ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
Сибирский колледж транспорта и строительства

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

К ПРАКТИЧЕСКИМ РАБОТАМ

ПМ.01 ВЫПОЛНЕНИЕ РАБОТ ПО ПРОЕКТИРОВАНИЮ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

МДК.01.01 Компьютерные сети

Тема 1.2. Принципы маршрутизации и коммутации по специальности

09.02.06 Сетевое и системное администрирование

базовая подготовка среднего профессионального образования

Иркутск 2022

РАССМОТРЕНО:
Цикловой методической
комиссией специальности 09.02.06
Сетевое и системное
администрирование
«08» июня 2022 г.
Председатель: _____/Саквенко Т.В.

СОГЛАСОВАНО:
Заместитель директора по УВР
_____/А.П.Ресельс
«09» июня 2022 г.

Разработчики: Фитисова Н.Н., преподаватель высшей категории Сибирского колледжа транспорта и строительства ФГБОУ ВО «Иркутский государственный университет путей сообщения».

Практическая работа 1. Обеспечение безопасности сетевых устройств

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	—
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка базовых мер безопасности на маршрутизаторе

Часть 3. Настройка базовых мер безопасности на коммутаторе

Общие сведения/сценарий

Все сетевые устройства рекомендуется настраивать с использованием хотя бы минимального набора эффективных команд обеспечения безопасности. Это относится к устройствам конечных пользователей, серверам и сетевым устройствам, таким как маршрутизаторы и коммутаторы.

В ходе лабораторной работы вы должны будете настроить сетевые устройства в топологии таким образом, чтобы разрешать SSH-соединения для удаленного управления. Кроме того, вы должны будете настроить основные эффективные меры обеспечения безопасности через интерфейс командной строки операционной системы Cisco IOS. Затем вам необходимо будет протестировать меры обеспечения безопасности и убедиться в том, что они правильно внедрены и работают без ошибок.

Примечание. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4) M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(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. Точные 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, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с ПО Cisco IOS версии 15.2(4)M3 с универсальным образом или аналогичная модель)
- 1 коммутатор (Cisco 2960 с ПО Cisco IOS версии 15.0(2) с образом lanbasek9 или аналогичная модель)
- 1 ПК (под управлением Windows 7 или 8 с программой эмуляции терминала, например, Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Настройка основных параметров устройств

В части 1 потребуется настроить топологию сети и основные параметры, такие как IP-адреса интерфейсов, доступ к устройствам и пароли на устройствах.

Шаг 1: Создайте сеть согласно топологии.

Подключите устройства, показанные в топологии, и кабели соответствующим образом.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Выполните настройку маршрутизатора и коммутатора.

a. Подключитесь к устройству с помощью консольного подключения и активируйте привилегированный режим EXEC.

b. Назначьте устройству имя в соответствии с таблицей адресации.

c. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

d. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

e. Назначьте cisco в качестве пароля консоли и включите вход в систему по паролю.

f. Назначьте cisco в качестве пароля VTY и включите вход в систему по паролю.

g. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

h. Настройте и активируйте на маршрутизаторе интерфейс G0/1, используя информацию, приведенную в таблице адресации.

i. Задайте для используемого по умолчанию интерфейса SVI сведения об IP-адресе согласно таблице адресации.

j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Часть 2: Настройка базовых мер безопасности на маршрутизаторе

Шаг 1: Зашифруйте открытые пароли.

```
R1(config)# service password-encryption
```

Шаг 2: Установите более надежные пароли.

Администратор должен следить за тем, чтобы пароли отвечали стандартным рекомендациям по созданию надежных паролей. В рекомендациях должны быть определены сочетания в пароле букв, цифр и специальных символов и его минимальная длина.

Примечание. Согласно данным рекомендациям по лучшим практическим методикам надежные пароли, примеры которых приведены в этой лабораторной работе, необходимо всегда использовать в реальной работе. Однако для упрощения выполнения работы в остальных лабораторных работах данного курса используются пароли cisco и class.

a. Измените зашифрованный пароль привилегированного режима EXEC в соответствии с рекомендациями.

```
R1(config)# enable secret Enable1p@55
```

b. Установите минимальную длину 10 символов для всех паролей.

```
R1(config)# security passwords min-length 10
```

Шаг 3: Разрешите подключения по протоколу SSH.

a. В качестве имени домена укажите CCNA-lab.com.

```
R1(config)# ip domain-name CCNA-lab.com
```

b. Создайте в базе данных локальных пользователей запись, которая будет использоваться при подключении к маршрутизатору через SSH. Пароль должен соответствовать стандартам надежных паролей, а пользователь — иметь права доступа уровня EXEC. Если уровень привилегий не задан в команде, то пользователь по умолчанию будет иметь права доступа EXEC (уровень 15).

```
R1(config)# username SSHadmin privilege 15 secret Admin1p@55
```

c. Настройте транспортный вход для линий VTY таким образом, чтобы они могли разрешать подключения по протоколу SSH, но не разрешали подключения по протоколу Telnet.

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

d. Аутентификация на линиях VTY должна выполняться с использованием базы данных локальных пользователей.

```
R1(config line)# login local
R1(config-line)# exit
```

e. Создайте ключ шифрования RSA с длиной 1024 бит.

```
R1(config)# crypto key generate rsa modulus 1024
```

Шаг 4: Обеспечьте защиту консоли и линий VTY.

a. Маршрутизатор можно настроить таким образом, чтобы он завершал сеанс подключения в случае отсутствия активности в течение заданного времени. Если сетевой администратор вошел в систему сетевого устройства, а потом был внезапно вынужден покинуть рабочее место, то по истечении установленного времени эта команда автоматически завершит сеанс подключения. Приведенные ниже команды обеспечивают закрытие сеанса линии связи через пять минут отсутствия активности.

```
R1(config)# line console 0
R1(config-line)# exec-timeout 5 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 5 0
R1(config-line)# exit
R1(config)#
```

b. Команда, приведенная ниже, не разрешает вход в систему с использованием метода полного перебора. Маршрутизатор блокирует попытки входа в систему на 30 секунд, если в течение 120

секунд будет дважды введен неверный пароль. Низкое значение этого таймера установлено специально для данной лабораторной работы.

заблокировать на 30 секунд

2 неудачные попытки в течение 120 секунд

```
R1(config)# login block-for 30 attempts 2 within 120
```

Что означает 2 within 120 в приведенной выше команде?

Что означает block-for 30 в приведенной выше команде?

Шаг 5: Убедитесь, что все неиспользуемые порты отключены.

Порты маршрутизатора отключены по умолчанию, однако рекомендуется лишний раз убедиться, что все неиспользуемые порты отключены администратором. Для этого можно воспользоваться командой show ip interface brief. Все неиспользуемые порты, не отключенные администратором, необходимо отключить с помощью команды shutdown в режиме конфигурации интерфейса.

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                unassigned      YES NVRAM  administratively down down
Serial0/0/1                unassigned      YES NVRAM  administratively down down
R1#
```

Шаг 6: Убедитесь, что все меры безопасности внедрены правильно.

a. С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколу Telnet. Разрешает ли R1 подключение по протоколу Telnet? Дайте пояснение.

- Нет, Telnet не был активирован во время настройки маршрутизатора.

a. С помощью программы Tera Term подключитесь к маршрутизатору R1 по протоколу SSH. Разрешает ли R1 подключение по протоколу SSH? Да.

b. Намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе после двух неудачных попыток.

Что произошло после ввода неправильных данных для входа в систему во второй раз?

Маршрутизатор отклоняет входящие соединения по протоколу SSH.

c. Из сеанса подключения к маршрутизатору с помощью консоли отправьте команду show login, чтобы проверить состояние входа в систему. В приведенном ниже примере команда show login была введена в течение 30-секундной блокировки доступа к системе и показывает, что маршрутизатор находится в режиме Quiet. Маршрутизатор не будет разрешать попытки входа в систему в течение еще 14 секунд.

```
R1# show login
     A default login delay of 1 second is applied.
     No Quiet-Mode access list has been configured.

     Router enabled to watch for login attacks.


     If more than 2 login failures occur in 120 seconds or less,
     logins will be disabled for 30 seconds.

     Router presently in Quiet Mode.
     Will remain in Quiet-Mode for 14 seconds.
     Denying logins from all sources.
R1#
```

d. По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и войдите в систему, используя имя SSHadmin и пароль Admin1p@55.

Что отобразилось после успешного входа в систему?

Баннер MOTD и интерпретатор.

e. Войдите в привилегированный режим EXEC и введите в качестве пароля Enablep@55.

Если вы неправильно вводите пароль, прерывается ли сеанс SSH после двух неудачных попыток в течение 120 секунд? Дайте пояснение.

Нет, так как login block-for защищает вход в консоль, а не в привилегированный режим EXEC.

f. Введите команду show running-config в строке приглашения привилегированного режима EXEC для просмотра установленных параметров безопасности.

Часть 3: Настройка базовых мер безопасности на коммутаторе

Шаг 1: Зашифруйте открытые пароли.

```
S1(config)# service password-encryption
```

Шаг 2: Установите более надежные пароли на коммутаторе.

Измените зашифрованный пароль привилегированного режима EXEC в соответствии с рекомендациями по установке надежного пароля.

```
S1(config)# enable secret Enable1p@55
```

Примечание. Команда безопасности password min-length на коммутаторах модели 2960 недоступна.

Шаг 3: Разрешите подключения по протоколу SSH.

a. В качестве имени домена укажите CCNA-lab.com.

```
S1(config)# username SSHadmin privilege 1 secret Admin1p@55
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config)# ip domain-name CCNA-lab.com
```

b. Создайте в базе данных локальных пользователей запись, которая будет использоваться при подключении к коммутатору через SSH. Пароль должен соответствовать стандартам надежных паролей, а пользователь — иметь права доступа уровня EXEC. Если уровень привилегий не задан в команде, то пользователь по умолчанию будет иметь права доступа EXEC (уровень 1).

c. Настройте транспортный вход для линий VTY таким образом, чтобы они могли разрешать подключения по протоколу SSH, но не разрешали подключения по протоколу Telnet.

d. Аутентификация на линиях VTY должна выполняться с использованием базы данных локальных пользователей.

```
S1(config line)# login local
S1(config line)# exit
```

e. Создайте ключ шифрования RSA с длиной 1024 бит.

```
S1(config)# crypto key generate rsa modulus 1024
```

Шаг 4: Обеспечьте защиту консоли и линий VTY.

a. Настройте коммутатор таким образом, чтобы он закрывал линию через десять минут отсутствия активности.

```
S1(config)# line console 0
S1(config-line)# exec-timeout 10 0
S1(config-line)# line vty 0 15
S1(config-line)# exec-timeout 10 0
S1(config-line)# exit
S1(config)#
```

b. Чтобы помешать попыткам входа в систему с использованием метода полного перебора, настройте коммутатор таким образом, чтобы он блокировал доступ к системе на 30 секунд после двух неудачных попыток входа в течение 120 секунд. Низкое значение этого таймера установлено специально для данной лабораторной работы.

```
S1(config)# login block-for 30 attempts 2 within 120
S1(config)# end
```

Шаг 5: Убедитесь, что все неиспользуемые порты отключены.

По умолчанию порты коммутатора включены. Отключите на коммутаторе все неиспользуемые порты.

a. Состояние портов коммутатора можно проверить с помощью команды show ip interface brief.

S1# show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.11	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down

FastEthernet0/2 0	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
FastEthernet0/22	unassigned	YES	unset	down	down
FastEthernet0/23	unassigned	YES	unset	down	down
FastEthernet0/2 4	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

S1#

b. Чтобы отключить сразу несколько интерфейсов, воспользуйтесь командой interface range.

```
S1(config)# interface range f0/1-4 , f0/7-24 , g0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

c. Убедитесь, что все неактивные интерфейсы отключены администратором. `S1# show ip interface brief`

Interface	IP-Address	OK?	Method	Status		Protocol
Vlan1	192.168.1.11	YES	manual	up		up
FastEthernet0/1	unassigned	YES	unset	administratively	down	down
FastEthernet0/2	unassigned	YES	unset	administratively	down	down
FastEthernet0/3	unassigned	YES	unset	administratively	down	down
FastEthernet0/4	unassigned	YES	unset	administratively	down	down
FastEthernet0/5	unassigned	YES	unset	up		up
FastEthernet0/6	unassigned	YES	unset	up		up
FastEthernet0/7	unassigned	YES	unset	administratively	down	down
FastEthernet0/8	unassigned	YES	unset	administratively	down	down
FastEthernet0/9	unassigned	YES	unset	administratively	down	down
FastEthernet0/10	unassigned	YES	unset	administratively	down	down
FastEthernet0/11	unassigned	YES	unset	administratively	down	down
FastEthernet0/12	unassigned	YES	unset	administratively	down	down
FastEthernet0/13	unassigned	YES	unset	administratively	down	down
FastEthernet0/14	unassigned	YES	unset	administratively	down	down
FastEthernet0/15	unassigned	YES	unset	administratively	down	down

FastEthernet0/16	unassigned	YES	unset	administratively	down	down
FastEthernet0/17	unassigned	YES	unset	administratively	down	down
FastEthernet0/18	unassigned	YES	unset	administratively	down	down
FastEthernet0/19	unassigned	YES	unset	administratively	down	down
FastEthernet0/2 0	unassigned	YES	unset	administratively	down	down
FastEthernet0/21	unassigned	YES	unset	administratively	down	down
FastEthernet0/22	unassigned	YES	unset	administratively	down	down
FastEthernet0/23	unassigned	YES	unset	administratively	down	down
FastEthernet0/2 4	unassigned	YES	unset	administratively	down	down

Шаг 6: Убедитесь, что все меры безопасности внедрены правильно.

Убедитесь, что протокол Telnet на коммутаторе отключен.

Подключитесь к коммутатору по протоколу SSH и намеренно укажите неверное имя пользователя и пароль, чтобы проверить, будет ли заблокирован доступ к системе.

По истечении 30 секунд повторите попытку подключения к R1 по протоколу SSH и войдите в систему, используя имя пользователя SSHadmin и пароль Admin1p@55.

Появился ли баннер после успешного входа в систему?

Войдите в привилегированный режим EXEC, используя Enablep@55 в качестве пароля.

Введите команду show running-config в строке приглашения привилегированного режима EXEC для просмотра установленных параметров безопасности.

Вопросы для повторения

1. В части 1 для консоли и линий VTY в вашей базовой конфигурации была введена команда password cisco. Когда используется этот пароль после применения наиболее эффективных мер обеспечения безопасности?

При подключении через консольный порт будет запрошен именно этот пароль «cisco».

2. Распространяется ли команда security passwords min-length 10 на настроенные ранее пароли, содержащие меньше десяти символов?

Нет.

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet № 1	Интерфейс Ethernet №2	Последовательный интерфейс № 1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/0/0)	Serial 0/1/1 (S0/0/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса.				

Практическая работа 2: доступ к сетевым устройствам по протоколу SSH

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
ПК-А	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть1. Настройка основных параметров устройства

Часть2. Настройка маршрутизатора для доступа по протоколу SSH

Часть3. Проверка сеанса связи по протоколу Telnet с помощью программы Wireshark

Часть4. Проверка сеанса связи по протоколу SSH с помощью программы Wireshark

Часть5. Настройка коммутатора для доступа по протоколу SSH

Часть6. Настройка протокола SSH в интерфейсе командной строки коммутатора

Исходные данные/сценарий

Раньше для удалённой настройки сетевых устройств в основном применялся протокол Telnet. При этом протоколы типа Telnet не включают проверку подлинности и шифрование информации, передаваемой между клиентом и сервером, что позволяет сетевым средствам слежения перехватывать пароли и данные конфигурации.

Secure Shell(SSH)— это сетевой протокол, устанавливающий безопасное подключение эмулятора терминала к маршрутизатору или иному сетевому устройству. Протокол SSH шифрует все сведения, которые поступают по сетевому каналу, и предусматривает аутентификацию удалённого компьютера. Протокол SSH всё больше заменяет Telnet — именно его выбирают сетевые специалисты в качестве средства удалённого входа в систему. Чаще всего протокол SSH

применяется для входа на удалённое устройство и выполнения команд, но может также передавать файлы по связанным протоколам SFTP или SCP.

Чтобы протокол SSH работал, на взаимодействующих сетевых устройствах должна быть настроена его поддержка. В ходе лабораторной работы вы активируете на маршрутизаторе SSH-сервер и подключитесь к маршрутизатору, используя ПК с клиентом SSH. В локальной сети подключение обычно устанавливается с помощью Ethernet и IP-адреса.

Кроме того, в ходе лабораторной работы вы настроите маршрутизатор для приёма подключений по протоколу SSH и воспользуетесь программой Wireshark для перехвата и просмотра сеансов Telnet и SSH. Это покажет, какую важную роль играет шифрование данных, осуществляемое протоколом SSH. И, наконец, вам придётся самостоятельно настроить коммутатор для подключения по протоколу SSH.

Примечание. Маршрутизаторы, используемые на практических занятиях CCNA: маршрутизаторы с интеграцией сервисов серии Cisco 1941 (ISR) установленной версии Cisco IOS 15.2(4) M3 (образ universalk9). Используемые коммутаторы: семейство коммутаторов Cisco Catalyst 2960 версии CISCO IOS 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии CISCO IOS. В зависимости от модели и версии Cisco IOS выполняемые доступные команды и выводы могут отличаться от данных, полученных в ходе лабораторных работ. Точные идентификаторы интерфейса см. в таблице сводной информации об интерфейсах маршрутизаторов в конце данной лабораторной работы.

Примечание. Убедитесь, что информация, имеющаяся на маршрутизаторе и коммутаторе, удалена и они не содержат файлов загрузочной конфигурации. Если вы не уверены, что сможете это сделать, обратитесь к инструктору.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с универсальным образом M3 версии CISCO IOS 15.2(4) или аналогичным)
- 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- Один ПК (Windows 7, Vista или XP с эмулятором терминала, например Tera Term, и установленной программой Wireshark)
- Консольные кабели для настройки устройств CISCO IOS через консольные порты
- Кабели Ethernet в соответствии с топологией

Часть 1: Основные настройки устройства

В части 1 потребуется настройка топологии сети и основных параметров, таких как IP-адреса интерфейсов, доступ к устройствам и пароли на маршрутизаторе.

Шаг 1: Создайте сеть в соответствии с изображенной на схеме топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 3: Настройте маршрутизатор.

a. Подключите консоль к маршрутизатору и активируйте привилегированный режим.

b. Войдите в режим конфигурации.

c. Отключите поиск в DNS, чтобы предотвратить попытки маршрутизатора преобразовывать неверно введённые команды таким образом, как будто они являются именами узлов.

d. Назначьте class в качестве пароля привилегированного режима.

e. Назначьте cisco в качестве пароля консоли и включите вход по паролю.

f. Назначьте cisco в качестве пароля виртуального терминала и включите вход по паролю.

g. Зашифруйте пароли.

h. Создайте баннер, который предупреждает о запрете несанкционированного доступа.

i. Настройте и активируйте интерфейс маршрутизатора G0/1 с помощью сведений, содержащихся в таблице адресации.

j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте ПК-А.

a. Настройте на ПК-А IP-адрес и маску подсети.

b. Настройте на ПК-А шлюз по умолчанию.

Шаг 5: Проверьте подключение к сети.

Отправьте эхо-запрос с помощью команды ping с ПК-А на маршрутизатор R1. Если эхо-запрос с помощью команды ping не проходит, найдите и устраните неполадки подключения.

Часть 2: Настройка маршрутизатора для доступа по протоколу SSH

Подключение к сетевым устройствам по протоколу Telnet сопряжено с риском для безопасности, поскольку вся информация передаётся в виде открытого текста. Протокол SSH шифрует данные сессии и требует аутентификации устройств, поэтому для удалённых подключений

рекомендуется использовать именно его. В части 2 вам нужно настроить маршрутизатор для приёма соединений по протоколу SSH по линиям VTY.

Шаг 1: Настройте аутентификацию устройств.

При генерации ключа шифрования используются имя устройства и домен. Это значит, что эти имена необходимо указать перед вводом команды crypto key.

a. Укажите имя устройства.

```
Router(config)# hostname R1
```

b. Укажите домен для устройства.

```
R1(config)# ip domain-name ccna-lab.com
```

Шаг 2: Создайте ключ шифрования с указанием его длины.

```
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R1(config)#
*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Шаг 3: Создайте имя пользователя в локальной базе учётных записей.

```
R1(config)# username admin privilege 15 secret adminpass
R1(config)#
*Feb  6 [illegible]: [illegible]
R1(config)#
```

Примечание. Пятнадцатый уровень привилегий предоставляет пользователю права администратора.

Шаг 4: Активируйте протокол SSH на линиях VTY.

a. Активируйте протоколы Telnet и SSH на входящих линиях VTY с помощью команды transport input.

```
R1(config)# line vty 0 4
R1(config-line)# transport input telnet ssh
```

b. Измените способ входа в систему — выберите проверку пользователей по локальной базе учётных записей.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
R1(config-line)# login local
R1(config-line)# end
R1#
```

Шаг 5: Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Часть 3: Проверка сеанса связи по протоколу Telnet с помощью программы Wireshark

В части 3 вы воспользуетесь программой Wireshark для перехвата и просмотра данных, передаваемых во время сеанса связи маршрутизатора по протоколу Telnet. С помощью программы Tera Term вы подключитесь к маршрутизатору R1 по протоколу Telnet, войдёте в систему и запустите на маршрутизаторе команду show run.

Примечание. Если на вашем компьютере нет программного обеспечения клиента Telnet/SSH, его необходимо установить. Чаще всего для работы с протоколами Telnet и SSH используются программы Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) и PuTTy (www.putty.org).

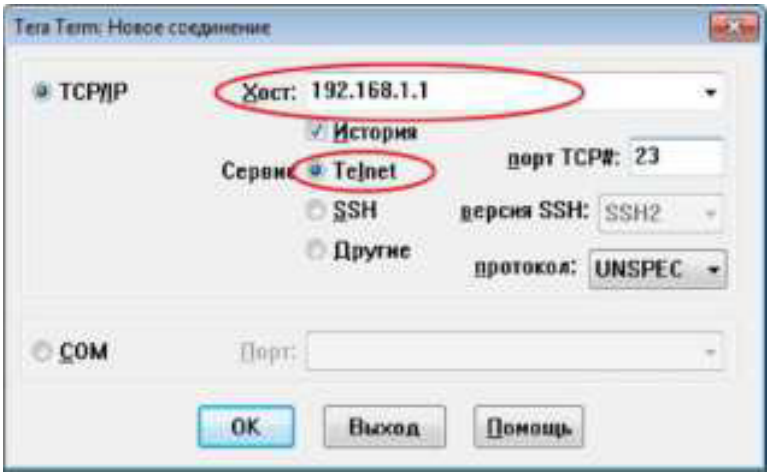
Примечание. По умолчанию доступ к Telnet из командной строки вWindows 7 отключён. Чтобы активировать подключение по протоколу Telnet из окна командной строки, нажмите кнопку Пуск >Панель управления>Программы>Программы и компоненты>Включение или отключение компонентов Windows. Установите флажок рядом с компонентом Клиент Telnet и нажмите кнопку OK.

Шаг 1: Откройте Wireshark и начните сбор данных в интерфейсе локальной сети.

Примечание. Если перехват данных в интерфейсе локальной сети запустить не удаётся, попробуйте открыть программу Wireshark с помощью параметра Запуск от имени администратора.

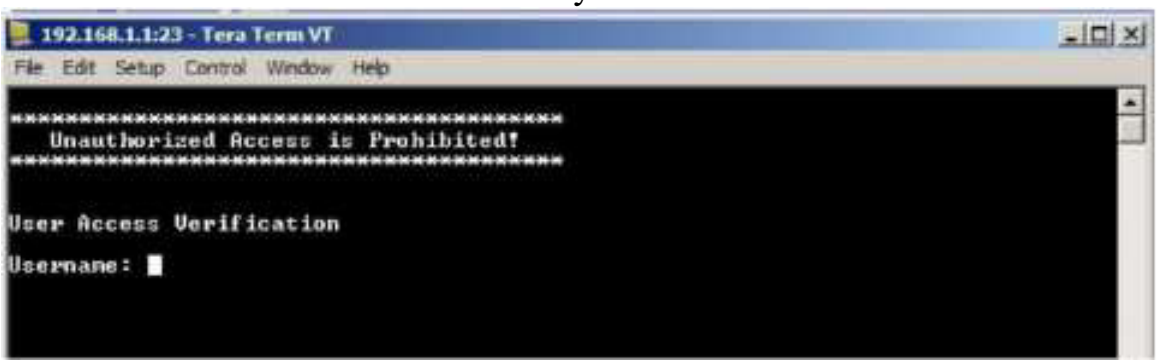
Шаг 2: Начните сеанс подключения к маршрутизатору по протоколу Telnet.

а. Запустите программу Tera Term, установите переключатель сервиса Telnet, а в поле «Host» введите 192.168.1.1



Какой порт TCP используется для сеансов Telnet по умолчанию?

b. В окне командной строки после приглашения Username: (Имя пользователя) введите admin, а после Password: (Пароль) — adminpass. Эти запросы появляются потому, что командой login local вы настроили линии VTY на использование локальной базы учётных записей.



c.Введите команду show run.

```
R1# show run
```

d.Введите команду exit, чтобы завершить сеанс работы с протоколом Telnet и выйти из программы Tera Term.

```
R1# exit
```

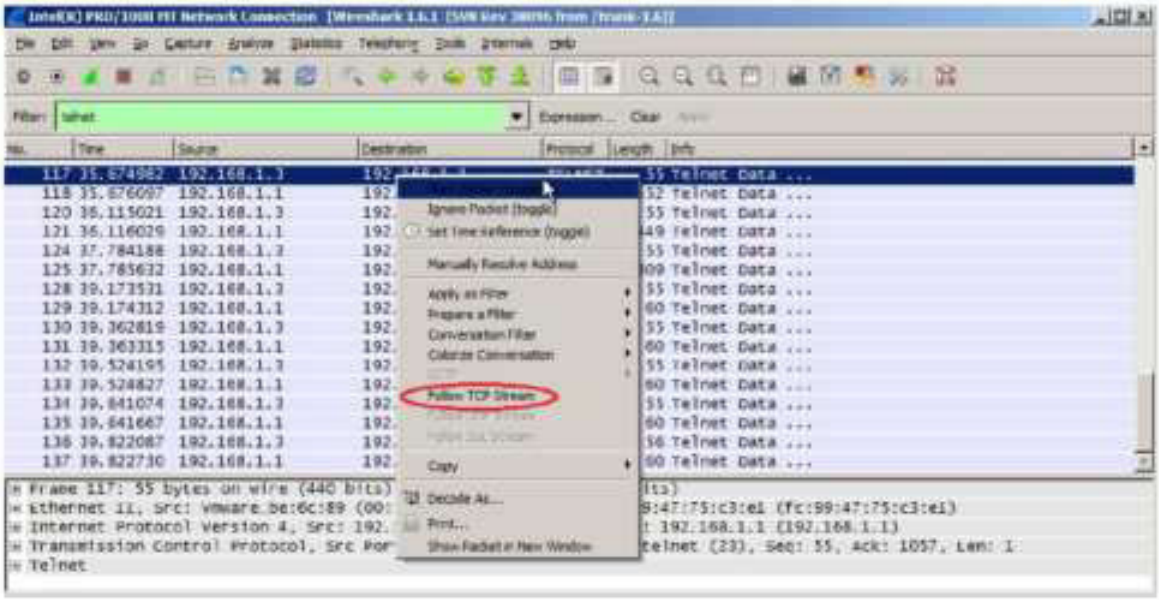
Шаг 3: Остановите сбор данных программой Wireshark.

Шаг 4: Примените один из фильтров Telnet для данных, собираемых программой Wireshark.

Шаг 5: Используйте функцию TCP в Wireshark для просмотра сеанса Telnet.

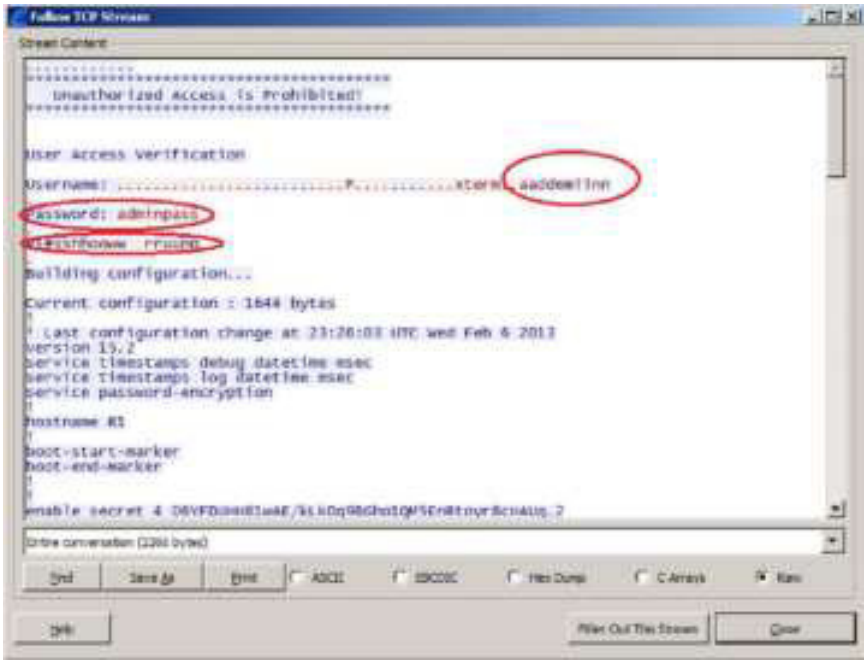
a. Нажмите правой кнопкой мыши на одну из строк Telnet в разделе Packet list (Список пакетов) программы Wireshark и выберите в

раскрывающемся списке пункт Follow TCP Stream (Следить за TCP-потоком).



b. В окне Follow TCP Stream (Следить за TCP-потоком) отображаются данные о текущем сеансе подключения к маршрутизатору по протоколу Telnet. Весь сеанс связи (включая пароль) отображается открытым текстом. Обратите внимание на то, что введённые имя пользователя и команда show run отображаются с повторяющимися символами. Это связано с настройкой отображения в Telnet, которая позволяет выводить на экран символы, набираемые на клавиату.

c. Закончив просмотр сеанса Telnet в окне Follow TCP Stream (Следить за TCP-потоком), нажмите кнопку Close (Закрыть).



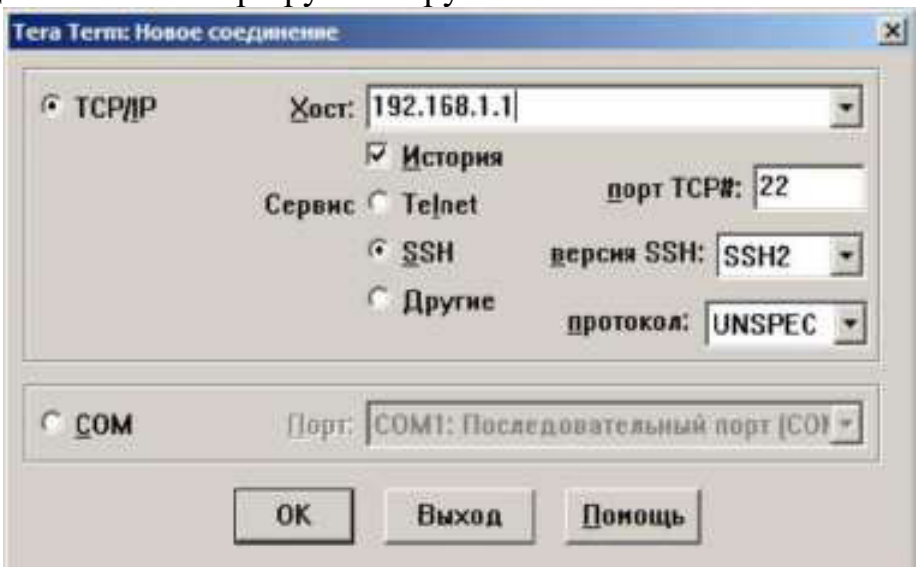
Часть 4: Проверка сеанса связи по протоколу SSH с помощью программы Wireshark

В части 4 вам нужно будет с помощью программы Tera Term установить сеанс подключения к маршрутизатору по протоколу SSH. Программа Wireshark будет использоваться для перехвата и просмотра данных этого сеанса.

Шаг 1: Откройте Wireshark и начните сбор данных в интерфейсе локальной сети.

