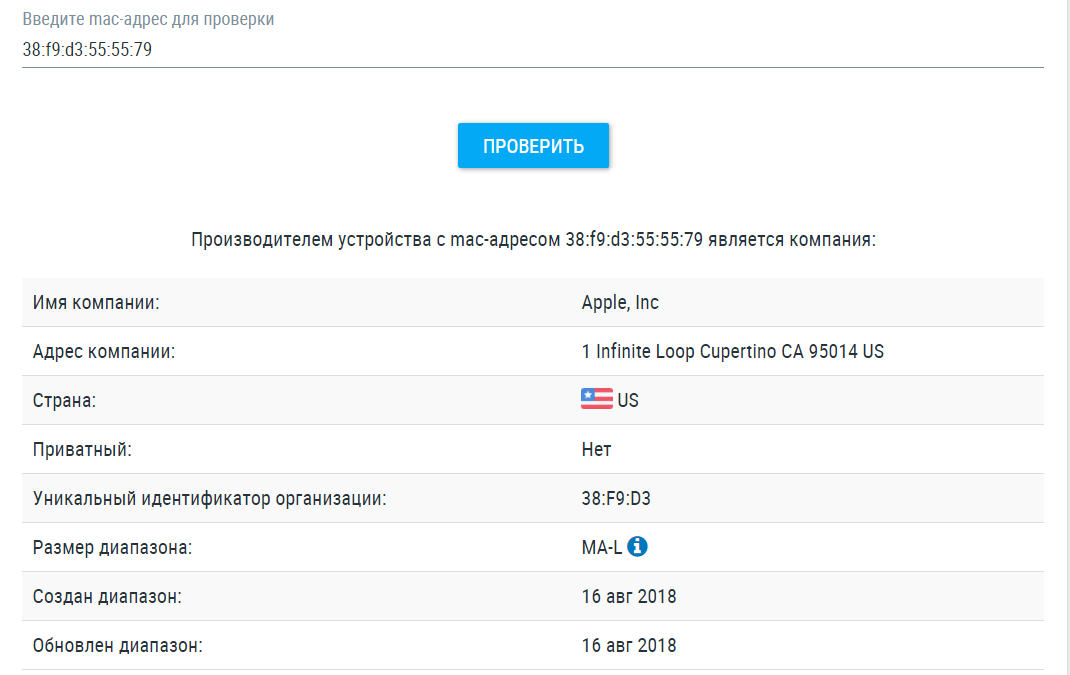
1. Необязательное задание: можно посмотреть целый фильм в консоли telnet towel.blinkenlights.nl :)

2. Узнайте о том, сколько действительно независимых (не пересекающихся) каналов есть в разделяемой среде WiFi при работе на 2.4 ГГц. Стандарты с полосой 5 ГГц более актуальны, но регламенты на 5 ГГц существенно различаются в разных странах, а так же не раз обновлялись. В качестве дополнительного вопроса вне зачета, попробуйте найти актуальный ответ и на этот вопрос.

1 (2,412 ГГц), 6 (2,437 ГГц) и 11 (2,462 ГГц), частоты которых отличаются более чем на 20 МГц

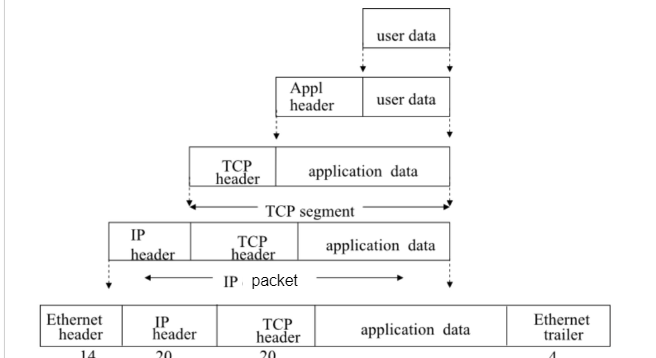
|  |  |  |
| --- | --- | --- |
| **Канал** | **Частота, ГГц** | **Страны** |
| 1 | 2,412 | США, Европа, РФ, Япония |
| 2 | 2,417 | США, Европа, РФ, Япония |
| 3 | 2,422 | США, Европа, РФ, Япония |
| 4 | 2,427 | США, Европа, РФ, Япония |
| 5 | 2,432 | США, Европа, РФ, Япония |
| 6 | 2,437 | США, Европа, РФ, Япония |
| 7 | 2,442 | США, Европа, РФ, Япония |
| 8 | 2,447 | США, Европа, РФ, Япония |
| 9 | 2,452 | США, Европа, РФ, Япония |
| 10 | 2,457 | США, Европа, РФ, Япония |
| 11 | 2,462 | США, Европа, РФ, Япония |
| 12 | 2,468 | Европа, РФ, Япония |
| 13 | 2,472 | Европа, РФ, Япония |
| 14 | 2,484 | Япония |

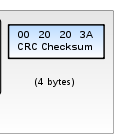
3. Адрес канального уровня – MAC адрес – это 6 байт, первые 3 из которых называются OUI – Organizationally Unique Identifier или уникальный идентификатор организации. Какому производителю принадлежит MAC 38:f9:d3:55:55:79?



