

Сертификационная подготовка Huawei

**Руководство
по выполнению лабораторных работ
для подготовки специалистов по
технологиям и оборудованию передачи
данных к сертификации HCIA-Datcom**

V1.0



Huawei Technologies Co., Ltd.

Авторские права © Huawei Technologies Co., Ltd. 2020 г. Все права защищены.

Воспроизведение и передача данного документа или какой-либо его части в любой форме и любыми средствами без предварительного письменного разрешения компании Huawei Technologies Co., Ltd. запрещены.

Товарные знаки



HUAWEI и прочие товарные знаки Huawei являются зарегистрированными товарными знаками компании Huawei Technologies Co., Ltd.

Другие товарные знаки и торговые наименования, упомянутые в настоящем документе, принадлежат исключительно их владельцам.

Примечание

Приобретаемые продукты, услуги и функции предусмотрены договором, заключенным между компанией Huawei и заказчиком. Все или отдельные части оборудования, услуг и конструктивных особенностей, описываемых в данном документе, могут не входить в объем покупки или объем эксплуатации. При отсутствии иных договоренностей, все утверждения, информация и рекомендации в настоящем документе предоставляются по принципу «как есть» без каких-либо явных или подразумеваемых гарантий.

Документ содержит актуальную информацию на момент его издания, которая может быть изменена без предварительного уведомления. Несмотря на то, что при подготовке данного документа были приложены все усилия для обеспечения точности его содержания, ни одно из содержащихся в нем утверждений, рекомендаций и никакая информация не является явной или подразумеваемой гарантией.

Huawei Technologies Co., Ltd.

Адрес: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Веб-сайт: <https://e.huawei.com/>

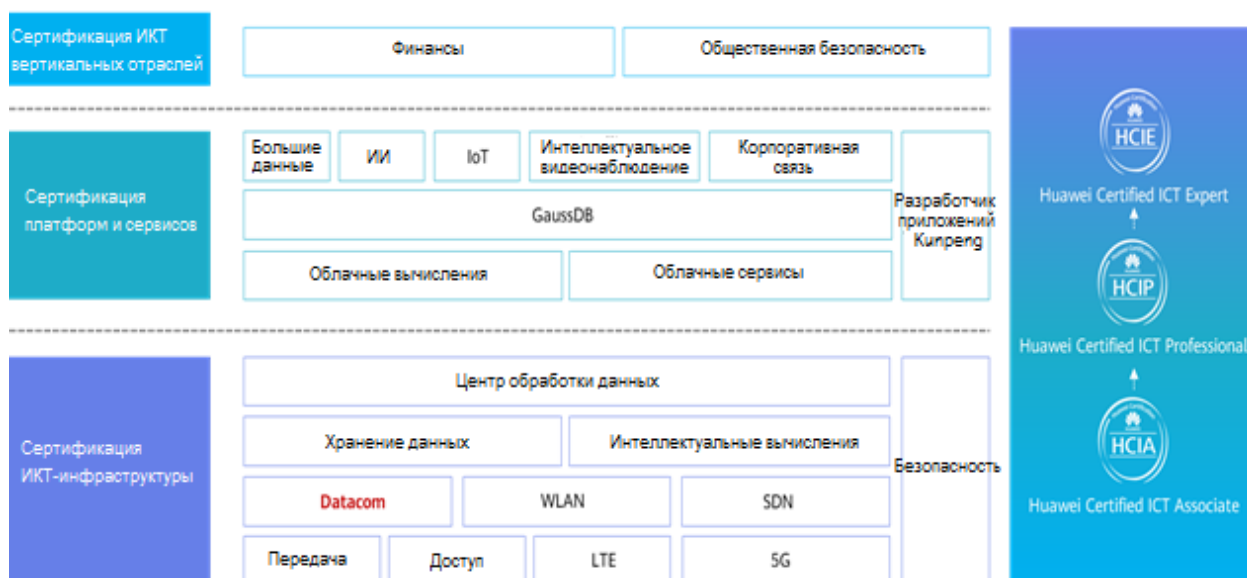
Система сертификации Huawei

Сертификация Huawei является элементом стратегии развития «Платформа+Экосистема», в рамках которой создается новая архитектура ИКТ-инфраструктуры, ориентированная на совместную работу и реализацию еще одной стратегии «Облако-Канал-Устройство». Компания Huawei создала комплексную систему сертификации, включающую три категории: ICT Infrastructure Certification, Platform and Service Certification, ICT Vertical Certification. Это единственная система сертификации, которая охватывает все технические аспекты ИКТ в отрасли. Компания Huawei предлагает три уровня сертификации для специалистов: «Huawei Certified ICT Associate (HCIA)», «Huawei Certified ICT Professional (HCIP)» и «Huawei Certified ICT Expert (HCIE)». Сертификация Huawei охватывает все области ИКТ и корректируется в соответствии с отраслевой тенденцией конвергенции ИКТ. С помощью своей передовой системы подготовки кадров и стандартов сертификации, компания Huawei стремится помочь талантливым специалистам получить знания и навыки в области ИКТ, необходимые в эпоху цифровых технологий, создавая надежную экосистему перспективного персонала в области ИКТ.

Уровень Huawei Certified ICT Associate-Datacom (HCIA-Datacom) предназначен для рядовых инженеров Huawei и всех, кто хочет разбираться в продуктах и технологиях передачи данных компании Huawei. Сертификация по технологиям и оборудованию передачи данных HCIA-Datacom охватывает принципы маршрутизации и коммутации, базовые принципы работы WLAN, основы управления, обеспечения безопасности, эксплуатации и технического обслуживания сети, базовые принципы SDN, а также основы программирования и автоматизации.

Система сертификации Huawei ориентирована на предоставление информации об отрасли и передовых знаний в области передачи данных, а также способствует внедрению инноваций.

Сертификация Huawei



Основные сведения о документе

Введение



Настоящий документ представляет собой курс подготовки к сертификации уровня HCIA-Datacom для специалистов, которые собираются сдавать экзамен HCIA-Datacom, или простых слушателей, которые хотят понять принципы маршрутизации и коммутации, основные принципы WLAN, основы управления, обеспечения безопасности, эксплуатации и технического обслуживания сети, базовые принципы SDN, а также основы программирования и автоматизации.

Требуемые базовые знания

Этот курс предназначен для подготовки к сертификации Huawei, подтверждающей базовые знания. Для понимания информации в этом курсе вам потребуются следующие знания и навыки:

- Базовые навыки работы с компьютером
- Базовые знания о процессе передачи данных

Символьные обозначения


Коммутатор
ПК
Кабель Ethernet
**Точка доступа
FIT AP**
Маршрутизатор
**Последовательный
кабель**

Лабораторная среда

Описание сети

Эта лабораторная среда предназначена для специалистов по технологиям и оборудованию передачи данных, которые готовятся к сдаче экзамена HCIA-Datacom. Каждая лабораторная среда включает два коммутатора (не поддерживающих PoE), два коммутатора PoE, две точки беспроводного доступа (AP) и два маршрутизатора.

Необходимые устройства

Для выполнения лабораторных работ необходимо подготовить устройства, представленные в следующей таблице.

Необходимые устройства

Название устройства	Модель устройства	Версия ПО
Коммутатор	CloudEngine S5731-H24T4XC	V200R019C00 или более поздней версии
Коммутатор PoE	CloudEngine S5731-H24P4XC	V200R019C00 или более поздней версии
Точка доступа	AirEngine 5760-10	V200R009 или более поздней версии
Маршрутизатор	NetEngine AR651C	V300R019 или более поздней версии

ПРИМЕЧАНИЕ

В настоящем руководстве информация о портах, результаты выполнения команд и конфигурации устройств предоставляются на основе рекомендованной топологии. Фактическая информация может отличаться в зависимости от лабораторной среды.



Содержание

Основные сведения о документе	4
1 Huawei VRP и основы конфигурирования	12
1.1 Общая информация	12
1.1.1 О лабораторной работе	12
1.1.2 Цели	12
1.1.3 Топология сети	12
1.2 Лабораторная работа	13
1.2.1 План работы	13
1.2.2 Процедура конфигурирования	13
1.3 Проверка	19
1.4 Справочные конфигурации	19
1.5 Вопросы	19
1.6 Приложение	19
2 Создание взаимосвязанной IP-сети	21
2.1 Лабораторная работа 1. Адресация и маршрутизация IPv4	21
2.1.1 Общая информация	21
2.1.1.1 О лабораторной работе	21
2.1.1.2 Цели	21
2.1.1.3 Топология сети	21
2.1.2 Лабораторная работа	22
2.1.2.1 План работы	22
2.1.2.2 Процедура конфигурирования	22
2.1.3 Проверка	32
2.1.4 Справочные конфигурации	32
2.1.5 Вопросы	33
2.2 Лабораторная работа 2. Маршрутизация OSPF	34
2.2.1 Общая информация	34
2.2.1.1 О лабораторной работе	34
2.2.1.2 Цели	34
2.2.1.3 Топология сети	34
2.2.2 Лабораторная работа	35
2.2.2.1 План работы	35
2.2.2.2 Процедура конфигурирования	35



2.2.3 Проверка	41
2.2.4 Справочные конфигурации	41
2.2.5 Вопросы	42
3 Создание коммутируемой сети Ethernet	43
3.1 Лабораторная работа 1. Основы Ethernet и конфигурирование VLAN	43
3.1.1 Общая информация	43
3.1.1.1 О лабораторной работе	43
3.1.1.2 Цели	43
3.1.1.3 Топология сети	44
3.1.2 Лабораторная работа	44
3.1.2.1 План работы	44
3.1.2.2 Процедура конфигурирования	44
3.1.3 Проверка	50
3.1.4 Справочные конфигурации	50
3.1.5 Вопросы	51
3.2 Лабораторная работа 2. Протокол связующего дерева (STP)	53
3.2.1 Общая информация	53
3.2.1.1 О лабораторной работе	53
3.2.1.2 Цели	53
3.2.1.3 Топология сети	53
3.2.2 Лабораторная работа	54
3.2.2.1 План работы	54
3.2.2.2 Процедура конфигурирования	54
3.2.3 Проверка	61
3.2.4 Справочные конфигурации	62
3.2.5 Вопросы	63
3.3 Лабораторная работа 3. Агрегирование каналов Ethernet	64
3.3.1 Общая информация	64
3.3.1.1 О лабораторной работе	64
3.3.1.2 Цели	64
3.3.1.3 Топология сети	64
3.3.2 Лабораторная работа	65
3.3.2.1 План работы	65
3.3.2.2 Процедура конфигурирования	65
3.3.3 Проверка	71
3.3.4 Справочные конфигурации	71
3.3.5 Вопросы	72
3.4 Лабораторная работа 4. Связь между VLAN	73
3.4.1 Общая информация	73

3.4.1.1 О лабораторной работе	73
3.4.1.2 Цели	73
3.4.1.3 Топология сети	73
3.4.2 Лабораторная работа	74
3.4.2.1 План работы	74
3.4.2.2 Процедура конфигурирования	74
3.4.3 Проверка	77
3.4.4 Справочные конфигурации	77
3.4.5 Вопросы	78
4 Основы сетевой безопасности и доступа к сети	79
4.1 Лабораторная работа 1. Настройка ACL	79
4.1.1 Общая информация	79
4.1.1.1 О лабораторной работе	79
4.1.1.2 Цели	79
4.1.1.3 Топология сети	79
4.1.2 Лабораторная работа	80
4.1.2.1 План работы	80
4.1.2.2 Процедура конфигурирования	80
4.1.3 Проверка	83
4.1.4 Справочные конфигурации (Способ 1)	84
4.1.5 Справочные конфигурации (Способ 2)	85
4.1.6 Вопросы	86
4.2 Лабораторная работа 2. Настройка локального механизма AAA	87
4.2.1 Общая информация	87
4.2.1.1 О лабораторной работе	87
4.2.1.2 Цели	87
4.2.1.3 Топология сети	87
4.2.2 Лабораторная работа	88
4.2.2.1 План работы	88
4.2.2.2 Процедура конфигурирования	88
4.2.3 Проверка	90
4.2.4 Справочные конфигурации	90
4.2.5 Вопросы	91
4.3 Лабораторная работа 3. Настройка NAT	92
4.3.1 Общая информация	92
4.3.1.1 О лабораторной работе	92
4.3.1.2 Цели	92
4.3.1.3 Топология сети	92
4.3.2 Лабораторная работа	93



4.3.2.1 План работы	93
4.3.2.2 Процедура конфигурирования	93
4.3.3 Проверка	97
4.3.4 Справочные конфигурации	97
4.3.5 Вопросы	99
5 Конфигурирование основных сетевых служб	100
5.1 Лабораторная работа 1. Настройка FTP	100
5.1.1 Общая информация	100
5.1.1.1 О лабораторной работе	100
5.1.1.2 Цели	100
5.1.1.3 Топология сети	100
5.1.2 Лабораторная работа	101
5.1.2.1 План работы	101
5.1.2.2 Процедура конфигурирования	101
5.1.3 Проверка	104
5.1.4 Справочные конфигурации	105
5.1.5 Вопросы	105
5.2 Лабораторная работа 2. Конфигурирование DHCP	106
5.2.1 Общая информация	106
5.2.1.1 О лабораторной работе	106
5.2.1.2 Цели	106
5.2.1.3 Топология сети	106
5.2.2 Лабораторная работа	107
5.2.2.1 План работы	107
5.2.2.2 Процедура конфигурирования	107
5.2.3 Проверка	109
5.2.3.1 Вывод на экран IP-адресов и маршрутов R1 и R3	109
5.2.3.2 Вывод на экран информации о назначении адресов на R2	110
5.2.4 Справочные конфигурации	110
5.2.5 Вопросы	111
6 Создание WLAN	112
6.1 Общая информация	112
6.1.1 О лабораторной работе	112
6.1.2 Цели	112
6.1.3 Топология сети	112
6.1.4 Планирование данных	113
6.2 Лабораторная работа	114
6.2.1 План работы	114
6.2.2 Процедура конфигурирования	114

6.3 Проверка	121
6.4 Справочные конфигурации	121
6.5 Вопросы.....	123
6.6 Приложение	123
7 Создание сети IPv6	125
7.1 Общая информация	125
7.1.1 О лабораторной работе	125
7.1.2 Цели	125
7.1.3 Топология сети	125
7.2 Лабораторная работа.....	126
7.2.1 План работы	126
7.2.2 Процедура конфигурирования.....	126
7.3 Проверка	133
7.4 Справочные конфигурации.....	133
7.5 Вопросы	134
8 Основы сетевого программирования и автоматизации	135
8.1 Общая информация	135
8.1.1 О лабораторной работе	135
8.1.2 Цели	135
8.1.3 Топология сети	135
8.2 Лабораторная работа	135
8.2.1 План работы	135
8.2.2 Процедура конфигурирования	136
8.2.3 Интерпретация кода	138
8.3 Проверка	140
8.4 Справочные конфигурации	140
8.5 Вопросы.....	140
9 Конфигурирование кампусной сети	141
9.1 Справочная информация	141
9.2 Общая информация.....	141
9.2.1 О лабораторной работе	141
9.2.2 Цели	141
9.2.3 Топология сети.....	142
9.3 Задачи лабораторной работы	142
9.3.1 Сбор и анализ требований	142
9.3.2 Планирование и проектирование.....	144
9.3.3 Реализация.....	154
9.3.4 Эксплуатация и техническое обслуживание сети (O&M)	159
9.3.5 Оптимизация сети.....	161



9.4 Проверка	161
9.5 Справочные конфигурации	161
9.6 Вопросы	182
Справочные ответы на вопросы в лабораторных работах	183

1 Huawei VRP и основы конфигурирования

1.1 Общая информация

1.1.1 О лабораторной работе

Данная лабораторная работа позволит вам изучить основные операции системы Huawei VRP путем настройки устройств Huawei.

1.1.2 Цели

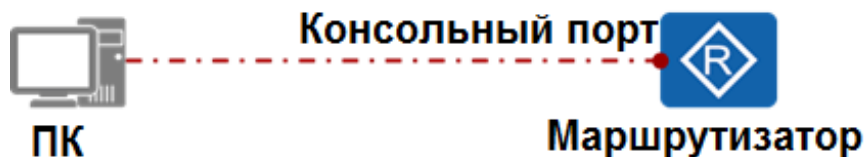
Лабораторная работа помогает получить практические навыки по изучению следующих тем:

- Режимы командной строки, способы входа и выхода из режимов командной строки
- Стандартные команды
- Использование интерактивной справки командной строки
- Отмена действия команды
- Использование сочетаний клавиш в командной строке

1.1.3 Топология сети

На следующей схеме сети маршрутизатор является новым устройством, не имеющим какой-либо конфигурации. Компьютер подключается к консольному порту маршрутизатора с помощью последовательного кабеля. Вам необходимо инициализировать маршрутизатор.

