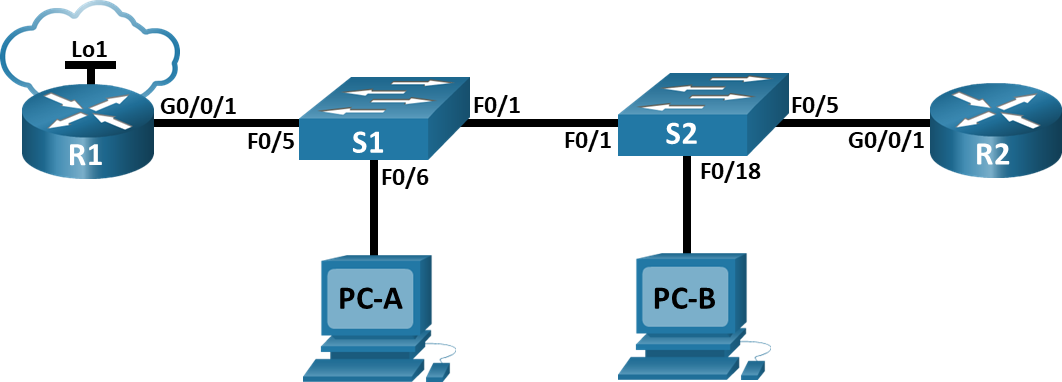
Лабораторная работа. Настройка и проверка расширенных списков контроля доступа.

# Топология



# Таблица адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска подсети | Шлюз по умолчанию |
| R1 | G0/0/1 | — | — | — |
| R1 | G0/0/1.20 | 10.20.0.1 | 255.255.255.0 | — |
| R1 | G0/0/1.30 | 10.30.0.1 | 255.255.255.0 | — |
| R1 | G0/0/1.40 | 10.40.0.1 | 255.255.255.0 | — |
| R1 | G0/0/1.1000 | — | — | — |
| R1 | Loopback1 | 172.16.1.1 | 255.255.255.0 | — |
| R2 | G0/0/1 | 10.20.0.4 | 255.255.255.0 | — |
| S1 | VLAN 20 | 10.20.0.2 | 255.255.255.0 | 10.20.0.1 |
| S2 | VLAN 20 | 10.20.0.3 | 255.255.255.0 | 10.20.0.1 |
| PC-A | NIC | 10.30.0.10 | 255.255.255.0 | 10.30.0.1 |
| PC-B | NIC | 10.40.0.10 | 255.255.255.0 | 10.40.0.1 |

# Таблица VLAN

| VLAN | Имя | Назначенный интерфейс |
| --- | --- | --- |
| 20 | Management | S2: F0/5 |
| 30 | Operations | S1: F0/6 |
| 40 | Sales | S2: F0/18 |
| 999 | ParkingLot | S1: F0/2-4, F0/7-24, G0/1-2  S2: F0/2-4, F0/6-17, F0/19-24, G0/1-2 |
| 1000 | Собственная | — |

# Задачи

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Настройка и проверка списков расширенного контроля доступа

# Общие сведения и сценарий

Вам было поручено настроить списки контроля доступа в сети небольшой компании. ACL являются одним из самых простых и прямых средств управления трафиком уровня 3. R1 будет размещать интернет-соединение (смоделированное интерфейсом Loopback 1) и предоставлять информацию о маршруте по умолчанию для R2. После завершения первоначальной настройки компания имеет некоторые конкретные требования к безопасности дорожного движения, которые вы несете ответственность за реализацию.

