МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

На правах рукописи

А.Н. Земцов

Методы и средства защиты облачной и сетевой инфраструктуры

Учебное пособие

Волгоград
2021

УДК 004.72:004.056

Земцов А.Н.

Методы и средства защиты облачной и сетевой инфраструктуры: учеб. пособие / А.Н. Земцов; ВолгГТУ. – Волгоград,2021. – 22 с.

В учебном пособии рассмотрены методы и средства защиты инфокоммуникационных систем искусственного интеллекта.

Учебное пособие предназначено для магистров, обучающихся по программам магистратуры по профилю «искусственный интеллект» по направлениям 09.04.01 «Информатика и вычислительная техника», 09.04.03 «Прикладная информатика», 09.04.02 «Информационные системы и технологии». Учебное пособие выполнено в рамках реализации гранта на разработку программ бакалавриата и программ магистратуры по профилю «Искусственный интеллект», а также на повышение квалификации педагогических работников образовательных организаций высшего образования в сфере искусственного интеллекта (конкурс 2021-ИИ-01 от 10.06.2021).

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В связи с расширяющейся цифровизацией самых разных сфер деятельности человека, в том числе в связи с повсеместным внедрением систем искусственного интеллекта, постоянно возрастает важность технических методов и средств защиты информационных систем и систем искусственного интеллекта от различных угроз. В настоящей работе приведены описания практических и лабораторных работ, посвященных различным аспектам организации защиты облачной и сетевой инфраструктуры.

1. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

1.1. Практика №1. Основы противодействия угрозам безопасности

1.1.1. Цель практической работы

Цель практической работы №1 состоит в том, чтобы на практических примерах дать студентам дать общее представление об основах противодействия угрозам безопасности

1.1.2. Описание практической работы

Основные вопросы, обсуждаемые на занятии.

1) Современные угрозы сетевой безопасности системам облачной и сетевой инфраструктуры, системам искусственного интеллекта.

2) Обеспечение безопасного доступа к системам облачной и сетевой инфраструктуры, системам искусственного интеллекта.

3) Назначение административных ролей.

4) Аутентификация.

5) Обеспечение безопасности канального уровня.

1.2. Практика №2. Системы обнаружения и предотвращения вторжения

1.2.1. Цель практической работы

Цель практической работы №3 состоит в том, чтобы на практических примерах дать студентам дать общее представление о системах обнаружения и предотвращения вторжения

1.2.2. Описание практической работы

Основные вопросы, обсуждаемые на занятии.

1) Технологии инспектирования трафика.

2) Системы обнаружения и предотвращения вторжения.

1.3. Практика №3. Технологии фильтрации трафика

1.3.1. Цель практической работы

Цель практической работы №3 состоит в том, чтобы на практических примерах дать студентам дать общее представление о технологиях фильтрации трафика.

1.3.2. Описание практической работы

Основные вопросы, обсуждаемые на занятии.

1) Технологии фильтрации трафика.

2) Конфигурирование межсетевых экранов

1.4. Практика №4. Виртуальные частные сети

1.4.1. Цель практической работы

Цель практической работы №4 состоит в том, чтобы на практических примерах дать студентам дать общее представление о защите систем и информации с помощью виртуальных частных сетей.

1.4.2. Описание практической работы

Основные вопросы, обсуждаемые на занятии.

1) Технология виртуальных частных сетей VPN.

2) Защита облачной и сетевой инфраструктуры с помощью технологии VPN.

3) Туннелирование с общей инкапсуляцией маршрутов.

4) Протокол туннелирования второго уровня

5) Организация виртуальной частной сети.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ

2.1 Лабораторная работа № 1 Обеспечение безопасности канального уровня.

2.1.1 Цели и задачи

Целью работы является ознакомление с функциональными возможностями механизмов защиты коммутаторов локальных сетей от атак канального уровня.

Задачи:

1. Изучение возможностей функции безопасности портов.
2. Конфигурирование аутентификации при доступе к сети.
3. Изучение технологий противодействия атакам канального уровня.

2.1.2 Теоретические положения

Теоретические положения отражены в руководствах по конфигурированию рассматриваемых технологий компании Cisco Systems, расширенной версии методических указаний к лабораторной работе.

2.1.3 Порядок выполнения работы

1. Построение сети с заданной топологией.
2. Настройка базовых параметров сетевого оборудования.
3. Создание и настройка виртуальных локальных сетей.
4. Изучение возможностей функции безопасности портов.

Конфигурирование режимов реагирования на нарушения безопасности.

5. Конфигурирование аутентификации при доступе к сети.
6. Конфигурирование технологий противодействия атакам канального уровня.
7. Моделирование атак.
8. Проверка реакции сетевого устройства на проводимую атаку.

9. Интерпретация результатов.

Методические материалы к п. 3 «Создание и настройка виртуальных локальных сетей в программе Cisco Packet Tracer»

VLAN (аббр. от англ. Virtual Local Area Network) — логическая ("виртуальная") локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети.

VLAN'ы могут быть настроены на коммутаторах, маршрутизаторах, других сетевых устройствах.

Преимущества:

- облегчается перемещение, добавление устройств и изменение их соединений друг с другом;
- достигается большая степень административного контроля вследствие наличия устройства, осуществляющего между сетями VLAN маршрутизацию на 3-м уровне;
- уменьшается потребление полосы пропускания по сравнению с ситуацией одного широковещательного домена;
- сокращается непроизводственное использование CPU за счет сокращения пересылки широковещательных сообщений;
- предотвращение широковещательных штормов и предотвращение петель.

Настройка VLAN на одном коммутаторе Cisco

Рассматривается настройка VLAN на коммутаторе фирмы Cisco на его портах доступа. Создайте сеть, логическая топология которой представлена на рисунке 1. Компьютеры соединены коммутатором Cisco 2960-24TT. В таблице 1 приведены адреса компьютеров.

Задача – сделать две независимые группы компьютеров: ПК0, ПК1 и ПК2 должны быть доступны только друг для друга, вторая независимая группа - компьютеры ПК3 и ПК4. Для этого создадим два отдельных VLAN (рисунок 1).

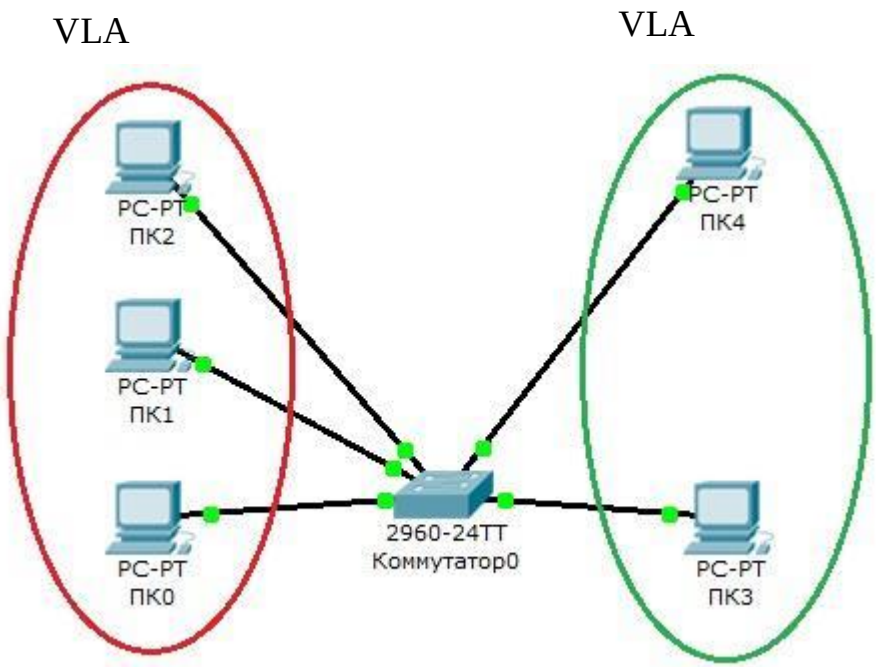


Рисунок 1 - Схема сети с одним коммутатором.