Рис. 1-1 Топология лабораторной сети для изучения операционной системы VRP



1.2 Лабораторная работа

1.2.1 План работы

1. Выполнение базовых настроек, включая настройку имени устройства и IP-адреса интерфейса маршрутизатора.
2. Сохранение конфигурации.
3. Перезагрузка устройства.

1.2.2 Процедура конфигурирования

Шаг 1 Войдите в интерфейс командной строки (CLI) маршрутизатора через консольный порт.
Подробности данной операции здесь не приводятся.

Шаг 2 Выведите на экран основную информацию об устройстве.

Выведите информацию о версии устройства.

```
<Huawei>display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.160 (AR651C V300R019C00SPC100)
Copyright (C) 2011-2016 HUAWEI TECH CO., LTD
Huawei AR651C Router uptime is 0 week, 0 day, 0 hour, 53 minutes
BKP 0 version information:
1. PCB      Version   : AR01BAK2C VER.B
2. If Supporting PoE   : No
3. Board    Type     : AR651C
4. MPU Slot Quantity   : 1
5. LPU Slot Quantity   : 1
```

Шаг 3 Настройте основные параметры устройства.

Измените имя маршрутизатора на имя **Datacom-Router**.

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]
Вы перешли из системного режима в режим пользователя.
[Huawei]sysname Datacom-Router
[Datacom-Router]
Имя устройства изменилось на Datacom-Router.
```

Устройства Huawei предоставляют широкий спектр функций и связанных команд конфигурирования и запроса информации. Чтобы облегчить конфигурирование интерфейс командной строки разделен на отдельные командные режимы. В каждом командном режиме предусмотрен собственный набор команд в зависимости от функций. Чтобы использовать функцию, сначала войдите в соответствующий командный режим, а затем выполните необходимые команды.

Войдите в режим интерфейса и настройте IP-адрес интерфейса.

```
[Datacom-Router]inter           //Нажмите Tab для выполнения команды.
[Datacom-Router]interface       //"interface" — необязательное ключевое слово.
[Datacom-Router]interface g     //Нажмите Tab для выполнения команды.
[Datacom-Router]interface GigabitEthernet // "GigabitEthernet" — необязательное ключевое слово.
[Datacom-Router]interface GigabitEthernet 0/0/1 //Введите команду полностью.
```

Введите несколько первых букв ключевого слова в команде и нажмите Tab, чтобы вывести на экран ключевое слово целиком. Однако эти буквы должны однозначно определять ключевое слово. Если они соответствуют разным ключевым словам, нажимайте Tab несколько раз подряд, пока на экране не отобразится нужное ключевое слово.

Например, с букв **inter** начинается только одна команда **interface**. Поэтому при вводе **inter** и после нажатия клавиши Tab на экране автоматически отобразится команда **interface**. Команда не изменится, даже если вы нажмете Tab несколько раз.

```
[Datcom-Router-GigabitEthernet0/0/1]
```

Отображается режим интерфейса GigabitEthernet0/0/1.

```
[Datcom-Router-GigabitEthernet0/0/1]i?
```

icmp	<Group> icmp command group
igmp	Specify parameters for IGMP
ip	<Group> ip command group
ipsec	Specify IPSec(IP Security) configuration information
ipv6	<Group> ipv6 command group
isis	Configure interface parameters for ISIS

При вводе только первого символа или нескольких первых символов ключевого слова команды можно воспользоваться функцией контекстно-зависимой справки, чтобы получить список всех ключевых слов, которые начинаются с этого символа или нескольких символов. Кроме того, в списке будут отображаться значения каждого ключевого слова.

Например, в режиме интерфейса GigabitEthernet0/0/1 введите **i** и вопросительный знак (**?**), чтобы посмотреть параметры всех команд, начинающихся с буквы **i**, которые доступны в текущем режиме. Далее можно нажать Tab, чтобы вывести команду целиком или вручную ввести полную команду на основе справочной информации. В приведенной выше информации **icmp** и **igmp** являются ключевыми словами, а **<Group> icmp command group** и **Specify parameters for IGMP** — описаниями ключевых слов.

```
[Datcom-Router-GigabitEthernet0/0/1]ip ?
```

accounting	<Group> accounting command group
address	<Group> address command group
binding	Enable binding of an interface with a VPN instance
fast-forwarding	Enable fast forwarding
forward-broadcast	Specify IP directed broadcast information
netstream	IP netstream feature
verify	IP verify

При вводе определенных ключевых слов команды и вопросительного знака (**?**) через пробел на экране будут отображены все ключевые слова, связанные с этой командой, с простыми описаниями.

Например, при вводе **ip**, пробела и вопросительного знака (**?**) отобразятся все команды, содержащие ключевое слово **ip**, с соответствующими описаниями.

```
[Datcom-Router-GigabitEthernet0/0/1]ip address ?
```

IP_ADDR<X.X.X.X>	IP address
bootp-alloc	IP address allocated by BOOTP
dhcp-alloc	IP address allocated by DHCP
unnumbered	Share an address with another interface

```
[Datcom-Router-GigabitEthernet0/0/1]ip address 192.168.1.1 ?
```

```
INTEGER<0-32>      Length of IP address mask
IP_ADDR<X.X.X.X>    IP address mask
[Datacom-Router-GigabitEthernet0/0/1]ip address 192.168.1.1 24 ?
sub                Indicate a subordinate address
<cr>               Please press ENTER to execute command
```

<cr> указывает, что на этой позиции ключевые слова или параметры отсутствуют. Для выполнения команды можно нажать Enter.

```
[Datacom-Router-GigabitEthernet0/0/1]dis this
#
interface GigabitEthernet0/0/1
ip address 192.168.1.1 255.255.255.0
#
```

Команда **display this** позволяет вывести на экран рабочую конфигурацию в текущем режиме. Действительные аргументы, для которых установлены значения по умолчанию, не отображаются. Настроенные аргументы, которые не были успешно зафиксированы, также не отображаются. Данная команда используется для проверки конфигурации.

В текущем режиме не нужно вводить ключевые слова полностью, если введенные символы соответствуют определенному ключевому слову команды. Эта функция повышает эффективность работы.

Например, на интерфейсе можно выполнить команду **dis this**, потому что эти символы соответствуют только команде **display this** в текущем режиме. Также можно выполнить команды **dis cu** и **d cu**, поскольку они соответствуют команде **display current-configuration**.

```
[Datacom-Router-GigabitEthernet0/0/1]quit
```

Команда **quit** возвращает устройство из текущего режима в режим более низкого уровня. Если устройство находится в системном режиме, то после выполнения данной команды оно перейдет в режим пользователя.

Отмените настройку IP-адреса, потому что данный IP-адрес должен быть назначен интерфейсу GigabitEthernet 0/0/2.

```
[Datacom-Router]interface GigabitEthernet 0/0/1
[Datacom-Router-GigabitEthernet0/0/1]undo ip address
```

Для этого необходимо отменить настройку IP-адреса GigabitEthernet0/0/1. В противном случае возникнет конфликт IP-адресов, и новые настройки не вступят в силу.

Чтобы отменить действие команды, введите перед ней ключевое слово **undo**. Команда **undo**, как правило, используется для восстановления настроек по умолчанию, отключения какой-либо функции или удаления конфигурации. Почти в каждой командной строке есть соответствующая команда отмены.

```
[Datacom-Router]interface GigabitEthernet 0/0/2
[Datacom-Router-GigabitEthernet0/0/2]ip address 192.168.1.1 24
[Datacom-Router-GigabitEthernet0/0/2]quit
```

Выведите на экран текущую конфигурацию устройства.

```
[Datacom-Router]display current-configuration
```

```
[V200R003C00]
#
sysname Datcom-Router
#
snmp-agent local-engineid 800007DB03000000000000
snmp-agent
#
clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load portalpage.zip
#
drop illegal-mac alarm
#
set cpu-usage threshold 80 restore 75
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher %$%$K8m.Nt84DZ}e#<o'8bmE3Uw}%$%$
local-user admin service-type http
#
---- More ----
```

Если информация не помещается полностью на одном экране, система приостанавливает ее вывод, чтобы пользователь мог посмотреть информацию. Если в конце командного вывода отображается ---- **More** ----, вы можете выполнить одно из следующих действий:

1. Нажать сочетание клавиш Ctrl+C или Ctrl+Z, чтобы остановить вывод информации или выполнение команды.
2. Нажать пробел, чтобы перейти к следующему экрану с информацией.
3. Нажать Enter, чтобы перейти к следующей строке.

Шаг 4 Сохраните текущую конфигурацию устройства.

Вернитесь в режим пользователя.

```
[Datcom-Router]quit
<Datcom-Router>
```

Помимо команды **quit**, для возврата в режим пользователя из любого другого режима можно воспользоваться:

1. командой **return**;
2. сочетанием клавиш Ctrl+Z.

Сохраните конфигурацию.

```
<Datcom-Router>save
The current configuration will be written to the device.
Are you sure to continue? .(y/n)[n]:y //Введите y для подтверждения.
It will take several minutes to save configuration file, please wait.....
```



```
Configuration file had been saved successfully
Note: The configuration file will take effect after being activated
```

Текущая конфигурация успешно сохранена.

Изменения конфигурации должны быть сохранены в конфигурационном файле, чтобы остаться в силе после перезагрузки системы. С помощью команды **save** можно сохранить текущую конфигурацию в папку по умолчанию и перезаписать исходный конфигурационный файл. Также можно выполнить команду **save configuration-file**, чтобы сохранить текущую конфигурацию в определенный файл на устройстве хранения. После выполнения этой команды текущий файл конфигурации системной загрузки останется без изменений.

Сравните текущую конфигурацию с конфигурацией в файле загрузки.

```
<Datcom-Router>compare configuration
The current configuration is the same as the next startup configuration file.
```

Текущая конфигурация осталась такой же, как и была в файле конфигурации загрузки.

Шаг 5 Выполните операции в файловой системе.

Выведите на экран список всех файлов в текущем каталоге.

```
<Datcom-Router>dir
Directory of flash:/

Idx  Attr   Size(Byte)  Date      Time(LMT)  FileName
  0  -rw-   126,538,240 Jul 04 2016 17:57:22  ar651c-v300r019c00Sspc100.cc
  1  -rw-      22,622 Feb 20 2020 10:35:18  mon_file.txt
  2  -rw-      737 Feb 20 2020 10:38:36  vrpcfg.zip
  3  drw-         - Jul 04 2016 18:51:04  CPM_ENCRYPTED_FOLDER
  4  -rw-      783 Jul 10 2018 14:46:16  default_local.cer
  5  -rw-         0 Sep 11 2017 00:00:54  brdxpon_snmp_cfg.efs
  6  drw-         - Sep 11 2017 00:01:22  update
  7  drw-         - Sep 11 2017 00:01:48  shelldir
  8  drw-         - Sep 21 2019 17:14:24  localuser
  9  drw-         - Sep 15 2017 04:35:52  dhcp
 10  -rw-      509 Feb 20 2020 10:38:40  private-data.txt
 11  -rw-      2,686 Dec 19 2019 15:05:18  mon_lpu_file.txt
 12  -rw-      3,072 Dec 18 2019 18:15:54  Boot_LogFile
```

510,484 KB total available (386,456 KB free)

vrpcfg.zip — конфигурационный файл. Расширение конфигурационного файла должно быть .cfg или .zip.

ar651c-v300r019c00Sspc100.cc — системное программное обеспечение. Расширение файла системного программного обеспечения должно быть .cc.

Сохраните текущую конфигурацию и назовите конфигурационный файл — test.cfg.

```
<Datcom-Router>save test.cfg
Are you sure to save the configuration to test.cfg? (y/n)[n]:y           //Введите y для
подтверждения.
It will take several minutes to save configuration file, please wait.....
Configuration file had been saved successfully
Note: The configuration file will take effect after being activated
```

Выведите снова список всех файлов в текущем каталоге.

```
<Datacom-Router>dir
Directory of flash:/

   Idx  Attr      Size(Byte)      Date    Time(LMT)      FileName
   ---  -
    0   -rw-    126,538,240    Jul 04 2016 17:57:22  ar651c- v300r019c00Sspc100.cc
    1   -rw-         22,622    Feb 20 2020 10:35:18  mon_file.txt
    2   -rw-         737    Feb 20 2020 10:38:36  vrpcfg.zip
    3   drw-          -    Jul 04 2016 18:51:04  CPM_ENCRYPTED_FOLDER
    4   -rw-         783    Jul 10 2018 14:46:16  default_local.cer
    5   -rw-          0    Sep 11 2017 00:00:54  brdxdp_on_snmp_cfg.efs
    6   drw-          -    Sep 11 2017 00:01:22  update
    7   drw-          -    Sep 11 2017 00:01:48  shell_dir
    8   drw-          -    Sep 21 2019 17:14:24  localuser
    9   drw-          -    Sep 15 2017 04:35:52  dhcp
   10  -rw-    1,404    Feb 20 2020 11:55:17  test.cfg
   11  -rw-         509    Feb 20 2020 11:55:18  private-data.txt
   12  -rw-     2,686    Dec 19 2019 15:05:18  mon_lpu_file.txt
   13  -rw-     3,072    Dec 18 2019 18:15:54  Boot_LogFile
```

510,484 KB total available (386 452 KB free)

Конфигурационный файл успешно сохранен.

Задайте этот файл в качестве файла конфигурации загрузки.

```
<Datacom-Router>startup saved-configuration test.cfg
This operation will take several minutes, please wait.....
Info: Succeeded in setting the file for booting system
```

Выведите на экран информацию о файле конфигурации загрузки.

```
<Datacom-Router>display startup
MainBoard:
Startup system software:          flash:/ ar651c- v300r019c00Sspc100.cc
Next startup system software:     flash:/ ar651c- v300r019c00Sspc100.cc
Backup system software for next startup: null
Startup saved-configuration file: flash:/vrpcfg.zip
Next startup saved-configuration file: flash:/test.cfg
Startup license file:             null
Next startup license file:        null
Startup patch package:            null
Next startup patch package:       null
Startup voice-files:              null
Next startup voice-files:         null
```

Команда **display startup** позволяет вывести на экран информацию о конфигурации и программном обеспечении системы, лицензиях, патчах и голосовых файлах.

Удалите файл конфигурации.

```
<Datacom-Router>reset saved-configuration
This will delete the configuration in the flash memory.
The device configuration
ns will be erased to reconfigure.
Are you sure? (y/n)[n]:y //Введите y для подтверждения.
Clear the configuration in the device successfully.
```

Шаг 6 Перезагрузите устройство.



```
<Datacom-Router>reboot
Info: The system is comparing the configuration, please wait.
System will reboot! Continue ? [y/n]:y           //Введите y для подтверждения.
Info: system is rebooting ,please wait...
The system is restarting.
<Datacom-Router>
Устройство перезагружается.