4. Каким будет payload TCP сегмента, если Ethernet MTU задан в 9001 байт, размер заголовков IPv4 – 20 байт, а TCP – 32 байта?

Размер payload TCP будет равен 8 927, из расчета что у нас имеется 9001 байт из него мы минусуем IPv4 – 20 байт, TCP – 32 байта, Ethernet header - 14, Ethernet trailer -4 - checksum.





5. Может ли во флагах TCP одновременно быть установлены флаги SYN и FIN при штатном режиме работы сети? Почему да или нет?

Не может быть одновременно установлены флаги SYN и FIN, так как требует установление соединения (SYN) и прекращения соединения (FIN).

6. sort = :53 s -ula sp на хосте имеет следующий вывод:

State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

UNCONN 0 0 127.0.0.53%lo:domain 0.0.0.0:\*

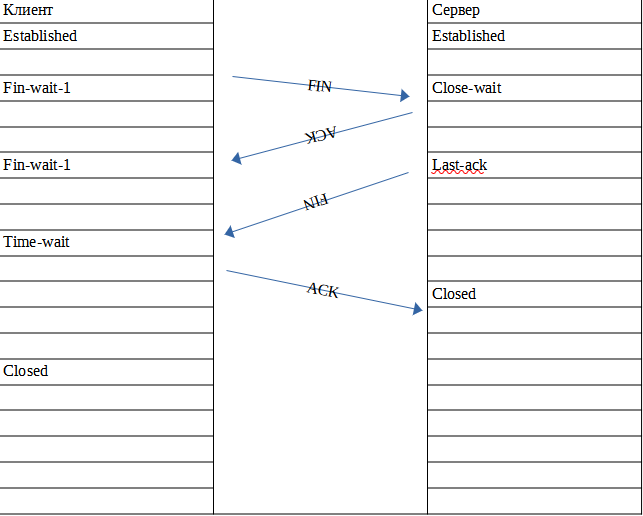
Почему в State присутствует только UNCONN, и может ли там присутствовать, например, TIME-WAIT?

пакет UDP отправляет пакет без установки соединения.

А в выводе ss -ula sport = :53 как раз мы выводим -ula собственно "прослушивания всех udp на 53 порту", 53 порт это порт днс.

У UDP может быть в state LISTEN, UCONN и ESTAB.

7. Обладая знаниями о том, как штатным образом завершается соединение (FIN от инициатора, FIN-ACK от ответчика, ACK от инициатора), опишите в каких состояниях будет находиться TCP соединение в каждый момент времени на клиенте и на сервере при завершении. Схема переходов состояния соединения вам в этом поможет.



8. TCP порт – 16 битное число. Предположим, 2 находящихся в одной сети хоста устанавливают между собой соединения. Каким будет теоретическое максимальное число соединений, ограниченное только лишь параметрами L4, которое параллельно может установить клиент с одного IP адреса к серверу с одним IP адресом? Сколько соединений сможет обслужить сервер от одного клиента? А если клиентов больше одного?

Сервер использует порт, к которому подключен клиент, в качестве порта источника, и поэтому он ограничен только (числом клиентских IP-адресов) \* (числом временных портов клиента) - большим числом.

9. Может ли сложиться ситуация, при которой большое число соединений TCP на хосте находятся в состоянии TIME-WAIT? Если да, то является ли она хорошей или плохой? Подкрепите свой ответ пояснением той или иной оценки.

Да ситуация с состоянием TIME-WAIT может сложиться ситуация с большим количеством состоянии TIME-WAIT. Так как “ Узел-1 получил сегмент с флагом FIN, отправил сегмент с флагом ACK и ждёт 2\*MSL секунд, перед окончательным закрытием соединения”

Разрастание состояния TIME-WAIT ведет к исчерпанию доступных ресурсов “на сервер”. Также может быть ситуация что исчерпаются все порты для подключения к “серверу” - Все порты будет в “TIME-WAIT”, клиент получит ошибку EADDRNOTAVAIL (errno=99).

10. Чем особенно плоха фрагментация UDP относительно фрагментации TCP?

фрагментация UDP плоха тем что фрагментированный пакет может потеряться по дороге, а так как UDP ненадежный информация будет искажена.

11. Если бы вы строили систему удаленного сбора логов, то есть систему, в которой несколько хостов отправляют на центральный узел генерируемые приложениями логи (предположим, что логи – текстовая информация), какой протокол транспортного уровня вы выбрали бы и почему? Проверьте ваше предположение самостоятельно, узнав о стандартном протоколе syslog.

