

1. LoRa

Технологию LoRa можно использовать в сложных условиях эксплуатации в рамках мегаполиса: у данной технологии хорошее покрытие и широкие возможности использования. Существует несколько вариантов реализации: топология «звезда» и ячеистая топология.

1.1. Расчет мощности полезного сигнала на входе приемника

Для расчёта мощности полезного сигнала на входе приемника необходимо знать энергетические параметры радиолинии и реальную чувствительность приемника.

В качестве передатчика выступает БС, в качестве приёмника – радиомодуль. Расчет производился в программе Mathcad 15. Исходные данные для расчетов представлены ниже. Чтобы высчитать длину волны необходимо знать скорость света и частоту:

$$c = 3 \times 10^8 \text{ м/с} \quad (1)$$

Рабочая частота системы:

$$f = 868 \times 10^6 \text{ Гц} \quad (2)$$

Расчет длины волны производился по следующей формуле:

$$\lambda = \frac{c}{f} = 0.346 \text{ м} \quad (3)$$

Выходную мощность передатчика взята из документации БС:

$$P_{\text{прд}} = 14 \text{ дБм} \quad (4)$$

Коэффициент усиления передающей антенны взят из сопроводительной документации на антенну АК-868:

$$G_{\text{прд}} = 7 \text{ дБи} \quad (5)$$

Коэффициент усиления приемной антенны взят из сопроводительной документации на антенну ANT-868-CW-HWR:

$$G_{\text{прм}} = -2.3 \text{ дБи} \quad (6)$$

Расчет в программе производился на расстоянии до 5 км. Расчет потерь при передаче производился по формуле (МСЭ-R P.525.2):

$$L_{\text{псп}} = 32.4 + 20 \log\left(\frac{f}{10^6}\right) + 20 \log\left(\frac{d}{10^3}\right) \quad (7)$$

$$L_{\text{псп}} = 105.15 \text{ дБ} \quad (8)$$

Дополнительные потери, обусловленные целым комплексом причин, включая ослабление сигнала в соединительных разъемах, потери из-за несовпадения поляризации антенн и т.п. определяются $L_{\text{доп}}$ и считаются отдельно на стадии оптимизации. Кроме того, при использовании внешних антенн, подключаемых к радиооборудованию с помощью коаксиальных кабелей, необходимо знать длину кабелей и величину погонного затухания в них, выражаемого в дБ/м. Результирующее затухание в кабелях добавляется к величине $L_{\text{доп}}$.

Также для расчета необходимо знать запас помехоустойчивости к внешним помехам. Его величина определяется электромагнитной обстановкой в районе, где предполагается реализовывать БСС, и, как правило, задается в пределах от 5 до 15 дБ. Исходя из того, что сеть радиодоступа планируется использовать в районе с достаточно плотной застройкой, то я взял максимальное значение в 15 дБ.

Формула расчета мощности полезного сигнала в точке приема определяется выражением:

$$P_{\text{прм}} = \frac{P_{\text{прд}} G_{\text{прд}} G_{\text{прм}} \lambda^2}{(4\pi r)^2 L_{\text{доп}} Z} \quad (9)$$

В децибелах выражение имеет вид:

$$P_{\text{прм}} = P_{\text{прд}} + G_{\text{прд}} + G_{\text{прм}} + 20 \log(\lambda) - 20 \log(4\pi) - 20 \log\left(\frac{d}{10^3}\right) - L_{\text{доп}} - Z \quad (10)$$

$$P_{\text{прм}} = -146.641 \text{ дБм} \quad (11)$$

Реальную чувствительность приемника обозначают как P_{min} , что соответствует физическому смыслу данного показателя, определяющего минимально необходимую для нормального приема мощность полезного сигнала на входе приемника. Величина этого параметра для приемников беспроводных сетей лежит в пределах от -94 до -67 дБм. Следует иметь в виду, что с увеличением скорости передачи реальная чувствительность ухудшается (численное значение P_{min} возрастает). Чувствительность приемника на радиомодуле равна $P_{\text{min}} = -148$ дБ. Также я произвел расчет запаса по мощности для того чтобы понимать максимальные расчетные возможности системы:

$$P_{\text{запас}} = P_{\text{прм}} - P_{\text{min}} \quad (12)$$

$$P_{\text{запас}} = 1.139 \text{ дБ} \quad (13)$$

Ниже, на рисунке 2.7 представлен графический расчет затухания сигнала при прохождении через свободное пространство.

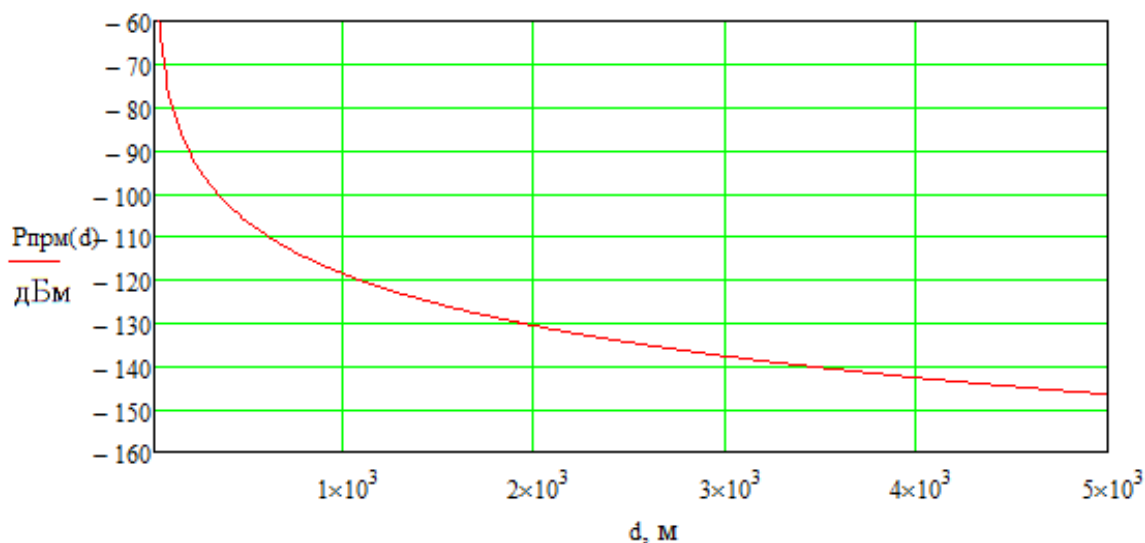


Рисунок 2.13 – Распространение сигнала в открытом пространстве

1.2. Расчет покрытия сети

Для расчета зоны покрытия сети радиодоступа в классическом варианте используют специализированные программы такие как Onega или Atoll Forsk. Эти программы позволяют максимально точно определить зону покрытия и возможные зоны ослабления радиосигнала. У меня не было возможности использовать данные операционно-технические средства, и поэтому было принято решение использовать уже существующие исследования распространения радиоволн из здания на улицу используя в качестве реальных цифр для проверки результаты 2-х проведенных в рамках данной работы экспериментов.

В настоящее время разработано достаточно много моделей распространения радиоволн и методик расчета уровней ослабления сигналов в условиях городской застройки. Как правило, такие модели можно разделить на три типа: модели распространения радиоволн в городских кварталах, модели распространения радиоволн внутри зданий и модели распространения радиоволн из здания и внутрь здания. При этом модели распространения радиоволн из здания и внутрь здания могут применяться как в виде самостоятельного аппарата прогнозирования, так и в виде связующего звена между моделями распространения в городе (вне зданий) и моделями распространения внутри здания.

На практике широкое применение нашли статистические модели распространения радиоволн из здания на улицу, полученные на основе обработки результатов экспериментальных исследований. Следует отметить, что указанные модели разрабатывались для определенных частотных диапазонов, используемых в различных мобильных системах связи общего пользования и беспроводных сетях передачи данных. Базовой моделью является COST 231 для диапазона частот 900 – 1800 МГц. Модель WINNER II построена на основе модели COST 231 и охватывает диапазон более высоких

частот 2 - 6 ГГц, позволяет учитывать дифракционные компоненты радиоволн, распространяющиеся через двери и окна, при этом полученные на основе экспериментов формулы справедливы только для частоты 8,45 ГГц на которой и проводились расчеты измерения.

Вместе с тем представляет интерес исследование ослабления радиоволн на трассе распространения из здания на улицу на частотах ниже 900 МГц, а именно 868 МГц (LoRaWAN).

Следует отметить, что статистические модели не позволяют в полной мере учесть особенности трасс распространения радиоволн. В связи с этим в некоторых случаях могут использоваться детерминированные модели. Такие модели весьма трудоемки в плане построения трасс распространения радиоволн и проведения расчетов и требуют множество исходных данных, которые не всегда известны. Однако преимущество детерминированных моделей заключается в возможности анализа с их использованием закономерностей распространения радиоволн для типовых трасс и различных диапазонов частот, что может использоваться в дальнейшем при корректировке статистических моделей.

Для расчета покрытия сети в плотной городской застройке была создана сводная таблица (таблица 1) на основе результатов экспериментов. Численные значения близки к результатам экспериментов инженеров из Смоленска, которые проводили подобные полевые испытания и расчет зоны покрытия в городе Смоленске.

Таблица 1 – Примерные радиусы действия системы

Расположение датчика	Outdoor	Light Indoor	Deep Indoor
Уверенная зона покрытия (м)	2000	600	300

Используя таблицу 1 построена карта радиопокрытия 1-й БС в предполагаемом районе развертывания радиосети (рисунки 1,2,3).

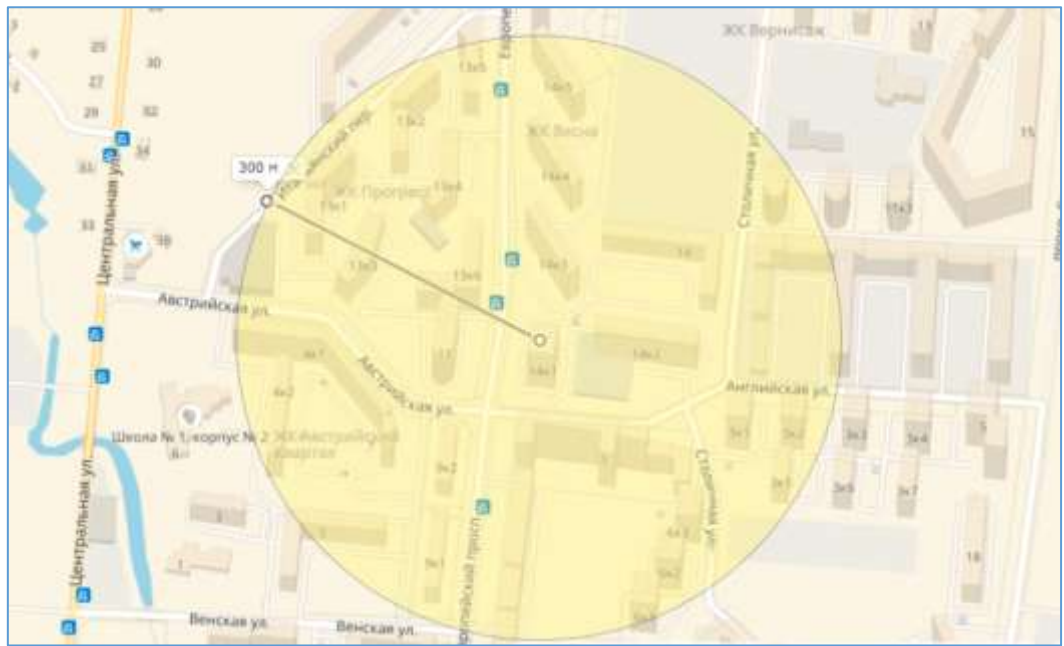


Рисунок 1 – Покрытие сети в Deer Indoor

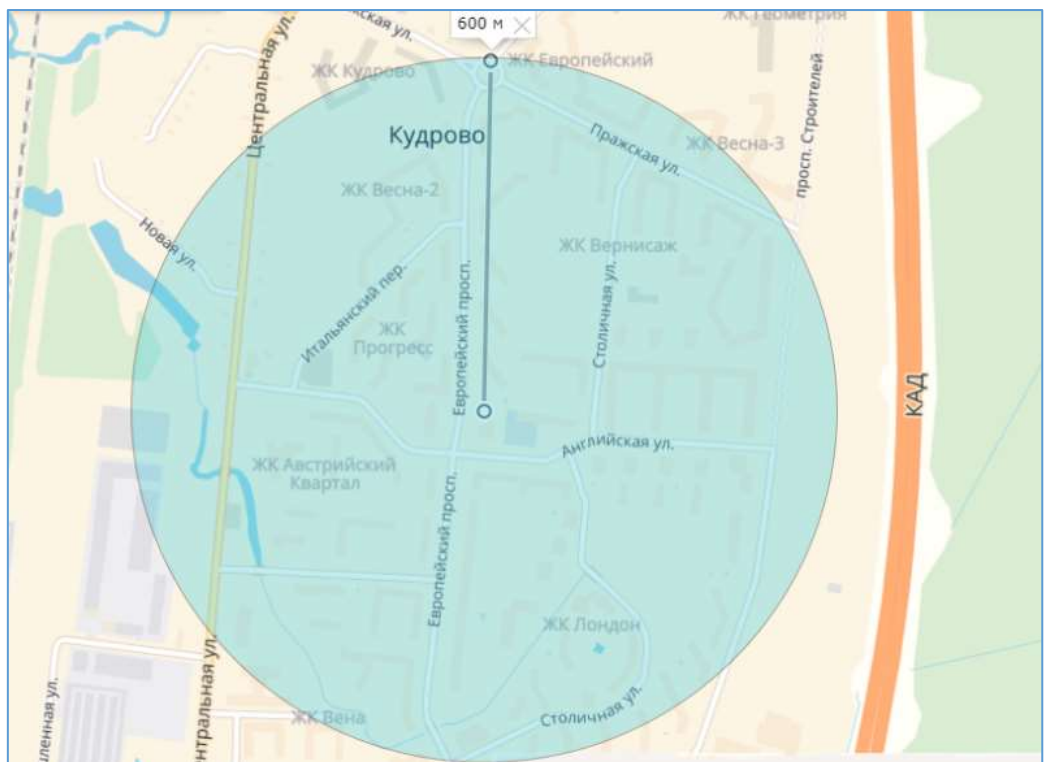


Рисунок 2 – Покрытие сети в Indoor

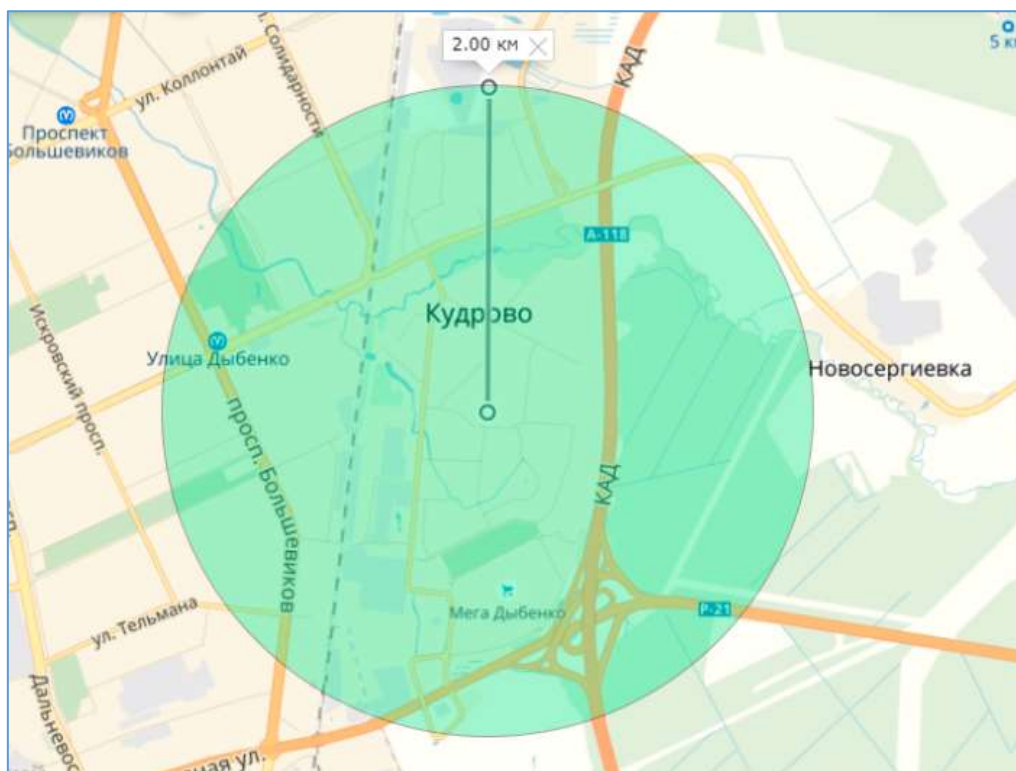


Рисунок 3 – Покрытие сети в Outdoor

Таким образом:

- в условиях плотной городской застройки в радиусе 300м будет уверенное радиопокрытие для зоны Deep Indoor (подвальные помещения, подземные паркинги)
- в пределах 0.6-1км от LoRa шлюза существует хорошее радиопокрытие outdoor и indoor (уровни не ниже -120dBm);
- в радиусе 1-1.5 км покрытие в зоне outdoor не ниже -120dBm, в indoor уровни составят около -130dBm (возможна потеря некоторых пакетов).
- на расстояниях 1.5-2.5 км связь остается, но с уровнем покрытия outdoor до -130dBm (возможна потеря пакетов), в indoor связь будет отсутствовать;
- более 2.5 км в условиях плотной городской застройки отсутствует outdoor/indoor покрытие.