----Конец
```

1.3 Проверка

Подробности данной операции здесь не приводятся.

1.4 Справочные конфигурации

Подробная информация здесь не приводится.

1.5 Вопросы

1. Ознакомьтесь с функциональными клавишами системы Huawei VRP в соответствии с разделом 1.6 Приложение.
2. На шаге 5 команда **reset saved-configuration** выполняется для удаления конфигурации. Почему после перезапуска устройства конфигурация сохраняется?

1.6 Приложение

Табл. 1-1 Функциональные клавиши системы

Сочетания клавиш	Функция
<Ctrl+A>	Перемещение курсора в начало текущей строки.
<Ctrl+B>	Перемещение курсора на один символ назад.
<Ctrl+C>	Завершение выполнения текущих функций.
<Ctrl+D>	Удаление символа на месте курсора.
<Ctrl+E>	Перемещение курсора в конец текущей строки.
<Ctrl+F>	Перемещение курсора на один символ вперед.
<Ctrl+H>	Удаление символа слева от курсора.

Сочетания клавиш	Функция
<Ctrl+K>	Завершение исходящего вызова во время установления соединения.
<Ctrl+N> или клавиша «стрелка вниз»	Отображение следующей команды в истории команд.
<Ctrl+N> или клавиша «стрелка вверх»	Отображение предыдущей команды в истории команд.
<Ctrl+T>	Ввод вопросительного знака (?).
<Ctrl+W>	Удаление строки символов (слова) слева от курсора.
<Ctrl+X>	Удаление всех символов слева от курсора.
<Ctrl+Y>	Удаление символа на месте курсора и всех символов справа от курсора.
<Ctrl+Z>	Возврат в режим пользователя.
<Ctrl+J>	Завершение или перенаправление входящих соединений.
<Esc+B>	Перемещение курсора на одну строку символов (слово) назад.
<Esc+D>	Удаление одной строки символов (слова) справа от курсора.
<Esc+F>	Перемещение курсора на строку символов (слово) вперед.

2

Создание взаимосвязанной IP-сети

2.1 Лабораторная работа 1. Адресация и маршрутизация IPv4

2.1.1 Общая информация

2.1.1.1 О лабораторной работе

IPv4 является четвертой версией интернет-протокола (IP). Это основной протокол из набора протоколов TCP/IP, который работает на уровне Интернета в модели TCP/IP или на сетевом уровне в модели OSI. Сетевой уровень обеспечивает передачу данных без установления соединения. Каждая IP-дейтаграмма передается независимо, что устраняет необходимость устанавливать соединение перед отправкой IP-дейтаграмм.

Маршрутизация — основной процесс в сетях передачи данных. Он позволяет выбирать маршруты в сети, по которым пакеты передаются от источника в пункт назначения.

С помощью этой лабораторной работы вы научитесь настраивать адреса IPv4 и статические маршруты IPv4, а также поймете основные принципы маршрутизации.

2.1.1.2 Цели

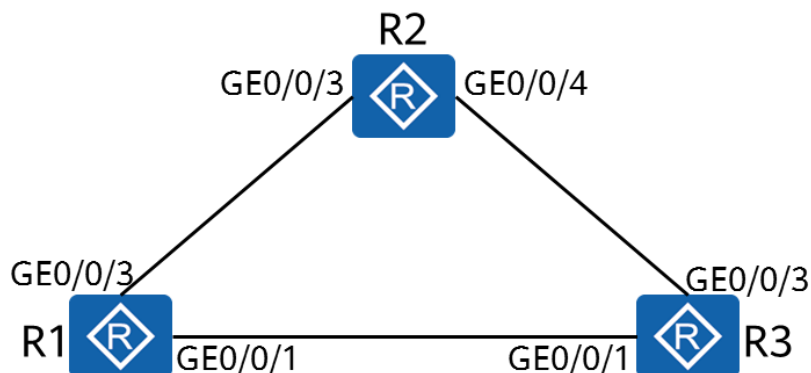
Лабораторная работа помогает получить практические навыки по изучению следующих тем:

- Процедура настройки IPv4-адреса на интерфейсе
- Функции и значение loopback-интерфейсов
- Принципы генерирования прямых маршрутов
- Процедура настройки статических маршрутов и условия, при которых используются статические маршруты
- Процедура проверки возможности установления соединения сетевого уровня с помощью инструмента ping
- Процедура настройки статических маршрутов и сценарии их применения

2.1.1.3 Топология сети

Маршрутизаторы R1, R2 и R3 являются шлюзами определенных сетей. Для подключения к этим сетям необходимо настроить шлюзы.

Рис. 2-1 Топология сети для настройки адресации и маршрутизации IPv4, используемая в данной лабораторной работе



2.1.2 Лабораторная работа

2.1.2.1 План работы

1. Настройка IP-адресов для интерфейсов на маршрутизаторах.
2. Настройка статических маршрутов для установления связи между маршрутизаторами.

2.1.2.2 Процедура конфигурирования

Шаг 1 Настройте основные параметры устройств.

Задайте имена устройствам.

Подробности данной операции здесь не приводятся.

Шаг 2 Выведите на экран IP-адрес текущего интерфейса и таблицу маршрутизации маршрутизатора.

Выведите на экран статус интерфейса на маршрутизаторе (в данном случае на примере R1).

```
[R1]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 3
The number of interface that is DOWN in Physical is 5
The number of interface that is UP in Protocol is 1
The number of interface that is DOWN in Protocol is 10
```

Interface	IP Address/Mask	Physical	Protocol
GigabitEthernet0/0/1	unassigned	up	down
GigabitEthernet0/0/2	unassigned	up	down
GigabitEthernet0/0/3	unassigned	up	down

Команда **display ip interface brief** позволяет вывести на экран краткую информацию об IP-адресах интерфейсов, включая IP-адреса, маски подсети, физический статус, статус протокола канального уровня и количество интерфейсов с различными статусами.

Для интерфейсов GigabitEthernet0/0/1 и GigabitEthernet0/0/3 маршрутизатора R1 не настроены IP-адреса. Следовательно, поле IP Address/Mask (IP-адрес/маска) имеет значение unassigned (не настроено), поле Protocol (Протокол) имеет значение down (не работает), а поле Physical (Физический статус) имеет значение up (работает).

Выведите на экран таблицу маршрутизации на маршрутизаторе (в данном случае на примере R1).

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
```

Routing Tables: Public
Destinations : 4 Routes : 4

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

InLoopBack0 — это loopback-интерфейс по умолчанию.

InLoopBack0 использует фиксированный кольцевой адрес 127.0.0.1/8 для приема пакетов данных, предназначенных для хоста, на котором находится InLoopBack0. IP-адрес интерфейса InLoopBack0 нельзя изменить или анонсировать с помощью протокола маршрутизации.

Шаг 3 Настройте IP-адреса для физических интерфейсов.

Настройте IP-адреса для физических интерфейсов на основе следующей таблицы.

Табл. 2-1 IP-адреса физических интерфейсов

Маршрутизатор	Интерфейс	IP-адрес/маска
R1	GigabitEthernet0/0/1	10.0.13.1/24
	GigabitEthernet0/0/3	10.0.12.1/24
R2	GigabitEthernet0/0/3	10.0.12.2/24
	GigabitEthernet0/0/4	10.0.23.2/24
R3	GigabitEthernet0/0/1	10.0.13.3/24
	GigabitEthernet0/0/3	10.0.23.3/24

```
<R1>system-view
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.13.1 24
[R1-GigabitEthernet0/0/1]quit
```

```
[R1]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.0.12.1 24
[R1-GigabitEthernet0/0/3]quit
```

```
<R2>system-view
[R2]interface GigabitEthernet0/0/3
[R2-GigabitEthernet0/0/3]ip address 10.0.12.2 24
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet0/0/4
[R2-GigabitEthernet0/0/4]ip address 10.0.23.2 24
[R2-GigabitEthernet0/0/4]quit
```

```
<R3>system-view
[R3]interface GigabitEthernet0/0/1
[R3-GigabitEthernet0/0/1]ip address 10.0.13.3 24
[R3-GigabitEthernet0/0/1]quit
[R3]interface GigabitEthernet0/0/3
[R3-GigabitEthernet0/0/3]ip address 10.0.23.3 24
[R3-GigabitEthernet0/0/3]quit
```

Проверьте наличие связи с помощью инструмента ping.

```
[R1]ping 10.0.12.2
  PING 10.0.12.2: 56 data bytes, press CTRL_C to break
    Reply from 10.0.12.2: bytes=56 Sequence=1 ttl=255 time=70 ms
    Reply from 10.0.12.2: bytes=56 Sequence=2 ttl=255 time=50 ms
    Reply from 10.0.12.2: bytes=56 Sequence=3 ttl=255 time=40 ms
    Reply from 10.0.12.2: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 10.0.12.2: bytes=56 Sequence=5 ttl=255 time=50 ms

  --- 10.0.12.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/48/70 ms
```

```
[R1]ping 10.0.13.3
  PING 10.0.13.3: 56 data bytes, press CTRL_C to break
    Reply from 10.0.13.3: bytes=56 Sequence=1 ttl=255 time=50 ms
    Reply from 10.0.13.3: bytes=56 Sequence=2 ttl=255 time=60 ms
    Reply from 10.0.13.3: bytes=56 Sequence=3 ttl=255 time=50 ms
    Reply from 10.0.13.3: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 10.0.13.3: bytes=56 Sequence=5 ttl=255 time=30 ms

  --- 10.0.13.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/44/60 ms
```

Выведите на экран таблицу маршрутизации R1.

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
```


Routing Tables: Public

Destinations : 10

Routes : 10

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.12.0/24	Direct	0	0	D	10.0.12.1	GigabitEthernet0/0/3
10.0.12.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.12.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.13.0/24	Direct	0	0	D	10.0.13.1	GigabitEthernet0/0/1
10.0.13.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

Из приведенных выше результатов выполнения команды видно, что после настройки IP-адресов для каждого интерфейса автоматически генерируются три прямых маршрута:

1. Маршрут к сети, в которой находится интерфейс
2. Маршрут от хоста к интерфейсу
3. Маршрут от хоста к широковещательному адресу в сети, в которой находится интерфейс

📖 ПРИМЕЧАНИЕ

Маршрут от хоста — это маршрут с 32-битной маской.

Шаг 4 Создайте loopback-интерфейс.

Настройте loopback-интерфейс в соответствии со следующей таблицей.

Табл. 2-2 IP-адреса loopback-интерфейсов

Маршрутизатор	Интерфейс	IP-адрес/маска
R1	LoopBack0	10.0.1.1/32
R2	LoopBack0	10.0.1.2/32
R3	LoopBack0	10.0.1.3/32

Loopback-интерфейсы — это настроенные вручную логические интерфейсы, которые физически не существуют. Логические интерфейсы могут использоваться для обмена данными. Loopback-интерфейс всегда находится в рабочем состоянии (статус Up) на физическом и канальном уровнях, если только он не был отключен вручную. Обычно loopback-интерфейс имеет 32-битную маску. Loopback-интерфейсы используются в следующих случаях:

1. В качестве адреса для идентификации и управления маршрутизатором.
2. В качестве идентификатора маршрутизатора в OSPF.
3. Для повышения надежности сети.

В этой лабораторной работе loopback-интерфейсы используются для имитации клиентов.

```
[R1]interface LoopBacko
[R1-LoopBacko]ip address 10.0.1.1 32
[R2]interface LoopBacko
[R2-LoopBacko]ip address 10.0.1.2 32
[R3]interface LoopBacko
[R3-LoopBacko]ip address 10.0.1.3 32
```

Выведите на экран таблицу маршрутизации на маршрутизаторе (в данном случае на примере R1).

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
```

Routing Tables: Public

Destinations : 11 Routes : 11

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.1.1/32	Direct	0	0	D	127.0.0.1	LoopBacko
10.0.12.0/24	Direct	0	0	D	10.0.12.1	GigabitEthernet0/0/3
10.0.12.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.12.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.13.0/24	Direct	0	0	D	10.0.13.1	GigabitEthernet0/0/1
10.0.13.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBacko
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBacko
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBacko
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBacko

Прямые маршруты сгенерированы.

Проверьте наличие связи между loopback-интерфейсами.

```
[R1]ping -a 10.0.1.1 10.0.1.2
PING 10.0.1.2: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- 10.0.1.2 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss
```

Команда **ping -a source-ip-address destination-ip-address** используется для указания IP-адресов источника и пункта назначения пакетов ping. На данный момент у маршрутизатора нет маршрута к IP-адресу пункта назначения. Таким образом, операция ping не выполняется.

Шаг 5 Настройте статические маршруты.

На маршрутизаторе R1 настройте маршрут к интерфейсам LoopBacko маршрутизаторов R2 и R3.

```
[R1]ip route-static 10.0.1.2 32 10.0.12.2
[R1]ip route-static 10.0.1.3 32 10.0.13.3
```

Выведите на экран таблицу маршрутизации R1.

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
```

```
-----
```

Routing Tables: Public

	Destinations : 13	Routes : 13					
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface	
10.0.1.1/32	Direct	0	0	D	127.0.0.1	LoopBacko	
10.0.1.2/32	Static	60	0	RD	10.0.12.2	GigabitEthernet0/0/3	
10.0.1.3/32	Static	60	0	RD	10.0.13.3	GigabitEthernet0/0/1	
10.0.12.0/24	Direct	0	0	D	10.0.12.1	GigabitEthernet0/0/3	
10.0.12.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3	
10.0.12.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3	
10.0.13.0/24	Direct	0	0	D	10.0.13.1	GigabitEthernet0/0/1	
10.0.13.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1	
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1	
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBacko	
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBacko	
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBacko	
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBacko	

Сконфигурированные статические маршруты были добавлены в таблицу IP-маршрутизации.

Проверьте возможность установления связи.

```
[R1]ping -a 10.0.1.1 10.0.1.2
PING 10.0.1.2: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- 10.0.1.2 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss
```

Связь с интерфейсом LoopBacko маршрутизатора R2 по-прежнему отсутствует, поскольку у R2 нет маршрута к интерфейсу LoopBacko маршрутизатора R1.

На R2 добавьте маршрут к интерфейсу LoopBacko маршрутизатора R1.

```
[R2]ip route-static 10.0.1.1 32 10.0.12.1
```

Проверьте возможность установления связи.

```
<R1>ping -a 10.0.1.1 10.0.1.2
PING 10.0.1.2: 56 data bytes, press CTRL_C to break
Reply from 10.0.1.2: bytes=56 Sequence=1 ttl=255 time=60 ms
Reply from 10.0.1.2: bytes=56 Sequence=2 ttl=255 time=30 ms
```

```
Reply from 10.0.1.2: bytes=56 Sequence=3 ttl=255 time=10 ms
Reply from 10.0.1.2: bytes=56 Sequence=4 ttl=255 time=50 ms
Reply from 10.0.1.2: bytes=56 Sequence=5 ttl=255 time=30 ms
```

```
--- 10.0.1.2 ping statistics ---
```

```
5 packet(s) transmitted
```

```
5 packet(s) received
```

```
0.00% packet loss
```

```
round-trip min/avg/max = 10/36/60 ms
```

LoopBacko на R1 может взаимодействовать с LoopBacko на R2.

Настройте другие необходимые маршруты.

```
[R2]ip route-static 10.0.1.3 32 10.0.23.3
```

```
[R3]ip route-static 10.0.1.1 32 10.0.13.1
```

```
[R3]ip route-static 10.0.1.2 32 10.0.23.2
```

Проверьте возможность установления связи между интерфейсами LoopBacko маршрутизаторов, следуя приведенной процедуре.

Шаг 6 Настройте маршрут от R1 к R2 через R3 в качестве резервного маршрута от LoopBacko R1 к LoopBacko R2.

Настройте статические маршруты на R1 и R2.

```
[R1]ip route-static 10.0.1.2 32 10.0.13.3 preference 100
```

```
[R2]ip route-static 10.0.1.1 32 10.0.23.3 preference 100
```

Выведите на экран таблицы маршрутизации R1 и R2.

```
[R1]display ip routing-table
```

```
Route Flags: R - relay, D - download to fib
```

```
-----
```

```
Routing Tables: Public
```

```
Destinations : 13
```

```
Routes : 13
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.1.1/32	Direct	0	0	D	127.0.0.1	LoopBacko
10.0.1.2/32	Static	60	0	RD	10.0.12.2	GigabitEthernet0/0/3
10.0.1.3/32	Static	60	0	RD	10.0.13.3	GigabitEthernet0/0/1
10.0.12.0/24	Direct	0	0	D	10.0.12.1	GigabitEthernet0/0/3
10.0.12.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.12.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.13.0/24	Direct	0	0	D	10.0.13.1	GigabitEthernet0/0/1
10.0.13.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBacko
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBacko
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBacko
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBacko

```
[R2]display ip routing-table
```

```
Route Flags: R - relay, D - download to fib
```

```
-----
```

```
Routing Tables: Public
```

Destinations : 13				Routes : 13			
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface	
10.0.1.1/32	Static	60	0	RD	10.0.12.1	GigabitEthernet0/0/3	
10.0.1.2/32	Direct	0	0	D	127.0.0.1	LoopBacko	
10.0.1.3/32	Static	60	0	RD	10.0.23.3	GigabitEthernet0/0/4	
10.0.12.0/24	Direct	0	0	D	10.0.12.2	GigabitEthernet0/0/3	
10.0.12.2/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3	
10.0.12.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3	
10.0.23.0/24	Direct	0	0	D	10.0.23.2	GigabitEthernet0/0/4	
10.0.23.2/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/4	
10.0.23.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/4	
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBacko	
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBacko	
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBacko	
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBacko	

Статический маршрут со значением предпочтения 100 не был добавлен в таблицу маршрутизации.

Отключите интерфейс GigabitEthernet0/0/3 на маршрутизаторах R1 и R2, чтобы сделать недействительным маршрут с наивысшим приоритетом.

```
[R1]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]shutdown
```

Выведите на экран таблицы маршрутизации на R1 и R2. Из командного вывода видно, что маршруты с более низким приоритетом активируются, когда маршруты с более высоким приоритетом становятся недействительными.

