

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ**

Северо-Кавказский филиал  
ордена Трудового Красного Знамени федерального государственного  
бюджетного образовательного учреждения высшего образования  
«Московский технический университет связи и информатики»»

Методические указания по проведению лабораторных работ

по дисциплине

**Проектирование и эксплуатация сетей связи  
Б1.В.16**

Направление подготовки **11.03.02 Инфокоммуникационные технологии  
и системы связи**  
Профиль **Сети связи и системы коммутации**

Формы обучения **очная, заочная**

Ростов-на-Дону

2019 г.

Методические указания по проведению лабораторных работ

по дисциплине

## **Проектирование и эксплуатация сетей связи**

Составитель: Н.В. Болдырихин

Рассмотрено и одобрено  
на заседании кафедры  
Протокол от «26» августа 2019 г. № 1

## Лабораторная работа №1 Настройка операционной системы Cisco

1. Изучение принципов функционирования маршрутизаторов Cisco
2. Первоначальная настройка сетевых параметров Cisco IOS

### Цель работы

Целью лабораторной работы является обучение методам и средствам первоначальной настройки специализированной ОС CiscoIOS, под управлением которой работают маршрутизаторы.

#### 1. Изучение принципов функционирования маршрутизаторов Cisco

*Cisco IOS* – это специализированная ОС, обеспечивающая функционирование сетевого оборудования компании «Cisco Systems, Inc». Взаимодействие с данной ОС возможно либо через web-браузер, либо через интерфейс командной строки (CLI-интерфейс).

Данная ОС поддерживает удаленный доступ к интерфейсу командной строки по протоколам Telnet или SSH. В Cisco IOS существует несколько режимов.

*Пользовательский режим* (user mode) – стандартный режим первоначального доступа к ОС. В этот же режим ОС переходит автоматически при продолжительном отсутствии ввода в режиме администратора. В режиме пользователя доступны только простые команды, не влияющие на конфигурацию оборудования. Приглашение командной строки имеет следующий вид:

```
router>
```

*Административный режим* (privileged mode). Открывается командой *enable*, введенной в режиме пользователя:

```
router> enable
```

В административном режиме доступны команды, позволяющие получить полную информацию о конфигурации оборудования и его состоянии, а также команды перехода в режим конфигурирования, команды сохранения и загрузки конфигурации. Приглашение командной строки имеет следующий вид:

```
router#
```

Обратный переход в пользовательский режим производится по команде *disable* или по истечении установленного времени неактивности. Завершение сессии – команда *exit*.

*Глобальный режим конфигурирования* (конфигурационный режим). Активизируется командой *config terminal*, введенной в административном режиме:

```
router# configure terminal
```

Глобальный режим конфигурирования организован иерархически – он содержит как непосредственно команды конфигурирования оборудования, так и команды перехода в режимы конфигурирования его подсистем (например, интерфейсов, протоколов маршрутизации, механизмов защиты).

Приглашения командной строки в наиболее часто используемых конфигурационных режимах имеют следующий вид:

```
router(config)#
router(config-if)#
router(config-router)#
router(config-ext-nacl)#
switch(config-line)#
switch(vlan)#
```

Выход из любого режима конфигурирования в режим верхнего уровня производится командой *exit* или комбинацией клавиш *Ctrl-Z*.

Кроме того, команда *end*, поданная в любом из режимов конфигурирования немедленно завершает процесс конфигурирования и возвращает пользователя в администраторский режим.

Любая команда изменения конфигурации вступает в действие немедленно после ввода. Все команды и параметры могут быть сокращены (например, "*enable*" – "*en*", "*configure terminal*" – "*conf t*", "*show running-config*" – "*sh run*").

В любом месте командной строки для получения помощи может быть использован вопросительный знак, например:

```
router#?
```

```
router#co?
```

```
router#conf ?
```

Имена сетевых интерфейсов также могут быть сокращены, например, вместо "*fast ethernet0/1*" достаточно написать "*fa0/1*".

Отмена любой команды (отключение опции или режима, включаемых командой, снятие или удаление параметров, назначаемых командой) производится подачей этой же команды с префиксом "*no*", например:

```
router(config)#int fa0/1
```

```
router(config-if)#shutdown
```

```
router(config-if)#no shutdown
```

При загрузке сетевого оборудования, работающего под управлением Cisco IOS, происходит считывание команд конфигурации из изменяемого постоянного запоминающего устройства (NVRAM), где они хранятся в виде текстового файла, называемого *рабочей конфигурацией* (running config). Конфигурация, сохраненная в NVRAM, называется *начальной конфигурацией* (startup config). В процессе работы оборудования администратор может вводить до полнительные конфигурационные команды, в результате чего рабочая конфигурация становится отличной от начальной.

