МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра космического приборостроения и систем связи

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__6__» ____08____ 2021 г.

ПРОЕКТИРОВАНИЕ И ЭКСПЛУАТАЦИЯ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ

Методические указания по выполнению практических работ по дисциплине «Проектирование и эксплуатация инфокоммуникационных систем и сетей»

Курск 2021

УДК 654:004.7 (075.8)

Составитель: А. Е. Севрюков

Рецензент
доктор технических наук, старший научный сотрудник,
профессор кафедры космического приборостроения и систем связи
В. Г. Андронов

Проектирование и эксплуатация инфокоммуникационных систем и сетей: методические указания по выполнению практических работ по дисциплине «Проектирование и эксплуатация инфокоммуникационных систем и сетей» / Юго-Зап. гос. ун-т; сост.: А. Е. Севрюков. – Курск, 2021. – 50 с.

Методические указания содержат сведения по вопросам изучения качественных характеристик передачи голосового трафика в локальных сетях, механизмов мониторинга функционирования локальных сетей и механизмов защиты корпоративных сетей, материалы и методические указания, необходимые для выполнения практических работ по данным вопросам, а также задания по выполнению этих работ.

Методические указания предназначены для студентов, обучающихся по направлению подготовки бакалавриата 11.03.02 Инфокоммуникационные технологии и системы связи, очной и заочной форм обучения, при изучении дисциплины «Проектирование и эксплуатация инфокоммуникационных систем и сетей», а также для студентов других направлений подготовки при изучении дисциплин, направленных на формирование компетенций, связанных с проектированием инфокоммуникационных систем.

Текст печатается в авторской редакции

Подписано печать 06.09.21. Формат 60x841/16.
Усл. печ. л. 2,91. Уч.-изд. 2,63. Тираж 100 экз. Заказ 1043 Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94

СОДЕРЖАНИЕ

Практическая работа №1
ИЗУЧЕНИЕ КАЧЕСТВЕННЫХ ХАРАКТЕРИСТИК ПЕРЕДАЧИ ГОЛОСОВОГО ТРАФИКА В БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ СЕТЯХ

Цель работы: получение практических навыков анализа передачи голоса по сетям Wi-Fi.

Задание

При помощи программного VoIP-анализатора CommView for WiFi проанализировать создание соединения при использовании сигнального протокола SIP, а также RTP-сессию. Получить опыт работы с сетевым анализатором, произвести измерение параметров качества звука.

Указания к выполнению работы

Внимание! Перед выполнением практической работы рекомендуется приостановить работу антивируса Kaspersky. Для этого достаточно выбрать значок антивируса на панели задач, нажать правой кнопкой мыши и выбрать пункт **Приостановка защиты и контроля.**

Примечание: для выполнения практической работы точки доступа следует переключить в режим 802.11bg с максимальной скоростью передачи 54 Мбит/с.

1. При помощи программного комплекса CommView for Wi-Fi изучить этапы установления соединения SIP-протокола. Для этого:

- Запустить программный пакет CommView for WiFi, нажав на соответствующую иконку  на рабочем столе.
- Настроить CommView for Wi-Fi на захват пакетов, передаваемых точкой доступа (AP) на соответствующем канале.

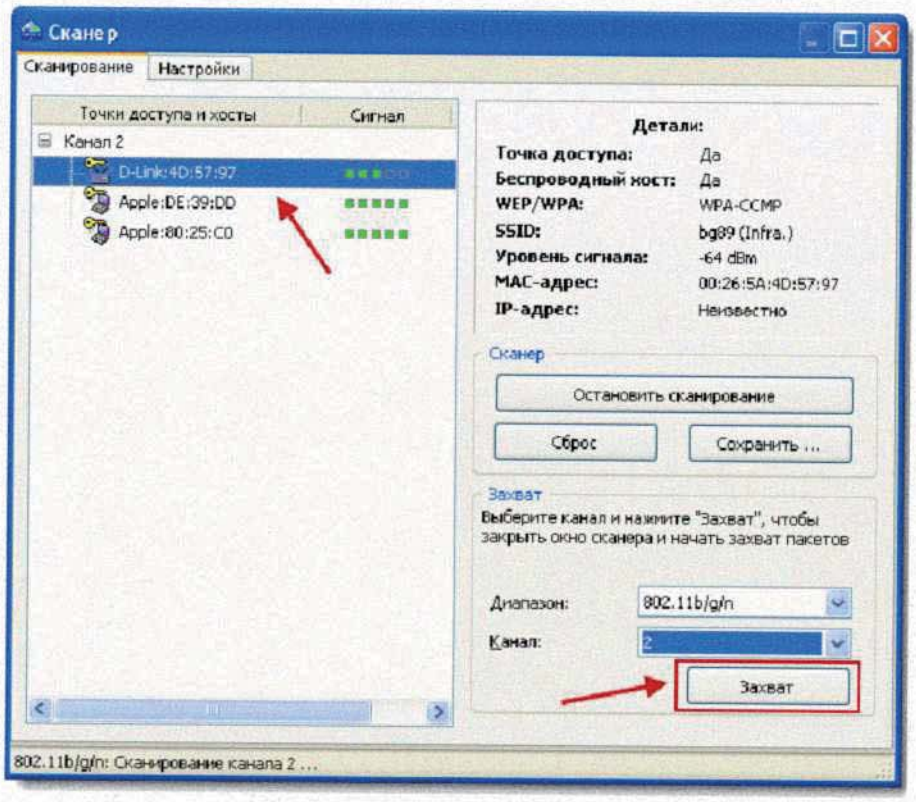


Рис.1.1.

Внимание: при использовании WPA-шифрования для успешного захвата VoIP-пакетов требуется произвести рассоциацию узлов (Инструменты/Рассоциация узлов).

- В рабочем окне CommView for WiFi перейти во вкладку VoIP, убедившись предварительно, что анализатор VoIP-данных не отключен (Настройка/Установки/VoIP).

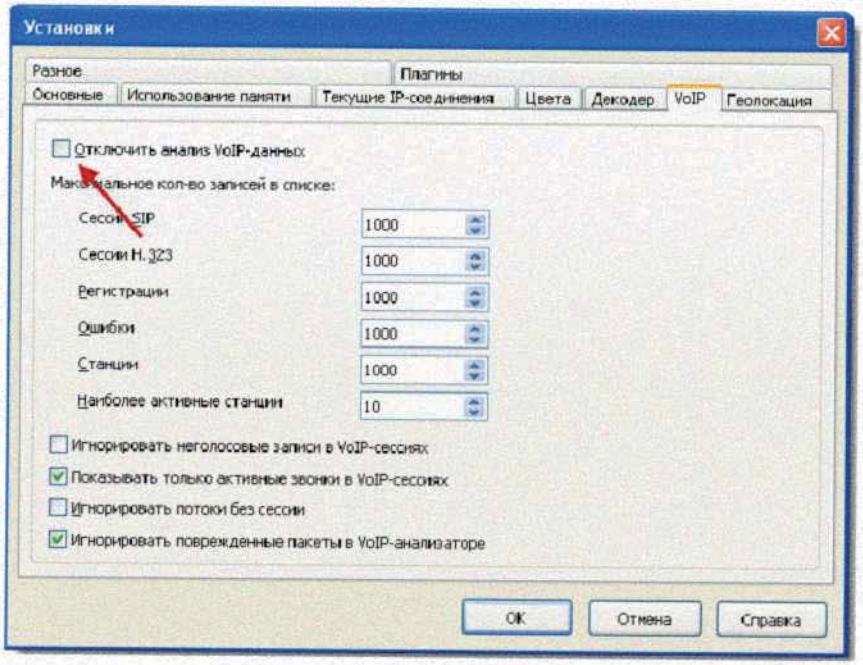


Рис.1.2.

- Очистить данные предыдущих VoIP-сессий (Файл/Очистить данные VoIP).
- С рабочего места 1 совершить исходящий вызов на рабочее место

2. На рабочем месте 2 «снять трубку». После непродолжительного разговора разорвать связь.

Параллельно на рабочем месте 3 (с установленным CommView for Wi-Fi) произвести анализ создания и разрыва SIP-соединения.

Внимание: В данной практической работе для установления соединения требуется использовать кодек Speex 16 kHz. Остальные кодеки рекомендуется деактивировать.

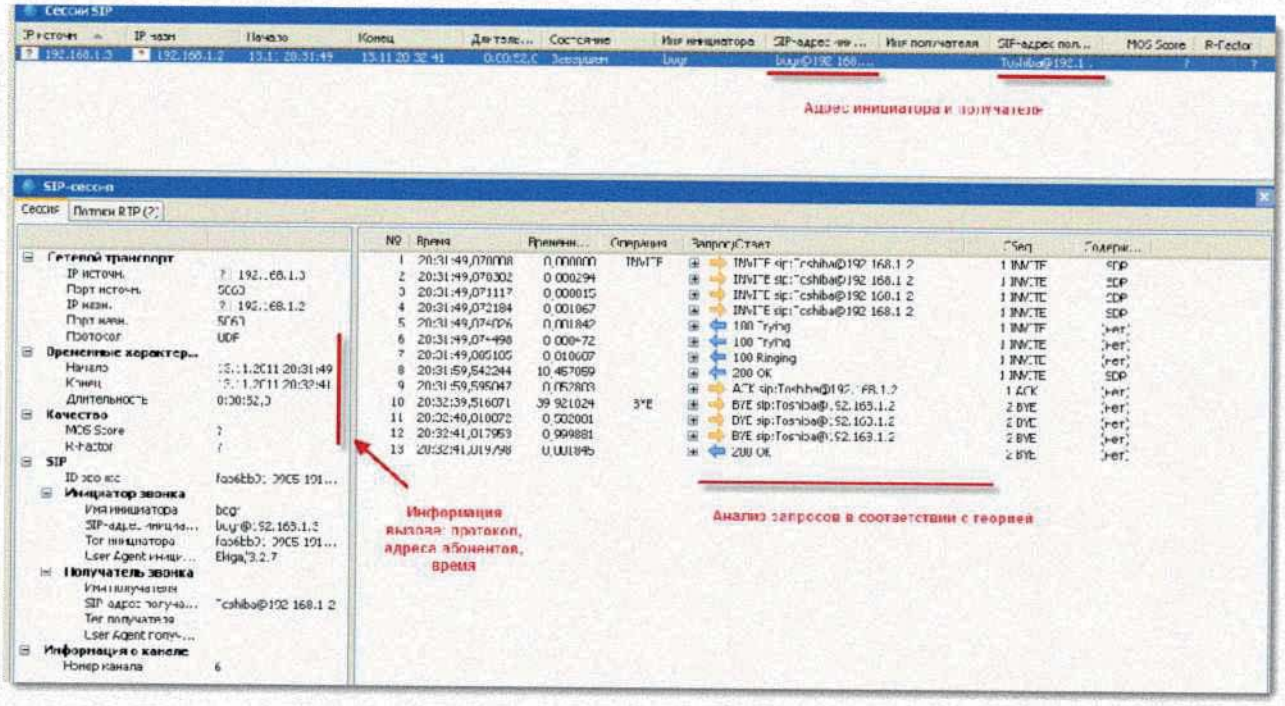
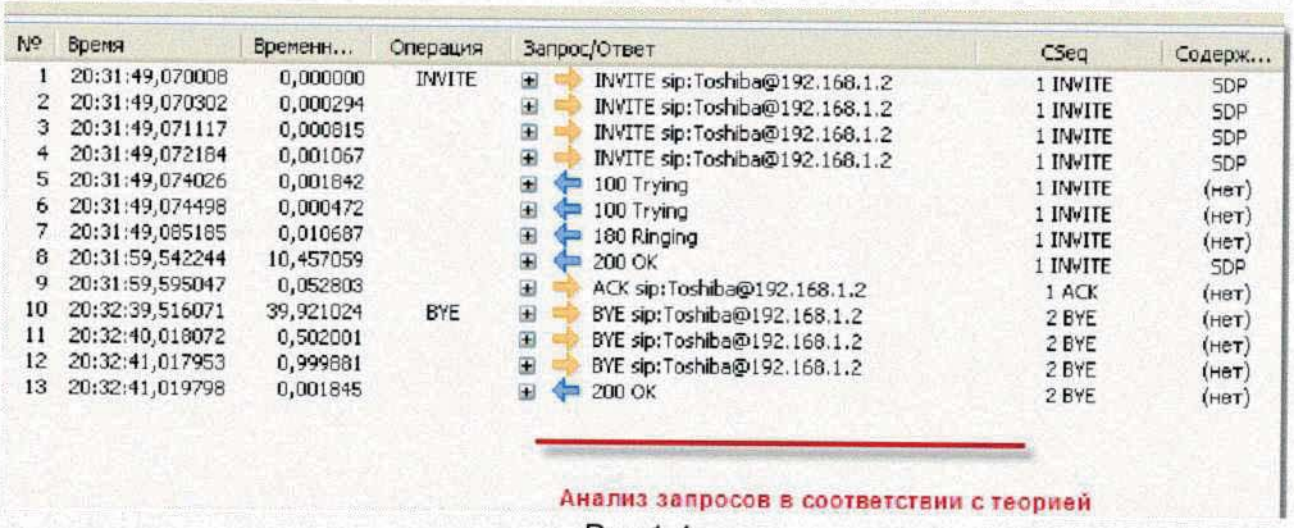


Рис.1.3.



№	Время	Временн...	Операция	Запрос/Ответ	CSeq	Содерж...
1	20:31:49,070008	0,000000	INVITE	INVITE sip:Toshiba@192.168.1.2	1 INVITE	SDP
2	20:31:49,070302	0,000294		INVITE sip:Toshiba@192.168.1.2	1 INVITE	SDP
3	20:31:49,071117	0,000815		INVITE sip:Toshiba@192.168.1.2	1 INVITE	SDP
4	20:31:49,072184	0,001067		INVITE sip:Toshiba@192.168.1.2	1 INVITE	SDP
5	20:31:49,074026	0,001842		100 Trying	1 INVITE	(нет)
6	20:31:49,074498	0,000472		100 Trying	1 INVITE	(нет)
7	20:31:49,085185	0,010687		180 Ringing	1 INVITE	(нет)
8	20:31:59,542244	10,457059		200 OK	1 INVITE	SDP
9	20:31:59,595047	0,052803		ACK sip:Toshiba@192.168.1.2	1 ACK	(нет)
10	20:32:39,516071	39,921024	BYE	BYE sip:Toshiba@192.168.1.2	2 BYE	(нет)
11	20:32:40,018072	0,502001		BYE sip:Toshiba@192.168.1.2	2 BYE	(нет)
12	20:32:41,017953	0,999881		BYE sip:Toshiba@192.168.1.2	2 BYE	(нет)
13	20:32:41,019798	0,001845		200 OK	2 BYE	(нет)

Анализ запросов в соответствии с теорией

Рис.1.4.