1.3. Выбор топологии

Для реализации построения проектной беспроводной сети возможны несколько видов топологии.

На рисунке 4 схематически изображен сценарий развития сети с одной базовой станцией которая связывается с каждым датчиком напрямую. Каждый прибор учета (электроэнергии, горячей и холодной воды) имеет встроенный радиомодуль, работающий на частоте базовой станции. Базовая станция подключена к коммутатору по Ethernet кабелю, который подключён к сети Internet для возможности передачи данных с датчиков на БС и на сервер и управления базовой станцией с помощью подсистемы приложений организованной на сервере компании.

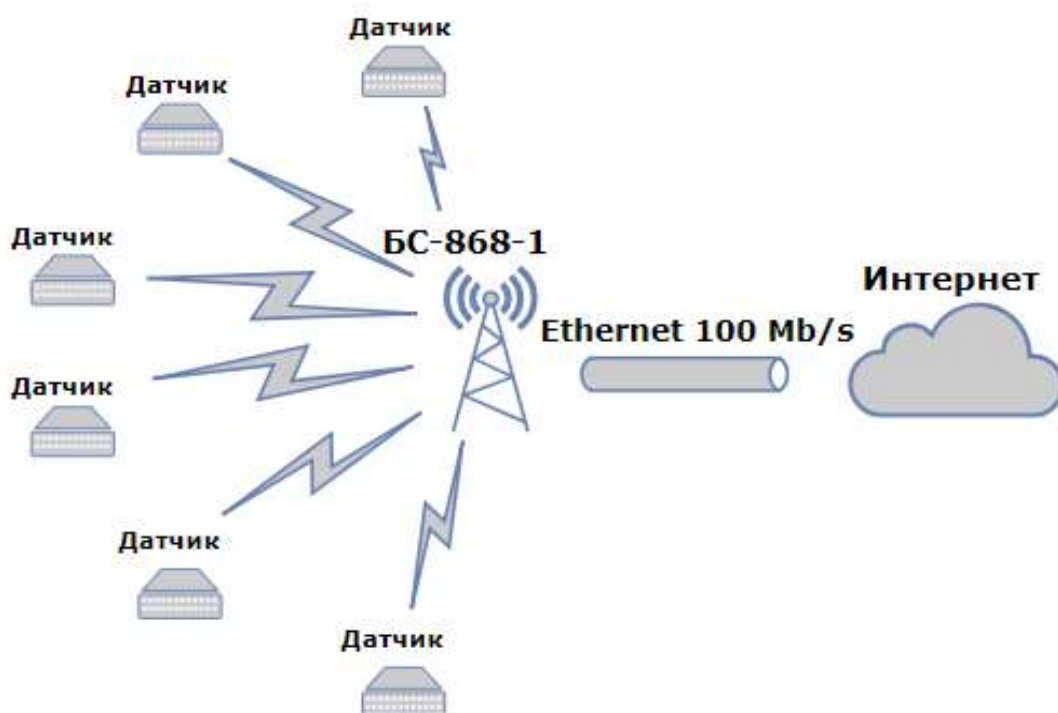


Рисунок 4 – Сценарий прямой связи с датчиками

Сценарий, изображенный на рисунке 5, предполагает использование одной базовой станции и концентраторов (радиомодулей РМ868-Б), каждый

из которых связан с прибором учета посредством обычного двухжильного кабеля и подсоединен к радиомодулю. Каждый прибор учета должен иметь импульсный выход.

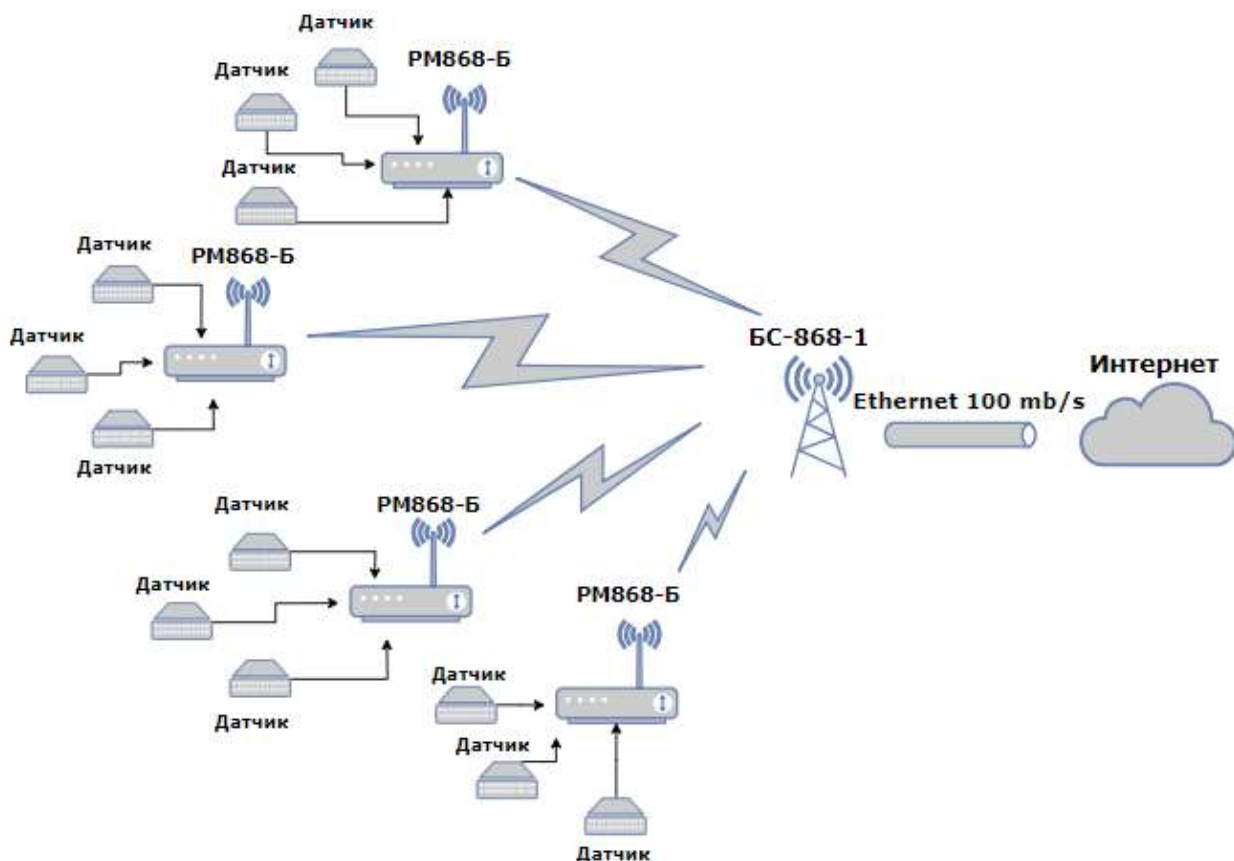


Рисунок 5 – Сценарий с использованием концентраторов

3-й сценарий построения сети — это система, использующая 2 базовые станции и радиомодули так же, как и во втором сценарии. Как предполагается, данная топология наиболее актуальна для очень плотной городской застройки (мегаполис). В спальнях районах неустойчивая электромагнитная обстановка (особенно в период ЧНН), что плохо влияет на передачу данных с маломощных радиомодулей. Также на пути распространения радиоволны в много препятствий в виде многоэтажных домов расположенных близко к другу другу.

Плюсом будет являться не только возможность покрытия большей зоны, но и возможность собирать данные с датчиков даже при отказе одной базовой станции.

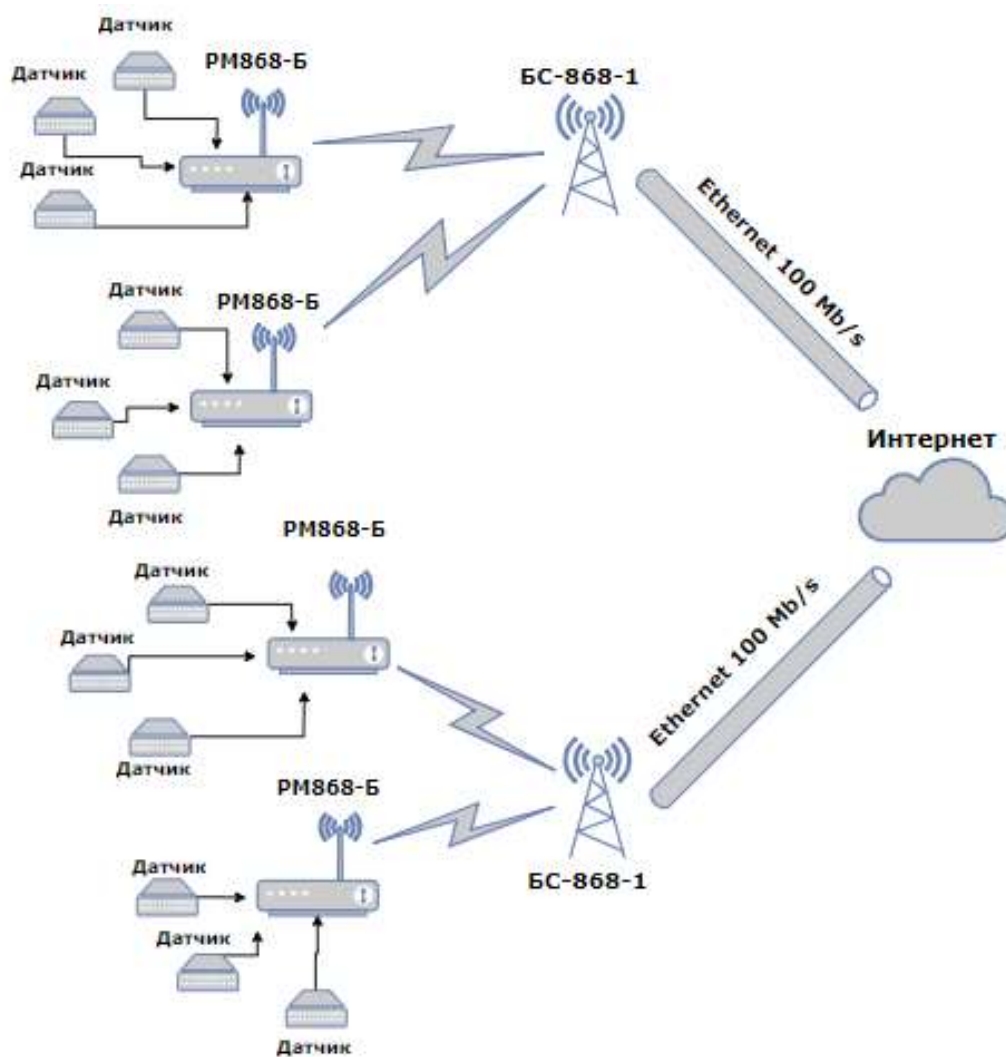


Рисунок 6 – Сценарий с использованием 2-х БС и концентраторов

2. МЕТОДИКА ПРОВЕДЕНИЯ ИССЛЕДОВАНИЯ МЕЖДИАПАЗОННОЙ СЕТИ Wi-Fi СПбГУТ

2.1 Программные и аппаратные средства проведения эксперимента

Программные средства

CommView for WiFi — это программа для мониторинга и анализа сетевых пакетов в беспроводных сетях стандартов 802.11 a/b/g/n/ac. Данная программа захватывает все сетевые пакеты, передаваемые в эфире, для последующего детального отображения важной информации: списка точек доступа и узлов, статистики по каждому узлу и каналу, уровня сигнала, списка пакетов и сетевых соединений, графиков распределения протоколов.

Программа может работать на компьютере под управлением Windows 7/8/8.1 /10 или Windows Server 2008/2012 (поддерживаются 32- и 64-битные версии) и получать данные от любого сетевого адаптера Ethernet, Wi-Fi или виртуального адаптера (VPN или dial-up).

CommView осуществляет полный анализ более 100 распространенных протоколов.

- Перехват интернет-трафика и/или трафика локальной сети, проходящий через сетевую карту или модем пользователя.
- Просматривание перехваченных и декодированных пакетов в реальном времени или в offline-режиме.
- Просмотр подробной статистики IP-соединений: IP-адреса, порты, сессии и т. д.
- Реконструирование TCP-сессии и UDP-поточков.
- Просмотр приложения, получающего или посылающего пакеты.
- Просмотр графика распределения протоколов, загрузки сети, списки активных сетевых узлов и их статистику.
- Генерирование отчетов.

- Создание поиска по строкам или hex-данным по содержимому перехваченных пакетов.
- Экспорт и импорт архивов с сохраненными пакетами в/из форматов Sniffer®, EtherPeek™, AiroPeek™, Observer®, NetMon и Wireshark/Tcpdump.
- Настройка предупреждений, которые сообщают пользователю о важных событиях: подозрительные пакеты, высокая загрузка сети, неизвестные адреса и т. д.
- Передача любого IP-адреса в SmartWhois для быстрого и простого получения информации о нем.
- Перехват loopback-трафика на локальной машине.

