

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению практических работ
по дисциплине «Защищенные локальные вычислительные сети»
для студентов направления подготовки
10.03.01 «Информационная безопасность»
Направленность (профиль)
«Организация и технологии защиты информации (по отрасли или в сфере профессиональной
деятельности)»

Ставрополь
2026

СОДЕРЖАНИЕ

Введение	
Практическая работа 1. Определение IPv4-адресов	6
Практическая работа 2. Определение IPv6-адресов	9
Практическая работа 3. Расчёт подсетей IPv4	18
Практическая работа 4. Разработка и внедрение схемы адресации VLSM	25
Практическая работа 5. Настройка параметров безопасности коммутатора	32
Практическая работа 6. Конфигурация сетей VLAN и транковых каналов	43
Практическая работа 7. Настройка маршрутизации между сетями VLAN на основе стандарта 802.1Q и транкового канала	57
Практическая работа 8. Реализация системы безопасности сети VLAN	62
Практическая работа 9. Создание статического маршрута	70
Практическая работа 10. Настройка протоколов RIPv2 и RIPv6	72
Практическая работа 11. Настройка и проверка стандартных списков контроля доступа для IPv4	88
Практическая работа 12. Настройка и проверка ACL-списков для IPv6	96
Практическая работа 13. Настройка динамического и статического NAT	107
Практическая работа 14. Настройка NAT-пула с перегрузкой и PAT	121
Практическая работа 15. Базовая настройка DHCPv4 на маршрутизаторе	127
Практическая работа 16. Настройка сервера DHCPv6 без отслеживания состояния и с отслеживанием состояния	132
Практическая работа 17. Настройка протоколов CDP и LLDP	144
Практическая работа 18. Настройка Syslog и NTP	151

1. Цель и задачи освоения дисциплины (модуля)

Целью изучения дисциплины «Защищенные локальные вычислительные сети» является формирование набора профессиональных компетенций будущего бакалавра, способствующих углубленной подготовке к решению профессиональных задач по созданию, сопровождению и защите локальных вычислительных сетей, а также приобретение набора профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Задачами дисциплины являются:

1. Подготовка бакалавров к выявлению сущности проблем, возникающих в процессе развертывания, настройки и сопровождения вычислительных сетей.
2. Теоретическая и практическая подготовка бакалавров к настройке и применению специфического аппаратного обеспечения вычислительных сетей
3. Мотивация студентов к деятельности исследовательского характера для развития их творческих способностей, а также инициирование самообразовательной деятельности в освоении предметной области, касающейся вопросов построения защищенных вычислительных сетей.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-1 Способен обеспечивать защиту от НСД сооружений и СССЭ (за исключением сетей связи специального назначения) в процессе их эксплуатации	ИД-2 ПК-1 Способен к управлению функционированием СССЭ, защищённостью от НСД сооружений СССЭ	-определяет необходимый состав, особенности размещения СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД; -организовывает и проводит монтаж и настройку СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД; -устанавливает и настраивает программное обеспечение, необходимое для управления СССЭ и средствами их защиты от НСД

	ИД-3 ПК-1 Способен к управлению персоналом, обслуживающим сооружения и СССЭ, а также программные, программно-аппаратные (в том числе криптографические) и технические средства и системы их защиты от НСД	-формирует цели, приоритеты, обязанности и полномочия персонала, обслуживающего сооружения и СССЭ, средства и системы их защиты от НСД, распределяет обязанности и полномочия персонала, обслуживающего сооружения и СССЭ, средства и системы их защиты от НСД, проверяет уровень квалификации персонала, обслуживающего сооружения и СССЭ, средства и системы их защиты от НСД, в том числе, при приеме на работу; -производит постановку задач персоналу по обеспечению защиты СССЭ от НСД и организует их выполнение, организует контроль выполнения организационно-технических мероприятий по обеспечению защиты СССЭ от НСД, организует перераспределение обязанностей и полномочий персонала, обслуживающего сооружения и СССЭ, средства и системы их защиты от НСД; -усвоил цели и задачи по управлению персоналом, обслуживающего сооружения и СССЭ, средства и системы их защиты от НСД, усвоил методику выбора и организации управленческих решений по обеспечению защиты сетей электросвязи от НСД, использует руководящие и
--	--	--

		методические документы уполномоченных федеральных органов исполнительной власти по защите информации
ПК-2 Способен администрировать средства защиты информации в компьютерных системах и сетях	ИД-1 ПК-2 Способен администрировать подсистемы защиты информации в операционных системах	-выделяет принципы функционирования средств защиты информации в операционных системах. в том числе использующих криптографические алгоритмы; -настраивает политики безопасности операционных систем; -разрабатывает порядок применения программно-аппаратных средств защиты информации в операционных системах
	ИД-2 ПК-2 Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях	-формирует шаблоны конфигурации программно-аппаратных средств защиты информации в компьютерных сетях; -настраивает программные и аппаратные средства построения компьютерных сетей, использующих криптографическую защиту информации;
	ИД-3 ПК-2 Способен администрировать средства защиты информации прикладного и системного программного обеспечения	-контролирует корректность функционирования программно-аппаратных средств защиты информации в компьютерных сетях; -управляет средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями

Практическая работа 1. Определение IPv4-адресов

Цели занятия:

Часть 1. Определение IPv4-адресов

- Определите сетевую и узловую части IP-адреса.
- Определите диапазон адресов узлов с использованием пары маски сети и префикса.

Часть 2. Классификация IPv4-адресов

- Определите тип адреса (адрес сети, узла, многоадресной или широковещательной рассылки).
- Определите, является ли адрес общим или частным.
- Определите, является ли присвоенный адрес допустимым адресом узла.

Формируемые компетенции: ПК-1; ПК-2

Исходные данные/сценарий

Адресация составляет важную функцию протоколов сетевого уровня, поскольку обеспечивает обмен данными между узлами в одной и той же сети или между разными сетями. В ходе практической работы вы изучите структуру протокола Интернета версии 4 (IPv4). Вы определите различные типы IPv4-адресов и компоненты, из которых они состоят — сетевую и узловую части, маску подсети. В число рассматриваемых типов адресов входят общие и частные адреса, адреса для одноадресной передачи и многоадресной рассылки.

Необходимые ресурсы

- Устройство с выходом в Интернет
- Дополнительно: калькулятор IPv4-адресов

Часть 1: Определение IPv4-адресов

В части 1 вы рассмотрите несколько примеров IPv4-адресов и заполните таблицы соответствующими данными.

Шаг 1: Проанализируйте приведённую ниже таблицу и определите сетевую и узловую части указанных IPv4-адресов.

Первые две строки содержат примеры заполнения таблицы.

Сокращения, используемые в таблице:

C = все 8 бит для октета содержатся в сетевой части адреса

c = бит в сетевой части адреса

У = все 8 бит для октета содержатся в узловой части адреса

y = бит в узловой части адреса

IP- адрес/префикс	Сеть/узел С, с = сеть У, у = узел	Маска подсети	Сетевой адрес
192.168.10.10/24	С.С.С.У	255.255.255.0	192.168.10.0
10.101.99.17/23	С.С.сссссссу.У	255.255.254.0	10.101.98.0
209.165.200.227/27			
172.31.45.252/24			
10.1.8.200/26			
172.16.117.77/20			
10.1.1.101/25			
209.165.202.140/27			
192.168.28.45/28			

Шаг 2: Проанализируйте приведённую ниже таблицу и укажите диапазон адресов узлов и широковещательных адресов в виде пары маски подсети и префикса.

В первой строке приведён пример завершения таблицы.

IP- адрес/префикс	Адрес первого узла	Адрес последнего узла	Широковещате льный адрес
192.168.10.10/24	192.168.10.1	192.168.10.254	192.168.10.255
10.101.99.17/23			
209.165.200.227/27			
172.31.45.252/24			
10.1.8.200/26			
172.16.117.77/20			
10.1.1.101/25			
209.165.202.140/27			
192.168.28.45/28			

Часть 2: Классификация IPv4-адресов

В части 2 вам необходимо определить и классифицировать несколько примеров IPv4-адресов.

Шаг 1: Проанализируйте приведённую ниже таблицу и определите тип адреса (адрес сети, узла, многоадресной или широковещательной рассылки).

В первой строке приведён пример завершения таблицы.

IP-адрес	Маска подсети	Тип адреса
10.1.1.1	255.255.255.252	узел
192.168.33.63	255.255.255.192	
239.192.1.100	255.252.0.0	
172.25.12.52	255.255.255.0	
10.255.0.0	255.0.0.0	
172.16.128.48	255.255.255.240	
209.165.202.159	255.255.255.224	
172.16.0.255	255.255.0.0	
224.10.1.11	255.255.255.0	

Шаг 2: Проанализируйте приведённую ниже таблицу и определите тип адреса — общий или частный.

IP-адрес/префикс	Общий или частный
209.165.201.30/27	
192.168.255.253/24	
10.100.11.103/16	
172.30.1.100/28	
192.31.7.11/24	
172.20.18.150/22	
128.107.10.1/16	
192.135.250.10/24	
64.104.0.11/16	

Шаг 3: Проанализируйте приведённую ниже таблицу и определите, является ли пара адреса и префикса допустимым адресом узла.

IP-адрес/префикс	Допустимый адрес узла?	Причина
127.1.0.10/24		
172.16.255.0/16		
241.19.10.100/24		
192.168.0.254/24		
192.31.7.255/24		
64.102.255.255/14		
224.0.0.5/16		
10.0.255.255/8		
198.133.219.8/24		

Вопросы на закрепление

Почему необходимо продолжать изучение IPv4-адресации, если доступное пространство IPv4-адресов исчерпано?

Список литературы, рекомендуемый к использованию по данной теме:

Основная: 1-3

Дополнительная: 1-8

Методическая: 1

Интернет-ресурсы: 1

Программное обеспечение: 1-4

Практическая работа 2. Определение IPv6-адресов

Топология



Цели занятия:

Часть 1. Определение различных типов IPv6-адресов

- Рассмотрите различные типы IPv6-адресов.
- Сопоставьте IPv6-адрес с правильным типом адреса.

Часть 2. Изучение сетевого интерфейса и IPv6-адреса узла

- Проверьте настройки сетевого IPv6-адреса на компьютере.

Часть 3. Отработка сокращения IPv6-адресов

- Изучите и проанализируйте правила сокращения IPv6-адресов.
- Отработайте сворачивание и развёртывание IPv6-адресов.

Часть 4. Определение иерархии сетевых префиксов глобальных IPv6-адресов одноадресной передачи

- Изучите и проанализируйте иерархию сетевого префикса IPv6.
- Отработайте извлечение данных сетевого префикса из IPv6-адреса.

Формируемые компетенции: ПК-1; ПК-2

Исходные данные/сценарий

Поскольку пространство сетевых IPv4-адресов неумолимо сокращается, а IPv6-адреса используются всё чаще, сетевым специалистам необходимо понимать, как функционируют сети IPv4 и IPv6. Множество устройств и приложений уже поддерживают протокол IPv6. Сюда входит обширная поддержка устройств с операционной системой сетевого взаимодействия Cisco IOS, а также поддержка операционной системы для рабочих станций и серверов, аналогичная поддержке Windows и Linux.

В данной Практической работе рассматриваются IPv6-адреса и их компоненты. В части 1 вы будете устанавливать типы IPv6-адресов, а в части 2 рассмотрите настройки IPv6 на ПК. В части 3 вы попрактикуетесь в сворачивании IPv6-адресов, а в части 4 займетесь идентификацией частей сетевого префикса IPv6, работая с глобальными адресами одноадресной передачи.

Необходимые ресурсы

- Один ПК (Windows 7 или Vista с доступом в Интернет)

Примечание. Активация протокола IPv6 в ОС Windows 7 и Vista установлена по умолчанию. В операционной системе Windows XP протокол IPv6 по умолчанию не активирован, поэтому данную ОС на этом практическом занятии использовать не рекомендуется. В данном практическом занятии используются узлы ПК с ОС Windows 7.

Часть 3: Определение различных типов IPv6-адресов

В части 1 вы рассмотрите характеристики и научитесь определять различные типы IPv6-адресов.

Шаг 1: Рассмотрите различные типы IPv6-адресов.

Длина IPv6-адреса составляет 128 бит. Чаще всего он состоит из 32 шестнадцатеричных символов. Каждый шестнадцатеричный символ равен 4 битам ($4 \times 32 = 128$). Несокращённый IPv6-адрес узла имеет следующий вид:

2001:0DB8:0001:0000:0000:0000:0000:0001

Гекстет — это шестнадцатеричная IPv6-версия октета IPv4. Длина IPv4-адреса составляет 4 октета с разделением точками. Длина IPv6-адреса составляет 8 гекстетов с разделением точками.

IPv4-адрес состоит из 4 октетов и обычно записывается или отображается в десятичном представлении.

255.255.255.255

IPv6-адрес состоит из 8 гекстетов и обычно записывается или отображается в шестнадцатеричном представлении.

FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

В IPv4-адресе каждый отдельный октет состоит из 8 двоичных символов (битов). Четыре октета равны одному 32-битному IPv4-адресу.

11111111 = 255

11111111.11111111.11111111.11111111 = 255.255.255.255

В IPv6-адресе длина каждого отдельного гексета составляет 16 бит. Восемь гекстетов равны одному 128-битному IPv6-адресу.

1111111111111111 = FFFF

1111111111111111.1111111111111111.1111111111111111.1111111111111111

.

1111111111111111.1111111111111111.1111111111111111.1111111111111111
= FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

Если читать IPv6-адрес слева направо, то первый (крайний слева) гекстет обозначает тип IPv6-адреса. Например, если в крайнем левом гексете IPv6-адреса указаны одни нули, то это, скорее всего, адрес логического интерфейса (loopback).

0000:0000:0000:0000:0000:0000:0001 = адрес логического интерфейса

::1 = сокращённый адрес логического интерфейса

Другой пример: если первый гекстет IPv6-адреса выглядит как FE80, мы имеем дело с локальным адресом канала.

FE80:0000:0000:0000:C5B7:CB51:3C00:D6CE = локальный адрес канала

FE80::C5B7:CB51:3C00:D6CE = сокращённый локальный адрес канала

Изучите приведённую ниже таблицу. Она поможет вам в определении различных типов IPv6-адресов по символам в первом гекстете.

Первый (крайний слева) гекстет	Тип IPv6-адреса
0000—00FF	Адрес логического интерфейса, любой адрес, не указанный адрес или IPv4-совместимый адрес
2000—3FFF	Глобальный адрес одноадресной передачи (маршрутизируемый адрес в диапазоне адресов, которые в настоящий момент распределяются Администрацией адресного пространства Интернет [IANA])
FE80—FEBF	Локальный адрес канала (адрес одноадресной передачи, идентифицирующий главный компьютер в локальной сети)
FC00—FCFF	Уникальный локальный адрес (адрес одноадресной передачи, который может быть назначен узлу для его идентификации как части определённой подсети в локальной сети)
FF00—FFFF	Многоадресная рассылка

Существуют и другие типы IPv6-адресов, которые ещё не нашли широкого применения, уже устарели либо более не поддерживаются. Например, **адреса anycast** — это новый тип IPv6-адресов, которые могут использоваться маршрутизаторами для распределения нагрузки и поиска альтернативных путей, если маршрутизатор становится недоступным. На адреса anycast должны реагировать только маршрутизаторы. В свою очередь, **локальные адреса организаций** теряют свою актуальность и постепенно вытесняются уникальными локальными адресами. Локальные адреса организаций обозначались символами FEC0 в первом гекстете.

В IPv6-сетях не используются адреса сетей (каналов) и широковещательные адреса, которые применяются в IPv4-сетях.

Шаг 2: Определите тип IPv6-адреса.

Сопоставьте IPv6-адреса с соответствующими типами. Обратите внимание на то, что адреса свёрнуты, а сетевой префикс в виде наклонной черты не отображается. Некоторые варианты ответов необходимо использовать несколько раз.

IPv6-адрес	Ответ
2001:0DB8:1:ACAD::FE55:6789:B210	1. _____
::1	2. _____
FC00:22:A:2::CD4:23E4:76FA	3. _____
2033:DB8:1:1:22:A33D:259A:21FE	4. _____
FE80::3201:CC01:65B1	5. _____

Варианты ответов

- Адрес обратной связи
- Глобальный адрес одноадресной передачи
- Локальный адрес канала
- Уникальный локальный адрес
- Многоадресная рассылка

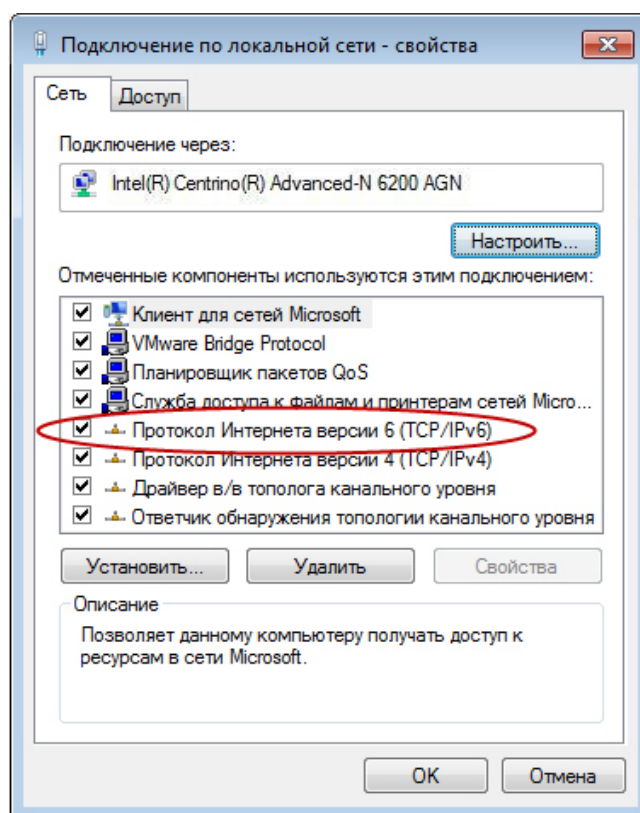
FF00::	6. _____
FF00::DB7:4322:A231:67C	7. _____
FF02::2	8. _____

Часть 4: Изучение сетевого интерфейса и IPv6-адреса узла

В части 2 вы проверите настройки IPv6-сети на компьютере и определите свой IPv6-адрес сетевого интерфейса.

Шаг 1: Проверьте настройки сетевого IPv6-адреса на компьютере.

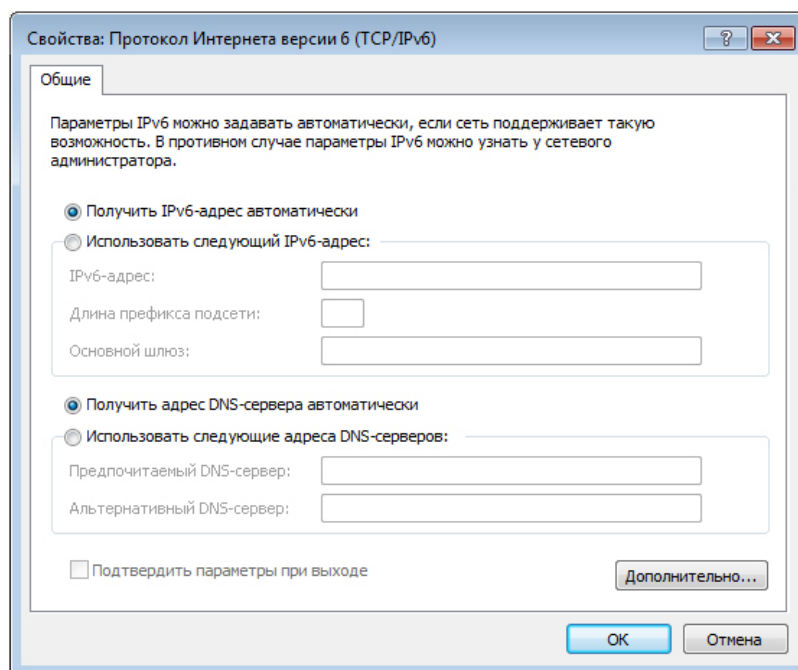
- Убедитесь в том, что протокол IPv6 установлен и активирован на ПК-А (проверьте параметры подключения по локальной сети).
- В системе Windows нажмите кнопку **Пуск**, откройте **Панель управления** и вместо **Просмотр: Категория** выберите **Просмотр: Мелкие значки**.
- Нажмите на значок **Центр управления сетями и общим доступом**.
- В левой части окна выберите **Изменение параметров адаптера**. Появятся значки, обозначающие установленные сетевые адаптеры. Нажмите правой кнопкой мыши на активный сетевой интерфейс (это может быть **Подключение по локальной сети** или **Подключение по беспроводной сети**) и выберите **Свойства**.
- Откроется окно «Свойства подключения по локальной сети». Прокрутите список элементов и определите наличие IPv6 — это будет означать, что данный компонент установлен. Также проверьте, установлен ли флажок рядом с IPv6 — он означает, что протокол активен.



- Выберите **Протокол Интернета версии 6 (TCP/IPv6)** и нажмите кнопку **Свойства**. Откроются свойства IPv6 для вашего сетевого интерфейса. Скорее всего, в окне свойств IPv6 будет выбран параметр **Получить IPv6-адрес автоматически**. Это не означает, что IPv6 зависит от протокола динамической конфигурации сетевого узла

(DHCP). Вместо DHCP IPv6 обращается к локальному маршрутизатору для получения данных IPv6-сети, а затем автоматически настраивает собственные IPv6-адреса. Для настройки IPv6 вручную необходимо указать IPv6-адрес, длину префикса подсети и шлюз по умолчанию.

Примечание. Для получения данных IPv6 (в частности, информации из DNS) локальный маршрутизатор может направлять запросы с узлов на сервер DHCPv6 сети.



- g. Убедившись в том, что компонент поддержки IPv6 на вашем компьютере установлен и активен, проверьте IPv6-адрес. Для этого нажмите кнопку **Пуск**, введите **cmd** в строке *Найти программы и файлы* и нажмите клавишу ВВОД. Откроется окно командной строки Windows.
- h. Введите команду **ipconfig /all** и нажмите клавишу ВВОД. Результаты выполнения команды должны выглядеть следующим образом:

```
C:\Users\user>ipconfig /all
```

```
Windows IP Configuration
```

```
<output omitted>
```

```
Wireless LAN adapter Wireless Network Connection:
```

```
    Connection-specific DNS Suffix  . : 
    Description . . . . . : Intel(R) Centrino(R)
Advanced-N 6200 AGN
    Physical Address. . . . . : 02-37-10-41-FB-48
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . :
fe80::8d4f:4f4d:3237:95e2%14 (Preferred)
    IPv4 Address. . . . . : 
192.168.2.106 (Preferred)
```

```
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, January 06,
2013 9:47:36 AM
Lease Expires . . . . . : Monday, January 07,
2013 9:47:38 AM
Default Gateway . . . . . : 192.168.2.1
DHCP Server . . . . . : 192.168.2.1
DHCPv6 IAID . . . . . : 335554320
DHCPv6 Client DUID. . . . . : 00-01-00-01-14-57-84-
B1-1C-C1-DE-91-C3-5D

DNS Servers . . . . . : 192.168.1.1
                        8.8.4.4
```

<output omitted>

- i. Как видно из выходных данных, клиенту ПК присвоен локальный IPv6-адрес канала с произвольно генерируемым идентификатором интерфейса. Что можно сказать в данном случае о глобальном IPv6-адресе одноадресной передачи, уникальном локальном IPv6-адресе или IPv6-адресе шлюза?

- j. Какой тип IPv6-адреса вы получили при использовании команды **ipconfig /all**?

Часть 5: Отработка сворачивания IPv6-адресов

В части 3 вам предстоит изучить и проанализировать правила сокращения IPv6-адресов, позволяющие правильно сворачивать и разворачивать IPv6-адреса.

Шаг 1: Изучите и проанализируйте правила сокращения IPv6-адресов.

Правило 1. В IPv6-адресе гекстет, состоящий из четырёх нулей, можно сократить до одного нуля.

2001:0404:0001:1000:**0000:0000**:0EF0:BC00

2001:0404:0001:1000:**0:0**:0EF0:BC00 (четыре нуля сокращены до одного)

Правило 2. В IPv6-адресе начальные нули в каждом гекстете можно опустить, в то время как конечные нули опускать нельзя.

2001:**0**404:**0001**:1000:0000:0000:**0**EF0:BC00

2001:404:1:1000:0:0:EF0:BC00 (опущены начальные нули)

Правило 3. В IPv6-адресе последовательность из четырёх или более нулей можно заменить на два двоеточия (::). Сокращение в виде двух двоеточий в IP-адресе можно использовать только один раз.

2001:0404:0001:1000:**0000:0000**:0EF0:BC00

2001:404:1:1000::**EF0:BC00** (начальные нули опущены,
а последовательность нулей заменена на два двоеточия)

Правила сокращения IPv6-адресов показаны в приведённой ниже схеме.

```
FF01:0000:0000:0000:0000:0000:0000:1
= FF01:0:0:0:0:0:0:1
= FF01::1
```

```
E3D7:0000:0000:0000:51F4:00C8:C0A8:6420
= E3D7::51F4:C8:C0A8:6420
```

```
3FFE:0501:0008:0000:0260:97FF:FE40:EFAB
= 3FFE:501:8:0:260:97FF:FE40:EFAB
= 3FFE:501:8::260:97FF:FE40:EFAB
```

Шаг 2: Отработайте сворачивание и развёртывание IPv6-адресов.

Используя правила сокращения IPv6-адресов, сверните или разверните следующие адреса:

- 1) 2002:0EC0:0200:0001:0000:04EB:44CE:08A2

- 2) FE80:0000:0000:0001:0000:60BB:008E:7402

- 3) FE80::7042:B3D7:3DEC:84B8

- 4) FF00::

- 5) 2001:0030:0001:ACAD:0000:330E:10C2:32BF

Часть 6: Определение иерархии сетевых префиксов глобальных IPv6-адресов одноадресной передачи

В части 4 вам необходимо изучить и проанализировать характеристики сетевого префикса IPv6 и определить его иерархические сетевые компоненты.

Шаг 1: Изучите и проанализируйте иерархию сетевого префикса IPv6.

IPv6-адрес представляет собой 128-битный адрес, состоящий из двух частей — сетевой части, которая определяется первыми 64 битами (или первыми четырьмя гекстетами), и узловой части, которая определяется последними 64 битами (или последними четырьмя

гекстетами). Следует помнить, что каждая цифра или символ в IPv6-адресе записываются в шестнадцатеричной системе счисления и равны четырём битам. Вот как выглядит типовой глобальный адрес одноадресной передачи:

Сетевая часть: **2001:DB8:0001:ACAD:xxxx:xxxx:xxxx:xxxx**
Узловая часть: xxxx:xxxx:xxxx:xxxx:**0000:0000:0000:0001**

В большинстве адресов одноадресной передачи (маршрутизируемых адресов) используется 64-битный сетевой префикс и 64-битный адрес узла. При этом длина сетевой части IPv6-адреса не ограничивается 64 битами, а обозначается косой чертой в конце адреса, после которой следует десятичное число, обозначающее длину. Если сетевой префикс имеет вид /64, значит, длина сетевой части IPv6-адреса при чтении слева направо равна 64 битам. Оставшуюся длину IPv6-адреса составляет узловая часть (идентификатор интерфейса), представленная последними 64 битами. В некоторых случаях, например в адресах логического интерфейса, сетевой префикс может иметь вид /128, т. е. длину 128 битов. В этом случае для идентификатора интерфейса битов не остаётся, а значит, сеть ограничена одним узлом. Вот несколько примеров IPv6-адресов с различной длиной сетевых префиксов:

Глобальный адрес одноадресной передачи,	2001:DB8:0001:ACAD:0000:0000:0000:0001/64
Адрес логического интерфейса:	::1/128
Адрес многоадресной рассылки:	FF00::/8
Адрес для всех сетей:	::/0 (аналогично адресу из четырёх нулей в IPv4)
Локальный адрес канала	fe80::8d4f:4f4d:3237:95e2%14 (обратите внимание на то, что значение /14 в конце адреса представлено в виде символа процентов и десятичного числа 14. Этот адрес взят из результатов выполнения команды «ipconfig /all» в окне командной строки Windows)

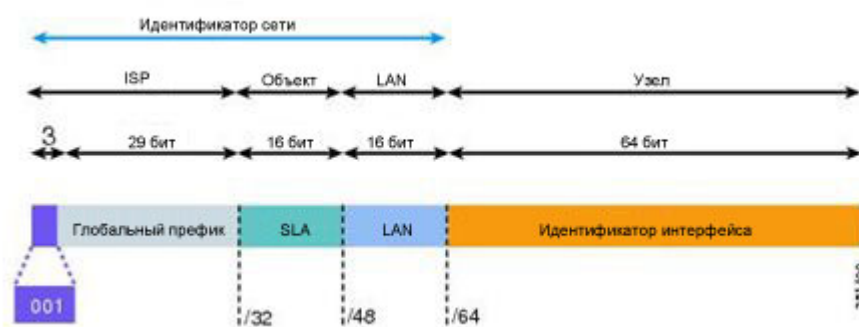
Слева направо сетевая часть глобального IPv6-адреса одноадресной передачи имеет иерархическую структуру, из которой можно получить следующую информацию:

- 1) Глобальный номер маршрутизации IANA (первые три двоичных бита имеют фиксированное значение 001)
200::/12
- 2) Префикс регионального реестра Интернет (RIR) биты с /12 до /23)
2001:0D::/23 (шестнадцатеричный символ D в двоичной системе имеет вид 1101. Биты с 21 по 23 — это 110, а последний бит является частью префикса интернет-провайдера)
- 3) Префикс интернет-провайдера (биты до /32)
2001:0DB8::/32
- 4) Префикс организации или идентификатор агрегата уровня организации (SLA), присваиваемый клиенту интернет-провайдером (биты до /48)
2001:0DB8:0001::/48
- 5) Префикс подсети (присваивается клиентом; биты до /64)
2001:0DB8:0001:ACAD::/64
- 6) Идентификатор интерфейса (узел определяется последними 64 битами в адресе)

2001:DB8:0001:ACAD:8D4F:4F4D:3237:95E2/64

На приведённой ниже схеме показано, что IPv6-адрес можно разделить на четыре основные части:

- 1) Глобальный префикс маршрутизации /32
- 2) Идентификатор агрегата уровня организации (SLA) /48
- 3) Идентификатор подсети (LAN) /64
- 4) Идентификатор интерфейса (последние 64 бита)



Узловая часть IPv6-адреса называется идентификатором интерфейса, поскольку определяет не фактический узел, а сетевой адаптер узла. Каждый сетевой интерфейс может иметь несколько IPv6-адресов, а значит, и несколько идентификаторов интерфейса.

Шаг 2: Оработайте извлечение данных сетевого префикса из IPv6-адреса.

Используя следующий адрес, ответьте на заданные ниже вопросы:

2000:1111:aaaa:0:50a5:8a35:a5bb:66e1/64

- a. Назовите идентификатор интерфейса.

- b. Назовите номер подсети.

- c. Назовите номер организации.

- d. Назовите номер интернет-провайдера.

- e. Как выглядит номер интернет-провайдера в двоичном формате?

- f. Назовите номер регионального реестра.

g. Как выглядит номер регионального реестра в двоичном формате?

h. Назовите глобальный номер IANA.

i. Назовите глобальный префикс маршрутизации.

Вопросы на закрепление

1. Как, на ваш взгляд, необходимо поддерживать IPv6 в будущем?

2. Как вы считаете, будут ли IPv4-сети использоваться и дальше или, в конце концов, все перейдут на IPv6? Как вы думаете, сколько времени займёт этот переход?

Список литературы, рекомендуемый к использованию по данной теме:

Основная: 1-3

Дополнительная: 1-8

Методическая: 1

Интернет-ресурсы: 1

Программное обеспечение: 1-4

Практическая работа 3. Расчёт подсетей IPv4

Цели занятия:

Часть 1. Определение данных сети по IPv4-адресу

- Определите адрес сети.
- Определите широковещательный адрес.
- Определите количество узлов.

Часть 2. Расчёт данных сети по IPv4-адресу

- Определите количество созданных подсетей.
- Определите количество узлов для каждой подсети.
- Определите адрес подсети.
- Определите диапазон узлов для подсети.

- Определите широковещательный адрес для подсети.

Формируемые компетенции: ПК-1; ПК-2

Исходные данные/сценарий

Умение работать с подсетями IPv4 и определять информацию о сетях и узлах на основе известного IP-адреса и маски подсети необходимо для понимания принципов работы IPv4-сетей. Цель первой части — закрепить знания о том, как рассчитывать IP-адрес сети на основе известного IP-адреса и маски подсети. Зная IP-адрес и маску подсети, вы всегда сможете установить следующие данные подсети:

- Сетевой адрес
- Широковещательный адрес
- Общее количество битов узлов
- Количество узлов в подсети

Во второй части Практической работы вы определите следующие данные для указанного IP-адреса и маски подсети:

- Сетевой адрес этой подсети
- Широковещательный адрес этой подсети
- Диапазон адресов узлов для этой подсети
- Количество созданных подсетей
- Количество узлов для каждой подсети

Необходимые ресурсы

- 1 ПК (Windows 7, Vista или XP с выходом в Интернет)
- Дополнительно: калькулятор IPv4-адресов

Часть 1: Определение данных сети по IPv4-адресу

В части 1 вам необходимо определить сетевой и широковещательный адреса, а также количество узлов, зная IPv4-адрес и маску подсети.

ОБЗОР. Чтобы определить сетевой адрес, выполните бинарную операцию И для IPv4-адреса, используя указанную маску подсети. В результате вы получите сетевой адрес. Совет: если маска подсети имеет в октете десятичное значение 255, результатом ВСЕГДА будет исходное значение этого октета. Если маска подсети имеет в октете десятичное значение 0, результатом для этого октета ВСЕГДА будет 0.

Пример.

IP-адрес	192.168.10.10
Маска подсети	255.255.255.0
	=====
Результат (сеть)	192.168.10.0

Зная это, вы можете выполнить бинарную операцию И только для того октета, значение которого в маске подсети отличается от 255 или 0.

Пример.

IP-адрес	172.30.239.145
Маска подсети	255.255.192.0

Проанализировав этот пример, вы увидите, что бинарная операция И требуется только для третьего октета. В этой маске подсети первые два октета дадут результат 172.30, а четвертый — 0.

IP-адрес	172.30.239.145
Маска подсети	255.255.192.0
	=====
Результат (сеть)	172.30.?0

Выполните бинарную операцию И для третьего октета.

Десятичное	Двоичное
239	11101111
192	11000000
	=====
Результат192	11000000

Анализ этого примера снова даст следующий результат:

IP-адрес	172.30.239.145
Маска подсети	255.255.192.0
	=====
Результат (сеть)	172.30.192.0

Рассчитать количество узлов для каждой сети в данном примере можно путём анализа маски подсети. Маска подсети будет представлена в десятичном формате с точкой-разделителем, например 255.255.192.0, или в формате сетевого префикса, например /18. IPv4-адрес всегда содержит 32 бита. Отняв количество битов, используемых сетевой частью (как показано в маске подсети), вы получите количество битов, используемых для узлов.

В нашем примере маска подсети 255.255.192.0 равна /18 в префиксной записи. Вычитание 18 бит сети из 32 бит даст нам 14 бит, оставшихся для узловой части. Исходя из этого, можно выполнить простой расчёт:

$$2^{(\text{количество битов узла}) - 2} = \text{количество узлов}$$

$$2^{14} = 16\,384 - 2 = 16\,382 \text{ узла}$$

Определите сетевые и широковещательные адреса и количество битов узлов для IPv4-адресов и префиксов, указанных в приведённой ниже таблице.

Адрес IPv4/префикс	Сетевой адрес	Широковещательный адрес	Общее количество битов узлов	Общее количество узлов
192.168.100.25/28				
172.30.10.130/30				
10.1.113.75/19				
198.133.219.250/24				
128.107.14.191/22				
172.16.104.99/27				

Часть 2: Расчёт данных сети по IPv4-адресу

Зная IPv4-адрес, а также исходную и новую маски подсети, можно определить следующие параметры:

- Сетевой адрес этой подсети
- Широковещательный адрес этой подсети
- Диапазон адресов узлов этой подсети
- Количество созданных подсетей
- Количество узлов в подсети

В приведённом ниже примере показана одна из задач и её решение.

Дано:	
IP-адрес узла	172.16.77.120
Исходная маска подсети	255.255.0.0
Новая маска подсети	255.255.240.0
Найти:	
Количество битов подсети	4
Количество созданных подсетей	16
Количество битов узлов в подсети	12
Количество узлов в подсети	4094
Сетевой адрес этой подсети	172.16.64.0
Адрес IPv4 первого узла в этой подсети	172.16.64.1
Адрес IPv4 последнего узла в этой подсети	172.16.79.254
Широковещательный адрес IPv4 в этой подсети	172.16.79.255

Давайте рассмотрим, как была получена такая таблица.

Исходная маска подсети имела вид 255.255.0.0 или /16. Новая маска подсети — 255.255.240.0 или /20. Полученная разница составляет 4 бита. Так как 4 бита были заимствованы, мы можем определить, что были созданы 16 подсетей, так как $2^4 = 16$.

В новой маске, равной 255.255.240.0 или /20, остаётся 12 бит для узлов. Если для узлов осталось 12 бит, воспользуемся следующей формулой: $2^{12} - 2 = 4096 - 2 = 4094$ узла для каждой подсети.

Бинарная операция И поможет определить подсеть для этой задачи, в результате чего

мы получим сеть 172.16.64.0.

В заключение необходимо установить первый узел, последний узел и широковещательный адрес для каждой подсети. Один из способов определения диапазона узлов — использовать двоичные значения для узловой части адреса. В нашем примере узловая часть — это последние 12 бит адреса. В первом узле для всех старших битов будет установлено значение 0, а для младшего бита — значение 1. В последнем узле для всех старших битов будет установлено значение 1, а для младшего бита — значение 0. В этом примере узловая часть адреса находится в третьем и четвертом октетах.

