**Packet Tracer - Исследование сетевой безопасности - Режим симуляции физического оборудования**

**Задачи**

**Часть 1. Знакомство с сетью**

**Часть 2. Осуществление мер безопасности**

**Общие сведения и сценарий**

В этом задании в режиме симуляции физического оборудования (PTPM) вы будете изучать и внедрять несколько процедур безопасности в разных местах в городе Гринвилл, штат Северная Каролина. Включая сети в центре обработки данных, интернет-провайдера, кафе и дома.

Центр обработки данных подготовлен для обеспечения экологической и физической безопасности. Существует также программное обеспечение, которое включено для поддержания контроля доступа. Вы установите детектор дыма Интернета вещей (IoT).

Кофейня предлагает своим посетителям бесплатный беспроводной доступ в Интернет. Вы будете реализовывать VPN для защиты трафика.

Дом включает в себя офис, студенческую спальню и гостиную. Вы настроите две домашние беспроводные локальные сети (WLAN), чтобы требовать аутентификации для двух разных типов пользователей: членов семьи и гостей. Эти сети также будут настроены с фильтрацией MAC-адресов для ограничения доступа.

**Примечание**: Это задание не оценивается. Тем не менее, вы будете использовать различные методы для проверки конфигураций, которые вы реализуете.

**Инструкции**

**Часть 1. Знакомство с Сетью**

В этой части вы изучите сети в центре обработки данных, поставщике услуг Интернета, кафе и дома.

**Шаг 1. Исследуйте Гринвилл.**

Задание начинается с Северной Каролины, США. Все задачи в этого упражнения происходят в Гринвилле. Нажмите Greenville, чтобы войти в вид города. Есть четыре места для изучения: Data Center, ISP, Home и Coffee Shop.

**Шаг 2. Ознакомьтесь с залами в центре обработки данных.**

a.     Есть два зала и различные устройства для изучения, включая серверную комнату, POP, сервер IoT, две точки доступа, ноутбук и несколько устройств IoT, подключенных к сети.

b.     Нажмите на Data Center Server Room. Обратите внимание, что большинство устройств являются серверами. В реальном дата-центре будут сотни стоек, заполненных серверами. Коммутаторы связывают серверы вместе избыточными подключениями. Маршрутизатор обеспечивает подключение к POP, который затем подключается к поставщику услуг Интернета.

Как называется маршрутизатор, который находится в этой стойке? ??????

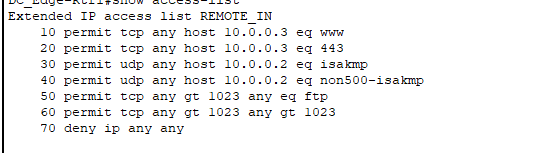
c.     Перейдите на один уровень вверх к Data Center.

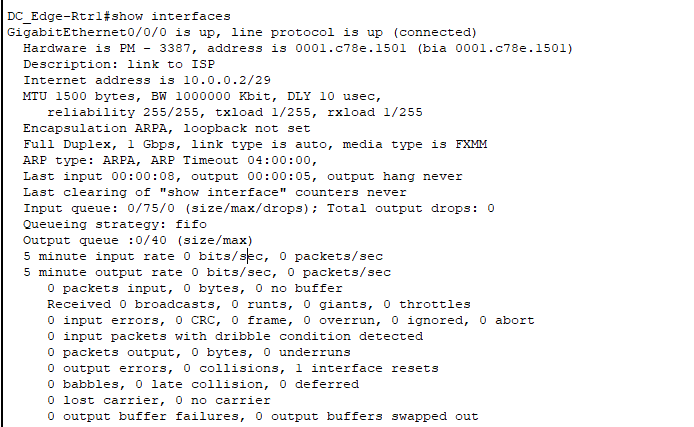
**Шаг 3. Исследуйте устройства в Data Center POP.**

a.     Нажмите на **Data Center POP**. Какой тип кабеля используется для подключения DC\_Edge-RTR1 к поставщику услуг Интернета? Оптоволокно

a.     Какое устройство выполняет преобразование адресов частных дата-центров в публичные? Router

b.     Выберите DC\_Edge-rtr1 > CLI. Используйте команду show access-lists, чтобы просмотреть список контроля доступа. Этот список доступа разрешает только определенный трафик в центр обработки данных. В этом задании разрешен трафик HTTP, HTTPS, IPSec и FTP. Весь прочий трафик блокируется.



c.     Исследуйте интерфейсы. На каком интерфейсе и в каком направлении применяется этот список доступа? 

G0/0/0

**Примечание.**Команды access-list в этой симуляции ограничены. На реальном пограничном маршрутизаторе списки доступа будут гораздо более сложными и еще более ограничительными для защиты всех сетевых устройств и данных в Data Center.

**Шаг 4. Изучите устройства IoT, настроенные для подключения к серверу DC IoT Server.**

a.     Перейдите в центр обработки данных. В зале Data Center POP нажмите на ноутбук на столе, а затем Desktop > Web Browser.

a.     Введите IP-адрес 172.31.0.2, который является DC IoT Server.

b.     В качестве имени пользователя и пароля введите admin и ciscorococks.



