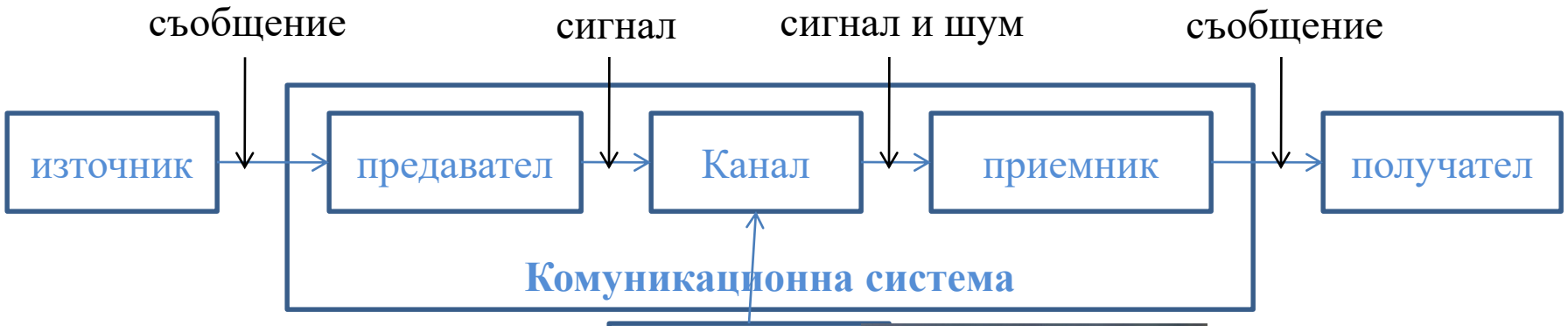
Безжични мрежи.WiFi

доц.д-р инж. Венета Алексиева

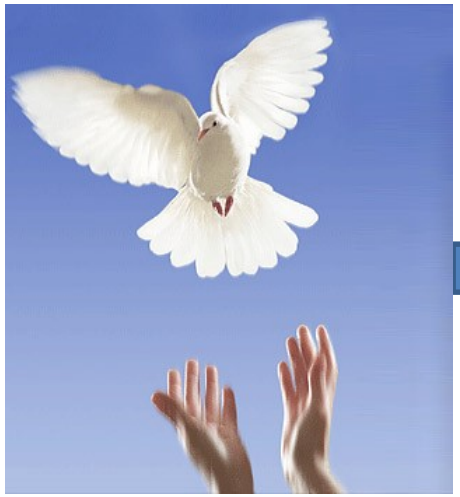
Основни моменти

- Безжични технологии
- Топологии
- Сигурност в LAN безжична мрежа
- Стъпки на конфигуриране на AP
- Проектиране на WLANs
- Отстраняване на проблеми в WLAN

Предаване на данни



Смущения при предаването



Пренос по канала за връзка

източник

получател

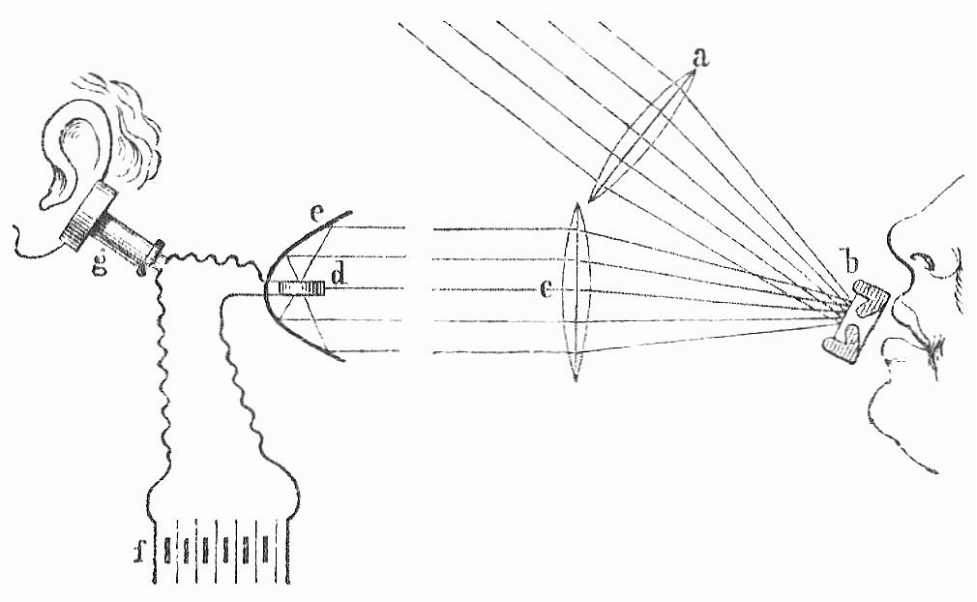
Идеята

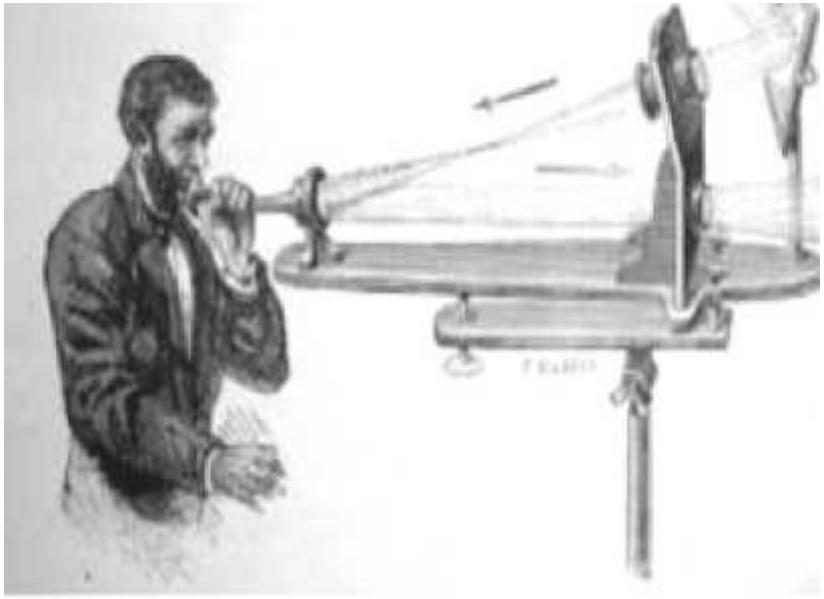
Характеристики:

- Ниски скорости 55 км/ч (рекорд 1896г. - 125км/ч)
- Half-duplex
- Загуба на пакети от смущения в преносната среда
- Разстояние – до 700 мили на ден

- Най-голямата мрежа за комуникации чрез гълъбите е създадена в Сирия и Персия около 5 век пр. Хр.
- През римската епоха - за предаване на резултатите от спортните събития по време на Олимпийските игри.
- ПСВ и ВСВ - информация по време на военни действия.
- Последната станция на пощенски гълъби е била закрита в Индия през 2004 година

Аналогов сигнал безжично?





- На 3 юни 1880 година асистентът на Александър Бел – Чарлз Тейнтър предава речеви сигнал чрез слънчев лъч от покрива на Franklin School към прозореца на Bell’s laboratory, на разстояние 213 метра. Изобретението е наречено **Фотофон**.
- Развитието на измервателната техника е позволило възраждането на photoacoustic ефект през 1970г.

Какво искат…

Потребителите	Провайдерите на услуги
•По-голямо покритие •Високо качество на услугите за пренос на глас и видео •Скорост •Издържливи батерии- малка консумация на енергия •Малък размер на устройствата - ергономичност •Ниска цена	•По-голяма печалба •По-малки инвестиции в инфраструктура •Сигурност – да не се крадат услуги •Лесна поддръжка/подмяна на устройства •Няколко услуги през съществуваща инфраструктура •Дълъг живот на устройствата •По-голям капацитет на връзките

Преди началото

- 1838г. - Самуел Морз – телеграф
- 1895г. - Маркони – първо радио предаване на 18 мили разстояние
- 1915г.- предаване на глас по безжична връзка между Ню Йорк и Сан Франциско
- 1946г. - първа мобилна телефонна услуга между 25 града в САЩ

Началото

- По време на Втората световна война за военна комуникация за армията на САЩ - базирани на радиовълнова технология и разпределен спектър.
  - разпределеният спектър е по-устойчив на заглушаване.
- След 1945 г. - за цивилните предприятия.
- 1962г. е изстрелян първият сателит в орбита.
- През 1970 г. Университета на Хавай, под ръководството на Норман Абрамсън е разработена **ALOHAnet.**
  - седем компютъра на различни острови общуват двупосочно с централен комутатор на остров Оаху
- **ALOHAnet дава началото и следват три поколения безжични мрежи до появата на стандарт…**

И след началото

- Първоначално хардуерът за WLAN е твърде скъп и се ползва само на места, където окабеляване не е възможно.
- Първите реализации не са стандартизирани, а са на всеки производител – собствени протоколи и хардуер.
- 1991г. HIPERLAN като 5 GHz стандартизирана технология (EN300652, ETS300836) е алтернативен на ATM.
- 1997г. стартира IEEE 802.11 за wireless LANs - Wi-Fi
- 2000г. се появява HIPERLAN/2

Първото поколение (1G)

- Разработено в началото на 1980 от радиолюбители.
- В САЩ се нарича Advance Mobile Phone Service (AMPS) (на 50 KHz , разделени на две 25 MHz канала за двете посоки)
- В Европа - European Total Access Communication System (ETACS)
- Много от клетъчните системи от първо поколение в Европа са несъвместими и това поражда появата на 2G.
- Характеристики:
  - Работи в честотния диапазон 901-928 MHz.
  - Скорости под 9600 bit/s
  - Клетъчно предаване
  - задръстване на честотната лента
  - относително ниска скорост
  - ограничена употреба от потребителите, предимно за военни цели

Безжични телефонни слушалки- предшественик на мобилния телефон

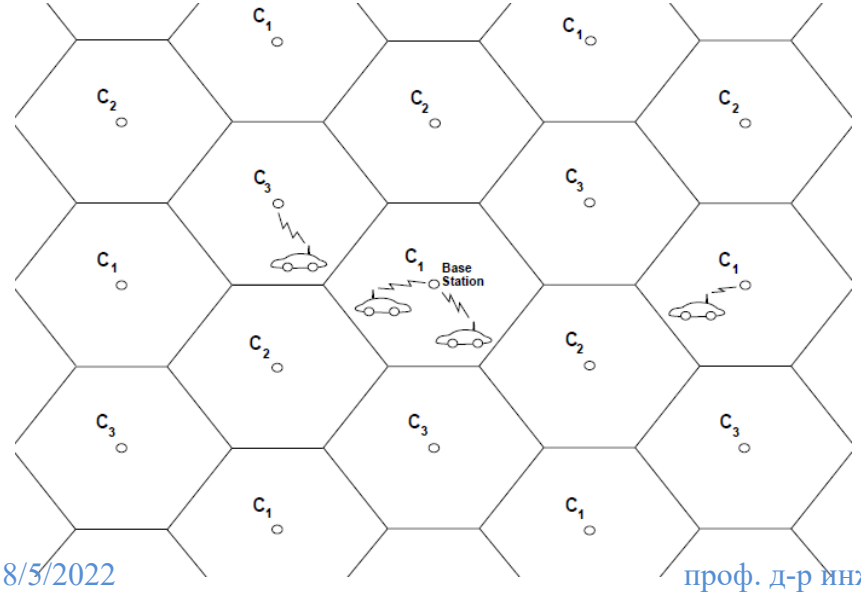
- Първоначалните безжични телефонни слушалки:
  - имат лошо качество на звука и бързо бяха отхвърлени от потребителите.
  - ограничено до няколко стаи от къща или офис.
  - Движението на тези безжични слушалки е изключително ограничено- трябва да останат в обсега на своята база.
  - по-висока плътност на тези системи в малка област, може да доведе до значително повлияване между системите.

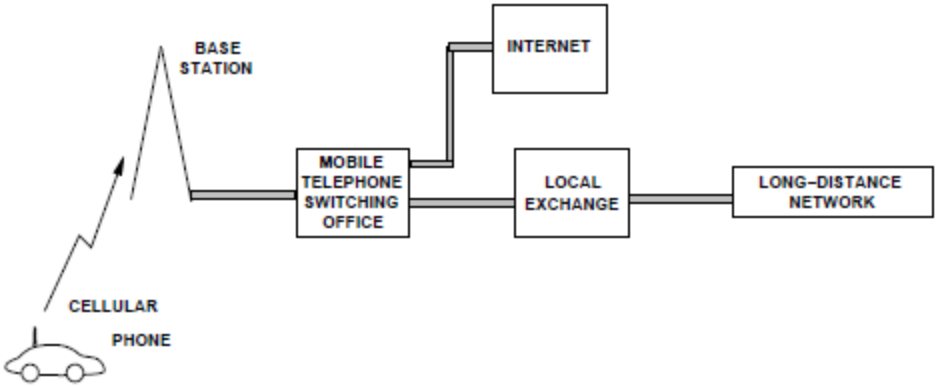
Второто поколение (2G)

- 1985г.- Разработено веднага след обявяването на Federal Communications Commission(FCC) на експериментални честотни ленти за невоенно използване на технологията за разширяване на спектъра.
- 3 различни стандарта за предаване – в САЩ, Европа и Япония
- Характеристики:
  - данни със скорост до 100 Kbit / sec.
  - честотни ленти 900MHz, 2.4GHz and 5.8GHz
  - За индустриални, научни и медицински цели (ISM)
  - Клетъчно предаване

Клетъчни системи

- Клетъчните системи осигуряват двупосочна комуникация с глас и данни с регионално, национално или международно покритие.
- Те първоначално са били предназначени за мобилни терминали в превозни средства с антени, монтирани върху покрива на превозното средство.
- Идея на клетъчния дизайн е повторно използване на честотата в пространствено разделени клетки, т.к. мощността на сигнала пада с разстоянието.