Описание	1-й октет	2-й октет	3-й октет	4-й октет	Описание
Сеть/узел	сccccccc	сccccccc	сccссуuuу	уууууууу	Маска подсети
Двоичное	10101100	00010000	01000000	00000001	Первый узел
Десятичное	172	16	64	1	Первый узел
Двоичное	10101100	00010000	01001111	11111110	Последний узел
Десятичное	172	16	79	254	Последний узел
Двоичное	10101100	00010000	01001111	11111111	Широковещательный
Десятичное	172	16	79	255	Широковещательный

Шаг 1: Заполните приведённые ниже таблицы, указав необходимые значения для указанного IPv4-адреса, а также исходной и новой масок подсети.

а. Задача 1.

Дано:	
IP-адрес узла	192.168.200.139
Исходная маска подсети	255.255.255.0
Новая маска подсети	255.255.255.224
Найти:	
Количество битов подсети	
Количество созданных подсетей	
Количество битов узлов в подсети	
Количество узлов в подсети	
Сетевой адрес этой подсети	
Адрес IPv4 первого узла в этой подсети	
Адрес IPv4 последнего узла в этой подсети	
Широковещательный адрес IPv4 в этой подсети	

б. Задача 2.

Дано:

IP-адрес узла	10.101.99.228
Исходная маска подсети	255.0.0.0
Новая маска подсети	255.255.128.0
Найти:	
Количество битов подсети	
Количество созданных подсетей	
Количество битов узлов в подсети	
Количество узлов в подсети	
Сетевой адрес этой подсети	
Адрес IPv4 первого узла в этой подсети	
Адрес IPv4 последнего узла в этой подсети	
Широковещательный адрес IPv4 в этой подсети	

с. Задача 3.

Дано:	
IP-адрес узла	172.22.32.12
Исходная маска подсети	255.255.0.0
Новая маска подсети	255.255.224.0
Найти:	
Количество битов подсети	
Количество созданных подсетей	
Количество битов узлов в подсети	
Количество узлов в подсети	
Сетевой адрес этой подсети	
Адрес IPv4 первого узла в этой подсети	
Адрес IPv4 последнего узла в этой подсети	
Широковещательный адрес IPv4 в этой подсети	

d. Задача 4.

Дано:	
IP-адрес узла	192.168.1.245
Исходная маска подсети	255.255.255.0
Новая маска подсети	255.255.255.252
Найти:	

Количество битов подсети	
Количество созданных подсетей	
Количество битов узлов в подсети	
Количество узлов в подсети	
Сетевой адрес этой подсети	
Адрес IPv4 первого узла в этой подсети	
Адрес IPv4 последнего узла в этой подсети	
Широковещательный адрес IPv4 в этой подсети	

е. Задача 5.

Дано:	
IP-адрес узла	128.107.0.55
Исходная маска подсети	255.255.0.0
Новая маска подсети	255.255.255.0
Найти:	
Количество битов подсети	
Количество созданных подсетей	
Количество битов узлов в подсети	
Количество узлов в подсети	
Сетевой адрес этой подсети	
Адрес IPv4 первого узла в этой подсети	
Адрес IPv4 последнего узла в этой подсети	
Широковещательный адрес IPv4 в этой подсети	

ф. Задача 6.

Дано:	
IP-адрес узла	192.135.250.180
Исходная маска подсети	255.255.255.0
Новая маска подсети	255.255.255.248
Найти:	
Количество битов подсети	
Количество созданных подсетей	
Количество битов узлов в подсети	
Количество узлов в подсети	
Сетевой адрес этой подсети	
Адрес IPv4 первого узла в этой подсети	
Адрес IPv4 последнего узла в этой подсети	
Широковещательный адрес IPv4 в этой подсети	

Вопросы на закрепление

Почему маска подсети имеет такое значение при анализе IPv4-адреса?

Список литературы, рекомендуемый к использованию по данной теме:

Основная: 1-3

Дополнительная: 1-8

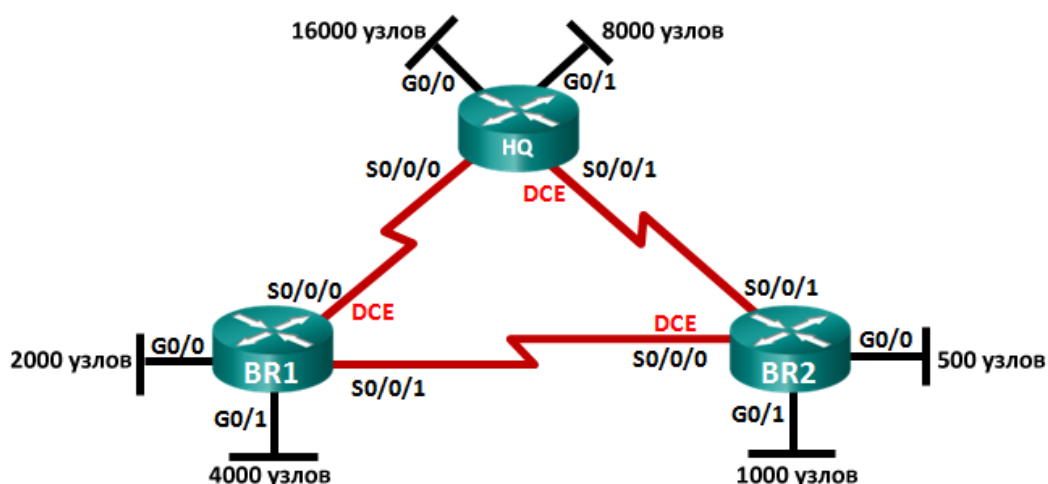
Методическая: 1

Интернет-ресурсы: 1

Программное обеспечение: 1-4

Практическая работа 4. Разработка и внедрение схемы адресации VLSM

Топология



Цели занятия:

Часть 1. Изучение требований к сети

Часть 2. Разработка схемы адресации VLSM

Часть 3. Подключение и настройка IPv4-сети

Формируемые компетенции: ПК-1; ПК-2

Исходные данные/сценарий

Маска подсети переменной длины (VLSM) предназначена для того, чтобы избежать потери IP-адресов. При использовании VLSM сеть разделяется на подсети, а затем каждая подсеть разделяется снова. Этот процесс может повторяться несколько раз и позволяет создавать подсети разных размеров, исходя из необходимого количества узлов для каждой подсети. Для эффективного использования VLSM требуется планирование адресов.

В этой Практической работе вам нужно разработать схему адресации для сети, изображённой в диаграмме топологии, используя адрес 172.16.128.0/17. VLSM обеспечивает соответствие требованиям адресации IPv4. После создания схемы адресации VLSM вам нужно будет настроить интерфейсы на маршрутизаторах, указав соответствующие IP-адреса.

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). Можно использовать другие маршрутизаторы 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 Практической работы.

Примечание. Убедитесь в том, что маршрутизаторы очищены от данных и не содержат файлы загрузочной конфигурации. Если вы не уверены, что сможете это сделать, обратитесь к инструктору.

Необходимые ресурсы

- Три маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3, универсальный образ или аналогичный)
- Один ПК (с эмулятором терминала, например Tera Term, для настройки маршрутизаторов)
- Консольный кабель для настройки устройств с операционной системой Cisco IOS через консольные порты
- Кабели Ethernet (дополнительно) и последовательные кабели, как показано в топологии
- Калькулятор Windows (дополнительно)

Часть 1: Изучение требований к сети

В части 1 вам необходимо изучить требования к сети и разработать схему адресации VLSM для сети, изображённой на диаграмме топологии, используя сетевой адрес 172.16.128.0/17.

Примечание. Для расчётов можно использовать калькулятор Windows и веб-калькулятор для IP-подсетей по адресу www.ipcalc.org.

Шаг 1: Определите количество доступных адресов узлов и подсетей.

Сколько адресов узлов доступны в сети /17? _____

Сколько всего адресов требует диаграмма топологии? _____

Сколько подсетей требует топология сети? _____

Шаг 2: Определите самую большую подсеть.

Дайте описание этой подсети (например, BR1 G0/1 LAN или канал BR1-HQ WAN).

Сколько IP-адресов требуется для самой большой подсети? _____

Какая маска подсети может поддерживать такое количество адресов узла?

Сколько всего адресов узла может поддерживать эта маска подсети? _____

Можно ли разделить сетевой адрес 172.16.128.0/17 на подсети для поддержки этой подсети? _____

Какие два сетевых адреса образуются в результате данной организации подсетей?

В данной подсети используйте первый сетевой адрес.

Шаг 3: Определите вторую по величине подсеть.

Дайте описание этой подсети. _____

Сколько IP-адресов требуется для второй по величине подсети? _____

Какая маска подсети может поддерживать такое количество адресов узла?

Сколько всего адресов узла может поддерживать эта маска подсети? _____

Возможно ли повторно организовать подсеть оставшейся подсети, поддерживая при этом данную подсеть? _____

Какие два сетевых адреса образуются в результате данной организации подсетей?

В данной подсети используйте первый сетевой адрес.

Шаг 4: Определите следующую по величине подсеть.

Дайте описание этой подсети. _____

Сколько IP-адресов требуется для следующей по величине подсети? _____

Какая маска подсети может поддерживать такое количество адресов узла?

Сколько всего адресов узла может поддерживать эта маска подсети? _____

Возможно ли повторно организовать подсеть оставшейся подсети, поддерживая при этом данную подсеть? _____

Какие два сетевых адреса образуются в результате данной организации подсетей?

В данной подсети используйте первый сетевой адрес.

Шаг 5: Определите следующую по величине подсеть.

Дайте описание этой подсети. _____

Сколько IP-адресов требуется для следующей по величине подсети? _____

Какая маска подсети может поддерживать такое количество адресов узла?

Сколько всего адресов узла может поддерживать эта маска подсети? _____

Возможно ли повторно организовать подсеть оставшейся подсети, поддерживая при этом данную подсеть? _____

Какие два сетевых адреса образуются в результате данной организации подсетей?

В данной подсети используйте первый сетевой адрес.

Шаг 6: Определите следующую по величине подсеть.

Дайте описание этой подсети. _____

Сколько IP-адресов требуется для следующей по величине подсети? _____

Какая маска подсети может поддерживать такое количество адресов узла?

Сколько всего адресов узла может поддерживать эта маска подсети? _____

Возможно ли повторно организовать подсеть оставшейся подсети, поддерживая при этом данную подсеть? _____

Какие два сетевых адреса образуются в результате данной организации подсетей?

В данной подсети используйте первый сетевой адрес.

Шаг 7: Определите следующую по величине подсеть.

Дайте описание этой подсети. _____

Сколько IP-адресов требуется для следующей по величине подсети? _____

Какая маска подсети может поддерживать такое количество адресов узла?

Сколько всего адресов узла может поддерживать эта маска подсети? _____

Возможно ли повторно организовать подсеть оставшейся подсети, поддерживая при этом данную подсеть? _____

Какие два сетевых адреса образуются в результате данной организации подсетей?

В данной подсети используйте первый сетевой адрес.

Шаг 8: Определите подсети, необходимые для поддержки последовательных каналов.

Сколько адресов узлов необходимо для каждого последовательного канала подсети?

Какая маска подсети может поддерживать такое количество адресов узла? _____

- g. Продолжайте делить на подсети первую подсеть каждой новой подсети, пока не получите четыре подсети /30. Запишите первые три сетевых адреса для этих подсетей /30.

- h. Запишите описания для этих трёх подсетей.

Часть 2: Разработка схемы адресации VLSM

Шаг 1: Рассчитайте данные подсетей.

Используя информацию, полученную в части 1, заполните приведённую ниже таблицу.

Описание подсети	Необходимое количество узлов	Сетевой адрес/CIDR	Адрес первого узла	Широковещательный адрес
HQ G0/0	16 000			
HQ G0/1	8000			
BR1 G0/1	4000			
BR1 G0/0	2000			
BR2 G0/1	1000			
BR2 G0/0	500			
HQ S0/0/0 – BR1 S0/0/1	2			
HQ S0/0/1 – BR2 S0/0/1	2			
BR1 S0/0/1 – BR2 S0/0/0	2			

Шаг 2: Заполните таблицу адресов интерфейсов устройств.

Присвойте первый адрес узла в подсети интерфейсам Ethernet. Маршрутизатору HQ необходимо присвоить первый адрес узла для последовательных каналов к BR1 и BR2. Маршрутизатору BR1 необходимо присвоить первый адрес узла для последовательного канала к BR2.

Устройство	Интерфейс	IP-адрес	Маска подсети	Интерфейс устройства
HQ	G0/0			16 000 Host LAN
	G0/1			8000 Host LAN
	S0/0/0			BR1 S0/0/0
	S0/0/1			BR2 S0/0/1
BR1	G0/0			2000 Host LAN
	G0/1			4000 Host LAN
	S0/0/0			HQ S0/0/0
	S0/0/1			BR2 S0/0/0
BR2	G0/0			500 Host LAN
	G0/1			1000 Host LAN
	S0/0/0			BR1 S0/0/1
	S0/0/1			HQ S0/0/1

Часть 3: Подключение и настройка сети IPv4

В части 3 вам необходимо подключить сетевую топологию и настроить три маршрутизатора, используя схему адресации VLSM, которую вы построили в части 2.

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

Шаг 2: Настройте основные параметры для каждого коммутатора.

- a. Назначьте маршрутизатору имя устройства.
- b. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверного преобразования введенных команд так, как если бы они были узлами.
- c. Назначьте **classv** качестве пароля привилегированного режима.
- d. Назначьте **ciscov** качестве пароля консоли и включите вход по паролю.
- e. Назначьте **ciscov** качестве пароля виртуального терминала и включите вход по паролю.
- f. Зашифруйте пароли, хранящиеся в открытом виде.
- g. Создайте баннер, который предупреждает о запрете несанкционированного доступа.

Шаг 3: Настройте интерфейсы на каждом маршрутизаторе.

- a. Назначьте IP-адрес и маску подсети для каждого интерфейса, используя таблицу, заполненную в части 2.
- b. Настройте описание интерфейса для каждого интерфейса.
- c. Установите для частоты синхронизации на всех последовательных интерфейсах DCE значение 128000.

```
HQ(config-if) # clock rate 128000
```
- d. Включите интерфейсы.

Шаг 4: Сохраните конфигурацию на всех устройствах.

Шаг 5: Проверьте подключения.

- a. С маршрутизатора HQ отправьте эхо-запрос с помощью команды ping на адрес интерфейса S0/0/0 маршрутизатора BR1.
- b. С маршрутизатора HQ отправьте эхо-запрос с помощью команды ping на адрес интерфейса S0/0/1 маршрутизатора BR2.
- c. С маршрутизатора BR1 отправьте эхо-запрос с помощью команды ping на адрес интерфейса S0/0/0 маршрутизатора BR2.
- d. Если эхо-запросы с помощью команды ping не прошли, найдите и устраните неполадки подключений.

Примечание. Эхо-запросы с помощью команды ping на интерфейсы GigabitEthernet других маршрутизаторов не дадут результата. Выполняется моделирование локальных сетей, определенных для интерфейсов GigabitEthernet. Поскольку в этих локальных сетях отсутствуют устройства, они будут в отключённом состоянии (down/down). Чтобы другие устройства получили информацию об этих подсетях, требуется протокол маршрутизации. Интерфейсы GigabitEthernet также должны быть активированы (up/up), только после этого протокол маршрутизации сможет добавить подсети в таблицу маршрутизации. Эти интерфейсы останутся в отключённом состоянии (down/down), пока к другому концу кабеля интерфейса Ethernet не будет подключено какое-либо устройство. В этой Практической работе основное внимание уделяется маске VLSM и настройке интерфейсов.

Вопросы на закрепление

Назовите быстрый способ вычисления сетевых адресов для последовательных подсетей /30?

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.

Список литературы, рекомендуемый к использованию по данной теме:

Основная: 1-3

Дополнительная: 1-8

Методическая: 1

Интернет-ресурсы: 1

Программное обеспечение: 1-4

Практическая работа 5. Настройка параметров безопасности коммутатора

Топология



Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

Цели занятия:

Часть 1. Настройка топологии и инициализация устройства

Часть 2. Настройка базовых параметров устройств и проверка подключения

Часть 3. Настройка и проверка доступа с помощью протокола SSH к коммутатору S1

- Настройте доступ по протоколу SSH.
- Измените параметры SSH.
- Проверьте конфигурацию SSH.

Часть 4. Настройка и проверка параметров безопасности для S1

- Настройте и проверьте общие функции безопасности.
- Настройте и проверьте функцию безопасности порта.

Формируемые компетенции: ПК-1; ПК-2

Исходные данные/Сценарий

На компьютерах и серверах следует ограничивать доступ, устанавливая качественную систему безопасности. На ваших устройствах сетевой инфраструктуры, например коммутаторах и маршрутизаторах, тоже важно настраивать функции безопасности.

В ходе данной Практической работе вам нужно настроить функции безопасности на коммутаторах LAN в соответствии с практическими рекомендациями. Вам следует разрешить только сеансы протокола SSH и безопасного протокола HTTPS. Кроме того, вам предстоит настроить и проверить работу функции безопасности порта, направленную на блокировку любого устройства с MAC-адресом, который неизвестен коммутатору.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторных работах используется коммутатор Cisco Catalyst 2960 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 Практической работы.

Примечание. Убедитесь, что информация из маршрутизаторов и коммутаторов удалена, и они не содержат файлов загрузочной конфигурации. Если вы не уверены, обратитесь к преподавателю или вернитесь к процедурам инициализации и перезагрузки устройств, описанных в предыдущей Практической работе.

Необходимые ресурсы:

- 1 маршрутизатор (Cisco 1941 с универсальным образом M3 под управлением ОС Cisco IOS 15.2(4) или аналогичная модель);
- 1 коммутатор (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 1 ПК (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.

Part 1: Настройка топологии и инициализация устройств

В первой части вам предстоит создать топологию сети и при необходимости удалить все конфигурации.

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

Step 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Если ранее на маршрутизаторе или коммутаторе были сохранены конфигурационные файлы, выполните инициализацию и перезагрузку устройств, чтобы восстановить базовые настройки.

Часть 2: Настройка базовых параметров устройств и проверка подключения

Во второй части Практической работы вам предстоит настроить базовые параметры маршрутизатора, коммутатора и ПК. Имена и адреса устройств можно найти в топологии и таблице адресации в начале этой Практической работы.

Step 1: Настройте IP-адрес на PC-A.

Step 2: Настройте базовые параметры на маршрутизаторе R1.

- а. Задайте имя устройства.
- б. Отключите поиск DNS.
- в. Настройте IP-адрес интерфейса в соответствии с таблицей адресации.
- г. Назначьте **class** в качестве пароля привилегированного режима EXEC.
- д. Назначьте **cisco** в качестве пароля консоли и виртуального терминала VTY и активируйте вход.
- е. Зашифруйте все незашифрованные пароли.
- ж. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Step 3: Выполните базовую настройку коммутатора S1.

Не рекомендуется назначать административный IP-адрес коммутатора для сети VLAN 1 (или любой другой VLAN с конечными пользователями). На данном этапе вам предстоит создать VLAN 99 на коммутаторе и назначить этой сети IP-адрес.

- а. Задайте имя устройства.
- б. Отключите поиск DNS.
- в. Назначьте **class** в качестве пароля привилегированного режима EXEC.
- г. Назначьте **cisco** в качестве пароля консоли и виртуального терминала VTY и

активируйте вход.

- e. Настройте шлюз по умолчанию для коммутатора S1 с помощью IP-адреса маршрутизатора R1.
- f. Зашифруйте все незашифрованные пароли.
- g. Сохраните текущую конфигурацию в загрузочную конфигурацию.
- h. Создайте на коммутаторе сеть VLAN 99 и назовите её **Management**.

```
S1(config)# vlan 99  
S1(config-vlan)# name Management  
S1(config-vlan)# exit  
S1(config)#
```

- i. Настройте IP-адрес интерфейса административной сети VLAN 99 в соответствии с таблицей адресации и включите интерфейс.

```
S1(config)# interface vlan 99  
S1(config-if)# ip address 172.16.99.11 255.255.255.0  
S1(config-if)# no shutdown  
S1(config-if)# end  
S1#
```

- j. Выполните команду **show vlan** на коммутаторе S1. В каком состоянии находится сеть VLAN 99?

- k. Выполните команду **show ip interface brief** на коммутаторе S1. В каком состоянии интерфейс VLAN 99 и протокол?

Почему протокол выключен несмотря на то, что вы выполнили команду **no shutdown** для интерфейса VLAN 99?

- l. Назначьте порты F0/5 и F0/6 для сети VLAN 99 на коммутаторе.

```
S1# config t  
S1(config)# interface f0/5  
S1(config-if)# switchport mode access  
S1(config-if)# switchport access vlan 99  
S1(config-if)# interface f0/6  
S1(config-if)# switchport mode access  
S1(config-if)# switchport access vlan 99  
S1(config-if)# end
```

- m. Выполните команду **show ip interface brief** на коммутаторе S1. В каком состоянии интерфейс VLAN 99 и протокол?

Примечание. При сходимости состояний портов может произойти небольшая задержка.

Step 4: Проверьте наличие подключения между всеми устройствами.

- a. От компьютера PC-A отправьте эхо-запрос на шлюз по умолчанию

- маршрутизатора R1. Успешно ли выполнены эхо-запросы? _____
- b. От компьютера PC-A отправьте эхо-запрос на адрес управления коммутатора S1. Успешно ли выполнены эхо-запросы? _____
 - c. От коммутатора S1 отправьте эхо-запрос на шлюз по умолчанию маршрутизатора R1. Успешно ли выполнены эхо-запросы? _____
 - d. В компьютере PC-A откройте веб-браузер и перейдите по адресу `http://172.16.99.11`. Если появится запрос на ввод имени пользователя пароля, оставьте имя пользователя пустым, а в качестве пароля введите **class**. Если появится запрос о защищённом подключении, ответьте **No**. Удалось ли вам получить доступ к веб-интерфейсу на коммутаторе S1? _____
 - e. Закройте сеанс браузера на компьютере PC-A.

Примечание. Незащищённый веб-интерфейс (сервер HTTP) коммутатора Cisco 2960 включён по умолчанию. Для обеспечения безопасности рекомендуется отключить данную службу, как описано в части 4.

Часть 3: Настройка и проверка доступа с помощью протокола SSH к коммутатору S1

Step 1: Настройте доступ к протоколу SSH на коммутаторе S1.

- a. Включите SSH на S1. В режиме глобальной конфигурации создайте имя домена **CCNA-Lab.com**.

```
S1(config)# ip domain-name CCNA-Lab.com
```

- b. Создайте запись локальной базы данных пользователей, которую вы будете использовать для подключения к коммутатору через SSH. Пользователь должен обладать правами доступа администратора.

Примечание. Используемый пароль не является надёжным. Он используется исключительно в рамках Практической работы.

```
S1(config)# username admin privilege 15 secret sshadmin
```

- c. Настройте вход транспортировки таким образом, чтобы в каналах VTY были разрешены только подключения по протоколу SSH. Для аутентификации используйте локальную базу данных.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
```

- d. Создайте ключ шифрования RSA с использованием модуля 1024 бит.

```
S1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: S1.CCNA-Lab.com
```

```
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-
exportable...
[OK] (elapsed time was 3 seconds)
```

```
S1(config)#
S1(config)# end
```

- е. Проверьте конфигурацию протокола SSH и ответьте на следующие вопросы.

S1# **show ip ssh**

Какую версию SSH использует коммутатор? _____

Сколько попыток аутентификации разрешает SSH? _____

На какое значение настроен лимит времени по умолчанию для SSH?

Step 2: Измените конфигурацию SSH на коммутаторе S1.

Измените конфигурацию SSH по умолчанию.

S1# **config t**

S1(config)# **ip ssh time-out 75**

S1(config)# **ip ssh authentication-retries 2**

Сколько попыток аутентификации разрешает SSH? _____

На какое значение настроен лимит времени для протокола SSH?

Step 3: Проверьте конфигурацию SSH на коммутаторе S1.

- а. С помощью клиентского программного обеспечения SSH на компьютере PC-A (например Tera Term), настройте SSH-подключение к коммутатору S1. Если в вашей клиентской программе SSH появилось сообщение о ключе узла, примите его. Войдите в систему, используя **admin** в качестве имени пользователя, и **cisco** в качестве пароля.

Удалось ли настроить связь? _____

Какой запрос был отображён на коммутаторе S1? Почему?

- б. Чтобы завершить сеанс SSH на коммутаторе S1, введите **exit**.

Часть 4: Настройка и проверка параметров безопасности для S1

В четвёртой части Практической работы вам предстоит закрыть неиспользуемые порты, выключить определённые сервисы, работающие на коммутаторе, и настроить функцию безопасности порта на основе MAC-адресов. Коммутаторы могут быть подвержены переполнению таблицы MAC-адресов, спуфинг-атакам и попыткам неавторизованных подключений к портам коммутатора. Вам нужно будет настроить функцию порта безопасности, чтобы ограничить количество MAC-адресов, которые могут быть получены портом коммутатора, а также отключить порт при превышении этого количества.

Step 1: Настройка общих функций безопасности на коммутаторе S1.

- а. Настройте баннер MOTD (сообщение дня) для коммутатора S1 в виде соответствующего предупреждения.
- б. Выполните команду **show ip interface brief** на коммутаторе S1. Какие физические порты включены?

-
- c. Выключите все неиспользуемые физические порты коммутатора. Используйте команду **interface range**.

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

- d. Выполните команду **show ip interface brief** на коммутаторе S1. В каком состоянии находятся порты от F0/1 до F0/4?
-

- e. Введите команду **show ip http server status**.

В каком состоянии находится сервер HTTP? _____

Какой порт сервера он использует? _____

В каком состоянии находится защищённый сервер HTTP?

Какой порт сервера он использует? _____

- f. Сеансы HTTP отправляют все данные в незашифрованном виде. Вам нужно отключить сервис HTTP, который работает на коммутаторе S1.

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

- g. В компьютере PC-A откройте веб-браузер и перейдите по адресу <http://172.16.99.11>. Что у вас получилось?
-

- h. В компьютере PC-A откройте защищённый сеанс веб-браузера по адресу <https://172.16.99.11>. Примите сертификат. Войдите в систему без имени пользователя, используйте пароль **class**. Что у вас получилось?
-

- i. Закройте сеанс браузера на компьютере PC-A.

Step 2: Настройка и проверка работы функции безопасности порта на коммутаторе S1.

- a. Запишите MAC-адрес интерфейса G0/1 маршрутизатора R1. В интерфейсе командной строки маршрутизатора R1 выполните команду **show interface g0/1** и запишите MAC-адрес интерфейса.

```
R1# show interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is
  30f7.0da3.1821 (bia 3047.0da3.1821)
```

Каков MAC-адрес интерфейса G0/1 маршрутизатора R1?

- b. В интерфейсе командной строки S1 выполните команду **show mac address-table** в привилегированном режиме. Найдите динамические записи для портов F0/5 и F0/6. Запишите их ниже.

MAC-адрес интерфейса F0/5: _____

MAC-адрес интерфейса F0/6: _____

- c. Настройка базовой безопасности порта.

Примечание. Как правило, эту процедуру выполняют на всех портах доступа коммутатора. Интерфейс F0/5 представлен в качестве примера.

- 1) Из интерфейса командной строки коммутатора S1 войдите в режим конфигурации интерфейса для порта, который подключается к R1.

```
S1(config)# interface f0/5
```

- 2) Выключите порт.

```
S1(config-if)# shutdown
```

- 3) Включите функцию безопасности порта на интерфейсе F0/5.

```
S1(config-if)# switchport port-security
```

Примечание. Выполнение команды **switchport port-security** позволит установить максимальное количество MAC-адресов на значение 1. При попытке нарушения безопасности порт будет выключен. Команды **switchport port-security maximum** и **switchport port-security violation** можно использовать для того, чтобы изменить настройки по умолчанию.

- 4) Настройте статическую запись для MAC-адреса интерфейса G0/1 маршрутизатора R1, записанного на шаге 2а.

```
S1(config-if)# switchport port-security mac-address  
xxxx.xxxx.xxxx
```

(Настоящий MAC-адрес интерфейса G0/1 маршрутизатора имеет формат xxxx.xxxx.xxxx).

Примечание. При желании вы можете использовать команду **switchport port-security mac-address**, чтобы добавить в текущую конфигурацию коммутатора защищённые MAC-адреса, которые были динамически получены на порте (до заданного максимального значения).

- 5) Включите порт коммутатора.

```
S1(config-if)# no shutdown  
S1(config-if)# end
```

- d. Проверьте функцию безопасности порта на интерфейсе F0/5 коммутатора S1 с помощью команды **showport-security interface**.

```
S1# show port-security interface f0/5  
Port Security           : Enabled  
Port Status              : Secure-up  
Violation Mode           : Shutdown  
Aging Time               : 0 mins
```

```
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

В каком состоянии находится порт F0/5?

-
- e. Из командной строки маршрутизатора R1 отправьте эхо-запрос на компьютер PC-A, чтобы проверить подключение.

```
R1# ping 172.16.99.3
```

- f. Далее, изменив MAC-адрес интерфейса маршрутизатора, вы нарушите систему безопасности. Войдите в режим конфигурации интерфейса для G0/1 и выключите его.

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# shutdown
```

- g. Настройте новый MAC-адрес для интерфейса, используя **aaaa.bbbb.cccc** в качестве адреса.

```
R1(config-if)# mac-address aaaa.bbbb.cccc
```

- h. По возможности, одновременно с этим шагом установите консольное подключение на коммутаторе S1. В консольном подключении к коммутатору S1 вы увидите различные сообщения о нарушении системы безопасности. Включите интерфейс G0/1 маршрутизатора R1.

```
R1(config-if)# no shutdown
```

- i. Из привилегированного режима коммутатора R1 отправьте эхо-запрос на компьютер PC-A. Успешно ли выполнен эхо-запрос? Поясните свой ответ.

-
- j. На коммутаторе проверьте функцию безопасности порта с помощью команд, указанных ниже.

```
S1# show port-security
```

```
Secure Port MaxSecureAddr CurrentAddr SecurityViolation
Security Action
```

```
(Count) (Count) (Count)
```

```
-----
-----
Fa0/5 1 1 1
Shutdown
```

```
-----
Total Addresses in System (excluding one mac per port)
:0
```

```
Max Addresses limit in System (excluding one mac per port)
```

:8192

S1# **show port-security interface f0/5**

```
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : aaaa.bbbb.cccc:99
Security Violation Count : 1
```

S1# **show interface f0/5**

FastEthernet0/5 is down, line protocol is down (err-disabled)

Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)

MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
<output omitted>

S1# **show port-security address**

Secure Mac Address Table

```
-----
-----
Vlan      Mac Address      Type                Ports
Remaining Age
(mins)
-----
99        30f7.0da3.1821      SecureConfigured    Fa0/5
-
```

Total Addresses in System (excluding one mac per port)
:0

Max Addresses limit in System (excluding one mac per port)
:8192

- k. На маршрутизаторе выключите интерфейс G0/1, удалите жёстко запрограммированный MAC-адрес из маршрутизатора и повторно включите интерфейс G0/1.

```
R1(config-if)# shutdown
R1(config-if)# no mac-address aaaa.bbbb.cccc
R1(config-if)# no shutdown
R1(config-if)# end
```

- l. Из маршрутизатора R1 повторите эхо-запрос на компьютер PC-A по адресу 172.16.99.3. Успешно ли выполнен эхо-запрос? _____

- m. Чтобы определить причину неудачи эхо-запроса, выполните команду **show interface f0/5**. Запишите полученные результаты.

- n. Очистите состояние выключения порта F0/5 в результате сбоя S1.

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

Примечание. При сходимости состояний портов может произойти небольшая задержка.

- o. Чтобы убедиться, что порт F0/5 вышел из состояния выключения в результате сбоя, на коммутаторе S1 выполните команду **show interface f0/5**.

```
S1# show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia
0023.5d59.9185)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
  reliability 255/255, txload 1/255, rxload 1/255
```

- p. Из командной строки маршрутизатора R1 повторите эхо-запрос на компьютер PC-A. Эхо-запрос должен пройти успешно.

Вопросы на закрепление

1. Зачем нужно включать функцию безопасности порта на коммутаторе?

2. Зачем нужно отключать неиспользуемые порты коммутатора?

Список литературы, рекомендуемый к использованию по данной теме:

Основная: 1-3

Дополнительная: 1-8

Методическая: 1

Интернет-ресурсы: 1

Программное обеспечение: 1-4

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 6. Конфигурация сетей VLAN и транковых каналов

Топология

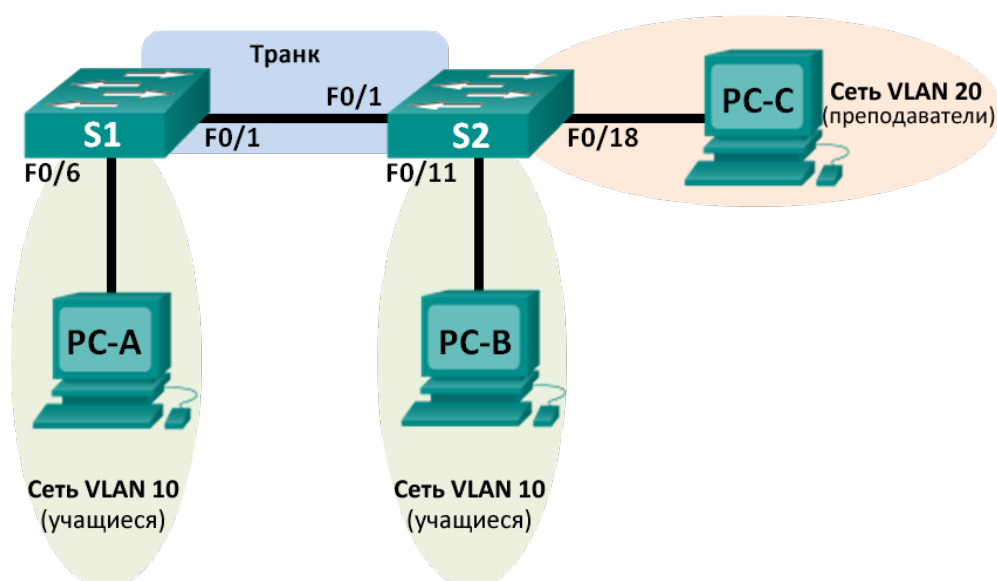


Таблица адресации

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

Цели занятия:

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

Формируемые компетенции: ПК-1; ПК-2**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, обеспечивая 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 Практической 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 Практической 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 5: Построение сети и настройка базовых параметров устройства

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

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

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

Step 2: Выполните инициализацию и перезагрузку коммутаторов.

Step 3: Настройте базовые параметры каждого коммутатора.

- Отключите поиск DNS.
- Присвойте имена устройствам в соответствии с топологией.
- Назначьте **class** в качестве пароля привилегированного режима EXEC.
- Активируйте вход и назначьте в качестве пароля **cisco** для консоли и VTY.
- Настройте **logging synchronous** для консольного канала.
- Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.
- Настройте IP-адрес, указанный в таблице адресации для сети VLAN 1, на обоих коммутаторах.
- Используя права администратора, отключите все неиспользуемые порты на коммутаторе.
- Сохраните текущую конфигурацию в загрузочную конфигурацию.

Step 4: Настройте узлы ПК.

Адреса узлов ПК можно посмотреть в таблице адресации.

Step 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 6: Создание сетей VLAN и назначение портов коммутатора

Во второй части Практической 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**.

Step 1: Создайте сети VLAN на коммутаторах.

- 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.

- 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?

Step 2: Назначьте сети VLAN соответствующим интерфейсам коммутатора.

а. 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
```

- 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
```

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

```
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 7: Поддержка назначения портов VLAN и базы данных VLAN

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

Step 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.

Step 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?

Step 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 Fa0/6, Fa0/7, Fa0/8 Fa0/10, Gi0/1, Gi0/2
10 Student	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/17, Fa0/18, Fa0/19 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	

Какая сеть по умолчанию присвоена сети VLAN 30 по умолчанию?

- с. 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 **noswitchport access vlan** на интерфейсе F0/24.
- f. Выполните команду **show vlan brief**, чтобы определить назначение 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 8: Конфигурация транкового канала стандарта 802.1Q между коммутаторами

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

Step 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.

- a. 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
```

You should also receive link status messages on S2.

```
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
*Mar 1 05:08:01.850: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Vlan1, 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.

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			
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 Практической 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.

Step 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

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 9: Удаление базы данных VLAN

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

Step 1: Определите, существует ли база данных VLAN.

Выполните команду **showflash**, 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.150-2.SE.bin
 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.

Step 2: Удалите базу данных VLAN.

- 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#
```

- Выполните команду **showflash**, 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.SE.bin
```

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?

