

Университет ИТМО

Лабораторная работа №2

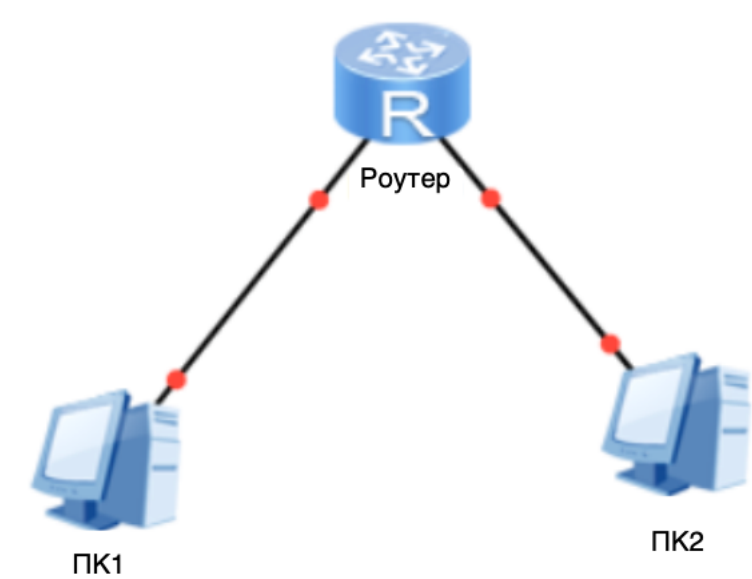
по дисциплине: Беспроводные сети

Выполнили: Соболев Иван, Верещагин Егор, Р34312


Преподаватель: Оголюк Александр Александрович

Санкт-Петербург
2024

1. Тестовый стенд



- ПК1 с ОС Windows 11, на котором установлена программа Microsoft Network Monitor.
- ПК2 с ОС macOS 14.4.1.
- Точка доступа ELTEX NTU-RG-5420G-Wac. Параметры точки доступа:

**NTU-RG-5420G-Wac**

Статус

LAN

WiFi

WAN

Сервисы

Дополнительно

Диагностика

Администрирование

Статистика

Устройство

Статус WAN

Статус LAN

IPv6

PON

LAN

Информация об устройстве

Модель	NTU-RG-5420G-Wac
Серийный номер	GP56251863
Серийный номер PON	454C5458870F6008
Заводской MAC-адрес	68:13:E2:CC:FE:80
Аппаратная версия	3v3
CRC версии прошивки образа 1	6d148324
CRC версии прошивки образа 2	aa6c5d15 (Active)
Версия загрузчика	U-Boot 2011.12.NA
Контрольная сумма загрузчика	ef953d67

Версия прошивки образа 1	2.9.1.1946
Версия прошивки образа 2	2.9.2.1375 (Active)
Версия Web-интерфейса	2.9.1.6
IPv4 Шлюз по умолчанию	ppp0
IPv6 Шлюз по умолчанию	
DNS	212.48.197.77, 78.37.77.77

- Расстояние от ПК1 до роутера: 200 см
- Расстояние от ПК2 до роутера: 240 см

- Тариф скорости интернета от провайдера: 300 Мбит/с

2. Настройка рабочей среды

Так как в тестовом стенде отсутствует возможность подключения Ethernet-кабеля к какому-либо ПК, точка доступа будет настроена с помощью Web-интерфейса.

2.1. Настройка статического IP-адреса на Ethernet-адаптере рабочей станции ПК1

На ПК1 настраиваем вручную IP-адрес

Сеть и Интернет > Wi-Fi > RT-5GPON-FE80

Изменение параметров IP-адреса сети

Вручную

IPv4

☒ Вкл.