Аппаратные средства

В эксперименте используются 2 двухдиапазонных USB-адаптера модели D-Link DWA-160

Таблица 2.1 Технические характеристики DWA-160 [7]

Стандарты	<ul style="list-style-type: none"> • IEEE 802.11n • IEEE 802.11g • IEEE 802.11a • IEEE 802.11b
Интерфейс	USB 2.0/1.1
Антенна	Две внутренние всенаправленные антенны с коэффициентами усиления 1,5 dBi в диапазоне 2.4 ГГц, 3,5 dBi в диапазоне 5 ГГц
Схема MIMO	2x2
Частотный диапазон	<ul style="list-style-type: none"> • От 2,4 ГГц до 2,472 ГГц • От 5,15 ГГц до 5,35 ГГц • От 5,725 ГГц до 5,850 ГГц

<p>Выходная мощность передатчика</p>	<ul style="list-style-type: none"> • IEEE 802.11a <ul style="list-style-type: none"> 14 dBm при 6, 9 Мбит/с 13 dBm при 12, 18 Мбит/с 12 dBm при 24, 36 Мбит/с 11 dBm при 48, 54 Мбит/с • IEEE 802.11b <ul style="list-style-type: none"> 17 dBm при 1,2,5.5,11 Мбит/с • IEEE 802.11g <ul style="list-style-type: none"> 17 dBm при 6, 9 Мбит/с 16 dBm при 12, 18 Мбит/с 15 dBm при 24, 36 Мбит/с 14 dBm при 48, 54 Мбит/с • IEEE 802.11n <ul style="list-style-type: none"> 2.4ГГц <ul style="list-style-type: none"> HT-20 14dBm при MCS0~15 HT-40 14dBm при MCS0~15 5 ГГц <ul style="list-style-type: none"> HT-20 11dBm при MCS0~15 HT-40 11dBm при MCS 0~15
<p>Чувствительность приёмника</p>	<ul style="list-style-type: none"> • IEEE 802.11a <ul style="list-style-type: none"> -82 dBm при 6 Мбит/с -81 dBm при 9 Мбит/с -79 dBm при 12 Мбит/с -77 dBm при 18 Мбит/с -74 dBm при 24 Мбит/с -70 dBm при 36 Мбит/с -66 dBm при 48 Мбит/с -65 dBm при 54 Мбит/с • IEEE 802.11b <ul style="list-style-type: none"> -76 dBm при 2 Мбит/с -76 dBm при 11 Мбит/с • IEEE 802.11g <ul style="list-style-type: none"> -82 dBm при 6 Мбит/с -81 dBm при 9 Мбит/с

	<p> -79 dBm при 12 Мбит/с -77 dBm при 18 Мбит/с -74 dBm при 24 Мбит/с -70 dBm при 36 Мбит/с -66 dBm при 48 Мбит/с -65 dBm при 54 Мбит/с IEEE 802.11n (2.4 ГГц) HT-20 -82 dBm при MCS0/8 -79 dBm при MCS1/9 -77 dBm при MCS2/10 -74 dBm при MCS3/11 -70 dBm при MCS4/12 -66 dBm при MCS5/13 -65 dBm при MCS6/14 -64 dBm при MCS7/15 HT-40 -79 dBm при MCS0/8 -76 dBm при MCS1/9 -74 dBm при MCS2/10 -71 dBm при MCS3/11 -67 dBm при MCS4/12 -63 dBm при MCS5/13 -62 dBm при MCS6/14 -61 dBm при MCS7/15 IEEE 802.11n (5 ГГц) HT-20 -82 dBm при MCS0/8 -79 dBm при MCS1/9 -77 dBm при MCS2/10 -74 dBm при MCS3/11 -70 dBm при MCS4/12 -66 dBm при MCS5/13 -65 dBm при MCS6/14 </p>
--	---

	<p>–64 dBm при MCS7/15</p> <p>HT-40</p> <p>–79 dBm при MCS0/8</p> <p>–76 dBm при MCS1/9</p> <p>–74 dBm при MCS2/10</p> <p>–71 dBm при MCS3/11</p> <p>–67 dBm при MCS4/12</p> <p>–63 dBm при MCS5/13</p> <p>–62 dBm при MCS6/14</p> <p>–61 dBm при MCS7/15</p>
Безопасность	<ul style="list-style-type: none"> • Wi-Fi Protected Access (WPA™ и WPA2™) • 802.1x • 64/128 битовое WEP-шифрование
Индикаторы	<ul style="list-style-type: none"> • Link • Activity
Поддержка ОС	Windows 98SE, ME, 2000, XP, Vista (32/64 бит)
Сертификаты	<ul style="list-style-type: none"> • FCC Class B • IC • Wi-Fi • Wi-Fi Protected Setup • WMM PS • CE • C-Tick • VCCI • TETEC
Рабочая температура	От 0° до 40°C
Рабочая влажность	От 10% до 90% (без образования конденсата)
Температура хранения	От -20° до 65°C
Влажность хранения	От 5% до 95% (без образования конденсата)
Размеры	13 x 89 x 28 мм
Вес	45,36 г

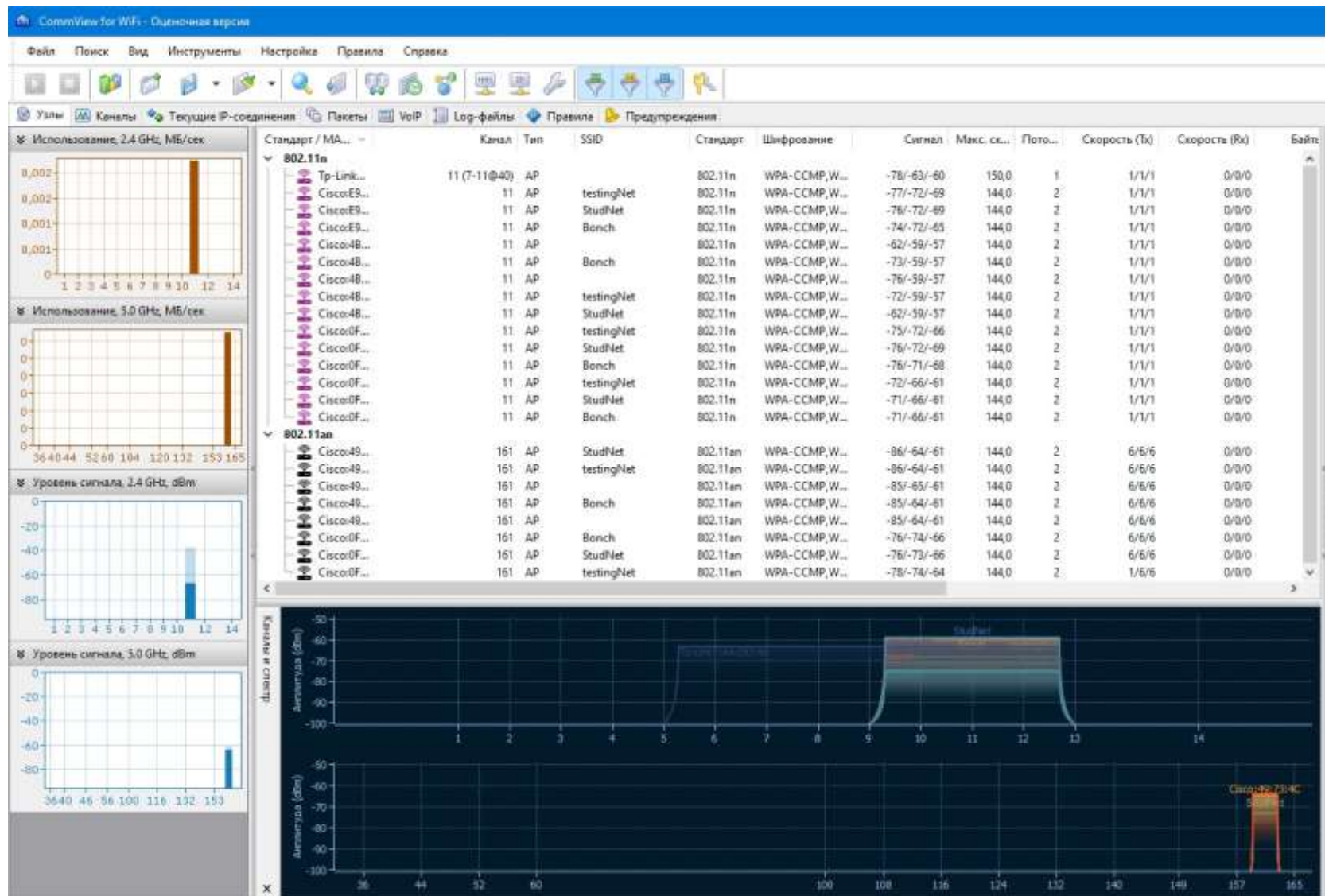


Рис. 2.1 Интерфейс программы ComView

2.2 Методика проведения эксперимента

Эксперимент проводится на 4 этаже 2 корпуса университета. Сеть данного этажа была разбита на 8 локальных сегментов (представлено на рисунке 2.2)

Для захвата пакетов использовалась программа CommView for Wi-Fi версии 7.1 и 2 двухдиапазонных USB-адаптера модели D-Link DWA-160.

Захват длился в 5 этапов:

- 1) Оценка загруженности каналов Wi-Fi
- 2) Выбор 2-х каналов на разных частотных диапазонах. Каждый из выбранных каналов отвечал следующему условию - превосходство по количеству доступных точек подключения и уровню сигнала над каналами того же частотного диапазона.
- 3) Перехват пакетов всех типов (*Management, Control, Data*) (суммарно 5 тыс. пакетов в каждом локальном сегменте)
- 4) Перехват исключительно *Management* пакетов
- 5) Анализ полученных результатов

На рисунках 2.3 и 2.4 приведены примеры фрейма *Probe response* на разных частотах. Сами фреймы являются «указателями» как на присутствие, так и на потенциальную возможность междиапазонного хэндовера в данном сегменте сети.

Подтверждение сетью возможности междиапазонного хэндовера для устройства. На рисунке 2.5 можно увидеть запрос от устройства на подключение к сети на 5 ГГц (фрейм №22), и ответное подтверждение сеть данной возможности (фреймы 22, 15-17). Ниже представлен подробный состав фрейма *Probe request* на разных частотах (рисунки 2.6 и 2.7).

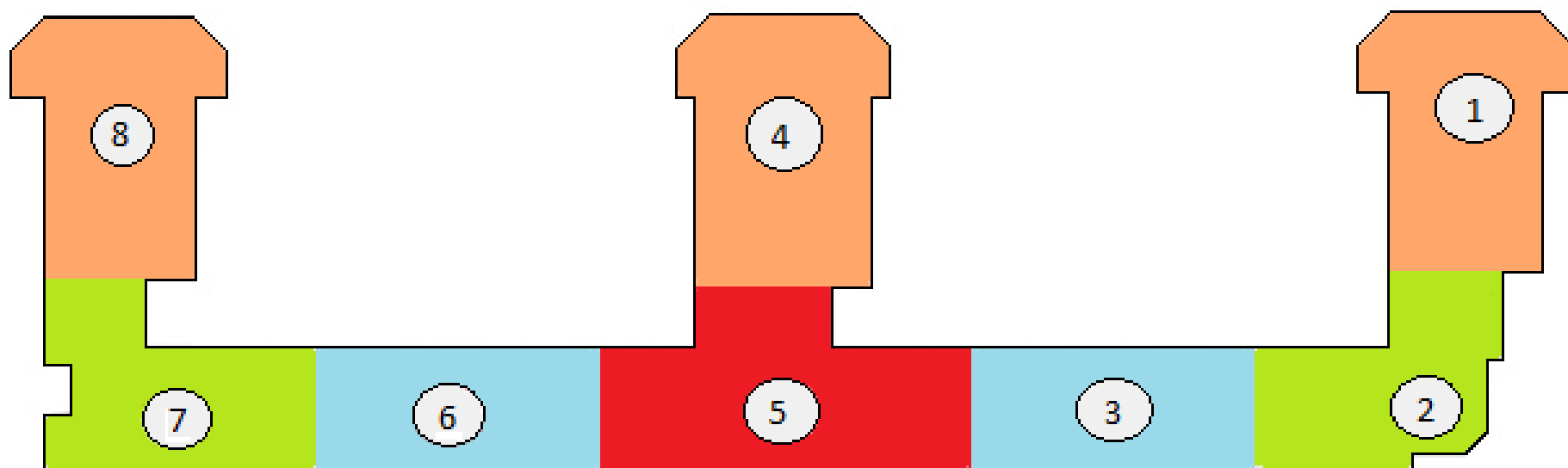


Рис. 2.2 Разделение сети Wi-Fi на локальные сегменты (4 этаж университета, корпус 2)

Log Viewer [4 etage .centr(2).1.ncf]

Файл Поиск Правила

Wireless Packet Info

- Signal level: 51%
- Signal level in dBm: -65
- Noise level in dBm: -96
- Rate: 6.0 Mbps
- Band: 5 GHz
- Channel: 161 - 5805 MHz
- Дата: 24-апр-2017
- Время: 16:20:48,080783
- Интервал: 0,000507
- Размер фрейма: 277 байты
- Номер фрейма: 5

802.11

- Frame Control: 0x0850 (2128)
- Protocol version: 0
- To DS: 0
- From DS: 0
- More Fragments: 0
- Retry: 1
- Power Management: 0
- More Data: 0
- Protected Frame: 0
- Order: 0
- Type: 0 - Management
- Subtype: 5 - Probe response
- Duration: 0x003C (60)
- Destination Address: 70:70:0D:
- Source Address: D4:A0:2A:49:7:
- BSS ID: D4:A0:2A:49:73:4B
- Fragment Number: 0x0000 (0)
- Sequence Number: 0x0F27 (3879)
- Probe response
- Timestamp: 1653811.100410 sec
- Rate: 6.0 Mbps

№	Протокол	MAC источ.	MAC назн.	IP источн.	IP назн.	Порт источн.	Порт назн.	Время	Сигнал	Скорость	Канал	Детали
8	ENCR. DATA	70:70:0D:80:79:F4	33:33:00:00:00:FB	? N/A	? N/A	N/A	N/A	16:20:45,837994	-71	11	11	WPA: Can't decrypt
6	MNGT/PROBE REQ.	70:70:0D:80:79:F4	Broadcast	? N/A	? N/A	N/A	N/A	16:20:48,070449	-83	6	161	SSID=Bonch, Seq=2647
1	MNGT/PROBE RESP.	Cisco:49:73:4B	70:70:0D:80:79:F4	? N/A	? N/A	N/A	N/A	16:20:48,070904	-64	6	161	SSID=Bonch, (Infra), Ch.#161, Seq=3878, BI=102
2	MNGT/PROBE RESP.	Cisco:49:73:4B	70:70:0D:80:79:F4	? N/A	? N/A	N/A	N/A	16:20:48,071539	-62	6	161	SSID=Bonch, (Infra), Ch.#161, Seq=3878, BI=102
7	MNGT/PROBE REQ.	70:70:0D:80:79:F4	Broadcast	? N/A	? N/A	N/A	N/A	16:20:48,079767	-82	6	161	SSID=Bonch, Seq=2648
4	MNGT/PROBE RESP.	Cisco:49:73:4B	70:70:0D:80:79:F4	? N/A	? N/A	N/A	N/A	16:20:48,080276	-63	6	161	SSID=Bonch, (Infra), Ch.#161, Seq=3879, BI=102
5	MNGT/PROBE RESP.	Cisco:49:73:4B	70:70:0D:80:79:F4	? N/A	? N/A	N/A	N/A	16:20:48,080783	-65	6	161	SSID=Bonch, (Infra), Ch.#161, Seq=3879, BI=102
3	MNGT/PROBE RESP.	Cisco:4B:82:44	70:70:0D:80:79:F4	? N/A	? N/A	N/A	N/A	16:20:48,161871	-59	1	11	SSID=Bonch, (Infra), Ch.#11, Seq=2368, BI=102
9	EAPOL	70:70:0D:80:79:F4	Cisco:CC:99:8F	? N/A	? N/A	N/A	N/A	16:20:48,207137	-86	6	161	EAPOL-Key (4-Way Handshake Message 4), Length = 95


```

0x0000 50 08 3C 00 70 70 0D 80-79 F4 D4 A0 2A 49 73 4B P.<.pp.БуФФ *IsK
0x0010 D4 A0 2A 49 73 4B 70 F2-FA BA D2 0E 81 01 00 00 Ф *IsКртъеТ.г...
0x0020 66 00 11 10 00 05 42 6F-6E 63 68 01 08 8C 12 98 f....Bonch..b.
0x0030 24 B0 48 60 6C 07 0C 52-55 20 24 08 14 84 03 14 $°H'1..RU $...
0x0040 95 04 14 0B 05 00 00 08-8D 5B 2D 1A 6E 18 1B FF *......К[-.п.я
0x0050 FF 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 я.....
0x0060 00 00 00 00 00 00 30 18-01 00 00 0F AC 02 02 00 .....0.....
0x0070 00 0F AC 02 00 0F AC 04-01 00 00 0F AC 02 28 00 .....(.....
0x0080 3D 16 A1 08 04 00 00 00-00 00 00 00 00 00 00 00 =.У.....
0x0090 00 00 00 00 00 00 00 00-85 1E 02 00 8F 00 0F 00 .....
0x00A0 FF 03 59 00 41 50 2E 34-2D 31 36 00 00 00 00 00 я.Y.AP.4-16....
0x00B0 00 00 00 00 00 00 39-96 06 00 40 96 00 11 00 .....9-...@-...
0x00C0 DD 1C 00 50 F2 01 01 00-00 50 F2 02 02 00 00 50 Э..Рт...Рт...Р
0x00D0 F2 02 00 50 F2 04 01 00-00 50 F2 02 00 00 DD 18 т..Рт...Рт...Э.
0x00E0 00 50 F2 02 01 01 80 00-03 A4 00 00 27 A4 00 00 .Рт...Ъ..н..н..
0x00F0 42 43 5E 00 62 32 2F 00-DD 06 00 40 96 01 01 04 ВС^..b2/.Э..@-...
0x0100 DD 05 00 40 96 03 05 DD-05 00 40 96 08 09 DD 05 Э..@-...Э..@-...Э.
0x0110 00 40 96 14 01 .@-...