Список литературы, рекомендуемый к использованию по данной теме:

Основная: 1-3

Дополнительная: 1-8

Методическая: 1

Интернет-ресурсы: 1

Программное обеспечение: 1-4

Практическая работа 7. Настройка маршрутизации между сетями VLAN на основе стандарта 802.1Q и транкового канала

Топология

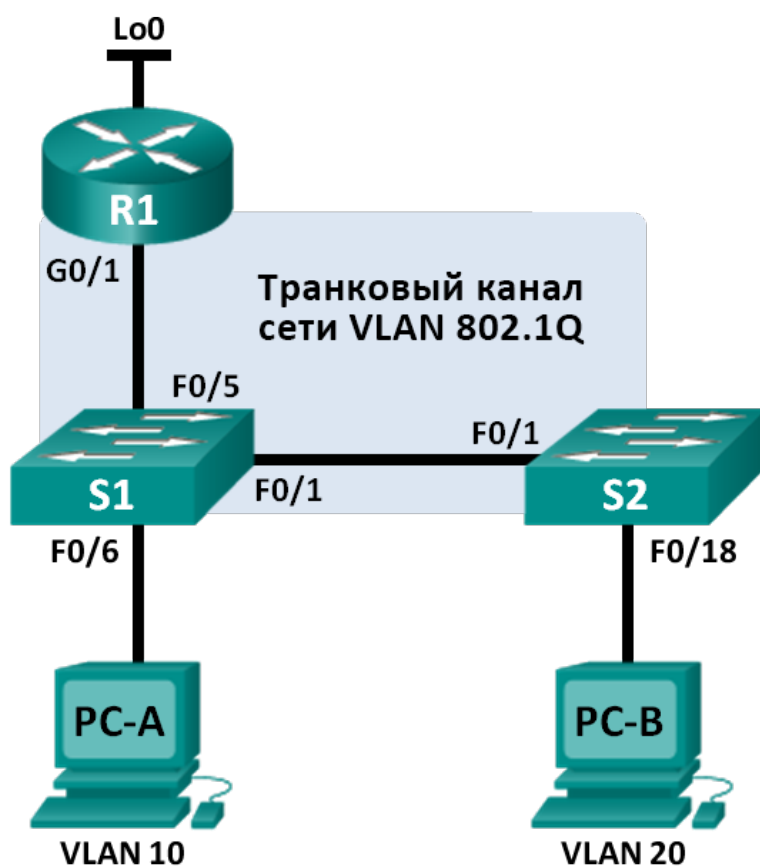


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1.1	192.168.1.1	255.255.255.0	—
	G0/1.10	192.168.10.1	255.255.255.0	—
	G0/1.20	192.168.20.1	255.255.255.0	—
	Lo0	209.165.200.225	255.255.255.224	—
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	—
S2 F0/1	Транковый канал 802.1Q	—
S1 F0/5	Транковый канал 802.1Q	—
S1 F0/6	Сеть VLAN 10 — учащиеся	192.168.10.0/24
S2 F0/18	Сеть VLAN 20 — преподаватели	192.168.20.0/24

Задачи

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Настройка коммутаторов с сетями VLAN и транковой связи

Часть 3. Настройка маршрутизации между сетями VLAN на основе транкового канала

Общие сведения/сценарий

Второй способ обеспечения маршрутизации и соединения нескольких VLAN заключается в использовании транкового канала стандарта 802.1Q между одним или несколькими коммутаторами и одним интерфейсом маршрутизатора. Также этот метод называют маршрутизацией между сетями VLAN с использованием метода router-on-a-stick. При использовании данного метода физический интерфейс маршрутизатора разделен на несколько подынтерфейсов, обеспечивающих логические пути ко всем подключенным сетям VLAN.

В рамках настоящей лабораторной работы вам предстоит настроить маршрутизацию между сетями VLAN на основе транкового канала и проверить подключение к узлам в разных сетях VLAN, как и с loopback-интерфейсом на маршрутизаторе.

Примечание. В данной лабораторной работе потребуются минимальный набор команд, необходимых для настройки маршрутизации между сетями VLAN на основе магистрального канала. Однако команды, необходимые для конфигурации сети VLAN, представлены в приложении А в конце этой лабораторной работы. Проверьте свои знания: настройте устройства, не обращаясь к информации, приведенной в приложении.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 с операционной системой Cisco IOS версии 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, а также других версий операционной системы Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Правильные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

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

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 (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: Создание сети и настройка основных параметров устройства

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

Step 1: Создайте сеть согласно топологии.

Step 2: Настройте узлы ПК.

Step 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Step 4: Настройте базовые параметры каждого коммутатора.

- а. Подключитесь к коммутатору с помощью консоли и перейдите в режим глобального конфигурирования.
- б. Скопируйте приведенную ниже базовую конфигурацию и вставьте ее в файл текущей конфигурации на коммутаторе.

```
no ip domain-lookup
service password-encryption
```

```
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

- c. Присвойте имена устройствам в соответствии с топологией.
- d. Настройте на коммутаторе IP-адрес, указанный в таблице адресации для сети VLAN 1.
- e. Настройте на коммутаторе шлюз по умолчанию.
- f. Используя права администратора, отключите все неиспользуемые порты на коммутаторе.
- g. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Step 5: Настройте базовые параметры для маршрутизатора.

- a. Подключитесь к маршрутизатору с помощью консоли и перейдите в режим глобальной настройки.
- b. Скопируйте приведенную ниже базовую конфигурацию и вставьте ее в текущую конфигурацию на маршрутизаторе.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

- c. Настройте IP-адрес loopback-интерфейса в соответствии с таблицей адресации. Пока не настраивайте субинтерфейс. Это будет сделано при выполнении части 3.
- d. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

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.

Примечание. Список команд, необходимых для выполнения части 2, приведен в приложении А. Проверьте свои знания, попробуйте настроить устройства без использования приложения.

Step 1: Настройте сети VLAN на коммутаторе S1.

- a. На коммутаторе S1 настройте сети VLAN и имена, указанные в таблице параметров назначения портов коммутатора. В специально отведенном месте напишите команды, которые вы использовали.

- b. На коммутаторе S1 настройте интерфейс, подключенный к маршрутизатору R1 в качестве транкового канала. Также настройте интерфейс, подключенный к маршрутизатору R2 в качестве транкового канала. В специально отведенном месте напишите команды, которые вы использовали.

-
-
- c. На коммутаторе S1 назначьте порт доступа для компьютера PC-A сети VLAN 10. В специально отведенном месте напишите команды, которые вы использовали.
-
-

Step 2: Настройка сетей VLAN на коммутаторе S2.

- a. На коммутаторе S2 настройте сети VLAN и имена, указанные в таблице параметров назначения портов коммутатора.
 - b. Убедитесь, что номера и имена VLAN на коммутаторе S2 совпадают с данными на коммутаторе S1. Ниже напишите команду, которую вы использовали.
-
- c. На коммутаторе S2 назначьте порт доступа для компьютера PC-B сети VLAN 20.
 - d. На коммутаторе S2 настройте интерфейс, подключенный к коммутатору S1 в качестве транкового канала.

Часть 3: Конфигурация маршрутизации между сетями VLAN на основе транкового канала

В третьей части лабораторной работы вам нужно настроить маршрутизатор R1 для маршрутизации данных в несколько сетей VLAN путем создания подынтерфейсов для каждой сети VLAN. Данный метод маршрутизации между сетями VLAN называется конфигурацией ROS (router-on-a-stick).

Примечание. Список команд, необходимых для выполнения части 3, приведен в приложении А. Проверьте свои знания, попробуйте настроить маршрутизацию между сетями VLAN с использованием метода router-on-a-stick (на основе магистрального канала) без использования приложения.

Step 1: Настройте подынтерфейс для сети VLAN 1.

- a. Создайте подынтерфейс на интерфейсе G0/1 маршрутизатора R1 для VLAN 1, где 1 — это идентификатор подынтерфейса. Ниже напишите команду, которую вы использовали.
-
- b. Настройте подынтерфейс для работы с VLAN 1. Ниже напишите команду, которую вы использовали.
-
- c. Настройте подынтерфейс с IP-адресом из таблицы адресов. Ниже напишите команду, которую вы использовали.
-

Step 2: Настройте подынтерфейс для сети VLAN 10.

- a. Создайте подынтерфейс на интерфейсе G0/1 маршрутизатора R1 для VLAN 10, где 10 — это идентификатор подынтерфейса.
- b. Настройте подынтерфейс для работы с VLAN 10.
- c. Настройте подынтерфейс с адресом из таблицы адресов.

Step 3: Настройте подынтерфейс для сети VLAN 20.

- a. Создайте подынтерфейс на интерфейсе G0/1 маршрутизатора R1 для VLAN 20, где 20 — это идентификатор подынтерфейса.
- b. Настройте подынтерфейс для работы с VLAN 20.

с. Настройте подынтерфейс с адресом из таблицы адресов.

Step 4: Включите интерфейс G0/1.

Включите интерфейс G0/1. В специально отведенном месте напишите команды, которые вы использовали.

Step 5: Проверьте подключение.

Введите команду, чтобы просмотреть таблицу маршрутизации на R1. Какие сети в ней перечислены?

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? _____

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

Если на какой-либо из этих вопросов был дан ответ **нет**, устраните неполадки в конфигурации и исправьте все ошибки.

Вопросы для повторения

В чем заключаются преимущества маршрутизации между сетями VLAN с использованием транкового канала или конфигурации ROS?

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 (S0/1/0)	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 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.				

Приложение А. Команды настройки

Коммутатор S1

```
S1(config)# vlan 10
S1(config-vlan)# name Students
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# exit
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

```
S1(config-if)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

Коммутатор S2

```
S2(config)# vlan 10
S2(config-vlan)# name Students
S2(config-vlan)# vlan 20
S2(config-vlan)# name Faculty
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
S2(config-if)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
```

Маршрутизатор R1

```
R1(config)# interface g0/1.1
R1(config-subif)# encapsulation dot1Q 1
R1(config-subif)# ip address 192.168.1.1 255.255.255.0
R1(config-subif)# interface g0/1.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# interface g0/1.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface g0/1
R1(config-if)# no shutdown
```

Практическая работа 8. Реализация системы безопасности сети VLAN

Топология

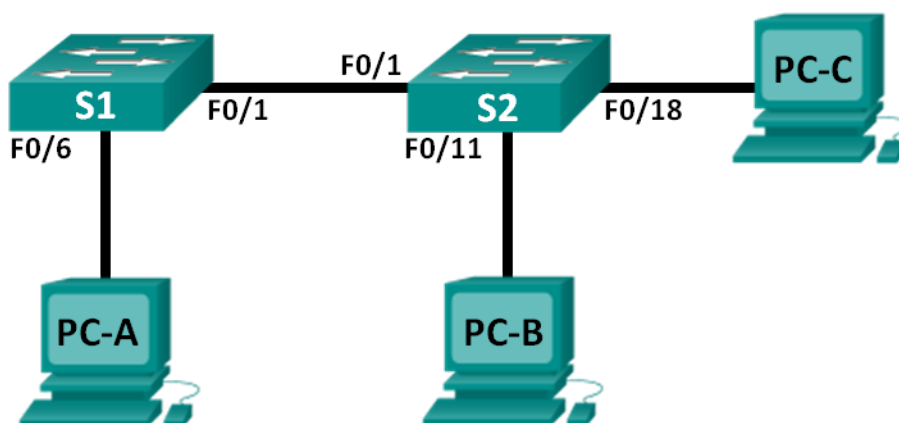


Таблица адресации

Устройств о	Интерфей с	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

Цели занятия:

Часть 1. Построение сети и настройка базовых параметров устройства

Часть 2. Внедрение средств обеспечения безопасности VLAN на коммутаторах

Формируемые компетенции: ПК-1; ПК-2

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 Практической 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 Практической 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 Практической работы нужно настроить базовые параметры на коммутаторах и компьютерах. Имена и адреса устройств указаны в таблице адресации.

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

Step 2: Выполните инициализацию и перезагрузку коммутаторов.

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

Адреса узловых ПК можно посмотреть в таблице адресации.

Step 4: Настройте базовые параметры каждого коммутатора.

- Отключите поиск DNS.
- Присвойте имена устройствам в соответствии с топологией.
- Назначьте **class** в качестве пароля привилегированного режима EXEC.
- Назначьте **cisco** в качестве пароля паролей консоли и VTY и активируйте вход для консоли и VTY каналов.
- Настройте logging synchronous для консоли и каналов vty.

Step 5: Настройте сети VLAN на каждом коммутаторе.

- Создайте и назначьте имена сетям VLAN в соответствии с таблицей назначений VLAN.
 - Настройте IP-адрес, указанный в таблице адресации для сети VLAN 99 на обоих коммутаторах.
 - Настройте порт F0/6 на коммутаторе S1 в качестве порта доступа и назначьте его сети VLAN 99.
 - Настройте порт F0/11 на коммутаторе S2 в качестве порта доступа и назначьте его сети VLAN 10.
 - Настройте порт F0/18 на коммутаторе S2 в качестве порта доступа и назначьте его сети VLAN 99.
 - 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?
-

Step 6: Настройте базовые параметры безопасности порта.

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

Step 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

Step 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 команду **show interface trunk** на обоих коммутаторах.

```
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

Step 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 %CDP-4-NATIVE_VLAN_MISMATCH:?

-
- 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

Step 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?

Step 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>
```

- a. Отключите согласование на коммутаторе S1.

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

- b. Отключите согласование на коммутаторе S2.

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

- c. 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>
```

Step 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 Практической 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
```

```

Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 999 (BlackHole)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<Output Omitted>

```

- e. 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.

- f. 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

```

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

- h. 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

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?

Список литературы, рекомендуемый к использованию по данной теме:

Основная: 1-3

Дополнительная: 1-8

Методическая: 1

Интернет-ресурсы: 1

Программное обеспечение: 1-4

Практическая работа 9. Создание статического маршрута

Задачи

Настройте статический маршрут.

Ввиду распространения IPv6-адресации сетевым администраторам требуются навыки распределения сетевого трафика между маршрутизаторами.

Для того чтобы подтвердить свои навыки корректного управления трафиком IPv6 и освежить свои знания о статическом маршруте IPv6 по умолчанию, воспользуйтесь топологией, приведенной в PDF-файле. Вместе с партнером напишите маршрут IPv6 для каждого из трех сценариев. Попробуйте прописать маршрут без обращения к сделанным ранее лабораторным работам, файлам Packet Tracer и т. д.

- **Сценарий 1**

Данные от маршрутизатора R2 направляются по статическому маршруту IPv6 по умолчанию через интерфейс S0/0/0 на адрес следующего перехода на маршрутизаторе R1.

- **Сценарий 2**

Данные от маршрутизатора R3 направляются по статическому маршруту IPv6 по умолчанию через интерфейс S0/0/1 на адрес следующего перехода на маршрутизаторе R2.

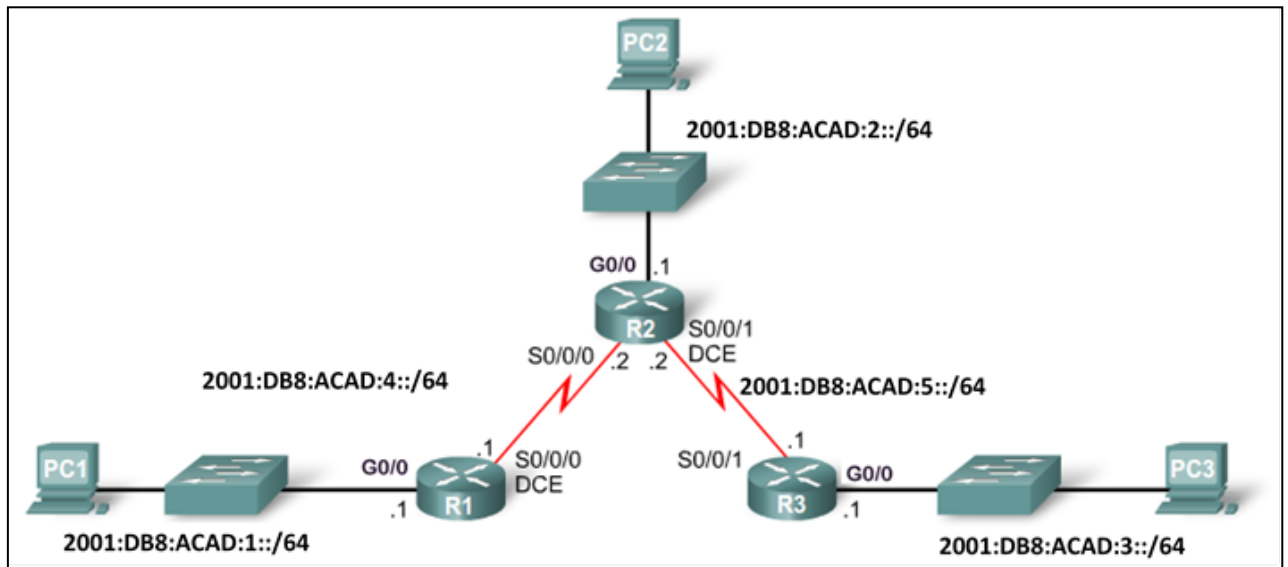
- **Сценарий 3**

Данные от маршрутизатора R2 направляются по статическому маршруту IPv6 по умолчанию через интерфейс S0/0/1 на адрес следующего перехода на маршрутизаторе R3.

По завершении объединитесь с другой группой и сравните свои письменные ответы. Обсудите найденные отличия.

Ресурсы

Диаграмма топологии



- **Scenario 1**

Статический маршрут IPv6 по умолчанию, направляющий все данные от R2 на адрес следующего перехода на R1.

Команда конфигурации	IPv6-сеть, требующая маршрутизации	IPv6-адрес следующего перехода
R2 (config) # ipv6 route		

- **Сценарий 2**

Статический маршрут IPv6 по умолчанию, направляющий все данные от R3 на адрес следующего перехода на R2.

Команда конфигурации	IPv6-сеть, требующая маршрутизации	IPv6-адрес следующего перехода
R3 (config) # ipv6 route		

- **Сценарий 3**

Статический маршрут IPv6 по умолчанию, направляющий все данные от R2 на адрес следующего перехода на R3.

Команда конфигурации	IPv6-сеть, требуемая маршрутизации	IPv6-адрес следующего перехода
R2 (config) # ipv6 route		

Справка для преподавателя

- **Scenario 1**

Статический маршрут IPv6 по умолчанию, направляющий все данные от R2 на адрес следующего перехода на R1.

Команда конфигурации	IPv6-сеть, требуемая маршрутизации	IPv6-адрес следующего перехода
R2 (config) # ipv6 route	::/0	2001:DB8:ACAD:4::1

- **Сценарий 2**

Статический маршрут IPv6 по умолчанию, направляющий все данные от R3 на адрес следующего перехода на R2.

Команда конфигурации	IPv6-сеть, требуемая маршрутизации	IPv6-адрес следующего перехода
R3 (config) # ipv6 route	::/0	2001:DB8:ACAD:5::2

- **Сценарий 3**

Статический маршрут IPv6 по умолчанию, направляющий все данные от R2 на адрес следующего перехода на R3.

Команда конфигурации	IPv6-сеть, требуемая маршрутизации	IPv6-адрес следующего перехода
R2 (config) # ipv6 route	::/0	2001:DB8:ACAD:5::1

Укажите элементы модели, которые соответствуют сфере ИТ.

- IPv6-адрес
- Адрес следующего перехода
- Выходной интерфейс
- Маршрутом по умолчанию
- Статический маршрут

Практическая работа 10. Настройка протоколов RIPv2 и RIPvng

Топология

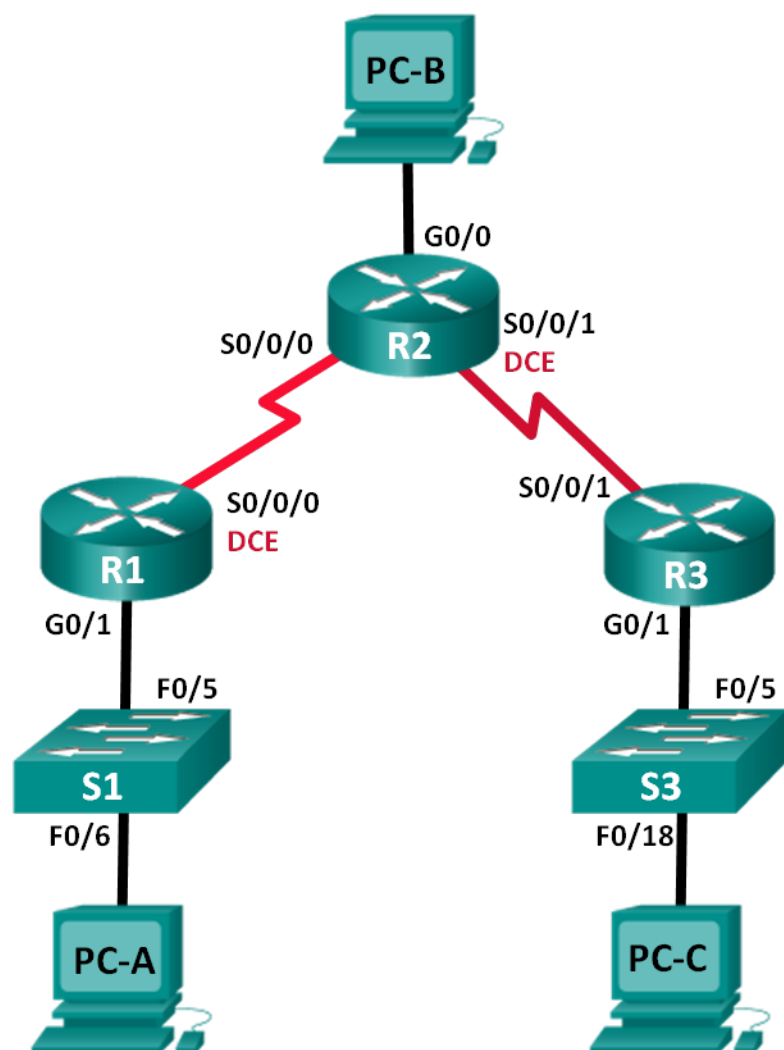


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	172.30.10.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	G0/0	209.165.201.1	255.255.255.0	N/A
	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
R3	G0/1	172.30.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	N/A	VLAN 1	N/A	N/A
S3	N/A	VLAN 1	N/A	N/A
PC-A	NIC	172.30.10.3	255.255.255.0	172.30.10.1
PC-B	NIC	209.165.201.2	255.255.255.0	209.165.201.1
PC-C	NIC	172.30.30.3	255.255.255.0	172.30.30.1

Цели занятия:

Часть 1. Построение сети и настройка базовых параметров устройства

Часть 2. Настройка и проверка маршрутизации RIPv2

- Настройте и проверьте работу маршрутизации RIPv2 на маршрутизаторах.
- Настройте пассивный интерфейс.
- Изучите таблицы маршрутизации.
- Отключите автоматическое суммирование маршрутов.
- Настройте маршрут по умолчанию.
- Проверьте наличие сквозного соединения.

Часть 3. Настройка протокола IPv6 на устройствах

Часть 4. Настройка и проверка маршрутизации RIPvng

- Настройте и проверьте работу маршрутизации RIPvng на маршрутизаторах.
- Изучите таблицы маршрутизации.
- Настройте маршрут по умолчанию.
- Проверьте наличие сквозного соединения.

Формируемые компетенции: ПК-1; ПК-2

Исходные данные/сценарий

Протокол RIP версии 2 (RIPv2) используется для маршрутизации IPv4-адресов в небольших сетях. RIPv2 — это бесклассовый протокол маршрутизации на базе векторов расстояния, определённый в RFC 1723. Поскольку RIPv2 является бесклассовым протоколом маршрутизации, маски подсетей включены в обновления маршрутизации. По умолчанию протокол RIPv2 автоматически суммирует сети на границах сети. После отключения функции автоматического суммирования протокол RIPv2 прекращает суммирование сетей по их классовому адресу на пограничных

маршрутизаторах.

RIPng (RIP следующего поколения) — это протокол маршрутизации на базе векторов расстояния для маршрутизации IPv6-адресов, определённый в RFC 2080. RIPng основан на RIPv2, у него такое же административная дистанция и ограничение по максимальному количеству переходов — 15.

В данной Практической работе необходимо настроить топологию сети с использованием маршрутизации RIPv2, отключить автоматическое суммирование, указать маршрут по умолчанию и использовать команды CLI для отображения и проверки сведений о маршрутизации RIP. Затем нужно настроить топологию сети с IPv6-адресами, настроить RIPng, распространить маршрут по умолчанию и использовать команды CLI для отображения и проверки сведений о маршрутизации RIPng.

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 Практической 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 Практической 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);
- 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 3: Построение сети и настройка базовых параметров устройства

В части 1 вам предстоит создать топологию сети и настроить основные параметры.

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

Step 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Step 3: Настройте основные параметры на каждом маршрутизаторе и коммутаторе.

- а. Отключите поиск DNS.
- б. Настройте имена устройств в соответствии с топологией.
- в. Настройте шифрование пароля.
- г. Назначьте **class** в качестве пароля привилегированного режима EXEC.

- e. Назначьте **cisco** в качестве паролей консоли и VTY.
- f. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.
- g. Настройте **logging synchronous** для консольного канала.
- h. Назначьте IP-адреса всем интерфейсам в соответствии с таблицей адресации.
- i. Для каждого интерфейса настройте описание с IP-адресом.
- j. Если возможно, установите значение тактовой частоты для последовательных интерфейсов DCE.
- k. Скопируйте текущую конфигурацию в загрузочную конфигурацию.

Step 4: Настройте узлы ПК.

Адреса узлов ПК можно посмотреть в таблице адресации.

Step 5: Проверка соединения.

На данный момент компьютеры не могут отправлять друг другу эхо-запросы.

- a. Каждая рабочая станция должна иметь возможность выполнять успешный эхо-запрос подключённого маршрутизатора. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.
- b. Маршрутизаторы должны иметь возможность отправлять успешные эхо-запросы друг другу. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

Часть 4: Настройка и проверка маршрутизации RIPv2

В части 2 вам предстоит настроить маршрутизацию RIPv2 на всех маршрутизаторах в сети, а затем убедиться, что таблицы маршрутизации обновляются правильно. После проверки RIPv2 вам предстоит отключить автоматическое суммирование, настроить маршрут по умолчанию и проверить сквозное соединение.

Step 1: Настройте маршрутизацию по протоколу RIPv2.

- a. На маршрутизаторе R1 настройте RIPv2 в качестве протокола маршрутизации и объявите соответствующие сети.

```
R1# config t
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# passive-interface g0/1
R1(config-router)# network 172.30.0.0
R1(config-router)# network 10.0.0.0
```

Команда **passive-**

interface прекращает отправку обновлений маршрутизации из указанного интерфейса. Данный процесс предотвращает нежелательную отправку маршрутизирующей информации в локальную сеть. Тем не менее, сеть, к которой относится указанный интерфейс, по-прежнему объявляется в обновлениях маршрутизации, которые отправляются из других интерфейсов.

- b. Настройте протокол RIPv2 на маршрутизаторе R3 и используйте команду **network**, чтобы добавить соответствующие сети и предотвратить обновления

маршрутизации в интерфейсе локальной сети.

- с. Настройте протокол RIPv2 на маршрутизаторе R2. Не объявляйте сеть 209.165.201.0.

Примечание. Не обязательно делать интерфейс G0/0 на маршрутизаторе R2 пассивным, поскольку сеть, связанная с этим интерфейсом, не объявляется.

Step 2: Проверьте текущее состояние сети.

- а. Состояние двух последовательных каналов можно легко проверить, выполнив команду **show ip interface brief** на маршрутизаторе R2.

```
R2# show ip interface brief
Interface                               IP-Address      OK? Method
Status                                 Protocol
Embedded-Service-Engine0/0            unassigned      YES  unset
administratively down down
GigabitEthernet0/0                     209.165.201.1   YES  manual up
up
GigabitEthernet0/1                     unassigned      YES  unset
administratively down down
Serial0/0/0                            10.1.1.2        YES  manual up
up
Serial0/0/1                            10.2.2.2        YES  manual up
up
```

- б. Проверьте наличие подключения между компьютерами.

Успешно ли отправляется эхо-запрос от узла PC-A на PC-B? _____ Почему?

Успешно ли проходит эхо-запрос с PC-A на PC-C? _____ Почему?

Успешно ли проходит эхо-запрос с узла PC-C на PC-B? _____ Почему?

Успешно ли проходит эхо-запрос с узла PC-C на PC-A? _____ Почему?

- с. Убедитесь в том, что протокол RIPv2 активирован на маршрутизаторах.

Чтобы проверить это, можно использовать команды **debug ip rip**, **show ip protocols** и **show run**. Выходные данные команды **show ip protocols** для маршрутизатора R1 показаны ниже.

```
R1# show ip protocols
Routing Protocol is "rip"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Sending updates every 30 seconds, next due in 7 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Redistributing: rip
```

```

Default version control: send version 2, receive 2
Interface          Send  Recv  Triggered RIP  Key-
chain
Serial0/0/0        2      2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
  GigabitEthernet0/1
Routing Information Sources:
  Gateway          Distance          Last Update
  10.1.1.2          120
Distance: (default is 120)

```

Какие сведения подтверждают работу RIPv2 при выполнении команды **debug ip rip** на маршрутизаторе R2?

Изучив выходные данные отладки, в командной строке привилегированного режима выполните команду **undebug all**.

Какие сведения подтверждают работу RIPv2 при выполнении команды **show run** на маршрутизаторе R3?

- d. Отключите автоматическое суммирование маршрутов.

Локальные сети, подключённые к маршрутизаторам R1 и R3, состоят из "разорванных" сетей. Маршрутизатор R2 отображает в таблице маршрутизации два пути к сети 172.30.0.0/16, имеющие одинаковую стоимость. Маршрутизатор R2 отображает только адрес главной классовой сети 172.30.0.0, но не отображает подсети этой сети.

R2# **show ip route**

<Output omitted>

```

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
R       172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:23,
Serial0/0/1
                        [120/1] via 10.1.1.1, 00:00:09,
Serial0/0/0
209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/24 is directly connected,
GigabitEthernet0/0
L       209.165.201.1/32 is directly connected,
GigabitEthernet0/0

```

Маршрутизатор R1 отображает только собственные подсети сети 172.30.0.0. В таблице маршрутизации R1 не содержатся маршруты для подсетей 172.30.0.0 маршрутизатора R3.

R1# **show ip route**

```
<Output omitted>
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:21,
Serial0/0/0
      172.30.0.0/16 is variably subnetted, 2 subnets, 2
masks
C       172.30.10.0/24 is directly connected,
GigabitEthernet0/1
L       172.30.10.1/32 is directly connected,
GigabitEthernet0/1
```

Маршрутизатор R3 отображает только собственные подсети сети 172.30.0.0. В таблице маршрутизации R3 не содержатся маршруты для подсетей 172.30.0.0 маршрутизатора R1.

R3# **show ip route**

```
<Output omitted>
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:23,
Serial0/0/1
      172.30.0.0/16 is variably subnetted, 2 subnets, 2
masks
C       172.30.30.0/24 is directly connected,
GigabitEthernet0/1
L       172.30.30.1/32 is directly connected,
GigabitEthernet0/1
```

Чтобы определить маршруты, полученные в обновлениях RIP от маршрутизатора R3, используйте команду **debug ip rip** на маршрутизаторе R2. Укажите их далее.

Маршрутизатор R3 не передаёт какие-либо подсети 172.30.0.0, только суммарный маршрут 172.30.0.0/16, включая маску подсети. Поэтому таблицы маршрутизации на R1 и R2 не отображают подсети 172.30.0.0 на R3.

Step 3: Отключите автоматическое суммирование маршрутов.

- a. Для отключения автоматического суммирования в RIPv2 используется команда **no auto-summary**. Отключите автоматическое суммирование на всех маршрутизаторах. Маршрутизаторы больше не суммируют маршруты на границах главной классовой сети. Маршрутизатор R1 приведён здесь в качестве примера.

```
R1(config)# router rip
R1(config-router)# no auto-summary
```

- b. Чтобы очистить таблицу маршрутизации, используйте команду **clear ip route ***.

```
R1(config-router)# end
R1# clear ip route *
```

- c. Изучите таблицы маршрутизации. Не забывайте, что для сходимости таблиц после того, как они были очищены, требуется некоторое время.

Подсети LAN, подключённые к маршрутизаторам R1 и R3, должны быть включены во все три таблицы маршрутизации.

```
R2# show ip route
```

<Output omitted>

Gateway of last resort is not set

```

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
R       172.30.0.0/16 [120/1] via 10.2.2.1, 00:01:01,
Serial0/0/1
[120/1] via 10.1.1.1, 00:01:15, Serial0/0/0
R       172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:21,
Serial0/0/0
R       172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:04,
Serial0/0/1
      209.165.201.0/24 is variably subnetted, 2 subnets, 2
masks
C       209.165.201.0/24 is directly connected,
GigabitEthernet0/0
L       209.165.201.1/32 is directly connected,
GigabitEthernet0/0
```

```
R1# show ip route
```

<Output omitted>

Gateway of last resort is not set

```

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:12,
Serial0/0/0
172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.30.10.0/24 is directly connected,
GigabitEthernet0/1
L       172.30.10.1/32 is directly connected,
GigabitEthernet0/1
R       172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:12,
Serial0/0/0
```

```
R3# show ip route
```

<Output omitted>

```

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:23,
```

```

Serial0/0/1
    172.30.0.0/16 is variably subnetted, 2 subnets, 2
masks
C        172.30.30.0/24 is directly connected,
GigabitEthernet0/1
L        172.30.30.1/32 is directly connected,
GigabitEthernet0/1
R        172.30.10.0 [120/2] via 10.2.2.2, 00:00:16,
Serial0/0/1

```

- d. Чтобы просмотреть обновления RIP, на маршрутизаторе R2 используйте команду **debug ip rip**.

R2# debug ip rip

Через 60 секунд выполните команду **no debug ip rip**.

Какие маршруты содержатся в обновлениях RIP, принятых от R3?

Включены ли маски подсети в обновления маршрутизации? _____

Step 4: Настройте и перераспределите маршрут по умолчанию для получения доступа к Интернету.

- a. На маршрутизаторе R2 создайте статический маршрут к сети 0.0.0.0 0.0.0.0 с помощью команды **ip route**. После выполнения этой команды любой трафик, направленный на неизвестный адрес назначения, пересылается на интерфейс G0/0 маршрутизатора R2. Интернет моделируется путём настройки шлюза «последней надежды» на маршрутизаторе R2.

R2(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.2**

- b. Маршрутизатор R2 объявит маршрут для других маршрутизаторов, если команда **default-information originate** будет добавлена в его конфигурацию RIP.

R2(config)# **router rip**

R2(config-router)# **default-information originate**

Step 5: Выполните проверку настройки маршрутизации.

- a. Просмотрите таблицу маршрутизации маршрутизатора R1.

R1# **show ip route**

<Output omitted>

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

```

R*      0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
        10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
R        10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:13,
Serial0/0/0
        172.30.0.0/16 is variably subnetted, 3 subnets, 2
masks
C        172.30.10.0/24 is directly connected,
GigabitEthernet0/1
L        172.30.10.1/32 is directly connected,

```

```
GigabitEthernet0/1
R      172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:13,
Serial0/0/0
```

Как на основании таблицы маршрутизации можно определить, что сеть, разбитая на подсети и используемая маршрутизаторами R1 и R3, имеет путь для интернет-трафика?

- b. Просмотрите таблицу маршрутизации на R2.

Каким образом путь для интернет-трафика появился в таблице маршрутизации маршрутизатора R2?

Step 6: Проверка соединения.

- a. Смоделируйте отправку трафика в Интернет, отправив эхо-запросы от узла PC-A и PC-C в сеть 209.165.201.2.

Успешно ли выполнен эхо-запрос? _____

- b. Убедитесь в том, что узлы в разбитой на подсети сети могут достичь друг друга. Для этого выполните эхо-запрос между узлами PC-A и PC-C.

Успешно ли выполнен эхо-запрос? _____

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

Часть 5: Настройка протокола IPv6 на устройствах

В части 3 вам предстоит настроить IPv6-адреса на всех интерфейсах и проверить подключение.

Таблица адресации

Устройство	Интерфейс	IPv6-адрес/длина префикса	Шлюз по умолчанию
R1	G0/1	2001:DB8:ACAD:A::1/64 FE80::1 локальный канал	Недоступно
	S0/0/0	2001:DB8:ACAD:12::1/64 FE80::1 локальный канал	Недоступно
R2	G0/0	2001:DB8:ACAD:B::2/64 FE80::2 локальный канал	Недоступно
	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2 локальный канал	Недоступно
	S0/0/1	2001:DB8:ACAD:23::2/64 FE80::2 локальный канал	Недоступно
R3	G0/1	2001:DB8:ACAD:C::3/64 FE80::3 локальный канал	Недоступно
	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 локальный канал	Недоступно
PC-A	NIC	2001:DB8:ACAD:A::A/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::B/64	FE80::2
PC-C	NIC	2001:DB8:ACAD:C::C/64	FE80::3

Step 1: Настройте узлы ПК.

Адреса узлов ПК можно посмотреть в таблице адресации.

Step 2: Настройте протокол IPv6 на маршрутизаторах.

Примечание. Назначение IPv6-адреса в дополнение к IPv4-адресу на интерфейсе называют двойным стеком. Подобное название определено тем, что оба стека протоколов IPv4 и IPv6 активны.

- Назначьте глобальный и локальный адрес канала каждому интерфейсу маршрутизатора, используя данные из таблицы адресации.
- Включите IPv6-маршрутизацию на каждом маршрутизаторе.
- Введите соответствующую команду, чтобы проверить IPv6-адреса и состояние канала. Запишите команду в строке ниже.

- Каждая рабочая станция должна иметь возможность выполнять успешный эхо-запрос подключённого маршрутизатора. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.
- Маршрутизаторы должны иметь возможность отправлять успешные эхо-запросы друг другу. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

Часть 6: Настройка и проверка маршрутизации RIPng

В части 4 вам предстоит настроить маршрутизацию RIPng на всех маршрутизаторах, убедиться в том, что таблицы маршрутизации обновляются верным образом, настроить и распространить маршрут по умолчанию и проверить сквозное соединение.

Step 1: Настройте маршрутизацию RIPng.

При использовании IPv6 на каждом интерфейсе обычно настроено несколько IPv6-адресов. Команда `network` не используется в RIPng. Вместо этого на уровне интерфейса включается маршрутизация RIPng и определяется локально-значимым именем процесса, в виду того, что RIPng может создавать множество процессов.

- a. Для каждого интерфейса на маршрутизаторе R1, который должен участвовать в маршрутизации RIPng, выполните команду **ipv6 rip Test1 enable**, где **Test1** является локально-значимым именем процесса.

```
R1(config)# interface g0/1
R1(config)# ipv6 rip Test1 enable
R1(config)# interface s0/0/0
R1(config)# ipv6 rip Test1 enable
```

- b. Настройте RIPng для последовательных интерфейсов на маршрутизаторе R2 с **Test2** в качестве имени процесса. Интерфейс G0/0 не следует настраивать подобным образом.
- c. Настройте RIPng для всех интерфейсов на маршрутизаторе R3 с **Test3** в качестве имени процесса.
- d. Убедитесь, что RIPng работает на маршрутизаторах.

