Wi-Fi

Wi-Fi

Wi-Fi – технология беспроводных локальных сетей

- Wi-Fi – торговая марка (принадлежит Wi-Fi Alliance)
- Стандарт IEEE 802.11

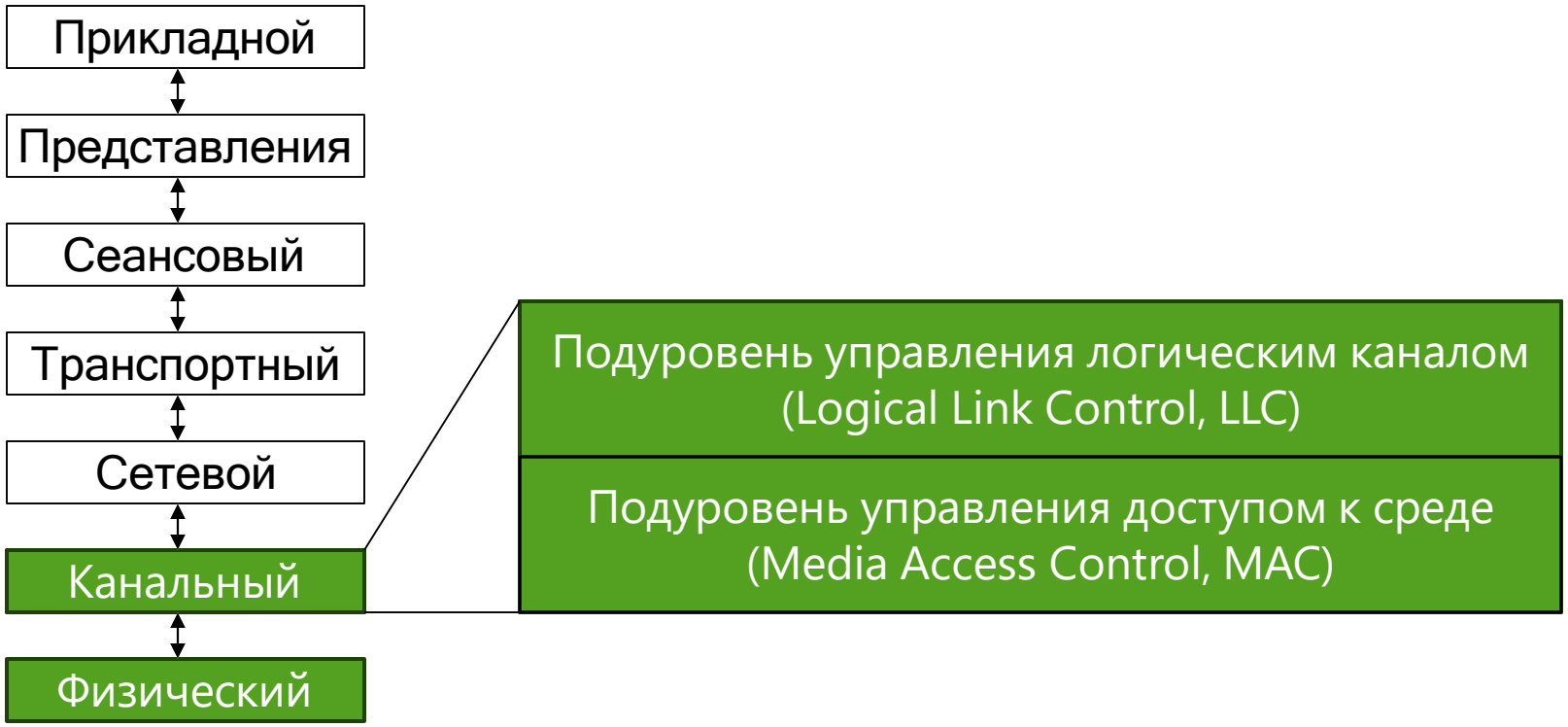
Никак не расшифровывается

- Игра слов с Hi-Fi
- Ранний вариант «Wireless Fidelity»

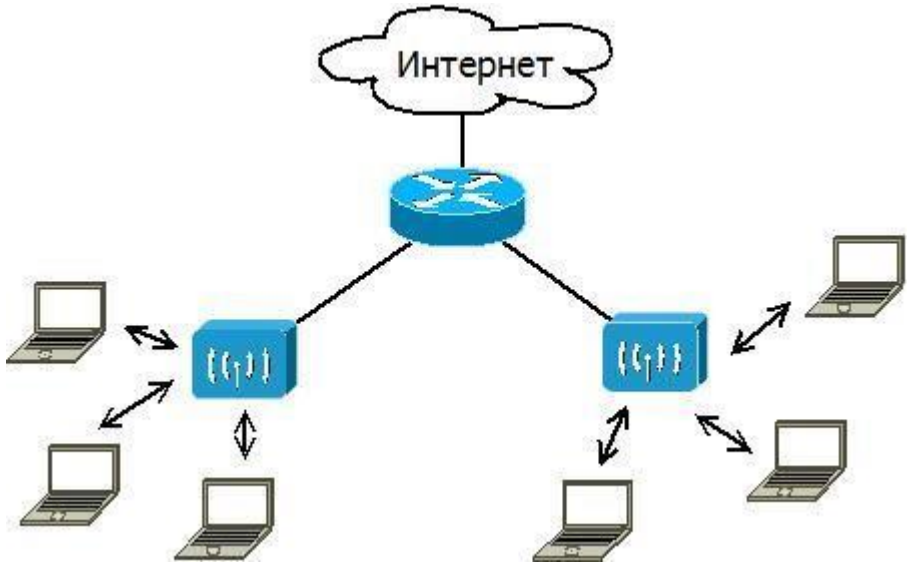
Wi-Fi Alliance проверяет оборудование на совместимость со стандартом

- Только после проверки можно использовать символ Wi-Fi
- Ethernet-оборудование не требует сертификации

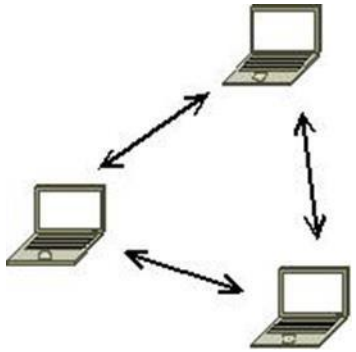
Место Wi-Fi в модели OSI



Режимы работы Wi-Fi



Инфраструктурный режим



Одноранговый режим (ad-hoc)

Wi-Fi и Ethernet

Технология Wi-Fi похожа на Ethernet

- Адресация – MAC-адреса

Разделяемая среда:

- Ethernet – кабели
- Wi-Fi – радиоэфир

Общий формат кадра уровня LLC

- Стандарт IEEE 802.2

Стандарты физического уровня Wi-Fi

Название	Год принятия	Скорость	Частота
802.11	1997	1-2 Мб/с	2,4 ГГц
802.11a	1999	54 Мб/с	5 ГГц
802.11b	1999	11 Мб/с	2,4 ГГц
802.11g	2003	54 Мб/с	2,4 ГГц
802.11n	2009	600 Мб/с	2,4 и 5 ГГц
802.11ac (Wi-Fi 5)	2014	6.77 Гб/с	5 ГГц
802.11ax (Wi-Fi 6/6E)	2019	9.6 Гбит/с	Wi-Fi 6 – 2,4 и 5 ГГц Wi-Fi 6E – 6 ГГц
802.11be (Wi-Fi 7)	2024	46 Гбит/с	2,4/5/6 ГГц

Физический уровень Wi-Fi

Инфракрасное излучение

- 802.11, устаревший метод

Электромагнитное излучение:

- 2,4 ГГц – 802.11b, 802.11g, 802.11n
- 5 ГГц – 802.11a, 802.11n, 802.11ac
- 6 ГГц – 802.11ax (Wi-Fi 6E), 802.11be

Диапазоны 2.4, 5 и 6 ГГц не требуют лицензирования:

- Можно использовать свободно
- Другие устройства также используют 2.4 и 5 ГГц и создают помехи
- 6 ГГц пока менее загружен, используется только современными устройствами

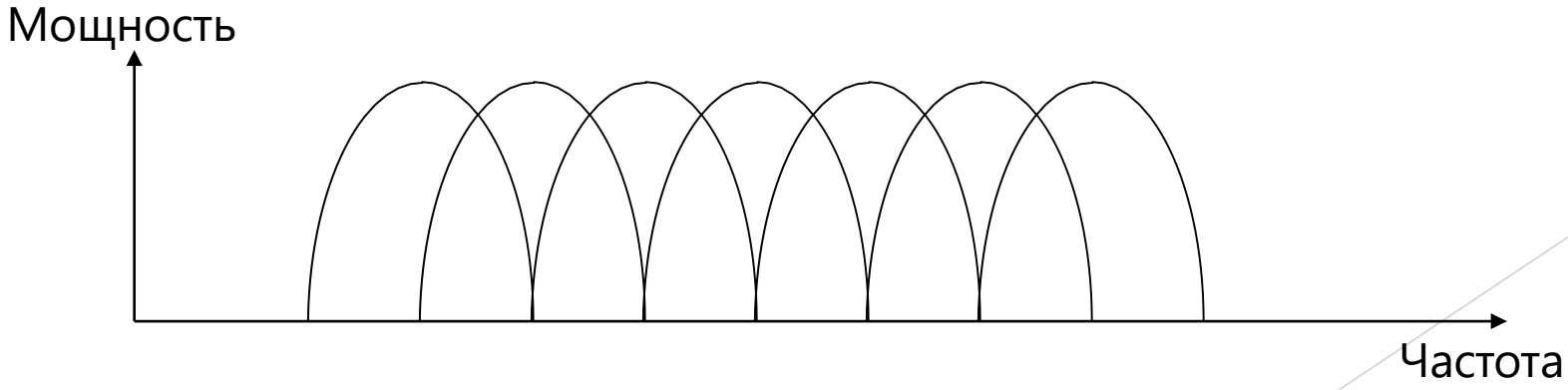
Представление сигнала

Современные стандарты Wi-Fi используют метод **OFDM**:

- Orthogonal Frequency Division Multiplexing
- Мультиплексирование с ортогональным частотным разделением
- Данные передаются параллельно на разных частотах

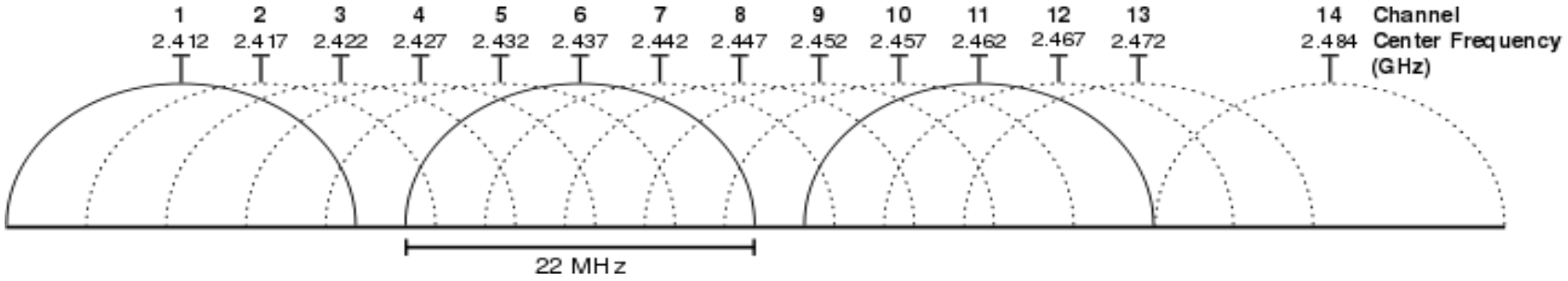
В Wi-Fi 6 и Wi-Fi 7 используется расширение **OFDMA**:

• Поднесущие делятся между несколькими устройствами одновременно



Каналы в диапазоне 2.4 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

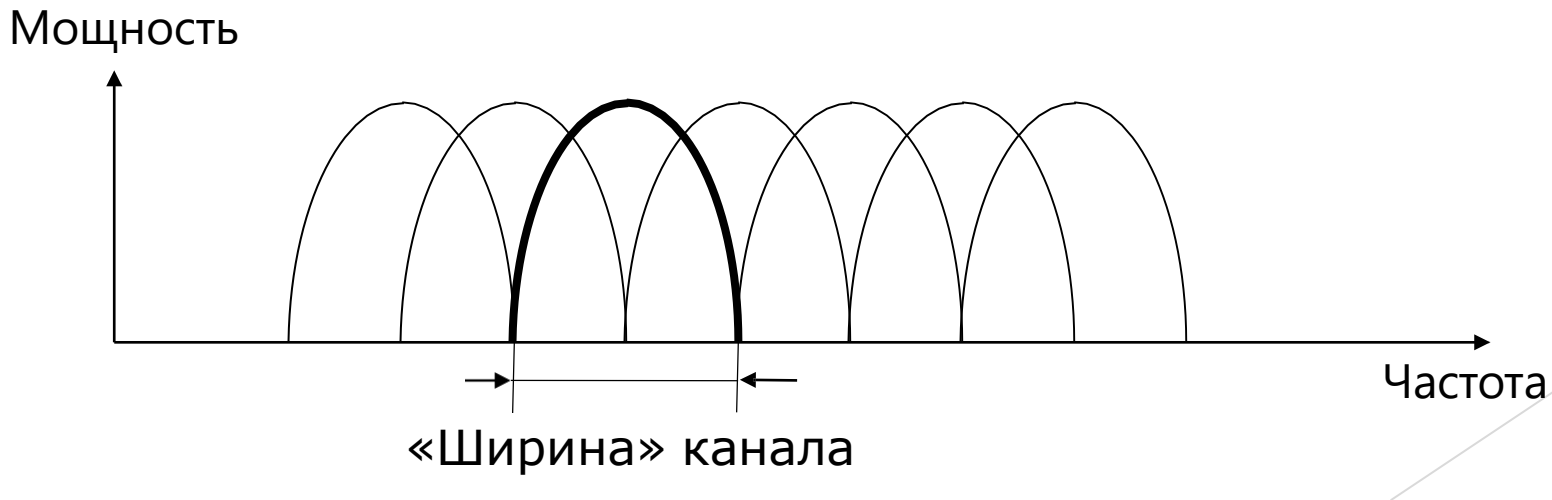


Ширина канала

Используемая ширина канала:

- 20 МГц – первые стандарты Wi-Fi
- 40 МГц – 802.11n
- 80 МГц – 802.11ac, 802.11ax
- 160 МГц – 802.11ac, 802.11ax
- 320 МГц – 802.11be

Широкие каналы → выше скорость, ниже устойчивость, больше риск помех



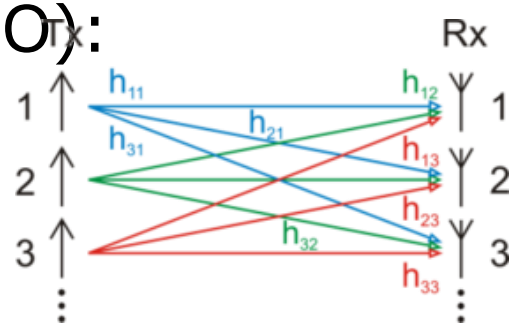
Пространственный поток

Использование нескольких антенн для передачи и приема сигнала:

- Стандарты 802.11n, 802.11ac, 802.11ax, 802.11be
- Пространственный поток – сигнал, распространяющийся от одной антенны до другой