```

Рис. 2.3 Фрейм *Probe response* на частоте 5 ГГц

Wireless Packet Info
 Signal level: 33%
 Signal level in dBm: -59
 Noise level in dBm: -96
 Rate: 1.0 Mbps
 Band: 2.4 GHz
 Channel: 11 - 2462 MHz
 Дата: 24-апр-2017
 Время: 16:20:48,161871
 Интервал: 0,090332
 Размер фрейма: 283 байты
 Номер фрейма: 3

802.11
 Frame Control: 0x0850 (2128)
 Protocol version: 0
 To DS: 0
 From DS: 0
 More Fragments: 0
 Retry: 1
 Power Management: 0
 More Data: 0
 Protected Frame: 0
 Order: 0
 Type: 0 - Management
 Subtype: 5 - Probe response
 Duration: 0x00DA (218)
 Destination Address: 70:70:0D:
 Source Address: D4:A0:2A:4B:8:
 BSS ID: D4:A0:2A:4B:82:44
 Fragment Number: 0x0000 (0)
 Sequence Number: 0x0940 (2368)
 Probe response
 Timestamp: 1653813.332903 sec

№	Протокол	MAC источ.	MAC назн.	IP источн.	IP назн.	Порт источн.	Порт назн.	Время	Сигнал	Скорость	Канал	Детали
8	ENCR. DATA	70:70:0D:80:79:F4	33:33:00:00:00:FB	? N/A	? N/A	N/A	N/A	16:20:45,837994	-71	11	11	WPA: Can't decrypt
6	MNGT/PROBE REQ.	70:70:0D:80:79:F4	Broadcast	? N/A	? N/A	N/A	N/A	16:20:48,070449	-83	6	161	SSID=Bonch, Seq=2647
1	MNGT/PROBE RESP.	Cisco:49:73:4B	70:70:0D:80:79:F4	? N/A	? N/A	N/A	N/A	16:20:48,070904	-64	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=3878, BI=102
2	MNGT/PROBE RESP.	Cisco:49:73:4B	70:70:0D:80:79:F4	? N/A	? N/A	N/A	N/A	16:20:48,071539	-62	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=3878, BI=102
7	MNGT/PROBE REQ.	70:70:0D:80:79:F4	Broadcast	? N/A	? N/A	N/A	N/A	16:20:48,079767	-82	6	161	SSID=Bonch, Seq=2648
4	MNGT/PROBE RESP.	Cisco:49:73:4B	70:70:0D:80:79:F4	? N/A	? N/A	N/A	N/A	16:20:48,080276	-63	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=3879, BI=102
5	MNGT/PROBE RESP.	Cisco:49:73:4B	70:70:0D:80:79:F4	? N/A	? N/A	N/A	N/A	16:20:48,080783	-65	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=3879, BI=102
3	MNGT/PROBE RESP.	Cisco:4B:82:44	70:70:0D:80:79:F4	? N/A	? N/A	N/A	N/A	16:20:48,161871	-59	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=2368, BI=102
9	EAPOL	70:70:0D:80:79:F4	Cisco:CC:99:8F	? N/A	? N/A	N/A	N/A	16:20:48,207137	-86	6	161	EAPOL-Key (4-Way Handshake Message 4), Length = 95

0x0000	50 08 DA 00 70 70 0D 80-79 F4 D4 A0 2A 4B 82 44	P.б.пр.БуфФ *K,D
0x0010	D4 A0 2A 4B 82 44 00 94-A7 CB F4 0E 81 01 00 00	Ф *K,D."\$ЛФ.f...
0x0020	66 00 31 14 00 05 42 6F-6E 63 68 01 08 82 84 8B	f.1...Bonch.,,.,,
0x0030	0C 12 96 18 24 03 01 08-07 06 52 55 20 01 0D 14	...\$.RU ...
0x0040	0B 05 00 00 B8 8D 5B 2A-01 00 2D 1A 2C 18 1B FF	...eK[*,.,.,я
0x0050	FF 00 00 00 00 00 00 00-00 00 00 00 00 00 00	я.....
0x0060	00 00 00 00 00 00 30 18-01 00 00 0F AC 02 02 000.....
0x0070	00 0F AC 02 00 0F AC 04-01 00 00 0F AC 02 28 007.(.
0x0080	32 04 30 48 60 6C 3D 16-08 00 07 00 00 00 00 00	2.0H^1=.....
0x0090	00 00 00 00 00 00 00 00-00 00 00 00 00 85 1E
0x00A0	0E 00 8F 00 0F 00 FF 03-59 00 41 50 2E 34 2D 31	..U...я.Y.AP.4-1
0x00B0	37 00 00 00 00 00 00 00-00 00 00 00 3A 96 06	7.....t-.
0x00C0	00 40 96 00 05 00 DD 1C-00 50 F2 01 01 00 00 50	.@-...Э..Рт....P
0x00D0	F2 02 02 00 00 50 F2 02-00 50 F2 04 01 00 00 50	т....Рт..Рт....P
0x00E0	F2 02 00 00 DD 18 00 50-F2 02 01 01 80 00 03 A4	т...Э..Рт...Б..н
0x00F0	00 00 27 A4 00 00 42 43-5E 00 62 32 2F 00 DD 06	..'н..BC^..b2/..Э.
0x0100	00 40 96 01 01 04 DD 05-00 40 96 03 05 DD 05 00	.@-...Э..@-...Э..
0x0110	40 96 0B 09 DD 05 00 40-96 14 01	@-...Э..@-...

Рис. 2.4 Фрейм Probe response на частоте 2.4 ГГц

4 этаж центральный сегмент (точка под номером 4 на схеме локальной сегментации)

№	Протокол	MAC источ.	MAC назн.	IP источн.	IP назн.	Порт источн.	Порт назн.	Время	Сигнал	Скорость	Канал	Детали
638	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:14:57,356498	-62	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
631	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:14:57,356646	-63	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
630	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:14:57,357123	-63	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
632	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:14:57,359184	-62	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
634	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:14:57,380925	-62	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
633	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:14:57,386620	-62	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
646	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:14:57,375893	-62	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
645	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:14:57,380800	-63	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
647	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:14:57,381000	-65	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
649	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:14:57,381876	-63	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
648	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:14:57,382376	-65	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
641	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:14:57,382524	-65	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
640	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:14:57,385000	-66	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
642	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:14:57,393378	-69	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
644	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:14:57,395994	-68	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
27	MNGT/PROBE REQ.	1C:CD:ES:3B:09...	Broadcast	? N/A	? N/A	N/A	N/A	16:14:58,120052	-58	1	11	SSID=any, Seq=899
26	MNGT/PROBE RES.	1C:CD:ES:3B:09...	Broadcast	? N/A	? N/A	N/A	N/A	16:14:58,121893	-58	1	11	SSID=any, Seq=900
14	MNGT/PROBE RESP.	Cisco:CC:99:80	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:14:58,124634	-51	1	11	SSID=Bonch, (infra), Ch.#11, Seq=1537, Bl=...
10	MNGT/PROBE RESP.	Cisco:CC:99:80	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:14:58,127634	-51	1	11	SSID=Bonch, (infra), Ch.#11, Seq=1537, Bl=...
9	MNGT/PROBE RESP.	Cisco:CC:99:82	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:14:58,133128	-52	1	11	SSID=testingNet, (infra), Ch.#11, Seq=1538, ...
13	MNGT/PROBE RESP.	Cisco:CC:99:82	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:14:58,136113	-51	1	11	SSID=testingNet, (infra), Ch.#11, Seq=1538, ...
11	MNGT/PROBE RESP.	Cisco:CC:99:81	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:14:58,139268	-52	1	11	SSID=StudNet, (infra), Ch.#11, Seq=1539, Bl=...
12	MNGT/PROBE RESP.	Cisco:CC:99:81	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:14:58,146124	-52	1	11	SSID=StudNet, (infra), Ch.#11, Seq=1539, Bl=...
24	MNGT/PROBE REQ.	1C:CD:ES:3B:09...	Broadcast	? N/A	? N/A	N/A	N/A	16:14:58,174766	-57	1	11	SSID=any, Seq=901
20	MNGT/PROBE REQ.	1C:CD:ES:3B:09...	Broadcast	? N/A	? N/A	N/A	N/A	16:14:58,176821	-56	1	11	SSID=any, Seq=902
18	MNGT/PROBE REQ.	1C:CD:ES:3B:09...	Broadcast	? N/A	? N/A	N/A	N/A	16:14:58,239525	-57	1	11	SSID=any, Seq=903
21	MNGT/PROBE REQ.	1C:CD:ES:3B:09...	Broadcast	? N/A	? N/A	N/A	N/A	16:14:58,241302	-59	1	11	SSID=any, Seq=904
5	MNGT/PROBE RESP.	Cisco:CC:99:80	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:14:58,243894	-51	1	11	SSID=Bonch, (infra), Ch.#11, Seq=1540, Bl=...
4	MNGT/PROBE RESP.	Cisco:CC:99:82	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:14:58,246764	-51	1	11	SSID=testingNet, (infra), Ch.#11, Seq=1541, ...
2	MNGT/PROBE RESP.	Cisco:CC:99:81	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:14:58,252165	-51	1	11	SSID=StudNet, (infra), Ch.#11, Seq=1542, Bl=...
1	MNGT/PROBE RESP.	Cisco:CC:99:80	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:14:58,257934	-52	1	11	SSID=Bonch, (infra), Ch.#11, Seq=1543, Bl=...
3	MNGT/PROBE RESP.	Cisco:CC:99:80	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:14:58,263009	-52	1	11	SSID=Bonch, (infra), Ch.#11, Seq=1543, Bl=...
7	MNGT/PROBE RESP.	Cisco:CC:99:82	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:14:58,267257	-51	1	11	SSID=testingNet, (infra), Ch.#11, Seq=1544, ...
6	MNGT/PROBE RESP.	Cisco:CC:99:82	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:14:58,271191	-51	1	11	SSID=testingNet, (infra), Ch.#11, Seq=1544, ...
8	MNGT/PROBE RESP.	Cisco:CC:99:81	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:14:58,274152	-51	1	11	SSID=StudNet, (infra), Ch.#11, Seq=1545, Bl=...
22	MNGT/PROBE REQ.	1C:CD:ES:3B:09...	Broadcast	? N/A	? N/A	N/A	N/A	16:15:00,398021	-63	6	161	SSID=any, Seq=921
16	MNGT/PROBE RESP.	Cisco:CC:99:8F	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:15:00,398519	-57	6	161	SSID=Bonch, (infra), Ch.#161, Seq=3089, Bl=...
15	MNGT/PROBE RESP.	Cisco:CC:99:8D	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:15:00,399657	-58	6	161	SSID=testingNet, (infra), Ch.#161, Seq=3090, B=...
17	MNGT/PROBE RESP.	Cisco:CC:99:8E	1C:CD:ES:3B:09...	? N/A	? N/A	N/A	N/A	16:15:00,400018	-58	6	161	SSID=StudNet, (infra), Ch.#161, Seq=3091, B=...
643	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:15:00,571010	-66	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
629	MNGT/AUTH	1C:CD:ES:3B:09...	Cisco:0F:5A:1F	? N/A	? N/A	N/A	N/A	16:15:00,571369	-66	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...

Рис. 2.5 Management- пакеты центрального локального сегмента сети (упорядочивание по времени)

Wireless Packet Info
 Signal level: 35%
 Signal level in dBm: -58
 Noise level in dBm: -96
 Rate: 1.0 Mbps
 Band: 2.4 GHz
 Channel: 11 - 2462 MHz
 Дата: 24-апр-2017
 Время: 16:14:58,120052
 Интервал: -0,001841
 Размер фрейма: 190 байты
 Номер фрейма: 27

802.11
 Frame Control: 0x0040 (64)
 Protocol version: 0
 To DS: 0

№	Протокол	MAC источ.	MAC назн.	IP источн.	IP назн.	Порт источн.	Порт назн.	Время	Сигнал	Скорость	Канал	Детали
27	MNGT/PROBE REQ.	1C:CD:E5:3B:09:...	Broadcast	? N/A	? N/A	N/A	N/A	16:14:58,120052	-58	1	11	SSID=any, Seq=899
26	MNGT/PROBE REQ.	1C:CD:E5:3B:09:...	Broadcast	? N/A	? N/A	N/A	N/A	16:14:58,121893	-58	1	11	SSID=any, Seq=900
14	MNGT/PROBE RESP.	Cisco:CC:99:80	1C:CD:E5:3B:09:...	? N/A	? N/A	N/A	N/A	16:14:58,124624	-51	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=1537, Bl=...

```

0x0000 40 00 00 00 FF FF FF FF FF 1C CD E5 3B 09 37 @...яяяяя.Не;.7
0x0010 FF FF FF FF FF FF 30 38-00 00 01 08 82 84 8B 96 яяяяяя08.....<
0x0020 0C 12 18 24 32 04 30 48-60 6C 7F 04 00 00 0A 02 ...$2.0H`ll.....
0x0030 DD 79 00 50 F2 04 10 4A-00 01 10 10 3A 00 01 00 Эу.Рт..J.....
0x0040 10 08 00 02 42 88 10 47-00 10 4E E4 A2 B6 A7 86 ...В€.Г..НдўЅ†
0x0050 5A 55 A9 C2 B8 B9 10 A3-09 94 10 54 00 08 00 0A ZU0B»№.Э.М.Т....
0x0060 00 50 F2 04 00 05 10 3C-00 01 03 10 02 00 02 00 .Рт....<.....
0x0070 00 10 09 00 02 00 00 10-12 00 02 00 00 10 21 00 .....!.....
0x0080 05 4D 65 69 7A 75 10 23-00 03 55 31 30 10 24 00 .Meizu.#.U10.$..
0x0090 03 55 31 30 10 11 00 09-6D 65 69 7A 75 5F 55 31 .U10....meizu_U1
0x00A0 30 10 49 00 06 00 37 2A-00 01 20 DD 11 50 6F 9A 0.I...7*.. Э.Роль...%.
0x00B0 09 02 02 00 25 00 06 05-00 52 55 04 51 0B- ...%.RU.Q.

```

Рис. 2.6 Фрейм Probe request на частоте 2.4 ГГц

Wireless Packet Info
 Signal level: 55%
 Signal level in dBm: -63
 Noise level in dBm: -96
 Rate: 6.0 Mbps
 Band: 5 GHz
 Channel: 161 - 5805 MHz
 Дата: 24-апр-2017
 Время: 16:15:00,398021
 Интервал: 2,156719
 Размер фрейма: 184 байты
 Номер фрейма: 22

802.11
 Frame Control: 0x0040 (64)
 Protocol version: 0
 To DS: 0
 From DS: 0

№	Протокол	MAC источ.	MAC назн.	IP источн.	IP назн.	Порт источн.	Порт назн.	Время	Сигнал	Скорость	Канал	Детали
8	MNGT/PROBE RESP.	Cisco:CC:99:81	1C:CD:E5:3B:09:...	? N/A	? N/A	N/A	N/A	16:14:58,274152	-51	1	11	SSID=StudNet, (Infra.), Ch.#11, Seq=1545, Bl=...
22	MNGT/PROBE RESP.	1C:CD:E5:3B:09:...	Broadcast	? N/A	? N/A	N/A	N/A	16:15:00,398021	-63	6	161	SSID=any, Seq=921
16	MNGT/PROBE RESP.	Cisco:CC:99:8F	1C:CD:E5:3B:09:...	? N/A	? N/A	N/A	N/A	16:15:00,398519	-57	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=3089, Bl=...

```

0x0000 40 00 00 00 FF FF FF FF FF 1C CD E5 3B 09 37 @...яяяяя.Не;.7
0x0010 FF FF FF FF FF FF 90 39-00 00 01 08 0C 12 18 24 яяяяяяћ9.....$
0x0020 30 48 60 6C 7F 04 00 00-0A 02 DD 79 00 50 F2 04 0H`ll.....Эу.Рт.
0x0030 10 4A 00 01 10 10 3A 00-01 00 10 08 00 02 42 88 .J.....В€.
0x0040 10 47 00 10 4E E4 A2 B6-A7 86 5A 55 A9 C2 B8 B9 .G..НдўЅ†ZU0B»№
0x0050 10 A3 09 94 10 54 00 08-00 0A 00 50 F2 04 00 05 .Э.М.Т.....Рт...
0x0060 10 3C 00 01 03 10 02 00-02 00 00 10 09 00 02 00 .<.....
0x0070 00 10 12 00 02 00 00 10-21 00 05 4D 65 69 7A 75 .....!...Meizu
0x0080 10 23 00 03 55 31 30 10-24 00 03 55 31 30 10 11 .#.U10.$..U10...
0x0090 00 09 6D 65 69 7A 75 5F-55 31 30 10 49 00 06 00 ..meizu_U10.I...
0x00A0 37 2A 00 01 20 DD 11 50-6F 9A 09 02 02 00 25 00 7*.. Э.Роль...%.
0x00B0 06 05 00 52 55 04 51 0B- ...RU.Q.

