МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности


# КОНФИГУРИРОВАНИЕ КОММУТАТОРОВ

Методические рекомендации по выполнению лабораторной работы №2
для студентов направления подготовки бакалавриата
10.03.01«Информационная безопасность»

Курск 2017

УДК 621.(076.1)

Составитель: А.Г. Спеваков

Рецензент

Кандидат технических наук, доцент кафедры
«Информационная безопасность» И.В. Калуцкий

**Конфигурирование коммутаторов** [Текст] : методические рекомендации по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: А.Г. Спеваков. – Курск, 2017. – 14 с.: ил. 3. – Библиогр.: с. 14.

Содержат сведения по вопросам работы в программном продукте Cisco Packet Tracer. Указывается порядок выполнения лабораторной работы, правила содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки бакалавриата 10.03.01 «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 0,81. Уч.-изд. л. 0,74. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

## 1.1 Конфигурирование паролей на подключение к устройству

Пароли обеспечивают некоторый уровень защиты коммутатора, предотвращающий неавторизованное подключение к нему. Коммутаторы Catalyst стандартно имеют два уровня парольной защиты: пользовательский и привилегированный. Для обеспечения защиты устройства следует применять аутентификацию пользователя с использованием локальной базы коммутатора и шифрование паролей.

Пароль уровня пользователя предотвращает доступ неавторизованных лиц к интерфейсу командной строки (CLI) из Telnet- или консольного сеанса. Он настраивается для каждой линии подключения отдельно с помощью команд **password**, параметром которой является устанавливаемый пароль, и **login** без параметров. Команда **login** обеспечивает процесс аутентификации пользователя и является обязательной для линий подключения

IOS-коммутаторов. До тех пор, пока пароль не будет установлен или в конфигурации линии будет отсутствовать команда **login**, подключение по Telnet невозможно. Выбор той или иной линии для ее конфигурирования осуществляется с помощью команды режима глобального конфигурирования:

**Switch(config)#line con 0** – для консольной линии,

**Switch(config)#line vty 0 4** – для линий виртуального терминала в диапазоне номеров с 0 по 4.

***ВЫПОЛНИТЬ!***

1. В текущей конфигурации найти команды, устанавливающие пароли на линии **con** и **vty.**
2. Установить пароль **console** для линии **con0.**
3. Выйти из сеанса консоли с помощью команды **logout** и войти в новый сеанс, используя введенные данные аутентификации.

Пароль привилегированного режима предотвращает доступ неавторизованных лиц к соответствующему режиму, в котором могут вноситься изменения в конфигурацию коммутатора и осуществляться другие функции администрирования. Он задается с помощью команды enable secret, обеспечивающей его шифрование, устаревшая команда enable password не шифрует пароль и

оставлена для совместимости с программным обеспечением ранних версий, причем во второй команде пароль должен отличаться от устанавливаемого в первой.

***ВЫПОЛНИТЬ!***

4. В текущей конфигурации найти команды, устанавливающие пароль для входа в привилегированный режим.

Для того чтобы пароли не хранились в файле конфигурации в открытом виде, можно использовать встроенную службу шифрования, но учтите, что она не обеспечивает их шифрование, а призвана лишь усложнить чтение паролей с экрана. Указанная служба запускается командой: **service password-encryption.**

***ВЫПОЛНИТЬ!***

5. Запустить службу шифрования паролей и в текущей конфигурации найти команды, устанавливающие пароли.

Как упоминалось ранее, предпочтительнее применять аутентификацию пользователя с использованием локальной базы данных коммутатора, для чего сначала создаются записи локальной базы пользователей с помощью команды:

**Switch(config)#username <имя> privilege <уровень> secret <пароль>.**

Затем для каждой линии подключения к коммутатору указывается команда **login** с параметром локальной аутентификации:

**Switch(config-line)#login local.**

***ВЫПОЛНИТЬ!***

6. Создать запись в локальной базе данных аутентификации о пользователе **admin** с уровнем привилегий **0** и секретным паролем **cisco**.