Multiple Input Multiple Output (MIMO):

- Метод кодирования сигнала для использования нескольких антенн



Адаптация скорости

Wi-Fi позволяет менять скорость при разном качестве сигнала:

- Высокое качество – скорость увеличивается
- Низкое качество – скорость уменьшается

Адаптация скорости реализуется засчет изменения параметров скорости (MCS):

- Ширины используемых каналов
- Методов модуляции
- Интервала между сигналами
- количество пространственных потоков

Адаптация скорости

На примере IEEE 802.11ac:

Theoretical throughput for single Spatial Stream (in Mbit/s)										
MCS index	Modulation type	Coding rate	20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
			800 ns GI	400 ns GI	800 ns GI	400 ns GI	800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	BPSK	1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65
1	QPSK	1/2	13	14.4	27	30	58.5	65	117	130
2	QPSK	3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195
3	16-QAM	1/2	26	28.9	54	60	117	130	234	260
4	16-QAM	3/4	39	43.3	81	90	175.5	195	351	390
5	64-QAM	2/3	52	57.8	108	120	234	260	468	520
6	64-QAM	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585
7	64-QAM	5/6	65	72.2	135	150	292.5	325	585	650
8	256-QAM	3/4	78	86.7	162	180	351	390	702	780
9	256-QAM	5/6	N/A	N/A	180	200	390	433.3	780	866.7

Канальный уровень Wi-Fi

- Одинаковый для разных стандартов физического уровня

Wi-Fi использует разделяемую среду передачи данных

- Возможны коллизии
- Необходимо разграничивать доступ к разделяемой среде

Особенности беспроводной среды

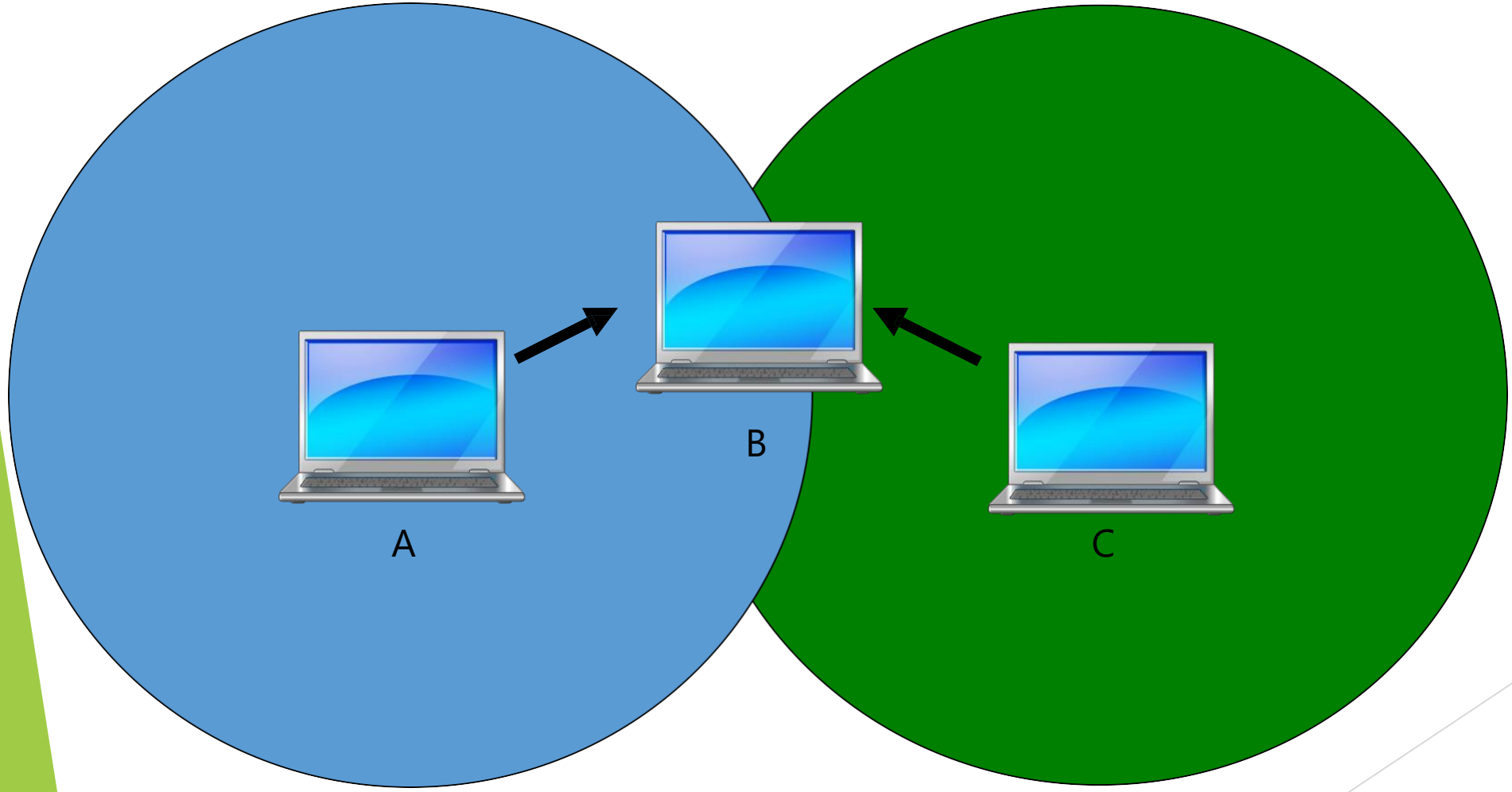
Вероятность ошибки передачи выше, чем в проводной среде

Мощность передаваемого сигнала намного выше, чем принимаемого

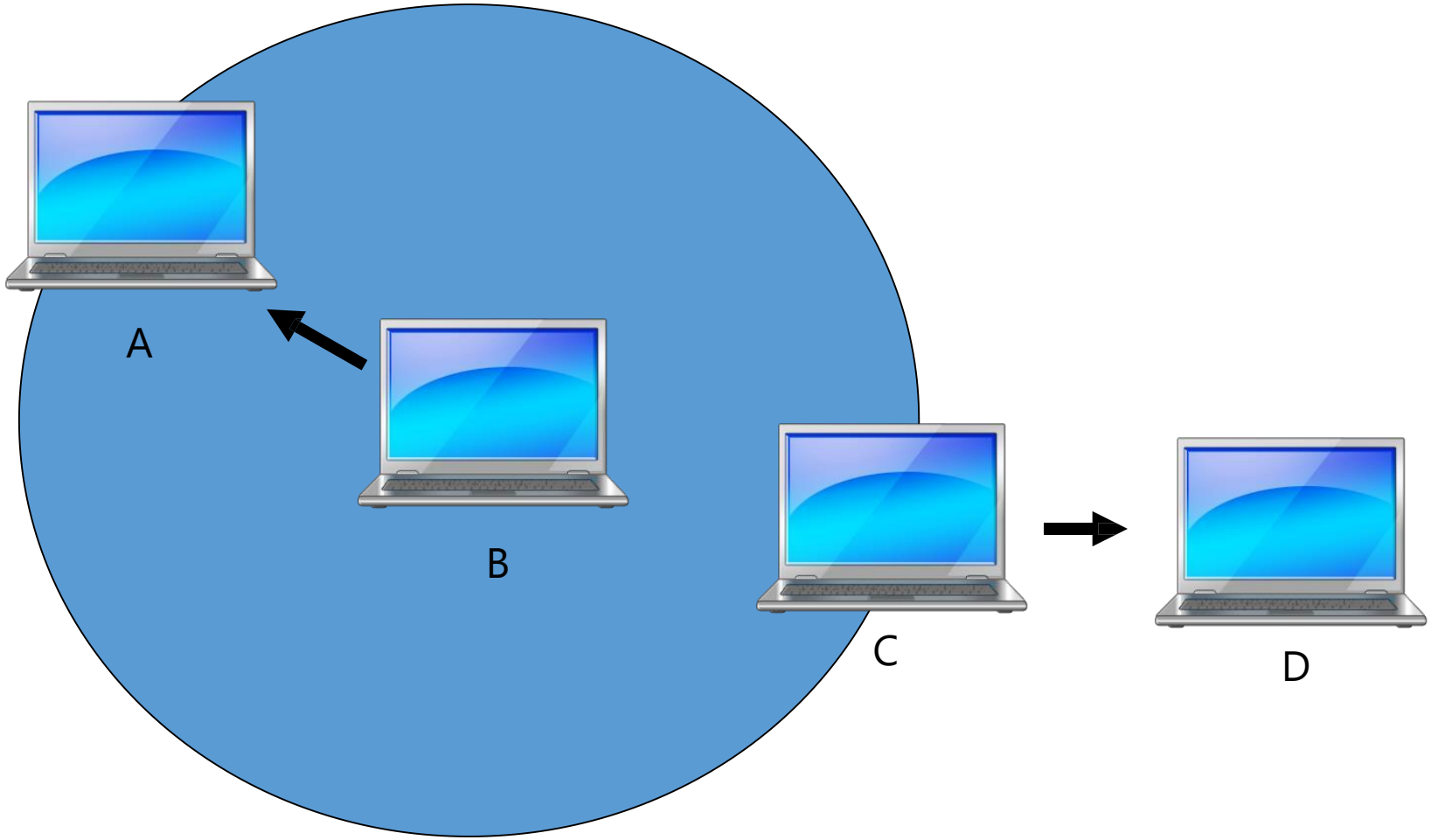
Ограниченный диапазон распространения сигнала – не все компьютеры в сети получают данные

- Проблема скрытой станции
- Проблема засвеченной станции

Проблема «скрытой» станции



Проблема «засвеченной» станции



Механизм подтверждения ACK

Из-за высокой вероятности ошибок в радиоэфире Wi-Fi использует подтверждение доставки кадров.

- Отправитель передаёт кадр и ожидает подтверждение ACK от получателя.
- Если подтверждение не получено в течение тайм-аута, кадр считается потерянным и отправляется повторно.
- Механизм ACK повышает надёжность Wi-Fi, но увеличивает задержки при коллизиях и помехах.

Обнаружение коллизий

Ethernet

- Компьютер передает и одновременно принимает сигнал
- Jam-последовательность для усугубления коллизии

Wi-Fi

- Передаваемый сигнал намного мощнее принимаемого
- Проблемы скрытой и засвеченной станции
- Сигнал о коллизии может не дойти до всех компьютеров

Коллизии в Wi-Fi

- Обнаружение коллизии в Wi-Fi
  - Отсутствие подтверждения получения кадра
- Коллизии в Ethernet дешевы
  - Обнаруживаются сразу после возникновения
  - Все компьютеры останавливают передачу данных
- Коллизия в Wi-Fi обходится очень дорого
  - Временные затраты: передача кадра, тайм-аут ожидания подтверждения

Метод доступа к среде

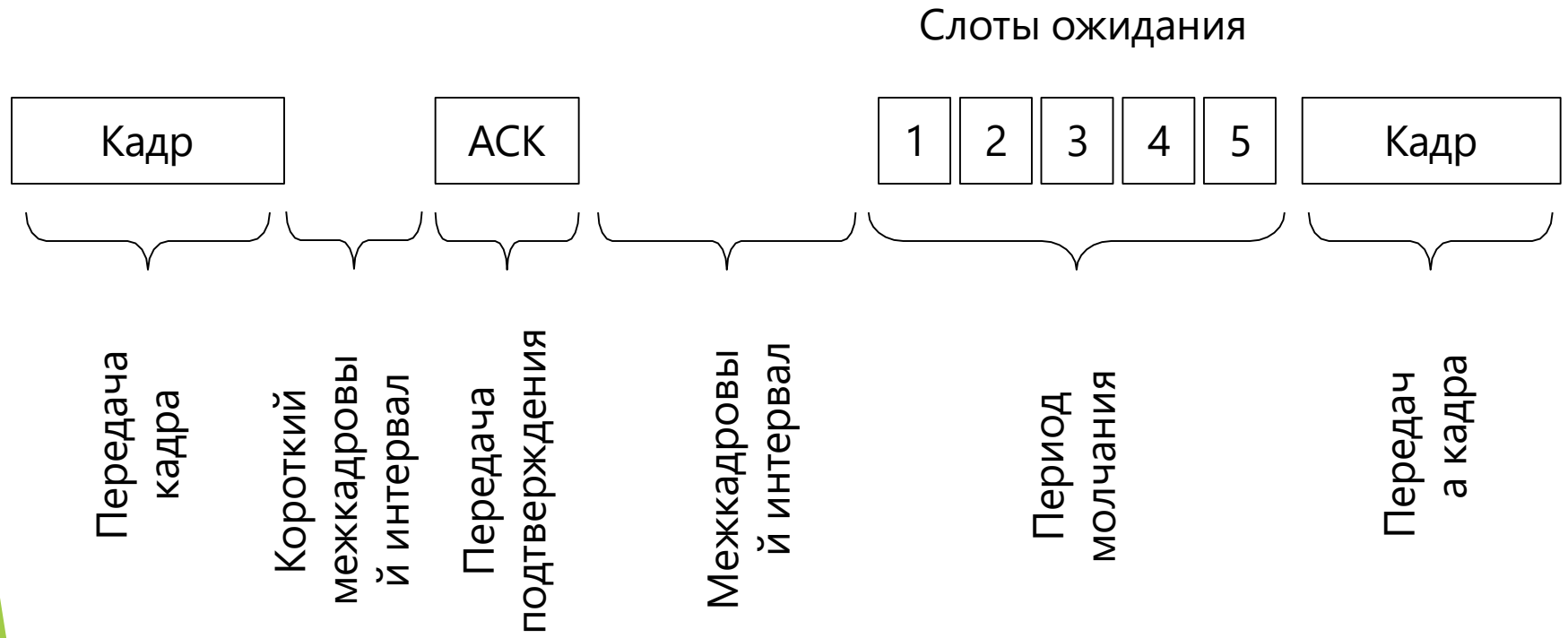
Метод доступа к среде в Ethernet:

- CSMA/CD - Множественный доступ с прослушиванием несущей частоты и распознаванием коллизий

Метод доступа к среде в Wi-Fi:

- CSMA/CA - Множественный доступ с прослушиванием несущей частоты с предотвращением коллизий