Таблица 1.

Компьютер	IP адрес	Порт коммутатора
ПК0	10.0.0.1/8	1
ПК1	10.0.0.2/8	2
ПК2	10.0.0.3/8	3
ПК3	10.0.0.4/8	4

ПК4	10.0.0.5/8	5

Далее будем считать, что ПК0, ПК1 и ПК2 находятся в VLAN 2, а ПК3 и ПК4 находятся в VLAN 3.

Для проверки конфигурации хоста ПК0 выполним команду ipconfig. Результат выполнения команды на рисунке 2. При желании можно выполнить аналогичную проверку на остальных хостах.

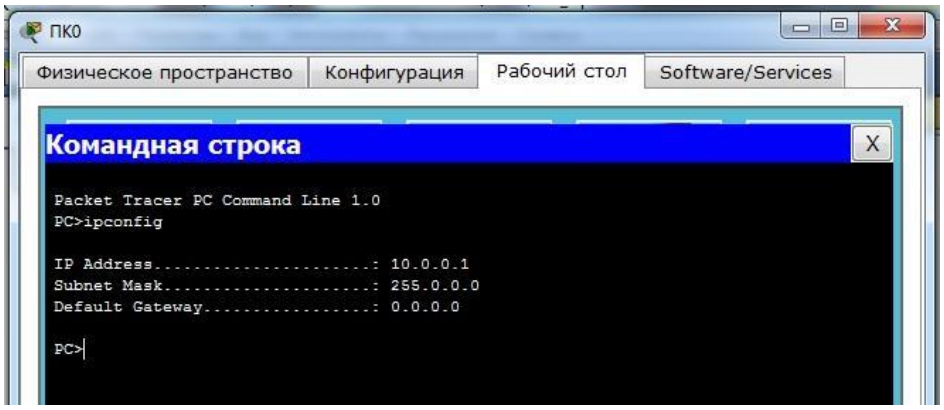


Рисунок 2 Проверка конфигурации хоста

Используя команду PING, проверим связь между всеми компьютерами. Сейчас они в одной сети и все доступны друг для друга

Теперь займемся настройкой VLAN 2 и VLAN3, чтобы структурировать сети на коммутаторе и навести в них порядок.

Далее перейдем к настройке коммутатора. Откроем его консоль. Для того чтобы это выполнить в Packet Tracer дважды щелкните левой кнопкой мыши по коммутатору в рабочей области.

В открывшемся окне перейдите на вкладку CLI. Вы увидите окно консоли. Нажмите Enter, чтобы приступить к вводу команд. Информация, которая в данный момент отражена на консоли, свидетельствует о том что интерфейсы FasteEthernet0/1 – FasteEthernet0/5 находятся в рабочем состоянии.

Перейдем в привилегированный режим выполнив команду enable:

Switch>**en**

Switch#

Просмотрим информацию о существующих на коммутаторе VLAN-ах (рисунок 3). Для этого выполним следующую команду:

Switch#**sh vl br**

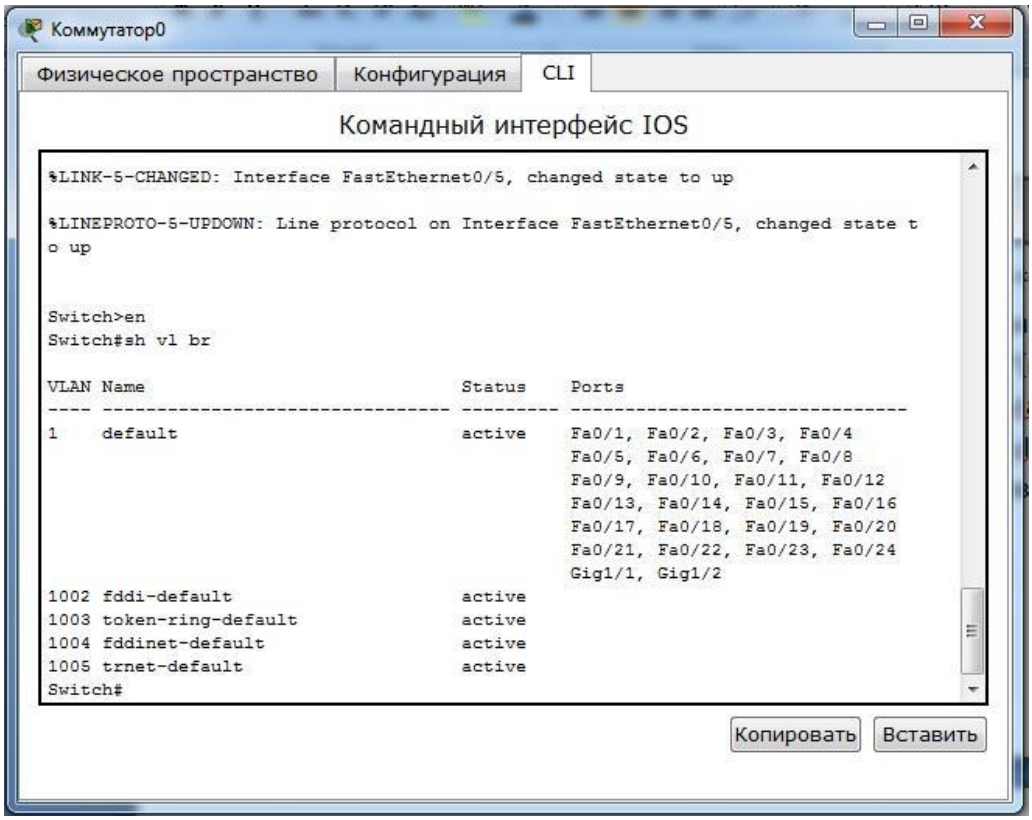


Рисунок 3. Просмотр информации о VLAN на коммутаторе

В результате выполнения команды на экране появится: номера VLAN – первый столбец, название VLAN - второй столбец, состояние VLAN (работает он в данный момент или нет) – третий столбец, порты

принадлежащие к данному VLAN – четвертый столбец. Как мы видим по умолчанию на коммутаторе существует пятьVLAN-ов. Все порты коммутатора по умолчанию принадлежат VLAN 1. Остальные четыре VLAN являются служебными и используются не очень часто.

Для реализации сети, которую мы запланировали сделать, создадим на коммутаторе еще два VLAN. Для этого в привилегированном режиме выполните следующую команду:

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

Вводим команду VLAN 2. Данной командой вы создадите на коммутаторе VLAN с номером 2. Указатель ввода Switch(config)# изменится на Switch(config-vlan)# это свидетельствует о том, что вы конфигурируете уже не весь коммутатор в целом, а только отдельный VLAN, в данном случае VLAN номер 2. Если вы используете команду «vlan x», где x номер VLAN, когда VLAN x еще не создан на коммутаторе, то он будет автоматически создан, и вы перейдете к его конфигурированию. Когда вы находитесь в режиме конфигурирования VLAN, возможно изменение параметров выбранной виртуальной сети, например можно изменить ее имя с помощью команды name.