7. Настроить линии **con0** и **vty0** – **vty4** на использование локальной аутентификации. Для отмены старых паролей можно использовать команду:

**Switch(config-line)#no password.**

8. Выйти из сеанса консоли и войти в новый сеанс, используя введенные данные аутентификации.

9. В текущей конфигурации найти команды, устанавливающие действующие на коммутаторе пароли.

10. Сохранить текущую конфигурацию.

## 1.2 Конфигурирование статических VLAN

Сети VLAN – это определенные внутри коммутаторов широковещательные домены, позволяющие внутри устройства второго уровня управлять широковещательными, групповыми, одноадресными рассылками, а также одноадресными рассылками с неизвестным получателем. Каждая сеть VLAN создается в локальной базе данных используемого коммутатора. Если в коммутаторе отсутствуют сведения о какой-либо VLAN-сети, то он не может передавать трафик для этой сети VLAN через свои порты. VLAN-сети создаются по номерам, при этом существует два диапазона, пригодных для использования VLAN-номеров (обычный диапазон 1 ÷ 1000 и расширенный – 1025 ÷ 4096). При создании VLAN-сети можно также назначить ей определенные атрибуты, такие как имя, тип и операционное состояние. По умолчанию на коммутаторе существуют предопределенные VLAN – их нельзя удалить или переименовать. Все физические порты устройства по умолчанию находятся в VLAN1, называемой стандартной сетью VLAN (default VLAN), поэтому ее в целях безопасности и не рекомендуют использовать. Для вывода краткой информации о VLAN служит команда:

**Switch#show vlan-switch brief.**

***ВЫПОЛНИТЬ!***

11. Вывести на экран информацию о VLAN, существующих в коммутаторе по умолчанию.

Процесс создания статических VLAN-сетей включает в себя несколько этапов. Во-первых, необходимо в режиме глобального конфигурирования (рекомендуется вместо режима конфигурирования базы данных VLAN) установить протокол VTP в прозрачный режим функционирования:

**Switch#configure terminal**

**Switch(config)#vtp mode transparent.**

***ВЫПОЛНИТЬ!***

12. Установить протокол VTP в прозрачный режим функционирования.

Во-вторых, создать собственно сеть VLAN и по желанию указать ее имя с помощью последовательности команд:

**Switch(config)#vlan <номер> Switch(config-vlan)#name <имя> Switch(config-vlan)#end.**

***ВЫПОЛНИТЬ!***

13. Создать две виртуальных локальных сети: с номерами 10 и 20 без имени и одну с номером 99 и именем – **Administration**.

14. Вывести на экран информацию о VLAN, существующих в коммутаторе.

В-третьих, необходимо назначить в созданные VLAN-сети физические порты коммутатора, для чего перейти в режим конфигурирования выбранного интерфейса, а затем перевести его в режим доступа и назначить его в соответствующую VLAN-сеть. Например, с помощью следующих команд порт FastEthernet 0/5 назначается в VLAN с номером 50:

**Switch#configure terminal**

**Switch(config)#interface FastEthernet 1/5 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 50.**

***ВЫПОЛНИТЬ!***

15. Назначить порт fa0/24 в VLAN с именем Administration.

Для выполнения некоторой последовательности команд одновременно для нескольких портов коммутатора можно использовать выбор диапазона портов, осуществляемый с помощью команды: **Switch(config)#interface range FastEthernet 1/5 - 8**

***ВЫПОЛНИТЬ!***

16. Назначить порты fa1/1 – fa0/10 в VLAN 10.

17. Назначить порты fa1/11 – fa0/20 в VLAN 20.
18. Сохранить текущую конфигурацию.
19. Вывести на экран информацию о VLAN, существующих в коммутаторе.
20. Добавить в схему сети компьютеры (VPCS) PC1–PC5, подсоединить их к соответствующим портам коммутатора, назначить им IP-адреса согласно схеме, приведенной на рисунке 1.