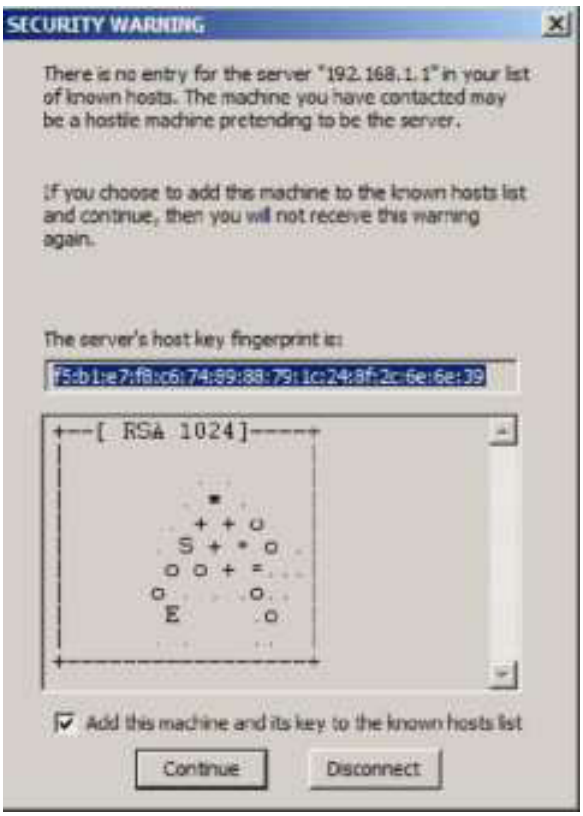
Шаг 2: Запустите на маршрутизаторе сеанс связи по протоколу SSH.

a. Откройте программу Tera Term и введите в поле «Host» окна «Tera Term: Новое соединение» IP- адрес интерфейса G0/1 маршрутизатора R1. Убедитесь в том, что переключатель SSH установлен, и нажмите кнопку OK для подключения к маршрутизатору.

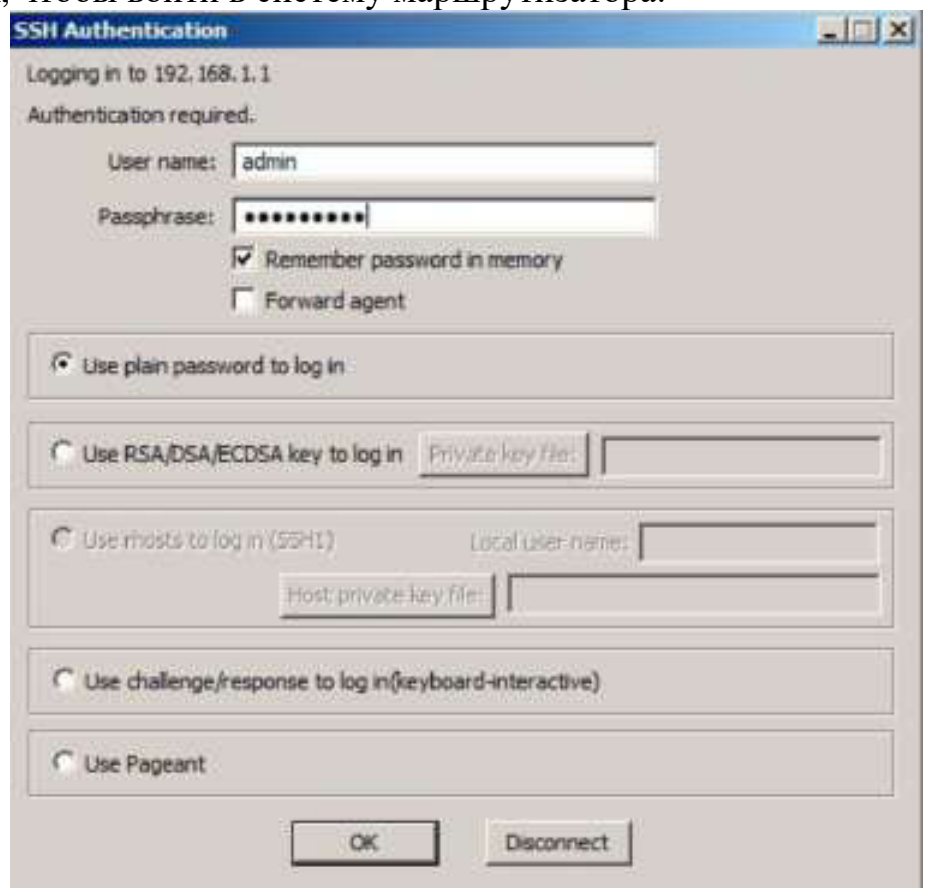


Какой порт TCP используется для сеансов SSH по умолчанию?

b. После первой установки подключения к устройству по протоколу SSH откроется окно SECURITY WARNING (Предупреждение безопасности), которое означает, что вы ещё не подключались к этому устройству. Это сообщение является частью процесса аутентификации. Прочтите текст предупреждения безопасности и нажмите кнопку Continue (Продолжить).



c. В окне SSH Authentication (Аутентификация SSH) в качестве имени пользователя укажите admin, а в качестве пароля — adminpass. Нажмите кнопку OK, чтобы войти в систему маршрутизатора.



d. Вы установили сеанс SSH на маршрутизаторе. Окно программы Tera Term очень похоже на окно командной строки. После приглашения введите команду show run.

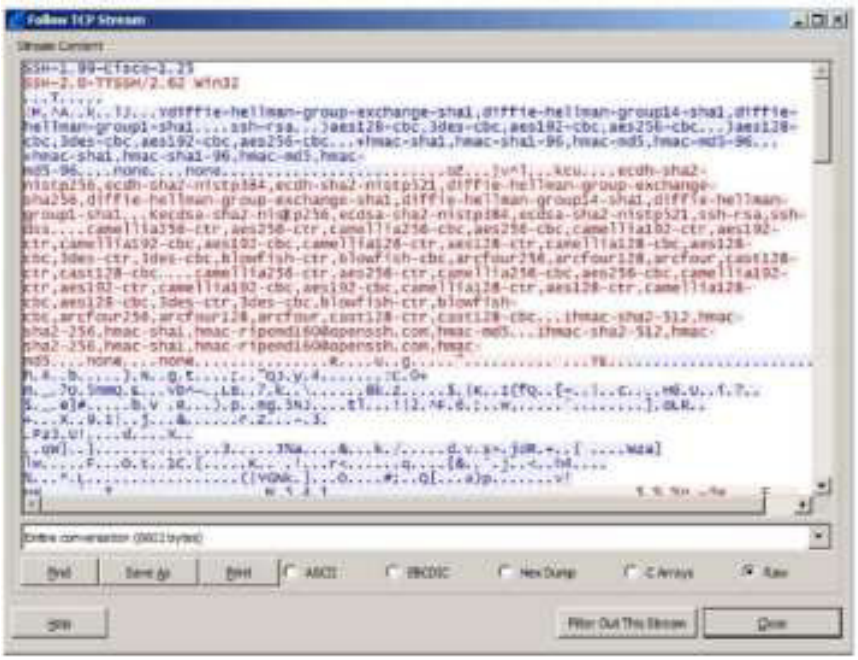
e. Чтобы завершить сеанс SSH и выйти из программы Tera Term, введите команду exit. `R1# exit` Шаг 3: Остановите сбор данных программой Wireshark.

Шаг 4: Примените один из фильтров SSH для данных, собираемых программой Wireshark.

Шаг 5: Используйте функцию TCP в Wireshark для просмотра сеанса Telnet.

a. Нажмите правой кнопкой мыши на одну из строк SSHv2 в разделе Packet list (Список пакетов) программы Wireshark и выберите в раскрывающемся списке пункт Follow TCP Stream (Следить за TCP-потоком).

b. Изучите окно Follow TCP Stream (Следить за TCP-потоком) сеанса SSH. Данные зашифрованы и не доступны для прочтения. Сравните данные сеанса SSH с данными сеанса Telnet.



Почему для удалённых подключений протокол SSH является более предпочтительным, чем протокол Telnet?

c. Завершив изучение сеанса SSH, нажмите кнопку Close (Закрыть).

d. Закройте программу Wireshark.

Часть 5: Настройка коммутатора для доступа по протоколу SSH

В части 5 вы настроите коммутатор в топологии для приёма подключений по протоколу SSH, а затем установите сеанс SSH с помощью программы Tera Term.

Шаг 1: Настройте базовые параметры коммутатора.

Шаг 2: Настройте коммутатор для доступа по протоколу SSH.

Для настройки протокола SSH на коммутаторе используйте те же команды, которые применялись для аналогичной настройки маршрутизатора в части 2.

Шаг 3: Установите подключение к коммутатору по протоколу SSH.

Запустите программу Tera Term на ПК-А, а затем установите подключение по протоколу SSH к интерфейсу SVI коммутатора S1.

Шаг 4: При необходимости устраните неполадки.

Удалось ли вам установить сеанс SSH с коммутатором?

Часть 6: Настройка протокола SSH в интерфейсе командной строки коммутатора

Клиент SSH интегрирован в операционную систему Cisco IOS и может запускаться из интерфейса командной строки. В части 6 вы установите подключение к маршрутизатору по протоколу SSH из интерфейса командной строки коммутатора.

Шаг 1: Посмотрите, какие параметры доступны для клиента SSH в Cisco IOS.

Введите вопросительный знак (?), чтобы отобразить варианты

-c	Select encryption algorithm
-l	Log in using this user name
-m	Select HMAC algorithm
-o	Specify options
-p	Connect to this port
-v	Specify SSH Protocol Version
-vrf	Specify vrf name
WORD	IP address or hostname of a remote system

параметров для команды ssh. S1# ssh ?

Шаг 2: Установите подключение коммутатора S1 к маршрутизатору R1 по протоколу SSH.

a. Чтобы подключиться к маршрутизатору R1 по протоколу SSH, введите команду -ladmin. Это позволит вам войти в систему под именем admin. При появлении запроса в качестве пароля введите adminpass.

```
S1# ssh -l admin 192.168.1.1
Password:
**********************************************
  Warning: Unauthorized Access is Prohibited!
    ********************************************** R1#
```

b. Чтобы вернуться к коммутатору S1, не закрывая сеанс подключения к маршрутизатору R1 по протоколу SSH, нажмите клавиши Ctrl+Shift+6. Отпустите клавиши Ctrl+Shift+6 и нажмите x. Откроется окно командной строки коммутатора с привилегированным режимом.

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]

R1#
R1# exit

[Connection to 192.168.1.1 closed by foreign host]
S1#
 R1#
 S1#
```

c. Чтобы вернуться к сеансу SSH на маршрутизаторе R1, нажмите клавишу ВВОД в пустом поле интерфейса командной строки. Чтобы открыть окно командной строки маршрутизатора, нажмите клавишу ВВОД ещё раз.

d. Чтобы завершить сеанс SSH на маршрутизаторе R1, введите в окне командной строки команду exit.

Какие версии протокола SSH поддерживаются интерфейсом командной строки?

Вопросы на закрепление

Как предоставить доступ к сетевому устройству нескольким пользователям, у каждого из которых есть

собственное имя пользователя?

Сводная таблица интерфейса маршрутизатора

Общие сведения об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet #1	Интерфейс Ethernet #2	Последовательный интерфейс #1	Последовательный интерфейс #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы для определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. Эта таблица включает в себя идентификаторы возможных сочетаний Ethernet и последовательных интерфейсов в устройстве. В таблицу интерфейсов не включены иные типы интерфейсов, даже если они присутствуют на каком-либо определённом маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое может использоваться в командах IOS для представления интерфейса.				

Практическая работа 3. Конфигурация сетей VLAN и транковых каналов

Топология

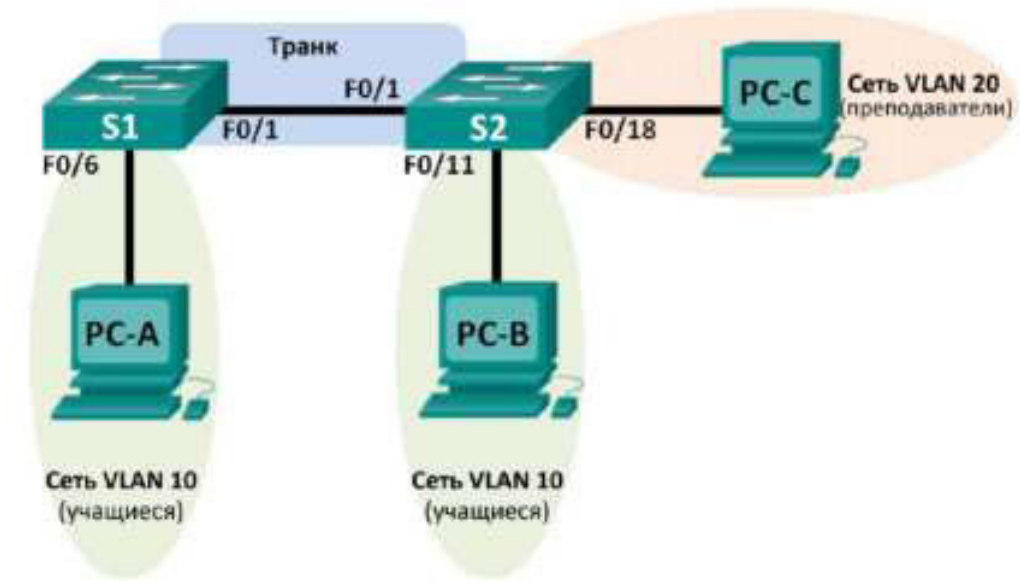


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	Сетевой адаптер	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	Сетевой адаптер	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	Сетевой адаптер	192.168.20.3	255.255.255.0	192.168.20.1

Задачи

Часть 1. Построение сети и настройка базовых параметров устройства

Часть 2. Создание виртуальных локальных сетей и назначение портов коммутатора

Часть 3. Поддержка назначения портов VLAN и базы данных VLAN

Часть 4. Конфигурация транкового канала стандарта 802.1Q между коммутаторами

Часть 5. Удаление базы данных VLAN

Исходные данные/сценарий

В целях повышения производительности сети большие широковещательные домены 2-го уровня делят на домены меньшего размера. Для этого современные коммутаторы используют виртуальные локальные сети (VLAN). Также сети VLAN можно использовать для определения узлов, между

которыми возможен обмен данными, что позволяет повысить уровень безопасности. Сети VLAN облегчают процесс проектирования сети, обеспечивающей помощь в достижении целей организации.

Транковые каналы сети VLAN используются для распространения сетей VLAN по различным устройствам. Транковые каналы разрешают передачу трафика из множества сетей VLAN через один канал, не нанося вред идентификации и сегментации сети VLAN.

В этой лабораторной работе вам предстоит создать сети VLAN на обоих коммутаторах в топологии, назначить сети VLAN в порты доступа на коммутаторе, проверить корректность работы сетей VLAN, а затем создать транковый канал сети VLAN между двумя коммутаторами, чтобы узлы в пределах одной сети VLAN могли обмениваться данными по транку вне зависимости от того, к какому коммутатору подключён узел.

Примечание. В лабораторной работе используются коммутаторы Cisco Catalyst 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование других моделей коммутаторов и других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ.

Примечание. Убедитесь, что информация из коммутаторов удалена, и они не содержат конфигураций загрузки. Если вы не уверены в этом, обратитесь к преподавателю

.

Необходимые ресурсы

- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Построение сети и настройка базовых параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить базовые параметры для узлов ПК и коммутаторов.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Подключите устройства в соответствии с топологией и проведите все необходимые кабели.

Шаг 2: Выполните инициализацию и перезагрузку коммутаторов.

Шаг 3: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте class в качестве пароля привилегированного режима EXEC.

d. Активируйте вход и назначьте в качестве пароля cisco для консоли и VTY.

e. Настройте logging synchronous для консольного канала.

f. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.

g. Настройте IP-адрес, указанный в таблице адресации для сети VLAN 1, на обоих коммутаторах.

h. Используя права администратора, отключите все неиспользуемые порты на коммутаторе.

i. Сохраните текущую конфигурацию в загрузочную конфигурацию.

j.

Шаг 4: Настройте узлы ПК.

Адреса узлов ПК можно посмотреть в таблице адресации.

Шаг 5: Проверка соединения.

Проверьте способность компьютеров обмениваться эхо-запросами.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Успешно ли выполняется эхо-запрос от узла PC-A на узел PC-B?

Успешно ли выполняется эхо-запрос от узла PC-A на узел PC-C?

Успешно ли выполняется эхо-запрос от узла PC-A на коммутатор S1?

Успешно ли выполняется эхо-запрос от узла PC-B на узел PC-C?

Успешно ли выполняется эхо-запрос от узла PC-B на коммутатор S2?

Успешно ли выполняется эхо-запрос от узла PC-C на коммутатор S2?

Успешно ли выполняется эхо-запрос от коммутатора S1 на коммутатор S2?

Если на один из этих вопросов вы ответили отрицательно, укажите причину неудавшейся отправки эхо-запросов.

Часть 2: Создание сетей VLAN и назначение портов коммутатора

Во второй части лабораторной работы вам необходимо создать сети VLAN для учащихся, преподавателей и руководства на обоих коммутаторах. Затем вам нужно назначить сети VLAN соответствующему интерфейсу. Для проверки параметров конфигурации используйте команду show vlan.

a. Создайте сети VLAN на коммутаторе S1.

```
S1(config)# vlan 10
S1(config vlan)# name Student
S1(config vlan)# vlan 20
S1(config vlan)# name Faculty
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# end
```

b. Создайте такую же сеть VLAN на коммутаторе S2.

Шаг 1: Создайте сети VLAN на коммутаторах.

c. Выполните команду show vlan, чтобы просмотреть список сетей VLAN на коммутаторе S1.

S1# show vlan

```
VLAN Name                             Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
10   Student                          active
20   Faculty                          active
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
```

1	enet	100001	1500	- - - -	- 0	0
10	enet	100010	1500	- - - -	- 0	0
20	enet	100020	1500	- - - -	- 0	0
99	enet	100099	1500	- - - -	- 0	0
VLAN	Type	SAID	MTU	Parent RingNo BridgeNo Stp	BrdgMode Trans1	Trans2
1002	fddi	101002	1500	- - - -	- 0	0
1003	tr	101003	1500	- - - -	- 0	0
1004	fdnet	101004	1500	- - - ieee	- 0	0
1005	trnet	101005	1500	- - - ibm	- 0	0
Remote SPAN VLANs						

```
---------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Какой является VLAN по умолчанию?

Какие порты назначены для сети VLAN по умолчанию?

Шаг 2: Назначьте сети VLAN соответствующим интерфейсам коммутатора.

a. Назначьте сети VLAN интерфейсам на коммутаторе S1. 1) Назначьте узел PC-A сети VLAN для учащихся.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

b. Выполните команду show vlan brief и убедитесь, что сети VLAN назначены правильным интерфейсам.

2) Переместите IP-адрес коммутатора сети VLAN 99.

```
S1(config)# interface vlan 1
S1(config-if)# no ip address
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# end
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
10   Student                          active    Fa0/6
20   Faculty                          active
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

c. Выполните команду show ip interfaces brief.

В каком состоянии находится сеть VLAN 99? Почему?

d. Используйте топологию, чтобы назначить сети VLAN соответствующим портам коммутатора S2.

e. Удалите IP-адрес для сети VLAN 1 на коммутаторе S2.

f. Настройте IP-адрес для сети VLAN 99 на коммутаторе S2 в соответствии с таблицей адресации.

g. Выполните команду show vlan brief, чтобы убедиться, что сети VLAN назначены правильным интерфейсам.

```
S2# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   Student                          active    Fa0/11


20   Faculty                          active    Fa0/18
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Успешно ли выполняется эхо-запрос от узла PC-A на узел PC-B? Почему? Успешно ли выполняется эхо-запрос от коммутатора S1 на коммутатор S2? Почему?

Часть 3: Поддержка назначения портов VLAN и базы данных VLAN

В третьей части лабораторной работы вам предстоит изменить назначения сети VLAN портам и удалить сети VLAN из базы данных VLAN.

Шаг 1: Назначьте сеть VLAN нескольким интерфейсам.

a. На коммутаторе S1 назначьте интерфейсы F0/11 - 24 сети VLAN 10.

```
S1(config)# interface range f0/11-24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# end
```

b. Выполните команду show vlan brief, чтобы проверить назначения VLAN.

c. Заново назначьте порты F0/11 и F0/21 сети VLAN 20.

d. Убедитесь, что назначения сети VLAN настроены верно.

Шаг 2: Удалите назначение VLAN из интерфейса.

a. Используйте команду no switchport access vlan, чтобы удалить назначение сети VLAN 10 для F0/24.

```
S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end
```

b. Убедитесь, что это изменение сети VLAN вступило в силу. С какой сетью VLAN теперь связан порт F0/24?

Шаг 3: Удалите идентификатор VLAN из базы данных VLAN.

a. Добавьте сеть VLAN 30 в интерфейс F0/24, не вводя команду сети VLAN.

```
S1(config)# interface f0/24
S1(config-if)# switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```

Примечание. Чтобы добавить сеть VLAN в базу данных, на современных коммутаторах больше не нужно выполнять команду vlan. Когда порту назначается неизвестная сеть VLAN, эта сеть VLAN добавляется в базу данных.

b. Убедитесь, что новая сеть VLAN отображается в таблице VLAN.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Gi0/1, Gi0/2
10   Student                          active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/22, Fa0/23
20   Faculty                          active    Fa0/11, Fa0/21
30   VLAN0030                         active    Fa0/24
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Какое имя присвоено сети VLAN 30 по умолчанию?

c. Используйте команду vlan 30, чтобы удалить сеть VLAN 30 из базы данных VLAN.

```
S1(config)# no vlan 30
S1(config)# end
```

d. Выполните команду show vlan brief. Порт F0/24 было назначен сети VLAN 30.

Какой сети VLAN назначен порт F0/24 после удаления сети VLAN 30? Что происходит с трафиком, предназначенным для узла, подключённого к F0/24?

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Gi0/1, Gi0/2
10   Student                          active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/22, Fa0/23
20   Faculty                          active    Fa0/11, Fa0/21
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

e. Выполните команду no switchport access vlan на интерфейсе F0/24.

f. Выполните команду show vlan brief, чтобы определить назначение

```
S1# show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99

S2# show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
```

сети VLAN для F0/24. Какой сети VLAN назначен порт F0/24?

Примечание. Прежде чем удалять сеть VLAN из базы данных, рекомендуется переназначить все порты, назначенные для этой сети VLAN.

Почему перед удалением сети VLAN из базы данных рекомендуется назначить порт другой сети VLAN?

Часть 4: Конфигурация транкового канала стандарта 802.1Q между коммутаторами

В четвёртой части лабораторной работы вам необходимо настроить интерфейс F0/1 для использования протокола динамического создания транкового канала (DTP), чтобы он мог согласовываться странковым режимом. После выполнения и проверки настройки вам нужно будет отключить DTP на интерфейсе F0/1 и вручную настроить его в качестве транкового канала.

Шаг 1: Для создания транковой связи на порте F0/1 используйте протокол DTP.

По умолчанию протокол DTP на порте коммутатора 2960 настроен на динамический автоматический режим. Благодаря этому интерфейс может преобразовать канал в транковый канал, если соседний интерфейс настроен на транковый или динамический рекомендуемый режим.

а. Настройте порт F0/1 на коммутаторе S1 для согласования транкового режима.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
*Mar  1 05:07:28.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to down
*Mar  1 05:07:29.744: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
S1(config-if)#
*Mar  1 05:07:32.772: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
S1(config-if)#
*Mar  1 05:08:01.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
*Mar  1 05:08:01.797: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

На S2 также должны отображаться сообщения о состоянии каналов.

```
S2#
*Mar  1 05:07:29.794: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
S2#
*Mar  1 05:07:32.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
S2#
```

*Mar 1 05:08:01.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

b. На коммутаторах S1 и S2 выполните команду show vlan brief. Интерфейс F0/1 больше не назначен сети VLAN 1. Транковые интерфейсы не указаны в таблице VLAN.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/24, Gi0/1, Gi0/2
10   Student                          active    Fa0/6, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/22, Fa0/23
20   Faculty                          active    Fa0/11, Fa0/21
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

c. Для просмотра транковых интерфейсов выполните команду show interfaces trunk. Обратите внимание, что на коммутаторе S1 настроен рекомендуемый режим, а на S2 настроен автоматический режим.

*Mar 1 05:08:01.850: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

```
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
```

Примечание. По умолчанию доступ в транковый канал разрешён для всех сетей VLAN. С помощью команды switchport trunk вы можете определить, какие сети VLAN имеют доступ к транковому каналу. В этой лабораторной работе оставьте настройки по умолчанию, чтобы все сети VLAN могли проходить через F0/1.

d. Убедитесь в том, что трафик сети VLAN проходит через транковый интерфейс F0/1.

Успешно ли выполняется эхо-запрос от коммутатора S1 на коммутатор S2?

Успешно ли выполняется эхо-запрос от узла PC-A на узел PC-B?

Успешно ли выполняется эхо-запрос от узла PC-A на узел PC-C?

Успешно ли выполняется эхо-запрос от узла PC-B на узел PC-C?

Успешно ли выполняется эхо-запрос от узла PC-A на коммутатор S1?

Успешно ли выполняется эхо-запрос от узла PC-B на коммутатор S2?

Успешно ли выполняется эхо-запрос от узла PC-C на коммутатор S2?

Если на один из этих вопросов вы ответили отрицательно, ниже объясните причины такого результата.

Шаг 2: Вручную настройте транковый интерфейс F0/1.

Команда switchport mode trunk позволяет вручную настроить порт в качестве транкового канала. Эту команду следует выполнять на обоих концах канала.

a. Измените режим порта коммутатора на интерфейсе F0/1, чтобы принудительно создать транковую связь. Не забудьте сделать это на обоих коммутаторах.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

b. Для просмотра транкового режима выполните команду show interfaces trunk. Обратите внимание, что режим изменён с рекомендуемого (desirable) на вкл (on).

```
S2# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
```

Почему вместо использования протокола DTP рекомендуется вручную настраивать интерфейс на транковый режим?

Часть 5: Удаление базы данных VLAN

В пятой части лабораторной работы вам предстоит удалить базу данных VLAN из коммутатора. Данную процедуру необходимо выполнять при сбросе настроек коммутатора на параметры по умолчанию.

Шаг 1: Определите, существует ли база данных VLAN.

Выполните команду show flash, чтобы проверить, содержится ли файл vlan.dat во флеш-памяти.

```
S1# show flash

Directory of flash:/

    2  -rwx        1285   Mar 1 1993 00:01:24 +00:00  config.text
    3  -rwx       43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
    4  -rwx           5   Mar 1 1993 00:01:24 +00:00  private-config.text
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-
    6  -rwx         736   Mar 1 1993 00:19:41 +00:00  vlan.dat

32514048 bytes total (20858880 bytes free)
```

Примечание. Если во флеш-памяти содержится файл vlan.dat, то база данных VLAN не содержит свои параметры по умолчанию.

Шаг 2: Удалите базу данных VLAN.

a. Выполните команду delete vlan.dat, чтобы удалить файл vlan.dat из флеш-памяти и вернуть настройки базы данных VLAN к параметрам по умолчанию. Вам понадобится два раза подтвердить удаление файла vlan.dat. Оба раза нажмите клавишу Enter.

```
S1# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
S1#
```

b. Выполните команду show flash, чтобы убедиться, что файл vlan.dat был удалён.

```
S1# show flash

Directory of flash:/

    2  -rwx        1285   Mar 1 1993 00:01:24 +00:00  config.text
    3  -rwx       43032   Mar 1 1993 00:01:24 +00:00  multiple-fs
    4  -rwx           5   Mar 1 1993 00:01:24 +00:00  private-config.text
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2

32514048 bytes total (20859904 bytes free)
```

Какие ещё команды нужно выполнить для восстановления параметров по умолчанию в коммутаторе?

Вопросы на закрепление

1. Что нужно для того, чтобы узлы в сети VLAN 10 могли обмениваться данными с узлами в сети VLAN 20?
2. В чём заключаются основные преимущества, которые получает организация при использовании сетей VLAN?

Практическая работа 4. Поиск и устранение неполадок в маршрутизации между сетями VLAN

Топология

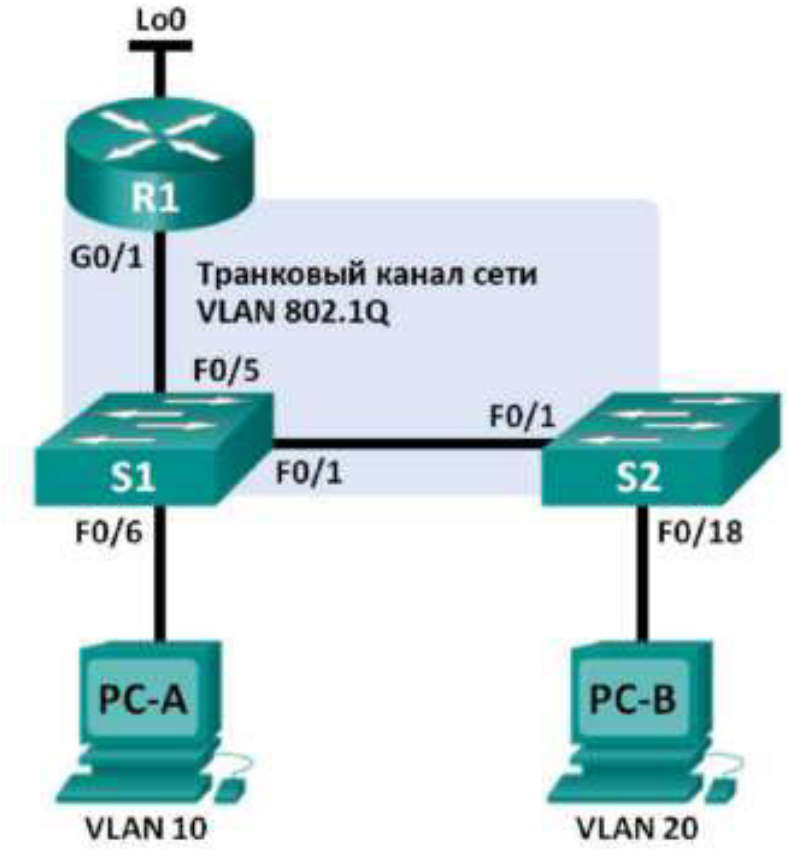


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1.1	192.168.1.1	255.255.255.0	N/A
	G0/1.10	192.168.10.1	255.255.255.0	N/A
	G0/1.20	192.168.20.1	255.255.255.0	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Параметры назначения портов коммутатора

Порты	Назначение	Сеть
S1 F0/1	Транковый канал 802.1Q	N/A
S2 F0/1	Транковый канал 802.1Q	N/A
S1 F0/5	Транковый канал 802.1Q	N/A
S1 F0/6	VLAN 10 - Исследования и разработки	192.168.10.0/24
S2 F0/18	Сеть VLAN 20 — Инженеры	192.168.20.0/24

Задачи

Часть 1. Построение сети и загрузка конфигурации устройств

Часть 2. Поиск и устранение неполадок в конфигурации маршрутизации между VLAN Часть 3: Проверка конфигурации сети VLAN, назначения портов и транковой связи Часть 4. Проверка подключения 3-го уровня

Исходные данные/Сценарий

Сеть была разработана и настроена для поддержки трёх сетей VLAN. Маршрутизация между VLAN обеспечивается внешним маршрутизатором, использующим транковый канал 802.1Q, который также называют конфигурацией router-on-a-stick. Маршрутизация на удалённый веб-сервер, смоделированная loopback-интерфейсом, также обеспечивается маршрутизатором R1. Однако маршрутизация работает неправильно, а жалобы пользователя не кажутся полезными и не помогают понять источник проблем.

В данной лабораторной работе первым делом нужно определить, что функционирует неправильно, а затем проанализировать существующие конфигурации для выявления и устранения источника проблем. Эта Практическая работа будет считаться завершённой, когда вы продемонстрируете IP- соединение между каждой из пользовательских сетей VLAN и сетью внешнего веб-сервера, а также между административной VLAN и сетью веб-сервера.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной

информации об интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

- 1 маршрутизатор (Cisco 1941 с универсальным образом M3 под управлением ОС Cisco IOS 15.2(4) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Построение сети и загрузка конфигураций устройств

В первой части лабораторной работы вам предстоит создать топологию сети и настроить базовые параметры для узлов, коммутаторов и маршрутизатора ПК.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Настройте узлы ПК.

Адреса узлов ПК можно посмотреть в таблице адресации.

Шаг 3: Загрузите конфигурации маршрутизаторов и коммутаторов.

Загрузите следующие конфигурации в соответствующий маршрутизатор или коммутатор. Все устройства настроены с одинаковыми паролями. Пароль привилегированного режима — class, пароль канала — cisco.

