Безжични локални мрежи.WiFi

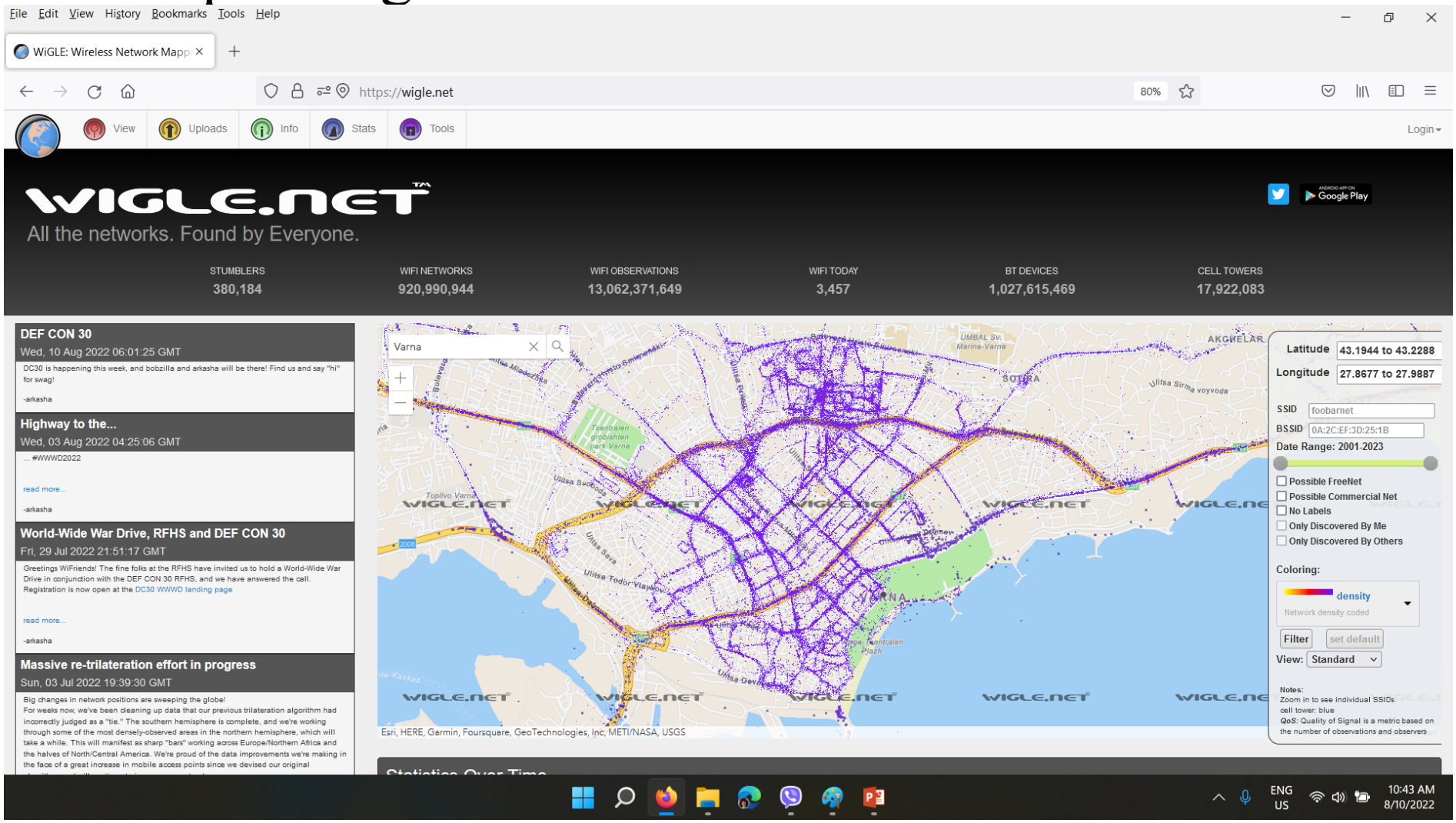
проф. д-р инж. Венета Алексиева

Основни моменти

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

Карта на WiFi мрежи по света

- https://wigle.net/



Картографиране с War driving

- Представлява търсене на Wi-Fi безжични мрежи от човек, обикновено в движещо се превозно средство, използващ лаптоп или смартфон.
- Софтуерът за wardriving е свободно достъпен в Интернет:
  - **За Linux :** Kismet; Swscanner
  - **За MAC :** KisMAC; MacStumbler
  - **За iPhone :** WiFi-Where
  - **За Windows :** NetStumbler; Insider; Ekahau HeatMapper
  - **За Android :** G-MoN; Wardrive
- Warbiking или warcycling е подобен на wardriving, но се прави от движещ се велосипед или мотоциклет.

История

- 1970г. в Университета на Хавай Норман Абрамсон осъществява първата компютърна безжична мрежа ALOHAnet.
- 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

HiperLAN 1

Характеристики:

- Обхват до 50 m
- Слаба мобилност - 1.4 m/s
- Поддържа асинхронен и синхронен трафик
- Скорост- 23.2 Mbit/s
- Честоти - 5 GHz
- Една иновативна функция на HIPERLAN 1, които други безжични мрежи не предлагат, е способността му да предаде пакети данни, с помощта на няколко relays, които удължават комуникацията на MAC слой извън радио обхвата.
- За съхраняване на енергията един възел използва специален модел за “събуждане”:
  - определя по кое време възелът е готов да получи съобщение, а в останалото време да изключи приемника си за икономия на енергия.
  - Тези възли се наричат p-savers и се нуждаят от p-supporters, които съдържат информация за моделите на събуждане на всички p-savers
  - p-supporter изпраща данни до p-saver само в момент, в който p-saver е буден. Това действие изисква механизми за буфериране на пакети.

HiperLAN/2

- През 2000г се появява версия 2: HiperLAN/2

Характеристики:

- Скорост- 54 Mbit/s
- Честоти - 5 GHz
- Физическият слой е същия като на IEEE 802.11a
- Media access control е Dynamic TDMA докато в IEEE 802.11a е CSMA/CA.
- Пренася данни, глас и видео
- Предлага сигурно предаване с DES или Triple DES
- Изисква автентикация на устройствата
- Производители на HiperLAN/2 са : Alvarion (Israel), Freescale (USA), Panasonic (Japan).
- **Но появата на IEEE 802.11, който е по-прост за имплементиране, го изхвърля от пазара.**

Стандарти

- IEEE 802.11 (a,b,g,n)
- EN300652, ETS300836
- Wi-Fi Alliance
  - Тества WLAN устройства на различни производители
  - Wi-Fi лого на устройството гарантира, че то отговаря на стандарта и е съвместимо с други устройства, отговарящи на стандарта

Стандарти 802.11-преди

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
802.11n (WiFi 4)	2009	2.4 GHz / 5 GHz	20, 40 MHz	130 Mbit/s	300 Mbit/s	~70 метра	~250 метра
802.11ac (WiFi 5)	2012	5 GHz	20, 40, 80, 160 MHz	87,6 Mbit/s	866,7 Mbit/s	-	-

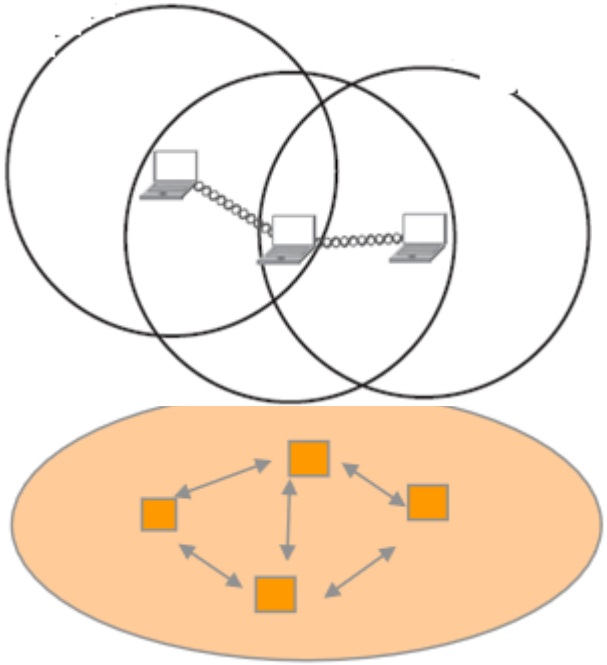
Стандарти 802.11-сега

Версия	Дата	Работна честота	Bandwidth	Скорост	Максимална скорост	Обхват в помещение	Обхват навън
802.11ad	Дек. 2012 г.	60 GHz		6,7 Gbps		на 3,3 метра	на 3,3 метра
802.11ah (Wi-Fi HaLow)	май 2017	900MHz		до 347Mbps	За IoT с ниска консумация		
802.11aj	Април 2018	45GHz/ 60GHz	За съвместимост с 802.11ad				
802.11ax (Wi-Fi 6)	февруари 2021 г.	2.4 GHz / 5 GHz	С висока плътност			30 метра	120 метра
802.11ay	2021г.	60GHz	4 канала по 8.64 GHz	Up to 20Gbps		10 метра	100 метра
802.11ba	Октомври 2021	2.4GHz / 5GHz	4.06MHz	62.5Kbps 250 Kbps			
802.11bb	Юли 2022	60 GHz/ 79GHz					

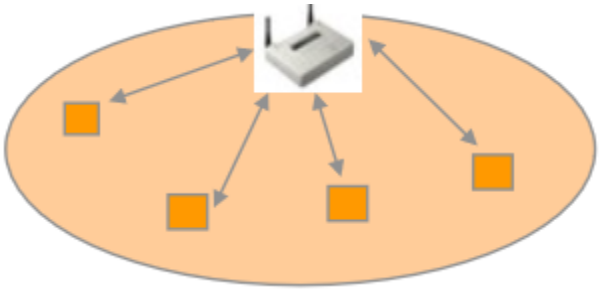
И още стандарти за Wi-Fi

- 802.11ak
  - За комбинирана мрежа 802.11 с 802.3 Ethernet. От ноември 2017 г. е в проект, публикуван е март 2018г.
- 802.11az - позициониране от следващо поколение (NGP)
  - стартира през януари 2015 г. Със създадена проучвателна група, която да разработи „станция за идентифициране на нейната абсолютна и относителна позиция към друга станция или станции, която е или асоциирана или несвързана с нея“. Планиран е за одобрение за март 2021 година.
- 802.11ba - “Wake-Up Radio” (WUR)
  - нова технология, насочена към удължаване на живота на батерията на устройства и сензори в мрежата на IoT. Целта на WUR е да "намали значително нуждата от често презареждане и подмяна на батерии, като същевременно поддържа оптимална производителност на устройството."

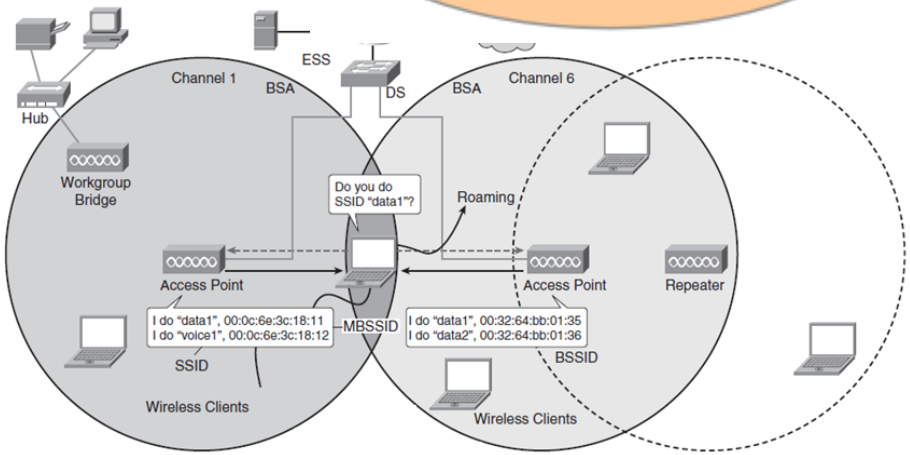
Топологии



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



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



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

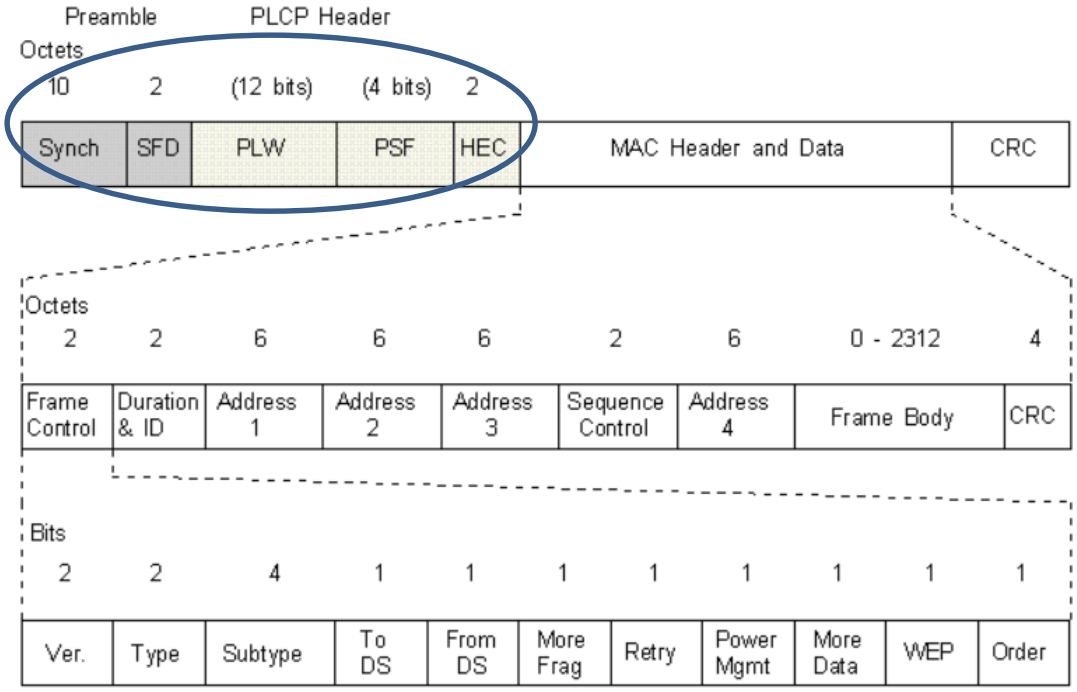
802.11	802.3
AP (работи като hub)	Hub, switch
Устройствата се захранват с батерии	Устройствата се захранват от ел.мрежа
Half duplex	full duplex
Има колизии	Има колизии
Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)	Carrier Sense Multiple Access with Collision Detect (CSMA/CD)
Сигурността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

