

Задание инвариантной части практического задания II уровня (демоверсия)

Часть 1

Исходные данные:

Под вашим управлением находится сеть, состоящая из двух коммутаторов и маршрутизатора, изображенная на рис 1.

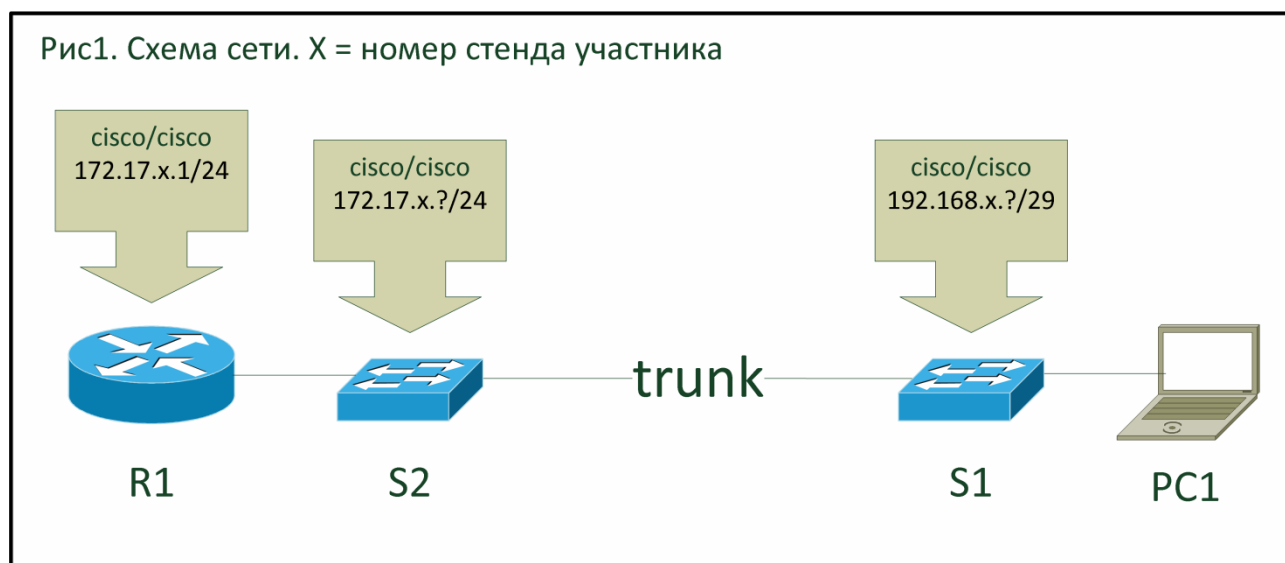
Коммутатор уровня доступа S1 был настроен и обслуживал клиентов, но по ошибке персонала на нем не была сохранена рабочая конфигурация, и при пропадании питания он вернулся к предыдущей, неверной конфигурации.

Вы знаете, что в предыдущей конфигурации на коммутатор S1 можно было попасть с его любого FastEthernet порта по telnet или SSH протоколам. Коммутатор имел последний адрес в бесклассовой сети 192.168.x.32/29 и пользователя cisco с паролем cisco.

Коммутатор S2 имеет рабочую конфигурацию и адрес в сети 172.17.x.0/24 и пользователя cisco с паролем cisco.

Маршрутизатор R1 имеет рабочую конфигурацию, первый адрес в сети 172.17.x.0/24 и пользователя cisco с паролем cisco.

При выполнении заданий вы будете должны найти несколько ошибок в конфигурациях, а также проявить свои знания на 1, 2 и 3-ем уровнях модели OSI.



Задание

1. Подключиться к коммутатору S1 и произвести его первичную настройку

- 1.1 Вычислить и записать адрес коммутатора S1, записать маску подсети в десятичном и двоичном виде, записать количество возможных хостов в этой сети.
- 1.2 Подключиться к коммутатору по протоколам telnet или SSH с использованием программы putty или стандартным telnet-клиентом Windows.
- 1.3 Удалить пользователя cisco и создать своего собственного с максимальными системными привилегиями и зашифрованным паролем. Запишите способ решения (использованные команды).

