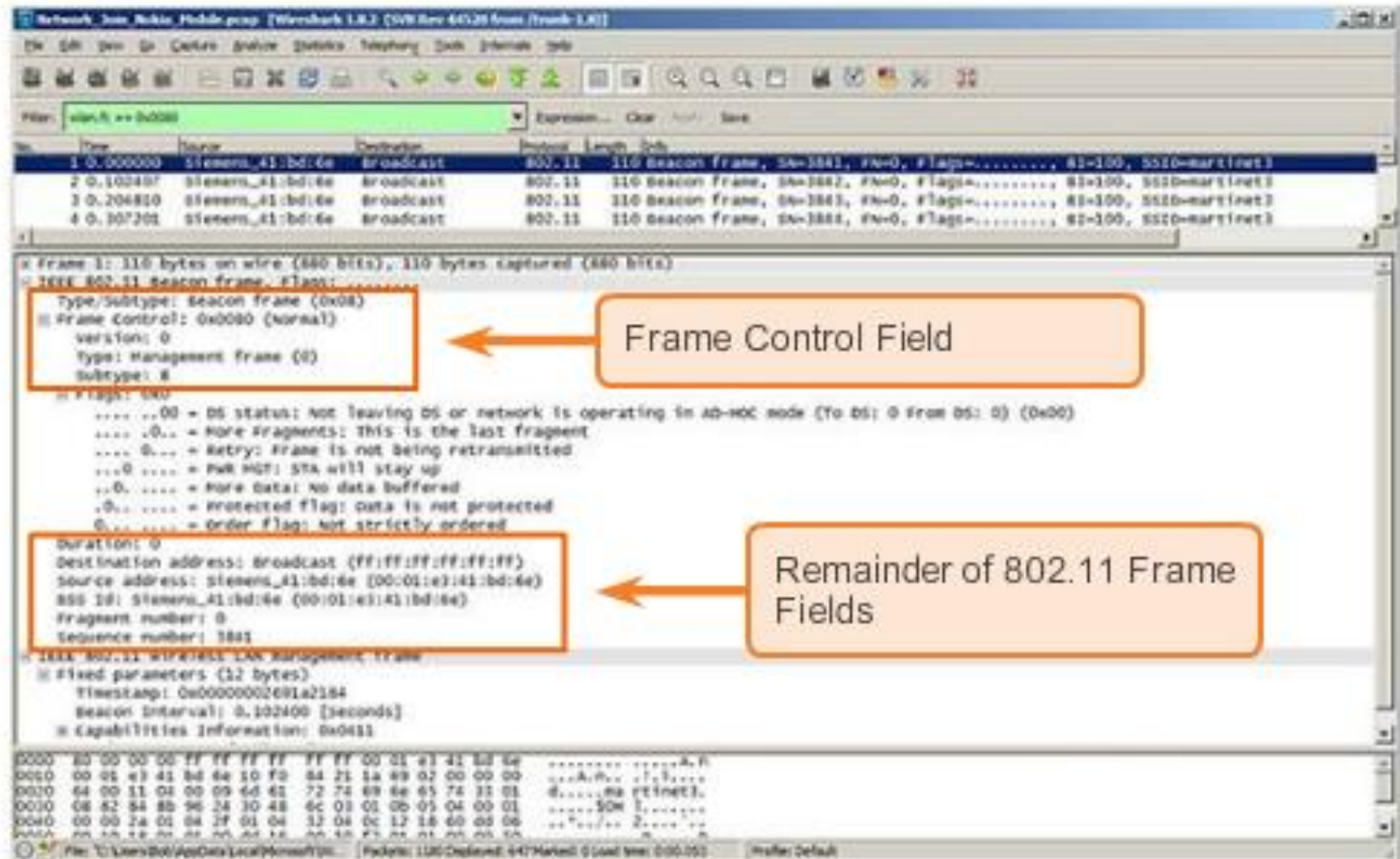
- IEEE 802.11 uspostavlja šemu kanala koji se koriste u nelicenciranom ISM RF opsegu u WLAN mrežama.
- 2,4 GHz opseg je raspodijeljen u 11 kanala u USA i 13 kanala u Evropi.
- Preporuka je da se izbjegava preklapanje kanala. Primjer: Ako se koriste tri AP mogu se koristiti kanali 1,6,11.



Wireless 802.11 Frame



Wireless 802.11 Frame



Wireless 802.11 Frame

The image shows a Wireshark packet capture window titled "Network_Join_Rokua_Mobile.pcap [Wireshark 1.8.2 (SVN Rev 44520 from /trunk/1.8)]". The filter is set to " wlan.fc == 0x0080 ". The packet list shows four packets, all of which are 802.11 Beacon frames from source "Siemens_41:bd:6e" to destination "Broadcast". The first packet is selected, and its details pane is expanded to show the "Frame Control" subfield.

Filter: wlan.fc == 0x0080

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=3841, FN=0, Flags=....., BI=100, SSID=martinet3
2	0.102407	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=3842, FN=0, Flags=....., BI=100, SSID=martinet3
3	0.204810	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=3843, FN=0, Flags=....., BI=100, SSID=martinet3
4	0.307201	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=3844, FN=0, Flags=....., BI=100, SSID=martinet3

Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)