Безжичен маршрутизатор

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

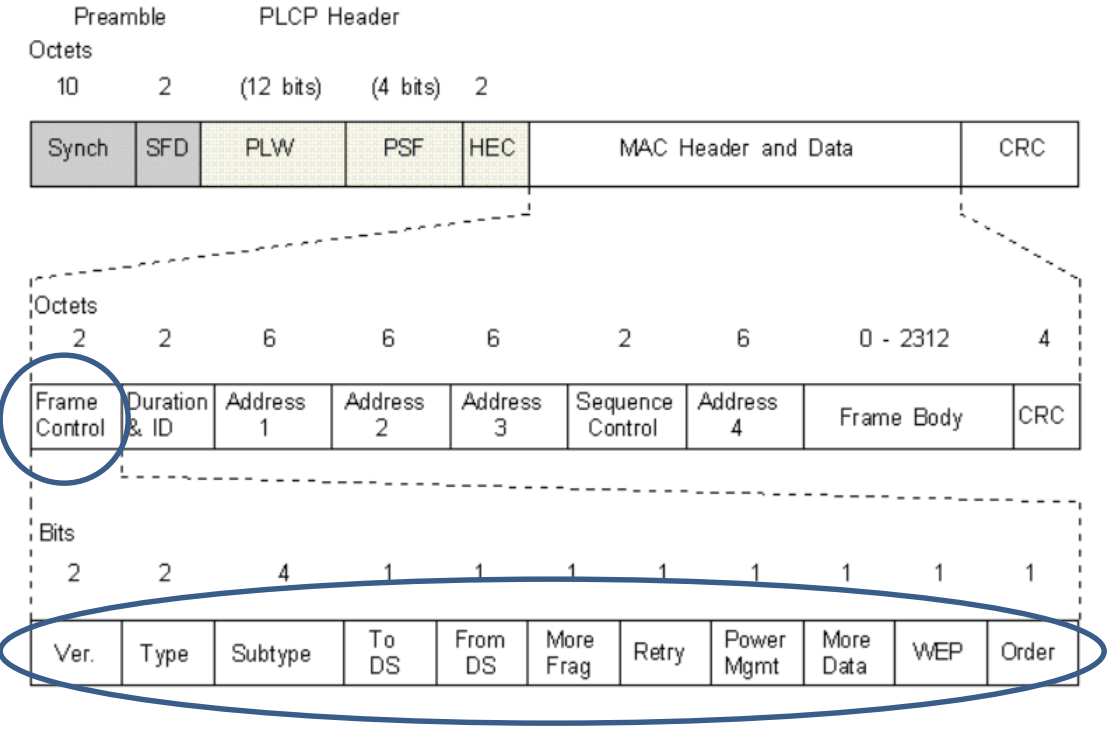
- точка за достъп,
- Ethernet комутатор,
- маршрутизатор.

802.11 фрейм



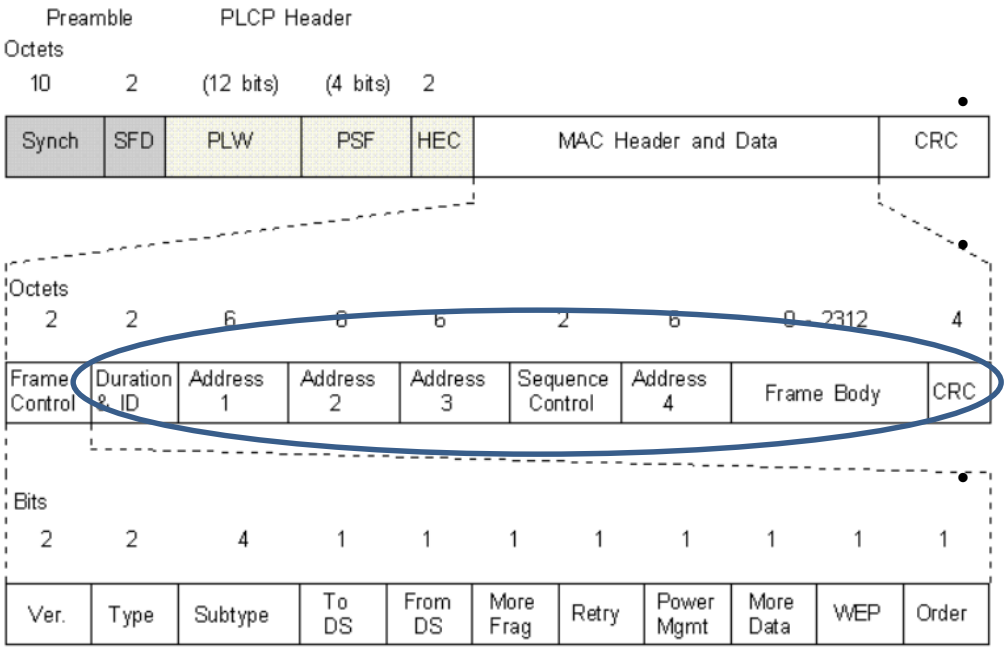
- **Synch** - 80 bits, но за DSSS PHY е 128 bits поредица от 101010…10
- **SFD -Start Frame Delimiter** - 16 bits- **0000 1100 1011 1101**
- **PLW - PLCP_PDU Length Word** -12 bits, дължина на пакета – винаги се предава със скорост 1MBps
- **PSF - PLCP Signalling Field** - 4 bits за скоростта на предаване на MAC частта. Bit 0 е винаги '0'. **000** - 1.0Mbps; **001** - 1.5Mbps; **010** - 2.0Mbps; **011** - 2.5Mbps; **100** - 3.0Mbps; **101** - 3.5Mbps; **110** - 4.0Mbps; **111** - 4.5Mbps
- **HEC - Header Error Check** -16 bit

802.11 фрейм



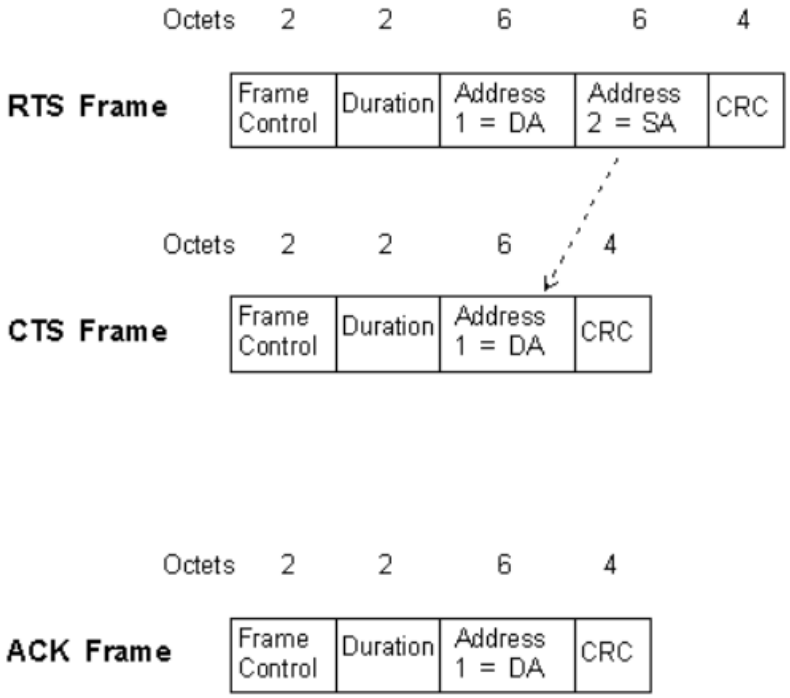
- **Frame Control** –
  - **Ver** – винаги **0**
  - **Type** - дали е **Management**, **Control** или **Data** фрейм.
  - **Subtype** – 4 bits за детайли на подтипа
  - **To DS** - to the Distribution System
  - **From DS** - from the Distribution System
  - **More Frag** – ако е фрагмент от по-голям фрейм
  - **Retry** – ако е препредаден фрейма
  - **Power Mgmt** – режимът дали е 'save‘ или 'active‘
  - **More Data** – от AP дали се пращат повече от 1 фрейм до тази дестинация , за да се буферират по време на ‘save’ режим и да се премине към 'active'.
  - **WEP** – ако се ползва WEP криптиране на тялото
  - **Order** – ако фреймът е изпратен по време на 'Strictly Ordered Class’

802.11 фрейм



- **Duration & ID** - В енергоспестяващото съобщение е ID на станцията, докато във всички други фреймове това е продължителността (обикновено 0)
- **Address 1** - адреса на получателя станция на BSS. Ако **To DS** е настроен, това е адреса на AP; ако **From DS** е настроен, това е адреса на станцията
- **Address 2** – Адресът на предаващата станция по BSS. Ако **To DS** е настроен, това е адреса на AP; ако **From DS** е настроен, това е адреса на станцията
- **Address 3** - Ако **Address 1** съдържа адреса на получателя след **Address 3** ще съдържа адреса на източника, ако **Address 2** съдържа адреса на източника **Address 3** ще съдържа адреса на получателя.
- **Address 4** – Ако **Wireless Distribution System (WDS)** се използва (с AP към AP комуникация), **Address 1** ще съдържа адреса на получаващото AP; **Address 2** – на предаващото AP; **Address 3** – дестинационния адрес и **Address 4** – сорсовия адрес.
- **Sequence Control** – съдържа **Fragment Number** и **Sequence Number** които посочват главния фрейм и номера на фрагмента от фрейма
- **Frame Body** – данните, т.е. IP пакета с размер до 2312B
- **CRC** - 32-bit Cyclic Redundancy Check за целия фрейм.

Контролни фреймове

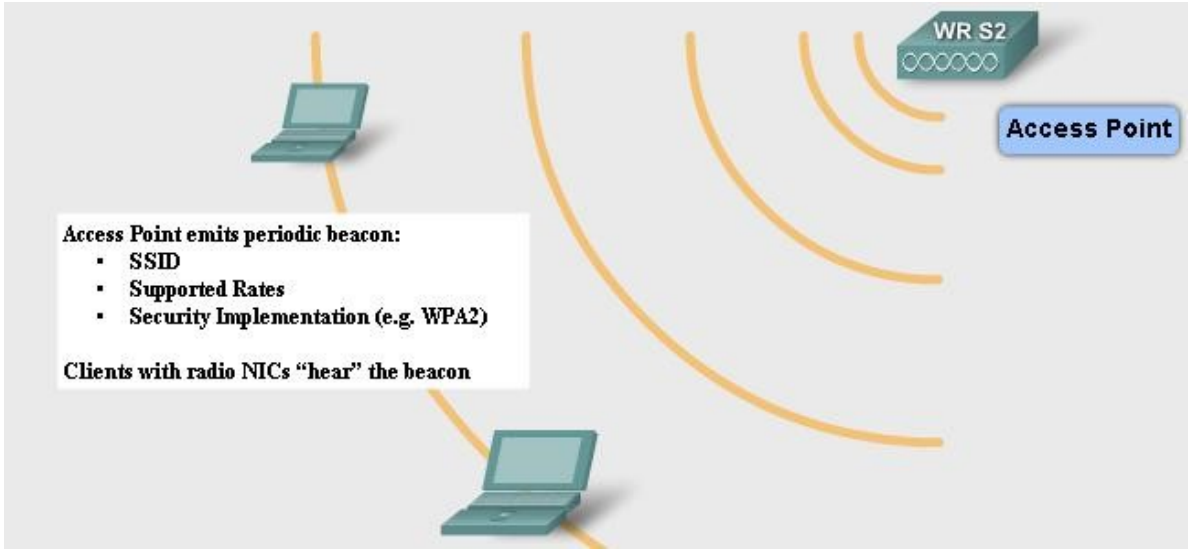


- **RTS Frame-** Destination Address (DA), Source Address (SA), Duration- в микросекунди – колко време следващия фрейм ще се предава + времето за CTS frame, ACK frame и три SIFSs (по един за RTS Frame, CTS frame и final ACK frame).
- **CTS Frame** - Destination Address се взема от Source Address на предходния RTS Frame, duration – намалява се с времето за CTS frame и неговия SIFS.
- **ACK Frame** - Destination Address се взема от Source Address на предния фрейм (RTS или друг), duration се намалява от предходния фрейм с времето за ACK frame и неговия SIFS. Ако в полето **More Frag=‘1’,** duration ='0'.

