

Бездротові мережі

Курс “Операційні системи і комп’ютерні мережі”

Лекція 17

Питання

1. Загальна характеристика бездротових мереж
2. Технологія Wi-Fi 6
3. Режими роботи бездротових мереж
4. Роумінг в бездротових мережах
5. Безпека в бездротових мережах

1. Загальна характеристика бездротових мереж

- Бездротові мережі володіють гнучкістю при конфігурації і розширенні. Можуть служити як додатковими, так і заміною провідних мереж при побудові мережевої інфраструктури
- Користувачі можуть вільно переміщатися, тому що бездротові мережі забезпечують доступ до мережевих ресурсів компанії з будь-якого місця.
- Бездротові мережі не тільки забезпечують мобільний доступ, а й самі мобільні, тому що можна легко перемістити мережу в інше місце.
- Швидка і легка інсталяція (Майже завжди)

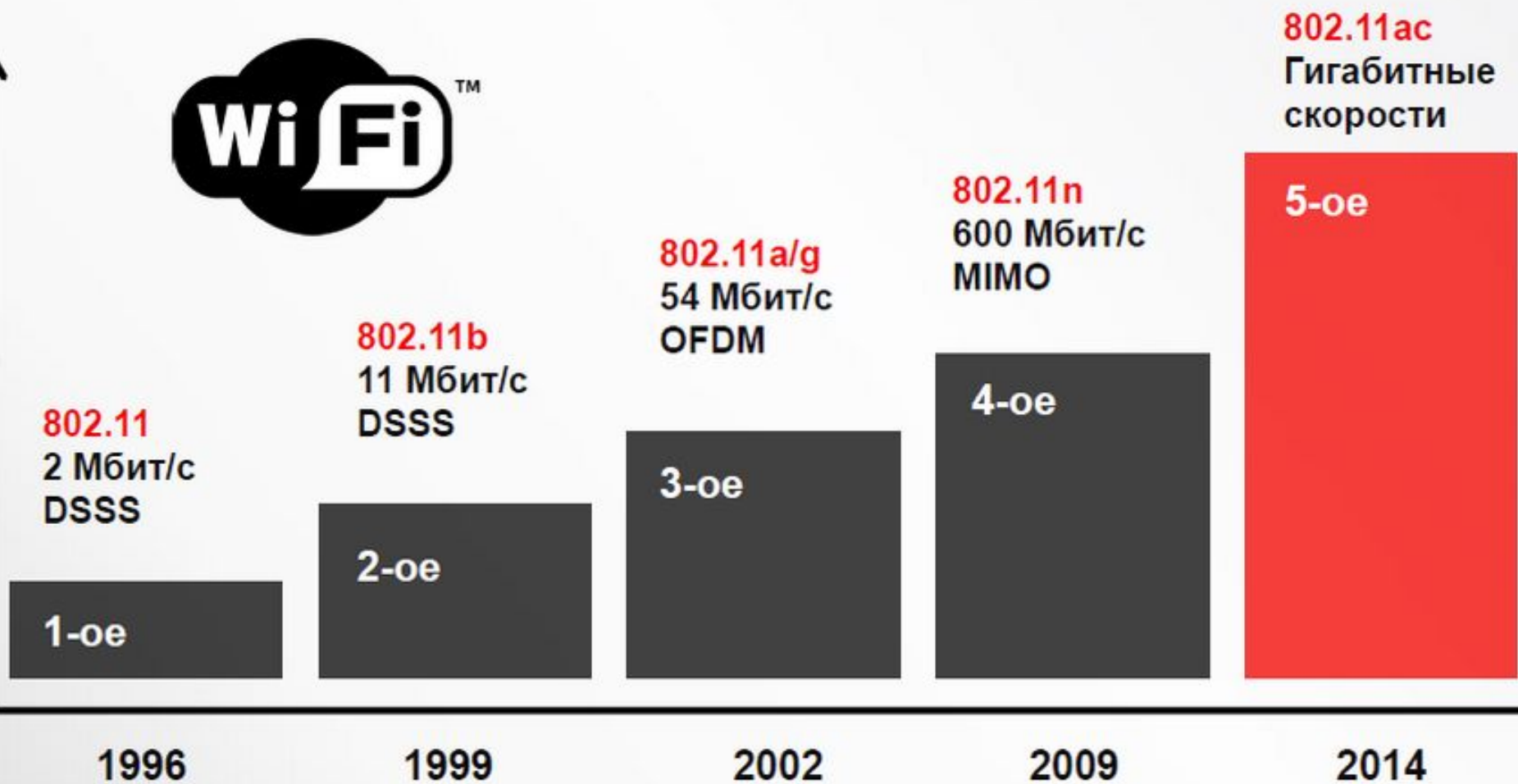
Сфери використання бездротових мереж

- Внутрішньоофісні мережі
- Домашні мережі
- Виставкові комплекси і конференц-зали
- Доступ до Інтернет в готелях, кафе, бібліотеках, студентських містечках і т.д. - "hot spot"
- Мережі провайдерів Інтернет: підключення клієнтів там, де немає можливості протягнути кабель
- «Гостьовий» доступ до корпоративної мережі для клієнтів і партнерів

Сімейство стандартів бездротових мереж IEEE 802.11




Стандарт IEEE 802.11 входить в серію стандартів IEEE 802.X, що відносяться до мереж і комунікацій, сюди також входять такі стандарти, як 802.3 Ethernet, 802.5 Token Ring і т.д.

Таким чином, стандарт IEEE 802.11 визначає компоненти і характеристики мережі на фізичному рівні передачі даних і на рівні доступу до середовища з урахуванням бездротового способу передачі даних і можливості взаємодії з існуючими мережами.



	802.11ac	802.11n	802.11g
Spectrum	5GHz	2.4GHz 5GHz	2.4GHz
Bandwidth	20MHz 80MHz 40MHz 160MHz	20MHz 40MHz	20MHz
Maximum Antennas	8X8 MIMO(MU-MIMO)	4X4 MIMO	1X1 SISO
Speed	433 Mbps 867 Mbps 1300 Mbps (80MHz)	150 Mbps 300 Mbps 450 Mbps (40MHz)	54 Mbps
Max. Speed	6.93Gbps	600 Mbps	54 Mbps

В 2019 році Нова нумерація

Generation of network connection	Sample user interface visual
Wi-Fi 6	 The icon for Wi-Fi 6, featuring a stylized signal tower with three curved lines representing signal strength and a large number '6' inside a circle.
Wi-Fi 5	 The icon for Wi-Fi 5, featuring a stylized signal tower with three curved lines representing signal strength and a large number '5' inside a circle.
Wi-Fi 4	 The icon for Wi-Fi 4, featuring a stylized signal tower with three curved lines representing signal strength and a large number '4' inside a circle.