- Для анализа каждый запрос следует рассмотреть подробнее, нажав на «+».

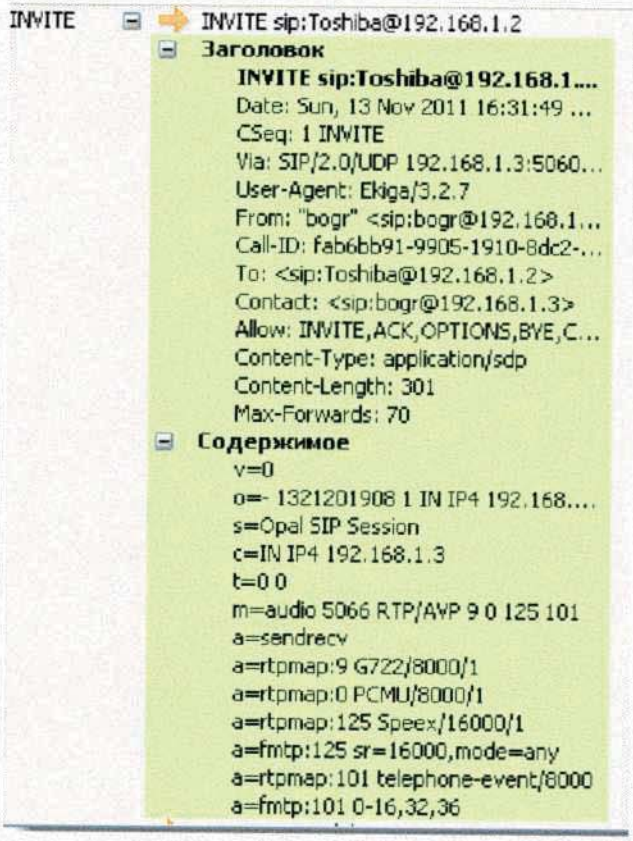


Рис.1.5.

- Проанализировать полученные результаты. Удостовериться в выполнении требований протокола. Сделать выводы.

2. Провести анализ RTP-сессии. Для этого:

- Проверить соответствие настроек Wi-Fi сети рекомендациям, представленным в лабораторной работе №2 (скорость передачи данных ограничить 1 Мбит/с).
- Совершить исходящий вызов с рабочего места 1 на рабочее место 2, используя в качестве сигнального протокола – SIP (кодек Speex 16 kHz).
- В CommView for WiFi проанализировать создание SIP-сессии и RTP-потоков.
- Во вкладке *VoIP/потоки-RTP* выделить RTP-поток текущего соединения и проанализировать его характеристики. Обратить внимание на значение параметров MOS Score и R-Factor.

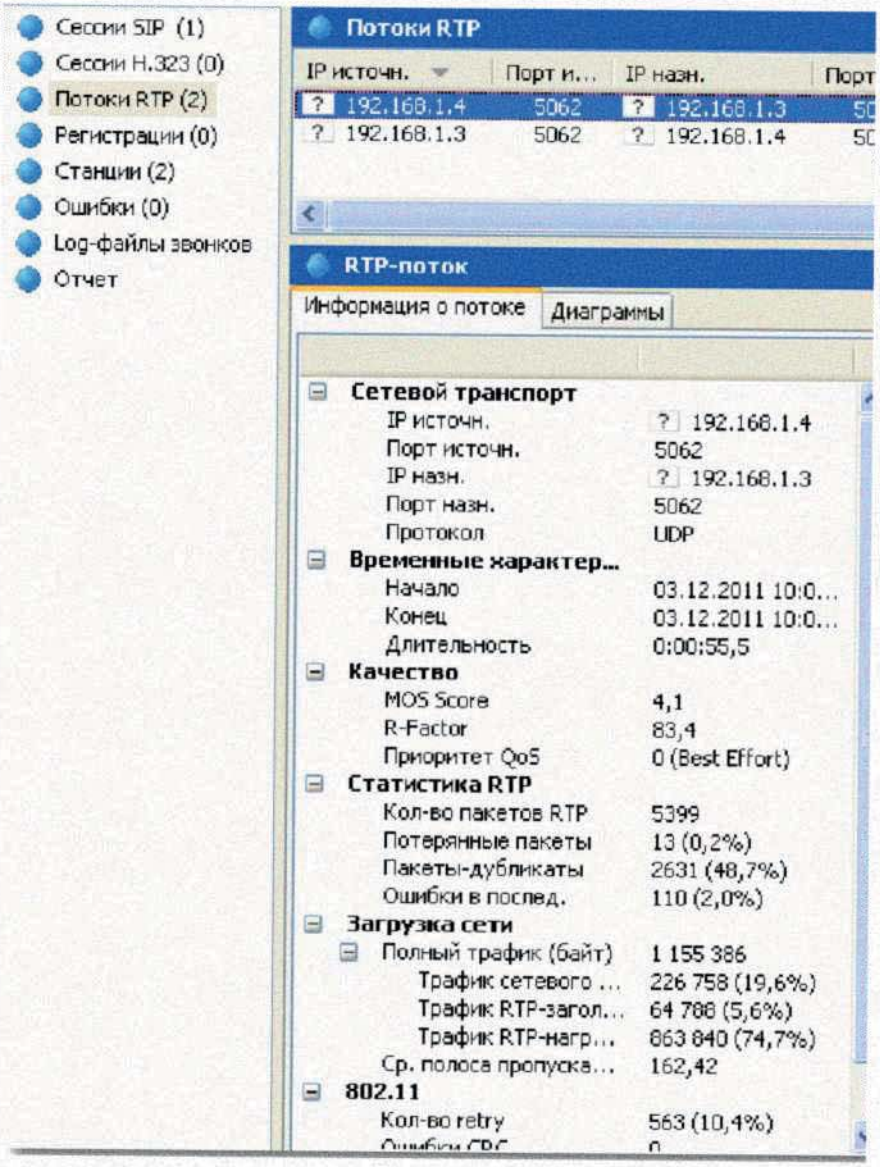


Рис.1.6.

- Перейти в закладку Диаграммы. Просмотреть и проанализировать диаграммы MOS Score и R-Factor.

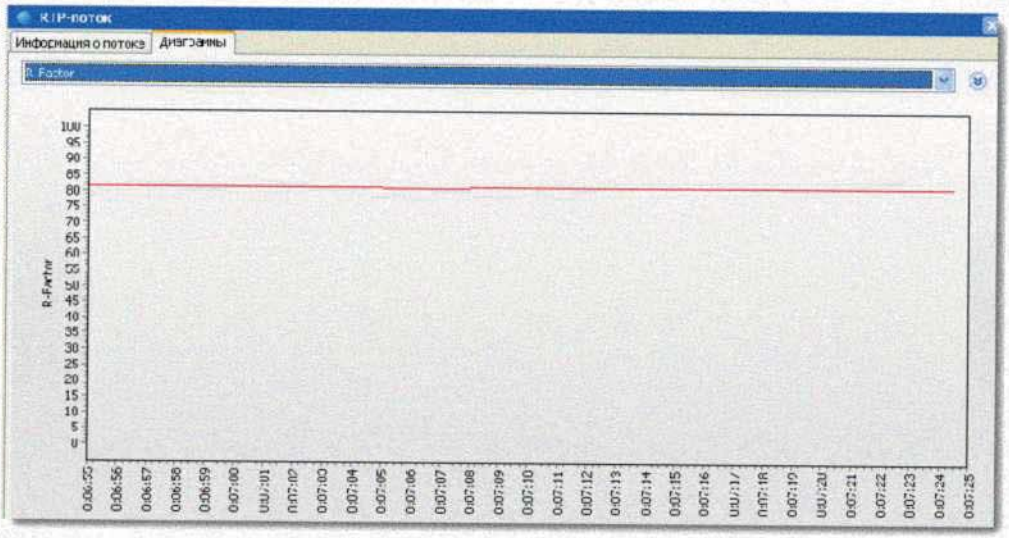


Рис.1.7.

- Параллельно с вызовом нагрузить сеть, осуществив передачу «тяжелого» файла собеседнику. Для этого достаточно на каждом рабочем месте выбрать по одной директории с предоставленным общим доступом (Мой компьютер/Сетевое окружение) и осуществить передачу файла.
- В течение 5-10 минут понаблюдать за изменениями диаграмм MOS Score и R-Factor. Объяснить изменения графиков.

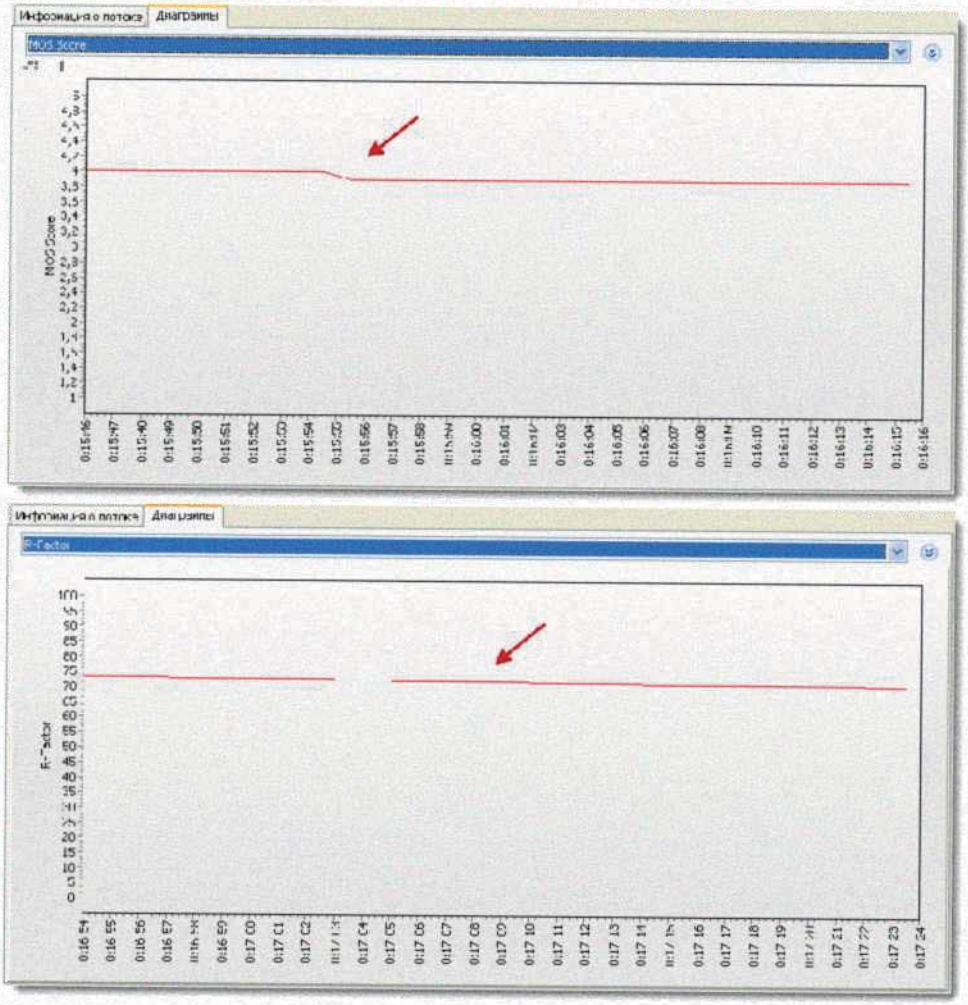


Рис.1.8.

- Убрать дополнительную нагрузку с сети, отменив передачу данных. В течение 10-15 минут понаблюдать за изменениями диаграмм MOS Score и R-Factor. Сделать выводы.

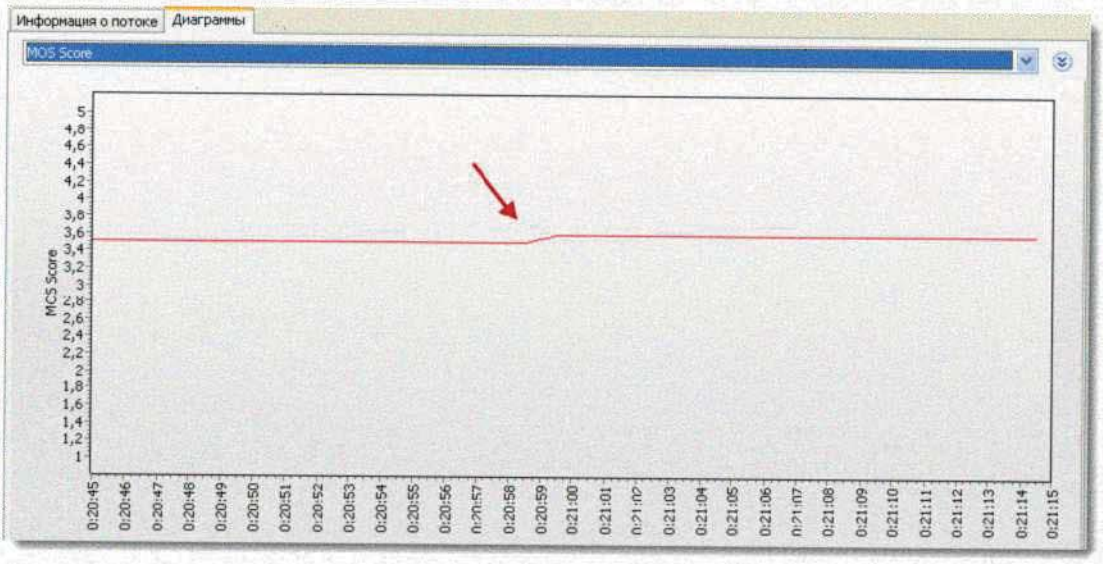


Рис.1.9.