Фреймове за управление

Предварителни:

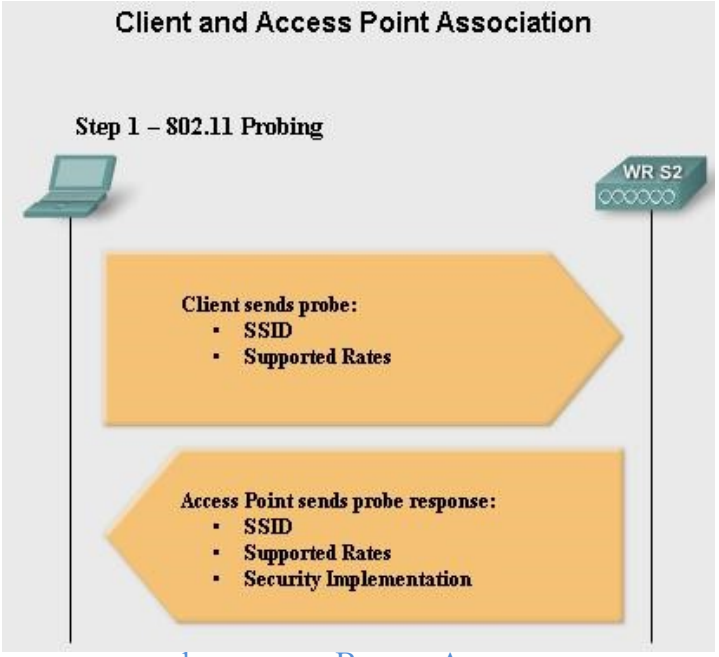
- **Beacon -** AP ги изпраща регулярно, за да се анонсира на близките устройства с SSID, timestamp и други параметри. Wireless NICs сканират всички канали за beacons, за да изберат с коя AP да се асоциират.



Фреймове за управление

Стъпка 1:

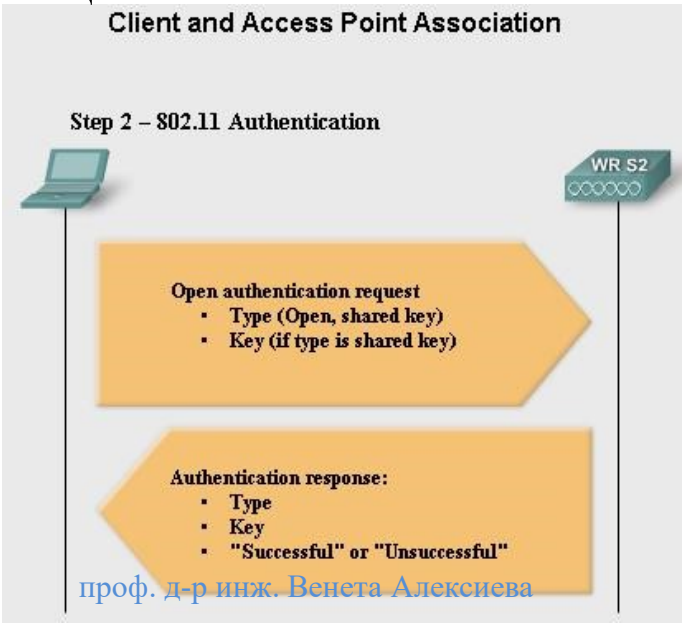
- **Probe Request** – изпраща се от станцията, за да се събере информация кои APs са в обхвата.
- **Probe Response-** Отговор на **Probe Request** с поддържани скорости и др.



Фреймове за управление

Стъпка 2а:

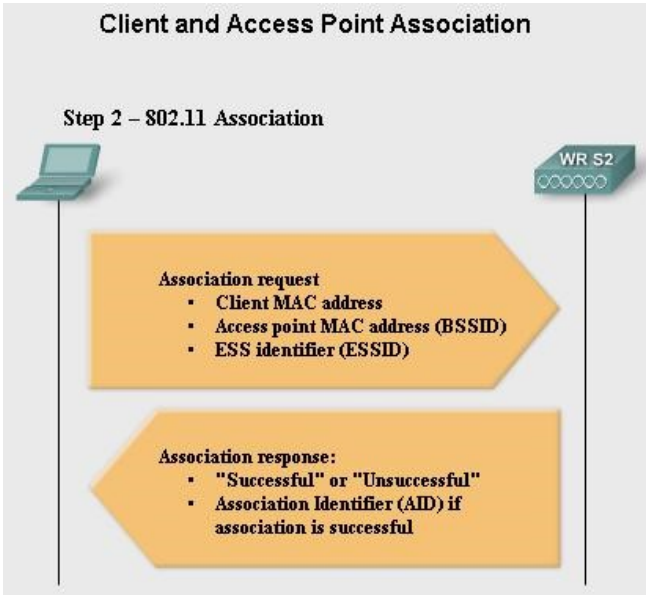
- **Authentication-** wireless NIC на станцията започва автентикация с AP, като се идентифицира.
  - По подразбиране е **Open Authentication** и NIC изпраща само authentication frame, а AP отговаря с acceptance/ rejection.
  - С **Shared Key Authentication -** NIC изпраща authentication frame, AP отговаря 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.



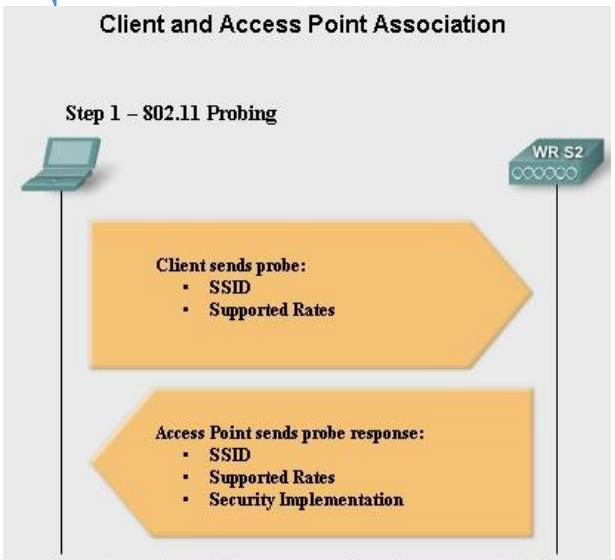
Фреймове за управление

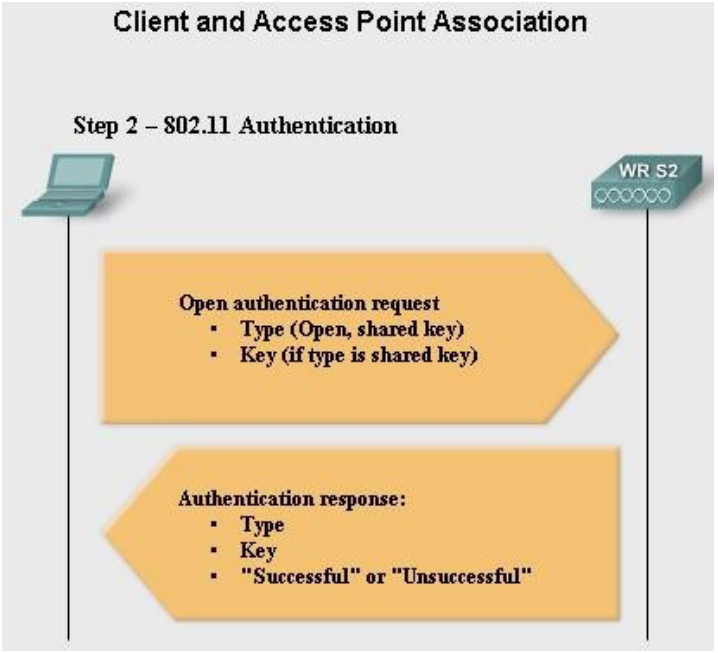
Стъпка 2б: Асоциацията с AP позволява заемане на ресурси и синхронизация с wireless NIC.

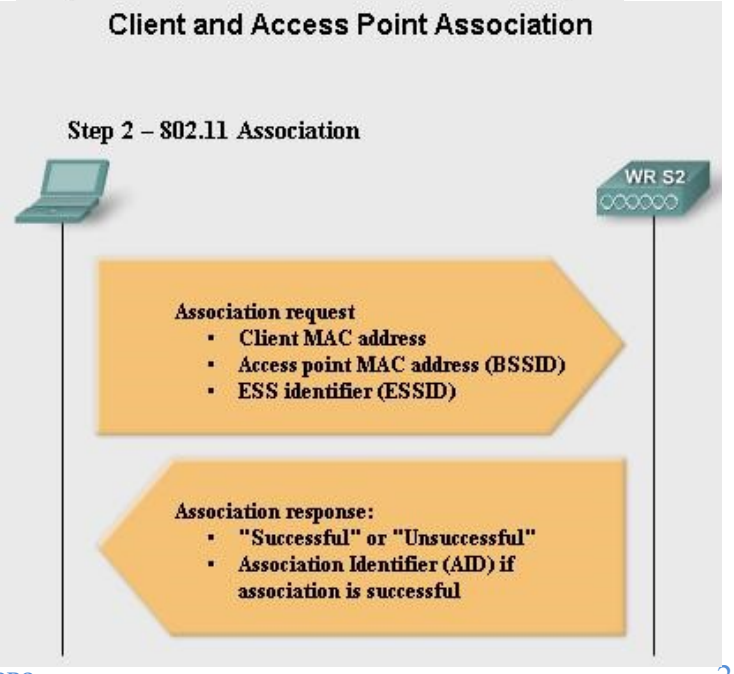
- **Association Request** –NIC я изпраща на AP и съдържа SSID, поддържани скорости, версия на **Cisco Compatible Extensions (CCX).** AP я получава, резервира ресурс за тази NIC и муу присвоява **Association ID**.
- **Association Response-** AP я изпраща на NIC с acceptance/ rejection. Ако е acceptance, 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.



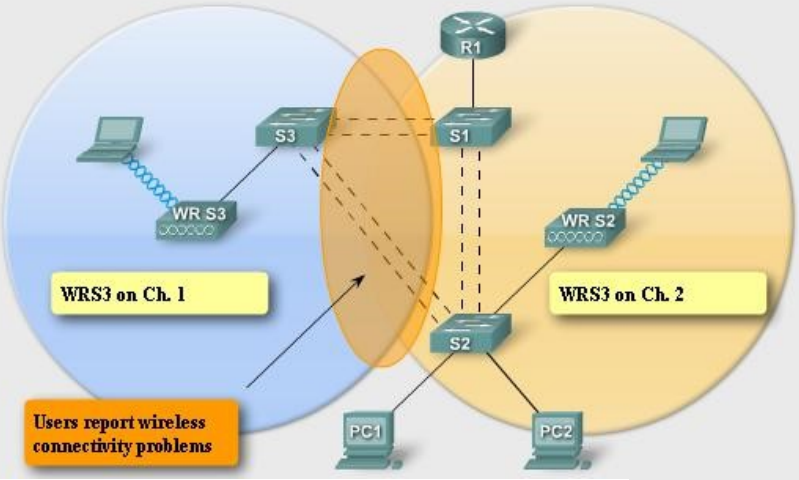
Целият процес



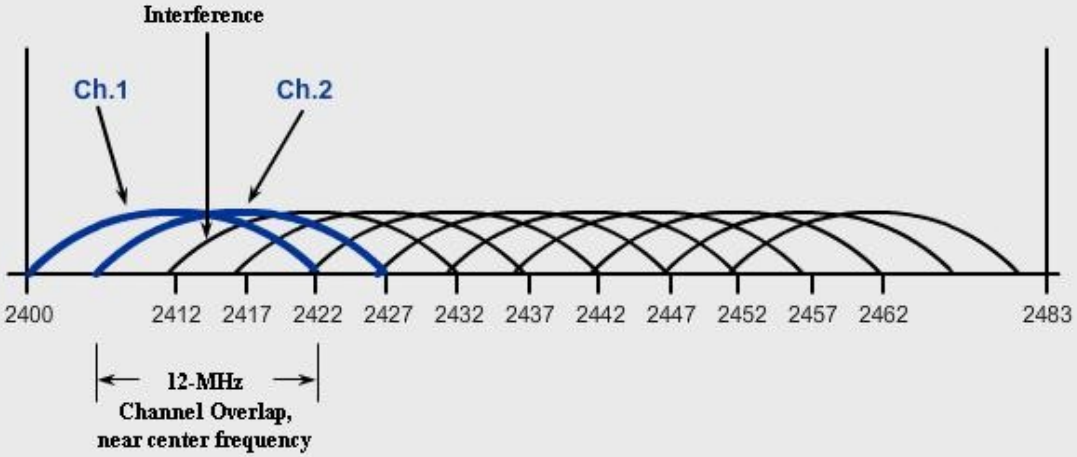




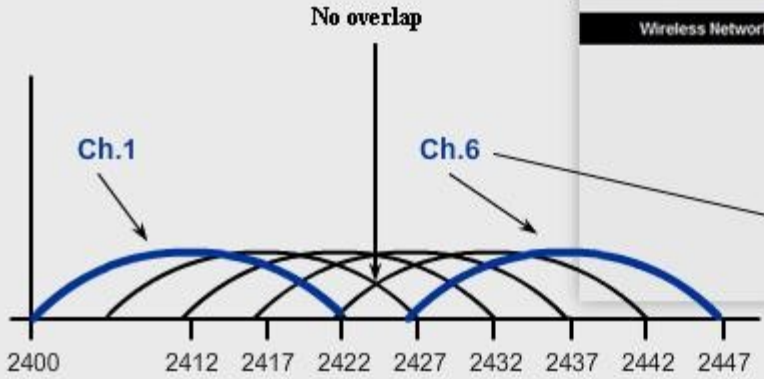
Resolve Issues of Incorrect Channel Settings



