Практическое задание в Cisco Packet Tracer

Описание ПО и оборудования для моделирования сети

Для выполнения задания необходимо ПО Cisco Packet Tracer v.7.1.1. Получить легальный доступ к ПО можно тремя способами:

1. в результате прохождения курса сетевой академии Cisco (www.netacad.com), расположенного по ссылке https://www.netacad.com/ru/courses/intro-packet-tracer/
2. если учебное заведение является участником программы Сетевых академий Cisco;

Оборудование

Маршрутизаторы R1, R2, R3 – платформа Cisco 2911 (в R3 в слот eHWIC0 вставлена плата HWIC-2T), маршрутизатор DHCP – платформа Cisco 2811, маршрутизатор RB – платформа Cisco 1841. Коммутаторы S1, S2, SB – платформа Cisco WS-C2960-24TT. Оконечное оборудование: ПК – устройство PC-PT, IP-телефоны типа 7960, сервер – Server-PT.

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
R3	Se0/0/0	209.165.24.33	255.255.255.240
	Gi0/0	192.168.0.1	255.255.255.240
	Gi0/1	10.0.0.1	255.255.255.252
	G0/2	10.0.0.5	255.255.255.252
R2	Gi0/0		
	Gi0/0.15	10.0.15.2	255.255.255.0
	Gi0/0.30 Gi0/0.45	10.0.30.2 10.0.45.2	255.255.255.0 255.255.255.0
	Gi0/0.60	10.0.60.2	255.255.255.0
	Gi0/0.75	10.0.75.2	255.255.255.0
	G0/2	10.0.0.6	255.255.255.252
R1	Gi0/0		
	Gi0/0.15	10.0.15.1	255.255.255.0
	Gi0/0.30	10.0.30.1	255.255.255.0

	Gi0/0.45	10.0.45.1	255.255.255.0
	Gi0/0.60	10.0.60.1	255.255.255.0
	Gi0/0.75	10.0.75.1	255.255.255.0
	Gi0/1	10.0.0.2	255.255.255.252
DHCP	Fa0/1		
	Fa0/1.15	10.0.15.3	255.255.255.0
	Fa0/1.30	10.0.30.3	255.255.255.0
	Fa0/1.45	10.0.45.3	255.255.255.0
	Fa0/1.60	10.0.60.3	255.255.255.0
	Fa0/1.75	10.0.75.3	255.255.255.0
S1	VLAN Manage	10.0.30.4	255.255.255.0
S2	VLAN Manage	10.0.30.5	255.255.255.0
RB	Fa0/0	192.168.1.254	255.255.255.0
	Fa0/1	209.165.24.49	255.255.255.240
SB	Vlan1	192.168.1.250	255.255.255.0
ПК-7	Fa0	192.168.1.151	255.255.255.0
ПК-8	Fa0	192.168.1.152	255.255.255.0
ПК-9	Fa0	192.168.1.153	255.255.255.0
Датчик влажности	Fa0	192.168.1.1	255.255.255.0
Датчик температуры	Fa0	192.168.1.2	255.255.255.0
Сервер	Gi1	192.168.0.2	255.255.255.240

Таблица сетей VLAN и назначений портов

Номер сети VLAN — имя	**Назначения портов**	**Сеть**
15 – Teachers	F0/11 — F0/20	10.0.15.0/24
30 – Management	F0/1 — F0/10	10.0.30.0/24
45 – Students	G0/1	10.0.45.0/24
60 – Guests	VLAN 60	10.0.60.0/24
75 – IP-Phones		10.0.75.0/24

Реализация

Все устройства в облаке (топология Интернет - рис.1) полностью настроены, Вы не имеете доступа к устройствам. Вы можете получить доступ ко всем сетевым устройствам основной сети (рис. 2) и устройствам сети филиала (рис.3) для выполнения настройки и проверки.

Используя документацию, реализуйте приведённые ниже требования:

На **всех устройствах** согласно таблице адресации настройте статические IP-адреса узла, маски подсети, шлюзы по умолчанию (при необходимости).