2. Технологія Wi-Fi 6

Підтримка діапазонів 2,4 і 5 ГГц (Нажаль на ринку занадто багато legacy- пристроїв)

Підтримка OFDM (Orthogonal frequency-division multiplexing) - мультиплексування з ортогональним частотним поділом каналів

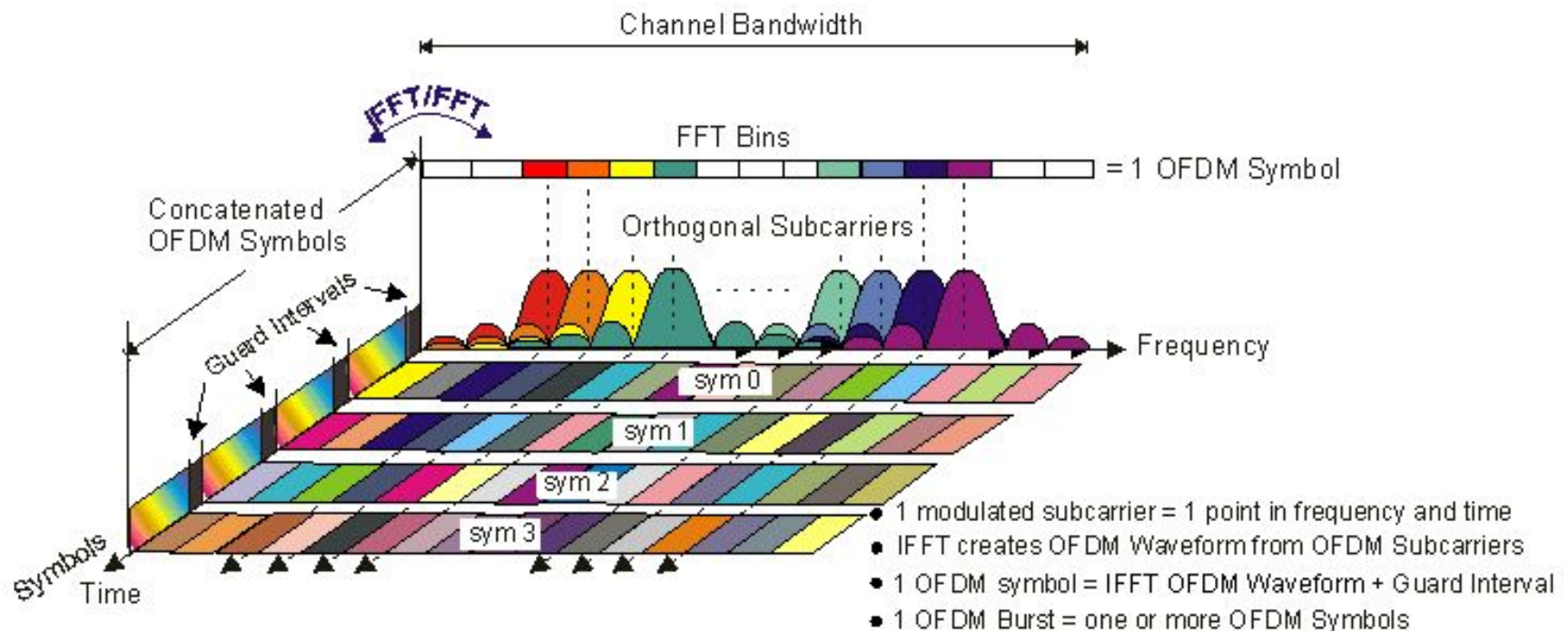
Одночасно MU-MIMO (Multi user Multiple Input Multiple Output) разом з OFDMA - до 11Гб/с

Target Wake Time - функція для економії електроенергії

OFDM

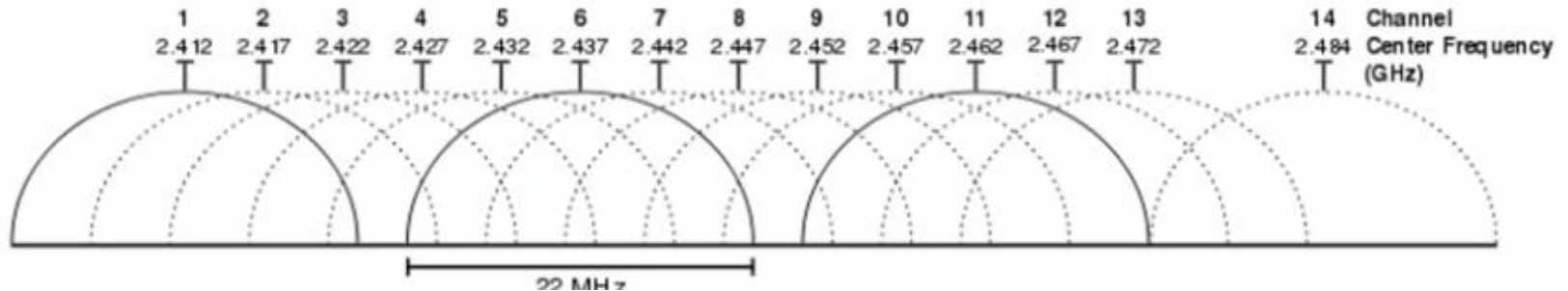
Мультиплексування з ортогональним частотним поділом каналів

OFDM сигнал формується N гармонійними поднесущими, які рознесені по частоті на рівні інтервали Δf

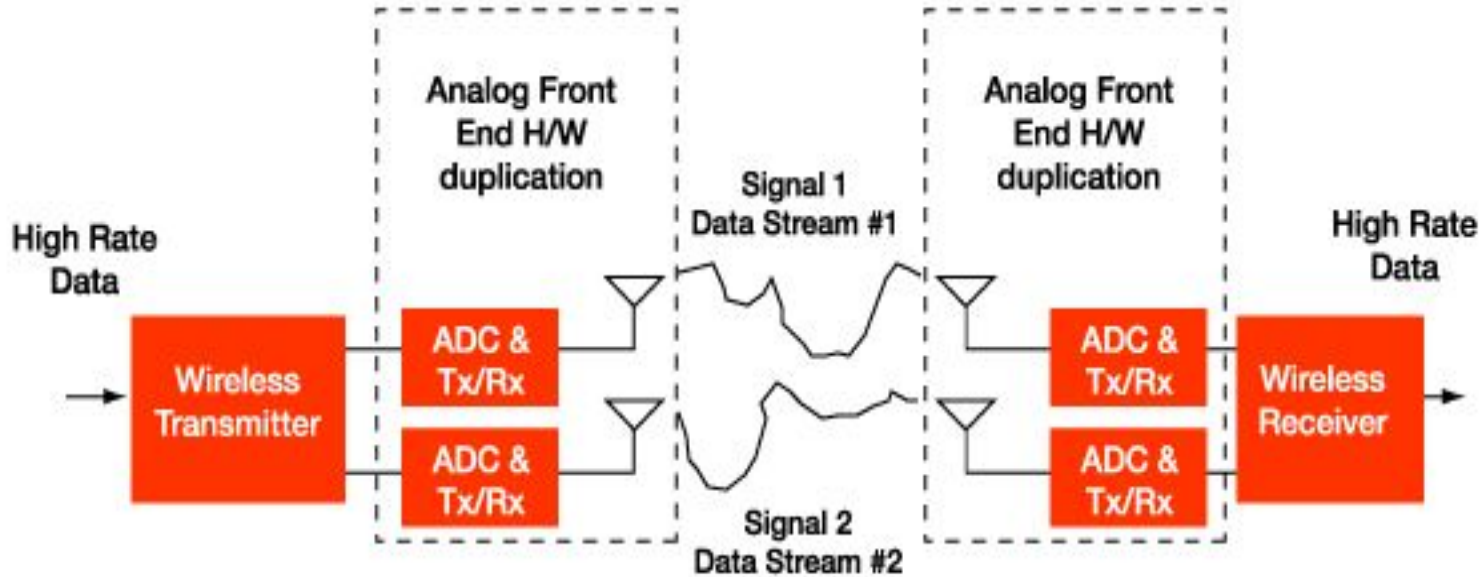


Канали в діапазоні 2,45 ГГц

Канал	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Частота (ГГц)	2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462	2.467	2.472	2.484



Технологія MIMO



За допомогою просторового мультиплексування Spatial Division Multiplexing (SDM) - передається кілька незалежних потоків даних одночасно всередині однієї спектральної смуги пропускання каналу.

Для реалізації MIMO необхідно, щоб для кожного потоку даних використовувалися свої антени прийому / передачі, окремі радіочастотні ланцюги і аналого-цифрові перетворювачі (АЦП) для кожної антени.