Resolve Issues of Incorrect Channel Settings



Resolve Issues of Incorrect Channel Settings



Reset access points to non-overlapping channels

Сигурност в WiFi комуникацията

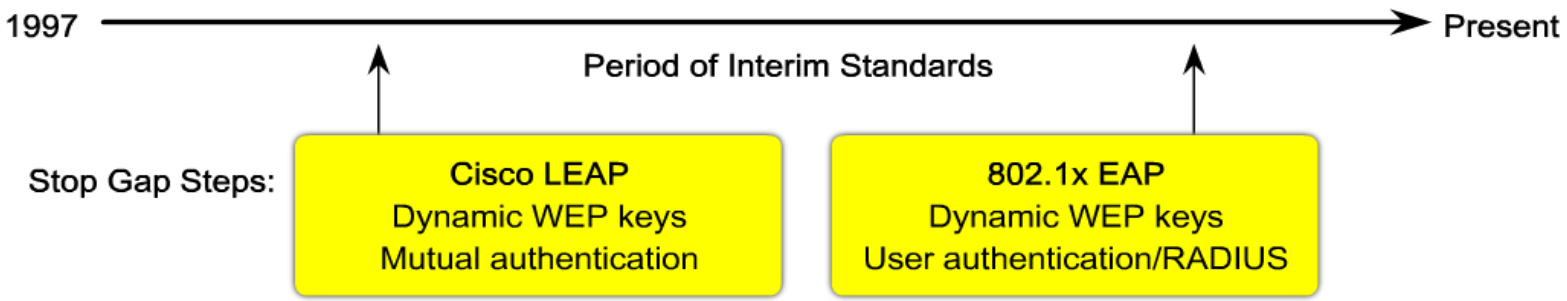
- **SSID прикриване** - точката за достъп не излъчва SSID за безжична мрежа
  - Може да се открие със снифер на комуникацията между точката за достъп и един от клиентите.
- **Филтриране по MAC адрес**
  - Може да се подправи MAC адреса при предаване на кадъра
- **Криптиране**
  - без криптиране и WEP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

Методи за криптиране в WiFi

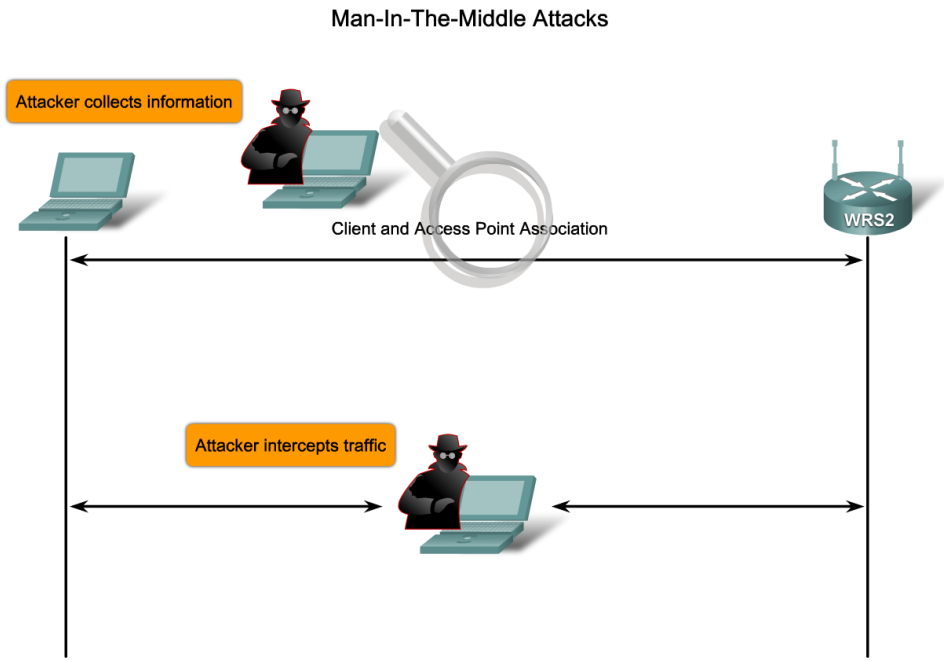
Wireless Protocol Overview

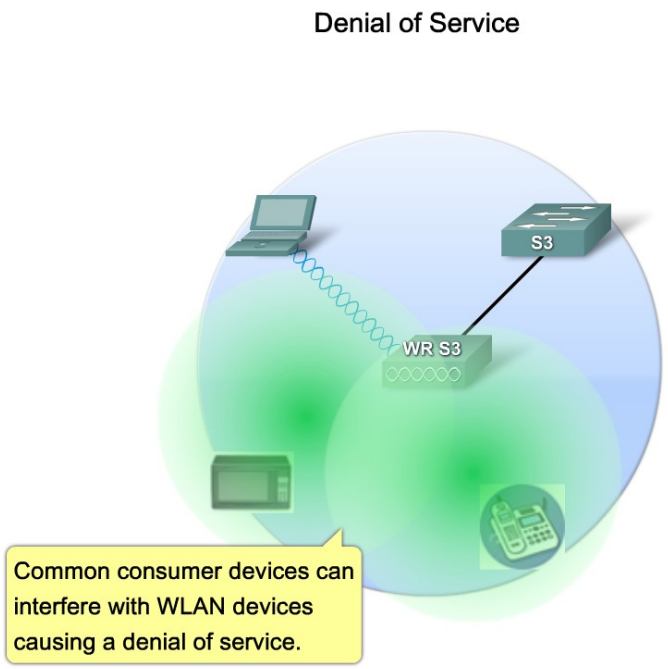
Major Stepping Stones to Secure WLAN

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



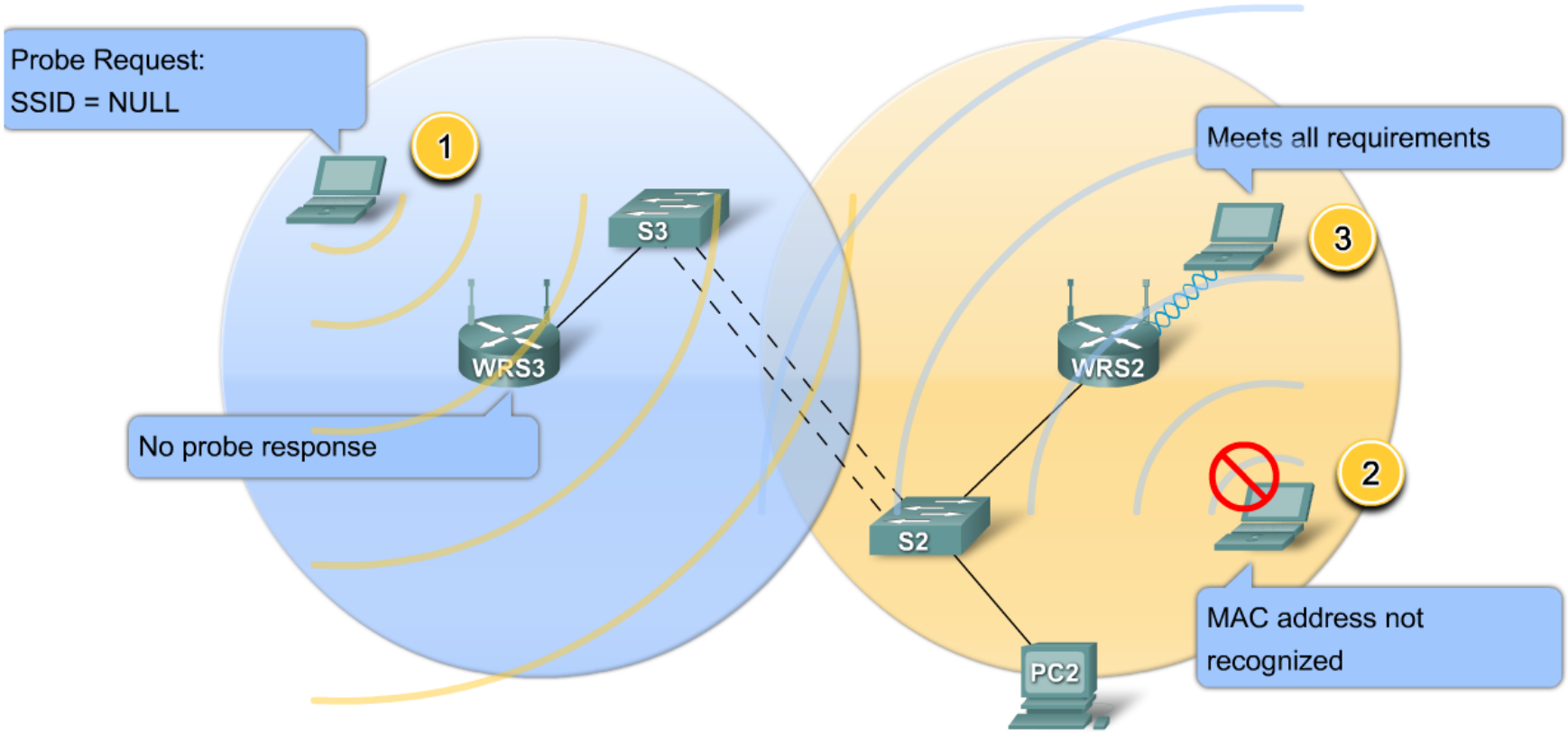


Неоторизиран достъп до мрежата:

- Потребители търсят отворени 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

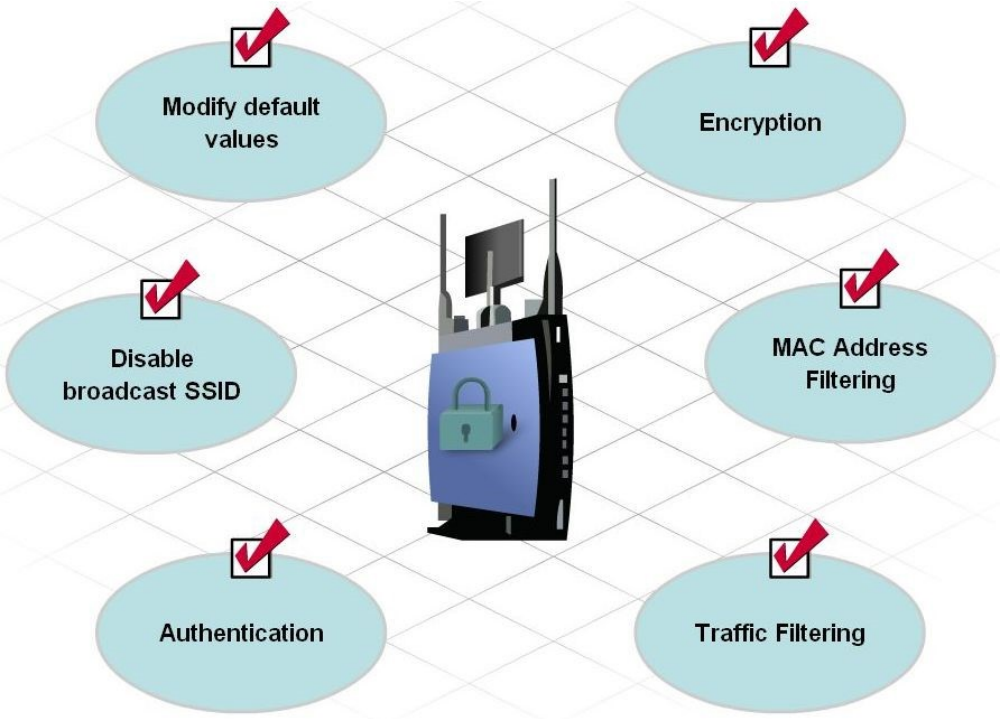


Methods for controlling wireless LAN access:

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

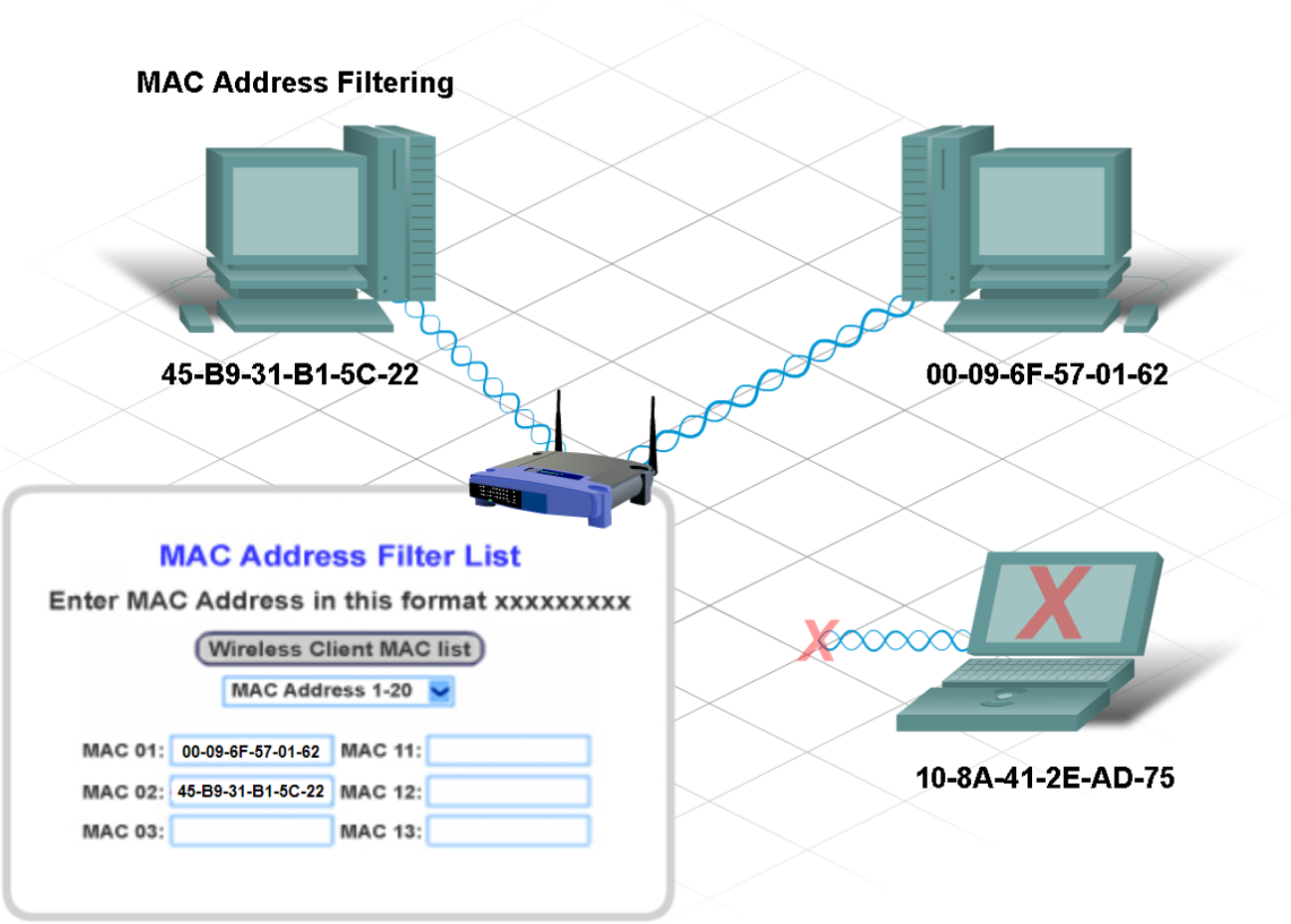
Инсталиране на AP



Стъпки:

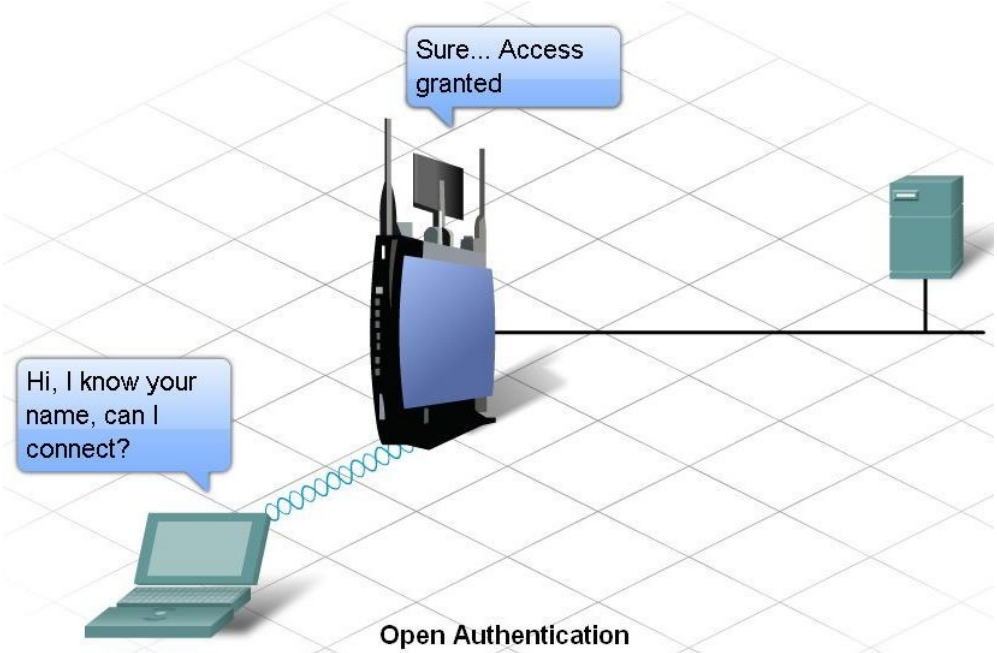
1. Проверява се в кабелната LAN мрежа достъп до Интернет и наличие на DHCP
2. Инсталира се AP
3. Конфигурира се AP – SSID без приложена сигурност
4. Инсталира се един WiFi клиент без приложена сигурност
5. Проверява се връзка има ли между тях
6. Конфигурира се криптиращ протокол – WPA2 или PSK
7. Отново 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



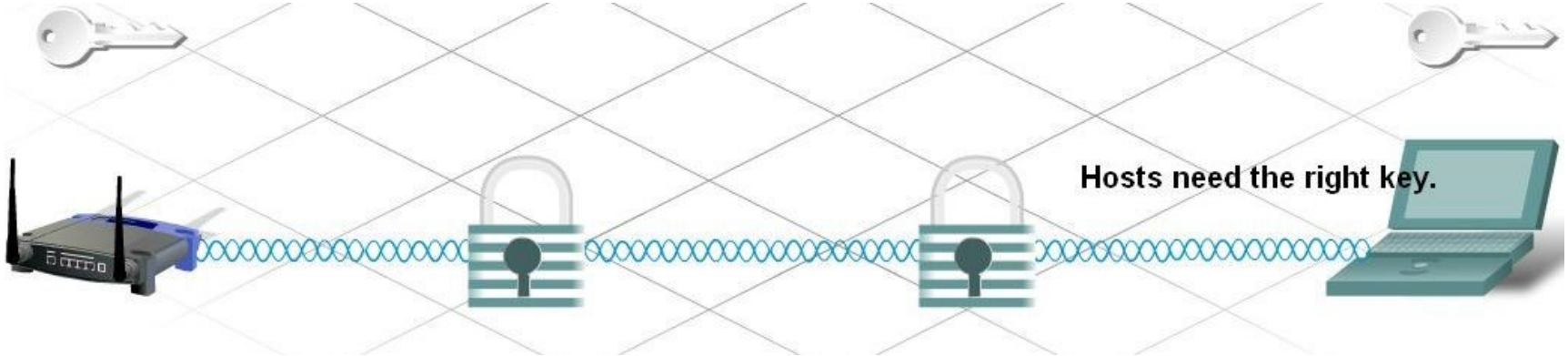
Автентикация

- 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.

Планиране на WiFi мрежа

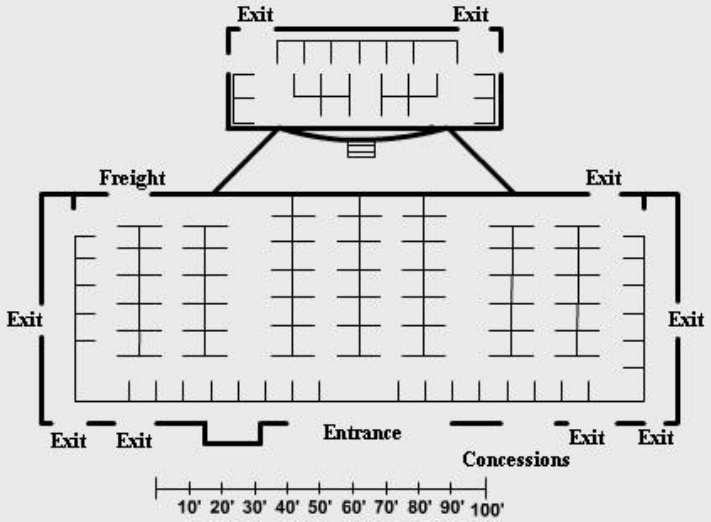
Броят на потребителите влияе на:

- модела на AP,
- безжичният стандарт, който се използва,
- разпределение на точките в пространството,
- скоростта на данните,
- очакванията на потребителите.

Проектирането на WiFi мрежата:

- Чертежи на сградата – на отделните етажи
- Чертеж на съществуващата кабелна инфраструктура
- Обозначаване на работните места
- От спецификациите на AP се взема зоната на покритие

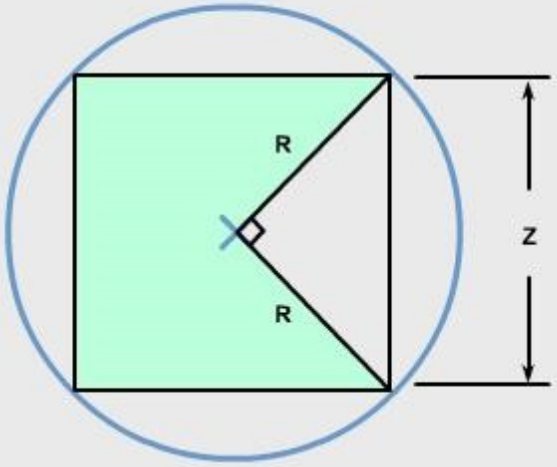
Planning the Wireless LAN



Planning the Wireless LAN

Requirements specify Coverage Area, A = 5000 square feet

Where $A = Z^2$, Find R



From Pythagoras:

$2R^2 = Z^2$

Exit

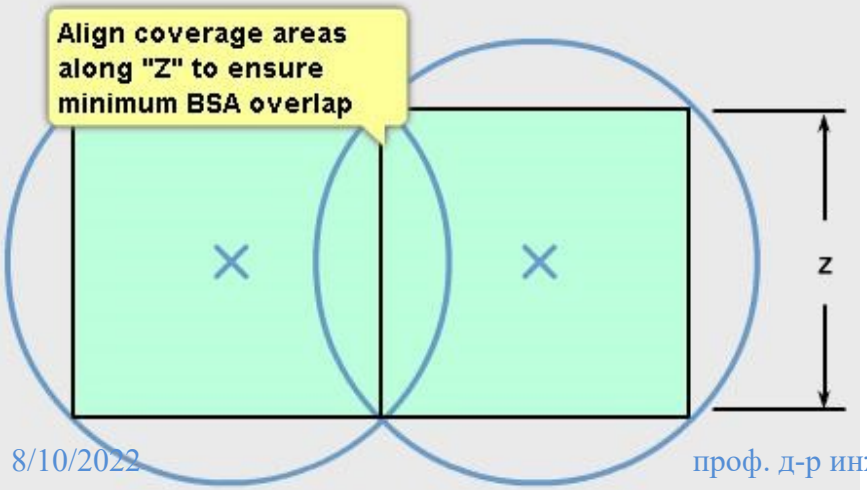
$R = \sqrt{Z^2/2}$

$R = \sqrt{5000 \text{ sq ft}/2}$

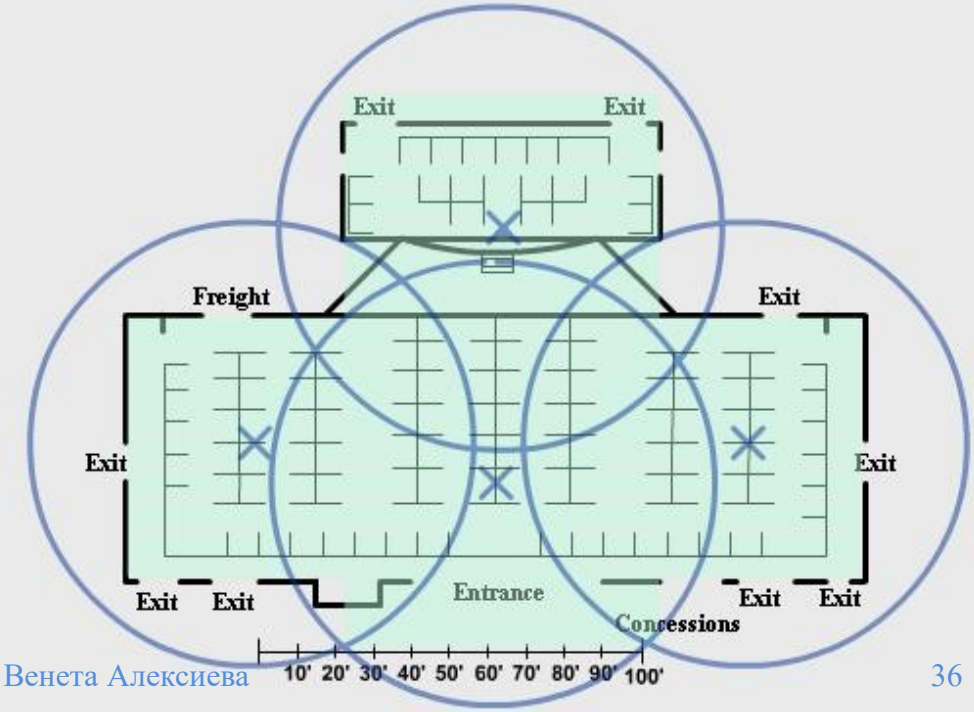
$R = \sqrt{2500 \text{ sq ft}}$

R = 50 feet; Z = 70.71 feet

Planning the Wireless LAN



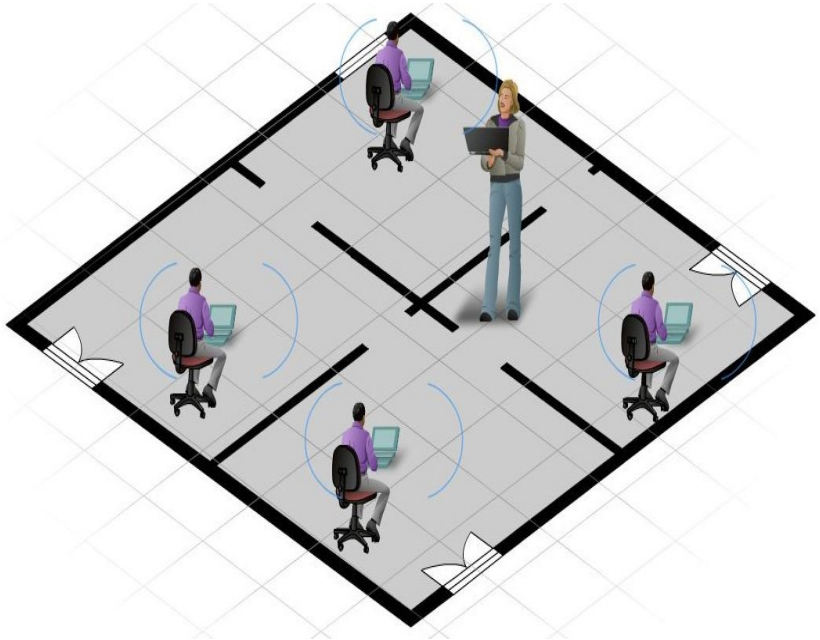
Planning the Wireless LAN



Реализация на WLAN

Етапи:

1. Предварително проучване
2. Подготовка
3. Планиране
4. Проектиране
5. Внедряване
6. Работа
7. Оптимизиране



Фаза Предварително проучване

- Да се разбере как потребителите работят с мрежовите ресурси и услуги
- Да се дефинират всички групи потребители
- Да се прецени дали ще се появят нови групи потребители
- Да се приоритизират бизнес целите
  - Ползата от решението
  - Разрастване на бизнеса
  - Потребителските очаквания
- Да се идентифицират и документират техническите изисквания

Фаза Подготовка -1

- Дефиниране на бизнес целите
  - Да подобри работата на потребителите
  - Да намали цената
  - Да добави нови услуги
  - Да поддържа разрастването на компанията
- Дефиниране на бизнес ограниченията
  - Бюджет
  - Квалификация на персонала
  - Текучество на персонала
  - Политики на компанията
  - Законови, социални и други специфични ограничения

Фаза Подготовка-2

- Разработване на стратегия и избор на решение
  - Избор на съвременни технологии
  - Настоящите приложения и планирани услуги подредени по приоритети въз основа на бизнес целите
  - Хора, процеси и средства, необходими за поддържане на работата и управлението на решеието
- Изработване на задание, на чиято основа ще се правят оферти
  - изискванията за новата мрежа
  - информация за процеса, които компанията използва за закупуване и инсталиране на мрежовите технологии
  - Набелязване на възможните изпълнители
  - графици, които трябва да се спазват.
- Разглеждане на офертите
  - Структурата на офертата трябва точно да отговаря на точките в заданието
  - Техническите термини, които не могат да се избягнат трябва да са дефинирани

Фаза Планиране

- Цялостна оценка на мястото(сградата) и операциите, които трябва да се изпълнят
  - оценява се настоящата мрежа,
  - Работата и управлението на мрежовата инфраструктура
  - Отбелязват се всички физически, екологични, и електрически модификации.
  - оценява се способността на настоящата инфраструктура за поддръжка на новото решение
  - Отбелязват се промени в инфраструктурата, персонала, процесите и инструментите
  - Потребителски приложения, които се добавят се описват.
  - Изработва се документ, който съдържа всички проектни изисквания.
- Планът включва:
  - Задачи
  - Срокове и критични етапи
  - Рискове и ограничения
  - Отговорности
  - необходимите ресурси
  - Да е в рамките на бюджета и да е съобразен с бизнес целите.

Фаза Проектиране

- Създава се цялостен проект на инсталацията, по който се прави изграждането
  - Съобразява се с изискванията за достъпност, разрастване на мрежата, сигурност, управление
  - Да бъде гъвкав – да позволява промени и допълнения
  - Технологиите да бъдат интегрирани в текущата мрежова инфраструктура
- Създава се окончателен проект
  - комплектова се с челна страница, обяснителна записка (ОЗ), спецификация и количествена сметка
  - Планира се инсталацията с указания към инсталатора в ОЗ
  - Включват се в ОЗ указания за тестване за свързаност, внедряване, демонстриране на функционалността на мрежата, мигриране на приложенията към новата мрежа, валидиране на работните процеси, обучение на потребителите и персонала по поддръжка на мрежата

Фаза Изпълнение

- Изграждане на мрежата съгласно чертежите
- Тестване
  - Тесване на всички нови решения в контролирана среда- идентифициране и решаване на проблеми преди реалната инсталация
- Инсталиране на нови решения
  - Интегрират се със съществуващата мрежа
  - Тетват се на място в реална среда дали отговарят на бизнес целите и изискванията на проекта
- Документиране
  - Документират се резултатите от тестовете

Работна фаза

- Наблюдава се ежедневно мрежата
  - да се постигне максимално разрастване, достъпност, сигурност и управление
  - Да се установи дали изпълнението отговаря на изискванията, заложени при фазите на подготовка и планиране
- Дефинират се политики и процедури
  - за да се отстраняват проблеми с инциденти по сигурността, конфигурационни проблеми, доставка и поддръжка на оборудване
  - Да се обновяват политиките и процедурите за да се намали времето на downtime, цената на поддръжка на мрежата и проблеми, свързани с промените в мрежата

Фаза Оптимизация

- Непрекъснат процес, който подобрява производителността и надеждността на мрежата
- Идентифицира и решава потенциални проблеми преди те да се случат:
  - Несъвместимост на решения
  - Недостатъчен капацитет на връзките
  - Проблеми с производителността на устройствата, когато изпълняват няколко функции
  - Проблеми с протоколите

Наблюдение на мрежата при фаза Оптимизация

Когато бизнес целите се променят, технологиите и работата може да не се адаптират адекватно и тогава процесът трябва да започне отначало

Слабости на дизайна

- Единичен отказ
  - В областите, където е ограничена или няма резервираност на връзките, може да доведе до липса на свързаност
- Отказ на голям домейн
  - Ако единичния отказ (няма резервен ISP) води до проблем в голяма част от мрежата, това може да повлияе на бизнеса като цяло
- Възможни тесни места
  - Претоварване на места от увеличен трафик – времето за отговор значително нараства
- Ограничения в разрастването на мрежата
  - Области или устройства да работят на максималния си капацитет и да не позволят бързо разрастване при необходимост, което ще наложи пре-проектиране на мрежата или скъп upgrade.
- Способности на съществуващия персонал
  - Прототипът на мрежата показва доколко е сложно конфигурирането и отстраняването на проблеми. Персоналът трябва да се обучи какво да прави при възникване на проблем или да се приложи друга стратегия за поддръжка на мрежата.

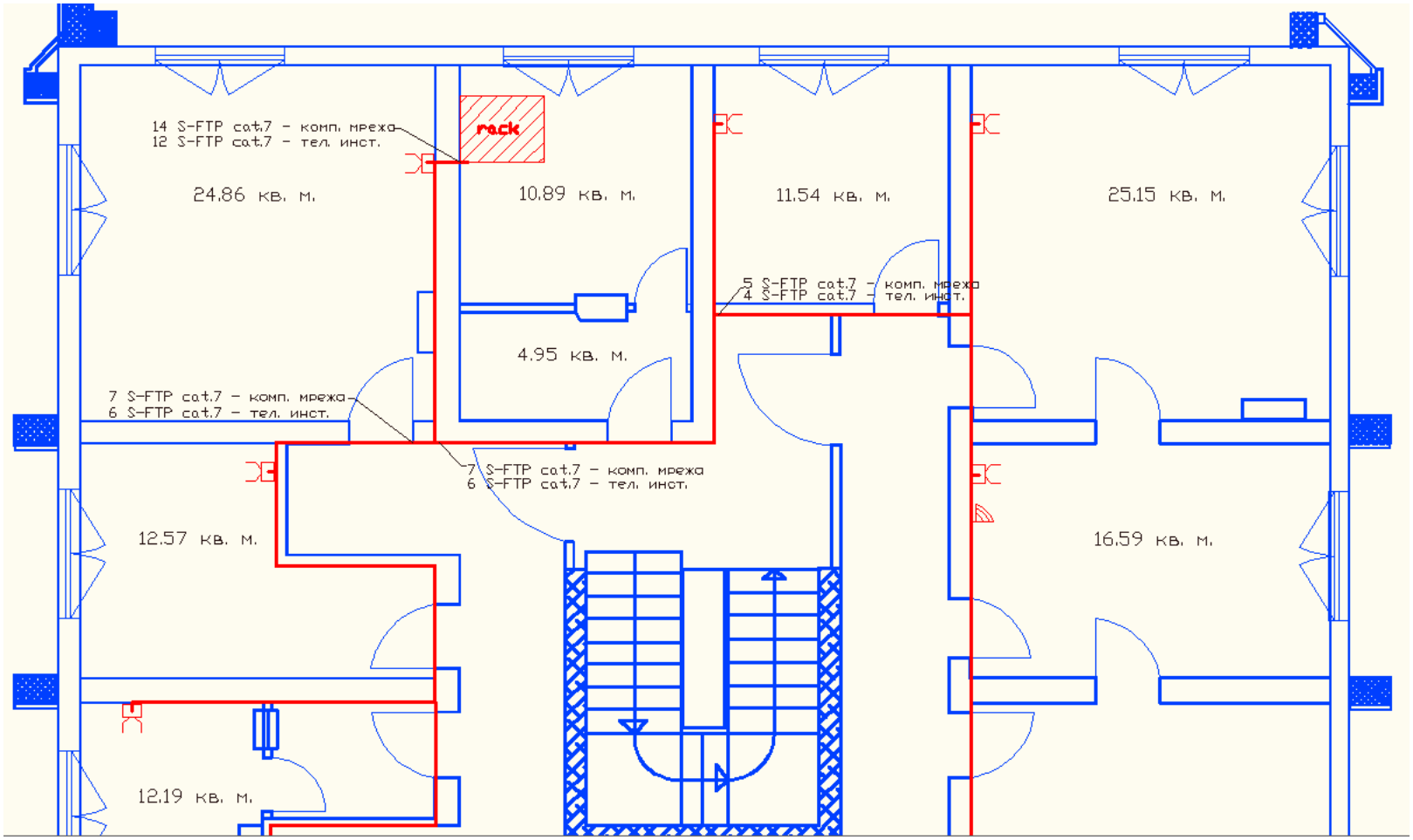
Изисквания към документацията

- Цел на проекта
- Обхват на проекта
- Изисквания към WLAN
- Текущо състояние на мрежата и възможности за постигане на настоящите бизнес цели
- Цели на проекто-предложението
- Обхват на мрежовия upgrade

Разполагане на АР

- В дома или в малък офис инсталирането на АР е свързано с малък брой устройства, които лесно се разместват, за да се получи покритие на областта и потребителските очаквания.
- В среден и голям офис подходът с местенето на АР не работи. Трябва да се определи предварително оптималния брой АР в рамките на бюджета, с които областта на офиса да се покрие и да се определят местата им.