Маршрутизаторы R1, R2, R3, DHCP, RB, коммутаторы S1, S2, SB:

- Настройте доступ к удалённому управлению устройством, в том числе IP-адресацию и SSH:
    - домен - **olimp-spo.ru**;
    - пользователь - **Admin,** секретный пароль - **P@55w0rd**;
    - длина ключа шифрования составляет 1024 бит;
    - протокол SSH версии 2 с ограничением на две попытки аутентификации и временем ожидания 60 секунд;
    - безопасный вход с локальной проверкой паролей на линиях VTY, консольном входе, линиях AUX сетевых устройств;
    - незашифрованные пароли необходимо зашифровать;
    - установить баннер MOTD **This is a secure system. Authorized Access Only!**;
    - настроить NTP:
        - NTP-сервер 192.168.0.2;
        - ключ №1;
        - аутентификация по алгоритму MD5 с паролем Ufa2018;
    - минимальная длина паролей - 8 символов;
    - настроить противодействие атакам типа «подбор пароля»: ограничение количества попыток входа на устройство (если было предпринято 5 неуспешных попыток входа в течении 60 секунд, то запретить дальнейшие попытки входа на 300 секунд), а также сохранение в журнале успешных и неудачных попыток подключения.

Маршрутизаторы R1, R2, R3, DHCP:

- настройте маршрутизацию между VLAN по стандарту IEEE 802.1Q;
- организуйте маршрутизацию:
    - в качестве протокола маршрутизации используйте OSPF;
    - все интерфейсы (подинтерфейсы) вышеуказанных маршрутизаторов должны принадлежать магистральной области (зоне);
    - отключите интерфейсы, которые не должны посылать сообщения OSPF;

- организуйте распространение статического маршрута в Интернет по умолчанию;
- настройте парольную защиту для работы протоколов динамической маршрутизации:
  - алгоритм аутентификации - MD5;
  - пароль OSPFGUARD;

На **маршрутизаторах R3, RB** настройте статические маршруты в Интернет по умолчанию.

Маршрутизатор DHCP:

- настройте службы DHCP для VLAN 15, 30, 45, 60, 75:
  - используйте слово **LAN_X** в качестве имени пула (с учетом регистра), где X - номер VLAN;
  - исключите из диапазона адреса A.B.C.1– A.B.C.5, A.B.C.10 для каждой VLAN;
  - для VLAN, используемой для IP-телефонии назначить адрес TFTP-сервера (option 150);
- настройте IP-телефонию:
  - максимальное количество телефонов - 4;
  - максимальное количество линий (номеров) - 4;
  - зарезервировать номера вручную по MAC-адресам IP-телефонов;
  - тип IP-телефона - 7960.

Маршрутизаторы R3, RB:

- настройте преобразование NAT:
  - настройте именованный список контроля доступа с именем **NAT**, содержащий одну запись. Сначала разрешите все IP-адреса, принадлежащие адресному пространству **10.0.0.0/16**;
  - далее настройте статический NAT для сервера **Сервисы**, заменяя его внутренний адрес на адрес 209.165.24.40;
  - настройте динамическую трансляцию NAT с использованием PAT, указав выбранное имя пула, маску /30 и следующие два общедоступных адреса для R3: 209.165.24.34 и 209.165.24.35;
  - настройте динамическую трансляцию NAT с использованием PAT, указав выбранное имя пула, маску /30 и следующие два общедоступных адреса для RB: 209.165.24.50 и 209.165.24.51;
- настройте VPN-туннель между маршрутизаторами (для пар подсетей 192.168.0.0/24-192.168.1.0/24, 192.168.1.0/24-10.0.15.0/24, 192.168.1.0/24-10.0.30.0/24, 192.168.1.0/24-10.0.45.0/24 создать расширенный список контроля доступа **110**):
  - первая фаза:
    - политика (приоритет) - 1;
    - тип алгоритма шифрования - **AES**;
    - тип алгоритма обеспечения целостного данных - **SHA**;

        - группа - 2;
        - тип аутентификации - с заранее заданным ключом (pre-share);
        - пароль - **VPN_P@55w0rd**;
    - вторая фаза:
        - название **VPN_SET**;
        - тип алгоритма шифрования - **AES**;
        - тип алгоритма обеспечения целостного данных - **SHA-HMAC**;
        - тэг (криптографическая карта) для дальнейшего использования на интерфейсе - **VPN_MAP**;
- настройте именованные списки контроля доступа **FROM_IN** для ограничения доступа из ЛВС:
    - разрешите для всех VLAN доступ по протоколам HTTP и HTTPS к любым веб-серверам в Интернете;
    - разрешите доступ по протоколу ICMP для сообщений типа **echo-reply**, **unreachable**, **source-quench** и запретите все остальные сообщения протокола ICMP;
- настройте именованные списки контроля доступа **FROM_OUT** для ограничения доступа из Интернета:
    - разрешите доступ по протоколу TCP, если соединение было установлено из ЛВС для всех VLAN;
    - разрешите доступ по протоколу ICMP для сообщений типа **echo**, **parameter-problem**, **packet-too-big**, **source-quench** и запретите все остальные сообщения протокола ICMP;
    - включите защиту от спуфинга от:
        - узла 0.0.0.0;
        - узла 255.255.255.255;
        - всех частных диапазонов подсетей;
        - подсети 127.0.0.0/8;
        - подсети 224.0.0.0/4.