Модель CSMA/CA



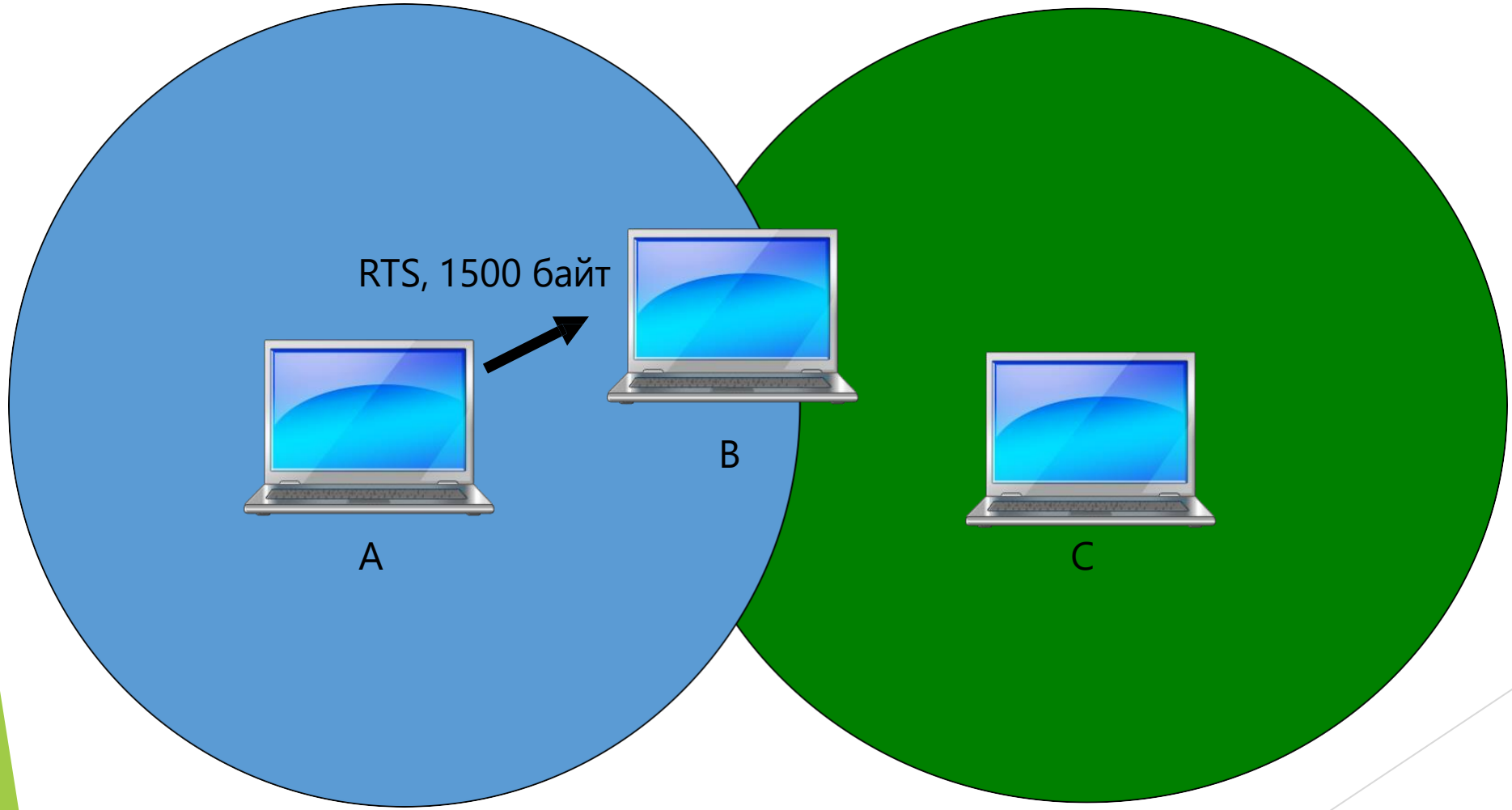
Протокол MACA

- Метод доступа CSMA/CA не решает проблему скрытой и засвеченной станции
  - Теоретически это так
  - На практике CSMA/CA почти всегда достаточно
- Протокол Multiple Access with Collision Avoidance (MACA)
  - Предназначен для решения проблем скрытой и засвеченной станции
  - Может использоваться в Wi-Fi (необязательно)

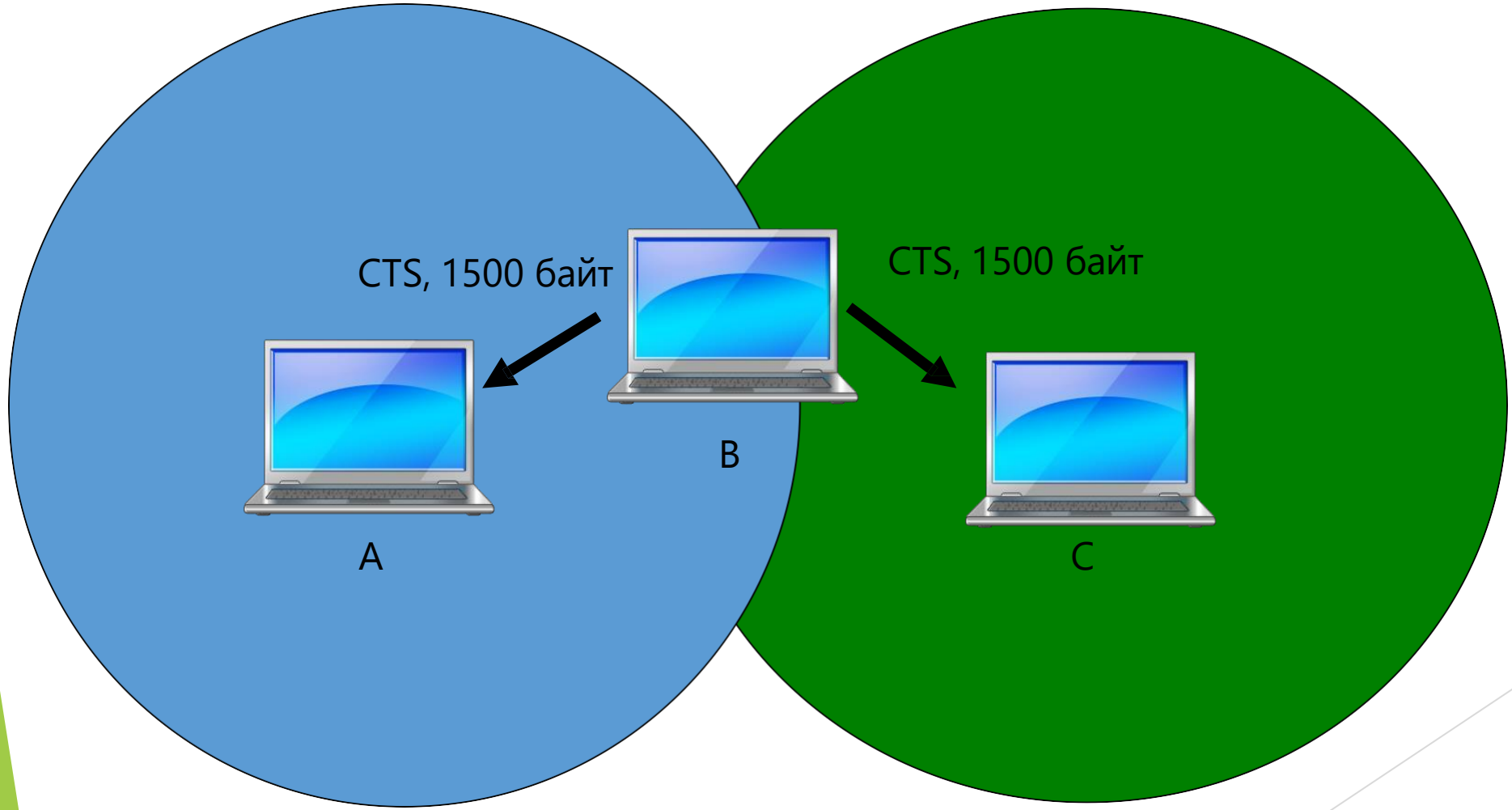
Протокол MACA

- Перед отправкой данных компьютер передает управляющее сообщение:
  - Request To Send (RTS)
  - Включает размер сообщения с данными
- Принимающий компьютер отвечает сообщением:
  - Clear To Send (CTS)
  - Также включает размер ожидаемого сообщения
- Компьютеры, увидевшее CTS, ждут:
  - Время на передачу данных (размер данных в CTS)
  - Время на передачу подтверждения