Для достижения поставленной в данном посте задачи, сконфигурируем VLAN 2 следующим образом:

```
Switch(config)#vlan 2
Switch(config-vlan)#name subnet_10
Switch(config)#interface range fastEthernet 0/1-3
Switch(config-if-range)#switchport mode access
```

Switch(config-if-range)#**switchport access vlan 2**

Разберем данную конфигурацию. Как уже говорилось ранее командой VLAN 2, мы создаем на коммутаторе новый VLAN с номером 2. Команда **name subnet_10** присваивает имя subnet_10 виртуальной сети номер 2. Выполняя команду **interface range fastEthernet 0/1-3** мы переходим к конфигурированию интерфейсов fastEthernet0/1, fastEthernet0/2 и fastEthernet0/3 коммутатора. Ключевое слово **range** в данной команде, указывает на то, что мы будем конфигурировать не один единственный порт, а целый диапазон портов, в принципе ее можно не использовать, но тогда последние три строки придется заменить на:

Switch(config)#**interface fastEthernet 0/1**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 2**
Switch(config)#**interface fastEthernet 0/2**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 2**
Switch(config)#**interface fastEthernet 0/3**
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan 2**

Команда **switchport mode access** конфигурирует выбранный порт коммутатора, как порт доступа (аксесс порт).

Команда **switchport access vlan 2** указывает, что данный порт является портом доступа для VLAN номер 2.

Выйдите из режима конфигурирования, дважды набрав команду **exit** и просмотрите результат конфигурирования (рисунок 4), выполнив уже знакомую нам команду **sh vl br** еще раз:

```
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig1/1, Gig1/2
2    subnet_10                         active    Fa0/1, Fa0/2, Fa0/3
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Рисунок 4 Распределение портов на VLAN

На коммутаторе появился еще один VLAN с номером 2 и именем subnet_10, портами доступа которого являются fastEthernet0/1, fastEthernet0/2 и fastEthernet0/3.

Далее аналогичным образом создадим VLAN 3 с именем subnet_192 и сделаем его портами доступа интерфейсы fastEthernet0/4 и fastEthernet0/5. Результат должен получиться следующим (рисунок 5):

```
Switch#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                 Gig1/2
2    subnet_10                         active    Fa0/1, Fa0/2, Fa0/3
3    subnet_192                        active    Fa0/4, Fa0/5
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

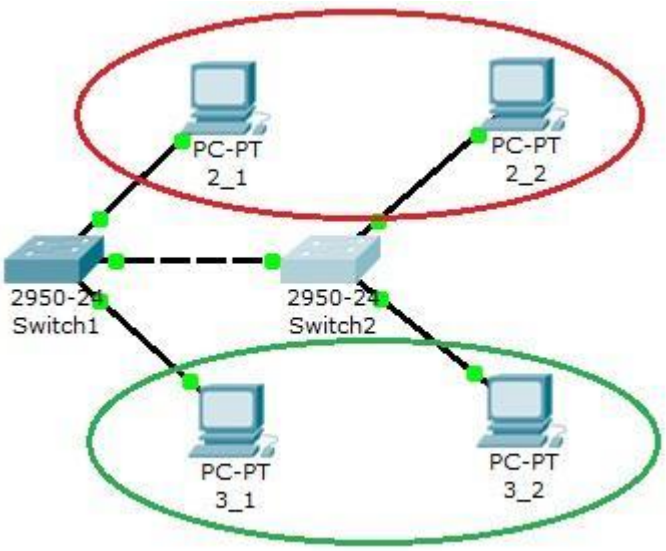
Рисунок 5. Распределение портов на VLAN

В принципе, уже все готово, и наша сеть настроена. Осталось лишь ее протестировать. Перейдите в консоль компьютера ПК0. Пропингуйте с него остальные компьютеры сети. Компьютеры ПК1 и ПК2 доступны, а компьютеры ПК3 и ПК4 не доступны. Все пять компьютеров теоретически должны находится в одной подсети 10.0.0.0/8 и видеть друг друга, на практике они находятся в разных виртуальных локальных сетях и поэтому не могут взаимодействовать между собой.

Настройка VLAN на двух коммутаторах Cisco

Создайте сеть, логическая топология которой представлена на рисунке 6. Компьютеры соединены коммутатором Cisco 2950-24. В таблице 2 приведены адреса компьютеров.

VLAN



VLAN

Рисунок 6 Схема сети

Таблица 2

Компьютер	IP адрес	Коммутатор	Порт коммутатора	Вилан
2_1	10.0.0.1/8	Switch1	1	VLAN 20
2_2	10.0.0.3/8	Switch2	1	VLAN 20
3_1	10.0.0.2/8	Switch1	2	VLAN 30
3_2	10.0.0.4/8	Switch2	2	VLAN 30

Далее будем считать, что 2_1 и 2_2 находятся в VLAN 20, а 3_1 и 3_2 находятся в VLAN 30.

Проверим связность получившейся сети. Для этого пропингуем с 2_1 все остальные компьютеры. Поскольку пока в сети нет разделения на VLAN, то все компьютеры должны быть доступны.

Теперь займемся настройкой VLAN 20 и VLAN30, чтобы структурировать сети на коммутаторах.

Перейдите к настройке коммутатора Switch1. Откройте его консоль. В открывшемся окне перейдите на вкладку CLI, войдите в

привилегированный режим и настройте VLAN 20 и VLAN30 согласно таблице 2.

Создайте на коммутаторе VLAN 20. Для этого в привилегированном режиме выполните следующую команду:

Switch1#**conf t**
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#

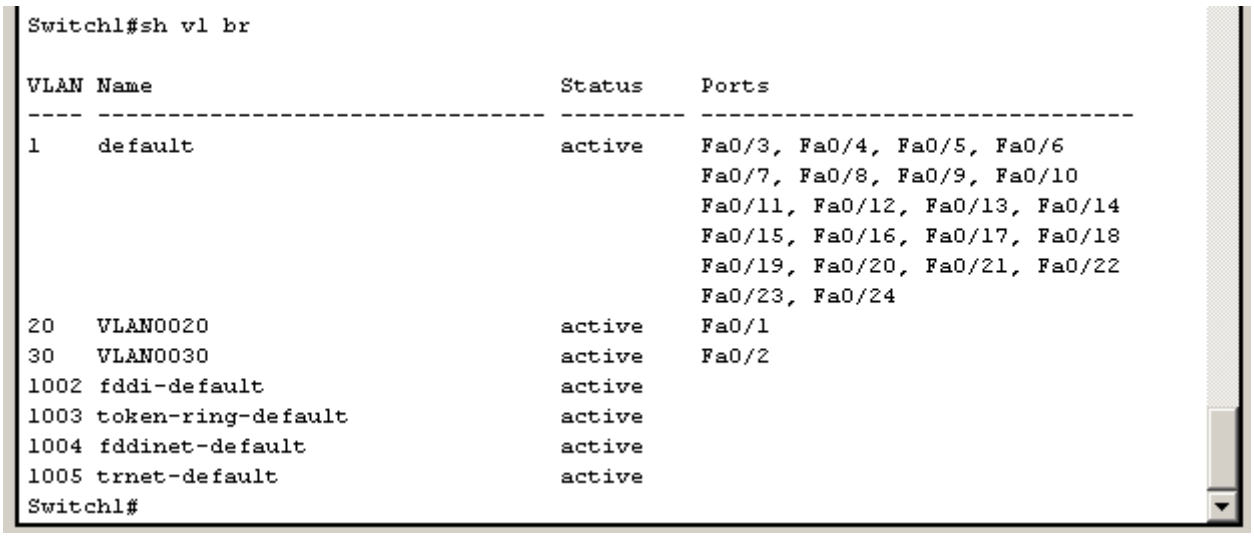
Для перехода в режим конфигурации и настройте VLAN 20 и VLAN 30 следующим образом:

Switch1(config)#**vlan 20**
Switch1(config)#**interface fastEthernet 0/1**
Switch1(config-if-range)#**switchport mode access**
Switch1(config-if-range)#**switchport access vlan 20**
Switch1(config-if-range)#**exit**
Switch1(config)#**vlan 30**
Switch1(config)#**interface fastEthernet 0/2**
Switch1(config-if-range)#**switchport mode access**
Switch1(config-if-range)#**switchport access vlan 30**

Просмотрите информацию о существующих на коммутаторе VLAN-ах командой:

Switch1#**sh vl br**

У вас должен получится результат, показанный на рисунке 7.