Вход на сайт не работает. В работе указан неверный пароль

c.     Какие устройства в настоящее время используются для защиты сетевого оборудования в центре обработки данных от факторов окружающей среды и физической безопасности?

d.     В списке устройств Интернета вещей щелкните Humidity Monitor, чтобы развернуть его. Каков текущий уровень влажности?

**Шаг 5. Исследуйте контролируемую дверь и сирену.**

a.     В списке устройств Интернета вещей щелкните Door, чтобы развернуть его. Обратите внимание, что индикатор Open имеет красный цвет. Это означает, что дверь закрыта.

a.     В списке устройств Интернета вещей щелкните Siren. Обратите внимание, что индикатор On имеет красный цвет. Это означает, что сирена не включена.

b.     Держите окно Web Browser открытым и найдите сирену Siren рядом с дверью Door в Data Center POP.

c.     Чтобы открыть дверь Door, нажмите на Unlock в списке устройств IoT, удерживая ALT и левой кнопкой миши дверь Door. Когда дверь Door открывается, сирена становится красной.

d.     В окне Web Browser индикатор Open стал зеленым, что означает, что дверь открыта. Индикатор сирена Siren в состоянии On, он также зеленый, что означает, что сирена Siren отключена. Снова закройте дверь Door, удерживая нажатой клавишу ALT и щелкнув левой кнопкой мыши на дверьDoor.

e.     В окне Web Browser в группе Door, нажмите Lock. Попробуйте снова открыть дверь, удерживая клавишу ALT и нажав левой кнопкой мыши на дверь Door. Дверь Door не должна открываться.

**Шаг 6. Исследуйте термостат.**

a.     В списке устройств Интернета вещей щелкните Thermostat, чтобы развернуть доступные функции и переменные. При какой температуре будет включаться кондиционер?

a.     В Data Center, нажмите на Thermostat > Config и затем на интерфейс Wireless0 в разделе INTERFACE. Каков IP-адрес для термостата Thermostat?

b.     При необходимости на DC\_Laptop закройте Web Browser. Выберите Command Prompt и выполните эхо-запрос до Thermostat. Ping должен пройти успешно.

**Шаг 7. Изучите сети ISP, Coffee Shop иHome.**

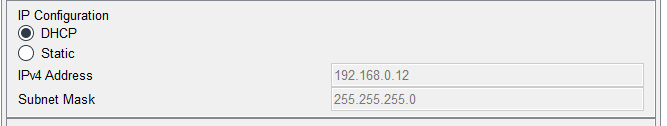
a.     Перейдите к ISP. Интернет-провайдер содержит два маршрутизатора, DNS-сервер и маршрутизатор Central Office, который подключает сеть Coffe Shop и Home к Интернету.

a.     Перейдите к Coffee Shop. Как клиенты подключаются к сети Coffee Shop? Через AP

b.     Какой тип среды используется для подключения кафе к Интернету? Беспроводной

c.     Какие устройства используются для создания сети Coffee Shop ? Нажмите на Wiring Cabinet, чтобы просмотреть дополнительные устройства. AP, ROUTER, WLC, MODEM

d.     Нажмите на каждый ноутбук в Coffee Shop. Откройте вкладку Config (Конфигурация) и щелкните интерфейс Wireless0 в разделе INTERFACE. Какие IP-адреса у них?



e.     Перейдите к сети Home. Вы настроили сеть позже в этом задании. Исследуйте устройства в сети. Как Home подключается к ISP? По коаксиальному кабелю

f.       HomeISPКакие устройства требуют подключения внутри дома? 2 ноутбука 2 пк

**Часть 2. Реализация мер по обеспечению безопасности**

В этой части вы настраиваете безопасность беспроводной сети для детектора дыма в Data Center, виртуальной частной сети (VPN) в Coffee Shopи двух беспроводных сетей в Home.