[R1]display IP routing-table							
Route Flags: R - relay, D - download to fib							

Routing Tables: Public							
Destinations : 10				Routes : 10			
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface	
10.0.1.1/32	Direct	0	0	D	127.0.0.1	LoopBacko	
10.0.1.2/32	Static	100	0	RD	10.0.13.3	GigabitEthernet0/0/1	
10.0.1.3/32	Static	60	0	RD	10.0.13.3	GigabitEthernet0/0/1	
10.0.13.0/24	Direct	0	0	D	10.0.13.1	GigabitEthernet0/0/1	
10.0.13.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1	
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1	
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBacko	
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBacko	
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBacko	
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBacko	

[R2]display ip routing-table							
Route Flags: R - relay, D - download to fib							

Routing Tables: Public							
Destinations : 10				Routes : 10			
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface	

10.0.1.1/32	Static	100	o	RD	10.0.23.3	GigabitEthernet0/0/4
10.0.1.2/32	Direct	o	o	D	127.0.0.1	LoopBacko
10.0.1.3/32	Static	60	o	RD	10.0.23.3	GigabitEthernet0/0/4
10.0.23.0/24	Direct	o	o	D	10.0.23.2	GigabitEthernet0/0/4
10.0.23.2/32	Direct	o	o	D	127.0.0.1	GigabitEthernet0/0/4
10.0.23.255/32	Direct	o	o	D	127.0.0.1	GigabitEthernet0/0/4
127.0.0.0/8	Direct	o	o	D	127.0.0.1	InLoopBacko
127.0.0.1/32	Direct	o	o	D	127.0.0.1	InLoopBacko
127.255.255.255/32	Direct	o	o	D	127.0.0.1	InLoopBacko
255.255.255.255/32	Direct	o	o	D	127.0.0.1	InLoopBacko

В этом случае исходный статический маршрут становится недействительным и активируется статический маршрут с более низким приоритетом.

Проверьте возможность установления связи.

```
[R1]ping -a 10.0.1.1 10.0.1.2
PING 10.0.1.2: 56 data bytes, press CTRL_C to break
Reply from 10.0.1.2: bytes=56 Sequence=1 ttl=254 time=80 ms
Reply from 10.0.1.2: bytes=56 Sequence=2 ttl=254 time=60 ms
Reply from 10.0.1.2: bytes=56 Sequence=3 ttl=254 time=60 ms
Reply from 10.0.1.2: bytes=56 Sequence=4 ttl=254 time=110 ms
Reply from 10.0.1.2: bytes=56 Sequence=5 ttl=254 time=80 ms

--- 10.0.1.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 60/78/110 ms
```

Выполните трассировку маршрута, по которому передаются пакеты данных.

```
[R1]tracert -a 10.0.1.1 10.0.1.2

traceroute to 10.0.1.2(10.0.1.2), max hops: 30 ,packet length: 40,press CTRL_C to break

1 10.0.13.3 40 ms 30 ms 50 ms

2 10.0.23.2 80 ms 80 ms 60 ms
```

С помощью команды **tracert** можно проследить путь пакетов от источника до пункта назначения.

Из командного вывода видно, что пакеты данных проходят через интерфейсы GigabitEthernet0/0/1 и GigabitEthernet0/0/3 маршрутизатора R3, а затем перенаправляются на интерфейс GigabitEthernet0/0/4 маршрутизатора R2.

ПРИМЕЧАНИЕ

В некоторых лабораторных условиях устройства могут не отвечать на пакеты ICMP из-за настроек безопасности. Поэтому результаты могут отличаться. Для завершения трассировки можно нажать сочетание клавиш Ctrl+C.

Шаг 7 Настройте маршруты по умолчанию для установления связи между интерфейсом LoopBacko маршрутизатора R1 и интерфейсом LoopBacko маршрутизатора R2.

Включите интерфейсы и удалите настроенные маршруты.

```
[R1]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]undo shutdown
[R1-GigabitEthernet0/0/3]quit
[R1]undo ip route-static 10.0.1.2 255.255.255.255 10.0.12.2
[R1]undo ip route-static 10.0.1.2 255.255.255.255 10.0.13.3 preference 100
```

Выведите на экран таблицу маршрутизации R1.

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
```

Routing Tables: Public

Destinations : 12 Routes : 12

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.1.1/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.1.3/32	Static	60	0	RD	10.0.13.3	GigabitEthernet0/0/1
10.0.12.0/24	Direct	0	0	D	10.0.12.1	GigabitEthernet0/0/3
10.0.12.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.12.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.13.0/24	Direct	0	0	D	10.0.13.1	GigabitEthernet0/0/1
10.0.13.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

R1 не имеет маршрута к LoopBack0 (10.1.1.2/32) маршрутизатора R2.

Настройте маршрут по умолчанию на R1.

```
[R1]ip route-static 0.0.0.0 0 10.0.12.2
```

Выведите на экран таблицу маршрутизации R1.

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
```

Routing Tables: Public

Destinations : 13 Routes : 13

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
0.0.0.0/0	Static	60	0	RD	10.0.12.2	GigabitEthernet0/0/3
10.0.1.1/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.1.3/32	Static	60	0	RD	10.0.13.3	GigabitEthernet0/0/1
10.0.12.0/24	Direct	0	0	D	10.0.12.1	GigabitEthernet0/0/3
10.0.12.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.12.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.13.0/24	Direct	0	0	D	10.0.13.1	GigabitEthernet0/0/1
10.0.13.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0

127.255.255.255/32	Direct	o	o	D	127.0.0.1	InLoopBacko
255.255.255.255/32	Direct	o	o	D	127.0.0.1	InLoopBacko

Маршрут по умолчанию был активирован.

Проверьте наличие связи между LoopBacko маршрутизатора R1 и LoopBacko маршрутизатора R2.

```
[R1]ping -a 10.0.1.1 10.0.1.2
PING 10.0.1.2: 56 data bytes, press CTRL_C to break
  Reply from 10.0.1.2: bytes=56 Sequence=1 ttl=255 time=50 ms
  Reply from 10.0.1.2: bytes=56 Sequence=2 ttl=255 time=30 ms
  Reply from 10.0.1.2: bytes=56 Sequence=3 ttl=255 time=20 ms
  Reply from 10.0.1.2: bytes=56 Sequence=4 ttl=255 time=40 ms
  Reply from 10.0.1.2: bytes=56 Sequence=5 ttl=255 time=20 ms

--- 10.0.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 20/32/50 ms
```

LoopBacko на R1 может взаимодействовать с LoopBacko на R2.

----Конец

2.1.3 Проверка

Для проверки связи между интерфейсами loopbacko на разных устройствах можно использовать команды ping и tracer.

2.1.4 Справочные конфигурации

Конфигурация на R1

```
#
sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.0.13.1 255.255.255.0
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.1 255.255.255.0
#
interface LoopBacko
 ip address 10.0.1.1 255.255.255.255
#
ip route-static 0.0.0.0 0.0.0.0 10.0.12.2
ip route-static 10.0.1.3 255.255.255.255 10.0.13.3
#
return
```

Конфигурация на R2

```
#
sysname R2
#
interface GigabitEthernet0/0/3
```



```
ip address 10.0.12.2 255.255.255.0
#
interface GigabitEthernet0/0/4
ip address 10.0.23.2 255.255.255.0
#
interface LoopBack0
ip address 10.0.1.2 255.255.255.255
#
ip route-static 10.0.1.1 255.255.255.255 10.0.12.1
ip route-static 10.0.1.1 255.255.255.255 10.0.23.3 preference 100
ip route-static 10.0.1.3 255.255.255.255 10.0.23.3
#
return
```

Конфигурация на R3

```
#
sysname R3
#
interface GigabitEthernet0/0/1
ip address 10.0.13.3 255.255.255.0
#
interface GigabitEthernet0/0/3
ip address 10.0.23.3 255.255.255.0
#
interface LoopBack0
ip address 10.0.1.3 255.255.255.255
#
ip route-static 10.0.1.1 255.255.255.255 10.0.13.1
ip route-static 10.0.1.2 255.255.255.255 10.0.23.2
#
return
```

2.1.5 Вопросы

1. В каких ситуациях настроенный статический маршрут будет добавлен в таблицу IP-маршрутизации? Можно ли добавить маршрут в таблицу IP-маршрутизации, если настроенный следующий переход недоступен?
2. Каким будет IP-адрес источника пакетов ICMP на шаге 3, если при проверке связи между loopback-интерфейсами не указать аргумент -a? Почему?

2.2 Лабораторная работа 2. Маршрутизация OSPF

2.2.1 Общая информация

2.2.1.1 О лабораторной работе

Протокол OSPF (Open Shortest Path First) представляет собой протокол внутреннего шлюза (Interior Gateway Protocol, IGP), разработанный сообществом IETF. Он основан на технологии отслеживания состояния канала (link-state). В настоящее время в сетях IPv4 используется OSPF версии 2 (RFC2328). Как протокол динамической маршрутизации, основанный на технологии отслеживания состояния каналов, OSPF имеет следующие преимущества:

- Многоадресная передача пакетов для снижения нагрузки на коммутаторы, на которых не работает OSPF.
- Бесклассовая междоменная маршрутизация (Classless Inter-Domain Routing, CIDR)
- Балансировка нагрузки между равноценными маршрутами
- Пакетная аутентификация

Благодаря перечисленным выше преимуществам OSPF широко применяется и используется в качестве IGP.

В ходе лабораторной работы вы выполните настройку OSPF для одной области, что позволит вам понять принцип действия OSPF и изучить основные конфигурации.

2.2.1.2 Цели

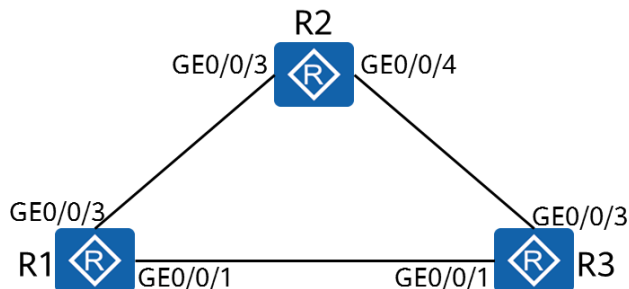
Лабораторная работа помогает получить практические навыки по изучению следующих тем:

- Основные команды OSPF
- Процедура проверки рабочего статуса OSPF
- Процедура настройки выбора маршрутов OSPF на основании их стоимости
- Анонсирование маршрутов по умолчанию в OSPF
- Процедура настройки аутентификации OSPF

2.2.1.3 Топология сети

Маршрутизаторы R1, R2 и R3 являются шлюзами определенных сетей. Для обеспечения связи между этими сетями необходимо сконфигурировать OSPF.

Рис. 2-2 Топология сети для конфигурирования OSPF, используемая в данной лабораторной работе



2.2.2 Лабораторная работа

2.2.2.1 План работы

1. Создание процессов OSPF на устройствах и включение OSPF на интерфейсах.
2. Настройка аутентификации OSPF.
3. Настройка OSPF для анонсирования маршрутов по умолчанию.
4. Управление выбором маршрутов OSPF на основании их стоимости.

2.2.2.2 Процедура конфигурирования

Шаг 1 Настройте основные параметры устройств.

Выполните шаги 1, 2, 3 и 4, приведенные в лабораторной работе 1, чтобы присвоить маршрутизаторам имена и настроить IP-адреса физических интерфейсов и loopback-интерфейсов.

Выведите на экран таблицу маршрутизации на маршрутизаторе (в данном случае на примере R1).

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 11          Routes : 11

Destination/Mask    Proto    Pre  Cost    Flags  NextHop    Interface
-----
10.0.1.1/32         Direct   0    0        D     127.0.0.1   LoopBack0
10.0.12.0/24         Direct   0    0        D     10.0.12.1   GigabitEthernet0/0/3
10.0.12.1/32         Direct   0    0        D     127.0.0.1   GigabitEthernet0/0/3
10.0.12.255/32       Direct   0    0        D     127.0.0.1   GigabitEthernet0/0/3
10.0.13.0/24         Direct   0    0        D     10.0.13.1   GigabitEthernet0/0/1
10.0.13.1/32         Direct   0    0        D     127.0.0.1   GigabitEthernet0/0/1
10.0.13.255/32       Direct   0    0        D     127.0.0.1   GigabitEthernet0/0/1
127.0.0.0/8          Direct   0    0        D     127.0.0.1   InLoopBack0
127.0.0.1/32         Direct   0    0        D     127.0.0.1   InLoopBack0
127.255.255.255/32   Direct   0    0        D     127.0.0.1   InLoopBack0
255.255.255.255/32   Direct   0    0        D     127.0.0.1   InLoopBack0
```

На данный момент на устройстве существуют только прямые маршруты.

Шаг 2 Настройте основные параметры OSPF.

Создайте процесс OSPF.

```
[R1]ospf 1
```

Настройка параметров OSPF станет возможной только после создания процесса OSPF. OSPF поддерживает несколько независимых процессов на одном устройстве. Обмен маршрутами между различными процессами OSPF осуществляется аналогично обмену маршрутами между разными протоколами маршрутизации. При создании процесса OSPF можно указать идентификатор процесса. Если идентификатор процесса не указан, то по умолчанию используется идентификатор процесса 1.

Создайте область OSPF и укажите интерфейсы, на которых необходимо включить OSPF.

```
[R1-ospf-1]area 0
```

С помощью команды **area** можно создать область OSPF и перейти в режим конфигурирования области OSPF.

```
[R1-ospf-1-area-0.0.0.0]network 10.0.12.1 0.0.0.255
```

```
[R1-ospf-1-area-0.0.0.0]network 10.0.13.1 0.0.0.255
```

```
[R1-ospf-1-area-0.0.0.0]network 10.0.1.1 0.0.0.0
```

С помощью команды **network network-address wildcard-mask** можно указать интерфейсы, на которых необходимо включить OSPF. OSPF будет работать на интерфейсе только при соблюдении следующих двух условий:

1. Длина маски IP-адреса интерфейса должна быть не короче, чем длина маски, указанная в команде **network**. Для OSPF должна использоваться обратная маска. Например, 0.0.0.255 указывает, что длина маски составляет 24 бита.
2. Адрес интерфейса должен находиться в пределах сетевого диапазона, указанного в команде **network**.

В данном примере OSPF можно включить на трех интерфейсах, и все они добавлены в область 0.

```
[R2]ospf
```

```
[R2-ospf-1]area 0
```

```
[R2-ospf-1-area-0.0.0.0]network 10.0.12.2 0.0.0.0
```

```
[R2-ospf-1-area-0.0.0.0]network 10.0.23.2 0.0.0.0
```

```
[R2-ospf-1-area-0.0.0.0]network 10.0.1.2 0.0.0.0
```

Если обратная маска в команде **network** включает только нули (0) и IP-адрес интерфейса совпадает с IP-адресом, указанным в команде **network-address**, то на интерфейс также будет работать OSPF.

```
[R3]ospf
```

```
[R3-ospf-1]area 0
```

```
[R3-ospf-1-area-0.0.0.0]network 10.0.13.3 0.0.0.0
```

```
[R3-ospf-1-area-0.0.0.0]network 10.0.23.3 0.0.0.0
```

```
[R3-ospf-1-area-0.0.0.0]network 10.0.1.3 0.0.0.0
```

Шаг 3 Выведите на экран рабочий статус OSPF.

Выведите на экран информацию о соседях OSPF.

```
[R1]display ospf peer

OSPF Process 1 with Router ID 10.0.1.1
Neighbors

Area 0.0.0.0 interface 10.0.13.1(GigabitEthernet0/0/1)'s neighbors
Router ID: 10.0.1.3      Address: 10.0.13.3
State: Full  Mode:Nbr is Master  Priority: 1
DR: 10.0.13.3  BDR: 10.0.13.1  MTU: 0
Dead timer due in 36 sec
Retrans timer interval: 0
Neighbor is up for 00:00:30
Authentication Sequence: [ 0 ]

Neighbors

Area 0.0.0.0 interface 10.0.12.1(GigabitEthernet0/0/3)'s neighbors
Router ID: 10.0.1.2      Address: 10.0.12.2
State: Full  Mode:Nbr is Master  Priority: 1
DR: 10.0.12.2  BDR: 10.0.12.1  MTU: 0
Dead timer due in 39 sec
Retrans timer interval: 4
Neighbor is up for 00:00:28
Authentication Sequence: [ 0 ]
```

Команда **display ospf peer** позволяет вывести на экран информацию о соседях в каждой области OSPF. Информация включает в себя область, к которой принадлежит сосед, идентификатор маршрутизатора соседа, статус соседа, DR и BDR.

Выведите на экран маршруты, полученные от OSPF.

```
[R1]display ip routing-table protocol ospf
Route Flags: R - relay, D - download to fib

-----
Public routing table : OSPF
Destinations : 3      Routes : 4

OSPF routing table status : <Active>
Destinations : 3      Routes : 4

Destination/Mask    Proto  Pre  Cost    Flags  NextHop    Interface
-----
10.0.1.2/32         OSPF   10   1        D     10.0.12.2   GigabitEthernet0/0/3
10.0.1.3/32         OSPF   10   1        D     10.0.13.3   GigabitEthernet0/0/1
10.0.23.0/24        OSPF   10   2        D     10.0.13.3   GigabitEthernet0/0/1
                   OSPF   10   2        D     10.0.12.2   GigabitEthernet0/0/3

OSPF routing table status : <Inactive>
Destinations : 0      Routes : 0
```

Шаг 4 Настройте аутентификацию OSPF.

Настройте на маршрутизаторе R1 аутентификацию интерфейса.