```
hostname R1
enable secret class
no ip domain lookup
line con 0
 password cisco
 login
 logging synchronous
line vty 0 4
 password cisco
 login
```

Настройка маршрутизатора R1:

```
interface loopback0
 ip address 209.165.200.225 255.255.255.224
interface gigabitethernet0/
 no ip address
interface gigabitethernet0/1.1
 encapsulation dot1q 1
 ip address 19[illegible] [illegible] [illegible]
interface gigabitethernet0/1.[illegible]
 encapsulation dot1q 10
 ip address 192.168.[illegible] 255.255.255.[illegible]
interface gigabitethernet0/1.99
 encapsulation dot1q 99
 ip address 192.168.[illegible] 255.255.255.[illegible]
end
```

Настройка коммутатора S1:

```
hostname S1
enable secret class
no ip domain-lookup
line con 0
 password cisco
 login
 logging synchronous
line vty 0 15
 password cisco
 login
vlan 10
 name R&D
 exit
interface fastethernet0/1
 switchport mode access
interface fastethernet0/5
 switchport mode trunk
interface vlan1
 ip address 192.168.1.11 255.255.255.0
ip default-gateway 192.168.1.1
end
hostname S2
enable secret class
no ip domain-lookup
line con 0
 password cisco
 login
 logging synchronous
```

Настройка коммутатора S2:

```
line vty 0 15
 password cisco
 login
vlan 20
 name Engineering
 exit
interface fastethernet0/1
 switchport mode trunk
interface fastethernet0/18
 switchport access vlan 10
 switchport mode access
interface vlan1
 ip address 192.168.1.12 255.255.255.0
ip default-gateway 192.168.1.1
end
```

Шаг 4: Сохраните текущую конфигурацию в загрузочную конфигурацию.

Часть 2: Поиск и устранение неполадок в конфигурации маршрутизации между VLAN

Во второй части лабораторной работы вам предстоит проверить настройку маршрутизации между сетями VLAN.

a. На маршрутизаторе R1 введите команду show ip route для просмотра записей таблицы маршрутизации.

Какие сети в ней перечислены?

Все ли сети представлены в таблице маршрутизации? Если нет, каких сетей не хватает? По каким причинам маршрут может отсутствовать в таблице маршрутизации?

b. На маршрутизаторе R1 выполните команду show ip interface brief.

Есть ли в выходных данных сведения о неполадках в интерфейсах маршрутизатора? Если да, то какие команды помогут устранить эти неполадки?

c. На маршрутизаторе R1 повторно выполните команду show ip route.

Убедитесь, что все сети присутствуют в таблице маршрутизации. Если нет, выполняйте поиск и устранение неполадок, пока все сети не появятся в таблице маршрутизации.

Часть 3: Проверка конфигурации сети VLAN, назначения портов и транковой связи

В третьей части лабораторной работы вам предстоит убедиться, что на коммутаторах S1 и S2 присутствуют верные сети VLAN, и что транковая связь настроена правильно.

Шаг 1: Проверьте конфигурацию VLAN и назначения портов.

a. На коммутаторе S1 введите команду show vlan brief, чтобы просмотреть базу данных VLAN.

Какие сети VLAN указаны в списке? Не обращайте внимания на сети VLAN с номерами от 1002 до 1005.

Имеются ли какие-либо номера или имена сетей VLAN, отсутствующие в выходных данных команды? Если да, перечислите их.

Были ли назначены порты доступа правильным сетям VLAN? Если нет, перечислите отсутствующие или некорректные назначения.

Если в сетях VLAN возникнут неполадки, какие команды помогут их решить?

b. На коммутаторе S1 повторно выполните команду show vlan brief, чтобы проверить конфигурацию.

c.На коммутаторе S2 введите команду show vlan brief, чтобы просмотреть базу данных VLAN.

Какие сети VLAN указаны в списке? Не обращайте внимания на сети VLAN с номерами от 1002 до 1005.

Имеются ли какие-либо номера или имена сетей VLAN, отсутствующие в выходных данных команды? Если да, перечислите их.

Были ли назначены порты доступа правильным сетям VLAN? Если нет, перечислите отсутствующие или некорректные назначения.

Если в сетях VLAN возникнут неполадки, какие команды помогут их решить?d. На коммутаторе S2 повторно выполните команду show vlan brief, чтобы проверить изменения конфигурации.

Шаг 2: Проверьте транковые интерфейсы.

a. На коммутаторе S1 введите команду show interface trunk, чтобы просмотреть транковые интерфейсы.

Какие порты находится в транковом режиме?

Имеются ли какие-либо порты, отсутствующие в выходных данных команды? Если да, перечислите их.

Если с транковыми портами возникнут неполадки, какие команды помогут их решить?

b. На коммутаторе S1 повторно выполните команду show interface trunk, чтобы проверить изменения конфигурации.

c.На коммутаторе S2 введите команду show interface trunk, чтобы просмотреть транковые интерфейсы.

Какие порты находится в транковом режиме?

Имеются ли какие-либо порты, отсутствующие в выходных данных команды? Если да, перечислите их.

Если с транковыми портами возникнут неполадки, какие команды помогут их решить?

Часть 4: Проверка подключения 3-го уровня

a. Теперь, устранив неполадки в конфигурации, пора проверить подключение.

Успешно ли отправляется эхо-запрос с компьютера PC-A на шлюз по умолчанию для VLAN 10?

Успешно ли отправляется эхо-запрос от узла PC-A на PC-B? Успешно ли отправляется эхо-запрос от узла PC-A на интерфейс Lo0?

Если на какой-либо из этих вопросов вы ответили отрицательно, выявите и устраните неполадки в конфигурации.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Успешно ли отправляется эхо-запрос от узла PC-A на коммутатор S1? Успешно ли отправляется эхо-запрос от PC-A на коммутатор S2?

Перечислите несколько проблем, которые могут препятствовать успешной отправке эхо-запросов на коммутаторы.

b. Один из способов решения проблемы — выполнение tracert от PC-A на коммутатор S1.

```
C:\Users\Admin> tracert 192.168.1.11
Трассировка маршрута к 192.168.1.11 с максимум 30 прыжков
  1    <1 мс    <1 мс    <1 мс  192.168.10.1
  2     *        *        *     Destinat timed out.
  3     *        *        *     Request timed out.
Трассировка завершена.
```

В этих выходных данных показано, что запрос от компьютера PC-A достигает шлюз по умолчанию на подынтерфейсе g0/1.10 маршрутизатора R1, но пакет останавливается на маршрутизаторе.

c.Вы уже проверили записи таблицы маршрутизации для маршрутизатора R1. Теперь выполните команду show run | section interface, чтобы проверить конфигурацию VLAN. Перечислите все ошибки конфигурации.

Какие команды необходимо выполнить для решения найденных проблем?

d. Убедитесь в том, что теперь эхо-запросы от PC-A достигают как коммутатор S1, так и S2. Успешно ли отправляется эхо-запрос от узла PC-A на коммутатор S1? Успешно ли отправляется эхо-запрос от PC-A на коммутатор S2?

Вопросы на закрепление

В чём заключаются преимущества просмотра таблицы маршрутизации в целях устранения неполадок?Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Практическая работа 5. Реализация системы безопасности сети VLAN

Топология

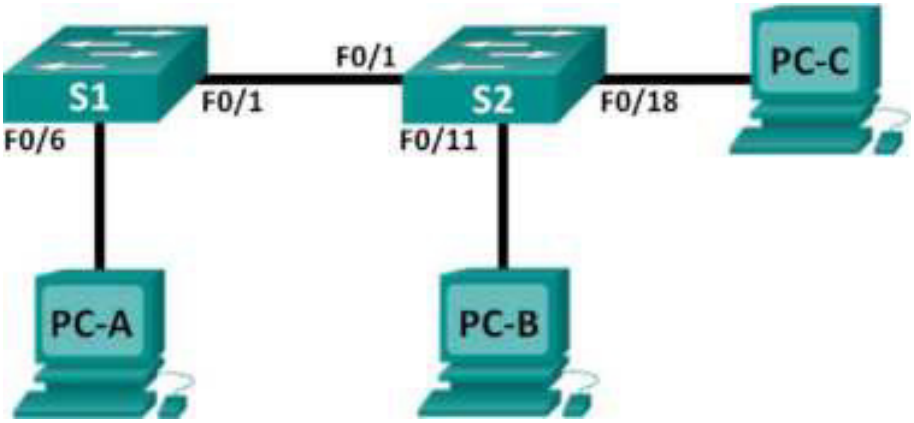


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
PC-A	Сетевой адаптер	172.17.99.3	255.255.255.0	172.17.99.1
PC-B	Сетевой адаптер	172.17.10.3	255.255.255.0	172.17.10.1
PC-C	Сетевой адаптер	172.17.99.4	255.255.255.0	172.17.99.1

Назначения VLAN

VLAN	Имя
10	Данные
99	Сеть Management&Native
999	Чёрный список

Задачи

Часть 1. Построение сети и настройка базовых параметров устройства

Часть 2. Внедрение средств обеспечения безопасности VLAN на коммутаторах

Исходные данные/Сценарий

Рекомендуется настраивать базовые параметры системы безопасности как на портах доступа, так и на транковых портах коммутатора. Это позволяет защитить сеть VLAN от угроз и возможного прослушивания сетевого трафика.

В этой лабораторной работе вам предстоит настроить на сетевых устройствах в топологии некоторые базовые параметры, проверить подключение, а затем применить на коммутаторах более надёжные меры безопасности. Вы изучите поведение коммутаторов Cisco при использовании различных команд show. Затем вам нужно будет применить меры безопасности.

Примечание. В лабораторной работе используются коммутаторы Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование других моделей коммутаторов и других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ.

Примечание. Убедитесь, что информация из коммутаторов удалена, и они не содержат конфигурации загрузки. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Построение сети и настройка базовых параметров устройства

В первой части лабораторной работы нужно настроить базовые параметры на коммутаторах и компьютерах. Имена и адреса устройств указаны в таблице адресации.

Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Выполните инициализацию и перезагрузку коммутаторов.

Шаг 3: Настройте IP-адреса на узлах PC-A, PC-B и PC-C.

Адреса узловых ПК можно посмотреть в таблице адресации.

Шаг 4: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте class в качестве пароля привилегированного режима EXEC.

d.Назначьте cisco в качестве пароля паролей консоли и VTY и активируйте вход для консоли и VTY каналов.

e. Настройте logging synchronous для консоли и каналов vty.

Шаг 5: Настройте сети VLAN на каждом коммутаторе.

a. Создайте и назначьте имена сетям VLAN в соответствии с таблицей назначений VLAN.

b. Настройте IP-адрес, указанный в таблице адресации для сети VLAN 99 на обоих коммутаторах.

c.Настройте порт F0/6 на коммутаторе S1 в качестве порта доступа и назначьте его сети VLAN 99.

d.Настройте порт F0/11 на коммутаторе S2 в качестве порта доступа и назначьте его сети VLAN 10.

e. Настройте порт F0/18 на коммутаторе S2 в качестве порта доступа и назначьте его сети VLAN 99.

f. Выполните команду show vlan brief, чтобы проверить назначения VLAN и портов.

Какой сети VLAN будет принадлежать не назначенный порт, например F0/8 на коммутаторе S2?

Шаг 6: Настройте базовые параметры безопасности порта.

a. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.

b. Зашифруйте все пароли.

c.Отключите все неиспользуемые физические порты.

d. Отключите основной текущий веб-сервис.

```
S1(config)# no ip http server
S2(config)# no ip http server
```

e. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 7: Проверьте подключение между устройствами и сведения о VLAN.

a. Из командной строки на ПК-А отправьте эхо-запрос на административный адрес коммутатора S1. Успешно ли выполнен эхо-запрос? Почему?

b. От коммутатора S1 отправьте эхо-запрос на административный адрес коммутатора S2. Успешно ли выполнен эхо-запрос? Почему?

c. Из командной строки на PC-B отправьте эхо-запрос на административные адреса коммутаторов S1 и S2 и на IP-адреса PC-A и PC-C. Успешно ли выполнены эхо-запросы? Почему?

d. Из командной строки узла PC-C отправьте эхо-запрос на административные адреса коммутаторов S1 и S2. Успешно ли выполнены эхо-запросы? Почему?

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Часть 2: Реализация системы безопасности сети VLAN на коммутаторах

Шаг 1: Настройте транковые порты на коммутаторах S1 и S2.

a. Настройте порт F0/1 на коммутаторе S1 в качестве транкового порта.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

b. Настройте порт F0/1 на коммутаторе S2 в качестве транкового порта.

```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
```

c. Проверьте транковую связь на коммутаторах S1 и S2. Выполните

```
S1# show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

команду show interface trunk на обоих коммутаторах.

Шаг 2: Измените сеть native VLAN для транковых портов на коммутаторах S1 и S2.

Изменение сети native VLAN для транковых портов с VLAN 1 на другую сеть VLAN — это хороший способ обеспечения безопасности.

a. Укажите текущую сеть native VLAN для интерфейсов F0/1 коммутаторов S1 и S2.

b. Настройте сеть Management&Native VLAN 99 на транковом интерфейсе F0/1 коммутатора S1 в качестве сети native VLAN.

```
S1# config t
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 99
```

c. Подождите несколько секунд. Вы должны получить сообщения об ошибке в консольном сеансе на коммутаторе S1. Что означает сообщение % C D P-4- NATIVE_VLAN_M ISMATC H: ?

d. Настройте сеть VLAN 99 на транковом интерфейсе F0/1 коммутатора S2 в качестве сети native VLAN.

```
S2(config)# interface f0/1
S2(config-if)# switchport trunk native vlan 99
```

e. Убедитесь, что сетью native VLAN на обоих коммутаторах является VLAN 99. Ниже показаны выходные данные коммутатора S1.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port         Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,999
```

Шаг 3: Убедитесь, что трафик успешно проходит через транковый канал.

a. Из командной строки на ПК-А отправьте эхо-запрос на административный адрес коммутатора S1. Успешно ли выполнен эхо-запрос? Почему?

b. В консольном сеансе на коммутаторе S1 отправьте эхо-запрос на административный адрес коммутатора S2. Успешно ли выполнен эхо-запрос? Почему?

c. Из командной строки на PC-B отправьте эхо-запрос на административные адреса коммутаторов S1 и S2 и на IP-адреса PC-A и PC-C. Успешно ли выполнены эхо-запросы? Почему?

d. Из командной строки на PC-C отправьте эхо-запрос на административные адреса коммутаторов S1 и S2 и на IP-адрес узла PC-A. Успешно ли выполнены эхо-запросы? Почему?

Шаг 4: Запретите использование DTP на коммутаторах S1 и S2.

На коммутаторах Cisco используется собственный протокол, который известен как протокол динамического создания транкового канала (DTP). Некоторые порты автоматически согласовываются для транковой связи. Согласование рекомендуется отключать. Такое поведение по умолчанию можно увидеть, выполнив следующую команду:

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Output Omitted>
```

Отключите согласование на коммутаторе S1.

```
S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate
```

a. Отключите согласование на коммутаторе S2.

```
S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate
```

b. Убедитесь, что согласование отключено, с помощью команды show interface f0/1 switchport на коммутаторах S1 и S2.

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
<Output Omitted>
```

Шаг 5: Настройте функцию безопасности на портах доступа на коммутаторах S1 и S2.

Если устройство подключено к одному из этих портов, а интерфейс включён, транковая связь может быть успешной, даже если вы выключите на коммутаторах неиспользуемые оставшиеся порты. Кроме того, все порты по умолчанию находятся в сети VLAN 1. Рекомендуется перевести неиспользуемые порты в сеть VLAN «чёрной дыры». На данном этапе вам нужно отключить транковую связь на всех неиспользуемых портах. Также вам нужно назначить неиспользуемые порты сети VLAN 999. Для этой лабораторной работы на обоих коммутаторах будут настроены только порты со 2-го по 5-й.

a. Выполните команду show interface f0/2 switchport на коммутаторе S1. Обратите внимание на административный режим и состояние для согласования транковой связи.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Output Omitted>
```

b. Отключите транковую связь на портах доступа коммутатора S1.

```
S1(config)# interface range f0/2 - 5
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
```

c. Отключите транковую связь на портах доступа коммутатора S2.

d. Убедитесь, что порт F0/2 на коммутаторе S1 настроен в качестве порта доступа.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
```

е. Убедитесь, что назначения портов VLAN настроены верно на обоих коммутаторах. Коммутатор S1 показан ниже в качестве примера.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   Data                             active
99   Management&Native                active    Fa0/6
999  BlackHole                        active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                       act/unsup
1003 token-ring-default                 act/unsup
1004 fddinet-default                    act/unsup
1005 trnet-default                      act/unsup
Restrict VLANs allowed on trunk ports.
```

По умолчанию все сети VLAN имеют доступ к транковым портам. Из соображений безопасности рекомендуется разрешать доступ к транковым каналам вашей сети только для нужных сетей VLAN.

Разрешите доступ к транковому порту F0/1 на коммутаторе S1 только для сетей VLAN 10 и 99.

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk allowed vlan 10,99
```

Разрешите доступ к транковому порту F0/1 на коммутаторе S2 только для сетей VLAN 10 и 99.

Проверьте разрешённые сети VLAN. Выполните команду show interface trunk в привилегированном режиме на коммутаторах S1 и S2.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99

Port        Vlans allowed and active in management domain
Fa0/1       10,99

Port        Vlans in spanning tree forwarding state and not pruned

Fa0/1       10,99
```

Какой получен результат?

Вопросы на закрепление

Есть ли проблемы в системе безопасности коммутатора Cisco с конфигурацией по умолчанию? Какие именно?

Практическая работа 6: тестирование сетевого подключения с помощью команд «ping» и «traceroute»

Топология

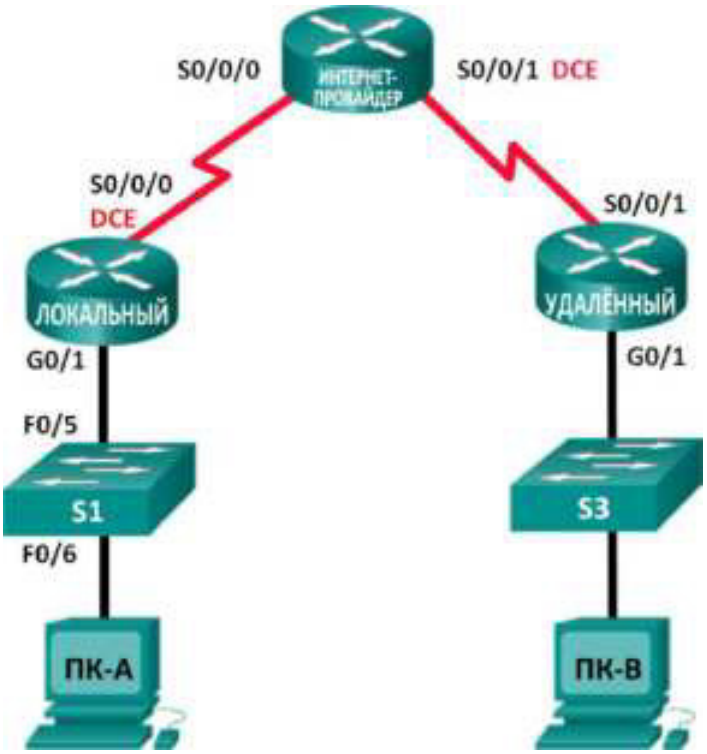


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
LOCAL	G0/1	192.168.1.1	255.255.255.0	Недоступно
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Недоступно
ISP	S0/0/0	10.1.1.2	255.255.255.252	Недоступно
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Недоступно
REMOTE	G0/1	192.168.3.1	255.255.255.0	Недоступно
	S0/0/1	10.2.2.1	255.255.255.252	Недоступно
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.3.11	255.255.255.0	192.168.3.1
ПК-А	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1
ПК-В	Сетевой адаптер	192.168.3.3	255.255.255.0	192.168.3.1

Задачи

Часть 1. Создание и настройка сети

- Подключите кабели.
- Настройте компьютеры.
- Настройте маршрутизаторы.

• Настройте коммутаторы.

Часть 2. Тестирование основной сети с помощью команды «ping»

• Отправьте эхо-запрос с помощью команды ping с компьютера.

• Отправьте эхо-запрос с помощью команды ping с устройств Cisco.

Часть 3. Тестирование основной сети с помощью команд tracert и traceroute

• Введите команду «tracert» на компьютере.

• Введите команду «traceroute» на устройствах Cisco. Часть 4. Поиск и устранение неисправностей в топологии

Исходные данные/сценарий

Команды «ping» и «traceroute» незаменимы при проверке подключения к сетям TCP/IP. Ping — это утилита администрирования сетей, которая используется для проверки доступности устройств в IP-сети. Кроме того, она определяет время прохождения сигнала для сообщений, отправленных с узла источника на компьютер назначения. Утилита ping доступна в ОС Windows, Unix-подобных операционных системах (OS) и операционной системе сетевого взаимодействия Cisco (IOS).

Traceroute — это утилита сетевой диагностики, отображающая маршрут и измеряющая задержки при передаче пакетов в IP-сетях. Утилита tracert доступна в ОС Windows, а в Unix-подобных операционных системах (OS) и в Cisco IOS используется её аналог — утилита traceroute.

В этой лабораторной работе рассматриваются команды ping и traceroute и изучаются параметры командной строки, позволяющие изменять их поведение. Для изучения команд в лабораторной работе используются компьютеры и устройства Cisco. На маршрутизаторах Cisco в качестве протокола маршрутизации будет использоваться усовершенствованный протокол внутренней маршрутизации между шлюзами (EIGRP). В лабораторной работе даются необходимые конфигурации для устройств Cisco.

Примечание. Маршрутизаторы, используемые на практических занятиях CCNA: маршрутизаторы с интеграцией сервисов серии Cisco 1941 (ISR) установленной версии Cisco IOS 15.2(4) M3 (образ universalk9). Используемые коммутаторы: семейство коммутаторов Cisco Catalyst 2960 версии CISCO IOS 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии ПО Cisco IOS. В зависимости от модели и версии Cisco IOS выполняемые доступные команды и выводы могут отличаться от данных, полученных в ходе лабораторных работ. Точные идентификаторы интерфейса см. В таблице сводной информации об интерфейсах маршрутизаторов в конце данной лабораторной работы.

Примечание. Убедитесь, что информация, имеющаяся на маршрутизаторе и коммутаторе, удалена и они не содержат файлов загрузочной конфигурации. Если вы не уверены, что сможете это сделать, обратитесь к инструктору.

Необходимые ресурсы

• 3 маршрутизатора (Cisco 1941 под управлением системы Cisco IOS версии 15.2(4)M3, универсальный образ или аналогичный)

• 2 коммутатора (Cisco 2960, ПО CISCO IOS версии 15.0(2), образ lanbasek9 или аналогичный)

• 2 ПК (Windows 7, Vista и XP с программой эмуляции терминала, например Tera Term)

• Консольные кабели для настройки устройств Cisco IOS через консольные порты

• Кабели Ethernet и последовательные кабели, как показано в топологии

Часть 1: Создание и настройка сети

В части 1 вам необходимо создать сеть в топологии и настроить компьютеры и устройства Cisco. Для справки приводятся загрузочные конфигурации маршрутизаторов и коммутаторов. В этой топологии для распределения пакетов между сетями используется протокол EIGRP.

Шаг 1: Создайте сеть в соответствии с изображенной на схеме топологией.

Шаг 2: Удалите настройки на маршрутизаторах и коммутаторах и перезагрузите устройства.

Шаг 3: Настройте IP-адреса и шлюзы по умолчанию для компьютеров в соответствии с таблицей адресации.

Шаг 4: Настройте маршрутизаторы LOCAL (Локальный), ISP (Интернет-провайдер)

и REMOTE (Удалённый), используя приведённые ниже загрузочные конфигурации.

Скопируйте и вставьте в окно командной строки режима общих настроек параметры конфигурации для каждого устройства. Сохраните конфигурацию в файл загрузочной конфигурации startup-config.

Загрузочная конфигурация для маршрутизатора LOCAL:

```
hostname LOCAL
no ip domain lookup
interface s0/0/0
 ip address 17.1.1.1 255.255.255.252
 clock rate 56000
 no shutdown
interface g0/
 ip add 192.168.1.1 255.255.255.0
 no shutdown
router eigrp
 network 17.1.1.0 0.0.0.3
 network 192.168.1.0 0.0.0.255
 no auto-summary
```

Загрузочная конфигурация для маршрутизатора ISP:

```
hostname ISP
no ip domain lookup
interface s0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
interface s0/0/1
 ip add 10.2.2.2 255.255.255.252
 clock rate 56000
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 no auto summary
end
```

Загрузочная конфигурация для маршрутизатора REMOTE:

```
hostname REMOTE
no ip domain-lookup
interface s0/0/1
 ip address 10.2.2.1 255.255.255.252
 no shutdown
interface g0/1
 ip add 192.168.3.1 255.255.255.0
 no shutdown
router eigrp 1
 network 10.2.2.0 0.0.0.3
 network 192.168.3.0 0.0.0.255
 no auto-summary
end
```

Шаг 5: Настройте загрузочную конфигурацию на коммутаторах S1 и S3. Загрузочная конфигурация для маршрутизатора S1:

```
hostname S1
no ip domain lookup
interface vlan 1
 ip add 192.168.1.11 255.255.255.0
 no shutdown
 exit
ip default gateway 192.168.1.1
end
```

Загрузочная конфигурация для маршрутизатора S3:

```
hostname S3
no ip domain-lookup
interface vlan 1
 ip add 192.168.3.11 255.255.255.0
 no shutdown
 exit
ip default gateway 192.168.3.1
end
```

Шаг 6: Настройте таблицу IP-узлов на маршрутизаторе LOCAL.

Таблица IP-узлов позволяет вместо IP-адреса использовать для подключения удалённого устройства имя узла. Таблица узлов обеспечивает разрешение имён для устройств с перечисленными ниже

конфигурациями. Скопируйте и вставьте указанные ниже конфигурации для маршрутизатора LOCAL. Они позволят вводить команды ping и traceroute на маршрутизаторе LOCAL, используя имена узлов.

```
ip host REMOTE 10.2.2.1 192.168.3.1
ip host ISP 10.1.1.2 10.2.2.2
ip host LOCAL 192.168.1.1 10.1.1.1
ip host PC-C 192.168.3.3
ip host PC-A 192.168.1.3
ip host S1 192.168.1.11
ip host S3 192.168.3.11
end
```

Часть 2: Тестирование основной сети с помощью команды ping

В части 2 лабораторной работы необходимо проверить сквозное подключение с помощью команды ping. Утилита ping отправляет пакеты протокола управляющих сообщений в Интернете (ICMP) на целевой узел, а затем ожидает ответа ICMP. Утилита фиксирует как время прохождения сигнала туда и обратно, так и потери пакетов.

Вы проанализируете результаты выполнения команды ping и другие параметры утилиты, доступные на компьютерах под управлением Windows и устройствах Cisco.

Шаг 1: Проверьте сетевое подключение из сети LOCAL, используя компьютер ПК-А.

Все эхо-запросы с помощью команды ping с ПК-А на другие устройства в топологии должны быть успешными. Если это не так, проверьте топологию и подключение кабелей, а также настройки устройств Cisco и компьютеров.

а. Отправьте эхо-запрос с помощью команды ping с ПК-А на шлюз по умолчанию (интерфейс GigabitEthernet 0/1 маршрутизатора LOCAL).

```
C:\Users\User1>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

В этом примере отправлено четыре (4) запроса ICMP по 32 байта каждый, а ответы получены менее чем через одну миллисекунду без потерь пакетов. Время передачи и получения ответов растёт по мере увеличения количества устройств, которые обрабатывают запросы и ответы ICMP в процессе их передачи к месту назначения и обратно.

b. Отправьте с компьютера ПК-А эхо-запросы с помощью команды ping на адреса, указанные

в приведённой ниже таблице, и запишите среднее время прохождения сигнала и существования (TTL).

Назначение	Среднее время прохождения сигнала (мс)	TTL
192.168.1.1 (LOCAL)		
192.168.1.11 (S1)		
10.1.1.1 (LOCAL)		
10.1.1.2 (ISP)		
10.2.2.2 (ISP)		
10.2.2.1 (REMOTE)		
192.168.3.1 (REMOTE)		
192.168.3.11 (S3)		
192.168.3.3 (PC-C)		

Обратите внимание на среднее время прохождения сигнала при отправке запроса на адрес 192.168.3.3 (ПК-В). Время увеличилось, поскольку до того, как ПК-А получил ответ от ПК-В, запросы ICMP обрабатывались тремя маршрутизаторами.

```
C:\Users\User1>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 40ms, Maximum = 41ms, Average = 40ms
```

Шаг 2: Отправьте расширенные команды ping с компьютера.

Используемая по умолчанию команда ping отправляет четыре запроса по 32 байта каждый. Ответ на каждый запрос ожидается в течение 4000 мс (4 с), после чего отображается сообщение Request timed out (Время запроса превышено). Для устранения неполадок в сети параметры команды ping можно настроить более точно.

a. В командной строке введите команду ping и нажмите клавишу ВВОД.

```
C:\Users\User1>ping -t 192.168.3.3
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
```

```
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.
C:\Users\User1>ping
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

b. Используя параметр -t, отправьте эхо-запрос с помощью команды ping на компьютер ПК-B, чтобы проверить его доступность.

Чтобы проиллюстрировать результаты запроса в случае недоступности узла, отсоедините кабель между маршрутизатором REMOTE и коммутатором S3 или отключите интерфейс GigabitEthernet 0/1 на маршрутизаторе REMOTE.

Пока сеть функционирует нормально, с помощью команды ping можно определить, поступает ли ответ от узла назначения и через какое время. В случае проблем с сетевым подключением команда ping выдаёт сообщение об ошибке.

c. Перед тем, как перейти к следующему шагу, снова подключите Ethernet-кабель или активируйте интерфейс GigabitEthernet на маршрутизаторе REMOTE (с помощью команды no shutdown). Через 30 секунд эхо-запрос с помощью команды ping снова должен быть успешным.

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
```

d. Чтобы остановить команду ping, нажмите клавиши Ctrl+C.

Шаг 3: Проверьте сетевое подключение из сети LOCAL, используя устройства Cisco.

Команду ping можно использовать и на устройствах Cisco. В этом шаге рассматривается выполнение

команды ping на маршрутизаторе LOCAL и коммутаторе S1.

a. С маршрутизатора LOCAL отправьте эхо-запрос с помощью команды ping на компьютер ПК-B в сети REMOTE, используя IP-адрес 192.168.3.3.

```
LOCAL# ping 192.168.3.3
Type escape sequence to abort.
Send ng 5,  00-byte ICMP Echos to 192.168.3.3, t meout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/64/68 ms
```

Восклицательный знак (!) показывает, что эхо-запрос с помощью команды ping с маршрутизатора LOCAL на ПК-B прошёл успешно. Сигнал проходит туда и обратно в среднем за 64 мс без потерь пакетов, о чём свидетельствует выполнение всех запросов.

b. Поскольку на маршрутизаторе LOCAL настроена таблица локальных узлов, эхо-запрос с помощью команды ping на ПК-B в сети REMOTE можно отправить, используя имя узла для маршрутизатора LOCAL.

```
LOCAL# ping PC-C
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/63/64 ms
```

c.Для команды ping доступны дополнительные параметры. В командной строке введите команду ping и нажмите клавишу ВВОД. Введите 192.168.3.3 или PC-C (ПК-B) в поле Target IP address (Целевой IP-адрес). Нажмите клавишу ВВОД, чтобы принять значение по умолчанию для других параметров.

```
LOCAL# ping
Protocol [ip]:
Target IP address: PC-C
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 60/63/64 ms

d. Если в сети возникают проблемы, можно отправить расширенный эхо-запрос с помощью команды ping. Отправьте команду ping на адрес 192.168.3.3 с числом повторов 500. Затем отсоедините кабель между маршрутизатором REMOTE и коммутатором S3 или отключите интерфейс GigabitEthernet 0/1 на маршрутизаторе REMOTE.

Когда вместо восклицательных знаков (!) появятся буква U и точки (.), снова подключите Ethernet- кабель или активируйте интерфейс GigabitEthernet на маршрутизаторе REMOTE. Через 30 секунд эхо-запрос с помощью команды ping снова должен быть успешным. Нажмите клавиши Ctrl+Shift+6, чтобы остановить команду ping.

```
LOCAL# ping
Protocol [ip]:
Target IP address: 192.168.3.3
Repeat count [5]: 500
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 500, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!
Success rate is 95 percent (479/500), round-trip min/avg/max = 60/62/72 ms
```

Буква U в результатах выполнения команды означает, что узел назначения не может быть достигнут. Маршрутизатор LOCAL получил протокольный блок данных (PDU) с ошибкой. Каждая точка (.) в полученных результатах означает, что в процессе ожидания ответа от ПК-В время эхо- запроса с помощью команды ping истекло. В этом примере за время моделирования сбоев в сети были потеряны 5 % пакетов.

Примечание. Такие же результаты позволит получить следующая команда:

```
S1# ping 192.168.3.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round trip min/avg/max   67/67/68 ms
LOCAL# ping 192.168.3.3 repeat 500
```

или

```
LOCAL# ping PC-C repeat 500
```

е. Кроме того, для проверки сетевого подключения можно использовать коммутатор. В этом примере коммутатор S1 отправляет эхо-запрос с помощью команды ping на коммутатор S3 в сети REMOTE.

Команда ping чрезвычайно полезна при поиске и устранении неполадок сетевого подключения. Однако, если запрос не проходит, узнать место возникновения проблемы с помощью этой команды нельзя.