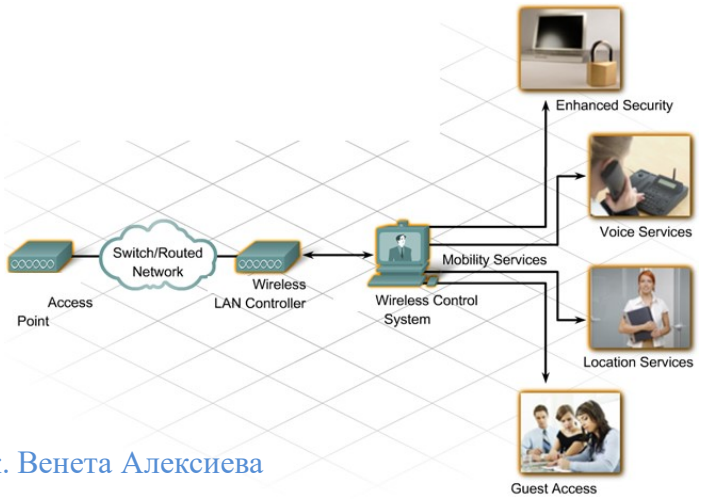
Един подход стъпка по стъпка



- Етаж от офис сграда със съществуваща кабелна мрежа

Един подход -стъпка-1

- Да се определи типа на wireless стандарта, който ще се ползва
- Да се определят най-подходящите устройства
- Да се съобрази с чертежа на съществуващата мрежа
- Да се съобрази с изискванията за сигурност
- Да има стратегия за back up, за обновяване на firmware на wireless устройствата

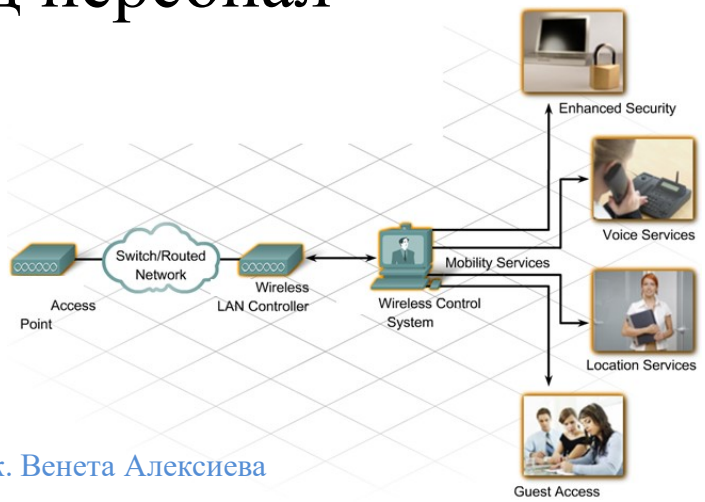


Един подход - стъпка-2

- Да се преценят изискванията за bandwidth
  - Какви приложения ще се ползват в WLAN – висококоростни или не
  - Колко потребители ще ползват WLAN едновременно - bandwidth се поделя между тях
- Да се преценят областите на покритие
  - Каква е съществуващата структура - ако има съществуваща WLAN и тя е по стандарт 802.11a, новата WLAN трябва да поддържа същия стандарт или да се замени изцяло мрежата по стандарт 802.11n
  - Различните стандарти поддържат различна област на покритие (на 2.4 GHz покриват по-голяма обаст от на 5 GHz), което води до по-малко оборудване и по-ниска цена на реализация.

Един подход - стъпка-3

- Да се влезе в рамките на бюджета
- Цената на притежание включва:
  - Цената на оборудването
  - Цената на инсталацията
  - Цената на тестването
- Цената на използване включва:
  - Цената на поддръжка – подмяна на дефектирало оборудване, добавяне на нови модули
  - Заплати за поддържащ персонал



Един подход - стъпка-4

- Разполагане на AP
  - site survey – проучване на място – да се измерят силата на сигналите на съществуващите WLAN и интерференцията им – има софтуерни средства
  - Да се определят източниците на интерференция – високоволтови кабели, мотори, други безжични устройства на същите честоти…
  - да се определи предварително оптималния брой AP в рамките на бюджета
  - да се определят местата им.
- Изследване на силата на сигнала на AP
- Брой потребители
- Динамично преконфигуриране
- Централизирано управление и наблюдение

Един подход - стъпка-5

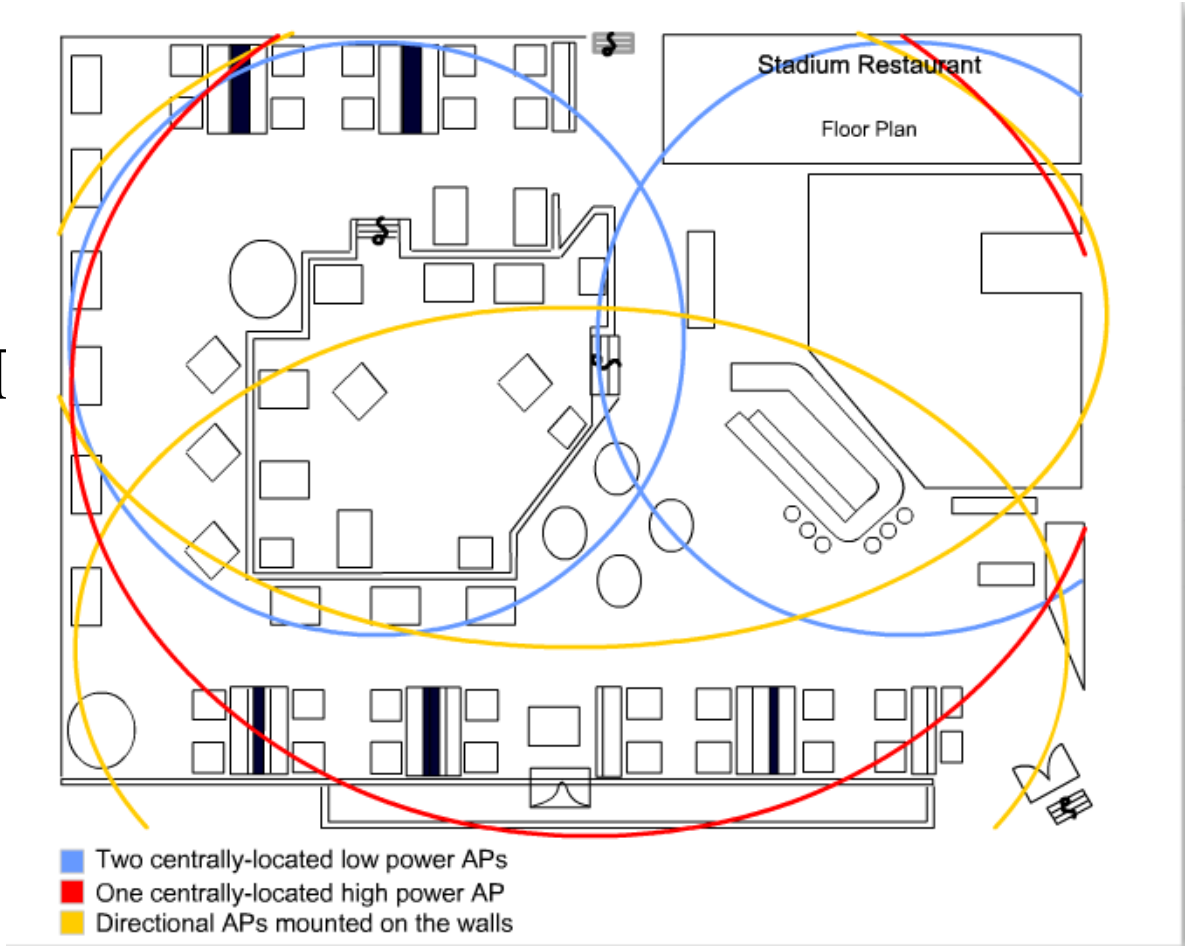
- Имплементиране на сигурност преди връзката с ISP:
  - Създаване на IP адресната схема за WLAN така че да позволява roaming на слой 3
  - Да се определи източника и естеството на потенциалните заплахи
  - Да се набележи на кои устройства ще се имплементират филтри и функции по сигурността
  - Да се дефинират основните категории услуги за сигурност:
    - Сигурни връзки
    - Защита на инфраструктурата
    - Откриване на заплахи, защита и преодоляване на проблеми
  - Да се направят филтри за достъп съгласно изискванията
    - Подходящи правила в защитните стени
    - Access control lists
    - VPNs

Един подход - стъпка-5

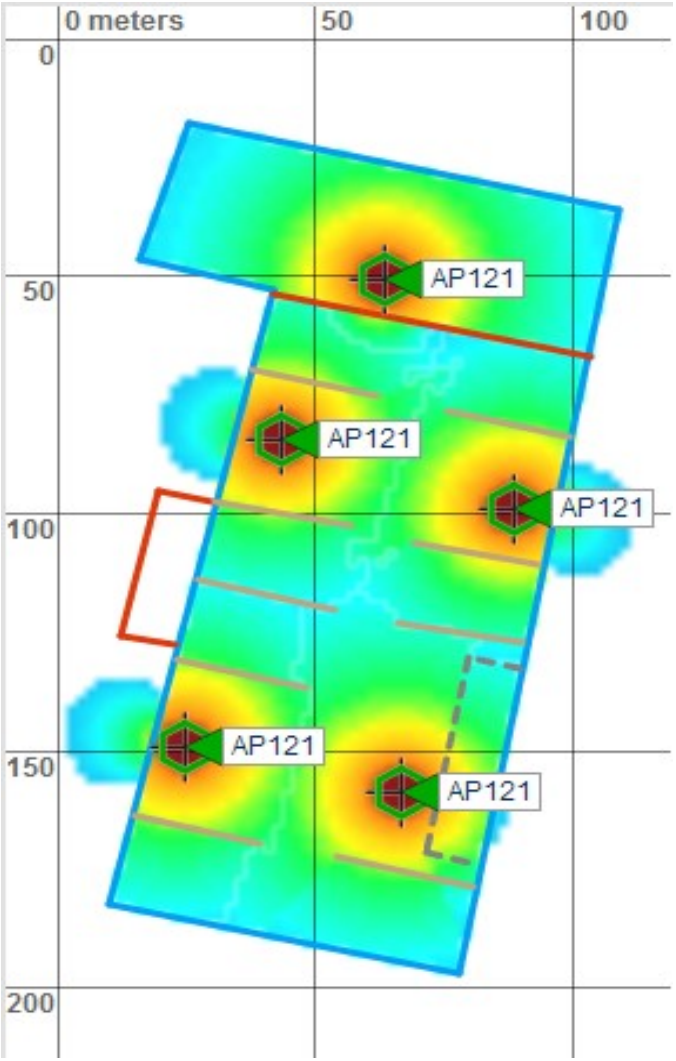
Слабости	Проблем	Възможно решение
Flat дизайн	Невъзможност за разрастване с достатъчна производителност	Да се създаде йерархичен дизайн с маршрутизатори
Flat дизайн	Няма сегментация на мрежата- не позволява да се филтрира трафик за целите на сигурността	Да се създадат VLANs Да се приложат филтри на трафика
Няма резервираност	Големи домейни, в които връзки или устройства ако се повредят влияят на голяма част от мрежата	Да се раздели на поддомейни Да се добави резервираност, където е възможно
Разпределени сървъри	Не е контролирана средата, няма backup захранване или резервни връзки	Да се преместят сървърите в отделно помещение(TR) или в data center
Разпределени сървъри	Няма високоскоростни връзки до сървърите	Да се подменят връзките с гигабитови
Няма защитни стени	Настоящите филтри на трафика не защитават от неоторизиран и нежелан трафик	Да се използват хардуерни защитни стени или маршрутизатори, позволяващи филтри на трафика
Защитна стена има само на граничния маршрутизатор	Няма защита от вътрешни атаки	Да се направят разслоени защитни стени и механизми за филтриране, да се добавят IDS и IPS в data center

Един подход - стъпка-6

- Достъпността до WLAN- покритие
  - VISIWAVE
  - Ekahau
  - TamoGraph
  - AIRMAGNET
  - Net Stumbler
  - Aerohive
  - ….