IP-адрес

192.168.0.1

Маска подсети

255.255.255.0

Шлюз

Предпочтительный DNS-сервер

DNS по протоколу HTTPS

Выключено

Сохранить Отмена

IPv4-адрес:

192.168.0.1

Физический адрес (MAC):

7C-2A-31-8B-53-2B

2.2. Изменение IP-адреса управления на точке доступа

На роутере настраиваем IP-адрес управления:



NTU-RG-5420G-Wac

Статус

LAN

WiFi

WAN

Сервисы

Дополнительно

Диагностика

Администрирование

Статистика

LAN

Параметры LAN интерфейса

Имя интерфейса:

LANInterface

IP-адрес:

192.168.1.50

Маска подсети:

255.255.255.0

Адрес IPv6:

fe80::1

Режим IPv6 DNS:

HGWPProxy

Режим префикса:

WANDelegated

Интерфейс WAN:

Брандмауэр:

☒ Отключено ☐ Включено

IGMP Snooping:

☐ Отключено ☒ Включено

Изоляция Ethernet от Wi-Fi:

☒ Отключено ☐ Включено

Изоляция WLAN0(2.4GHz) от WLAN1(5GHz):

☒ Отключено ☐ Включено

Применить изменения

После этого необходимо переподключиться к точке доступа по новому IP:

The screenshot shows the web interface of an NTU-RG-5420G-Wac device. The browser address bar shows the URL 192.168.1.50/client/index.html#status/device. The interface has a top navigation bar with tabs: Статус, LAN, WiFi, WAN, Сервисы, Дополнительно, Диагностика, Администрирование, and Статистика. The main content area is titled 'Информация об устройстве' (Device Information). On the left, there is a sidebar with links: Устройство, Статус WAN, Статус LAN, IPv6, PON, and LAN. The main table displays the following information:

Параметр	Значение
Модель	NTU-RG-5420G-Wac
Серийный номер	GP56251863
Серийный номер PON	454C5458870F6008
Заводской MAC-адрес	68:13:E2:CC:FE:80
Аппаратная версия	3v3
CRC версии прошивки образа 1	8974fd54 (Active)
CRC версии прошивки образа 2	aa6c5d15
Версия загрузчика	U-Boot 2011.12.NA
Контрольная сумма загрузчика	ef953d67

2.3. Изменение IP-адреса рабочей станции ПК1

На ПК1 снова меняем IP-адресс

IPv4-адрес: 192.168.1.1
Маска IPv4: 255.255.255.0

2.4. Уменьшение выходной мощности передатчика точки доступа до 12.5%

На точке доступа есть возможность понизить мощность передатчика только до 20%:

The screenshot shows the wireless settings interface. At the top, there is a row of 12 checkboxes, all of which are checked. Below this, the 'Канал:' (Channel) is set to 1. The 'Мощность передатчика(mW):' (Transmit power) dropdown menu is open, showing options: 100%, 80%, 60%, 40%, and 20% (which is selected with a checkmark). Below this, 'Максимальное количество клиентов:' (Maximum number of clients) is set to 'Отключено' (Disabled). The 'Подключенные клиенты:' (Connected clients) section shows a button 'Показать активных клиентов WLAN'. There is a checkbox for 'Включить режим универсального ретранслятора (одновременная работа в качестве точки доступа и клиента)' (Enable universal relay mode (simultaneous operation as access point and client)), which is currently unchecked. The 'Regdomain:' is set to 'RUSSIAN(12)'. At the bottom, there is a blue button labeled 'Применить изменения' (Apply changes).

2.5. Создание беспроводной сети с SSID class_N

Так как на предыдущих шагах в качестве переменной N мы использовали значение 1, то создадим сеть с SSID class_1:

WLAN Basic Settings

☐ Disable WLAN Interface

Band: 2.4 GHz (B+G+N)