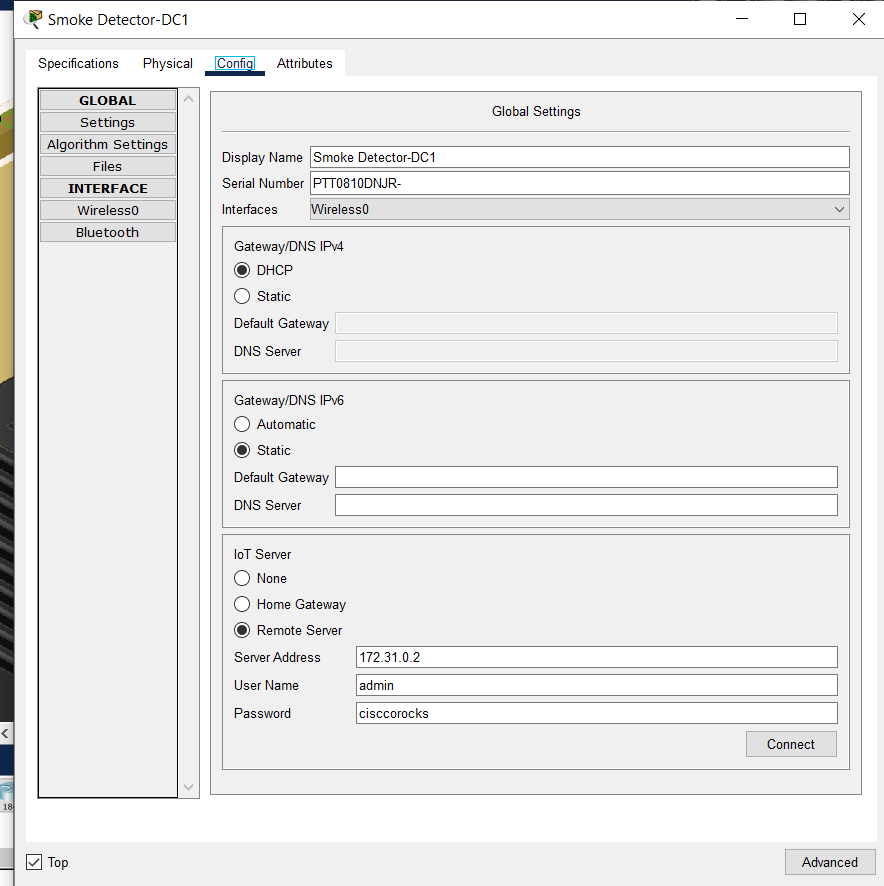
**Шаг 1. Настройте детектор дыма IoT в Data Center.**

a.     Вернитесь в Data Center. Нажмитен на Smoke Detector на стене в Data Center Server Room, а затем перейдите на вкладку Config. Выполните следующие настройки:

1)     Измените Display Name на Smoke Detector-DC1.

2)     В разделе Gateway/DNS IPv4 включите DHCP.

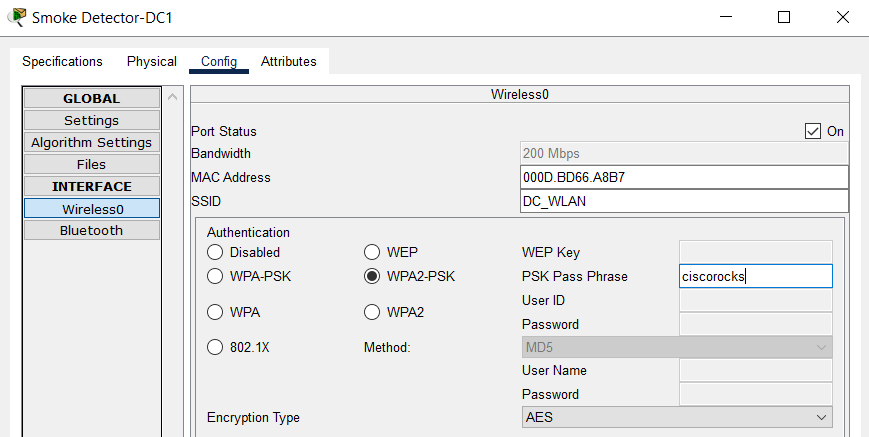
3)     В разделе IoT Server измените IP адрес Remote Server на 172.31.0.2. Имя пользователя — admin, пароль — cisccorocks.



a.     Нажмитен на Wireless0 в разделе INTERFACE и выполните следующие настрйоки:

1)     Измените SSID на DC\_WLAN.

2)     Измените тип аутентификации на WPA2-PSK и в поле PSK Pass Phrase (Кодовая фраза PSK) введите ciscorocks.



3)     Вернитесь в раздел Settings. В разделе IoT Server нажмите на Connect. Сервер регистрации обновит шлюз по умолчанию и IP-адрес детектора дыма через DHCP.

Примечание: Кнопка Connect изменится на Refresh после успешного подключения.

b.     Нажмитен на Smoke Detector-DC1, а затем нажмите на ноутбук в Data Center POP. Если вы ранее закрывали веб-браузер, откройте его снова и авторизуйтесь на сервере IoT-Server по адресу 172.3.1.0.2, используя имя пользователя admin и пароль ciscorocks.

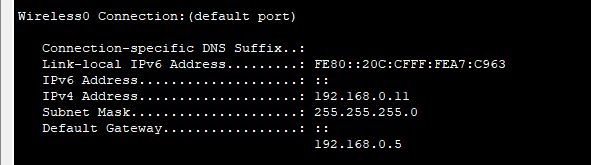
c.     Обратите внимание, что Smoke Detector-DC1 теперь добавлен в список устройств IoT. Нажмите на Smoke Detector-DC1 в веб-браузере. Индикатор Alarm должен быть красным, что означает, что сигнал тревоги не активирован.