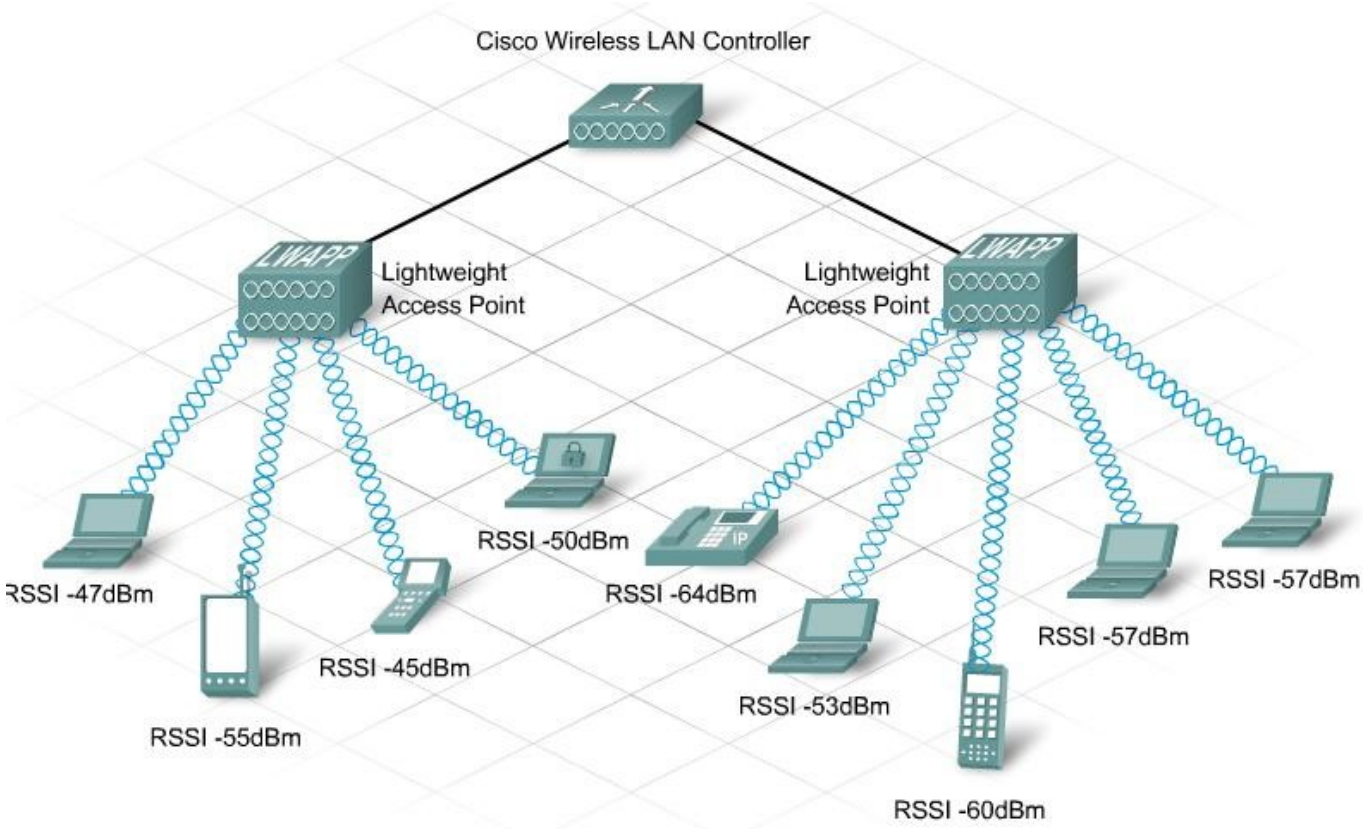


Пример - Hometmax



Един подход - стъпка-7

- Резервираност
- Централизирано балансиране на натоварването на мрежата



Един подход - стъпка-8

- Защитна стена на edge маршрутизатора не гарантира сигурността на мрежата.
- Да се определи кои данни и комуникации са изложени на риск, и потенциалните източници на атаки.
  - Ресурси, които са достъпни за вътрешни потребители
  - Ресурси, които се използват от външни потребители
  - Пътища за достъп до мрежата
- Заплахите могат да идват и от вътрешни източници
  - услуги за сигурност трябва да бъдат поставени на подходящи места в цялата мрежа.
  - Използване на интегрирани услуги - да се премахне необходимостта от допълнителни устройства за сигурност.
- Основно сигурността е:
  - Защита на инфраструктурата
  - Защита на връзките
  - Откриване на заплахи, проблеми и преодоляването им

Един подход - стъпка-9

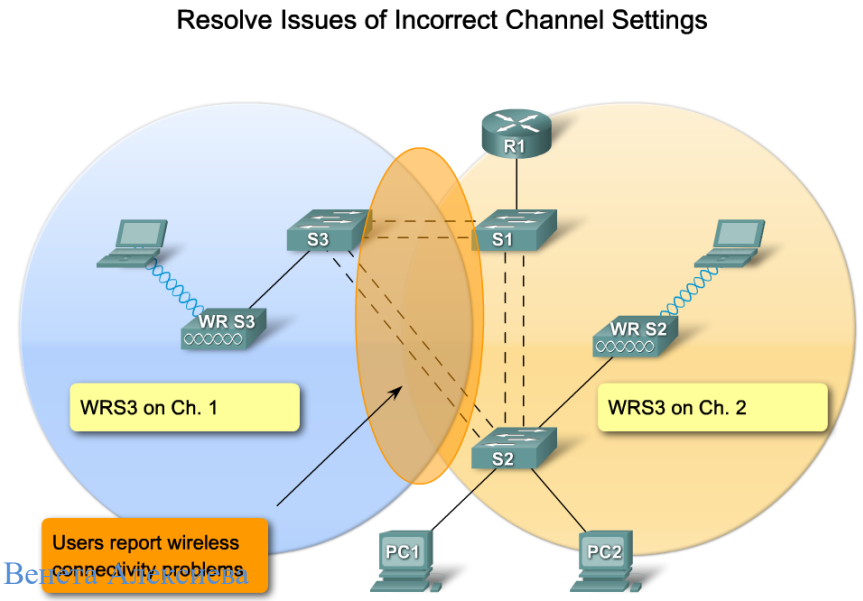
- Управлението на мрежата включва:
  - Промени в конфигурацията на мрежата
  - Идентифициране на мрежови грешки
  - Мониторинг на сигурността
  - Управленско счетоводство за индивидуално и групово ползване на мрежата
- Наблюдението гарантира, че са спазени спецификациите на дизайна
- Наблюдението и управлението:
  - подобряват точността и ефективността на персонала, който обслужва мрежата
  - води до опростяване на конфигурирането и бързо идентифициране и определяне на проблеми в мрежата

Един подход - стъпка-10

- Анализ на слабостите на мрежата и риска, свързан с тях
- Тестване на различните елементи на дизайна, за да се гарантира, че са изпълнени целите на модернизацията на мрежата
  - Неправилно настройване на каналите
  - Проблеми с RF интерференция
  - Неправилно разполагане на AP
  - Проблеми с WLAN автентикация и криптиране

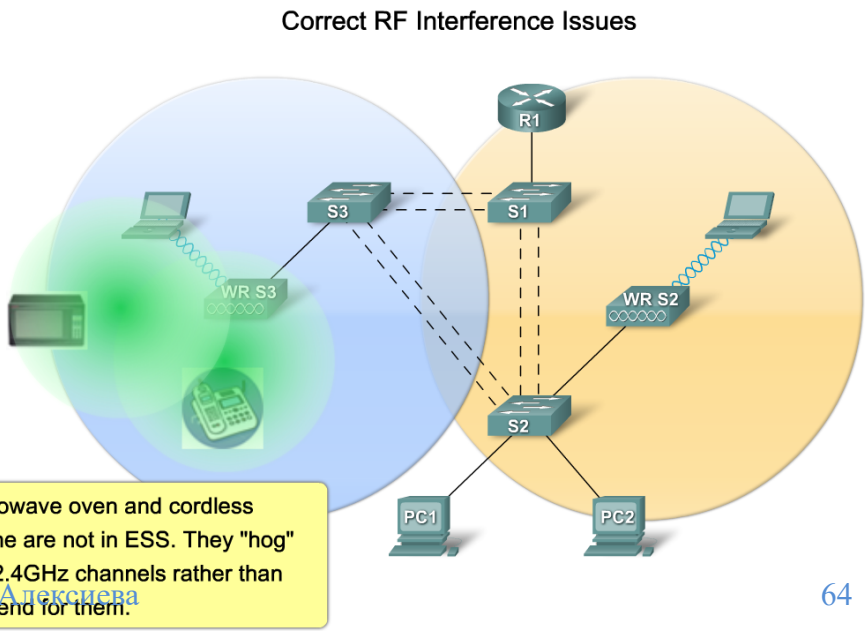
Неправилно настройване на каналите

- 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.



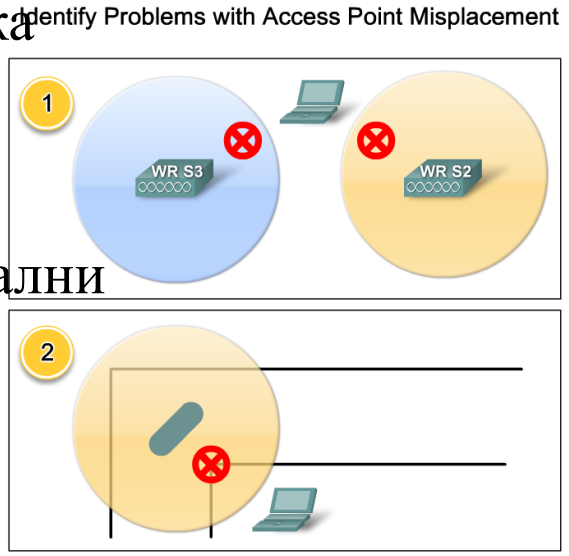
Проблеми с RF интерференция

- 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 AP

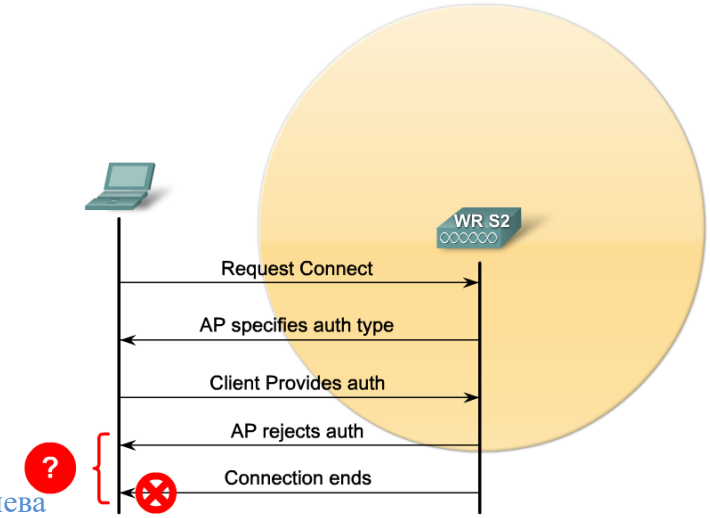
- Разстоянието между точките за достъп е твърде далеч, за да се припокриват.
  - на минимум 10 до 15% припокриване,
- Ориентацията на антените на AP в коридорите и ъгли намалява покритието.
  - вертикално близо до тавана в центъра на всяка зона на покритие, ако е възможно
  - AP да не са монтирани по-близо от 20 см от тялото на всички лица.
  - AP да не са в близост от поне 91,4 см от метални прегради.
  - AP да са далеч от микровълнови печки
  - AP да се монтират вертикално
  - AP 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



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



Въпроси ?

Благодаря за вниманието !

За самопроверка

1. Какво представлява ALOHAnet? A HiperLAN? A HiperLAN/2?
2. Какъв е механизмът за пестене на енергия в HiperLAN?
3. Кога се появява стандартът 802.11?
4. Какъв е форматът на фрейма при 802.11?
5. Какви са управляващите съобщения на фаза асоциация с AP? Представете графично. Какви проблеми могат да възникнат по време на този процес?
6. Какви са управляващите съобщения на фаза автентикация с AP? Представете графично. Какви проблеми могат да възникнат по време на този процес?
7. Какви методи за криптиране на връзката с AP познавате? Какви са техните предимства и недостатъци. Какви проблеми могат да възникнат по време на този процес?
8. Какви са фазите на проектиране на една безжична мрежа? Какви са основните задачи на всяка една фаза?
9. Какви са възможните рискове от неправилен дизайн на мрежата?
10. Какви са потенциалните проблеми при конфигуриране на AP?
11. Какви са стъпките на конфигуриране на AP?
12. Как се препоръчва да се конфигурират каналите на припокриващите се AP, за да се минимизира интерференцията между тях? Защо?
13. Каква площ на припокриване трябва да има между съседните AP? Защо?
14. По какво си приличат и по какво се различават 802.3 и 802.11?
15. Какви са стъпките при наблюдение на мрежата на фаза оптимизация?
16. Какви са потенциалните слабости на дизайна на безжична мрежа и как се преодоляват?