Mode: AP

Multiple AP

SSID: class_1

Hide SSID: ☐ Enabled ☒ Disabled

Channel Width: Auto

Current Channel Width: 40MHz

Control Sideband: Upper

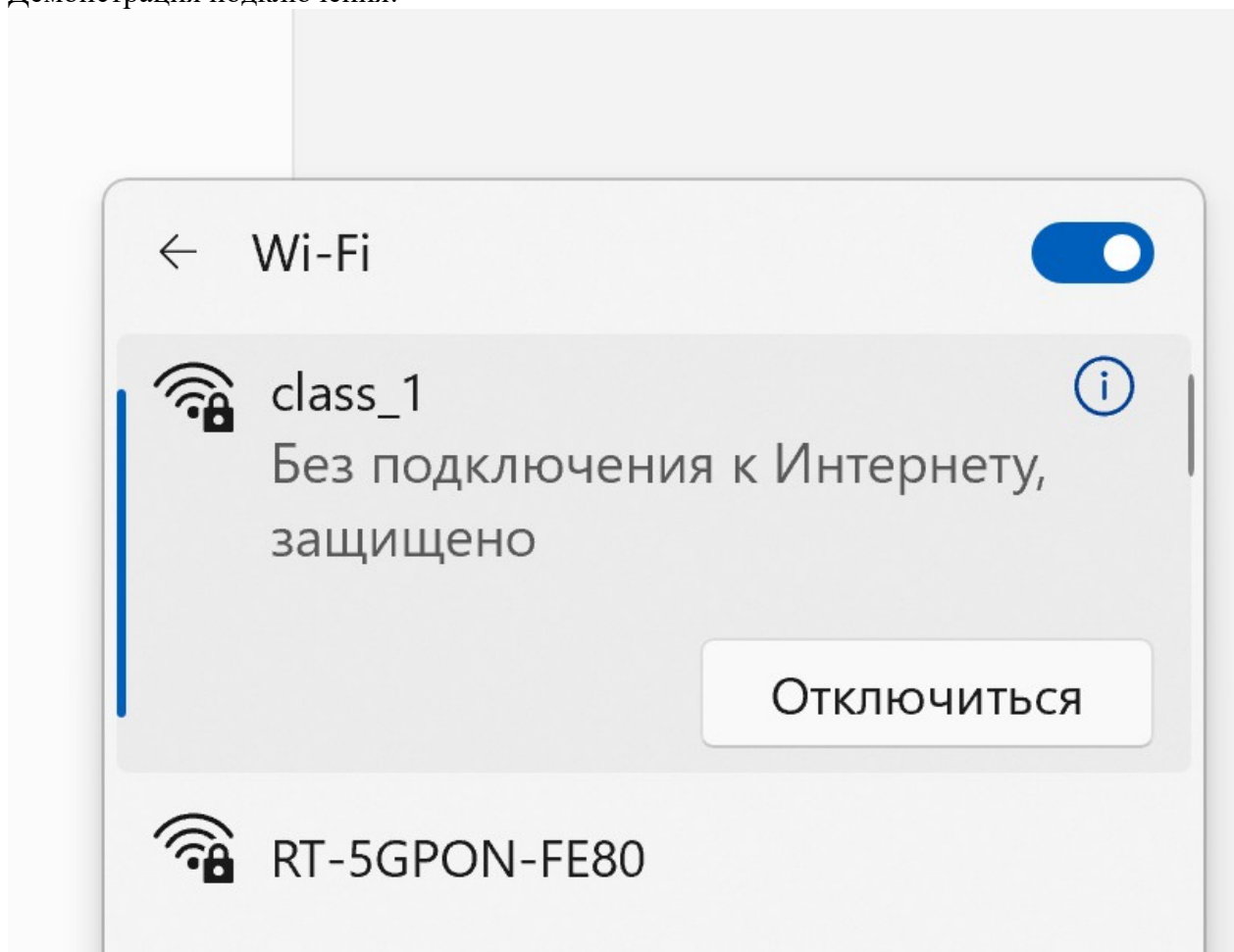
Channel Number: 6

Настройка IP-адреса на ПК2:

 Wi-Fi 

Configure IPv4	Manually 
IP address	192.168.1.3
Subnet mask	255.255.255.0
Router	192.168.1.50

Демонстрация подключения:



WLAN Status

WLAN Configuration

Mode	AP
Band	2.4 GHz (B+G+N)
SSID	class_1
Channel Number	6
Channel Width	Auto
Current Channel Width	40MHz
Encryption	WPA2 Mixed
BSSID	68:13:e2:cc:fe:80
Associated Clients	1

< > Wi-Fi



Wi-Fi



class_1



Connected



Weak Security



Details...