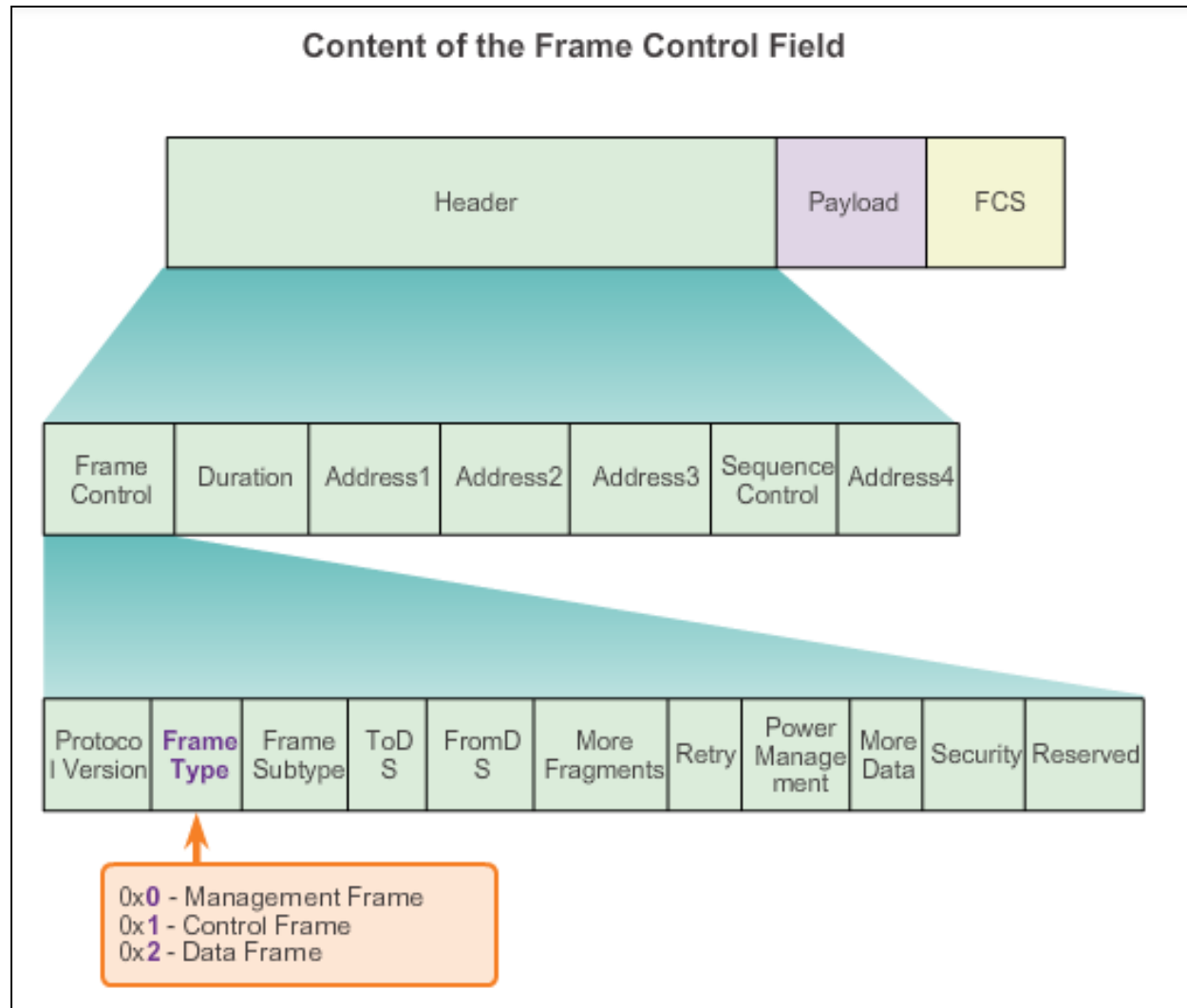
- IEEE 802.11 Beacon frame, Flags:
- Type/Subtype: Beacon frame (0x08)
- Frame Control: 0x0080 (Normal)
- Version: 0
- Type: Management frame (0)
- Subtype: 8
- Flags: 0x0
 -00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
 -0.. = More fragments: This is the last fragment
 - 0... = Retry: Frame is not being retransmitted
 - ...0 = PWR MGT: STA will stay up
 - ..0. = More Data: No data buffered
 - ..0... = Protected flag: Data is not protected
 - 0... = Order flag: Not strictly ordered
- Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
- Source address: Siemens_41:bd:6e (00:01:e3:41:bd:6e)
- BSS id: Siemens_41:bd:6e (00:01:e3:41:bd:6e)
- Fragment number: 0
- Sequence number: 3841
- IEEE 802.11 wireless LAN management frame
- Fixed parameters (12 bytes)
 - Timestamp: 0x00000002691a2184
 - Beacon Interval: 0.102400 [seconds]
 - Capabilities Information: 0x0411

Frame Control Subfields

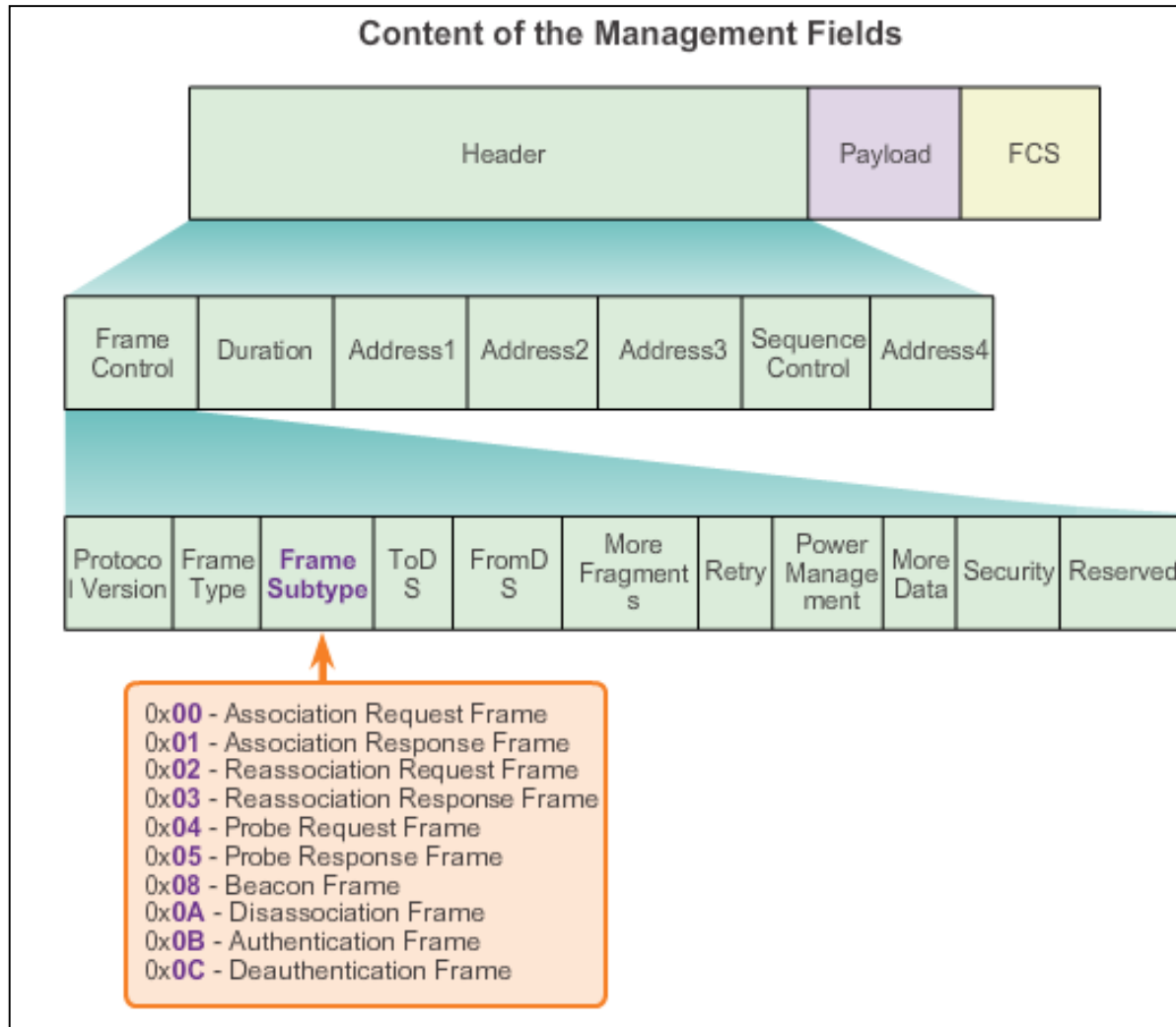
0000 80 00 00 00 ff ff ff ff ff ff 00 01 e3 41 bd 6eA.n
0010 00 01 e3 41 bd 6e 10 f0 84 21 1a 69 02 00 00 00A.n...
0020 64 00 11 04 00 09 6d 81 72 74 69 6e 65 74 33 01 d.....ma rtinet3.
0030 08 82 84 8b 96 24 30 48 6c 03 01 0b 05 04 00 0110m t...
0040 00 00 2a 01 04 2f 01 04 32 04 0c 12 18 60 d5 06/... 2.....
.....