Отобразить информацию о маршруте и задержках в сети позволяет команда tracert (или traceroute).

Часть 3: Тестирование основной сети с помощью команд tracert и traceroute

Команды для отслеживания маршрутов доступны на компьютерах и сетевых устройствах. На компьютере под управлением ОС Windows команда tracert отслеживает путь к узлу назначения, используя сообщения ICMP. Команда traceroute отслеживает маршруты к узлам назначения на устройствах Cisco и компьютерах под управлением Unix-подобных операционных систем, используя датаграммы UDP.

В части 3 вы изучите команды traceroute и определите путь, который проходит пакет до узла назначения. На компьютерах под управлением Windows вы будете использовать команду tracert, а на устройствах Cisco — команду traceroute. Вы также рассмотрите параметры, доступные для точной настройки результатов traceroute.

Шаг 1: Отправьте команду tracert с компьютера ПК-А на компьютер ПК-В.

а. В командной строке введите tracert 192.168.3.3.

```
C:\Users\User1>tracert 192.168.3.3
Tracing route to [illegible] [192.168.3.3]
Over a maximum of 30 hops:

  1    [illegible] ms    [illegible] ms    [illegible] ms    [illegible]
  2    [illegible] ms    [illegible] ms    [illegible] ms    [illegible]
  3    [illegible] ms    [illegible] ms    [illegible] ms    [illegible]
  4    [illegible] ms    [illegible] ms    [illegible] ms    [illegible]

Trace complete.
```

Согласно результатам выполнения команды tracert, от ПК-А до ПК-В данные прошли следующий путь: ПК-А — маршрутизатор LOCAL — маршрутизатор ISP — маршрутизатор REMOTE — ПК-В. Маршрут к узлу

```
C:\Users\User1>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for targe
    -j host-list       Loose source route along host-list (IPv4-o
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round trip path (IPv6 only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

b. Используйте параметр -d. Обратите внимание на то, что IP-адрес 192.168.3.3 не определяется как ПК-В.

назначения ПК-В прошёл через три маршрутизатора.

Шаг 2: Изучите дополнительные параметры команды tracert.

a. В командной строке введите команду tracert и нажмите клавишу ВВОД.

```
C:\Users\User1>tracert -d 192.168.3.3
Tracing route to 192.168.3.3over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    192.168.1.1
  2    24 ms    24 ms    24 ms    10.1.1.2
  3    48 ms    48 ms    48 ms    10.2.2.1
  4    59 ms    59 ms    59 ms    192.168.3.3

Trace complete.
```

Шаг 3: Отправьте команду traceroute с маршрутизатора LOCAL на ПК-В.

a. В командной строке маршрутизатора LOCAL введите traceroute 192.168.3.3 или traceroute PC-C. Имена узлов будут определены, поскольку на маршрутизаторе LOCAL настроена таблица локальных IP-узлов.

```
LOCAL# traceroute 192.168.3.3
Type escape sequence to abort.
Tracing the route to PC-C (192.168.3.3)
VRF info: (vrf in name/id, vrf out name/id)
  1 ISP (10.1.1.2) 16 msec 16 msec 16 msec
  2 REMOTE (10.2.2.1) 28 msec 32 msec 28 msec
  3 PC-C (192.168.3.3) 32 msec 28 msec 32 msec

LOCAL# traceroute PC-C
Type escape sequence to abort.
Tracing the route to PC-C (192.168.3.3)
VRF info: (vrf in name/id, vrf out name/id)
  1 ISP (10.1.1.2) 16 msec 16 msec 16 msec
  2 REMOTE (10.2.2.1) 28 msec 32 msec 28 msec
  3 PC-C (192.168.3.3) 32 msec 32 msec 28 msec
```

Шаг 4: Отправьте команду traceroute с коммутатора S1 на ПК-В.

b. На коммутаторе S1 введите traceroute 192.168.3.3. В результатах выполнения программы

traceroute имена узлов не отображаются, поскольку на этом коммутаторе таблица локальных IP- узлов не настроена.

```
S1# traceroute 192.168.3.3
Type escape sequence to abort.
Tracing the route to 192.168.3.3
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.1.1 1007 msec 0 msec 0 msec
  2 10.1.1.2 17 msec 17 msec 16 msec
  3 10.2.2.1 34 msec 33 msec 26 msec
  4 192.168.3.3 33 msec 34 msec 33 msec
```

Команда traceroute имеет дополнительные параметры. Чтобы их посмотреть, после ввода команды traceroute в командной строке введите знак вопроса ? или просто нажмите клавишу ВВОД.

Дополнительную информацию о командах ping и traceroute для устройств Cisco можно найти на странице

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products tech note09186a00800a6057.shtml

Часть 5: Поиск и устранение неисправностей в топологии

Шаг 1: Удалите неисправности в топологии на маршрутизаторе REMOTE. Шаг 2: Перезагрузите маршрутизатор REMOTE.

Шаг 3: Скопируйте и вставьте в маршрутизатор REMOTE указанную ниже конфигурацию.

```
hostname REMOTE
no ip domain lookup
interface s0/0/1
 ip address 10.2.2.1 255.255.255.252
 no shutdown
interface g0/1
 ip add 192.168.3.1 255.255.255.0
 no shutdown
router eigrp 1
 network 10.2.2.0 0.0.0.3
 network 192.168.3.0 0.0.0.255
 no auto summary
end
```

Шаг 4: Из сети LOCAL отправьте команды ping и tracert или traceroute, чтобы найти и устранить проблемы в сети REMOTE.

а. На компьютере ПК-А введите команды ping и tracert.

Команду tracert можно использовать для проверки сквозного сетевого подключения. В данном случае результаты выполнения команды tracert показывают, что компьютер ПК-А достигает шлюза по умолчанию с адресом 192.168.1.1, но не может подключиться к ПК-В.

```
C:\Users\User1>ping 10.2.2.2

Pinging 10.2.2.2 with 32 bytes of data:
Reply from 10.2.2.2: bytes 32 time 41ms TTL 254
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
Reply from 10.2.2.2: bytes 32 time 41ms TTL 254

Ping statistics for 10.2.2.2:

C:\Users\User1>tracert 192.168.3.3

Tracing route to 192.168.3.3 over a maximum of 30 hops
  1  <1 ms  <1 ms  <1 ms  192.168.1.1
  2  192.168.1.1  reports: Destination host unreachable.

Trace complete.
```

Один из способов обнаружения проблемы в сети — это эхо-запрос с помощью команды ping на каждый встречающийся в сети переход на пути к ПК-В. Сначала выясните, может ли компьютер ПК-А подключиться к интерфейсу Serial 0/0/1 маршрутизатора ISP с IP-адресом 10.2.2.2.

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Эхо-запрос с помощью команды ping к маршрутизатору ISP прошёл успешно. Следующий переход в сети — маршрутизатор REMOTE. Отправьте эхо-запрос с помощью команды ping на интерфейс Serial 0/0/1 маршрутизатора REMOTE с IP-адресом 10.2.2.1.

```
C:\Users\User1>ping 10.2.2.1

Pinging 10.2.2.1 with 32 bytes of data:
Reply from 10.2.2.1: bytes 32 time 41ms TTL 253
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
Reply from 10.2.2.1: bytes 32 time 41ms TTL 253

Ping statistics for 10.2.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 41ms, Average = 40ms
```

Компьютер ПК-А достигает маршрутизатора REMOTE. Судя по успешному прохождению эхо- запроса с помощью команды ping с компьютера ПК-А на маршрутизатор REMOTE, проблема с подключением связана с сетью 192.168.3.0/24. Отправьте эхо-запрос с помощью команды ping на шлюз ПК-В по умолчанию, в качестве которого выступает интерфейс GigabitEthernet 0/1 маршрутизатора REMOTE.

```
C:\Users\Cisco>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Как видно из результатов выполнения команды ping, компьютер ПК-А не может подключиться к интерфейсу GigabitEthernet 0/1 маршрутизатора REMOTE.

Чтобы проверить сетевое подключение, с компьютера ПК-А можно также отправить эхо-запрос с помощью команды ping на коммутатор S3 — для этого в командной строке введите ping 192.168.3.11. Поскольку ПК-А не может подключиться к интерфейсу GigabitEthernet 0/1 маршрутизатора REMOTE, эхо-запрос с помощью команды ping с ПК-А на коммутатор S3, скорее всего, не пройдёт, что и показывают приведённые ниже результаты.

```
C:\Users\Cisco>ping 192.168.3.11

Pinging 192.168.3.11 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.3.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Результаты выполнения команд tracer! и ping говорят о том, что компьютер ПК-А подключается к маршрутизаторам LOCAL, ISP и REMOTE, но не может связаться с ПК-В, коммутатором S3 или шлюзом ПК-В по умолчанию.

b. Проверьте текущие параметры конфигурации маршрутизатора REMOTE с помощью команд show. `REMOTE# show ip interface brief`

Interface	IP-Address	OK?	Method	Status		Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively	down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively	down	down
GigabitEthernet0/1	192.168.8.1	YES	manual	up		up
Serial0/0/0	unassigned	YES	unset	administratively	down	down
Serial0/0/1	10.2.2.1	YES	manual	up		up

```
REMOTE# show run
<output omitted>
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
ip address 192.168.8.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
<output omitted>
```

Результаты выполнения команд show run и show ip interface brief показывают, что интерфейс GigabitEthernet 0/1 функционирует нормально (up/up), но IP-адрес в нём указан неправильно.

c. Укажите правильный IP-адрес для интерфейса GigabitEthernet 0/1.

```
REMOTE# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
REMOTE(config)# interface GigabitEthernet 0/1
REMOTE(config-if)# ip address 192.168.3.1 255.255.255.0
```

d. Убедитесь в том, что компьютер ПК-А может отправлять команды ping и tracert на ПК-В.

```
C:\Users\User1>ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=44ms TTL=125
```

Примечание. Для этого также можно отправить команды ping и traceroute из интерфейса командной строки на маршрутизатор LOCAL и коммутатор S1, предварительно убедившись в отсутствии проблем подключения в сети 192.168.1.0/24.

Вопросы на закрепление

1. Что, кроме проблем сетевого подключения, может помешать ответам команд ping или traceroute вернуться на исходное устройство?

2. Какое сообщение выдаст команда ping, если отправить эхо-запрос с помощью команды ping на несуществующий адрес в удалённой сети, например 192.168.3.4? Что это означает? Если вы отправите эхо-запрос с помощью команды ping на действительный узел и получите такой ответ, что нужно будет проверить?

3. Какое сообщение выдаст команда ping, если с компьютера под управлением ОС Windows отправить эхо-запрос с помощью команды ping на адрес, который не существует ни в одной из сетей вашей топологии, например 192.168.5.3? Что означает данное сообщение?Сводная таблица интерфейса маршрутизатора

Общие сведения об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet #1	Интерфейс Ethernet #2	Последовательный интерфейс #1	Последовательный интерфейс #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы для определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. Эта таблица включает в себя идентификаторы возможных сочетаний Ethernet и последовательных интерфейсов в устройстве. В таблицу интерфейсов не включены иные типы интерфейсов, даже если они присутствуют на каком-либо определённом маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое может использоваться в командах IOS для представления интерфейса.				

Практическая работа 7. Настройка маршрутизации между VLAN для каждого интерфейса

Топология

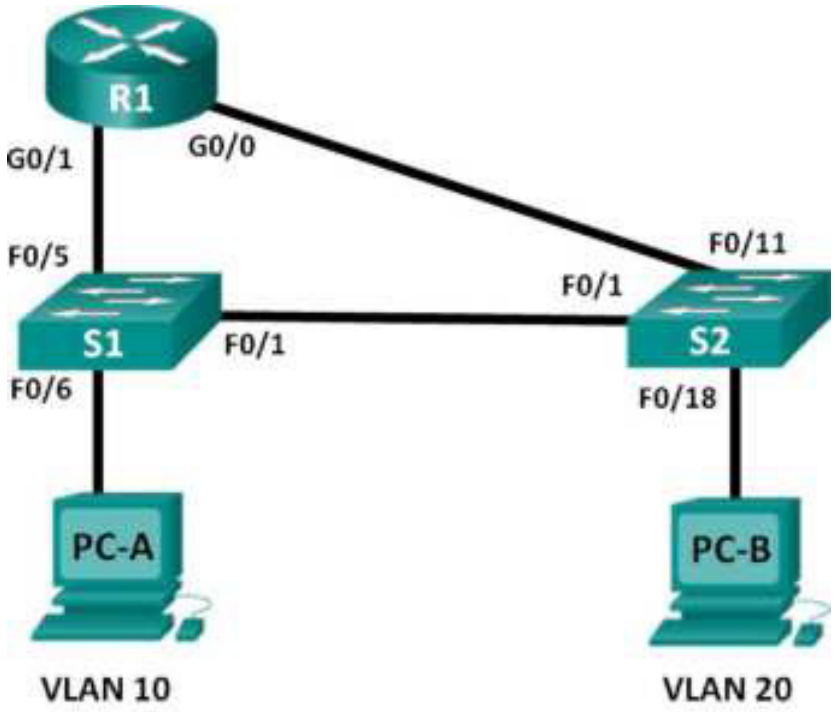


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.20.1	255.255.255.0	N/A
	G0/1	192.168.10.1	255.255.255.0	N/A
S1	VLAN 10	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN 10	192.168.10.12	255.255.255.0	192.168.10.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192 .168 .20 .1

Задачи

Часть 1. Построение сети и настройка базовых параметров устройства

Часть 2. Настройка коммутаторов с сетями VLAN и транковой связи

Часть 3. Проверка транковой связи, сетей VLAN, маршрутизации и подключения

Исходные данные/Сценарий

Однако, прежде чем переходить к маршрутизации между VLAN методом router-on-a-stick (ROS) или настройке коммутации 3-го уровня, рекомендуется получить представление и навыки настройки непосредственно этого типа маршрутизации. Кроме того, вы можете столкнуться с интерфейсной маршрутизацией между VLAN в

организациях с очень маленькими сетями. Простота в использовании — это одно из преимуществ маршрутизации между VLAN с использованием устаревшего метода.

В рамках настоящей лабораторной работы вам предстоит настроить один маршрутизатор с двумя сетями, подключёнными через интерфейсы маршрутизатора Gigabit Ethernet. На коммутаторах будут настроены две отдельные сети VLAN, и вам будет необходимо настроить маршрутизацию между этими VLAN.

Примечание. В этой лабораторной работе содержится минимальный набор фактических команд, необходимых для настройки маршрутизатора и коммутатора. Необходимые команды для конфигурации сети VLAN представлены в приложении А в конце этой лабораторной работы. Проверьте свои знания — настройте устройства, не обращаясь к информации, приведённой в приложении.

Примечание. В лабораторной работе используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с универсальным образом M3 под управлением ОС Cisco IOS 15.2(4) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Построение сети и настройка базовых параметров устройства

В первой части лабораторной работы вы настроите топологию сети и при необходимости удалите все конфигурации.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 3: Настройте базовые параметры для маршрутизатора R1.

a. Отключите поиск DNS.

b. Назначьте имя устройства.

c. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

d. Назначьте cisco в качестве пароля консоли и виртуального терминала VTY и активируйте вход.

e. Настройте адресацию на интерфейсах G0/0 и G0/1 и включите оба интерфейса.

Шаг 4: Настройте базовые параметры на коммутаторах S1 и S2.

a. Отключите поиск DNS.

b. Назначьте имя устройства.

c. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

d. Назначьте cisco в качестве пароля консоли и виртуального терминала VTY и активируйте вход.

Шаг 5: Настройте базовые параметры на компьютерах PC-A и PC-B.

На компьютерах PC-A и PC-B настройте IP-адреса и адрес шлюза по умолчанию в соответствии с таблицей адресации.

Часть 2: Настройте коммутаторы для работы с сетями VLAN и создания транковых каналов

Во второй части лабораторной работы вы будете настраивать коммутаторы для сетей VLAN и транковых каналов.

Шаг 1: Настройте сети VLAN на коммутаторе S1.

a. Создайте сеть VLAN 10 на коммутаторе S1. Назначьте Student в качестве имени сети VLAN.

b. Создайте виртуальную локальную сеть VLAN 20. Назначьте Faculty-Admin в качестве имени для этой сети VLAN.

c. Настройте F0/1 в качестве транкового порта.

d. Назначьте порты F0/5 и F0/6 сети VLAN 10 и настройте оба порта в качестве портов доступа.

e. Назначьте IP-адрес сети VLAN 10 и активируйте его. Сверьтесь с таблицей адресации.

f. Настройте шлюз по умолчанию в соответствии с таблицей адресации.

Шаг 2: Настройте сети VLAN на коммутаторе S2.

a. Создайте сеть VLAN 10 на коммутаторе S2. Назначьте Student в качестве имени сети VLAN.

b. Создайте виртуальную локальную сеть VLAN 20. Назначьте Faculty-Admin в качестве имени для этой сети VLAN.

c. Настройте F0/1 в качестве транкового порта.

d.Назначьте порты F0/11 и F0/18 сети VLAN 20 и настройте оба порта в качестве портов доступа.

e. Назначьте IP-адрес сети VLAN 10 и активируйте его. Сверьтесь с таблицей адресации.

f. Настройте шлюз по умолчанию в соответствии с таблицей адресации.

Часть 3: Проверка транковой связи, сетей VLAN, маршрутизации и подключения

Шаг 1: Проверьте таблицу маршрутизации маршрутизатора R1.

a. На маршрутизаторе R1 выполните команду show ip route. Какие маршруты указаны в маршрутизаторе R1?

b. На коммутаторах S1 и S2 выполните команду show interface trunk. Настроен ли порт F0/1 на обоих коммутаторах на транковую связь?

c.На коммутаторах S1 и S2 выполните команду show vlan brief. Убедитесь, что сети VLAN 10 и 20 активны и что соответствующие порты в коммутаторах находятся в соответствующих VLAN. Почему порт F0/1 не указан в какой-либо из активных VLAN?

d. От компьютера PC-A в сети VLAN 10 отправьте эхо-запрос на компьютер PC-B в сети VLAN 20. Если маршрутизация VLAN работает правильно, эхо-запросы между сетями 192.168.10.0

и 192.168.20.0 должны быть успешными.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

e. Проверьте наличие подключения между всеми устройствами. Эхо-запросы должны быть успешными между всеми устройствами. Если эхо-запросы не удались, исправьте неполадки.

Вопросы на закрепление

В чём заключается преимущество использования устаревшего метода маршрутизации между VLAN?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Приложение А. Команды настройки

Коммутатор S1

```
S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# exit
S1(config)# vlan 20
S1(config-vlan)# name Faculty-Admin
S1(config-vlan)# exit
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# interface range f0/5 - 6
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# interface vlan 10
S1(config-if)# ip address 192.168.10.11 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.10.1
```

Коммутатор S2

```
S2(config)# vlan 10
S2(config-vlan)# name Student
S2(config-vlan)# exit
S2(config)# vlan 20
S2(config-vlan)# name Faculty-Admin
S2(config-vlan)# exit
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
S2(config-if)# interface f0/11
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if-range)# interface vlan 10
S2(config-if)#ip address 192.168.10.12 255.255.255.0
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.10.1
```

Практическая работа 8. Настройка базового протокола OSPFv2 для одной области

Топология

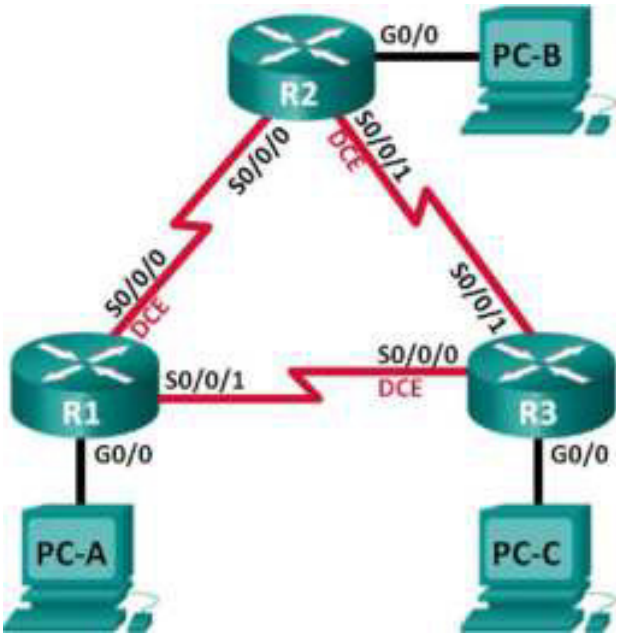


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/0/1	192.168.13.1	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	192.168.12.2	255.255.255.252	N/A
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	N/A
	S0/0/1	192.168.23.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Задачи

Часть 1. Построение сети и настройка базовых параметров устройства

Часть 2. Настройка и проверка маршрутизации OSPF

Часть 3. Изменение значения ID маршрутизатора

Часть 4. Настройка пассивных интерфейсов OSPF

Часть 5. Изменение метрик OSPF

Исходные данные/сценарий

Алгоритм кратчайшего пути (OSPF) — протокол маршрутизации для IP-сетей на базе состояния канала. Версия OSPFv2 используется для сетей протокола IPv4, а OSPFv3 - для сетей IPv6. OSPF обнаруживает изменения в топологии, например сбой канала, и быстро сходится в новой беспетлевой структуре маршрутизации. OSPF рассчитывает каждый маршрут с помощью алгоритма Дейкстры, т.е. алгоритма кратчайшего пути.

В данной лабораторной работе необходимо настроить топологию сети с маршрутизацией OSPFv2, изменить значения ID маршрутизатора, настроить пассивные интерфейсы, установить метрики OSPF и использовать несколько команд интерфейса командной строки для вывода и проверки данных маршрутизации OSPF.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). Возможно использование других маршрутизаторов и версий Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и настройка базовых параметров устройства

В первой части вам предстоит создать топологию сети и настроить основные параметры для узлов и маршрутизаторов.

Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Выполните запуск и перезагрузку маршрутизаторов.

Шаг 3: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте class в качестве пароля привилегированного режима EXEC.

d. Назначьте cisco в качестве паролей консоли и VTY.

e. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.

f. Настройте logging synchronous для консольного канала.

g. Назначьте IP-адреса всем интерфейсам в соответствии с таблицей адресации.

h. Установите значение тактовой частоты на всех последовательных интерфейсах DCE на 128000.

i. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 4: Настройте узлы ПК.

Шаг 5: Проверка соединения.

Маршрутизаторы должны иметь возможность отправлять успешные эхо-запросы друг другу, и все ПК должны иметь возможность отправлять успешные эхо-запросы на свои шлюзы по умолчанию. Компьютеры не могут отправлять успешные эхо-запросы на другие ПК, пока не настроена маршрутизация OSPF. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

Часть 2: Настройка и проверка маршрутизации OSPF

Во второй части вам предстоит настроить маршрутизацию OSPFv2 на всех маршрутизаторах в сети, а затем убедиться, что таблицы маршрутизации обновляются верным образом. После проверки OSPF, для повышения уровня безопасности необходимо настроить на каналах аутентификацию протокола OSPF.

Шаг 1: Настройте маршрутизацию OSPF на маршрутизаторе R1.

a. Используйте команду router ospf в режиме глобальной конфигурации, чтобы активировать OSPF на маршрутизаторе R1.

```
R1(config)# router ospf 1
```

Примечание. Идентификатор процесса OSPF хранится локально и не имеет отношения к другим маршрутизаторам в сети.

b. Используйте команду network для сетей маршрутизатора R1. Используйте идентификатор области, равный 0.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 192.168.12.0 0.0.0.3 area 0
R1(config-router)# network 192.168.13.0 0.0.0.3 area 0
```

Шаг 2: Настройте OSPF на маршрутизаторах R2 и R3.

Используйте команду router ospf и добавьте команду network для сетей маршрутизаторов R2 и R3. Когда маршрутизация OSPF будет настроена на R2 и R3, на маршрутизаторе R1 появятся сообщения об установленных отношениях смежности.

```
R1#
00:22:29: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.1 on Serial0/0/0 from LOADING to
FULL, Loading Done
R1#
00:23:14: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.23.2 on Serial0/0/1 from LOADING to
FULL, Loading Done
R1#
```

Шаг 3: Проверьте информацию о соседях и маршрутизации OSPF.

a. Используйте команду show ip ospf neighbor для проверки списка смежных маршрутизаторов на каждом маршрутизаторе в соответствии с топологией.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.23.2      0   FULL/  -        00:00:33    192.168.13.2    Serial0/0/1
192.168.23.1      0   FULL/  -        00:00:30    192.168.12.2    Serial0/0/0
```

b. Выполните команду show ip route, чтобы убедиться, что в таблицах маршрутизации всех маршрутизаторов отображаются все сети.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0
                        [110/128] via 192.168.13.2, 00:31:38, Serial0/0/1
```

Какую команду вы бы применили, чтобы просмотреть только маршруты OSPF в таблице маршрутизации?

Шаг 4: Проверьте настройки протокола OSPF.

Команда show ip protocols обеспечивает быструю проверку критически важных данных конфигурации OSPF. К таким данным относятся идентификатор процесса OSPF, идентификатор маршрутизатора, сети, объявляемые маршрутизатором, соседние устройства, от которых маршрутизатор принимает обновления, и значение административной дистанции по умолчанию, равное 110 для OSPF.

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.13.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.23.2         110      00:19:16
    192.168.23.1         110      00:20:03
  Distance: (default is 110)
```

Шаг 5: Проверьте данные процесса OSPF.

Используйте команду show ip ospf, чтобы просмотреть идентификаторы процесса OSPF и маршрутизатора. Данная команда отображает данные о зоне OSPF и показывает время, когда последний раз выполнялся алгоритм поиска кратчайшего пути SPF.

```
R1# show ip ospf
 Routing Process "ospf 1" with ID 192.168.13.1
 Start time: 00:20:23.260, Time elapsed: 00:25:08.296
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Supports NSSA (compatible with RFC 3101)
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
 IETF NSF helper support enabled
 Cisco NSF helper support enabled
 Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm last executed 00:22:53.756 ago
        SPF algorithm executed 7 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x019A61
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Шаг 6: Проверьте настройки интерфейса OSPF.

a. Выполните команду show ip ospf interface brief, чтобы отобразить сводку об интерфейсах, на которых активирован алгоритм OSPF.

```
R_# show ip ospf interface brief
```

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs F/C
Se0/0/1	1	0	192.168.13.1/30	64	P2P	1/1
Se0/0/0	1	0	192.168.12.1/30	64	P2P	1/1
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0

b. Для того чтобы увидеть более подробные данные об интерфейсах, на которых активирован OSPF, выполните команду show ip ospf interface.

```
R1# show ip ospf interface
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.12.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.3.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:0_
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.23.2
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet Address 192.168.12.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.3.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
```

```
    Adjacent with neighbor 192.168.23.1
  Suppress hello for 0 neighbor(s)
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 192.168.13.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.13.1, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Шаг 7: Проверьте наличие сквозного соединения.

Все компьютеры должны успешно выполнять эхо-запросы ко всем остальным компьютерам, указанным в топологии. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Часть 3: Изменение значения ID маршрутизатора

Идентификатор OSPF-маршрутизатора используется для уникальной идентификации маршрутизатора в домене маршрутизации OSPF. Маршрутизаторы компании Cisco получают ID маршрутизатора одним из трёх способов в следующем порядке:

1) IP-адрес, установленный с помощью команды OSPF router-id (при наличии)

2) Наивысший IP-адрес любого из loopback-адресов маршрутизатора (при наличии)

3) Наивысший активный IP-адрес любого из физических интерфейсов маршрутизатора

Поскольку ни на одном из трёх маршрутизаторов не настроены идентификаторы маршрутизатора или loopback-интерфейсы, идентификатор каждого маршрутизатора определяется наивысшим IP-адресом любого активного интерфейса.

В третьей части вам необходимо изменить значение ID идентификатора OSPF-маршрутизатора с помощью loopback-адресов. Также вам предстоит использовать команду router-id для изменения идентификатора маршрутизатора.

Шаг 1: Измените идентификаторы маршрутизатора, используя loopback-адреса.

a. Назначьте IP-адрес loopback 0 для маршрутизатора R1.

```
R1(config)# interface lo0

R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
```

b. Назначьте IP-адреса loopback 0 для маршрутизаторов R2 и R3. Используйте IP-адрес 2.2.2.2/32 для R2 и 3.3.3.3/32 для R3.

c. Сохраните текущую конфигурацию в загрузочную на всех трёх маршрутизаторах.

d. Для того чтобы идентификатор маршрутизатора получил значение loopback-адреса, необходимо перезагрузить маршрутизаторы. Выполните команду reload на всех трёх маршрутизаторах. Нажмите клавишу Enter, чтобы подтвердить перезагрузку.

e. После перезагрузки маршрутизатора выполните команду show ip protocols, чтобы просмотреть новый идентификатор маршрутизатора

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:01:00
    2.2.2.2              110      00:01:14
  Distance: (default is 110)
```

f. Выполните show ip ospf neighbor, чтобы отобразить изменения идентификатора маршрутизатора для соседних маршрутизаторов.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:35    192.168.13.2    Serial0/0/1
2.2.2.2           0   FULL/  -        00:00:32    192.168.12.2    Serial0/0/0
R1#
```

Шаг 2: Измените идентификатор маршрутизатора R1 с помощью команды router-id.

Наиболее предпочтительным способом изменения ID маршрутизатора осуществляется с помощью

команды router-id.

a. Чтобы переназначить идентификатор маршрутизатора, выполните команду router-id 11.11.11.11 на маршрутизаторе R1. Обратите внимание на уведомление, которое появляется при выполнении команды router-id.

```
R1(config)# router ospf 1
R1(config-router)# router-id 11.11.11.11
Reload or use "clear ip ospf process" command, for this to take effect
R1(config)# end
```

b. Вы получите уведомление о том, что для того, чтобы изменения вступили в силу, вам необходимо либо перезагрузить маршрутизатор, либо использовать команду clear ip ospf process. Выполните команду clear ip ospf process на всех трёх маршрутизаторах. Введите yes, чтобы подтвердить сброс, и нажмите клавишу Enter.

c.Для маршрутизатора R2 настройте идентификатор 22.22.22.22, а для маршрутизатора R3 - идентификатор 33.33.33.33. Затем используйте команду clear ip ospf process, чтобы сбросить процесс маршрутизации OSPF.

d.Выполните команду show ip protocols, чтобы проверить изменился ли идентификатор маршрутизатора R1.

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 11.11.11.11
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    192.168.12.0 0.0.0.3 area 0
    192.168.13.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    33.33.33.33          110      00:00:19
    22.22.22.22          110      00:00:31
    3.3.3.3              110      00:00:41
    2.2.2.2              110      00:00:41
  Distance: (default is 110)
```

e. Выполните команду show ip ospf neighbor на маршрутизаторе R1, чтобы убедиться, что новые идентификаторы маршрутизаторов R2 и R3 содержатся в списке.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
33.33.33.33       0   FULL/  -        00:00:36    192.168.13.2    Serial0/0/1
22.22.22.22       0   FULL/  -        00:00:32    192.168.12.2    Serial0/0/0
```

Часть 4: Настройка пассивных интерфейсов OSPF

Команда passive-interface запрещает отправку обновлений маршрутизации из определённого интерфейса маршрутизатора. В большинстве случаев команда используется для уменьшения трафика в сетях LAN, поскольку им не нужно получать сообщения протокола динамической маршрутизации. В четвёртой части вам предстоит использовать команду passive-interface для настройки интерфейса в качестве пассивного. Также вы настроите OSPF таким образом, чтобы все интерфейсы маршрутизатора были пассивными по умолчанию, а затем включите объявления протокола маршрутизации OSPF на выбранных интерфейсах.

Шаг 1: Настройте пассивный интерфейс.

a. Выполните команду show ip ospf interface g0/0 на маршрутизаторе R1. Обратите внимание на таймер, указывающий время получения очередного пакета приветствия. Пакеты приветствия отправляются каждые 10 секунд и используются маршрутизаторами OSPF для проверки работоспособности соседних устройств.