Маршрутизаторы R1, R2:

- настроить протокола резервирования шлюза HSRP на R1:
    - для VLAN 15, 30 назначить группу резервирования 1, приоритет 110, отслеживание интерфейса Gi0/1;
    - для VLAN 45, 60 назначить группу резервирования 2, приоритет 90, отслеживание интерфейса Gi0/1;
- настроить протокола резервирования шлюза HSRP на R2:
    - для VLAN 15, 30 назначить группу резервирования 1, приоритет 90, отслеживание интерфейса Gi0/2;
    - для VLAN 45, 60 назначить группу резервирования 2, приоритет 110, отслеживание интерфейса Gi0/2.

Коммутаторы S1, S2:

- настройте сети VLAN, присвойте им имена и выполните назначение портов доступа;
- включите функцию PortFast для портов доступа;
- создайте между S1 и S2 агрегированный канал по технологии Etherchannel:
    - интерфейсы используемые для создания канала - Fa0/15- Fa0/20;
    - название канала - Port-channel 1;
    - группа каналов - 1;
    - режим и протокол работы - активный/LACP;
    - переведите его в режим транка (магистрального канала);
- настройте транки (магистральные каналы);
- выключите неиспользуемые порты коммутаторов;
- создайте стандартный список контроля доступа из двух строк с номером 20 в котором разрешите доступ узлу ПК-8 а также из VLAN Management и примените его для линий VTY;
- настройте защиту протоколов связующего дерева на S1:
    - для VLAN 1, 15, 30 назначить его основным корневым мостом;
    - для VLAN 35, 60, 75 назначить его вспомогательным корневым мостом;
- настройте защиту протоколов связующего дерева на S2:
    - для VLAN 1, 15, 30 назначить его вспомогательным корневым мостом;
    - для VLAN 35, 60, 75 назначить его основным корневым мостом;
- настройте функцию Port Security для интерфейсов Fa0/1, Fa0/2:
    - разрешите доступ для трѐх MAC-адресов, которые автоматически добавляются в файл конфигурации после обнаружения;
    - в случае нарушения безопасности порт не должен выключаться, но должно быть зафиксировано сообщение системного журнала;
- настройте функцию Port Security для интерфейса Fa0/3:
    - разрешите доступ для одного MAC-адреса, которые автоматически добавляются в файл конфигурации после обнаружения;
    - в случае нарушения безопасности порт не должен выключаться, но должно быть зафиксировано сообщение системного журнала;
- настройте функцию Port Security для интерфейса Fa0/24 коммутатора S1:
    - разрешите доступ для одного MAC-адреса, которые автоматически добавляются в файл конфигурации после обнаружения;
    - в случае нарушения безопасности порт не должен выключаться, но должно быть зафиксировано сообщение системного журнала;
- настройте защиты от атак, связанных с протоколами ARP(DAI) и DHCP(DHCP Snooping):
    - для VLAN 15, 30,45,60,75;
    - примените еѐ на интерфейсе Port-channel 1 коммутатора S1 и на интерфейсе Fa0/24 коммутатора S2;
    - настройте защиту IP Source guard для всех портов;

– настройте защиту Loop guard по умолчанию.

Коммутатор SB:

- выполните назначение портов доступа;
- включите функцию PortFast для портов доступа;
- выключите неиспользуемые порты коммутаторов;
- создайте стандартный список контроля доступа из двух строк с номером 20 в котором разрешите доступ узлу ПК-8 а также из VLAN Management и примените его для линий VTY;
- настройте функцию Port Security для интерфейсов Fa0/1, Fa0/2, Fa0/15:
    - разрешите доступ для трѐх MAC-адресов, которые автоматически добавляются в файл конфигурации после обнаружения;
    - в случае нарушения безопасности порт не должен выключаться, но должно быть зафиксировано сообщение системного журнала;
- настройте функцию Port Security для интерфейса Fa0/3, Fa0/16:
    - разрешите доступ для одного MAC-адреса, которые автоматически добавляются в файл конфигурации после обнаружения;
    - в случае нарушения безопасности порт не должен выключаться, но должно быть зафиксировано сообщение системного журнала;
- настройте защиту IP Source guard для всех портов.