**Шаг 2. Создайте VPN на ноутбуке в Coffee Shop для защиты трафика.**

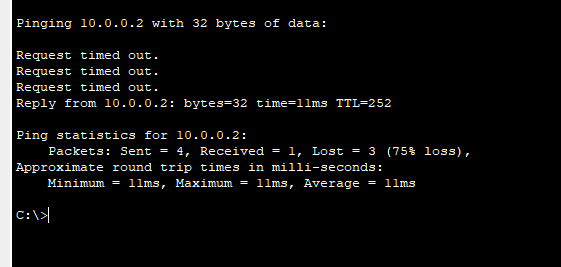
Бесплатный Wi-Fi в таких предприятиях, как кафе, обычно «открыт», что означает отсутствие конфиденциальности и возможность легко захватить трафик. Чтобы избежать этой проблемы, вы будете использовать VPN-клиент на одном из ноутбуков для подключения к FTP-серверу в центре обработки данных. Туннель, созданный VPN, будет шифровать любые данные, передаваемые между ноутбуком и сервером. Пограничный маршрутизатор в центре обработки данных уже настроен для VPN.

a.     Перейдите в Coffee Shopи выберите VPN-laptop.

b.     Нажмите на Desktop > Command Prompt и введите командуipconfig. Какой IP-адрес, назначенный этому ноутбуку?



1. Чтобы ускорить сходимость в Packet Tracer, запустите эхо-запрос до VPN-сервера, который подключен к DC\_Edge-RTR1 с адресом 10.0.0.2.



b.     Закройте окно Command Prompt и нажмите на VPN. Выполните следующие настройки:

GroupName: REMOTE

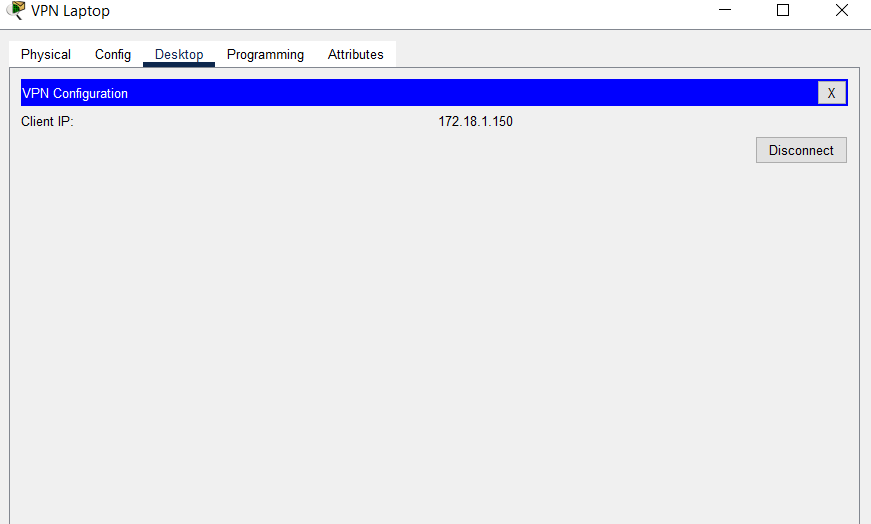
Group Key: CISCO

Host IP (Server IP): 10.0.0.2

Username: VPN

Password: ciscorocks

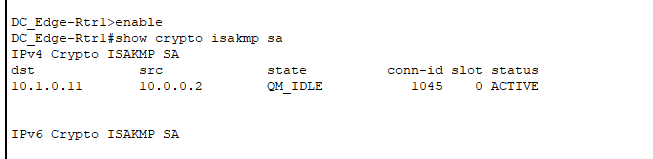
1. Нажмите кнопку Connect. Нажмите кнопку ОК на сообщении VPN is connected. Если у вас возникли проблемы, убедитесь, что конфигурация верна и что ранее вы успешно выполнили эхо-запрос до 10.0.0.2. В окне VPN Configuration можно увидеть значение Client IP. Каков его IP-адрес?



d.     Верейдите в Data Center и нажмите на Data Center POP > DC\_Edge-Rtr1.

e.     Нажмите на вклдадку CLI. В привилегированном режиме EXEC введите команду show crypto isakmp sa для отображения активных соединений IPsec. Какой статус указан в выходных данных команды?

f.       Какой IP-адрес назначения указан в выходных данных? Можете ли вы определить, к какому устройству принадлежит этот IP-адрес?



g.     Чтобы проверить VPN, вернитесь на VPN Laptop. В окне Command Prompt введите команду ftp 172.19.0.3 для свзяи с FTP-сервером в Data Center. При появлении запроса введите имя пользователя remote и пароль ciscorocks.