Выбрал бы TCP так как гарантированно информация доходила до системы сбора логов.

Syslog работает ([UDP](https://ru.wikipedia.org/wiki/UDP) или [TCP](https://ru.wikipedia.org/wiki/TCP))

12. Сколько портов TCP находится в состоянии прослушивания на вашей виртуальной машине с Ubuntu, и каким процессам они принадлежат?

root@vagrant:/# ss -utla

Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

udp UNCONN 0 0 127.0.0.1:8125 0.0.0.0:\*

udp UNCONN 0 0 127.0.0.53%lo:domain 0.0.0.0:\*

udp UNCONN 0 0 10.0.2.15%eth0:bootpc 0.0.0.0:\*

udp UNCONN 0 0 0.0.0.0:sunrpc 0.0.0.0:\*

udp UNCONN 0 0 [::1]:8125 [::]:\*

udp UNCONN 0 0 [::]:sunrpc [::]:\*

tcp LISTEN 0 4096 0.0.0.0:19999 0.0.0.0:\*

tcp LISTEN 0 4096 0.0.0.0:sunrpc 0.0.0.0:\*

tcp LISTEN 0 4096 127.0.0.53%lo:domain 0.0.0.0:\*

tcp LISTEN 0 128 0.0.0.0:ssh 0.0.0.0:\*

tcp LISTEN 0 4096 127.0.0.1:8125 0.0.0.0:\*

tcp ESTAB 0 0 10.0.2.15:ssh 10.0.2.2:50064

tcp LISTEN 0 4096 \*:9100 \*:\*

tcp LISTEN 0 4096 [::]:sunrpc [::]:\*

tcp LISTEN 0 128 [::]:ssh [::]:\*

tcp LISTEN 0 4096 [::1]:8125 [::]:\*

9 в LISTEN

В основном ssh

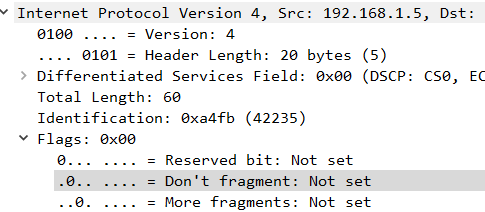
13. Какой ключ нужно добавить в tcpdump, чтобы он начал выводить не только заголовки, но и содержимое фреймов в текстовом виде? А в текстовом и шестнадцатеричном?

в текстовом виде записать “-w”, прочитать из файла “-r”

в текстовом и шестнадцатеричном - “-X” ”-XX”

14. Попробуйте собрать дамп трафика с помощью tcpdump на основном интерфейсе вашей виртуальной машины и посмотреть его через tshark или Wireshark (можно ограничить число пакетов -c 100). Встретились ли вам какие-то установленные флаги Internet Protocol (не флаги TCP, а флаги IP)? Узнайте, какие флаги бывают. Как на самом деле называется стандарт Ethernet, фреймы которого попали в ваш дамп? Можно ли где-то в дампе увидеть OUI?

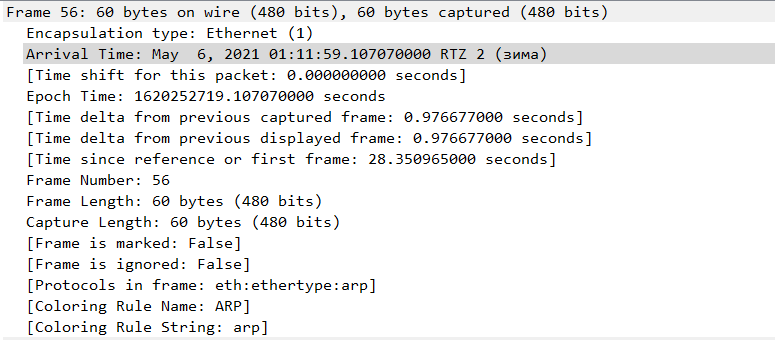
Попробовал собрал))



Только Flags: 0x00

Если под названием стандарт Ethernet имеется в виду выделенный фрагмент:





Вид инкапсуляции

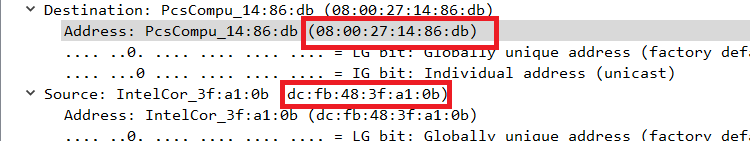
время

Номер фрайма

длина

Протокол фрейма

OUI:



Куда, откуда пришел пакет , собственно по мак адресу мы можем понять что за устройство. производитель)