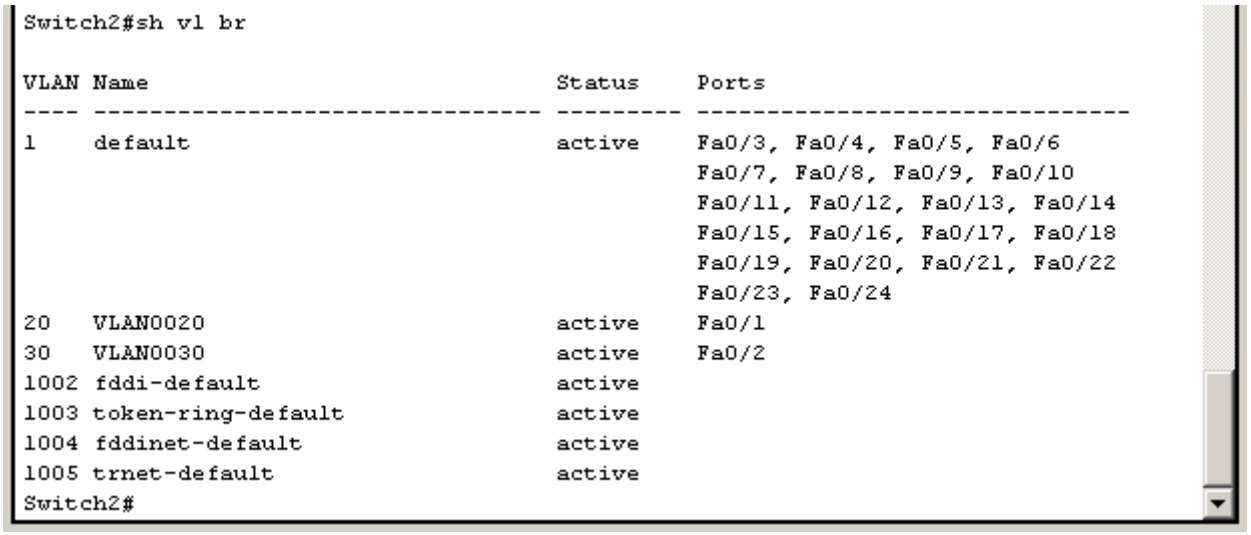


```
Switch1#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
20   VLAN0020                          active    Fa0/1
30   VLAN0030                          active    Fa0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch1#
```

Рисунок 7 - Конфигурация Switch1.

Аналогичным образом сконфигурируйте Switch2 (рисунок 8).



```
Switch2#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
20   VLAN0020                          active    Fa0/1
30   VLAN0030                          active    Fa0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch2#
```

Рисунок 8 Конфигурация Switch2

Поскольку в данный момент нет обмена информации о виланах, то компьютеры будут пинговать только себя.

Теперь организуем магистраль обмена между коммутаторами. Для этого настроим третий порт на каждом коммутаторе как транковый.

Войдите в консоль коммутатора Switch1 и задайте транковый порт:

Switch1>**en**

Switch1#**conf t**

Switch1(config)#**interface fastEthernet 0/3**

Switch1(config)#**switchport mode trunk**

Switch1(config)#**no shutdown**
Switch1(config)#**exit**

Откройте конфигурацию коммутатора на интерфейсе FastEthernet0/3 и убедитесь, что порт транковый (рисунок 9).

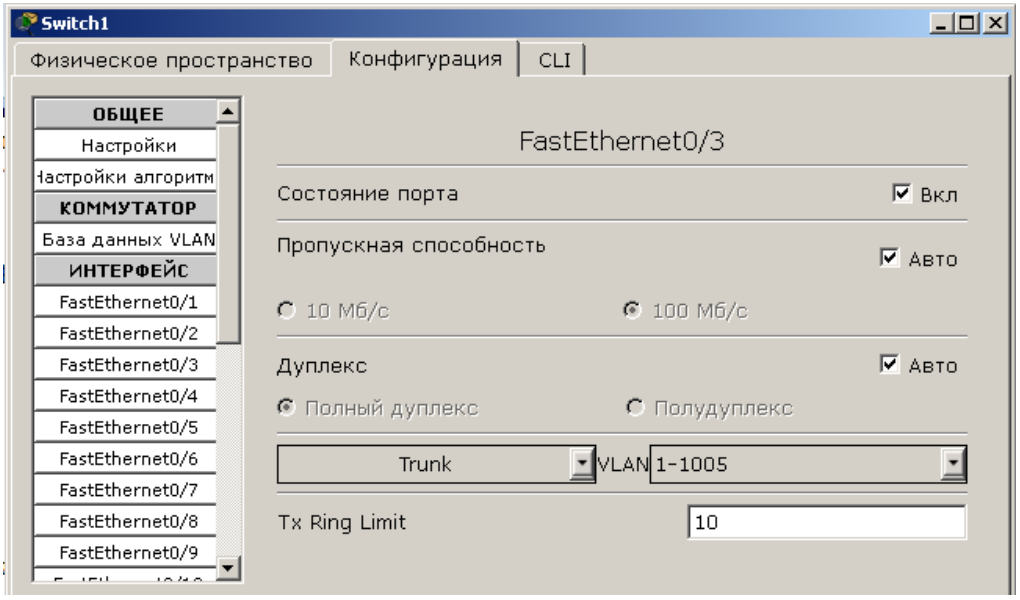


Рисунок 9 Конфигурация интерфейса FastEthernet0/3

На коммутаторе Switch2 интерфейс FastEthernet0/3 автоматически настроится как транковый.

Теперь компьютеры, входящие в один виллан должны пинговаться. У вас должна появиться связь между компьютерами 2_1 и 2_2, а так же между 3_1 и 3_2. Но компьютеры в другом виллане будут недоступны.

Сохраните схему сети.

Теперь объединим две виртуальные сети с помощью маршрутизатора.

Добавьте в схему сети маршрутизатор, как показано на рисунке 10. Маршрутизатор соединен с интерфейсами **fastEthernet 0/4** коммутаторов.

Разобьем нашу сеть 10.0.0.0 на две подсети: 10.2.0.0 и 10.3.0.0. Для этого поменяйте IP адреса и маску подсети на 255.255.0.0, как указано в таблице 3.

Таблица 3.

Компьютер	IP адрес	Коммутатор	Порт коммутатора	Вилан
2_1	10.2.0.1/16	Switch1	1	VLAN 20
2_2	10.2.0.3/16	Switch2	1	VLAN 20
3_1	10.3.0.2/16	Switch1	2	VLAN 30
3_2	10.3.0.4/16	Switch2	2	VLAN 30

Компьютеры должны пинговаться в пределах одного вилана и одной подсети.