```
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ospf authentication-mode md5 1 cipher HCIA-Datcom
[R1]interface GigabitEthernet0/0/3
```

```
[R1- GigabitEthernet0/0/3]ospf authentication-mode md5 1 cipher HCIA-Datcom
[R1- GigabitEthernet0/0/3]display this
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.1 255.255.255.0
 ospf authentication-mode md5 1 cipher foCQTYsq-4.A\^38y!DVwQo#
#
```

При просмотре конфигурации пароль отображается в зашифрованном виде, поскольку в команде указано слово «cipher», обеспечивающее шифрование текста.

Выведите на экран соседей OSPF.

```
[R1]display ospf peer brief
```

```
OSPF Process 1 with Router ID 10.0.1.1
Peer Statistic Information
```

Area Id	Interface	Neighbor id	State
---------	-----------	-------------	-------

```
Total Peer(s): 0
```

На других маршрутизаторах аутентификация не настроена. Следовательно, аутентификация не выполняется, и данные о соседях недоступны.

Настройте аутентификацию интерфейса на маршрутизаторе R2.

```
[R2]interface GigabitEthernet0/0/3
[R2- GigabitEthernet0/0/3]ospf authentication-mode md5 1 cipher HCIA-Datcom
[R2]interface GigabitEthernet0/0/4
[R2- GigabitEthernet0/0/4]ospf authentication-mode md5 1 cipher HCIA-Datcom
```

Выведите на экран соседей OSPF на R2.

```
[R2]display ospf peer brief
```

```
OSPF Process 1 with Router ID 10.0.1.2
Peer Statistic Information
```

Area Id	Interface	Neighbor id	State
0.0.0.0	GigabitEthernet0/0/3	10.0.1.1	Full

```
Total Peer(s): 1
```

Маршрутизатор R2 установил отношения соседства с маршрутизатором R1.

Настройте аутентификацию области на R3.

```
[R3]ospf
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]authentication-mode md5 1 cipher HCIA-Datcom
```

Выведите на экран соседей OSPF на R3.

```
[R3]display ospf peer brief
```

```
OSPF Process 1 with Router ID 10.0.1.3
Peer Statistic Information
```

Area Id	Interface	Neighbor id	State
---------	-----------	-------------	-------

0.0.0.0	GigabitEthernet0/0/1	10.0.1.1	Full
0.0.0.0	GigabitEthernet0/0/3	10.0.1.2	Full

Total Peer(s): 2

Маршрутизатор R3 установил отношения соседства с маршрутизаторами R1 и R2.

Примечание: аутентификация интерфейса OSPF и аутентификация области OSPF реализуют аутентификацию пакетов OSPF на интерфейсах OSPF.

Шаг 5 Предположим, что R1 является граничным маршрутизатором всех сетей. Таким образом, маршрутизатор R1 анонсирует маршрут OSPF по умолчанию.

Анонсируйте маршрут по умолчанию на R1.

```
[R1]ospf
[R1-ospf-1]default-route-advertise always
```

Команда **default-route-advertise** позволяет анонсировать маршрут по умолчанию в общую область OSPF. Если аргумент **always** не указан, маршрут по умолчанию анонсируется другим маршрутизаторам только тогда, когда в таблице маршрутизации локального маршрутизатора есть активные маршруты по умолчанию других протоколов, не OSPF. В данном случае в локальной таблице маршрутизации маршрут по умолчанию отсутствует. Таким образом, необходимо использовать аргумент **always**.

Выведите на экран таблицы IP-маршрутизации R2 и R3.

```
[R2]display ip routing-table
Route Flags: R - relay, D - download to fib
```

Routing Tables: Public

Destinations : 15 Routes : 16

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
0.0.0.0/0	O_ASE	150	1		D 10.0.12.1	GigabitEthernet0/0/3
10.0.1.1/32	OSPF	10	1		D 10.0.12.1	GigabitEthernet0/0/3
10.0.1.2/32	Direct	0	0		D 127.0.0.1	LoopBack0
10.0.1.3/32	OSPF	10	1		D 10.0.23.3	GigabitEthernet0/0/4
10.0.12.0/24	Direct	0	0		D 10.0.12.2	GigabitEthernet0/0/3
10.0.12.2/32	Direct	0	0		D 127.0.0.1	GigabitEthernet0/0/3
10.0.12.255/32	Direct	0	0		D 127.0.0.1	GigabitEthernet0/0/3
10.0.13.0/24	OSPF	10	2		D 10.0.12.1	GigabitEthernet0/0/3
	OSPF	10	2		D 10.0.23.3	GigabitEthernet0/0/4
10.0.23.0/24	Direct	0	0		D 10.0.23.2	GigabitEthernet0/0/4
10.0.23.2/32	Direct	0	0		D 127.0.0.1	GigabitEthernet0/0/4
10.0.23.255/32	Direct	0	0		D 127.0.0.1	GigabitEthernet0/0/4
127.0.0.0/8	Direct	0	0		D 127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0		D 127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0		D 127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0		D 127.0.0.1	InLoopBack0

```
[R3]display ip routing-table
Route Flags: R - relay, D - download to fib
```

Routing Tables: Public

Destinations : 15		Routes : 16				
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
0.0.0.0/0	O_ASE	150	1	D	10.0.13.1	GigabitEthernet0/0/1
10.0.1.1/32	OSPF	10	1	D	10.0.13.1	GigabitEthernet0/0/1
10.0.1.2/32	OSPF	10	1	D	10.0.23.2	GigabitEthernet0/0/3
10.0.1.3/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.12.0/24	OSPF	10	2	D	10.0.23.2	GigabitEthernet0/0/3
	OSPF	10	2	D	10.0.13.1	GigabitEthernet0/0/1
10.0.13.0/24	Direct	0	0	D	10.0.13.3	GigabitEthernet0/0/1
10.0.13.3/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.23.0/24	Direct	0	0	D	10.0.23.3	GigabitEthernet0/0/3
10.0.23.3/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.23.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

R2 и R3 получили маршрут по умолчанию.

Шаг 6 Измените значения стоимости интерфейсов на R1, чтобы LoopBack0 на R1 мог достигать LoopBack0 на R2 через R3.

Согласно таблице маршрутизации R1 стоимость маршрута от маршрутизатора R1 до LoopBack0 маршрутизатора R2 равна 1, а стоимость маршрута от R1 к R2 через R3 равна 2. Следовательно, необходимо только установить для стоимости маршрута от маршрутизатора R1 до LoopBack0 маршрутизатора R2 значение больше 2.

```
[R1]interface GigabitEthernet0/0/3
[R1- GigabitEthernet0/0/3]ospf cost 10
```

Выведите на экран таблицу маршрутизации R1.

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
```

Routing Tables: Public

Destinations : 14		Routes : 14				
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.1.1/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.1.2/32	OSPF	10	2	D	10.0.13.3	GigabitEthernet0/0/1
10.0.1.3/32	OSPF	10	1	D	10.0.13.3	GigabitEthernet0/0/1
10.0.12.0/24	Direct	0	0	D	10.0.12.1	GigabitEthernet0/0/3
10.0.12.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.12.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.13.0/24	Direct	0	0	D	10.0.13.1	GigabitEthernet0/0/1
10.0.13.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.23.0/24	OSPF	10	2	D	10.0.13.3	GigabitEthernet0/0/1
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0


```
255.255.255.255/32 Direct o o D 127.0.0.1 InLoopBacko
```

В этом случае следующим переходом маршрута от R1 до LoopBacko на R2 является GigabitEthernet0/0/1 на R3.

Проверьте результат конфигурирования с помощью команды Tracert.

```
[R1]tracert -a 10.0.1.1 10.0.1.2
```

```
traceroute to 10.0.1.2(10.0.1.2), max hops: 30, packet length: 40, press CTRL_C to break
```

```
1 10.0.13.3 40 ms 50 ms 50 ms
```

```
2 10.0.23.2 60 ms 110 ms 70 ms
```

----Конец

2.2.3 Проверка

1. Проверьте наличие связи между интерфейсами на разных устройствах с помощью инструмента Ping.
2. Отключите интерфейсы, чтобы смоделировать неисправность канала, и проверьте изменения в таблицах маршрутизации.

2.2.4 Справочные конфигурации

Конфигурация на R1

```
#
sysname R1
#
interface GigabitEthernet0/0/1
ip address 10.0.13.1 255.255.255.0
ospf authentication-mode md5 1 cipher %^%#`f*R'6q/RMq(+5*g(sP~SB8oQ49;%7WE:07P7X:W%^%#
#
interface GigabitEthernet0/0/3
ip address 10.0.12.1 255.255.255.0
ospf cost 10
ospf authentication-mode md5 1 cipher %^%#]e)pBf~7Bo.FM~U;bRAVgEs$U>%X;>T\M\tLIYRj2%^%#
#
interface LoopBack0
ip address 10.0.1.1 255.255.255.255
#
ospf 1
default-route-advertise always
area 0.0.0.0
network 10.0.1.1 0.0.0.0
network 10.0.12.0 0.0.0.255
network 10.0.13.0 0.0.0.255
#
return
```

Конфигурация на R2

```
#
sysname R2
#
```

```
interface GigabitEthernet0/0/3
 ip address 10.0.12.2 255.255.255.0
 ospf authentication-mode md5 1 cipher %^%#z+72ZaTk2+v/g7E-AmR"NFYAKC>LZ8~Y`[*Gh=&%^%#
#
interface GigabitEthernet0/0/4
 ip address 10.0.23.2 255.255.255.0
 ospf authentication-mode md5 1 cipher %^%#=@2jEBu!&UYoB*(RDVLC5t~<1B_a-PwC$WH%jQ3%^%#
#
interface LoopBack0
 ip address 10.0.1.2 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.0.1.2 0.0.0.0
  network 10.0.12.2 0.0.0.0
  network 10.0.23.2 0.0.0.0
#
return
```

Конфигурация на R3

```
#
sysname R3
#
interface GigabitEthernet0/0/1
 ip address 10.0.13.3 255.255.255.0
#
interface GigabitEthernet0/0/3
 ip address 10.0.23.3 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.3 255.255.255.255
#
ospf 1
 area 0.0.0.0
  authentication-mode md5 1 cipher %^%#Rl<.SVIn1M>[Gk"v/OeSEW|:o:4*h;b|-d:N"s{>%^%#
  network 10.0.1.3 0.0.0.0
  network 10.0.13.3 0.0.0.0
  network 10.0.23.3 0.0.0.0
#
return
```

2.2.5 Вопросы

1. Какой маршрут будет использоваться на шаге 6 маршрутизатором R2 для возврата пакетов ICMP на маршрутизатор R1? Попробуйте объяснить причину.

3

Создание коммутируемой сети Ethernet

3.1 Лабораторная работа 1. Основы Ethernet и конфигурирование VLAN

3.1.1 Общая информация

3.1.1.1 О лабораторной работе

В сетях Ethernet используется метод доступа к общей среде передачи данных, называемый методом множественного доступа с контролем несущей и обнаружением коллизий (Carrier Sense Multiple Access/Collision Detection, CSMA/CD). При наличии в сети Ethernet большого количества хостов коллизии становятся серьезной проблемой, приводящей к ширококестельным штормам. Это снижает производительность сети или даже может полностью вывести ее из строя. Использование коммутаторов для подключения к локальным сетям (LAN) позволяет сократить число коллизий, но ширококестельная передача по-прежнему может создавать проблемы.

Для подавления ширококестельных штормов используется технология VLAN, которая позволяет разделить физическую локальную сеть (LAN) на несколько виртуальных локальных сетей (VLAN), чтобы ширококестельные домены были меньше. Хосты внутри VLAN могут напрямую взаимодействовать только с хостами той же VLAN. А их связь с хостами в других VLAN реализуется через маршрутизатор.

С помощью этой лабораторной работы вы узнаете, как настроить VLAN на коммутаторах Huawei.

3.1.1.2 Цели

Лабораторная работа помогает получить практические навыки по изучению следующих тем:

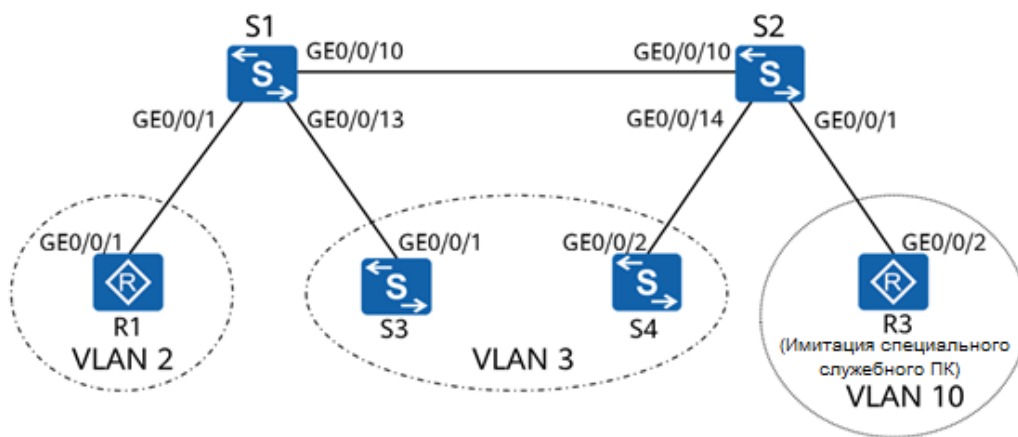
- Создание VLAN
- Конфигурирование портов доступа, магистральных портов и гибридных портов
- Конфигурирование VLAN на основе портов
- Конфигурирование VLAN на основе MAC-адресов
- Просмотр таблицы MAC-адресов и информации о VLAN

3.1.1.3 Топология сети

Компании необходимо разделить сеть уровня 2 на несколько VLAN для удовлетворения служебных требований. Кроме того, VLAN 10 должна обеспечивать более высокий уровень безопасности, поэтому в нее можно добавить только специальные ПК.

Для этого пользовательские порты идентичных служб на S1 и S2 необходимо назначить в одну и ту же VLAN, а порты с определенными MAC-адресами на S2 — в другую VLAN.

Рис. 3-1 Топология сети для конфигурирования VLAN, используемая в данной лабораторной работе



3.1.2 Лабораторная работа

3.1.2.1 План работы

1. Создание VLAN.
2. Конфигурирование VLAN на основе портов.
3. Конфигурирование VLAN на основе MAC-адресов.

3.1.2.2 Процедура конфигурирования

Шаг 1 Настройте имена для S1 и S2 и отключите ненужные порты.

Задайте имена устройств.

Подробности данной операции здесь не приводятся.

Отключите порты GE0/0/11 и GE0/0/12 на S1. Этот шаг можно выполнять только в среде, описанной в *Руководстве по выполнению лабораторных работ для подготовки к сертификации HCIA-Datcom V1.0*.

```
[S1]interface GigabitEthernet 0/0/11
[S1-GigabitEthernet0/0/11]shutdown
[S1-GigabitEthernet0/0/11]quit
[S1]interface GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12]shutdown
[S1-GigabitEthernet0/0/12]quit
```

Отключите порты GE0/0/11 и GE0/0/12 на S2.

```
[S2]interface GigabitEthernet 0/0/11
[S2-GigabitEthernet0/0/11]shutdown
[S2-GigabitEthernet0/0/11]quit
[S2]interface GigabitEthernet 0/0/12
[S2-GigabitEthernet0/0/12]shutdown
[S2-GigabitEthernet0/0/12]quit
```

Шаг 2 Настройте IP-адреса устройств.

Установите для R1 и R3 IP-адреса 10.1.2.1/24 и 10.1.10.1/24 соответственно.

```
[R1]interface GigabitEthernet0/1
[R1-GigabitEthernet0/1]ip address 10.1.2.1 24
```

```
[R3]interface GigabitEthernet0/2
[R3-GigabitEthernet0/2]ip address 10.1.10.1 24
```

Установите для S3 и S4 IP-адреса 10.1.3.1/24 и 10.1.3.2/24 соответственно.
(Сценарий 1: интерфейсы коммутаторов S3 и S4 поддерживают переключение из режима уровня 2 в режим уровня 3.)

```
[S3]interface GigabitEthernet0/1
[S3-GigabitEthernet0/1]undo portswitch
The interface changes to Layer 3 mode.
```

Команда **undo portswitch** позволяет переключать интерфейсы Ethernet из рабочего режима уровня 2 в рабочий режим уровня 3.

```
[S3-GigabitEthernet0/1]ip address 10.1.3.1 24
```

```
[S4]interface GigabitEthernet0/2
[S4-GigabitEthernet0/2]undo portswitch
[S4-GigabitEthernet0/2]ip address 10.1.3.2 24
```

Установите для VLANIF3 на S3 и S4 IP-адреса 10.1.3.1/24 и 10.1.3.2/24 соответственно.
(Сценарий 2: интерфейсы коммутаторов S3 и S4 не поддерживают переключение из режима уровня 2 в режим уровня 3.)