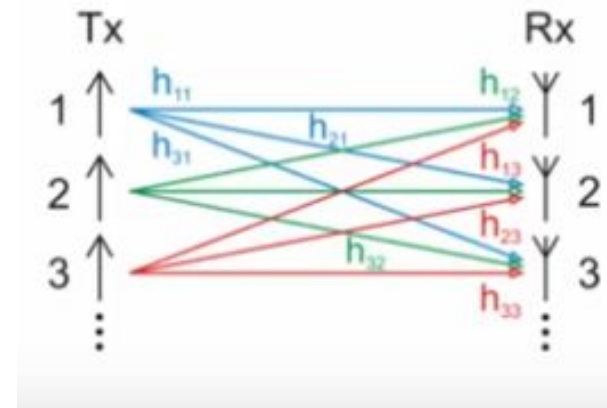
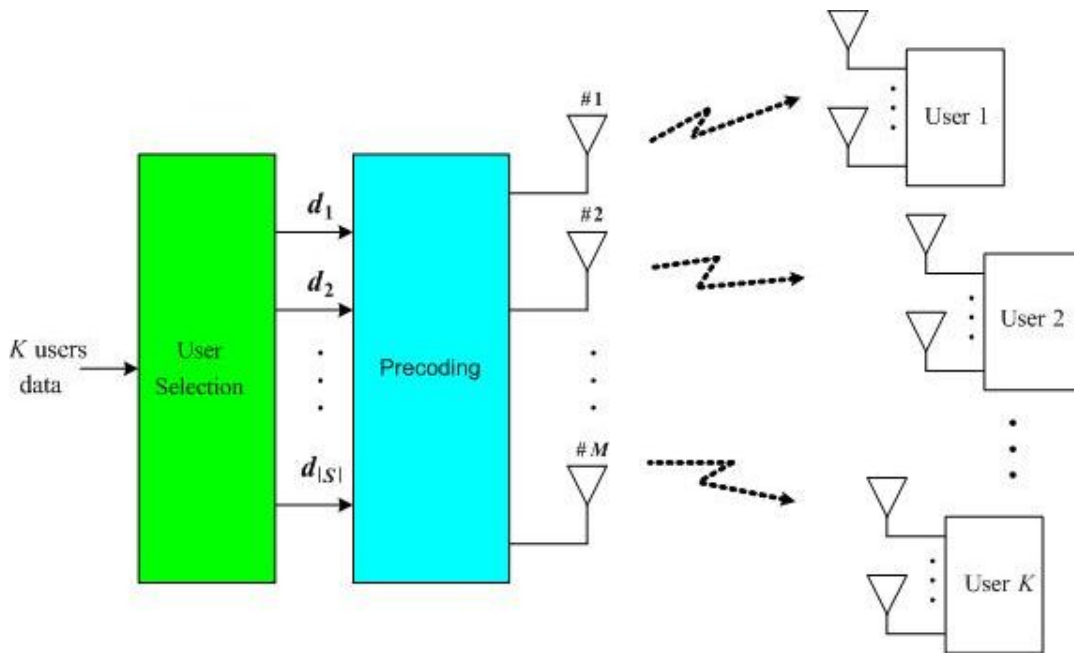
MU-MIMO

MIMO розшифровується як multiple input, multiple output - «множинний введення, множинний виведення. Це метод просторового кодування сигналу, що використовує систему з багатьма каналами передачі і прийому даних.

Залежно від кількості користувачів, на адресу яких здійснюється одночасна передача даних, існує два типи MIMO:

SU-MIMO: однопользовательские системи MIMO (Single User MIMO)

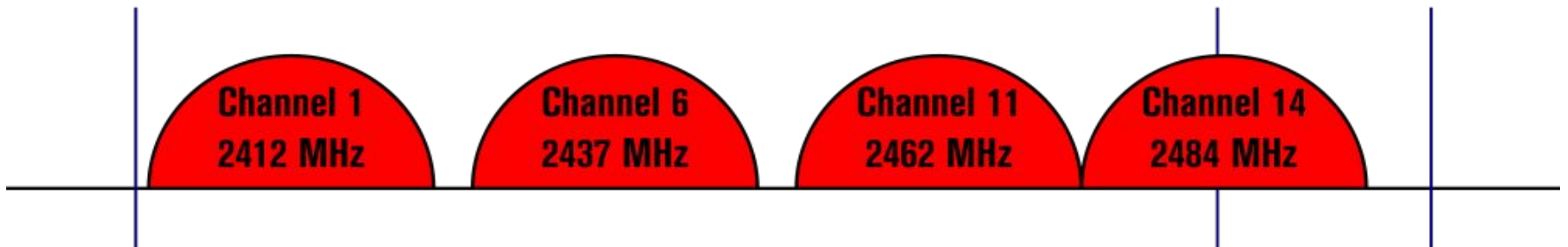
MU-MIMO: розраховані на багато користувачів системи MIMO (Multi User MIMO)



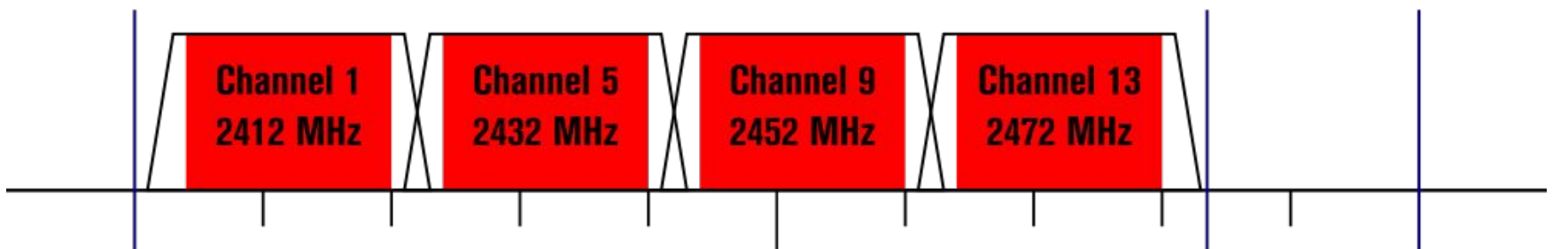
Частоти каналів

Канали, що перекриваються, в
діапазоні 2,4 ГГц

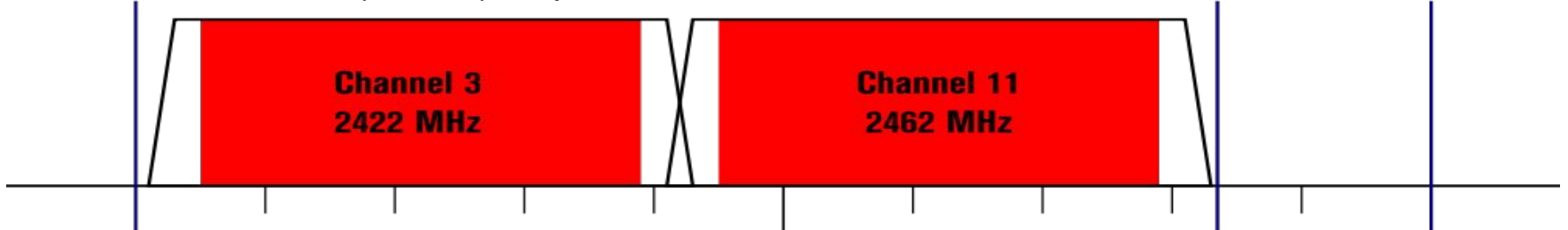
2.4 GHz 802.11b (DSSS) ширина канала 22 МГц