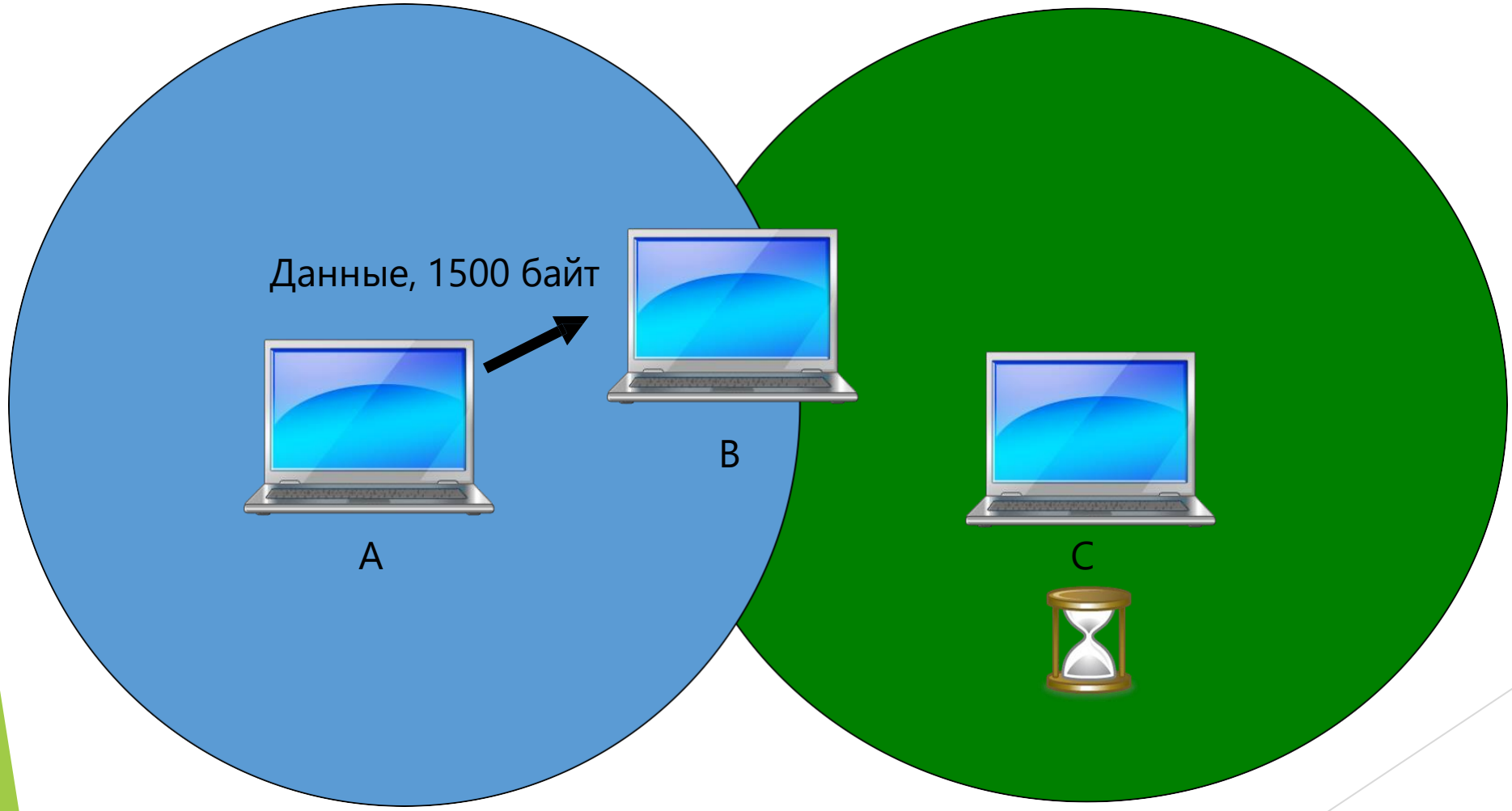
Протокол MACA и скрытая станция



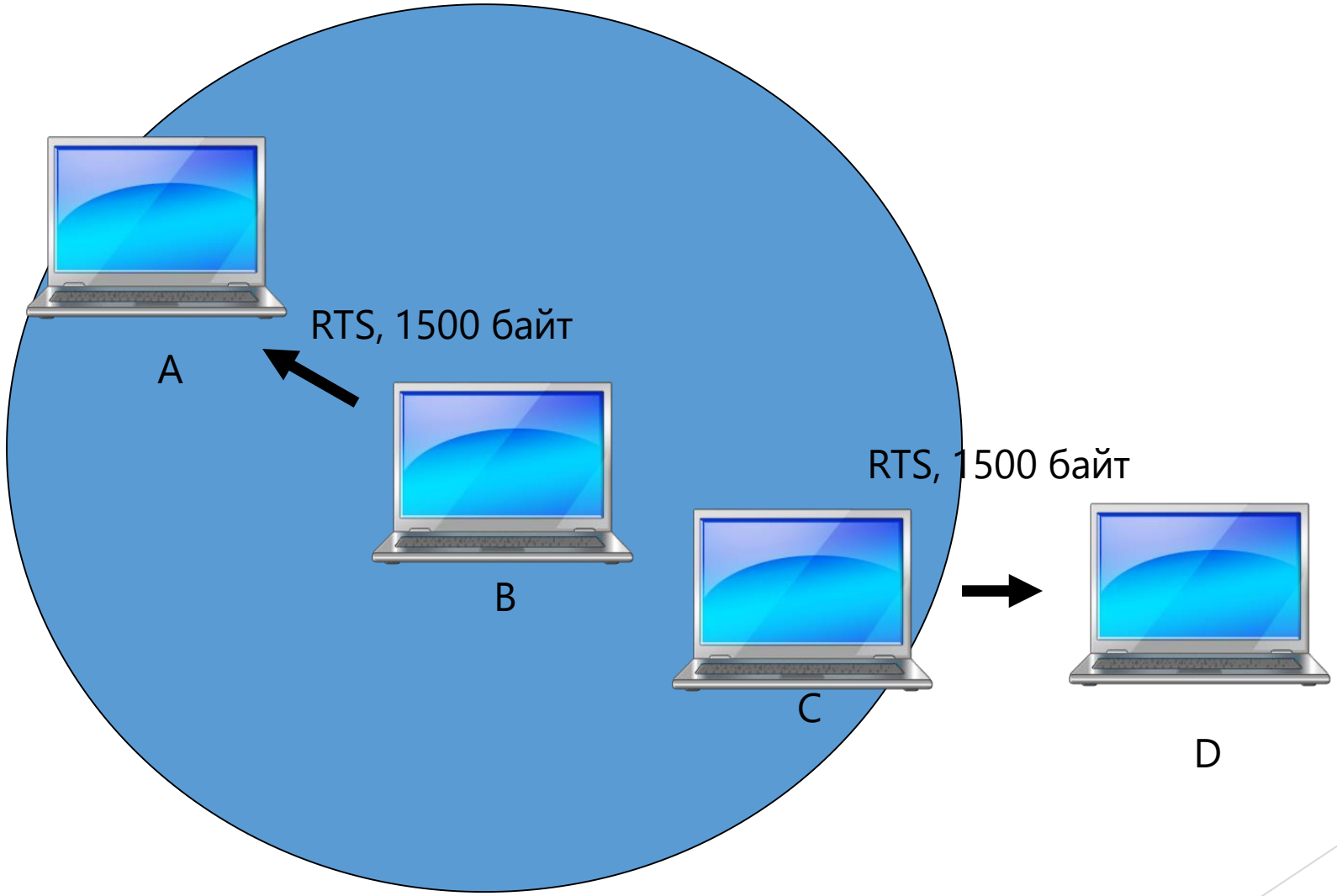
Протокол MACA и скрытая станция



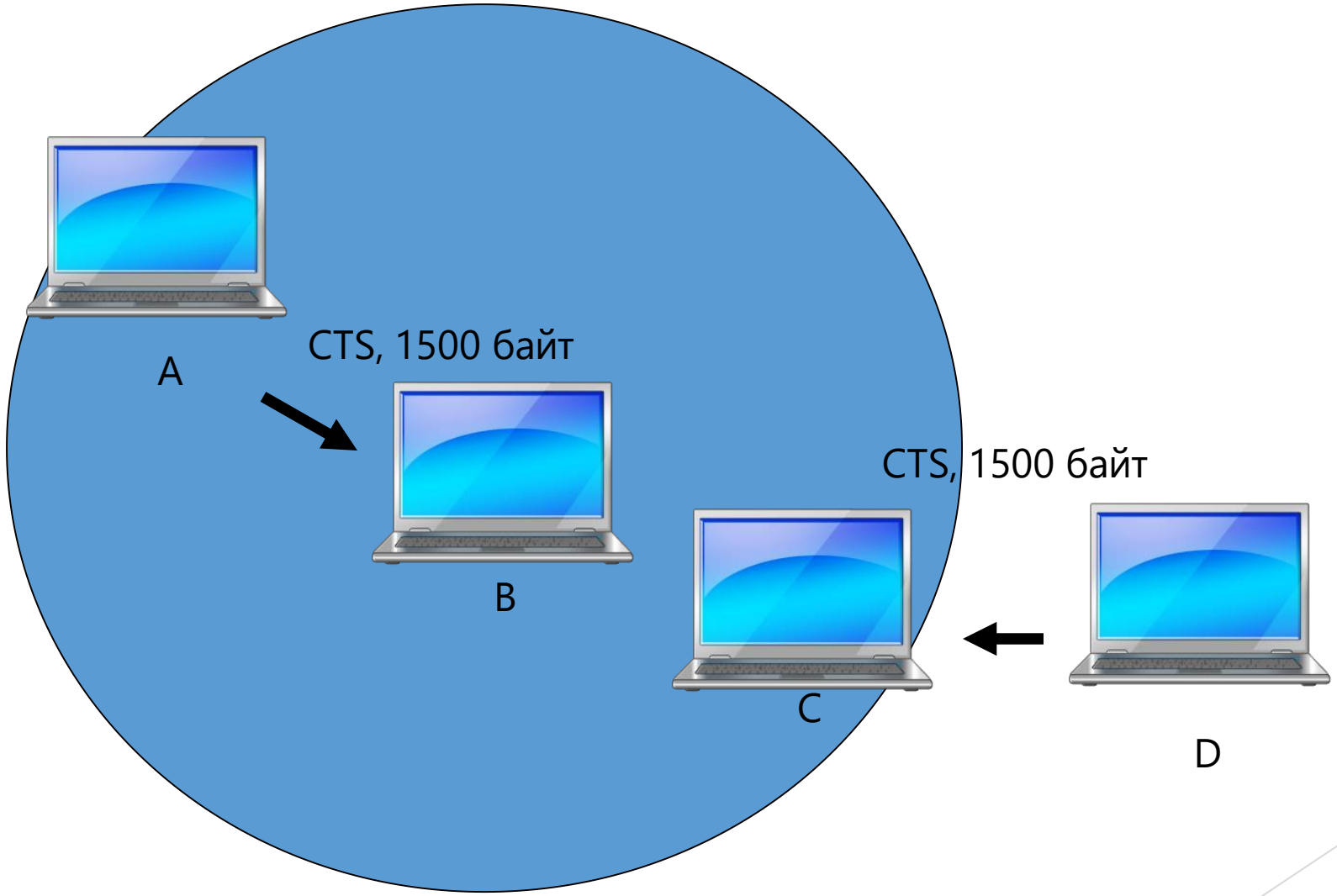
Протокол MACA и скрытая станция



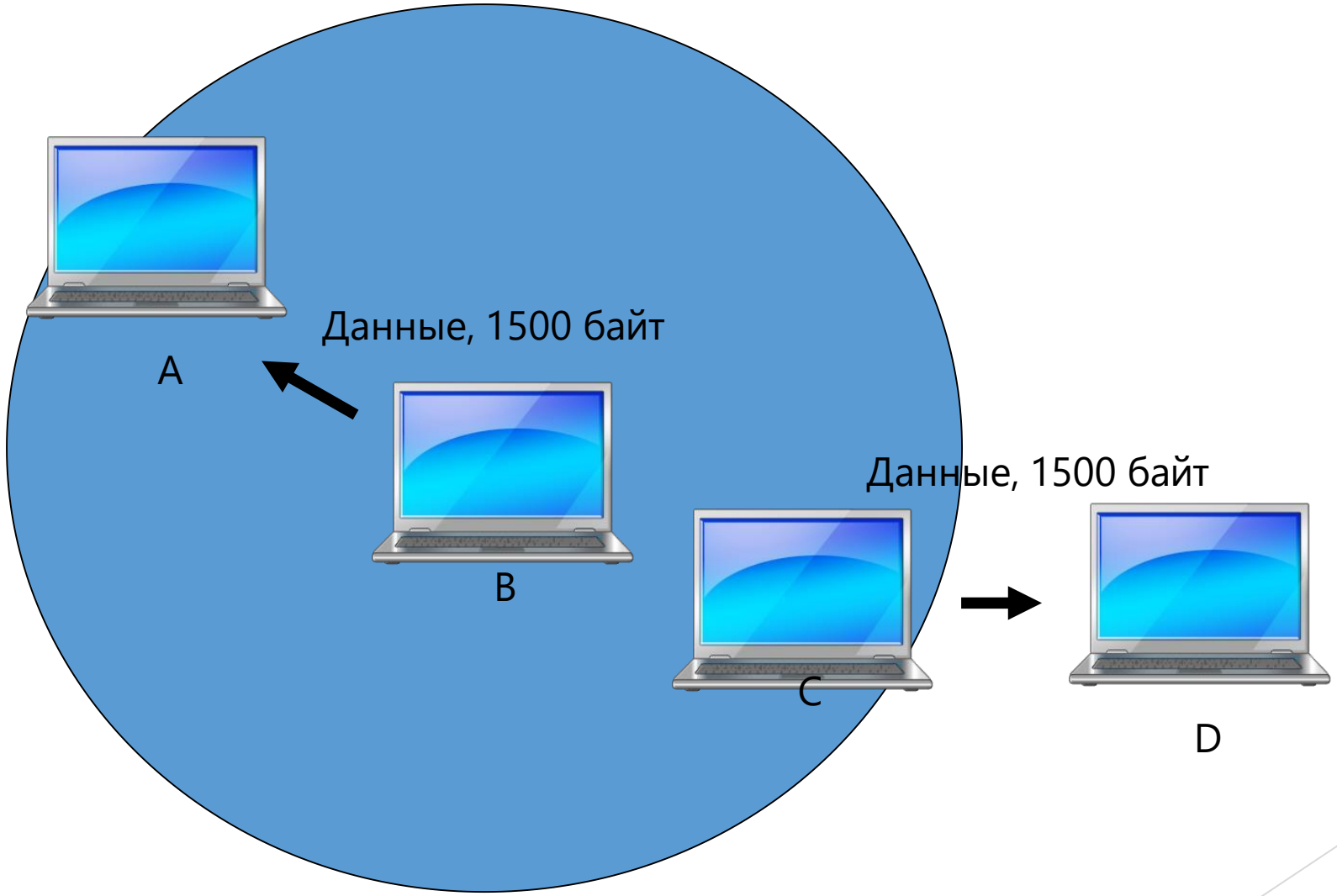
Протокол MACA и засвеченная станция



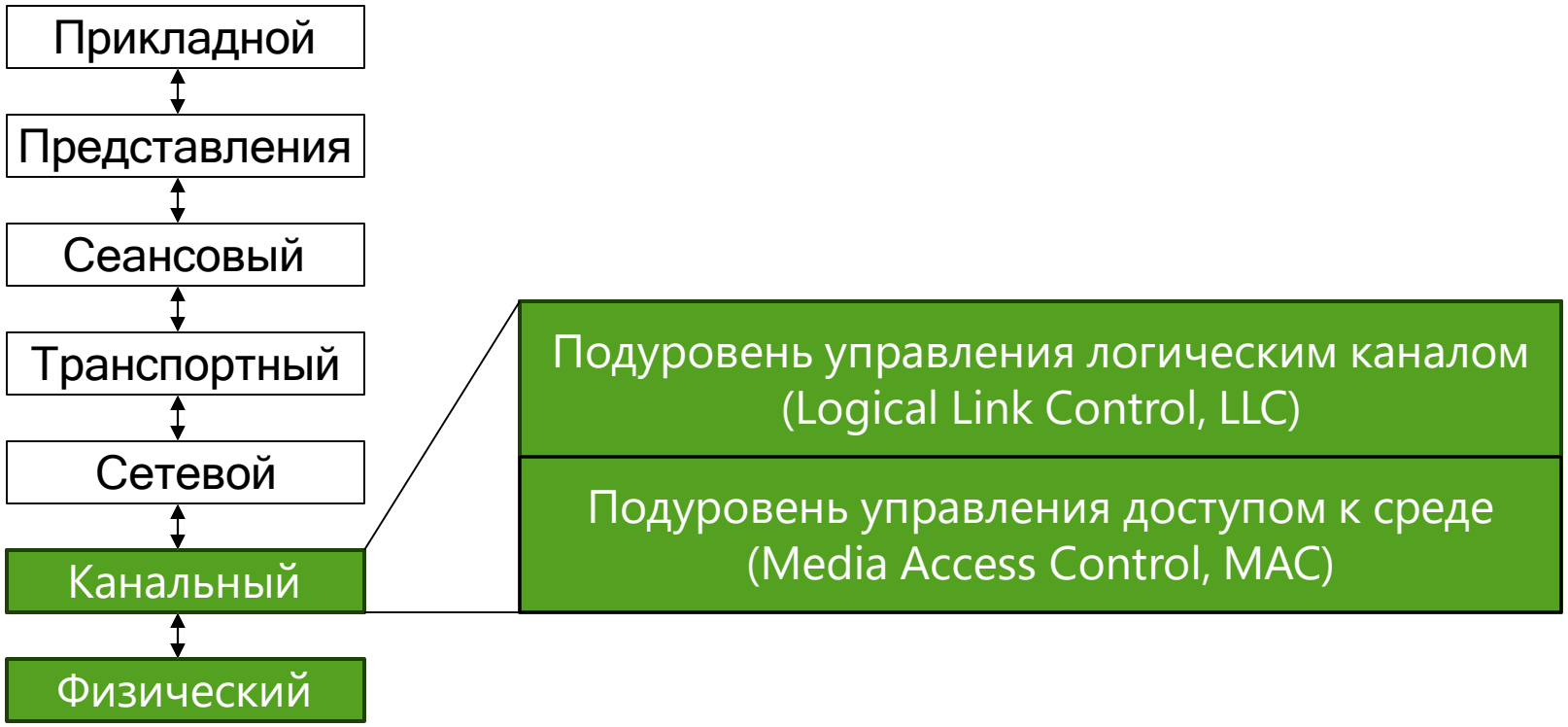
Протокол MACA и засвеченная станция



Протокол MACA и засвеченная станция



Место Wi-Fi в модели OSI



Формат кадра Wi-Fi уровня MAC

2 байта	2 байта	6 байт	6 байт	6 байт	2 байта	6 байт	0-2304 байт	4 байта
Управление кадром	Длительность	Адрес 1	Адрес 2	Адрес 3	Управление очередностью	Адрес 4	Тело кадра	Контрольная сумма

Для сравнения, формат кадра Ethernet выглядит следующим образом:

6 байт	6 байт	2 байта	46-1500 байт	4 байта
Адрес получателя	Адрес отправителя	Тип	Данные	Контрольная сумма

Заголовок

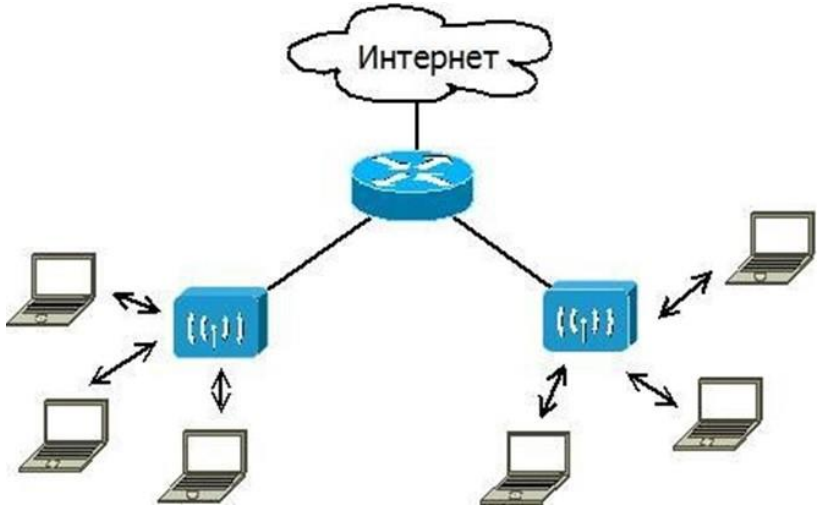
Концевик

Формат кадра Wi-Fi уровня MAC

Почему в кадре Wi-Fi четыре адреса?

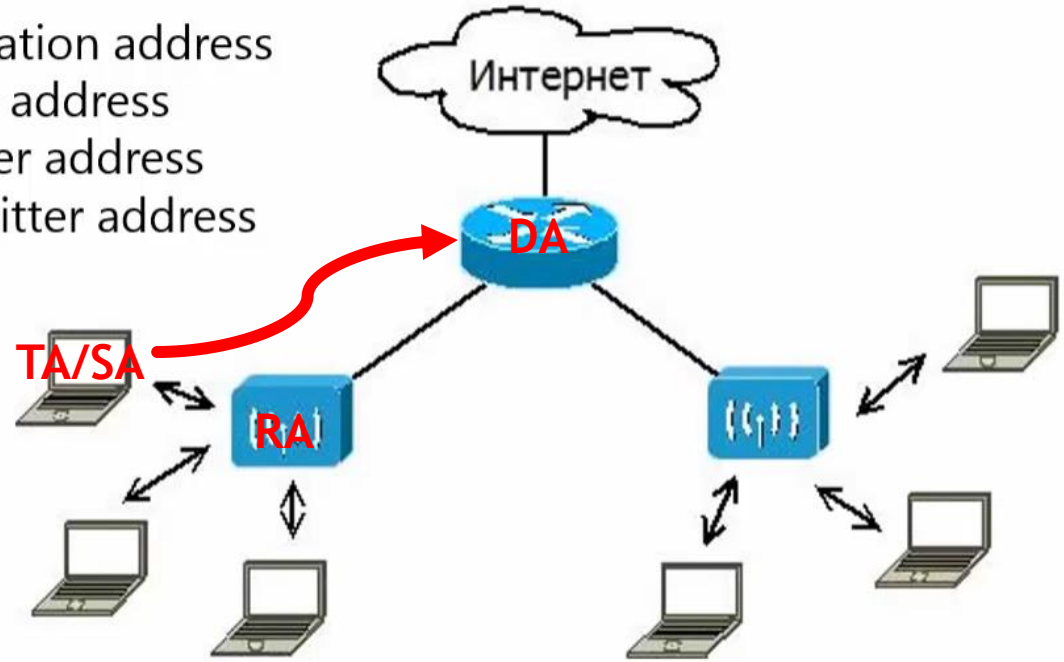
Назначение адресов:

- Адрес получателя(Destination Address)
- Адрес отправителя(Source Address)
- Адрес точки доступа получателя(Receiver Address)
- Адрес точки доступа отправителя(Transmitter Address)



