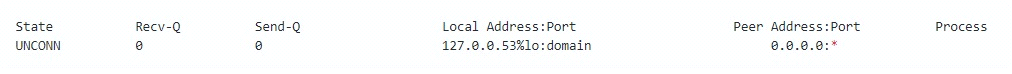
2) Узнайте о том, сколько действительно независимых (не пересекающихся) каналов есть в разделяемой среде WiFi при работе на 2.4 ГГц. Стандарты с полосой 5 ГГц более актуальны, но регламенты на 5 ГГц существенно различаются в разных странах, а так же не раз обновлялись. В качестве дополнительного вопроса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

Ответ: на частоте 2.4 ГГц непересекающийся каналов может быть 4шт. для стран Европы и России. Для США 2,4 ГГц непересекающийся каналов всего 3.  
  
  
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?

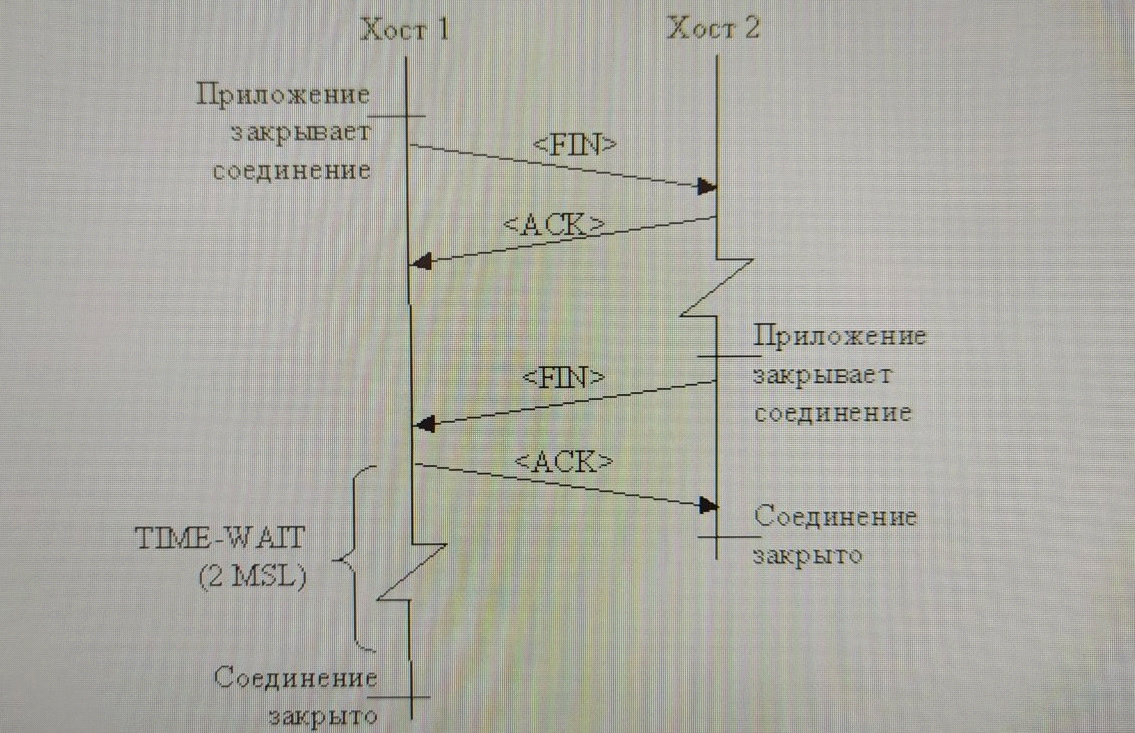
Ответ:  
данный mac address принадлежит компании Apple

4) Каким будет payload TCP сегмента, если Ethernet MTU задан в 9001 байт, размер заголовков IPv4 – 20 байт, а TCP – 32 байта?  
  
Ответ: syn и fin не могут работать одновременно, т.к. syn это установка соединения а fin это разрыв соедниния  
  
5) Может ли во флагах TCP одновременно быть установлены флаги SYN и FIN при штатном режиме работы сети? Почему да или нет?  
  
Ответ: При нормальном поведении TCP они никогда не должны быть установлены в 1 (вкл) в одном пакете. Существует [множество инструментов, позволяющих создавать TCP-пакеты](http://sectools.org/tag/packet-crafters/), но это нарушение стандартов и при выходе во в нешнюю сеть могут возникнуть проблемы.  
  
6)ss -ula sport = :53 на хосте имеет следующий вывод:



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

Ответ:   
ss- это инструмент, используемый для вывода сетевой статистики в виде, похожем на тот, который выдаёт команда netstat, более подробные сведения о TCP-подключениях и о состояниях соединений, чем большинство других инструментов.

Да, должен присутствовать TIME-WAIT, т.к.   
  


Состояние TIME-WAIT служит двум целям:

-не дать соединению пропасть при потере последнего ACK, присланного активной стороной, в результате чего другая сторона посылает fin.