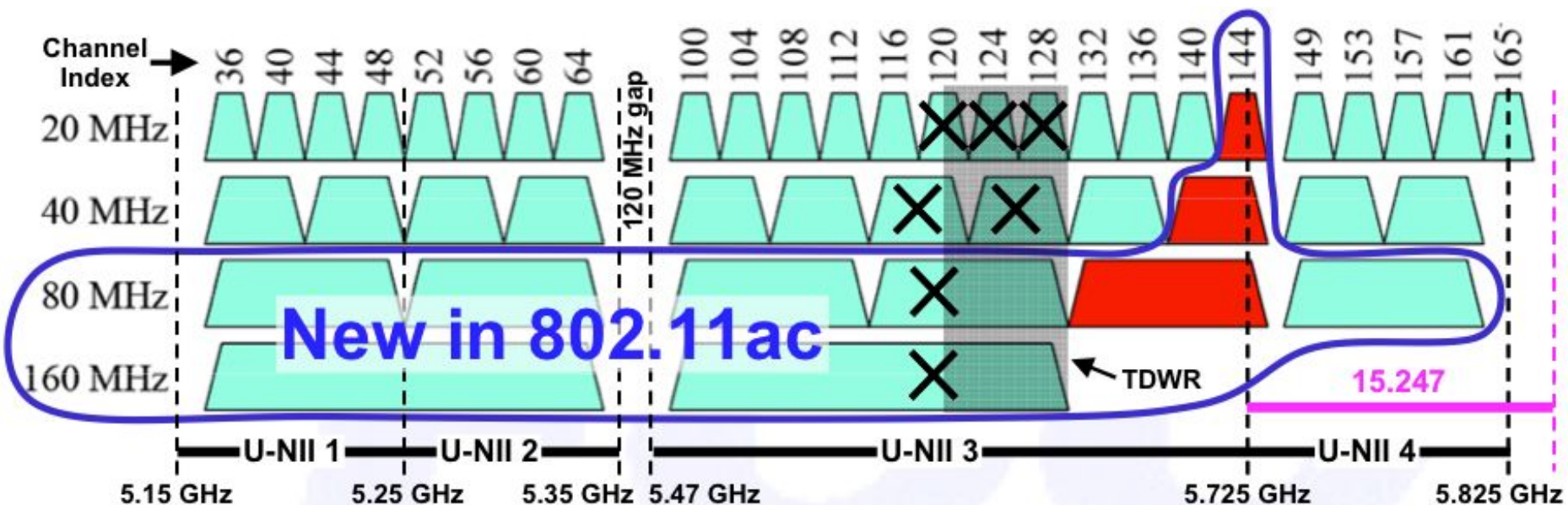
2.4 GHz 802.11g/n (OFDM) ширина канала 20 МГц



2.4 GHz 802.11n (OFDM) ширина канала 40 МГц



Ширина каналу - швидкість передачі



3. Режими роботи бездротових мереж

Бездротові мережеві адаптери

- Ad Hoc
- Інфраструктурний

Точки доступу

- Точка доступу
- WDS
- WDS +AP
- Бездротовий клієнт
- Повторювач

Ad Hoc режим



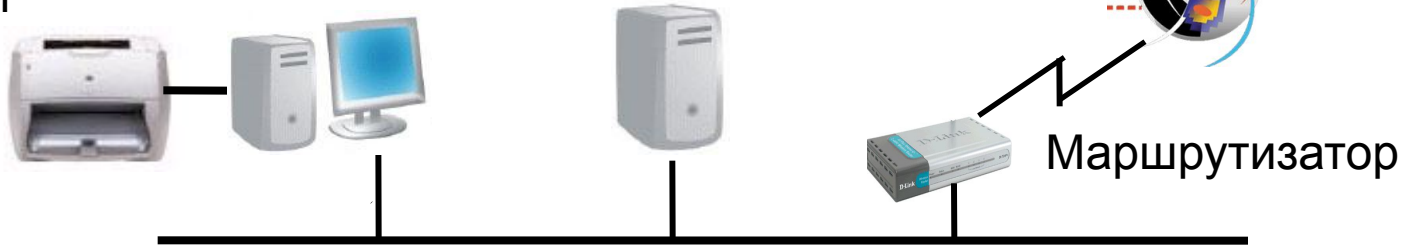
Однорангове взаємодія по типу «точка-точка».
Комп'ютери взаємодіють безпосередньо без застосування точок доступу

Інфраструктурний режим

ПК с провідниковим адаптером і спільним принтером

Сервер, підключеним до провідникового сегменту мережі

Інтернет



Провідниковий сегмент мережі

Точка доступу

Бездротова мережа

ПК с бездротовим адаптером DWA-525 або ноутбук с DWA-645

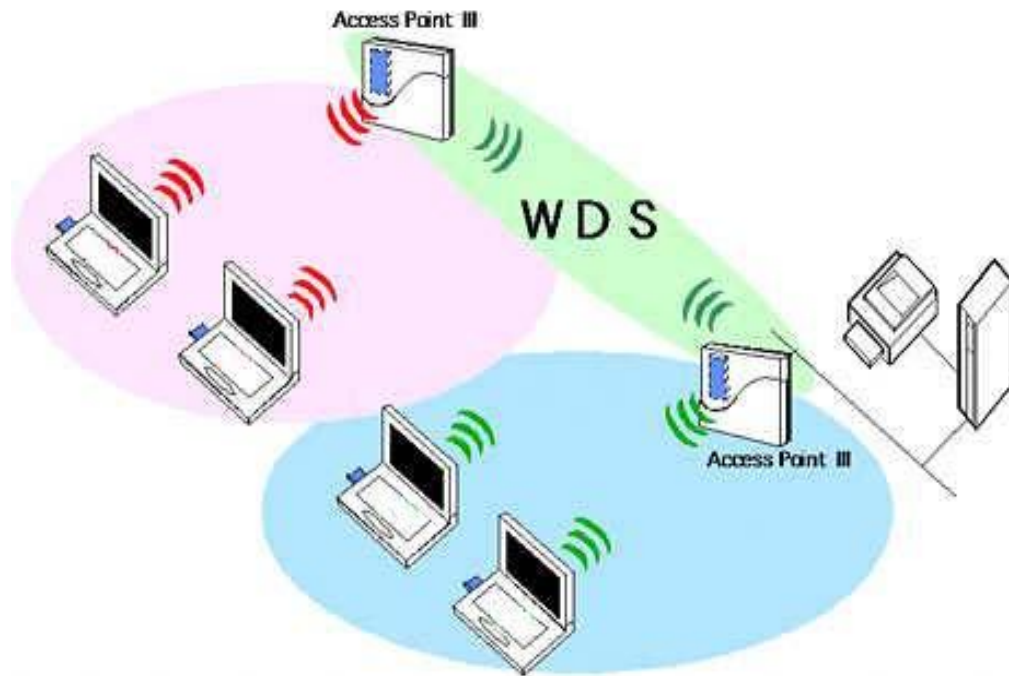


Точки доступу забезпечують зв'язок клієнтських комп'ютерів. Точку доступу можна розглядати як бездротової концентратор

Технологія WDS (Wireless Distribution System)