**Примечание**: В случае сбоя подключения убедитесь, что VPN все еще подключен.

C:\> **ftp 172.19.0.3**

Trying to connect...172.19.0.3

Connected to 172.19.0.3

220- Welcome to PT Ftp server

Username: **remote**

331- Username ok, need password

Password: **ciscorocks**

230- Logged in

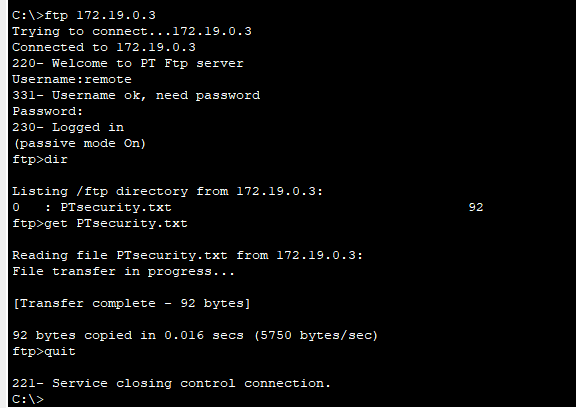
(passive mode On)

ftp>

h.     В ответ на приглашение ftp> введите команду dir для просмотра текущих файлов, сохраненных на удаленном FTP-сервере. Каково имя файла в списке?

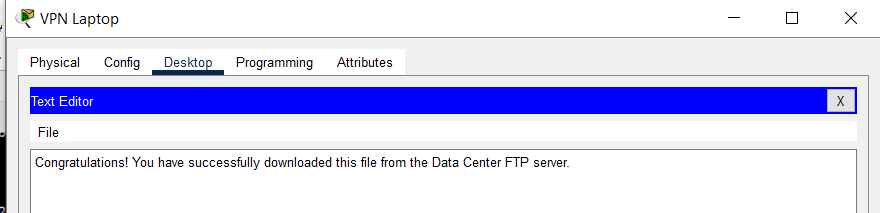
i.       Введите команду get *filename*, заменяющую имя файла на имя файла для загрузки на ноутбук.

j.       Введите команду quit, чтобы выйти из сеанса FTP.

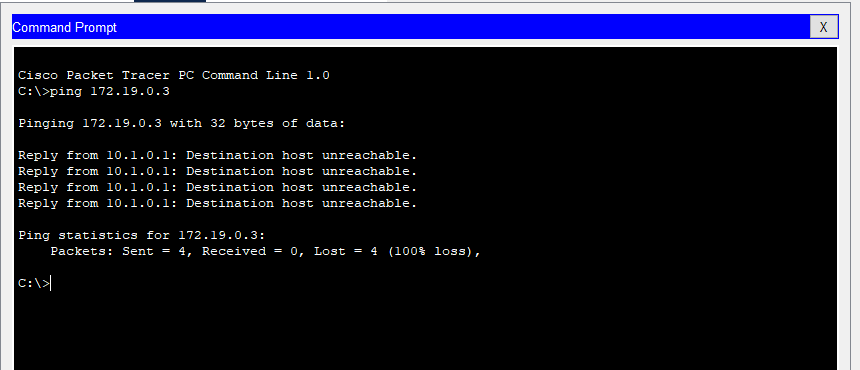


k.     Чтобы просмотреть содержимое файла, закройте окно Command Prompt и откройте Text Editor.

l.       Нажмите на File > Open. Нажмите на загруженный файл и нажмите кнопку Open. Какое первое слово в сообщении?



m.    В Coffee Shop выберите ноутбук и нажмите на Desktop > Command Prompt. Попытайтесь отправить эхо-запрос до FTP-сервера 172.19.0.3. Была ли проверка успешной? Поясните свой ответ.



На ноутбуке нет впн, поэтому он не может подключиться к серверу

n.     На реальном оборудовании вам потребуется VPN-сервис и их VPN-клиентское программное обеспечение, установленное на ноутбуке. Используйте Интернет для исследования различных VPN-сервисов/приложений, доступных для ноутбуков, планшетов и смартфонов. Какие три примера VPN-сервисов/приложений, которые можно использовать в открытой беспроводной сети для защиты данных?

**Шаг 3. Настройте безопасные WLAN в домашней сети.**

Для домашней сети вы выполните первоначальную настройку беспроводной сети, создадите отдельные сети для домашнего офиса и гостей, защитите каждую сеть надежной аутентификацией и включите фильтрацию MAC-адресов.

a.     Перейдите к сети Home. Исследуйте прокладку кабелей. Обратите внимание, что два компьютера, один в домашнем офисе, а другой в спальне, используют проводное соединение. Ноутбук в офисе будет использовать WLAN home office, а ноутбук в гостиной будет использовать guest WLAN.

b.     Используйте инструмент масштабирования (или Ctrl + прокрутки среднего колесика мыши) для увеличения масштаба домашнего офиса.

c.     Нажмите на Home Router. Это левое устройство, стоящее на полке за столом. Затем перейдите на вкладку GUI. Маршрутизатор использует DHCP для автоматического получения IP-адресации от ISP.

d.     Настройте следующие параметры в разделе Network Setup (Настройка сети):