Содержание отчета

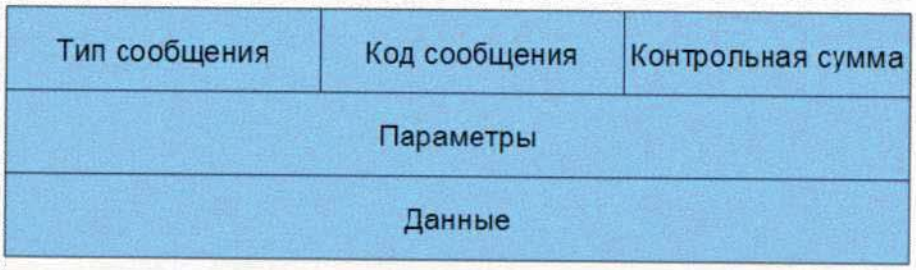
1. Перечень запросов/ответов при установлении SIP-соединения.
2. Диаграммы изменения показателей MOS Score и R-Factor при включении и выключении дополнительной нагрузки на сеть, а также выводы на их основе.

Практическая работа №2
МОНИТОРИНГ В СЕТЯХ СВЯЗИ: ПРОТОКОЛ ICMP, СПЕЦИАЛИЗИРОВАННЫЕ УТИЛИТЫ

Цель работы: овладение основными инструментами мониторинга сетей.

Краткая теоретическая справка

Протокол ICMP (Internet Control Message Protocol) является протоколом сообщений об ошибках. Несмотря на то, что ICMP считается протоколом сетевого уровня, его сообщения инкапсулируются в IP. Сообщения ICMP довольно разнообразны, но имеют единый формат (рис. 2.1). На этом протоколе базируются средства мониторинга сетей связи, а также сообщения о недоступности узла в некоторых протоколах прикладного уровня, например, ошибка 404 в HTTP.



Тип сообщения – согласно классификации
Код сообщения – дополнительные сведения об ошибке
Параметры – например, IP-адрес узла
Данные – например, IP-заголовок и первые 64 бита пакета, переадресованного на другой узел.

Рис.2.1. Формат сообщений ICMP

Протокол ICMP для IPv4 и его сообщения описаны в RFC 792, работа с масками сетей – в RFC 950 [2]. Протокол ICMP для IPv6 описан в RFC 4443 [3].

Инструменты мониторинга утилиты *ping* и *traceroute* описаны в RFC 2529 [4].

Утилита *ping* (Packet Internet Groper – одно из возможных прочтений) является одним из главных средств, используемых для

отладки сетей, и служит для принудительного вызова ответа конкретной машины. Она позволяет проверять работу приложений TCP/IP (по портам) на удаленных машинах, адреса устройств в локальной сети, адрес удаленного сетевого устройства. В выполнении команды *ping* участвуют система маршрутизации, схемы разрешения адресов и сетевые шлюзы. Это утилита низкого уровня, которая не требует наличия серверных процессов на зондируемой машине, поэтому успешный результат при прохождении запроса вовсе не означает, что выполняются какие- либо сервисные программы высокого уровня, а говорит о том, что сеть находится в рабочем состоянии, питание зондируемой машины включено, и машина не отказала. Утилита *ping* входит во все реализации TCP/IP не зависимо от операционной системы.

Получив эхо-запрос *ping*, программное обеспечение, реализующее протокол IP у адресата, посылает эхо-ответ. Эхо- запросы посылаются заданное количество раз (ключ *-n*) или по умолчанию до тех пор, пока пользователь не введет команду прерывания (Ctrl+C или Del), после чего выводятся статистические данные. В некоторых реализациях количество посылок эхо- запросов ограничено, например, в Windows их 4. В некоторых случаях можно в целях обеспечения безопасности (защита от DDOS-атак) выставить запрет на эхо-ответы. Список ключей и формат команды можно посмотреть самостоятельно, набрав в командной строке ping.

На практике большинство опций в формате команды можно опустить, тогда в командной строке может быть: ping имя_узла или ping IP-адрес.

Пример:

```
C:\Users\admin>ping yandex.ru
Обмен пакетами с yandex.ru [77.88.21.11] с 32 байтами данных:
Ответ от 77.88.21.11: число байт=32 время=1651мс TTL=57  Ответ от
77.88.21.11: число байт=32 время=154мс TTL=57
Ответ от 77.88.21.11: число байт=32 время=79мс TTL=57 Ответ от
77.88.21.11: число байт=32 время=77мс TTL=57
Статистика Ping для 77.88.21.11:
Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0%
потерь)
```

```
    Приблизительное время приема-передачи в мс:
    Минимальное = 77мсек, Максимальное = 1651 мсек, Среднее = 490
мсек
```

Утилита *traceroute* (в реализациях Windows используется написание *tracert*) позволяет выявлять последовательность шлюзов, через которые проходит IP-пакет на пути к пункту своего назначения. У этой команды есть много опций, большинство из которых применяются крайне редко. Традиционно используется формат traceroute имя_узла, которое может быть задано в символической или числовой форме. Выходная информация представляет собой список машин, начиная с первого шлюза и кончая пунктом назначения.

Принцип работы *traceroute* основан на установке поля времени жизни (TTL) исходящего пакета таким образом, чтобы это время истекало до достижения пакетом пункта назначения. При получении пакета с обнуленным полем TTL текущий шлюз отправит сообщение об ошибке на машину-источник. Каждое приращение поля времени жизни позволяет пакету пройти на один шлюз дальше.

Утилита *traceroute* посылает для каждого значения поля TTL три пакета. Если промежуточный шлюз распределяет трафик по нескольким маршрутам, то эти пакеты могут возвращаться разными машинами. Некоторые системы не посылают уведомлений о пакетах, время жизни которых истекло, а некоторые посылают уведомления, которые поступают обратно с задержкой, превышающей время ожидания на машине-источнике. Эти шлюзы обозначаются рядом звездочек. Если конкретный шлюз определить нельзя, все равно с помощью *traceroute* можно увидеть следующие за ним узлы маршрута. Заметим, что в связи с использованием на сетях динамической маршрутизации, в разные моменты времени можно получить различные маршруты прохождения пакетов. Это также относится к зеркалированным узлам.

Пример:

```
    admin@ddd:~$ traceroute lenta.ru
    traceroute to lenta.ru (81.19.85.92), 30 hops max, 60 byte
packets
    1 172.24.255.254 172.24.255.254) 13.218 ms
    14.129 ms 14.019 ms
```

```
2 84.204.14.254(84.204.14.254) 13.848 ms
15.145 ms 15.040 ms
3 46.47.255.33 (46.47.255.33) 13.910 ms 13.815 ms 14.594 ms
4 mx960-spb.peterstar.net(82.196.95.169) 15.117 ms 25.568 ms
26.261 ms
5 ix-j-mx240.m9.ramtel.ru(193.232.244.118 39.993 ms
39.870 ms 39.750 ms
6 s193-mx240.vr.rambler.ru (81.19.64.93) 39.672 ms17.704 ms
19.828 ms
7 81.19.94.132 (81.19.94.132) 19.772 ms 19.708 ms 19.590 ms
8 81.19.85.92 (81.19.85.92) 19.529 ms 19.424 ms 28.634 ms
```

Пример:

```
C:\Users\admin>tracert yandex.ru
Трассировка маршрута к yandex.ru [87.250.251.11] с максимальным
числом прыжков 30:
1 100 ms 104 ms 106 ms HS2-1-16.xG.SPb.SkyLink.RU [89.253.1.16]
2 119 ms 99 ms 106 ms HS2-0-1.xG.SPb.SkyLink.RU [89.253.0.1]
3 107 ms 106 ms 106 ms 212.129.96.227
4 112 ms 104 ms 106 ms aurora-spb-ix.yandex.net
[194.226.100.90]
5 128 ms 198 ms 110 ms 213.180.213.134
* * * Превышен интервал ожидания для запроса.
124 ms 108 ms 105 ms s650-eto2c1.yandex.net [213.180.213.65]
8 121 ms 132 ms 133 ms l3-s550-s650.yandex.net
[213.180.213.28]
9 116 ms 106 ms 133 ms yandex.ru [87.250.251.11] Трассировка
завершена.
```

Существует комбинированная диагностическая утилита *mtr* (My Traceroute), сочетающая в себе функциональность рассмотренных выше *traceroute* и *ping*. Данная утилита основана на библиотеке *libncurses* (консольная версия) или на базе GTK+ (оконная версия), позволяет в реальном времени отслеживать маршрут до заданного узла и изменяющееся время ответа каждого из промежуточных узлов, а также процент потерянных пакетов. Консольный вывод утилиты *mtr* представлен на рисунке 2.2. На данный момент *mtr* включена практически во все дистрибутивы Linux.

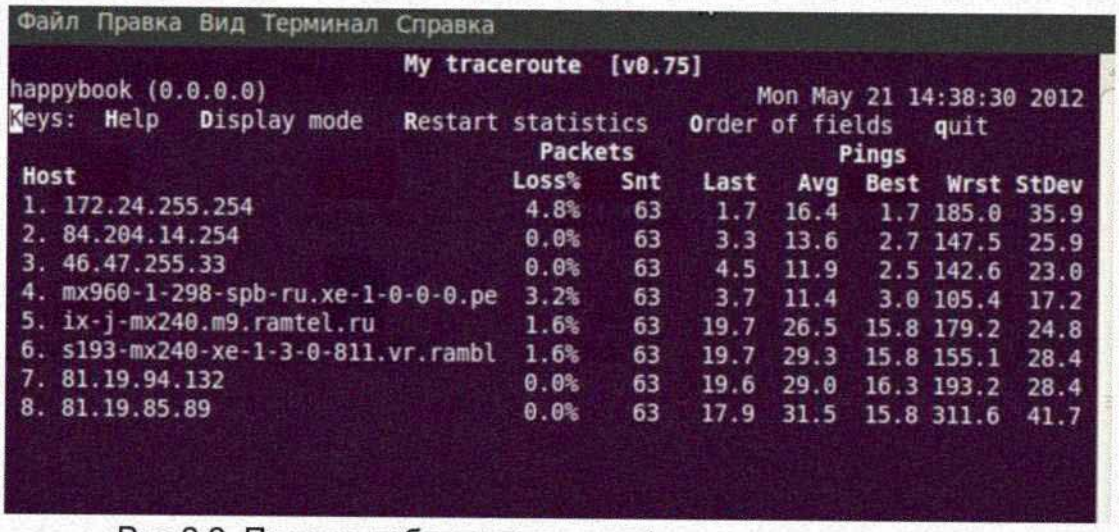


Рис.2.2. Пример работы утилиты *mtr* в консольном режиме

Утилита *netstat* выводит информацию о локальной сети и средствах TCP/IP. Она реализована непосредственно в операционной системе и занимается сбором статистики об ошибках, текущих соединениях, состоянии портов и соединений. Содержание и форма выходной информации зависят от операционной системы, но обычно выводятся следующие данные: список соединений, статистика сетевых интерфейсов, статистика по буферам данных, содержание таблицы маршрутизации, статистика работы протоколов. Характер выводимой информации можно выбирать с помощью опций командной строки. Рассмотрим основные возможности мониторинга с помощью утилиты *netstat.*

Список соединений

Утилита *netstat* обладает набором ключей для отображения портов, находящихся в активном и/или пассивном состоянии.

Таким образом, можно получить список всех серверных приложений, работающих на данном компьютере. Отметим, что формат списка соединений для сервера с системой NAT и для клиентской машины будет разным.

Информация выводится столбцами. В первом из них указан протокол, затем размеры очередей приема и передачи для установленного соединения на данной машине (на другом конце соединения размеры очередей могут быть другими), локальный и удаленный адреса и текущее состояние соединения.

Пример:

```
admin@ddd:~$ netstat -ta
Активные соединения с интернетом (servers and
established) Proto Recv-Q Send-Q Local Address
Foreign Address State tcp      0 0 *:29011          *:*
     LISTEN
tcp  0 0 localhost:ipp    *:* LISTEN
tcp  0 0 172.24.0.157:35608
     213.199.179.141:40041 ESTABLISHED
tcp  0 0 172.24.0.157:37760    163-
247.static.quie:www TIME_WAIT
tcp  0 0 172.24.0.157:36441    95-28-49-
237.broa:26647 ESTABLISHED
tcp  0 0      172.24.0.157:38541      172.24.0.170:55554          TIME_WAIT
tcp  0 0      172.24.0.157:54369            bos-w031b-rdr1.bl:https
ESTABLISHED
tcp  0 0      172.24.0.157:38543      172.24.0.170:55554          TIME_WAIT
tcp  0 0      172.24.0.157:55651            broadband-95-84-1:17654
ESTABLISHED
tcp  0 0 172.24.0.157:43546
     178.204.199.167:26639 ESTABLISHED
tcp  0 0 172.24.0.157:44763    agama.yande:xmpp-
client ESTABLISHED
tcp  0 0 172.24.0.157:43715    chat-p01c-
rdr1.bl:https ESTABLISHED
tcp  0 0 172.24.0.157:53870    broadband-109-
173:20143 ESTABLISHED
tcp  0 0 172.24.0.157:43067    h178-129-218-
223.d:8740 ESTABLISHED
tcp  0 0 172.24.0.157:53809
     89.189.134.198.dy:22113 ESTABLISHED
tcp  0 0 172.24.0.157:44762    agama.yande:xmpp-
client ESTABLISHED
tcp  0 0 172.24.0.157:53246
     212.8.166.36:https ESTABLISHED
tcp  0 0 172.24.0.157:55257    bart-
w04b.blue.ic:https ESTABLISHED
tcp  0 0 172.24.0.157:33021
     dialin.customers.:26770 ESTABLISHED
tcp  0 0 172.24.0.157:58275
     140.222.81.95.chtt:4078 ESTABLISHED
tcp  0 0 172.24.0.157:46402
     91.190.216.24:12350 ESTABLISHED
tcp6  0 0 localhost:ipp   [::]:*              LISTEN
```

Состояние соединения имеет значение только для протокола TCP. Протокол UDP факта установления соединения не проверяет.