File: C:\Users\Bob\AppData\Local\Microsoft\... Packets: 1180 Displayed: 647 Marked: 0 Load time: 0:00.053 Profile: Default

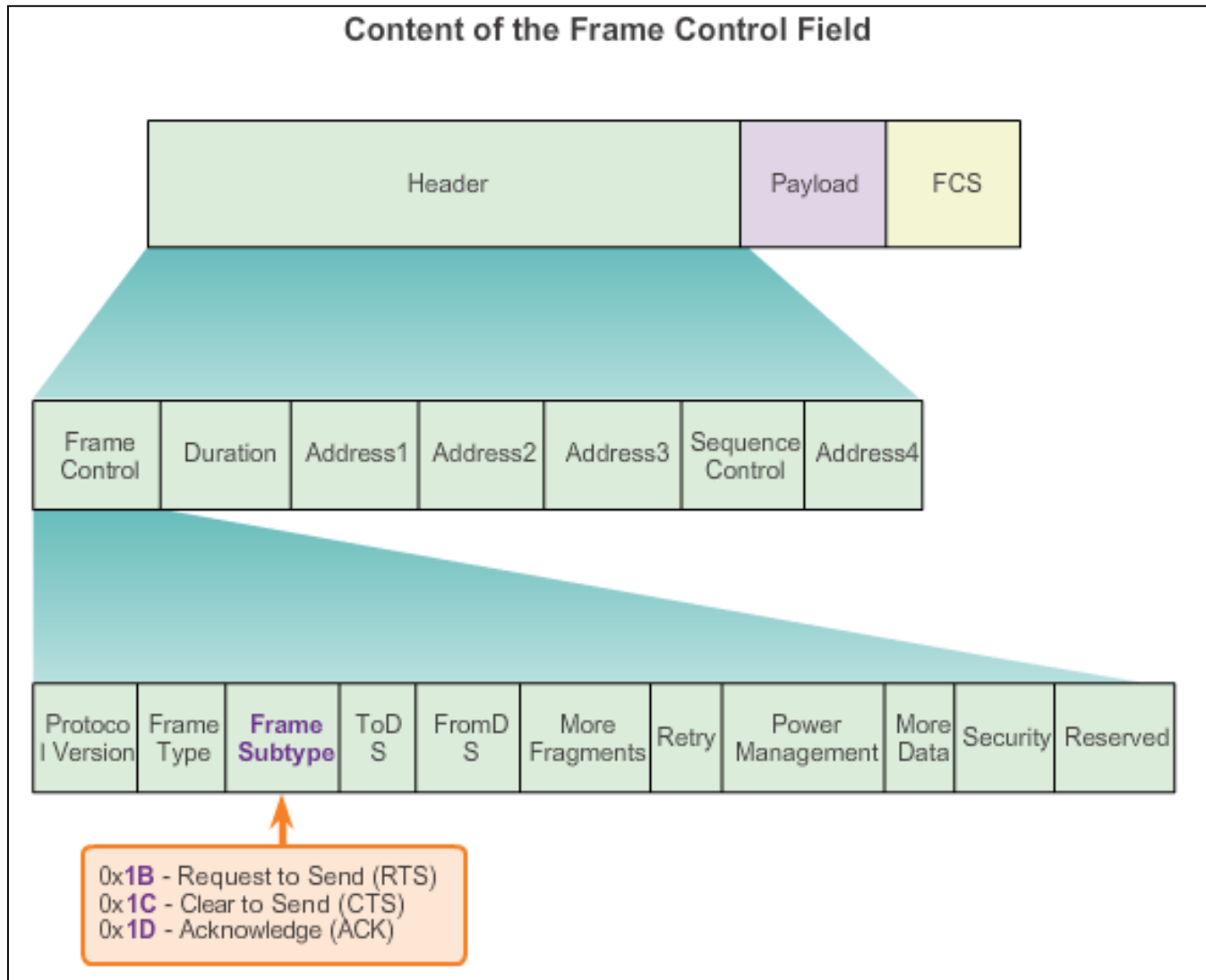
Wireless Frame Type



Management Frames



Control Frames

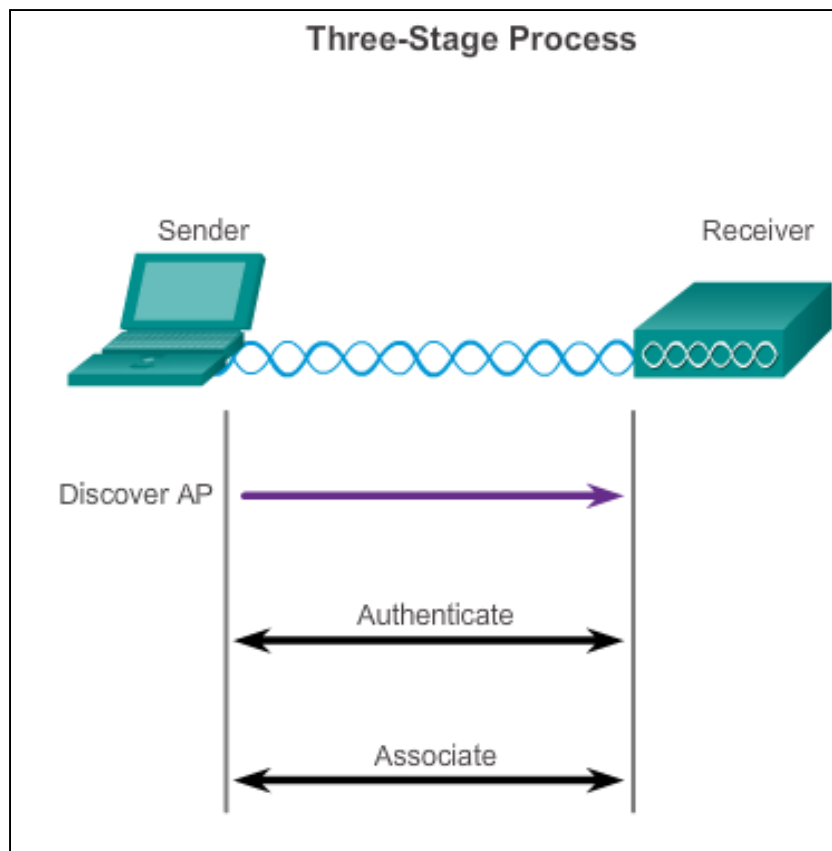


Asocijacija klijenata na AP –tri faze

- Otkrivanje AP