IP Address: 192.168.0.254

Subnet Mask: 255.255.255.0

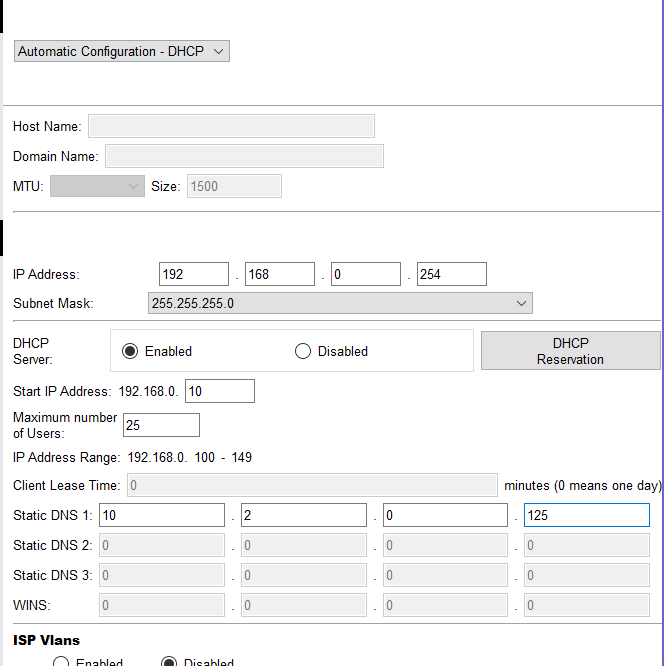
DHCP: Enabled

Start IP Address: 192.168.0.10

Maximum number of Users: 25

Static DNS 1: 10.2.0.125

e.     Прокрутите страницу вниз и нажмите кнопку Save Settings (Сохранить параметры).



f.       Прокрутите вверх и нажмите Wireless. В доп меню Basic Wireless Settings настройте SSID - HomeNet для кажой беспроводной стеи и отключите все широковещательные рассылки SSID.

g.     Прокрутите страницу вниз и нажмите кнопку Save Settings (Сохранить параметры).

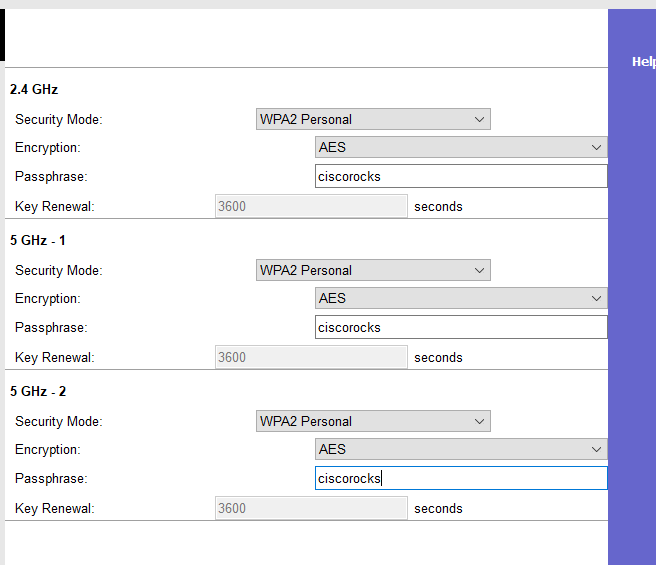
h.     Прокрутите назад вверх и выберите вложенную вкладку Wireless Security. Настройте следующие параметры для всех трех WLAN.

Security Mode: WPA2 Personal

Encryption: AES

Passphrase: ciscorocks

1. Прокрутите страницу вниз и нажмите кнопку Save Settings (Сохранить параметры).



j.       Прокрутите вверх и щелкните подменю Guest Network. Настройте следующие параметры для всех трех WLAN:

Enable Guest Profile

Network Name (SSID): GuestNet

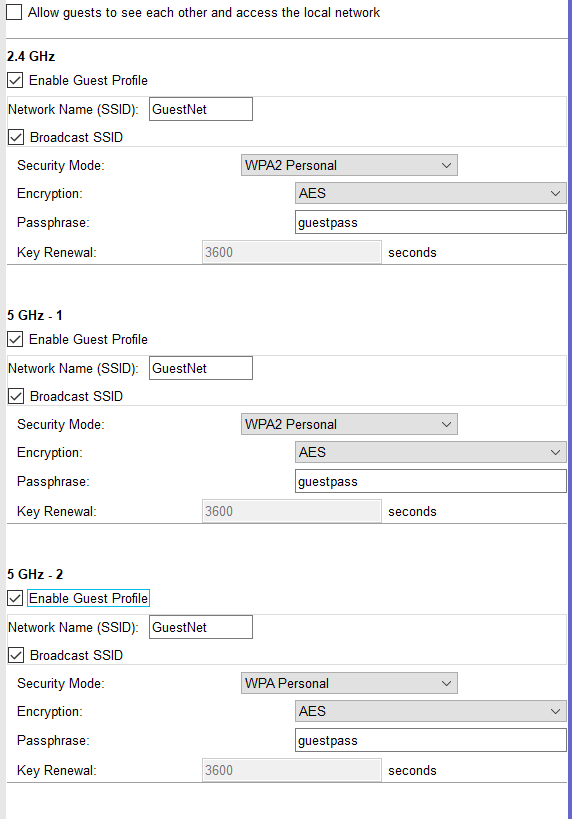
Enable Broadcast SSID

Security Mode: WPA2 Personal

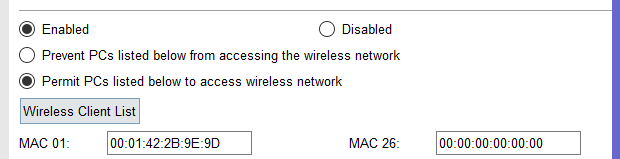
Encryption: AES

Passphrase: guestpass

k.     Прокрутите страницу вниз и нажмите кнопку Save Settings (Сохранить параметры).