```
R1# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

b. Выполните команду passive-interface, чтобы интерфейс G0/0 маршрутизатора R1 стал пассивным.

```
R1(config)# router ospf 1
R1(config-router)# passive-interface g0/0
```

c.Повторно выполните команду show ip ospf interface g0/0, чтобы убедиться, что интерфейс G0/0 стал пассивным.

```
R1# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 11.11.11.11, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 11.11.11.11, Interface address 192.168.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
```

d. Выполните команду show ip route на маршрутизаторах R2 и R3, чтобы убедиться, что маршрут к сети 192.168.1.0/24 по-прежнему доступен.

```
R2# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      2.0.0.0/32 is subnetted, 1 subnets
C        2.2.2.2 is directly connected, Loopback0
O     192.168.1.0/24 [110/65] via 192.168.12.1, 00:58:32, Serial0/0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet0/0
L        192.168.2.1/32 is directly connected, GigabitEthernet0/0
O     192.168.3.0/24 [110/65] via 192.168.23.2, 00:58:19, Serial0/0/1
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/30 is directly connected, Serial0/0/0
L        192.168.12.2/32 is directly connected, Serial0/0/0
      192.168.13.0/30 is subnetted, 1 subnets
O        192.168.13.0 [110/128] via 192.168.23.2, 00:58:19, Serial0/0/1
                      [110/128] via 192.168.12.1, 00:58:32, Serial0/0/0
      192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.23.0/30 is directly connected, Serial0/0/1
L        192.168.23.1/32 is directly connected, Serial0/0/1
```

Шаг 2: Настройте маршрутизатор так, чтобы все его интерфейсы были пассивными по умолчанию.

a. Выполните команду show ip ospf neighbor на маршрутизаторе R1, чтобы убедиться, что R2 указан в качестве соседа OSPF.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
33.33.33.33       0   FULL/  -        00:00:31    192.168.13.2    Serial0/0/1
22.22.22.22       0   FULL/  -        00:00:32    192.168.12.2    Serial0/0/0
```

b. Выполните команду passive-interface default на R2, чтобы по умолчанию настроить все интерфейсы OSPF в качестве пассивных.

```
R2(config)# router ospf 1
R2(config-router)# passive-interface default
R2(config-router)#
*Apr  3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from
FULL to DOWN, Neighbor Down: Interface down or detached
*Apr  3 00:03:00.979: %OSPF-5-ADJCHG: Process 1, Nbr 33.33.33.33 on Serial0/0/1 from
FULL to DOWN, Neighbor Down: Interface down or detached
```

c. Повторно выполните команду show ip ospf neighbor на R1. После истечения таймера простоя маршрутизатор R2 больше не будет указан, как сосед OSPF.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
33.33.33.33       0   FULL/  -        00:00:34    192.168.13.2    Serial0/0/1
```

d. Выполните команду show ip ospf interface S0/0/0 на маршрутизаторе R2, чтобы просмотреть состояние OSPF интерфейса S0/0/0.

```
R2# show ip ospf interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 192.168.12.2/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 22.22.22.22, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

e. В случае если все интерфейсы маршрутизатора R2 являются пассивными, маршрутизирующая информация объявляться не будет. В этом случае маршрутизаторы R1 и R3 больше не должны иметь маршрут к

сети 192.168.2.0/24. Это можно проверить с помощью команды show ip route.

f. На маршрутизаторе R2 выполните команду no passive-interface, чтобы маршрутизатор отправлял и получал обновления маршрутизации OSPF. После ввода этой команды появится уведомление

о том, что на маршрутизаторе R1 были установлены отношения смежности.

```
R2(config)# router ospf 1
R2(config-router)# no passive-interface s0/0/0
R2(config-router)#
*Apr  3 00:18:03.463: %OSPF-5-ADJCHG: Process 1, Nbr 11.11.11.11 on Serial0/0/0 from
LOADING to FULL, Loading Done
```

g. Повторно выполните команды show ip route и show ipv6 ospf neighbor на маршрутизаторах R1 и R3 и найдите маршрут к сети 192.168.2.0/24.

Какой интерфейс использует R3 для прокладки маршрута к сети 192.168.2.0/24? Чему равна суммарная стоимость для сети 192.168.2.0/24 на R3? Отображается ли маршрутизатор R2 как сосед OSPF на маршрутизаторе R1? Отображается ли маршрутизатор R2 как сосед OSPF на маршрутизаторе R3? Что даёт вам эта информация?

h. Настройте интерфейс S0/0/1 маршрутизатора R2 таким образом, чтобы он мог объявлять маршруты OSPF. Ниже запишите используемые команды.

i. Повторно выполните команду show ip route на маршрутизаторе R3.

Какой интерфейс использует R3 для прокладки маршрута к сети 192.168.2.0/24?

Чему равна суммарная стоимость для сети 192.168.2.0/24 на R3? Как она была рассчитана?

Отображается ли маршрутизатор R2 как сосед OSPF для маршрутизатора R3?

Часть 5: Изменение метрик OSPF

В части 3 необходимо изменить метрики OSPF с помощью команд auto-cost reference-bandwidth, bandwidth и ip ospf cost.

Примечание. В части 1 на всех интерфейсах DCE нужно было установить значение тактовой частоты 128000.

Шаг 1: Измените заданную пропускную способность на маршрутизаторах.

Заданная пропускная способность по умолчанию для OSPF равна 100 Мб/с (скорость Fast Ethernet). Однако скорость каналов в большинстве современных устройств сетевой инфраструктуры превышает 100 Мб/с. Поскольку метрика стоимости OSPF должна быть целым числом, стоимость во всех каналах со скоростью передачи 100 Мб/с и выше равна 1. Вследствие этого интерфейсы Fast Ethernet, Gigabit Ethernet и 10G Ethernet имеют одинаковую стоимость. Поэтому, для правильного

использования сетей со скоростью канала более 100 Мб/с, заданную пропускную способность необходимо установить на большее значение.

a. Выполните команду show interface на маршрутизаторе R1, чтобы просмотреть значение пропускной способности по умолчанию для интерфейса G0/0.

```
R1# show interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is c471.fe45.7520 (bia c471.fe45.7520)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45

     output flow-control is unsupported, input flow-control is unsupported
     ARP type: ARPA, ARP Timeout 04:00:00
     Last input never, output 00:17:31, output hang never
     Last clearing of "show interface" counters never
     Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
     Queueing strategy: fifo
     Output queue: 0/40 (size/max)
     5 minute input rate 0 bits/sec, 0 packets/sec
     5 minute output rate 0 bits/sec, 0 packets/sec
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts (0 IP multicasts)
        0 runts, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
        0 watchdog, 0 multicast, 0 pause input
        279 packets output, 89865 bytes, 0 underruns
        0 output errors, 0 collisions, 1 interface resets
        0 unknown protocol drops
        0 babbles, 0 late collision, 0 deferred
        1 lost carrier, 0 no carrier, 0 pause output
        0 output buffer failures, 0 output buffers swapped out
```

Примечание. Пропускная способность на интерфейсе G0/0 может отличаться от значения, приведённого выше, если интерфейс узла ПК может поддерживать только скорость Fast Ethernet. Если интерфейс узла ПК не поддерживают скорость передачи 1 Гб/с, то пропускная способность, скорее всего, будет отображена как 100000 Кб/с.

b. Выполните команду show ip route ospf на R1, чтобы определить маршрут к сети 192.168.3.0/24.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:57, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/128] via 192.168.13.2, 00:00:57, Serial0/0/1
                      [110/128] via 192.168.12.2, 00:01:08, Serial0/0/0
```

Примечание. Суммарная стоимость маршрута к сети 192.168.3.0/24 от маршрутизатора R1 должна быть равна 65.

c. Выполните команду show ip ospf interface на маршрутизаторе R3, чтобы определить стоимость маршрутизации для интерфейса G0/0.

```
R3# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
    Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
    Topology-MTID    Cost    Disabled    Shutdown      Topology Name
          0           1         no          no            Base
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
    No backup designated router on this network
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      oob-resync timeout 40
      Hello due in 00:00:05
    Supports Link-local Signaling (LLS)
    Cisco NSF helper support enabled
    IETF NSF helper support enabled
    Index 1/1, flood queue length 0
    Next 0x0(0)/0x0(0)
    Last flood scan length is 0, maximum is 0
    Last flood scan time is 0 msec, maximum is 0 msec
    Neighbor Count is 0, Adjacent neighbor count is 0
    Suppress hello for 0 neighbor(s)
```

d. Выполните команду show ip ospf interface s0/0/1 на маршрутизаторе R1, чтобы просмотреть стоимость маршрутизации для интерфейса S0/0/1.

```
R1# show ip ospf interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           64        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.23.2
  Suppress hello for 0 neighbor(s)
```

Как видно из выходных данных команды show ip route, сумма метрик стоимости этих двух интерфейсов и суммарная стоимость маршрута к сети 192.168.3.0/24 на маршрутизаторе R3 рассчитывается по формуле 1 + 64 = 65.

e. Выполните команду auto-cost reference-bandwidth 10000 на маршрутизаторе R1, чтобы изменить параметр заданной пропускной способности по умолчанию. С подобной установкой стоимость интерфейсов 10 Гб/с будет равна 1, стоимость интерфейсов 1 Гбит/с будет равна 10, а стоимость интерфейсов 100 Мб/с будет равна 100.

```
R1(config)# router ospf 1

R1(config-router)# auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
```

f. Выполните команду auto-cost reference-bandwidth 10000 на маршрутизаторах R2 и R3.

g. Повторно выполните команду show ip ospf interface, чтобы просмотреть новую стоимость интерфейса G0/0 на R3 и интерфейса S0/0/1 на R1.

```
R3# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.3.1/24, Area 0, Attached via Network Statement
  Process ID 1, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 10
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           10        no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.23.2, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Примечание. Если устройство, подключённое к интерфейсу G0/0, не поддерживает скорость Gigabit Ethernet, то стоимость будет отличаться от отображаемых выходных данных. Например, для скорости Fast Ethernet (100 Мб/с) стоимость будет равна 100.

```
R1# show ip ospf interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.13.1/30, Area 0, Attached via Network Statement
  Process ID 1, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 6476
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0          6476       no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:05
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
```

Adjacent with neighbor 192.168.23.2 Suppress hello for 0 neighbor(s)

h. Повторно выполните команду show ip route ospf, чтобы просмотреть новую суммарную стоимость для маршрута 192.168.3.0/24 (10 + 6476 = 6486).

Примечание. Если устройство, подключённое к интерфейсу G0/0, не поддерживает скорость Gigabit Ethernet, то стоимость будет отличаться от того, что отображается в выходных данных. Например, если интерфейс

G0/0 работает на скорости Fast Ethernet (100 Мб/с), то суммарная стоимость будет равна 6576.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.2.0/24 [110/6486] via 192.168.12.2, 00:05:40, Serial0/0/0
O     192.168.3.0/24 [110/6486] via 192.168.13.2, 00:01:08, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/12952] via 192.168.13.2, 00:05:17, Serial0/0/1
                      [110/12952] via 192.168.12.2, 00:05:17, Serial0/0/
```

Примечание. Изменение заданной пропускной способности по умолчанию на маршрутизаторах с 100 на 10 000 изменяет суммарные стоимости всех маршрутизаторов в 100 раз, но стоимость каждого канала и маршрута интерфейса рассчитывается точнее.

i. Для того чтобы восстановить заданную пропускную способность до значения по умолчанию, на всех трёх маршрутизаторах выполните команду auto-cost reference-bandwidth 100.

```
R1(config)# router ospf 1
R1(config-router)# auto-cost reference-bandwidth 100
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
```

Для чего имеет смысл изменять заданную пропускную способность OSPF?

Шаг 2: Измените пропускную способность для интерфейса.

На большинстве последовательных каналов метрика пропускной способности имеет значение по умолчанию, равное 1544 Кбит (T1). В случае если реальная скорость последовательного канала другая, то для правильного расчёта стоимости маршрута в OSPF параметр пропускной способности нужно будет изменить, чтобы она была равна фактической скорости. Используйте команду bandwidth, чтобы откорректировать значение пропускной способности на интерфейсе.

Примечание. Согласно распространённому заблуждению, команда bandwidth может изменить физическую пропускную способность (или скорость) канала. Команда изменяет метрику пропускной способности, используемой алгоритмом OSPF для расчёта стоимости маршрутизации, но не изменяет фактическую пропускную способность (скорость) канала.

a. Выполните команду show interface s0/0/0 на маршрутизаторе R1, чтобы просмотреть установленное значение пропускной способности на интерфейсе S0/0/0. Реальная скорость передачи данных на этом

интерфейсе, установленная командой clock rate, составляет 128 Кб/с, при этом установленное значение пропускной способности по-прежнему равно 1544 Кб/с.

```
R1# show interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 192.168.12.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
<Output omitted>
```

b. Выполните команду show ip route ospf на маршрутизаторе R1, чтобы просмотреть суммарную стоимость для маршрута к сети 192.168.23.0/24 через интерфейс S0/0/0. Обратите внимание, что к сети 192.168.23.0/24 есть два маршрута с равной стоимостью (128): один через интерфейс S0/0/0, другой через интерфейс S0/0/1.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.3.0/24 [110/65] via 192.168.13.2, 00:00:26, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/128] via 192.168.13.2, 00:00:26, Serial0/0/1
                      [110/128] via 192.168.12.2, 00:00:42, Serial0/0/0
```

c. Выполните команду bandwidth 128, чтобы установить на интерфейсе S0/0/0 пропускную способность равную 128 Кб/с.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
R1(config)# interface s0/0/0
R1(config-if)# bandwidth 128
```

d. Повторно выполните команду show ip route ospf. В таблице маршрутизации больше не отображается маршрут к сети 192.168.23.0/24 через интерфейс S0/0/0. Это связано с тем, что оптимальный маршрут с наименьшей стоимостью проложен через S0/0/1.

```
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.3.0/24 [110/65] via 192.168.13.2, 00:04:51, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/128] via 192.168.13.2, 00:04:51, Serial0/0/1
```

e. Выполните show ip ospf interface brief. Стоимость для интерфейса S0/0/0 изменилась с 64 на 781, что является более точным представлением стоимости скорости канала. `R1# show ip ospf interface brief`

Interface	PID	Area	IP Address/Mask	Cost	State	Nbrs F/C
Se0/0/1	1	0	192.168.13.1/30	64	P2P	1/1
Se0/0/0	1	0	192.168.12.1/30	781	P2P	1/1
Gi0/0	1	0	192.168.1.1/24	1	DR	0/0

f. Измените пропускную способность для интерфейса S0/0/1 на значение, установленное для интерфейса S0/0/0 маршрутизатора R1.

g. Повторно выполните команду show ip route ospf, чтобы просмотреть суммарную стоимость обоих маршрутов к сети 192.168.23.0/24. Обратите внимание, что к сети 192.168.23.0/24 есть два маршрута с одинаковой стоимостью (845): один через интерфейс S0/0/0, другой через интерфейс S0/0/1.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.3.0/24 [110/782] via 192.168.13.2, 00:00:09, Serial0/0/1
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/845] via 192.168.13.2, 00:00:09, Serial0/0/1
                      [110/845] via 192.168.12.2, 00:00:09, Serial0/0/0
```

Объясните, как были рассчитаны стоимости для сетей 192.168.3.0/24 и 192.168.23.0/30 от маршрутизатора R1.Стоимость маршрута к сети 192.168.3.0/24: R1 S0/0/1 + R3 G0/0 (781+1=782). Стоимость маршрута к сети 192.168.23.0/30: R1 S0/0/1 + R3 S0/0/1 (781+64=845).

h. Выполните команду show ip route ospf на R3. Суммарная стоимость сети 192.168.1.0/24 по- прежнему равна 65. В отличие от

команды clock rate, команду bandwidth следует выполнить на каждом конце последовательного канала.

```
R3# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.1.0/24 [110/65] via 192.168.13.1, 00:30:58, Serial0/0/0
      192.168.12.0/30 is subnetted, 1 subnets
O        192.168.12.0 [110/128] via 192.168.23.1, 00:30:58, Serial0/0/1
                      [110/128] via 192.168.13.1, 00:30:58, Serial0/0/0
```

i. Выполните команду bandwidth 128 на всех остальных последовательных интерфейсах в топологии.

Чем равна новая суммарная стоимость для сети 192.168.23.0/24 на R1? Почему?

Шаг 3: Измените стоимость маршрута.

Для расчёта стоимости канала OSPF использует значение, установленное командой bandwidth. Рассчитанную стоимость можно изменить, настроив вручную стоимость канала с помощью команды ip ospf cost. Как и команда bandwidth, команда ip ospf cost действует только на той стороне канала, на которой она была применена.

a. Введите команду show ip route ospf на маршрутизаторе R1.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.2.0/24 [110/782] via 192.168.12.2, 00:00:26, Serial0/0/0
O     192.168.3.0/24 [110/782] via 192.168.13.2, 00:02:50, Serial0/0/1


      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/1562] via 192.168.13.2, 00:02:40, Serial0/0/1
                      [110/1562] via 192.168.12.2, 00:02:40, Serial0/0/0
```

b. Выполните команду ip ospf cost 1565 на интерфейсе S0/0/1 маршрутизатора R1. Стоимость 1565 является выше суммарной стоимости маршрута, проходящего через R2 (1562).

```
R1(config)# int s0/0/1
R1(config-if)# ip ospf cost 1565
```

c.Повторно выполните команду show ip route ospf на R1, чтобы отобразить изменения в таблице маршрутизации. Теперь все маршруты OSPF для маршрутизатора R1 направляются через маршрутизатор R2.

```
R1# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O     192.168.2.0/24 [110/782] via 192.168.12.2, 00:02:06, Serial0/0/0
O     192.168.3.0/24 [110/1563] via 192.168.12.2, 00:05:31, Serial0/0/0
      192.168.23.0/30 is subnetted, 1 subnets
O        192.168.23.0 [110/1562] via 192.168.12.2, 01:14:02, Serial0/0/0
```

Примечание. Изменение метрик стоимости канала с помощью команды ip ospf cost — это наиболее простой и предпочтительный способ изменения стоимости маршрутов OSPF. Помимо изменения стоимости в связи с реальным значением пропускной способности, у сетевого администратора могут быть другие причины для изменения стоимости маршрута, например, известная пропускная способность, предоставляемой оператором связи или фактическая стоимость канала или маршрута.

Почему маршрут к сети 192.168.3.0/24 маршрутизатора R1 теперь проходит через R2?

Вопросы на закрепление

1. Почему так важно контролировать значение ID маршрутизатора при использовании протокола OSPF?

2. Почему процесс выбора DR/BDR не рассматривается в этой лабораторной работе?

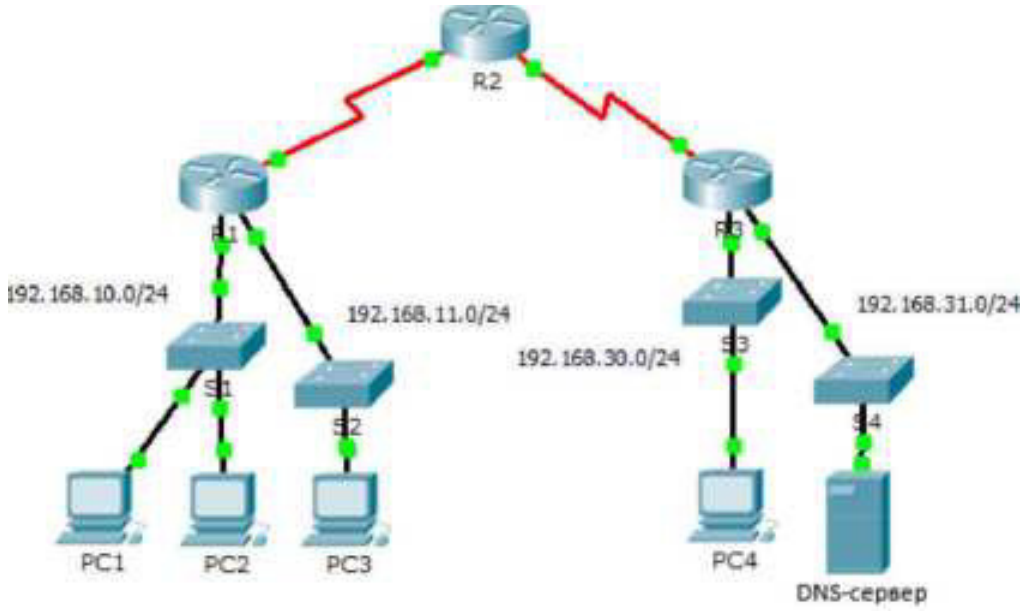
3. Почему имеет смысл устанавливать интерфейс OSPF в качестве пассивного?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Практическая работа 9. Наглядное представление работы ACL-списка

Топология



Задачи

Часть 1. Проверка локального подключения и тестирование работы списка контроля доступа Часть 2. Удаление списка контроля доступа и повторное тестирование

Исходные данные

В рамках этого задания вы получите представление о том, как можно использовать список контроля доступа (ACL) для запрещения эхо-запросов, отправленных на узлы удалённых сетей. После удаления ACL-списка из конфигурации эхо-запросы будут успешными.

Часть 1. Проверка локального подключения и тестирование списка контроля доступа

Шаг 1: Отправьте эхо-запросы по локальной сети, чтобы проверить подключение.

a. Из командной строки узла PC1 отправьте эхо-запрос на PC2.

b. Из командной строки узла PC1 отправьте эхо-запрос на PC3. Почему эхо-запросы прошли успешно?

Шаг 2: Отправьте эхо-запросы в удалённые сети, чтобы протестировать работу ACL- списка.

a. Из командной строки узла PC1 отправьте эхо-запрос на PC4.

b. Из командной строки узла PC1 отправьте эхо-запрос на DNS-сервер.

Почему эхо-запросы были выполнены неудачно? (Совет. Чтобы узнать источник проблемы, используйте режим моделирования или просмотрите конфигурации маршрутизатора).

Часть 2. Удаление ACL-списка и повторное тестирование

Шаг 1: Используйте команды show, чтобы проверить конфигурацию ACL-списка.

a. Используйте команды show run и show access-lists, чтобы просмотреть текущие ACL-списки. Для быстрого просмотра текущих ACL-списков используйте команду show access-lists. Введите команду show access-lists, после которой нажмите ПРОБЕЛ и поставьте вопросительный знак (?), чтобы просмотреть доступные параметры:

```
R1#show access-lists ?
  <1-199>  ACL number
  WORD     ACL name
  <cr>
```

Если вы знаете номер или имя ACL-списка, вы можете дополнительно отфильтровать выходные данные команды show. Однако, маршрутизатор R1 обладает только одним списком контроля доступа; поэтому команды show access-lists будет достаточно.

```
R1#show access-lists
Extended IP access list 101
    deny icmp any any echo
    permit ip any any
```

Первая строка ACL-списка запрещает передачу эхо-запросов ICMP из любого источника к любому месту назначению. Вторая строка списка пропускает остальной IP-трафик, направленный от любого источника к любому месту назначения (ip any any).

b. Для работы ACL-списка на маршрутизаторе, его необходимо применить. В этом сценарии ACL- список используется для фильтрации трафика на интерфейсе. Несмотря на возможность просматривать сведения об IP с помощью команды show ip interface, в некоторых случаях эффективнее использовать команду show run. К какому интерфейсу применяется ACL-список при использовании одной или обеих команд?

Шаг 2: Удаление списка доступа 101 из конфигурации

ACL-список можно удалить из конфигурации, применив команду no access list *[номер списка ACL]*.

В то время как применение команды no access-list приводит к удалению всех ACL-списков,

настроенных на маршрутизаторе, команда no access-list *[номер списка контроля доступа]* позволяет

удалить конкретный список контроля доступа.

a. В режиме глобальной конфигурации удалите ACL-список посредством следующей команды:

```
R1(config)# no access-list 101
```

b. Убедитесь, что теперь узел PC1 может отправить эхо-запрос на DNS-сервер.Предлагаемый способ подсчёта баллов

Пункт, содержащий вопрос	Возможное количество баллов	Количество заработанных баллов
Часть 1, шаг 1b.	50	
Часть 1, шаг 2b.	40	
Часть 2, шаг 2b.	10	
Общее количество баллов	100	

Практическая работа 10. Настройка и проверка стандартных ACL-списков

Топология

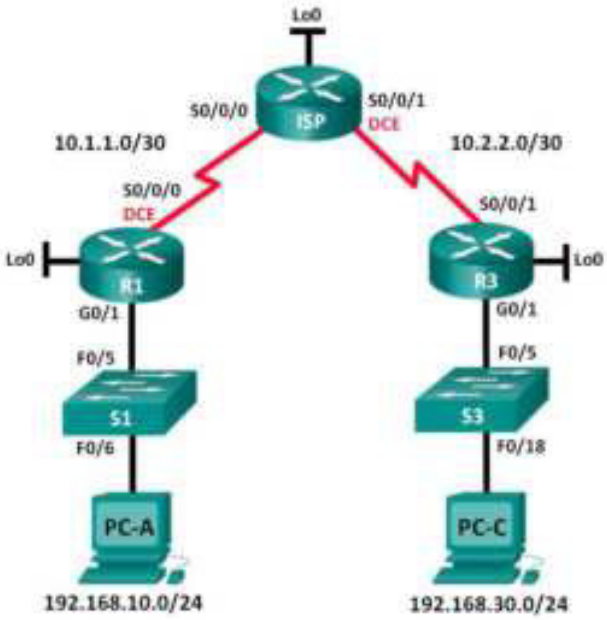


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	192.168.20.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Задачи

Часть 1. Настройка топологии и установка исходного состояния устройства

- Настройте оборудование в соответствии с топологией сети.
- Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

- Часть 2. Конфигурация устройств и проверка подключения
- Назначьте компьютерам статический IP-адрес.
- Настройте базовые параметры на маршрутизаторах.
- Настройте базовые параметры на коммутаторах.
- Настройте маршрутизацию EIGRP на маршрутизаторах R1, ISP и R3.
- Проверьте наличие подключения между всеми устройствами.

Часть 3. Настройка и проверка стандартных нумерованных списков ACL и стандартных именованных ACL-списков

- Настройте, примените и проверьте работу нумерованных стандартных ACL-списков.
- Настройте, примените и проверьте работу стандартных именованных ACL-списков. Часть 4. Изменение стандартного ACL-списка
- Измените и проверьте работу стандартного именованного ACL-списка.
- Проверьте работу ACL-списка.Исходные данные/сценарий

Обеспечение сетевой безопасности является важным аспектом при разработке и управлении IP- сетями. Ценным навыком является умение применять соответствующие правила для фильтрации пакетов на основе установленной политики безопасности.

В данной лабораторной работе вы настроите правила фильтрации для двух офисов, представленных маршрутизаторами R1 и R3. Руководство определило некоторые правила в рамках политики безопасности для сетей LAN, расположенных на маршрутизаторах R1 и R3, которые вы должны реализовать. На маршрутизаторе ISP, расположенном между R1 и R3, ACL-списки не будут использоваться. У вас не будет прав административного доступа к маршрутизатору ISP, поскольку вы можете управлять только собственным оборудованием.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсе маршрутизатора в конце этой лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

• 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);

• 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);

• консольные кабели для настройки устройств Cisco IOS через консольные порты;

• кабели Ethernet и последовательные кабели в соответствии с топологией.

•

Часть 1: Настройка топологии и инициализация устройств

В первой части лабораторной работы вам предстоит создать топологию сети и при необходимости удалить все текущие настройки.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Часть 2: Настройка устройств и проверка подключения

Во второй части вам предстоит настроить базовые параметры маршрутизаторов, коммутаторов и компьютеров. Имена и адреса устройств указаны в топологии и таблице адресации.

Шаг 1: Настройте IP-адреса на PC-A и PC-C.

Шаг 2: Настройте базовые параметры маршрутизаторов.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Создайте интерфейсы loopback на каждом маршрутизаторе в соответствии с таблицей адресации.

d. Настройте IP-адреса интерфейсов в соответствии с топологией и таблицей адресации.

e. Установите пароль class для доступа к привилегированному режиму EXEC.

f. Установите тактовую частоту на 128000 для всех последовательных интерфейсов DCE.

g. Назначьте cisco в качестве пароля консоли.

h. Назначьте cisco в качестве пароля виртуального терминала VTY и активируйте доступ через Telnet.

Шаг 3: Настройка базовых параметров на коммутаторах (дополнительно).

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте административный IP-адрес интерфейса в соответствии с таблицами топологии и адресации.

d. Установите пароль class для доступа к привилегированному режиму EXEC.

e. Настройте шлюз по умолчанию.

f. Назначьте cisco в качестве пароля консоли.

g. Назначьте cisco в качестве пароля виртуального терминала VTY и активируйте доступ через Telnet.

Шаг 4: Настройте маршрутизацию EIGRP на маршрутизаторах R1, ISP и R3.

a. Настройте автономную систему (AS) номер 10 и объявите все сети на маршрутизаторах R1, ISP и R3. Отключите автоматическое суммирование маршрутов.

b. После настройки EIGRP на маршрутизаторах R1, ISP и R3 убедитесь, что все маршрутизаторы имеют заполненные таблицы маршрутизации с необходимыми для работы сетями. В случае необходимости выполните поиск и устранение неполадок.

Шаг 5: Проверьте наличие подключения между всеми устройствами.

Примечание. Соединение важно проверять перед настройкой и применением списков доступа!

Удостовериться в правильной работе сети необходимо до начала фильтрации трафика.

a. От узла PC-A отправьте эхо-запрос на PC-C и интерфейс loopback маршрутизатора R3. Успешно ли выполнены эхо-запросы?

b. От маршрутизатора R1 отправьте эхо-запрос на PC-C и loopback-интерфейс на маршрутизаторе R3. Успешно ли выполнены эхо-запросы?

c. От узла PC-C отправьте эхо-запрос на PC-A и интерфейс loopback маршрутизатора R1. Успешно ли выполнены эхо-запросы?

d. От маршрутизатора R3 отправьте эхо-запрос на PC-A и интерфейс loopback маршрутизатора R1. Успешно ли выполнены эхо-запросы?

Часть 3: Настройка и проверка стандартных нумерованных ACL-списков и стандартных именованных ACL-списков

Шаг 1: Настройка стандартного именованного ACL-списка.

Стандартные ACL-списки фильтруют трафик, исходя только из адреса источника. Согласно принятой рекомендации стандартные ACL-списки следует настраивать и применять как можно ближе к назначению. Для первого списка доступа создайте стандартный нумерованный ACL-список, который пропускает трафик от всех узлов в сети 192.168.10.0/24 и всех узлов в сети 192.168.20.0/24 ко всем узлам в сети 192.168.30.0/24. Согласно политике безопасности в конце всех ACL-списков должна содержаться запрещающая запись контроля доступа deny any (ACE), которую также называют оператором ACL-списка.

Какую шаблонную маску вы будете использовать, чтобы разрешить всем узлам из сети 192.168.10.0/24 доступ к сети 192.168.30.0/24?

Следуя практическим рекомендациям Cisco, на каком маршрутизаторе вы разместите ACL-список?

На каком интерфейсе вы разместите этот список? В каком направлении вы его примените?

a. Настройте ACL-список на маршрутизаторе R3. В качестве номера списка доступа используйте 1.

```
R3(config)# access-list 1 remark Allow R1 LANs Access
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255
R3(config)# access-list 1 deny any
```

b. Примените ACL-список к подходящему интерфейсу в нужном направлении.

```
R3(config)# interface g0/1
R3(config-if)# ip access-group 1 out
```

c.Проверьте нумерованный ACL-список.

Использование команды show поможет вам при проверке синтаксиса и размещении списков ACL в вашем маршрутизаторе.

Какую команду вы будете использовать для просмотра полного списка доступа 1 со всеми записями ACE?

Какую команду вы будете использовать, чтобы просмотреть, где и в каком направлении был применён список доступа?

1) На маршрутизаторе R3 выполните команду show access-lists 1.

```
R3# show access-list 1
Standard IP access list 1
    10 permit 192.168.10.0, wildcard bits 0.0.0.255
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
    30 deny   any
```

На маршрутизаторе R3 выполните команду show ip interface g0/1.

```
R3# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 1
  Inbound access list is not set
  Output omitted
```

2)Проверьте, пропускает ли ACL-список трафик из сети 192.168.10.0/24 в сеть 192.168.30.0/24. Из командной строки узла PC-A отправьте эхо-запрос на IP-адрес PC-C. Успешно ли выполнен эхо-запрос?

3)Проверьте, пропускает ли ACL-список трафик из сети 192.168.20.0/24 в сеть 192.168.30.0/24. Вам нужно выполнить расширенный эхо-запрос и использовать loopback-адрес 0 на маршрутизаторе R1 в качестве источника. Отправьте эхо-запрос на IP-адрес узла PC-C. Успешно ли выполнен эхо-запрос?

```
R1# ping
Protocol [ip]:
Target IP address: 192.168.30.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.20.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

d. Из командной строки маршрутизатора R1 снова отправьте эхо-запрос на IP-адрес узла PC-C. `R1# ping 192.168.3.3` Успешно ли выполнен эхо-запрос? Поясните свой ответ.

Шаг 2: Настройте стандартный именованный ACL-список.

Создайте стандартный именованный ACL-список, который соответствует следующему правилу: список должен разрешать доступ для трафика со всех узлов из сети 192.168.40.0/24 ко всем узлам в сети 192.168.10.0/24. Кроме того, доступ в сеть 192.168.10.0/24 должен быть разрешён только для узла PC- C. Этот список доступа должен быть назван BRANCH-OFFICE-POLICY.

Следуя практическим рекомендациям Cisco, на каком маршрутизаторе вы разместите ACL-список? На каком интерфейсе вы разместите этот список? В каком направлении вы его примените?

a. Создайте стандартный ACL-список под именем BRANCH-OFFICE-POLICY на маршрутизаторе R1.