Третото поколение (3G)

- Международния съюз по далекосъобщения (ITU) определя стандарт CDMA, който е в основата на 3G.
- Стандартът 3G е несъвместим с 2G, така че доставчиците на услуги трябва да инвестират в нова инфраструктура, преди те да могат да осигурят 3G услуги.
- Първите 3G системи са в Япония, т.к. честотите за 3G са свободни.
- В Европа и САЩ честотите за 3G се разпределят въз основа на търг, т.е. ISP влага огромна първоначална инвестиция, за да предостави 3G услуги.
- 1990г.- безжични модеми, насочени към съвместимост със съществуващите локални мрежи с данни със скорост до 2Mbit / sec.
- 1991г. – първият IEEE семинар за безжична LAN
- 1997г.- поява на 802.11 IEEE стандарт
- 1998г. – спецификации за GSM
- 2000г. – поява на GPRS
- 2002г. – поява на 802.16 IEEE стандарт
- 2003г.- поява на 802.15 IEEE стандарт

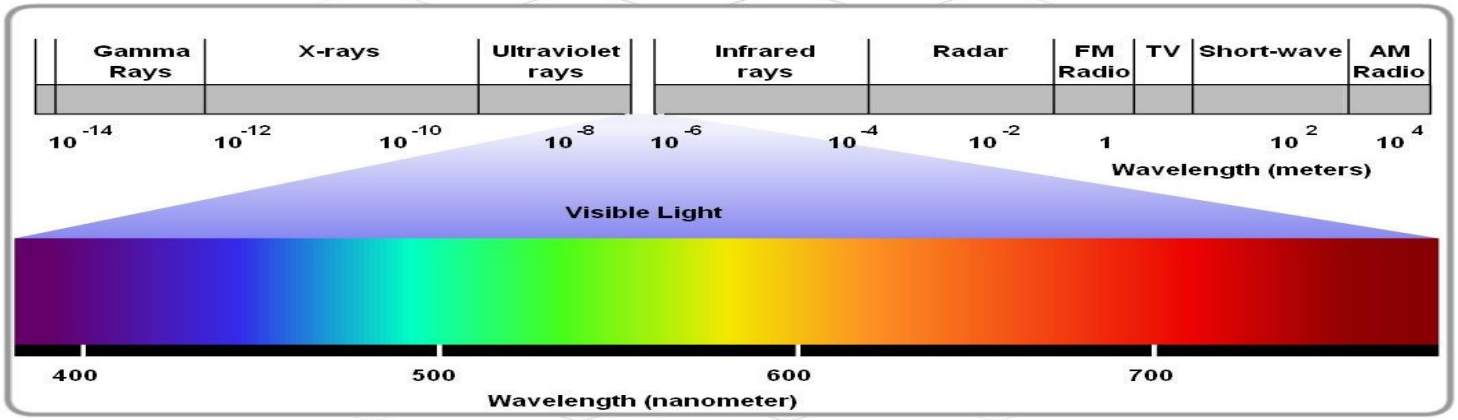
4G/5G

- Технологията поддържа максимална скорост на обмен на данни до 100 Mbps при честотна лента 20 MHz 100 Mbps при движещ се клиент, и 1 Gbps в неподвижно състояние.
- 4G е пригоден специално за пренос на данни, което за потребителите означава по-високи скорости и интерактивни услуги
- 2005г.-поява на 802.16e IEEE стандарт
- 2009г.- начало на стандарти LTE
- 2015г. – началото на LiFi- в Германия – от професор Harald Haas
- На 14.07.2016 FCC одобрява честотен обхват за 5G от 28 GHz, 37 GHz ,39 GHz
- От 2017г Европейската комисия освобождава за 5G честотен обхват от 700MHz

5G

- След излизането на работната програма за 2014-2015 г. на “Horizon 2020 LEIT”, редица организации предлагат набор от проекти, насочени изцяло към разработване на 5G.
- Европейската комисия официално подписа договор „5G-PPP” през декември 2013г. за развитие на 5G мрежите, който има за цел в Европа да се разработят и използват най-малко 20% 5G Standards Essential Patents.
- Цел – преминаване към следващото поколение безжични мрежи - Next Generation Mobile Networks (NGMN).

Същност на безжичните технологии

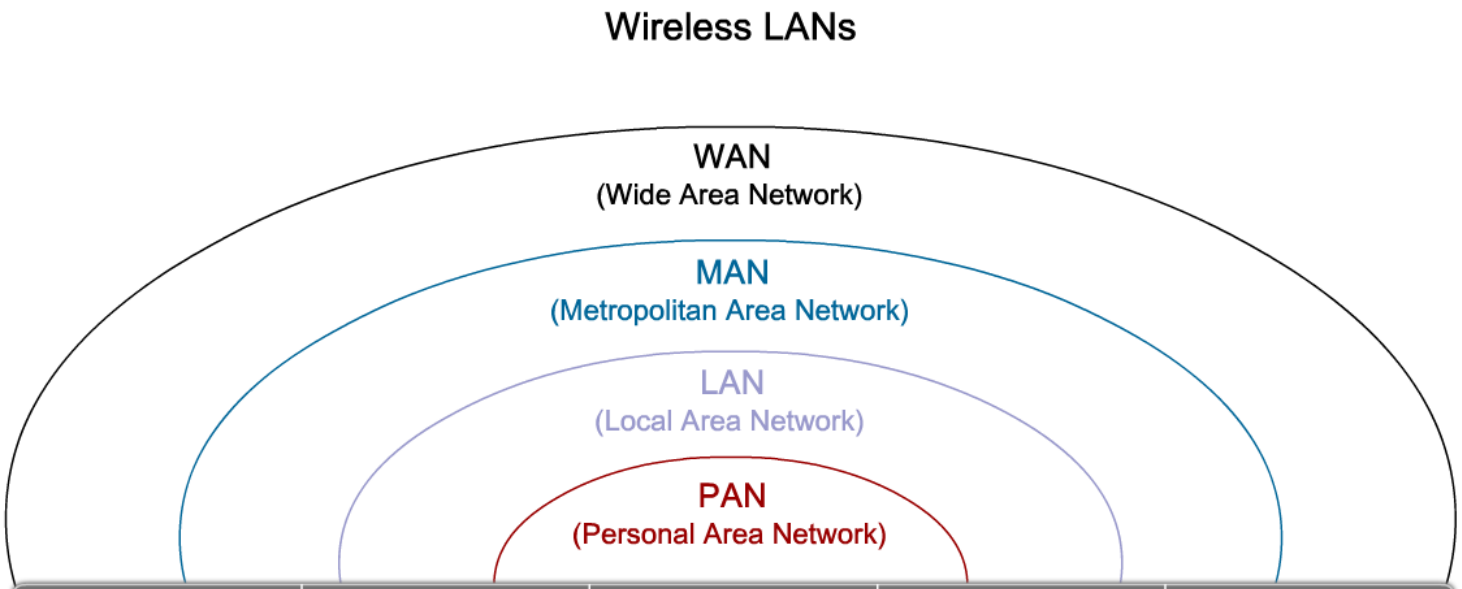


- Някои видове електромагнитни вълни не са подходящи за пренасяне на данни.
- Други части на спектъра са регламентирани от правителствата и лицензирани за различни организации или за специфични приложения.
- Например от 2017г. до 2020г. честотния диапазон на 700MHz, който се използва за радио и телевизионен сигнал се даде на мобилните мрежи по решение на Европейската комисия.

Характеристики на средата

- Устройствата трябва да позволяват няколко режима на работа за пренос на глас, видео, текст, изображения
- Да позволяват roaming
- Да позволяват връзка с >=2 LANs в MAN област
- Енергията е особено важен ресурс в мрежи, където устройствата не могат да презаредят батериите си (сензорни мрежи).
- Безжичните мрежи решават най-важния проблем на икономическата инфраструктура - бързо, надеждно и сравнително евтино на места, където за прокарването на кабелна мрежа трябват големи инвестиции и продължително време.

Видове Wireless мрежи



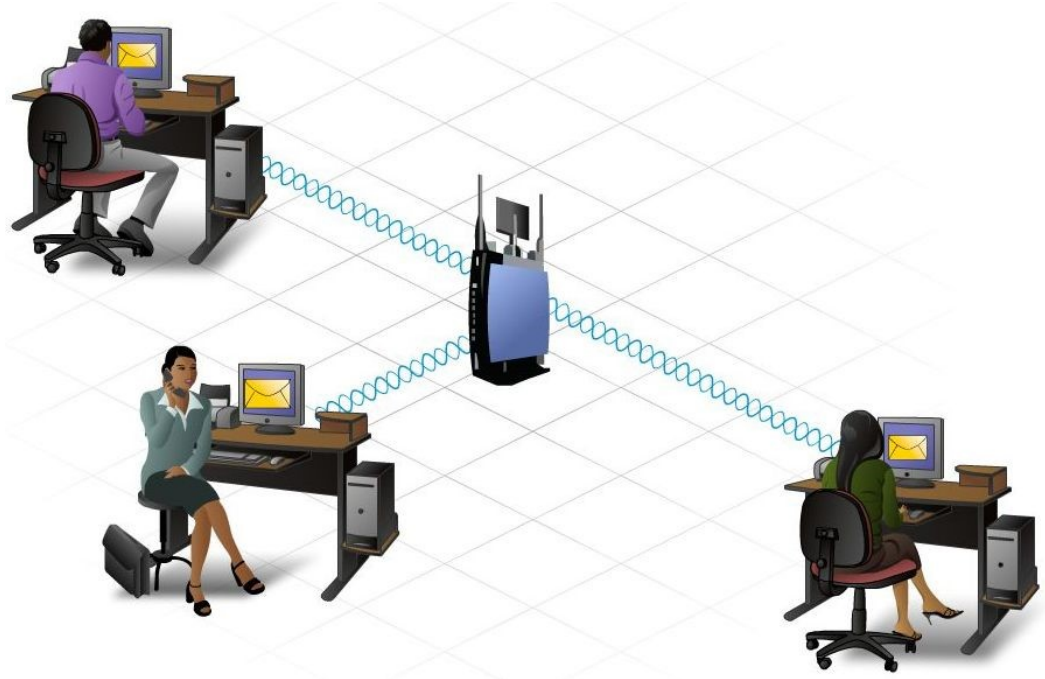
	PAN	LAN	MAN	WAN
Standards	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satellite
Speed	< 1 Mbps	11 to 54 Mbps	10-100+ Mbps	10 Kbps-2 Mbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise Networks	Last Mile Access	Mobile Data Devices

Предимства на Wireless

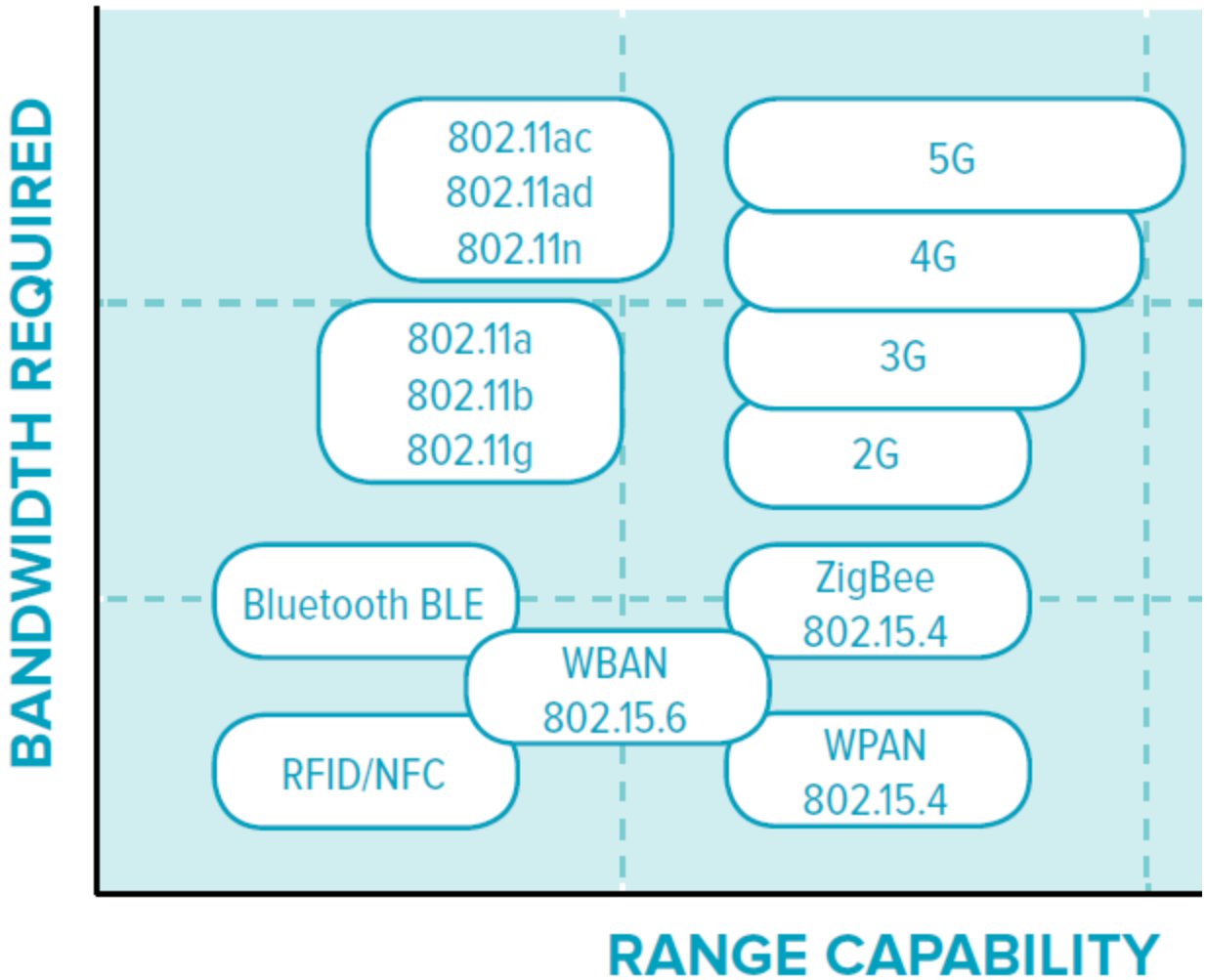
- Удобство
- Мобилност
- Продуктивност
- Лесно внедряване
- Разширяемост
- Цена
- Свързване на абонати, разпръснати в слабонаселена (и труднодостъпна) територия