Передача кадра в распределительную систему

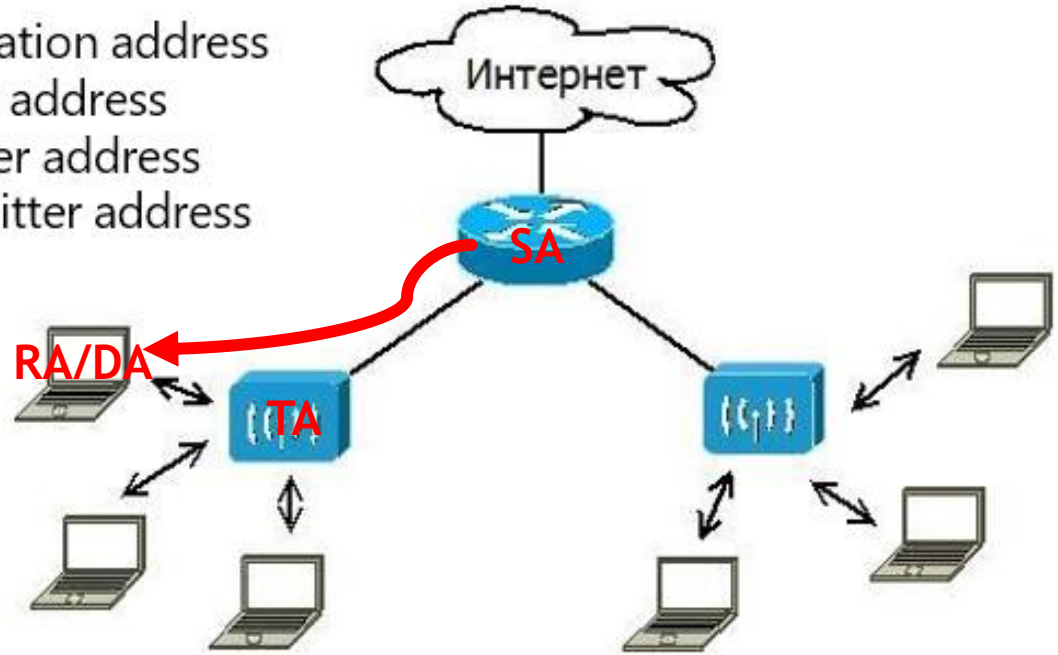
DA — Destination address
SA — Source address
RA — Receiver address
TA — Transmitter address



Адрес 1	Адрес 2	Адрес 3
RA	TA/SA	DA

Передача кадра от распределительной системы

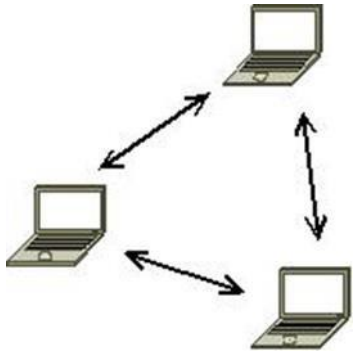
DA — Destination address
SA — Source address
RA — Receiver address
TA — Transmitter address



Адрес 1	Адрес 2	Адрес 3
RA/DA	TA	SA

Передача кадра в одноранговом режиме

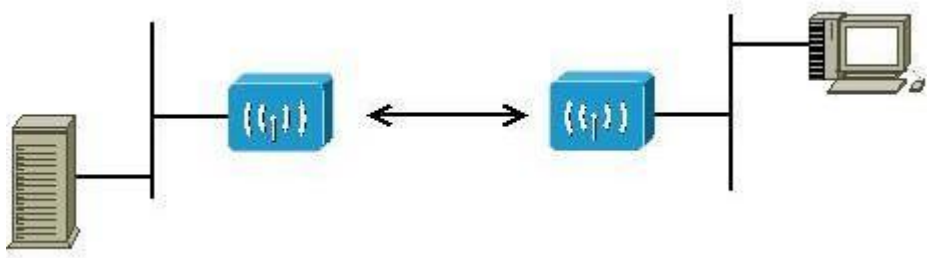
DA — Destination address
SA — Source address
RA — Receiver address
TA — Transmitter address



Адрес 1	Адрес 2	Адрес 3
RA/DA	TA/SA	Идентификатор сети (BSSID)

Беспроводной мост

DA — Destination address
SA — Source address
RA — Receiver address
TA — Transmitter address



Адрес 1	Адрес 2	Адрес 3	Адрес 4
RA	TA	DA	SA

Формат кадра Wi-Fi уровня MAC

2 байта	2 байта	6 байт	6 байт	6 байт	2 байта	6 байт	0-2304 байт	4 байта
Управление кадром	Длительность	Адрес 1	Адрес 2	Адрес 3	Управление очередностью	Адрес 4	Тело кадра	Контрольная сумма

Для сравнения, формат кадра Ethernet выглядит следующим образом:

6 байт	6 байт	2 байта	46-1500 байт	4 байта
Адрес получателя	Адрес отправителя	Тип	Данные	Контрольная сумма

Заголовок

Концевик

Формат кадра Wi-Fi уровня MAC

2 байта	2 байта	6 байт	6 байт	6 байт	2 байта	6 байт	0-2304 байт	4 байта
Управление кадром	Длительность	Адрес 1	Адрес 2	Адрес 3	Управление очередностью	Адрес 4	Тело кадра	Контрольная сумма

2 бита	2 бита	4 бита	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит
Версия протокола	Тип	Подтип	To DS	From DS	MF	RT	Power Mgmt	MD	Protection Frame	Order

Типы кадров в Wi-Fi

Кадры данных
- Передача данных

Кадры контроля (control frames)
- Служебные кадры
- RTS, CTS, ACK

Кадры управления (management frames)
- Реализация сервисов Wi-Fi
- Примеры: ассоциация с точкой доступа

Формат кадра Wi-Fi уровня MAC

2 байта	2 байта	6 байт	6 байт	6 байт	2 байта	6 байт	0-2304 байт	4 байта
Управление кадром	Длительность	Адрес 1	Адрес 2	Адрес 3	Управление очередностью	Адрес 4	Тело кадра	Контрольная сумма

2 бита	2 бита	4 бита	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит
Версия протокола	Тип	Подтип	To DS	From DS	MF	RT	Power Mgmt	MD	Protection Frame	Order

Передача кадров

Ошибки при передаче случаются часто

- 1 ошибка на 1000 байт
- Длинные кадры нужно разбить на фрагменты менее 1000 байт
- Скорость упадет, но данные будут передаваться

Поле MF (More Fragments)

Поле «Управление очередностью»

- Номер последовательности (Sequence Number)
- Номер фрагмента (Fragment Number)

Фрагментация

2 байта	2 байта	6 байт	6 байт	6 байт	2 байта	6 байт	0-2304 байт	4 байта
Управление кадром	Длительность	Адрес 1	Адрес 2	Адрес 3	Управление очередностью	Адрес 4	Тело кадра	Контрольная сумма

2 бита	2 бита	4 бита	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит
Версия протокола	Тип	Подтип	To DS	From DS	MF	RT	Power Mgmt	MD	Protection Frame	Order

Фрагментация в Wi-Fi

1500 байт

Номер последовательности: 39876
Номер фрагмента: 1
MF: 1

Номер последовательности: 39876
Номер фрагмента: 2
MF: 1

Номер последовательности: 39876
Номер фрагмента: 3
MF: 0

Формат кадра Wi-Fi уровня MAC

2 байта	2 байта	6 байт	6 байт	6 байт	2 байта	6 байт	0-2304 байт	4 байта
Управление кадром	Длительность	Адрес 1	Адрес 2	Адрес 3	Управление очередностью	Адрес 4	Тело кадра	Контрольная сумма

2 бита	2 бита	4 бита	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит
Версия протокола	Тип	Подтип	To DS	From DS	MR	RT	Power Mgmt	MD	Protection Frame	Order

Управление питанием

Wi-Fi часто используется в мобильных устройствах

- Очень важно экономить электроэнергию чтобы продлить срок работы батареи

Стандарт IEEE 802.11 PSM

- Режимы работы станции: активный и спящий
- В спящем режиме станция не принимает и не передает данные
- Точка доступа записывает кадры для «спящей» станции в буфер
- «Спящая» станция регулярно просыпается и читает все кадры от точки доступа
- Передавать кадры станция может в любое время

Формат кадра Wi-Fi уровня MAC

2 байта	2 байта	6 байт	6 байт	6 байт	2 байта	6 байт	0-2304 байт	4 байта
Управление кадром	Длительность	Адрес 1	Адрес 2	Адрес 3	Управление очередностью	Адрес 4	Тело кадра	Контрольная сумма

2 бита	2 бита	4 бита	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит	1 бит
Версия протокола	Тип	Подтип	To DS	From DS	MR	RT	Power Mgmt	MD	Protection Frame	Order

Сервисы Wi-Fi

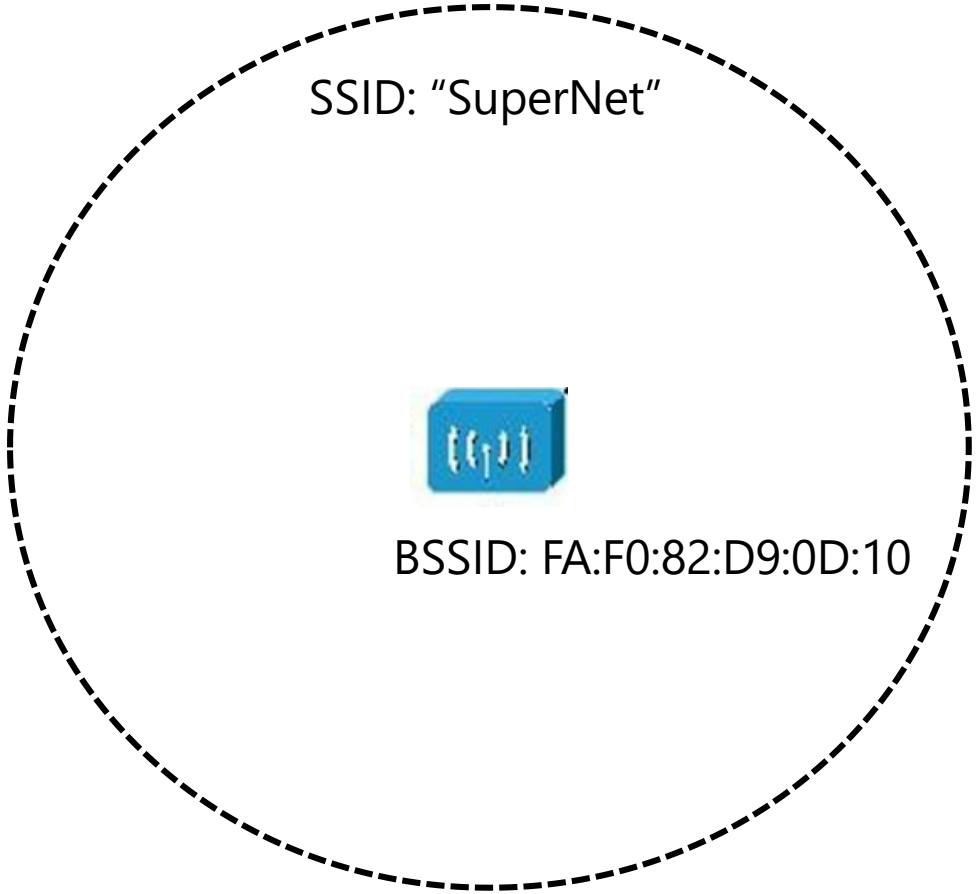
Сервисы Ethernet

- Передача данных

Сервисы Wi-Fi

- Ассоциация
- Аутентификация
- Передача данных
- Защита информации (шифрование)
- и др.