```
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# permit host 192.168.30.3
R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255
R1(config-std-nacl)# end
R1#
*Feb 15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console
```

Взгляните на первую запись ACE в списке доступа и ответьте, можно ли записать это иначе?

b. Примените ACL-список к подходящему интерфейсу в нужном направлении.

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out
```

c.Проверьте именованный ACL-список.

1) На R1 выполните команду show access-lists.

```
R1# show access lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3
    20 permit 192.168.40.0, wildcard bits 0.0.0.255
```

Существуют ли различия между ACL-списком на маршрутизаторе R1 и ACL-списком на маршрутизаторе R3? Если да, в чём они заключаются?

2) На маршрутизаторе R1 выполните команду show ip interface g0/1.

```
R1# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is BRANCH-OFFICE-POLICY
  Inbound access list is not set
<Output omitted>
```

3) Проверьте работу ACL-списка. Из командной строки узла PC-C отправьте эхо-запрос на IP- адрес узла PC-A. Успешно ли выполнен эхо-запрос?

4) Проверьте ACL-список, чтобы удостовериться, что доступ к сети 192.168.10.0/24 настроен только на узле PC-C. Вам нужно выполнить расширенный эхо-запрос и использовать адрес G0/1 на маршрутизаторе R3 в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A. Успешно ли выполнен эхо-запрос?

5) Проверьте, пропускает ли ACL-список трафик из сети 192.168.40.0/24 в сеть 192.168.10.0/24. Вам нужно выполнить расширенный эхо-запрос и использовать loopback-адрес 0 на маршрутизаторе R3 в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A. Успешно ли выполнен эхо-запрос?

Часть 4: Изменение стандартного ACL-списка

Политика безопасности нередко претерпевает изменения. По этой причине ACL-списки тоже необходимо изменять. В четвёртой части вам предстоит изменить один из ранее настроенных вами ACL-списков для соответствия новой политике безопасности.

Руководство решило, что пользователи из сети 209.165.200.224/27 должны получить полный доступ к сети 192.168.10.0/24. Также руководство хочет, чтобы правила в ACL-списках на всех их маршрутизаторах выполнялись последовательно. В конце всех ACL-списков должна быть внесена запись ACE deny any. Вам необходимо изменить ACL-список с именем BRANCH-OFFICE-POLICY.

Также вам предстоит добавить в этот список ACL две дополнительные строки. Это можно сделать двумя способами:

Вариант 1: Выполните команду no access-list standard BRANCH-OFFICE-POLICY в режиме глобальной конфигурации. Это исключит весь ACL-список из маршрутизатора. В зависимости от IOS маршрутизатора, произойдет один из следующих вариантов: вся фильтрация пакетов будет отменена, и все пакеты будут пропускаться через маршрутизатор; либо, поскольку команда ip access-group в интерфейс G0/1 активна, фильтрация останется прежней. В любом случае, когда ACL-список будет удалён, вы сможете заново ввести весь ACL-список или вырезать и вставить записи из текстового редактора.

Вариант 2: ACL-списки можно изменить, не удаляя, добавив или удалив конкретные строки из ACL- списка. Этот вариант наиболее удобен, особенно в случае если ACL-список содержит много записей. При повторном вводе всего ACL-списка или при вырезании и копировании могут возникнуть ошибки. В изменении определённых строк в списках ACL нет ничего сложного.

Примечание. В ходе данной лабораторной работы используйте вариант 2.

Шаг 1: Изменение стандартного именованного ACL-списка.

а. В привилегированном режиме маршрутизатора R1 выполните команду show access-lists.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
```

Добавьте две дополнительные строки в конец ACL-списка. В режиме глобальной конфигурации измените ACL-список с именем BRANCH-OFFICE-POLICY.

```
R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31
R1(config-std-nacl)# 40 deny any
R1(config-std-nacl)# end
```

Проверьте ACL-список.

1) На R1 выполните команду show access-lists.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
    30 permit 209.165.200.224, wildcard bits 0.0.0.31
    40 deny   any
```

Нужно ли вам применить список под именем BRANCH-OFFICE-POLICY на интерфейсе G0/1 маршрутизатора R1?

2) Из командной строки ISP выполните расширенный эхо-запрос. Проверьте, пропускает ли список ACL трафик из сети 209.165.200.224/27 в сеть 192.168.10.0/24. Вам нужно выполнить расширенный эхо-запрос и использовать 1оорЬаск-адрес 0 на ISP в качестве источника. Отправьте

эхо-запрос на IP-адрес компьютера PC-A. Успешно ли выполнен эхо-запрос?

Вопросы на закрепление

1. Как вы видите, стандартные ACL-списки достаточно эффективны и полезны. Почему вам может понадобиться использовать расширенные списки ACL?

2. В большинстве случаев при использовании именованного ACL-списка требуется введение большего количества строк, нежели при использовании нумерованного ACL-списка. Почему вы бы предпочли использовать именованный ACL-список, а не нумерованный?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Практическая работа 11. Настройка расширенных ACL-списков. Сценарий 1

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	172.22.34.65	255.255.255.224	N/A
	G0/1	172.22.34.97	255.255.255.240	N/A
	G0/2	172.22.34.1	255.255.255.192	N/A
Server	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

Задачи

Часть 1. Настройка, применение и проверка расширенного нумерованного ACL-списка Часть 2. Настройка, применение и проверка расширенного именованного ACL-списка

Исходные данные/сценарий

Двум работникам предприятия требуется доступ к службам, предоставляемым сервером. Узлу PC1 требуется доступ только к FTP, в то время как PC2 нужен доступ только к веб-сети. Оба компьютера могут отправлять эхо-запросы серверу, но не друг другу.

Часть 1. Настройка, применение и проверка расширенного нумерованного ACL-списка

Шаг 1: Настройте ACL-список на разрешение FTP и ICMP.

a. В режиме глобальной конфигурации на маршрутизаторе R1 введите следующую команду, чтобы определить первый допустимый номер для расширенного списка доступа.

```
R1(config)# access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
```

b. Добавьте 100 к команде, а затем поставьте вопросительный знак.

```
R1(config)# access-list 100 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
  remark  Access list entry comment
```

c. Чтобы разрешить трафик FTP, введите permit, после которого поставьте вопросительный знак.

```
R1(config)# access-list 100 permit ?
  ahp    Authentication Header Protocol
  eigrp  Cisco's EIGRP routing protocol
  esp    Encapsulation Security Payload
  gre    Cisco's GRE tunneling
  icmp   Internet Control Message Protocol
  ip     Any Internet Protocol
  ospf   OSPF routing protocol
  tcp    Transmission Control Protocol
  udp    User Datagram Protocol
```

d. Данный ACL-список разрешает FTP и ICMP. ICMP включён в список, указанный выше, в отличие от FTP, который использует протокол TCP. Таким образом, необходимо ввести TCP. Введите tcp, чтобы обновить ACL-список.

```
R1(config)# access-list 100 permit tcp ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
```

e. Обратите внимание, что мы могли бы настроить фильтрацию только для PC1, используя ключевое слово host, а также могли бы разрешить доступ для любого узла. В этом случае доступ разрешён любому устройству с адресом, принадлежащим сети 172.22.34.64/27. Введите сетевой адрес со знаком вопроса в конце.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 ?
  A.B.C.D  Source wildcard bits
```

f. Рассчитайте шаблонную маску, определяющую двоичную противоположность маски подсети.

```
11111111.11111111.11111111.11170000 - 255.255.255.224
0.0.0.255.0.0.0.255.0.0.0.255.0.011111 - 0.0.0.31
```

g. Введите шаблонную маску со знаком вопроса в конце.

```
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?
```

h. Настройте адрес узла-назначения. В этом сценарии мы

A.B.C.D	Destination address	
any	Any destination host	
eq	Match only packets on a given port number	
gt	Match only packets with a	greater port number
host	A single destination host	
lt	Match only packets with a	lower port number
neq	Match only packets not on	a given port number
range	Match only packets in the	range of port numbers

фильтруем трафик в пользу только одного адресата — сервера. Введите ключевое слово host, за которым следует IP-адрес сервера.

```
R1(config)# access-list 100 permit icmp 172.22.34.64 0.0.0.31 host
172.22.34.62
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ?
  <0-65535>  Port number
  ftp        File Transfer Protocol (21)
  pop3       Post Office Protocol v3 (110)
  smtp       Simple Mail Transport Protocol (25)
  telnet     Telnet (23)
  www        World Wide Web (HTTP, 80)
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 eq ftp
R1(config)# access-list 100 permit tcp 172.22.34.64 0.0.0.31 host
172.22.34.62 ?
  ack          Match packets with given ack or rst
  eq           Match only packets on a given port number
  established  established
  gt           Match only packets with a greater port number
  lt           Match only packets with a lower port number
  neq          Match only packets not on a given port number
  precedence   Match packets with given precedence value
  range        Match only packets in the range of port numbers
  <cr>
```

i. Обратите внимание на параметр <cr> (возврат каретки). Другими словами, вы можете нажать клавишу ВВОД, и согласно правилу будет разрешён весь трафик TCP. Однако мы хотим разрешить только трафик FTP. Поэтому введите ключевое слово eq, после которого поставьте вопросительный знак, чтобы отобразить доступные параметры. Затем введите ftp и нажмите ВВОД.

j. Создайте второе правило списка доступа, разрешающее передачу трафика ICMP (эхо-запрос и др.) от PC1 на сервер. Обратите внимание на то, что номер списка доступа остается неизменным, конкретный тип трафика ICMP не требует определения.

k. Остальной трафик запрещён по умолчанию.

Шаг 2: Примените ACL-список на соответствующем интерфейсе для фильтрации трафика.

С точки зрения маршрутизатора R1, трафик, к которому применяется список ACL 100, является

входящим из сети, подключённой к интерфейсу Gigabit Ethernet 0/0. Войдите в режим настройки

интерфейса и примените ACL-список.

```
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip access-group 100 in
```

Шаг 3: Проверьте работу ACL-списка.

a. Отправьте эхо-запрос от узла PC1 на сервер. В случае неудачных эхо-запросов проверьте IP- адреса перед тем, как продолжить работу.

b. Отправьте FTP-трафик от узла PC1 на сервер. Имя пользователя и пароль — cisco.

```
PC> ftp 172.22.34.62
```

c. Выйдите из службы FTP на сервере.

```
ftp> quit
```

d. Отправьте эхо-запрос от узла PC1 на PC2. Узел назначения должен быть недоступен, поскольку отсутствует разрешение на трафик в явном виде.

Часть 2. Настройка, применение и проверка расширенного именованного ACL-списка

Шаг 1: Настройте ACL-список на разрешение HTTP-доступа и ICMP.

a. Именованные ACL-списки начинаются с ключевого слова ip. В режиме глобальной конфигурации маршрутизатора R1 введите следующую команду, после которой поставьте вопросительный знак.

```
R1(config)# ip access-list ?
  extended  Extended Access List
  standard  Standard Access List
```

b. Можно настроить именованные стандартные и расширенные ACL-списки. Посредством этого списка доступа фильтруются как IP-адреса источника, так и IP-адреса узла-назначения; таким образом, список должен быть расширенным. Введите HTTP_ONLY в качестве имени. (для оценки работы в Packet Tracer должно задаваться имя, чувствительное к регистру).

```
R1(config)# ip access-list extended HTTP_ONLY
```

c. Командная строка изменится. Теперь активирован режим настройки именованного расширенного ACL-списка. Всем устройствам в локальной сети узла PC2 требуется доступ TCP. Введите сетевой адрес со знаком вопроса в конце.

```
R1(config-ext-nacl)# permit tcp 172.22.24.96 ?
  A.B.C.D  Source wildcard bits
```

d. Другой способ расчёта маски заключается в вычитании маски подсети из 255.255.255.255.

```
  255.255.255.255
- 255.255.255.240
-----------------
=   0.   0.   0. 15
```

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 ?
```

Допишите правило, определив адрес сервера как в части 1, и настроив фильтрацию трафика www.

```
R1(config-ext-nacl)# permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www
```

e. Создайте второе правило списка доступа, разрешающее передачу трафика ICMP (эхо-запрос и др.) от PC2 на сервер. Примечание. Командная строка не меняется, отсутствует необходимость задавать конкретный тип трафика ICMP.

```
R1(config-ext-nacl)# permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62
```

f. Остальной трафик запрещён по умолчанию. Выйдите из режима настройки именованного расширенного ACL-списка.

Шаг 2: Примените ACL-список на соответствующем интерфейсе для фильтрации трафика.

С точки зрения маршрутизатора R1, трафик, к которому применяется ACL-список HTTP_ONLY,

является входящим из сети, подключённой к интерфейсу Gigabit Ethernet 0/1. Войдите в режим

настройки интерфейса и примените ACL-список.

```
R1(config)# interface gigabitEthernet 0/1
R1(config-if)# ip access-group HTTP_ONLY in
```

Шаг 3: Проверьте работу ACL-списка.

a. Отправьте эхо-запрос от узла PC2 на сервер. В случае неудачных эхо-запросов проверьте IP- адреса перед тем, как продолжить работу.

b. Отправьте FTP-трафик от PC2 на сервер. Подключение не должно установиться.

c. Откройте веб-браузер на узле PC2 и введите IP-адрес сервера в виде URL. Подключение должно быть успешным.

Практическая работа 12. Поиск и устранение неполадок в настройке и размещении ACL-списков

Топология

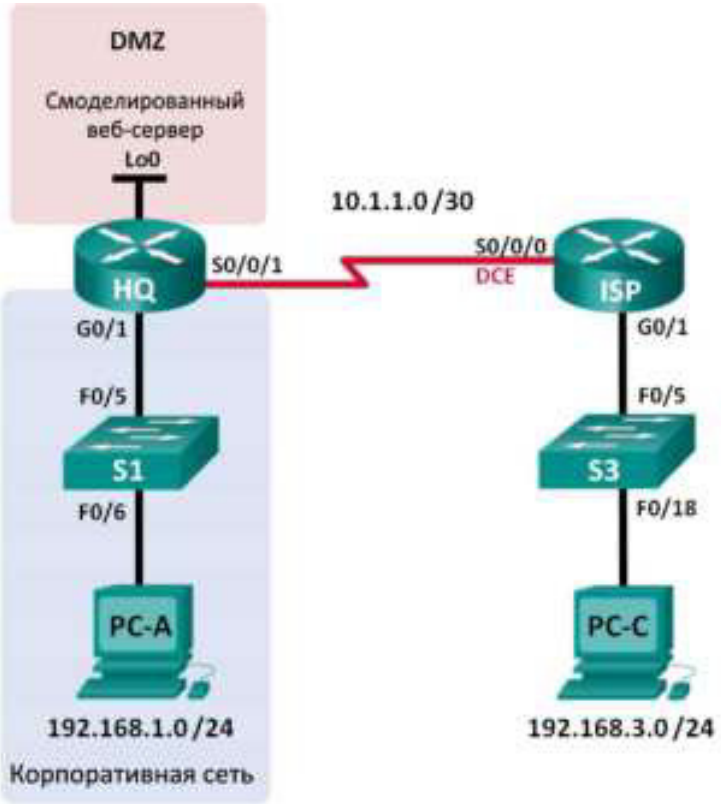


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
HQ	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	10.1.1.2	255.255.255.252	N/A
	Lo0	192.168.4.1	255.255.255.0	N/A
ISP	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.3.11	255.255.255.0	192.168.3.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Задачи

Часть 1. Построение сети и настройка базовых параметров устройства Часть 2. Поиск и устранение неполадок внутреннего доступа Часть 3. Поиск и устранение неполадок удалённого доступа

Исходные данные/сценарий

Список контроля доступа (ACL) — это последовательность команд IOS, обеспечивающая базовую фильтрацию трафика на маршрутизаторе

Cisco. С помощью ACL-списков можно выбирать типы трафика, подлежащие обработке. Каждое отдельное выражение ACL-списка называют записью контроля доступа (ACE). Записи ACE в ACL-списках оцениваются сверху вниз. В конце списка стоит скрытая запись запрета deny all. Также ACL-списки контролируют тип трафика, входящего или исходящего из сети, используя узлы или сеть источника и назначения. Размещение ACL-списков имеет решающее значение для правильной обработки нужного трафика.

В контексте данной лабораторной работы небольшая компания только что добавила в сеть веб-сервер, чтобы клиенты могли получить доступ к конфиденциальной информации. Корпоративная сеть разделена на две зоны: зону корпоративной сети и демилитаризованную зону (DMZ). В зоне корпоративной сети будут размещены частные серверы и внутренние клиенты. В зоне DMZ содержится внешне доступный веб-сервер (смоделированный как интерфейс Lo0 в HQ). Поскольку компания может управлять только собственным маршрутизатором HQ, на нём необходимо применить все ACL-списки.

- ACL-список 101 реализован для ограничения трафика, выходящего из зоны корпоративной сети. Эта зона содержит частные сервера и внутренних клиентов (192.168.1.0/24). Доступ других сетей в корпоративную сеть должен быть закрыт.
- ACL-список 102 применяется для ограничения трафика, входящего в корпоративную сеть. Доступ в эту сеть разрешён только для ответов на запросы, созданные внутри корпоративной сети. К ним относятся TCP-запросы от внутренних узлов, например, на веб- или FTP-сервере. ICMP обладает доступом в сеть для устранения неполадок, чтобы входящие ICMP-сообщения, созданные в ответ на эхо-запросы, могли быть получены внутренними узлами.
- ACL-список 121 контролирует внешний трафик, входящий в зону DMZ и корпоративную сеть. Доступом к веб-серверу DMZ обладает только HTTP-трафик (смоделированный как интерфейс Lo0 на маршрутизаторе R1). Остальной трафик из внешних сетей, например EIGRP, разрешён. Кроме того, допустимым внутренним частным адресам, например, 192.168.1.0, loopback-адресам, например, 127.0.0.0 и групповым адресам доступ к корпоративной сети запрещён в целях предотвращения вредоносных атак со стороны внешних пользователей.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных

работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсе маршрутизатора в конце этой лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

• 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);

• 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);

• 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);

• консольные кабели для настройки устройств Cisco IOS через консольные порты;

• кабели Ethernet и последовательные кабели в соответствии с топологией.

•

Часть 1: Построение сети и настройка базовых параметров устройства

В первой части лабораторной работы вам нужно создать топологию сети и настроить некоторые базовые параметры на маршрутизаторах и коммутаторах, например пароли и IP-адреса. В качестве исходных настроек маршрутизаторов также даны предварительные настройки. Также вам предстоит настроить параметры IP для компьютеров в приведённой топологии.

Шаг 1: Подключите кабели в сети в соответствии с топологией. Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 4: Настройте базовые параметры каждого коммутатора (дополнительно).

a. Отключите поиск DNS.

b. Настройте имена узлов в соответствии с топологией.

c. Настройте IP-адрес и шлюз по умолчанию в таблице адресации.

d. Назначьте cisco в качестве паролей консоли и VTY.

e. Назначьте class в качестве пароля привилегированного режима EXEC.

f. Настройте logging synchronous, чтобы сообщения от консоли не могли прерывать ввод команд.

Шаг 5: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.

b. Настройте имена узлов в соответствии с топологией.

c. Назначьте cisco в качестве паролей консоли и VTY.

d. Назначьте class в качестве пароля привилегированного режима EXEC.

e. Настройте logging synchronous, чтобы сообщения от консоли не могли прерывать ввод команд.

Шаг 6: Настройте HTTP-доступ и учётные данные пользователя на маршрутизаторе HQ.

Для получения доступа к смоделированному веб-серверу (192.168.4.1) необходимо настроить учётные данные пользователя.

```
hostname ISP
interface GigabitEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 no shutdown
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 128000
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.3.0
 no auto-summary
end
hostname HQ
interface Loopback0
 ip address 192.168.4.1 255.255.255.0
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip access-group 101 out
 ip access-group 102 in
 no shutdown
interface Serial0/0/1
 ip address 10.1.1.2 255.255.255.252
HQ(config)# ip http server
HQ(config)# username admin privilege 15 secret adminpass
HQ(config)# ip http authentication local
```

Шаг 7: Загрузите настройки маршрутизатора.

В вашем распоряжении конфигурации для маршрутизаторов ISP и HQ. Эти настройки содержат ошибки. Ваша задача — найти ошибки и исправить их.

Часть 2: Поиск и устранение неполадок внутреннего доступа

Во второй части нужно проверить ACL-списки на маршрутизаторе HQ, чтобы убедиться в правильности их настройки.

Шаг 1: Поиск и устранение неполадок в ACL-списке 101

ACL-список 101 реализован для ограничения трафика, выходящего из зоны корпоративной сети. В этой зоне содержатся только внутренние клиенты и частные сервера. Правом выхода из этой зоны корпоративной сети обладает только сеть 192.168.1.0/24.

a. Успешно ли проходит эхо-запрос от узла PC-A на его шлюз по умолчанию?

b. Убедившись в правильности настройки узла PC-A, просмотрите сводку ACL-списка 101, чтобы найти в конфигурации

маршрутизатора HQ возможные ошибки. Введите команду show access-lists 101.

```
HQ# show access-lists 101
Extended IP access list 101
    10 permit ip 192.168.11.0 0.0.0.255 any
    20 deny ip any any
```

c. Удалось ли вам найти какие-либо ошибки в ACL-списке 101?

d. Проверьте интерфейс шлюза по умолчанию для сети 192.168.1.0 /24. Убедитесь, что ACL-список 101 применён на правильном направлении интерфейса G0/1. Введите show ip interface g0/1.

```
HQ# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is [illegible] /24
  Broadcast address is 255.255.255.255
    Address determined by setup command
    MTU is 1500 bytes
    Helper address is not set
    Directed broadcast forwarding is disabled
    Multicast reserved groups joined: 224.0.0.10
    Outgoing access list is 101
    Inbound  access list is 102
```

Правильно ли настроено направление интерфейса G0/1 для ACL-списка 101?

e. Исправьте ошибки, найденные в ACL-списке 101, и убедитесь, что трафик из сети 192.168.1.0 /24 может покидать корпоративную сеть. Запишите команды, используемые для исправления ошибок.

f. Проверьте, успешно ли выполняется эхо-запрос с узла PC-A на интерфейс его шлюза по умолчанию.

Шаг 2: Поиск и устранение неполадок в ACL-списке 102

ACL-список 102 применяется для ограничения трафика, входящего в корпоративную сеть. Трафик, создаваемый во внешней сети, не допускается в корпоративную сеть. Удалённый трафик допускается в корпоративную сеть, если трафик был создан во внутренней сети. Ответные ICMP-сообщения допускаются в целях устранения неполадок.

a. Успешно ли выполняется эхо-запрос от узла PC-A на узел PC-C?

b. Просмотрите сводку ACL-списка 102, чтобы найти возможные ошибки в конфигурации маршрутизатора HQ. Введите команду show access-lists 102.

```
HQ# show access-lists 102
Extended IP access list 102
    10 permit tcp any any established
    20 permit icmp any any echo-reply
    30 permit icmp any any unreachable
    40 deny ip any any (57 matches)
```

c. Удалось ли вам найти какие-либо ошибки в ACL-списке 102?

d. Убедитесь, что ACL-список 102 применён на правильном направлении интерфейса G0/1. Введите show ip interface g0/1.

```
HQ# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.10
Outgoing access list is 101
Inbound  access list is 101
```

e. Удалось ли вам найти какие-либо ошибки в применении ACL-списка 102 на интерфейсе G0/1?

f. Устраните все ошибки в ACL-списке 102. Запишите команды, используемые для исправления ошибок.

g. Успешно ли теперь отправляется эхо-запрос от узла PC-A на узел PC-C?

Часть 3: Поиск и устранение неполадок удалённого доступа

В третьей части лабораторной работы ACL-список 121 настроен для предотвращения спуфинг-атак со стороны внешних сетей и разрешения только удалённого HTTP-доступа к веб-серверу (192.168.4.1) в зоне DMZ.

a. Проверьте настройки ACL-списка 121. Введите show ip access-list 121.

```
HQ# show ip access-lists 121
Extended IP access list 121
    10 permit tcp any host 192.168.4.1 eq 89
    20 deny icmp any host 192.168.4.11
    30 deny ip 192.168.1.0 0.0.0.255 any
    40 deny ip 127.0.0.0 0.255.255.255 any
    50 deny ip 224.0.0.0 31.255.255.255 any
    60 permit ip any any (354 matches)
    70 deny ip any any
```

Удалось ли вам найти какие-либо ошибки в этом ACL-списке?

b. Убедитесь, что ACL-список 121 применён на правильном направлении интерфейса S0/0/1 на маршрутизаторе R1. Введите команду show ip interface s0/0/1.

```
HQ# show ip interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet address is 10.1.1.2/30
  Broadcast address is 255.255.255.255
<output omitted>
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is 121
```

Удалось ли вам найти какие-либо ошибки в применении этого ACL-списка?

c. При обнаружении ошибок внесите соответствующие изменения в конфигурацию ACL 121 и задокументируйте их.

d. Убедитесь, что через веб-браузер узел PC-C может получить доступ только к смоделированному веб-серверу на маршрутизаторе HQ. Для доступа к веб-серверу (192.168.4.1) используйте имя пользователя admin и пароль adminpass.

Вопросы на закрепление

1. В каком порядке следует указывать ACL-операторы? От общего к частному или наоборот?

2. Что произойдёт, если вы удалите ACL-список с помощью команды no access-list, а этот список будет по-прежнему применён на интерфейсе?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Практическая работа 13. Базовая настройка DHCPv4 на марш рутизаторе

Топология

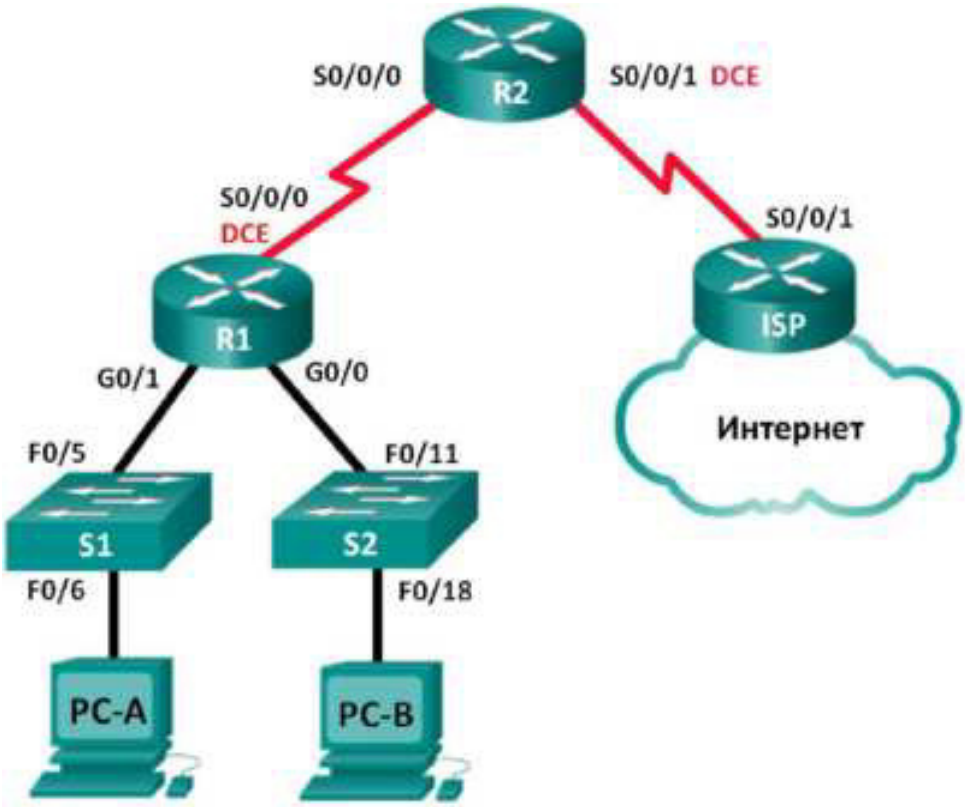


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.2.253	255.255.255.252	N/A
R2	S0/0/0	192.168.2.254	255.255.255.252	N/A
	S0/0/1 (DCE)	209.165.200.226	255.255.255.224	N/A
ISP	S0/0/1	209.165.200.225	255.255.255.224	N/A
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

Задачи

Часть 1. Построение сети и настройка базовых параметров устройства Часть 2. Выполнение настройки DHCPv4-сервера и агента-ретранслятора DHCP

Исходные данные/сценарий

Протокол динамической конфигурации сетевого узла (DHCP) — сетевой протокол, позволяющий сетевым администраторам управлять и

автоматизировать назначение IP-адресов. Без использования DHCP администратору необходимо вручную назначать и настраивать IP-адреса, предпочтительные DNS-серверы и шлюзы по умолчанию. По мере увеличения сети и перемещении устройств из одной внутренней сети в другую это становится административной проблемой.

В предложенном сценарии размеры компании увеличились, и сетевые администраторы больше не имеют возможности назначать IP-адреса для устройств вручную. Ваша задача заключается в настройке маршрутизатора R2 для назначения ^4-адресов в двух разных подсетях, подключённых к маршрутизатору R1.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимых для настройки DHCP. Список требуемых команд приведён в приложении А. Проверьте свои знания — настройте устройства, не обращаясь к информации, приведённой в приложении.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и настройка базовых параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить основные параметры на маршрутизаторах и

коммутаторах, такие как пароли и IP-адреса. Также вам предстоит настроить параметры IP для компьютеров в приведённой топологии.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 3: Настройте базовые параметры каждого маршрутизатора.

a. Отключите DNS-поиск.

b. Настройте имя устройства в соответствии с топологией.

c. Назначьте class в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

d. Назначьте cisco в качестве паролей консоли и VTY.

e. Настройте logging synchronous, чтобы сообщения от консоли не могли прерывать ввод команд.

f. Назначьте IP-адреса всем интерфейсам маршрутизатора в соответствии с таблицей адресации.

g. Настройте последовательный интерфейс DCE на маршрутизаторах R1 и R2 с тактовой частотой 128000.

h. Сконфигурируйте EIGRP для R1.

```
R2(config)# ip route 192.168.0.0 255.255.252.0 209.165.200.226
R2(config)# router eigrp 1
R2(config-router)# network 192.168.2.252 0.0.0.3
R2(config-router)# redistribute static
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
R1(config)# router eigrp 1
R1(config-router)# network 192.168.0.0 0.0.0.255
R1(config-router)# network 192.168.1.0 0.0.0.255
R1(config-router)# network 192.168.2.252 0.0.0.3
R1(config-router)# no auto-summary
```

i. Настройте EIGRP и маршрут по умолчанию для интернет-провайдера на маршрутизаторе R2.

j. Настройте суммарный статический маршрут на ISP для доступа к сетям маршрутизаторов R1 и R2.

k. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 4: Выполните проверку сетевого соединения между маршрутизаторами.

При неудачных эхо-запросах между маршрутизаторами прежде чем переходить к следующему шагу исправьте возникшие ошибки. Используйте команды show ip route и show ip interface brief, чтобы определить возможные неполадки.

Шаг 5: Убедитесь, что ПК на узлах настроены для работы DHCP.

Часть 2: Настройка DHCPv4-сервера и агента-ретранслятора DHCP

Для того чтобы автоматически назначить адресную информацию в сети, вам необходимо настроить маршрутизатор R2 в качестве сервера DHCPv4, а маршрутизатор R1 в качестве агента- ретранслятора.

Шаг 1: Выполните настройку сервера DHCPv4 на маршрутизаторе R2.

На маршрутизаторе R2 необходимо создать пул DHCP-адресов для каждой локальной сети маршрутизатора R1. Используйте имя пула R1G0 для интерфейса G0/0 LAN и R1G1 для интерфейса G0/1 LAN. Также вам нужно исключить адреса, которые не будут назначаться из пула адресов. Исключать адреса рекомендуется в первую очередь, чтобы предотвратить их случайную аренду для других устройств.

Исключите первые девять адресов из каждой локальной сети маршрутизатора R1, начиная с .1. Все другие адреса должны быть доступны в пуле DHCP. Убедитесь, что каждый пул DHCP содержит шлюз по умолчанию, домен ccna-lab.com, сервер DNS (209.165.200.225), а срок аренды составляет два дня.

В строках ниже запишите команды, необходимые для настройки служб DHCP на маршрутизаторе R2, включая те, что требуются для исключения DHCP-адресов и создания пулов DHCP.

Примечание. Команды, необходимые для выполнения заданий второй части лабораторной работы, приведены в приложении А. Для того чтобы проверить свои знания, попробуйте настроить DHCP на маршрутизаторах R1 и R2, не обращаясь к приложению.

На узлах PC-A или PC-B откройте командную строку и введите команду ipconfig /all. Получил ли какой-либо из узловых ПК IP-адрес от сервера DHCP? Почему?

Шаг 2: Настройте маршрутизатор R1 в качестве агента ретрансляции.

Настройте вспомогательные IP-адреса на маршрутизаторе R1, чтобы переслать все DHCP-запросы на сервер DHCP маршрутизатора R2.

В строках ниже запишите команды, необходимые для настройки маршрутизатора R1 в качестве агента DHCP-ретрансляции для локальных сетей маршрутизатора R1.