Недостатъци на Wireless

- Сигурност
- Обхват
- Надеждност
- Скорост



Стандарти



- **Bluetooth -** IEEE 802.15

WiMAX (Worldwide Interoperability for Microwave Access)- IEEE 802.16

Cellular Broadband- 4G/5G

Satellite Broadband

Стандарти 802.11

Версия	Дата	Работна честота	Bandwidth	Скорост	Максимална скорост	Обхват в помещение	Обхват навън
Legacy	1997	2.4 GHz	20 MHz	0,9 Mbit/s	2 Mbit/s	~20 метра	~100 метра
802.11a	1999	5 GHz	20 MHz	23 Mbit/s	54 Mbit/s	~35 метра	~120 метра
802.11b	1999	2.4 GHz	20 MHz	4.3 Mbit/s	11 Mbit/s	~38 метра	~140 метра
802.11g	2003	2.4 GHz	20 MHz	19 Mbit/s	54 Mbit/s	~38 метра	~140 метра
802.11n	2009	2.4 GHz / 5 GHz	20, 40 MHz	130 Mbit/s	300 Mbit/s	~70 метра	~250 метра
802.11y	2008	3.7 GHz	20, 40 MHz	23 Mbit/s	54 Mbit/s	~50 метра	~5000 метра
802.11ac	2012	5 GHz	20, 40, 80, 160 MHz	87,6 Mbit/s	866,7 Mbit/s	-	-
802.11ax	2019	2.4 GHz / 5 GHz	1 GHz-7 GHz-20,40,80,160MHz	11 Gbit/s			
802.11ay	2019	60 GHz		20–40 Gbit/s	1 stream - 44Gbit/s, 4-streams - 176Gbit/s		300–500 метра

Метод за достъп до средата

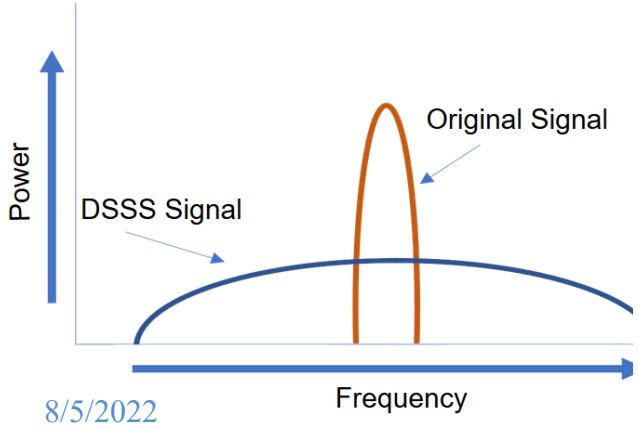
- Методът за достъп до преносната среда определя начинът, по който няколко устройства ползват обща преносна среда, за да предават/приемат през нея.
- Делят се на:
  - **Channel based** - достъпът се реализира с мултиплексиране, което позволява няколко потоци данни / сигнали да споделят една и съща физическа среда за пренос. То се осигурява от физическия слой.
  - **Packet based** - достъпът също се основава на протокол за множествен достъп и контролен механизъм- контрол на достъпа до средата (MAC). Той се осигурява от MAC подслоя на DataLink слоя на модела OSI.

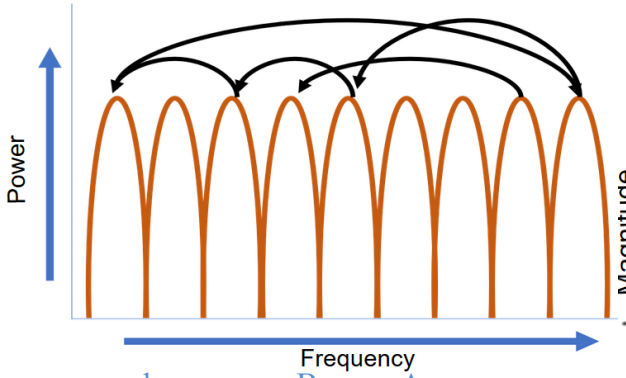
Методи за достъп

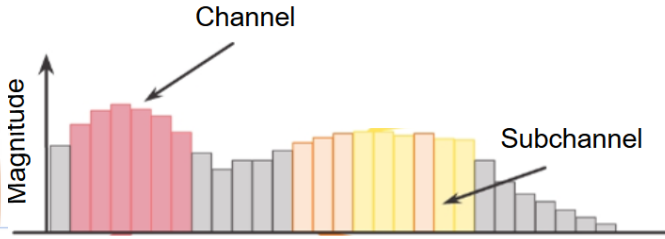
Метод за достъп до средата	Честота(F), време(T), код (C), поляризация(P), Пулс (P)	Конкретни реализации
Channel based	FDMA	OFDMA, WDMA, SC-FDMA
	TDMA	MF-TDMA, STDMA
	CDMA	W-CDMA, TD-CDMA, TD-SCDMA, DS-CDMA, FH-CDMA, MC-CDMA
	SDMA	HC-SDMA
	PDMA	
	PAMA	
Packet based	Collision recovery	ALOHA, Slotted ALOHA, R-ALOHA,AX.25
	Collision avoidance	MACA, MACAW, CSMA, CSMA/CD, CSMA/CA, DCF, PCF, HCF, CSMA/CARP
	Collision free	Token ring, Token bus, MS-ALOHA
	Delay & disruption tolerant	MANET, VANET, DTN, Dynamic Source Routing
Duplex methods	TDD, FDD	

Насищане на канала по честота

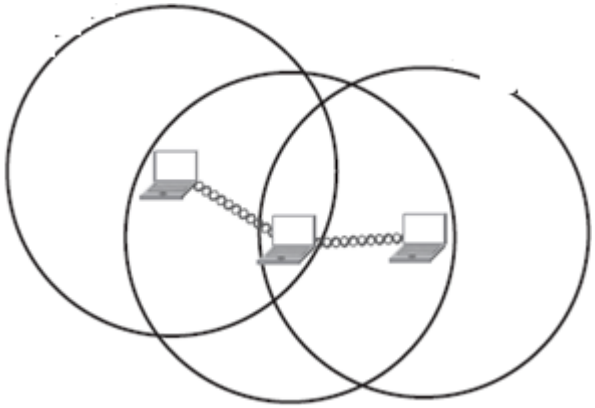
- Direct-Sequence Spread Spectrum (DSSS) - разпръскване на сигнала върху по-широка честота, която ефективно крие разпознаваемия пик на сигнала (при 802.11b)
- Frequency-Hopping Spread Spectrum (FHSS) - бързо превключване на носещия сигнал между много честотни канали (при 802.11, уоки-токи и безжични телефони с мощност 900 MHz , Bluetooth).
- Orthogonal Frequency-Division Multiplexing (OFDM)- един канал използва множество подканали на съседни честоти. Подканалите са ортогонални (802.11a / g / n / ac, 802.11ax е с OFDMA)

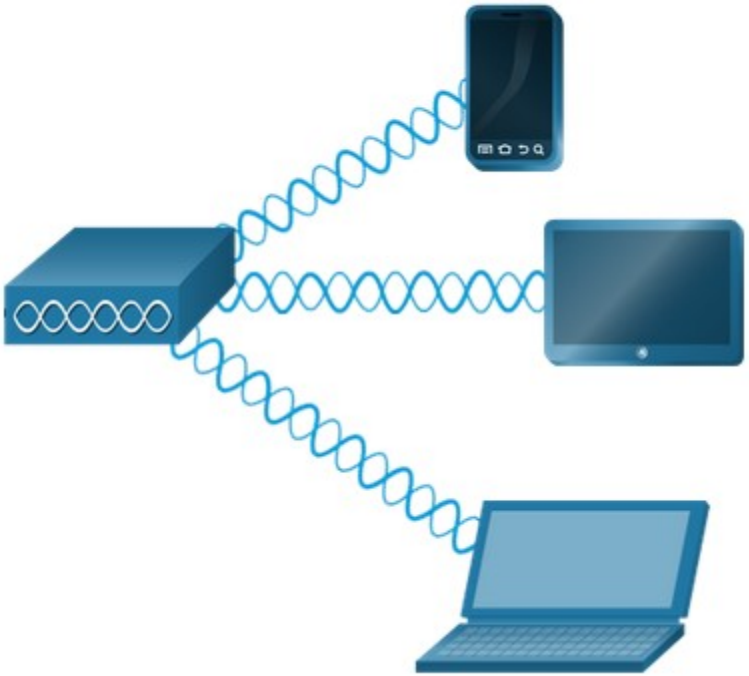






Топологии (1)

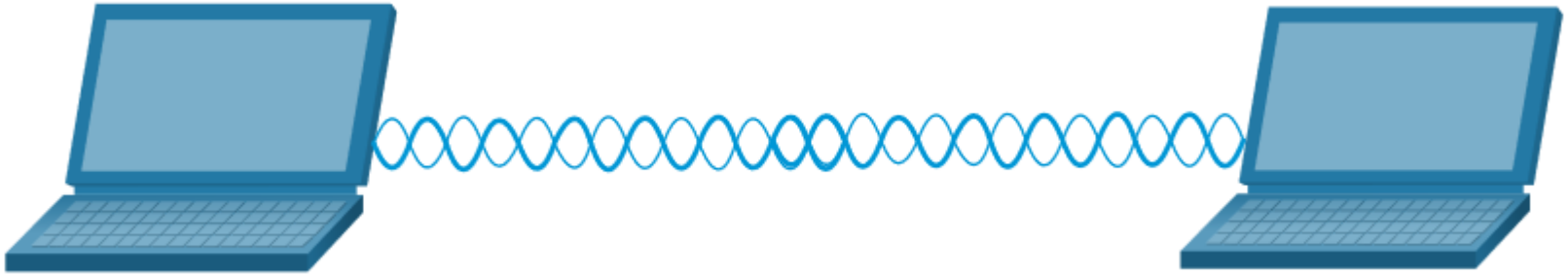




- **Infrastructure**
  - Комуникация през AP
  - AP свързва с кабелна мрежа
  - Няма директна комуникация между крайни устройства

Топологии(2)

- **Ad-hoc**
  - Само директна комуникация
  - Няма relay



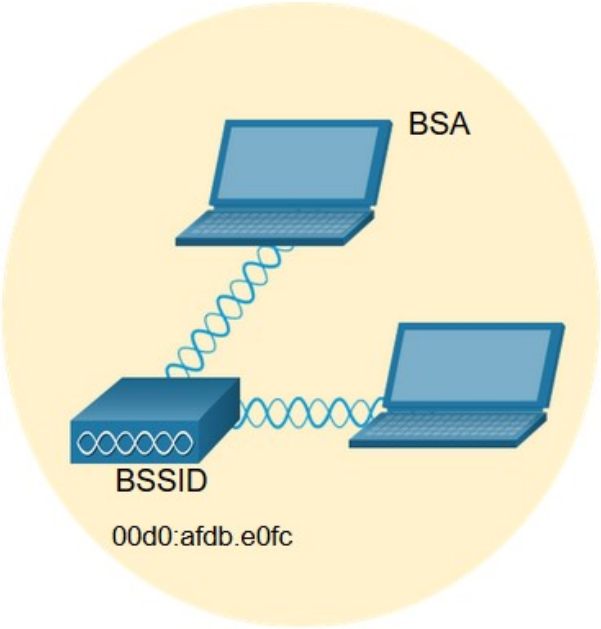
Топологии (3)