2. Необходимо подключиться к коммутатору S2 с коммутатора S1

- 2.1 Определить, какими интерфейсами соединены коммутаторы S1 и S2. Записать названия соответствующих интерфейсов в таблицу. Запишите способ решения.
- 2.2 Вы должны добиться прохождения ICMP - пакетов с коммутатора S1 до коммутатора S2. Адрес коммутатора S2 находится в подсети 172.17.x.0/24 и неизвестен вам.
 - 2.2.1 Найдите ошибку в конфигурации интерфейса/интерфейсов на коммутаторе S1 и устраните ее. Сконфигурируйте на соответствующем SVI интерфейсе коммутатора IP последний адрес из подсети 172.17.x.0/24. Остерегайтесь потери управления коммутатором S1 с вашей рабочей станции! Подумайте о правильной последовательности действий.
 - 2.2.2 Определите IP адрес коммутатора S2 максимальным количеством способов. Запишите адрес коммутатора S2 и способы его получения.
 - 2.2.3 Подключите вашу рабочую станцию к той же подсети 172.17.x.0/24. Проверьте доступность S1, S2, R1 с PC1.

3. Оптимизируйте использование имеющихся ресурсов

- 3.1 Коммутаторы S1 и S2 соединены двумя линками, однако в активном состоянии находится только один из них. Запишите причину.
- 3.2 Предложите способ использования обоих линков одновременно и настройте такое подключение. Запишите способ решения.

3.3 Обратите внимание, что гигабитные интерфейсы коммутаторов S1-S2 работают в режиме FastEthernet. Исправьте и запишите причины.

4. Зафиксируйте свои результаты.

4.1 Сохраните конфигурацию на TFTP сервер на вашей рабочей станции. Подумайте, все ли вы сделали для предотвращения повторения исходной ситуации.

Часть 2

Исходные данные:

Ваша сеть развивается (рис.2). Вы решили запустить собственный web-сервер и думаете о безопасном его размещении в Intranet. На рис.2 представлена схема демилитаризованной зоны (DMZ) с использованием одного маршрутизатора с функциями межсетевое экрана.

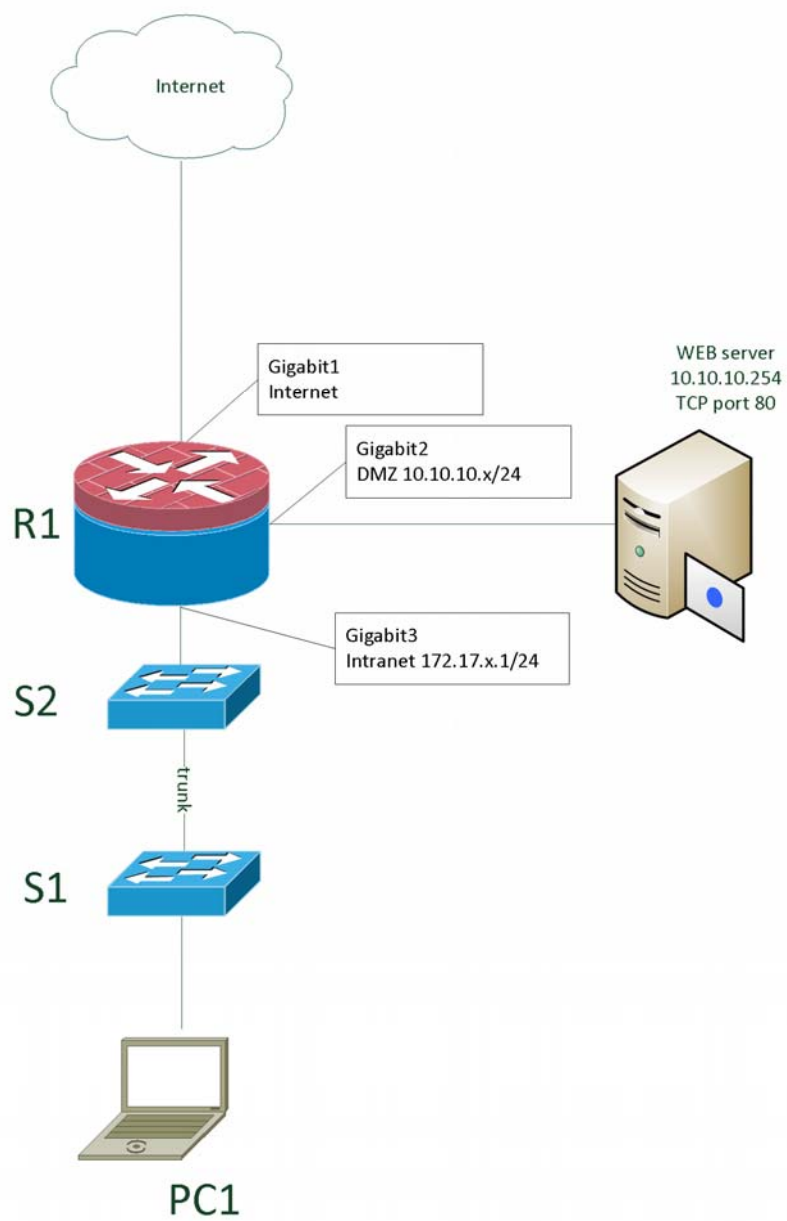
Вы хотите, чтобы ваш web-сервер был доступен из сети Internet по адресу интерфейса Gigabit1 маршрутизатора R1 по TCP порту 8080.