Для проверки RIPng можно использовать команды **show ipv6 protocols**, **show run**, **show ipv6 rip database** и **show ipv6 rip имя процесса**. На маршрутизаторе R1 выполните команду **show ipv6 protocols**.

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip Test1"
  Interfaces:
    Serial0/0/0
    GigabitEthernet0/1
  Redistribution:
    None
```

Каким образом протокол RIPng указан в выходных данных?

- e. Выполните команду **show ipv6 rip Test1**.

```
R1# show ipv6 rip Test1
RIP process "Test1", port 521, multicast-group FF02::9, pid
314
  Administrative distance is 120. Maximum paths is 16
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
  Periodic updates 1, trigger updates 0
  Full Advertisement 0, Delayed Events 0
  Interfaces:
    GigabitEthernet0/1
    Serial0/0/0
```

Redistribution:
None

Что общего между протоколами RIPv2 и RIPv6?

- f. Просмотрите таблицу маршрутизации IPv6 каждого маршрутизатора. В строке ниже запишите команду, используемую для просмотра таблицы маршрутизации.

Сколько маршрутов было получено с помощью протокола RIPv6 на маршрутизаторе R1? _____

Сколько маршрутов было получено с помощью протокола RIPv6 на маршрутизаторе R2? _____

Сколько маршрутов было получено с помощью протокола RIPv6 на маршрутизаторе R3? _____

- g. Проверьте наличие подключения между компьютерами.

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

Успешно ли проходит эхо-запрос с PC-A на PC-C? _____

Успешно ли проходит эхо-запрос с узла PC-C на PC-B? _____

Успешно ли проходит эхо-запрос с узла PC-C на PC-A? _____

Почему некоторые эхо-запросы были выполнены успешно, а другие нет?

Step 2: Настройте и распространите маршрут по умолчанию.

- a. На маршрутизаторе R2 создайте статический маршрут по умолчанию к сети ::0/64 с помощью команды **ipv6 route** и IP-адреса выходного интерфейса G0/0. Выполнение команды пересылает любой трафик с неизвестным адресом назначения из интерфейса G0/0 маршрутизатора R2 по направлению к PC-B, моделируя работу Интернета. Ниже напишите команду, которую вы использовали.

- b. Статические маршруты могут быть включены в обновления RIPv6 с помощью команды **ipv6 rip имя-процесса default-information originate** в режиме конфигурации интерфейса. Настройте отправку маршрута по умолчанию в обновлениях RIPv6 из последовательных каналов маршрутизатора R2.

```
R2(config)# int s0/0/0
```

```
R2(config-rtr)# ipv6 rip Test2 default-information  
originate
```

```
R2(config)# int s0/0/1
```

```
R2(config-rtr)# ipv6 rip Test2 default-information  
originate
```

Step 3: Выполните проверку настройки маршрутизации.

- a. Просмотрите таблицу маршрутизации IPv6 маршрутизатора R2.

```
R2# show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B -
BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS
- ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
        D - EIGRP, EX - EIGRP external
S   ::/64 [1/0]
via 2001:DB8:ACAD:B::B
R   2001:DB8:ACAD:A::/64 [120/2]
    via FE80::1, Serial0/0/0
C   2001:DB8:ACAD:B::/64 [0/0]
    via ::, GigabitEthernet0/1
L   2001:DB8:ACAD:B::2/128 [0/0]
    via ::, GigabitEthernet0/1
R   2001:DB8:ACAD:C::/64 [120/2]
    via FE80::3, Serial0/0/1
C   2001:DB8:ACAD:12::/64 [0/0]
    via ::, Serial0/0/0
L   2001:DB8:ACAD:12::2/128 [0/0]
    via ::, Serial0/0/0
C   2001:DB8:ACAD:23::/64 [0/0]
    via ::, Serial0/0/1
L   2001:DB8:ACAD:23::2/128 [0/0]
    via ::, Serial0/0/1
L   FF00::/8 [0/0]
    via ::, Null0
```

Как на основании данных в таблице маршрутизации можно определить, что маршрутизатор R2 имеет путь для интернет-трафика?

- b. Просмотрите таблицы маршрутизации на маршрутизаторах R1 и R3.

Каким образом обеспечивается путь для интернет-трафика в таблицах маршрутизации R1 и R3?

Step 4: Проверка соединения.

Смоделируйте отправку трафика в Интернет, отправив эхо-запрос от узла PC-A и PC-C к адресу 2001:DB8:ACAD:B::B/64.

Успешно ли выполнен эхо-запрос? _____

Вопросы на закрепление

1. Зачем может потребоваться выключение автоматического суммирования при работе RIPv2?

2. Каким образом маршрутизаторы R1 и R3 узнали путь в Интернет?

3. В чём заключаются различия в настройке протоколов RIPv2 и RIPv6?

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.

Список литературы, рекомендуемый к использованию по данной теме:

Основная: 1-3

Дополнительная: 1-8

Методическая: 1

Интернет-ресурсы: 1

Практическая работа 11. Настройка и проверка стандартных списков контроля доступа для IPv4

Топология

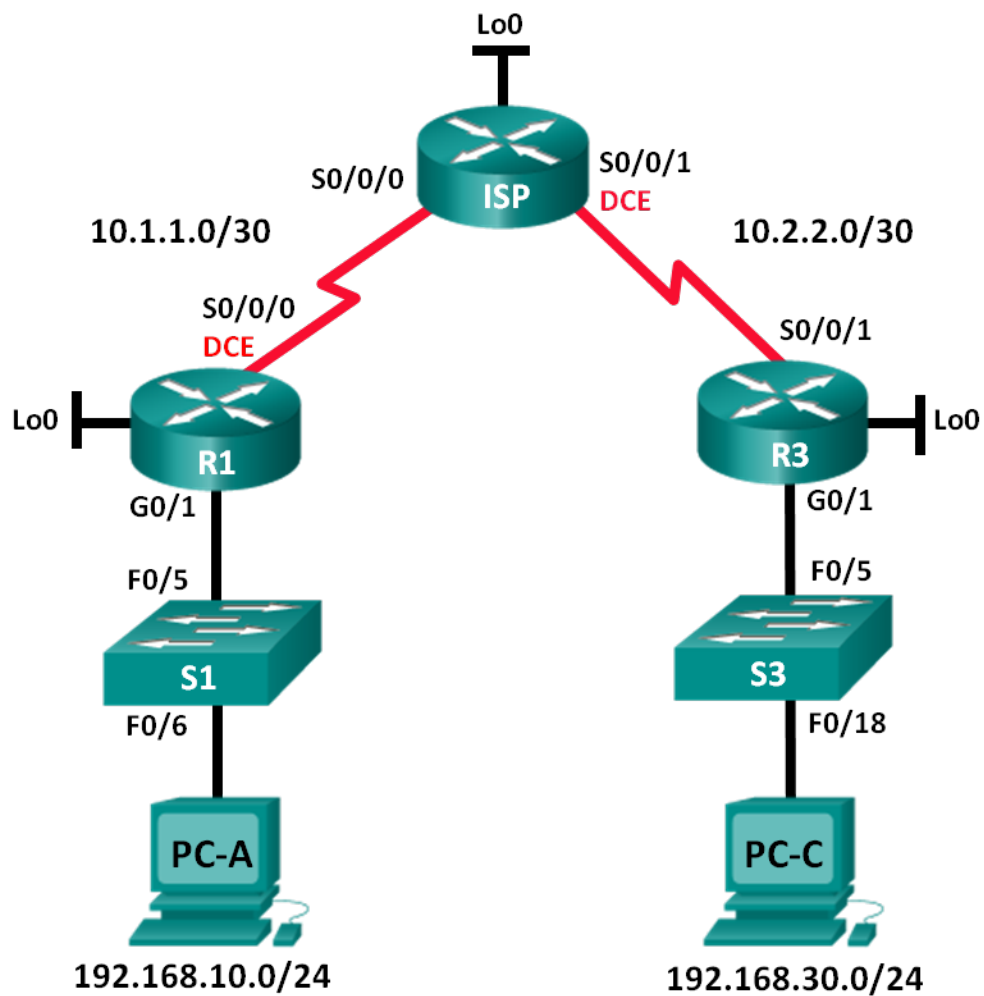


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.10.1	255.255.255.0	—
	Lo0	192.168.20.1	255.255.255.0	—
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	—
ISP	S0/0/0	10.1.1.2	255.255.255.252	—
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	—
	Lo0	209.165.200.225	255.255.255.224	—
R3	G0/1	192.168.30.1	255.255.255.0	—
	Lo0	192.168.40.1	255.255.255.0	—
	S0/0/1	10.2.2.1	255.255.255.252	—
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 инициализация устройств**

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

Часть 2. Настройка устройств и проверка подключения

- Назначьте компьютерам статический IP-адрес.
- Настройте базовые параметры на маршрутизаторах.
- Настройте базовые параметры на коммутаторах.
- Настройте маршрутизацию RIP 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.

Общие сведения/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 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. Правильные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

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

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель)
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 2 ПК (Windows 7, Vista или XP с программой эмуляции терминалов, например, Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet и последовательные кабели согласно топологии

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: Создайте сеть согласно топологии.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов 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.

- Подключитесь к маршрутизатору с помощью консоли и перейдите в режим глобальной настройки.
- Скопируйте приведенную ниже базовую конфигурацию и вставьте ее в текущую конфигурацию на маршрутизаторе.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```
- Присвойте имена устройствам в соответствии с топологией.
- Создайте интерфейсы loopback на каждом маршрутизаторе в соответствии с таблицей адресации.
- Настройте IP-адреса интерфейсов в соответствии с топологией и таблицей адресации.
- Установите тактовую частоту на **128000** для всех последовательных интерфейсов DCE.
- Разрешите доступ по Telnet.

- h. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 3: Настройка базовых параметров на коммутаторах (дополнительно).

- a. Подключитесь к коммутатору с помощью консоли и перейдите в режим глобального конфигурирования.
- b. Скопируйте приведенную ниже базовую конфигурацию и вставьте ее в файл текущей конфигурации на коммутаторе.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```
- c. Присвойте имена устройствам в соответствии с топологией.
- d. Назначьте административный IP-адрес интерфейса в соответствии с таблицами топологии и адресации.
- e. Настройка шлюза по умолчанию.
- f. Разрешите доступ по Telnet.
- g. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте маршрутизацию RIP на маршрутизаторах R1, ISP и R3.

- a. Настройте протокол RIP версии 2 и анонсируйте все сети на маршрутизаторах R1, ISP и R3. Конфигурация RIP для маршрутизаторов R1 и ISP приведена в справочных целях.

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.10.0
R1(config-router)# network 192.168.20.0
R1(config-router)# network 10.1.1.0

ISP(config)# router rip
ISP(config-router)# version 2
ISP(config-router)# network 209.165.200.224
ISP(config-router)# network 10.1.1.0
ISP(config-router)# network 10.2.2.0
```
- b. После настройки RIP на маршрутизаторах R1, ISP и R3 убедитесь, что все маршрутизаторы имеют заполненные таблицы маршрутизации со всеми 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 применен 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
```

- 2) 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
Выходные данные опущены
```

- 3) 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 выполнена проверка связи? _____ **Да**
- 4) 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 выполнена проверка связи? _____ **Да**

```
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 192.168.30.3
```

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 разрешен 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 чем 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
<Данные опущены>
```

- 3) Проверьте работу ACL-списка. Из командной строки узла PC-C отправьте эхо-запрос на IP-адрес узла PC-A. Успешно ли выполнена проверка связи? \_\_\_\_\_
- 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 выполнена проверка связи? \_\_\_\_\_
- 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 выполнена проверка связи? \_\_\_\_\_

## Часть 4: Изменение стандартного ACL-списка

Политика безопасности нередко претерпевает изменения. По этой причине ACL-списки тоже необходимо изменять. В части 4 необходимо изменить один из ранее настроенных списков контроля доступа 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 удален, 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 определенных строк в списках ACL нет ничего сложного.

**Примечание.** В ходе данной лабораторной работы используйте вариант 2.

### Шаг 1: Изменение стандартного именованного ACL-списка.

- a. На маршрутизаторе R1 в исполнительском режиме EXEC 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)
```

- b. 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
```

- c. 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 loopback-адрес 0 на ISP в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A. Успешно ли выполнена проверка связи? \_\_\_\_\_

## Вопросы для повторения

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 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 (S0/1/0)          | 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)          |
| <b>Примечание.</b> 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 12. Настройка и проверка ACL-списков для IPv6

## Топология

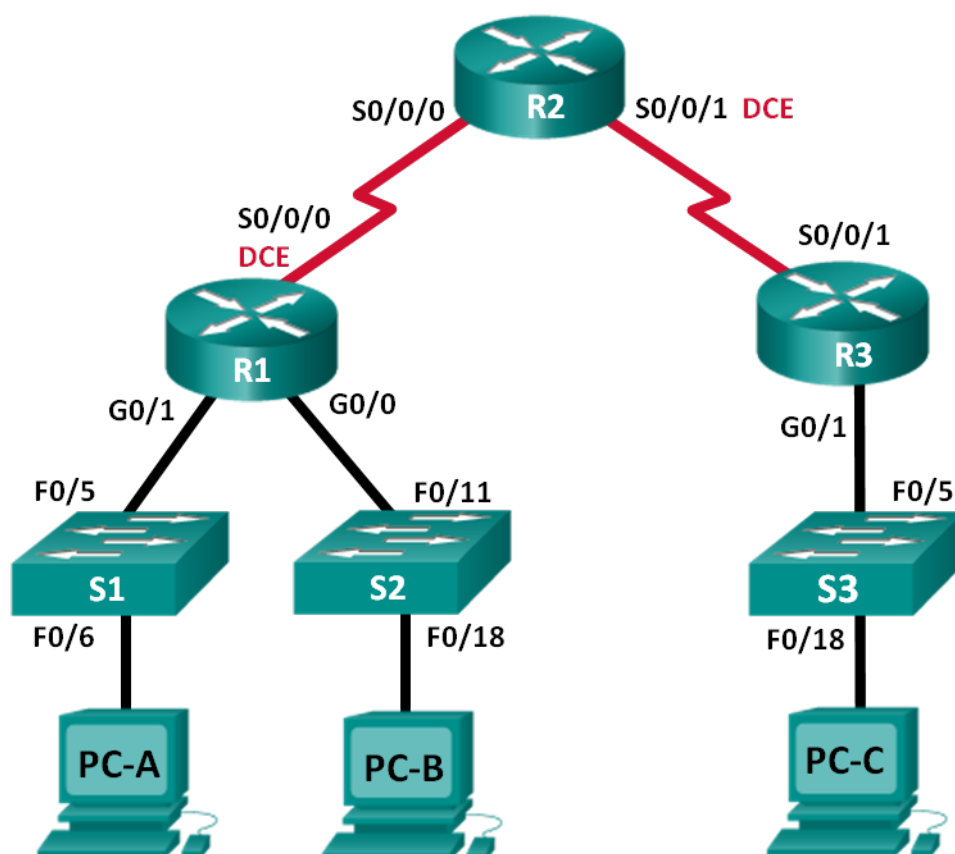


**Таблица адресации**

| Устройство | Интерфейс    | IP-адрес              | Шлюз по умолчанию |
|------------|--------------|-----------------------|-------------------|
| R1         | G0/0         | 2001:DB8:ACAD:B::1/64 | N/A               |
|            | G0/1         | 2001:DB8:ACAD:A::1/64 | N/A               |
|            | S0/0/0 (DCE) | 2001:DB8:AAAA:1::1/64 | N/A               |
| R2         | S0/0/0       | 2001:DB8:AAAA:1::2/64 | N/A               |
|            | S0/0/1 (DCE) | 2001:DB8:AAAA:2::2/64 | N/A               |
| R3         | G0/1         | 2001:DB8:CAFE:C::1/64 | N/A               |
|            | S0/0/1       | 2001:DB8:AAAA:2::1/64 | N/A               |
| S1         | VLAN1        | 2001:DB8:ACAD:A::A/64 | N/A               |
| S2         | VLAN1        | 2001:DB8:ACAD:B::A/64 | N/A               |
| S3         | VLAN1        | 2001:DB8:CAFE:C::A/64 | N/A               |
| PC-A       | NIC          | 2001:DB8:ACAD:A::3/64 | FE80::1           |
| PC-B       | NIC          | 2001:DB8:ACAD:B::3/64 | FE80::1           |
| PC-C       | NIC          | 2001:DB8:CAFE:C::3/64 | FE80::1           |

**Цели занятия:**

**Часть 1. Настройка топологии и установка исходного состояния устройства**

**Часть 2. Конфигурация устройств и проверка подключения**

**Часть 3. Настройка и проверка ACL-списков для IPv6**

**Часть 4. Редактирование ACL-списков для IPv6**

**Формируемые компетенции:** ПК-1; ПК-2

**Исходные данные/сценарий**

Фильтрация IPv6-трафика путём создания ACL-списков для IPv6 и их применения на интерфейсах аналогична способу, по которому вы создавали именованные ACL-списки для IPv4. В IPv6 определены расширенные и именованные ACL-списки. Стандартные и нумерованные ACL-списки больше не используются для IPv6. Чтобы применить ACL-список IPv6 на интерфейсе vty, следует использовать новую команду **ipv6 traffic-filter**. Команда **ipv6 access-class** до сих пор используется для применения ACL-списков IPv6 на интерфейсах.

В рамках Практической работы вам предстоит применить правила фильтрации IPv6, а затем убедиться в правильной работе списков для ограничения доступа. Также вам нужно будет внести изменения в ACL-список IPv6 и очистить счётчики совпадений.

**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 Практической 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 Практической 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 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 и последовательные кабели в соответствии с топологией.

#### **Часть 7: Настройка топологии и инициализация устройств**

В первой части Практической работы вам нужно настроить топологию сети и при необходимости удалить все конфигурации.

**Step 1: Подключите кабели в сети в соответствии с топологией.**

**Step 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.**

#### **Часть 8: Настройка устройств и проверка подключения**

Во второй части вам предстоит настроить базовые параметры маршрутизаторов, коммутаторов и компьютеров. Имена и адреса устройств можно найти в топологии и таблице адресации в начале этой Практической работы.

**Step 1: Настройте IPv6-адреса на всех ПК.**

Настройте глобальный индивидуальный IPv6-адрес в соответствии с таблицей адресации. Используйте локальный адрес канала **FE80::1** для шлюза по умолчанию на всех ПК.

**Step 2: Настройте коммутаторы.**

- а. Отключите поиск DNS.
- б. Назначьте имя узла.

- c. Назначьте имя домена для **ccna-lab.com**.
- d. Зашифруйте все незашифрованные пароли.
- e. Создайте баннер MOTD, предупреждающий пользователей о том, что неавторизованный доступ запрещён.
- f. Создайте базу данных локального пользователя с именем пользователя **admin** и паролем **classadm**.
- g. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
- h. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.
- i. Активируйте возможность входа на линии VTY с помощью локальной базы данных.
- j. Создайте ключ шифрования RSA для SSH с длиной 1024 бит.
- k. Измените настройку линий VTY transport input на настройку all только для протоколов SSH и Telnet.
- l. Назначьте IPv6-адрес для VLAN 1 в соответствии с таблицей адресации.
- m. От имени администратора отключите все неактивные интерфейсы.

**Step 3: Настройте базовые параметры на всех маршрутизаторах.**

- a. Отключите поиск DNS.
- b. Назначьте имя узла.
- c. Назначьте имя домена для **ccna-lab.com**.
- d. Зашифруйте все незашифрованные пароли.
- e. Создайте баннер MOTD, предупреждающий пользователей о том, что неавторизованный доступ запрещён.
- f. Создайте базу данных локального пользователя с именем пользователя **admin** и паролем **classadm**.
- g. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
- h. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.
- i. Активируйте возможность входа на линии VTY с помощью локальной базы данных.
- j. Создайте ключ шифрования RSA для SSH с длиной 1024 бит.
- k. Измените настройку линий VTY transport input на настройку all только для протоколов SSH и Telnet.

**Step 4: Настройте IPv6-параметры на маршрутизаторе R1.**

- a. Настройте индивидуальный IPv6-адрес на интерфейсах G0/0, G0/1 и S0/0/0.
- b. Настройте локальный IPv6-адрес канала на интерфейсах G0/0, G0/1 и S0/0/0. На всех трёх интерфейсах используйте **FE80:: 1** в качестве локального адреса канала.
- c. На интерфейсе S0/0/0 установите тактовую частоту 128000.
- d. Включите интерфейсы.

- e. Включите IPv6-маршрутизацию одноадресной передачи.
- f. Настройте маршрут IPv6 по умолчанию для использования интерфейса S0/0/0.

```
R1(config)# ipv6 route ::/0 s0/0/0
```

#### Step 5: Настройте параметры IPv6 на маршрутизаторе R2.

- a. Настройте индивидуальный IPv6-адрес на интерфейсах S0/0/0 и S0/0/1.
- b. Настройте локальный IPv6-адрес канала на интерфейсах S0/0/0 и S0/0/1. На обоих интерфейсах используйте **FE80:: 2** в качестве локального адреса канала.
- c. На интерфейсе S0/0/1 установите тактовую частоту со значением 128000.
- d. Включите интерфейсы.
- e. Включите IPv6-маршрутизацию одноадресной передачи.
- f. Настройте статические IPv6-маршруты для маршрутизации трафика на подсети LAN, подключенные к маршрутизаторам R1 и R3.

```
R2(config)# ipv6 route 2001:db8:acad::/48 s0/0/0
```

```
R2(config)# ipv6 route 2001:db8:cafe:c::/64 s0/0/1
```

#### Step 6: Настройте параметры IPv6 на маршрутизаторе R3.

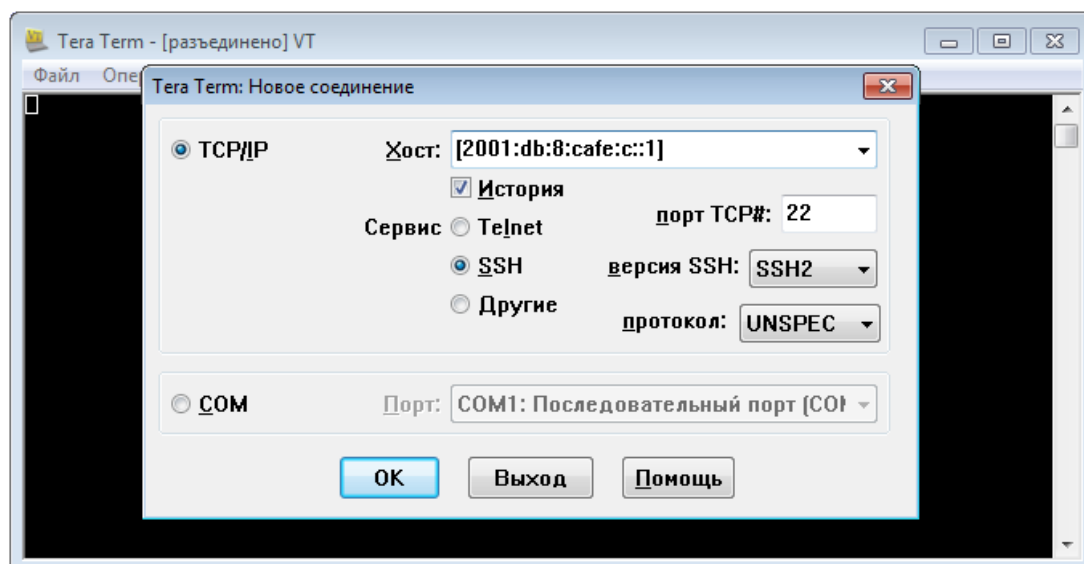
- a. Настройте индивидуальный IPv6-адрес на интерфейсах G0/1 и S0/0/1.
- b. Настройте локальный IPv6-адрес канала на интерфейсах G0/1 и S0/0/1. На обоих интерфейсах используйте **FE80:: 1** в качестве локального адреса канала.
- c. Включите интерфейсы.
- d. Включите IPv6-маршрутизацию одноадресной передачи.
- e. Настройте маршрут IPv6 по умолчанию для использования интерфейса S0/0/1.

```
R3(config)# ipv6 route ::/0 s0/0/1
```

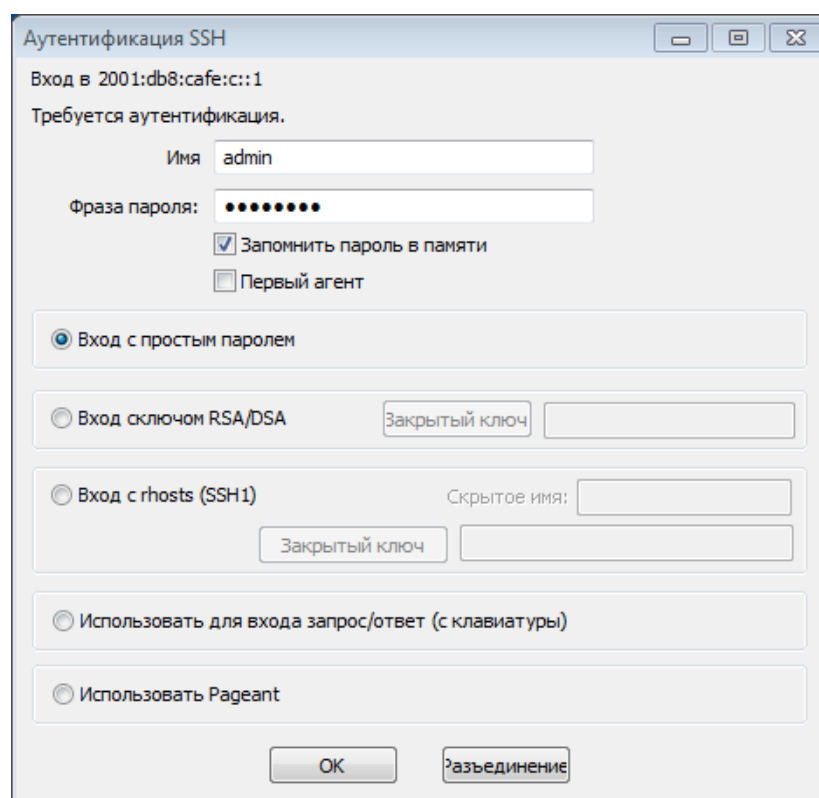
#### Step 7: Проверка соединения.

- a. Все компьютеры должны успешно выполнять эхо-запросы ко всем остальным компьютерам, указанным в топологии.
- b. Подключитесь по Telnet к маршрутизатору R1 со всех компьютеров в топологии.
- c. Подключитесь по SSH к маршрутизатору R1 со всех компьютеров в топологии.
- d. Подключитесь по Telnet к коммутатору S1 со всех компьютеров в топологии.
- e. Подключитесь по SSH к коммутатору S1 со всех компьютеров в топологии.
- f. Теперь выявите и устраните неполадки с подключением, поскольку ACL-списки, которые вы создадите в третьей части Практической работы, ограничат доступ к определённым областям сети.

**Примечание.** В соответствии с требованиями Tera Term IPv6-адрес назначения должен быть в скобках. Введите IPv6-адрес, как показано, нажмите **ОК**, а затем нажмите **Continue (Продолжить)**, чтобы принять предупреждение системы безопасности и подключиться к маршрутизатору.



Введите настроенные учётные данные пользователя (имя пользователя **admin**, пароль **classadm**) и в диалоговом окне SSH Authentication (Аутентификация SSH) выберите **Use plain password to log in (Использовать незашифрованный пароль)**. Для продолжения нажмите кнопку **OK**.



## Часть 9: Настройка и проверка ACL-списков для IPv6

### Step 1: Настройте и проверьте ограничения VTY на маршрутизаторе R1.

- Создайте ACL-список, в соответствии с которым доступ к маршрутизатору R1 через Telnet разрешён только для узлов из сети 2001:db8:acad:a::/64. Все узлы должны обладать доступом к маршрутизатору R1 только через telnet.

```
R1(config)# ipv6 access-list RESTRICT-VTY
```

```
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:a::/64 any
```

```
R1(config-ipv6-acl)# permit tcp any any eq 22
```

- b. Примените ACL-список под именем RESTRICT-VTY на линиях VTY маршрутизатора R1.

```
R1(config-ipv6-acl)# line vty 0 4
R1(config-line)# ipv6 access-class RESTRICT-VTY in
R1(config-line)# end
R1#
```

- c. Отобразите новый ACL-список.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
permit tcp 2001:DB8:ACAD:A::/64 any sequence 10
permit tcp any any eq 22 sequence 20
```

- d. Убедитесь, что ACL-список RESTRICT-VTY пропускает только Telnet-трафик из сети 2001:db8:acad:a::/64.

Каким образом ACL-список RESTRICT-VTY разрешает доступ к маршрутизатору R1 через Telnet только для узлов из сети 2001:db8:acad:a::/64?

---

---

---

---

---

---

---

---

Какую функцию выполняет второе правило permit в ACL-списке RESTRICT-VTY?

---

---

## Step 2: Ограничьте доступ через Telnet к сети 2001:db8:acad:a::/64.

- a. Создайте ACL-список под именем RESTRICTED-LAN, который заблокирует доступ через Telnet к сети 2001:db8:acad:a::/64.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# remark Block Telnet from outside
R1(config-ipv6-acl)# deny tcp any 2001:db8:acad:a::/64 eq telnet
R1(config-ipv6-acl)# permit ipv6 any any
```

- b. Примените ACL-список RESTRICTED-LAN на интерфейсе G0/1 для всего исходящего трафика.

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

- c. Подключитесь по Telnet к коммутатору S1 от узлов PC-B и PC-C, чтобы проверить ограничение Telnet. Подключитесь по SSH к коммутатору S1 от узла PC-B, чтобы убедиться, что к этому узлу по-прежнему можно получить доступ через SSH. При необходимости выявите и устраните любые неполадки.

- d. Используйте команду **show ipv6 access-list**, чтобы просмотреть ACL-список RESTRICTED-LAN.

```
R1# show ipv6 access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
deny tcp any 2001:DB8:ACAD:A::/64 eq telnet (6 matches)
sequence 20
permit ipv6 any any (45 matches) sequence 30
```

Обратите внимание, что каждое правило определяет количество попаданий или совпадений, возникших с момента применения ACL-списка на интерфейсе.

- e. Используйте команду **clear ipv6 access-list**, чтобы сбросить счётчики совпадений для ACL-списка RESTRICTED-LAN.

```
R1# clear ipv6 access-list RESTRICTED-LAN
```

- f. Снова отобразите ACL-список с помощью команды **show access-lists**, чтобы убедиться, что счётчики удалены.

```
R1# show access-lists RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
permit ipv6 any any sequence 30
```

## Часть 10: Редактирование ACL-списков для IPv6

В четвёртой части вам предстоит внести изменения в ACL-список RESTRICTED-LAN, созданный в предыдущей части Практической работы. Перед внесением изменений в ACL-список рекомендуется удалить его из интерфейса, на котором он применён. Завершив редактирование, снова примените ACL-список на интерфейсе.

**Примечание.** Многие сетевые администраторы делают копию ACL-списка и вносят изменения в копии. После изменения копии администратор удаляет старый ACL-список и применяет на интерфейсе отредактированный вариант. Благодаря этому ACL-список можно не удалять, пока отредактированная копия не будет готова для применения.

### Step 1: Удалите ACL-список из интерфейса.

```
R1(config)# int g0/1
R1(config-if)# no ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

### Step 2: Используйте команду show access-lists, чтобы просмотреть ACL-список.

```
R1# show access-lists
IPv6 access list RESTRICT-VTY
permit tcp 2001:DB8:ACAD:A::/64 any (4 matches) sequence 10
permit tcp any any eq 22 (6 matches) sequence 20
IPv6 access list RESTRICTED-LAN
deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
permit ipv6 any any (36 matches) sequence 30
```

### Step 3: Создайте новую запись в ACL-списке, используя последовательную нумерацию.

```
R1(config)# ipv6 access-list RESTRICTED-LAN
R1(config-ipv6-acl)# permit tcp 2001:db8:acad:b::/64 host
```

**2001:db8:acad:a::a eq 23 sequence 15**

Какую функцию выполняет добавленная разрешающая запись permit?

---

**Step 4: Создайте новое правило ACL, вставив его в конец списка.**

```
R1(config-ipv6-acl)# permit tcp any host 2001:db8:acad:a::3
eq www
```

**Примечание.** Данная разрешающая запись используется только для того, чтобы продемонстрировать добавление записи в конец ACL-списка. Для данной строки списка не должно быть совпадений, поскольку предыдущая запись permit совпадает со всем.

**Step 5: Используйте команду show access-lists, чтобы просмотреть изменения ACL-списка.**

```
R1(config-ipv6-acl)# do show access-list
IPv6 access list RESTRICT-VTY
permit tcp 2001:DB8:ACAD:A::/64 any (2 matches) sequence 10
permit tcp any any eq 22 (6 matches) sequence 20
IPv6 access list RESTRICTED-LAN
permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq
telnet sequence 15
deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
permit ipv6 any any (124 matches) sequence 30
permit tcp any host 2001:DB8:ACAD:A::3 eq www sequence 40
```

**Примечание.** Для выполнения любой команды привилегированного режима в режиме глобальной конфигурации или подрежиме можно использовать команду **do**.

**Step 6: Удалите запись ACL-списка.**

Используйте команду **no**, чтобы удалить только что добавленное правило permit.

```
R1(config-ipv6-acl)# no permit tcp any host
2001:DB8:ACAD:A::3 eq www
```

**Step 7: Используйте команду do show access-lists RESTRICTED-LAN, чтобы просмотреть ACL-список.**

```
R1(config-ipv6-acl)# do show access-list RESTRICTED-LAN
IPv6 access list RESTRICTED-LAN
permit tcp 2001:DB8:ACAD:B::/64 host 2001:DB8:ACAD:A::A eq
telnet sequence 15
deny tcp any 2001:DB8:ACAD:A::/64 eq telnet sequence 20
permit ipv6 any any (214 matches) sequence 30
```

**Step 8: Снова примените список ACL RESTRICTED-LAN на интерфейсе G0/1.**

```
R1(config-ipv6-acl)# int g0/1
R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out
R1(config-if)# end
```

**Step 9: Проверьте изменения в ACL-списке.**

От узла PC-B подключитесь к коммутатору S1 по Telnet. При необходимости выявите

и устраните любые неполадки.

### Вопросы на закрепление

1. Из-за чего счётчик совпадений для записи **permit ipv6 any any** списка RESTRICTED-LAN продолжает расти?

---

---

---

---

---

---

---

2. Какую команду следует использовать, чтобы сбросить счётчики для ACL-списка на каналах VTY?

---

---

### Список литературы, рекомендуемый к использованию по данной теме:

*Основная:* 1-3

*Дополнительная:* 1-8

*Методическая:* 1

*Интернет-ресурсы:* 1

*Программное обеспечение:* 1-4

## 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. Настройка динамического и статического NAT

### Топология

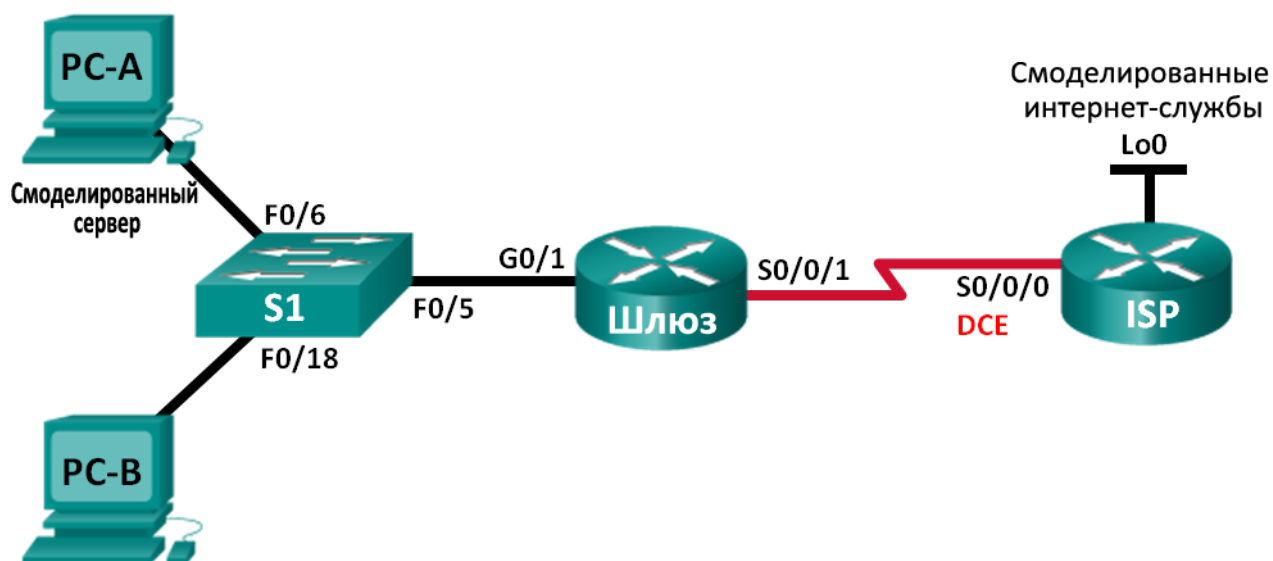


**Таблица адресации**

| 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<br>(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       |

**Цели занятия:**

**Часть 1. Построение сети и проверка подключения**

**Часть 2. Настройка и проверка статического преобразования NAT**

**Часть 3. Настройка и проверка динамического преобразования NAT**

**Время 6 часов**

**Формируемые компетенции: ПК-1; ПК-2**

## 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 IPv4-адресов ограничено.

Согласно сценарию данной Практической 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 маршрут 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 Практической 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 Практической 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 11: 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.

### Step 1: Подключите кабели в сети в соответствии с топологией.

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

### Step 2: Настройте узлы ПК.

**Step 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.**

#### Step 4: Настройте базовые параметры каждого маршрутизатора.

- a. Отключите поиск DNS.
- b. Настройте IP-адреса для маршрутизаторов, указанных в таблице адресации.
- c. Установите тактовую частоту на **128000** для всех последовательных интерфейсов DCE.
- d. Присвойте имена устройствам в соответствии с топологией.
- e. Назначьте **cisco** в качестве паролей консоли и VTY.
- f. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.
- g. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.