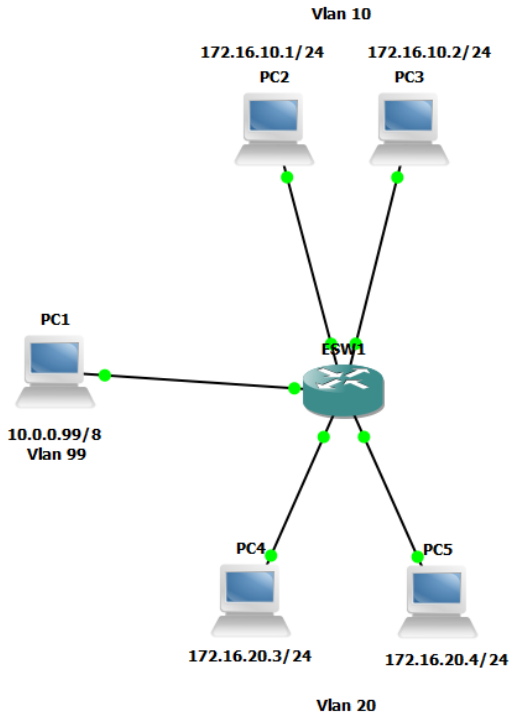


Рисунок 1 - Схема сети с VLAN99, VLAN10 и VLAN20

Состояние интерфейсов коммутатора на канальном и сетевом уровнях можно отобразить с помощью следующих команд соответственно (после параметра **interface** можно указать имя интерфейса для вывода информации только о его состоянии):

**Switch#show interface**
**Switch#show interface switchport.**
***ВЫПОЛНИТЬ!***

21. Используя приведенные команды, изучите параметры функционирования портов коммутатора, выясните различия в режимах работы портов, к которым подключены и не подключены компьютеры, а также портов, которые не настраивались Вами.

22. С помощью команды **ping** убедитесь, что в рамках VLANсетей взаимодействие между компьютерами возможно, а между сетями нет.

## 1.3 Конфигурирование IP-адреса административного управления

IP-адреса используются в коммутаторах второго уровня только в целях администрирования. Данный этап не является обязательным для функционирования коммутатора. В случае, если IP-адрес не был задан, единственным способом управления коммутатором является консольное соединение. Для конфигурирования IP-адреса используется последовательность команд:

**Switch(config)#interface vlan <номер> Switch(config-if)#ip address <адрес> <маска> Switch(config-if)#exit.**

***ВЫПОЛНИТЬ!***

23. Назначить административный IP-адрес 10.0.0.10/8 интерфейсу vlan99.
24. Сохранить текущую конфигурацию.
25. Используя команду **ping**, убедитесь, что PC0 может взаимодействовать с коммутатором.
26. Используя команду **telnet**, подключитесь с PC0 к коммутатору.

Для просмотра информации об административном интерфейсе можно использовать следующие команды:

**Switch#show interface vlan <номер> Switch#show ip interface vlan <номер>.**

***ВЫПОЛНИТЬ!***

27. Вывести информацию о настройках административного интерфейса vlan99.

Для просмотра краткой информации обо всех интерфейсах можно использовать команду:

**Switch#show ip interface brief.**

***ВЫПОЛНИТЬ!***

28. Вывести информацию об IP-интерфейсах коммутатора.

## 1.4 Работа с таблицей коммутации (CAM-таблица)

В таблице коммутации (switching table) содержатся MAC-адреса, номера VLAN и порты коммутатора, на которых эти адреса были определены автоматически или сконфигурированы статически. Просмотр содержимого таблицы коммутации осуществляется с помощью команд привилегированного режима:

**Switch#show mac-address-table** – все записи таблицы;

**Switch#show mac-address-table dynamic** – динамические записи;

**Switch#show mac-address-table static** – статических записи;

**Switch#show mac-address-table interface** – записи для указанного интерфейса.

***ВЫПОЛНИТЬ!***

29. Вывести содержимое таблицы коммутации коммутатора.
30. Выполнить команды **ping** на PC1 в адрес PC2 и на PC3 в адрес PC4.
31. Вывести содержимое таблицы коммутации коммутатора. Что изменилось?

