МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,

СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»

(СПбГУТ)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Факультет инфокоммуникационных сетей и систем

Кафедра защищенных систем связи

Дисциплина принципы организации глобальных вычислительных сетей

ЛАБОРАТОРНАЯ РАБОТА №3

Packet Tracer – Исследование сетевой безопасности – Режим симуляции физического оборудования

*(тема лабораторной работы)*

Направление/специальность подготовки

11.03.02 Инфокоммуникационные технологии и системы связи

*(код и наименование направления/специальности)*

Студенты:

Миколаени Матвей Сергеевич, Громов Артем Андреевич, ИКТЗ-83 \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Преподаватель:

К.т.н., доцент каф. ЗСС, Ушаков Игорь Александрович

(учетная степень, учетное звание, ФИО)

(дата, подпись)

ОГЛАВЛЕНИЕ

[ЗАДАЧИ 3](#_Toc95945702)

[ОБЩИЕ СВЕДЕНИЯ И СЦЕНАРИИ 3](#_Toc95945703)

[ВЫПОЛНЕНИЕ 3](#_Toc95945704)

[Часть 1 – Знакомство с сетью 3](#_Toc95945705)

[Часть 2. Реализация мер по обеспечению безопасности 10](#_Toc95945706)

# ЗАДАЧИ

Часть 1. Знакомство с сетью;

Часть 2. Осуществление мер безопасности.

# ОБЩИЕ СВЕДЕНИЯ И СЦЕНАРИИ

В этом задании в режиме симуляции физического оборудования (PTPM) мы будем 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. Мы установим детектор дыма Интернета вещей (IoT).

Кофейня предлагает своим посетителям бесплатный беспроводной доступ в Интернет. Мы будем реализовывать VPN для защиты трафика.

Дом включает в себя офис, студенческую спальню и гостиную. Мы настроим 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.