```

Рис. 2.7 Фрейм Probe request на частоте 5 ГГц

1 локальный сегмент сети Wi-Fi

Все перехваченные Management- пакеты были на диапазоне 5ГГц, что является показателем отсутствия необходимости междиапазонного хэндовера в данном сегменте сети (рис. 2.9)

The screenshot displays network analysis data. On the left, 'Wireless Packet Info' shows signal level at -85 dBm, noise level at -96 dBm, and a rate of 6.0 Mbps on a 5 GHz channel. Below it, 'Frame Control: 0x0040 (64)' lists protocol version, DS, and management type. The main table lists 8 management packets with their protocols, MAC addresses, and details. At the bottom, a hex dump shows the raw bytes of a packet, with ASCII characters visible on the right side.

№	Протокол	MAC источ.	MAC назн.	IP источн.	IP назн.	Порт источн.	Порт назн.	Время	Сигнал	Скорость	Канал	Детали
1	MNGT/PR...	E2:E3:D6:82:3F:55	Broadcast	? N/A	? N/A	N/A	N/A	15:23:...	-85	6	64	SSID=any, Seq=3654
2	MNGT/PR...	Cisco:CC:9D:4B	E2:E3:D6:82:3F:55	? N/A	? N/A	N/A	N/A	15:23:...	-78	6	64	SSID=Borch, (Infra.), Ch.#64, Seq=216, BI=102
3	MNGT/PR...	Cisco:CC:9D:4B	E2:E3:D6:82:3F:55	? N/A	? N/A	N/A	N/A	15:23:...	-78	6	64	SSID=Borch, (Infra.), Ch.#64, Seq=213, BI=102
4	MNGT/PR...	Cisco:CC:9D:4E	E2:E3:D6:82:3F:55	? N/A	? N/A	N/A	N/A	15:23:...	-78	6	64	SSID=StudNet, (Infra.), Ch.#64, Seq=215, BI=...
5	MNGT/PR...	Cisco:CC:9D:4D	E2:E3:D6:82:3F:55	? N/A	? N/A	N/A	N/A	15:23:...	-78	6	64	SSID=testingNet, (Infra.), Ch.#64, Seq=214, BI=...
6	MNGT/PR...	Cisco:CC:9D:4D	E2:E3:D6:82:3F:55	? N/A	? N/A	N/A	N/A	15:23:...	-78	6	64	SSID=testingNet, (Infra.), Ch.#64, Seq=214, BI=...
7	MNGT/PR...	Cisco:CC:9D:4D	E2:E3:D6:82:3F:55	? N/A	? N/A	N/A	N/A	15:23:...	-79	6	64	SSID=testingNet, (Infra.), Ch.#64, Seq=217, BI=...
8	MNGT/PR...	Cisco:CC:9D:4E	E2:E3:D6:82:3F:55	? N/A	? N/A	N/A	N/A	15:23:...	-78	6	64	SSID=StudNet, (Infra.), Ch.#64, Seq=218, BI=...

Hex dump details (hex | ASCII):

```

0x0000 40 00 00 00 FF FF FF FF FF E2 E3 D6 82 3F 55 @...яяяяяяЦ,?U
0x0010 FF FF FF FF FF FF 60 E4 00 00 01 00 0C 12 18 24 яяяяяя'д.....$
0x0020 30 48 60 6C 10 1A 65 00 17 FF 00 00 00 00 00 00 0H'L-...н.....
0x0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x0040 7F 00 04 00 00 04 00 00 00 40 6B 07 0F FF FF FF 1.....@...ннн
0x0050 FF FF FF 0F 0C 32 50 00 0F FE FF 00 00 FE FF 00 ннн1.2РЬ.нн...ннн
0x0060 00 00 00 00 17 F2 0A 00 01 04 00 00 00 00 00 00 -Э...Т.....Э..
0x0070 00 50 F2 00 00 0F 00 00 0D 09 00 18 18 02 00 00 -Рт.....Э.....
0x0080 10 00 00 ...
  
```

Рис. 2.8 Management- пакеты 1 локального сегмента сети (упорядочивание по времени)

2 локальный сегмент сети Wi-Fi

Наличие фрейма Probe response на канале 161 частотного диапазона 5 ГГц, являющегося запросом устройства на подключение к сети в данном частотном диапазоне, отсутствие фрейма Probe request на канале 161. Хэндовер возможен (так как устройство поддерживает 5 ГГц – подключение), но отсутствует (см. рис. 2.9)

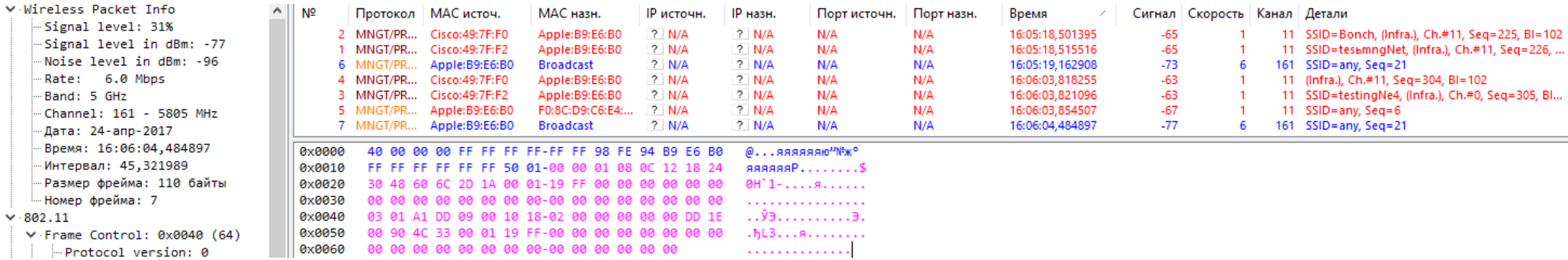


Рис. 2.9 Management- пакеты 2 локального сегмента сети (упорядочивание по времени)

3 локальный сегмент сети Wi-Fi

На рисунке 2.10 показан случай, при котором устройство поддерживает 5 ГГц, сеть обеспечивает возможность междиапазонного хэндовера. Несмотря на это, в том же локальном сегменте было обнаружено устройство, не получившее ответ от сети на этом диапазоне, хэндовер не произошел (см. рис.2.11)

№	Протокол	MAC источ.	MAC назн.	IP источ.	IP назн.	Порт источ.	Порт назн.	Вр...	Сигнал	Скорость	Канал	Детали
113	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-56	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2041, Bl...
55	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-75	6	161	SSID=Bonch, Seq=1567
106	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-54	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2040, Bl...
103	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-56	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2040, Bl...
62	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-75	6	161	SSID=Bonch, Seq=1566
124	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-56	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2039, Bl...
123	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-55	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2039, Bl...
60	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-76	6	161	SSID=Bonch, Seq=1565
127	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-55	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2038, Bl...
134	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-57	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2038, Bl...
49	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-75	6	161	SSID=Bonch, Seq=1564
102	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-54	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2037, Bl...
132	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-55	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2037, Bl...
76	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-75	6	161	SSID=Bonch, Seq=1563
137	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-54	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2036, Bl...
139	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-54	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2036, Bl...
69	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-77	6	161	SSID=Bonch, Seq=1562
79	MNGT/PR...	40:B8:9A:19:42:47	E4:FF:FF:FF:FF:FF	?/N/A	?/N/A	N/A	N/A	16:10:...	-72	1	11	SSID=any, Seq=1557
201	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-54	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2035, Bl...
200	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-54	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2035, Bl...
51	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-79	6	161	SSID=Bonch, Seq=1551
203	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-55	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2034, Bl...
202	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-54	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2034, Bl...
93	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-76	6	161	SSID=Bonch, Seq=1550
190	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-54	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2033, Bl...
95	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-78	6	161	SSID=Bonch, Seq=1549
189	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-56	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2032, Bl...
188	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-55	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2032, Bl...
90	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-79	6	161	SSID=Bonch, Seq=1548
193	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-56	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2031, Bl...
192	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-55	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2031, Bl...
94	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-79	6	161	SSID=Bonch, Seq=1547
191	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-54	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2030, Bl...
92	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-79	6	161	SSID=Bonch, Seq=1546
187	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-55	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2029, Bl...
103	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-56	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2029, Bl...
91	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-78	6	161	SSID=Bonch, Seq=1545
73	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-76	6	161	SSID=Bonch, Seq=1544
182	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-55	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2027, Bl...
72	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-77	6	161	SSID=Bonch, Seq=1543
181	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-56	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2026, Bl...
186	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-56	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2026, Bl...
75	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-78	6	161	SSID=Bonch, Seq=1542
185	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-56	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2025, Bl...
184	MNGT/PR...	Cisco:0F:30:4F	40:B8:9A:19:42:47	?/N/A	?/N/A	N/A	N/A	16:10:...	-55	6	161	SSID=Bonch (Infra), Ch.#161, Seq=2025, Bl...
67	MNGT/PR...	40:B8:9A:19:42:47	Broadcast	?/N/A	?/N/A	N/A	N/A	16:10:...	-79	6	161	SSID=Bonch, Seq=1541

Рис. 2.10 Management- пакеты 3 локального сегмента сети (упорядочивание по времени)

№	Протокол	MAC источ.	MAC назн.	IP источн.	IP назн.	Порт источн.	Порт назн.	Вр... /	Сигнал	Скорость	Канал	Детали
1	MNGT/PR...	Apple:39:FD:E7	Broadcast	? N/A	? N/A	N/A	N/A	16:10:...	-71	1	11	SSID=any, Seq=25
2	MNGT/PR...	Apple:39:FD:E7	Broadcast	? N/A	? N/A	N/A	N/A	16:10:...	-85	6	161	SSID=any, Seq=56
3	MNGT/PR...	Apple:39:FD:E7	Broadcast	? N/A	? N/A	N/A	N/A	16:09:...	-73	1	11	SSID=any, Seq=6
4	MNGT/PR...	Cisco:49:7F:F0	Apple:39:FD:E7	? N/A	? N/A	N/A	N/A	16:10:...	-70	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=1044, BI=...
5	MNGT/PR...	Cisco:49:7F:F1	Apple:39:FD:E7	? N/A	? N/A	N/A	N/A	16:10:...	-69	1	11	(Infra.), Ch.#0, Seq=1043, BI=102
6	MNGT/PR...	Cisco:49:7F:F2	Apple:39:FD:E7	? N/A	? N/A	N/A	N/A	16:10:...	-70	1	11	SSID=testingNet, (Infra.), Ch.#11, Seq=1042, ...
7	MNGT/PR...	Cisco:49:7F:F0	Apple:39:FD:E7	? N/A	? N/A	N/A	N/A	16:09:...	-70	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=1019, BI=...
8	MNGT/PR...	Cisco:49:7F:F0	Apple:39:FD:E7	? N/A	? N/A	N/A	N/A	16:09:...	-70	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=1019, BI=...
9	MNGT/PR...	Cisco:49:7F:F2	Apple:39:FD:E7	? N/A	? N/A	N/A	N/A	16:09:...	-69	1	11	SSID=testingNet, (Infra.), Ch.#11, Seq=1020, ...
10	MNGT/PR...	Cisco:49:7F:F1	Apple:39:FD:E7	? N/A	? N/A	N/A	N/A	16:09:...	-68	1	11	SSID=StudNet, (Infra.), Ch.#11, Seq=1021, Bl...
11	MNGT/PR...	Cisco:85:F1:E5	Apple:39:FD:E7	? N/A	? N/A	N/A	N/A	16:10:...	-71	1	11	SSID=StudNet, (Infra.), Ch.#11, Seq=1077, Bl...
12	MNGT/PR...	Cisco:49:7F:F0	Apple:39:FD:E7	? N/A	? N/A	N/A	N/A	16:10:...	-69	1	11	SSID=Bonch, (Infra.), Ch.#131, Seq=1047, Bl...

Рис. 2.11 *Management*- пакеты 3 локального сегмента сети (между другими устройствами)

5 локальный сегмент сети Wi-Fi

Отсутствие хэндовера

№	Протокол	MAC источ.	MAC назн.	IP источн.	IP назн.	Порт источн.	Порт назн.	Время	Сигнал	Скорость	Канал	Детали
1	MNGT/PR...	B2:90:70:FC:8F:E6	Broadcast	? N/A	? N/A	N/A	N/A	16:25:48,410077	-83	6	64	SSID=any, Seq=431
3	MNGT/PR...	Cisco:49:7D:21	B2:90:70:FC:8F:E6	? N/A	? N/A	N/A	N/A	16:25:47,625612	-70	1	11	SSID=StudNet, (Infra.), Ch.#11, Seq=78, BI=1...
6	MNGT/PR...	Cisco:49:7D:21	B2:90:70:FC:8F:E6	? N/A	? N/A	N/A	N/A	16:25:47,597660	-69	1	11	SSID=StudNet, (Infra.), Ch.#11, Seq=78, BI=1...
7	MNGT/PR...	Cisco:49:7D:22	B2:90:70:FC:8F:E6	? N/A	? N/A	N/A	N/A	16:25:47,592040	-69	1	11	SSID=testingNet, (Infra.), Ch.#11, Seq=77, Bl...
5	MNGT/PR...	Cisco:49:7D:22	B2:90:70:FC:8F:E6	? N/A	? N/A	N/A	N/A	16:25:47,577670	-70	1	11	SSID=testingNet, (Infra.), Ch.#11, Seq=77, Bl...
4	MNGT/PR...	Cisco:49:7D:24	B2:90:70:FC:8F:E6	? N/A	? N/A	N/A	N/A	16:25:47,574796	-69	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=76, BI=102
2	MNGT/PR...	B2:90:70:FC:8F:E6	FF:FF:EF:F6:FF:FF	? N/A	? N/A	N/A	N/A	16:25:47,569718	-73	1	11	SSID=any, Seq=414

Рис. 2.12 *Management*- пакеты 5 локального сегмента сети (упорядочивание по времени)

6 локальный сегмент сети Wi-Fi

Отсутствие междиапазонного хэндовера, устройство не получает ответ от сети на подключение 5 ГГц (см. рис. 2.13)

№	Протокол	MAC источ.	MAC назн.	IP источн.	IP назн.	Порт источн.	Порт назн.	Время	Сигнал	Скорость	Канал	Детали
6	MNGT/PR...	Cisco:0F:66:70	74:23:44:9B:16:56	? N/A	? N/A	N/A	N/A	16:31:52,827020	-57	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=2168, Bl=...
8	MNGT/PR...	74:23:44:9B:16:56	Broadcast	? N/A	? N/A	N/A	N/A	16:31:52,824482	-54	1	11	SSID=Bonch, Seq=523
5	MNGT/PR...	Cisco:0F:66:70	74:23:44:9B:16:56	? N/A	? N/A	N/A	N/A	16:31:52,815098	-61	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=2167, Bl=...
7	MNGT/PR...	74:23:44:9B:16:56	Broadcast	? N/A	? N/A	N/A	N/A	16:31:52,809995	-55	1	11	SSID=Bonch, Seq=522
9	MNGT/PR...	74:23:44:9B:16:56	Broadcast	? N/A	? N/A	N/A	N/A	16:31:41,475747	-64	6	64	SSID=Bonch, Seq=491
10	MNGT/PR...	74:23:44:9B:16:56	Broadcast	? N/A	? N/A	N/A	N/A	16:31:41,460648	-64	6	64	SSID=Bonch, Seq=490
4	MNGT/PR...	Cisco:0F:66:70	74:23:44:9B:16:56	? N/A	? N/A	N/A	N/A	16:31:41,013757	-63	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=2151, Bl=...
3	MNGT/PR...	Cisco:0F:66:70	74:23:44:9B:16:56	? N/A	? N/A	N/A	N/A	16:31:41,011014	-66	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=2151, Bl=...
2	MNGT/PR...	Cisco:0F:66:70	74:23:44:9B:16:56	? N/A	? N/A	N/A	N/A	16:31:41,002936	-62	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=2151, Bl=...
11	MNGT/PR...	74:23:44:9B:16:56	Broadcast	? N/A	? N/A	N/A	N/A	16:31:41,000327	-73	1	11	SSID=Bonch, Seq=487
1	MNGT/PR...	Cisco:0F:66:70	74:23:44:9B:16:56	? N/A	? N/A	N/A	N/A	16:31:40,987692	-63	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=2150, Bl=...