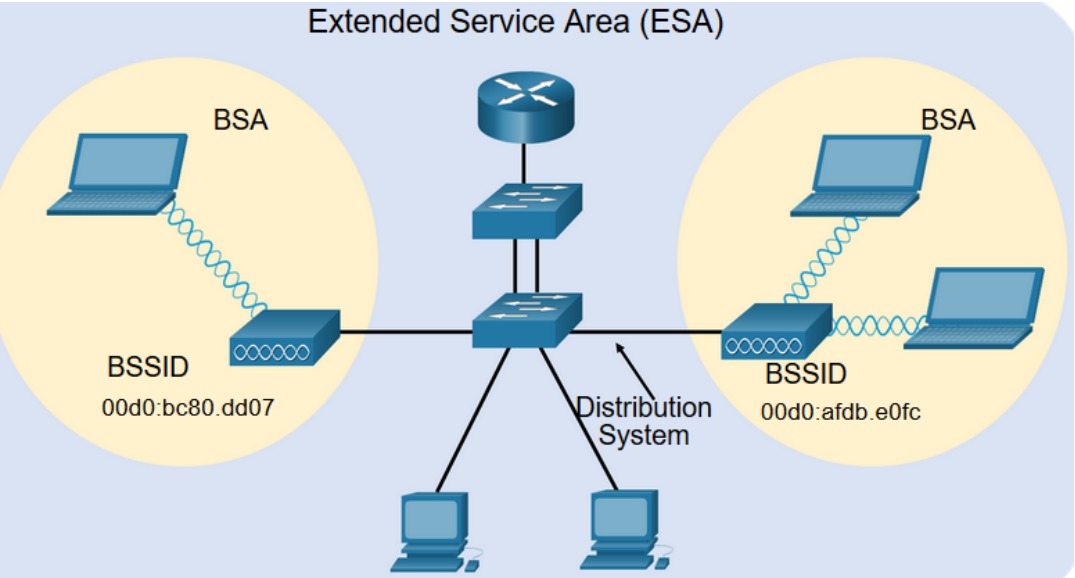
- **Tethering**
  - Вариант на ad-hoc топология
  - Смартфон /таблет с достъп до 3G/4G/5G създава персонален hotspot
  - Другото устройство се свързва със смартфон /таблет по Wi-Fi

BSS/ESS

BSS- Basic Service Set – 1 AP свързва всички клиенти в 1 Basic Service Area (BSA)

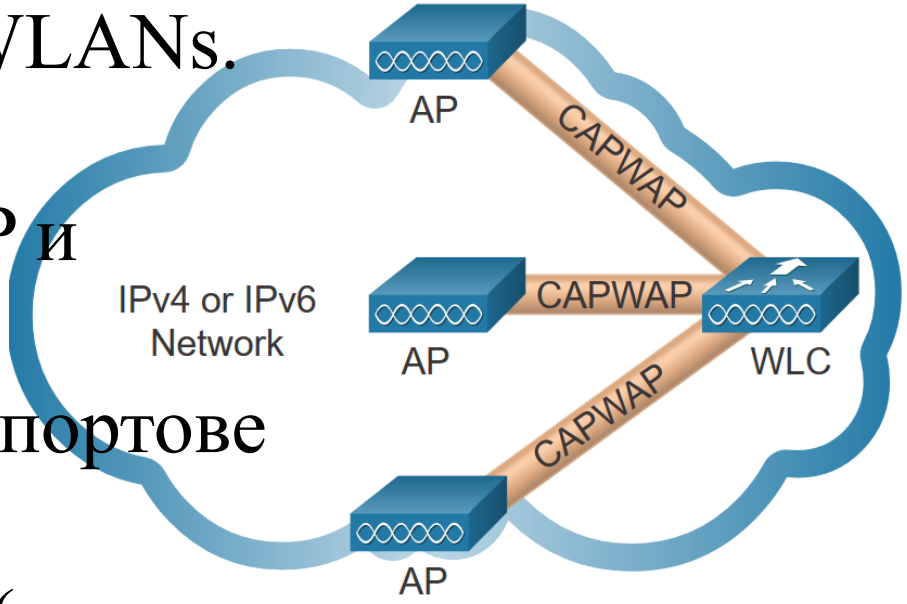
ESS- Extended Service Set ->=2AP изграждат distribution system (DS) (свързват няколко BSS)





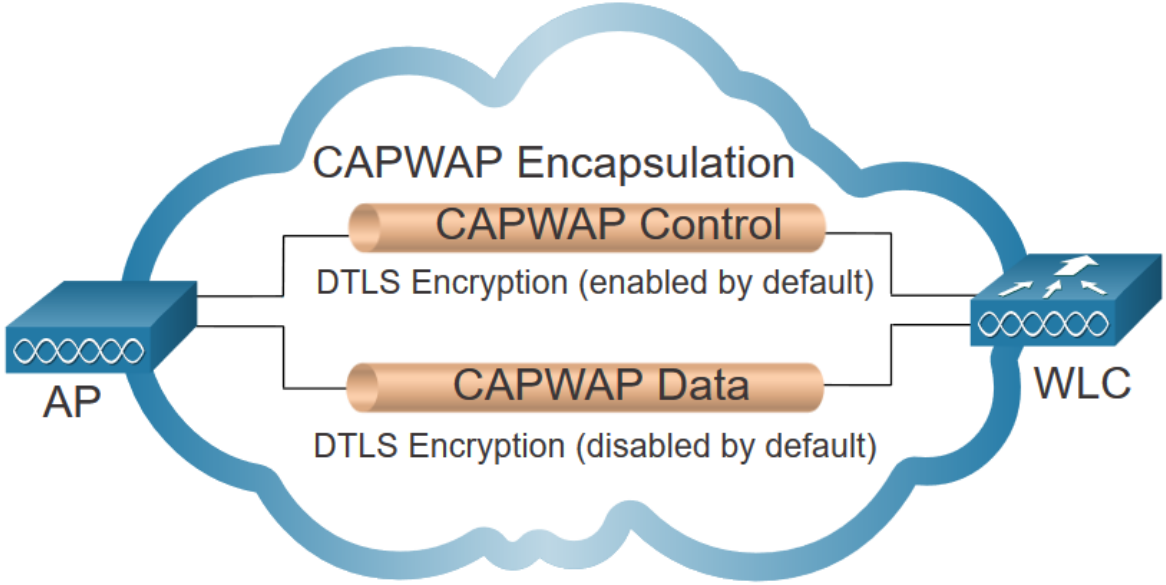
CAPWAP

- CAPWAP е IEEE стандартен протокол за управление на клиенти и няколко AP и WLANs.
- CAPWAP определя енкапсулацията между AP и устройствата.
- CAPWAP работи по UDP портове 5246 и 5247.
- CAPWAP пренася и IPv4 (по подразбиране) и IPv6.
- В хедъра на L2 в полето за IP при IPv4 пише 17, а при IPv6 - 136.



DTLS криптиране

- DTLS е криптиращ протокол за сигурност между AP и WLC.
- DTLS по подразбиране е включен за контролния канал CAPWAP, но за данновия канал е изключен и се включва опционално.



Компоненти

- **Крайни устройства (Клиенти)** – трябва да имат wireless NIC.
- **Точка за достъп (Access Points, AP)** – прилича на bridge – преобразува фрейма от wireless в wired фрейм и обратно. Те са свързани с кабелна връзка в мрежата.
- **Мрежова инфраструктура** – осигурява достъп до мрежовите ресурси за wireless клиенти.

WiFi-Ethernet -Разлики

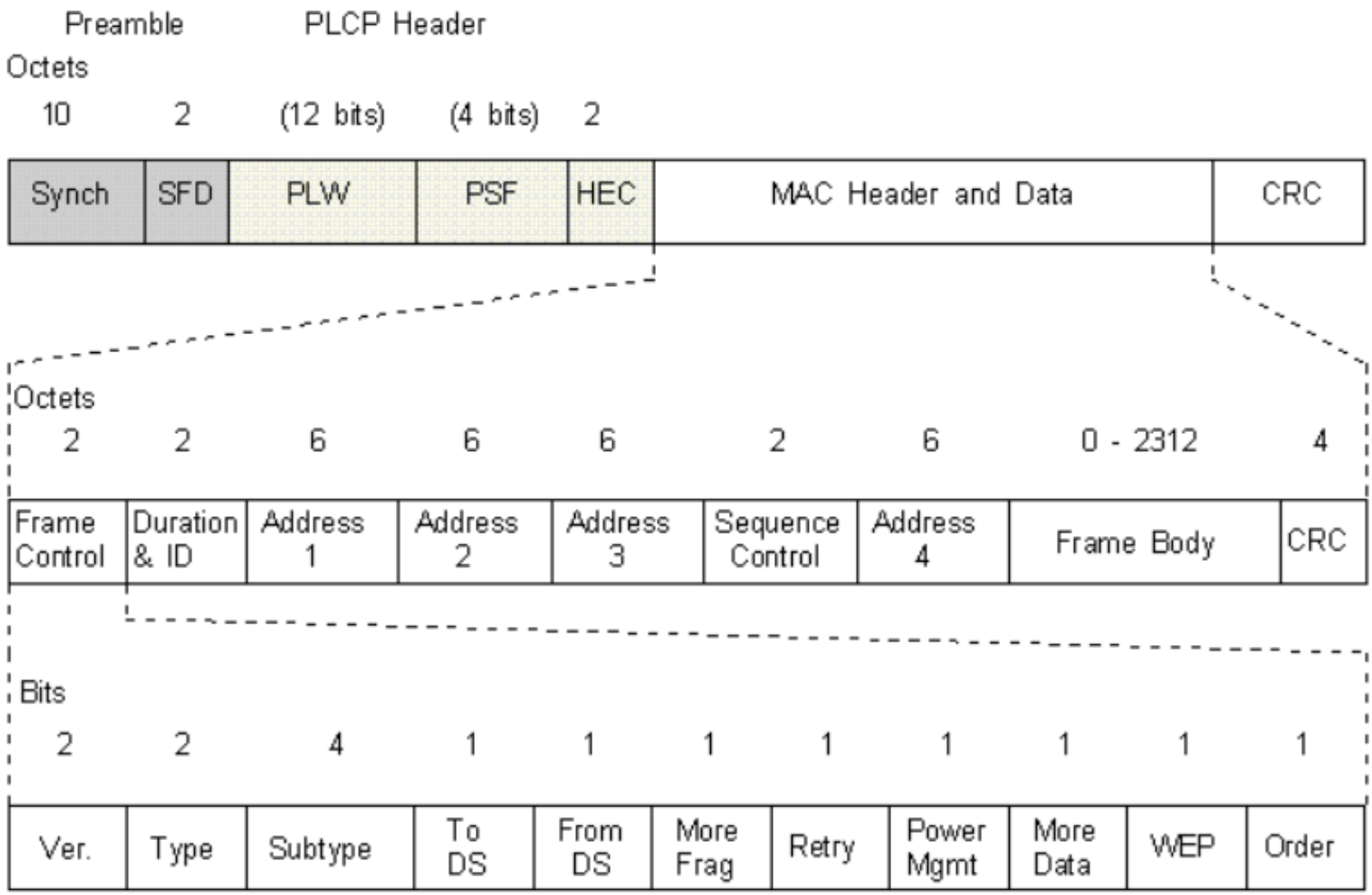
802.11	802.3
AP (работи като hub)	Hub, switch
Устройствата се захранват с батерии	Устройствата се захранват от ел.мрежа
Half duplex	full duplex
Има колизии	Има колизии
Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)	Carrier Sense Multiple Access with Collision Detect (CSMA/CD)
Сигурността е проблем, т.к. сигналите излизат извън помещението	Сигурността не е проблем