Personal Hotspots

iPhone (Иван) (2)



Known Networks

✓ class_1



RT-5GPON-FE80



3. Работа в Microsoft Network Monitor

3.1. Анализ кадров данных

The screenshot displays the Microsoft Network Monitor interface. The top section shows a list of captured frames with columns for Frame Number, Time Date Local Adjusted, Time Offset, Process Name, Source, Destination, Protocol Name, Description, and Conn Id. The frames are filtered by 'WiFi.FrameControl.Type ==2'. The bottom section shows the details of a selected frame (Frame Number 24), including its metadata (RSSI, Rate), frame control (Version 0, Data, QoS Data), and the payload (SSDP:Request, NOTIFY *).

Какие подтипы кадра данных встречаются чаще всего? – Самым распространённым подтипом кадра является Data. Также встречается много кадров с типом QoS Data:

22	22:50:34 19.11.2024	12.2952414	msedge.exe	192.168.1.4	192.168.1.1	ILS	ILS: ILS Rec Layer-1 SSL Application
23	22:50:34 19.11.2024	12.3390839	msedge.exe	192.168.1.1	192.168.1.4	TCP	TCP:Flags=...A..., SrcPort=2854, Dst
24	22:50:36 19.11.2024	14.9510865		192.168.1.50	224.0.0.1	IGMP	IGMP:IGMP Membership query
25	22:50:38 19.11.2024	16.9992686		192.168.1.50	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
26	22:50:39 19.11.2024	17.1628365		192.168.1.50	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
27	22:50:39 19.11.2024	17.3048558	msedge.exe	192.168.1.1	192.168.1.4	TLS	TLS:TLS Rec Layer-1 SSL Application
28	22:50:39 19.11.2024	17.3181707	msedge.exe	192.168.1.50	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
29	22:50:39 19.11.2024	17.3181707	msedge.exe	192.168.1.4	192.168.1.1	TLS	TLS:TLS Rec Layer-1 SSL Application
30	22:50:39 19.11.2024	17.3676021	msedge.exe	192.168.1.1	192.168.1.4	TCP	TCP:Flags=...A..., SrcPort=2854, Dst
31	22:50:39 19.11.2024	17.4816565		192.168.1.50	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
32	22:50:39 19.11.2024	17.6384424		192.168.1.50	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
33	22:50:39 19.11.2024	17.7936028		192.168.1.1	224.0.0.251	IGMP	IGMP:IGMPv2 Membership Report
34	22:50:39 19.11.2024	17.7990180		192.168.1.50	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
35	22:50:39 19.11.2024	17.9581867		192.168.1.50	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
36	22:50:39 19.11.2024	18.1186337		192.168.1.50	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
37	22:50:40 19.11.2024	18.2001846		192.168.1.50	239.255.255.250	SSDP	SSDP:Request, NOTIFY *

The screenshot shows the 'Frame Details' window for frame 24. It displays the frame's metadata (RSSI, Rate), frame control (Version 0, Data, QoS Data), and the payload (SSDP:Request, NOTIFY *). The 'SubType' is highlighted as 'QoS Data'.

Их отличие состоит в том, что в QoS Data включены дополнительные поля, которые позволяют устройствам в сети обрабатывать пакеты на основе заданных параметров качества обслуживания, что важно для чувствительных к задержкам приложений.

Какой процент составляют кадры данных от общего числа захваченных кадров? $522/524 * 100\% = 99.6$

3.2. Анализ повторно переданных кадров данных

Wireshark packet capture analysis showing a list of frames with a filter `WiFi.FrameControl.Type == 2 && WiFi.FrameControl.Retry == 1`. The packet list shows multiple retransmissions of frames 3, 6, 11, 12, 21, 22, 24, 26, 37, 38, 39, 46, 48, 51, 57, 95, 118, 124, 135, 148, 149, 151, 159, 165, 166, 180, 195, 200, 205, 207. The packet details for frame 207 show `ICMPv6: Router Solicitation` and `Hex Details` showing the packet structure.