Рис. 2.13 *Management*- пакеты 6 локального сегмента сети (упорядочивание по времени)

7 локальный сегмент сети Wi-Fi

Присутствие междиапазонного хэндовера, подтверждение запроса от устройства сетью на подключение к каналу 161 (5ГГц), показано на рисунке 2.14

№	Протокол	MAC источ.	MAC назн.	IP источн.	IP назн.	Порт источн.	Порт назн.	Время	Сигнал	Скорость	Канал	Детали
1	MNGT/PR...	Cisco:CC:99:80	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,003474	-70	1	11	SSID=Bonch, (infra), Ch.#11, Seq=3816, Bl=...
2	MNGT/PR...	Cisco:CC:99:80	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,011600	-71	1	11	SSID=Bonch, (infra), Ch.#11, Seq=3816, Bl=...
3	MNGT/PR...	Cisco:CC:99:80	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,019907	-70	1	11	SSID=Bonch, (infra), Ch.#11, Seq=3817, Bl=...
4	MNGT/PR...	Cisco:CC:99:82	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,027969	-68	1	11	SSID=testingNet, (infra), Ch.#11, Seq=3818, ...
5	MNGT/PR...	Cisco:CC:99:82	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,030762	-69	1	11	SSID=testingNet, (infra), Ch.#11, Seq=3818, ...
6	MNGT/PR...	Cisco:CC:99:80	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,041969	-71	1	11	SSID=Bonch, (infra), Ch.#11, Seq=3819, Bl=...
7	MNGT/PR...	Cisco:CC:99:80	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,049730	-71	1	11	SSID=Bonch, (infra), Ch.#11, Seq=3819, Bl=...
8	MNGT/PR...	Cisco:CC:99:81	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,053010	-69	1	11	SSID=StudNet, (infra), Ch.#11, Seq=3820, Bl=...
9	MNGT/PR...	Cisco:CC:99:81	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,061224	-68	1	11	SSID=StudNet, (infra), Ch.#11, Seq=3820, Bl=...
10	MNGT/PR...	Cisco:CC:99:80	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,064593	-70	1	11	SSID=Bonch, (infra), Ch.#11, Seq=3821, Bl=...
11	MNGT/PR...	Cisco:CC:99:80	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,072597	-69	1	11	SSID=Bonch, (infra), Ch.#11, Seq=3821, Bl=...
12	MNGT/PR...	Cisco:CC:99:82	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,077849	-68	1	11	SSID=testingNet, (infra), Ch.#11, Seq=3822, ...
13	MNGT/PR...	Cisco:CC:99:82	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,083375	-68	1	11	SSID=testingNet, (infra), Ch.#11, Seq=3822, ...
14	MNGT/PR...	Cisco:CC:99:81	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,082223	-69	1	11	SSID=StudNet, (infra), Ch.#11, Seq=3823, Bl=...
15	MNGT/PR...	Cisco:CC:99:81	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,090907	-69	1	11	SSID=StudNet, (infra), Ch.#11, Seq=3823, Bl=...
16	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,489014	-83	6	161	SSID=Bonch, (infra), Ch.#161, Seq=4056, Bl=...
17	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,489470	-84	6	161	SSID=Bonch, (infra), Ch.#161, Seq=4056, Bl=...
18	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,489667	-83	6	161	SSID=Bonch, (infra), Ch.#161, Seq=4057, Bl=...
19	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,490468	-83	6	161	SSID=Bonch, (infra), Ch.#161, Seq=4057, Bl=...
20	MNGT/PR...	Cisco:E9:4B:2D	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,490966	-82	6	161	SSID=testingNet, (infra), Ch.#161, Seq=4058, ...
21	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,509995	-83	6	161	SSID=Bonch, (infra), Ch.#161, Seq=4060, Bl=...
22	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,510438	-82	6	161	SSID=Bonch, (infra), Ch.#161, Seq=4060, Bl=...
23	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,510936	-84	6	161	SSID=Bonch, (infra), Ch.#161, Seq=4061, Bl=...
24	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:39,511439	-87	6	161	SSID=Bonch, (infra), Ch.#161, Seq=4061, Bl=...
25	MNGT/AU...	Apple:22:ED:34	Cisco:E9:4B:2F	? N/A	? N/A	N/A	N/A	16:39:41,456078	-85	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
26	CTRL/ACK	N/A	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:41,456085	-85	6	161	
27	MNGT/AU...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:41,458568	-84	6	161	Status=Successful, Trans.Seq=2, Algo=Open ...
28	MNGT/AU...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:41,457073	-83	6	161	Status=Successful, Trans.Seq=2, Algo=Open ...
29	MNGT/AU...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:41,457080	-86	6	161	Status=Successful, Trans.Seq=2, Algo=Open ...
30	MNGT/PR...	Cisco:CC:99:80	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:42,278240	-66	1	11	SSID=Bonch, (infra), Ch.#11, Seq=3827, Bl=...
31	MNGT/PR...	Cisco:CC:99:80	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:42,290005	-67	1	11	SSID=Bonch, (infra), Ch.#11, Seq=3827, Bl=...
32	MNGT/PR...	Cisco:CC:99:82	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:42,321197	-67	1	11	SSID=testingNet, (infra), Ch.#11, Seq=3828, ...
33	MNGT/PR...	Cisco:CC:99:81	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:42,324200	-67	1	11	SSID=StudNet, (infra), Ch.#11, Seq=3829, Bl=...
34	MNGT/PR...	Cisco:CC:99:81	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:42,327828	-66	1	11	SSID=StudNet, (infra), Ch.#11, Seq=3829, Bl=...
35	MNGT/PR...	Apple:22:ED:34	Broadcast	? N/A	? N/A	N/A	N/A	16:39:42,540323	-85	6	161	SSID=any, Seq=144
36	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:42,540828	-84	6	161	SSID=Bonch, (infra), Ch.#161, Seq=4064, Bl=...
37	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:42,541328	-83	6	161	SSID=Bonch, (infra), Ch.#161, Seq=4064, Bl=...
38	MNGT/PR...	Cisco:E9:4B:2D	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:42,541831	-82	6	161	SSID=testingNet, (infra), Ch.#161, Seq=4065, ...
39	MNGT/PR...	Cisco:E9:4B:2D	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:42,542455	-83	6	161	SSID=testingNet, (infra), Ch.#161, Seq=4065, ...
40	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:42,551485	-83	6	161	SSID=Bonch, (infra), Ch.#161, Seq=4067, Bl=...
41	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:42,551953	-84	6	161	SSID=Bonch, (infra), Ch.#161, Seq=4067, Bl=...
42	MNGT/PR...	Cisco:E9:4B:2D	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:42,552573	-83	6	161	SSID=testingNet, (infra), Ch.#161, Seq=4068, ...
43	MNGT/PR...	Cisco:E9:4B:2E	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:42,554203	-84	6	161	SSID=StudNet, (infra), Ch.#161, Seq=4069, B=...
44	ENCR. DATA	Apple:22:ED:34	33:33:00:00:00:FB	? N/A	? N/A	N/A	N/A	16:39:47,000554	-70	5,5	11	WPA: Can't decrypt
45	ENCR. DATA	Apple:22:ED:34	01:00:5E:00:00:FB	? N/A	? N/A	N/A	N/A	16:39:47,001298	-67	5,5	11	WPA: Can't decrypt
46	ENCR. DATA	Apple:22:ED:34	33:33:00:00:00:FB	? N/A	? N/A	N/A	N/A	16:39:51,068819	-66	5,5	11	WPA: Can't decrypt
47	ENCR. DATA	Apple:22:ED:34	01:00:5E:00:00:FB	? N/A	? N/A	N/A	N/A	16:39:51,071432	-65	5,5	11	WPA: Can't decrypt

Рис. 2.14 Management- пакеты 7 локального сегмента сети (упорядочивание по времени)

8 локальный сегмент сети Wi-Fi

Абонентское устройство получило ответ от сети на канале 161 (5ГГц), пример подтвержденного междиапазонного хэндовера на рисунке 2.15

№	Протокол	MAC источ.	MAC назн.	IP источн.	IP назн.	Порт источн.	Порт назн.	Время	Сигнал	Скорость	Канал	Детали
12	MNGT/PROBE RESP.	Cisco:E9:62:32	00:9A:CD:CE:61:...	? N/A	? N/A	N/A	N/A	16:42:45,241948	-65	1	11	SSID=testingNet, (Infra.), Ch.#11, Seq=1872, ...
11	MNGT/PROBE RESP.	Cisco:E9:62:32	00:9A:CD:CE:61:...	? N/A	? N/A	N/A	N/A	16:42:45,247430	-65	1	11	SSID=testingNet, (Infra.), Ch.#11, Seq=1872, ...
13	MNGT/PROBE RESP.	Cisco:E9:5C:E0	00:9A:CD:CE:61:...	? N/A	? N/A	N/A	N/A	16:42:45,278150	-73	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=2301, Bl=...
14	MNGT/PROBE RESP.	Cisco:E9:5C:E0	00:9A:CD:CE:61:...	? N/A	? N/A	N/A	N/A	16:42:45,283289	-74	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=2301, Bl=...
2	MNGT/PROBE REQ.	00:9A:CD:CE:61:...	Broadcast	? N/A	? N/A	N/A	N/A	16:42:46,925413	-83	6	161	SSID=any, Seq=43
17	MNGT/PROBE RESP.	Cisco:E9:62:3F	00:9A:CD:CE:61:...	? N/A	? N/A	N/A	N/A	16:42:46,925941	-80	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=1671, Bl...
16	MNGT/PROBE RESP.	Cisco:E9:62:3F	00:9A:CD:CE:61:...	? N/A	? N/A	N/A	N/A	16:42:46,926409	-79	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=1671, Bl...
15	MNGT/PROBE RESP.	Cisco:E9:62:3D	00:9A:CD:CE:61:...	? N/A	? N/A	N/A	N/A	16:42:46,927035	-80	6	161	SSID=testingNet, (Infra.), Ch.#161, Seq=1672...
10	MNGT/PROBE RESP.	Cisco:E9:62:3D	00:9A:CD:CE:61:...	? N/A	? N/A	N/A	N/A	16:42:46,927535	-77	6	161	SSID=testingNet, (Infra.), Ch.#161, Seq=1672...
3	MNGT/PROBE RESP.	Cisco:E9:62:3E	00:9A:CD:CE:61:...	? N/A	? N/A	N/A	N/A	16:42:46,928035	-79	6	161	SSID=StudNet, (Infra.), Ch.#161, Seq=1673, B...
4	MNGT/PROBE RESP.	Cisco:E9:62:3E	00:9A:CD:CE:61:...	? N/A	? N/A	N/A	N/A	16:42:46,928533	-80	6	161	SSID=StudNet, (Infra.), Ch.#161, Seq=1673, B...
1	MNGT/PROBE REQ.	00:9A:CD:CE:61:...	Broadcast	? N/A	? N/A	N/A	N/A	16:42:46,967033	-79	6	161	SSID=any, Seq=44
6	MNGT/PROBE RESP.	Cisco:E9:62:3F	00:9A:CD:CE:61:...	? N/A	? N/A	N/A	N/A	16:42:46,967429	-80	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=1674, Bl...
7	MNGT/PROBE RESP.	Cisco:E9:62:3D	00:9A:CD:CE:61:...	? N/A	? N/A	N/A	N/A	16:42:46,967986	-80	6	161	SSID=testingNet, (Infra.), Ch.#161, Seq=1675...
9	MNGT/PROBE RESP.	Cisco:E9:62:3D	00:9A:CD:CE:61:...	? N/A	? N/A	N/A	N/A	16:42:46,968536	-80	6	161	SSID=testingNet, (Infra.), Ch.#161, Seq=1675...
8	MNGT/PROBE RESP.	Cisco:E9:62:3E	00:9A:CD:CE:61:...	? N/A	? N/A	N/A	N/A	16:42:46,969038	-80	6	161	SSID=StudNet, (Infra.), Ch.#161, Seq=1676, B...
5	MNGT/PROBE RESP.	Cisco:E9:62:3E	00:9A:CD:CE:61:...	? N/A	? N/A	N/A	N/A	16:42:46,969543	-80	6	161	SSID=StudNet, (Infra.), Ch.#161, Seq=1676, B...

Рис. 2.15 Management- пакеты 8 локального сегмента сети (упорядочивание по времени)

2.3 Территориальный анализ междиапазонного хэндовера

Фрейм-запрос *Проба* (*Probe request frame*)

Мобильные устройства с Wi-Fi отправляют фреймы-запросы *Пробы*, чтобы получить информацию от другого устройства. Например, радиокарта мобильного устройства отправляет *Пробы*-запросы, чтобы определить какие точки доступа находятся внутри зоны покрытия.

Фрейм-ответ на *Пробу* (*Probe response frame*)

Устройства с Wi-Fi будут отвечать фреймом-ответом на полученный фрейм-запрос *Проба*. Фрейм-ответ *Проба* содержит информацию о функциональности, поддерживаемых скоростях передачи данных и т.п.

Интенсивность появления запросов напрямую связано с количеством устройств, поддерживающих подключение к сети на частоте 5 ГГц. Она существенно варьируется в зависимости от локального сегмента сети, в котором проводился эксперимент.

Как видно из рисунка 2.16, междиапазонный хэндовер был подтвержден в сегментах 1,3,4,7,8. Проблемы с переходом устройств на частотный диапазон 5 ГГц были зафиксированы в сегментах 2, 5 и 6.

№	Протокол	MAC источ.	MAC назн.	IP источн.	IP назн.	Порт источн.	Порт назн.	Вр...	Сигнал	Скорость	Канал	Детали
8	MNGT/PR...	Cisco:CC:99:81	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-69	1	11	SSID=StudNet, (Infra.), Ch.#11, Seq=3820, Bl...
9	MNGT/PR...	Cisco:CC:99:81	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-68	1	11	SSID=StudNet, (Infra.), Ch.#11, Seq=3820, Bl...
10	MNGT/PR...	Cisco:CC:99:80	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-70	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=3821, Bl=...
11	MNGT/PR...	Cisco:CC:99:80	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-69	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=3821, Bl=...
12	MNGT/PR...	Cisco:CC:99:82	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-68	1	11	SSID=testingNet, (Infra.), Ch.#11, Seq=3822, ...
13	MNGT/PR...	Cisco:CC:99:82	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-68	1	11	SSID=testingNet, (Infra.), Ch.#11, Seq=3822, ...
14	MNGT/PR...	Cisco:CC:99:81	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-69	1	11	SSID=StudNet, (Infra.), Ch.#11, Seq=3823, Bl...
15	MNGT/PR...	Cisco:CC:99:81	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-69	1	11	SSID=StudNet, (Infra.), Ch.#11, Seq=3823, Bl...
16	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-83	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=4056, Bl...
17	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-84	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=4056, Bl...
18	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-83	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=4057, Bl...
19	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-83	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=4057, Bl...
20	MNGT/PR...	Cisco:E9:4B:2D	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-82	6	161	SSID=testingNet, (Infra.), Ch.#161, Seq=4058...
21	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-83	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=4060, Bl...
22	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-82	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=4060, Bl...
23	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-84	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=4061, Bl...
24	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-87	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=4061, Bl...
25	MNGT/AU...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-85	6	161	Status=Successful, Trans.Seq=1, Algo=Open ...
26	CTRL/ACK	N/A	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-85	6	161	
27	MNGT/AU...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-84	6	161	Status=Successful, Trans.Seq=2, Algo=Open ...
28	MNGT/AU...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-83	6	161	Status=Successful, Trans.Seq=2, Algo=Open ...
29	MNGT/AU...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-86	6	161	Status=Successful, Trans.Seq=2, Algo=Open ...
30	MNGT/PR...	Cisco:CC:99:80	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-66	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=3827, Bl=...
31	MNGT/PR...	Cisco:CC:99:80	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-67	1	11	SSID=Bonch, (Infra.), Ch.#11, Seq=3827, Bl=...
32	MNGT/PR...	Cisco:CC:99:82	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-67	1	11	SSID=testingNet, (Infra.), Ch.#11, Seq=3828, ...
33	MNGT/PR...	Cisco:CC:99:81	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-67	1	11	SSID=StudNet, (Infra.), Ch.#11, Seq=3829, Bl...
34	MNGT/PR...	Cisco:CC:99:81	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-66	1	11	SSID=StudNet, (Infra.), Ch.#11, Seq=3829, Bl...
35	MNGT/PR...	Apple:22:ED:34	Broadcast	? N/A	? N/A	N/A	N/A	16:39:...	-85	6	161	SSID=any, Seq=144
36	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-84	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=4064, Bl...
37	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-83	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=4064, Bl...
38	MNGT/PR...	Cisco:E9:4B:2D	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-82	6	161	SSID=testingNet, (Infra.), Ch.#161, Seq=4065...
39	MNGT/PR...	Cisco:E9:4B:2D	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-83	6	161	SSID=testingNet, (Infra.), Ch.#161, Seq=4065...
40	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-83	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=4067, Bl...
41	MNGT/PR...	Cisco:E9:4B:2F	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-84	6	161	SSID=Bonch, (Infra.), Ch.#161, Seq=4067, Bl...
42	MNGT/PR...	Cisco:E9:4B:2D	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-83	6	161	SSID=testingNet, (Infra.), Ch.#161, Seq=4068...
43	MNGT/PR...	Cisco:E9:4B:2E	Apple:22:ED:34	? N/A	? N/A	N/A	N/A	16:39:...	-84	6	161	SSID=StudNet, (Infra.), Ch.#161, Seq=4069, B...
44	ENCR. DATA	Apple:22:ED:34	33:33:00:00:00:FB	? N/A	? N/A	N/A	N/A	16:39:...	-70	5,5	11	WPA: Can't decrypt
45	ENCR. DATA	Apple:22:ED:34	01:00:5E:00:00:FB	? N/A	? N/A	N/A	N/A	16:39:...	-67	5,5	11	WPA: Can't decrypt
46	ENCR. DATA	Apple:22:ED:34	33:33:00:00:00:FB	? N/A	? N/A	N/A	N/A	16:39:...	-66	5,5	11	WPA: Can't decrypt
47	ENCR. DATA	Apple:22:ED:34	01:00:5E:00:00:FB	? N/A	? N/A	N/A	N/A	16:39:...	-65	5,5	11	WPA: Can't decrypt