Ваш web-сервер должен быть доступен из сети Intranet по адресу 10.10.10.254 по tcp порту 80.

Из соображений безопасности вы не хотите, чтобы с web-сервера можно было попадать в сеть Intranet.

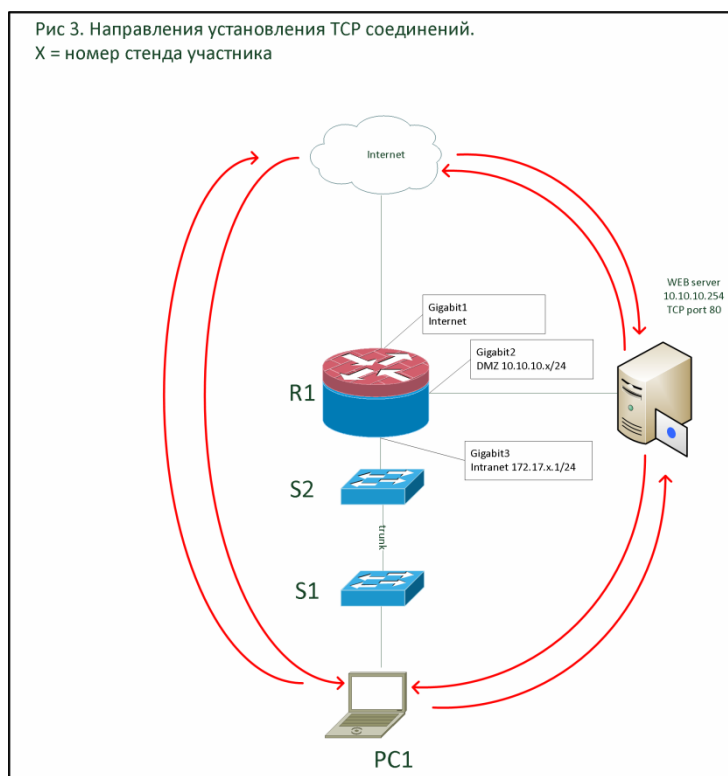
Пользователям сети Intranet вы хотите разрешить полный доступ в сеть Internet.

Рис 2. Схема сети с DMZ.
X = номер стенда участника



5. Рисуем направления разрешенных TCP-соединений

1.1 На рис 3 стрелками показаны направления TCP-соединений (от источника к назначению). Исходя из соображений безопасности, зачеркните лишние по вашему мнению направления.



6. Доступ PC1 в интернет

6.1 Подключитесь с вашей рабочей станции к маршрутизатору R1.

Проверьте доступ в интернет с маршрутизатора R1 с помощью ICMP. Отредактируйте конфигурацию маршрутизатора, если доступ отсутствует.

6.2 Подпишите на рис.3 интерфейсы Inside и Outside маршрутизатора R1.

6.3 Настройте трансляцию сетевых адресов для рабочей станции PC1 любого вида, используя адрес интерфейса Gigabit1, как внешний адрес.

7. Предоставляем доступ к web-серверу

7.1 Проверьте, есть ли у вас доступ к web-серверу по протоколу TCP, по порту 80, с рабочей станции.

7.2 На R1 настройте трансляцию сетевых адресов таким образом, чтобы web-сервер стал доступен из сети Internet по адресу интерфейса gigabit1 и порту TCP 8080

8. Думаем о безопасности

8.1С помощью списков доступа защитите маршрутизатор R1 от атак со стороны сети Internet таким образом, чтобы web-сервер остался доступным.

8.2С помощью списков доступа защитите вашу Intranet сеть от проникновения со стороны сети DMZ.

9. Зафиксируйте свои результаты.

Сохраните конфигурацию на TFTP сервер на вашей рабочей станции.

Список необходимых навыков:

- 1) Знание основ конфигурирования устройств на основе Cisco IOS
- 2) Умение использовать сетевые протоколы telnet/ssh
- 3) Понятие о протоколах физического уровня семейства Ethernet.
- 4) Работа с протоколами канального уровня, реализованных в коммутационном оборудовании основных производителей.
- 5) Знание адресного пространства IPv4 и умение в нем ориентироваться.
- 6) Понимание взаимосвязей уровней модели OSI.
- 7) Умение использовать встроенные средства оборудования для определения неисправностей.
- 8) Знание основ маршрутизации
- 9) Знание механизма преобразования адресов в сетях TCP/IP
- 10) Использование списков контроля доступа.