Содержание таблицы маршрутизации

Каждое соединение машины с сетью называется сетевым интерфейсом. Машина, имеющая более одного интерфейса, может принимать данные по одному интерфейсу и передавать их по другому, осуществляя пересылку данных между сетями. Эта функция называется маршрутизацией, а машина, выполняющая ее – шлюзом.

Данные маршрутизации хранятся в так называемых таблицах маршрутизации, которые могут быть статическими и динамическими в зависимости от уровня сети и протокола маршрутизации. Для направления пакета по конкретному адресу подбирается наилучший маршрут согласно метрике. Если такой маршрут отсутствует, и нет маршрута по умолчанию, то отправителю возвращается сообщение об ошибке.

Утилита netstat -r позволяет отображать таблицу маршрутизации.

Пункты назначения и шлюзы могут показываться в виде имен машин или в виде их IP-адресов. Флаги дают оценку маршрута.

Пример:

```
admin@ddd:~ >
netstat -r Kernel IP
routing table
Destination     Gateway       Genmask       Flags       Ifac
ddd.sut.ru        *               255.255.255.255  UH  eth1
195.19.219.120 *              255.255.255.248 U  eth0
195.19.219.128 *              255.255.255.192     U    eth1
192.168.1.0       *               255.255.255.0  U    eth0
195.19.221.0      lgw.ccs.sut.ru 255.255.255.0  UG   eth1
193.125.0.0     lgw.ccs.sut.ru  255.255.0.0    UG   eth1
loopback          *               255.0.0.0      U    lo
default           lgw.ccs.sut.ru 0.0.0.0        UG   eth1
```

Статистика сетевых интерфейсов

При использовании ключа -e на экран будут выведены

статистические данные всех используемых Ethernet-интерфейсов. Исходя из них, можно выяснить, исправно ли соединение с сетью.

Пример:

```
admin@ddd:~ >
netstat -e Kernel
Interface table
```

Iface	MTU	Met	RX-OK	RX-ERR	RX-DRP	RX-OVR	TX-OK	TX-ERR	TX-DRP	TX-OVR	Flg
eth0	1000	0	844904	0	17	0	1454454	5	0	0	BRU
eth1	1500	0	590844	0	7	0	434438	59	0	0	BRU
lo	3924	0	45754	0	0	0	45754	0	0	0	LRU

Ошибки являются следствием проблем в кабельной системе или следствием неисправности платы сетевого адаптера. В нормально работающей сети количество конфликтов (RX-OVR, TX-OVR) не должно превышать 3% от числа пакетов, а другие ошибки не должны составлять более 0,5% от общего числа пакетов.

Статистика передачи данных

Использование *netstat -s* позволяет вывести содержимое счетчиков сетевых программ. В выходной информации есть разделы, относящиеся к различным протоколам: IP, ICMP, TCP, UDP. С ее помощью можно определить место появления ошибки в принятом пакете.

Пример:

```
admin@ddd:~$ netstat -s Ip:
всего пакетов принято 17058
2 с неверными адресами

0 перенаправлено
0 входящих пакетов отклонено входящих пакетов доставлено: 4364
запросов отправлено: 3936
Icmp:
ICMP сообщений получено: 306 неудачных входящих ICMP
сообщений: 0 Гистограмма входа ICMP
пункт назначения недоступен: 8 потери при прохождении: 263
эхо-ответы: 35
послано сообщений ICMP: 280 неудачные сообщения ICMP: 0
Гистограмма выхода ICMP
пункт назначения недоступен: 8 эхо-запросов: 14
IcmpMsg:
InType0: 35
InType3: 8
```

```
    InType11: 263
    OutType3: 8
    OutType8: 14
    OutType69: 258

    Tcp:

    Udp:

    открытия активных соединений: 148 открытия пассивных
соединений: 0 неудачные попытки соединения: 4 получено сбросов
соединений: 2 соединений установлено: 0
    сегментов получено: 3386
    отправлено сегментов: 2895 повторно передано сегментов: 39
плохих сегментов получено: 0 сбросов послано: 8

    пакетов принято: 661
    принято пакетов на неизвестный порт: 8 ошибок приема пакетов:
0
    пакетов послано: 723

    UdpLite: TcpExt:
    пакеты, вырезанные из очереди приема по причине переполнения
буфера сокета: 1
    67 TCP sockets finished time wait in fast timer задержанных
подтверждений послано: 119

    Режим быстрого подтверждения приема был активирован 69 раз
    11 packets directly queued to recvmsg prequeue.
    3635 bytes directly received in process context from prequeue
ожидаемых заголовков пакетов: 1745
    ожидаемых заголовков пакетов, непосредственно стоявших в
очереди к пользователю: 5
    311 acknowledgments not containing data payload received
ожидаемые подтверждения: 299
    congestion windows recovered without slow start after partial
ack

    1 timeouts in loss state
    19 retransmits in slow start других TCP тайм-аутов: 19
    22 packets collapsed in receive queue due to low socket buffer
получено DSACKs: 9
    соединения сброшены из-за неожиданных данных
    connections reset due to early user close
TCPDSACKIgnoredNoUndo: 3 TCPSackShiftFallback: 9
    IpExt:
```

```
InMcastPkts: 15
OutMcastPkts: 19
InOctets: 4353792
OutOctets: 405434
InMcastOctets: 2714
OutMcastOctets: 2990
```

Изучаемые в процессе выполнения практической работы средства мониторинга относятся к универсальным в сетях IP. Они являются встроенными во все операционные системы с поддержкой IP, работают как с IPv4, так и с IPv6. Для своей работы утилита *netstat* использует статистику, собранную при помощи ICMP. Так как ICMP для IPv4 и IPv6 имеет отличия, связанные непосредственно с изменением формата заголовка, то и результат для этих протоколов будет отличаться. Современные операционные системы поддерживают обе версии ICMP.

Задание на практическую работу:

1. Провести трассировку трех узлов по заданию преподавателя. По результатам построить графики зависимости времени прохождения пакета от номера узла. Указать шлюзы перехода из одной сети в другую. Листинги трассировки привести в отчете.

2. Провести оценку работоспособности узлов: узлов в подсети лаборатории, шлюза подсети, 5 узлов из ранее сделанных трассировок. Оценить TTL для каждого из них.

3. Запустить несколько сетевых приложений на клиентской машине (например, несколько сайтов, интернет-мессенджер и т.п.). Снять с клиентской машины при помощи утилиты *netstat* таблицу маршрутизации, список соединений, статистику передачи данных, состояние интерфейса Ethernet. На основании списка соединений построить карту сети. На основе таблицы маршрутизации зарисовать архитектуру сети.

К защите:

1. Знать основные принципы мониторинга сетей, характеристики сетей (TTL, время приема-передачи и т.п.), принципы работы средств мониторинга (всех используемых в практической работе утилит).

2. Уметь использовать средства мониторинга IP-сетей.

3. Представить отчет, содержащий листинги работоспособности узлов, результаты трассировки, графики зависимости времени прохождения пакета от номера узла, статистику работы сети согласно netstat, карту сети, архитектуру сети на основе таблицы маршрутизации.

Рекомендуемая литература

1. RFC 792 Internet control message protocol. September, 1981.

2. RFC 950 Internet Standard Subnetting Procedure. August 1985

3. RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. March, 2006

4. RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations. September, 2000.

5. Олифер Н. А., Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. Издание 4-е. Питер, 2010.

Практическая работа №3
ИЗУЧЕНИЕ МЕХАНИЗМОВ УДАЛЕННОГО МОНИТОРИНГА СЕТИ WI-FI

Цель работы: получение практических навыков мониторинга состояния сети Wi-Fi.

Задание

Используя возможности сетевого анализатора CommView for WiFi, осуществить сканирование сети с целью обнаружения перегрузки, неизвестного MAC-адреса, неизвестного IP-адреса, неизвестных точек доступа (AP), а также Ad-hoc сетей.

Указание к выполнению работы

Внимание! Перед выполнением практической работы рекомендуется приостановить работу антивируса Kaspersky. Для этого достаточно выбрать значок антивируса на панели задач, нажать правой кнопкой мыши и выбрать пункт **Приостановка защиты и контроля...**

1. Определить перегрузку беспроводной сети:

- В соответствии с рекомендациями п.1.3.2 лабораторной работы 2 настроить беспроводную сеть с топологией BSS.
- Запустить программу-анализатор CommView for WiFi  . Очистить данные предыдущих VoIP-сессий (Файл/Очистить данные VoIP).
- Перейти на вкладку *Предупреждения* и нажать кнопку **Добавить**.

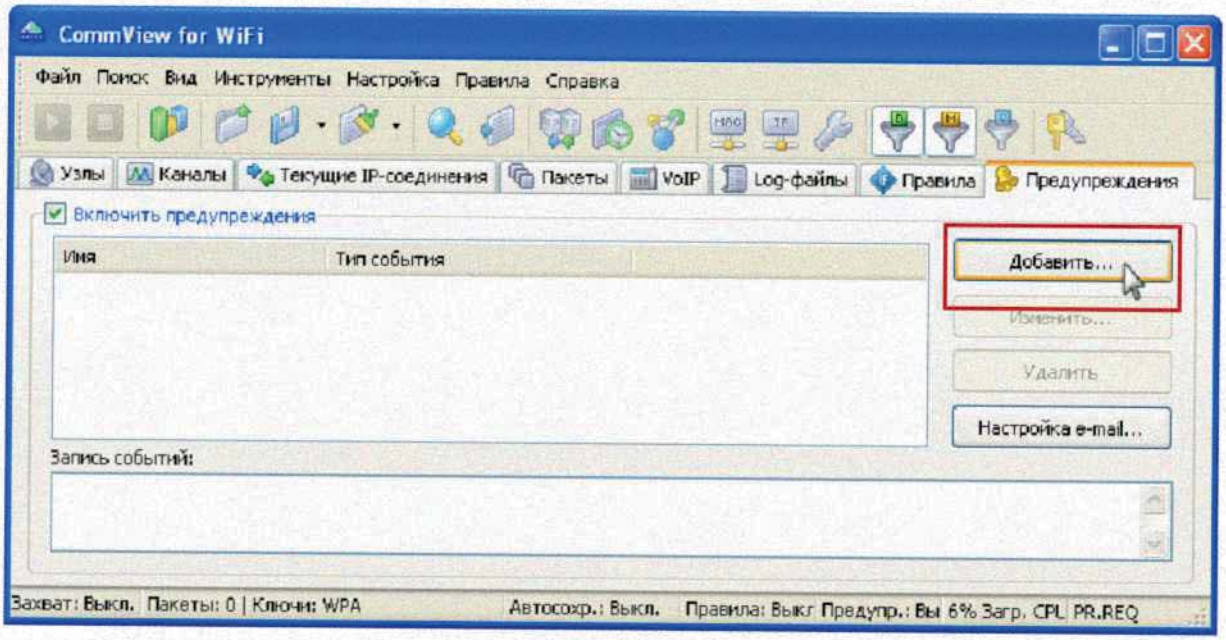


Рис.3.1.

- Для начала эксперимента выставите параметры, как показано на рисунке ниже и нажмите кнопку **Ок**.

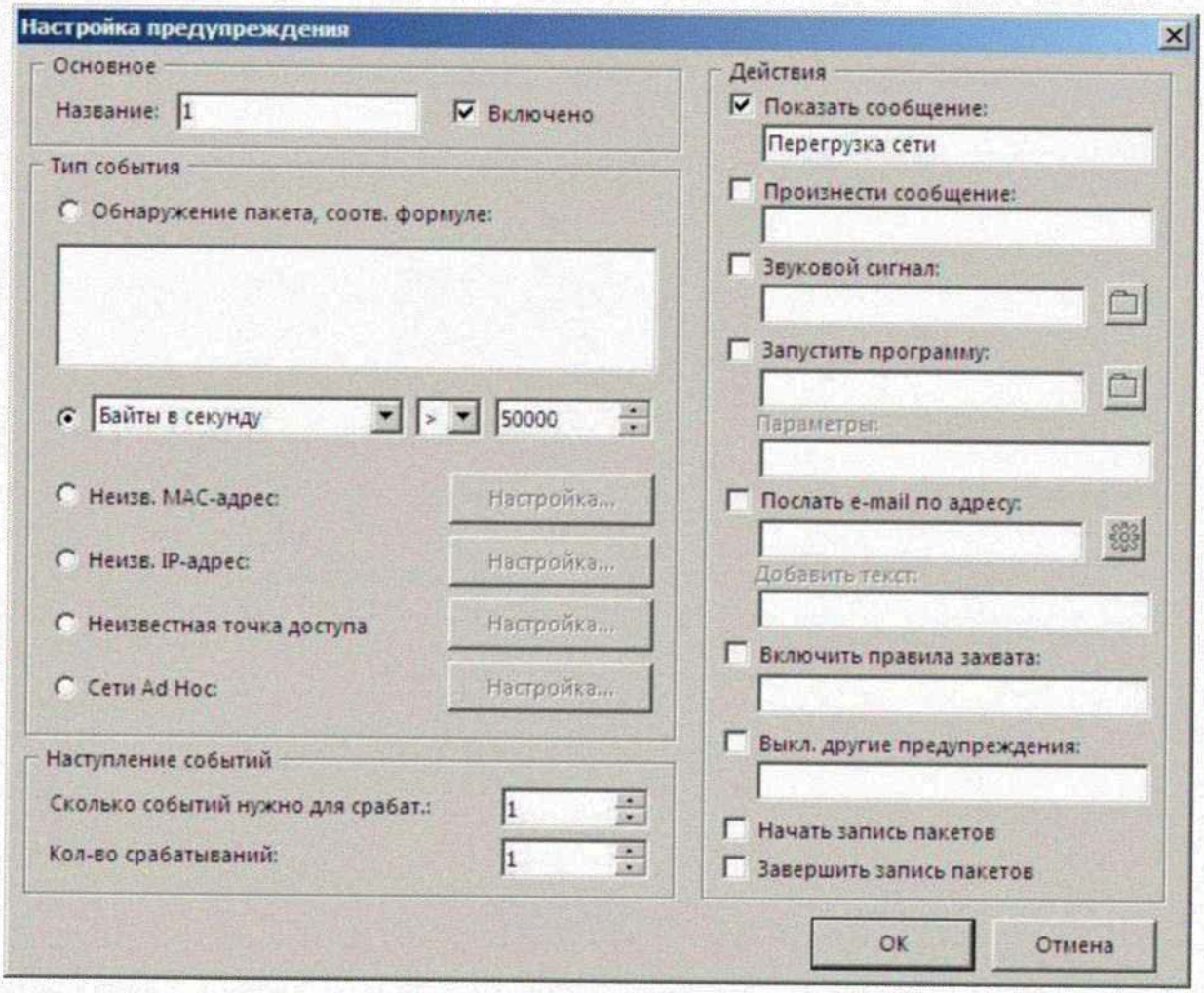


Рис.3.2.