Шаг 3: Запишите IP-параметры для компьютеров PC-A и PC-B.

На компьютерах PC-A и PC-B выполните команду ipconfig /all, чтобы убедиться, что компьютеры получили информацию об IP-адресах от DHCP-сервера маршрутизатора R2. Запишите IP- и MAC- адреса для каждого ПК.

Исходя из пула DHCP, настроенного на маршрутизаторе R2, какие первые доступные IP-адреса могут быть арендованы компьютерами PC-A и PC-B?

Шаг 4: Проверьте работу служб DHCP и аренды адресов на маршрутизаторе R2.

a. На маршрутизаторе R2 выполните команду show ip dhcp binding, чтобы просмотреть список арендованных DHCP адресов.

Какая другая полезная информация для идентификации пользователя содержится в выходных данных, помимо арендованных IP-адресов?

b. На маршрутизаторе R2 выполните команду show ip dhcp show statistics, чтобы отобразить статистику пула DHCP и активность сообщений.

Сколько типов сообщений DHCP представлено в выходных данных?

c. На маршрутизаторе R2 выполните команду show ip dhcp pool, чтобы просмотреть настройки пула DHCP.

К чему относится показатель Current в выходных данных команды show ip dhcp pool?

d. На маршрутизаторе R2 выполните команду show run | section dhcp, чтобы просмотреть конфигурацию DHCP в текущей конфигурации.

e. На маршрутизаторе R2 выполните команду show run interface для интерфейсов G0/0 и G0/1, чтобы просмотреть настройки ретранслятора DHCP в текущей конфигурации.

Вопросы на закрепление

Как вы думаете, в чём заключается преимущество использования агентов DHCP-ретрансляции вместо использования нескольких маршрутизаторов, работающих в качестве серверов DHCP?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Приложение А. Команды настройки DHCP

Маршрутизатор R1

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.2.254
R1(config-if)# exit
R1(config-if)# interface g0/1
R1(config-if)# ip helper-address 192.168.2.254
```

Маршрутизатор R2

```
R2(config)# ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)# ip dhcp pool R1G1
R2(dhcp-config)# network 192.168.1.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.1.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
R2(dhcp-config)# exit
R2(config)# ip dhcp pool R1G0
R2(dhcp-config)# network 192.168.0.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.0.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
```

Практическая работа 14. Базовая настройка DHCPv4 на коммутаторе

Топология

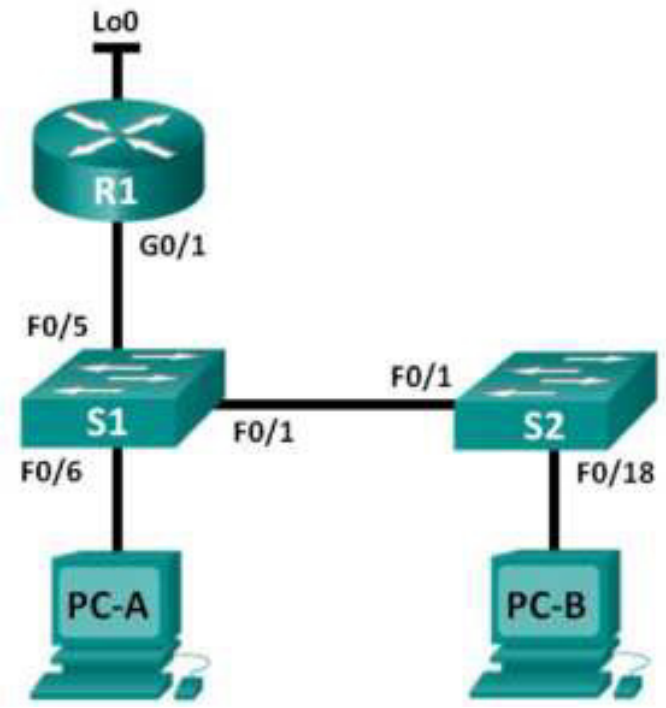


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
R1	G0/1	192.168.1.10	255.255.255.0
	Lo0	209.165.200.225	255.255.255.224
S1	VLAN 1	192.168.1.1	255.255.255.0
	VLAN 2	192.168.2.1	255.255.255.0

Задачи

Часть 1. Построение сети и настройка базовых параметров устройства Часть 2. Изменение параметров SDM

- Настройка на маршрутизаторе S1 параметра SDM на lanbase-routing. Часть 3. Настройка DHCPv4
- Настройка DHCPv4 для сети VLAN 1.
- Проверка DHCPv4 и соединения.Часть 4. Настройка DHCP для нескольких VLAN
- Назначение портов сети VLAN 2.
- Настройка DHCPv4 для сети VLAN 2.
- Проверка DHCPv4 и соединения. Часть 5. Активация IP-маршрутизации
- Активируйте на коммутаторе IP-маршрутизацию.
- Создание статических маршрутов.

Исходные данные/Сценарий

Коммутатор Cisco 2960 может работать в качестве сервера DHCPv4. Сервер Cisco DHCPv4 назначает и управляет ^4-адресами из указанных пулов адресов, связанных с конкретными сетями VLAN и виртуальными интерфейсами коммутатора. Коммутатор Catalyst 2960 может функционировать в качестве устройства 3-го уровня и маршрутизировать данные между сетями VLAN и ограниченным количеством статических маршрутов. В данной лабораторной работе вам предстоит настроить DHCPv4 на коммутаторе Cisco 2960 как для одной, так и для нескольких сетей VLAN, активировать маршрутизацию на коммутаторе для обеспечения связи между сетями VLAN, а также добавить статические маршруты для обеспечения связи между всеми узлами.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимых для настройки DHCP. Список требуемых команд приведён в приложении А. Проверьте свои знания — настройте устройства, не обращаясь к информации, приведённой в приложении.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с универсальным образом M3 под управлением ОС Cisco IOS 15.2(4) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Построение сети и настройка базовых параметров устройства

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 3: Настройте основные параметры устройств.

a. Присвойте устройствам имена в соответствии с топологией.

b. Отключите поиск DNS.

c. Установите class в качестве пароля привилегированного режима. В качестве паролей консоли и виртуального терминала vty установите cisco.

d. Назначьте IP-адреса интерфейсам G0/1 и Lo0 маршрутизатора R1 в соответствии с таблицей адресации.

e. Назначьте IP-адреса интерфейсам VLAN 1 и VLAN 2 коммутатора S1 в соответствии с таблицей адресации.

f. Сохраните файл текущей конфигурации в файл загрузочной конфигурации.

Часть 2: Изменение параметра SDM

Диспетчер базы данных коммутатора Cisco (Switch Database Manager, SDM) содержит несколько шаблонов для коммутатора 2960. Шаблоны можно применять для выполнения определённых функций в зависимости от того, как коммутатор используется в сети. В данной лабораторной работе используется шаблон SDM lanbase-routing, чтобы разрешить коммутатору маршрутизировать данные между сетями VLAN, а также разрешить поддержку статической маршрутизации.

Шаг 1: Отобразите параметр SDM на коммутаторе S1.

На коммутаторе S1 выполните команду show sdm prefer в привилегированном режиме. Если шаблон не был изменен, то используются заводские настройки, шаблон default. Шаблон default не поддерживает статическую маршрутизацию. При включённой IPv6-адресации шаблоном по умолчанию будет dual-ipv4-and-ipv6.

```
S1# show sdm prefer
The current template is "default" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.

  number of unicast mac addresses:                  8K
  number of IPv4 IGMP groups:                       0.25K
  number of IPv4/MAC qos aces:                      0.125K
  number of IPv4/MAC security aces:                 0.375K
```

Какой шаблон активирован на данный момент?Шаг 2: Измените параметр SDM на коммутаторе S1.

a. Настройте параметр SDM на lanbase-routing. (Если lanbase-routing является текущим шаблоном, перейдите к части 3). В режиме глобальной конфигурации выполните команду sdm prefer lanbase- routing.

```
S1(config)# sdm prefer lanbase-routing
Changes to the running SDM preferences have been stored, but cannot take effect
until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
```

Какой шаблон будет активен после перезагрузки?

b. Для активации шаблона коммутатор нужно перезагрузить.

```
S# reload

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]
```

Примечание. Новый шаблон будет использоваться после перезагрузки, даже если текущая конфигурация не была сохранена. Для того чтобы сохранить текущую конфигурацию после внесения изменений в систему, выберите yes.

Шаг 3: Убедитесь, что шаблон lanbase-routing загружен.

Для проверки, загружен ли на маршрутизаторе S1 шаблон lanbase-routing, выполните команду show sdm prefer.

```
S1# show sdm prefer
The current template is "lanbase-routing" template.
The selected template optimizes the resources in
the system to support this mix of features for
IP routed interfaces and the VTP.

  number of unicast mac addresses:                  6K
  number of IPv4 IGMP groups + multicast routes:    0.25K
  number of IPv4 unicast routes:                    0.75K
    number of directly connected IPv4 hosts:        0.75K
    number of indirect IPv4 routes:                 16
  number of IPv4 multicast groups:                  0.375K
  number of directly connected IPv6 addresses:      0.75K
    number of indirect IPv6 unicast routes:         16
  number of IPv6 multicast group address:           9
  number of IPv4/MAC qos aces:                      0.125K
  number of IPv4/MAC security aces:                 0.375K
  number of IPv6 policy based routing aces:         0
  number of IPv6 qos aces:                          0.375K
  number of IPv6 security aces:                     127
```

Часть 3: Настройка DHCPv4

В части 3 вам предстоит настроить DHCPv4 для VLAN 1, проверить настройки IP на узловых компьютерах, чтобы подтвердить успешную работу DHCP, а также проверить наличие подключения у всех устройств в сети VLAN 1.

Шаг 1: Настройте DHCP для сети VLAN 1.

a. Исключите первые десять допустимых адресов узлов из сети 192.168.1.0/24. Ниже напишите команду, которую вы использовали.

b. Создайте пул DHCP с именем DHCP1. Ниже напишите команду, которую вы использовали.

c. Для доступных адресов назначьте сеть 192.168.1.0/24. Ниже напишите команду, которую вы использовали.

d. Укажите в качестве шлюза по умолчанию: 192.168.1.1. Ниже напишите команду, которую вы использовали.

e. Укажите в качестве адреса сервера DNS: 192.168.1.9. Ниже напишите команду, которую вы использовали.

f. Настройте срок аренды — три дня. Ниже напишите команду, которую вы использовали.

g. Сохраните файл текущей конфигурации в файл загрузочной конфигурации.

Шаг 2: Проверка DHCP и соединения.

a. На компьютерах PC-A и PC-B откройте командную строку и выполните команду ipconfig. Если IP- информация отсутствует или представлена не полностью, выполните команду ipconfig /release, а после неё команду ipconfig /renew.

Для PC-A перечислите следующие параметры IP:

IP-адрес:

Маска подсети:

Шлюз по умолчанию:

Для PC-B перечислите следующие параметры IP:

IP-адрес:

Маска подсети:

Шлюз по умолчанию:

b. Проверьте подключение, отправив эхо-запросы от компьютера PC-A на шлюз по умолчанию, компьютер PC-B и маршрутизатор R1.

Успешно ли проходит эхо-запрос от компьютера PC-A на шлюз по умолчанию сети VLAN? Успешно ли отправляется эхо-запрос от узла PC-A на PC-B?

Успешно ли проходит эхо-запрос от компьютера PC-A на интерфейс G0/1 маршрутизатора R1?

Если на какой-либо из этих вопросов вы ответили отрицательно, выявите и устраните неполадки в конфигурации.

Часть 4: Настройка DHCPv4 для нескольких сетей VLAN

В части 4 вам предстоит назначить порт PC-A в VLAN 2, настроить DHCPv4 для сети VLAN 2, обновить конфигурацию IP компьютера PC-A для проверки DHCPv4, а также проверить соединение в пределах сети VLAN.

Шаг 1: Назначьте порт сети VLAN 2.

Разместите порт F0/6 в сети VLAN 2. Ниже напишите команду, которую вы использовали.

Шаг 2: Настройте DHCPv4 для сети VLAN 2

a. Исключите первые десять допустимых адресов узлов из сети 192.168.2.0. Ниже напишите команду, которую вы использовали.

b. Создайте пул DHCP под названием DHCP2. Ниже напишите команду, которую вы использовали.

c. Для доступных адресов назначьте сеть 192.168.2.0/24. Ниже напишите команду, которую вы использовали.

d. Укажите в качестве шлюза по умолчанию: 192.168.2.1. Ниже напишите команду, которую вы использовали.

e. Укажите в качестве адреса сервера DNS: 192.168.2.9. Ниже напишите команду, которую вы использовали.

f. Настройте срок аренды — три дня. Ниже напишите команду, которую вы использовали.

g. Сохраните файл текущей конфигурации в файл загрузочной конфигурации.

Шаг 3: Проверьте DHCPv4 и соединение.

a. На компьютере PC-A откройте командную строку и выполните команду ipconfig /release, а затем команду ipconfig /renew.

Для PC-A перечислите следующие параметры IP:

IP-адрес:

Маска подсети:

Шлюз по умолчанию:

b. Проверьте соединение, отправив эхо-запросы от компьютера PC-A на шлюз по умолчанию сети VLAN 2 и компьютер PC-B.

Успешно ли проходит эхо-запрос с узла PC-A на шлюз по умолчанию? Успешно ли отправляется эхо-запрос от узла PC-A на PC-B?

Успешно ли выполнены эхо-запросы? Почему?

c. Выполните команду show ip route на коммутаторе S1. Что видно из результатов выполнения этой команды?

Часть 5: Активация IP-маршрутизации

В части 5 вам предстоит включить IP-маршрутизацию на коммутаторе, которая необходима для обмена данными между сетями VLAN. Для обеспечения связи между всеми сетями, на коммутаторе S1 и маршрутизаторе R1 необходимо реализовать статические маршруты.

Шаг 1: Включите IP-маршрутизацию на коммутаторе S1.

a. Для того чтобы активировать маршрутизацию на коммутаторе S1, используйте команду ip-routing в режиме глобальной конфигурации

```
S1(config)# ip routing
```

b. Проверьте наличие подключения между сетями VLAN. Успешно ли отправляется эхо-запрос от узла PC-A на PC-B? Какую функцию выполняет коммутатор?

c. Просмотрите информацию в таблице маршрутизации S1.

Какая информация о маршрутизации содержится в выходных данных этой команды?

d. Просмотрите информацию в таблице маршрутизации R1.

Какая информация о маршрутизации содержится в выходных данных этой команды?

e. Успешно ли проходит эхо-запрос от компьютера PC-A на маршрутизатор R1? Успешно ли отправляется эхо-запрос от узла PC-A на интерфейс Lo0?

Что требуется настроить для обеспечения передачи данных между всеми сетями, если принимать во внимание данные из таблицы маршрутизации этих двух устройств?

Шаг 2: Назначьте статические маршруты.

После включения IP-маршрутизации коммутатор сможет маршрутизировать данные между сетями VLAN, назначенных на коммутаторе. Для обеспечения связи между всеми сетями VLAN и маршрутизатором в таблицы маршрутизации коммутатора и маршрутизатора следует добавить статические маршруты.

a. На коммутаторе S1 создайте статический маршрут по умолчанию к маршрутизатору R1. Ниже напишите команду, которую вы использовали.

b. На маршрутизаторе R1 создайте статический маршрут до сети VLAN 2. Ниже напишите команду, которую вы использовали.

c. Просмотрите информацию в таблице маршрутизации S1.

Как в таблице представлен статический маршрут по умолчанию?

d. Просмотрите информацию в таблице маршрутизации R1. Как в таблице представлен статический маршрут?

e. Успешно ли проходит эхо-запрос от компьютера PC-A на маршрутизатор R1? Успешно ли отправляется эхо-запрос от узла PC-A на интерфейс Lo0?

Вопросы на закрепление

Почему при настройке DHCPv4 перед созданием пула DHCPv4 следует исключить статические маршруты?

Каким образом коммутатор назначает узлам IP-информацию при наличии нескольких пулов DHCPv4?

Какие функции может выполнять коммутатор Cisco 2960 помимо коммутации?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Приложение А. Команды настройки Настройка DHCPv4

```
S1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)# ip dhcp pool DHCP1
S1(dhcp-config)# network 192.168.1.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.1.1
S1(dhcp-config)# dns-server 192.168.1.9
S1(dhcp-config)# lease 3
```

Настройка DHCPv4 для нескольких сетей VLAN

```
S1(config)# interface f0/6
S1(config-if)# switchport access vlan 2
S1(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.10
S1(config)# ip dhcp pool DHCP2
S1(dhcp-config)# network 192.168.2.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.2.1
S1(dhcp-config)# dns-server 192.168.2.9
S1(dhcp-config)# lease 3
```

Активация IP-маршрутизации

```
S1(config)# ip routing
S1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.10
R1(config)# ip route 192.168.2.0 255.255.255.0 g0/1
```

Практическая работа 15. Поиск и устранение неполадок в работе DHCPv4

Топология

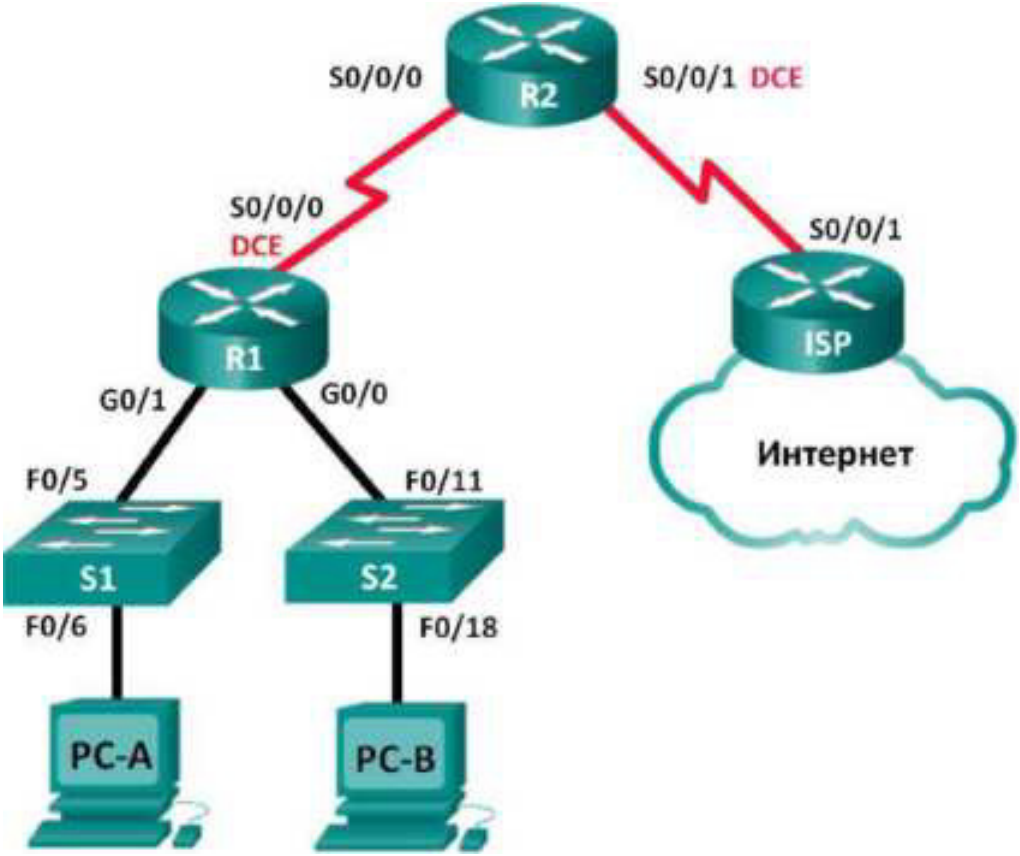


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	192.168.0.1	255.255.255.128	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.0.253	255.255.255.252	N/A
R2	S0/0/0	192.168.0.254	255.255.255.252	N/A
	S0/0/1 (DCE)	209.165.200.226	255.255.255.252	N/A
ISP	S0/0/1	209.165.200.225	255.255.255.252	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.0.2	255.255.255.128	192.168.0.1
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

Задачи

Часть 1. Построение сети и настройка базовых параметров устройства

Часть 2. Выполнение поиска и устранения неполадок в работе DHCPv4

Исходные данные/сценарий

Протокол динамической конфигурации сетевого узла (DHCP) — сетевой протокол, позволяющий сетевым администраторам управлять назначением и автоматизировать назначение IP-адресов. Без использования DHCP администратору приходится вручную назначать и настраивать IP-адреса, предпочтительные DNS-серверы и шлюз по умолчанию. По мере увеличения сети и перемещении устройств из одной внутренней сети в другую это становится административной проблемой.

В предложенном сценарии размеры компании увеличились, и сетевые администраторы больше не имеют возможности назначать IP-адреса для устройств вручную. Маршрутизатор R2 был настроен в качестве сервера DHCP для назначения IP-адресов узловым устройствам в локальных сетях маршрутизатора R1. В результате нескольких ошибок в настройках возникли проблемы со связью. Вас попросили выполнить поиск и устранение неполадок в конфигурации и написать отчёт о проделанной работе.

Убедитесь в том, что сеть соответствует следующим требованиям:

1) Маршрутизатор R2 должен функционировать в качестве сервера DHCP для сетей 192.168.0.0/25 и 192.168.1.0/24, подключённых к маршрутизатору R1.

2) Все ПК, подключённые к коммутаторам S1 и S2, должны получить IP-адрес в нужной сети с помощью DHCP.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9).

В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через

консольные порты;

• кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и настройка базовых параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить основные параметры на маршрутизаторах и коммутаторах, такие как пароли и IP-адреса. Также вам предстоит настроить параметры IP для компьютеров в приведённой топологии.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 3: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте class в качестве пароля привилегированного режима EXEC.

d. Назначьте cisco в качестве паролей консоли и VTY.

e. Настройте logging synchronous, чтобы сообщения от консоли не могли прерывать ввод команд.

f. Назначьте IP-адреса всем интерфейсам маршрутизатора.

g. Установите тактовую частоту на 128000 для всех интерфейсов маршрутизатора DCE.

h. Настройте EIGRP на маршрутизаторе R1.

```
R1(config)# router eigrp 1
R1(config-router)# network 192.168.0.0 0.0.0.127
R1(config-router)# network 192.168.0.252 0.0.0.3
R1(config-router)# network 192.168.1.0
R1(config-router)# no auto-summary
```

i. На маршрутизаторе R2 настройте EIGRP и статический маршрут по умолчанию.

```
R2(config)# router eigrp 1
R2(config-router)# network 192.168.0.252 0.0.0.3
```

```
R2(config-router)# redistribute static
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

j. Настройте суммарный статический маршрут на маршрутизаторе ISP к сетям на маршрутизаторах R1 и R2.

```
ISP(config)# ip route 192.168.0.0 255.255.254.0 209.165.200.226
```

Шаг 4: Выполните проверку сетевого соединения между маршрутизаторами.

При неудачных эхо-запросах между маршрутизаторами исправьте обнаруженные ошибки, прежде чем переходить к следующему шагу. Используйте команды show ip route и show ip interface brief, чтобы определить возможные неполадки.

Шаг 5: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте IP-адрес интерфейсу VLAN 1 и шлюз по умолчанию для каждого коммутатора.

d. Назначьте class в качестве пароля привилегированного режима EXEC.

e. Назначьте cisco в качестве паролей консоли и VTY.

f. Настройте logging synchronous для консольного канала.

Шаг 6: Убедитесь в том, что на узлах включена работа с DHCP.

Шаг 7: Загрузите начальную конфигурацию DHCP для маршрутизаторов R1 и R2. **Маршрутизатор R1**

```
interface GigabitEthernet0/1
 ip helper address 192.168.0.235
```

Маршрутизатор R2

```
ip dhcp excluded-address 192.168.11.1 192.168.11.9
 p dhc  ex  ded-address 192.168.0.1  192.168.0.9
 p dhc  poo  R1-P1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
ip dhcp pool R2-P0
 network 192.168.0.0 255.255.255.128
 default-router 192.168.11.1
```

Часть 2: Поиск и устранение неполадок в работе DHCPv4

После настройки маршрутизаторов R1 и R2 с параметрами DHCPv4 появилось несколько ошибок в настройке DHCP, которые привели к неполадкам в подключении. Маршрутизатор R2 настроен в качестве сервера DHCP. В обоих пулах адресов DHCP первые девять адресов зарезервированы для маршрутизаторов и коммутаторов. Маршрутизатор R1 ретранслирует информацию о DHCP во все локальные сети маршрутизатора R1. На данный момент компьютеры PC-A и PC-B не имеют доступа к сети. Используйте команды show и debug для выявления и исправления проблем с сетевым соединением.

Шаг 1: Запишите IP-параметры для компьютеров PC-A и PC-B.

a. В командной строке компьютеров PC-A и PC-B введите ipconfig /all для отображения IP- и MAC- адресов.

b. Запишите IP- и MAC-адреса в таблице ниже. MAC-адрес можно использовать для определения какой ПК упоминается в сообщении

об ошибке.

	IP-адрес/маска подсети	MAC-адрес
PC-A		
PC-B		

Шаг 2: Устраните неполадки в работе DHCP для сети 192.168.1.0/24 на маршрутизаторе R1.

Маршрутизатор R1 является агентом DHCP-ретрансляции для всех сетей LAN маршрутизатора R1. На данном этапе будет рассматриваться только процесс DHCP для сети 192.168.1.0/24. Первые девять адресов зарезервированы для других сетевых устройств, включающих маршрутизаторы, коммутаторы и серверы.

a. Для наблюдения за процессом DHCP на маршрутизаторе R2 используйте команду DHCP debug.

```
R2# debug ip dhcp server events
```

b. На маршрутизаторе R1 отобразите текущую конфигурацию интерфейса G0/1.

```
R1# show run interface g0/1
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 192.168.0.253
 duplex auto
 speed auto
```

При наличии каких-либо проблем с DHCP-ретрансляцией, запишите команды, которые понадобятся для исправления ошибок конфигурации.

c. В командной строке компьютера PC-A введите ipconfig /renew, чтобы получить адрес от сервера DHCP. Запишите полученный IP-адрес, маску подсети и шлюз по умолчанию для PC-A.

d.Проследите за процессом обновления информации для PC-A с

```
*Mar  5 06:32:16.939: DHCPD: Sending notification of DISCOVER:
*Mar  5 06:32:16.939:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:32:16.939:   DHCPD: circuit id 00000000
*Mar  5 06:32:16.939: DHCPD: Seeing if there is an internally specified pool class:
*Mar  5 06:32:16.939:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:32:16.939:   DHCPD: circuit id 00000000
*Mar  5 06:32:16.943: DHCPD: Allocated binding 2944C764
*Mar  5 06:32:16.943: DHCPD: Adding binding to radix tree (192.168.1.1)
*Mar  5 06:32:16.943: DHCPD: Adding binding to hash tree
*Mar  5 06:32:16.943: DHCPD: assigned IP address 192.168.1.1 to client
0100.5056.be76.8c.
*Mar  5 06:32:16.951: %DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged
192.168.1.1.
*Mar  5 06:32:16.951: DHCPD: returned 192.168.1.1 to address pool R1G1.
*Mar  5 06:32:16.951: DHCPD: Sending notification of DISCOVER:
*Mar  5 06:32:16.951:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:32:16.951:   DHCPD: circuit id 00000000
*Mar  5 06:32:1
[illegible]: DHCPD: Seeing if there is an internally specified pool class
[illegible]  DHCPD: htype [illegible] chaddr [illegible]
*Mar  5 06:32:16.951:   DHCPD: circuit id 00000000
*Mar  5 06:32:16.951: DHCPD: Allocated binding 31DC93C8
*Mar  5 06:32:16.951: DHCPD: Adding binding to radix tree (192.168.1.2)
*Mar  5 06:32:16.951: DHCPD: Adding binding to hash tree
*Mar  5 06:32:16.951: DHCPD: assigned IP address 192.168.1.2 to client
0100.5056.be76.8c.
*Mar  5 06:32:18.383: %DHCPD-4-PING_CONFLICT: DHCP address conflict:  server pinged
192.168.1.2.
*Mar  5 06:32:18.383: DHCPD: returned 192.168.1.2 to address pool R1G1.
*Mar  5 06:32:18.383: DHCPD: Sending notification of DISCOVER:
*Mar  5 06:32:18.383:   DHCPD: htype 1 chaddr 0050.56be.6c89
*Mar  5 06:32:18.383:   DHCPD: circuit id 00000000
*Mar  5 06:32:18.383: DHCPD: Seeing if there is an internally specified pool class:
*Mar  5 06:32:18.383:   DHCPD: htype 1 chaddr 0050.56be.6c89
*Mar  5 06:32:18.383:   DHCPD: circuit id 00000000
*Mar  5 06:32:18.383: DHCPD: Allocated binding 2A40E074
*Mar  5 06:32:18.383: DHCPD: Adding binding to radix tree (192.168.1.3)
*Mar  5 06:32:18.383: DHCPD: Adding binding to hash tree
*Mar  5 06:32:18.383: DHCPD: assigned IP address 192.168.1.3 to client
0100.5056.be76.8c.
<output omitted>
```

помощью отладочных сообщений на маршрутизаторе R2. Сервер DHCP пытался назначить компьютеру PC-A адрес 192.168.1.1/24. Данный адрес уже используется для интерфейса G0/1 маршрутизатора R1. Та же проблема возникла с IP-адресом 192.168.1.2/24, поскольку в начальной конфигурации адрес был назначен коммутатору S1. Поэтому компьютеру PC-A был назначен IP-адрес 192.168.1.3/24. Конфликт при назначении адреса DHCP указывает, что при настройке сервера DHCP на маршрутизаторе R2 определенные адреса могли быть не исключены из пула DHCP.

e.Отобразите конфигурацию сервера DHCP на маршрутизаторе R2.

Первые девять адресов для сети 192.168.1.0/24 не исключены из пула DHCP.

```
R2# show run | section dhcp
ip dhcp excluded-address 192.168.11.1 192.168.11.9
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp pool R1G1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
ip dhcp pool R1G0
 network 192.168.0.0 255.255.255.128
 default-router 192.168.0.1
```

Запишите команды для решения обнаруженной проблемы на маршрутизаторе R2.

f. В командной строке компьютера PC-A введите ipconfig /release, чтобы вернуть адрес 192.168.1.3 обратно в пул DHCP. За процессом можно проследить с помощью сообщений команды debug на маршрутизаторе R2.

```
*Mar  5 06:49:59.563: DHCPD: Sending notification of TERMINATION:
*Mar  5 06:49:59.563:  DHCPD: address 192.168.1.3 mask 255.255.255.0
*Mar  5 06:49:59.563:  DHCPD: reason flags: RELEASE
*Mar  5 06:49:59.563:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:49:59.563:   DHCPD: lease time remaining (secs) = 85340
*Mar  5 06:49:59.563: DHCPD: returned 192.168.1.3 to address pool R1G1.
```

g. В командной строке компьютера PC-A введите ipconfig /renew, чтобы компьютеру был назначен новый IP-адрес сервером DHCP. Запишите назначенные IP-адреса и данные шлюза по умолчанию.

За процессом можно проследить с помощью сообщений команды debug на маршрутизаторе R2.

```
*Mar  5 06:50:11.863: DHCPD: Sending notification of DISCOVER:
*Mar  5 06:50:11.863:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:50:11.863:   DHCPD: circuit id 00000000
*Mar  5 06:50:11.863: DHCPD: Seeing if there is an internally specified pool c
*Mar  5 06:50:11.863:   DHCPD: htype 1 chaddr 0050.56be.768c
*Mar  5 06:50:11.863:   DHCPD: circuit id 00000000
*Mar  5 06:50:11.863: DHCPD: requested address 192.168.1.3 has already been as
*Mar  5 06:50:11.863: DHCPD: Allocated binding 3003018C
*Mar  5 06:50:11.863: DHCPD: Adding binding to radix tree (192.168.1.10)
*Mar  5 06:50:11.863: DHCPD: Adding binding to hash tree
*Mar  5 06:50:11.863: DHCPD: assigned IP address 192.168.1.10 to client
0100.5056.be76.8c.
<output omitted>
```

h. Проверьте сетевое соединение.

Можно ли отправить эхо-запрос от компьютера PC-A на назначенный шлюз по умолчанию?

Можно ли отправить эхо-запрос от компьютера PC-A на маршрутизатор R2?

Можно ли отправить эхо-запрос от компьютера PC-A на маршрутизатор ISP?

Шаг 3: Выполните поиск и устранение неполадок в работе DHCP для сети 192.168.0.0/25 на маршрутизаторе R1.