Процент повторно переданных кадров равен $104/524 * 100\% = 19.8$

3.3. Анализ контрольных кадров

С помощью команды `netsh wlan show all` было выяснено, что сетевой адаптер ПК1 не поддерживает режим сетевого монитора:

программная точка беспроводного доступа (AP)
Режим сетевого монитора : не поддерживается

Из-за чего контрольные кадры отсутствуют:

Wireshark packet capture analysis showing a list of frames with a filter `WiFi.FrameControl.Type == 1`. The packet list is empty, indicating no frames were captured for this type. The packet details for frame 1 show `ICMPv6: Router Solicitation` and `Hex Details` showing the packet structure.

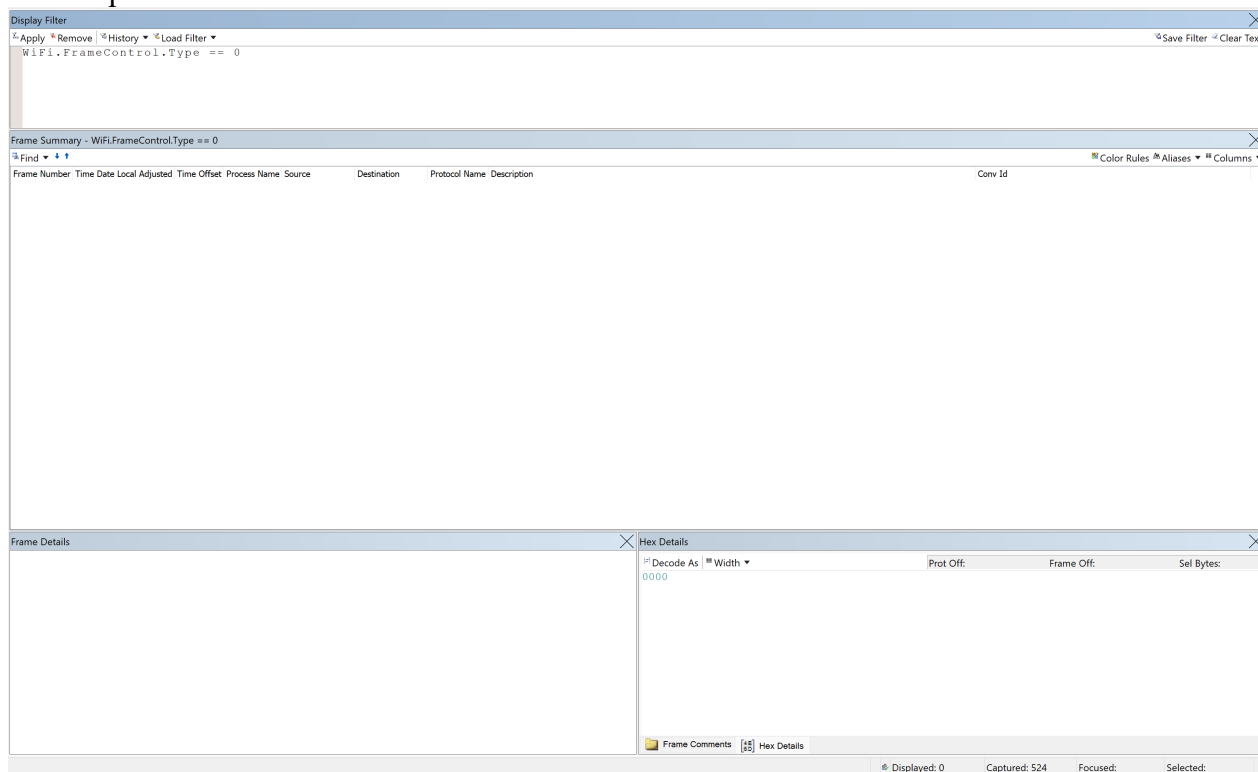
Дадим ответы на вопросы аналитически:

Какой подтип контрольных кадров является самым распространенным из захваченных кадров? – В основном самым распространенным подтипом контрольных кадров может быть RTS (Request to Send – Запрос на передачу информационного кадра) или CTS (Clear to Send – Предоставление права на отправку информационного кадра).