Просмотр начальной и рабочей конфигураций маршрутизатора производится в административном режиме:

```
router#show startup-config
```

```
router#show running-config
```

Вывод последней команды позволяет просмотреть текущую конфигурацию. Однако если администратор не менял значения параметров, используемых в ОС по умолчанию, то они при выводе не отобразятся.

При копировании одной конфигурации поверх другой возможны два варианта: перезапись и слияние. При перезаписи старая конфигурация предварительно удаляется. При слиянии команды новой конфигурации добавляются к командам старой, как если бы они вводились вручную.

Ниже приведен список команд копирования конфигурации, первая из которых выполняется в режиме перезаписи, а последняя в режиме слияния:

```
router#copy running-config startup-config
```

```
router#copy startup-config running-config
```

Рассмотрим базовые команды получения информации о работе оборудования и его подсистем.

Просмотр информации об оборудовании (модель, объемы памяти, версия IOS, число и тип интерфейсов) выполняется по следующей команде:

```
router#show version
```

Просмотр содержимого флэш-памяти:

```
router#show flash:
```

Мониторинг загрузки процессора:

```
router#show processes
```

Рассмотрим основные команды первоначальной конфигурации маршрутизатора.

Установить имя маршрутизатора:

```
router(config)#hostname my_router
```

Установить пароль администратора, требуемый при переходе в вводе команды *enable*:

```
router(config)#enable secret my_secret
```

Отключение разрешения DNS-имен:

```
router(config)#no ip domain-lookup
```

Базовая настройка FastEthernet-интерфейса:

```
router#configure terminal
```

```
router(config)#interface fastEthernet 0/1
```

```
router(config-if)#ip address 192.168.0.1
```

```
255.255.255.0
```

```
router(config-if)#speed 100
```

```
router(config-if)#duplex full
```

```
router(config-if)#no shutdown
```

```
router(config-if)#exit
```

Для последовательного интерфейса устройства, выполняющего роль DCE, необходимо указывать тактовую частоту (пропускную способность), при этом данная команда выполняется только на одной стороне линии связи:

```
router(config)#interface serial0  
router(config-if)#clock rate 125000
```

Если на последовательном интерфейсе необходимо использовать другой протокол 2-го уровня (например, Frame Relay), то это делается с помощью команды:

```
router(config-if)#encapsulation frame-relay
```

Параметры интерфейсов, протоколов 2-го уровня, а также статистика отправленных и полученных кадров может быть просмотрена следующей командой в режиме администратора:

```
router#show interface
```

Подробная информация о параметрах протокола IP доступна в режиме администратора по команде:

```
router#show ip interface interface
```

Краткая сводная таблица состояний IP-интерфейсов:

```
router#show ip interface brief
```

Рассмотрим настройку статической маршрутизации. Маршруты, ведущие в сети, к которым маршрутизатор подключен непосредственно, автоматически добавляются в маршрутную таблицу после конфигурирования интерфейса при условии, что интерфейс корректно функционирует.

Для назначения дополнительных статических маршрутов в режиме глобальной конфигурации вводится команда:

```
router(config)#ip route prefix mask ip_address
```

Маршрут по умолчанию (стандартный маршрут) назначается следующей командой:

```
router(config)#ip route 0.0.0.0 0.0.0.0  
ip_address
```

Просмотреть таблицу маршрутов можно по команде:

```
router#show ip route
```

## *2. Первоначальная настройка сетевых параметров Cisco IOS*

Постановка задачи: выполнить первоначальную настройку сетевых параметров ОС Cisco IOS маршрутизатора Cisco 2811 с рабочей станции администратора сети, используя данные в следующих данных:

IP-адрес интерфейса: Fa0/0 10.194.7.1/24.

IP-адрес интерфейса: Fa0/1 192.168.100.26/30.

Стандартный шлюз: 192.168.100.25.

Имя маршрутизатора: R7.

Домен: net.bank.

Пароль доступа: enable xkld7Hn434!2&.

Локальный пользователь/пароль: пос/nTefa#51.

Последовательность действий.