**Примечание**: Маршрутизаторы, используемые в практических лабораторных работах CCNA, - это Cisco 4221 с Cisco IOS XE Release 16.9.4 (образ universalk9). В лабораторных работах используются коммутаторы Cisco Catalyst 2960 с Cisco IOS версии 15.2(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Правильные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

**Примечание.** Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены в этом, обратитесь к инструктору.

# Необходимые ресурсы

* 2 маршрутизатора (Cisco 4221 с универсальным образом Cisco IOS XE версии 16.9.4 или аналогичным)
* 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.2(2) (образ lanbasek9) или аналогичная модель)
* 2 ПК (ОС Windows с программой эмуляции терминалов, такой как Tera Term)
* Консольные кабели для настройки устройств Cisco IOS через консольные порты.
* Кабели Ethernet, расположенные в соответствии с топологией

# Инструкции

## Создание сети и настройка основных параметров устройства

### Создайте сеть согласно топологии.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

### Произведите базовую настройку маршрутизаторов.

Откройте окно конфигурации

* + - 1. Назначьте маршрутизатору имя устройства.
      2. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
      3. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
      4. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.
      5. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.
      6. Зашифруйте открытые пароли.
      7. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
      8. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Закройте окно настройки.

### Настройте базовые параметры каждого коммутатора.

Откройте окно конфигурации

* + - 1. Присвойте коммутатору имя устройства.
      2. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
      3. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
      4. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.
      5. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.
      6. Зашифруйте открытые пароли.
      7. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
      8. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Закройте окно настройки.

## Настройка сетей VLAN на коммутаторах.

### Создайте сети VLAN на коммутаторах.

Откройте окно конфигурации

* + - 1. Создайте необходимые VLAN и назовите их на каждом коммутаторе из приведенной выше таблицы.
      2. Настройте интерфейс управления и шлюз по умолчанию на каждом коммутаторе, используя информацию об IP-адресе в таблице адресации.
      3. Назначьте все неиспользуемые порты коммутатора VLAN Parking Lot, настройте их для статического режима доступа и административно деактивируйте их.

Примечание. Команда interface range полезна для выполнения этой задачи с помощью необходимого количества команд.

### Назначьте сети VLAN соответствующим интерфейсам коммутатора.

* + - 1. Назначьте используемые порты соответствующей VLAN (указанной в таблице VLAN выше) и настройте их для режима статического доступа.
      2. Выполните команду **show vlan brief**, чтобы убедиться, что сети VLAN назначены правильным интерфейсам.

Закройте окно настройки.

## ·Настройте транки (магистральные каналы).

### Вручную настройте магистральный интерфейс F0/1.

Откройте окно конфигурации

* + - 1. Измените режим порта коммутатора на интерфейсе F0/1, чтобы принудительно создать магистральную связь. Не забудьте сделать это на обоих коммутаторах.
      2. В рамках конфигурации транка установите для native vlan значение 1000 на обоих коммутаторах. При настройке двух интерфейсов для разных собственных VLAN сообщения об ошибках могут отображаться временно.
      3. В качестве другой части конфигурации транка укажите, что VLAN 10, 20, 30 и 1000 разрешены в транке.
      4. Выполните команду **show interfaces trunk** для проверки портов магистрали, собственной VLAN и разрешенных VLAN через магистраль.

### Вручную настройте магистральный интерфейс F0/5 на коммутаторе S1.

* + - 1. Настройте интерфейс S1 F0/5 с теми же параметрами транка, что и F0/1. Это транк до маршрутизатора.
      2. Сохраните текущую конфигурацию в файл загрузочной конфигурации.
      3. Используйте команду **show interfaces trunk** для проверки настроек транка.

Закройте окно настройки.

## Настройте маршрутизацию.

### Настройка маршрутизации между сетями VLAN на R1.

Откройте окно конфигурации

* + - 1. Активируйте интерфейс G0/0/1 на маршрутизаторе.
      2. Настройте подинтерфейсы для каждой VLAN, как указано в таблице IP-адресации. Все подинтерфейсы используют инкапсуляцию 802.1Q. Убедитесь, что подинтерфейс для собственной VLAN не имеет назначенного IP-адреса. Включите описание для каждого подинтерфейса.
      3. Настройте интерфейс Loopback 1 на R1 с адресацией из приведенной выше таблицы.
      4. С помощью команды **show ip interface brief** проверьте конфигурацию подынтерфейса.