Безжичен маршрутизатор

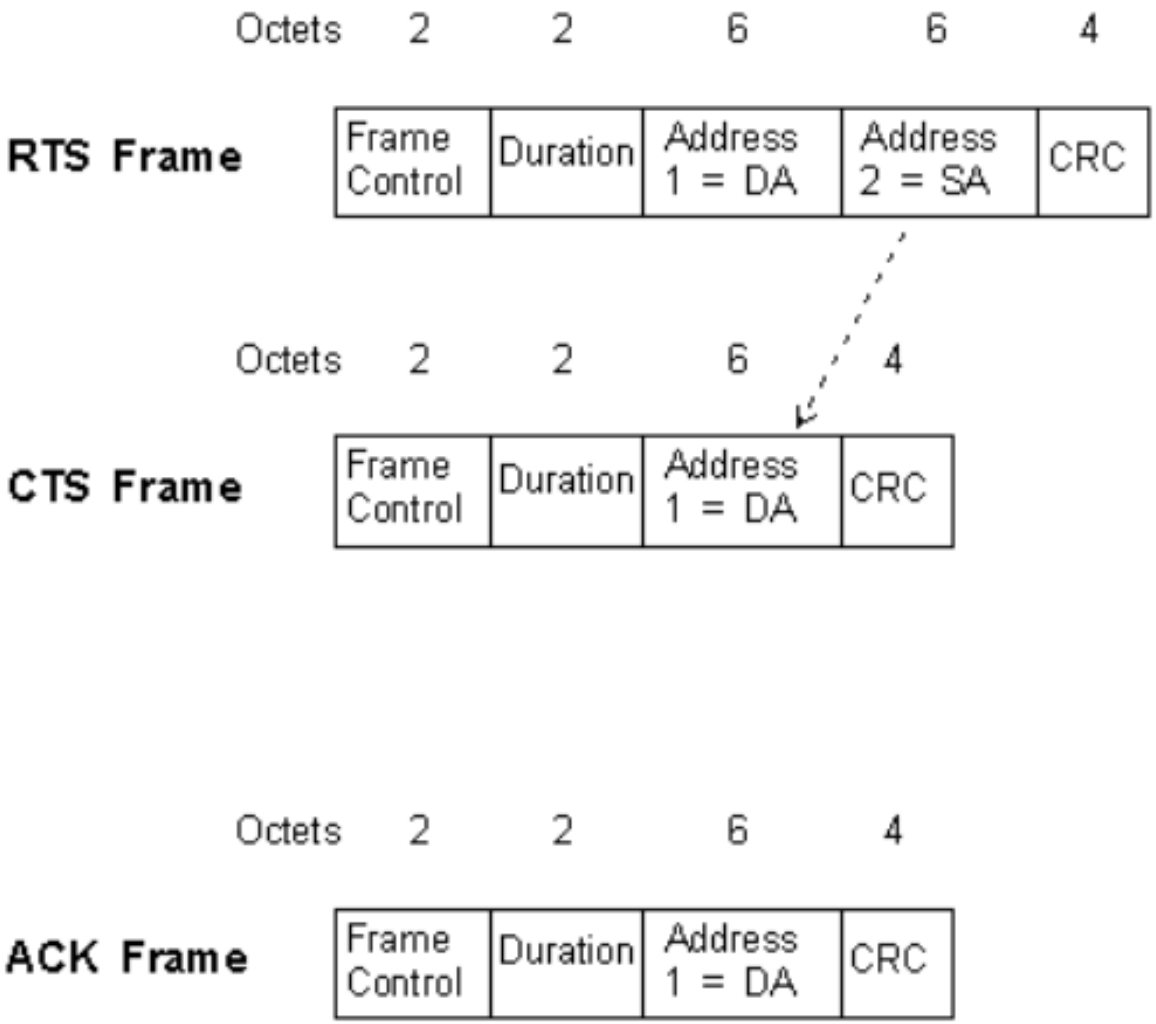
Безжичният маршрутизатор е интегрирано устройство, което може да функционира като :

- точка за достъп,
- Ethernet комутатор,
- маршрутизатор.

802.11 фрейм


Preamble
PLCP Header
Octets
10
2
(12 bits)
(4 bits)
2
Synch
SFD
PLW
PSF
HEC
MAC Header and Data
CRC
Octets
2
2
6
6
6
2
6
0 - 2312
4
Frame Control
Duration & ID
Address 1
Address 2
Address 3
Sequence Control
Address 4
Frame Body
CRC
Bits
2
2
4
1
1
1
1
1
1
1
1
Ver.
Type
Subtype
To DS
From DS
More Frag
Retry
Power Mgmt
More Data
WEP
Order

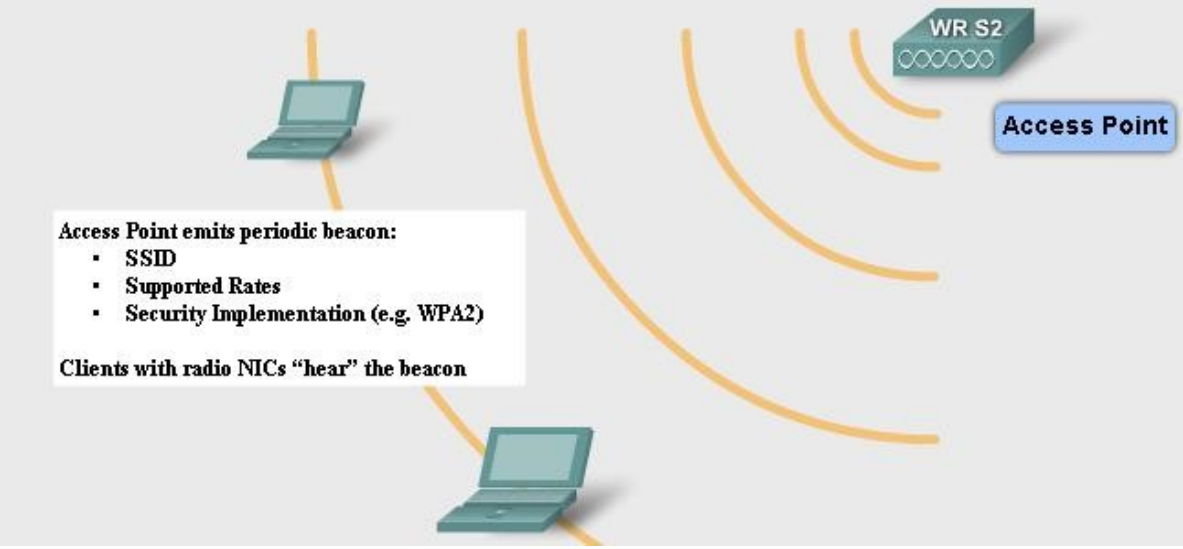
Контролни фреймове



Фреймове за управление

Предварителни:

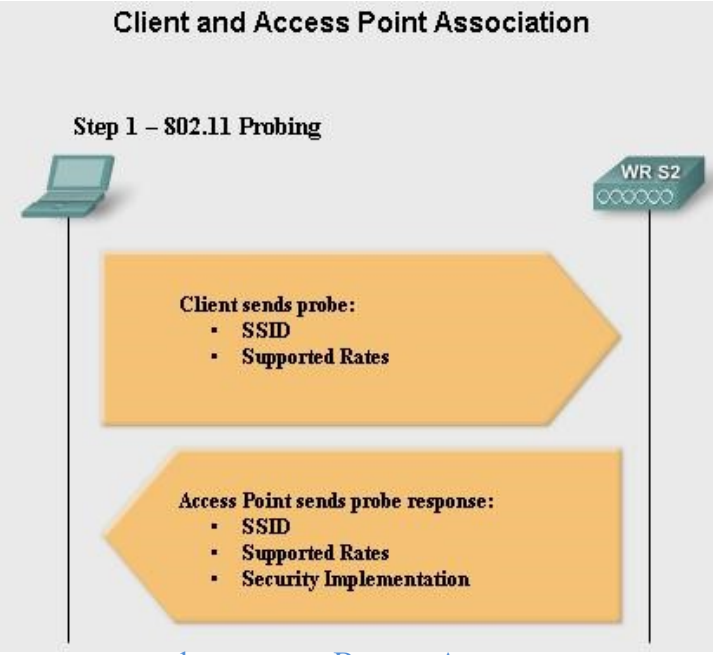
- **Beacon -** AP ги изпраща регулярно, за да се анонсира на близките устройства с SSID, timestamp и други параметри. Wireless NICs сканират всички канали за beacons, за да изберат с коя AP да се асоциират.



Фреймове за управление

Стъпка 1:

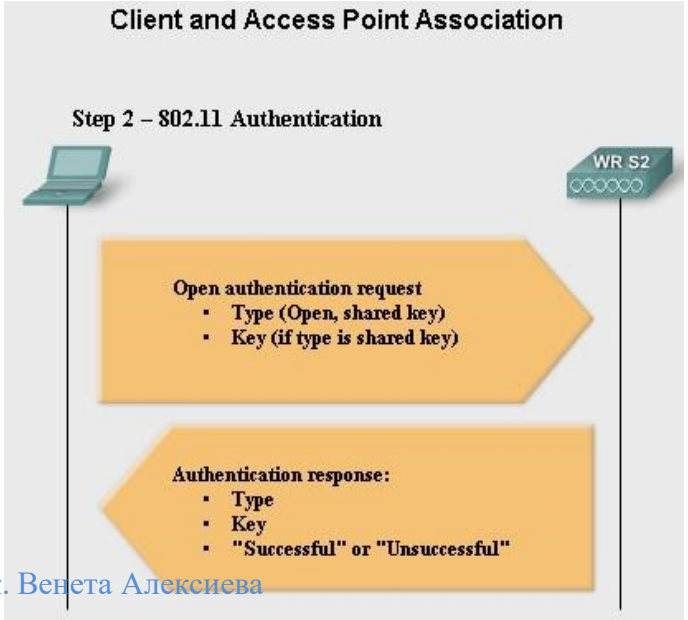
- **Probe Request** – изпраща се от станцията, за да се събере информация кои APs са в обхвата.
- **Probe Response-** Отговор на **Probe Request** с поддържани скорости и др.



Фреймове за управление

Стъпка 2а:

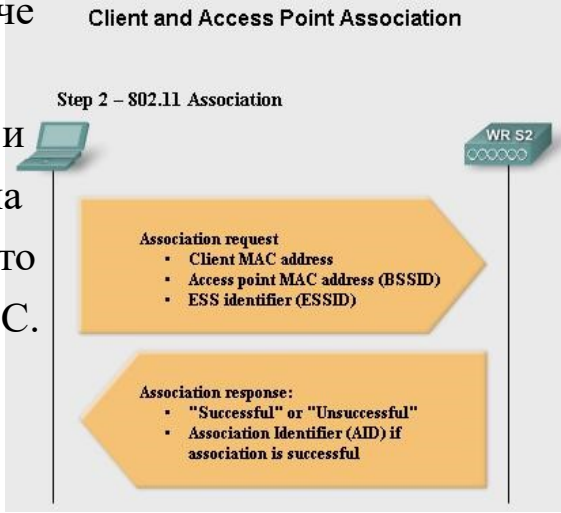
- **Authentication-** wireless NIC на станцията започва автентикация с AP, като се идентифицира.
  - По подразбиране е **Open Authentication** и NIC изпраща само authentication frame, а AP отговаря с acceptance/ rejection.
  - С **Shared Key Authentication -** NIC изпраща authentication frame, AP отговаря с challenge . NIC изпраща WEP криптирана версия на challenge на AP. AP я проверява чрез декриптиране и сравнение с оригиналния challenge. AP отговаря на NIC с acceptance/ rejection.
- **Deauthentication-** Една станция я изпраща на друга, ако желае да спре криптираната комуникация.



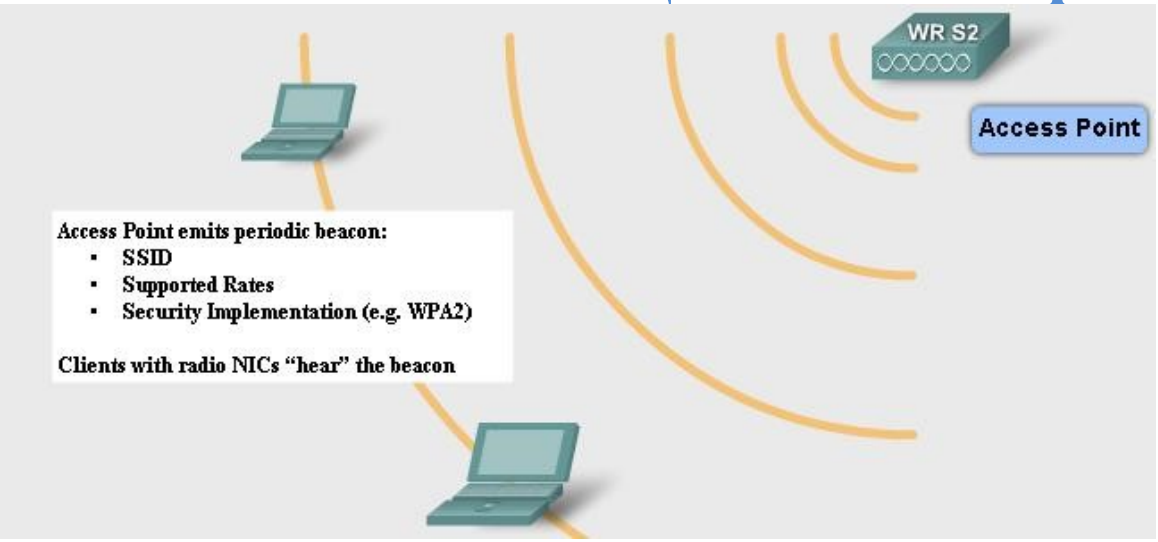
Фреймове за управление

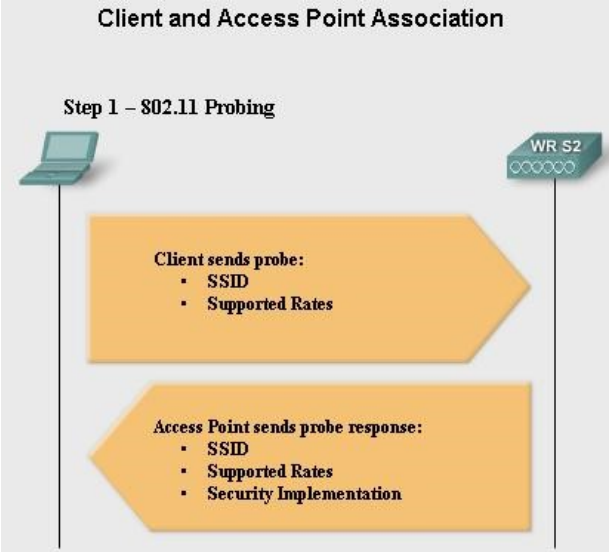
Стъпка 2б: Асоциацията с AP позволява заемане на ресурси и синхронизация с wireless NIC.