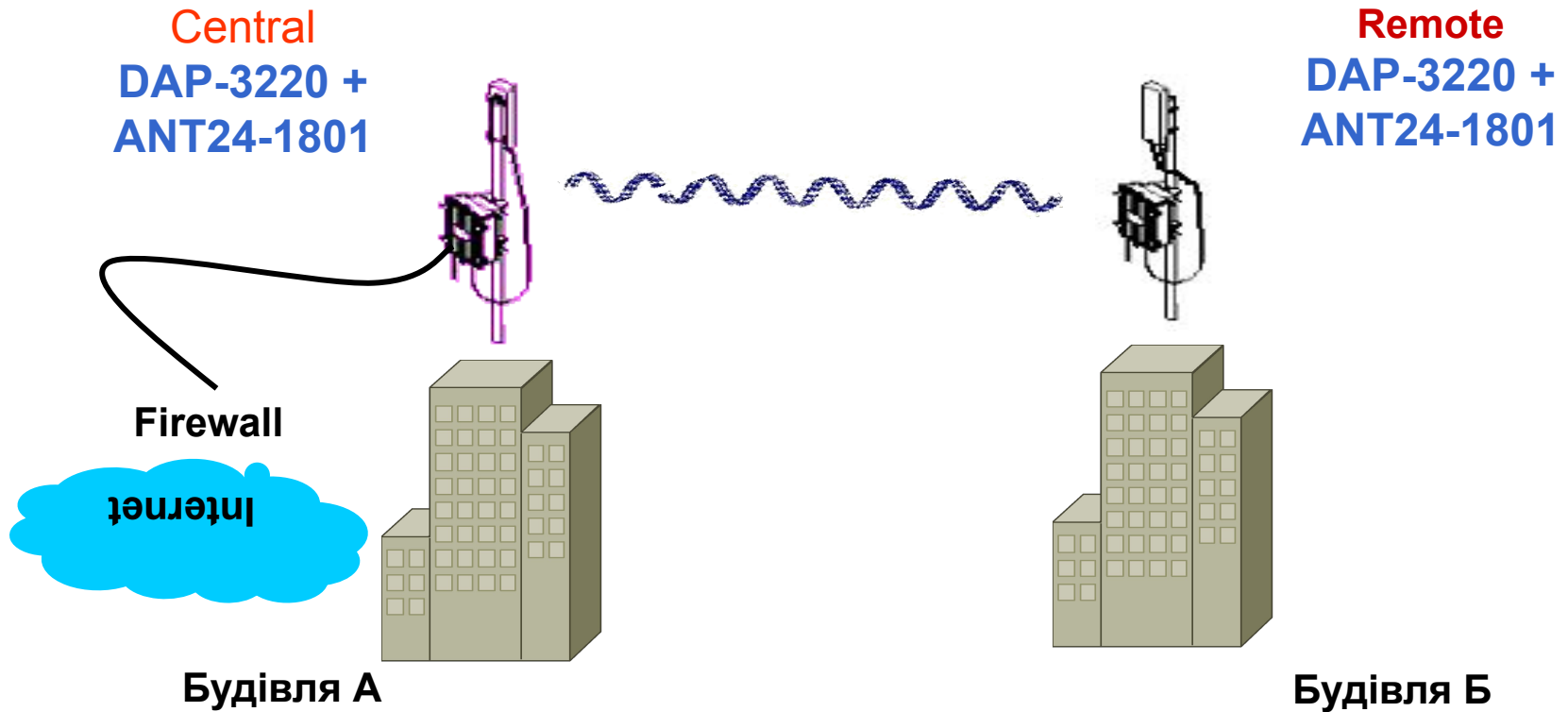
- Термін WDS (Wireless Distribution System) розшифровується як «розподілена бездротова система». Якщо говорити спрощено, то дана технологія дозволяє взаємодіяти точкам доступу для бездротового з'єднання не тільки з бездротовими клієнтами, а й між собою.
- Технологія WDS може використовуватися для реалізації двох режимів бездротових з'єднань між точками доступу: режиму бездротового мосту (радіомосту) і режиму бездротового повторювача.
- Режим бездротового мосту (WDS) дозволяє точкам доступу працювати тільки з іншими точками доступу, але не з клієнтськими адаптерами.
- Режим бездротового повторювача (WDS with AP) дозволяє точкам доступу працювати як з іншими точками доступу, так і з клієнтськими адаптерами.

Технологія WDS (Wireless Distribution System)



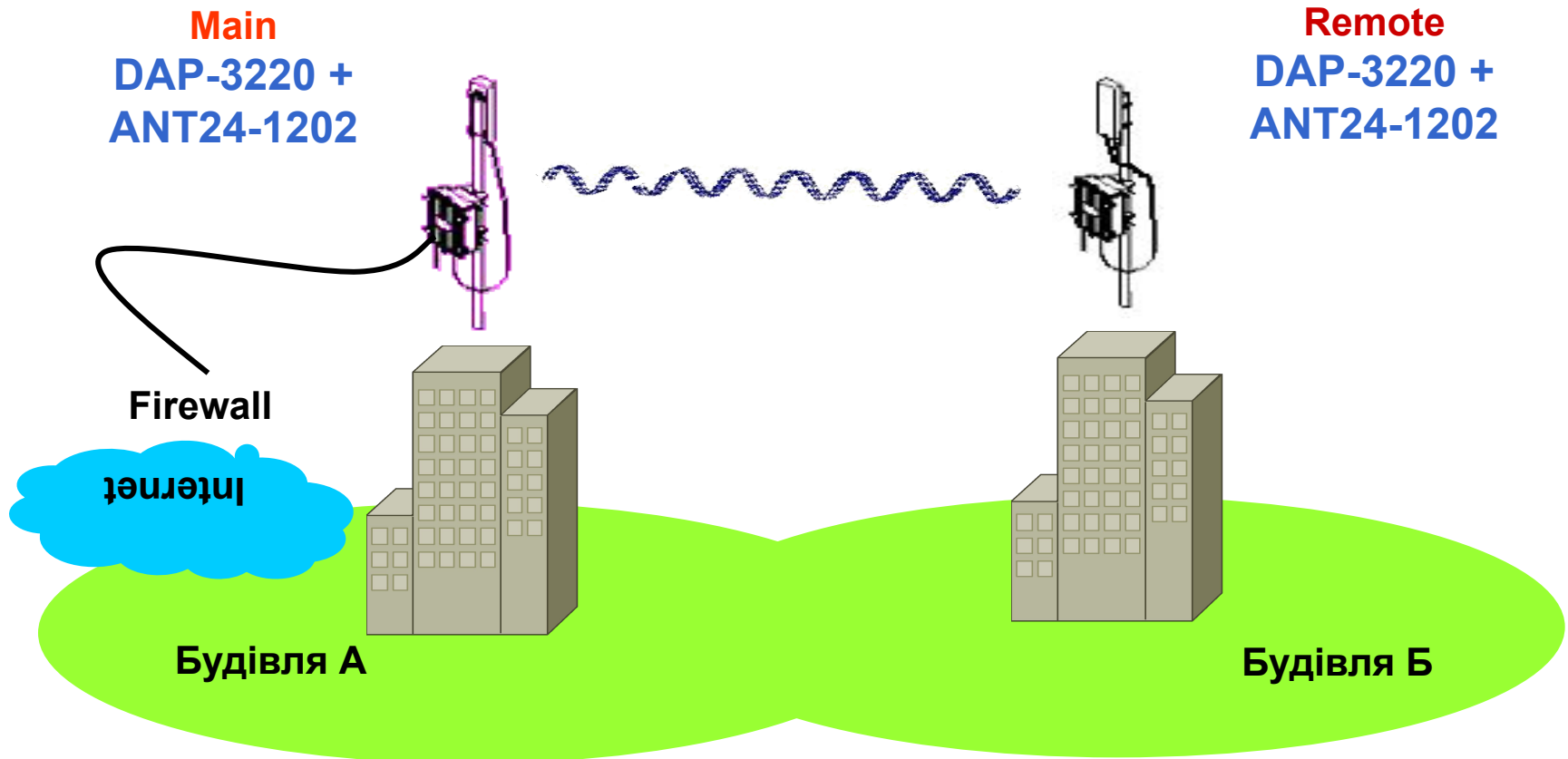
Дана технологія дозволяє одночасно підключати бездротових клієнтів до точки доступу, що працюють в режимі "бездротовий міст"

WDS



Використовується для об'єднання двох або більше провідних сегментів LAN, що знаходяться на відстані до декількох км.

WDS with AP



Використовується для об'єднання двох або більше провідних сегментів LAN + можливість підключення бездротових клієнтів у радіусі.

- Використання режиму WDS with AP в умовах офісу. Точка 2 використовується як ретранслятор.