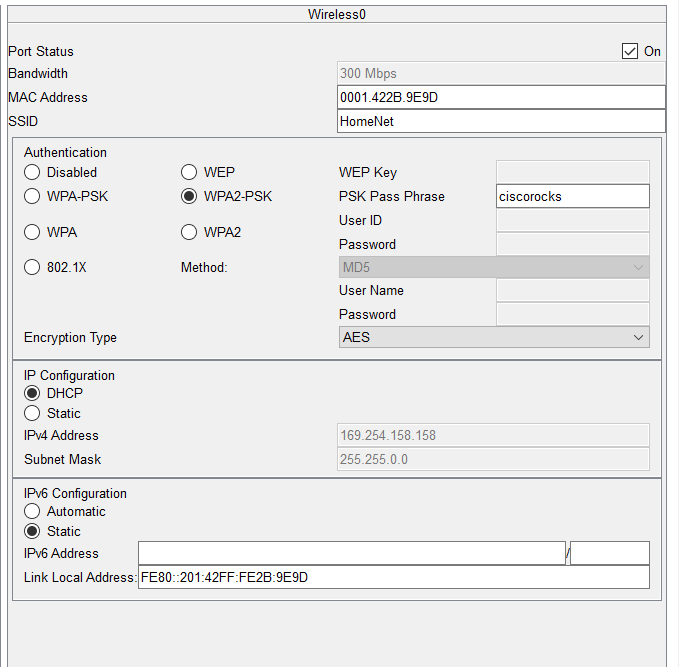


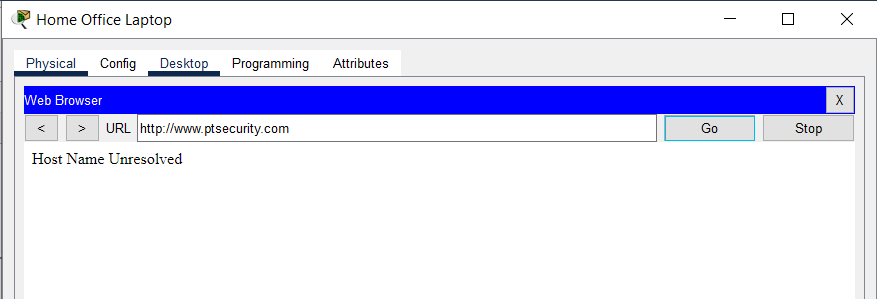
a.     Прокрутите назад вверх и выберите вложенную вкладку Wireless MAC Filter. Разрешите MAC-адрес ноутбука в домашнем офисе - 00:01:42:2 B:9E:9D. Обязательно разрешите MAC-адрес для всех трех WLAN. Вверху рядом с Wireless Port в выпадающем меню вы можете выбрать режимы 2.4G, 5G(1) и 5G(2).

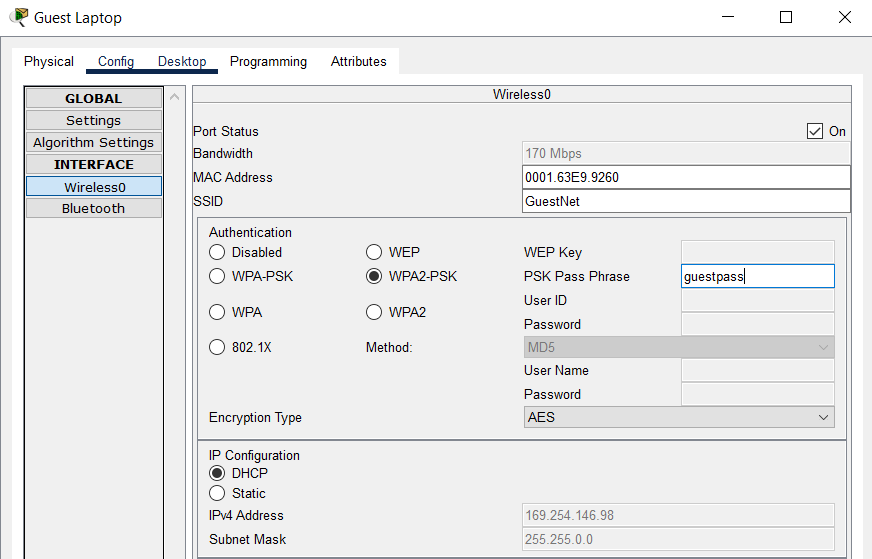


b.     Прокрутите страницу вниз и нажмите кнопку Save Settings (Сохранить параметры).

c.     В Home Office на столе перед диваном нажмите на ноутбук, а затем вкладку Config. Настройте параметры беспроводной сети, необходимые для доступа к локальной сети HomeNet.