Маршрутизатор R1 является агентом DHCP-ретрансляции для всех сетей LAN маршрутизатора R1. На этом этапе будет рассматриваться только процесс DHCP для сети 192.168.0.0/25. Первые девять адресов зарезервированы для других сетевых устройств.

a. Для наблюдения за процессом DHCP на маршрутизаторе R2 используйте команду DHCP debug.

```
R2# debug ip dhcp server events
```

b. Отобразите текущую конфигурацию интерфейса G0/0 маршрутизатора R1, чтобы определить возможные проблемы в работе DHCP.

```
R1# show run interface g0/0
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.128
 duplex auto
 speed auto
```

Запишите обнаруженные проблемы и все команды, которые понадобятся для исправления ошибок конфигурации.

c. В командной строке компьютера PC-B введите ipconfig /renew, чтобы получить адрес от сервера DHCP. Запишите полученный IP-адрес, маску подсети и шлюз по умолчанию для PC-B.

d. За процессом обновления для PC-A можно проследить с помощью сообщений команды debug на маршрутизаторе R2. Сервер DHCP назначил компьютеру PC-B адрес 192.168.0.10/25.

```
*Mar  5 07:15:09.663: DHCPD: Sending notification of DISCOVER:
*Mar  5 07:15:09.663:   DHCPD: htype 1 chaddr 0050.56be.f6db
*Mar  5 07:15:09.663:   DHCPD: circuit id 00000000
*Mar  5 07:15:09.663: DHCPD: Seeing if there is an internally specified pool
*Mar  5 07:15:09.663:   DHCPD: htype 1 chaddr 0050.56be.f6db
*Mar  5 07:15:09.663:   DHCPD: circuit id 00000000
*Mar  5 07:15:09.707: DHCPD: Sending notification of ASSIGNMENT:
*Mar  5 07:15:09.707:  DHCPD: address 192.168.0.10 mask 255.255.255.128
*Mar  5 07:15:09.707:   DHCPD: htype 1 chaddr 0050.56be.f6db
*Mar  5 07:15:09.707:   DHCPD: lease time remaining (secs) = 86400
```

e. Проверьте сетевое соединение.

Можно ли отправить эхо-запрос от компьютера PC-B на шлюз по умолчанию, назначенный сервером DHCP?

Можно ли отправить эхо-запрос от PC-B на его шлюз по умолчанию (192.168.0.1)? Можно ли отправить эхо-запрос от компьютера PC-B на маршрутизатор R2?

Можно ли отправить эхо-запрос от компьютера PC-B на маршрутизатор ISP?

f. При возникновении каких-либо неполадок на шаге e, запишите обнаруженные проблемы и все команды, необходимые для устранения неполадок.

g. Очистите и обновите настройки IP на компьютере PC-B. Повторите шаг e для проверки сетевого соединения.

```
R2# undebug all
All possible debugging has been turned off
```

h. Прервите процесс отладки с помощью команды undebug all.

Вопросы на закрепление

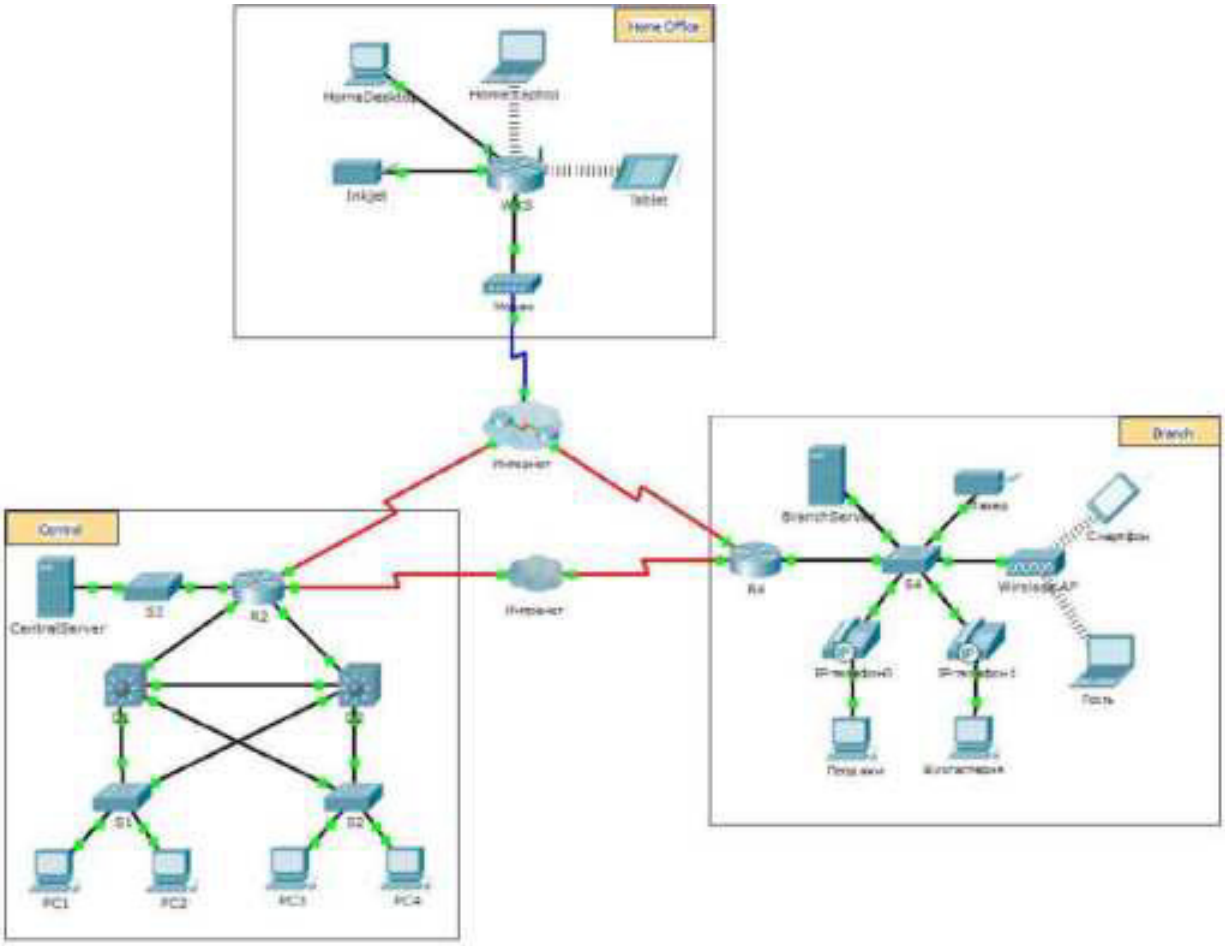
Каковы преимущества использования DHCP?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно				

Практическая работа 16. Изучение принципа работы NAT

Топология



Задачи

Часть 1. Изучение работы NAT во внутренней сети (Intranet)

Часть 2. Изучение работы NAT в сети Интернет Часть 3. Проведение дальнейших исследований

Сценарий

При передаче кадра по сети MAC-адреса могут меняться. При пересылке пакета устройством, поддерживающим NAT, IP-адреса также могут меняться. В рамках данного задания мы исследуем, что происходит с IP-адресами в процессе преобразования NAT.

Часть 1. Изучение работы NAT во внутренней сети (Intranet)

Шаг 1: Дождитесь окончания схождения сети.

Схождение всех служб в сети может занять несколько минут. Процесс можно ускорить, нажав Fast Forward Time (Ускорить).

Шаг 2: С любого ПК в центральном домене (Central) создайте запрос HTTP.

a.На любом ПК из домена Central откройте веб-браузер и введите следующий адрес, не нажимая ВВОД или Go (Перейти): http://branchserver.pka.

b.Перейдите в режим Simulation (Моделирование) и настройте фильтры таким образом, чтобы появлялись только HTTP-запросы.

c. Щёлкните кнопку перехода (Go) в браузере — появится конверт протокольного блока данных PDU.

d. Нажимайте Oapture/Forward (Захват/Вперед), пока PDU не покинет D1 или D2. Запишите IP- адреса узла-источника и узла-назначения. Каким устройствам принадлежат эти адреса?

e. Нажимайте Capture/Forward (Захват/Вперед), пока PDU не покинет маршрутизатор R2. Запишите IP-адреса узла-источника и узла-назначения в исходящем пакете. Каким устройствам принадлежат эти адреса?

f. Войдите в маршрутизатор R2, используя пароль «class» для перехода в привилегированный режим, и отобразите текущую конфигурацию. Адрес был получен из следующего пула адресов:

ip nat pool R2Pool 64.100.100.3 64.100.100.31 netmask 255.255.255.224

g. Нажимайте Capture/Forward (Захват/Вперед), пока PDU не покинет маршрутизатор R4. Запишите IP-адреса узла-источника и узла-назначения в исходящем пакете. Каким устройствам принадлежат эти адреса?

h. Нажимайте Capture/Forward (Захват/Вперед), пока PDU не покинет Branserver.pka. Запишите адреса источника и назначения TCP-портов в исходящем сегменте.

i. На маршрутизаторах R2 и R4 выполните следующую команду и сопоставьте IP-адреса и порты, записанные выше, с соответствующей строкой выходных данных:

R2# show ip nat translations **R4#** show ip nat translations

j. Что общего у внутренних локальных IP-адресов?

k. Частные адреса попадали во внутреннюю сеть (Intranet)? ,

l. Вернитесь в режим Realtime (режим реального времени).

Часть 2. Изучение работы NAT в сети Интернет

Шаг 1: С любого ПК из домашнего офиса (Home Office) создайте HTTP-запрос.

a. На любом ПК из домашнем офисе (Home Office) откройте веб-браузер и введите следующий адрес, не нажимая ВВОД или Go (Перейти): http://centralserver.pka.

b. Перейдите в режим Simulation (Моделирование). Для отображения только HTTP-запросов на этом этапе уже должны быть установлены соответствующие фильтры.

c. Щёлкните кнопку перехода (Go) в браузере — появится конверт протокольного блока данных PDU.

d. Нажимайте Захват/Вперед (Capture/Forward), пока PDU не покинет WRS. Запишите IP-адреса узла-источника и узла-назначения для входящих и исходящих пакетов. Каким устройствам принадлежат эти адреса?

e. Нажимайте Capture/Forward (Захват/Вперед), пока PDU не покинет маршрутизатор R2. Запишите IP-адреса узла-источника и узла-назначения в исходящем пакете. Каким устройствам принадлежат эти адреса?

f. На маршрутизаторе R2 выполните следующую команду и сопоставьте IP-адреса и порты, записанные выше, с соответствующей строкой выходных данных:

R2# show ip nat translations

g. Вернитесь в режим Realtime (режим реального времени). Все ли страницы открылись в браузерах?

Часть 3. Проведение дальнейших исследований

a. Поэкспериментируйте как с HTTP-пакетами, так и с пакетами HTTPS. Ознакомьтесь со списком вопросов, которые необходимо учитывать при выполнении задания:

- Увеличиваются ли таблицы преобразования NAT?
- Имеется ли в WRS пул адресов?
- Данный способ используется для подключения компьютеров в учебной аудитории к сети Интернет?
- Почему механизм NAT использует четыре столбца адресов и портов?

Предлагаемый способ подсчёта баллов

Раздел, содержащий задание	Пункт, содержащий вопрос	Возможное количество баллов	Количество заработанных баллов
Часть 1. Запрос веб-страницы во внутренней сети	Шаг 2d	12	
	Шаг 2e	12	
	Шаг 2g	13	
	Шаг 2j	12	
	Шаг 2k	12	
Часть 1. Всего		61	
Часть 2. Запрос веб-страницы в сети Интернет	Шаг 1d	13	
	Шаг 1e	13	
	Шаг 1g	13	
Часть 2. Всего		39	
Общее количество баллов		100	

Практическая работа 17. Настройка динамического и статического NAT

Топология

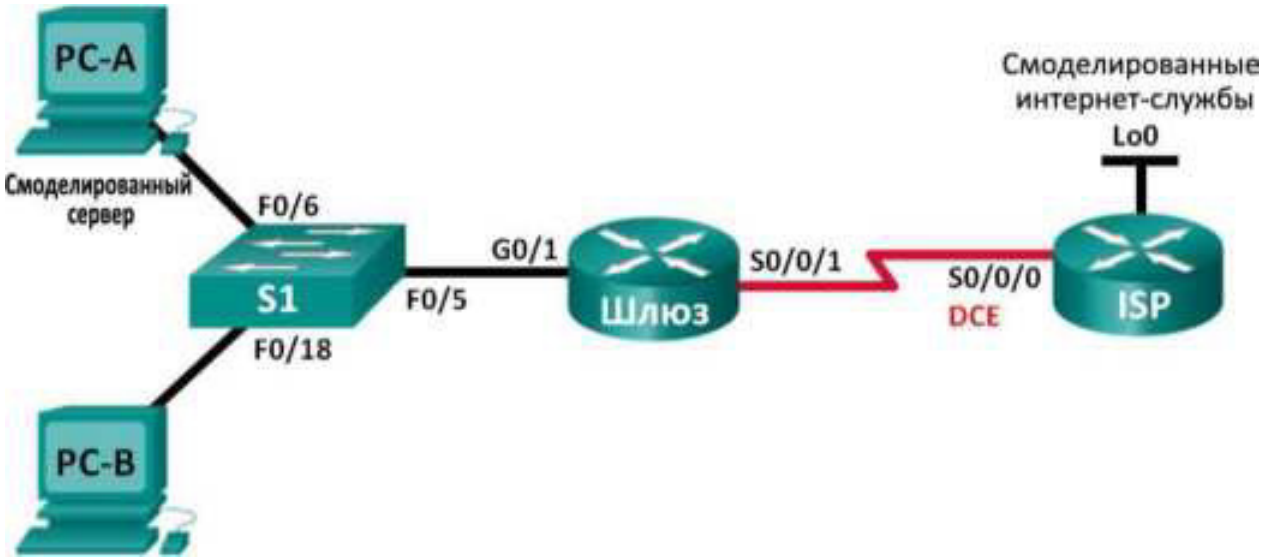


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Шлюз	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
Интернет-провайдер	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A (смоделированный сервер)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Задачи

Часть 1. Построение сети и проверка подключения

Часть 2. Настройка и проверка статического преобразования NAT

Часть 3. Настройка и проверка динамического преобразования NAT

Исходные данные/Сценарий

Преобразование сетевых адресов (NAT) — это процесс, при котором сетевое устройство, например маршрутизатор Cisco, назначает публичный адрес узловым устройствам в пределах частной сети.

NAT используют для того, чтобы сократить количество публичных IP-адресов, используемых организацией, поскольку количество доступных публичных ^4-адресов ограничено.

Согласно сценарию данной лабораторной работы интернет-провайдер выделил для компании пространство публичных IP-адресов 209.165.200.224/27. В результате компания получила 30 публичных IP-

адресов. Адреса от 209.165.200.225 до 209.165.200.241 подлежат статическому распределению, а адреса от 209.165.200.242 до 209.165.200.254 — динамическому распределению. Статический маршрутом является путь от интернет-провайдера до шлюзового маршрутизатора, в то время как маршрут по умолчанию представлен в качестве пути от шлюза до маршрутизатора интернет-провайдера. Подключение интернет-провайдера к Интернету смоделировано loopback-адресом на маршрутизаторе интернет-провайдера.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9).

В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

- 2 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 1 коммутатор (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Построение сети и проверка подключения

В первой части вам предстоит настроить топологию сети и выполнить базовые настройки, например IP-адрес интерфейса, статическая маршрутизация, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Подключите устройства в соответствии с топологией и проведите все необходимые кабели.

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.Отключите поиск DNS.

a.Настройте IP-адреса для маршрутизаторов, указанных в таблице

адресации.

b. Установите тактовую частоту на 128000 для всех последовательных интерфейсов DCE.

c. Присвойте имена устройствам в соответствии с топологией.

d. Назначьте cisco в качестве паролей консоли и VTY.

e. Назначьте class в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

f. Настройте logging synchronous, чтобы сообщения от консоли не могли прерывать ввод команд.

Шаг 5: Создайте модель веб-сервера для интернет-провайдера.

a. Создайте локального пользователя под именем webuser с зашифрованным паролем webpass.

ISP(config)# username webuser privilege 15 secret webpass

b. Включите службу HTTP-сервера на маршрутизаторе интернет-провайдера.

ISP(config)# ip http server

c. Настройте сервис HTTP таким образом, чтобы он использовал локальную базу данных.

ISP(config)# ip http authentication local

Шаг 6: Настройте статическую маршрутизацию.

a. Создайте статический маршрут от маршрутизатора интернет-провайдера до маршрутизатора шлюза, используя диапазон назначенных публичных сетевых адресов 209.165.200.224/27.

ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18

b. Создайте маршрут по умолчанию от маршрутизатора Gateway к маршрутизатору ISP. Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17

Шаг 7: Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 8: Проверьте сетевое соединение.

a. С узлов ПК отправьте эхо-запросы на интерфейс G0/1 на шлюзовом маршрутизаторе. Выявите и устраните неполадки, если эхо-запрос не проходит.

b. Отобразите таблицы маршрутизации на обоих маршрутизаторах, чтобы убедиться, что статические маршруты содержатся в таблице маршрутизации и правильно настроены на обоих маршрутизаторах.

Часть 2: Настройка и проверка статического преобразования NAT

Статический NAT использует сопоставление локальных и глобальных адресов по схеме «один к одному». Метод статического преобразования сетевых адресов особенно полезен для веб-серверов или устройств, которые должны иметь постоянный адрес, доступный из Интернета — например, для веб-сервера компании.

Настроенная статическая привязка позволяет маршрутизатору осуществлять трансляцию адресов между частным внутренним адресом сервера 192.168.1.20 и публичным адресом 209.165.200.225. Благодаря этому пользователь может получить доступ к компьютеру PC-A через Интернет. Компьютер PC-A моделирует сервер или устройство с постоянным адресом, к которому можно получить доступ через Интернет.

```
Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.2
```

Шаг 2: Задайте интерфейсы.

Выполните команды **ip nat inside** и **ip nat outside** на интерфейсах.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

Шаг 3: Проверьте конфигурацию.

a. Отобразите таблицу статических преобразований NAT с помощью команды **show ip n translations**.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
```

Во что был преобразован внутренний адрес локального узла?

192.168.1.20 =

Кем назначен внутренний глобальный адрес?

Кем назначен внутренний локальный адрес?

b. Из компьютера PC-A отправьте эхо-запрос на интерфейс Lo0 (192.31.7.1) интернет-провайдера. Если эхо-запрос прошёл неудачно, найдите и устраните проблемы. На шлюзовом маршрутизаторе (Gateway) отобразите таблицу NAT.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:1 192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
--- 209.165.200.225    192.168.1.20       ---                ---
```

Когда компьютер PC-A отправил ICMP-запрос (эхо-запрос) на адрес интернет-провайдера 192.31.7.1, в таблицу была добавлена запись NAT, где ICMP указан в виде протокола.

Какой номер порта использовался в данном обмене ICMP?

Примечание. Для успешной передачи эхо-запросов в рамках этой лабораторной может потребоваться отключение брандмауэра.

c. От компьютера PC-A отправьте сообщение по Telnet на интерфейс интернет-провайдера Lo0 и отобразите таблицу NAT.

```
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:1 192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
```

```
tcp 209.165.200.225:1034 192.168.1.20:1034  192.31.7.1:23      192.31.7.1:23
--- 209.165.200.225      192.168.1.20       ---                ---
```

Примечание. NAT для ICMP-запроса может истечь, из-за чего он будет удалён из таблицы NAT. Какой протокол использовался для этого преобразования?

Укажите номера используемых портов.

Внутренний глобальный/локальный:

Внешний глобальный/локальный:

d. Поскольку статический NAT настроен для компьютера PC-A, убедитесь в успешной отправке эхозапроса от интернет-провайдера на компьютер PC-A с частным публичным NAT-адресом (209.165.200.225).

e. На шлюзовом маршрутизаторе (Gateway) отобразите таблицу NAT, чтобы проверить преобразование.

```
Gateway# show ip nat translations
Pro Inside global        Inside local       Outside local      Outside global
icmp 209.165.200.225:12 192.168.1.20:12    209.165.201.17:12  209.165.201.17:1
--- 209.165.200.225      192.168.1.20       ---                ---
```

Обратите внимание, что внешний локальный и внешний глобальный адреса совпадают. Этот адрес — адрес источника удалённой сети интернет-провайдера. Для успешной отправки эхозапроса от интернет-провайдера, внутренний глобальный статический NAT-адрес 209.165.200.225 был преобразован во внутренний локальный адрес компьютера PC-A. (192.168.1.20).

f. Проверьте статистику NAT, выполнив команду show ip nat statistics на шлюзовом маршрутизаторе (Gateway).

```
Gateway# show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39  Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Примечание. Отображаемые выходные данные приводятся исключительно в качестве примера. Полученные вами выходные данные могут с ними не совпадать.

Часть 3: Настройка и проверка динамического преобразования NAT

Метод динамического преобразования сетевых адресов (динамический NAT) использует пул публичных адресов, которые присваиваются в порядке живой очереди. Когда внутреннее устройство запрашивает доступ к внешней сети, динамический NAT присваивает доступный публичный IPv4- адрес из пула. Динамический NAT представляет собой сопоставление адресов по схеме «многие ко многим» между локальными и глобальными адресами.

Шаг 1: Очистите данные NAT.

Перед добавлением динамических преобразований очистите все NAT и удалите статистику из части 2.

```
Gateway# clear ip nat translation *
Gateway# clear ip nat statistics
```

Шаг 2: Создайте ACL-список, который соответствует диапазону частных IP-адресов локальной сети.

Для трансляции адресов из сети 192.168.1.0/24 используется ACL1

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Шаг 3: Убедитесь, что конфигурации интерфейса NAT все ещё действительны.

Чтобы проверить конфигурации NAT, на маршрутизаторе Gateway выполните команду show ip nat statistics.

Шаг 4: Определите пул пригодных к использованию публичных IP-адресов.

```
Gateway(config)# ip nat pool public_access 209.165.200.242 209.165.200
netmask 255.255.255.224
```

Шаг 5: Определите соответствие в NAT внутреннего списка адресов источника и пула внешних адресов.

Примечание. Помните, что имена пула NAT чувствительны к регистру, а имя пула, вводимое здесь, должно совпадать с именем, использованным на предыдущем шаге.

```
Gateway(config)# ip nat inside source list 1 pool public_access
```

Шаг 6: Проверьте конфигурацию.

а. Из компьютера PC-B отправьте эхо-запрос на интерфейс Lo0 (192.31.7.1) интернет-провайдера. Если эхо-запрос прошёл неудачно, найдите и устраните проблемы. На шлюзовом маршрутизаторе (Gateway) отобразите таблицу NAT.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
icmp 209.165.200.242:1 192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
--- 209.165.200.242    192.168.1.21       ---                ---
```

Как выглядит преобразованный внутренний адрес локального узла для компьютера PC-B? 192.168.1.21 =

Когда компьютер PC-B отправил ICMP-сообщение на адрес интернет-провайдера 192.31.7.1, в таблицу была добавлена динамическая запись NAT, где ICMP указан в виде протокола.

Какой номер порта использовался в данном обмене ICMP?

b. В компьютере PC-B откройте веб-браузер и введите IP-адрес смоделированного веб-сервера интернет-провайдера (интерфейс Lo0). При запросе войдите в систему под именем webuser и с паролем webpass.

c. Отобразите таблицу NAT.

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.225	192.168.1.20	---	---
tcp	209.165.200.242:1038	192.168.1.21:1038	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1039	192.168.1.21:1039	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1040	192.168.1.21:1040	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1041	192.168.1.21:1041	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1042	192.168.1.21:1042	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1043	192.168.1.21:1043	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1044	192.168.1.21:1044	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1045	192.168.1.21:1045	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1046	192.168.1.21:1046	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1047	192.168.1.21:1047	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1048	192.168.1.21:1048	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1049	192.168.1.21:1049	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1050	192.168.1.21:1050	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1051	192.168.1.21:1051	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1052	192.168.1.21:1052	192.31.7.1:80	192.31.7.1:80
	209.165.200.242	192.168.1.22		

Какой протокол использовался для этого преобразования?

Укажите номера используемых портов.

Внутренний:

Внешний:

Какие известные номер порта и сервис использовались?

d. Проверьте статистику NAT, выполнив команду show ip nat statistics на шлюзовом маршрутизаторе (Gateway).

```
Gateway# show ip nat statistics
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Peak translations: 17, occurred 00:06:40 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 345  Misses: 0
CEF Translated packets: 345, CEF Punted packets: 0
Expired translations: 20
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
```

```
        type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Примечание. Отображаемые выходные данные приводятся исключительно в качестве примера. Полученные вами выходные данные могут с ними не совпадать.

Шаг 7: Удалите запись статического NAT.

На шаге 7 запись статического NAT удалена, вы можете просмотреть запись NAT.

a. Удалите статический NAT из части 2. При запросе об удалении дочерних записей введите yes.

```
Gateway(config)# no ip nat inside source static 192.168.1.20 209.165.20

Static entry in use, do you want to delete child entries? [no]: yes
```

b. Очистите преобразования NAT и статистику.

c. Отправьте эхо-запрос на интернет-провайдер (192.31.7.1) от обоих узлов.

d. Отобразите таблицу и статистику NAT.

```
Gateway# show ip nat statistics
 total active translations: 4 (0 static, 4 dynamic; 2 extended)
 total translations: 15, occurred 00:00:03 ago
Outside interfaces:
  Serial0/2/1
 Inside interfaces:
  G gabitEthernet0/1
Hits: 16  Misses: 2
CEF Translated packets: 284, CEF Punted packets: 0
Expired translations:
Dynamic mappings:
   -- Inside Source
[id: 1, access list 1 pool public_access refcount 4
 pool public_access: netmask 255.255.255.252
        start 209.165.200.247 end 209.165.200.254
        type generic, total addresses 13, allocated 2 (15%), misses 0

 Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0

Gateway# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.243    192.168.1.20       ---                ---
 icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512     192.31.7.1:512
    209.165.200.242    192.168.1.21
```

Примечание. Отображаемые выходные данные приводятся исключительно в качестве примера. Полученные вами выходные данные могут с ними не совпадать.

Вопросы на закрепление

1. Зачем нужно использовать NAT в сети?
2. Каковы ограничения NAT?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	Интерфейс Ethernet №1	Интерфейс Ethernet №2	Последовательный интерфейс №1	Последовательный интерфейс №2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно				

Практическая работа 18. Проверка, поиск и устранение неполадок конфигураций NAT

Топология

10.4.11.0/24

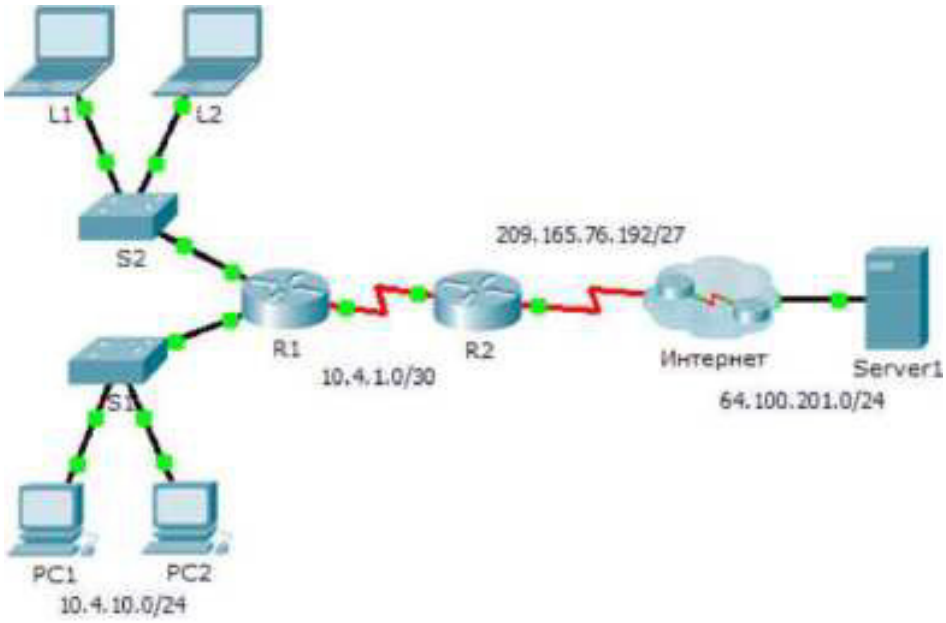


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	10.4.10.254	255.255.255.0	N/A
	G0/1	10.4.11.254	255.255.255.0	N/A
	S0/0/1	10.4.1.2	255.255.255.252	N/A
R2	S0/0/0	209.165.76.194	255.255.255.224	N/A
	S0/0/1	10.4.1.1	255.255.255.252	N/A
Serverl	NIC	64.100.201.5	255.255.255.0	64.100.201.1
PC1	NIC	10.4.10.1	255.255.255.0	10.4.10.254
PC2	NIC	10.4.10.2	255.255.255.0	10.4.10.254
L1	NIC	10.4.11.1	255.255.255.0	10.4.11.254
L2	NIC	10.4.11.2	255.255.255.0	10.4.11.254

Задачи

Часть 1. Выявление неполадок

Часть 2. Устранение неполадок в конфигурации NAT

Часть 3. Проверка подключения

Сценарий

Подрядчик восстановил прежние настройки на новом маршрутизаторе, поддерживающем NAT. Однако после применения прежних настроек сеть изменилась, и была добавлена новая подсеть. Ваша задача — привести сеть в рабочее состояние.

Часть 1. Выявление неполадок

Отправьте эхо-запрос на сервер **Serverl** с **PCI**, **PC2**, **LI**, **L2** и **R2**. Запишите результаты каждого эхозапроса. В случае необходимости отправьте эхо-запрос на любой другой компьютер.

Часть 2. Устранение неполадок в конфигурации NAT

Шаг 1: Просмотрите преобразования NAT на маршрутизаторе R2.

Если механизм NAT работает, в таблице должны быть записи.

Шаг 2: Просмотрите текущую конфигурацию маршрутизатора R2.

Проверьте, что внутреннему порту NAT назначен частный адрес, а внешнему порту NAT назначен публичный адрес.

Шаг 3: Исправьте настройки интерфейсов.

Примените команды **ip nat inside** и **ip nat outside** к соответствующим портам.

Шаг 4: Отправьте эхо-запрос на сервер Server1 с PC1, PC2, L1, L2 и R2.

Запишите результаты каждого эхо-запроса. В случае необходимости отправьте эхо-запрос на любой другой компьютер.

Шаг 5: Просмотрите преобразования NAT на маршрутизаторе R2.

Если механизм NAT работает, в таблице должны быть записи.

Шаг 6: Отобразите список доступа 101 на маршрутизаторе R2.

Шаблонная маска должна включать в себя сети 10.4.10.0 и 10.4.11.0.

Шаг 7: Внесите изменения в список доступа.

Удалите список доступа 101 и замените его похожим списком, содержащим всего одну запись. Единственным отличием должна быть шаблонная маска.Часть 3. Проверка подключения

Шаг 1: Проверьте подключение к серверу Server1.

Запишите результаты каждого эхо-запроса. Все узлы должны успешно отправлять эхо-запросы на сервер **Serverl**, **R1** и **R2**. В случае неудачных эхо-запросов выявите и устраните неполадки.

Шаг 2: Просмотрите преобразования NAT на маршрутизаторе R2.

В результате применения NAT в таблице должно быть отображено множество записей.

Основная литература:

1. Кузин, А.В. Компьютерные сети : учеб. пособие / А.В. Кузин, Д.А. Кузин. — 4-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2019. — 190 с. — (Среднее профессиональное образование). - Режим доступа: http://znanium.com/catalog/product/983172 - Договор № 5669 от 10.01.2022 г.

Дополнительная литература:

1. Максимов, Н.В. Компьютерные сети : учеб. пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 464 с. — (Среднее профессиональное образование). - Режим доступа: http://znanium.com/catalog/product/792686 - Договор № 5669 от 10.01.2022 г.
2. Сысоев, Э.В. Администрирование компьютерных сетей /Э.В. Сысоев, А.В. Терехов, Е.В. Бурцева; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный технический университет». – Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2017. – 80 с. : ил. – Режим доступа:– URL: http://biblioclub.ru/index.php?page=book&id=499414. – Библиогр. в кн. – ЭБС Университетская библиотека

Интернет-источники:

1. Журнал сетевых решений LAN [Электронный ресурс]. — Режим доступа: URL:http://www.osp.ru/lan/#/home
2. Журнал о компьютерных сетях и телекоммуникационных технологиях «Сети и системы связи» [Электронный ресурс]. — Режим доступа: URL: http://www.ccc.ru/
3. Научно-технический и научно-производственный журнал «Информационные технологии» [Электронный ресурс]. — Режим доступа: URL: http://www.novtex.ru/IT/
4. Национальный Открытый Университет «ИНТУИТ» [Электронный ресурс]. — Режим доступа: URL: http://www.intuit.ru/
5. Журнал CHIP [Электронный ресурс]. — Режим доступа: URL: http://www.ichip.ru/
6. Журнал "ComputerBild" [Электронный ресурс]. — Режим доступа: URL: http://www.computerbild.ru

7. Проектирование сетевой инфраструктуры на базе Windows Server 2008: видеокурс <Электронный ресурс>. - Режим доступа: http://soft-wins.net/video- lessons/4495-video-kurs-m6435-proektirovanie-setevoy-infrastruktury-na-baze-windjws- server-2008.html.