# ВЫПОЛНЕНИЕ

## Часть 1 – Знакомство с сетью

Шаг 1. Исследуйте Гринвилл

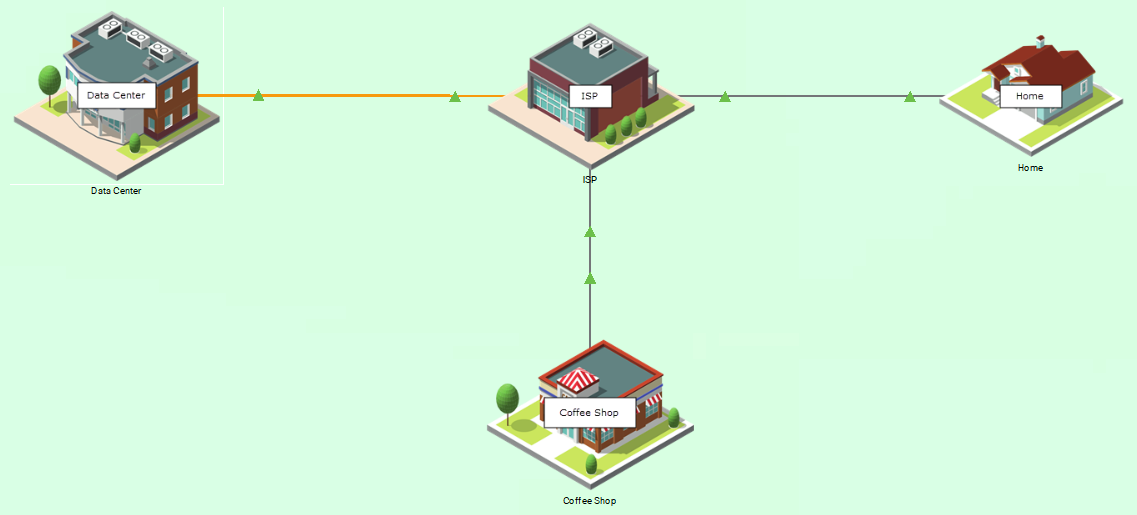


Рисунок 1 - Сеть Гринвилла

Шаг 2. Ознакомиться с залами в центре обработки данных

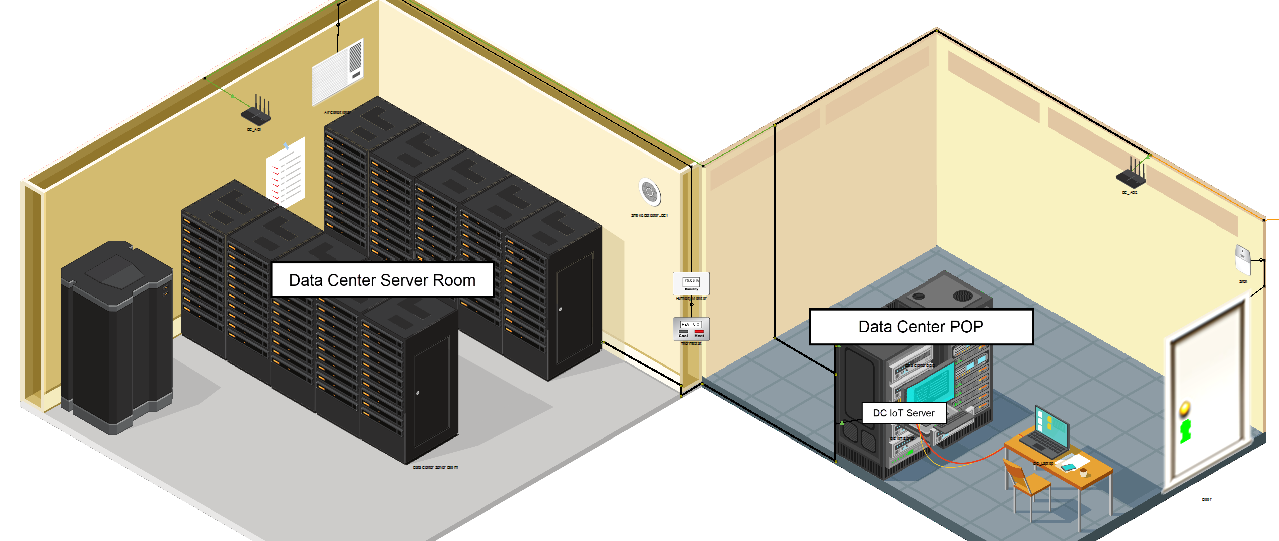


Рисунок 2 - Data Center Room

В данном примере два зала, в которых имеется следующее оборудование:

* Data Center POP;
* IoT Server;
* 2 точки доступа;
* Ноутбук;
* Несколько устройств IoT.

Как называется маршрутизатор в Data Center Server Room? – DC1\_R1

Шаг 3. Исследуйте устройства в Data Center POP

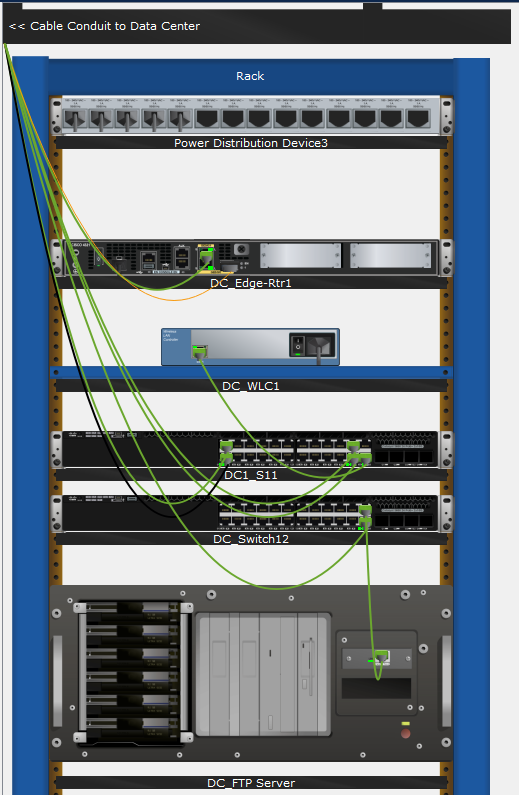


Рисунок 3 - Data Center POP

Какой тип кабеля используется для подключения DC\_Edge-RTR1 к поставщику услуг интернета? – Fiber

Какое устройство выполняет преобразование адресов частных дата-центров в публичные? - DC\_Edge-Rtr1

Просмотрим список доступа – access-list

DC\_Edge-Rtr1>en

DC\_Edge-Rtr1#show access-lists

Extended IP access list REMOTE\_IN

10 permit tcp any host 10.0.0.3 eq www

20 permit tcp any host 10.0.0.3 eq 443

30 permit udp any host 10.0.0.2 eq isakmp

40 permit udp any host 10.0.0.2 eq non500-isakmp

50 permit tcp any gt 1023 any eq ftp

60 permit tcp any gt 1023 any gt 1023

70 deny ip any any

(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).