Базовый набор сервисов



Одна точка доступа

- Рассылает идентификаторы своего набора сервисов

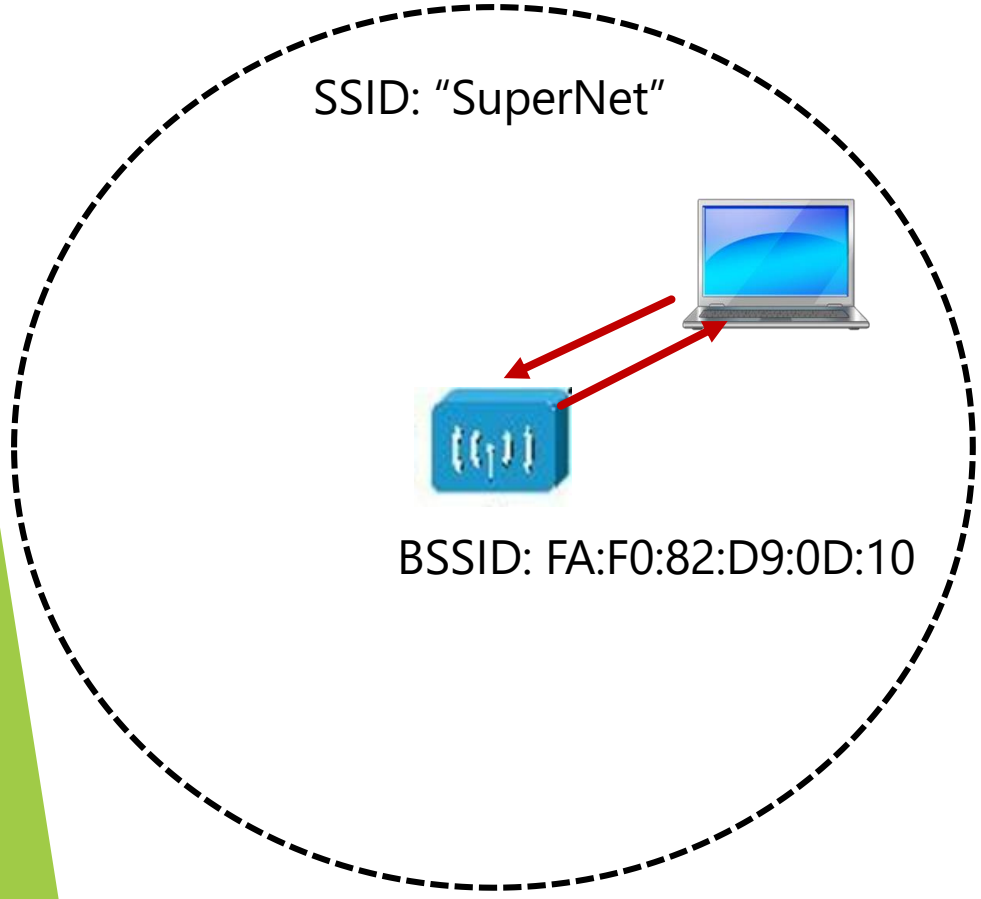
Basic Service Set IDentifier

- MAC-адрес точки доступа

Service Set Identifier

- Имя сети

Аутентификация



Открытая аутентификация

- Подключение без пароля

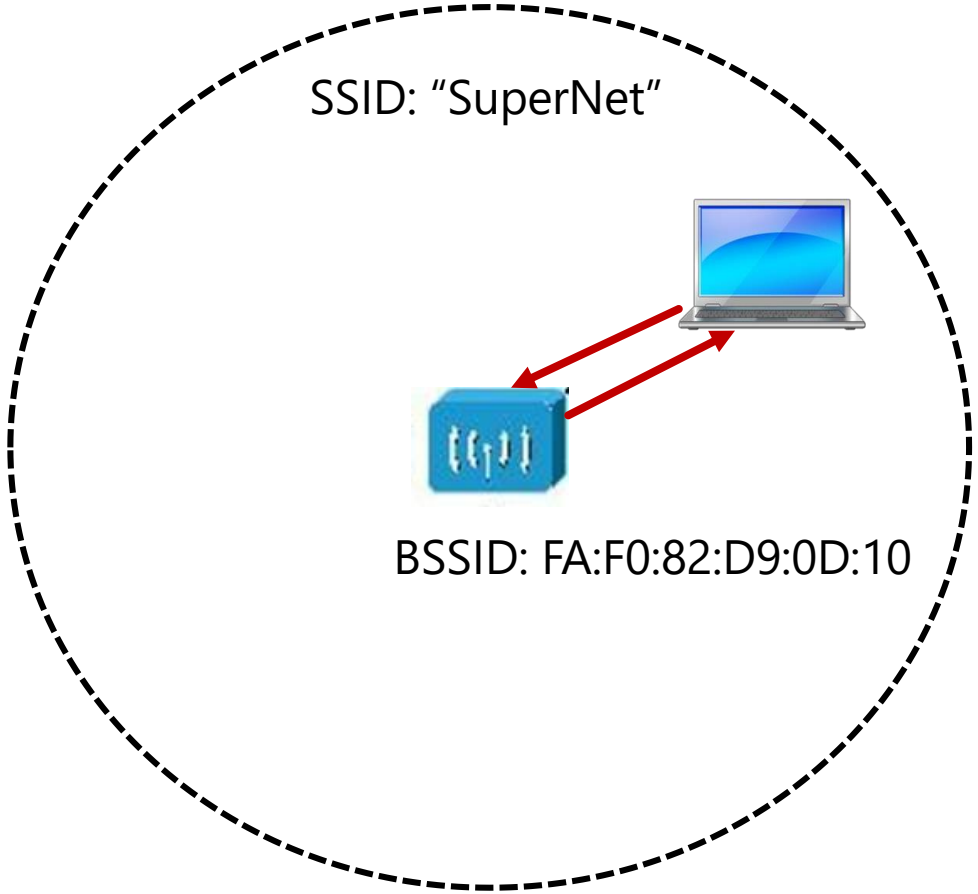
Personal

- Единый пароль для всех устройств в сети

Enterprise

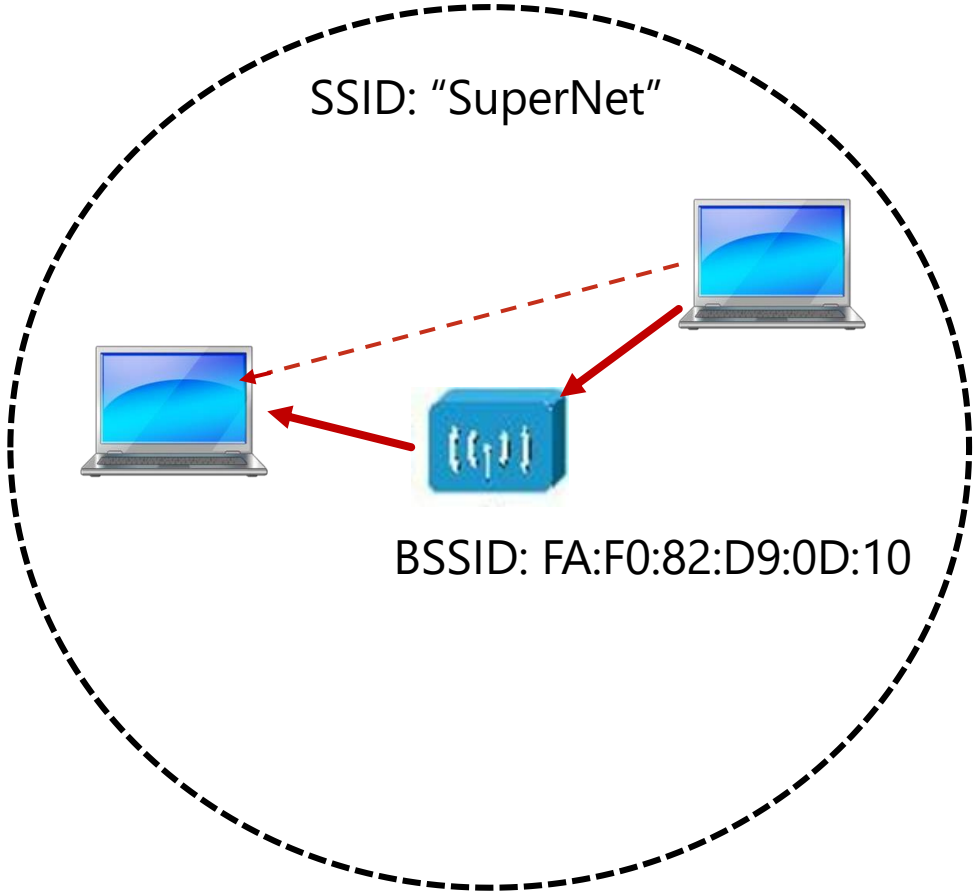
- Отдельные пароли для разных пользователей с применением сервера аутентификации (RADIUS, LDAP и т.п.)

Ассоциация



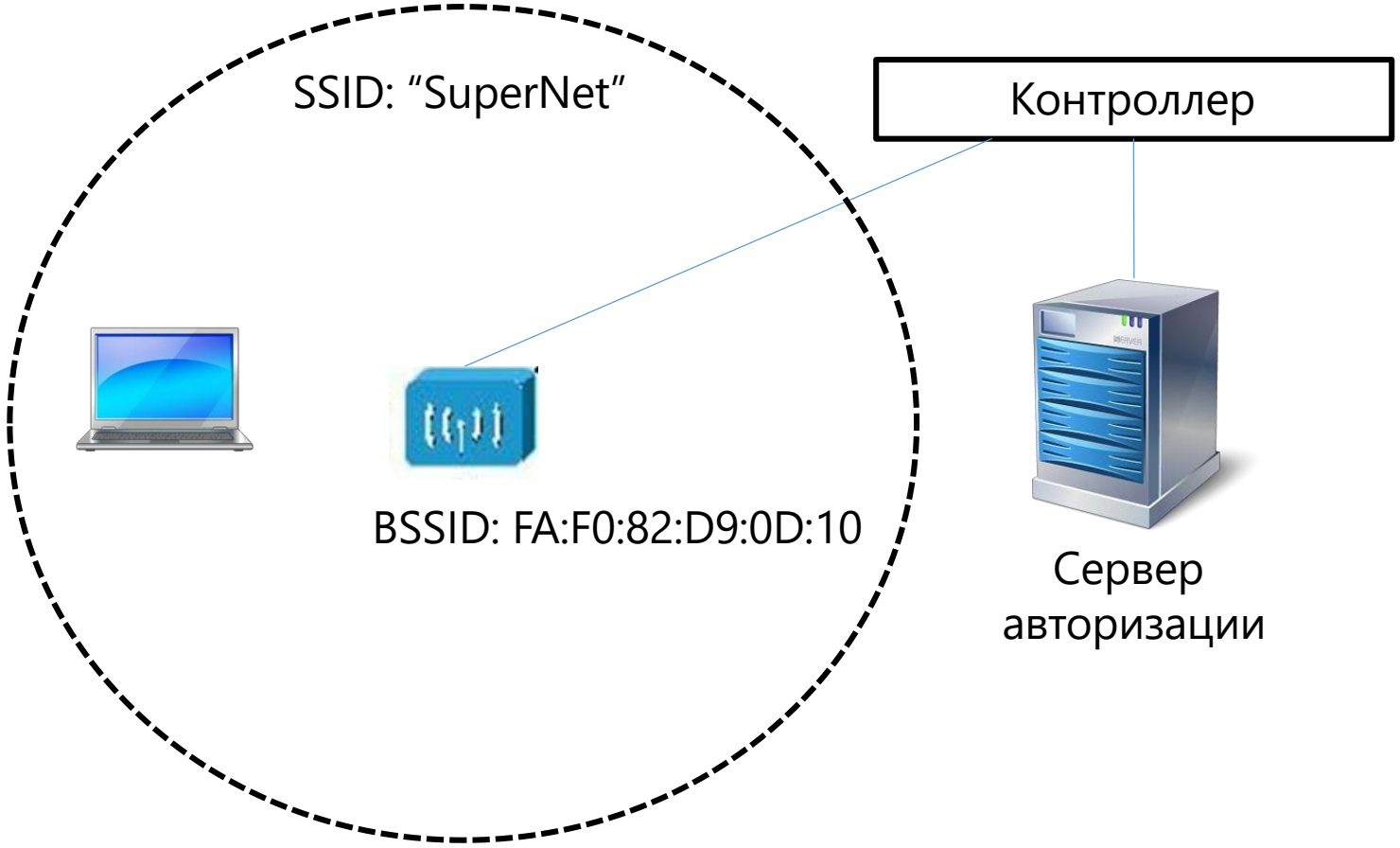
- Клиент передает параметры Wi-Fi, с которыми может работать
- Если параметры подходят, то точка доступа высылает кадр с успешной ассоциацией

Передача данных

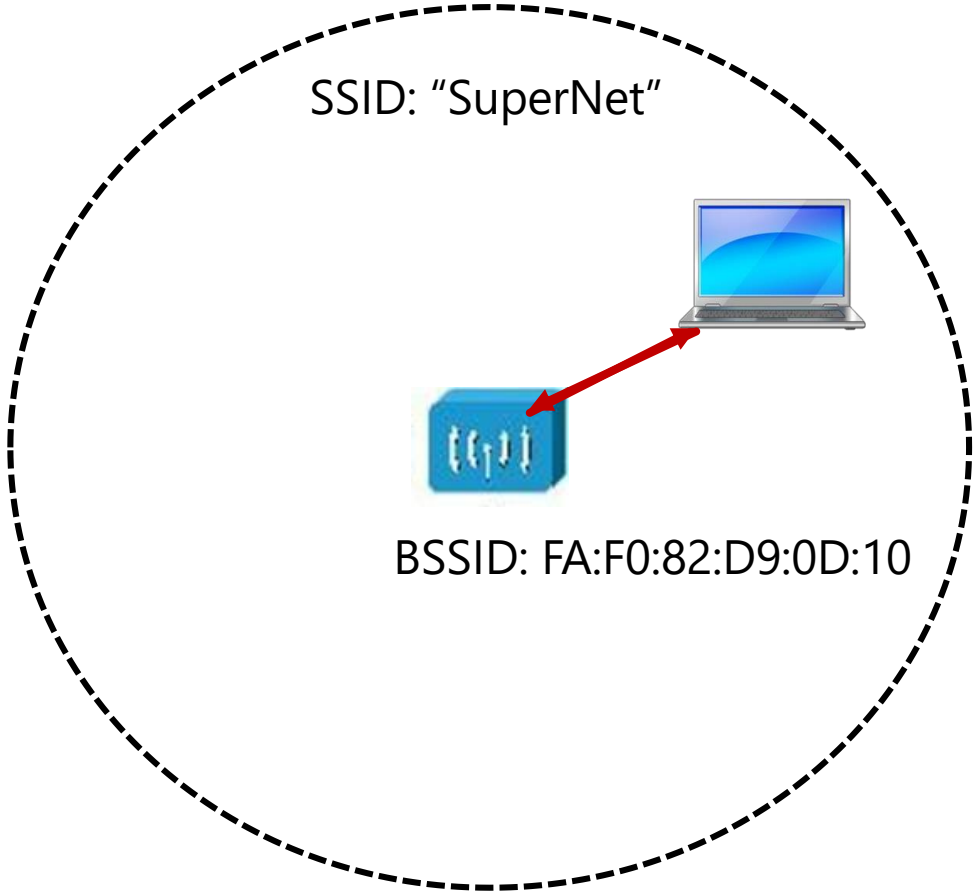


- После аутентификации и ассоциации, клиент может передавать данные в беспроводную сеть