Рис. 2.16 Пример определения наличия междиапазонного хэндовера

№	Протокол	MAC ист.	MAC нак.	IP ист.	IP нак.	Порт ист.	Порт нак.	Вр...	Сигнал	Скорость	Канал	Детали
17	ENCR_DATA	40:B8:9A:19:42:47	01:00:5E:00:00:FC	? N/A	? N/A	N/A	N/A	16:10...	-56	6	161	WR: Can't decrypt
18	ENCR_DATA	40:B8:9A:19:42:47	01:00:5E:00:00:FC	? N/A	? N/A	N/A	N/A	16:10...	-54	6	161	WR: Can't decrypt
19	ENCR_DATA	40:B8:9A:19:42:47	01:00:5E:00:00:FC	? N/A	? N/A	N/A	N/A	16:10...	-54	6	161	WR: Can't decrypt
12	ENCR_DATA	40:B8:9A:19:42:47	01:00:5E:00:00:FB	? N/A	? N/A	N/A	N/A	16:10...	-56	6	161	WR: Can't decrypt
16	ENCR_DATA	40:B8:9A:19:42:47	01:00:5E:00:00:FB	? N/A	? N/A	N/A	N/A	16:10...	-54	6	161	WR: Can't decrypt
153	MNGT.FR...	Cisco49:7F:FD	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-70	7	11	SSID=Bonch, (Infra), Ch#11, Seq=1068, Bl...
67	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-79	6	161	SSID=Bonch, Seq=1541
184	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-55	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2025, Bl...
185	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-56	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2025, Bl...
75	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-78	6	161	SSID=Bonch, Seq=1542
188	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-56	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2026, Bl...
181	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-56	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2026, Bl...
72	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-77	6	161	SSID=Bonch, Seq=1543
182	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-55	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2027, Bl...
73	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-78	6	161	SSID=Bonch, Seq=1544
91	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-78	6	161	SSID=Bonch, Seq=1545
183	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-56	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2028, Bl...
187	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-55	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2028, Bl...
92	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-79	6	161	SSID=Bonch, Seq=1546
121	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-54	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2030, Bl...
94	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-79	6	161	SSID=Bonch, Seq=1547
192	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-55	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2031, Bl...
193	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-56	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2031, Bl...
95	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-79	6	161	SSID=Bonch, Seq=1548
188	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-55	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2032, Bl...
189	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-56	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2032, Bl...
95	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-78	6	161	SSID=Bonch, Seq=1549
190	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-54	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2033, Bl...
93	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-78	6	161	SSID=Bonch, Seq=1550
202	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-54	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2034, Bl...
203	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-55	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2034, Bl...
51	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-79	6	161	SSID=Bonch, Seq=1551
200	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-54	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2035, Bl...
201	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-54	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2035, Bl...
78	MNGT.FR...	40:B8:9A:19:42:47	EA:FF:FF:FF:FF:FF	? N/A	? N/A	N/A	N/A	16:10...	-72	1	11	SSID=Bonch, Seq=1557
65	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-77	6	161	SSID=Bonch, Seq=1562
129	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-54	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2036, Bl...
157	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-54	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2036, Bl...
78	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-75	6	161	SSID=Bonch, Seq=1563
132	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-55	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2037, Bl...
102	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-54	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2037, Bl...
48	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-75	6	161	SSID=Bonch, Seq=1564
134	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-57	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2038, Bl...
127	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-55	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2038, Bl...
60	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-76	6	161	SSID=Bonch, Seq=1565
123	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-55	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2039, Bl...
124	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-56	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2039, Bl...
62	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-75	6	161	SSID=Bonch, Seq=1566
103	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-56	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2040, Bl...
106	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-54	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2040, Bl...
55	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-75	6	161	SSID=Bonch, Seq=1567
113	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-56	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2041, Bl...
108	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-54	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2041, Bl...
47	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-76	6	161	SSID=Bonch, Seq=1568
111	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-56	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2042, Bl...
109	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-56	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2042, Bl...
63	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-75	6	161	SSID=Bonch, Seq=1569
116	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-56	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2043, Bl...
45	MNGT.FR...	40:B8:9A:19:42:47	Broadcast	? N/A	? N/A	N/A	N/A	16:10...	-76	6	161	SSID=Bonch, Seq=1570
133	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-56	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2044, Bl...
100	MNGT.FR...	CiscoCF:30:4F	40:B8:9A:19:42:47	? N/A	? N/A	N/A	N/A	16:10...	-54	6	161	SSID=Bonch, (Infra), Ch#161, Seq=2044, Bl...

Рис. 2.17 Пример перехвата Probe request frame и Probe response frame на каналах 11 и 161 в частотных диапазонах 2,4 и 5 ГГц

2.4 Анализ количества устройств и их распределения по частотным диапазонам

Рассмотрим анализ одного из локальных сегментов (центральная часть 4-го этажа 2-го корпуса университета). В каждом сегменте было перехвачено и проанализировано 5 тыс. пакетов.

Для анализа результатов был использован следующий алгоритм:

1. Открыть отформатированный файл в программе Microsoft Excel.
2. С помощью встроенной функции «Удалить дубликаты» получить наглядное представление всех устройств, подключенных к сети.
3. Найти количество устройств, использующих частоту 5 ГГц.

Таким образом, в примере всего устройств в сети (без учета маршрутизаторов Cisco) 758, из них 5 устройств, использующих частоту 5 ГГц (0,66%). По итогам анализа была построена диаграмма распределения устройств (рис. 2.18).

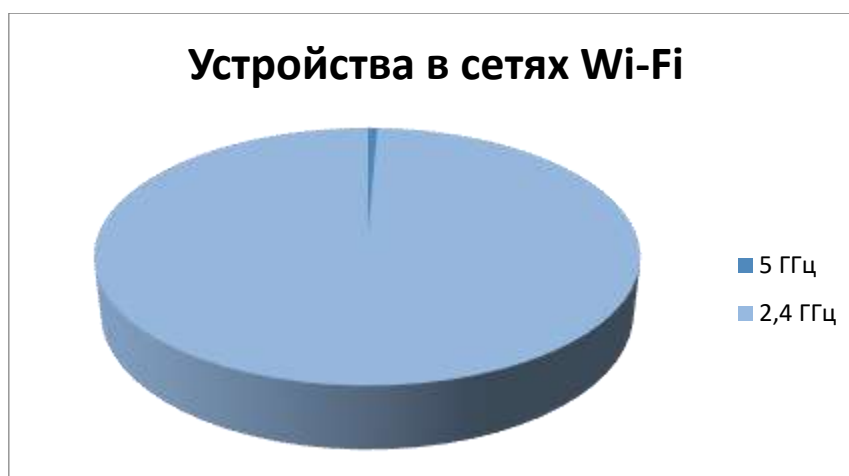


Рис. 2.18 Диаграмма распределения устройств в центральном локальном сегменте сети Wi-Fi

Далее эксперимент проводится еще в 7 локальных сегментах сети Wi-Fi СПбГУТ.

No	Протокол	MAC источ.	MAC назн.	IP источ.	IP назн.	Порт источ.	Порт назн.	Время	Размер	Сигнал	Скорость	Начал	Ошибки	Детали	Data
1	MNGT/BEACON	Cisco:48:82:44	Broadcast	N/A	N/A	N/A	N/A	20:41,0	289	-59	1	11		SSID=Bonch, (Infra.), Ch.#11, Seq=3214, Bi=102	0x80000000FFFFFFFF4A02A4
2	CTRL/ACK	N/A	25:54:28:13:BF:21	N/A	N/A	N/A	N/A	20:41,0	10	-69	34	11	CRC		0xD45577F125542813BF21
3	MNGT/BEACON	Cisco:49:73:48	Broadcast	N/A	N/A	N/A	N/A	20:41,0	279	-65	6	161		(Infra.), Ch.#161, Seq=738, Bi=102	0x80000000FFFFFFFF4A02A4
4	MNGT/BEACON	Cisco:48:82:42	Broadcast	N/A	N/A	N/A	N/A	20:41,0	294	-62	1	11		SSID=testingNet, (Infra.), Ch.#11, Seq=3215, Bi=102	0x80000000FFFFFFFF4A02A4
5	CTRL/RESERVED	38:B5:61:68:2E:DA	E9:D9:42:7E:96:50	N/A	N/A	N/A	N/A	20:41,0	2368	-66	5,5	11	CRC		0x064C36F3E9D9427E9650B56168
6	MNGT/BEACON	Cisco:49:73:4C	Broadcast	N/A	N/A	N/A	N/A	20:41,0	279	-64	6	161		(Infra.), Ch.#161, Seq=739, Bi=102	0x80000000FFFFFFFF4A02A4
7	MNGT/BEACON	Cisco:0F:36:6F	Broadcast	N/A	N/A	N/A	N/A	20:41,0	283	-75	6	161		SSID=Bonch, (Infra.), Ch.#161, Seq=348, Bi=102	0x80000000FFFFFFFFF2C36F80F
8	FRAGMENT	3E:AC:70:32:67:26	91:06:4E:A3:19:78	N/A	N/A	N/A	N/A	20:41,0	523	-67	1	11	CRC		0x8897C87091064EA319785EAC703
9	MNGT/RESERVED	D3:32:A9:0D:75:FF	52:7F:5A:0C:21:8E	N/A	N/A	N/A	N/A	20:41,0	3627	-65	5,5	11	CRC		0x73E3F0088A552907A350332A90
10	CTRL/RTS	85:07:2B:D3:01:DA	D6:BC:F2:88:A3:E1	N/A	N/A	N/A	N/A	20:41,0	4073	-67	5,5	11	CRC		0x840D030068CF28BA3E145072BD
11	MNGT/BEACON	Cisco:48:82:41	Broadcast	N/A	N/A	N/A	N/A	20:41,0	291	-59	1	11		SSID=StudNet, (Infra.), Ch.#11, Seq=3216, Bi=102	0x80000000FFFFFFFF4A02A4
12	MNGT/BEACON	Cisco:0F:36:6D	Broadcast	N/A	N/A	N/A	N/A	20:41,0	289	-62	1	11		SSID=Bonch, (Infra.), Ch.#11, Seq=3561, Bi=102	0x80000000FFFFFFFFF2C36F80F
13	MNGT/BEACON	Cisco:0F:36:6D	Broadcast	N/A	N/A	N/A	N/A	20:41,0	288	-75	6	161		SSID=testingNet, (Infra.), Ch.#161, Seq=349, Bi=102	0x80000000FFFFFFFFF2C36F80F
14	MNGT/BEACON	Tr-LinkT:AA:DD:AA	Broadcast	N/A	N/A	N/A	N/A	20:41,0	342	-61	1	11		(Infra.), Ch.#11, Seq=184, Bi=100	0x80000000FFFFFFFFF4CC2DAA
15	MNGT/BEACON	Cisco:48:82:47	Broadcast	N/A	N/A	N/A	N/A	20:41,0	296	-59	1	11		(Infra.), Ch.#11, Seq=3217, Bi=102	0x80000000FFFFFFFF4A02A4
16	MNGT/BEACON	Cisco:49:73:48	Broadcast	N/A	N/A	N/A	N/A	20:41,0	283	-65	6	161		SSID=Bonch, (Infra.), Ch.#161, Seq=740, Bi=102	0x80000000FFFFFFFF4A02A4
17	MNGT/BEACON	Cisco:48:82:43	Broadcast	N/A	N/A	N/A	N/A	20:41,0	296	-59	1	11		(Infra.), Ch.#11, Seq=3218, Bi=102	0x80000000FFFFFFFF4A02A4
18	MNGT/BEACON	Cisco:0F:36:62	Broadcast	N/A	N/A	N/A	N/A	20:41,0	294	-62	1	11		SSID=testingNet, (Infra.), Ch.#11, Seq=3562, Bi=102	0x80000000FFFFFFFFF2C36F80F
19	MNGT/BEACON	Cisco:0F:36:6E	Broadcast	N/A	N/A	N/A	N/A	20:41,0	285	-75	6	161		SSID=StudNet, (Infra.), Ch.#161, Seq=350, Bi=102	0x80000000FFFFFFFFF2C36F80F
20	MNGT/BEACON	Cisco:0F:64:70	Broadcast	N/A	N/A	N/A	N/A	20:41,0	289	-72	1	11		SSID=Bonch, (Infra.), Ch.#11, Seq=4019, Bi=102	0x80000000FFFFFFFFF2C36F80F
21	ENCR. DATA	00:00:00:00:00:00	A6:C1:95:5E:EB:DC	N/A	N/A	N/A	N/A	20:41,0	10	-69	34	11	CRC		0x58485089A6C1955EEBDC
22	MNGT/BEACON	Cisco:49:73:4D	Broadcast	N/A	N/A	N/A	N/A	20:41,0	288	-65	6	161		SSID=testingNet, (Infra.), Ch.#161, Seq=741, Bi=102	0x80000000FFFFFFFF4A02A4
23	CTRL/BLOCKACK	69:70:51:C0:F4:85	DD:72:CF:8F:38:A8	N/A	N/A	N/A	N/A	20:41,0	1379	-68	1	11	CRC		0x949018EADD72CF8F38A8697051
24	MNGT/BEACON	Cisco:E9:44:A0	Broadcast	N/A	N/A	N/A	N/A	20:41,0	289	-71	1	11		SSID=Bonch, (Infra.), Ch.#11, Seq=1048, Bi=102	0x80000000FFFFFFFFFA45630E9
25	ENCR. DATA	00:00:00:00:00:00	C4:FB:F7:9A:AE:F8	N/A	N/A	N/A	N/A	20:41,0	10	-70	24	11	CRC	WEP: Can't decrypt, Key#1	0x08EB2754C4FBF79AAEF8
26	ENCR. DATA	00:00:00:00:00:00	00:00:00:00:00:00	N/A	N/A	N/A	N/A	20:41,0	10	-68	24	11	CRC	WEP: Can't decrypt, Key#1	0x0A50E12ED374CA80EF
27	MNGT/BEACON	Cisco:0F:36:61	Broadcast	N/A	N/A	N/A	N/A	20:41,1	291	-62	1	11		SSID=StudNet, (Infra.), Ch.#11, Seq=3563, Bi=102	0x80000000FFFFFFFFF2C36F80F
28	MNGT/BEACON	Cisco:0F:64:72	Broadcast	N/A	N/A	N/A	N/A	20:41,1	294	-72	1	11	CRC	SSID=testingNet, (Infra.), Ch.#11, Seq=4020, Bi=102	0x80000000FFFFFFFFF2C36F80F
29	MNGT/ASS. RESP.	8D:C3:B1:98:12:7F	D9:9D:F3:DB:C7:33	N/A	N/A	N/A	N/A	20:41,1	4073	-66	2	11	CRC	Reserved, Assoc.ID=5298, Seq=1119	0x11793CDD118B1063C96DC5813
30	MNGT/BEACON	Cisco:49:73:4E	Broadcast	N/A	N/A	N/A	N/A	20:41,1	285	-65	6	161		SSID=StudNet, (Infra.), Ch.#161, Seq=742, Bi=102	0x80000000FFFFFFFF4A02A4
31	MNGT/BEACON	Cisco:49:73:48	Broadcast	N/A	N/A	N/A	N/A	20:41,1	279	-65	6	161		(Infra.), Ch.#161, Seq=743, Bi=102	0x80000000FFFFFFFF4A02A4
32	MNGT/BEACON	Cisco:48:82:42	Broadcast	N/A	N/A	N/A	N/A	20:41,1	294	-59	1	11		SSID=testingNet, (Infra.), Ch.#11, Seq=3220, Bi=102	0x80000000FFFFFFFF4A02A4
33	MNGT/BEACON	Cisco:49:73:4C	Broadcast	N/A	N/A	N/A	N/A	20:41,1	279	-64	6	161		(Infra.), Ch.#161, Seq=744, Bi=102	0x80000000FFFFFFFF4A02A4
34	MNGT/BEACON	Cisco:0F:36:6F	Broadcast	N/A	N/A	N/A	N/A	20:41,1	283	-74	6	161		SSID=Bonch, (Infra.), Ch.#161, Seq=351, Bi=102	0x80000000FFFFFFFFF2C36F80F
35	MNGT/BEACON	Cisco:E9:44:A1	Broadcast	N/A	N/A	N/A	N/A	20:41,1	291	-70	1	11		SSID=StudNet, (Infra.), Ch.#11, Seq=1050, Bi=102	0x80000000FFFFFFFFFA45630E9
36	MNGT/BEACON	Cisco:48:82:41	Broadcast	N/A	N/A	N/A	N/A	20:41,1	291	-59	1	11		SSID=StudNet, (Infra.), Ch.#11, Seq=3221, Bi=102	0x80000000FFFFFFFF4A02A4
37	MNGT/BEACON	Tr-LinkT:AA:DD:AA	Broadcast	N/A	N/A	N/A	N/A	20:41,1	342	-62	1	11		(Infra.), Ch.#11, Seq=185, Bi=100	0x80000000FFFFFFFFF4CC2DAA
38	MNGT/BEACON	Cisco:0F:36:6D	Broadcast	N/A	N/A	N/A	N/A	20:41,1	288	-75	6	161		SSID=testingNet, (Infra.), Ch.#161, Seq=352, Bi=102	0x80000000FFFFFFFFF2C36F80F
39	MNGT/BEACON	Cisco:0F:36:60	Broadcast	N/A	N/A	N/A	N/A	20:41,1	289	-67	1	11		SSID=Bonch, (Infra.), Ch.#11, Seq=3564, Bi=102	0x80000000FFFFFFFFF2C36F80F
40	MNGT/BEACON	Cisco:48:82:47	Broadcast	N/A	N/A	N/A	N/A	20:41,1	290	-59	1	11		(Infra.), Ch.#11, Seq=3222, Bi=102	0x80000000FFFFFFFF4A02A4