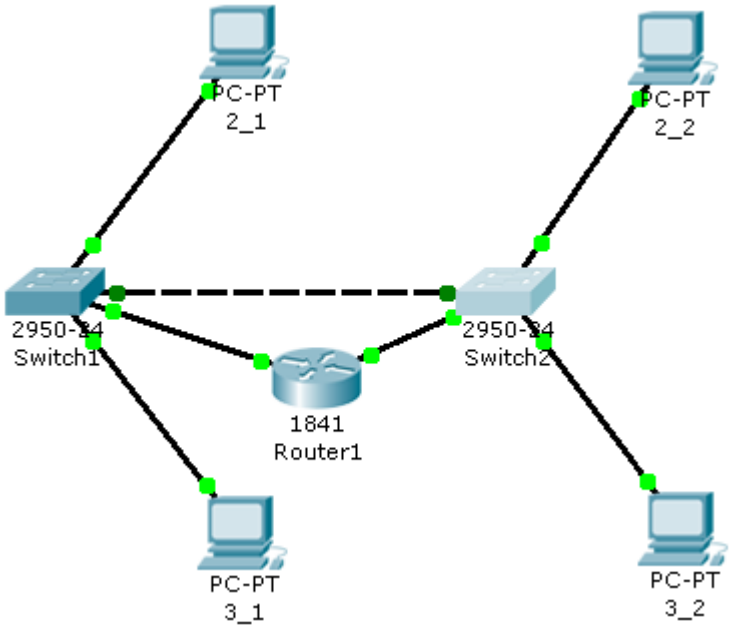


Рисунок 10 Схема сети

Обозначим на коммутаторах интерфейсы, подсоединенные к маршрутизатору в виртуальные сети.

Войдите в конфигурацию первого коммутатора Switch1 и задайте параметры четвертого порта:

Switch1(config)#**interface fastEthernet 0/4**

Switch1(config-if)#**switchport access vlan 20**

Проверьте настройки первого коммутатора Switch1 (рисунок 11):

```
Switch1#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
20   VLAN0020                          active    Fa0/1, Fa0/4
30   VLAN0030                          active    Fa0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch1#
```

Рисунок 11 Настройки коммутатора Switch1

Войдите в конфигурацию второго коммутатора Switch2 и задайте параметры четвертого порта:

Switch2(config)#**interface fastEthernet 0/4**

Switch2(config-if)#**switchport access vlan 30**

Проверьте настройки второго коммутатора Switch2 (рисунок 12):

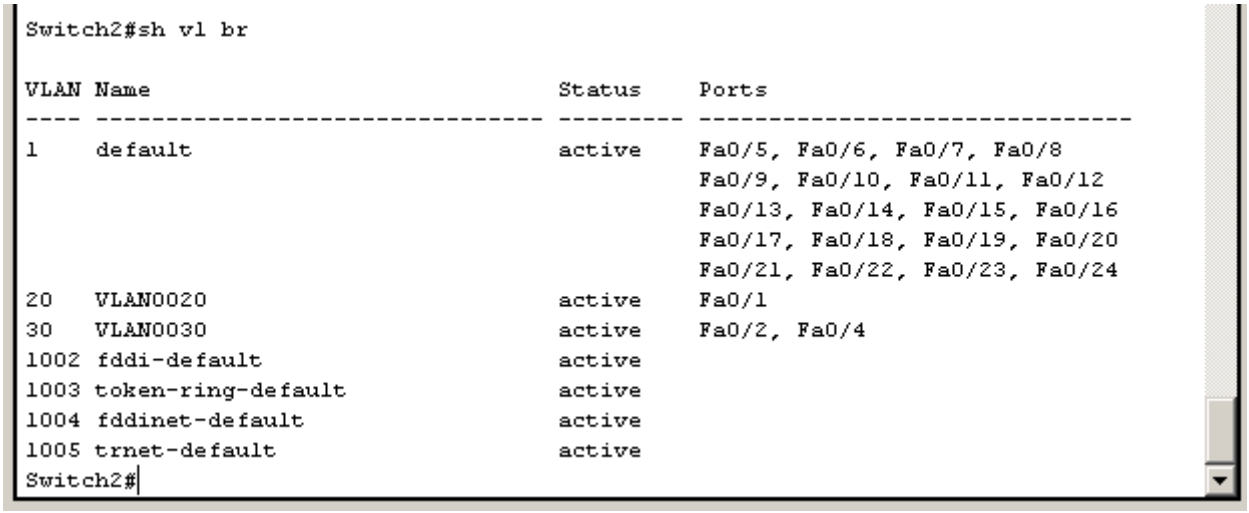


Рисунок 12 Настройки коммутатора Switch2

Войдите в конфигурацию маршрутизатора и настройте IP адреса на маршрутизаторе:

Router1(config-if)#**interface fa0/0**
Router1(config-if)#**ip address 10.2.0.254 255.255.0.0**
Router1(config-if)#**no shutdown**
Router1(config-if)#**interface fa0/1**
Router1(config-if)#**ip address 10.3.0.254 255.255.0.0**
Router1(config-if)#**no shutdown**

С этого момента мы установили маршрутизацию между двумя подсетями. Осталось установить шлюзы на компьютерах (таблица 4).

Таблица 4

Компьютер	Gataway
2_1	10.2.0.254
2_2	10.2.0.254
3_1	10.3.0.254
3_2	10.3.0.254

Проверьте доступность компьютеров в сети. Теперь все компьютеры должны быть доступны и все адреса должны пинговаться.

Настройка VLAN в корпоративной сети

Создайте следующую схему сети, представленную на рисунке 13.

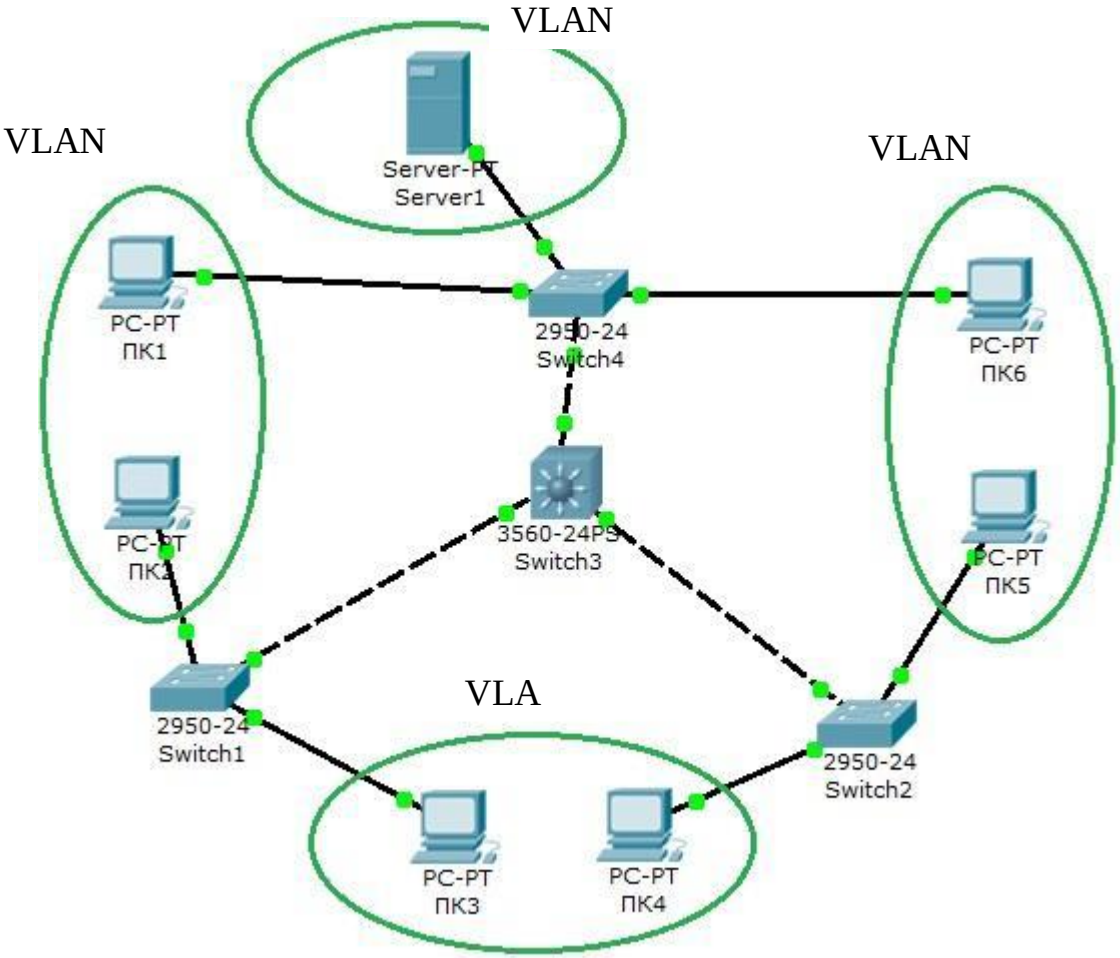


Рисунок 13 Схема корпоративной сети

Состав сети:

- три коммутатора второго уровня распределения 2950-24 (Switch1, Switch2, Switch4);

- центральный коммутатор третьего уровня 3560-24PS (Switch3), выполняющий роль роутера;

- сервер (Server1);

- три подсети по два узла в каждой

Задача:

Для любого вилана могут быть доступны только узлы этого же вилана и сервер Server1.

В таблице 5 и 6 приведены данные для установки параметров компьютеров и коммутаторов.

Таблица 5. Конфигурация компьютеров.

Компьютер	IP адрес	Коммутатор	Порт коммутатора	VLAN
ПК1	10.11.0.11/16	Switch4	4	VLAN 11
ПК2	10.11.0.2/16	Switch1	1	VLAN 11
ПК3	10.13.0.3/16	Switch1	2	VLAN 13
ПК4	10.13.0.4/16	Switch2	1	VLAN 13
ПК5	10.12.0.5/16	Switch2	2	VLAN 12
ПК6	10.12.0.6/16	Switch4	2	VLAN 12
Server1	10.10.0.7/16	Switch4	1	VLAN 10

Таблица 6. Связь коммутаторов по портам.

Порт центрального коммутатора Switch3	Порт коммутатора второго уровня распределения
1	Switch1 – 3 порт
2	Switch4 – 3 порт
3	Switch2 – 3 порт

После настройки всех коммутаторов установите самостоятельно шлюзы на всех компьютерах и сервере.

Сконфигурируйте центральный коммутатор:

Этап 1.

Перейдите к конфигурации центрального коммутатора Switch3 и создайте на нем базу VLAN.

1. Создайте VLAN 10:
Switch3>**en**

Switch3#**conf t**

Switch3(config)#**vlan 10**

Switch3(config-vlan)#**exit**

2. Создайте VLAN 11, VLAN 12 и VLAN 13.

3. Настройте протокол VTP в режиме сервера:

Switch3(config)#**vtp domain HOME**

Switch3(config)#**vtp password HOME**

Switch3(config)#**vtp mode server**

4. Просмотрите информацию о конфигурации VTP:

Switch#**sh vtp status**

5. Настройте все интерфейсы на транк:

Switch3(config)#**int fa0/1**
Switch3(config-if)#**switchport mode trunk**
Switch3(config-if)#**exit**

и повторите эти настройки для второго и третьего интерфейсов.

Этап 2.

Перейдите к конфигурации коммутатора Switch4 и переведите его в режим client:

1. Создайте на коммутаторе VLAN 10 и задайте в нем порт 1 как access порт:

Switch4>**en**

Switch4#**conf t**

Switch4(config)#**vlan 10**

Switch4(config-vlan)#**exit**

Switch4(config)#**int fa0/1**
Switch4(config-if)#**switchport access vlan 10**

Switch4(config-if)#**switchport mode access**

Switch4(config-if)#**no shut**

2. Создайте на коммутаторе VLAN 11 и задайте в нем порт 4 как access порт.

3. Создайте на коммутаторе VLAN 12 и задайте в нем порт 2 как access порт.

4. Переведите коммутатор в режим clint:

Switch4(config)#**vtp domain HOME**

Switch4(config)#**vtp password HOME**

Switch4(config)#**vtp mode client**

ВАЖНО! При вводе имени домена и пароля соблюдайте нужный регистр.

Этап 4.

Перейдите к конфигурации коммутатора Switch1 и выподните следующие настройки:

.

1. Создайте на коммутаторе VLAN 11 и задайте в нем порт 1 как access порт.

2. Создайте на коммутаторе VLAN 13 и задайте в нем порт 2 как access порт.

3. Переведите коммутатор в режим client.

Этап 5.

Перейдите к конфигурации коммутатора Switch2.

1. Создайте на коммутаторе VLAN 12 и задайте в нем порт 2 как access порт.

2. Создайте на коммутаторе VLAN 13 и задайте в нем порт 1 как access порт.

3. Переведите коммутатор в режим client.

Этап 6.

Проверьте работоспособность сети на канальном уровне модели OSI.

После установки всех настроек таблица VLAN разойдется по коммутаторам с помощью протокола VTP.

В результате компьютеры, расположенные в одном виллане, будут доступны друг для друга, а другие компьютеры недоступны. Проверьте связь командой PING между следующими парами компьютеров:

- ПК1 – ПК2;

- ПК3 – ПК4;

- ПК5 – ПК6.

Если Вы все сделали правильно, то ping между парами пройдет, если нет – проверьте следующие установки:

- транковыми портами являются: на Switch3 все порты, на Switch1, Switch2 и Switch4 – третий порт;

- соединения интерфейсов на коммутаторах;

- названия и пароли доменов на каждом коммутаторе (команда sh vtp status);

- привязку интерфейсов к вилланам на коммутаторах (команда sh vl br).

Этап 7.

Настройка маршрутизации на центральном коммутаторе.

Создадим интерфейсы для каждого VLAN.

Настройка интерфейса для vlan 10 (шлюз по умолчанию):

Switch3(config)#**int vlan 10**
Switch3(config-if)#**ip address 10.10.0.1 255.255.0.0**
Switch3(config-if)#**no shut**
Switch3(config-if)#**exit**

Повторите эти настройки для каждого VLAN, задавая адрес IP: 10.[VLAN].0.1 и маску /16.

После этого зайдите в настройки каждого компьютера и установите нужный шлюз по умолчанию. Например для ПК1 – 10.11.0.1.

Включите маршрутизацию командой:

Switch3(config)#**ip routing**
Этап 8.

Проверьте работоспособность сети на сетевом уровне модели OSI.

После включения маршрутизации все компьютеры будут доступны с любого хоста.

Этап 9.

Выполним основную задачу работы: для любого вилана могут быть доступны только узлы этого же вилана и сервер Server1.

Для этого введем следующие ограничения на трафик сети:

1 - Разрешить пакеты от любого хоста к серверу.

2 - Разрешить пакеты от сервера до любого хоста.

3 – Трафик от одной подсети к этой же подсети разрешить.

4 – Правило по умолчанию: запретить всё остальное.

Ограничения на трафик сети задаются с помощью команды фильтрации **access-list**. Данная команда задает критерии фильтрации в списке опций разрешения и запрета, называемом списком доступа. Списки доступа имеют два правила: **permit** – разрешить и **deny** – запретить. Данные правила либо пропускают пакет дальше по сети, либо блокируют его доступ.