Проверка

В рамках задания необходимо:

1. Успешно отправить эхо-запросы между узлами:
    - ПК-1 - ПК-4;
    - ПК-2 - ПК-5;
    - ПК-3 - ПК-6;
    - ПК-1 - ПК-7;
    - ПК-2 - ПК-8;
    - ПК-3 - ПК-9.
2. Получить доступ с узлов ПК-1, ПК-2, ПК-3 к серверу **Сервисы** по протоколу HTTP.

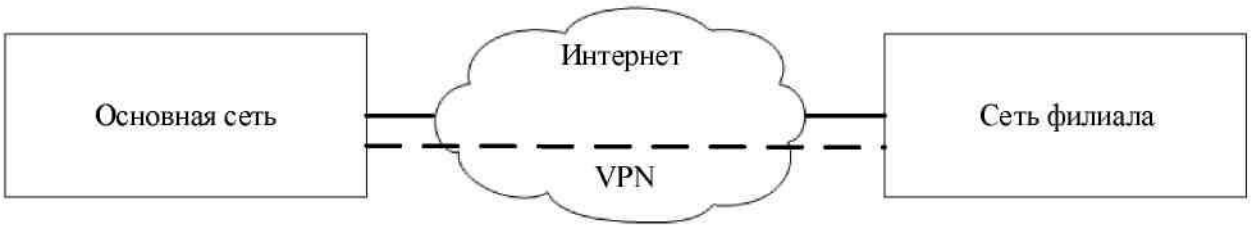

Рисунок 1 – Общая топология сети

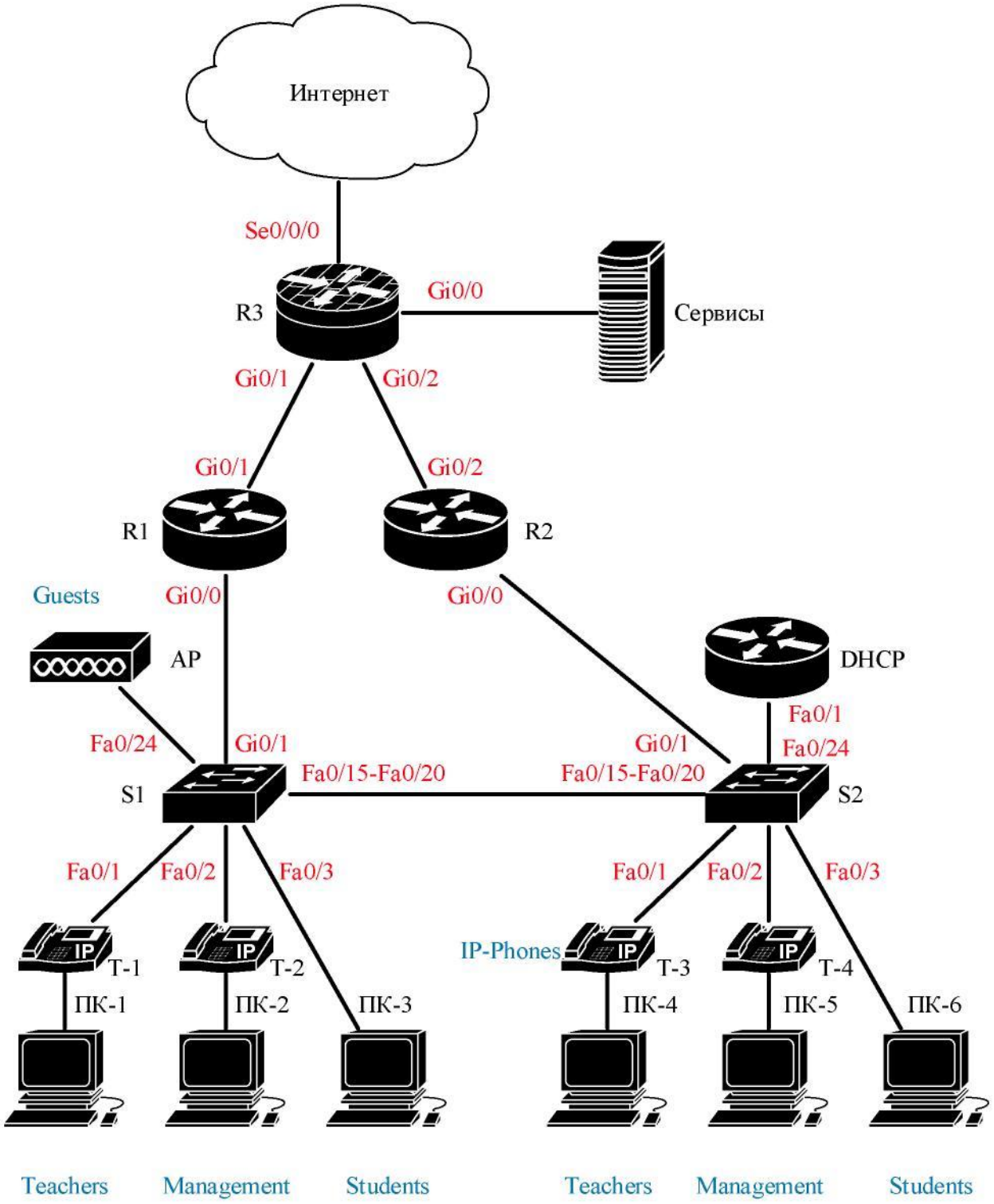

Рисунок 2 – Топология основной сети (синим цветом указана принадлежность портов к VLAN)

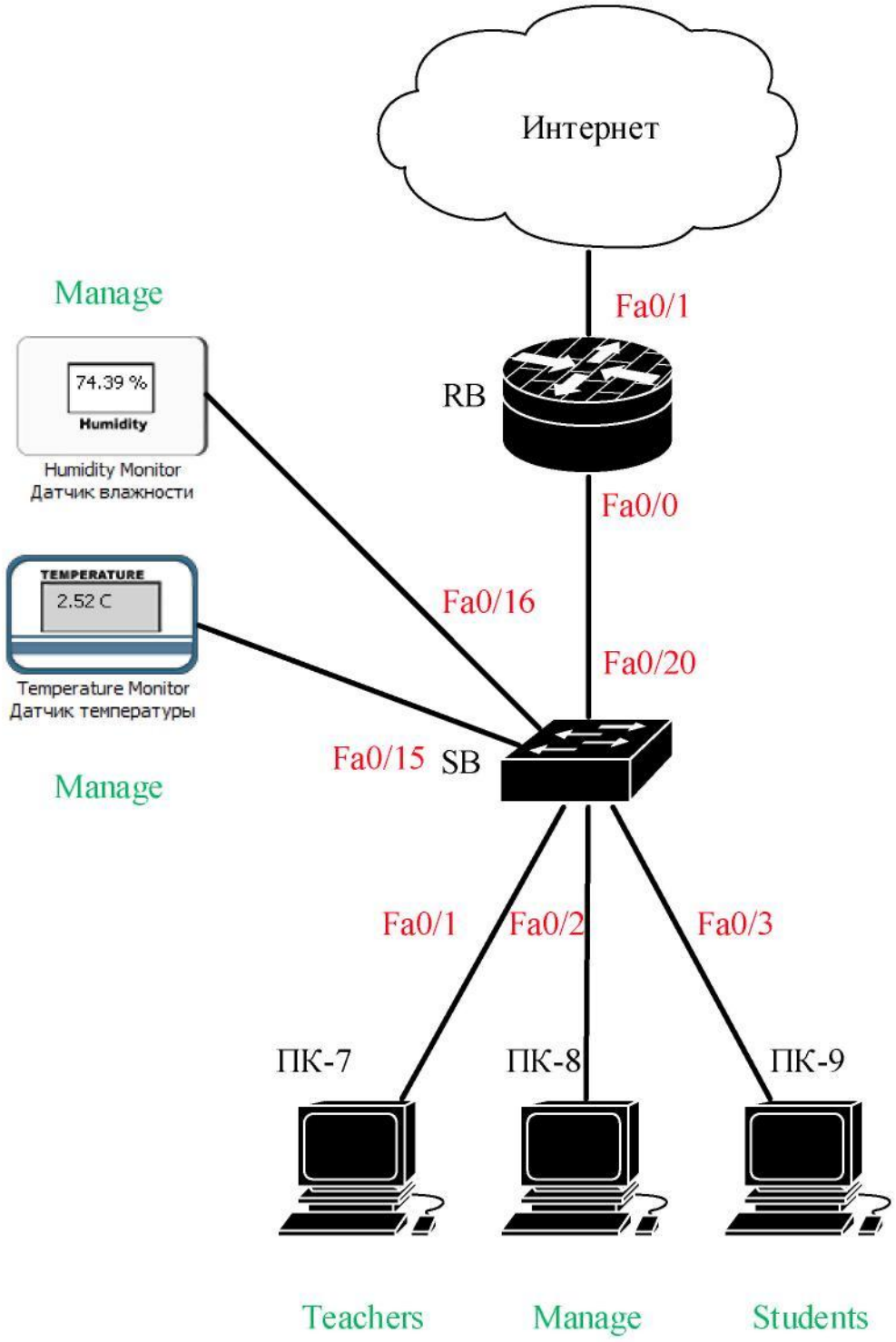

Рисунок.3 –Топология сети филиала