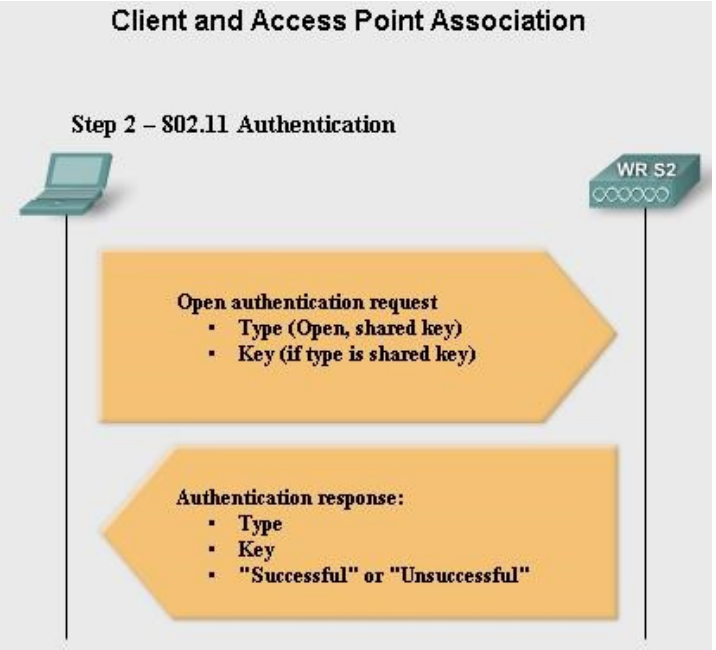
- **Association Request –**NIC я изпраща на AP и съдържа SSID, поддържани скорости, версия на **Cisco Compatible Extensions (CCX).** AP я получава, резервира ресурс за тази NIC и муу присвоява **Association ID**.
- **Association Response-** AP я изпраща на NIC с acceptance/ rejection. Ако е acceptance, се включва Association ID и поддържани скорости. NIC вече може да ползва мрежата през този AP.
- **Reassociation Request -**Ако NIC се мести и се разкача от текущия AP и търси друг AP с по-добър beacon сигнал, NIC изпраща Reassociation на новото AP. Новото AP координира препращането на фреймовете, които може да са буферирани в предното AP и да чакат да се предадат до NIC.
- **Reassociation Response-** AP я изпраща с acceptance/ rejection до NIC, който е изпратил **Reassociation Request**. Съдържа Association ID и поддържани скорости.
- **Disassociation –** Една станция я изпраща на друга ако иска да прекрати асоциацията с нея. Така AP ще изтрие NIC от таблицата си association table и ще освободи заетите от него ресурси. Например при изключване на PC, неговия NIC я праща, че ще се изключи.

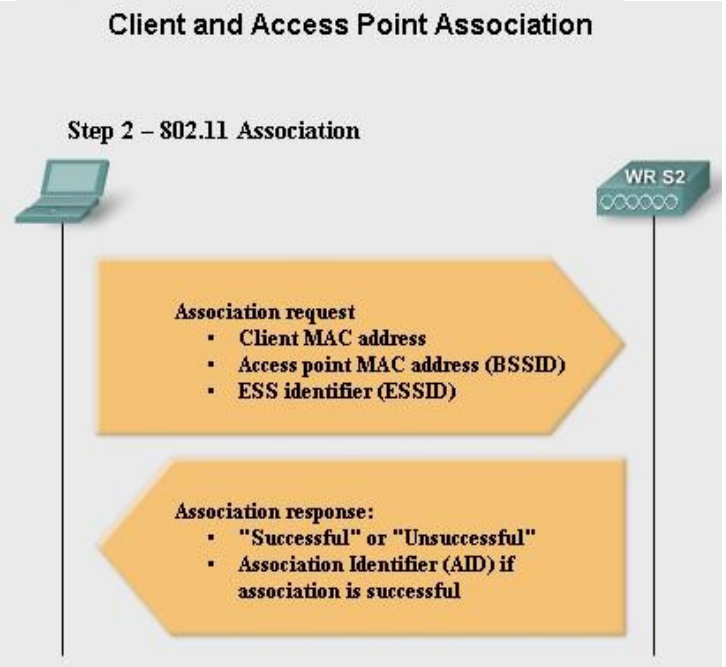


Целият процес

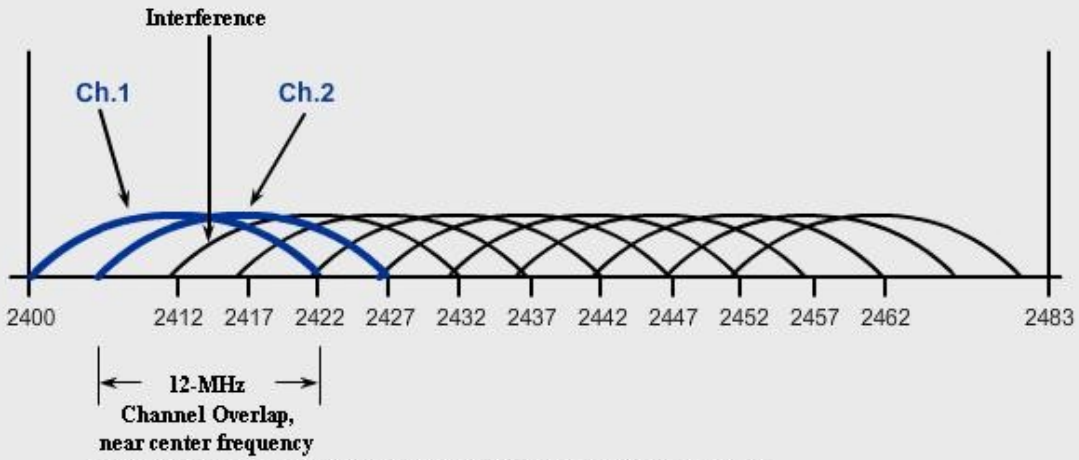




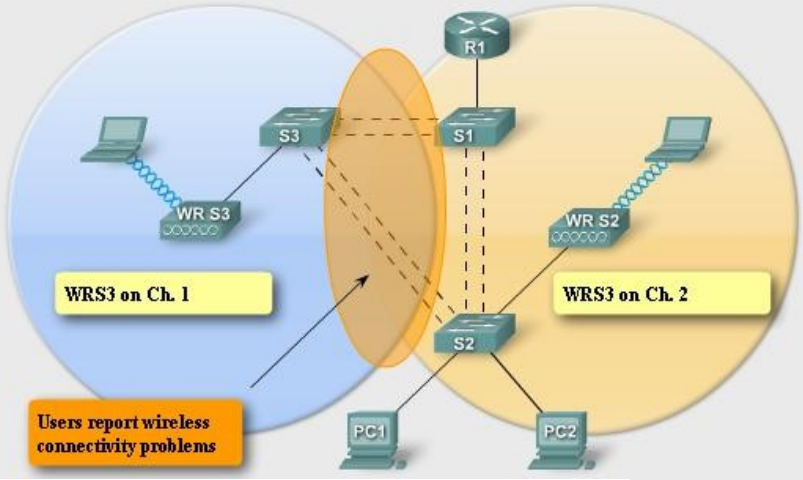




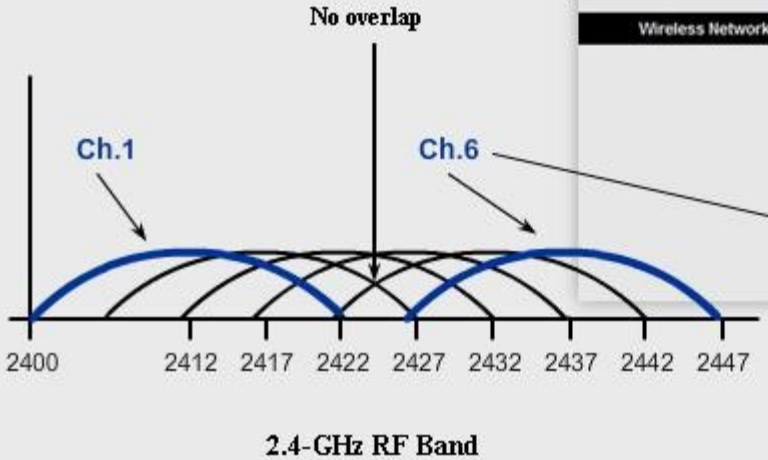
Resolve Issues of Incorrect Channel Settings



Resolve Issues of Incorrect Channel Settings



Resolve Issues of Incorrect Channel Settings



Reset access points to non-overlapping channels

Сигурност в WiFi комуникацията

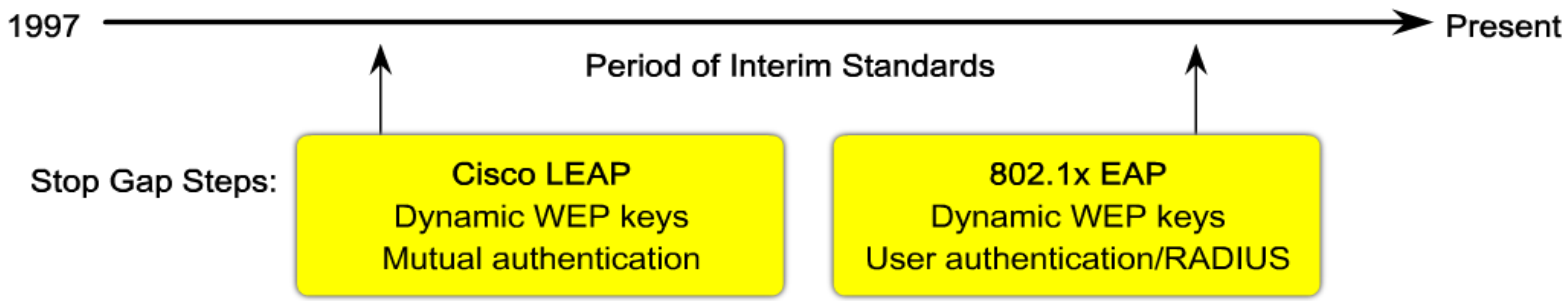
- **SSID прикриване** - точката за достъп не излъчва SSID за безжична мрежа
  - Може да се открие със снифер на комуникацията между точката за достъп и един от клиентите.
- **Филтриране по MAC адрес**
  - Може да се подправи MAC адреса при предаване на кадъра
- **Криптиране**
  - без криптиране и WEP са лесно достъпни. Предпочита се WPA и WPA2

Методи за криптиране в WiFi

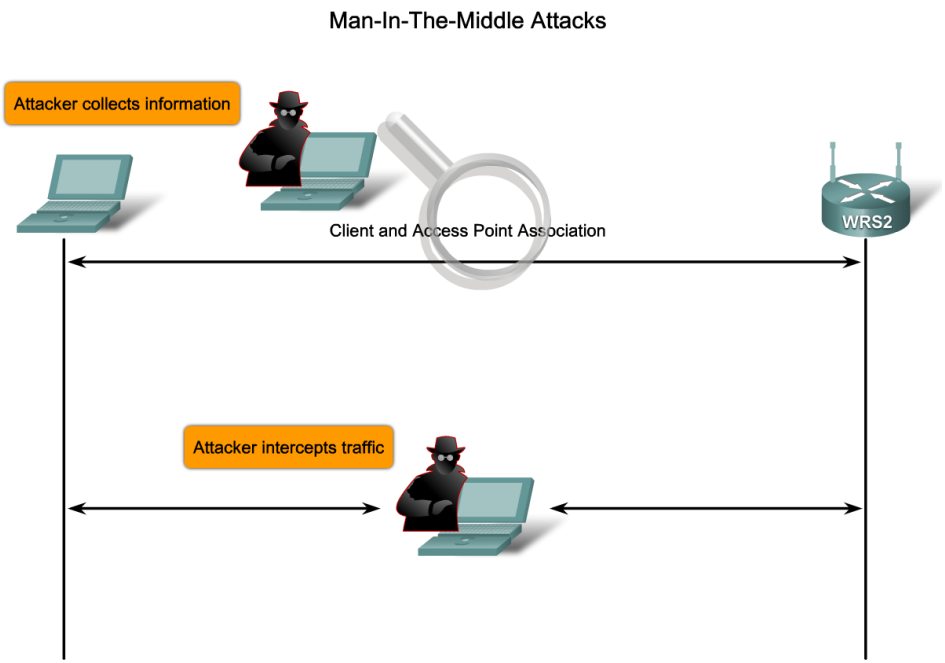
Wireless Protocol Overview

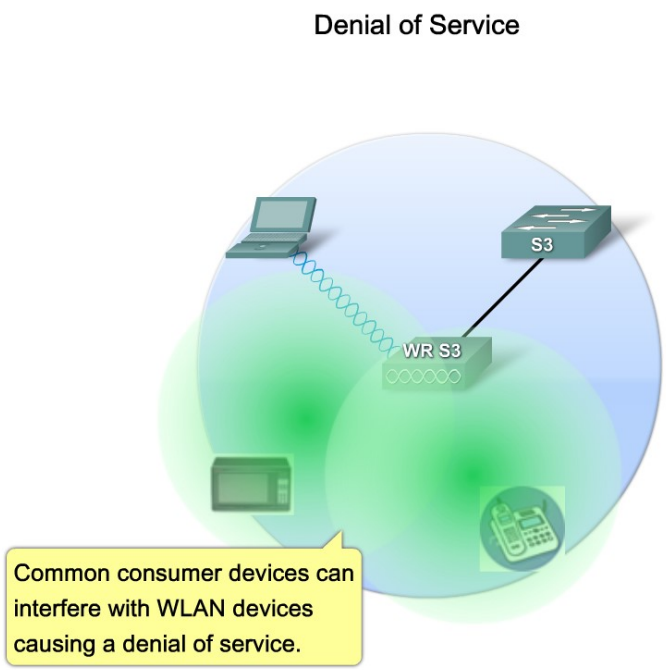
Major Stepping Stones to Secure WLAN

Open Access	First Generation Encryption	Interim	Present
SSID	WEP	WPA	802.11i/WPA2
• No encryption • Basic authentication • Not a security handle	• No strong authentication • Static, breakable keys • Not scalable	• Standardized • Improved encryption • Strong, user-based authentication (e.g., LEAP, PEAP, EAP-FAST)	• AES Encryption • Authentication: 802.1X • Dynamic key management • WPA2 is the Wi-Fi Alliance implementation of 802.11i