#### Step 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
```

#### Step 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
```

#### Step 7: Сохраните текущую конфигурацию в загрузочную конфигурацию.

#### Step 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 1: 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.

### Step 1: Настройте статическое сопоставление.

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
209.165.200.225
```

### Step 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
```

### Step 3: Проверьте конфигурацию.

- a. Отобразите таблицу статических преобразований NAT с помощью команды **show ip nat 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 Практической 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 эхо-запроса 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
209.165.201.17:12 209.165.201.17:12
--- 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 эхо-запроса 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 2: 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.

### Step 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
```

### Step 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
```

### Step 3: Убедитесь, что конфигурации интерфейса NAT все ещё действительны.

Чтобы проверить конфигурации NAT, на маршрутизаторе Gateway выполните команду **show ip nat statistics**.

### Step 4: Определите пул пригодных к использованию публичных IP-адресов.

```
Gateway(config)# ip nat pool public_access
209.165.200.242 209.165.200.254 netmask 255.255.255.224
```

### Step 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
```

### Step 6: Проверьте конфигурацию.

- 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.

### Step 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
192.168.1.20 209.165.200.225
```

```
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)
Peak translations: 15, occurred 00:00:43 ago
Outside interfaces:
 Serial0/0/1
Inside interfaces:
 GigabitEthernet0/1
Hits: 16 Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 4
pool public_access: netmask 255.255.255.224
start 209.165.200.242 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)         |
| <p><b>Примечание.</b> 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.</p> |                             |                             |                               |                               |

#### Список литературы, рекомендуемый к использованию по данной теме:

*Основная:* 1-3

*Дополнительная:* 1-8

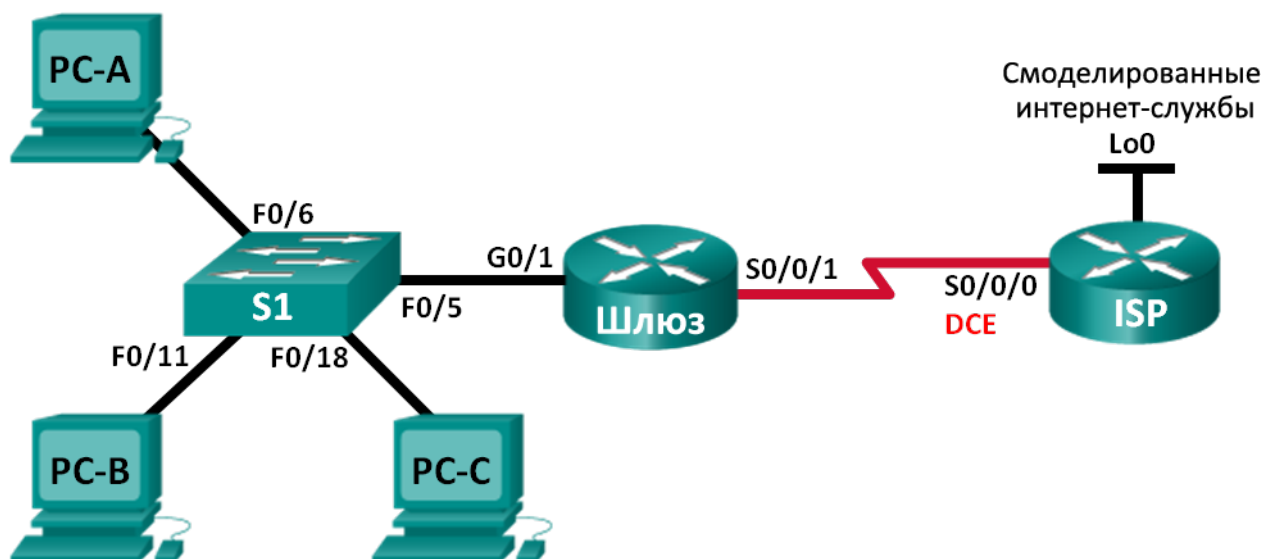
*Методическая:* 1

*Интернет-ресурсы:* 1

*Программное обеспечение:* 1-4

## Практическая работа 14. Настройка NAT-пула с перегрузкой и PAT

### Топология



### Таблица адресации

| Устройство | Интерфейс    | IP-адрес       | Маска подсети   | Шлюз по умолчанию |
|------------|--------------|----------------|-----------------|-------------------|
| Gateway    | 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               |
| ISP        | 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       | 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       |
| PC-C       | NIC          | 192.168.1.22   | 255.255.255.0   | 192.168.1.1       |

### Цели занятия:

Часть 1. Построение сети и проверка подключения

Часть 2. Настройка и проверка NAT-пула с перегрузкой

Часть 3. Настройка и проверка преобразования PAT

Время 6 часов

### Формируемые компетенции: ПК-1; ПК-2

### Исходные данные/сценарий

По сценарию первой части Практической работы интернет-провайдер выделил вашей компании диапазон публичных IP-адресов 209.165.200.224/29. Благодаря этому компания получила шесть публичных IP-адресов. Перегрузка пула динамического NAT использует пул IP-адресов по модели «множество к множеству». Маршрутизатор использует первый IP-адрес в пуле и назначает подключения с помощью IP-адреса и уникального номера порта. После достижения на маршрутизаторе максимального количества преобразований для одного IP-адреса (для платформы и оборудования), используется следующий IP-адрес в пуле.

Во второй части интернет-провайдер выделил вашей компании один IP-адрес, 209.165.201.18, для подключения к Интернету от маршрутизатора Gateway к сети

интернет-провайдера. Для преобразования нескольких внутренних адресов в один пригодный для использования публичный адрес используйте преобразование адресов портов (PAT). Вы выполните тестирование, отображение и проверку осуществления всех преобразований и проанализируете статистику NAT/PAT для контроля процесса.

**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 Практической 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 Практической 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);
- 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 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.

**Step 1: Подключите кабели в сети в соответствии с топологией.**

**Step 2: Настройте узлы ПК.**

**Step 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.**

**Step 4: Настройте базовые параметры каждого маршрутизатора.**

- а. Отключите поиск DNS.
- б. Настройте IP-адреса для маршрутизаторов, указанных в таблице адресации.
- в. Установите тактовую частоту на **128000** для всех последовательных интерфейсов DCE.
- г. Присвойте имена устройствам в соответствии с топологией.
- д. Назначьте **cisco** в качестве паролей консоли и VTY.
- е. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному

режиму EXEC.

- g. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.

#### Step 5: Настройте статическую маршрутизацию.

- a. Создайте статический маршрут от интернет-провайдера к маршрутизатору Gateway.

```
ISP(config)# ip route 209.165.200.224 255.255.255.248
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
```

#### Step 6: 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. Проверьте настройку статических маршрутов на обоих маршрутизаторах.

### Часть 2: Настройка и проверка NAT-пула с перегрузкой

Во второй части вам предстоит настроить маршрутизатор Gateway для преобразования IP-адреса из сети 192.168.1.0/24 в один из шести пригодных к использованию адресов в диапазоне 209.165.200.224/29.

#### Step 1: 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
```

#### Step 2: Определите пул пригодных к использованию публичных IP-адресов.

```
Gateway(config)# ip nat pool public_access 209.165.200.225
209.165.200.230 netmask 255.255.255.248
```

#### Step 3: Определите соответствие в NAT внутреннего списка адресов источника и пула внешних адресов.

```
Gateway(config)# ip nat inside source list 1 pool
public_access overload
```

#### Step 4: 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
```

#### Step 5: Проверьте конфигурацию NAT-пула с перегрузкой.

- a. Из каждого ПК отправьте эхо-запрос на адрес маршрутизатора интернет-провайдера — 192.31.7.1.

- b. Отобразите статистику NAT по маршрутизатору Gateway.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3
extended)
Peak translations: 3, occurred 00:00:25 ago
Outside interfaces:
 Serial0/0/1
Inside interfaces:
 GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 3
pool public_access: netmask 255.255.255.248
start 209.165.200.225 end 209.165.200.230
type generic, total addresses 6, allocated 1 (16%), misses
0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

- c. Отобразите преобразования NAT на маршрутизаторе Gateway.

```
Gateway# show ip nat translations
Pro Inside global Inside local Outside local
Outside global
icmp 209.165.200.225:0 192.168.1.20:1 192.31.7.1:1
192.31.7.1:0
icmp 209.165.200.225:1 192.168.1.21:1 192.31.7.1:1
192.31.7.1:1
icmp 209.165.200.225:2 192.168.1.22:1 192.31.7.1:1
192.31.7.1:2
```

**Примечание.** В зависимости от времени, истекшего с момента отправки эхо-запросов с каждого ПК, вы можете не увидеть все три преобразования. ICMP-преобразованиям характерны низкие значения лимита времени.

Сколько внутренних локальных IP-адресов указано в примере выходных данных выше? \_\_\_\_\_

Сколько указано внутренних глобальных IP-адресов? \_\_\_\_\_

Сколько номеров портов используется в паре с внутренними глобальными адресами \_\_\_\_\_

Что произойдёт в результате отправки эхо-запроса на внутренний локальный адрес компьютера PC-A от маршрутизатора интернет-провайдера? Почему?

---

---

---

### Часть 3: Настройка и проверка преобразования PAT

В третьей части вам предстоит настроить PAT, используя интерфейс для определения внешних адресов вместо пула адресов. Не все команды из части 2 будут использоваться в части 3.

**Step 1: Очистите преобразования NAT и статистику из маршрутизатора Gateway.**

**Step 2: Проверьте конфигурацию NAT.**

- Убедитесь, что статистика удалена.
- Убедитесь, что внешние и внутренние интерфейсы настроены для преобразований NAT.
- Убедитесь, что ACL-список по-прежнему настроен для преобразований NAT.

Какую команду вы использовали для того, чтобы подтвердить результаты после выполнения шагов от а до с?

---

**Step 3: Удалите пул пригодных к использованию публичных IP-адресов.**

```
Gateway(config)# no ip nat pool public_access
209.165.200.225 209.165.200.230 netmask 255.255.255.248
```

**Step 4: Удалите NAT трансляцию между ACL-списком и пулом внешних адресов.**

```
Gateway(config)# no ip nat inside source list 1 pool
public_access overload
```

**Step 5: Сопоставьте список источника с внешним интерфейсом.**

```
Gateway(config)# ip nat inside source list 1 interface
serial 0/0/1 overload
```

**Step 6: Проверьте конфигурацию PAT.**

- Из каждого ПК отправьте эхо-запрос на адрес маршрутизатора интернет-провайдера — 192.31.7.1.
- Отобразите статистику NAT по маршрутизатору Gateway.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3
extended)
Peak translations: 3, occurred 00:00:19 ago
Outside interfaces:
 Serial0/0/1
Inside interfaces:
 GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 interface Serial0/0/1 refcount 3
```

```
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

с. Отобразите преобразования NAT на Gateway.

```
Gateway# show ip nat translations
Pro Inside global Inside local Outside local
Outside global
icmp 209.165.201.18:3 192.168.1.20:1 192.31.7.1:1
192.31.7.1:3
icmp 209.165.201.18:1 192.168.1.21:1 192.31.7.1:1
192.31.7.1:1
icmp 209.165.201.18:4 192.168.1.22:1 192.31.7.1:1
192.31.7.1:4
```

### Вопросы на закрепление

В чём заключаются преимущества PAT?

---



---



---



---

### 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.

**Список литературы, рекомендуемый к использованию по данной теме:**

Основная: 1-3  
Дополнительная: 1-8  
Методическая: 1  
Интернет-ресурсы: 1  
Программное обеспечение: 1-4

**Практическая работа 15. Базовая настройка DHCPv4 на маршрутизаторе**

**Топология**

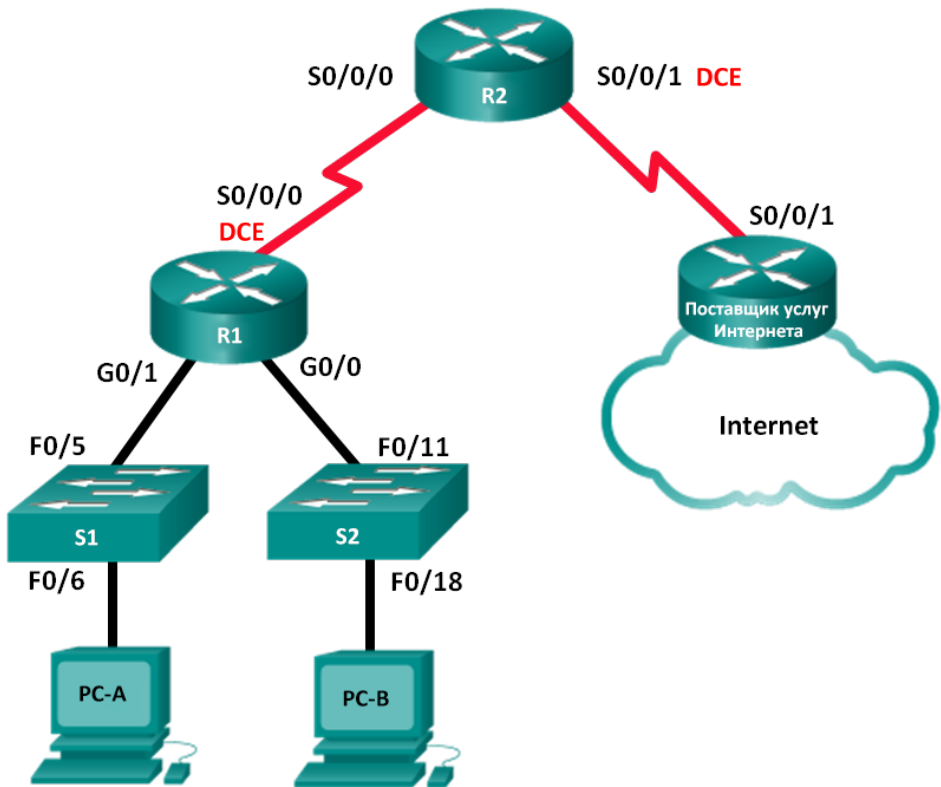


**Таблица адресации**

| Устройство | Интерфейс       | IP-адрес        | Маска подсети   | Шлюз по умолчанию |
|------------|-----------------|-----------------|-----------------|-------------------|
| R1         | G0/0            | 192.168.0.1     | 255.255.255.0   | —                 |
|            | G0/1            | 192.168.1.1     | 255.255.255.0   | —                 |
|            | S0/0/0 (DCE)    | 192.168.2.253   | 255.255.255.252 | —                 |
| R2         | S0/0/0          | 192.168.2.254   | 255.255.255.252 | —                 |
|            | S0/0/1 (DCE)    | 209.165.200.226 | 255.255.255.224 | —                 |
| ISP        | S0/0/1          | 209.165.200.225 | 255.255.255.224 | —                 |
| PC-A       | Сетевой адаптер | DHCP            | DHCP            | DHCP              |
| PC-B       | Сетевой адаптер | DHCP            | DHCP            | DHCP              |

**Задачи**

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Выполнение настройки DHCPv4-сервера и агента-ретранслятора DHCP

**Общие сведения/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 IPv4-адресов в двух разных подсетях, подключенных к маршрутизатору R1.

**Примечание.** В данной лабораторной работе содержится минимальный набор команд, необходимых для настройки DHCP. Список требуемых команд приведен в Приложении А. Проверьте свои знания: настройте устройства, не заглядывая в приложение.

**Примечание.** В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сетевыми сервисами (ISR) Cisco 1941 с операционной системой 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). Допускается использование коммутаторов и маршрутизаторов других моделей, а также других версий операционной системы 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 интерфейсов 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

- 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель).
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель).
- 2 ПК (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 согласно топологии.

## Часть 1: Создание сети и настройка основных 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 приведенной топологии.

**Step 1: Создайте сеть согласно топологии.**

**Step 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.**

**Step 3: Произведите базовую настройку маршрутизаторов.**

- а. Подключитесь к маршрутизатору с помощью консоли и перейдите в режим глобальной настройки.
- б. Скопируйте приведенную ниже базовую конфигурацию и вставьте ее в текущую конфигурацию на маршрутизаторе.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
```

login

- c. Настройте имена хостов в соответствии с топологией.
- d. Настройте на маршрутизаторе IPv4-адреса в соответствии с топологией.
- e. Для последовательных интерфейсов DCE установите тактовую частоту 128000.

**Step 4: Настройте на маршрутизаторах динамическую маршрутизацию, статическую маршрутизацию и маршрутизацию по умолчанию.**

- a. Настройте протокол RIPv2 на маршрутизаторе R1.

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.0.0
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.2.252
R1(config-router)# no auto-summary
```

- b. Настройте протокол RIPv2 и маршрут по умолчанию к ISP на маршрутизаторе R2.

```
R2(config)# router rip
R1(config-router)# version 2
R2(config-router)# network 192.168.2.252
R2(config-router)# default-information originate
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

- c. Настройте суммарный статический маршрут на ISP для доступа к сетям маршрутизаторов R1 и R2.

```
ISP(config)# ip route 192.168.0.0 255.255.252.0 209.165.200.226
```

- d. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

**Step 5: 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.

**Step 6: 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.

**Step 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.** Список команд, необходимых для выполнения части 2, приведен в приложении А. Проверьте свои знания, попробуйте настроить DHCP на R1 и R2 без использования приложения.

---

---

---

[illegible]

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?

### Step 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.

---

---

---

**Step 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?

**Step 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?

---

- б. 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 index 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 R1 выполните команду **show run interface** для интерфейсов G0/0 и G0/1, чтобы просмотреть настройки ретранслятора DHCP в текущей конфигурации.

### Вопросы для повторения

Как вы думаете, в чем заключается преимущество использования агентов DHCP-ретрансляции вместо использования нескольких маршрутизаторов, работающих в качестве серверов DHCP?

---

---

---

---

### 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 (S0/1/0)          | 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 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.

## 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 M2

```
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 16. Настройка сервера DHCPv6 без отслеживания состояния и с отслеживанием состояния

### Топология



### Таблица адресации

| Устройство | Интерфейс | IPv6-адрес                          | Длина префикса | Шлюз по умолчанию           |
|------------|-----------|-------------------------------------|----------------|-----------------------------|
| R1         | G0/1      | 2001:DB8:ACAD:A::1                  | 64             | —                           |
| S1         | VLAN 1    | Назначен протоколом SLAAC           | 64             | Назначен протоколом SLAAC   |
| PC-A       | NIC       | Назначен протоколами SLAAC и DHCPv6 | 64             | Назначен маршрутизатором R1 |

### Задачи

**Часть 1. Создание сети и настройка основных параметров устройства**

**Часть 2. Настройка сети для функции SLAAC**

**Часть 3. Настройка сети для сервера DHCPv6 без отслеживания состояния**

**Часть 4. Настройка сети для сервера DHCPv6 с отслеживанием состояния**

### Общие сведения/сценарий

Динамическое назначение глобальных индивидуальных IPv6-адресов можно настроить тремя способами:

- Только автоматическая настройка адреса без отслеживания состояния (SLAAC).
- DHCPv6 без отслеживания состояния.
- Адресация DHCPv6 с учетом состояний.

В случае использования SLAAC (произносится как «слэк»), сервер DHCPv6 не требуется для получения узлами IPv6-адресов. Сервер DHCP можно использовать для получения дополнительной информации, необходимой узлу, например доменного имени или адреса сервера доменных имен (DNS). Когда SLAAC используется для назначения IPv6-адресов узлам, а DHCPv6 используется для получения других сетевых параметров, подобная настройка носит название DHCPv6 без отслеживания состояния.

При использовании DHCPv6 с отслеживанием состояния, сервер DHCP назначает всю информацию, включая IPv6-адрес узла.

Определение способа получения динамической IPv6-адресации зависит от установленных значений флагов, содержащихся в объявлениях маршрутизатора (сообщениях RA).

В начале данной лабораторной работы вам предстоит провести настройку сети для использования

функции SLAAC. После проверки соединения вы выполните настройку DHCPv6 и измените сеть на использование DHCPv6 без отслеживания состояния. Убедившись, что DHCPv6 без отслеживания состояния работает без неполадок, вы настроите маршрутизатор R1 для использования DHCPv6 с отслеживанием состояния. Для проверки всех трех конфигураций сети будет использоваться программа Wireshark.

**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). Допускается использование коммутаторов и маршрутизаторов других моделей, а также других версий операционной системы 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 интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

**Примечание.** Убедитесь, что информация из маршрутизаторов и коммутаторов удалена, и они не содержат файлов загрузочной конфигурации. Если вы не уверены, обратитесь к инструктору.

**Примечание.** Шаблон **default bias** (по умолчанию используемый диспетчером базы данных коммутатора SDM) не предоставляет возможностей IPv6-адресации. Убедитесь, что SDM использует шаблон **dual-ipv4-and-ipv6** или **lanbase-routing**. После перезагрузки будет использоваться последний выбранный шаблон, даже если настройки не были сохранены.

```
S1# show sdm prefer
```

Чтобы установить шаблон **dual-ipv4-and-ipv6** в качестве шаблона SDM по умолчанию, выполните следующие действия:

```
S1# config t
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

## Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с операционной системой Cisco IOS 15.2(4)M3 (универсальный образ) 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 ОС Windows 7, Vista или XP с Wireshark и программой эмулятора терминала, например Tera Term).
- Консольные кабели для настройки устройств Cisco IOS через консольные порты.
- Кабели Ethernet, расположенные в соответствии с топологией.

**Примечание.** Клиентские службы DHCPv6 отключены на Windows XP. Для выполнения этой лабораторной работы рекомендуется использовать узел под управлением Windows 7.

## Часть 1: Создание сети и настройка основных параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и выполнить настройку базовых параметров: имен устройств, паролей и IP-адресов интерфейсов.

**Step 1: Создайте сеть согласно топологии.**

**Step 2: Выполните запуск и перезагрузку маршрутизатора и коммутатора.**

**Step 3: Настройте маршрутизатор R1.**

- а. Подключитесь к маршрутизатору R1 с помощью консоли и перейдите в режим глобальной настройки.
- б. Скопируйте приведенную ниже базовую конфигурацию и вставьте ее в файл текущей конфигурации на маршрутизаторе R1.

```
no ip domain-lookup
```

```
service password-encryption
hostname R1
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

- c. Сохранение текущей конфигурации в качестве начальной.

#### **Step 4: Настройте коммутатор S1.**

- a. Подключитесь к коммутатору S1 с помощью консоли и перейдите в режим глобальной настройки.
- b. Скопируйте приведенную ниже базовую конфигурацию и вставьте ее в файл текущей конфигурации на коммутаторе S1.

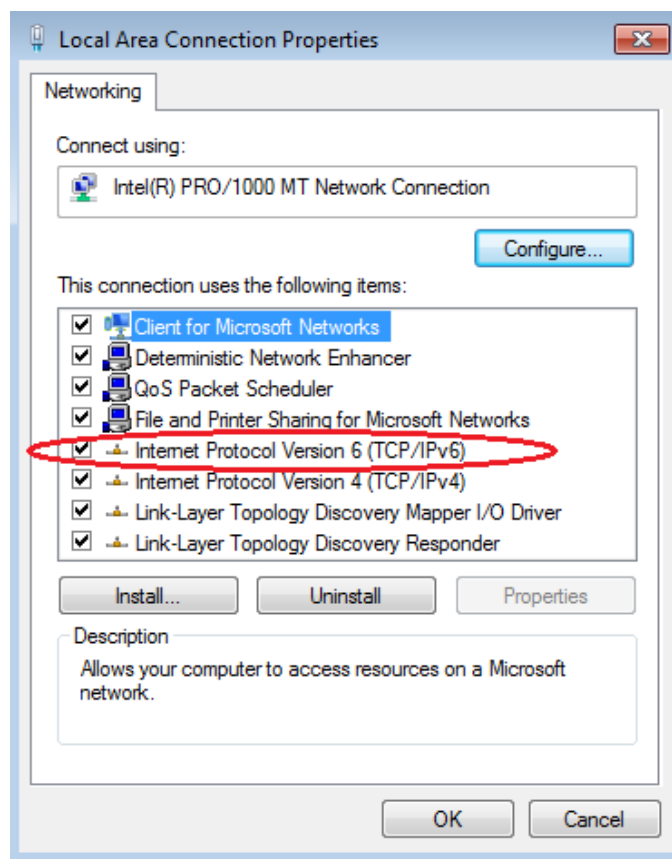
```
no ip domain-lookup
service password-encryption
hostname S1
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

- c. От имени администратора отключите все неактивные интерфейсы.
- d. Сохраните текущую конфигурацию в загрузочную конфигурацию.

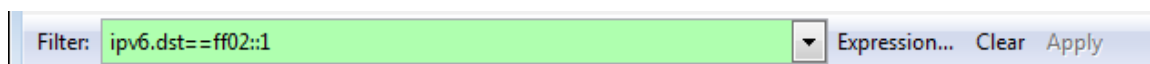
## **Часть 2: Настройка сети для функции SLAAC**

#### **Step 1: Подготовьте PC-A.**

- a. Убедитесь, что протокол IPv6 включен в окне «Подключение по локальной сети — свойства». Если напротив пункта Протокол Интернета версии 6 (TCP/IPv6) не стоит флажок, щелкните для его активации.



- b. Начните захват трафика на сетевом адаптере с помощью Wireshark.
- c. Отфильтруйте захват данных так, чтобы видеть только сообщения RA. Это можно сделать путем фильтрации IPv6-пакетов с адресом назначения FF02::1, который является групповым адресом для отправки пакетом всем узлам локальной сети. Как показано, в Wireshark используется фильтр **ipv6.dst==ff02::1**.



### Step 2: Настройте маршрутизатор R1.

- a. Включите маршрутизацию IPv6 unicast-трафика.
- b. Назначьте индивидуальный IPv6-адрес интерфейсу G0/1 в соответствии с таблицей адресации.
- c. Назначьте FE80::1 в качестве локального IPv6-адреса канала интерфейса G0/1.
- d. Активируйте интерфейс G0/1.

### Step 3: Проверьте, является ли маршрутизатор R1 частью группы многоадресной рассылки для всех маршрутизаторов.

Для того чтобы проверить, является ли интерфейс G0/1 частью многоадресной группы для всех маршрутизаторов (FF02::2), используйте команду **show ipv6 interface g0/1**. Без назначения этой группы сообщения RA не отправляются из интерфейса G0/1.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
 2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
 FF02::1
 FF02::2
 FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
```

```

ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.

```

#### Step 4: Настройте коммутатор S1.

Для того чтобы получить IPv6-адрес с помощью SLAAC, в сети VLAN 1 используйте команду **ipv6 address autoconfig**.

```

S1(config)# interface vlan 1
S1(config-if)# ipv6 address autoconfig
S1(config-if)# end

```

#### Step 5: Убедитесь, что SLAAC предоставил коммутатору S1 индивидуальный адрес.

Для того чтобы проверить, предоставил ли SLAAC индивидуальный адрес сети VLAN 1 на коммутаторе S1, используйте команду **show ipv6 interface**.

```

S1# show ipv6 interface
Vlan1 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::ED9:96FF:FEE8:8A40
 No Virtual link-local address(es):
 Stateless address autoconfig enabled
 Global unicast address(es):
 2001:DB8:ACAD:A:ED9:96FF:FEE8:8A40, subnet is 2001:DB8:ACAD:A::/64
[EUI/CAL/PRE]
 valid lifetime 2591988 preferred lifetime 604788
 Joined group address(es):
 FF02::1
 FF02::1:FFE8:8A40
 MTU is 1500 bytes
 ICMP error messages limited to one every 100 milliseconds
 ICMP redirects are enabled
 ICMP unreachable are sent
 Output features: Check hwidb
 ND DAD is enabled, number of DAD attempts: 1
 ND reachable time is 30000 milliseconds (using 30000)
 ND NS retransmit interval is 1000 milliseconds
 Default router is FE80::1 on Vlan1

```

#### Step 6: Убедитесь, что SLAAC предоставил информацию об IPv6-адресе компьютеру PC-A.

- Из командной строки компьютера PC-A выполните команду **ipconfig /all**. Убедитесь, что компьютер PC-A имеет IPv6-адрес с префиксом 2001:db8:acad:a::/64. Шлюз по умолчанию должен иметь адрес FE80::1.

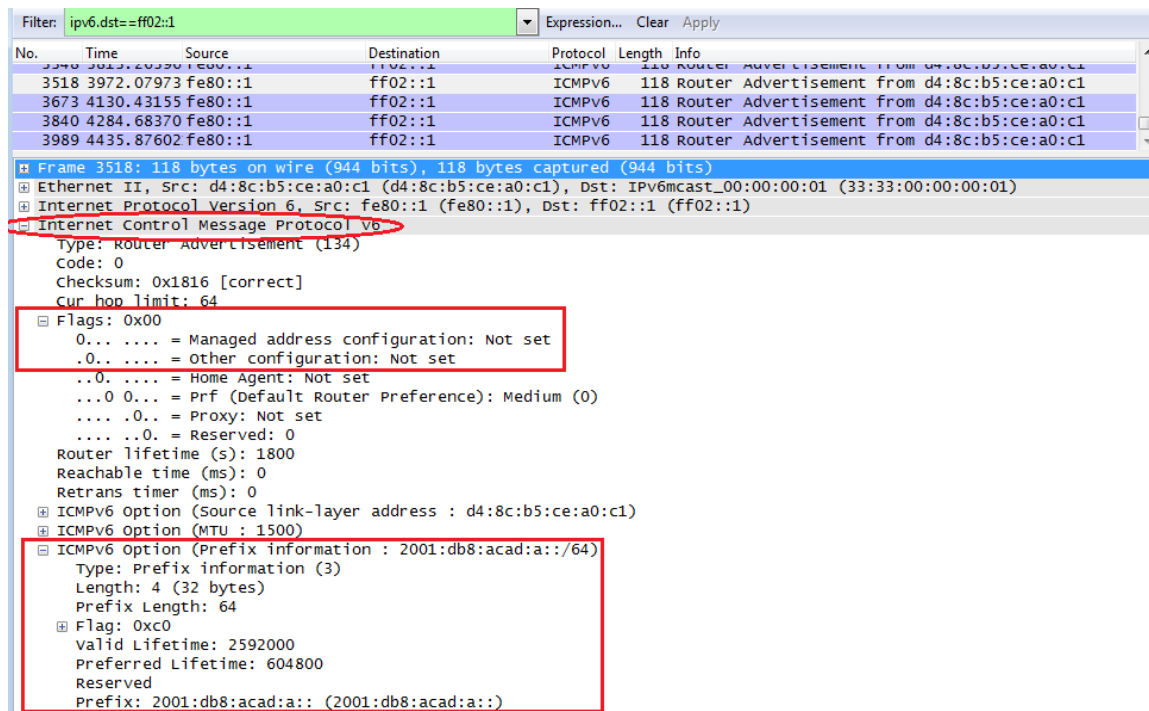
```

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description : Intel(R) PRO/1000 MT Network Connection
Physical Address. : 00-50-56-BE-76-8C
DHCP Enabled. : Yes
Autoconfiguration Enabled : Yes
IPv6 Address. : 2001:db8:acad:a:24ba:a0a0:9f0:ff88 (Preferred)
Temporary IPv6 Address. : 2001:db8:acad:a:c05b:d3f7:31be:100e (Preferred)
Link-local IPv6 Address : fe80::24ba:a0a0:9f0:ff88%11 (Preferred)
Autoconfiguration IPv4 Address. . . . : 169.254.255.136 (Preferred)
Subnet Mask : 255.255.0.0
Default Gateway : fe80::1:1
DNS Servers : fec0:0:0:ffff::1%1
 : fec0:0:0:ffff::2%1
 : fec0:0:0:ffff::3%1
NetBIOS over Tcpip. : Enabled

```

- b. В программе Wireshark изучите одно из захваченных объявлений маршрутизатора. Разверните вкладку Internet Control Message Protocol v6, чтобы просмотреть информацию о флагах и префиксе. Первые два флага отслеживают использование DHCPv6 и не отмечены, если DHCPv6 не настроен. Данные о префиксе также содержатся в этом сообщении RA.



### Часть 3: Настройка сети для DHCPv6 без отслеживания состояния

#### Step 1: Настройте сервер DHCP IPv6 на маршрутизаторе R1.

- Создайте пул DHCP IPv6.  
R1(config)# **ipv6 dhcp pool IPV6POOL-A**
- Назначьте пулу имя домена.  
R1(config-dhcpv6)# **domain-name ccna-statelessDHCPv6.com**
- Назначьте адрес сервера DNS.  
R1(config-dhcpv6)# **dns-server 2001:db8:acad:a::abcd**  
R1(config-dhcpv6)# **exit**
- Назначьте пул DHCPv6 интерфейсу.  
R1(config)# **interface g0/1**  
R1(config-if)# **ipv6 dhcp server IPV6POOL-A**
- Установите обнаружение сети DHCPv6 (ND) на managed-config-flag.  
R1(config-if)# **ipv6 nd other-config-flag**  
R1(config-if)# **end**

#### Step 2: Проверьте настройки DHCPv6 на интерфейсе G0/1 маршрутизатора R1.

Для того чтобы проверить, является ли интерфейс частью многоадресной группы всех DHCPv6-серверов IPv6 (FF02::1:2), используйте команду **show ipv6 interface g0/1**. Последняя строка выходных данных данной команды **show** подтверждает установку флага other-config-flag.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
 2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
```

```

FF02::1
FF02::2
FF02::1:2
FF02::1:FF00:1
FF05::1:3
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
Хосты используют DHCPv6 для получения другой конфигурации.

```

### Step 3: Изучите изменения в сети компьютера PC-A.

Для просмотра изменений в сети используйте команду **ipconfig /all**. Обратите внимание, что дополнительные сведения, включая имя домена и информацию о сервере DNS, получены от сервера DHCPv6. Однако глобальные индивидуальные IPv6-адреса и локальные IPv6-адреса канала были получены ранее от SLAAC.

```

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : ccna-statelessDHCPv6.com
Description : Intel(R) Ethernet Network Connection
Physical Address. : 00-50-56-BE-76-8C
DHCP Enabled. : Yes
Autoconfiguration Enabled : Yes
IPv6 Address. : 2001:db8:acad:a:24ba:a0a0:9f0:ff88(Preferred)
Temporary IPv6 Address. : 2001:db8:acad:a:103a:4344:4b5e:ab1d(Preferred)
Link-local IPv6 Address : fe80::24ba:a0a0:9f0:ff88%11(Preferred)
Autoconfiguration IPv4 Address. . : 169.254.255.136(Preferred)
Subnet Mask : 255.255.0.0
Default Gateway : fe80::1%11
DHCPv6 IAID : 234884137
DHCPv6 Client DUID. : 00-01-00-01-17-F6-72-3D-00-0C-29-8D-54-44

DNS Servers : 2001:db8:acad:a::abcd
NetBIOS over Tcpip. : Enabled
Connection-specific DNS Suffix Search List :
ccna-statelessDHCPv6.com

Tunnel adapter isatap.{E2FC1866-B195-460A-BF40-F04F42A38FFE}:

Media State : Media disconnected
Connection-specific DNS Suffix . : ccna-statelessDHCPv6.com
Description : Microsoft ISATAP Adapter
Physical Address. : 00-00-00-00-00-00-00-00-E0
DHCP Enabled. : No
Autoconfiguration Enabled : Yes

```

### Step 4: Просмотрите сообщения RA с помощью программы Wireshark.

Прокрутите вниз до последнего сообщения маршрутизатора, отображаемого в Wireshark, и разверните его, чтобы просмотреть установку флажка ICMPv6. Обратите внимание, что флажок другой конфигурации (other configuration flag) настроен на значение 1.

Filter: **ipv6.dst==ff02::1** Expression... Clear Apply

| No. | Time       | Source  | Destination | Protocol | Length | Info                                        |
|-----|------------|---------|-------------|----------|--------|---------------------------------------------|
| 191 | 190.005980 | fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from d4:8c:b5:ce:a0:c1 |
| 422 | 383.803033 | fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from d4:8c:b5:ce:a0:c1 |
| 696 | 581.355847 | fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from d4:8c:b5:ce:a0:c1 |
| 877 | 776.644829 | fe80::1 | ff02::1     | ICMPv6   | 118    | Router Advertisement from d4:8c:b5:ce:a0:c1 |

Frame 877: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)

Ethernet II, Src: d4:8c:b5:ce:a0:c1 (d4:8c:b5:ce:a0:c1), Dst: IPv6mcast\_00:00:00:01 (33:33:00:00:00:01)

Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)

Internet Control Message Protocol v6

Type: Router Advertisement (134)  
Code: 0  
Checksum: 0x17d6 [correct]  
Cur hop limit: 64  
Flags: 0x40  
0... .. = Managed address configuration: Not set  
**1... .. = Other configuration: Set**  
..0. .... = Home Agent: Not set  
...0 .... = Prf (Default Router Preference): Medium (0)  
....0.. = Proxy: Not set  
.....0. = Reserved: 0  
Router lifetime (s): 1800  
Reachable time (ms): 0  
Retrans timer (ms): 0

ICMPv6 Option (Source link-layer address : d4:8c:b5:ce:a0:c1)

ICMPv6 Option (MTU : 1500)

ICMPv6 Option (Prefix information : 2001:db8:acad:a::/64)

#### Step 5: Убедитесь, что компьютер PC-A не получил свой IPv6-адрес от сервера DHCPv6.

Для того, чтобы убедиться, что компьютер PC-A не получил свой IPv6-адрес из пула DHCPv6, используйте команды **show ipv6 dhcp binding** и **show ipv6 dhcp pool**.

```
R1# show ipv6 dhcp binding
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-statelessDHCPv6.com
Active clients: 0
```

#### Step 6: Сбросьте сетевые параметры IPv6 компьютера PC-A.

- Выключите интерфейс F0/6 коммутатора S1.