Шаг 1. Подключить к маршрутизатору Cisco 2811 рабочую станцию через консольный шнур и интерфейс RS-232.

Шаг 2. Запустить терминальный клиент и проверить правильность параметров его настройки.

Шаг 3. Просмотреть список команд пользовательского режима.

Выполнить команду:

```
router>show version
```

Шаг 4. Перейти в административный режим, выполнив команду:

```
router>enable
```

Шаг 5. Просмотреть уровень доступа в системе и текущую конфигурацию:

```
router#show privilege
```

```
router#show running-config
```

Шаг 6. Просмотреть список доступных команд. Определить и выполнить все возможные информационные команды. Например:

```
router#show flash
```

```
router#show version
```

```
router#show logging
```

Шаг 7. Выполнить настройку маршрутизатора в соответствии с указанными параметрами, выполнив следующие команды:

```
configure terminal
hostname R7
interface fastEthernet 0/1
ip address 192.168.100.26 255.255.255.252
no shutdown
interface fastEthernet 0/0
ip address 10.194.7.1 255.255.255.0
no shutdown
ip domain-name net.bank
ip route 0.0.0.0 0.0.0.0 192.168.100.25
```

Шаг 8. Сохранить конфигурацию маршрутизатора, выполнив команду:

```
write memory
```

Шаг 9. Выключить питание маршрутизатора. Установить сетевой модуль NM-ESW161. Включить питание маршрутизатора. Проверить возможность загрузки маршрутизатора с новой конфигурацией.

Шаг 10. Просмотреть список всех портов и их имен:

```
sh ip interface brief
```

Шаг 11. Выполнить следующие команды и посмотреть их результаты:

```
sh processes
sh file systems
```

Шаг 12. Выключить режим шифрования паролей в конфигурационном файле, создать пользователя и убедиться, что пароль в конфигурационном файле записан в открытом виде, затем включить режим шифрования паролей и убедиться, что теперь пароль представляется в зашифрованном виде:

```
no service password-encryption
username noc1 secret test
username noc2 password test
```

```
enable secret test2
show running-config
service password-encryption
show running-config
```

Шаг 13. Удалить всех созданных ранее пользователей, задать стойкие к перебору пароли пользователей и пароли для административного доступа. Проверить, что для подключения к маршрутизатору и перехода в административный режим требуется пароль:

```
line console 0
password n&bbR4d21
login
no username noc1
no username noc2
enable secret xkld7Hn434!2&^
username noc secret nTefa#51
```

Шаг 14. Выполнить настройку механизма ролевого управления доступа к командам маршрутизатора, реализующего следующую политику безопасности.

Существуют следующие роли и соответствующие им уровни безопасности: администратор (15), инженер (5) и оператор (3). Доступ пользователям, авторизованным на роль инженера, может быть предоставлен только через консольную сессию. При этом могут быть выполнены основные команды по диагностике и настройке средств маршрутизации, коммутации и адресации.

Пользователи, авторизованные на роль оператора, могут только просматривать диагностические данные на маршрутизаторе. Роль администратора имеет все привилегии:

```
username admin privilege 15 secret nTefa#51
enable secret 15 secret Rc@sxa&h
username engineer privilege 5 secret LwqndhR5
enable secret 5 secret Jnfbn&gd
username operator privilege 3 secret *mmfjj&D
```

```
enable secret 3 secret Mf88MMh1
privilege exec level 3 show running-config
privilege exec level 3 show startup-config
privilege exec level 3 show
privilege exec level 3 ping
privilege exec level 3 ssh
privilege exec level 3 telnet
privilege exec level 3 exit
privilege exec level 5 configure terminal
privilege exec level 5 configure
privilege configure level 5 ip
privilege configure level 5 no ip
privilege configure level 5 ip route
privilege configure level 5 no ip route
privilege configure level 5 router
privilege configure level 5 no router
privilege configure level 5 interface
line console 0
privilege 3
```

*Контрольные вопросы:*

1. Особенности работы в пользовательском режиме маршрутизатора Cisco.
2. Особенности работы в административном режиме маршрутизатора Cisco.
3. Настройки маршрутизатора Cisco в глобальном режиме конфигурирования.
4. Конфигурационный файл маршрутизатора Cisco.
5. Наименование модулей линейных карт и сетевых интерфейсов на маршрутизаторах Cisco.