WiFi проблеми



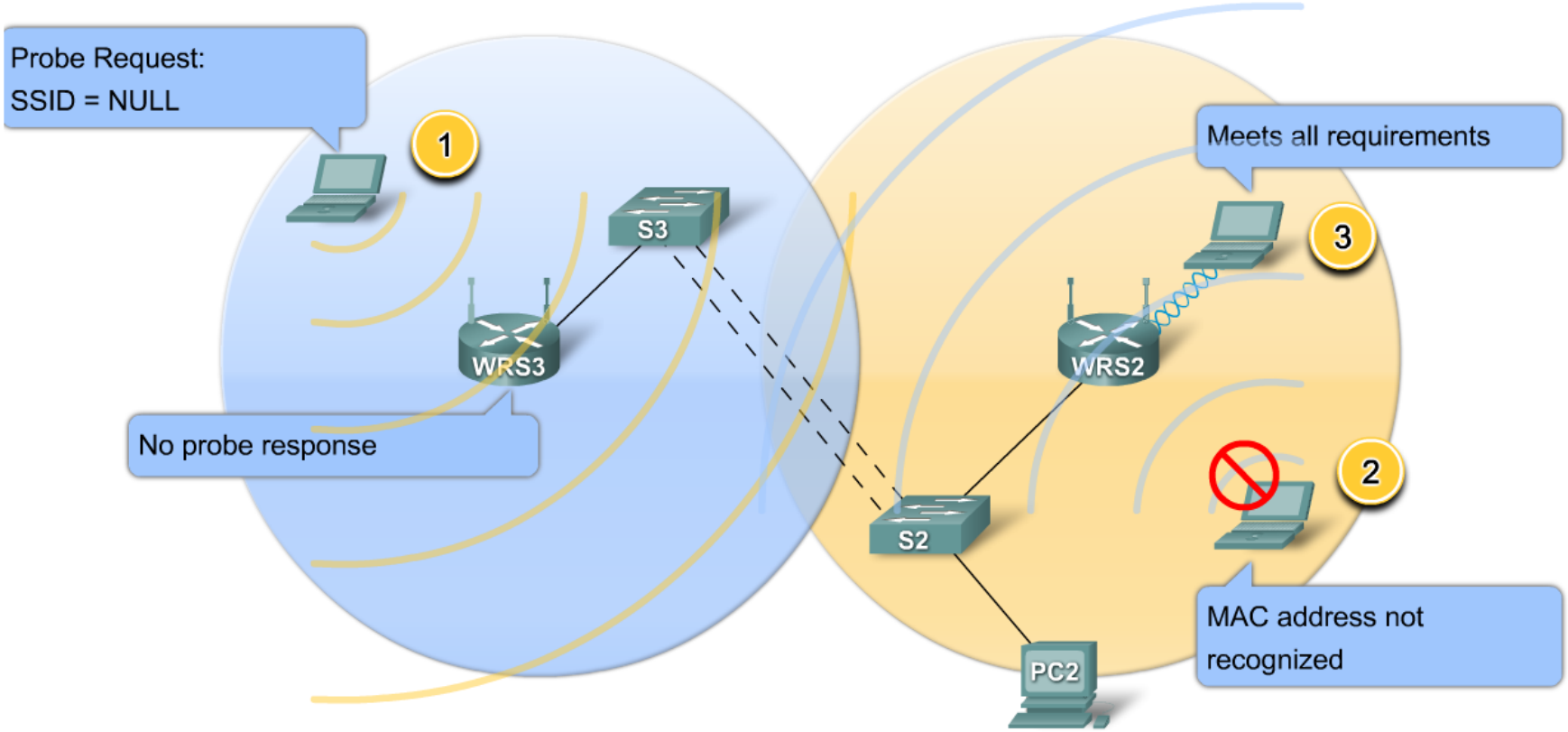


Неоторизиран достъп до мрежата:

- Потребители търсят “open”мрежи и ги използват
- Хакерите използват слабите мерки за сигурност
- Служителите на компанията слагат своя AP в Ethernet порта, който им е предоставен, за да ползват своя безжична мрежа

WiFi проблеми

Controlling Access to the Wireless LAN

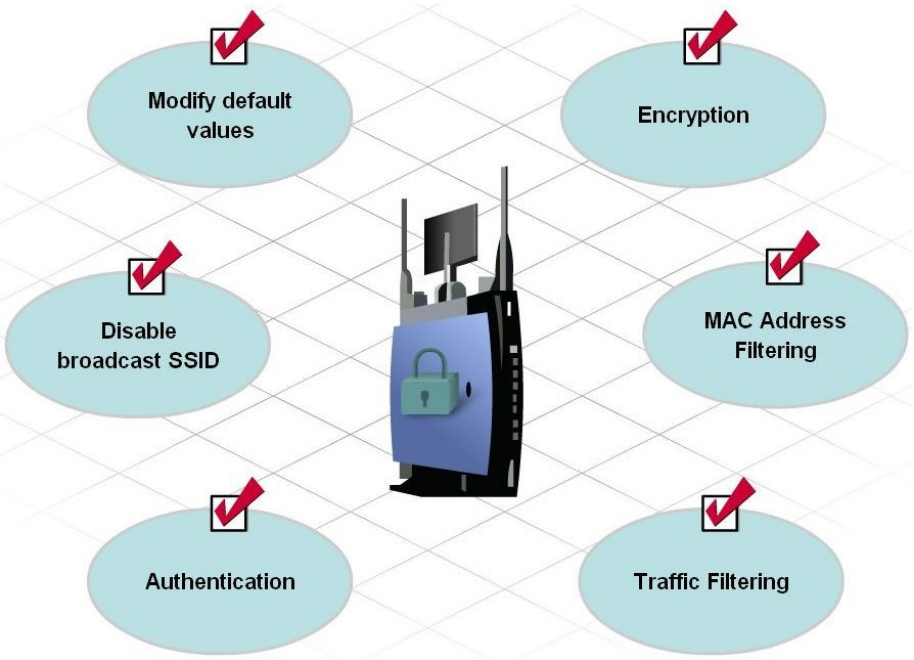


Methods for controlling wireless LAN access:

1. SSID broadcasts from access points are off
2. MAC Address filtering is enabled
3. WPA2 Security implemented

CAUTION: Neither items 1 or 2 are considered valid security measures

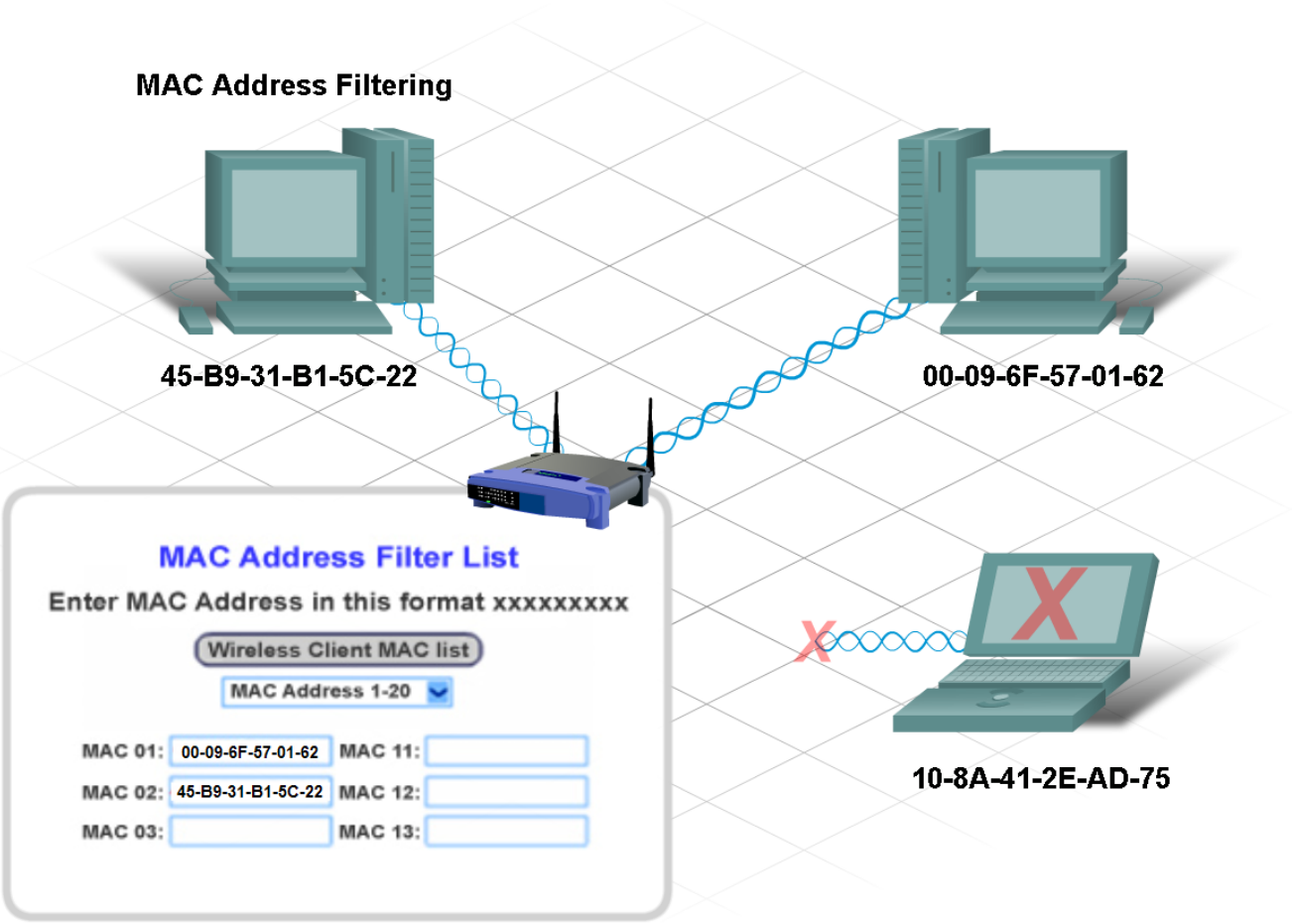
Инсталиране на AP



Стъпки:

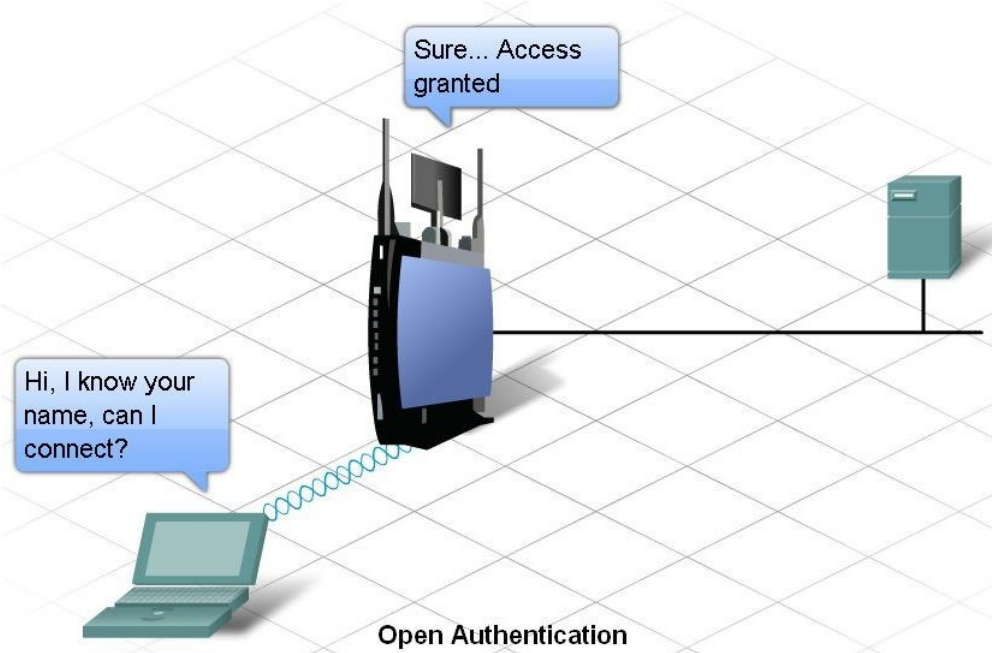
1. Проверява се в кабелната LAN мрежа достъп до Интернет и наличие на DHCP
2. Инсталира се AP
3. Конфигурира се AP – SSID без приложена сигурност
4. Инсталира се един WiFi клиент без приложена сигурност
5. Проверява се връзка има ли между тях
6. Конфигурира се криптиращ протокол – WPA2 или PSK
7. Отново се проверява връзка има ли между тях
8. Добавят се правила за филтриране по MAC
9. Добавят се правила за филтриране на трафика
10. Добавя се автентикация
11. Забранява се SSID разпространение
12. Модифицират се стойностите по подразбиране