Какой процент составляют контрольные кадры от общего числа захваченных кадров? - Обычно контрольные кадры составляют небольшую часть от общего числа захватываемых кадров, порядка 5-10%.

3.4. Анализ кадров управления

Аналогично контрольным кадрам в нашем случае кадры управления не были зафиксированы из-за невозможности работы сетевого адаптера в режиме сетевого монитора:

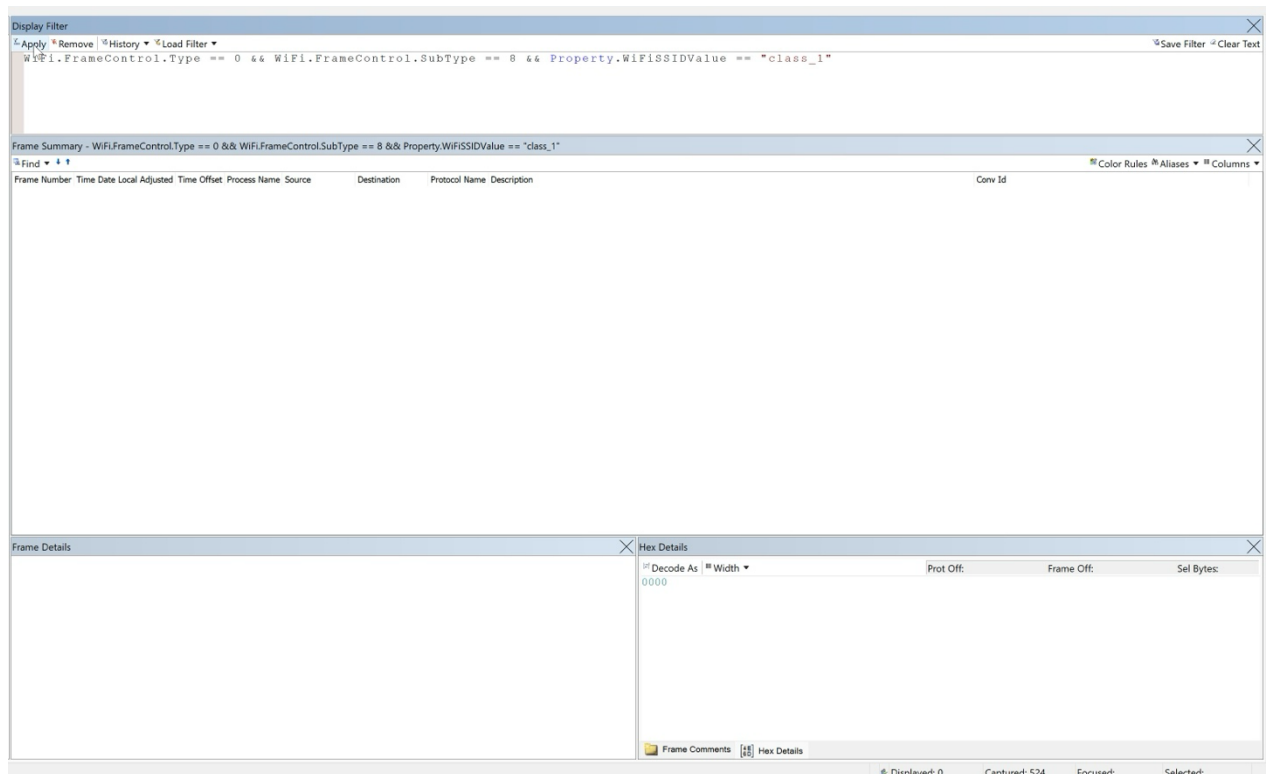


Дадим ответы на вопросы аналитически:

Какой подтип кадров управления является самым распространенным из захваченных кадров? – Наиболее распространенным подтипом в этой категории часто являются кадры Ассоциации (Association Request – запрос на ассоциацию с точкой доступа).

Какой процент составляют кадры управления от общего числа захваченных кадров? - Они могут составлять около 10-20% от общего числа запечатленных кадров, в зависимости от активности сети.