## Лабораторная работа №2. Проектирование коммутируемой сети с использованием технологии VLAN

1. Изучение технологии VLAN
2. Проектирование ЛВС филиала банка с использованием технологии VLAN

### *Цель работы.*

Целью лабораторной работы является обучение методам и средствам защиты инфраструктуры коммутации при использовании технологии виртуальных ЛВС (VLAN), их настройке и маршрутизации.

### *1. Изучение технологии VLAN*

*Виртуальная ЛВС* или *VLAN* – широковещательный домен второго уровня.

Порты коммутаторов, принадлежащие одной VLAN, могут обмениваться кадрами между собой, но не могут обмениваться кадрами с портами других VLAN.

Для централизованного управления VLAN на коммутаторах может быть использован протокол VTP.

Для передачи кадров нескольких VLAN между коммутаторами используются *магистральные соединения*, или *транки*.

Порты коммутаторов, образующие магистральный канал, называются *магистральными*, или *транковыми* портами. На магистральных портах (в отличие от портов доступа) производится идентификация и инкапсуляция кадров VLAN с помощью протоколов ISL или IEEE 802.1Q.

Для динамического создания магистрального канала между коммутаторами может использоваться протокол DTP. Порты коммутатора, передающие кадры только одной VLAN, называются *портами доступа* (access port). Как правило, по умолчанию все порты коммутаторов являются портами доступа и находятся в VLAN с номером 1, называемой *собственной* или *стандартной* VLAN (native VLAN). Для собственных VLAN не применяются никакие протоколы инкапсуляции.

Различают статические и динамические VLAN. В *статических* VLAN назначение порта осуществляется администратором на этапе настройки коммутатора. В *динамических* VLAN назначение порта осуществляется по

некоторому протоколу и, как правило, на основе MAC-адреса узла сети. В настоящее время в основном используются статические VLAN.

Компьютеры, находящиеся в разных VLAN могут обмениваться данными только через маршрутизатор (или любое другое устройство уровня L3), имеющий интерфейсы в этих VLAN. Такие VLAN называются маршрутизируемыми, иначе – изолированными.

В настоящее время рекомендуется использовать следующие принципы при создании и настройке защищенных коммутируемых ЛВС:

1. Не использовать для распространения информации об используемых VLAN в ЛВС протокол VTP (включать режим transparent).
  2. В качестве протокола инкапсуляции использовать протокол IEEE 802.1Q.
  3. Запретить передавать кадры собственной VLAN по магистральным каналам. В качестве native VLAN использовать специально для этого выделенную VLAN, не используемую ни для каких других целей.
  4. Не использовать стандартную VLAN 1 в ЛВС ни для каких целей, особенно для управления сетевым оборудованием.
  5. На магистральных портах использовать только необходимые VLAN – VLAN, которым принадлежат порты коммутаторов на другой стороне. Все другие VLAN запрещать.
  6. Не использовать одинаковые VLAN на разных коммутаторах. Наиболее предпочтительный вариант проектирования – один коммутатор, одна VLAN, одна IP-подсеть.
  7. Все неиспользуемые порты коммутатора переводить в режим shutdown и назначать их в специально созданную для этого немаршрутизируемую и изолированную VLAN.
  8. На портах доступа отключать использование протокола DTP.
- Для минимизации времени восстановления функционирования системы при подключении канала на магистральных портах устанавливать протокол DTP в режимах On/On и Nonegotiate (отключать согласование).

## *2. Проектирование ЛВС филиала банка с использованием технологии VLAN*

Постановка задачи: ЛВС филиала банка построена на базе двух коммутаторов уровня доступа филиала Cisco Catalyst 2960 (SW4-2, SW4-3), коммутатора уровня ядра-распределения филиала Cisco Catalyst 3560 (SW4-1) и маршрутизатора доступа Cisco 2811 (R4).

Требуется создать VLAN с номерами для рабочих станций, принтеров и серверов банка в соответствии со схемой, представленной на рис. 1, настроить маршрутизацию между этими VLAN при их подключении к маршрутизатору R4 по магистральному каналу, а также выполнить настройки в соответствии с приведенными выше рекомендациями.

Последовательность действий.