Открываем центральный коммутатор (Switch3) и меняем его конфигурацию с помощью команды фильтрации **access-list**:

Switch3(config)#**ip access-list extended 100**
(создается расширенный список доступа под номером 100)
Switch3(config-ext-nacl)#**permit ip any 10.10.0.0 0.0.0.255**
Switch3(config-ext-nacl)#**permit ip 10.10.0.0 0.0.0.255 any**
(разрешается доступ к сети 10.10.0.0/24)

Switch3(config-ext-nacl)#**permit ip 10.11.0.0 0.0.0.255 10.11.0.0 0.0.0.255**
Switch3(config-ext-nacl)#**permit ip 10.12.0.0 0.0.0.255 10.12.0.0 0.0.0.255**
Switch3(config-ext-nacl)#**permit ip 10.13.0.0 0.0.0.255 10.13.0.0 0.0.0.255**
(разрешается: доступ из сети 10.11.0.0/24 в эту же сеть;
доступ из сети 10.12.0.0/24 в эту же сеть;
доступ из сети 10.13.0.0/24 в эту же сеть).
Switch3(config-ext-nacl)#**exit**

Теперь этот access-list наложим на конкретный интерфейс и применим ко всем VLAN-ам на входящий трафик (опция **in –** на входящий трафик, **out –** на исходящий трафик):

Switch3(config)#**int vlan 10**
Switch3(config-if)#**ip access-group 100 in**
Этот шаг повторяем для каждого из VLAN-ов.

В результате получим:

для любого вилана могут быть доступны только узлы этого же вилана и сервер Server1.

2.1.4 Требования и состав отчёта

1. Отчёт должен быть выполнен на листах размера А4.

2. Отчёт должен начинаться с титульного листа с названием вуза и факультета, номером и названием лабораторной работы, вариантом, ФИО студента, № группы, ФИО преподавателя, городом и годом.

3. В отчёте нужно кратко описать задание, показать основные этапы решения задачи, сформулировать выводы.

4. Отчёт предоставить в бумажном или электронном виде (записать на флэш-накопитель и продублировать на электронную почту).

2.1.5 Вопросы и задания

1. Перечислите современные угрозы сетевой безопасности.
2. Как осуществляется назначение административных ролей?
3. Каким образом применение виртуальных локальных сетей позволяет сказывается на защищенности сети?
4. Каким образом применение виртуальных локальных сетей уменьшает долю широковещательного трафика в сети?
5. Перечислите наиболее распространенные сетевые атаки.
6. Перечислите основные методы противодействия сетевым атакам.
7. Опишите методику противодействия спуфингу протокола разрешения адреса.
8. При защите отчёта надо уметь отвечать на вопросы по постановке задачи, этапам ее решения, использованным инструментам, справочникам и нормативным документам.

2.2 Лабораторная работа № 2 Технологии фильтрации трафика

2.3.1 Цели и задачи

Целью работы является ознакомление с технологией фильтрации трафика, а также выработка навыков поиска и устранения возможных неполадок в применении списков контроля доступа, и взаимодействия сетевых устройств при их использовании.

Задачи:

1. Изучение стандартных списков контроля доступа.
2. Изучение расширенных списков контроля доступа.

3. Устранение неполадок в сети при использовании списков контроля доступа.

2.3.2 Теоретические положения

Теоретические положения отражены в руководствах по конфигурированию рассматриваемых технологий компании Cisco Systems, расширенной версии методических указаний к лабораторной работе.

2.3.3 Порядок выполнения работы

1. Построение сети с заданной топологией.
2. Настройка базовых параметров сетевого оборудования.
3. Конфигурирование стандартных списков контроля доступа.
4. Конфигурирование расширенных списков контроля доступа.
5. Проверка межсетевого взаимодействия при использовании списков контроля доступа.
6. Интерпретация результатов межсетевого взаимодействия.
7. Конфигурирование учета нарушений правил списков доступа.
8. Устранение неполадок в сети при использовании списков контроля доступа.

2.3.5 Требования и состав отчёта

1. Отчёт должен быть выполнен на листах размера А4.

2. Отчёт должен начинаться с титульного листа с названием вуза и факультета, номером и названием лабораторной работы, вариантом, ФИО студента, № группы, ФИО преподавателя, городом и годом.

3. В отчёте нужно кратко описать задание, показать основные этапы решения задачи, сформулировать выводы.

4. Отчёт предоставить в бумажном или электронном виде (записать на флэш-накопитель и продублировать на электронную почту).

2.3.6 Вопросы и задания

1. Поясните принципы работы списков контроля доступа.

2. Поясните различия стандартных и расширенных списков контроля доступа.

3. Опишите процедуру создания именованных списков контроля доступа.

4. Поясните основные принципы конфигурирования списков контроля доступа.

7. Перечислите возможные неисправности при использовании списков контроля доступа и методы их поиска.

8. Повторить и закрепить информацию из методических рекомендаций компании Cisco Systems.

9. При защите отчёта надо уметь отвечать на вопросы по постановке задачи, этапам ее решения, использованным командам, принципам функционирования рассматриваемых технологий.

2.3 Лабораторная работа № 3 Конфигурирование межсетевого экрана

2.3.1 Цели и задачи

Целью работы является изучение вопросов, связанных с конфигурированием межсетевого экрана, а также выработка навыков поиска и устранения возможных неполадок в функционировании межсетевого экрана, и взаимодействия сетевых устройств при его использовании.

Задачи:

1. Построение сети с заданной топологией.

2. Изучение технологии CBAC.

3. Конфигурирование брандмауэра зональной политики.

4. Устранение неполадок в сети при использовании списков контроля доступа.

2.3.2 Теоретические положения

Теоретические положения отражены в руководствах по конфигурированию рассматриваемых технологий компании Cisco Systems, расширенной версии методических указаний к лабораторной работе.

2.3.4 Порядок выполнения работы

1. Построение сети с заданной топологией.
2. Настройка базовых параметров сетевого оборудования.
3. Конфигурирование CBAC.
4. Конфигурирование зон межсетевого экрана.
5. Распределение сетевых интерфейсов по зонам.
6. Конфигурирование политик фильтрации трафика.
7. Проверка межсетевого взаимодействия.
8. Интерпретация результатов межсетевого взаимодействия.
9. Устранение неполадок в функционировании межсетевого экрана.

2.3.5 Требования и состав отчёта

1. Отчёт должен быть выполнен на листах размера А4.

2. Отчёт должен начинаться с титульного листа с названием вуза и факультета, номером и названием лабораторной работы, вариантом, ФИО студента, № группы, ФИО преподавателя, городом и годом.

3. В отчёте нужно кратко описать задание, показать основные этапы решения задачи, сформулировать выводы.

4. Отчёт предоставить в бумажном или электронном виде (записать на флэш-накопитель и продублировать на электронную почту).

2.3.6 Вопросы и задания

1. Поясните основные принципы инспектирования трафика.

2. Поясните основные принципы технологии CBAC.

3. Перечислите основные функции межсетевого экрана.

4. Перечислите основные особенности брандмауэра зональной политики.

5. Опишите, каким образом осуществляется конфигурирование зон межсетевого экрана.

6. Опишите процесс распределения сетевых интерфейсов по зонам.

7. Опишите, каким образом осуществляется конфигурирование политик фильтрации трафика.

8. Повторить и закрепить информацию из методических рекомендаций компании Cisco Systems.

9. При защите отчёта надо уметь отвечать на вопросы по постановке задачи, этапам ее решения, использованным командам, принципам функционирования рассматриваемых технологий.