Добавление статических записей в таблицу осуществляется с помощью команды режима глобального конфигурирования (пример приведен для MAC-адреса 11-11-22-22-33-33 в Vlan номер 99 на интерфейсе fa1/15):

**Switch(config)#mac-address-table static**
**1111.2222.3333 vlan 99 int fa1/15.**

***ВЫПОЛНИТЬ!***

32. Добавить статические записи о компьютерах PC2 и PC4.
33. Выполнить команды **ping** на PC2 в адрес PC3 и на PC4 в адрес PC5.
34. Вывести содержимое таблицы коммутации коммутатора.

Удаление динамических записей из таблицы коммутации осуществляется с помощью команды привилегированного режима: **Switch#clear mac-address-table dynamic,** а статических записей – с

помощью команды режима глобального конфигурирования (пример приведен для MAC-адреса 11-11-22-2233-33 в Vlan номер 99 на интерфейсе fa1/15):

**Switch(config)#no mac-address-table static 1111.2222.3333 vlan 99 int fa1/15.**

Очистка таблицы коммутации осуществляется с помощью команды привилегированного режима:

**Switch#clear mac-address-table.**

***ВЫПОЛНИТЬ!***

35. Удалить статическую запись о компьютере PC2 и вывести содержимое таблицы коммутации коммутатора.

36. Удалить динамические записи из таблицы коммутации и вывести содержимое таблицы коммутации коммутатора.

37. Очистить таблицу коммутации, убедиться в том, что в ней нет записей.

***ВЫПОЛНИТЬ!***

38. Справа от имеющейся схемы создать сеть, изображенную на рисуноке 2. Интерфейсы коммутатора FastEthernet с номерами с 1 по 5 назначить в VLAN10, с 6 по 10 – в VLAN20 и подключить HUB1 к Fa1/1, Server0 – к Fa1/2, Server1 – к Fa1/6.