Шаг 1. На коммутаторе уровня доступа филиала SW4-3 отключить протокол VTP, создать необходимые VLAN, настроить магистральный порт и порты доступа коммутатора:

```
vtp mode transparent
vlan 30
name AS_Client_Bank
vlan 40
name Service
vlan 700
name unused ports
vlan 701
name native
```

Шаг 2. Настроить используемые магистральные порты и порты доступа коммутатора SW4-3:

```
interface fastEthernet 0/1
switchport mode trunk
switchport nonegotiate
switchport trunk native vlan 701
interface fastEthernet 0/2
```

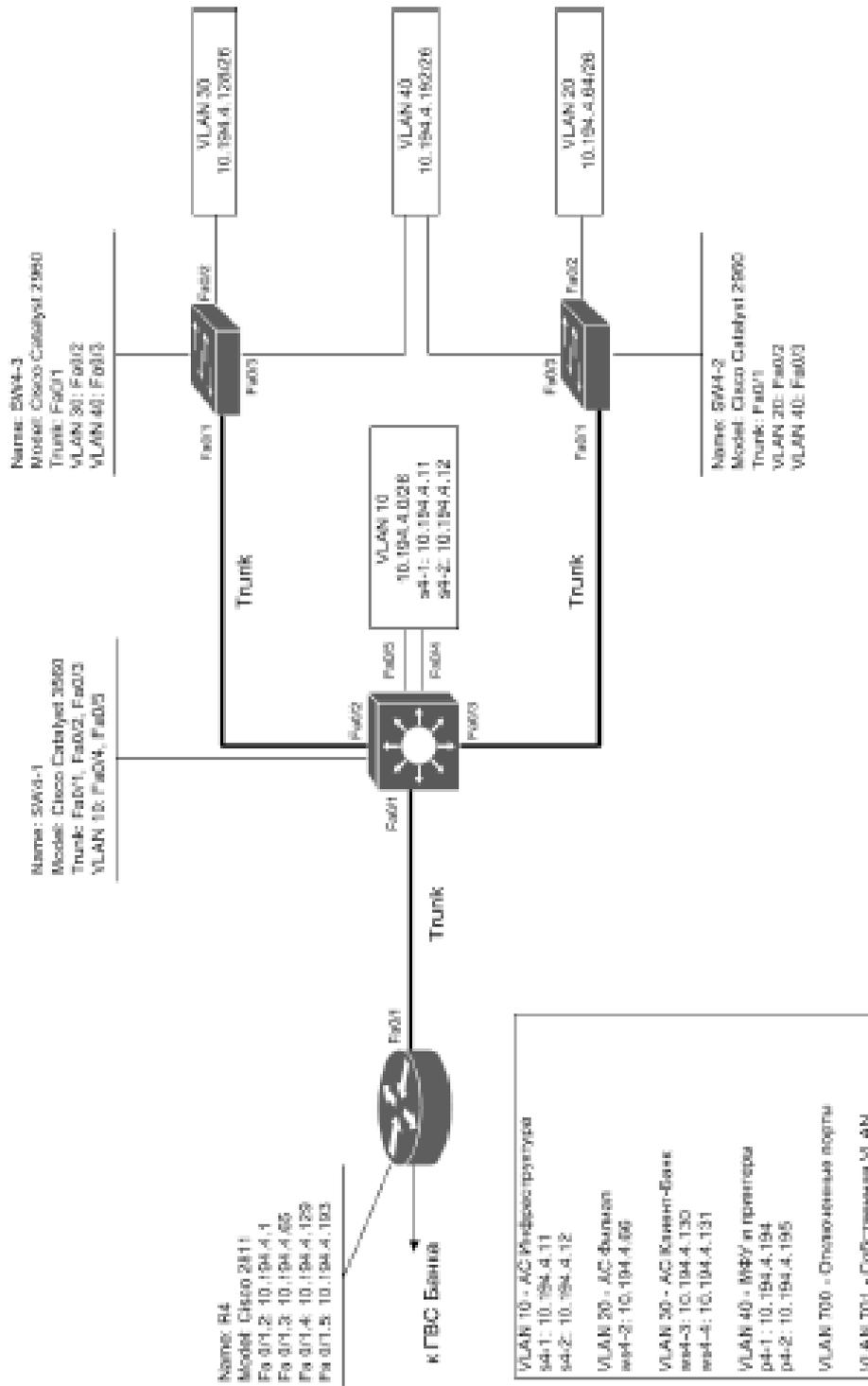


Рисунок 1- Схема соединения оборудования ЛВС

switchport mode access

switchport nonegotiate

```
switchport access vlan 30
```

Шаг 3. Настроить неиспользуемые порты коммутатора SW4-3, используя возможность указания диапазона портов:

```
interface range fastEthernet 0/4-24
```

```
switchport mode access
```

```
switchport nonegotiate
```

```
switchport access vlan 700
```

```
shutdown
```

Шаг 4. Выполнить аналогичные настройки с учетом требуемых VLAN, на коммутаторе SW4-2.