1. Создайте VLAN 3 на S3 и S4.

```
[S3]vlan 3
[S3-vlan3]
```

```
[S4]vlan 3
[S4-vlan3]
```

2. Настройте порты на S3 и S4 в качестве портов доступа и назначьте их в соответствующие VLAN.

```
[S3]interface GigabitEthernet0/1
[S3-GigabitEthernet0/1]port link-type access
[S3-GigabitEthernet0/1]port default vlan 3
[S3-GigabitEthernet0/1]quit
```

```
[S4]interface GigabitEthernet0/0/2
[S4-GigabitEthernet0/0/2]port link-type access
[S4-GigabitEthernet0/0/2]port default vlan 3
[S4-GigabitEthernet0/0/2]quit
```

3. # Создайте интерфейсы VLANIF и настройте IP-адреса.

```
[S3] interface Vlanif 3
```

С помощью команды **interface vlanif *vlan-id*** можно создать интерфейс VLANIF и перейти в режим конфигурирования интерфейса VLANIF.

```
[S3-Vlanif3]ip address 10.1.3.1 24
```

```
[S4] interface Vlanif 3
[S4-Vlanif3]ip address 10.1.3.2 24
```

Шаг 3 Создайте VLAN.

Создайте VLAN 2, 3 и 10 на S1 и S2.

```
[S1]vlan batch 2 to 3 10
Info: This operation may take a few seconds. Please wait for a moment...done.
VLANs 2, 3, and 10 are created successfully.
```

С помощью команды **vlan *vlan-id*** можно создать VLAN и перейти в режим конфигурирования VLAN. Если VLAN существуют, то режим VLAN отобразится на экране.

Команда **vlan batch { *vlan-id1* [to *vlan-id2*] }** позволяет создавать сразу несколько VLAN.

```
[S2]vlan batch 2 to 3 10
```

Шаг 4 Настройте сети VLAN на основе портов.

Настройте пользовательские порты на S3 и S4 в качестве портов доступа и назначьте их в соответствующие VLAN.

```
[S1]interface GigabitEthernet0/0/1
[S1-GigabitEthernet0/0/1]port link-type access
```

С помощью команды **port link-type { access | hybrid | trunk }** можно задать тип интерфейса, который может быть Access, Trunk или Hybrid.

```
[S1-GigabitEthernet0/0/1]port default vlan 2
```

Команда **port default vlan *vlan-id*** позволяет настроить VLAN по умолчанию для интерфейса и назначить интерфейс в эту VLAN.

```
[S1-GigabitEthernet0/0/1]quit
[S1]interface GigabitEthernet0/0/13
[S1-GigabitEthernet0/0/13]port link-type access
[S1-GigabitEthernet0/0/13]port default vlan 3
[S1-GigabitEthernet0/0/13]quit
[S2]interface GigabitEthernet0/0/14
```

```
[S2-GigabitEthernet0/0/14]port link-type access  
[S2-GigabitEthernet0/0/14]port default vlan 3  
[S2-GigabitEthernet0/0/14]quit
```

Настройте порты, соединяющие S1 и S2, в качестве магистральных портов и разрешите прохождение только пакетов из VLAN 2 и VLAN 3.

```
[S1]interface GigabitEthernet0/0/10  
[S1-GigabitEthernet0/0/10]port link-type trunk  
[S1-GigabitEthernet0/0/10]port trunk allow-pass vlan 2 3
```

Команда **port trunk allow-pass vlan** позволяет назначить магистральный порт в определенные сети VLAN.

```
[S1-GigabitEthernet0/0/10]undo port trunk allow-pass vlan 1
```

Команда **undo port trunk allow-pass vlan** позволяет удалить магистральный порт из определенных сетей VLAN.

По умолчанию VLAN 1 находится в списке разрешенных сетей. Если VLAN 1 не используется какой-либо службой, ее необходимо удалить в целях безопасности.

```
[S2]interface GigabitEthernet0/0/10  
[S2-GigabitEthernet0/0/10]port link-type trunk  
[S2-GigabitEthernet0/0/10]port trunk allow-pass vlan 2 3  
[S2-GigabitEthernet0/0/10]undo port trunk allow-pass vlan 1
```

Шаг 5 Сконфигурируйте сети VLAN на основе MAC-адресов.

Как показано на схеме сети, R3 имитирует специальный служебный ПК. Допустим, что данный ПК имеет MAC-адрес a008-6fe1-0c46. Предполагается, что ПК будет подключаться к сети через любой из портов GigabitEthernet0/0/1, GigabitEthernet0/0/2 и GigabitEthernet0/0/3 на S2 и передавать данные через VLAN 10.

Настройте на S2 привязку MAC-адреса ПК к VLAN 10.

Принадлежность к VLAN зависит от исходных MAC-адресов пакетов, и соответственно добавляются теги VLAN. Этот метод назначения VLAN не зависит от местоположения, обеспечивая более высокий уровень безопасности и гибкости.

```
[S2] vlan 10  
[S2-vlan10] mac-vlan mac-address a008-6fe1-0c46
```

Команда **mac-vlan mac-address** позволяет установить привязку MAC-адреса к VLAN.

Настройте GigabitEthernet0/0/1, GigabitEthernet0/0/2 и GigabitEthernet0/0/3 на S2 в качестве гибридных портов и разрешите прохождение пакетов из VLAN на основе MAC-адресов.

На портах доступа и магистральных портах назначение VLAN на основе MAC-адресов можно использовать только в том случае, если VLAN соответствует PVID. Поэтому рекомендуется настроить назначение VLAN на основе MAC-адресов на гибридном порте для получения из нескольких VLAN нетегированных пакетов.

```
[S2]interface GigabitEthernet0/0/1  
[S2-GigabitEthernet0/0/1]port link-type hybrid  
[S2-GigabitEthernet0/0/1]port hybrid untagged vlan 10
```

Команда **port hybrid untagged vlan** позволяет назначить гибридный порт в определенные сети VLAN, чтобы передавать нетегированные кадры.

```
[S2-GigabitEthernet0/0/1]quit
[S2]interface GigabitEthernet0/0/2
[S2-GigabitEthernet0/0/2]port link-type hybrid
[S2-GigabitEthernet0/0/2]port hybrid untagged vlan 10
[S2-GigabitEthernet0/0/2]quit
[S2]interface GigabitEthernet0/0/3
[S2-GigabitEthernet0/0/3]port link-type hybrid
[S2-GigabitEthernet0/0/3]port hybrid untagged vlan 10
[S2-GigabitEthernet0/0/3]quit
```

Настройте на портах, соединяющих S1 и S2, разрешение на прохождение пакетов из VLAN 10.

Порты должны разрешать прохождение тегированных кадров из нескольких VLAN. Следовательно, порты можно настроить в качестве магистральных портов.

```
[S1]interface GigabitEthernet0/0/10
[S1-GigabitEthernet0/0/10]port trunk allow-pass vlan 10
[S1-GigabitEthernet0/0/10]quit
```

```
[S2]interface GigabitEthernet0/0/10
[S2-GigabitEthernet0/0/10]port trunk allow-pass vlan 10
[S2-GigabitEthernet0/0/10]quit
```

Настройте S2 и включите назначение VLAN на основе MAC-адресов на GE0/0/1, GE0/0/2 и GE0/0/3.

Чтобы включить на порте передачу пакетов на основе привязки между MAC-адресом и VLAN, необходимо выполнить команду **mac-vlan enable**.

```
[S2]interface GigabitEthernet0/0/1
[S2-GigabitEthernet0/0/1]mac-vlan enable
```

Команда **mac-vlan enable** позволяет включить функцию назначения VLAN на основе MAC-адреса для порта.

```
[S2-GigabitEthernet0/0/1]quit
[S2]interface GigabitEthernet0/0/2
[S2-GigabitEthernet0/0/2]mac-vlan enable
[S2-GigabitEthernet0/0/2]quit
[S2]interface GigabitEthernet0/0/3
[S2-GigabitEthernet0/0/3]mac-vlan enable
[S2-GigabitEthernet0/0/3]quit
```

Шаг 6 Выведите на экран информацию о конфигурации.

Выведите на экран информацию о VLAN на коммутаторе.

```
[S1]display vlan
```

Команда **display vlan** позволяет вывести на экран информацию о сетях VLAN.

С помощью команды **display vlan verbose** можно вывести на экран подробную информацию определенной VLAN, включая идентификатор, тип, описание и



состояние VLAN, состояние функции статистики трафика, порты VLAN и режим, в котором осуществляется назначение портов в VLAN.

The total number of vlans is : 4

U: Up; D: Down; TG: Tagged; UT: Untagged;
MP: Vlan-mapping; ST: Vlan-stacking;
#: ProtocolTransparent-vlan; *: Management-vlan;

VID	Type	Ports
1	common	UT: GE0/0/2(D) GE0/0/3(D) GE0/0/4(D) GE0/0/5(D) GE0/0/6(D) GE0/0/7(D) GE0/0/8(D) GE0/0/9(D) GE0/0/11(D) GE0/0/12(D) GE0/0/14(D) GE0/0/15(D) GE0/0/16(D) GE0/0/17(D) GE0/0/18(D) GE0/0/19(D) GE0/0/20(D) GE0/0/21(D) GE0/0/22(D) GE0/0/23(D) GE0/0/24(D)
2	common	UT: GE0/0/1(U) TG: GE0/0/10(U)
3	common	UT: GE0/0/13(U) TG: GE0/0/10(U)
10	common	TG: GE0/0/10(U)

VID	Status	Property	MAC-LRN Statistics		Description
1	enable	default	enable	disable	VLAN 0001
2	enable	default	enable	disable	VLAN 0002
3	enable	default	enable	disable	VLAN 0003
10	enable	default	enable	disable	VLAN 0010

[S2]display vlan

The total number of vlans is : 4

U: Up; D: Down; TG: Tagged; UT: Untagged;
MP: Vlan-mapping; ST: Vlan-stacking;
#: ProtocolTransparent-vlan; *: Management-vlan;

VID	Type	Ports
1	common	UT: GE0/0/1(U) GE0/0/2(D) GE0/0/3(D) GE0/0/4(D) GE0/0/5(D) GE0/0/6(D) GE0/0/7(D) GE0/0/8(D) GE0/0/9(D) GE0/0/11(D) GE0/0/12(D) GE0/0/13(D) GE0/0/15(D) GE0/0/16(D) GE0/0/17(D) GE0/0/18(D) GE0/0/19(D) GE0/0/20(D) GE0/0/21(D) GE0/0/22(D) GE0/0/23(D) GE0/0/24(D)
2	common	TG: GE0/0/10(U)
3	common	UT: GE0/0/14(U) TG: GE0/0/10(U)
10	common	UT: GE0/0/1(U) GE0/0/2(D) GE0/0/3(D) TG: GE0/0/10(U)

VID	Status	Property	MAC-LRN Statistics		Description
-----	--------	----------	--------------------	--	-------------

```
-----
1   enable  default      enable  disable  VLAN 0001
2   enable  default      enable  disable  VLAN 0002
3   enable  default      enable  disable  VLAN 0003
10  enable  default      enable  disable  VLAN 0010
-----
```

Выведите на экран конфигурацию назначения VLAN на основе MAC-адресов, имеющуюся на коммутаторе.

```
[S2]display mac-vlan vlan 10
```

```
-----
MAC Address      MASK                VLAN    Priority
-----
00e0-fc1c-47a7   ffff-ffff-ffff     10      0
-----
```

```
Total MAC VLAN address count: 1
```

Команда **display mac-vlan** позволяет вывести на экран конфигурацию назначения VLAN на основе MAC-адресов.

3.1.3 Проверка

Проверьте подключение устройства и конфигурацию VLAN.

1. Выполните команду Ping на S4 для проверки связи с S3 и убедитесь, что операция ping успешно выполняется.
2. Выполните команду Ping на R1 для проверки связи с другими устройствами и убедитесь, что операция ping не выполняется.
3. Выполните команду **display mac-address verbose** на S1 и S2, чтобы проверить таблицы MAC-адресов на коммутаторах.

3.1.4 Справочные конфигурации

Конфигурация на S1

```
#
sysname S1
#
vlan batch 2 to 3 10
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/10
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2 to 3 10
#
interface GigabitEthernet0/0/11
 shutdown
#
interface GigabitEthernet0/0/12
 shutdown
#
```

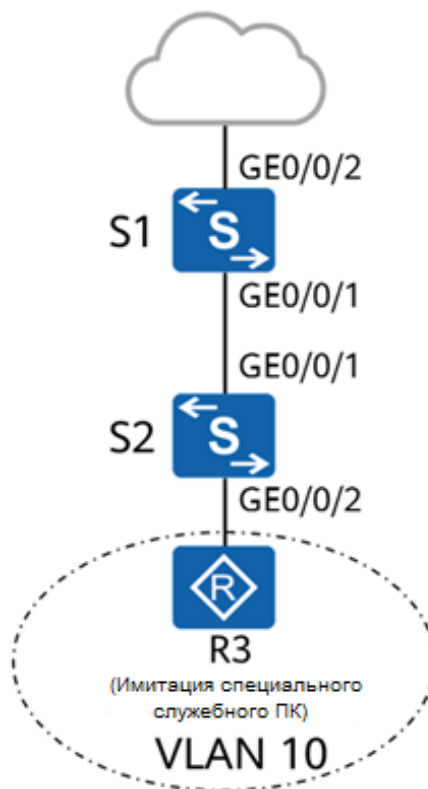
```
interface GigabitEthernet0/0/13
port link-type access
port default vlan 3
#
return
```

Конфигурация на S2

```
#
sysname S2
#
vlan batch 2 to 3 10
#
vlan 10
mac-vlan mac-address a008-6fe1-0c46 priority 0
#
interface GigabitEthernet0/0/1
port link-type hybrid
port hybrid untagged vlan 10
mac-vlan enable
#
interface GigabitEthernet0/0/2
port link-type hybrid
port hybrid untagged vlan 10
mac-vlan enable
#
interface GigabitEthernet0/0/3
port link-type hybrid
port hybrid untagged vlan 10
mac-vlan enable
#
interface GigabitEthernet0/0/10
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 2 to 3 10
#
interface GigabitEthernet0/0/11
shutdown
#
interface GigabitEthernet0/0/12
shutdown
#
interface GigabitEthernet0/0/14
port link-type access
port default vlan 3
#
return
```

3.1.5 Вопросы

1. Как показано на следующем рисунке, для обеспечения информационной безопасности определенной услуги только специальные ПК могут получить доступ к сети через VLAN 10. Как это требование можно реализовать на S1?



3.2 Лабораторная работа 2. Протокол связующего дерева (STP)

3.2.1 Общая информация

3.2.1.1 О лабораторной работе

В коммутируемой сети Ethernet для реализации резервирования путей связи и повышения сетевой доступности используются резервные каналы. Однако серьезным недостатком их применения является образование петель, которые могут вызывать широковещательные шторма, нестабильность таблицы MAC-адресов, ухудшение или даже прерывание связи. Чтобы предотвратить образование петель, ассоциация IEEE разработала протокол связующего дерева (Spanning Tree Protocol, STP).

STP, определенный в стандарте IEEE 802.1D, был усовершенствован до протокола быстрого связующего дерева (Rapid Spanning Tree Protocol, RSTP), определенного в стандарте IEEE 802.1W, и протокола множественного связующего дерева (Multiple Spanning Tree Protocol, MSTP), определенного в стандарте IEEE 802.1S.

С помощью этой лабораторной работы вы узнаете базовую конфигурацию STP, поймете принципы и некоторые особенности RSTP.