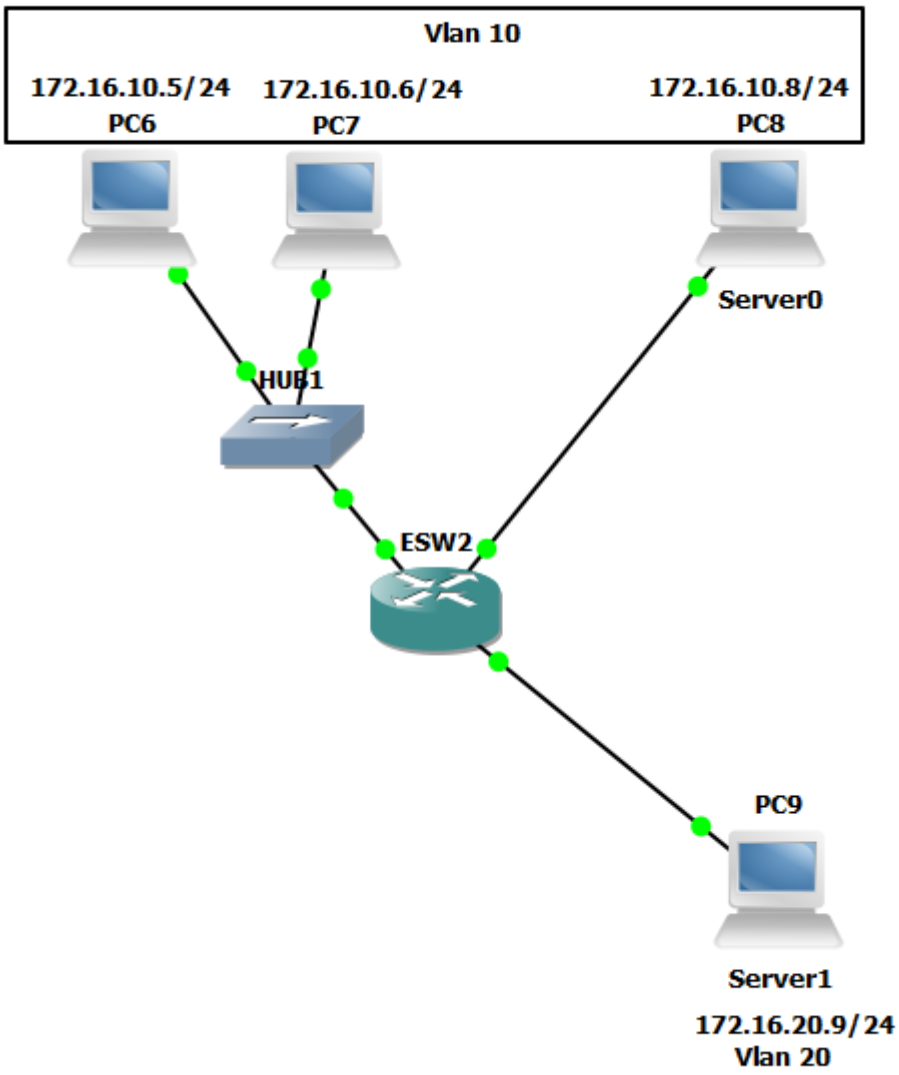


Рисунок 2 - Расширение имеющейся сети

1.6 Конфигурирование магистральных (транковых) линий

Дело в том, что VLAN-сети являются локальными в базе данных каждого коммутатора, и информация о принадлежности узлов к ним не передается между коммутаторами. Магистральные каналы (trunk links – транковые линии) обеспечивают VLAN-идентификацию для кадров, перемещающихся между коммутаторами сети. В коммутаторах фирмы Cisco имеются два механизма Ethernet-транкинга: протокол ISL и стандарт IEEE 802.1Q. Некоторые типы коммутаторов способны согласовывать параметры магистральных каналов. Магистральные каналы

стандартно транспортируют трафик от всех VLAN-сетей к коммутатору и от него, но могут быть настроены на поддержку трафика только определенной VLAN-сети.

***ВЫПОЛНИТЬ!***

39. Соединить ESW1 и ESW2 друг с другом, используя для этого их интерфейсы fa0/1. У Вас должна получиться схема сети, представленная на рисунке 3.