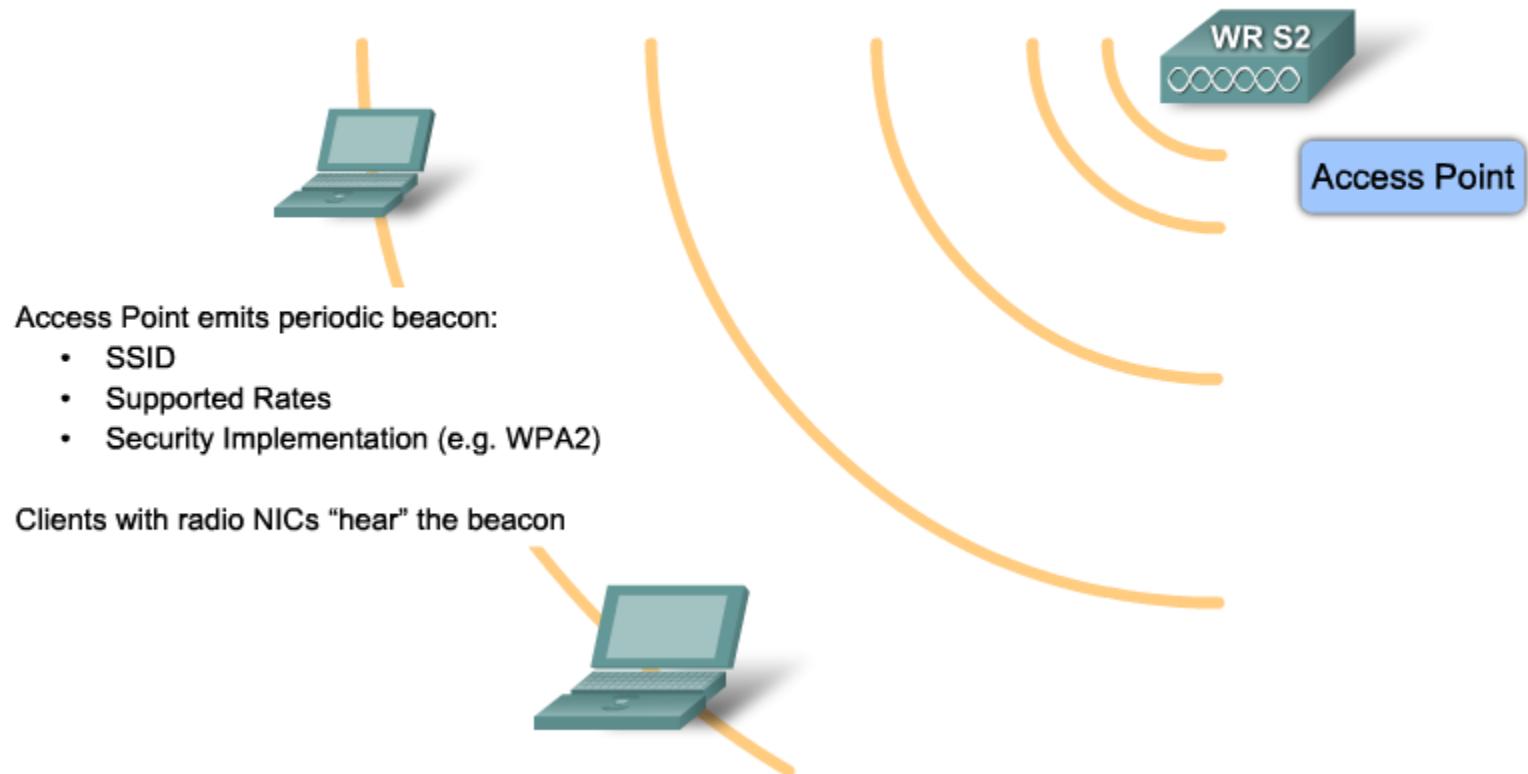
Passive Mode: Ne mora se poznavati SSID

Active Mode: Klijent mora da poznaje SSID



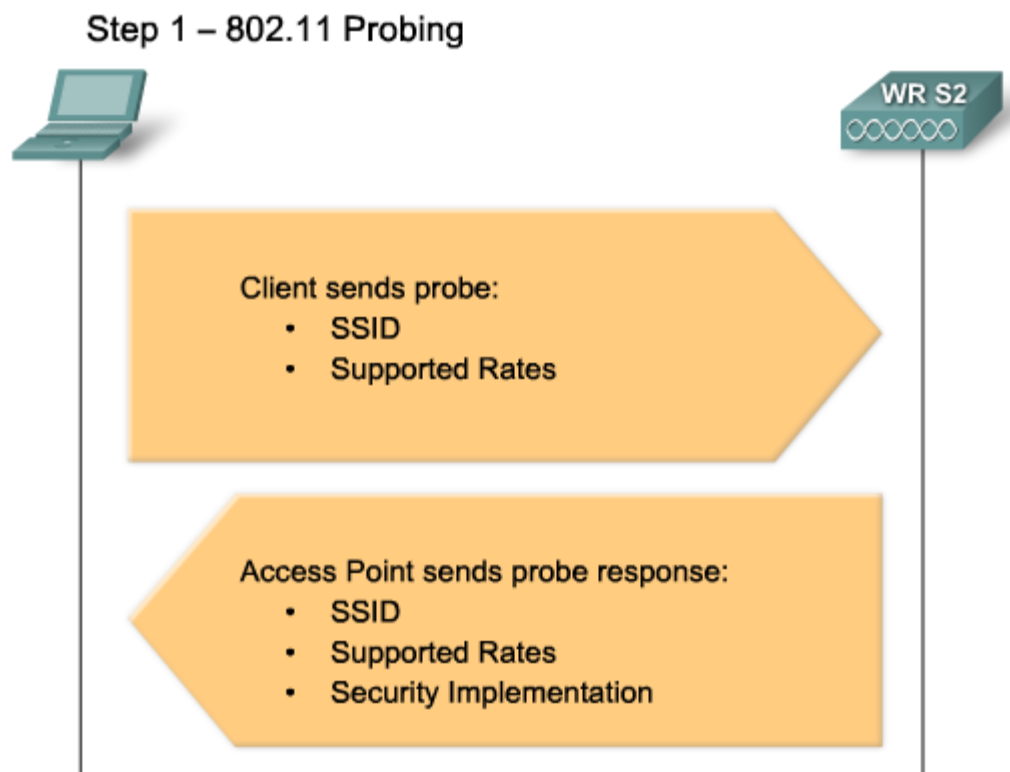
Asocijacija klijenata na AP - Beacon

- Beacon je frejm koji se u WLAN mrežama koristi da se oglasi prisustvo.
- Uloga je da WLAN klijenti uče koje mreže i AP su raspoložive u datoj oblasti.