**Примечание.** Отключение интерфейса F0/6 не позволит компьютеру PC-A получить новый IPv6-адрес прежде, чем вы настроите маршрутизатор R1 на DHCPv6 с отслеживанием состояния в части 4.

```
S1(config)# interface f0/6
S1(config-if)# shutdown
```

- Остановите процесс захвата трафика программой Wireshark с сетевого адаптера компьютера PC-A.
- Сбросьте параметры IPv6 на PC-A, чтобы удалить настройки DHCPv6 без отслеживания состояния.
  - Откройте окно «Подключение по локальной сети — свойства», снимите флажок с пункта **Протокол Интернета версии 6 (TCP/IPv6)** и нажмите **ОК**, чтобы принять внесенные изменения.
  - Снова откройте окно «Подключение по локальной сети: свойства». Установите флажок **Протокол Интернета версии 6 (TCP/IPv6)** и щелкните **ОК**, чтобы принять внесенные изменения.

## Часть 4: Настройка сети для DHCPv6 с отслеживанием состояния

#### Step 1: Подготовьте PC-A.

- Начните захват трафика на сетевом адаптере с помощью Wireshark.
- Отфильтруйте захват данных так, чтобы видеть только сообщения RA. Это можно сделать путем фильтрации IPv6-пакетов с адресом назначения FF02::1, который является групповым адресом для отправки пакетом всем узлам локальной сети.

|                                  |               |       |       |
|----------------------------------|---------------|-------|-------|
| Filter: <b>ipv6.dst==ff02::1</b> | Expression... | Clear | Apply |
|----------------------------------|---------------|-------|-------|

#### Step 2: Измените пул DHCPv6 на маршрутизаторе R1.

- Добавьте префикс сети в пул.

```
R1(config)# ipv6 dhcp pool IPV6POOL-A
R1(config-dhcpv6)# address prefix 2001:db8:acad:a::/64
```

- b. Измените имя домена на **ccna-statefulDHCPv6.com**.

**Примечание.** Необходимо удалить прежнее имя домена. Имя домена нельзя сменить с помощью команды **domain-name**.

```
R1(config-dhcpv6)# no domain-name ccna-statelessDHCPv6.com
R1(config-dhcpv6)# domain-name ccna-StatefulDHCPv6.com
R1(config-dhcpv6)# end
```

- c. Проверьте настройки пула DHCPv6.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
 Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400
 (0 in use, 0 conflicts)
 DNS server: 2001:DB8:ACAD:A::ABCD
 Domain name: ccna-StatefulDHCPv6.com
 Active clients: 0
```

- d. Войдите в режим отладки, чтобы проверить, как DHCPv6 с отслеживанием состояния назначает адреса.

```
R1# debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
```

### Step 3: На интерфейсе G0/1 установите флажок для DHCPv6 с отслеживанием состояний.

**Примечание.** Отключение интерфейса G0/1 до внесения изменений гарантирует отправку сообщения маршрутизатора при включении интерфейса.

```
R1(config)# interface g0/1
R1(config-if)# shutdown
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# no shutdown
R1(config-if)# end
```

### Step 4: Включите интерфейс F0/6 на коммутаторе S1.

Теперь, когда маршрутизатор R1 настроен для DHCPv6 с отслеживанием состояния, компьютер PC-A можно переподключить к сети путем активации интерфейса F0/6 коммутатора S1.

```
S1(config)# interface f0/6
S1(config-if)# no shutdown
S1(config-if)# end
```

### Step 5: Проверьте настройки DHCPv6 с отслеживанием состояния на маршрутизаторе R1.

- a. Для того чтобы проверить, находится ли интерфейс в режиме DHCPv6 с отслеживанием состояния, выполните команду **show ipv6 interface g0/1**.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::1
 No Virtual link-local address(es):
 Global unicast address(es):
 2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
 Joined group address(es):
 FF02::1
 FF02::2
 FF02::1:2
 FF02::1:FF00:1
 FF05::1:3
 MTU is 1500 bytes
 ICMP error messages limited to one every 100 milliseconds
 ICMP redirects are enabled
 ICMP unreachables are sent
 ND DAD is enabled, number of DAD attempts: 1
 ND reachable time is 30000 milliseconds (using 30000)
 ND advertised reachable time is 0 (unspecified)
```

```

ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Хосты используют DHCP для получения маршрутизируемых адресов.
Хосты используют DHCP для получения другой конфигурации.

```

- b. В командной строке компьютера PC-A введите **ipconfig /release6**, чтобы освободить текущий назначенный IPv6-адрес. Затем введите **ipconfig /renew6**, чтобы запросить IPv6-адрес от сервера DHCPv6.
- c. Для того чтобы проверить количество активных клиентов, выполните команду **show ipv6 dhcp pool**.

```

R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
 Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400
 (1 in use, 0 conflicts)
 DNS server: 2001:DB8:ACAD:A::ABCD
 Domain name: ccna-StatefulDHCPv6.com
 Active clients: 1

```

- d. Для того чтобы убедиться, что компьютер PC-A получил индивидуальный IPv6-адрес из пула DHCP, выполните команду **show ipv6 dhcp binding**. Сравните адрес клиента с локальным IPv6-адресом канала на компьютере PC-A с помощью команды **ipconfig /all**. Сравните адрес, полученный с помощью команды **show**, с IPv6-адресом, полученным с помощью команды **ipconfig /all**, выполненной на компьютере PC-A.

```

R1# show ipv6 dhcp binding
Client: FE80::D428:7DE2:997C:B05A
DUID: 0001000117F6723D000C298D5444
Username : unassigned
IA NA: IA ID 0x0E000C29, T1 43200, T2 69120
 Address: 2001:DB8:ACAD:A:B55C:8519:8915:57CE
 preferred lifetime 86400, valid lifetime 172800
 expires at Mar 07 2013 04:09 PM (171595 seconds)

```

```

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : ccna-StatefulDHCPv6.com
Description : Intel(R) PRO/1000 MT Network Connection
Physical Address. : 00-50-56-BE-6C-89
DHCP Enabled. : Yes
Autoconfiguration Enabled : Yes
IPv6 Address. : 2001:db8:acad:a:b55c:8519:8915:57ce (Preferred)
Lease Obtained. : Tuesday, March 05, 2013 11:53:11 AM
Lease Expires : Thursday, March 07, 2013 11:53:11 AM
IPv6 Address. : 2001:db8:acad:a:d428:7de2:997c:b05a (Preferred)
Temporary IPv6 Address. : 2001:db8:acad:a:dd37:1e42:948c:225b (Preferred)
Link-local IPv6 Address : fe80::d428:7de2:997c:b05a%11 (Preferred)
Autoconfiguration IPv4 Address. . . . : 169.254.176.98 (Preferred)
Subnet Mask : 255.255.0.0
Default Gateway : fe80::1%11
DHCPv6 IAID : 234884137
DHCPv6 Client DUID. : 00-01-00-01-17-F6-72-3D-00-0C-29-8D-54-44

DNS Servers : 2001:db8:acad:a::abcd
NetBIOS over Tcpip. : Enabled
Connection-specific DNS Suffix Search List :
ccna-StatefulDHCPv6.com

```

- e. Выполните команду **undebg all** на маршрутизаторе R1, чтобы остановить отладку DHCPv6.

**Примечание.** Сокращенная форма этой команды — **u all**. Она полезна для того, чтобы остановить появление сообщений об отладке на экране сеанса терминала. Если одновременно происходит несколько процессов отладки, команда **undebg all** прекратит их все.

```

R1# u all
All possible debugging has been turned off

```

- f. Изучите сообщения отладки, которые появились на экране терминала вашего маршрутизатора R1.

1) Просмотрите сообщение запроса от компьютера PC-A, запрашивающее информацию о сети.

```

*Mar 5 16:42:39.775: IPv6 DHCP: Received SOLICIT from

```

```

FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1
*Mar 5 16:42:39.775: IPv6 DHCP: detailed packet contents
*Mar 5 16:42:39.775: src FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)
*Mar 5 16:42:39.775: dst FF02::1:2
*Mar 5 16:42:39.775: type SOLICIT(1), xid 1039238
*Mar 5 16:42:39.775: option ELAPSED-TIME(8), len 2
*Mar 5 16:42:39.775: elapsed-time 6300
*Mar 5 16:42:39.775: option CLIENTID(1), len 14

```

2) Просмотрите сообщение ответа, отправленное компьютеру PC-A от сервера DHCP с информацией об адресации.

```

*Mar 5 16:42:39.779: IPv6 DHCP: Sending REPLY to FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1
*Mar 5 16:42:39.779: IPv6 DHCP: detailed packet contents
*Mar 5 16:42:39.779: src FE80::1
*Mar 5 16:42:39.779: dst FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)
*Mar 5 16:42:39.779: type REPLY(7), xid 1039238
*Mar 5 16:42:39.779: option SERVERID(2), len 10
*Mar 5 16:42:39.779: 00030001FC994775C3E0
*Mar 5 16:42:39.779: option CLIENTID(1), len 14
*Mar 5 16:42:39.779: 00010001
R1#17F6723D000C298D5444
*Mar 5 16:42:39.779: option IA-NA(3), len 40
*Mar 5 16:42:39.779: IAID 0x0E000C29, T1 43200, T2 69120
*Mar 5 16:42:39.779: option IAADDR(5), len 24
*Mar 5 16:42:39.779: IPv6 address 2001:DB8:ACAD:A:B55C:8519:8915:57CE
*Mar 5 16:42:39.779: preferred 86400, valid 172800
*Mar 5 16:42:39.779: option DNS-SERVERS(23), len 16
*Mar 5 16:42:39.779: 2001:DB8:ACAD:A::ABCD
*Mar 5 16:42:39.779: option DOMAIN-LIST(24), len 26
*Mar 5 16:42:39.779: ccna-StatefulDHCPv6.com

```

**Step 6: Проверка DHCPv6 с отслеживанием состояния на компьютере PC-A**

- Остановите захват данных программой Wireshark на компьютере PC-A.
- Разверните последнее сообщение RA, отображаемое в Wireshark. Убедитесь, что был установлен флаг **Managed address configuration** (Управляемая конфигурация адреса).

The screenshot shows the Wireshark interface. The top filter bar contains the filter `ipv6.dst==ff02::1`. The packet list shows several ICMPv6 Router Advertisement packets from source `fc:99:47:75:c3:e1` to destination `ff02::1`. The packet details pane for the selected packet (Frame 775) shows the following structure:

- Ethernet II, Src: fc:99:47:75:c3:e1 (fc:99:47:75:c3:e1), Dst: IPv6mcast\_00:00:00:01 (33:33:00:00:00:01)
- Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
- Internet Control Message Protocol v6
  - Type: Router Advertisement (134)
  - Code: 0
  - Checksum: 0x3a82 [correct]
  - Cur hop limit: 64
  - Flags: 0xc0
    - 1... .... = Managed address configuration: Set
    - ..1. .... = Other configuration: Set
    - ..0. .... = Home Agent: Not set
    - ...0 ... = Prf (Default Router Preference): Medium (0)
    - .... 0.. = Proxy: Not set
    - .... ..0. = Reserved: 0
  - Router lifetime (s): 1800

- Измените фильтр в Wireshark для просмотра только **DHCPv6**-пакетов, введя **dhcpv6**, а затем **Примените фильтр (Apply)**. Выделите последний отображаемый ответ DHCPv6 и разверните сведения, полученные от сервера DHCPv6. Изучите сведения DHCPv6, содержащиеся в этом пакете.

| Filter: dhcpv6                                                                                                  |            | Expression... Clear Apply    |                              |          |        |                                                    |
|-----------------------------------------------------------------------------------------------------------------|------------|------------------------------|------------------------------|----------|--------|----------------------------------------------------|
| No.                                                                                                             | Time       | Source                       | Destination                  | Protocol | Length | Info                                               |
| 250                                                                                                             | 443.078236 | fe80::d428:7de2:997ff02::1:2 |                              | DHCPv6   | 146    | Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2   |
| 267                                                                                                             | 475.083284 | fe80::d428:7de2:997ff02::1:2 |                              | DHCPv6   | 146    | Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2   |
| 425                                                                                                             | 656.281211 | fe80::d428:7de2:997ff02::1:2 |                              | DHCPv6   | 146    | Solicit XID: 0xc86c32 CID: 0001000117f6723d000c2   |
| 429                                                                                                             | 656.282249 | fe80::1                      | fe80::d428:7de2:997ff02::1:2 | DHCPv6   | 191    | Advertise XID: 0xc86c32 CID: 0001000117f6723d000c2 |
| 460                                                                                                             | 657.292018 | fe80::d428:7de2:997ff02::1:2 |                              | DHCPv6   | 188    | Request XID: 0xc86c32 CID: 0001000117f6723d000c2   |
| 462                                                                                                             | 657.292638 | fe80::1                      | fe80::d428:7de2:997ff02::1:2 | DHCPv6   | 191    | Reply XID: 0xc86c32 CID: 0001000117f6723d000c298   |
| Ethernet II, Src: fc:99:47:75:c3:e1 (fc:99:47:75:c3:e1), Dst: Vmware_be:6c:89 (00:50:56:be:6c:89)               |            |                              |                              |          |        |                                                    |
| Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: fe80::d428:7de2:997c:b05a (fe80::d428:7de2:997c:b05a) |            |                              |                              |          |        |                                                    |
| User Datagram Protocol, Src Port: dhcpv6-server (547), Dst Port: dhcpv6-client (546)                            |            |                              |                              |          |        |                                                    |
| DHCPv6                                                                                                          |            |                              |                              |          |        |                                                    |
| Message type: Reply (7)                                                                                         |            |                              |                              |          |        |                                                    |
| Transaction ID: 0xc86c32                                                                                        |            |                              |                              |          |        |                                                    |
| Server Identifier: 00030001fc994775c3e0                                                                         |            |                              |                              |          |        |                                                    |
| Client Identifier: 0001000117f6723d000c298d5444                                                                 |            |                              |                              |          |        |                                                    |
| Identity Association for Non-temporary Address                                                                  |            |                              |                              |          |        |                                                    |
| Option: Identity Association for Non-temporary Address (3)                                                      |            |                              |                              |          |        |                                                    |
| Length: 40                                                                                                      |            |                              |                              |          |        |                                                    |
| value: 0e000c290000a8c000010e000005001820010db8acad000a...                                                      |            |                              |                              |          |        |                                                    |
| IAID: 0e000c29                                                                                                  |            |                              |                              |          |        |                                                    |
| T1: 43200                                                                                                       |            |                              |                              |          |        |                                                    |
| T2: 69120                                                                                                       |            |                              |                              |          |        |                                                    |
| IA Address: 2001:db8:acad:a:b55c:8519:8915:57ce                                                                 |            |                              |                              |          |        |                                                    |
| DNS recursive name server                                                                                       |            |                              |                              |          |        |                                                    |
| Option: DNS recursive name server (23)                                                                          |            |                              |                              |          |        |                                                    |
| Length: 16                                                                                                      |            |                              |                              |          |        |                                                    |
| value: 20010db8acad000a000000000000abcd                                                                         |            |                              |                              |          |        |                                                    |
| DNS servers address: 2001:db8:acad:a::abcd                                                                      |            |                              |                              |          |        |                                                    |
| Domain Search List                                                                                              |            |                              |                              |          |        |                                                    |
| Option: Domain Search List (24)                                                                                 |            |                              |                              |          |        |                                                    |
| Length: 25                                                                                                      |            |                              |                              |          |        |                                                    |
| value: 1363636e612d537461746566756c44484350763603636f6d...                                                      |            |                              |                              |          |        |                                                    |
| DNS Domain Search List                                                                                          |            |                              |                              |          |        |                                                    |
| Domain: ccna-statefulDHCPv6.com                                                                                 |            |                              |                              |          |        |                                                    |

## Вопросы для повторения

1. Какой метод IPv6-адресации использует больше ресурсов памяти маршрутизатора, настроенного в качестве сервера DHCPv6 — DHCPv6 без отслеживания состояния или DHCPv6 с отслеживанием состояния? Почему?

---



---



---

2. Какой тип динамического назначения IPv6-адресов рекомендует компания Cisco: DHCPv6 без отслеживания состояния или DHCPv6 с отслеживанием состояния?

---



---

## 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 (S0/1/0)          | 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 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 17. Настройка протоколов CDP и LLDP

### Топология



### Таблица адресации

| Устройство                | Интерфейс    | IP-адрес        | Маска подсети   |
|---------------------------|--------------|-----------------|-----------------|
| Шлюз                      | G0/1         | 192.168.1.254   | 255.255.255.0   |
|                           | S0/0/1       | 209.165.200.226 | 255.255.255.252 |
| Поставщик услуг Интернета | S0/0/1 (DCE) | 209.165.200.225 | 255.255.255.252 |

### Задачи

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Обнаружение сетевых ресурсов с помощью протокола CDP

Часть 3. Обнаружение сетевых ресурсов с помощью протокола LLDP

## Общие сведения/сценарий

Протокол Cisco Discovery Protocol (CDP) — собственный протокол Cisco для обнаружения сетевых ресурсов, функционирующий на канальном уровне. Он служит для обмена информацией, например именами устройств и версиями ПО IOS, с другими физически подключенными устройствами Cisco. Протокол Link Layer Discovery Protocol (LLDP) — это не зависящий от производителя протокол для обнаружения сетевых ресурсов, функционирующий на канальном уровне. В основном он используется сетевыми устройствами в локальной сети (LAN). Сетевые устройства сообщают соседям такие данные о себе, как идентификаторы и сведения о функциональных возможностях.

В этой лабораторной работе вам предстоит задокументировать порты, которые используются для подключения к другим коммутаторам по протоколам CDP и LLDP. Полученные результаты следует указать в диаграмме сетевой топологии. Также вам потребуется при необходимости включить или отключить эти протоколы обнаружения сетевых ресурсов.

**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 интерфейсов 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

- 2 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель)
- 3 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet, расположенные в соответствии с топологией

## Часть 1: Создание сети и настройка основных параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить основные параметры для маршрутизатора и коммутаторов.

### Шаг 1: Создайте сеть согласно топологии.

В топологии не указаны Ethernet-порты, используемые на коммутаторах. Можно воспользоваться любыми Ethernet-портами для подключения коммутаторов с помощью сетевого кабеля, как указано на диаграмме топологии.

### Шаг 2: При необходимости инициализируйте и перезагрузите сетевые устройства.

### Шаг 3: Настройте основные параметры коммутаторов.

- а. Подключитесь к устройству с помощью консольного подключения и активируйте привилегированный режим EXEC.
- б. Войдите в режим конфигурации.
- в. Отключите поиск DNS, чтобы предотвратить попытки коммутатора неверно преобразовывать введенные команды таким образом, будто они являются именами хостов.
- г. Укажите имя хоста в соответствии с топологией.
- д. Убедитесь, что порты коммутаторов, к которым подключены кабели Ethernet, включены.
- е. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

#### Шаг 4: Настройте основные параметры маршрутизаторов.

- Подключитесь к устройству с помощью консольного подключения и активируйте привилегированный режим EXEC.
- Войдите в режим конфигурации.
- Скопируйте и вставьте следующие конфигурации для маршрутизаторов.

##### ISP:

```
hostname ISP
no ip domain lookup
interface Serial0/0/1
 ip address 209.165.200.225 255.255.255.252
 no shutdown
```

##### Шлюз:

```
hostname Gateway
no ip domain lookup
interface GigabitEthernet0/1
 ip address 192.168.1.254 255.255.255.0
 ip nat inside
 no shutdown
interface Serial0/0/1
 ip address 209.165.200.226 255.255.255.252
 ip nat outside
 no shutdown
ip nat inside source list 1 interface Serial0/0/1 overload
access-list 1 permit 192.168.1.0 0.0.0.255
```

- Сохраните текущую конфигурацию в файл загрузочной конфигурации.

## Часть 2: Обнаружение сетевых ресурсов с помощью протокола CDP

На устройствах Cisco протокол CDP включен по умолчанию. Воспользуйтесь CDP, чтобы обнаружить порты, к которым подключены кабели.

- На маршрутизаторе Gateway введите команду **show cdp** в исполнительском режиме, чтобы убедиться в том, что на маршрутизаторе включен протокол CDP.

```
Gateway# show cdp
Global CDP information:
 Sending CDP packets every 60 seconds
 Sending a holdtime value of 180 seconds
 Sending CDPv2 advertisements is enabled
```

С какой периодичностью отправляются пакеты CDP?

---

Если на маршрутизаторе шлюза отключен протокол CDP, включите его. Для этого выполните команду **cdp run** в режиме глобальной настройки.

```
Gateway(config)# cdp run
Gateway(config)# end
```

- Выполните команду **show cdp interface**, чтобы отобразить список интерфейсов, участвующих в объявлениях CDP.

```
Gateway# show cdp interface
Embedded-Service-Engine0/0 is administratively down, line protocol is down
 Encapsulation ARPA
 Sending CDP packets every 60 seconds
 Holdtime is 180 seconds
GigabitEthernet0/0 is administratively down, line protocol is down
 Encapsulation ARPA
 Sending CDP packets every 60 seconds
 Holdtime is 180 seconds
GigabitEthernet0/1 is up, line protocol is up
```

```

Encapsulation ARPA
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
Serial0/0/0 is administratively down, line protocol is down
Encapsulation HDLC
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
Serial0/0/1 is up, line protocol is up
Encapsulation HDLC
Sending CDP packets every 60 seconds
Holdtime is 180 seconds

cdp enabled interfaces : 5
interfaces up : 2
interfaces down : 3

```

Сколько интерфейсов участвует в объявлениях CDP? Какие из них активны?

- 
- c. Выполните команду **show cdp neighbors**, чтобы определить соседей CDP.

```

Gateway# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
 S - Switch, H - Host, I - IGMP, r - Repeater, P -
 Phone,
 D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID Local Intrfce Holdtme Capability Platform
Port ID
ISP Ser 0/0/1 158 R B S I CISCO1941 Ser
0/0/1
S3 Gig 0/1 170 S I WS-C2960- Fas
0/5

```

- d. Чтобы отобразить более подробные сведения о соседях CDP, выполните команду **show cdp neighbors detail**.

```

Gateway# show cdp neighbors detail

Device ID: ISP
Entry address(es):
 IP address: 209.165.200.225
Platform: Cisco CISCO1941/K9, Capabilities: Router Source-Route-Bridge
Switch IGMP
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/1
Holdtime : 143 sec

Version :
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version
15.4(3)M2, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Fri 06-Feb-15 17:01 by prod_rel_team

advertisement version: 2
Management address(es):
 IP address: 209.165.200.225

Device ID: S3
Entry address(es):
Platform: cisco WS-C2960-24TT-L, Capabilities: Switch IGMP
Interface: GigabitEthernet0/1, Port ID (outgoing port):
FastEthernet0/5
Holdtime : 158 sec

```

```
Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version
15.0(2)SE7, RELEASE SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 23-Oct-14 14:49 by prod_rel_team
```

```
advertisement version: 2
Protocol Hello: OUI=0x00000C, Protocol ID=0x0112; payload len=27,
value=00000000FFFFFFFFF010221FF00000000000000CD996E87400FF0000
VTP Management Domain: ''
Native VLAN: 1
Duplex: full
```

- e. Какую информацию можно узнать об ISP и S3 в результате выполнения команды **show cdp neighbors detail**?

- f. Настройте интерфейс SVI на S3. Укажите доступный IP-адрес в пределах сети 192.168.1.0/24. В качестве шлюза по умолчанию укажите 192.168.1.254.

```
S3(config)# interface vlan 1
S3(config-if)# ip address 192.168.1.3 255.255.255.0
S3(config-if)# no shutdown
S3(config-if)# exit
S3(config)# ip default-gateway 192.168.1.254
```

- g. Выполните команду **show cdp neighbors detail** на маршрутизаторе Gateway. Какие дополнительные сведения доступны теперь?

- h. Из соображений безопасности рекомендуется отключить протокол CDP на интерфейсах, которые используются для подключения к внешним сетям. Выполните команду **no cdp enable** в режиме интерфейсной настройки S0/0/1 на маршрутизаторе Gateway.

```
Gateway(config)# interface s0/0/1
Gateway(config-if)# no cdp enable
Gateway(config-if)# end
```

Чтобы проверить, отключен ли протокол CDP для интерфейса S0/0/1, выполните команду **show cdp neighbors** или **show cdp interface**. Возможно, потребуется подождать, пока истечет время удержания. Время удержания — это время, в течение которого сетевые устройства хранят пакеты CDP, пока эти пакеты не будут отклонены устройствами.

```
Gateway# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
 S - Switch, H - Host, I - IGMP, r - Repeater, P -
Phone,
 D - Remote, C - CVTA, M - Two-port Mac Relay
```

| Device ID | Local Intrfce | Holdtme | Capability | Platform  |
|-----------|---------------|---------|------------|-----------|
| Port ID   |               |         |            |           |
| S3        | Gig 0/1       | 161     | S I        | WS-C2960- |
| 0/5       |               |         |            | Fas       |

Интерфейс S0/0/1 маршрутизатора Gateway больше не связан с маршрутизатором ISP посредством отношений смежности (adjacency) CDP. Однако у этого интерфейса по-прежнему имеются отношения смежности с другими интерфейсами.

```
Gateway# show cdp interface
Embedded-Service-Engine0/0 is administratively down, line protocol is
down
 Encapsulation ARPA
 Sending CDP packets every 60 seconds
 Holdtime is 180 seconds
GigabitEthernet0/0 is administratively down, line protocol is down
```

```

Encapsulation ARPA
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
GigabitEthernet0/1 is up, line protocol is up
Encapsulation ARPA
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
Serial0/0/0 is administratively down, line protocol is down
Encapsulation HDLC
Sending CDP packets every 60 seconds
Holdtime is 180 seconds

cdp enabled interfaces : 4
interfaces up : 1
interfaces down : 3

```

- i. Чтобы отключить протокол CDP в глобальном масштабе, выполните команду **no cdp run** в режиме глобальной настройки.

```

Gateway# conf t
Gateway(config)# no cdp run
Gateway(config)# end

```

Какие команды необходимо выполнить, чтобы убедиться в том, что протокол CDP отключен?

---

- j. Включите протокол CDP глобально на маршрутизаторе шлюза. На скольких интерфейсах включен протокол CDP? На каких интерфейсах этот протокол отключен?
- 

- k. Подключитесь ко всем коммутаторам через консоль и выполните необходимые команды CDP, чтобы определить Ethernet-порты, которые используются для подключения к другим устройствам. Ниже представлен пример команд CDP для S3.

```

S3# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
 S - Switch, H - Host, I - IGMP, r - Repeater, P -
Phone,
 D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID Local Intrfce Holdtme Capability Platform
Port ID
Gateway
0/1 Fas 0/5 143 R B S I CISCO1941 Gig
S2
0/4 Fas 0/2 173 S I WS-C2960- Fas
S1
0/4 Fas 0/4 171 S I WS-C2960- Fas

```

### Часть 3: Обнаружение сетевых ресурсов с помощью протокола LLDP

На устройствах Cisco протокол LLDP может быть включен по умолчанию. Воспользуйтесь LLDP, чтобы обнаружить порты, к которым подключены кабели.

- a. На маршрутизаторе шлюза выполните команду **show lldp** в исполнительском режиме EXEC.

```

Gateway# show lldp
% LLDP is not enabled (LLDP не включен)

```

Если на маршрутизаторе Gateway отключен протокол LLDP, включите его. Для этого выполните команду **lldp run** в режиме глобальной настройки.

```

Gateway(config)# lldp run

```

- b. На маршрутизаторе Gateway введите команду **show lldp**, чтобы убедиться в том, что на маршрутизаторе включен протокол LLDP.

```

Gateway# show lldp

```

Global LLDP Information:

Status: ACTIVE

LLDP advertisements are sent every 30 seconds

LLDP hold time advertised is 120 seconds

LLDP interface reinitialisation delay is 2 seconds

Выполните команду **show lldp neighbors**. Какие устройства имеются по соседству с маршрутизатором Gateway?

- 
- c. Если у маршрутизатора Gateway нет соседей LLDP, включите протокол LLDP на коммутаторах. На этих устройствах выполните команду **lldp run** в режиме глобальной настройки.

```
S1(config)# lldp run
```

```
S2(config)# lldp run
```

```
S3(config)# lldp run
```

- d. Выполните команду **show lldp neighbors** на коммутаторах и маршрутизаторе, чтобы отобразить список портов, на которых включен LLDP. Ниже представлен результат выполнения команды на маршрутизаторе Gateway.

```
Gateway# show lldp neighbors
```

Capability codes:

(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device

(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

| Device ID | Local Intf | Hold-time | Capability | Port ID |
|-----------|------------|-----------|------------|---------|
| S3        | Gi0/1      | 120       | B          | Fa0/5   |

Total entries displayed: 1

- e. На маршрутизаторе Gateway выполните команду **show lldp neighbors detail**.

```
Gateway# show lldp neighbors detail
```

```

Local Intf: Gi0/1
```

```
Chassis id: 0cd9.96e8.7400
```

```
Port id: Fa0/5
```

```
Port Description: FastEthernet0/5
```

```
System Name: S3
```

```
System Description:
```

```
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version
15.0(2)SE7, RELEASE SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2014 by Cisco Systems, Inc.
```

```
Compiled Thu 23-Oct-14 14:49 by prod_rel_team
```

```
Time remaining: 103 seconds
```

```
System Capabilities: B
```

```
Enabled Capabilities: B
```

```
Management Addresses:
```

```
IP: 192.168.1.3
```

```
Auto Negotiation - supported, enabled
```

```
Physical media capabilities:
```

```
100base-TX(FD)
```

```
100base-TX(HD)
```

```
10base-T(FD)
```

```
10base-T(HD)
```

```
Media Attachment Unit type: 16
```

```
Vlan ID: 1
```

Total entries displayed: 1

Какой порт используется на S3 для подключения к маршрутизатору шлюза?

- f. Используйте результаты выполнения команды **show** для протоколов CDP и LLDP, чтобы указать подключенные порты в топологии сети.



### Вопросы для повторения

Для каких интерфейсов в пределах сети не следует использовать протоколы обнаружения сетевых ресурсов? Поясните ответ.

---



---



---



---

### 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 (S0/1/0)          | 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 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 18. Настройка Syslog и NTP

## Топология



## Таблица адресации

| Устройство | Интерфейс    | IP-адрес   | Маска подсети   | Шлюз по умолчанию |
|------------|--------------|------------|-----------------|-------------------|
| R1         | S0/0/0 (DCE) | 10.1.1.1   | 255.255.255.252 | —                 |
| R2         | S0/0/0       | 10.1.1.2   | 255.255.255.252 | —                 |
|            | G0/0         | 172.16.2.1 | 255.255.255.0   | —                 |
| PC-B       | NIC          | 172.16.2.3 | 255.255.255.0   | 172.16.2.1        |

## Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка NTP

Часть 3. Настройка Syslog

## Общие сведения/сценарий

Сообщения Syslog, создаваемые сетевыми устройствами, могут собираться и архивироваться на сервере Syslog. Эту информацию можно использовать для наблюдения, отладки и поиска и устранения неполадок. Администратор может настраивать место сохранения и отображения сообщений. Сообщения Syslog могут сопровождаться метками времени для анализа последовательности сетевых событий; поэтому важно синхронизировать часы всех сетевых устройств с помощью сервера NTP.

В этой лабораторной работе необходимо настроить маршрутизатор R1 в качестве сервера NTP, а маршрутизатор R2 в качестве клиента Syslog и NTP. Серверное приложение Syslog (например, Tftpd32 или другая аналогичная программа) будет работать на компьютере PC-B. Кроме того, вы будете контролировать уровень важности сообщений журнала, которые собираются и архивируются на сервере Syslog.

**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). Допускается использование маршрутизаторов других моделей, а также других версий операционной системы 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 интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

**Примечание.** Убедитесь, что все настройки маршрутизаторов удалены и загрузочная конфигурация отсутствует. Если вы не уверены, обратитесь к инструктору.

## Необходимые ресурсы

- 2 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель).
- 1 компьютер (с операционной системой Windows 7, Vista или XP, с программой эмуляции терминала, например Tera Term, и ПО Syslog, например tftpd32).
- Консольные кабели для настройки устройств Cisco IOS через консольные порты.
- Кабели Ethernet и последовательные кабели согласно топологии.

## Часть 1: Настройка основных параметров устройств

В части 1 необходимо настроить топологию сети и базовые параметры, например IP-адреса интерфейса, маршрутизацию, доступ к устройствам и пароли.

**Step 1: Создайте сеть согласно топологии.**

**Step 2: Выполните запуск и перезагрузку маршрутизаторов.**

**Step 3: Произведите базовую настройку маршрутизаторов.**

- a. Подключитесь к маршрутизатору с помощью консоли и перейдите в режим глобальной настройки.
- b. Скопируйте приведенную ниже базовую конфигурацию и вставьте ее в текущую конфигурацию на маршрутизаторе.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```
- c. Настройте имена хостов в соответствии с топологией.
- d. Примените IP-адреса к интерфейсам Serial и Gigabit Ethernet в соответствии с таблицей адресации и включите физические интерфейсы.
- e. Установите тактовую частоту **128000** для последовательного интерфейса DCE.

**Step 4: Настройте маршрутизацию.**

Включите RIPv2 на маршрутизаторах. Добавьте все сети в процесс RIPv2.

**Step 5: Настройте ПК В.**

Настройте IP-адрес и шлюз по умолчанию для ПК В согласно таблице адресации.

**Step 6: Проверьте наличие сквозного соединения.**

Убедитесь, что все устройства могут отправлять эхо-запросы на каждое другое устройство в сети. Если нет, устраните неполадки, чтобы установить связь между конечными устройствами.

**Step 7: Сохранение текущей конфигурации в качестве начальной.**

## Часть 2: Настройка NTP

В части 2 необходимо настроить маршрутизатор R1 в качестве сервера NTP, а маршрутизатор R2 в качестве клиента NTP маршрутизатора R1. Необходимо выполнить синхронизацию времени для Syslog и отладочных функций. Если время не синхронизировано, сложно определить, какое сетевое событие стало причиной данного сообщения.

**Step 1: Выведите на экран текущее время.**

Введите команду **show clock** для отображения текущего времени на R1.

```
R1# show clock
*12:30:06.147 UTC Tue May 14 2013
```

Запишите отображаемые сведения о текущем времени в следующей таблице.

|              |  |
|--------------|--|
| Дата         |  |
| Время        |  |
| Часовой пояс |  |

### Step 2: Установите время.

С помощью команды **clock set** установите время на маршрутизаторе R1. Ниже приводится пример настройки даты и времени.

```
R1# clock set 9:39:00 05 july 2013
R1#
*Jul 5 09:39:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from
12:30:54 UTC Tue May 14 2013 to 09:39:00 UTC Fri Jul 5 2013, configured from
console by console.
```

**Примечание.** Время можно также настроить с помощью команды **clock timezone** в режиме глобальной конфигурации. Для получения дополнительной информации о команде **clock timezone** посетите веб-сайт [www.cisco.com](http://www.cisco.com) и определите часовой пояс для вашего региона.

### Step 3: Настройте главный сервер NTP.

Настройте маршрутизатор R1 в качестве главного сервера NTP с помощью команды **ntp master stratum-number** в режиме глобальной конфигурации. Значение stratum показывает в каком количестве переходов NTP от доверенного источника времени находится сервер. В этой лабораторной работе в качестве stratum данного сервера NTP используется число 5.

```
R1(config)# ntp master 5
```

### Step 4: Настройте клиент NTP.

- Введите команду **show clock** на маршрутизаторе R2. Запишите текущее время, отображаемое на маршрутизаторе R2, в следующей таблице.

|              |  |
|--------------|--|
| Дата         |  |
| Время        |  |
| Часовой пояс |  |

- Настройте R2 в качестве клиента NTP. Используйте команду **ntp server**, чтобы указать на IP-адрес или имя компьютера сервера NTP. Команда **ntp update-calendar** периодически обновляет календарь на основе времени NTP.

```
R2(config)# ntp server 10.1.1.1
R2(config)# ntp update-calendar
```

### Step 5: Проверьте настройку NTP.

- Используйте команду **show ntp associations**, чтобы проверить, что маршрутизатор R2 связан через NTP с маршрутизатором R1.

```
R2# show ntp associations
```

```
address ref clock st when poll reach delay offset disp
*~10.1.1.1 127.127.1.1 5 11 64 177 11.312 -0.018 4.298
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

- Введите команду **show clock** на маршрутизаторах R1 и R2 и сравните метку времени.

**Примечание.** Синхронизация метки времени на маршрутизаторе R2 с меткой времени на маршрутизаторе R1 может занять несколько минут.

```
R1# show clock
09:43:32.799 UTC Fri Jul 5 2013
R2# show clock
9:43:37.122 UTC Fri Jul 5 2013
```

## Часть 3: Настройте Syslog

Сообщения Syslog от сетевых устройств могут собираться и архивироваться на сервере Syslog. В этой лабораторной работе в качестве программного обеспечения сервера Syslog используется Tftpd32.

Администратор может настраивать типы сообщений, которые можно отправлять на сервер Syslog.

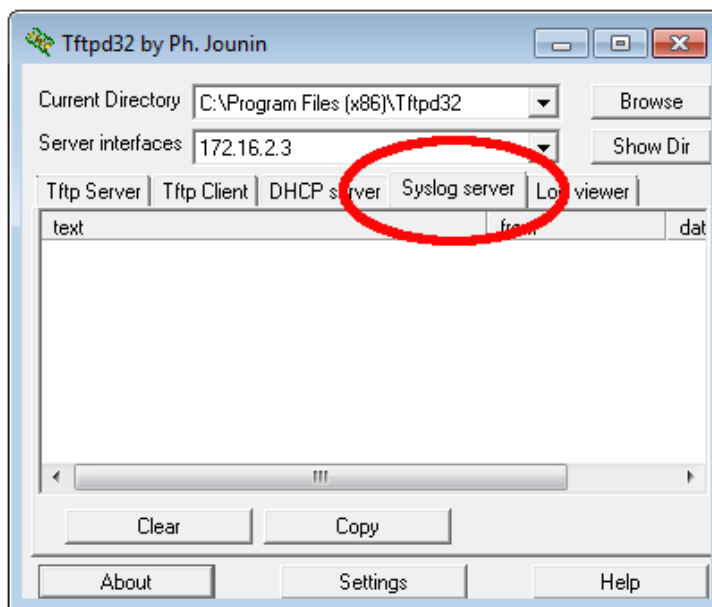
**Step 1: (Дополнительно) Установите сервер Syslog.**

Если сервер Syslog еще не установлен на компьютере, загрузите и установите последнюю версию сервера Syslog, например Tftpd32. Последнюю версию Tftpd32 можно найти по следующей ссылке:

<http://tftpd32.jounin.net/>

**Step 2: Запустите сервер Syslog на компьютере ПК В.**

После запуска приложения Tftpd32 перейдите на вкладку **Syslog server**.



**Step 3: Убедитесь, что на маршрутизаторе R2 включена служба меток времени.**

С помощью команды **show run** проверьте, что служба меток времени включена для журналирования на маршрутизаторе R2.