3.2.1.2 Цели

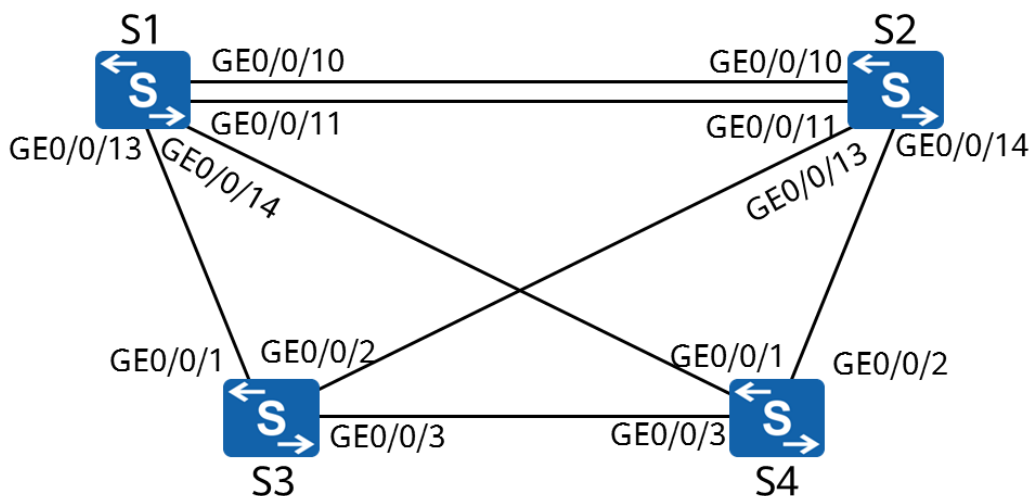
Лабораторная работа помогает получить практические навыки по изучению следующих тем:

- Включение и отключение STP/RSTP.
- Процедура изменения режима STP коммутатора.
- Процедура изменения приоритетов мостов для управления выбором корневого моста.
- Процедура изменения приоритетов портов для управления выбором корневого порта и назначенного порта.
- Процедура изменения стоимости портов для управления выбором корневого порта и назначенного порта.
- Процедура настройки граничных портов.
- Включение и отключение RSTP.

3.2.1.3 Топология сети

В целях повышения сетевой доступности, компании необходимо создать резервные каналы в своей коммутируемой сети уровня 2. Кроме того, необходимо развернуть протокол STP, чтобы предотвратить образование петель на резервных каналах, вызывающих широковещательный шторм и нестабильность MAC-адресов.

Рис. 3-2 Топология сети для конфигурирования STP, используемая в данной лабораторной работе



3.2.2 Лабораторная работа

3.2.2.1 План работы

1. Включение STP.
2. Изменение приоритетов мостов, чтобы контролировать выбор корневого моста.
3. Изменение параметров порта, чтобы определить роль порта.
4. Изменение протокола на протокол RSTP.
5. Настройка граничных портов.

3.2.2.2 Процедура конфигурирования

Шаг 1 Отключите ненужные порты. Этот шаг можно выполнять только в среде, описанной в *Руководстве по выполнению лабораторных работ для подготовки к сертификации HCIA-Datcom V1.0*.

Отключите порт GigabitEthernet0/0/12 между S1 и S2.

```
[S1]interface GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12]shutdown
```

```
[S2]interface GigabitEthernet 0/0/12
[S2-GigabitEthernet0/0/12]shutdown
```

Шаг 2 Включите STP.

Включите STP глобально.

```
<S1>system-view
Enter system view, return user view with Ctrl+Z.
[S1]stp enable
```

Команда **stp enable** позволяет включить протокол STP, RSTP или MSTP на коммутационном устройстве или порте. По умолчанию на коммутаторах включен протокол STP, RSTP или MSTP.

Измените режим связующего дерева на STP.

```
[S1]stp mode stp
Info: This operation may take a few seconds. Please wait for a moment...done.
```

С помощью команды **stp mode{mstp | rstp | stp}** можно установить режим работы протокола связующего дерева на коммутационном устройстве. По умолчанию коммутационное устройство работает в режиме MSTP. Режим связующего дерева текущего устройства был изменен на STP.

```
[S2]stp mode stp
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```
[S3]stp mode stp
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```
[S4]stp mode stp
Info: This operation may take a few seconds. Please wait for a moment...done.
```

Выведите на экран статус связующего дерева. В данном случае для примера используется S1.

```
[S1]display stp
-----[CIST Global Info][Mode STP]-----
CIST Bridge           :32768.4c1f-cc33-7359           //Идентификатор моста устройства.
Config Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC        :32768.4c1f-cc10-5913 / 20000     //Идентификатор и стоимость маршрута
текущего корневого моста.
CIST RegRoot/IRPC     :32768.4c1f-cc33-7359 / 0
CIST RootPortId       :128.14
BPDU-Protection       :Disabled
TC or TCN received    :47
TC count per hello    :0
STP Converge Mode     :Normal
Time since last TC    :0 days 0h:0m:38s
Number of TC          :15
Last TC occurred      :GigabitEthernet0/0/14
```

Выведенная информация также включает данные состояния порта, которые не были включены в предыдущий командный вывод.

Выведите на экран краткую информацию о связующем дереве на каждом коммутаторе.

```
[S1]display stp brief
```

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/10	DESI	FORWARDING	NONE
0	GigabitEthernet0/0/11	DESI	FORWARDING	NONE
0	GigabitEthernet0/0/13	DESI	FORWARDING	NONE

o	GigabitEthernet0/0/14	ROOT	FORWARDING	NONE
---	-----------------------	------	------------	------

[S2]display stp brief

MSTID	Port	Role	STP State	Protection
o	GigabitEthernet0/0/10	ALTE	DISCARDING	NONE
o	GigabitEthernet0/0/11	ALTE	DISCARDING	NONE
o	GigabitEthernet0/0/13	DESI	FORWARDING	NONE
o	GigabitEthernet0/0/14	ROOT	FORWARDING	NONE

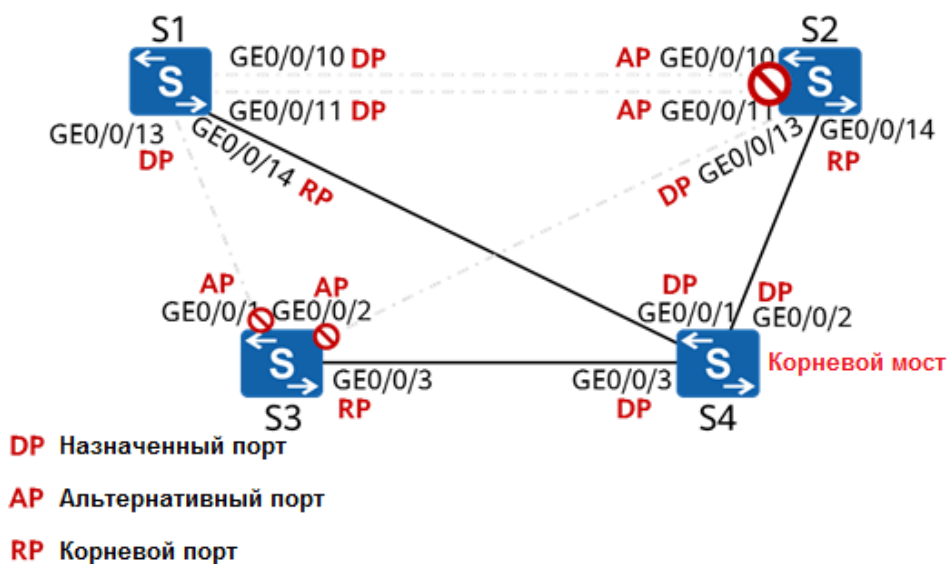
[S3]display stp brief

MSTID	Port	Role	STP State	Protection
o	GigabitEthernet0/0/1	ALTE	DISCARDING	NONE
o	GigabitEthernet0/0/2	ALTE	DISCARDING	NONE
o	GigabitEthernet0/0/3	ROOT	FORWARDING	NONE

[S4]display stp brief

MSTID	Port	Role	STP State	Protection
o	GigabitEthernet0/0/1	DESI	FORWARDING	NONE
o	GigabitEthernet0/0/2	DESI	FORWARDING	NONE
o	GigabitEthernet0/0/3	DESI	FORWARDING	NONE

На основании идентификатора корневого моста и информации о порте каждого коммутатора текущая топология выглядит следующим образом:



Пунктирной линией показаны каналы, которые не передают служебные данные.

ПРИМЕЧАНИЕ

Данная топология приводится исключительно в справочных целях, поэтому может не совпадать с фактической топологией связующего дерева в лабораторной среде.

Шаг 3 Измените параметры устройства, чтобы сделать S1 корневым мостом, а S2 — резервным корневым мостом.

Измените приоритеты мостов S1 и S2.

```
[S1]stp root primary
```

Так как корневой мост играет очень важную роль в сети, то в качестве него обычно выбирается коммутатор с высокой производительностью и высоким уровнем сетевой иерархии. Однако такое устройство может иметь невысокий приоритет. Поэтому необходимо установить коммутатору высокий приоритет, чтобы он мог быть выбран в качестве корневого моста. С помощью команды **stp root** можно настроить коммутатор в качестве корневого моста или резервного корневого моста связующего дерева.

- Команда **stp root primary** позволяет задать коммутатор в качестве корневого коммутационного устройства. В этом случае коммутатор получит приоритет в связующем дереве, равный 0, и его нельзя будет изменить.
- Команда **stp root secondary** позволяет задать коммутатор в качестве резервного корневого моста. В этом случае коммутатор получит приоритет, равный 4096, и его нельзя будет изменить.

```
[S2]stp root secondary
```

Выведите на экран статус STP на S1.

```
[S1]display stp
```

```
-----[CIST Global Info][Mode STP]-----
```

```
CIST Bridge           :0       .4c1f-cc33-7359           //Идентификатор моста устройства.
Config Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC        :0       .4c1f-cc33-7359 / 0       //Идентификатор и стоимость маршрута текущего
корневого моста.
CIST RegRoot/IRPC     :0       .4c1f-cc33-7359 / 0
CIST RootPortId       :0.0
BPDU-Protection       :Disabled
CIST Root Type        :Primary root
TC or TCN received    :84
TC count per hello    :0
STP Converge Mode     :Normal
Time since last TC    :0 days 0h:1m:44s
Number of TC          :21
Last TC occurred      :GigabitEthernet0/0/10
```

В этом случае идентификатор моста S1 совпадает с идентификатором корневого моста, а стоимость корневого маршрута равна 0, что указывает на то, что S1 является корневым мостом текущей сети.

Выведите на экран краткую информацию о статусе STP на всех устройствах.

```
[S1]display stp brief
```

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/10	DES1	FORWARDING	NONE
0	GigabitEthernet0/0/11	DES1	FORWARDING	NONE
0	GigabitEthernet0/0/13	DES1	FORWARDING	NONE
0	GigabitEthernet0/0/14	DES1	FORWARDING	NONE

```
[S2]display stp brief
```

MSTID	Port	Role	STP State	Protection
-------	------	------	-----------	------------

o	GigabitEthernet0/0/10	ROOT	FORWARDING	NONE
o	GigabitEthernet0/0/11	ALTE	DISCARDING	NONE
o	GigabitEthernet0/0/13	DESI	FORWARDING	NONE
o	GigabitEthernet0/0/14	DESI	FORWARDING	NONE

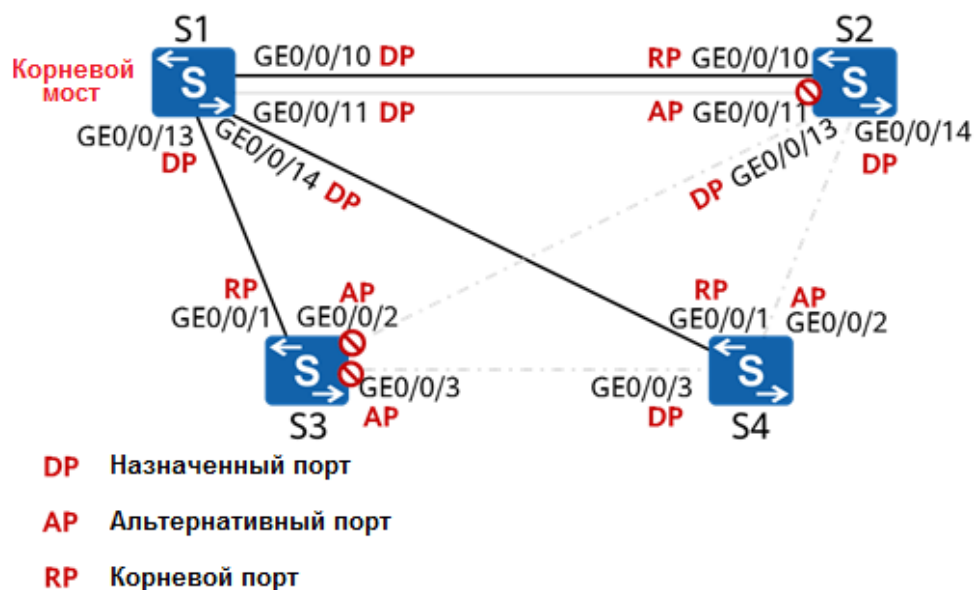
[S3]display stp brief

MSTID	Port	Role	STP State	Protection
o	GigabitEthernet0/0/1	ROOT	FORWARDING	NONE
o	GigabitEthernet0/0/2	ALTE	DISCARDING	NONE
o	GigabitEthernet0/0/3	ALTE	DISCARDING	NONE

[S4]display stp brief

MSTID	Port	Role	STP State	Protection
o	GigabitEthernet0/0/1	ROOT	FORWARDING	NONE
o	GigabitEthernet0/0/2	ALTE	DISCARDING	NONE
o	GigabitEthernet0/0/3	DESI	FORWARDING	NONE

На основании идентификатора корневого моста и информации о порте каждого коммутатора текущая топология выглядит следующим образом:



Шаг 4 Измените параметры устройства, чтобы назначить порт GigabitEthernet0/0/2 коммутатора S4 корневым портом.

Выведите на экран информацию STP на S4.

[S4]display stp

-----[CIST Global Info][Mode STP]-----

```
CIST Bridge           :32768.4c1f-cc10-5913
Config Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC        :o .4c1f-cc33-7359 / 20000
CIST RegRoot/IRPC     :32768.4c1f-cc10-5913 / o
CIST RootPortId       :128.1
BPDU-Protection       :Disabled
```

```
TC or TCN received      :93
TC count per hello      :0
STP Converge Mode       :Normal
Time since last TC      :0 days 0h:9m:55
Number of TC            :18
Last TC occurred        :GigabitEthernet0/0/1
```

Стоимость корневого маршрута от S4 до S1 имеет значение 20000.

Измените стоимость STP порта GigabitEthernet 0/0/1 коммутатора S4 на 50000.

```
[S4]interface GigabitEthernet 0/0/1
[S4-GigabitEthernet0/0/1]stp cost 50000
```

Выведите на экран краткую информацию о статусе STP.

```
[S4]display stp brief
```

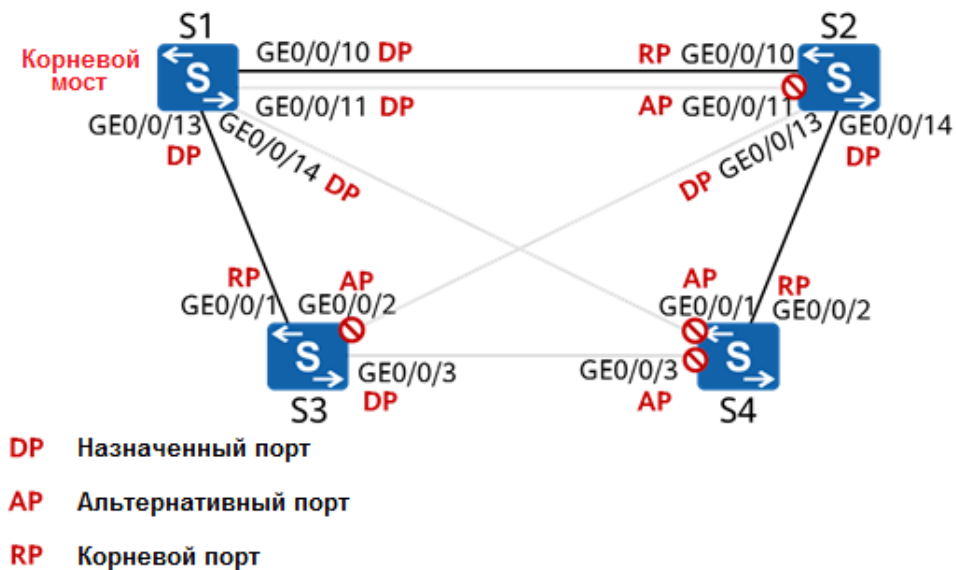
MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/1	ALTE	DISCARDING	NONE
0	GigabitEthernet0/0/2	ROOT	FORWARDING	NONE
0	GigabitEthernet0/0/3	ALTE	DISCARDING	NONE

Порт GigabitEthernet0/0/2 на S4 стал корневым портом.