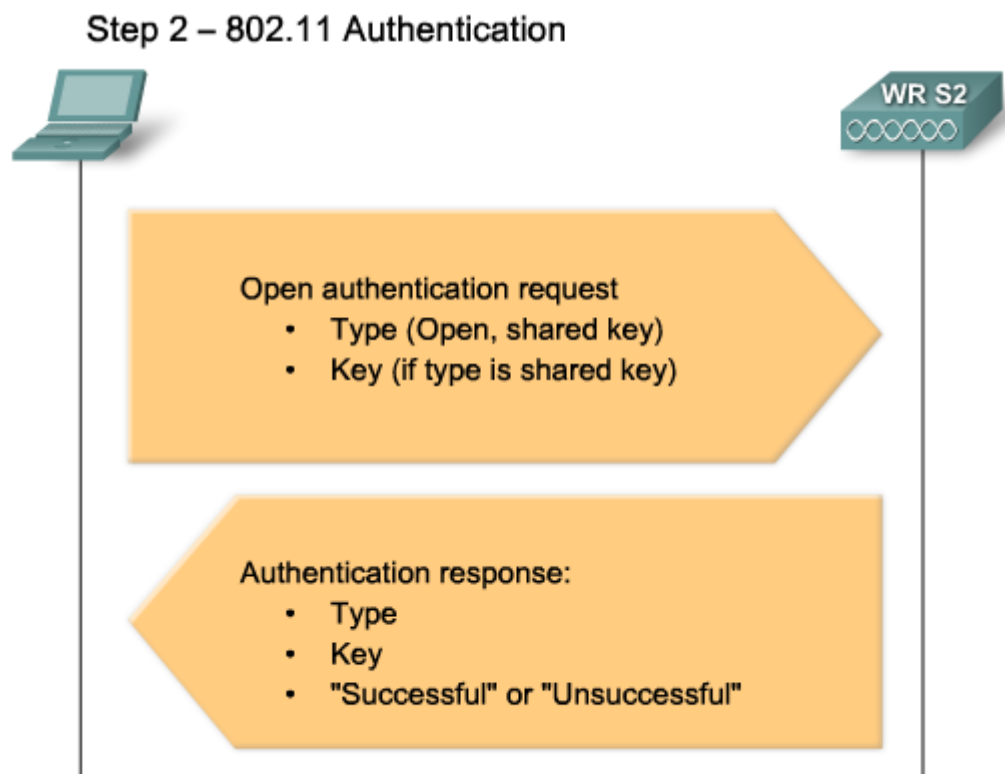
Asocijacija klijenata na AP - Probing

- Klijenti traže mrežu šaljući „probe“ zahtjev na više kanala
- Probe request specificira SSID i bit rate.



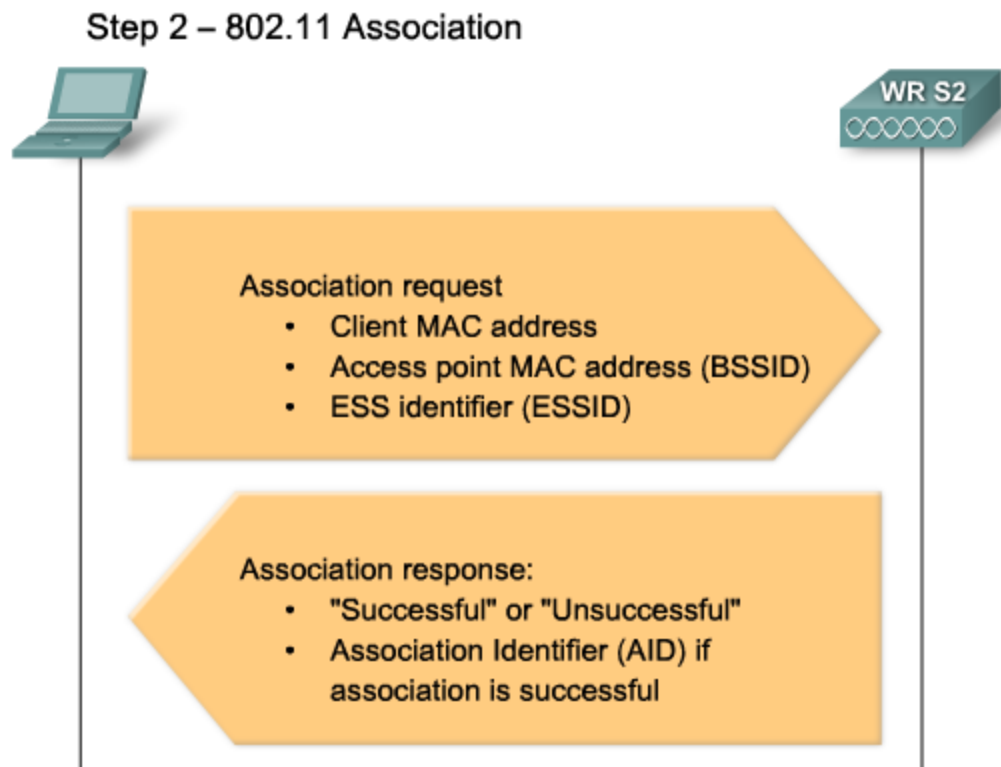
Asocijacija klijenata na AP - autentifikacija

- Dva mehanizma autentifikacije:
 - open authentication,
 - upotreba ključeva koji se dijele između AP i klijenta