Рис. 2.19. Пример обработки файла в Microsoft Excel

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
284	1761 FRAGMENT	F1:F6:1C:BC:4F:2D	33:33:11:DC:13:80	N/A	N/A	N/A	N/A	20:48,5	124	-71	11	11	CRC	WPA: Can't decrypt	0x08420000333311DC138031B2828D8A55F1F61C8C4F2052E0AA075BA5C04E5
285	1774 MNGT/PROBE RESP.	B5:24:CA:3D:8B:6F	F3:78:A8:96:5C:E3	N/A	N/A	N/A	N/A	20:48,5	506	-66	1	11	CRC	(Infra.), Ch.#0, Seq=3127, BI=24699	0x51289251F578A8965CE38524CA3D8B6F982C983EE0BA7AC3D6C7A57716971
286	1775 FRAGMENT	F3:99:C1:E8:0B:C0	BF:90:A8:D1:45:68	N/A	N/A	N/A	N/A	20:48,5	2937	-66	11	11	CRC		0x28758D1F7885C16F423AF399C1E80BC08F90A8D145682B8A4338DA47C7861
287	1779 ENCR. DATA	F2:4A:35:9F:C0:81	E4:8D:8E:C9:E7:A2	N/A	N/A	N/A	N/A	20:48,5	506	-66	1	11	CRC		0x7858889E48D8EC9E7A2F3A4359FC0811861FEAC5A2E9668869A87C98B8E
288	1784 FRAGMENT	1C:62:02:C0:64:D1	A1:A0:31:8E:C3:48	N/A	N/A	N/A	N/A	20:48,6	158	-74	11	11	CRC		0x1A0B5D99A1A0318EC34B1C6202C064D14971D32527F48A2A057767900B4
289	1785 FRAGMENT	C8:67:17:62:7E:87	B0:33:00:00:00:FB	N/A	N/A	N/A	N/A	20:48,6	178	-71	11	11	CRC	WPA: Can't decrypt	0x08420001B03300000FB2CBEFC0F7DC5C86717627E87BACB2C95D2200001
290	1789 CTRL/RESERVED	C4:11:3C:D2:01:ED	4F:C1:90:68:37:E4	N/A	N/A	N/A	N/A	20:48,6	1507	-65	1	11	CRC		0x2604068F4FC1906837E4C4113CD201EDF86EB8A233D6A847B10FF88F5005
291	1807 MNGT/PROBE REQ.	ED:22:6C:31:23:41	38:F0:20:5A:F1:A8	N/A	N/A	N/A	N/A	20:48,7	3499	-66	5,5	11	CRC	SSID=ary, Seq=4035	0x41FC92CF2BF0205AF1A8ED226C312341D743D9F3085D30FC42A3D851ABAA
292	1812 MNGT/DISASS	52:E6:3D:79:D8:47	88:B0:C2:27:39:89	N/A	N/A	N/A	N/A	20:48,7	970	-66	1	11	CRC	Reason=Reserved, Seq=737	0xA0ACC9888880C227398952E63079D84771F4C3364F41B2E7C98E42182F4
293	1817 MNGT/BEACON	A4:56:F4:C3:47:A2	FF:FF:A7:9E:FF:FF	N/A	N/A	N/A	N/A	20:48,7	294	-70	1	11	CRC	SSID=testingNet, (Infra.), Ch.#11, Seq=1267, BI=32870	0x80000000FFFF79EFFFFA456F4C547A2A456308972A2304F77895F30810100
294	1823 MNGT/BEACON	32:08:BD:95:88:90	58:A1:E8:0A:39:4D	N/A	N/A	N/A	N/A	20:48,7	538	-67	2	11	CRC	(Infra.), Ch.#0, Seq=1826, BI=21484	0x82799975784CA042DE73208B095889058A1E80A394D29728982C60840D58
295	1832 FRAGMENT	A4:F7:26:00:99:7E	01:00:5E:00:9D:8F	N/A	N/A	N/A	N/A	20:48,8	113	-72	11	11	CRC	WPA: Can't decrypt	0x086200001005E009D8F2867C9096470A4F726D0997E1F6FEE39E7A0000000
296	1833 ENCR. DATA	60:21:7A:69:C9:CB	01:00:5E:00:00:FC	N/A	N/A	N/A	N/A	20:48,8	105	-73	11	11	CRC	WEP: Can't decrypt, Key#2	0x086200001005E0000FC0C357CC562B060217A69C9CB00FB3FD65CC7FDA
297	1834 ENCR. DATA	2C:82:4A:68:C9:CB	01:00:5E:00:00:FC	N/A	N/A	N/A	N/A	20:48,8	112	-71	11	11	CRC	WPA: Can't decrypt	0x084200001005E0000FC2C36F80F64702C824A69C9CBED0FB3FB881D90009
298	1836 MNGT/ACTION	68:3F:D6:D9:2C:00	2F:0E:5D:6F:D4:DF	N/A	N/A	N/A	N/A	20:48,8	481	-66	1	11	CRC	Category=Unknown code, Seq=1388	0xD3AD2C7BAAE5A87635E4683FD6092C0027F0E5D6FD4DFC0569E966CD039C
299	1860 802.2	70:24:D8:9F:A0:4E	A5:A5:1E:F4:82:F1	N/A	N/A	N/A	N/A	20:48,9	16	-84	24	161	CRC		0x288433DDA5A51EF482F17024D89FA0ME
300	1868 CTRL/RESERVED	52:33:5C:6C:81:DC	0E:F3:9D:B2:58:2D	N/A	N/A	N/A	N/A	20:48,9	16	-86	24	161	CRC		0x160CFB780EF39D82582D52335C6C81DC
301	1879 FRAGMENT	13:8C:5A:91:8F:80	33:33:00:80:84:1D	N/A	N/A	N/A	N/A	20:49,0	148	-72	11	11	CRC	WPA: Can't decrypt	0x084200003333008084102C36F83FF756138C5A918FB0739838E60AB2804848
302	1888 FRAGMENT	72:8F:21:C3:13:70	7A:86:08:84:17:77	N/A	N/A	N/A	N/A	20:49,0	1203	-66	5,5	11	CRC		0x79BC45F67A860884177728F21C5137020E921BC570905FEF25EE1EE41CF5D
303	1897 MNGT/DEAUTH	CA:0D:08:3A:37:56	54:F6:D5:73:9F:87	N/A	N/A	N/A	N/A	20:49,1	506	-66	1	11	CRC	Reason=Reserved, Seq=3034	0xC3D1EA481A3D92708368CA0D083A375654F6D5739F87A8BD289D69EC72A
304	1902 ENCR. DATA	B5:0A:82:DF:89:0F	DA:04:89:ED:15:6A	N/A	N/A	N/A	N/A	20:49,1	954	-66	1	11	CRC		0x58F673790A0489ED156A14C071107E57850A82DF890F50078742284988E61
305	1903 MNGT/BEACON	6E:1F:30:F1:18:77	C5:78:F2:19:05:69	N/A	N/A	N/A	N/A	20:49,1	2919	-66	1	11	CRC	(Infra.), Ch.#0, Seq=1351, BI=20156	0x81E32FBCC578F21905696E1F30F11877186187CFED707E54679FB4CFCC5C3
306	1912 MNGT/DISASS	F8:E9:AC:50:BF:13	BF:24:03:4F:81:CF	N/A	N/A	N/A	N/A	20:49,1	25	-67	1	11	CRC	Reason=Reserved, Seq=1950	0xA2F870EBF24034F81CFFB8E9AC306F13483AA6C147C5EB7988
307	1927 FRAGMENT	23:EF:D8:3D:76:3A	F1:54:48:01:19:9D	N/A	N/A	N/A	N/A	20:49,2	133	-73	11	11	CRC		0xA88707CBF1544801199D23EFDB3D763AFD36285FC460EB108DE9690DD85
308	1928 FRAGMENT	F2:37:68:7A:A3:AF	33:33:00:01:00:01	N/A	N/A	N/A	N/A	20:49,2	125	-74	11	11	CRC	WPA: Can't decrypt	0x08620000333300010001F38BED6786ADF2376B7A43AF11BF3F10A5D900
309	1929 ENCR. DATA	2D:36:F8:3F:F7:74	01:00:5E:00:02:CD	N/A	N/A	N/A	N/A	20:49,2	113	-73	11	11	CRC	WPA: Can't decrypt	0x08C894001005E0002CD2D36F83FF7742C33688800CD80B7290FB826F983A1
310	1930 ENCR. DATA	2C:1F:02:3E:23:CA	01:00:5E:00:00:FC	N/A	N/A	N/A	N/A	20:49,2	112	-71	11	11	CRC	WPA: Can't decrypt	0x084200001005E0000FC2C97C1AEE702C1F023E23CA2011C0D130A10000E2
311	1947 FRAGMENT	88:E9:38:7D:2F:08	33:9B:26:FD:4C:06	N/A	N/A	N/A	N/A	20:49,3	84	-65	54	11	CRC		0x7888D900339B26FD4C0688E938702F08503832B886C6A730C004D4CB78D0
312	1954 MNGT/PROBE RESP.	08:8C:D9:56:00:8A	8C:D7:04:2B:69:4E	N/A	N/A	N/A	N/A	20:49,3	3315	-66	2	11	CRC	(Infra.), Ch.#3, Seq=531, BI=55312	0x503F9EA78CD7042B694E088CD9560DBA24608016E95C3321A8587655BAC9E
313	1956 MNGT/RESERVED	59:89:6F:60:34:64	4E:E7:A4:C9:4A:3C	N/A	N/A	N/A	N/A	20:49,3	2912	-65	1	11	CRC		0x7194307B4EE7A4C94A3C59896F6034646E362AA867D4CF6880EA322FB9308
314	1962 MNGT/RESERVED	78:82:7D:48:DD:0A	15:7A:CC:D0:FE:38	N/A	N/A	N/A	N/A	20:49,3	88	-65	5,5	11	CRC		0x63398797123C2DA816ED78827D46DD0DA157ACDD0FE38217786B29AA7D46C
315	1969 FRAGMENT	B0:9B:F8:55:DB:67	2E:3E:4A:03:88:30	N/A	N/A	N/A	N/A	20:49,3	2000	-67	12	11	CRC	WEP: Can't decrypt, Key#3	0x08582AC32E3E4A038830B09BF8550B6701A5CBEA386E44F0605DD2967E9F
316	1970 FRAGMENT	8A:DA:40:F9:9C:52	AD:1E:0C:D3:19:E1	N/A	N/A	N/A	N/A	20:49,4	28	-85	24	161	CRC		0x780BA684AD1E0CD319E18AD44DF99C522CA86C2D85360DAAC758970F
317	1976 MNGT/BEACON	D7:AF:73:AE:C7:D5	22:6A:02:A3:D3:FF	N/A	N/A	N/A	N/A	20:49,4	3081	-65	1	11	CRC	(Ad Hoc), Ch.#0, Seq=9636, BI=6922	0x837968948D22048A29AAD7AF73AEC7D5226A02A3D3F45E32F91C4A285D2

Рис. 2.20. Результат выделения уникальных устройств

No	Протокол	MAC источ.	MAC назн.	IP источ.	IP наз.	Порт с	Порт н	Врем.	Разм.	Сигн.	Скорос.	Канал	Т. Ошиб.	Детали	Data
172	DATA/NULL FUNC	D7:FA:74:84:0E:E3	57:6D:CD:C8:99:8F	N/A	N/A	N/A	N/A	20:48,3	24	-88	24	161	CRC		0x48012C00A44343688B69D7FA74E40EE3576DCDC8998F1026
173	FRAGMENT	20:49:0D:8D:2A:D3	A9:69:82:7E:94:E9	N/A	N/A	N/A	N/A	20:48,3	24	-83	24	161	CRC		0x1BD4CD00A969827E94E920490D8D3AD3A4FAF576019CF940
186	802.2	70:24:DB:9F:A0:4E	A5:A5:1E:F4:82:F1	N/A	N/A	N/A	N/A	20:48,9	16	-84	24	161	CRC		0x2B84330DA5A51EF482F17024DB9FA04E
188	CTRL/RESERVED	52:33:5C:6C:81:DC	DE:F3:9D:82:58:2D	N/A	N/A	N/A	N/A	20:48,9	16	-86	24	161	CRC		0x160CFB780EF9DB25B2D52335C6C81DC
197	FRAGMENT	8A:D4:4D:F9:9C:52	A0:1E:0C:D3:19:E1	N/A	N/A	N/A	N/A	20:49,4	28	-85	24	161	CRC		0x780BA084AD1E0CD319E18AD44DF99C522CAB0C2D85360DAAC758570F

Рис. 2.21. Список устройств, использующих частоту 5 ГГц

Пример: анализ 1-го локального сегмента (правое крыло 4 этажа 2 корпуса университета):

- Всего 165 устройств
- Из них 58 используют частоту 5 ГГц (34,94%)



Рис. 2.22. Распределение устройств Wi-Fi по диапазонам во 1-м локальном сегменте сети СПбГУТ