Шаг 5. На коммутаторе уровня ядра-распределения филиала SW4-1 настроить магистральные порты для соединения с маршрутизатором и коммутаторами доступа по схеме магистрального подключения. Выполнить настройки безопасности согласно приведенным выше рекомендациям:

```
ip routing
```

```
interface fa0/1
```

```
switchport trunk encapsulation dot1q
```

```
switchport mode trunk
```

```
switchport nonegotiate
```

```
switchport trunk native vlan 701
```

```
switchport trunk allowed vlan 10,20,30,40
```

Шаг 6. На маршрутизаторе филиала R4 создать необходимые VLAN, настроить sub-интерфейсы на порту Fa0/1 и включить инкапсуляцию по протоколу IEEE 802.1Q:

```
interface fa0/1
```

```
no shutdown
```

```
no ip address
```

```
interface fa0/1.2
```

```
encapsulation dot1q 10
```

```
ip address 10.194.4.1 255.255.255.192
```

```
interface fa0/1.3
encapsulation dot1q 20
ip address 10.194.4.65 255.255.255.192
interface fa0/1.4
encapsulation dot1q 30
ip address 10.194.4.129 255.255.255.192
interface fa0/1.5
encapsulation dot1q 40
ip address 10.194.4.193 255.255.255.192
```

Шаг 7. Проверить доступность серверов АС с рабочих станций, исследовать формат кадров, передающихся по магистральному каналу между коммутатором ядра-распределения и маршрутизатором.

Убедиться в невозможности взаимодействия с серверами АС из VLAN 700.

Шаг 8. Убедиться, что кадры native VLAN не инкапсулируются протоколом IEEE 802.1q при их передаче по магистральному каналу.

*Контрольные вопросы.*

1. Определение виртуальной ЛВС.
2. Дайте рекомендации по настройке механизмов защиты виртуальных ЛВС.
3. Определение статической и динамической VLAN.
4. Поясните назначение и общие принципы функционирования протокола DTP.
5. Назначение портов типа trunk и access.

### **Лабораторная работа №3. Проектирование отказоустойчивой сети на основе на основе протокола STP**

1. *Изучение протокола STP*
2. *Проектирование отказоустойчивой сети на основе на основе протокола STP*

#### *Цель работы.*

Целью лабораторной работы является изучение методов и средств построения, защиты и оптимизации отказоустойчивых ЛВС на основе протокола STP.

#### *1. Изучение протокола STP*

Протоколы и механизмы оптимизации и защиты семейства STP предназначены для предотвращения петель (циклов) в сетях с множественными маршрутами на канальном уровне ЛВС. За счет обмена служебными BPDU-кадрами коммутаторы, на которых запущен протокол STP, строят топологию, в которой между любыми двумя коммутаторами существует только один активный в данный момент маршрут на канальном уровне.

В настоящее время семейство протоколов STP включает протоколы и механизмы IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, IEEE 802.1t, а также расширение Cisco Spanning Tree Toolkit.

Одним из основных элементов протокола STP является корневой коммутатор. Некорректный выбор корневого коммутатора, вызванный ошибками конфигурирования оборудования или атаками нарушителей, может привести к нарушению штатного функционирования сетевой инфраструктуры или перенаправлению и перехвату информационных потоков на канальном уровне.

В настоящее время используются следующие принципы при проектировании, настройке и оптимизации протоколов семейства STP.

1. Использовать протоколы семейства STP с целью построения отказоустойчивых ЛВС только при необходимости. По возможности для обеспечения отказоустойчивости и высокой доступности ЛВС использовать механизмы и протоколы маршрутизации сетевого уровня.

2. Применение протокола STP является обязательным в случае передачи данных в одной и той же виртуальной ЛВС, организованной на разных коммутаторах, а также для защиты от действий пользователей на портах доступа коммутаторов ЛВС и ошибок обслуживающего персонала.

3. В семействе протоколов STP рекомендуется использовать протокол Rapid-PVST+.