Asocijacija klijenata na AP -asocijacija

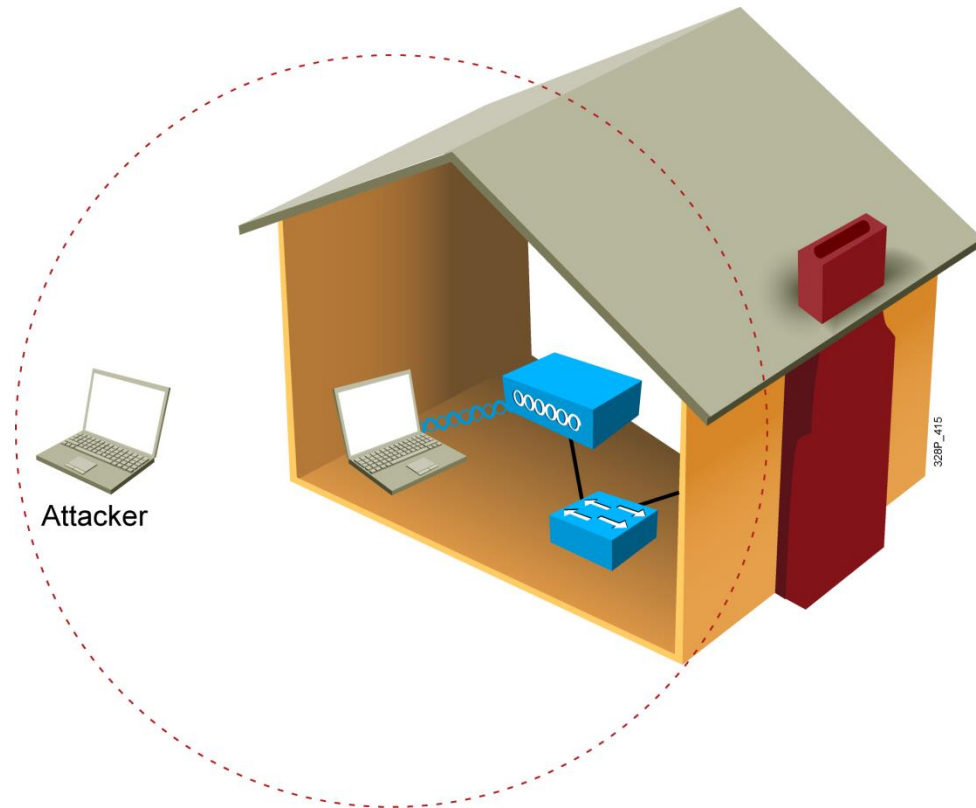
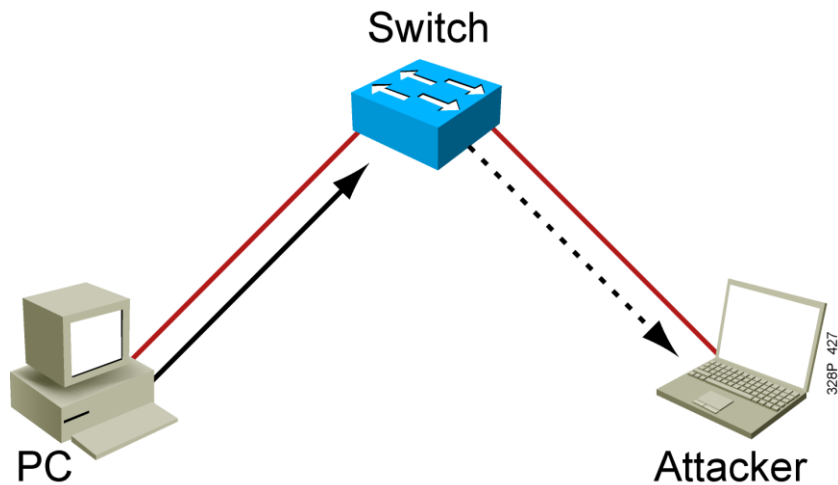
- Uspostavlja se veza između AP i klijenta
- Klijent uči BSSID, a AP mapira logički port (AID) za klijenta
- AID (association identifier) je ekvivalent portu na switch-u



Wireless LAN

-osnovni pojmovi sigurnosti

Privatnost: Wired / Wireless



Autentifikacija-opšti koncepti

- Dokaz o identitetu se može pružiti koristeći:

- Nešto što se poznaje!

- Password

- „Something you do“

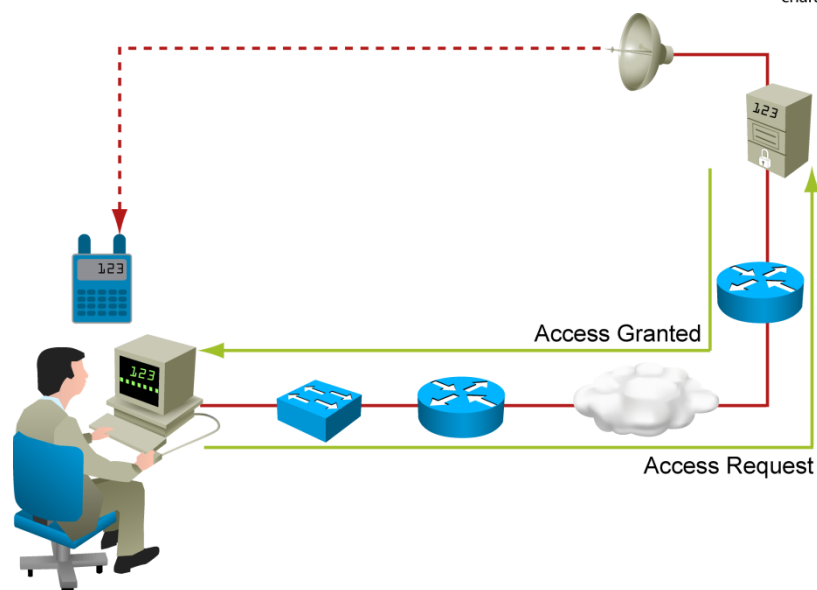
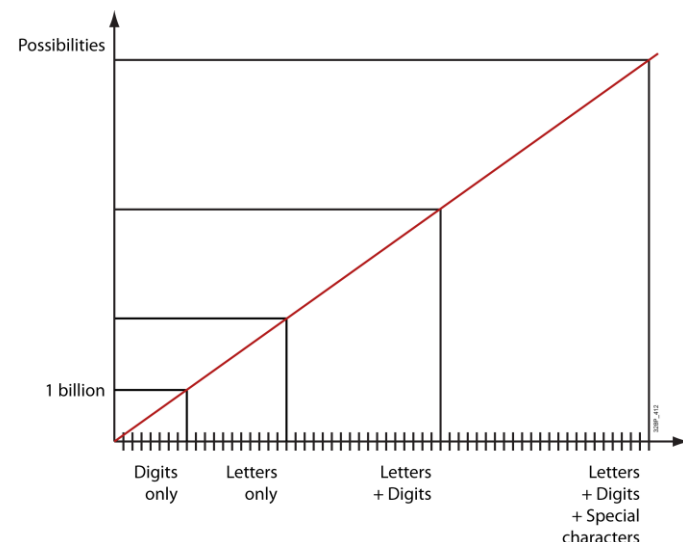
- Nešto što se posjeduje!