В соответствии с указаниями произвести сканирование эфира на предмет сигналов Wi-Fi. Из появившегося списка выбрать требуемую («нашу») точку доступа и нажать кнопку **Захват**.

- Начать передавать «тяжелый» файл между компьютерами беспроводной сети. Убедиться в работе предупреждения.

2. Обнаружение неизвестного MAC-адреса. Для выполнения эксперимента необходимо:

- На рабочих местах определить MAC-адреса адаптеров и точек доступа. Для определения физического адреса адаптера можно воспользоваться запросом *ipconfig /all*, введенным в командной строке Windows. Адрес точки доступа указан на нижней стороне устройства.

Примечание: MAC-адрес точки доступа также можно посмотреть через web-интерфейс её настроек.

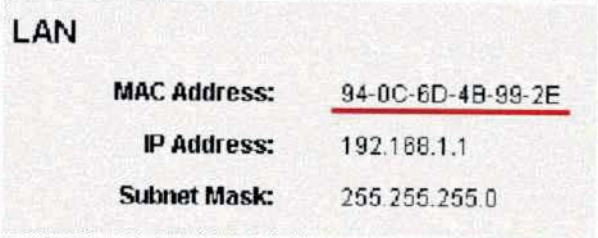


Рис.3.3.

- В соответствии с рекомендациями п.1.3.2 лабораторной работы 2 настроить беспроводную сеть с топологией BSS, подключив к точке доступа **только** один компьютер.
- Перейти во вкладку *Предупреждения* CommView for WiFi и выставить параметры, как показано на рисунке ниже.

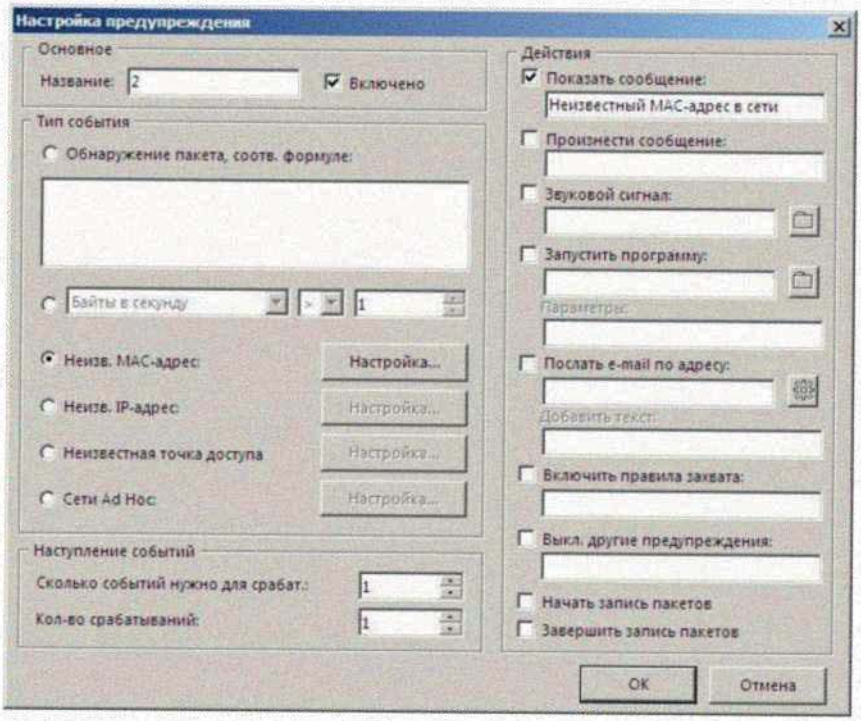


Рис.3.4.

- Нажать кнопку **Настройка** и ввести MAC-адреса известных устройств (точки доступа и одного из двух компьютеров). После чего нажать кнопку **ОК**.

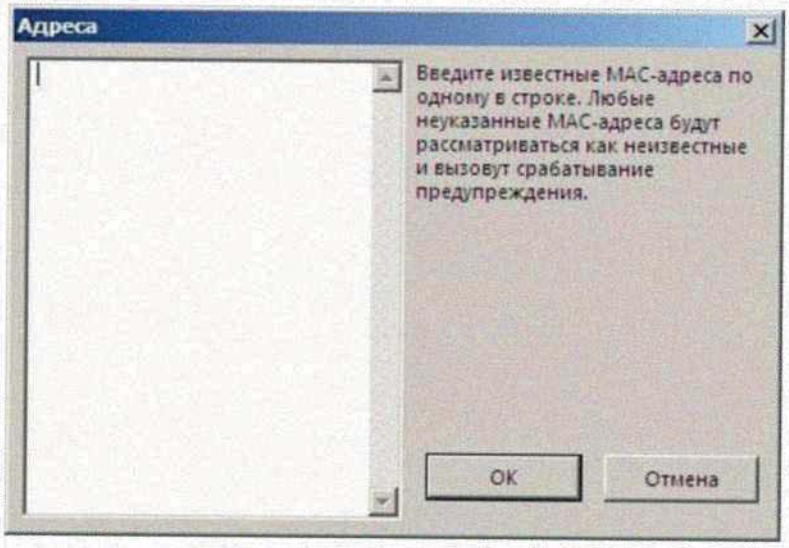


Рис.3.5.

Примечание: Значение MAC-адреса необходимо указывать в формате: 00:00:00:00:00:00

- Запустить захват пакетов на рабочем канале.
- Подключить к точке доступа второй компьютер, MAC-адрес которого не был указан в списке. Убедиться в работе предупреждения.

3. Обнаружение неизвестного IP-адреса. Для выполнения

эксперимента необходимо:

- На рабочих местах определить IP-адреса адаптеров и точек доступа. Для определения IP-адреса адаптера можно воспользоваться запросом *ipconfig /all*, введенным в командной строке Windows. IP-адрес точки доступа должен соответствовать требованиям п. 1.3.2. Проверить значение можно через web- интерфейс настройки.

Табл. 3.1.

	1	**2**	**3**
SSID	group1	group2	group3
Канал	2	4	8
IP-адреса AP	192.168.1.10	192.168.1.20	192.168.1.30
IP-адреса SS	192.168.1.11 192.168.1.12	192.168.1.21 192.168.1.22	192.168.1.31 192.168.1.32

- В соответствии с рекомендациями п.1.3.2 лабораторной работы 2 настроить беспроводную сеть с топологией BSS, подключив к точке доступа **только** один компьютер.
- Перейти во вкладку *Предупреждения* CommView for WiFi и выставить параметры, как показано на рисунке ниже.

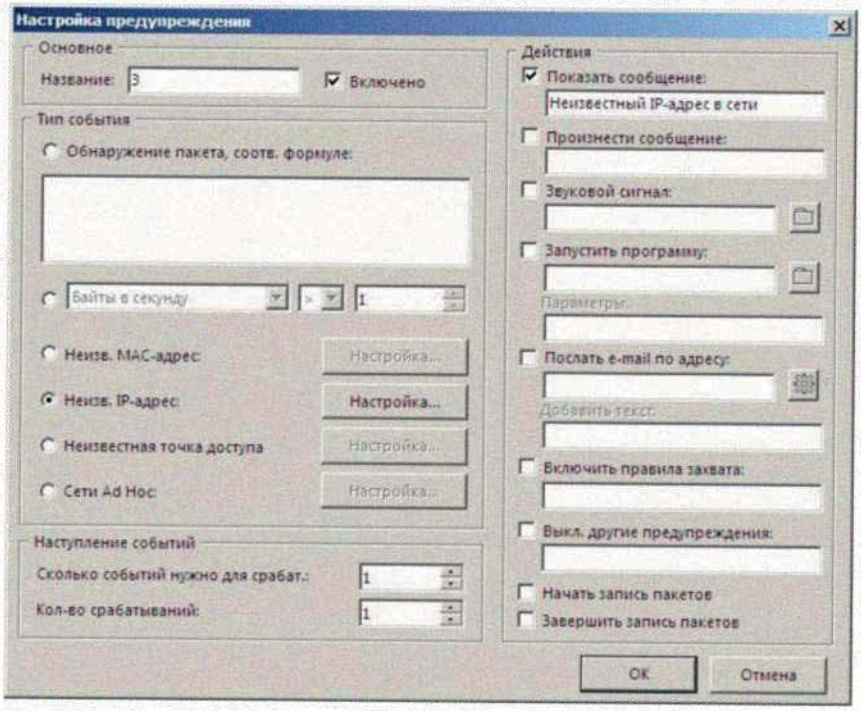


Рис.3.6.

- Нажать кнопку **Настройка** и ввести ip-адреса известных устройств (точки доступа и одного из двух компьютеров). После чего нажать кнопку **ОК**.

Примечание: Для выполнения эксперимента необходимо проверить, что включен режим захвата пакетов данных (Правила/ Захватывать data- пакеты).

- Запустить захват пакетов на рабочем канале.
- Подключить к точке доступа второй компьютер, ip-адрес которого не был указан в списке. Убедиться в работе предупреждения.

4. Обнаружение неизвестной точки доступа (AP), работающей на одном канале с нашей точкой. Для выполнения эксперимента требуется:

- В соответствии с рекомендациями п.1.3.2 лабораторной работы 2 настроить беспроводную сеть с топологией BSS.
- Перейти во вкладку *Предупреждения* CommView for WiFi и выставить параметры, как показано на рисунке ниже.

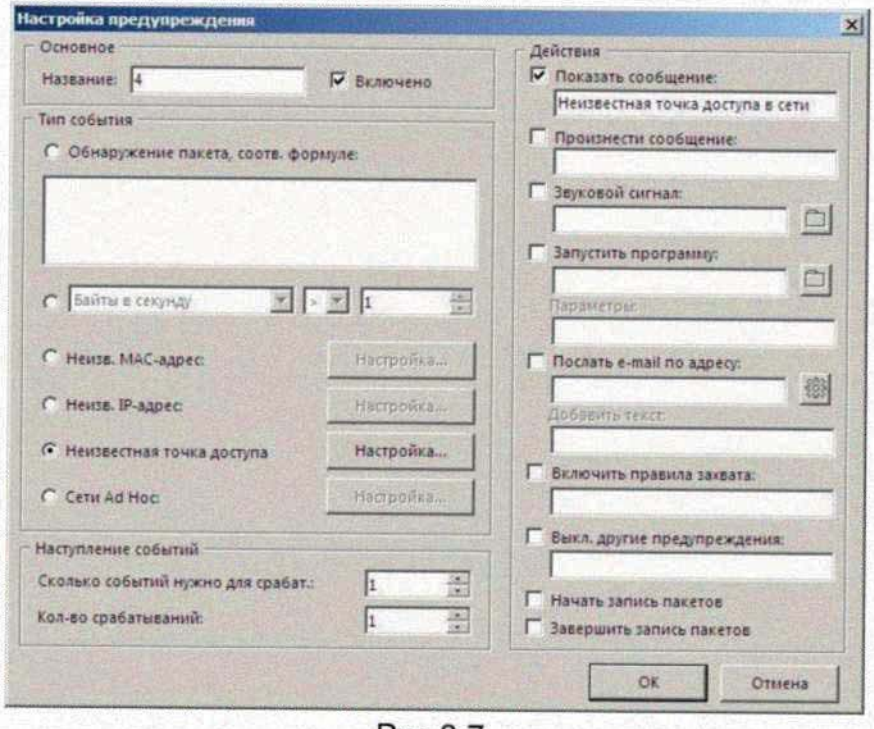


Рис.3.7.

Примечание: Обнаружение новой точки доступа осуществляется по beacon-пакетам. По этой причине для выполнения эксперимента необходимо убедиться, что в CommView for Wi-Fi выключено

игнорирование таких пакетов.

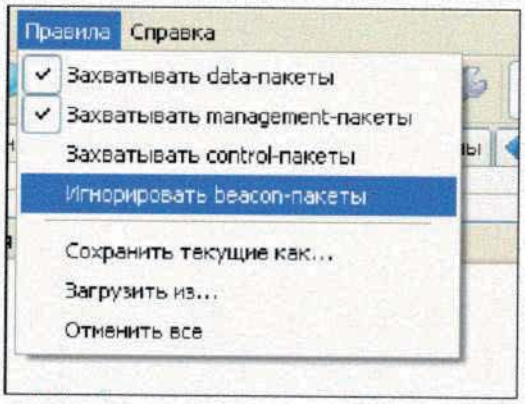


Рис.3.8.

- Нажать кнопку **Настройка** и ввести MAC-адрес «известной» рабочей точки доступа, после чего нажать кнопку **ОК**.
- Запустить захват пакетов на рабочем канале.
- Перевести соседнюю точку доступа на канал работы нашей точки. Убедиться в работе предупреждения.

5. Обнаружение неизвестных Ad-hoc сетей. Для выполнения эксперимента требуется:

- В соответствии с методическими указаниями п. 1.3.2 развернуть на рабочих местах Ad-hoc сеть.
- С помощью программы «inSSIDer» определить канал работы нашей Ad Hoc сети.
- Разорвать сеть Ad-hoc.
- Перейти во вкладку *Предупреждения* CommView for WiFi и выставить параметры, как показано на рисунке ниже.