Внешняя аутентификация

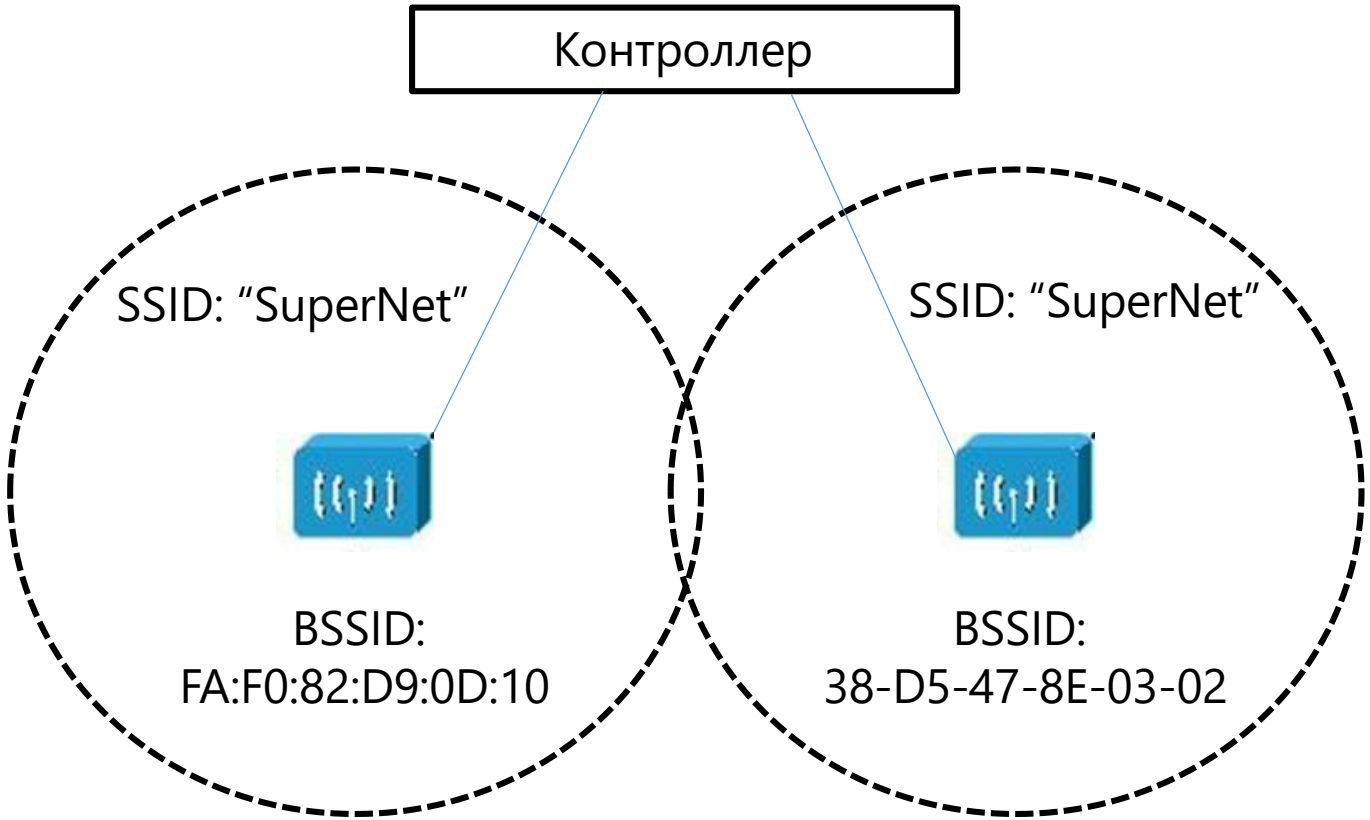


Отключение клиента

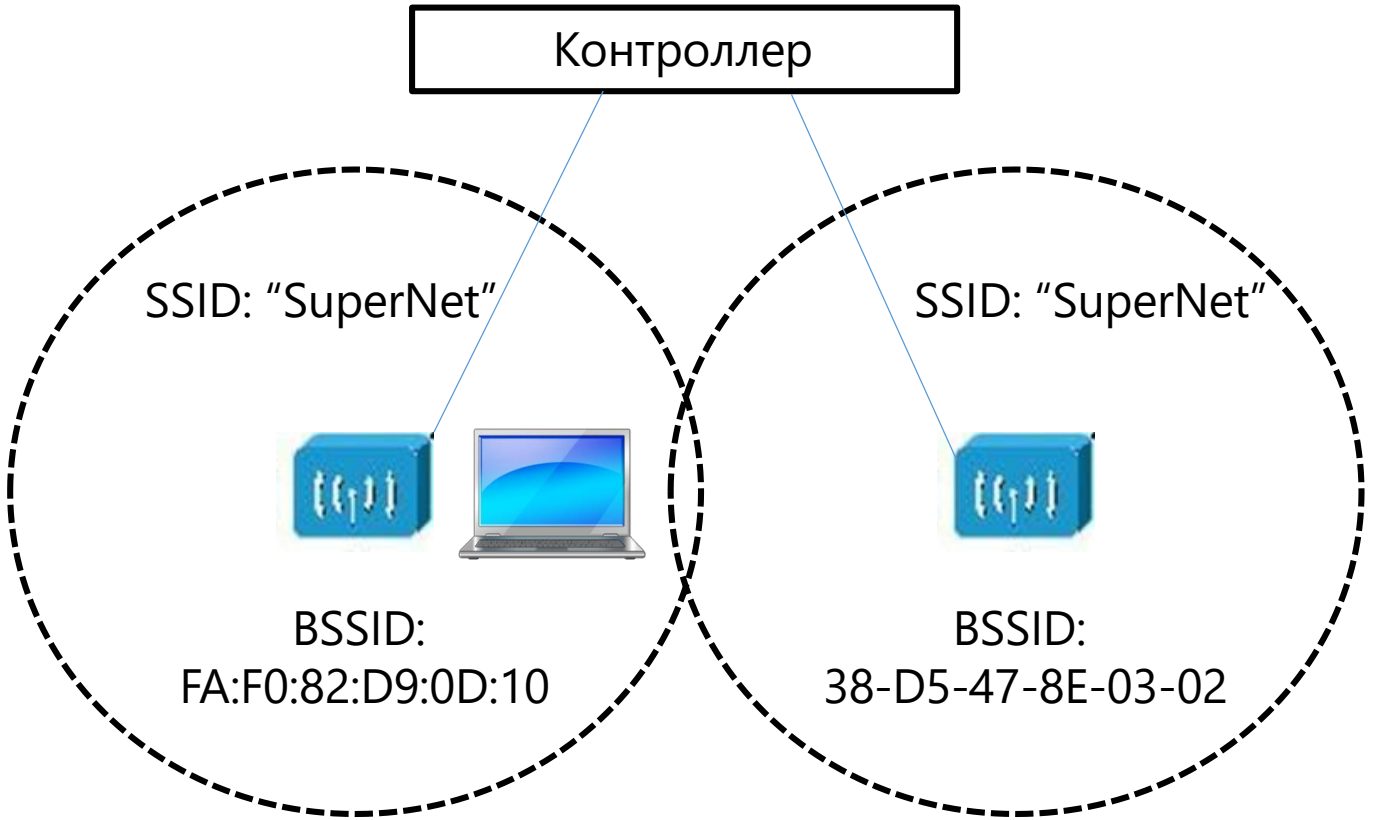


- Клиент отправляет запрос на деассоциацию
- Точка доступа высылает ответ и отключает его от сети

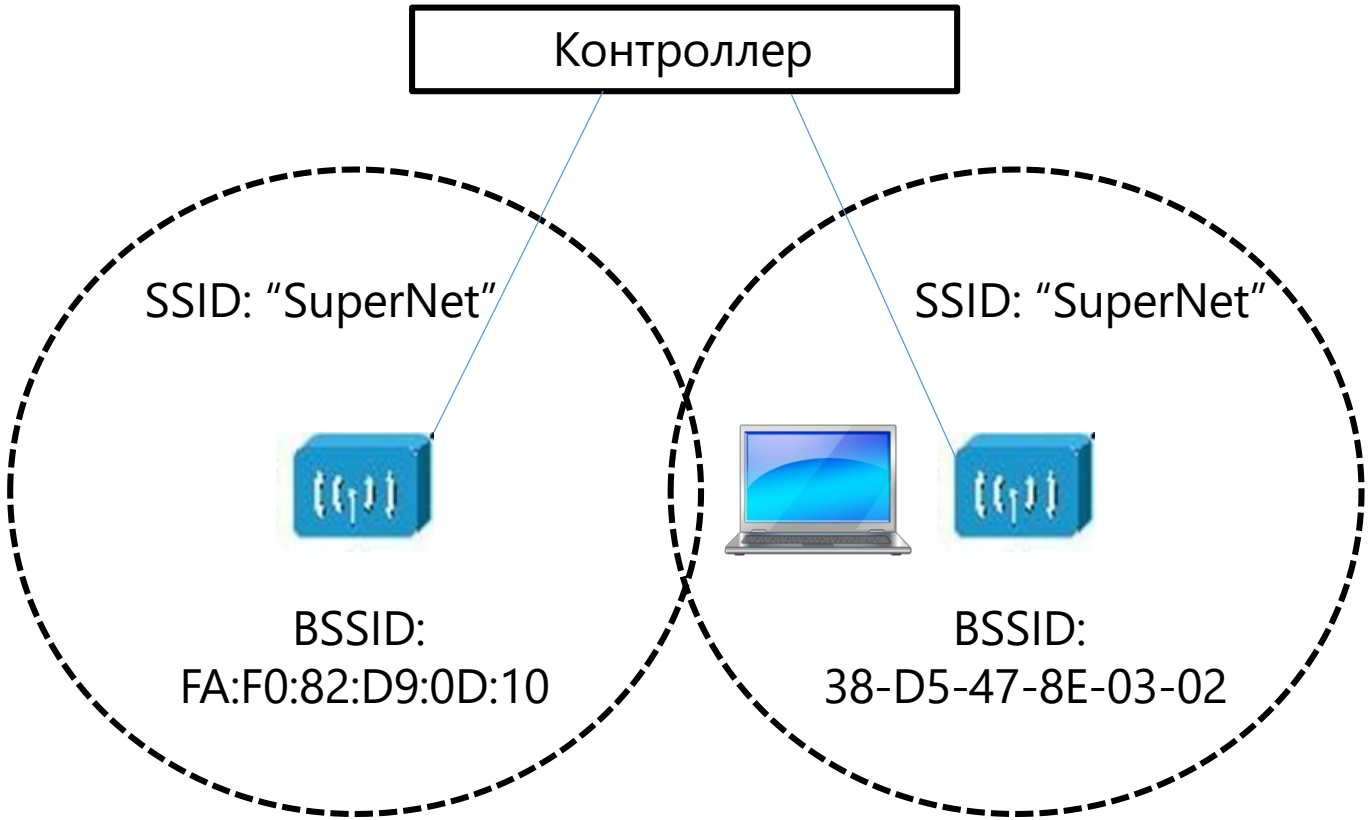
Расширенный набор сервисов



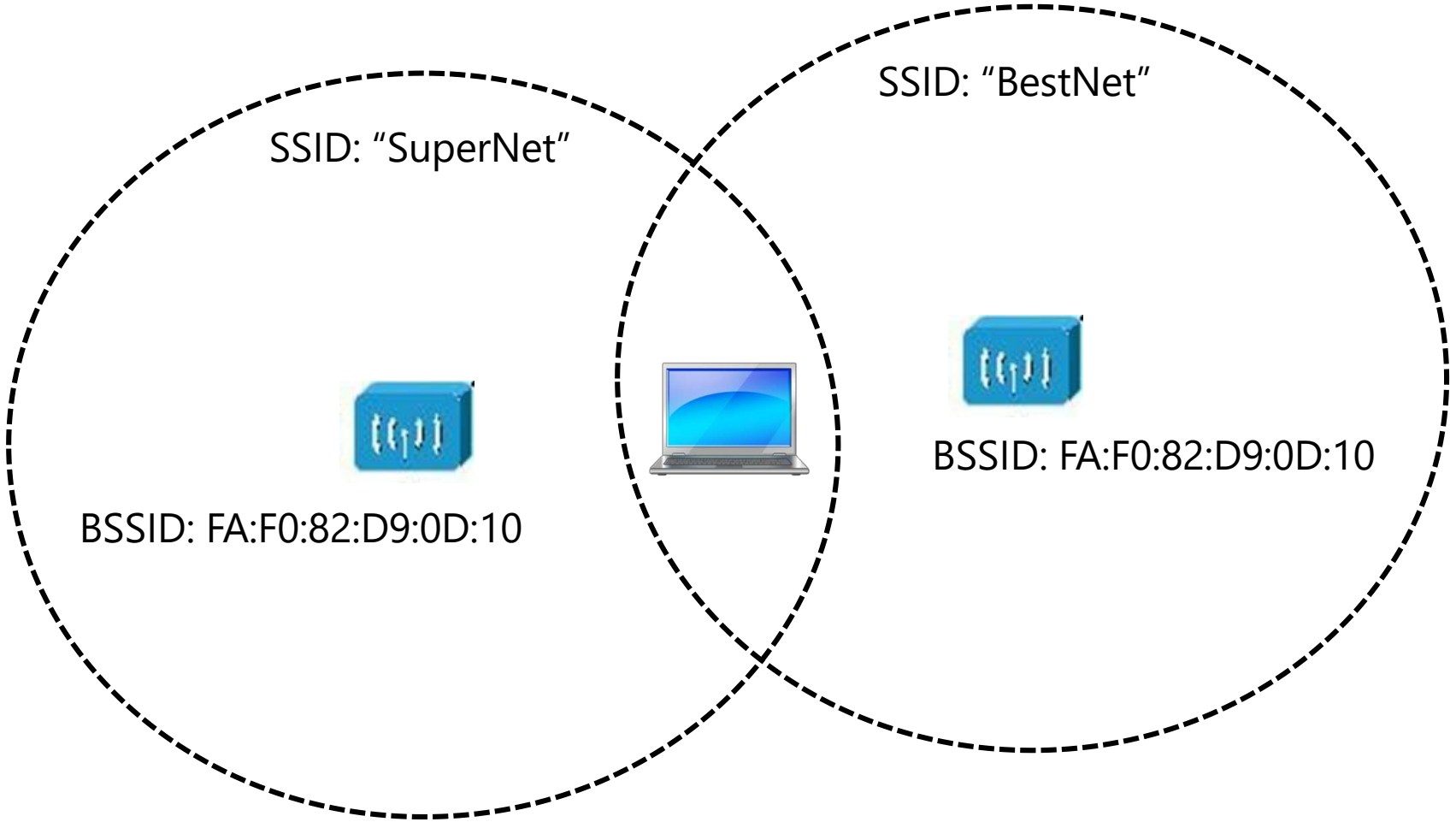
Роуминг


Контроллер
SSID: “SuperNet”
SSID: “SuperNet”
BSSID:
FA:F0:82:D9:0D:10
BSSID:
38-D5-47-8E-03-02