- „Physical object“

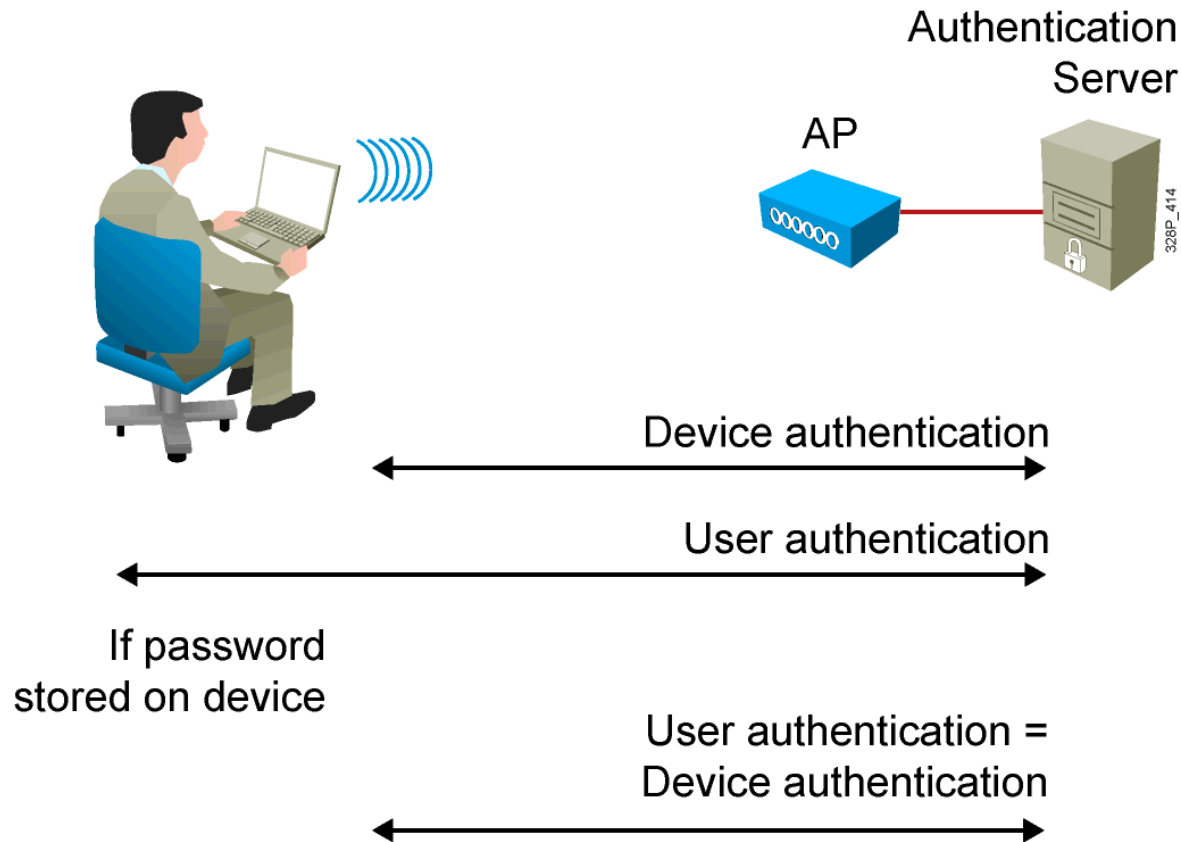
- „Value read from a device you have“

- Nešto što jesi!

- „Biometric reading“

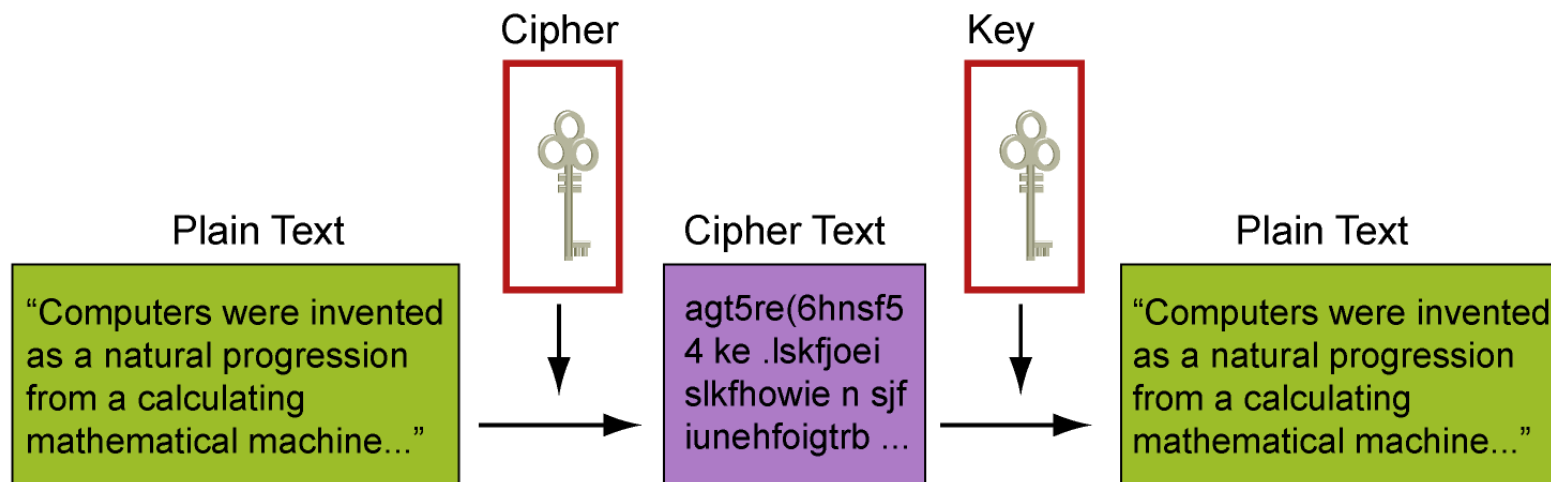


Authentifikacija uređaja/korisnika

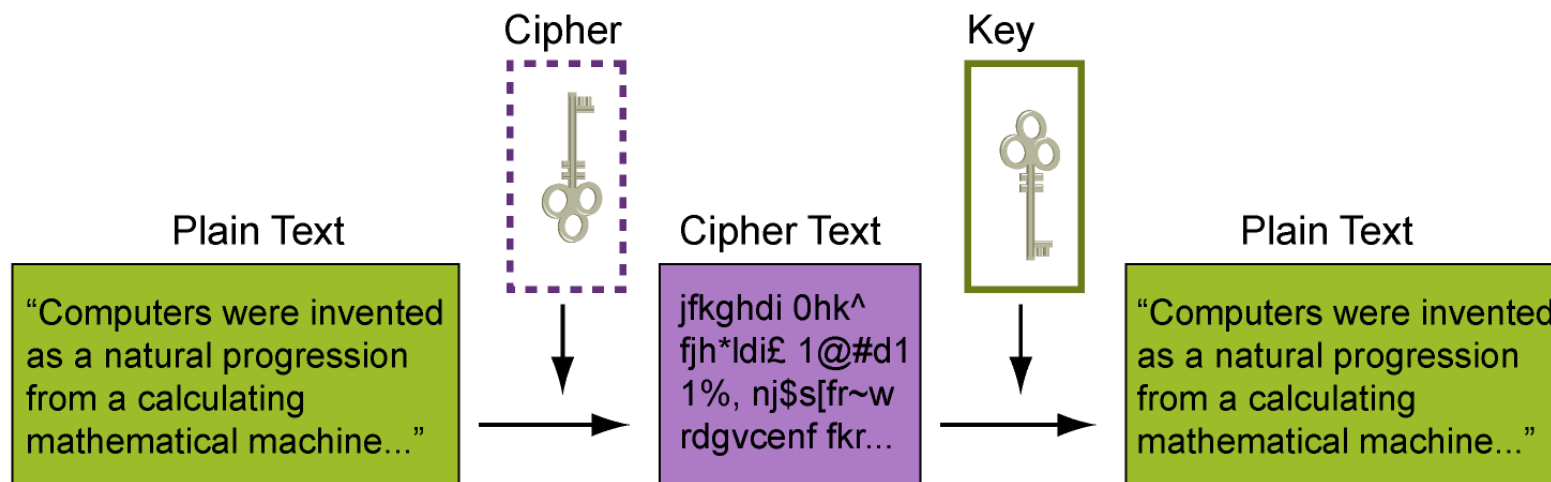


Simetrična i asimetrična enkripcija

Symmetric



Asymmetric



Open, WEP, MAC-osnovni pojmovi

- Open autentifikacija je „default“ IEEE 802.11 metod pristupa. Bazira se samo na poznavanju SSID.
- WEP se može koristiti i za autentifikaciju i enkripciju. Ne smatra se pouzdanim metodom zaštite privatnosti u bežičnim mrežama.
- Moguće je realizovati filtriranje bazirano na MAC adresama po WLAN. Autorizacija klijenata po MAC adresama se može izvesti lokalno, na kontroleru ili pomoću RADIUS servera.