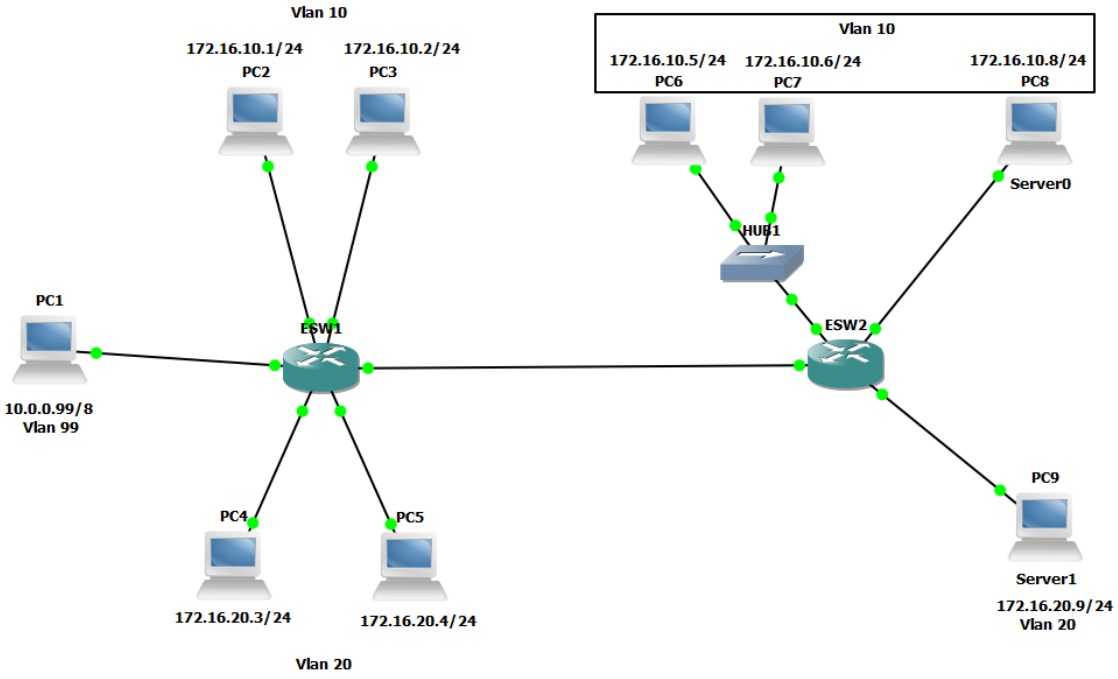


Рисунок 3 - Схема сети с магистральным каналом

***ВЫПОЛНИТЬ!***

40. Убедиться в том, что взаимодействие узлов, принадлежащих одной и той же VLAN-сети, невозможно, если они подключены к разным коммутаторам.

Для создания транка между коммутаторами необходимо выполнить для каждого интерфейса создаваемого канала описанную ниже последовательность действий (один из вариантов):

- перевести интерфейс в режим **trunk** с помощью команды:

**Switch(config-if)#switchport mode trunk;**

- указать метод инкапсуляции, используемый в канале, с помощью команды:

**Switch(config-if)#switchport trunk encapsulation <negotiate|isl|dotlQ>.**

Для некоторых коммутаторов стандартным методом инкапсуляции является ISL, используемый нами Catalyst-2960 поддерживает только лишь IEEE 802.1Q, поэтому данная команда в его ОС отсутствует, а при конфигурировании, например, Catalyst-3560 она необходима;

- удалить неиспользуемые VLAN-сети из магистрального канала вручную (необязательно, но рекомендуется) с помощью команды:

**Switch(config-if)#switchport trunk allowed vlan remove <список>;**

- в случае необходимости, добавить новые VLAN-сети в магистральный канал с помощью команды:

**Switch(config-if)#switchport trunk allowed vlan add <список>.**

Для отображения информации о магистральных каналах используется команда привилегированного режима: **Switch#show interfaces trunk.**

***ВЫПОЛНИТЬ!***

56. Вывести информацию о магистральных каналах коммутаторов.

Библиографический список

1. Защита информации в компьютерных сетях. Практический курс : учеб. пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский [и др.] ; под ред. Н. И. Синадского. – Екатеринбург : УГТУ-УПИ, 2008. – 248 с.

2. Americas Headquarters Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x. – USA : Cisco Systems, 2009. – 136 p.

3. Gary Hallen, G. Kellogg Security Monitoring with Cisco Security MARS. – USA : Cisco Press, 2007. – 335 p.

4. James Burton, Ido Dubrawsky, Vitaly Osipov Cisco Security Professional's Guide to Secure Intrusion Detection Systems. – USA : Syngress Publishing, 2003. – 673 p.

5. Installation Guide for the Cisco Secure PIX Firewall Version 5.2. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

6. Install and Setup Guide for Cisco Security Monitoring Analysis and Response System. Release 4.3.x., 2008. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

7. Стивенс У. Р. Протоколы TCP/IP. Практическое руководство / пер. с англ. – СПб. : БХВ-Петербург, 2003. – 672 с.

8. Кульгин М. Практика построения компьютерных сетей. Для профессионалов. – СПб. : Питер, 2001. – 320 с.