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 Безопасность компьютерных сетей

ЛАБОРАТОРНАЯ РАБОТА №9 – Часть 1

Packet Tracer - Layer 2 Security

11.03.02 Инфокоммуникационные технологии и системы связи

Студенты:

Громов А. А., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Жиляков Г. В., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Миколаени М. С., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Проверил:

К.т.н., доцент каф. ЗСС, Кушнир Д. В.

# Топология:

# 

**Задачи**

         Назначение центрального коммутатора (Central) в качестве корневого моста.

         Защита параметров связующего дерева для предотвращения атак путем манипуляций с протоколом STP.

         Включение защиты портов для предотвращения атак путем переполнения таблиц CAM.

**Исходные данные/ сценарий**

Недавно сеть подверглась нескольким атакам. Поэтому сетевой администратор поручил вам настроить безопасность на 2-м уровне.

Для обеспечения оптимальной производительности и безопасности администратор хотел бы, чтобы в качестве корневого моста использовался коммутатор 3560 Central. Чтобы предотвратить атаки путем манипуляций с протоколом STP, администратору требуется гарантированная защита параметров STP. Чтобы предотвратить атаки путем переполнения таблиц CAM, сетевой администратор решил настроить защиту портов для ограничения количества MAC-адресов, которые может получить каждый порт коммутатора. Если число MAC-адресов превышает заданное ограничение, порт должен быть отключен.

На всех коммутаторах были предварительно настроены следующие параметры.

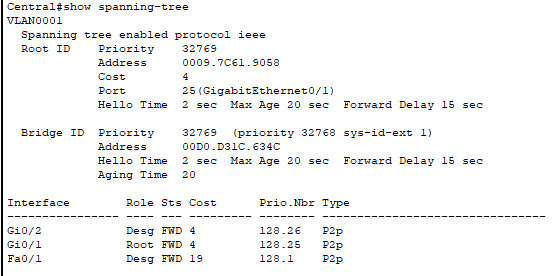
o    Пароль привилегированного доступа: **ciscoenpa55**

o    Пароль консоли: **ciscoconpa55**

o    Имя пользователя и пароль SSH: **SSHadmin**/**ciscosshpa55**

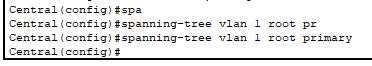
**Часть 1. Настройка корневого моста**

**Шаг 1. Определите текущий корневой мост.**

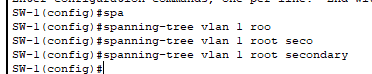
****

Корневой мост – SW-1

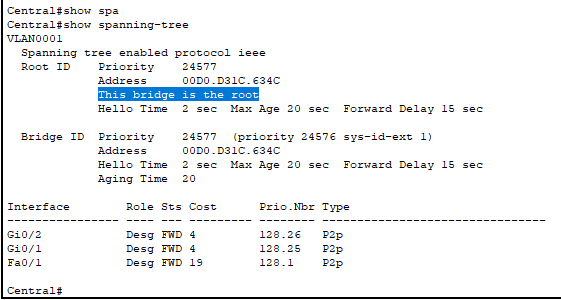
**Шаг 2. Назначьте коммутатор Central главным корневым мостом.**

****

**Шаг 3. Назначьте коммутатор SW-1 вторичным корневым мостом.**

****

**Шаг 4. Проверьте конфигурацию связующего дерева.**

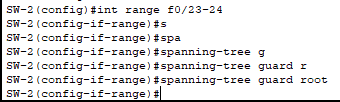
****

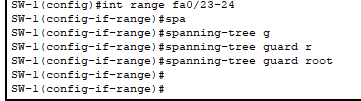
**Часть 2. Защита от атак на STP**

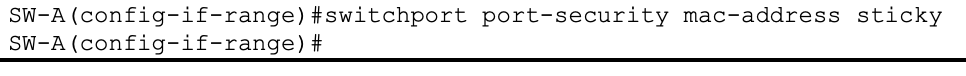
**Шаг 1. Включите функцию PortFast на всех портах доступа.**