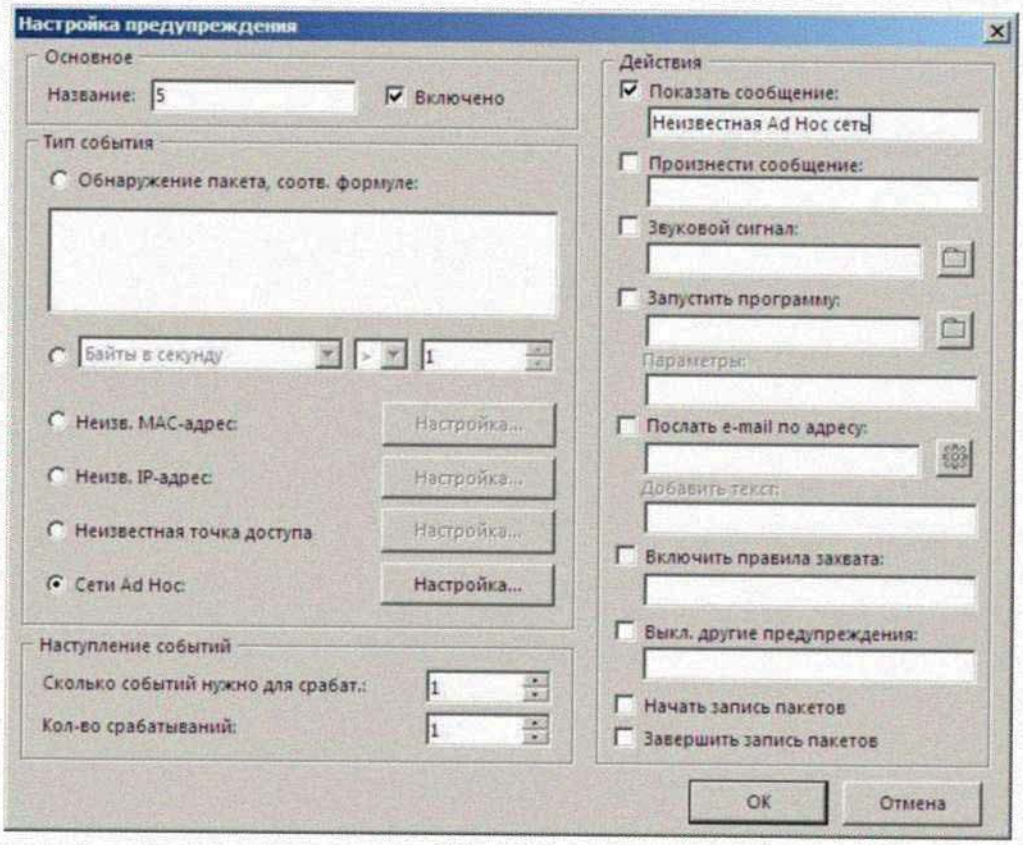


Рис.3.9.

Примечание: Обнаружение ad-hoc сетей осуществляется по beacon- пакетам. По этой причине для выполнения эксперимента необходимо убедиться, что в CommView for Wi-Fi выключено игнорирование таких пакетов.

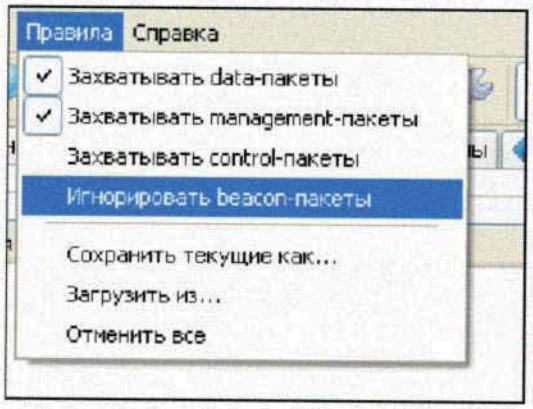


Рис.3.10.

- В закладке *Настройка* **не** следует прописывать MAC-адреса станций известных Ad Hoc сетей.
- Запустить захват пакетов на канале работы нашей Ad-Hoc сети.
- Повторно установить Ad-Hoc сеть.
- Убедиться в срабатывании предупреждения.

Содержание отчета

Отчет должен содержать краткое описание всех 5 экспериментов с указанием ip-адресов и схем взаимодействия компонентов.

Рекомендуемая литература

1. RFC 792 Internet control message protocol. September, 1981.
2. RFC 950 Internet Standard Subnetting Procedure. August 1985
3. RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. March, 2006
4. RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations. September, 2000.
5. Олифер Н. А., Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. Издание 4-е. Питер, 2010.

Практическая работа №4
ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ В ЛОКАЛЬНЫХ СЕТЯХ. ЗАЩИТА КОРПОРАТИВНЫХ СЕТЕЙ

Цель работы: получение практических навыков защиты сложных беспроводных корпоративных локальных сетей.

Задание

- Создать сеть топологии ESS и подключить RADIUS-сервер к этой сети.
- Настроить доступ к RADIUS-серверу с каждой рабочей станции.
- Сконфигурировать RADIUS-сервер.
- Проверить работоспособность RADIUS-сервера.

Указание к выполнению работы

Внимание! Перед выполнением практической работы рекомендуется приостановить работу антивируса Kaspersky. Для этого достаточно выбрать значок антивируса на панели задач, нажать правой кнопкой мыши и выбрать пункт **Приостановка защиты и контроля...**

1. Настройка точек доступа и беспроводного клиентского оборудования.

- На рабочих местах настроить беспроводную сеть с топологией ESS, руководствуясь методическими указаниями к лабораторной работе 4.
- По Ethernet соединению подключить RADIUS-сервер к коммутатору.
- Проверить соответствие сетевых настроек ПК требованиями лабораторной работы 2.

Табл. 4.1

	1	2	3
IP-адрес ПК	192.168.1.19	192.168.1.29	192.168.1.39
Маска подсети	255.255.255.0	255.255.255.0	255.255.255.0

• Сбросить настройки беспроводного маршрутизатора в заводские, нажав и удерживая некоторое время кнопку **reset**, находящуюся на задней панели устройства.

• Осуществить настройку точек доступа в соответствии с заданием к лабораторной работе 2.

Табл. 4.2.

Параметр настройки	Задание для бригады		
	1	**2**	**3**
Режим работы	Access Point		
SSID	group1	group2	group3
Канал	2	4	8
IP-адрес AP	192.168.1.10	192.168.1.20	192.168.1.30
IP-адреса SS	192.168.1.11 192.168.1.12	192.168.1.21 192.168.1.22	192.168.1.31 192.168.1.32
Маска подсети	255.255.255.0	255.255.255.0	255.255.255.0

• Проверить наличие соединения Рабочее место – RADIUS-сервер (путь: *Wi-Fi адаптер – Точка доступа – Коммутатор – RADIUS-сервер*), выполнив ping-запрос с рабочего места до RADIUS- сервера (команда *ping 192.168.1.5)*.

Примечание: IP-адрес RADIUS-сервера: 192.168.1.5 Не изменяется!

2. Рассмотреть основные параметры конфигурационного файла radiusd.conf. Для этого:

• Для осуществления подключения к серверу через SSH протокол запустить утилиту PuTTY  .

Внимание! Перед запуском утилиты обязательно сменить язык раскладки клавиатуры на английский.

• В настройках указать ip-адрес RADIUS-сервера, тип соединения – SSH.

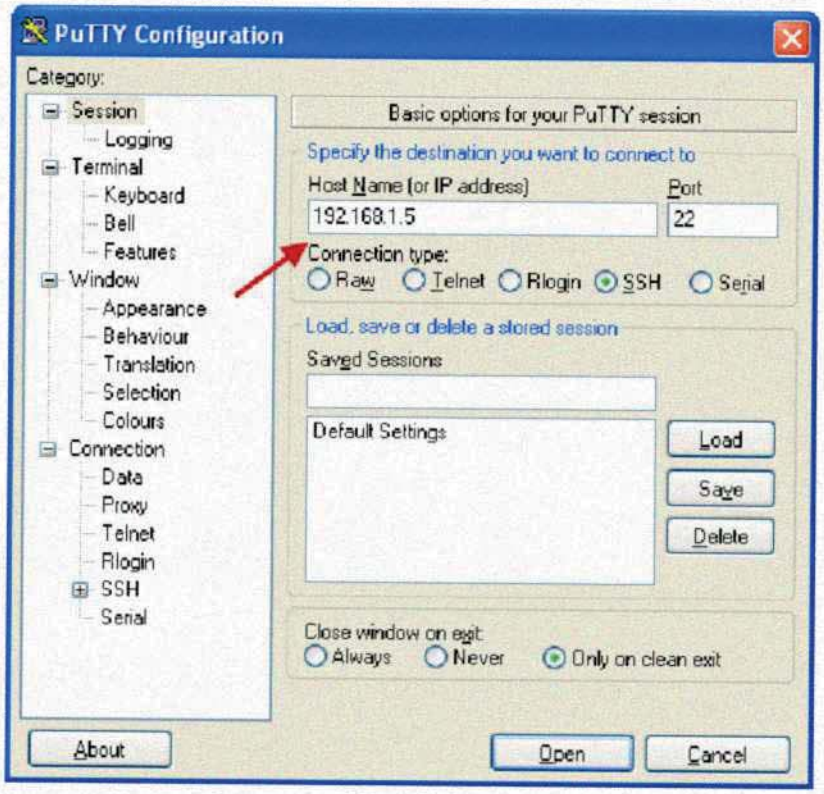


Рис.4.1.

- Перейти в раздел *Window/Translation*, где выбрать кодировку UTF-8. После нажать кнопку **OPEN**.

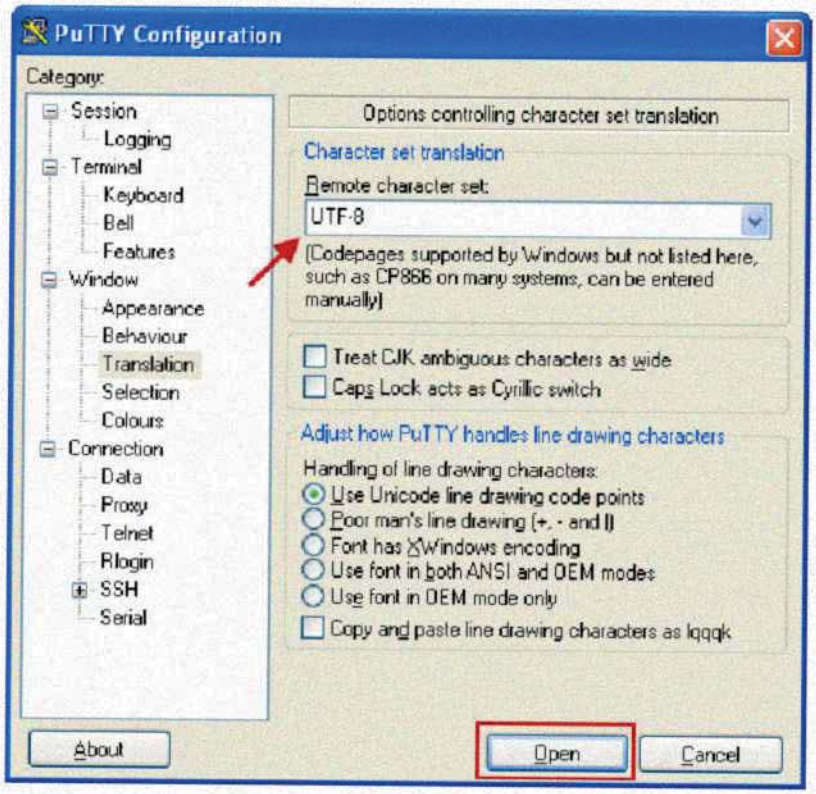


Рис.4.2.

- Для получения доступа ввести логин/пароль сервера:

root/radius

- Конфигурационный файл radiusd.conf находится в директории /etc/raddb
- Для просмотра файла следует воспользоваться утилитой mc (midnight commander), для запуска которой через консоль ввести команду ***mc***
- Проверить соответствие конфигурационного файл примеру, представленному ниже.

```
listen {
# IP адрес, с которого могут прийти обращения.
# Возможные значения:
#  Обычная форма записи ip адреса (1.2.3.4)
#  Имя узла     (radius.example.com)
#  Любой  (*) ipaddr = *

# ЛИБО можно использовать IPv6 адрес, НО НЕ ОДНОВРЕМЕННО
#ipv6addr = :: # any. ::1 == localhost

# Порт, на который могут прийти обращения
# Возможные значения:
#  число (1812)
#  0 означает "использовать /etc/services для определения порта"
port = 0
# Наименование сетевого интерфейса, если их несколько
# узнать имеющиеся интерфейсы можно командой ifconfig interface
= eth0
```

3. Отредактировать конфигурационный файл clients.conf

Внимание: редактирование файла должно осуществляться бригадами по очереди. Не допускается одновременное редактирование с двух рабочих мест. Порядок работы бригад определяется преподавателем в процессе выполнения практической работы.

- Редактирование файла осуществляется по SSH протоколу при помощи утилиты PuTTY. Если настоящий пункт выполняется сразу за предыдущим, то соединение уже установлено и его перезапуск не требуется.
- При помощи утилиты **mc** открыть на редактирование (клавиша F4) конфигурационный файл **clients.conf** по пути /etc/raddb/clients.conf

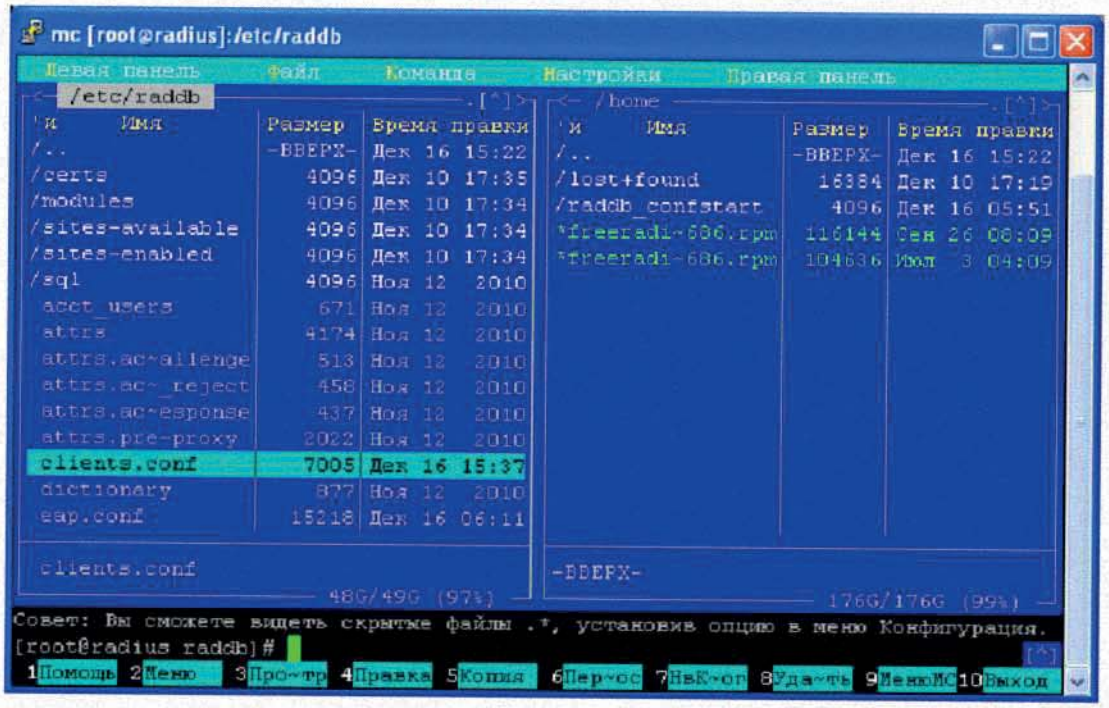


Рис.4.3.