Исследуем интерфейсы. На каком интерфейсе и в каком направлении применяется этот список доступа? - Лист-доступа настроен, но он не применяется ни к одному интерфейсу

interface GigabitEthernet0/0/0

description link to ISP

bandwidth 1000000

media-type sfp

ip address 10.0.0.2 255.255.255.248

ip nat outside

crypto map CLIENT\_MAP

!

interface GigabitEthernet0/0/1

ip address 172.16.1.1 255.255.0.0

ip nat inside

duplex auto

speed auto

!

interface Vlan1

no ip address

shutdown

!

ip local pool MYPOOL 172.18.1.150 172.18.1.200

ip nat inside source static 172.17.1.100 10.0.0.3

ip classless

ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0

ip route 172.17.0.0 255.255.0.0 172.16.1.2

ip route 172.31.0.0 255.255.0.0 172.16.1.2

ip route 10.2.0.0 255.255.0.0 10.0.0.1

ip route 10.1.0.0 255.255.0.0 10.0.0.1

ip route 172.19.0.0 255.255.0.0 172.16.1.2

!

ip flow-export version 9

!

!

ip access-list extended REMOTE\_IN

permit tcp any host 10.0.0.3 eq www

permit tcp any host 10.0.0.3 eq 443

permit udp any host 10.0.0.2 eq isakmp

permit udp any host 10.0.0.2 eq non500-isakmp

permit tcp any gt 1023 any eq ftp

permit tcp any gt 1023 any gt 1023

deny ip any any

!

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

В Data Center POP зайдем в ноутбук, перейдем на сайт по 172.31.0.2, который является DC IoT Server и откроем список устройств.

Какие устройства в настоящее время используются для защиты сетевого оборудования в центре обработки данных от факторов окружающей среды и физической безопасности? – Кондиционер, термостат, датчик влажности, дверь, сирена.

Каков текущий уровень влажности в списке устройств? – 75%

Шаг 5. Исследуйте контролируемую дверь и сирену

При помощи интернета вещей мы включали и отключали Siren, а также открывали и закрывали дверь