3.5. Анализ сигнальных кадров



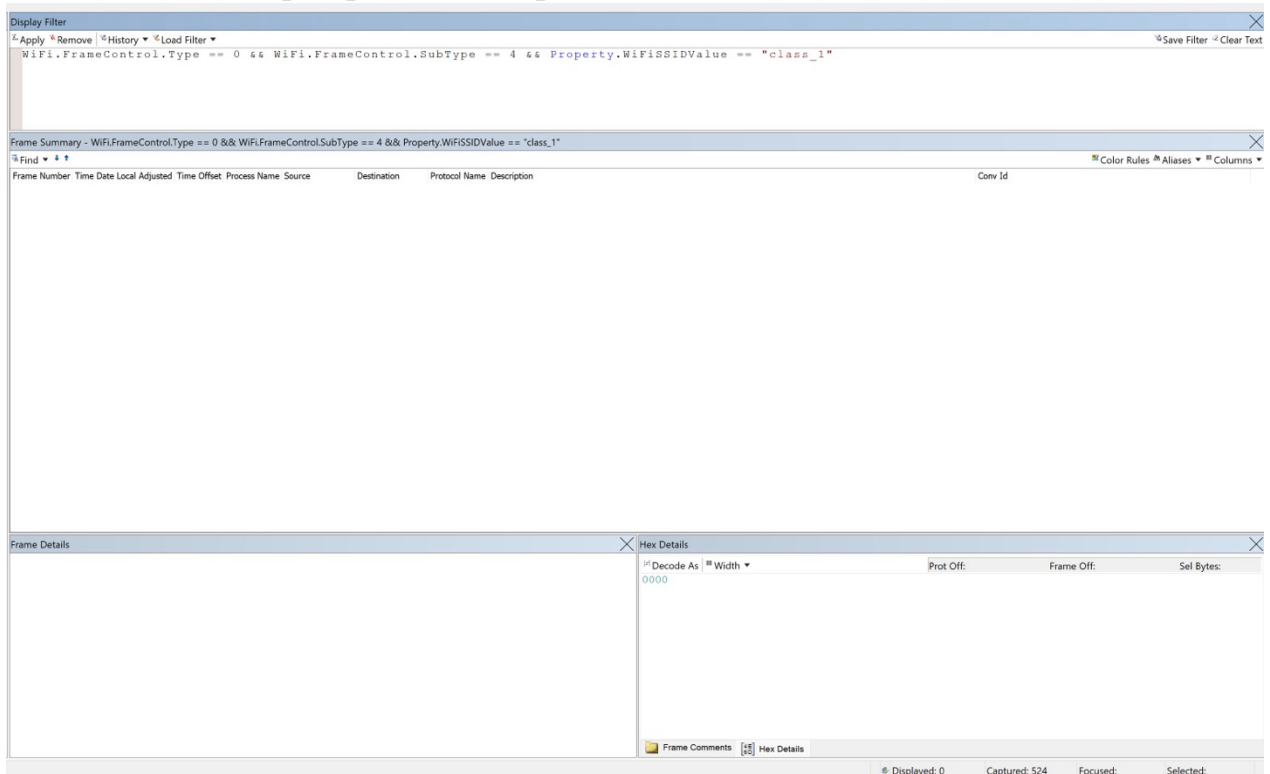
Сигнальные кадры также не поддерживаются, так как они являются подтипом кадров управления.

Различия SSID и BSSID:

- **SSID** — это имя беспроводной сети, которое отображается пользователям при подключении. Одно и то же имя SSID может использоваться несколькими точками доступа в пределах одной сети.
- **BSSID** же — это уникальный идентификатор конкретной точки доступа в сети, что позволяет отличать её от других точек, даже если они имеют одно и то же имя SSID.

Точка доступа рассылает сигнальные кадры (Beacon) с определённым интервалом, обычно значение по умолчанию составляет 100 миллисекунд, но это может варьироваться в зависимости от конфигурации точки доступа.