Незважаючи на переваги технології WDS, тут є свої підводні камені, серед яких варто відзначити наступні:

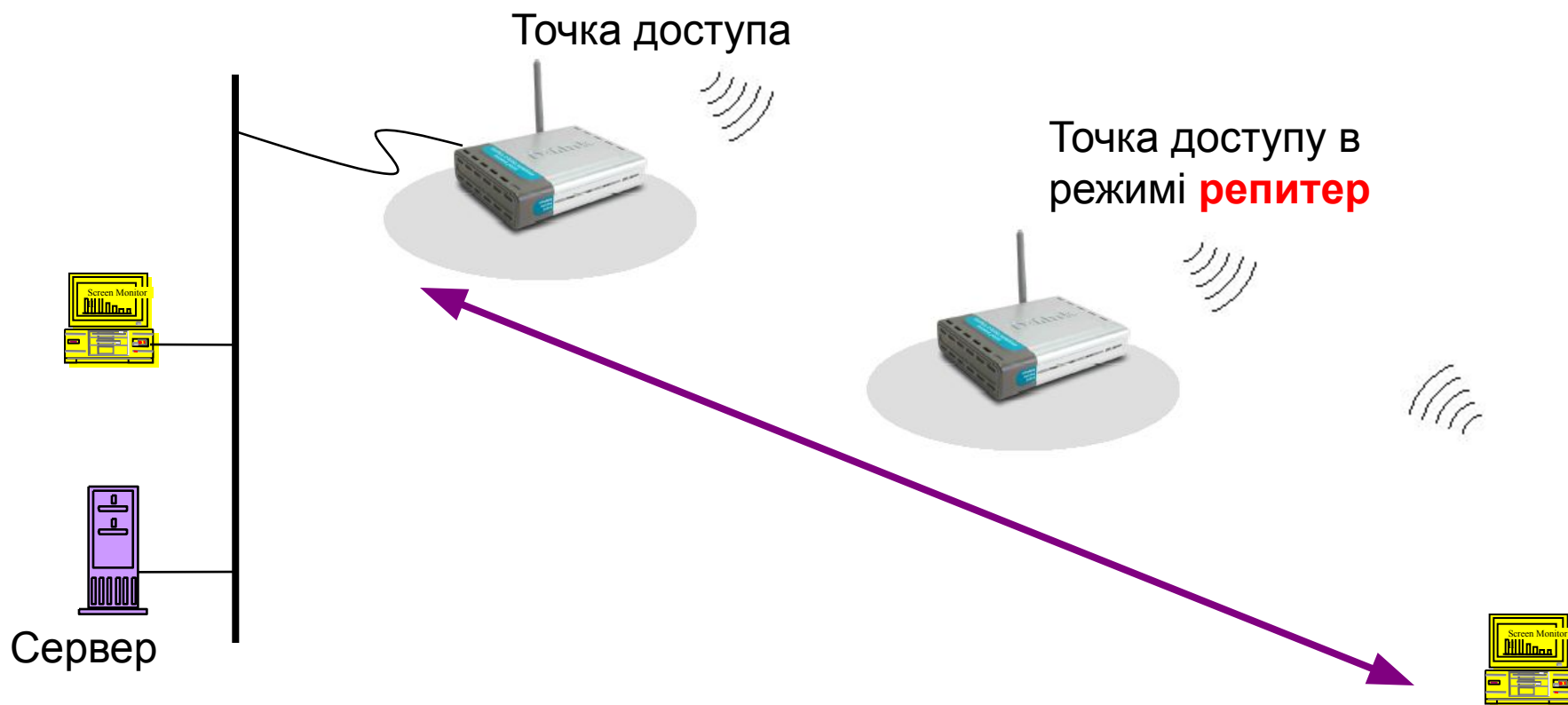
- зменшення швидкості з'єднання в WDS мережі;
- проблема сумісності обладнання різних виробників.

Зменшення швидкості з'єднання в бездротовій мережі при реалізації WDS технології пов'язано з тим, що всі точки доступу використовують один і той же канал зв'язку

Проблема WDS-мереж - це проблема сумісності обладнання різних виробників. Єдиною 100% гарантією сумісності обладнання є використання однакових точок доступу для розгортання WDS-мережі.

Додаткові режими точок доступу: як правило фірмові, тобто підтримуються не всіма постачальниками.

Режим повторювача – Repeater



Точка доступу в режимі Клієнт

Режим можна застосовувати при підключенні до бездротової мережі пристроїв з портом Ethernet, але без можливості установки бездротового адаптера.



4. Роумінг в бездротових мережах

Оскільки клієнти переміщуються в зоні дії від однієї точки доступу до іншої, роумінг дозволяє не втрачати з'єднання, а передавати його між точками доступу.

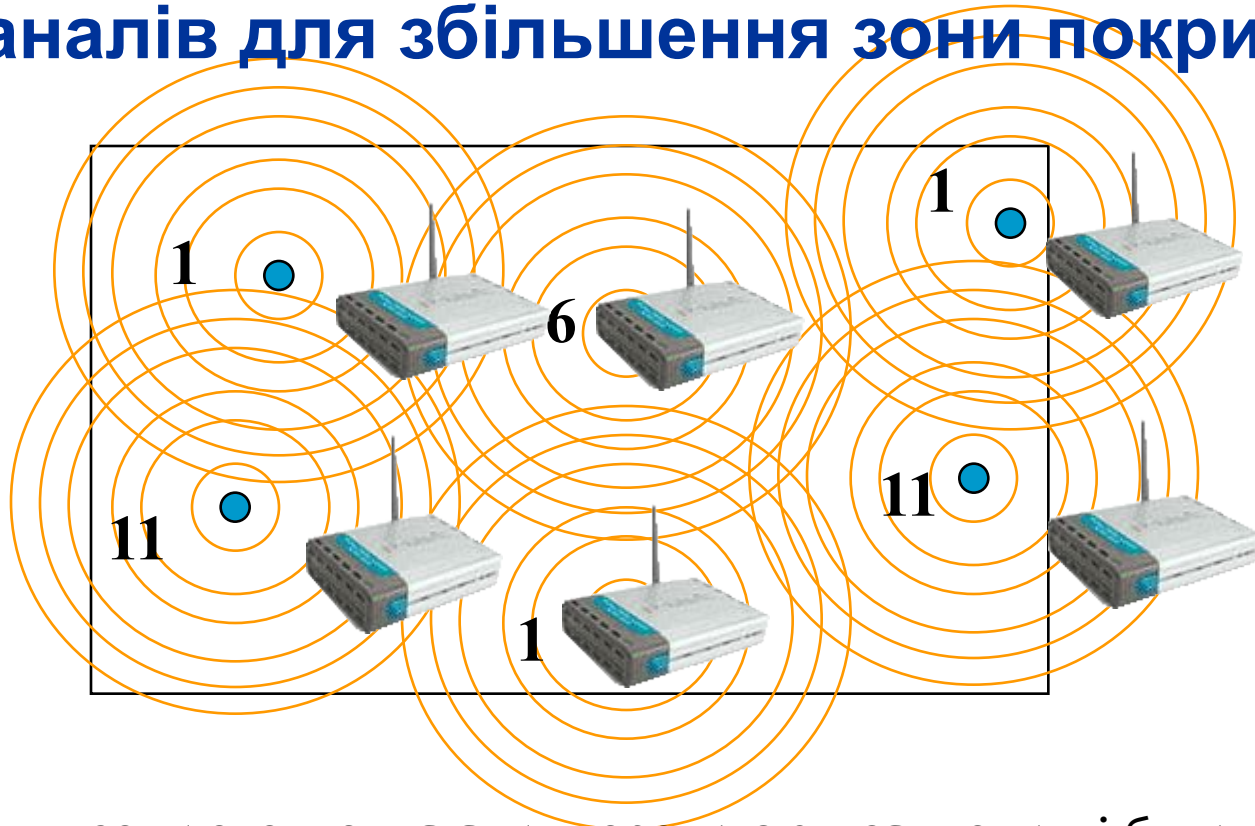
Для цього точки доступу потрібно підключити до провідної мережі.