- Этот файл содержит данные о беспроводных точках доступа, которые работают с данным RADIUS-сервером. Добавить новую точку доступа, дописав в конец файла следующий блок:

```
client 192.168.1.10 {
ipaddr = 192.168.1.10 secret = password1 shortname = AP1
}
```

192.168.1.10 – IP адрес точки доступа, работающей в связке с RADIUS сервером в примере. Заменить на ip адрес в соответствии с указаниями к заданию.

password 1– кодовое слово, известное точке доступа и RADIUS серверу. Вводится при настройке точки доступа.

AP1 – название точки доступа. Может быть любым.

Табл.4.3.

Бригада	1	2	3
Название точки доступа	AP1	AP2	AP3
IP-адрес точки доступа	192.168.1.10	192.168.1.20	192.168.1.30
Пароль	password1	password2	password3

- Сохранить внесенные изменения.

4. Отредактировать файл eap.conf

- Редактирование файла осуществляется по SSH протоколу при помощи утилиты PuTTY. Если настоящий пункт выполняется сразу за предыдущим, то соединение уже установлено и его перезапуск не требуется.

- При помощи утилиты **mc** открыть на редактирование (клавиша F4) конфигурационный файл **eap.conf** по пути */etc/raddb/eap.conf* и внести следующие изменения в файл:

В секции eap {} найти строчку «default_eap_type» и установить протокол peap по умолчанию, если изначально был другой протокол. Строчка должна выглядеть так: **default_eap_type = peap**

- Повторить предыдущий пункт с секцией tls {}, отвечающей за EAP-TLS. После редактирования этот блок должен иметь вид:

```
tls {
private_key_password = whatever private_key_file =
${raddbdir}/certs/cert-srv.pem certificate_file =
${raddbdir}/certs/cert-srv.pem CA_file =
${raddbdir}/certs/demoCA/cacert.pem dh_file = ${raddbdir}/certs/dh
random_file = ${raddbdir}/certs/random
```

- Активировать, если требуется, секцию peap {}, раскомментировав ее строчки. Строчка считается закомментированной (программа ее не учитывает), если перед ней стоит знак #, т.е. секция peap {} должна выглядеть следующим образом:

```
peap{
default_eap_type = mschapv2
}
```

Сохранить внесенные изменения.

5. Конфигурирование базы пользователей

Внимание: Выполнение данного пункта осуществляется бригадами по очереди. Не допускается одновременное редактирование файла users с двух рабочих мест. Порядок работы бригад определяется преподавателем в процессе выполнения практической работы.

- Пользовательская база конфигурируется изменением файла **users**. Редактирование файла осуществляется по SSH протоколу при

помощи утилиты PuTTY. Если настоящий пункт выполняется сразу за предыдущим, то соединение уже установлено и его перезапуск не требуется.

- При помощи утилиты **mc** открыть на редактирование (клавиша F4) конфигурационный файл **users** по пути */etc/raddb/users*
- Добавить нового пользователя, выбрав имя пользователя и пароль доступа в соответствии с заданием в зависимости от номера рабочего места.

Табл.4.4.

Рабочее место	IP-адрес пользователя	Имя пользователя	Пароль
1	192.168.1.11	lab01	lab01
2	192.168.1.12	lab02	lab02
3	192.168.1.21	lab03	lab03
4	192.168.1.22	lab04	lab04
5	192.168.1.31	lab05	lab05
6	192.168.1.32	lab06	lab06

Для того, чтобы добавить нового пользователя требуется в конце файла вставить строчку:

```
login Cleartext-Password := "password"
```

Пример: для рабочего места №2 строчка будет иметь вид:

```
lab02 Cleartext-Password := " lab02"
```

6. После редактирования всех конфигурационных файлов и сохранения изменений, необходимо перезапустить сервер.

- Запустить новое окно терминала PuTTY, подключиться к RADIUS-серверу, используя настройки аналогичные п.2 данной практической работы.
- Текущий пункт выполняется только одной бригадой. Исполнители выбираются преподавателем во время проведения практической работы.
- Для определения номера процесса **radius** выполнить команду ***ps***–*A*. В результате будет выведен список всех запущенных процессов с указанием их номеров (PID).

- Для погашения процесса ввести команду ***kill <PID>***, где <PID> - номер процесса **radiusd**.

Внимание! При выполнении команды kill необходимо быть крайне внимательным.

- Перейти в папку init.d, для этого ввести команду **cd** с указанием пути:

```
cd /etc /init.d
```

- Для запуска процесса выполнить команду: ***radiusd –X***

В случае успешного выполнения команды будет выведено сообщение «**Ready to process requests.**»

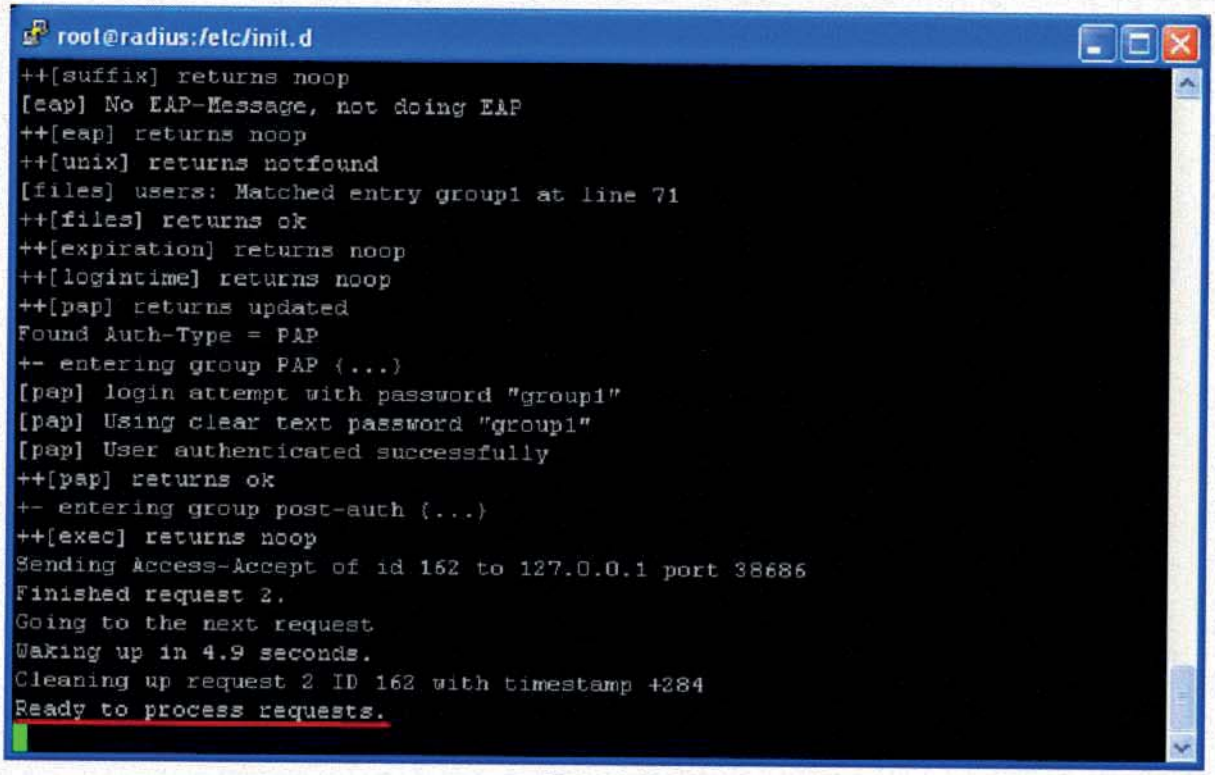


Рис.4.4.

7. Проверка работоспособности RADIUS-сервера.

Проверка работы RADIUS-сервера осуществляется при помощи установленной утилиты radtest. Для этого:

- Для удобства работы запустить новое окно терминала PuTTY, подключиться к RADIUS-серверу, используя настройки аналогичные п.2 данной практической работы.
- Перейти в директорию *bin*, выполнив команду ***cd /usr/bin***
- Выполнить команду: ***radtest lab01 lab01 localhost 0 testing123***

Где **lab01/lab01** – имя пользователя и пароль в зависимости от номера

бригады.

Табл.4.5.

Рабочее место	IP-адрес пользователя	Имя пользователя	Пароль
1	192.168.1.11	lab01	lab01
2	192.168.1.12	lab02	lab02
3	192.168.1.21	lab03	lab03
4	192.168.1.22	lab04	lab04
5	192.168.1.31	lab05	lab05
6	192.168.1.32	lab06	lab06

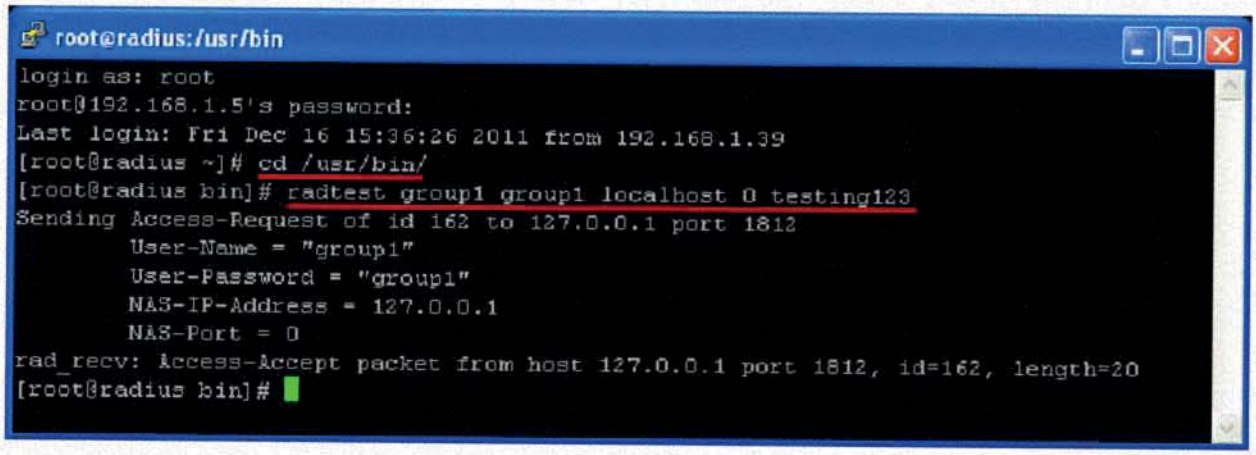


Рис.4.5.

Наличие строчки Access-Accept говорит о корректной работе RADIUS- сервера.

Примечание: на рисунке выше в качестве имени пользователя и пароля заданы group1/group1

- Закрыть дополнительное окно терминала.

Внимание! «Грубое» выключение RADIUS-сервера из сети может привести к его поломке. Для корректного выключения необходимо выполнить следующие операции в терминале RADIUS-сервера:

- Определить номер (PID) процесса RADIUS-сервера выполнением команды:

```
ps -A |grep radiusd
```

- Остановить процесс при помощи команды ***kill <PID>***, где

<PID> - номер процесса.

- Чтобы убедиться, что процесс остановлен, повторно ввести команду ***ps –A***. В списке должен отсутствовать процесс **radiusd**.
- Ввести команду выключения сервера ***poweroff***

Содержание отчета

- Структурная схема исследуемой сети с указанием IP адресов точек доступа, рабочих станций и RADIUS-сервера.
- Алгоритм и последовательность настройки RADIUS-сервера.

Рекомендуемая литература

1. RFC 792 Internet control message protocol. September, 1981.
2. RFC 950 Internet Standard Subnetting Procedure. August 1985
3. RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. March, 2006
4. RFC 2925 Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations. September, 2000.
5. Олифер Н. А., Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. Издание 4-е. Питер, 2010.

Приложение А
СИГНАЛЬНЫЙ ПРОТОКОЛ SIP. ТРАНСПОРТНЫЙ RTP-ПРОТОКОЛ. ОЦЕНКА КАЧЕСТВА ЗВУКА.

SIP

SIP (Session Initiation Protocol) – протокол инициализации сессии.

В первоначальной версии протокола (*RFC 3261*) было определено шесть типов запросов. С помощью запросов клиент сообщает о текущем местоположении, приглашает пользователей принять участие в сеансах связи, модифицирует уже установленные сеансы, завершает их и т. д.

Тип запроса указывается в стартовой строке.

- **INVITE** – Приглашает пользователя к сеансу связи. Обычно содержит SDP-описание сеанса.
- **ACK** – Подтверждает приём ответа на запрос **INVITE**.
- **BYE** – Завершает сеанс связи. Может быть передан любой из сторон, участвующих в сеансе
- **CANCEL** – Отменяет обработку ранее переданных запросов, но не влияет на запросы, которые уже закончили обрабатываться.
- **REGISTER** – Переносит адресную информацию для регистрации пользователя на сервере определения местоположения.
- **OPTIONS** – Запрашивает информацию о функциональных возможностях терминала.