### Настройка интерфейса R2 g0/0/1 с использованием адреса из таблицы и маршрута по умолчанию с адресом следующего перехода 10.20.0.1

Закройте окно настройки.

## Настройте удаленный доступ

### Настройте все сетевые устройства для базовой поддержки SSH.

Откройте окно конфигурации

* + - 1. Создайте локального пользователя с именем пользователя SSHadmin и зашифрованным паролем $cisco123!
      2. Используйте **ccna-lab.com** в качестве доменного имени.
      3. Генерируйте криптоключи с помощью 1024 битного модуля.
      4. Настройте первые пять линий VTY на каждом устройстве, чтобы поддерживать только SSH-соединения и с локальной аутентификацией.

### Включите защищенные веб-службы с проверкой подлинности на R1.

* + - 1. Включите сервер HTTPS на R1.

R1(config)# **ip http secure-server**

* + - 1. Настройте R1 для проверки подлинности пользователей, пытающихся подключиться к веб-серверу.

R1(config)# **ip http authentication local**

Закройте окно настройки.

## Проверка подключения

### Настройте узлы ПК.

Адреса ПК можно посмотреть в таблице адресации.

### Выполните следующие тесты. Эхозапрос должен пройти успешно.

**Примечание.** Возможно, вам придется отключить брандмауэр ПК для работы ping

| От | Протокол | Назначение |
| --- | --- | --- |
| PC-A | Ping | 10.40.0.10 |
| PC-A | Ping | 10.20.0.1 |
| PC-B | Ping | 10.30.0.10 |
| PC-B | Ping | 10.20.0.1 |
| PC-B | Ping | 172.16.1.1 |
| PC-B | HTTPS | 10.20.0.1 |
| PC-B | HTTPS | 172.16.1.1 |
| PC-B | SSH | 10.20.0.1 |
| PC-B | SSH | 172.16.1.1 |

## Настройка и проверка списков контроля доступа (ACL)

При проверке базового подключения компания требует реализации следующих политик безопасности:

**Политика**1. Сеть Sales не может использовать SSH в сети Management (но в другие сети SSH разрешен).

**Политика 2**. Сеть Sales не имеет доступа к IP-адресам в сети Management с помощью любого веб-протокола (HTTP/HTTPS). Сеть Sales также не имеет доступа к интерфейсам R1 с помощью любого веб-протокола. Разрешён весь другой веб-трафик (обратите внимание — Сеть Sales может получить доступ к интерфейсу Loopback 1 на R1).

**Политика**3. Сеть Sales не может отправлять эхо-запросы ICMP в сети Operations или Management. Разрешены эхо-запросы ICMP к другим адресатам.

**Политика 4**: Cеть Operations не может отправлять ICMP эхозапросы в сеть Sales. Разрешены эхо-запросы ICMP к другим адресатам.

### Проанализируйте требования к сети и политике безопасности для планирования реализации ACL.

### Разработка и применение расширенных списков доступа, которые будут соответствовать требованиям политики безопасности.

Откройте окно конфигурации

Закройте окно настройки.

### Убедитесь, что политики безопасности применяются развернутыми списками доступа.

Выполните следующие тесты. Ожидаемые результаты показаны в таблице:

|  |  |  |  |
| --- | --- | --- | --- |
| От | Протокол | Назначение | Результат |
| PC-A | Ping | 10.40.0.10 | Сбой |
| PC-A | Ping | 10.20.0.1 | Успех |
| PC-B | Ping | 10.30.0.10 | Сбой |
| PC-B | Ping | 10.20.0.1 | Сбой |
| PC-B | Ping | 172.16.1.1 | Успех |
| PC-B | HTTPS | 10.20.0.1 | Сбой |
| PC-B | HTTPS | 172.16.1.1 | Успех |
| PC-B | SSH | 10.20.0.4 | Сбой |
| PC-B | SSH | 172.16.1.1 | Успех |

Конец документа