Роумінг в бездротових мережах



Як тільки користувач переміщається від однієї точки доступу до іншої, бездротової адаптер автоматично перевстановлює з'єднання і підключається до найближчої точки для забезпечення кращої якості сигналу і продуктивності

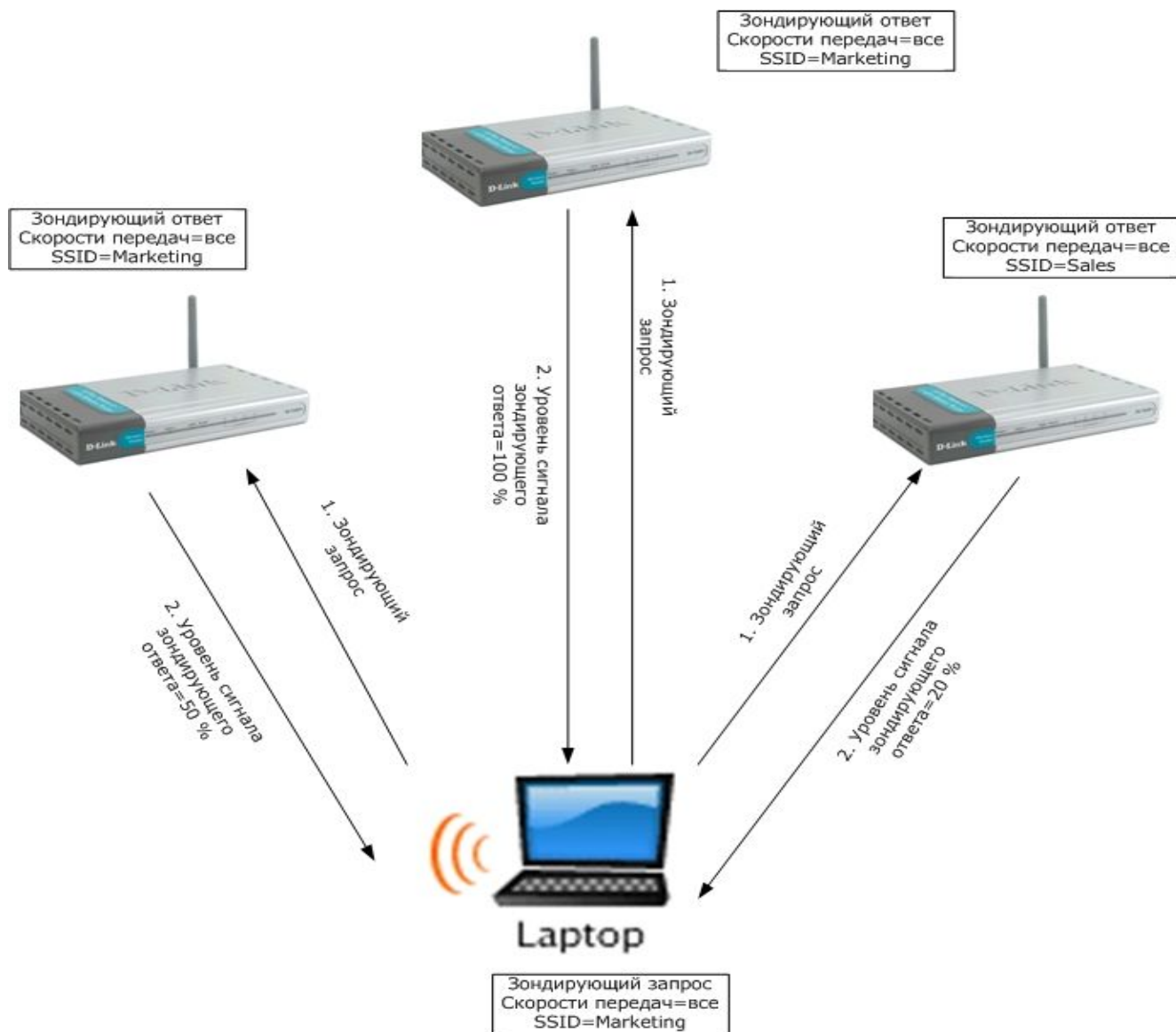
Роумінг – використання одних і тих самих каналів для збільшення зони покриття



Точки доступу, зони охоплення яких перетинаються, повинні бути налаштовані на різні канали. Але можна використовувати однакові канали на точках доступу з непересічними зонами охоплення. Таким чином, можна збільшувати загальне покриття мережі практично без обмежень!

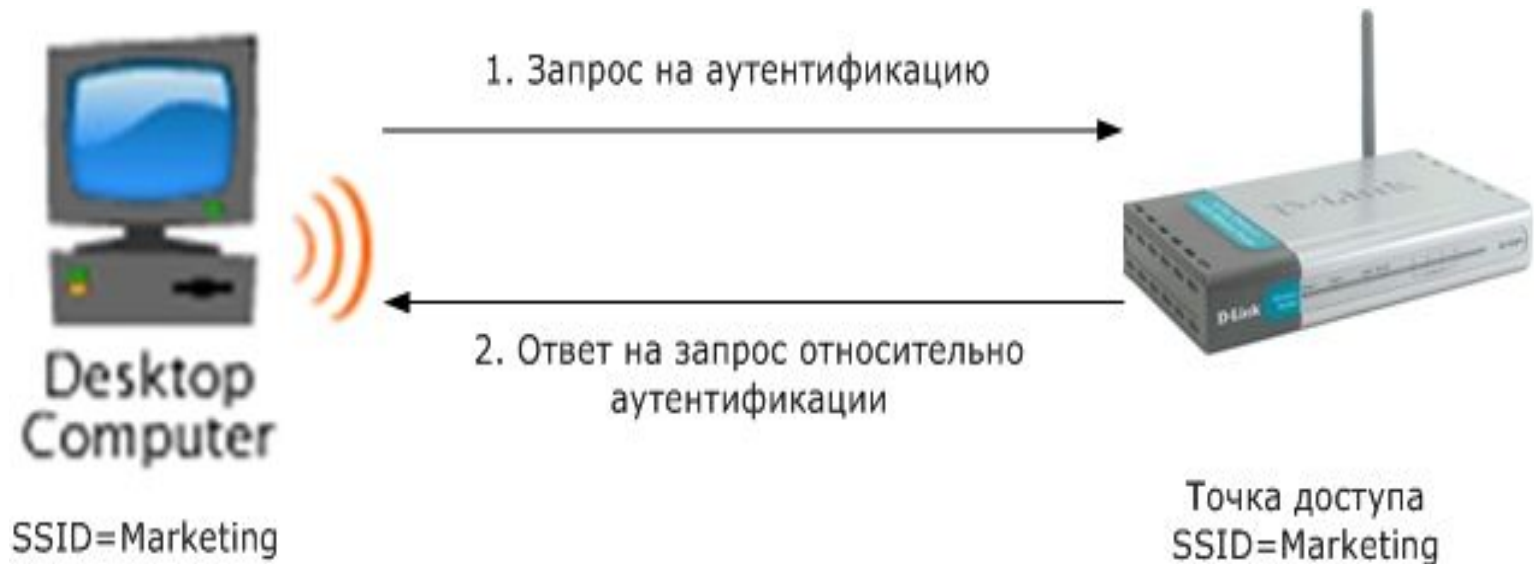
- Сигнал-маяк - "Beacon" посиляється точкою доступу кожні 100 мілісекунд
- Клієнти використовують цей маяк для оцінки якості зв'язку
- Клієнти теж можуть посилати маяк (Beacon), або пробний запит (Probe request)
- Точка доступу відповість (Probe response) або пошле маяк (Beacon)
- Грунтуючись на якості зв'язку, клієнт приймає рішення, з якою точкою доступу працювати
- Таким чином, при правильному розміщенні точок доступу на території підприємства користувачі зможуть переміщатися по ній практично без втрати доступу до мережі.