-дать время исчезнуть "заблудившимся сегментам" принадлежавшим этому соединению

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.  
  
Ответ: см. скриншот Вопрос 7 Домашнее задание к занятию 3.6. Компьютерные сети, лекция 1.jpg

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?

Ответ: зависит от типа сетей, далее класс IP

А = 256 в третьей степени > 16,5 млн. хостов пример 255.0 .0 .0

B = 256 в квадрате чуть более 65тыч. хостов пример 255.255.0 .0

С = 256 - 4 (т.к. 2 хоста и 1 номер сети и 1 адрес широковещательной рассылки) = 252 пример 255.255.255.0

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.

Ответ: TIME\_WAIT - это нормально. Это состояние после закрытия сокета, используемое ядром для отслеживания пакетов, которые могли быть потеряны и поздно явились на сторону. Большое количество подключений TIME\_WAIT - это симптом получения большого количества недолговечных подключений, не о чем беспокоиться.

10) Чем особенно плоха фрагментация UDP относительно фрагментации TCP?

Ответ: TCP имеет высокую надежность, поскольку позволяет не терять данные при передаче, запрашивает подтверждения о получении от принимающей стороны и в случае необходимости отправляет данные повторно. При этом отправляемые пакеты данных сохраняют порядок отправки, то есть можно сказать, что передача данных упорядочена. Минусом данного протокола является относительно низкая скорость передачи данных, за счет того что выполнение надежной и упорядоченной передачи занимает больше времени, чем в альтернативном протоколе UDP.  
  
TCP   
+надежный (запрашивает подтверждение о получении от принимающей стороны данные)

+ сохраняет порядок отправки

- низкая скорость передачи данных (занимает больше времени чем UDP

UDP

+ простой (необязательно устанавливать соединение между отправителем и получателем)

+ быстрый (по сравнениню с TCP)

- менее надежный (при передаче некоторые фрагменты данных могут теряться).

- не соблюдается упорядоченность данных, возможен не последовательный прием данных получателем.

11) Если бы вы строили систему удаленного сбора логов, то есть систему, в которой несколько хостов отправяют 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.

Ответ: протокол IP, важно записать все данные, в правильном порядке.  
  
12) Сколько портов TCP находится в состоянии прослушивания на вашей виртуальной машине с Ubuntu, и каким процессам они принадлежат?

ss -утилита для вывода статистики сокета в формате netstat.

ss -l или --listening - посмотреть только прослушиваемые порты;

sudo ss -tulpn выведет все порты, а так же процессы используемые на каждом порте.

sudo ss -tulpn | grep :80 выведет все процессы по 80 порту.

sudo lsof -i -P # где lsof утилита которая позволяет посмотреть открытые в системе соединения, где флаг -i показывает сетевые соединения, флаг -p отобразит именно порты.

sudo lsof -i :80, где мы увидим какие процессы прослушивают 80ый порт.

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 шестнадцатиричном?

Ответ:  
tcpdump -XX

-x Делает распечатку пакета в шестнадцатеричной системе, полезно для более детального анализа пакета. Количество отображаемых данных зависит от параметра -s

-xx плюс содержимое Ethernet-фрейма.

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?

14.1 ) Встретились ли вам какие-то установленные флаги Internet Protocol (не флаги TCP, а флаги IP)?

Ответ: см. скрин: “14 вопрос флаги Домашнее задание к занятию 3.6. Компьютерные сети, лекция 1.jpg”

14.2 ) Узнайте, какие флаги бывают

Ответ:

Флаги

Поле Flags используется для управления тем, как конкретный IP-пакет обрабатывается устройством. Поле состоит из 3 бита и имеет следующий формат:

Первый бит всегда равен 0

Второй бит указывает, можно ли фрагментировать пакет (не фрагментировать [md] DF) или разбить на несколько частей.

Значение 0 означает, что пакет может быть фрагментирован.

Значение 1 означает, что пакет НЕ может быть фрагментирован.

Третий бит представляет «местоположение» пакета в серии фрагментированных пакетов.

Значение 0 означает, что пакет является последним фрагментом в серии ИЛИ пакет, который совсем не фрагментирован.

Значение 1 означает, что пакет не является последним фрагментом в серии и следует ожидать большего количества фрагментов.

14.3 Как на самом деле называется стандарт Ethernet, фреймы которого попали в ваш дамп?

IEEE 802.3 назывался по старому  
Ethernet-II по новому.

14.4 Можно ли где-то в дампе увидеть OUI?

как мы знаем: Destenation IP адрес получателя подчеркнутый красным (сверху)

Ловил пакеты в wireshark на Worldofwarcraft.com (1 слайд) где нашел мак адрес графу Destenation

См. скрин : “14 вопрос wireshark Домашнее задание к занятию 3.6. Компьютерные сети, лекция 1.jpg”

я должен вотнкнуть на сайт

<https://www.wireshark.org/tools/oui-lookup.html>

смотри скрин:  
“14 вопрос Сайт для получения индификации Домашнее задание к занятию 3.6. Компьютерные сети, лекция 1.jpg”