Autentifikacija -open



- 1- Client sends probe request. [RF-Packet]
- 2- Access points (A/B) send probe response. Client evaluates access point response, selects best access point. [RF-Packet]
- 3- Client sends authentication request to selected access point (A). [RF-Packet]
- 4- Access point (A) confirms authentication and registers client. [RF-Packet]
- 5- Client sends association request to selected access point (A). [RF-Packet]
- 6- Access point (A) confirms association and registers client. [RF-Packet]

Primjer: WLANs > Edit > Security

WLANs > Edit

General	Security	QoS	Advanced
Layer 2	Layer 3	AAA Servers	
<p>Layer 2 Security <input type="text" value="None"/> <input checked="" type="checkbox"/></p> <p><input type="checkbox"/> MAC Filtering</p>			

Autentifikacija : PSK (WEP)

- WLAN sigurnosni protokol definisan u 802.11 specifikaciji:
 - Realizuje se na Layer 2 i ne omogućuje „end-to-end“ sigurnost




- 4- Access point (A) sends authentication response containing the unencrypted challenge text. [RF-Packet]
- ← 5- Client encrypts the challenge text using one of its WEP keys and sends it to access point (A). [RF-Packet]
- 6- Access point (A) compares the encrypted challenge text with its copy of the encrypted challenge text. If the text is the same, access point (A) will allow the client onto the WLAN. [RF-Packet]

Primjer: WEP konfiguracija

WLANs > Edit

General Security QoS Advanced




Layer 2 Layer 3 AAA Servers

Layer 2 Security Static WEP 

☐ MAC Filtering

Static WEP Parameters

802.11 Data Encryption Current Key: 104 bits WEP Static Key (Key Index = 1)

Type	Key Size	Key Index	Encryption Key	Key Format
WEP	not set 	1 		ASCII 

☐ Allow Shared Key Authentication

☐ Enable

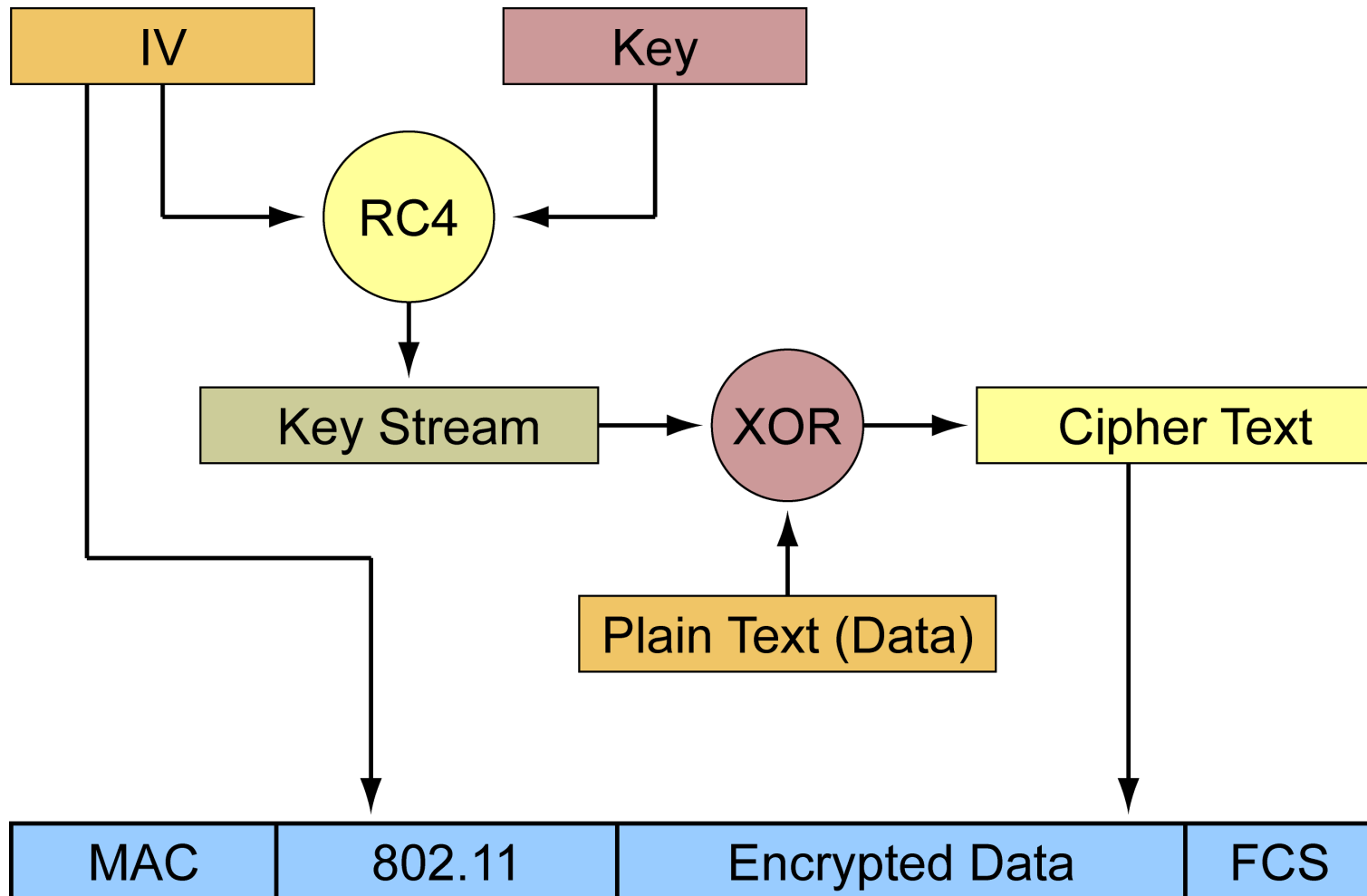
not set

40 bits

104 bits

128 bits

WEP Engine



Primjer: WLAN > Edit

Može se realizovati kombinacija sa drugim principima Layer 2 ili Layer 3 sigurnosti