Филтриране по MAC



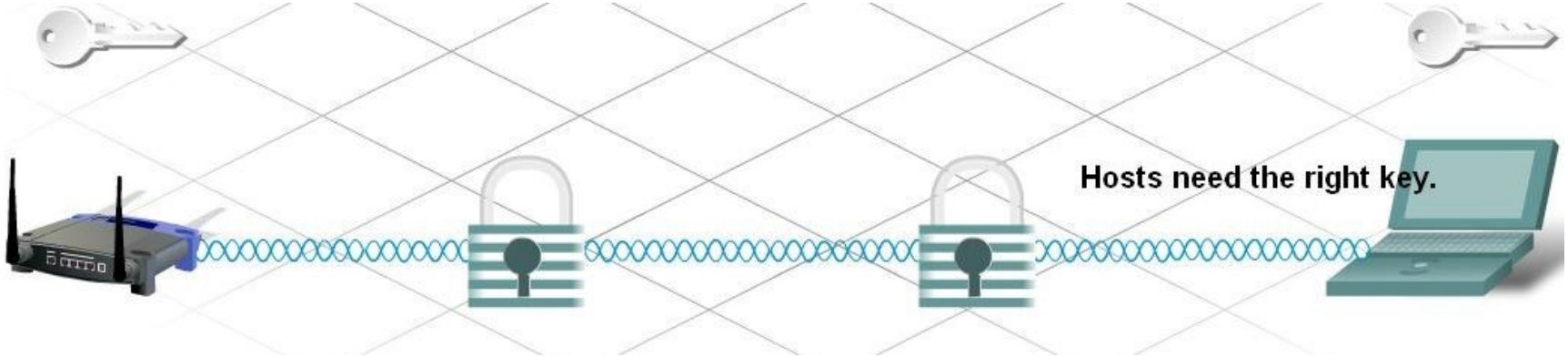
Автентикация

- Това е процес на разрешаване за влизане в мрежа въз основа на набор от удостоверения (credentials).
- Режими:
  - Без автентикация (Open Authentication)
  - Предварително споделени ключове (PSK)
  - Extensible Authentication Protocol (EAP)



Криптиране

- Това е процес на преобразуване на данните, така че дори и да се прихванат, те са неизползваеми.
- Протоколи:
  - Wired Equivalency Protocol (WEP) - използва предварително конфигурирани ключове за криптиране и декриптиране на данни.
  - Wi-Fi Protected Access (WPA) - WPA също използва криптиращи ключове от 64 бита до 256 бита, но WPA, за разлика от WEP, генерира нови, динамични ключове всеки път, когато клиентът установява връзка с AP.



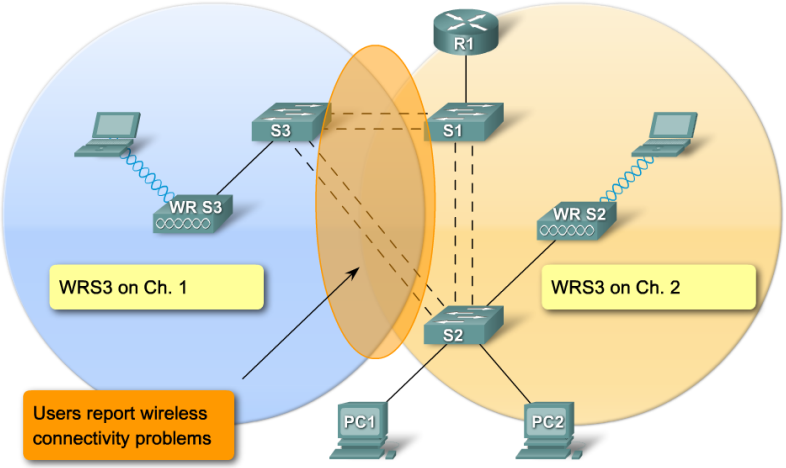
Филтриране на трафика

- Блокира нежелания входящ и изходящ трафик в безжичната мрежа.
- Освобождава честотна лента за полезен трафик и подобрява работата на WLAN.
- Осъществява се по определен MAC или IP адрес на сорса или дестинацията.
- Може да се забранят номера на портове за някои приложения.

Неправилно настройване на каналите

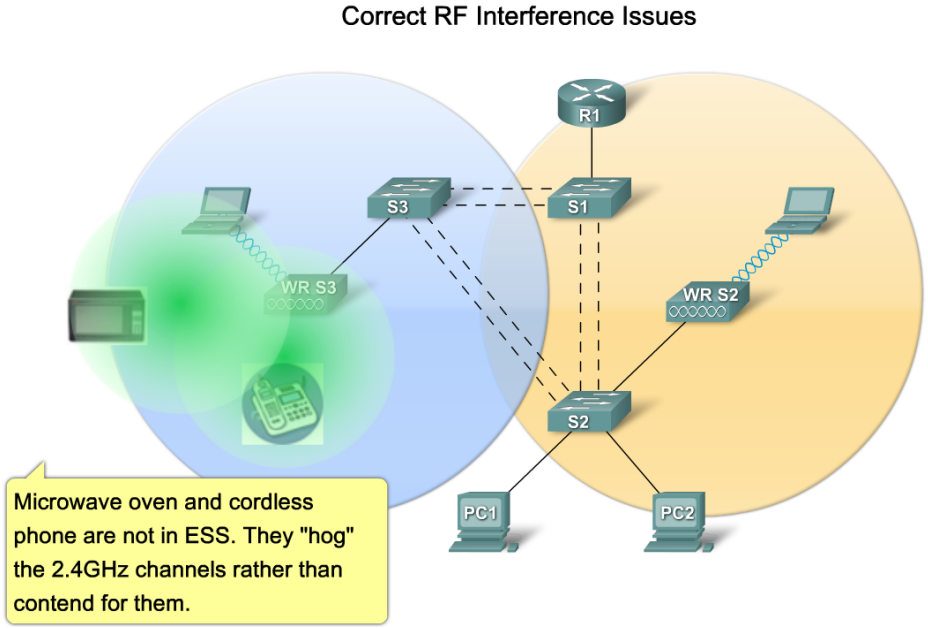
- Повечето безжични мрежи днес работят в честотната лента от 2,4 GHz, която може да има най-много 14 канала, всеки, заемащ 22MHz от честотната лента.
- Интерференция може да се случи, когато има припокриване на канали, затова каналите трябва да са на интервали от пет канала- канал 1, канал 6, и канал 11 за 802.11b/g/n на 2,4GHz и канал 36, канал 48, и канал 60 за 802.11a/n/ac на 5GHz.

Resolve Issues of Incorrect Channel Settings



Проблеми с RF интерференция

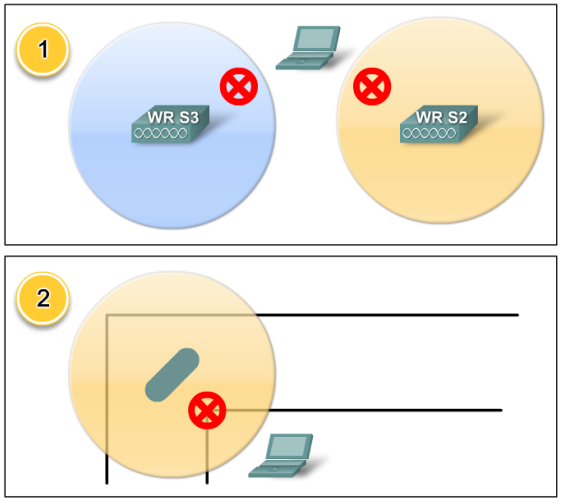
- Влияние от микровълнови печки, безжични телефони или бебефони, други AP и потенциални клиенти
- Повечето устройства работят на канал 6. Трябва да се настрои на 1 или 11 канал.



Неправилно разполагане на АР

- Разстоянието между точките за достъп е твърде далеч, за да се припокриват.
  - на минимум 10 до 15% припокриване,
- Ориентацията на антените на АР в коридорите и ъгли намалява покритието.
  - вертикално близо до тавана в центъра на всяка зона на покритие, ако е възможно
  - АР да не са монтирани по-близо от 20 см от тялото на всички лица.
  - АР да не са в близост от поне 91,4 см от метални прегради.
  - АР да са далеч от микровълнови печки
  - АР да се монтират вертикално
  - АР да не се монтиат на външни стени
  - При монтаж на точка за достъп в ъгъла на коридора да се монтират под ъгъл от 45 градуса спрямо двата коридора

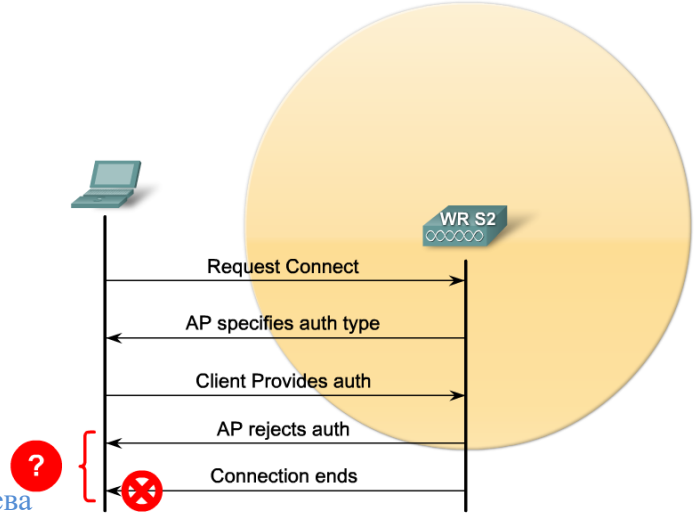
Identify Problems with Access Point Misplacement



Проблеми с WLAN автентикация и криптиране

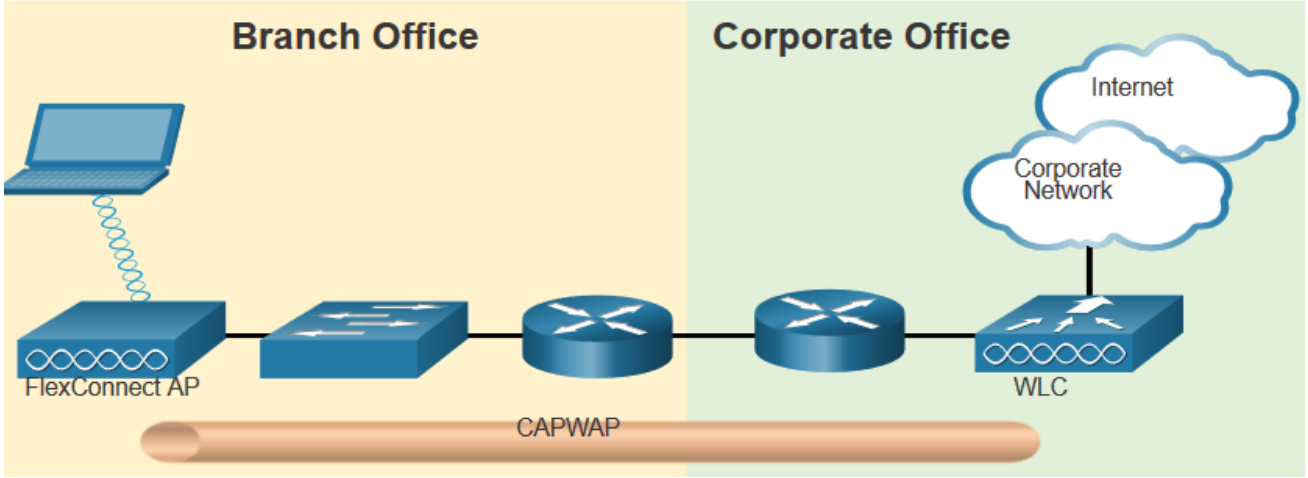
- Ако AP очаква един вид криптиране, а клиентът предлага различен тип, процесът на удостоверяване е неуспешен.
- Всички устройства, свързващи се към AP, трябва да използват един и същ вид сигурност, като тази, конфигурирана на AP.

Resolve Problems with Wireless LAN Encryption and Authentication



FlexConnect AP

- FlexConnect е безжично решение за връзка на отдалечени офиси.
- Той позволява да се конфигурират и контролират AP по WAN връзка, без да има контролер във всеки офис.
- Connected mode - FlexConnect AP по CAPWAP се свързва с WLC , като WLC управлява CAPWAP.
- Standalone mode- WLC е недостъпен. FlexConnect може локално без WLC да превключва трафик на клиентски данни и да автентицира клиенти.



Въпроси ?

Благодаря за вниманието !