1. Откройте вкладку Desktop и нажмитен на Web Browser. Введите URL-адрес www.ptsecurity.com и нажмите кнопку Go. Отображение веб-страницы может занять несколько секунд. Если появляется сообщение о тайм-ауте запроса, нажмите кнопку Go еще раз.
2. 
3. Вернитесь в Hoem и увеличьте масштаб гостиной. Выберите Guest Laptop, а затем Wireless0 в разделе INTERFACE. Настройте параметры беспроводной сети, необходимые для доступа к беспроводной сети GuestNet. Убедитесь, что в разделе IP Configuration выбран параметр DHCP. Получил ли ноутбук IP-адресацию от Home Router? Поясните свой ответ. Адрес не получен, т.к мак этого ноутбука не в списке разрешенных

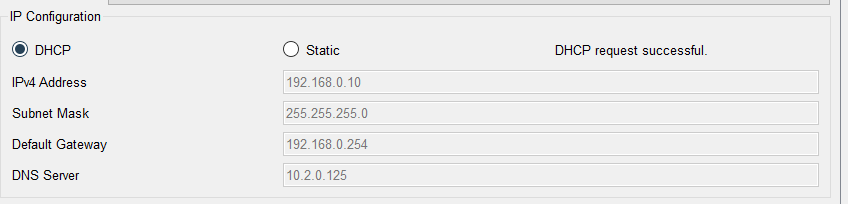


1. Вернитесь на вкладку GUI для Home Router и исправьте проблему.

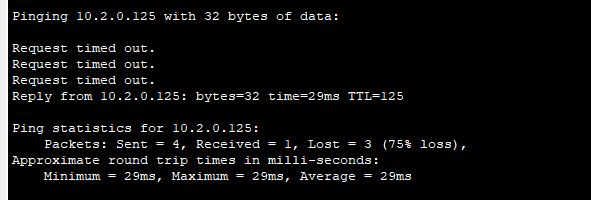
Добавим мак в список разрешенных



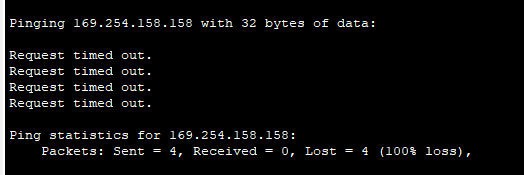
1. Вернитесь к Guest Laptop. В разделе Wireless0 > IP Configuration теперь отображается IP-адресация из пула, настроенного ранее на Home Router. Если нет, переключайтесь между DHCP и Static для обновления запросов DHCP.



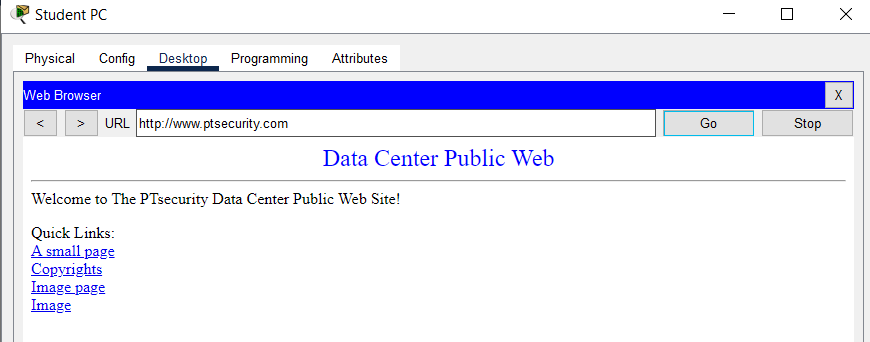
h.     Нажмите на Desktop > Command Prompt и выполните эхо-запрос до DNS-сервера поставщика услуг Интернета 10.2.0.125, чтобы проверить доступ к внешним устройствам. Ping должен пройти успешно.



1. Проверьте доступ к любому другому устройству в домашней сети. Успешно ли выполнены эхо-запросы? Поясните свой ответ. Ping не проходят, т.к ноутбук находится в другой WLAN



1. Закройте окно Command Prompt и нажмите на Web Browser. Проверьте доступ к www.ptsecurity.com. Доступ должен быть успешным.



**Вопросы для повторения**

a.     Перечислите все различные подходы к обеспечению безопасности, которые использовались в этой ситуации. VPN, пароли на AP, создание списка разрешенных MAC, создания нескольких WLAN для изоляции

b.     В ситуации, когда используется реальное оборудование, перечислите другие предложения, которые могут быть добавлены в этот сценарий, чтобы сделать его более безопасным. ????

*Конец документа*