2.4 Лабораторная работа № 4 Организация виртуальной частной сети

2.4.1 Цели и задачи

Цель работы : изучить возможности программ OpenVPN и SoftEther VPN, построить виртуальную частную сеть по типу «клиент – сервер» [17]

Задачи:

1. Ознакомление с общими принципами создания VPN
2. Изучение программы OpenVPN.
3. Настройка сервера OpenVPN

4. Настройка клиента OpenVPN
5. Изучение программы SoftEtherVPN
6. Настройка клиента и сервера SoftEtherVPN
7. Тестирование VPN.

2.4.2 Порядок выполнения работы

Порядок выполнения работы отражен в пособии [17], стр. 18-25.

2.4.3 Требования и состав отчёта

1. Отчёт должен быть выполнен на листах размера А4.

2. Отчёт должен начинаться с титульного листа с названием вуза и факультета, номером и названием лабораторной работы, вариантом, ФИО студента, № группы, ФИО преподавателя, городом и годом.

3. В отчёте нужно кратко описать задание, показать основные этапы решения задачи, сформулировать выводы.

4. Отчёт предоставить в бумажном или электронном виде (записать на флэш-накопитель и продублировать на электронную почту).

2.4.4 Вопросы и задания

1. Повторить и закрепить информацию о VPN из пособий, приведенных в списке литературы.

2. Как осуществляется установка SSL – соединения ?

3. Как осуществляется выбор алгоритма шифрования в OpenVPN ?

4. Какие функции реализует SoftEther по администрированию VPN ?

5. При защите отчёта надо уметь отвечать на вопросы по постановке задачи, этапам ее решения, использованным инструментам, справочникам и нормативным документам.

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ВЫПОЛНЕНИЮ КОНТРОЛЬНОЙ РАБОТЫ

3.1. Задание на контрольную работу и методические указания по ее выполнению

На контрольную работу студенту выдается индивидуальное задание (по вариантам), заключающееся в организации безопасного взаимодействия офисов организации. Работа выполняется в письменной форме в течение 10 недель с момента выдачи задания. Контрольный срок сдачи – последний месяц семестра. Правила оформления контрольной работы

- контрольная работа оформляется в редакторе MS Word / OpenOffice (*.doc, *.docx, *.odt);
- листы формата А4, ориентация книжная;
- поля: левое – 2 см, остальные – по 1 см;
- шрифт – Times New Roman;
- размер шрифта 14 pt;
- междустрочный интервал – 1,5;
- абзацный отступ – 1,25 см;
- нумерация страниц сквозная, номер на первой странице не ставится;
- в конце работы необходим список использованной литературы согласно ГОСТ Р 7.0.5 – 2008;
- объем работы зависит от степени раскрытия основных пунктов контрольной работы.

3.2. Примерное содержание контрольной работы

Примерное содержание контрольной работы

1. Титульный лист.
2. Формулировка варианта задания.

3. Основная часть, включающая:

1) Схема сети организации с указанием адресов и номеров портов.

2) Тексты конфигурационных файлов оборудования.

3) Последовательное описание процесса конфигурирования сетевых устройств.

4) Список использованных источников (включая источники Интернет).

3.3. Примерные варианты заданий контрольной работы

Задание выполняется по вариантам. Организация состоит из 2 офисов, между которыми через промежуточные узлы осуществляется маршрутизация на основе протокола OSPF. Необходимо выполнить проектирование топологии сети организации, схематично показать расположение конечных устройств, маршрутизаторов, коммутационного оборудования с указанием портов, выполнить настройку сетевого преобразования адресов, организовать взаимодействие офисов с помощью организованного туннеля VPN, настроить списки контроля доступа.

ЗАКЛЮЧЕНИЕ

В рамках курса на практических примерах и в лабораторном практикуме рассмотрены методы и средства защиты инфокоммуникационных систем искусственного интеллекта и способы их применения в современных мультисервисных сетях.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА ПО КУРСУ

1) Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837

2) Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — 2-е изд., испр. — Санкт-Петербург : Лань, 2020. — 124 с. — ISBN 978-5-8114-4404-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/133924

3) Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131717

4) Страшун, Ю. П. Технические средства автоматизации и управления на основе IIoT/IoT : учебное пособие / Ю. П. Страшун. — Санкт-Петербург: Лань, 2020. — 76 с. — ISBN 978-5-8114-5018-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/143701

5) Ли, П. Архитектура интернета вещей / П. Ли ; перевод с английского М. А. Райтман. — Москва : ДМК Пресс, 2019. — 454 с. — ISBN 978-5-97060-672-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/112923. — Режим доступа: для авториз. пользователей.

6) Смычёк, М. А. Технологические сети и системы связи : учебное пособие / М. А. Смычёк. — Вологда : Инфра-Инженерия, 2019. — 400 с. — ISBN 978-5-9729-0338-2. — Текст : электронный // Лань : электронно-

библиотечная система. — URL: https://e.lanbook.com/book/124698. — Режим доступа: для авториз. пользователей.

7) Эделман, Д. Автоматизация программируемых сетей : руко-водство / Д. Эделман, С. С. Лоу, М. Осуолт ; перевод с английского А. В. Снастина. — Москва : ДМК Пресс, 2019. — 616 с. — ISBN 978-5-97060-699-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/123708

8) Применение межсетевого экрана D-Link DFL-860E для безопасности компьютерных сетей : учебно-методическое пособие / А. В. Пролетарский, А. Д. Пономарев, А. А. Митьковский [и др.]. — Москва : МГТУ им. Н.Э. Баумана, 2019. — 241 с. — ISBN 978-5-7038-5022-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/172827

9) Васин, Н. Н. Технологии пакетной коммутации : учебник / Н. Н. Васин. — Санкт-Петербург : Лань, 2019. — 284 с. — ISBN 978-5-8114-3866-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125735

10) Технологии создания интеллектуальных устройств, подключенных к интернет : учебное пособие / А. В. Приемышев, В. Н. Крутов, В. А. Треяль, О. А. Коршакова. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 100 с. — ISBN 978-5-8114-2310-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/169110

11) Мошак, Н. Н. Защищенные информационные системы : учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180099

12) Журавлев, А. Е. Инфокоммуникационные системы. Программное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В.

Иванищев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 376 с. — ISBN 978-5-8114-8515-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176658. — Режим доступа: для авториз. пользователей.

13) Журавлев, А. Е. Инфокоммуникационные системы. Аппаратное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 392 с. — ISBN 978-5-8114-8514-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/ — Режим доступа: для авториз. пользователей.

14) Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А. И. Белоус. — Вологда : Инфра-Инженерия, 2020. — 644 с. — ISBN 978-5-9729-0512-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/148386

15) Проектирование и моделирование сетей связи. Лабораторный практикум : учебное пособие / В. Н. Тарасов, Н. Ф. Бахарева, С. В. Малахов, Ю. А. Ушаков. — Санкт-Петербург : Лань, 2019. — 240 с. — ISBN 978-5-8114-3298-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111917 . — Режим доступа: для авториз. пользователей.

16) Скворцова, Т. И. Компьютерные коммуникации и сети : учебно-методическое пособие / Т. И. Скворцова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163825. — Режим доступа: для авториз. пользователей.

17) Бизин, Д. И. Виртуальные частные сети (VPN) : учебно-методическое пособие / Д. И. Бизин, О. Н. Коваленко. — Омск : ОмГУПС,

2019. — 37 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165629

18) Бизин, Д. И. Конфигурирование маршрутизаторов в глобальных вычислительных сетях : учебно-методическое пособие / Д. И. Бизин, О. Н. Коваленко. — Омск : ОмГУПС, 2020. — 40 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165630

Учебное издание

Андрей Николаевич Земцов

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ОБЛАЧНОЙ И СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Учебное пособие

Волгоградский государственный технический университет.
400005, г. Волгоград, просп. В. И. Ленина, 28, корп. 1.