4. Административно определять и назначать корневые коммутаторы. Использовать дополнительные механизмы и средства защиты протокола STP (Root Guard, Loop Guard, UplinkFast, UDLD) для предотвращения получения роли корневого коммутатора другими коммутаторами.

5. На портах доступа коммутаторов ЛВС выполнять настройки по предотвращению возможности появления или фильтрации BPDU-пакетов протокола STP (механизмы BPDU Guard и BPDU Filter соответственно), а также выполнять настройки для быстрого включения и защиты корневого коммутатора (механизмы PortFast и Root Guard соответственно).

## *2. Проектирование отказоустойчивой сети на основе на основе протокола STP*

### Постановка задачи

На коммутаторах ЛВС филиала банка выполнить настройки протокола STP и механизмов его защиты. Построенная ЛВС должна обеспечивать состояние доступности при отказе:

- одного из коммутаторов SW7-1 или SW7-2;
- активного коммутируемого порта маршрутизатора R7;
- одной из линий связи канала EtherChannel;
- активного порта линии связи между коммутатором уровня доступа

и коммутатором уровня ядра-распределения.

Последовательность действий.

Шаг 1. Построить схему логического соединения коммутаторов ЛВС и найти возможные циклы на канальном уровне (см. рис. 3).

Определить оптимальное положение корневого коммутатора в соответствии с маршрутами информационных потоков.

Шаг 2. К маршрутизатору R7 в слот № 3 подключить модуль HWIC-4ESW, обеспечивающий наличие дополнительных четырех коммутируемых Ethernet-портов. Создать на коммутирующем модуле маршрутизатора виртуальные ЛВС и для каждой из них настроить интерфейс SVI, обеспечивающий маршрутизацию виртуальных ЛВС:

```
vlan database
vlan 10 name Servers
vlan 20 name AS_Filial
vlan 30 name AS_Client_Bank
vlan 40 name Service
interface vlan10
ip address 10.194.7.1 255.255.255.192
interface vlan20
ip address 10.194.7.65 255.255.255.192
interface vlan30
ip address 10.194.7.129 255.255.255.192
interface vlan40
ip address 10.194.7.193 255.255.255.192
interface fastEthernet 3/0/0
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
switchport trunk native vlan 701
interface fastEthernet 3/0/1
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
switchport trunk native vlan 701
```



```
interface port-channel 1
no shutdown
switchport mode trunk
switchport trunk native vlan 701
switchport trunk allowed vlan 10,20,30,40
```

Шаг 5. На коммутаторе SW7-1 настроить протокол Rapid-PVST для требуемых виртуальных ЛВС и задать наивысший приоритет коммутатора, обеспечив ему роль корневого моста в указанных VLAN:

```
spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30,40,701 root primary
```

Шаг 6. На коммутаторе SW7-2 настроить протокол Rapid-PVST для требуемых VLAN и задать наивысший приоритет коммутатора, обеспечив ему роль корневого моста в указанных VLAN в случае выхода из строя коммутатора SW7-1:

```
spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30,40,701 root secondary
```

Шаг 7. На коммутаторах SW7-1 и SW7-2 настроить механизм Root Guard:

```
interface range fa0/2-3
spanning-tree guard root
```

Шаг \_\_\_\_ 8. На коммутаторах SW7-3 и SW7-4 настроить протокол Rapid-PVST для требуемых VLAN:

```
spanning-tree mode rapid-pvst
spanning-tree vlan 20,30,40,701
```

Шаг 9. На портах доступа коммутаторов SW7-3 и SW7-4 настроить протокол STP в режиме portfast, включить механизмы защиты BPDU Guard:

```
interface range fa0/3-4
switchport mode access
spanning-tree bpduguard enable
spanning-tree portfast
```

Шаг 10. Убедиться в корректности настройки протокола STP на коммутаторах ЛВС. Проверить возможность функционирования сети при отключении порта

Fa0/0/1 маршрутизатора R7, при отключении порта Gi0/1 коммутатора SW7-1, при отключении коммутатора SW7-1 или при отключении порта Fa0/1 коммутатора SW7-3.

*Контрольные вопросы.*

1. Принцип функционирования сети на основе протокола STP.
2. Поясните структуру BPDU-кадра.
3. Назовите дополнительные механизмы и средства защиты протокола STP.
4. Поясните выбор портов активации механизма Root Guard на коммутаторах уровня ядра-распределения филиала.  
Обоснование выбора корневого коммутатора