Процес зондування



Процес аутентифікації

У мережах 802.11 використовуються два види аутентифікації: відкрита аутентифікація (open authentication) і аутентифікацію з спільно використовуваним ключем (shared-key authentication).



Процес об'єднання станцій в зону обслуговування



5. Безпека в бездротових мережах

Для забезпечення безпеки в бездротових мережах використовується декілька засобів:

- Контроль за підключенням до точки доступу на основі MAC-адрес і імені мережі
- Шифрування на основі протоколу WEP (RC4)
- Контроль за доступом до середовища передачі на основі протоколу 802.1x
- Підтримка протоколів WPA2
- Налаштування VPN поверх бездротового з'єднання
- Винос бездротової мережі за міжмережевий екран, як мережі з низькою довірою

Контроль доступу

За ім'ям мережі: можна використовувати унікальний ESSID щоб уникнути несанкціонованого втручання в Вашу бездротову мережу

За MAC-адресою: Ви можете задати на точці доступу список MAC-адрес, якому Ви хочете дозволити авторизацію в Вашій групі в мережі на Вашій точці

Типи шифрування

Wired Equivalent Privacy (WEP)

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access2 (WPA2)

Wi-Fi Protected Access3 (WPA3)

Протокол 802.1x

Для аутентифікації і авторизації користувачів з подальшим наданням їм доступу до середовища передачі даних, розроблений стандарт безпеки IEEE 802.1x, який орієнтований на всі види мереж доступу, що відповідають стандартам IEEE.

Перш ніж отримати доступ до бездротової (або провідної) мережі, клієнт повинен пройти перевірку на сервері RADIUS, і тільки в разі успішної перевірки йому дозволяється доступ в неї.

Протокол Wi-Fi Protected Access – WPA 2

WPA2 визначається стандартом **IEEE 802.11i**, прийнятим в червні 2004 року, для заміни WPA.

У ньому реалізований алгоритм шифрування **CCMP** (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol - протокол блочного шифрування з кодом автентичності повідомлення і режимом зчеплення блоків і лічильника), який використовує алгоритм **AES** (Advanced Encryption Standard - симетричний алгоритм блочного шифрування), за рахунок чого WPA2 став більш захищеним, ніж попередній тип безпеки.

На відміну від TKIP, управління ключами і цілісністю повідомлень здійснюється одним компонентом, побудованим навколо AES з використанням 128-бітного ключа, 128-бітного блоку.

З 13 березня 2006 року підтримка WPA2 є обов'язковою умовою для всіх сертифікованих Wi-Fi пристроїв.

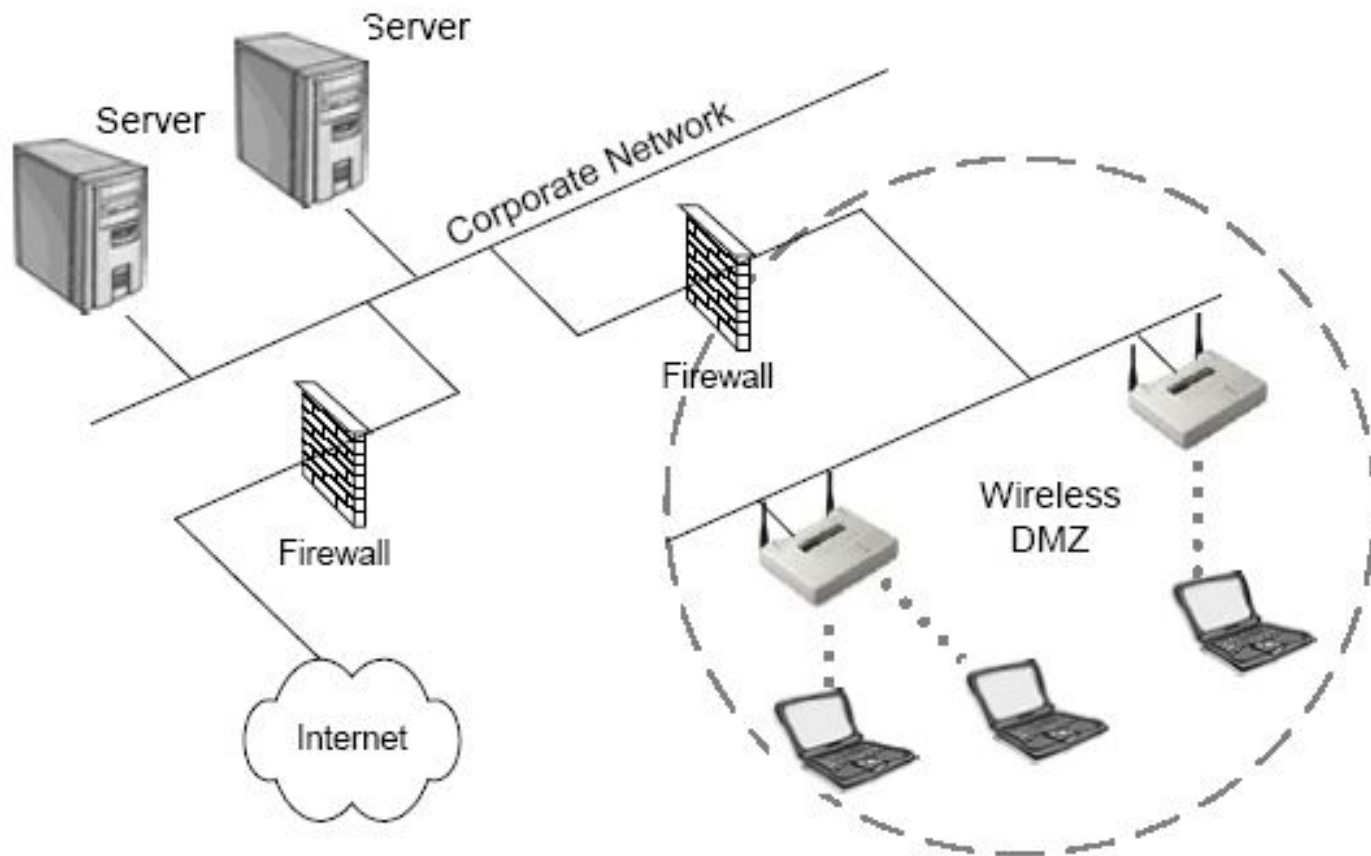
Wireless i VPN

Для додаткової безпеки ви можете налаштувати VPN поверх вашої бездротової мережі.

Аутентифікація користувачів і шифрування трафіку засобами VPN забезпечує надійний захист.

Засоби VPN працюють на мережевому рівні, транспортом може служити як провідна, так і бездротова мережа.

Захист на основі міжмережевого екрану (DFL-260/860/1600)



Розгортання і планування і бездротової мережі підприємства

При розгортанні бездротової мережі необхідно визначити щільність розміщення точок доступу для забезпечення роумінгу і безперервної зв'язку при переміщенні клієнтів

Необхідно розмістити точки доступу так, щоб:

- Збільшити зону покриття

- Забезпечити якість зв'язку і необхідну пропускну здатність

- Не допустити перетину каналів точок доступу

При плануванні бездротової мережі необхідно враховувати наступні моменти:

1. Розташування точок доступу залежить від необхідної площі охоплення і конструкції будівлі.
2. Товсті стіни, або стіни з металевими конструкціями, блокуватимуть сигнал сильніше, ніж конструкції, що пропускають світло.
3. Кількість стін і перегородок бажано звести до мінімуму - кожна стіна може скорочувати максимальну дистанцію для передачі даних на 1 - 30 м.