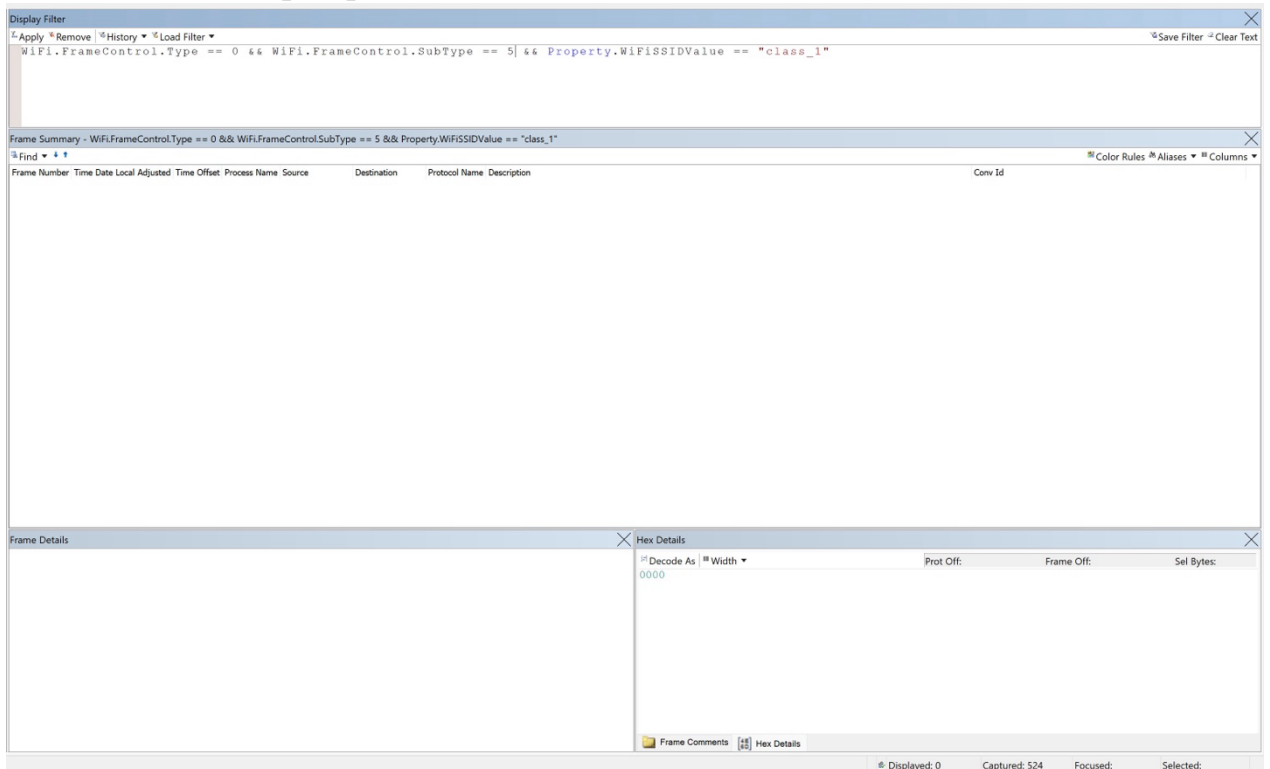
3.6. Анализ кадра пробного запроса



Кадры пробного запроса также не поддерживаются, так как они являются подтипом кадров управления.

Probe Request (запрос на проверку) — это сообщение, которое отправляет устройство в поисках доступных Wi-Fi сетей. Когда устройство хочет подключиться к сети, оно отправляет Probe Request в эфир, чтобы узнать, какие сети доступны в этом районе.

3.7. Анализ кадра пробного ответа



Кадры пробного ответа также не поддерживаются, так как они являются подтипом кадров управления.

Probe Response (ответ на проверку) — это сообщение, отправляемое точкой доступа в ответ на Probe Request, полученный от клиента. Когда точка доступа принимает этот запрос, она отвечает, информируя устройство о наличии своей сети.

4. Выводы

В ходе выполнения лабораторной работы мы познакомились с типами и подтипами кадров 802.11, изучили наиболее распространённые типы кадров, передаваемых по сети – таким типом оказался кадр данных. Также мы настроили локальную сеть между двумя ПК и точкой доступа с помощью настройки IP-адресов и назначения SSID сети.