**Шаг 2. Включите функцию BPDU Guard на всех портах доступа.**

**Шаг 3. Включите Root Guard.**

****

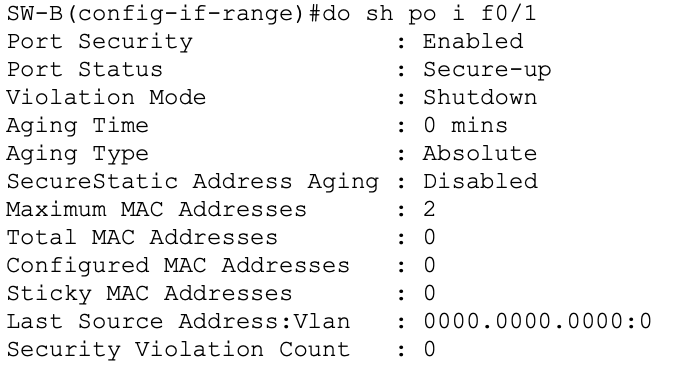
****

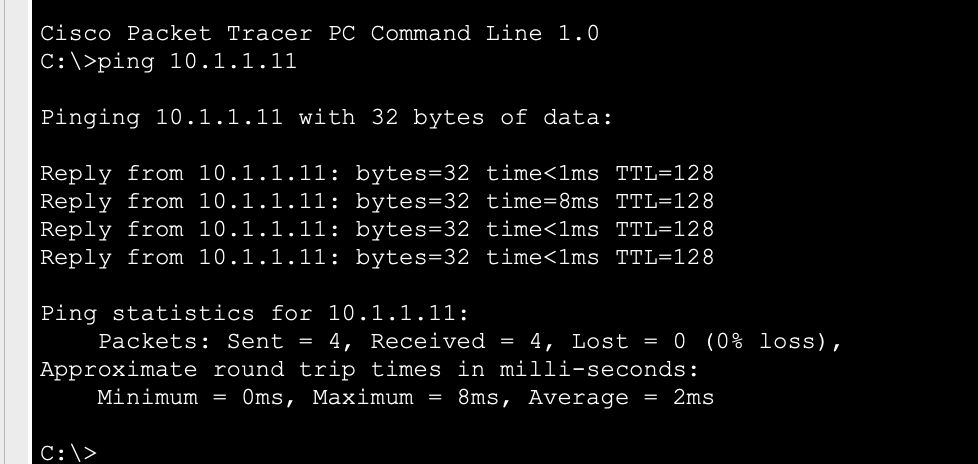
****

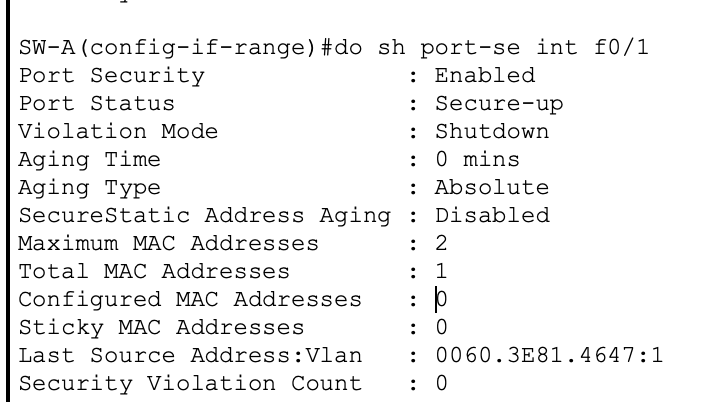
**Часть 3. Настройка безопасности портов и отключение неиспользуемых портов**

**Шаг 1. Настройте базовый уровень безопасности на всех портах, подключенных к хост-устройствам.**

**Шаг 2. Проверьте безопасность портов.**

****

****

****

**Шаг 3. Отключите неиспользуемые порты.**

**Шаг 4. Проверьте результаты.**