```
R2# show run | include timestamp
service timestamps debug datetime msec
service timestamps log datetime msec
```

Если служба меток времени не включена, используйте следующую команду, чтобы включить ее.

```
R2(config)# service timestamps log datetime msec
```

**Step 4: Настройте R2 для сохранения сообщений журнала на сервере Syslog.**

Настройте маршрутизатор R2 для отправки syslog-сообщений на сервер Syslog (компьютер PC-B). IP-адрес сервера Syslog на PC-B: 172.16.2.3.

```
R2(config)# logging host 172.16.2.3
```

**Step 5: Выведите на экран параметры по умолчанию для журналирования.**

Используйте команду **show logging**, чтобы вывести на экран параметры журналирования по умолчанию.

```
R2# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)
```

```
No Active Message Discriminator.
```

```
No Inactive Message Discriminator.
```

```
Console logging: level debugging, 47 messages logged, xml disabled,
```

```

filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
filtering disabled
Buffer logging: level debugging, 47 messages logged, xml disabled,
filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

```

No active filter modules.

```

Trap logging: level informational, 49 message lines logged
Logging to 172.16.2.3 (udp port 514, audit disabled,
link up),
6 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled
Logging Source-Interface: VRF Name:

```

Назовите IP-адрес сервера Syslog. \_\_\_\_\_

Какие протокол и порт использует сервер Syslog? \_\_\_\_\_

Какой уровень сообщений настроен? \_\_\_\_\_

**Step 6: Настройте и проверьте результат настройки уровней важности для журналирования на маршрутизаторе R2.**

- a. С помощью команды **logging trap ?** определите доступность различных уровней сообщений. При настройке уровня сообщений, отправляемые на сервер Syslog, будут включать сообщения настроенного уровня и сообщения более низких уровней.

```

R2(config)# logging trap ?
<0-7> Logging severity level
alerts Immediate action needed (severity=1)
critical Critical conditions (severity=2)
debugging Debugging messages (severity=7)
emergencies Систему нельзя использовать (серьезность=0)
errors Состояние ошибки (серьезность=3)
informational Информационные сообщения (серьезность=6)
notifications Нормальное, но значащее состояние (серьезность=5)
warnings Состояние предупреждения (серьезность=4)
<cr>

```

Если введена команда **logging trap warnings**, сообщения с какими уровнями важности будут регистрироваться?

---

- b. Укажите уровень важности для журналирования равный 4.

```
R2(config)# logging trap warnings
```

или

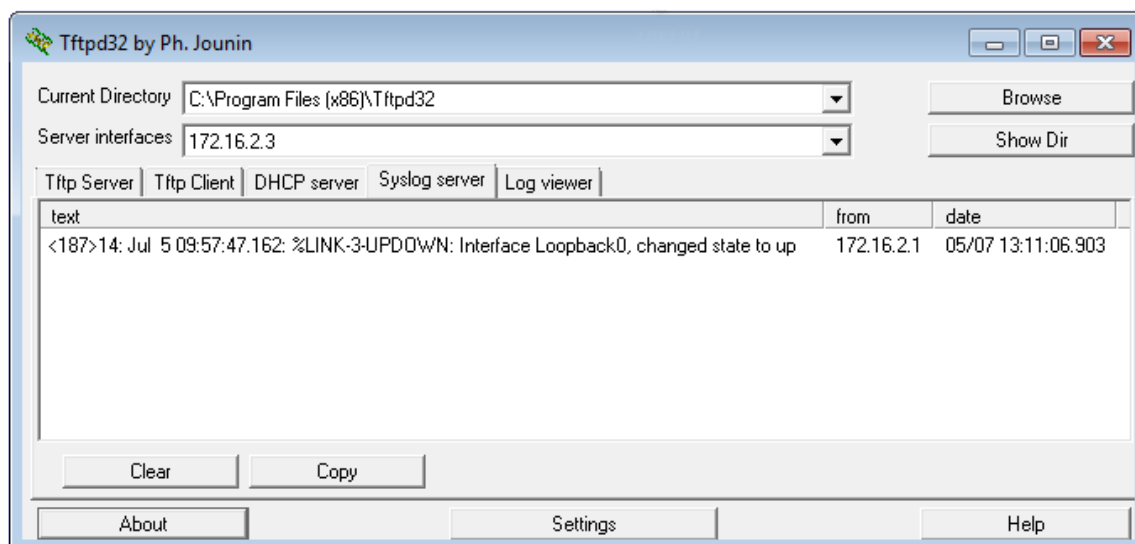
```
R2(config)# logging trap 4
```

- c. Создайте интерфейс Loopback0 на маршрутизаторе R2 и просмотрите сообщения журнала как в окне терминала, так и в окне сервера Syslog на ПК В.

```

R2(config)# interface lo 0
R2(config-if)#
Jul 5 09:57:47.162: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
Jul 5 09:57:48.162: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up

```



- d. Удалите интерфейс Loopback 0 на маршрутизаторе R2 и просмотрите сообщения журнала.

```
R2(config-if)# no interface lo 0
```

```
R2(config)#
```

```
Jul 5 10:02:58.910: %LINK-5-CHANGED: Interface Loopback0, changed state to administratively down
```

```
Jul 5 10:02:59.910: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to down
```

Отображаются ли какие-либо сообщения на сервере Syslog при выборе уровня серьезности 4? Если какие-либо сообщения журнала отображаются, объясните, какие сообщения отображаются и почему.

---



---



---

- e. Укажите уровень важности для журналирования равный 6.

```
R2(config)# logging trap informational
```

или

```
R2(config)# logging trap 6
```

- f. Удалите все записи в журнале Syslog на компьютере PC-B. Для этого щелкните **Clear** (Очистить) в диалоговом окне Tftpd32.

- g. Создайте интерфейс Loopback 1 на маршрутизаторе R2.

```
R2(config)# interface lo 1
```

```
Jul 5 10:05:46.650: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
```

```
Jul 5 10:05:47.650: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
```

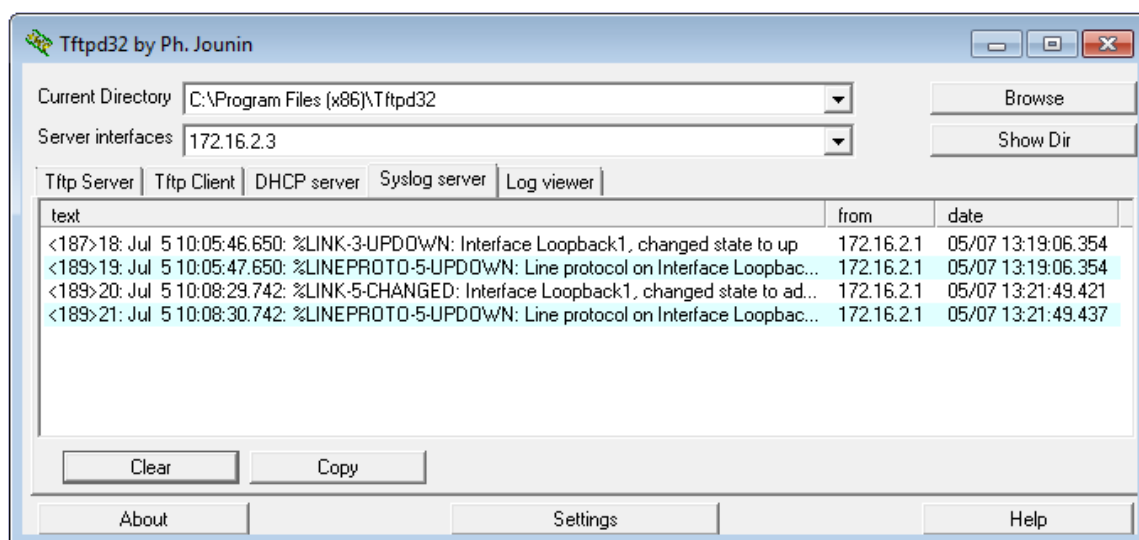
- h. Удалите интерфейс Loopback 1 с маршрутизатора R2.

```
R2(config-if)# no interface lo 1
```

```
R2(config-if)#
```

```
Jul 5 10:08:29.742: %LINK-5-CHANGED: Interface Loopback1, changed state to administratively down
```