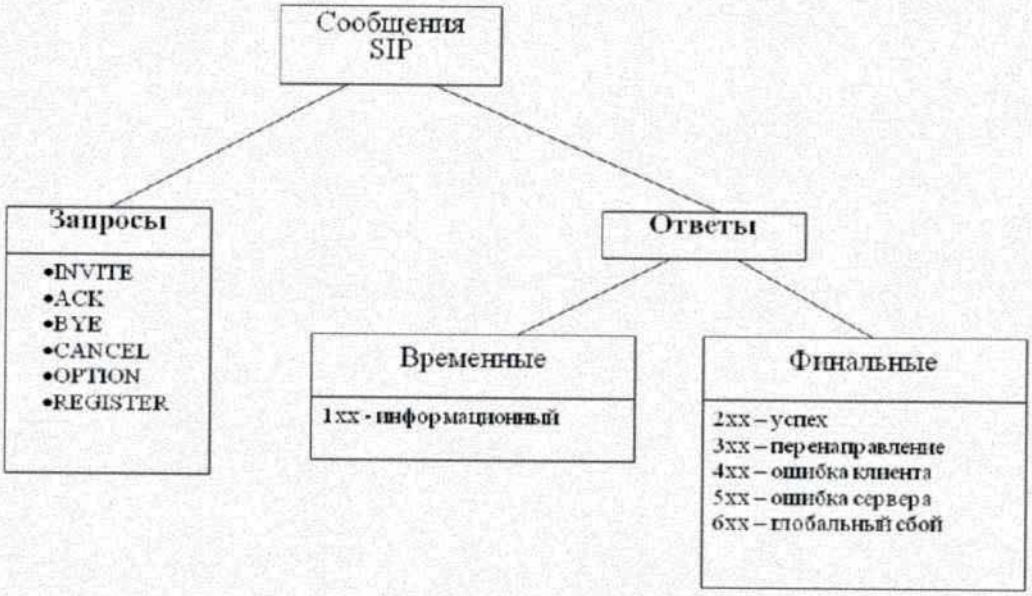


Рис.А.1.

Стоит отметить, что протокол SIP использует текстовый формат сообщений, подобно протоколу HTTP. Это облегчает синтаксический анализ и генерацию кода, позволяет реализовать протокол на базе любого языка программирования, облегчает эксплуатационное управление, облегчает анализ сообщений.

Изучение основных возможностей сетевого анализатора. Анализ RTP-сессии.

После нахождения участников соединения и установления самого соединения (при помощи протокола SIP или H.323) начинается потоковая передача голосовых пакетов. Для обеспечения естественного звучания разговора без эха и задержек голосовые пакеты должны передаваться по IP-сети в режиме реального времени. Все стандарты VoIP для потоковой передачи голосовых пакетов в реальном времени используют протокол RTP (Real-time Transport Protocol).

RTP не использует протокол TCP для передачи голосовых пакетов.

Несмотря на то, что TCP гарантирует доставку пакетов, время установления сессии и задержки совершенно неприемлемы для передачи мультимедийных данных в режиме реального времени.

В каждом голосовом пакете RTP содержится дополнительная информация, включая идентификацию полезной нагрузки (payload type) для определения типа передаваемых данных, порядковые номера для обнаружения и идентификации потерянных пакетов и временные отметки для синхронизации и расчета джиттера (флуктуации времени задержки).

Информация о существующих RTP-потоках в CommView for WiFi отображается во вкладке *VoIP/потоки RTP*, на которой приведен анализ существующих VoIP-сессий.

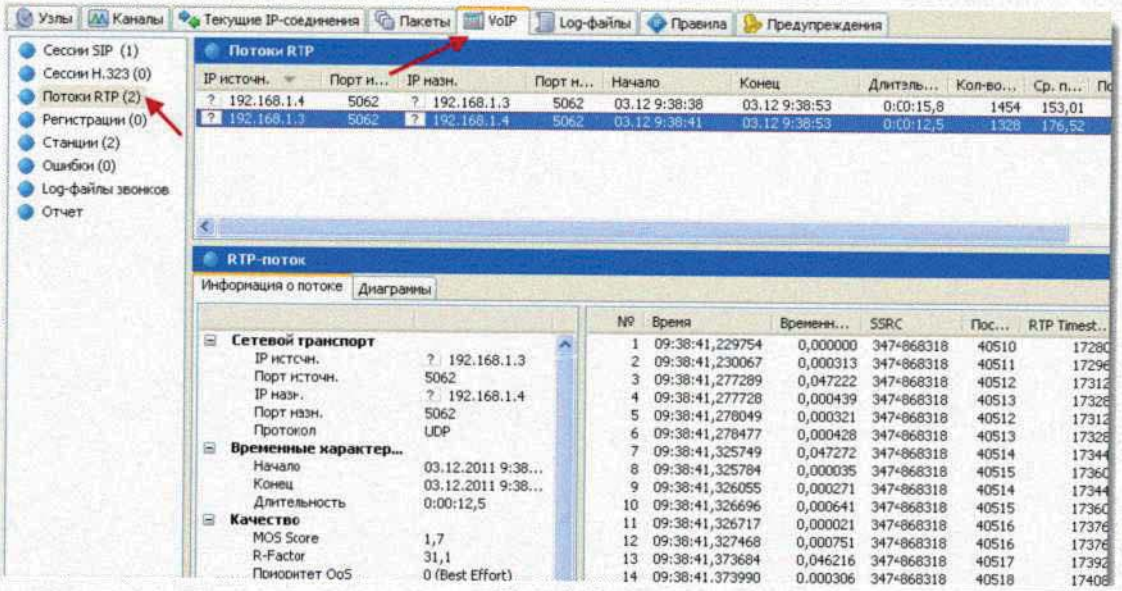


Рис.А.2.

Возможность просмотра детальной информации о текущих звонках позволяет идентифицировать и решить проблемы со связью на сетевом и протокольном уровнях. В детализацию RTP-сессии входят IP-адреса источника и точки назначения, время начала и окончания разговора, длительность разговора, статус звонка, показатели качества, названия VoIP-устройств пользователей, а также дополнительные данные, зависящие от используемого протокола.

Оценка качества звука

Для количественной оценки качества VoIP-переговоров была введена шкала MOS – усредненная оценка разборчивости речи (Mean Opinion Score). MOS включает в себя показатель воспринимаемого качества звука по балльной шкале от 1 до 5.

Изначально MOS представлял собой среднее арифметическое всех оценок качества, данных людьми, которые прослушивали тестовый звонок и давали ему свою оценку. На сегодняшний день для оценки качества звукового потока человеческого участия не требуется.

Современный инструментарий оценки качества VoIP включает в себя искусственные программные модели для расчета MOS.

R-Factor является альтернативным способом оценки качества звука.

Балльная шкала от 0 до 120 в отличие от сокращенной шкалы MOS

(1-5) позволяет делать более точную оценку показателя качества. R-Factor рассчитывается с учетом ощущений пользователя и объективных факторов, которые влияют на общее качество VoIP-системы.

Приложение Б
RADIUS

RADIUS (англ. Remote Authentication in Dial-In User Service) — протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах, разработанный для передачи сведений между центральной платформой и оборудованием.

RADIUS-протокол предназначен для работы в связке с сервером аутентификации, в качестве которого обычно выступает RADIUS-сервер. В этом случае беспроводные точки доступа работают в enterprise-режиме. Если сети отсутствует RADIUS-сервер, то роль сервера аутентификации выполняет сама точка доступа. Этот режим называется WPA-PSK.

При таком методе защиты применяется единый ключ, известный как на абонентских станциях, так и на точках доступа. Если потребуется запретить доступ к сети какому-либо абоненту, то придется менять PSK ключ на всех точках доступа, и сообщать о его изменении остальным абонентам. Таким образом, режим, когда в качестве сервера аутентификации выступает сама точка доступа, пригоден лишь для сетей с небольшим числом абонентов (например, домашняя сеть).

В режиме WPA-Enterprise точка доступа перестает выполнять функции сервера аутентификации и перекладывает эти полномочия на выделенный RADIUS-сервер. Последний сверяет данные абонента с базой данных пользователей и разрешает или запрещает доступ в сеть. В этом случае регистрационные данные индивидуальны для каждого абонента, что облегчает управление пользователями.

Функции аутентификации возлагаются на протокол EAP, который сам по себе является лишь каркасом для методов аутентификации. Протокол EAP позволяет вести свободный диалог между клиентом удаленного доступа и системой проверки подлинности. Такой диалог состоит из запросов системы проверки подлинности на необходимую ей информацию и ответов клиента удаленного доступа. Например, когда протокол EAP используется с генераторами кодов доступа, сервер, выполняющий проверку подлинности, может отдельно

запрашивать у клиента удаленного доступа имя пользователя, идентификатор и код доступа. После ответа на каждый такой запрос клиент удаленного доступа проходит определенный уровень проверки подлинности. Когда на все запросы будут получены удовлетворительные ответы, проверка подлинности клиента удаленного доступа успешно завершается.

Схемы проверки подлинности, использующие протокол EAP, называются типами EAP. Для успешной проверки подлинности клиент удаленного доступа и сервер, выполняющий проверку подлинности, должны поддерживать один и тот же тип EAP.

Существует множество типов EAP:

- EAP-SIM, EAP-AKA — используются в сетях GSM мобильной связи.
- LEAP — проприетарный метод от Cisco systems
- EAP-MD5 — простейший метод, аналогичный CHAP (не стойкий)
- EAP-MSCHAPv2 — метод аутентификации на основе имени пользователя/пароля пользователя в MS-сетях
- EAP-TLS — аутентификация на основе цифровых сертификатов
- EAP-PEAP

Протокол EAP-TLS (EAP-Transport Level Security) — это тип EAP, применяемый в системах безопасности, использующих сертификаты. Если проверка подлинности при удаленном доступе осуществляется с помощью смарт-карт, необходимо использовать метод проверки подлинности EAP-TLS. Обмен сообщениями EAP-TLS позволяет выполнять взаимную проверку подлинности, согласование метода шифрования и определение зашифрованного ключа между клиентом удаленного доступа и сервером, выполняющим проверку подлинности. EAP-PEAP сам по себе не определяет метод проверки подлинности, однако в нем используется протокол безопасности TLS (Transport Layer Security), создающий зашифрованный канал между клиентом и RADIUS-сервером, тем самым повышая безопасность.

Аутентификация чаще всего происходит по протоколу EAP-MSCHAPv2.

Приложение В

Форма отчета обучающегося о выполненной практической работе

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

Кафедра космического приборостроения и систем связи

ОТЧЁТ

по выполнению практической работы

«Планирование адресного пространства локальной сети»

по дисциплине «Проектирование и эксплуатация инфокоммуникационных систем и сетей»

Выполнил: студент группы ИТ-91б
Иванов М.О.

Проверил: доцент кафедры КПиСС
Севрюков А.Е.

_____ «____»_____2021 г.
(подпись)

Курск 2021

Планирование адресного пространства локальной сети

Целью работы является освоение принципов и методик разделения адресного пространства локальной сети на подсети; получение практических навыков разделения сетей на нужное количество подсетей нужного (различного) размера.

1.1 Индивидуальное задание

1. Сгенерировать индивидуальный IP-адрес и префикс подсети (суперсети).

2. Определить основные параметры заданной подсети:

а) адрес узла в точечно-двоичной нотации;

б) класс сетевого адреса (традиционный);

в) маску подсети (или суперсети, если префикс оказался меньше традиционного для класса) в точечно-десятичной нотации;

г) шаблон для выделения адресов узлов в подсети (в суперсети);

д) количество узлов в подсети (суперсети);

е) IP-адрес подсети (суперсети);

ж) IP-адрес шлюза;

з) IP-адрес первого узла в подсети;

и) IP-адрес последнего узла в подсети;

к) IP-адрес широковещательных сообщений для данной подсети.

3. Используя схему сети предприятия, приведенную на рисунке 1, а также, информацию о количестве компьютеров в отделах предприятия, заданную вариантом (таблица 1), разбить заданную сеть на подсети.

Таблица 1 – Исходные данные сети предприятия

Вариант	Исходная сеть (блок адресов)	Количество компьютеров в отделах		
		А	Б	В
7	126.61.74.0 /23	8	61	17

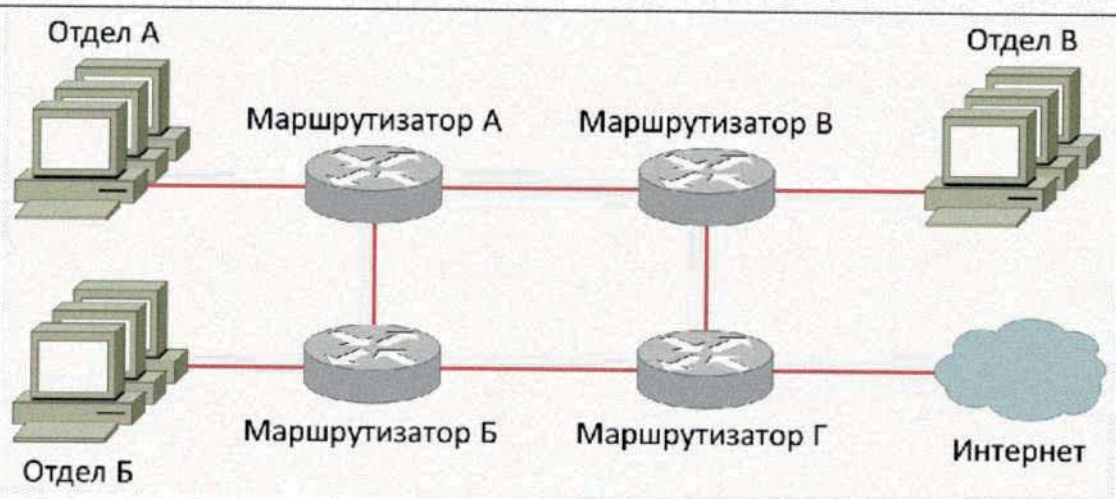


Рисунок 1 – Схема сети предприятия

1.2 Ход работы

.....

Вывод