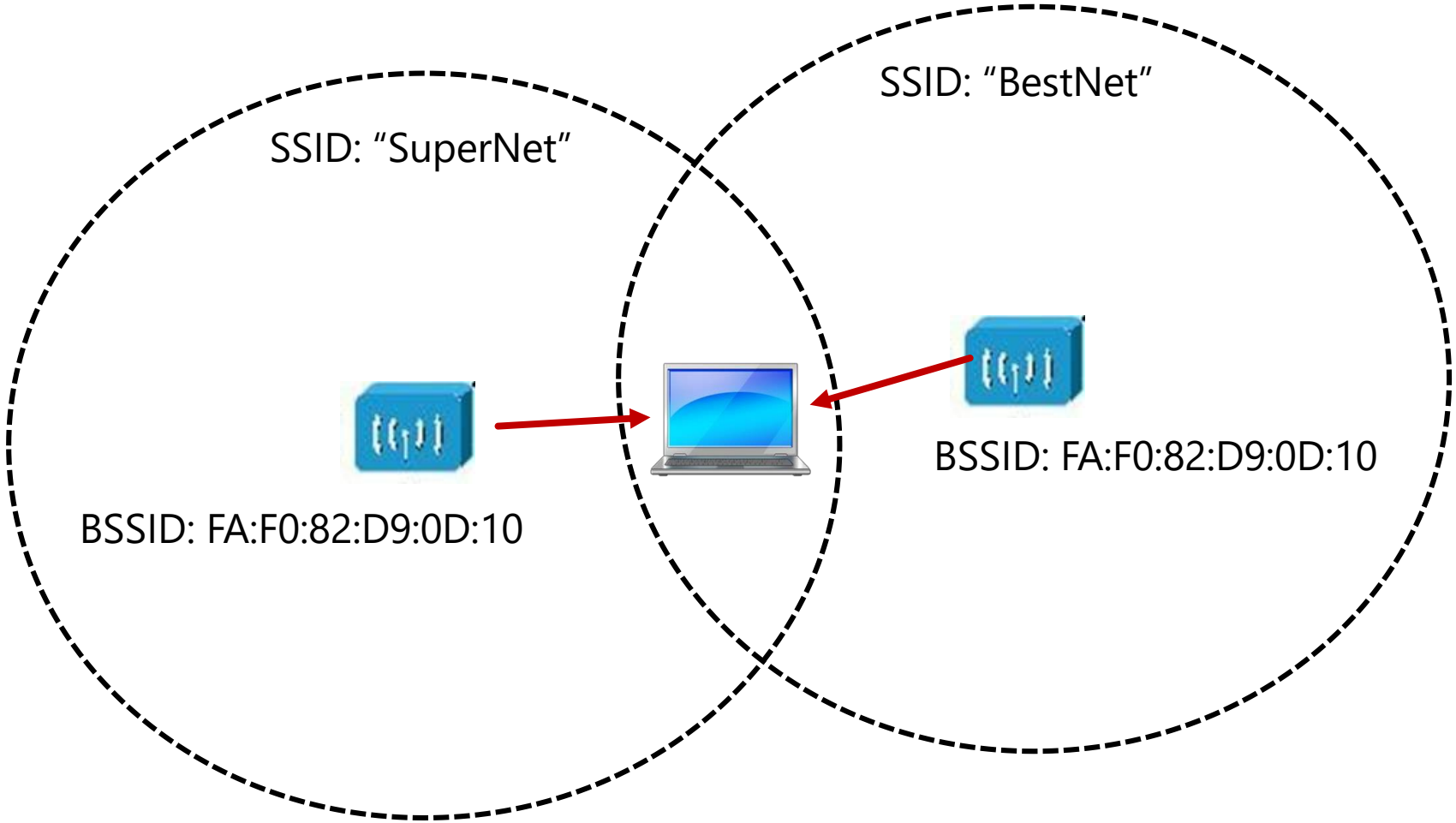
Реассоциация



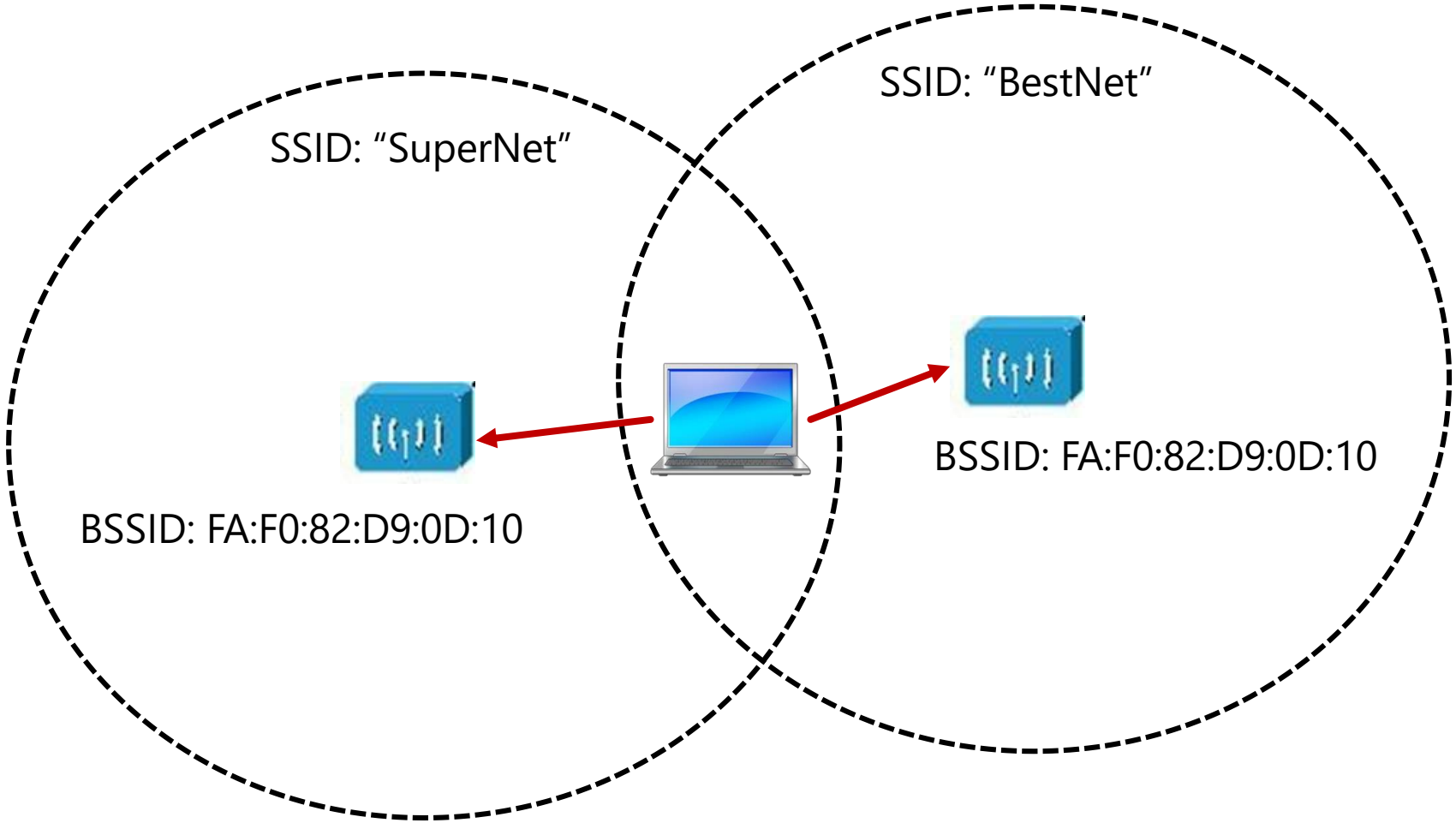
Сканирование



Пассивное сканирование. Beacon



Активное сканирование. Probe



Шифрование

Шифрование в Wi-Fi

- Установлен флаг Protection Frame
- Шифруются только данные, но не заголовки

Типы шифрования

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA2)
- Wi-Fi Protected Access 2 (WPA3)

WPA2 и WPA3

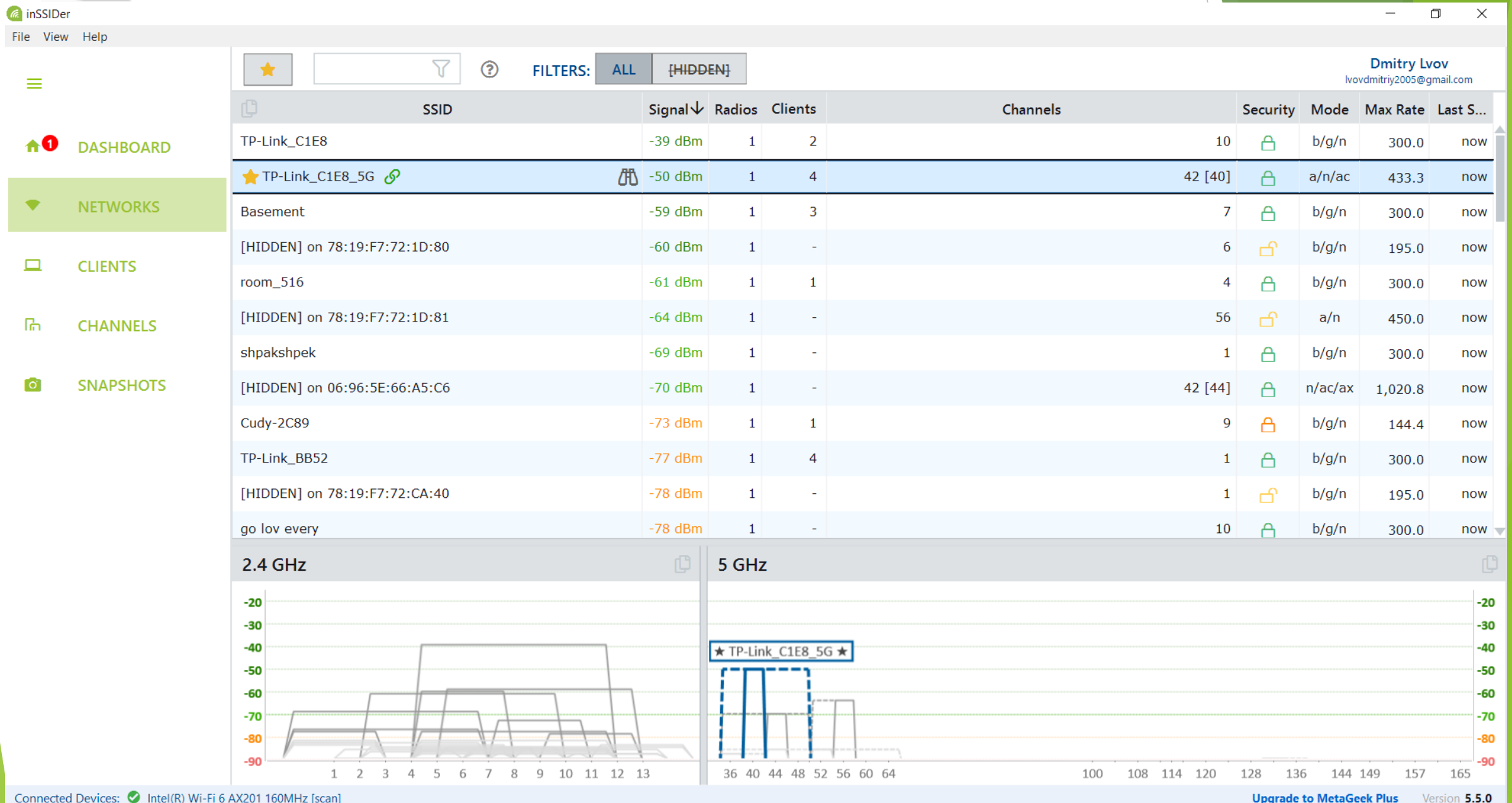
WPA2

- Протокол Pre-Shared Key
- Аутентификация уязвима к перебору пароля

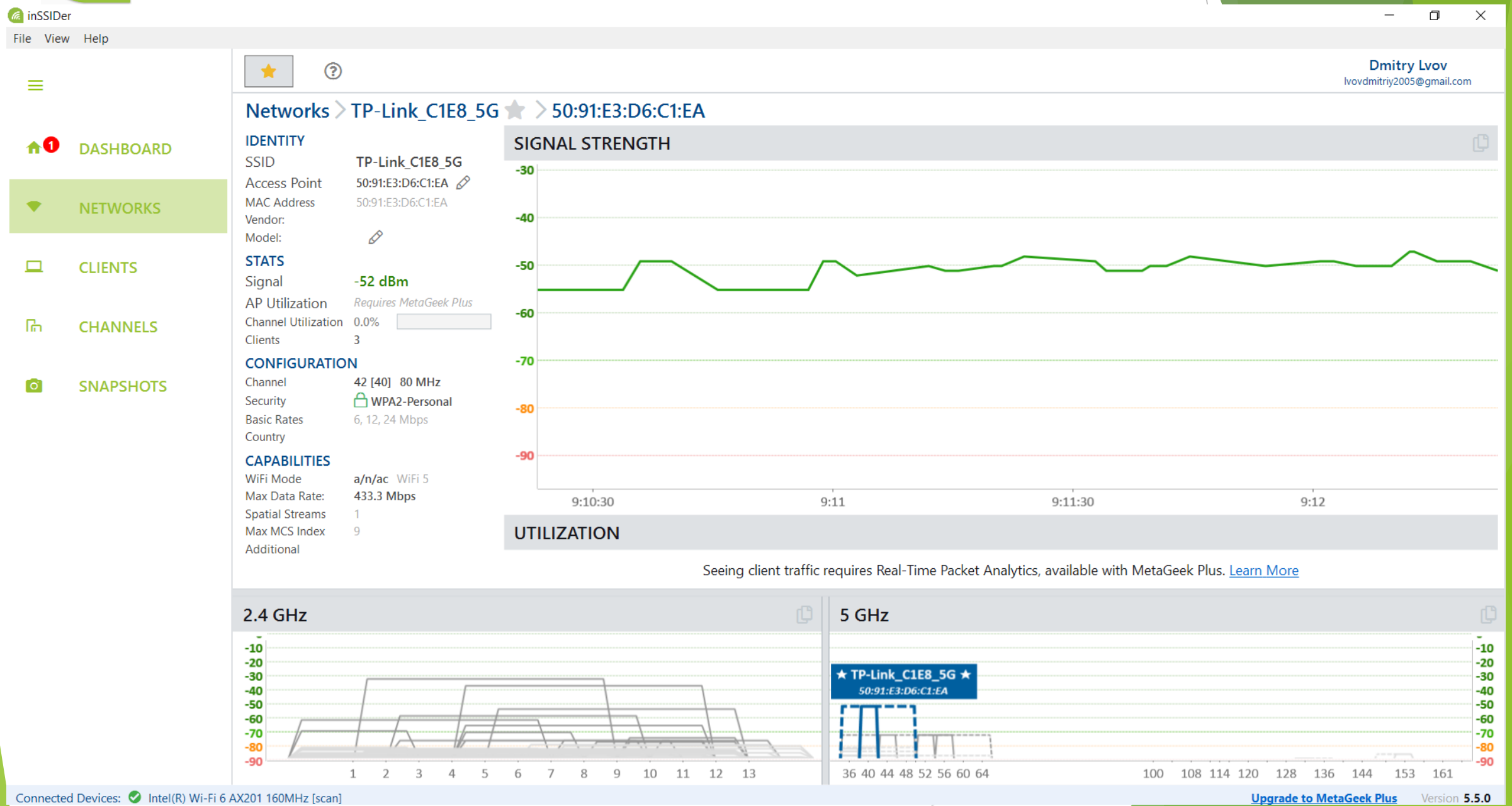
WPA3

- Протокол Simultaneous Authentication of Equals
- Предотвращает офлайн-атаки методом подбора пароля
- Forward Secrecy
- Enhanced Open
- OWE

inSSIDer


inSSIDer
File View Help
FILTERS: ALL [HIDDEN]
Dmitry Lvov
lvovdmitriy2005@gmail.com
DASHBOARD
NETWORKS
CLIENTS
CHANNELS
SNAPSHOTS
SSID Signal Radios Clients Channels Security Mode Max Rate Last S...
TP-Link_C1E8 -39 dBm 1 2 10 b/g/n 300.0 now
TP-Link_C1E8_5G -50 dBm 1 4 42 [40] a/n/ac 433.3 now
Basement -59 dBm 1 3 7 b/g/n 300.0 now
[HIDDEN] on 78:19:F7:72:1D:80 -60 dBm 1 - 6 b/g/n 195.0 now
room_516 -61 dBm 1 1 4 b/g/n 300.0 now
[HIDDEN] on 78:19:F7:72:1D:81 -64 dBm 1 - 56 a/n 450.0 now
shpakshpek -69 dBm 1 - 1 b/g/n 300.0 now
[HIDDEN] on 06:96:5E:66:A5:C6 -70 dBm 1 - 42 [44] n/ac/ax 1,020.8 now
Cudy-2C89 -73 dBm 1 1 9 b/g/n 144.4 now
TP-Link_BB52 -77 dBm 1 4 1 b/g/n 300.0 now
[HIDDEN] on 78:19:F7:72:CA:40 -78 dBm 1 - 1 b/g/n 195.0 now
go lov every -78 dBm 1 - 10 b/g/n 300.0 now
2.4 GHz
5 GHz
★ TP-Link_C1E8_5G ★
Connected Devices: Intel(R) Wi-Fi 6 AX201 160MHz [scan]
Upgrade to MetaGeek Plus
Version 5.5.0

inSSIDer


inSSIDer
File View Help
DASHBOARD
NETWORKS
CLIENTS
CHANNELS
SNAPSHOTS
Dmitry Lvov
lvovdmitriy2005@gmail.com
Networks > TP-Link_C1E8_5G > 50:91:E3:D6:C1:EA
IDENTITY
SSID TP-Link_C1E8_5G
Access Point 50:91:E3:D6:C1:EA
MAC Address 50:91:E3:D6:C1:EA
Vendor:
Model:
STATS
Signal -52 dBm
AP Utilization Requires MetaGeek Plus
Channel Utilization 0.0%
Clients 3
CONFIGURATION
Channel 42 [40] 80 MHz
Security WPA2-Personal
Basic Rates 6, 12, 24 Mbps
Country
CAPABILITIES
WiFi Mode a/n/ac WiFi 5
Max Data Rate: 433.3 Mbps
Spatial Streams 1
Max MCS Index 9
Additional
SIGNAL STRENGTH
-30
-40
-50
-60
-70
-80
-90
9:10:30
9:11
9:11:30
9:12
UTILIZATION
Seeing client traffic requires Real-Time Packet Analytics, available with MetaGeek Plus. Learn More
2.4 GHz
-10
-20
-30
-40
-50
-60
-70
-80
-90
1 2 3 4 5 6 7 8 9 10 11 12 13
5 GHz
★ TP-Link_C1E8_5G ★
50:91:E3:D6:C1:EA
36 40 44 48 52 56 60 64
100 108 114 120 128 136 144 153 161
Connected Devices: Intel(R) Wi-Fi 6 AX201 160MHz [scan]
Upgrade to MetaGeek Plus
Version 5.5.0