```
Jul 5 10:08:30.742: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to down
```



- i. Проанализируйте выходные данные сервера Syslog. Сравните эти результаты с результатами на уровне важности 4. Каковы ваши наблюдения?

---



---



---

### Вопросы для повторения

Какая проблема возникает при настройке слишком высокого (самый маленький номер) или слишком низкого (самый большой номер) уровня важности для Syslog?

---



---



---

### 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 (S0/1/0)          | 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 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.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

для обучающихся по организации и проведению самостоятельной работы  
по дисциплине «Защищенные локальные вычислительные сети»

для студентов направления подготовки  
10.03.01 «Информационная безопасность»

Направленность (профиль):

«Организация и технологии защиты информации (по отрасли или в сфере  
профессиональной деятельности)»

## **СОДЕРЖАНИЕ**

Введение

Общая характеристика самостоятельной работы студента

Технологическая карта самостоятельной работы студента

Порядок выполнения самостоятельной работы

Список рекомендуемой литературы

## **ВВЕДЕНИЕ**

*Целью* изучения дисциплины «Защищенные локальные вычислительные сети» является формирование набора профессиональных компетенций будущего бакалавра, способствующих углубленной подготовке к решению профессиональных задач по созданию, сопровождению и защите локальных вычислительных сетей, а также приобретение набора профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 Информационная безопасность.

*Задачами* дисциплины являются:

1. Подготовка бакалавров к выявлению сущности проблем, возникающих в процессе развертывания, настройки и сопровождения вычислительных сетей.
2. Теоретическая и практическая подготовка бакалавров к настройке и применению специфического аппаратного обеспечения вычислительных сетей
3. Мотивация студентов к деятельности исследовательского характера для развития их творческих способностей, а также инициирование самообразовательной деятельности в освоении предметной области, касающейся вопросов построения защищенных вычислительных сетей.

### **1. Общая характеристика самостоятельной работы студента**

Самостоятельная работа включает те разделы курса, которые не получили достаточного освещения на лекциях по причине ограниченности лекционного времени и большого объема изучаемого материала.

Методическое обеспечение самостоятельной работы по дисциплине состоит из:

- 1) Определения учебных вопросов, которые студенты должны изучить самостоятельно;
  - 2) Подбора необходимой учебной литературы, обязательной для проработки и изучения;
  - 3) Поиска дополнительной научной литературы, к которой студенты могут обращаться по желанию, если у них возникает интерес в данной теме;
  - 4) Определения контрольных вопросов, позволяющих студентам самостоятельно проверить качество полученных знаний;
  - 5) Организации консультаций преподавателя со студентами для разъяснения вопросов, вызвавших у обучающихся затруднения при самостоятельном освоении учебного материала.
- Самостоятельная работа студента – это особым образом организованная деятельность, включающая в свою структуру такие компоненты, как:
- уяснение цели и поставленной учебной задачи;
  - четкое и системное планирование самостоятельной работы;
  - поиск необходимой учебной и научной информации;
  - освоение собственной информации и ее логическая переработка;
  - использование методов исследовательской, научно-исследовательской работы для решения поставленных задач;
  - выработка собственной позиции по поводу полученной задачи;
  - представление, обоснование и защита полученного решения;
  - проведение самоанализа и самоконтроля

**К основным видам самостоятельной работы студентов относится:**

- работа с понятийным аппаратом;
- конспектирование первоисточников;
- проектирование фрагментов исследовательской деятельности;
- подготовка доклада по теме.

Контроль знаний студентов включает формы текущего и итогового контроля. Текущий контроль осуществляется в процессе изучения курса и включает в себя оценку работы студентов на практических занятиях (круглый стол, собеседование, групповые научные проекты, тестирование), а также подготовку домашнего задания.

### **2. Технологическая карта самостоятельной работы студента**

| Коды<br>реализуемых<br>копетенций                | Вид<br>деятельности<br>студентов         | Итоговый<br>продукт<br>самостоятельной<br>работы | Средства и<br>технологии оценки | Объем часов, в том числе |                                          |       |
|--------------------------------------------------|------------------------------------------|--------------------------------------------------|---------------------------------|--------------------------|------------------------------------------|-------|
|                                                  |                                          |                                                  |                                 | СРС                      | Контактная<br>работа с<br>преподавателем | Всего |
| 3 семестр                                        |                                          |                                                  |                                 |                          |                                          |       |
| ПК-1 ИД-2<br>ПК-2 ИД-1<br>ПК-2 ИД-2<br>ПК-2 ИД-3 | Подготовка к<br>практическому<br>занятию | Отчет по<br>Практической<br>работе               | Собеседование                   | 16.00                    | 2.00                                     | 18.00 |
| ПК-1 ИД-2<br>ПК-2 ИД-1<br>ПК-2 ИД-2<br>ПК-2 ИД-3 | Подготовка к<br>лекции                   | Конспект лекций                                  | Собеседование                   | 16.00                    | 2.00                                     | 18.00 |
| Итого за 3 семестр                               |                                          |                                                  |                                 | 32.00                    | 4.00                                     | 36.00 |
| 4 семестр                                        |                                          |                                                  |                                 |                          |                                          |       |
| ПК-1 ИД-2<br>ПК-2 ИД-1<br>ПК-2 ИД-2<br>ПК-2 ИД-3 | Подготовка к<br>практическому<br>занятию | Отчет по<br>Практической<br>работе               | Собеседование                   | 16.00                    | 2.00                                     | 18.00 |
| ПК-1 ИД-2<br>ПК-2 ИД-1<br>ПК-2 ИД-2<br>ПК-2 ИД-3 | Подготовка к<br>лекции                   | Конспект лекций                                  | Собеседование                   | 16.00                    | 2.00                                     | 18.00 |
| ПК-1 ИД-2<br>ПК-2 ИД-1<br>ПК-2 ИД-2<br>ПК-2 ИД-3 | Подготовка к<br>экзамену                 | Экзамен                                          | Вопросы к экзамену              | 16.00                    | 2.00                                     | 18.00 |
| Итого за 4 семестр                               |                                          |                                                  |                                 | 48.00                    | 6.00                                     | 54.00 |
| Итого                                            |                                          |                                                  |                                 | 80.00                    | 10.00                                    | 90.00 |

### 3. Порядок выполнения самостоятельной работы

#### 3.1 Методические рекомендации по изучению теоретического материала

Комплексное изучение предлагаемой студентам учебной дисциплины «Защищенные локальные вычислительные сети» предполагает овладение материалами лекций, учебников, программы, творческую работу студентов в ходе проведения практических занятий, а также систематическое выполнение заданий для самостоятельной работы.

В ходе лекций раскрываются основные вопросы в рамках рассматриваемых тем, делаются акценты на наиболее сложные и интересные положения изучаемого материала, которые должны быть приняты студентами во внимание. Материалы лекций являются основой для подготовки студентов к практическим занятиям.

#### **Работа с конспектом лекций**

Просмотрите конспект сразу после занятий. Отметьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале,

сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю.

Каждую неделю отводите время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам и тестам.

### ***Выполнение практических занятий по дисциплине «Защищенные локальные вычислительные сети»***

На первом занятии получите у преподавателя задания по курсу, планы подготовки к практическим занятиям. Обзаведитесь всем необходимым методическим обеспечением.

Перед практическими занятиями изучите теорию вопроса, предполагаемого к исследованию, ознакомьтесь с опытом других исследователей в этом направлении.

Целью практических занятий является:

- закрепление методов приложения теории к решению практических задач анализа и синтеза психологического знания;
- проверка уровня понимания студентами вопросов, рассмотренных на лекциях и по учебной литературе, степени и качества усвоения материала;
- обучение навыкам освоения методики эксперимента и работы с нормативно-справочной литературой;
- восполнение пробелов в пройденной теоретической части курса и оказание помощи в его усвоении.

### ***3.2 Методические рекомендации по конспектированию первоисточников***

Изучение и анализ литературных источников является обязательным видом самостоятельной работы студентов. Изучение литературы по избранной теме имеет своей задачей проследить характер постановки и решения определенной проблемы различными авторами, аргументацию их выводов и обобщений, провести анализ и систематизировать полученный материал на основе собственного осмысления с целью выяснения современного состояния вопроса.

Проработка отобранного материала обязательно должна идти с одновременным ведением записей прочитанного и своих замечаний. Запись может иметь как форму конспекта, так и выписок, а также картотеку положений, тезисов, идей, методик, что в дальнейшем облегчит классификацию и систематизацию полученного материала. Такого рода записи являются лучшим способом накопления и первичной обработки материала, одной из обязательных форм организации умственного труда.

**Планом** удобно пользоваться при подготовке к устному выступлению по выбранной теме. Каждый пункт плана должен раскрывать одну из сторон избранной темы, а весь план должен охватывать ее целиком.

**Тезисы** предполагают сжатое изложение основных положений текста в форме утверждения или отрицания. Они являются более совершенной формой записей и представляют основу для дискуссии. К тому же их легко запомнить.

**Конспектирование** – процесс мысленной переработки и письменной фиксации информации, в виде краткого изложения основного содержания, смысла какого-либо текста.

Результат конспектирования – запись, позволяющая конспектирующему немедленно или через некоторый срок с нужной полнотой восстановить полученную информацию. Конспект в переводе с латыни означает «обзор». По существу его и составлять надо как обзор, содержащий основные мысли текста без подробностей и второстепенных деталей. Конспект носит индивидуализированный характер: он рассчитан на самого автора и поэтому может оказаться малопонятным для других.

Для того чтобы осуществлять этот вид работы, в каждом конкретном случае необходимо грамотно решить следующие задачи:

1. Сориентироваться в общей композиции текста (уметь определить вступление, основную часть, заключение).
2. Увидеть логико-смысловую канву сообщения, понять систему изложения автором информации в целом, а также ход развития каждой отдельной мысли.

3. Выявить «ключевые» мысли, т. е. основные смысловые вехи, на которые «нанизано» все содержание текста.
4. Определить детализирующую информацию.
5. Лаконично сформулировать основную информацию, не перенося на письмо все целиком и дословно.

Во всяком научном тексте содержится информация 2-х видов: основная и вспомогательная. Основной является информация, имеющая наиболее существенное значение для раскрытия содержания темы или вопроса. К ней относятся: определения научных понятий, формулировки законов, теоретических принципов и т. д. Назначение вспомогательной информации – помочь читателю лучше усвоить предлагаемый материал. К этому типу информации относятся разного рода комментарии. Основную – записываем как можно полнее, вспомогательную, как правило, опускаем. Содержание конспектирования составляет переработка основной информации в целях ее обобщения и сокращения. Обобщить – значит представить ее в более общей, схематической форме, в виде тезисов, выводов, отдельных заголовков, изложения основных результатов и т. п. Читая, мы интуитивно используем некоторые слова и фразы в качестве опорных. Такие опорные слова и фразы называются ключевыми. Ключевые слова и фразы несут основную смысловую и эмоциональную нагрузку содержания текста.

Выбор ключевых слов – это первый этап смыслового свертывания, смыслового сжатия материала. Важными требованиями к конспекту являются наглядность и обозримость записей и такое их расположение, которое давало бы возможность уяснить логические связи и иерархию понятий.

**По форме конспекты подразделяются на формализованные и графические.**

**1. Формализованные** (все записи вносятся в заранее подготовленные таблицы).

Это удобно, во-первых, при конспектировании материалов, когда перечень характеристик описываемых предметов или явлений более или менее постоянен, во-вторых, при подготовке единого конспекта по нескольким источникам. Особенно если есть необходимость сравнения отдельных данных.

Разновидностью формализованного конспекта является запись, составленная в форме ответов на заранее подготовленные вопросы, обеспечивающие исчерпывающие характеристики однотипных предметов или явлений.

**2. Графические** (элементы конспектируемой работы располагаются в таком виде, при котором видна иерархия понятий и взаимосвязь между ними).

По каждой работе может быть не один, а несколько графических конспектов, отображающих книгу в целом и отдельные ее части. Ведение графического конспекта - наиболее совершенный способ изображения внутренней структуры книги, а сам этот процесс помогает усвоению ее содержания. Можно выделить следующие основные **типы конспектов: плановый, текстуальный, сводный, тематический.**

**Плановый** – легко получить с помощью предварительно сделанного плана произведения, каждому вопросу плана отвечает определенная часть конспекта:

а) вопросно-ответный (на пункты плана, выраженные в вопросительной форме, конспект дает точные ответы);

б) схематичный плановый конспект (отражает логическую структуру и взаимосвязь отдельных положений).

**Текстуальный** – это конспект, созданный в основном из цитат.

**Сводный конспект** – сочетает выписки, цитаты, иногда тезисы; часть его текста может быть снабжена планом.

**Тематический** – дает более или менее исчерпывающий ответ (в зависимости из числа привлеченных источников и другого материала, например, своих же записей) на поставленный вопрос – тему: обзорный; хронологический.

Роль конспекта – чисто учебная: он помогает зафиксировать основные понятия и положения первичного текста и в нужный момент их воспроизвести, например, при написании реферата или подготовке к экзамену.

**Способы конспектирования.**

- **Тезисы** – это кратко сформулированные основные мысли, положения изучаемого материала. Тезисы лаконично выражают суть читаемого, дают возможность раскрыть содержание. Приступая к освоению записи в виде тезисов, полезно в самом тексте отмечать места, наиболее четко формулирующие основную мысль, которую автор доказывает (если, конечно, это не библиотечная книга). Часто такой

отбор облегчается шрифтовым выделением, сделанным в самом тексте.

- **Линейно-последовательная запись текста.** При конспектировании линейно – последовательным способом целесообразно использование плакатно-оформительских средств, которые включают в себя следующие:

- сдвиг текста конспекта по горизонтали, по вертикали;
- выделение жирным (или другим) шрифтом особо значимых слов;
- использование различных цветов;
- подчеркивание;
- заключение в рамку главной информации.

- **Способ «вопросов – ответов».** Он заключается в том, что, поделив страницу тетради пополам вертикальной чертой, конспектирующий в левой части страницы самостоятельно формулирует вопросы или проблемы, затронутые в данном тексте, а в правой части дает ответы на них.

Одна из модификаций способа «вопросов – ответов» - таблица, где место вопроса занимает формулировка проблемы, поднятой автором (лектором), а место ответа – решение данной проблемы. Иногда в таблице могут появиться и дополнительные графы: например, «мое мнение» и т. п.

- **Схема с фрагментами** – способ конспектирования, позволяющий ярче выявить структуру текста, - при этом фрагменты текста (опорные слова, словосочетания, пояснения всякого рода) в сочетании с графикой помогают созданию рационально - лаконичного конспекта.

- **Простая схема** – способ конспектирования, близкий к схеме с фрагментами, объяснений к которой конспектирующий не пишет, но должен уметь давать их устно. Этот способ требует высокой квалификации конспектирующего. В противном случае такой конспект нельзя будет использовать.

- **Параллельный способ** конспектирования. Конспект оформляется на двух листах параллельно или один лист делится вертикальной чертой пополам и записи делаются в правой и в левой части листа.

**Однако лучше использовать разные способы конспектирования для записи одного и того же материала.**

**Комбинированный конспект** – вершина овладения рациональным конспектированием. При этом умело используются все перечисленные способы, сочетая их в одном конспекте (один из видов конспекта свободно перетекает в другой в зависимости от конспектируемого текста, от желания и умения конспектирующего). Именно при комбинированном конспекте более всего проявляется уровень подготовки и индивидуальность студента.

## **Принципы составления конспекта прочитанного.**

1. Записать все выходные данные источника: автор, название, год и место издания. Если текст взят из периодического издания (газеты или журнала), то записать его название, год, месяц, номер, число, место издания.

2. Выделить поля слева или справа, можно с обеих сторон. Слева на полях отмечаются страницы оригинала, структурные разделы статьи или книги (названия параграфов, подзаголовки и т. п.), формулируются основные проблемы. Справа – способы фиксации прочитанной информации.

Один из видов чтения – углубленное – предполагает глубокое усвоение прочитанного и часто сохранение информации в целях последующего обращения к ней. Эффективность такого чтения повышается, если прочитанное зафиксировано не только в памяти, но и на бумаге. Психологи утверждают, что записанное лучше и полнее усваивается, прочнее откладывается в памяти.

Установлено, что если прочитать 1000 слов и затем записать 50, подытоживающих прочитанное, то коэффициент усвоения будет выше, чем, если прочитать 10000 слов, не записав ни одного. Кроме того, при записи прочитанного формируется навык свертывания информации. И, наконец, чередование чтения и записывания уменьшает усталость, повышает работоспособность и производительность умственного труда.

### *1. Резюмирование.*

Резюме – краткий итог прочитанного, содержащий его оценку. Резюме характеризует основные выводы книги, главные итоги.

Выбор языковых средств для построения резюме-выводов подчинен основной задаче свертывания информации: минимум языковых средств – максимум информации. Это обычно одно – три четких, кратких, выразительных предложения, раскрывающих, по мнению автора, самую суть описываемого объекта.

## *2. Аннотация.*

Аннотация – краткая обобщенная характеристика печатной работы (книги, статьи), включающая иногда и его оценку. Это наикратчайшее изложение содержания первичного документа, дающее общее представление о теме.

Основное ее назначение – дать некоторое представление о книге (статье, научной работе) с тем, чтобы рекомендовать ее определенному кругу читателей или воспользоваться своими записями при выполнении работы исследовательского, реферативного характера. Поэтому аннотации не требуется изложения содержания произведения, в ней лишь перечисляются вопросы, которые освещены в первоисточнике (содержание этих вопросов не раскрывается). Аннотация отвечает на вопрос: «О чем говорится в первичном тексте?», дает представление только о главной теме и перечне вопросов, затрагиваемых в тексте первоисточника.

Текст аннотации не стандартизирован. В научной литературе можно встретить различные требования к составлению аннотаций. Например, текст справочной аннотации может включать следующие сведения:

- тип и название аннотируемого документа (монография, диссертация, сборник, статья и т. п.)
- задачи, поставленные автором аннотируемого документа
- метод, которым пользовался автор (эксперимент, сравнительный анализ, компиляция других источников)
- принадлежность автора к определенной научной школе или направлению
- структуру аннотируемого документа
- предмет и тему произведения, основные положения и выводы автора
- характеристику вспомогательных иллюстративных материалов, дополнений, приложений, справочного аппарата, включая указатели и библиографию.

## **Вопросы для собеседования по практическим занятиям**

### **Задания базового уровня:**

1. Протестируйте кроссовый кабель Ethernet с помощью устройства для проверки кабелей.
2. Соедините два ПК с помощью кроссового кабеля Ethernet
3. Из командной строки ПК-А отправьте эхо-запрос с помощью команды ping на IP-адрес ПК-Б.
4. Настройте свой ПК с одним из IP-адресов, указанных в таблице адресации.
5. Изобразить цветовую схему и расположение выводов для стандарта 568-В.
6. Изобразить цветовую схему и расположение выводов для стандарта 568-А.
7. Выполните инициализацию и перезапуск маршрутизатора и коммутатора.
8. Назначьте интерфейсам ПК статическую информацию IP-адреса.
9. Настройте маршрутизатор.
10. Проверьте подключение к сети.
11. Подключите консоль к маршрутизатору и активируйте привилегированный режим.
12. Настройте на маршрутизаторе
13. Продемонстрировать захват пакетов TCP с использованием Wireshark.
14. Продемонстрировать захват пакетов UDP с использованием Wireshark.
15. Продемонстрировать захват пакетов DNS с использованием Wireshark.
16. Продемонстрировать захват пакетов ICMP с использованием Wireshark.
17. Продемонстрировать захват пакетов SNMP с использованием Wireshark.
18. Продемонстрировать захват пакетов ARP с использованием Wireshark.
19. Определите сетевую и узловую части IP-адреса.

20. Определите диапазон адресов узлов с использованием пары маски сети и префикса.
21. Определите тип адреса (адрес сети, узла, многоадресной или широковещательной рассылки).
22. Проверьте настройки сетевого IPv6-адреса на компьютере.
23. Проанализируйте правила сокращения IPv6-адресов.
24. Отработайте сворачивание и развёртывание IPv6-адресов
25. Определите количество созданных подсетей.
26. Определите количество узлов для каждой подсети.
27. Определите адрес подсети.
28. Определите диапазон узлов для подсети.
29. Определите широковещательный адрес для подсети
30. Назовите быстрый способ вычисления сетевых адресов для последовательных подсетей

/30

31. Настройте доступ по протоколу SSH на коммутаторе
32. Измените параметры SSH на коммутаторе.
33. Проверьте конфигурацию SSH на коммутаторе.
34. Настройте на коммутаторе IP-адрес интерфейса административной сети VLAN 99
35. Настройте новый MAC-адрес для интерфейса
36. На маршрутизаторе выключите интерфейс G0/1, удалите жёстко запрограммированный MAC-адрес из маршрутизатора и повторно включите интерфейс G0/1
37. Удалите IP-адрес для сети VLAN 1 на коммутаторе.
38. Добавьте сеть VLAN 30 в интерфейс, не вводя команду сети VLAN.
39. Поясните назначение команды **switchport mode dynamic desirable**.
40. Поясните назначение команды **switchport mode trunk**
41. Удалите базу данных VLAN
42. Поясните, что нужно для того, чтобы узлы в сети VLAN 10 могли обмениваться данными с узлами в сети VLAN 20
43. Проверьте состояние интерфейсов на маршрутизаторе R1 с помощью команды **show ip interface brief**.
44. Просмотрите таблицу маршрутизации на маршрутизаторе R1 с помощью команды **show ip route**.
45. На маршрутизаторе R1 настройте статический маршрут к сети 198.133.219.0, указывая один из параметров настройки статического маршрута.
46. Удалите статические маршруты для loopback-адресов.
47. На маршрутизаторе настройте маршрут по умолчанию, используя выходной интерфейс S0/0/1.
48. Пояснить структуру таблицы Db.
49. Настройте **logging synchronous** для консольного канала.
50. Отобразите изменения идентификатора маршрутизатора для соседних маршрутизаторов.
51. Измените идентификатор маршрутизатора R1 с помощью команды router-id.
52. Пояснить команду **clear ip ospf process**.
53. Настройте пассивный интерфейс в OSPF.
54. Измените заданную пропускную способность на маршрутизаторах.
55. Настройте и проверьте работу маршрутизации RIPv2 на маршрутизаторах.
56. Настройте пассивный интерфейс.
57. Отключите автоматическое суммирование маршрутов.
58. Настройте маршрут по умолчанию.
59. Проверьте наличие сквозного соединения.
60. Настройте и проверьте работу маршрутизации RIPv6 на маршрутизаторах.
61. Создайте базу данных локального пользователя с именем пользователя **admin** и паролем **classadm**.
62. Активируйте возможность входа на линии VTY с помощью локальной базы данных.
63. Измените настройку линий VTY transport input на настройку all только для протоколов SSH и Telnet.
64. Создайте ACL-список, в соответствии с которым доступ к маршрутизатору R1 через Telnet разрешён только для узлов из сети 2001:db8:acad:a::/64.
65. Создайте ACL-список под именем RESTRICTED-LAN, который заблокирует доступ через

Telnet к сети 2001:db8:acad:a::/64.

66. Создайте новую запись в ACL-списке, используя последовательную нумерацию.
67. Пояснить команду **ipv6 address autoconfig**.
68. Убедитесь, что SLAAC предоставил коммутатору S1 индивидуальный адрес.
69. Убедитесь, что SLAAC предоставил информацию об IPv6-адресе компьютеру.
70. Настройте сервер DHCP IPv6 на маршрутизаторе.
71. Проверьте настройки DHCPv6 на интерфейсе G0/1 маршрутизатора.
72. Пояснить, какой метод IPv6-адресации использует больше ресурсов памяти маршрутизатора, настроенного в качестве сервера DHCPv6.
73. Настройте статическое сопоставление NAT.
74. Проверьте статистику NAT, выполнив команду **show ip nat statistics** на шлюзовом маршрутизаторе.
75. Создайте ACL-список, который соответствует диапазону частных IP-адресов локальной сети.
76. Определите пул пригодных к использованию публичных IP-адресов.
77. Удалите запись статического NAT.
78. Проверьте конфигурацию NAT-пула с перегрузкой.

#### **Задания повышенного уровня:**

79. Изготовьте и обработайте разъём кабеля TIA/EIA 568-A.
80. Изготовьте и обработайте разъём кабеля TIA/EIA 568-B.
81. Выведите на маршрутизатор сведения об интерфейсе.
82. Выведите на маршрутизатор и коммутатор сводный список интерфейсов.
83. Захватите данные веб-сеанса на узле [www.google.com](http://www.google.com).
84. Изучите содержащиеся в пакетах данные, включая IP-адреса, номера портов TCP и флажки управления TCP.
85. Сопоставьте IPv6-адрес с правильным типом адреса.
86. Отработайте извлечение данных сетевого префикса из IPv6-адреса
87. Создайте сеть в соответствии с изображенной на схеме топологией.
88. Определите количество доступных адресов узлов и подсетей.
89. Настройте и проверьте общие функции безопасности.
90. Настройте и проверьте функцию безопасности порта.
91. Создайте сети VLAN на коммутаторе
92. Назначьте сети VLAN интерфейсам на коммутаторе.
93. На маршрутизаторе настройте статический маршрут к сети 192.168.1.0, используя IP-адрес последовательного интерфейса Serial 0/0/0 маршрутизатора в качестве адреса следующего перехода
94. На маршрутизаторе настройте статический маршрут к сети 198.133.219.0, указывая один из параметров настройки статического маршрута
95. Настройте протокол IPv6 на маршрутизаторах.
96. Настройте маршрутизацию RIPv6
97. Настройте маршрутизацию OSPF на маршрутизаторе.
98. Измените идентификаторы маршрутизатора, используя loopback-адреса.
99. Настройте индивидуальный IPv6-адрес на интерфейсах G0/0, G0/1 и S0/0/0.
100. Настройте локальный IPv6-адрес канала на интерфейсах G0/0, G0/1 и S0/0/0. На всех трёх интерфейсах используйте FE80:: 1 в качестве локального адреса канала..
101. Измените пул DHCPv6 на маршрутизаторе.
102. Проверьте настройки DHCPv6 с отслеживанием состояния на маршрутизаторе.
103. Определите соответствие в NAT внутреннего списка адресов источника и пула внешних адресов.
104. От компьютера PC-A отправьте сообщение по Telnet на интерфейс интернет-провайдера и отобразите таблицу NAT

### **3.3 Методические указания по подготовке к экзамену**

Контроль и оценка знаний студентов является неотъемлемой составной частью учебно-воспитательного процесса в вузе. Экзаменационная сессия – самая ответственная пора в студенческой

жизни: она является итогом большой работы студентов в семестре. Экзамен – это метод проверки знаний студентов по части или полному курсу учебной дисциплины, произведенный путем постановки устных или письменных вопросов. Он дает объективную официально фиксируемую оценку успехов студентов за определенный отрезок времени.

Экзамен преследует многогранную цель: во-первых, это – проверка знаний студента, во-вторых, они сами по себе являются важным звеном в овладении наукой, в-третьих, это продолжение учебного процесса; наконец, он имеет большое значение как фактор стимулирования глубокого изучения предмета.

Подготовка к экзамену состоит из двух взаимосвязанных этапов. Первый – систематический труд на протяжении семестра, учебного года, охватывающий все формы учебного процесса: лекции, изучение и конспектирование рекомендованной литературы, активное участие в семинарских (практических) и лабораторных занятиях.

Второй – подготовка непосредственно перед экзаменом. Она позволяет студентам за сравнительно короткий отрезок времени охватить всю перспективу изученного и лучше понять основные закономерности и явления.

Ограниченность времени (3-4 дня) для непосредственной подготовки к экзамену по предмету требует от студентов спокойно, без нервной суеты и спешки еще раз внимательно продумать изученный в течение семестра материал, тщательно отработать вопросы, недостаточно изученные или плохо понятые, с тем, чтобы по возможности устранить все пробелы в своих знаниях.

Готовиться надо по строго продуманному графику, последовательно переходя от темы к теме, не пропуская ни одну из них.

Сложные вопросы, недостаточно уясненные в процессе подготовки к экзамену, необходимо записать и получить на них разъяснения у преподавателей во время предэкзаменационных консультаций.

Следует заметить, что студенты, которые не ходят на консультации из-за отсутствия, по их мнению, сложных вопросов, поступают опрометчиво. На консультациях очень часто лектор не только отвечает на заданные вопросы, но и по собственной инициативе разъясняет наиболее трудные разделы курса.

Итак, основной задачей подготовки студентов к экзамену является систематизация знаний учебного материала, его творческое осмысливание. Важнейшим учебным пособием на этом этапе работы студента является собственный конспект прослушанных лекций и самостоятельно проработанных тем курса.

В соответствии с положением об экзаменах их, как правило, принимают преподаватели, читающие курс лекций.

Получив билет, студент должен хорошо продумать содержание поставленных вопросов. Значительное число неудачных ответов объясняется неясным пониманием поставленной проблемы. Правильное понимание вопроса обеспечит успех при ответе на него. При подготовке к ответу на билет нужно составить развернутый план по каждому вопросу.

Отвечая на вопросы экзаменационного билета, не следует спешить. Надо излагать материал спокойно, не торопясь, владеть собой, следить за построением фраз. Следует избегать подходов издали, общих рассуждений. Рекомендуется строить ответы четко, последовательно, конкретно, по возможности исчерпывающе. Вместе с тем весьма желательно быстро и правильно иллюстрировать свой ответ примерами.

От экзаменуемого требуется: определение понятий, обоснование выдвинутых положений, свободное оперирование фактическим материалом, дать альтернативные подходы по отдельным проблемам. Логичность, стройность, литературная грамотность изложения являются неотъемлемыми чертами полноценного ответа. Нельзя при ответе допускать ни излишней краткости, переходящей в схематизм, ни многословия. И то, и другое не оправдано. Краткость не дает преподавателю возможности понять, владеет ли студент учебным материалом, а многословие может показать, что студент не умеет акцентировать внимание на главном и говорит слишком расплывчато.

## **Вопросы к экзамену**

### **Базовый уровень:**

#### **Вопросы для проверки уровня обученности**

1. Персональные компьютеры и приложения.

2. Двоичное представление данных.
3. Компоненты компьютера и периферийные устройства.
4. Выбор, установка и обслуживание операционной системы.
5. Принципы связи и обмен данными в локальной проводной сети.
6. Создание уровня доступа и распределения в сети Ethernet.
7. Планирование структуры локальной сети и подключение устройств.
8. Сетевые устройства в НОС. Кабели и контакты.
9. Прокладка кабелей "витая пара".
10. IP-адреса и маски подсети.
11. Типы IP-адресов.
12. Получение IP-адресов и управление ими.
13. Взаимодействие клиентов и серверов.
14. Прикладные протоколы и сервисы.
15. Многоуровневая модель и протоколы.
16. Беспроводные локальные сети.
17. Обеспечение безопасности беспроводной локальной сети.
18. Настройка интегрированной точки доступа и беспроводного клиента.
19. Сетевые угрозы.
20. Методы атак.
21. Политика безопасности.
22. Использование межсетевых экранов.
23. Устранение проблем с сетями.
24. Общие проблемы, процесс и задачи устранения проблем.
25. Устранение неполадок и справочная служба.
26. Поставщики услуг Интернета (ISP).
27. Связь с поставщиком интернет-услуг.
28. Модель OSI.
29. Устранение неполадок на уровне поставщика интернет-услуг.
30. Общие проблемы и планирование обновления сети.
31. Приобретение и обслуживание оборудования.
32. IP-адресация в ЛВС.
33. NAT и PAT.

### **Список рекомендуемой литературы**

#### **1. Основная литература**

1. Информатика : учеб. пособие / И. П. Хвостова, И.М. Ратнер, И. И. Каргина [и др.] ; ГОУ ВПО Сев. Кав. гос. техн. ун-т, Ч. 3 . - Ставрополь : Изд-во СевКавГТУ, 2013. - 224 с. : ил. - Библиогр.: с. 232-233
2. Основы компьютерного моделирования: учебное пособие / К. А. Катков, И. П. Хвостова, В. И. Лебедев, Е. Н. Косова, А. А. Плетухина, О. Л. Серветник, О. В. Вельц, М. Г. Крамаренко. – Ставрополь : Изд-во СКФУ, 2018. – 273 с.
3. Акулов, О.А. Информатика : базовый курс : учебник / О.А. Акулов, Н.В. Медведев . - 5-е изд., исправ. и доп. - М. : Омега-Л, 2013. - 574 с. : ил. ; 22. - (Высшее техническое образование). - Библиогр.: с. 573-574 (28 назв.). - ISBN 978-5-365-00901-1

#### **2. Дополнительная литература**

1. Информатика : учеб. пособие / В. И. Лебедев, Е. Н. Косова, И. П. Хвостова и др. ; ГОУ ВПО Сев. Кав. гос. техн. ун-т, Ч. 1 . - Ставрополь : Изд-во СевКавГТУ, 2014. - 240 с. : ил. - Библиогр.: с. 238-239
2. Информатика : учеб. пособие / В. И. Лебедев, Е. Н. Косова, И. П. Хвостова [и др.] ; ГОУ ВПО Сев. Кав. гос. техн. ун-т, Ч. 2 . - Ставрополь : Изд-во СевКавГТУ, 2014. - 232 с. : ил. - Библиогр.: с. 230-231
3. Агальцов, В. П. Информатика для экономистов : учебник для студ. вузов / В. П. Агальцов, В. М. Титов . - Москва : ФОРУМ : ИНФРА-М, 2016. - 447 с. : ил. - (Высшее образование). - Указ.: с. 443-445. - Библиогр.: с. 420 (15 назв.). - ISBN 5-8199-0274-

4. Курилович, В. Информатика в задачах, примерах, алгоритмах / Вик Курилович . - М. : СОЛОН-Р, 2005. - 143 с. - (Библиотека студента и школьники). - ISBN 5-93455-193-0
5. Залогова, Л. А. Компьютерная графика : практикум / Л. А. Залогова . - 2-е изд. - М. : БИНОМ. Лаборатория знаний, 2013. - 245 с. - (Информатика. Элективный курс). - ISBN 978-5-94774-656-3
6. Информатика : учебник для студентов вузов / [Н. В. Макарова, Л. А. Матвеев, В. Л. Бройдо и др.] ; под ред. проф. Н. В. Макаровой . - 3-е перераб. изд. - М. : Финансы и статистика, 2014. - 768 с. : схем. - Библиогр. в конце гл. - Предм. указ.: с. 7
7. Могилев, А. В. Информатика : учеб. пособие для вузов / А. В. Могилев, Е. К. Хеннер, Н. И. Пак, ; под ред. А. В. Могилева . - М. : Академия, 2016. - 327 с. : ил., табл. - (Высшее профессиональное образование. Педагогические специальности). - Библио
8. Экономическая информатика : учебник для вузов / [В. П. Косарев и др.] ; под ред. В. П. Косарева . - 3-е изд., перераб. и доп. - М. : Финансы и статистика, 2016. - 656 с. - Библиогр.: с. 626-628. - Кратк. сл. термин.: с. 629-638.

### **3. Методическая литература**

Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : Питер, 2015. - 944 с.

### **4. Интернет-ресурсы:**

[www.netacad.com](http://www.netacad.com)

### **5. Программное обеспечение:**

Cisco Packet Tracer 6.11

Terra Term

GNS3

Wireshark

### **6. Материально-техническое обеспечение дисциплины (модуля)**

- учебная аудитория, оборудованная учебной мебелью и доской, ноутбук, проектор, экран
- компьютерный класс с выходом в Internet, комплект маршрутизаторов, коммутаторов и беспроводных ISR.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**  
по выполнению курсовой работы  
по дисциплине «Защищенные локальные вычислительные сети»  
для студентов направления подготовки  
10.03.01 «Информационная безопасность»  
Направленность (профиль)  
«Организация и технологии защиты информации (по отрасли или в сфере профессиональной  
деятельности)»

Ставрополь  
2026

## **1 Общие требования к выполнению курсовой работы**

Курсовая работа – обязательный вид учебной работы, выполняется студентом в течение семестра.

Курсовая работа является самостоятельной исследовательской работой студента и представляет собой логически завершенное и оформленное научное исследование. Курсовая работа направлена на формирование у студента навыков научно-исследовательской работы, повышение уровня его профессиональной (теоретической и практической) подготовки, углубление знаний по учебной дисциплине, развитие интереса и навыков самостоятельной работы с научной и справочной литературой.

### **1.1 Цели и задачи курсовой работы**

Выполнение курсовой работы имеет целью расширение знаний студентов, обучение методам теоретического анализа явлений и закономерностей науки, отработку навыков самостоятельного применения теоретических знаний к комплексному решению профессиональных задач, использования справочной литературы, методов математической обработки экспериментальных данных, компьютерных технологий.

Системой курсовых работ студент подготавливается к выполнению выпускной квалификационной работы.

В процессе выполнения курсовой работы студентом должны решаться следующие задачи:

- приобретение новых теоретических знаний в соответствии с темой работы и заданием руководителя;
- развитие умений систематизировать, обобщать и логично излагать концепции, альтернативные точки зрения исследуемых проблем;
- развитие учебно-исследовательских и методических умений, необходимых для построения системы научного анализа изучаемого аспекта;
- совершенствование профессиональной подготовки.

### **1.2 Тематика курсовых работ**

Одним из важных компонентов в системе постановки курсового проектирования (курсовой работы) является правильное определение тематики.

Тематика курсовых работ должна быть актуальной, отвечать учебным задачам данного предмета, а также потребностям науки и практики. Актуальность тематики курсовых работ - это, прежде всего, научность, современность и направленность к получению студентами навыков самостоятельной творческой работы.

Темы курсовых работ должны быть комплексными, т.е. содержать ряд взаимосвязанных между собой проблем и строиться на фактическом материале профильных предприятий и учреждений, а также на итогах учебной и производственной практики студентов, на научных работах членов кафедры, студенческих научных кружков и

проблемных групп, с использованием новейших достижений отечественной и зарубежной науки, актуальных прикладных аспектов.

Темы курсовых работ утверждаются на заседании кафедры, ведущей дисциплины, по которым учебными планами предусмотрены курсовые работы. Выписка из протокола заседания кафедры передается в дирекцию факультета, где формируется распоряжение об утверждении тем курсовых работ. В течение 10 дней после выхода распоряжения об утверждении тем курсовых работ специалист по учебно-методической работе дирекции вносит названия тем в автоматизированную базу университета.

Основные содержательные и процессуальные аспекты, необходимые для выполнения работы, оформляются кафедрой в заданиях на курсовую работу (Приложение А). В заданиях необходимо четко сформулировать название темы работы и требования, определяющие его объем, содержание, а также исходные данные для выполнения количественных расчетов.

### **1.3 Содержание и структура курсовых работ**

Курсовая работа (проект) должна содержать элементы новизны, наряду с фундаментальным аспектом должен быть проведен анализ современного состояния изучаемой проблемы, а также отражены региональные особенности.

Задание по курсовой работе необходимо индивидуализировать с учетом интересов и способностей студентов.

Курсовая работа (проект) должна состоять из:

- содержания;
- введения;
- теоретической части;
- эмпирической части;
- заключения;
- списка использованных источников;
- приложения.

В отдельных случаях, в соответствии с тематикой работы, эмпирическая часть может отсутствовать.

Титульный лист оформляется в соответствии с Приложением Б.

Содержание включает названия разделов, подразделов работы с указанием страницы начала каждой части (Приложение В).

Во введении обосновывается актуальность выбранной темы исследования; отражаются объект, предмет, задачи, цели, методы, новизна, теоретическая и практическая значимость исследования.

Теоретическая часть должна содержать анализ состояния изучаемой проблемы на основе обзора научной, научно-информационной, справочной литературы. Представленный материал должен быть логически связан с целью исследования. В параграфах теоретической части необходимо отражать отдельные компоненты проблемы и завершать их выводами.

Эмпирическая (практическая, расчетно-графическая) часть (при наличии) включает описание системы экспериментального исследования, обоснование методов исследования, анализ результатов экспериментального исследования, схемы, графические и математические способы интерпретации полученных данных, выводы.

Заключение содержит выводы, подтверждающие или опровергающие первоначальные предположения (гипотезы), перспективы дальнейшего изучения проблемы, связь с практикой, анализ реализации целей и задач исследования.

Список использованных источников должен содержать перечень всех используемых автором нормативных документов, монографий, учебных и учебно-методических пособий, статей и интернет-источников (Приложение Г).

При ссылке в тексте номер источника из списка литературы заключается в квадратные скобки, например, [1], [1, 3-4] или [1-2].

Приложение содержит весь фактический материал экспериментальных исследований (анкеты, опросники, схемы, чертежи, расчетные материалы, карты, рисунки, ответы респондентов и т.д.).

## **2. Рекомендации по подготовке и оформлению курсовой работы**

Курсовые работы (проекты) рекомендуется представлять в объеме 30-40 страниц. Текст работы должен быть напечатан через 1,5 интервала на одной стороне стандартного листа белой бумаги (А - 4).

Текст курсовой работы выполняют с использованием компьютера на одной стороне листа белой бумаги, формата А4, шрифт - Times New Roman 14-го размера, межстрочный интервал - 1,5. Номер страницы проставляют в правом нижнем углу листа. Страницы текстового материала следует нумеровать арабскими цифрами, соблюдая сквозную нумерацию по всему документу. Титульный лист текстового документа включают в общую нумерацию страниц. Номер страницы на титульном листе не проставляют. Расстояние от края бумаги до границ текста следует оставлять: в начале строк - 30 мм; в конце строк - 10 мм; от верхней или нижней строки текста до верхнего или нижнего края бумаги - 20 мм. Размер абзацного отступа должен быть одинаковым по всему тексту работы и равным 12,5 мм.

Разделы должны иметь порядковые номера в пределах всей курсовой работы, обозначенные арабскими цифрами. Подразделы должны иметь нумерацию в пределах каждого раздела. Номера подразделов состоят из номера раздела и подраздела, разделенных точкой. В конце номера подраздела точка не ставится. Нумерация пунктов должна состоять из номера раздела, подраздела и пункта, разделенных точкой.

Заголовок разделов, подразделов и пунктов следует печатать с абзацного отступа, с прописной буквы, без точки в конце, не подчеркивая. Переносы слов в заголовках не допускаются. Если заголовок состоит из двух предложений, их разделяют точкой.

Ниже каждого заголовка должна быть оставлена одна свободная строка, выше - не менее одной свободной строки. Оставляют свободные строки между разделами и подразделами.

### **Пример**

#### **1 Методы испытаний**

##### **1.1 Аппараты, материалы и реактивы**

#### **2 Подготовка к испытанию**

##### **2.1 Нумерация пунктов первого подраздела третьего раздела документа**

### 3.2 Подготовка к испытанию

### 3.3 Нумерация пунктов второго подраздела третьего раздела документа

Если раздел или подраздел состоит из одного пункта, он также нумеруется. Если текст документа подразделяется только на пункты, они нумеруются порядковыми номерами в пределах документа.

Пункты, при необходимости, могут быть разбиты на подпункты, которые должны иметь порядковую нумерацию в пределах каждого пункта, например: 4.2.1; 4.2.1.1; 4.2.1.2; 4.2.2 и т. д. Между подпунктами и текстом интервалы не оставляются. Подпункты с тройной нумерацией (1.1.1...) и больше в содержание не выносятся.

Внутри пунктов или подпунктов могут быть приведены перечисления.

Перед каждым перечислением следует ставить дефис или, при необходимости ссылки в тексте документа на одно из перечислений, строчную букву, после которой ставится скобка.

Для дальнейшей детализации перечислений необходимо использовать цифры, после которых ставится скобка, а запись производится с абзацного отступа, как показано в примере.

Пример:

- \_\_\_\_\_
- \_\_\_\_\_
  - 1) \_\_\_\_\_
  - 2) \_\_\_\_\_
- \_\_\_\_\_

Каждый раздел курсовой работы следует начинать с нового листа (страницы).

В документе большого объема на первом (заглавном) листе помещают содержание, включающее номера и наименования разделов и подразделов с указанием номеров листов (страниц). Содержание включают в общее количество листов данного документа. Слово "Содержание" записывают в виде заголовка (симметрично тексту) с прописной буквы. Наименования, включенные в содержание, записывают строчными буквами, начиная с прописной буквы.

Список использованных источников должен быть оформлен в соответствии с ГОСТом 7.1-2003 «Библиографическая запись. Библиографическое описание».

### 2.1 Изложение текста

Текст документа должен быть кратким, четким и не допускать различных толкований.

При изложении обязательных требований в тексте должны применяться слова "должен", "следует", "необходимо", "требуется, чтобы", "разрешается только", "не допускается", "запрещается", "не следует". При изложении других положений следует применять слова - "могут быть", "как правило", "при необходимости", "может быть", "в случае" и т.д.

При этом допускается использовать повествовательную форму изложения текста документа, например "применяют", "указывают" и т.п.

В тексте должны применяться научно-технические термины, обозначения и определения, установленные соответствующими стандартами, а при их отсутствии – общепринятые в научно-технической литературе.

В тексте не допускается:

- применять обороты разговорной речи, техницизмы, профессионализмы;
- применять для одного и того же понятия различные научно-технические термины, близкие по смыслу (синонимы), а также иностранные слова при наличии равнозначных слов и терминов на русском языке;
- сокращать обозначения единиц физических величин, если они употребляются без цифр, за исключением единиц физических величин в головках и боковиках таблиц, в расшифровках буквенных обозначений, входящих в формулы и рисунки; применять математический знак минус (-) перед отрицательными значениями величин (следует писать слово «минус»);
- применять без числовых значений математические знаки, например, > (больше), < (меньше), = (равно),  $\neq$  (не равно), а также знака № (номер), % (процент); применять индексы стандартов без регистрирующего номера; перечень допускаемых сокращений слов установлен в ГОСТ 2.316, ГОСТ 7.12; в тексте следует применять стандартизованные единицы физических величин, их наименование и обозначение, установленные в ГОСТ 8.417;
- если в тексте курсовой работы приводится диапазон числовых значений физической величины, то обозначение единицы физической величины указывается, после последнего числового значения диапазона.

Примеры: 1. От 1 до 5 мм.

2. От плюс 10 до минус 40° С.

Недопустимо отделять единицу физической величины от числового значения (переносить их на разные строки или страницы), кроме единиц физических величин, помещенных в таблицах, выполненных машинописным способом.

## 2.2 Формулы

Уравнения и формулы следует выделять из текста в отдельную строку. Выше и ниже каждой формулы или уравнения должно быть оставлено не менее одной свободной строки. Если уравнение не уместится в одну строку, то оно должно быть перенесено после знака равенства (=) или после знаков плюс (+), минус (-), умножения (x), деления (:), или других математических знаков, причем знак в начале следующей строки повторяют. При переносе формулы на знаке, символизирующем операцию умножения, применяют знак «X».

Пояснение значений символов и числовых коэффициентов следует приводить непосредственно под формулой в той же последовательности, в которой они даны в формуле.

Формулы в курсовой работе следует нумеровать порядковой нумерацией в пределах всей курсовой работы арабскими цифрами в круглых скобках в крайнем правом положении на строке.

Формулы, за исключением формул, помещаемых в приложении, должны нумероваться сквозной нумерацией арабскими цифрами, которые записывают на уровне формулы справа в круглых скобках. Одну формулу обозначают - (1).

Формулы, помещаемые в приложениях, должны нумероваться отдельной нумерацией арабскими цифрами в пределах каждого приложения с добавлением перед каждой цифрой обозначения приложения, например формула

(В.1).

Допускается нумерация формул в пределах раздела. В этом случае номер формулы состоит из номера раздела и порядкового номера формулы, разделенных точкой, например (3.1).

После формулы помещают перечень всех принятых в формуле символов с расшифровкой их значений и указанием размерности (если в этом есть необходимость). Буквенные обозначения дают в той же последовательности, в которой они приведены в формуле. Первая строка пояснения должна начинаться со слова «где» без двоеточия после него.

$$PS = \langle F, Z, I \rangle, \quad (1)$$

где  $F$  - рабочая память системы (называемая также базой данных), содержащая текущие данные (элементы рабочей памяти);

$Z$  - база знаний, содержащая множество продукций (правил вида: "условие  $\rightarrow$  действие");

$I$  - интерпретатор (решатель), реализующий процедуры вывода.

Формулы, следующие одна за другой и не разделенные текстом, разделяют запятой.

Формулы, помещаемые в приложениях, должны нумероваться отдельной нумерацией арабскими цифрами в пределах каждого приложения с добавлением перед каждой цифрой обозначения приложения, например формула (В. 1). Ссылки в тексте на порядковые номера формул дают в скобках.

Пример -... в формуле (1).

### 2.3 Иллюстрации и приложения

Иллюстрации (чертежи, графики, схемы, компьютерные распечатки, диаграммы, фотоснимки) следует располагать в курсовой работе непосредственно после текста, в котором они упоминаются впервые, или на следующей странице.

Иллюстрации могут быть в компьютерном исполнении, в том числе и цветные. На все иллюстрации должны быть даны ссылки в курсовой работе. Чертежи, графики, диаграммы, схемы, иллюстрации, помещаемые в курсовой работе, должны соответствовать требованиям государственных стандартов Единой системы конструкторской документации (ЕСКД).

Допускается выполнение чертежей, графиков, диаграмм, схем посредством использования компьютерной печати.

Фотоснимки размером меньше формата А4 должны быть наклеены на стандартные листы белой бумаги.

Иллюстрации, за исключением иллюстрации приложений, следует нумеровать арабскими цифрами сквозной нумерацией. Если рисунок один, то он обозначается «Рисунок 1». Слово «рисунок» и его наименование располагают посередине строки.

Иллюстрации каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения. Например - Рисунок А.3.

Допускается нумеровать иллюстрации в пределах раздела. В этом случае номер иллюстрации состоит из

номера раздела и порядкового номера иллюстрации, разделенных точкой. Например Рисунок 1.1.

Выше и ниже каждой иллюстрации должно быть оставлено не менее одной свободной строки.

Пример:



Рисунок 1 – Основные характеристики системы защиты

Иллюстрации, при необходимости, могут иметь наименование и пояснительные данные (подрисуночный текст).

Иллюстрации каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения. Например, Рисунок А.3.

При ссылках на иллюстрации следует писать «... в соответствии с рисунком 2».

Материал, дополняющий текст документа, допускается помещать в приложениях. Приложениями могут быть, например, графический материал, таблицы большого формата, расчеты, описания аппаратуры и приборов, описания алгоритмов и программ задач, решаемых на ЭВМ и т.д.

Приложение оформляют как продолжение данного документа на последующих его листах или выпускают в виде самостоятельного документа.

Каждое приложение следует начинать с новой страницы с указанием наверху посередине страницы слова "Приложение" и его обозначения, а под ним в скобках для обязательного приложения пишут слово "обязательное", а для информационного - "рекомендуемое" или "справочное".

Приложение должно иметь заголовок, который записывают симметрично относительно текста с прописной буквы отдельной строкой.

Приложения обозначают заглавными буквами русского алфавита, начиная с А, за исключением букв Ё, З, Й, О, Ч, Ь, Ы, Ъ. После слова "Приложение" следует буква, обозначающая его последовательность. Приложения, как правило, выполняют на листах формата А4. Допускается оформлять приложения на листах формата А3, А4 3, А4 4, А2 и А1 по ГОСТ 2.301.

Приложения должны иметь общую с остальной частью документа сквозную нумерацию страниц.

Пример:

## **Приложение А**

(обязательное)

Все приложения должны быть перечислены в содержании документа (при наличии) с указанием их номеров и заголовков.

## 2.4 Таблицы

Таблицы применяют для лучшей наглядности и удобства сравнения показателей. Название таблицы, при его наличии, должно отражать ее содержание, быть точным, кратким. Слово "Таблица" указывают один раз слева над первой частью таблицы, над другими частями пишут слова "Продолжение таблицы" с указанием номера (обозначения) таблицы. При переносе части таблицы название помещают только над первой частью таблицы, нижнюю горизонтальную черту, ограничивающую таблицу, не проводят.

Таблицу следует располагать в курсовой работе непосредственно после текста, в котором она упоминается впервые, или на следующей странице, а при необходимости, в приложении к документу.

Допускается помещать таблицу вдоль длинной стороны листа документа. На все таблицы должны быть ссылки в отчете. При ссылке следует писать слово «таблица» с указанием ее номера.

Таблицу с большим количеством строк допускается переносить на другой лист (страницу).

При переносе части таблицы на другой лист (страницу) слово «Таблица» и номер ее указывают слева над первой частью таблицы, над другими частями пишут «Продолжение таблицы 1».

Цифровой материал, как правило, оформляют в виде таблиц в соответствии с рисунком 1.

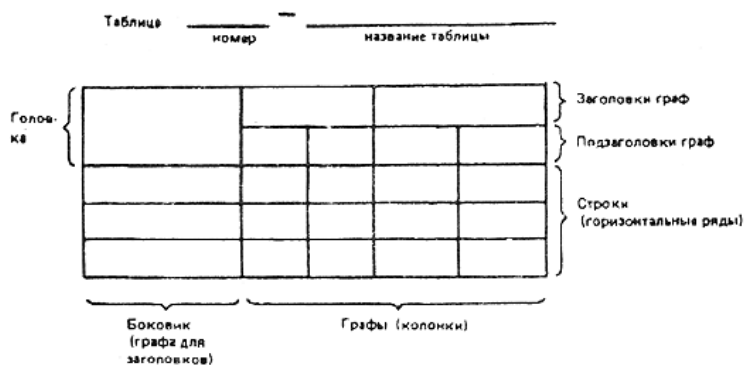


Рисунок 1– Пример таблицы

Если цифровые или иные данные в какой-либо строке таблицы не приводят, то в ней ставят прочерк.

Таблицы, за исключением таблиц приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

Таблицы каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения.

Если в документе одна таблица, то она должна быть обозначена «Таблица 1» или «Таблица В. 1», если она приведена в приложении В.

Заголовки граф и строк таблицы следует писать с прописной буквы в единственном числе, а подзаголовки граф — со строчной буквы, если они составляют одно предложение с заголовком, или с прописной буквы, если они имеют самостоятельное значение. В конце заголовков и подзаголовков таблиц точки не ставят.

Таблицы слева, справа и снизу, как правило, ограничивают линиями. Допускается применять размер шрифта в таблице меньший, чем в тексте.

Разделять заголовки и подзаголовки боковика и граф диагональными линиями не допускается. Высота строк таблицы должна быть не менее 8 мм.

Заголовки граф, как правило, записывают параллельно строкам таблицы. При необходимости допускается перпендикулярное расположение заголовков граф.

Если строки или графы таблицы выходят за формат страницы, ее делят на части, помещая одну часть под другой или рядом, при этом в каждой части таблицы повторяют ее головку и боковик. При делении таблицы на части допускается ее головку или боковик заменять соответственно номером граф и строк. При этом нумеруют арабскими цифрами графы и (или) строки первой части таблицы. Оформление таблиц в курсовой работе должно соответствовать ГОСТ 1.5 и ГОСТ 2.105.

Пример:

Таблица 1 – Результаты структурирования информации

| № элемента информации | Наименование элемента информации | Гриф конфиденциальности информации | Цена информации | Наименование источника информации | № элемента информации |
|-----------------------|----------------------------------|------------------------------------|-----------------|-----------------------------------|-----------------------|
| 1                     | 2                                | 3                                  | 4               | 5                                 | 6                     |
|                       |                                  |                                    |                 |                                   |                       |
|                       |                                  |                                    |                 |                                   |                       |

Продолжение таблицы 1

| № элемента информации | Наименование элемента информации | Гриф конфиденциальности информации | Цена информации | Наименование источника информации | № элемента информации |
|-----------------------|----------------------------------|------------------------------------|-----------------|-----------------------------------|-----------------------|
| 1                     | 2                                | 3                                  | 4               | 5                                 | 6                     |
|                       |                                  |                                    |                 |                                   |                       |
|                       |                                  |                                    |                 |                                   |                       |

Графическая часть курсовой работы (чертежи, схемы и т. п.) выполняется с соблюдением соответствующих государственных стандартов. Каждое приложение должно начинаться с нового листа с указанием вверху листа по центру слова «Приложение» и иметь тематический заголовок.

### 3 Организация выполнения и порядок руководства курсовыми работами

Руководство курсовыми работами должно поручаться наиболее квалифицированным преподавателям кафедры, обладающим методическим опытом и научной квалификацией. Для учета специфики курсовых работ по специальностям каждой кафедре необходимо разработать методические указания по выполнению курсовых работ.

Руководство курсовыми работами начинается с выдачи задания студентам. В этот период необходимым условием, обеспечивающим эффективность дальнейшего руководства, является индивидуальная беседа руководителя со студентом по заданию. В ходе беседы руководитель должен выяснить степень подготовленности студента к выполнению данного задания, рекомендовать необходимую литературу и информировать о порядке выполнения задания. В результате индивидуальной беседы может быть уточнена или выбрана студентом другая тема работы.

Задание выдается за подписью руководителя работы, датируется днем выдачи и регистрируется в кафедральном журнале.

В ряде случаев необходимо организовывать на кафедре чтение вводных лекций профессора или одного из опытных руководителей с целью разъяснения значения курсовой работы для данной дисциплины, требований, предъявляемых к работе.

В рамках отведенного для руководства курсовыми работами времени должны регулярно проводиться индивидуальные консультации.

Одной из важных форм руководства является предварительный просмотр выполненной курсовой работы. Если работа содержит экспериментальную часть, то руководитель, прежде всего, должен провести экспертизу этой части, а затем указать все ошибки, неточности по работе в целом.

После проверки выполнения студентом одного этапа работы, руководитель работы разрешает студенту перейти к следующему.

Заведующий кафедрой должен периодически проверять состояние работы, контролировать направленность и методику деятельности отдельных руководителей, давая на заседаниях кафедры соответствующие методические указания.

Работа перед сдачей руководителю подписывается студентом. Если работа удовлетворяет требованиям, предъявляемым к курсовым работам, она допускается к защите, о чем руководитель делает надпись на титульном листе.

#### **4. Защита курсовых работ**

Защита курсовой работы является обязательной формой проверки выполнения работы. Защита производится на заседании кафедры, научно-методического семинара кафедры, научной проблемной группы специальной комиссией, состоящей обычно из 3 преподавателей кафедры, при непосредственном участии руководителя, в присутствии студентов. Результаты наиболее интересных курсовых работ могут быть доложены на научных конференциях.

Защита состоит в коротком докладе студента по выполненной работе и в ответах на вопросы присутствующих на защите. Научный руководитель зачитывает отзыв на курсовую работу студента (Приложение Д).

Результаты защиты курсовой работы, согласно действующему Положению о текущем контроле и промежуточной аттестации в СКФУ, оцениваются дифференцированной отметкой по пятибалльной системе. Оценка курсовой работы заносится в зачетную книжку студента и зачетно-экзаменационную ведомость (Приложение Д), составляемую в 2-х экземплярах, один из которых хранится на кафедре в течение всего срока обучения студента, другой представляется в дирекцию факультета.

Защита курсовых работ, предусмотренных учебным планом, проводится не позднее, чем за две недели до начала зачетно-экзаменационной сессии.

Студент, не представивший в установленный срок курсовую работу или не защитивший ее по неуважительной причине, считается имеющим академическую задолженность.

Курсовые работы, представляющие теоретический и практический интерес, следует представлять на конкурс в студенческие научные общества, конференции, отмечать приказом по университету.

Выполненные работы после их защиты должны храниться на кафедре в течение 2 лет, не считая года

написания, затем работы, не представляющие для кафедры интерес, уничтожаются по акту.

Итоги выполнения курсовых работ ежегодно обсуждаются на кафедрах и по мере необходимости на Ученом совете факультета, а в отдельных случаях и на заседаниях Ученого Совета университета.

## Приложение А

(обязательное)

УТВЕРЖДАЮ

Заведующий кафедрой  
организации и технологии  
защиты информации  
канд. техн. наук, доцент

\_\_\_\_\_  
В.И. Петренко  
«05» февраля 2014 г.

|                        |                                                     |
|------------------------|-----------------------------------------------------|
| Институт               | Математики и компьютерных наук имени Н.И. Червякова |
| Кафедра                | Организации и технологии защиты информации          |
| Направление подготовки | Информационная безопасность                         |
| Профиль подготовки     | Организации и технологии защиты информации          |

### ЗАДАНИЕ на курсовую работу

студента

Перевязка Владислав Сергеевич

\_\_\_\_\_  
(фамилия, имя, отчество)

по дисциплине

Защита информации от утечки по техническим каналам

1. Тема работы

2. Цель

3. Задачи

4. Перечень подлежащих разработке вопросов:

а) по теоретической части

б) по аналитической части

5. Исходные данные:

а) по литературным источникам

б) по вариантам, разработанным преподавателем

в) иное

6. Список рекомендуемой литературы

7. Контрольные сроки представления отдельных разделов курсовой работы:

25 % - Первый раздел «27» февраля 2014 г.

50 % - Второй раздел «17» апреля 2014 г.

75 % - Третий раздел «20» мая 2014 г.

100 % - Оформленная работа, прошедшая нормоконтроль «26» мая 2014 г.

8. Срок защиты студентом курсовой работы «27» мая 2014 г.

Дата выдачи задания «05» февраля 2014 г.

Руководитель курсовой работы

доцент кафедры ОТЗИ

(ученая степень, звание)

(личная подпись)

Гусева Т.М.

(инициалы, фамилия)

Задание принял(а) к исполнению студент(ка) очной формы обучения

2 курса ИНБ-6-о-13-1 группы

(личная подпись)

Перевязка В.В.

(инициалы, фамилия)

## Приложение Б

(обязательное)

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ФГАОУ ВО  
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»  
ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК ИМЕНИ ПРОФЕССОРА Н.И. ЧЕРВЯКОВА  
КАФЕДРА ОРГАНИЗАЦИИ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

### КУРСОВАЯ РАБОТА

по дисциплине

«Защита информации от утечки по техническим каналам»

на тему:

«Анализ механизма OSINT»

#### Выполнил:

Перевязка Владислав Сергеевич  
студент 2 курса группы ИНБ-б-о-13-1  
направления подготовки «Информационная  
безопасность» очной формы обучения

---

(подпись)

#### Руководитель работы:

Гусева татьяна Михайловна  
Доцент кафедры организации и технологии защиты  
информации

г

Работа допущена к защите \_\_\_\_\_  
(подпись)

26.05.2014 г.  
(дата)

Работа выполнена и  
защищена с оценкой \_\_\_\_\_

Дата защиты 28.05.2014 г.

Члены комиссии: Зав. кафедрой ОТЗИ  
(должность)

\_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(И.О. Фамилия)

Доцент кафедры ОТЗИ

Тебучева Ф.Б.

Доцент кафедры ОТЗИ

Минкина Т.В.

Ставрополь, 2014 г.

## Приложение В

(обязательное)

### Содержание

|                                                                                                                        |    |
|------------------------------------------------------------------------------------------------------------------------|----|
| Введение.....                                                                                                          | 3  |
| 1 Обзор существующих методов отслеживания установленного программного обеспечения на предприятии.....                  | 4  |
| 1.1 Понятие отслеживания установленного программного обеспечения.....                                                  | 5  |
| 1.2 Инвентаризация программного обеспечения.....                                                                       | 9  |
| 1.3 Аудит программного обеспечения.....                                                                                | 12 |
| 1.4 Выводы по главе.....                                                                                               | 16 |
| 2 Способы отслеживания установленного программного обеспечения в информационной среде предприятия.....                 | 17 |
| 2.1 Обзор существующих программ отслеживания установленного программного оборудования.....                             | 17 |
| 2.2 Realité: реальный контроль.....                                                                                    | 26 |
| 2.3 Выводы по главе.....                                                                                               | 29 |
| 3 Разработка программы для инвентаризации и учета программ на компьютерных сетях «учет программного обеспечения» ..... | 31 |
| 3.1 Понятие и способы применения программы «Учет программного обеспечения».....                                        | 32 |
| 3.2 Существующие виды программы и её достоинства.....                                                                  | 31 |
| 3.3 Выводы по главе.....                                                                                               | 33 |
| Заключение.....                                                                                                        | 35 |
| Список использованных источников.....                                                                                  | 37 |

## **Приложение Г**

(обязательное)

### **Список использованных источников**

#### **В.1 Нормативно-руководящие документы**

1 ГОСТ Р 51275-99. Защита информации. Объект информации. Факторы, воздействующие на информацию. Общие положения. – Введ.01.01.2000. – М.: Изд.стандартов, 2002.

2 ГОСТ Р 50739-95. Средства Вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. – Введ.01.01.96. – М.: Изд.стандартов, 2002.

#### **В.2 Книги с различным количеством авторов:**

*- количество авторов не более трех:*

3 Завгородний В.А. Комплексная защита информации в компьютерных системах. – М.: Логос, 2003. – 264 с.

*- количество авторов не более четырех:*

4 Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: Учебное пособие. – М.: Издательско-торговая корпорация «Дашков и К°», 2004. – 336 с.

*- количество авторов более четырех:*

5 Сотрудничество /И.И.Иванов,П.П.Петров,С.С.Сидоров и др:АН СССР. ИПМ. – Киев; Наук.думка, 2006. – 270 с.

#### **В.3 Тезисы доклада, сообщения, доклад, другие материалы совещаний (конференций)**

6 Росенко А.П., Евстафиади С.П., Феник Е.В. Структура Нейросетевой экспертной системы защиты информации // Сборник трудов научно-практической конференции «Проблемы физико-математических наук». Материалы 48 научно-методической конференции «Университетская наука – региону» – Ставрополь: Изд-во СГУ, 2003. – С.199–202.

#### **В.4 Статьи из журналов и периодических сборников, продолжающихся сборников, ежегодников:**

*- статья в книге и сборнике:*

7 Соколов Н.В., Шангин А.П. Защита информации в компьютерных сетях и системах. – М.: ДМК, 2002. – С.234–256.

*- статья на депоненте:*

8 Лисипин Л.Г., Медведев А.И. Определение характеристик/ ЦНИИ. –М., 1933. –18 с. –Деп.в ЦНИИНТИ 27.02.03; № 13924.

#### **В.5 Источники из Интернета**

9 Сердюк В.А. Новое поколение систем обнаружения и предотвращения информационных атак. – <http://www.infoforum.ru/>.

## **Приложение Д**

(обязательное)

### **Отзыв**

на курсовую работу студента/ки \_\_\_\_ курса

Ф.И.О.

тема

Актуальность: курсовая работа посвящена .....

В первой главе ....

Вторая глава ....

Выводы, сделанные в Заключение, соответствуют целям, поставленным во Введении.

Проанализирован ....объем литературы...

За время работы студент/ка проявил/а себя как.....

Таким образом, работа выполнена на ... уровне, соответствует требованиям, предъявляемым к курсовым работам, и заслуживает ... оценки.

Научный руководитель  
степень, звание, должность  
место работы

Ф.И.О.

Печать

"....".....201...г.