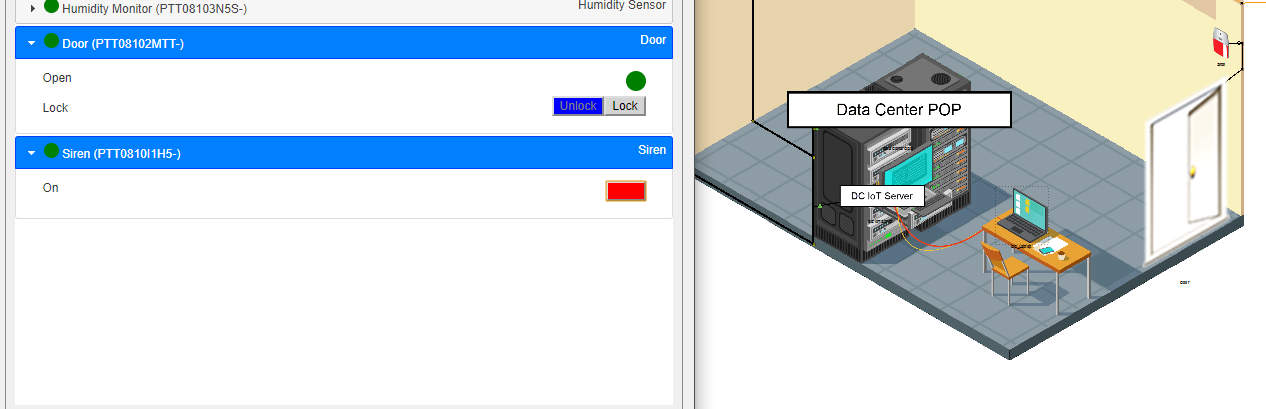


Рисунок 4 - Управление сиреной и дверью

Шаг 6. Исследовать термостат

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

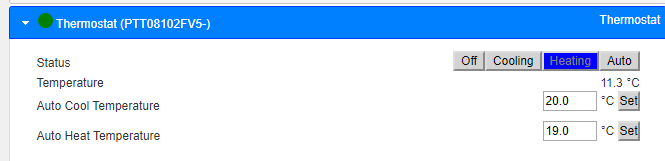


Рисунок 5 - Управление термостатом

В DC найдем термостат, зайдем в config и перейдем на интерфейс Wireless 0. Каков IP-адрес для термостата? - 172.31.0.13 255.255.0.0

Шаг 7 Изучите сети ISP, Coffee Shop и Home



Рисунок 6 - Coffee Shop

Перейдите к Coffee Shop. Как клиенты подключаются к сети Coffee Shop? – Через Wi-Fi.

Какой тип среды используется для подключения кафе к Интернету? - Коаксиальный кабель (см. Wiring cabinet)

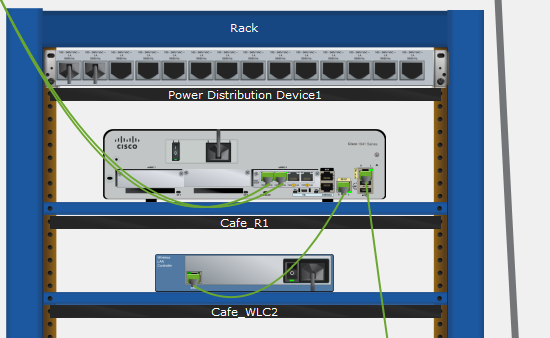


Рисунок 7 - Устройства Coffee Shop

Какие устройства используются для создания сети Coffee Shop? – Коммутатор, маршрутизатор, WLC-управление, ноутбук, модем.

Нажмите на каждый ноутбук в Coffee Shop. Откройте вкладку config (Конфигурация) и щелкните интерфейс Wireliss 0 в разделе Interface. Какие IP-адреса у них? - Coffee Shop Customer - 192.168.0.11, VPN Laptop - 192.168.0.12

Перейти в Home:



Рисунок 8 - Home Network

Как Home подключается к ISP? - Через Cable Modem

Какие устройства требуют подключения внутри дома? - Home Office PC, Home office Laptop, Student PC, Guest Laptop

## Часть 2. Реализация мер по обеспечению безопасности

В этой части мы настроим безопасность беспроводной сети для детектора дыма в Data Center, виртуальной частной сети (VPN) в Coffee Shop и двух беспроводных сетей в Home.

Шаг 1. Настройте детектор дыма IoT в Data Center

Настройка Smoke Detector:

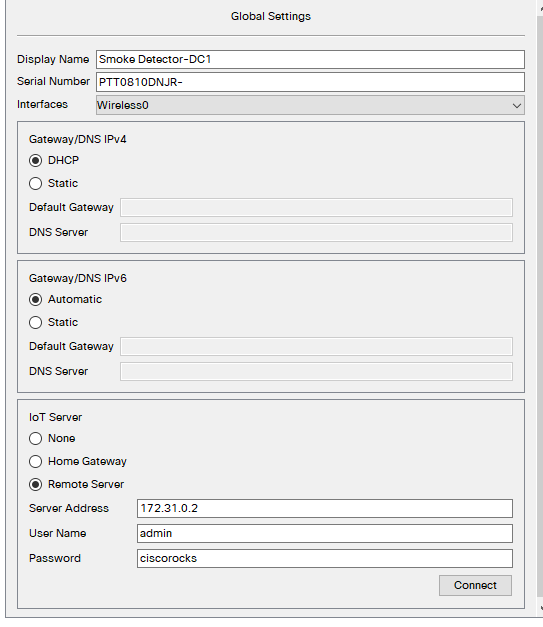


Рисунок 9 - Smoke Detector Global Setting

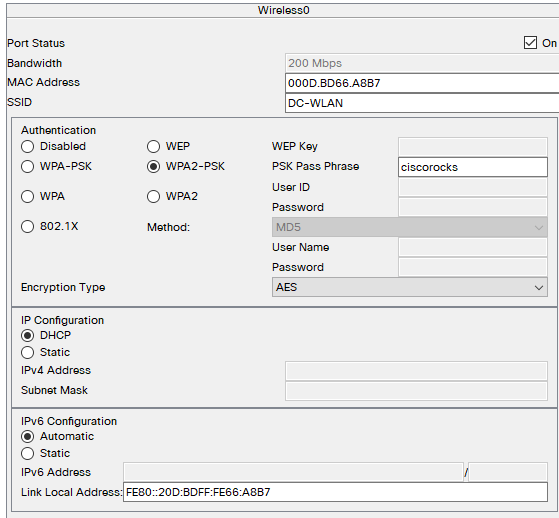


Рисунок 10 - Smoke Detector Int Wireless 0

После данных настроек, данный датчик дыма появился на Web-интерфейсе 172.31.0.2.

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

Зачем нужен VPN?

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.

Открыв VPN laptop, прописав cmd ipconfig увидим следующий IP – 192.168.0.12

Какой IP VPN клиента - 172.18.1.150

Настроим и подключимся

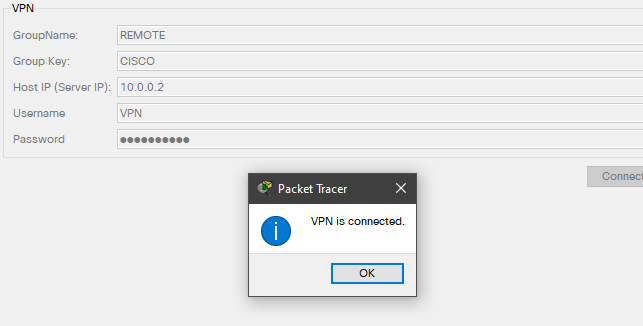


Рисунок 11 - Подключение по VPN

Войдя в DC POP – DC\_Edge-Rtr1 – CLI и введя show crypto isakmp sa – увидим статус Active

Какой Ip-адрес назначения указан в выходных данных? - 10.1.0.11 (на интерфейсе)

Можете ли вы определить, к какому устройству принадлежит этот IP-адрес? - Принадлежит Cafe\_R1 Interface G0/0

Проверим VPN соединение и проверим файлы на удаленном ftp-сервере:

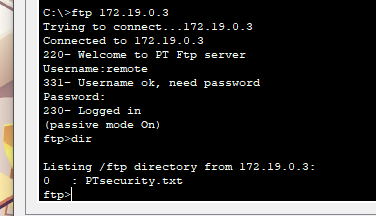


Рисунок 12 - Подключение к FTP

Посмотрим содержимое файла:

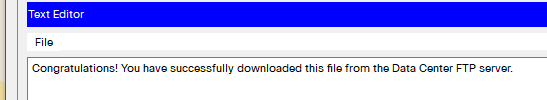


Рисунок 13 - Содержимое файла PTsecurity.txt

Какое первое слово в сообщении? – Congratulations!

Если на Coffee laptop пропинговать FTP сервер, то ничего не получится, т.к.VPN отключен.

Какие три примера VPN-сервисов/приложений, которые можно использовать в открытой беспроводной сети для защиты данных? - SSTP, Wireguard, OpenVPN.

Шаг 3. Настроить безопасные WLAN в домашней сети.

Настройки Home Router:

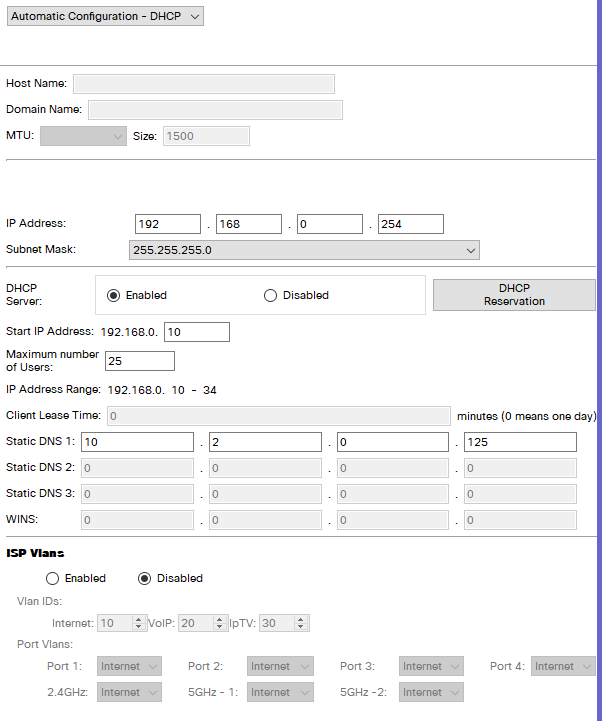


Рисунок 14 - Setting Home Router Basic Setup

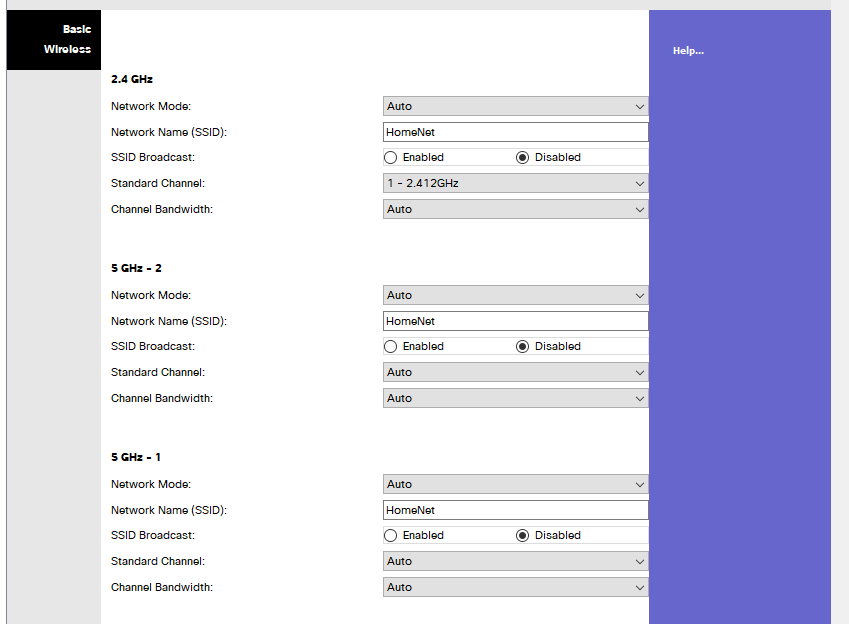


Рисунок 15 - Basic Wireless setup

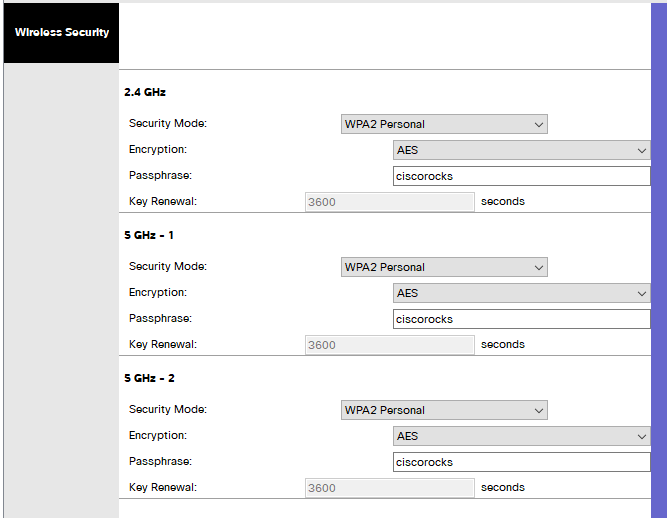


Рисунок 16 - Wireless security

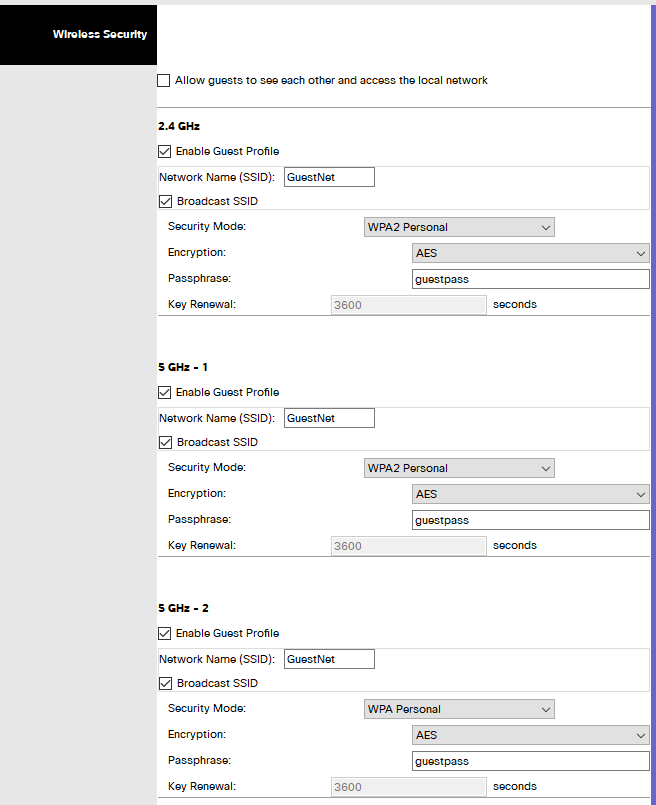


Рисунок 17 - Wireless Security 2

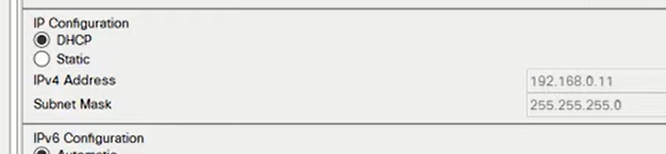
На устройстве Home office попробуем получить доступ к [www.ptsecurity.com](http://www.ptsecurity.com)



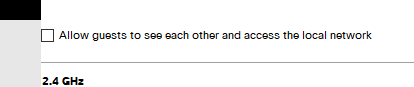
Рисунок 18 - Успешно зашли на ptsecurity

На Guest Laptop невозможно получить адресацию от сети, т.к. на роутере не настроен его MAC-адрес.

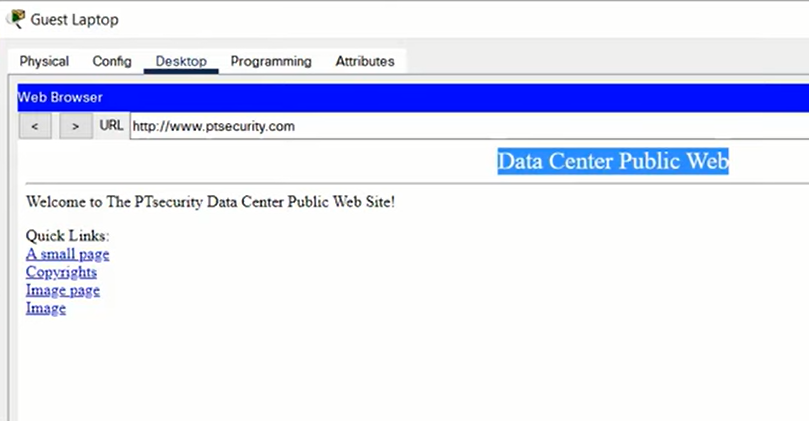
После настройки MAC-адреса, Laptop успешно получил адресацию по DHCP.



Если попробовать пропинговать домашние устройства, то ничего не получится, т.к. роутер запрещает доступ к локальным ресурсам (настройка в GUI роутера).



Ресурс ptsecurity также доступен.\



Вопросы для повторения:

1. Перечислите все различные подходы к обеспечению безопасности, которые использовались в этой ситуации.
   1. Фильтрация по MAC-адресам
   2. Использование VPN в открытых сетях
   3. Размещение различных IoT устройств в серверных;
   4. Защита ЦОД-ов дверью с охраной
2. В ситуации, когда используется реальное оборудование, перечислите другие предложения, которые могут быть добавлены в этот сценарий, чтобы сделать его более безопасным.
   1. Использовать VPN дома;
   2. Создание резервных ЦОД-ов;
   3. Использование надежных паролей.