Выведите на экран информацию о текущем статусе STP.

```
[S4]display stp
-----[CIST Global Info][Mode STP]-----
CIST Bridge          :32768.4c1f-cc10-5913
Config Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :0 .4c1f-cc33-7359 / 40000 //Стоимость корневого маршрута = 20000 + 20000 = 40000
CIST RegRoot/IRPC    :32768.4c1f-cc10-5913 / 0
CIST RootPortId      :128.2
BPDU-Protection      :Disabled
TC or TCN received   :146
TC count per hello    :0
STP Converge Mode     :Normal
Time since last TC    :0 days 0h:2m:25s
Number of TC         :20
Last TC occurred      :GigabitEthernet0/0/2
```

Текущая топология выглядит следующим образом:



Шаг 5 Измените режим связующего дерева на RSTP.

Измените режим связующего дерева на всех устройствах.

```
[S1]stp mode rstp
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S2]stp mode rstp
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S3]stp mode rstp
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S4]stp mode rstp
```

Info: This operation may take a few seconds. Please wait for a moment...done.

Выведите на экран статус связующего дерева. В данном случае для примера используется S1.

```
[S1]display stp
```

```
-----[CIST Global Info][Mode RSTP]-----
```

```
CIST Bridge           :0       .4c1f-cc33-7359
Config Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC        :0       .4c1f-cc33-7359 / 0
CIST RegRoot/IRPC     :0       .4c1f-cc33-7359 / 0
CIST RootPortId       :0.0
BPDU-Protection       :Disabled
CIST Root Type        :Primary root
TC or TCN received    :89
```

```
TC count per hello      :0
STP Converge Mode      :Normal
Time since last TC     :0 days 0h:0m:44s
Number of TC           :27
Last TC occurred       :GigabitEthernet0/0/11
```

После изменения режима топология связующего дерева не изменилась.

Шаг 6 Настройте граничные порты.

Порты GigabitEthernet 0/0/10-0/0/24 коммутатора S3 подключены только к терминалам, поэтому их необходимо настроить в качестве граничных портов.

```
[S3]interface range GigabitEthernet 0/0/10 to GigabitEthernet 0/0/24
```

Устройство предоставляет несколько портов Ethernet, многие из которых имеют одинаковую конфигурацию. Настраивать их по очереди утомительно и чревато возможными ошибками. Самый простой способ — добавить эти порты в группу портов и выполнить настройку всей группы сразу. Система автоматически выполнит команды на всех портах в группе.

ПРИМЕЧАНИЕ

Эта функция может быть недоступна для некоторых продуктов.

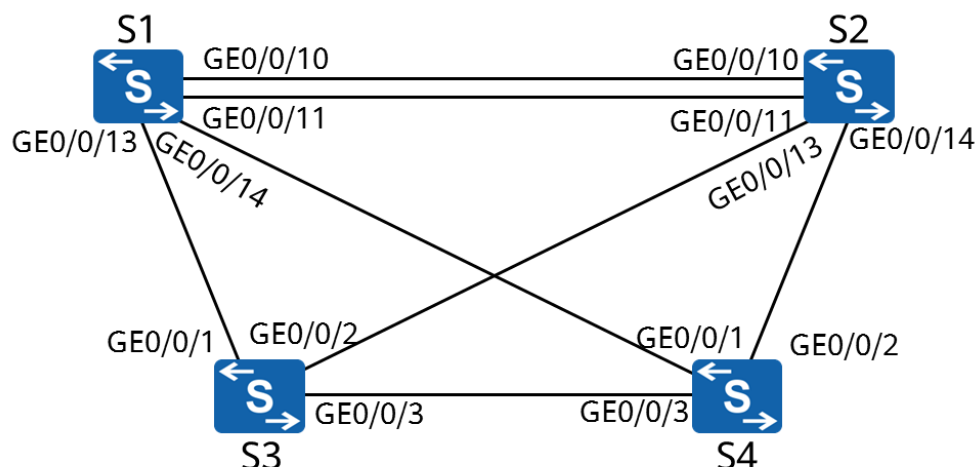
```
[S3-port-group]stp edged-port enable
```

Команда **stp edged-port enable** позволяет задать текущий порт в качестве граничного порта. Если после настройки граничный порт коммутационного устройства получает BPDU, коммутационное устройство автоматически отменяет настройки порта в качестве граничного порта и пересчитывает связующее дерево.

----Конец

3.2.3 Проверка

1. Отметьте корневой мост и роль каждого порта в лабораторной среде на основании фактической конвергенции сети.



2. Отключите какой-нибудь порт на любом коммутаторе и проверьте, может ли трафик передаваться на другие коммутаторы по резервным каналам.

3.2.4 Справочные конфигурации

Конфигурация на S1

```
#
sysname S1
#
stp mode rstp
stp instance 0 root primary
#
interface GigabitEthernet0/0/12
 shutdown
#
return
```

Конфигурация на S2

```
#
sysname S2
#
stp mode rstp
stp instance 0 root secondary
#
interface GigabitEthernet0/0/12
 shutdown
#
return
```

Конфигурация на S3

```
#
sysname S3
#
stp mode rstp
#
interface GigabitEthernet0/0/10
 stp edged-port enable
#
interface GigabitEthernet0/0/11
 stp edged-port enable
#
interface GigabitEthernet0/0/12
 stp edged-port enable
#
interface GigabitEthernet0/0/13
 stp edged-port enable
#
interface GigabitEthernet0/0/14
 stp edged-port enable
#
interface GigabitEthernet0/0/15
 stp edged-port enable
#
```

```
interface GigabitEthernet0/0/16
 stp edged-port enable
#
interface GigabitEthernet0/0/17
 stp edged-port enable
#
interface GigabitEthernet0/0/18
 stp edged-port enable
#
interface GigabitEthernet0/0/19
 stp edged-port enable
#
interface GigabitEthernet0/0/20
 stp edged-port enable
#
interface GigabitEthernet0/0/21
 stp edged-port enable
#
interface GigabitEthernet0/0/22
 stp edged-port enable
#
interface GigabitEthernet0/0/23
 stp edged-port enable
#
interface GigabitEthernet0/0/24
 stp edged-port enable
#
return
```

Конфигурация на S4

```
#
sysname S4
#
stp mode rstp
#
interface GigabitEthernet0/0/1
 stp instance 0 cost 5000
#
return
```

3.2.5 Вопросы

1. Можно ли будет достичь желаемого результата, если на шаге 3 изменить стоимость GigabitEthernet 0/0/14 коммутатора S1 на 50000? Почему?
2. Как необходимо изменить конфигурацию в текущей топологии, чтобы назначить порт GigabitEthernet0/0/11 коммутатора S2 корневым портом?
3. Могут ли два канала между S1 и S2 одновременно находиться в режиме передачи данных? Почему?

3.3 Лабораторная работа 3. Агрегирование каналов Ethernet

3.3.1 Общая информация

3.3.1.1 О лабораторной работе

В условиях постоянно растущего числа пользователей обеспечить более высокую пропускную способность и доступность могут только магистральные сети Ethernet. Еще недавно единственным способом увеличения пропускной способности считалась модернизация сети с помощью высокоскоростных LPU. Однако этот способ был дорогостоящим и не отличался гибкостью.

В отличие от него, технология агрегирования каналов позволяет увеличить полосу пропускания за счет объединения группы физических портов в один логический порт и не требует модернизации оборудования. Кроме того, данная технология реализует механизмы резервирования каналов, что значительно повышает их доступность. Агрегирование каналов имеет следующие преимущества:

- Повышение пропускной способности: максимальная пропускная способность группы агрегирования каналов (Link Aggregation Group, LAG) — совокупная пропускная способность всех каналов-участников группы.
- Повышение доступности: при неисправности одного канала трафик можно переключить на другие доступные каналы-участники.
- Балансировка нагрузки: нагрузка трафика распределяется между активными каналами-участниками в группе LAG.

С помощью этой лабораторной работы вы узнаете, как настроить агрегирование каналов Ethernet вручную и в режиме LACP.

3.3.1.2 Цели

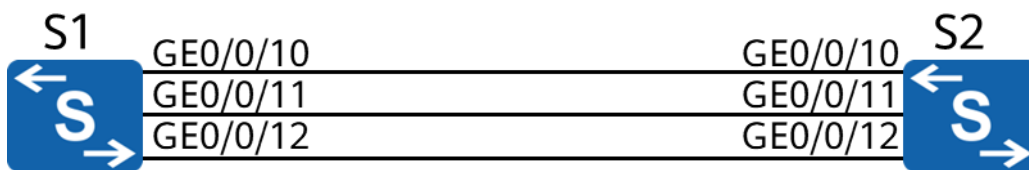
Лабораторная работа помогает получить практические навыки по изучению следующих тем:

- Ручная настройка агрегирования каналов.
- Настройка агрегирования каналов в статическом режиме LACP.
- Определение активных каналов в статическом режиме LACP.
- Настройка некоторых функций статического режима LACP.

3.3.1.3 Топология сети

В лабораторной работе на тему протокола связующего дерева два канала между S1 и S2 не могли одновременно находиться в состоянии передачи данных. Для полноценного использования полосы пропускания двух каналов между S1 и S2 необходимо настроить агрегирование каналов Ethernet.

Рис. 3-3 Топология сети для настройки агрегирования каналов Ethernet, используемая в данной лабораторной работе



3.3.2 Лабораторная работа

3.3.2.1 План работы

1. Настройка агрегирования каналов вручную.
2. Настройка агрегирования каналов в режиме LACP.
3. Изменение параметров для определения активных каналов.
4. Изменение режима балансировки нагрузки.

3.3.2.2 Процедура конфигурирования

Шаг 1 Настройте агрегирование каналов вручную.

Создайте Eth-Trunk.

```
[S1]interface Eth-Trunk 1
```

Команда **interface eth-trunk** позволяет перейти в режим существующего Eth-Trunk или создать Eth-Trunk и перейти в его режим. Цифра **1**, используемая в примере, означает номер порта.

```
[S2]interface Eth-Trunk 1
```

Сконфигурируйте режим агрегирования каналов для Eth-Trunk.

```
[S1-Eth-Trunk1]mode manual load-balance
```

Команда **mode** позволяет настроить рабочий режим Eth-Trunk, который может быть LACP или ручная балансировка нагрузки. По умолчанию используется режим ручной балансировки нагрузки. Таким образом, предыдущую операцию выполнять не требуется, она приводится только для наглядности.

Добавьте порт в Eth-Trunk.

```
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]eth-trunk 1
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1-GigabitEthernet0/0/10]quit
[S1]interface GigabitEthernet 0/0/11
[S1-GigabitEthernet0/0/11]eth-trunk 1
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1-GigabitEthernet0/0/11]quit
[S1]interface GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12]eth-trunk 1
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```
[S1-GigabitEthernet0/0/12]quit
```

Для добавления определенного порта в Eth-Trunk можно перейти в режим его интерфейса и выполнить операцию. Для добавления нескольких портов в Eth-Trunk можно выполнить команду **trunkport** в режиме интерфейса Eth-Trunk.

```
[S2]interface Eth-Trunk 1
```

```
[S2-Eth-Trunk1]trunkport GigabitEthernet 0/0/10 to 0/0/12
```

```
Info: This operation may take a few seconds. Please wait for a moment...done.
```

При добавлении физических портов в Eth-Trunk необходимо учитывать следующие нюансы:

- Агрегированный канал Eth-Trunk может содержать максимум 8 портов-участников.
- Eth-Trunk нельзя добавить к другому Eth-Trunk.
- Порт Ethernet можно добавить только к одному Eth-Trunk. Чтобы добавить порт Ethernet к другому Eth-Trunk, сначала необходимо удалить его из исходного.
- Дистанционные порты, напрямую подключенные к локальным портам-участникам Eth-Trunk, также должны быть добавлены в Eth-Trunk; в противном случае два конца не смогут взаимодействовать.
- Такие параметры, как количество физических портов, скорость порта и дуплексный режим, должны совпадать на обоих концах канала Eth-Trunk.

Выведите на экран статус Eth-Trunk.

```
[S1]display eth-trunk 1
```

```
Eth-Trunk1's state information is:
```

```
WorkingMode: NORMAL
```

```
Hash arithmetic: According to SIP-XOR-DIP
```

```
Least Active-linknumber: 1
```

```
Max Bandwidth-affected-linknumber: 32
```

```
Operate status: up
```

```
Number Of Up Port In Trunk: 3
```

PortName	Status	Weight
GigabitEthernet0/0/10	Up	1
GigabitEthernet0/0/11	Up	1
GigabitEthernet0/0/12	Up	1

Шаг 2 Настройте агрегирование каналов в режиме LACP.

Удалите порты-участники из Eth-Trunk.

```
[S1]interface Eth-Trunk 1
```

```
[S1-Eth-Trunk1]undo trunkport GigabitEthernet 0/0/10 to 0/0/12
```

```
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```
[S2]interface Eth-Trunk 1
```

```
[S2-Eth-Trunk1]undo trunkport GigabitEthernet 0/0/10 to 0/0/12
```

```
Info: This operation may take a few seconds. Please wait for a moment...done.
```

Перед изменением режима работы Eth-Trunk убедитесь, что в Eth-Trunk нет портов-участников.

Измените режим агрегирования.

```
[S1]interface Eth-Trunk 1
```

```
[S1-Eth-Trunk1]mode lacp
```

Команда **mode lacp** позволяет установить LACP в качестве рабочего режима Eth-Trunk.

Примечание: в некоторых версиях для этого используется команда **mode lacp-static**.

```
[S2]interface Eth-Trunk 1
```

```
[S2-Eth-Trunk1]mode lacp
```

Добавьте порт в Eth-Trunk.

```
[S1]interface Eth-Trunk 1
```

```
[S1-Eth-Trunk1]trunkport GigabitEthernet 0/0/10 to 0/0/12
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S2]interface Eth-Trunk 1
```

```
[S2-Eth-Trunk1]trunkport GigabitEthernet 0/0/10 to 0/0/12
```

Info: This operation may take a few seconds. Please wait for a moment...done.

Выведите на экран статус Eth-Trunk.

```
[S1]display eth-trunk 1
```

Eth-Trunk1's state information is:

Local:

LAG ID: 1	WorkingMode: STATIC
Preempt Delay: Disabled	Hash arithmetic: According to SIP-XOR-DIP
System Priority: 32768	System ID: 4c1f-cc33-7359
Least Active-linknumber: 1	Max Active-linknumber: 8
Operate status: up	Number Of Up Port In Trunk: 3

ActorPortName	Status	PortType	PortPri	PortNo	PortKey	PortState	Weight
GigabitEthernet0/0/10	Selected	1GE	32768	11	305	10111100	1
GigabitEthernet0/0/11	Selected	1GE	32768	12	305	10111100	1
GigabitEthernet0/0/12	Selected	1GE	32768	13	305	10111100	1

Partner:

ActorPortName	SysPri	SystemID	PortPri	PortNo	PortKey	PortState
GigabitEthernet0/0/10	32768	4c1f-ccc1-4a02	32768	11	305	10111100
GigabitEthernet0/0/11	32768	4c1f-ccc1-4a02	32768	12	305	10111100
GigabitEthernet0/0/12	32768	4c1f-ccc1-4a02	32768	13	305	10111100

Шаг 3 В обычных условиях в состоянии передачи данных должны находиться только GigabitEthernet0/0/11 и GigabitEthernet0/0/12, а GigabitEthernet0/0/10 должен использоваться в качестве резервного порта. Когда количество активных портов становится меньше 2, Eth-Trunk отключается.

Установите приоритет LACP для S1, чтобы сделать S1 активным устройством.

```
[S1]lacp priority 100
```

Настройте самый высокий приоритет портам GigabitEthernet0/0/11 и GigabitEthernet0/0/12.

```
[S1]interface GigabitEthernet 0/0/10
```

```
[S1-GigabitEthernet0/0/10]lacp priority 40000
```

В режиме LACP пакеты LACPDU (LACP Data Unit) передаются и принимаются обеими сторонами группы агрегирования каналов.

Сначала выбирается активный инициатор.

1. Выполняется сравнение полей приоритета системы. По умолчанию используется значение приоритета 32768. Чем меньше значение, тем выше приоритет. Сторона с более высоким приоритетом выбирается в качестве активного инициатора LACP.
2. При одинаковых приоритетах активным инициатором становится сторона с меньшим MAC-адресом.

После того, как активный инициатор выбран, устройства на обеих сторонах выбирают активные порты в соответствии с настройками приоритета порта на активном инициаторе.

Задайте верхний и нижний пороги активных портов.

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]max active-linknumber 2
[S1-Eth-Trunk1]least active-linknumber 2
```

Пропускная способность и статус Eth-Trunk зависят от количества активных портов. Под пропускной способностью Eth-Trunk подразумевается общая пропускная способность всех портов-участников в состоянии Up. Для того, чтобы стабилизировать статус и пропускную способность Eth-Trunk, а также сократить влияние частых изменений статусов каналов-участников, можно настроить следующие пороговые значения.

- Нижний порог: при сокращении количества активных портов ниже этого порога Eth-Trunk отключается. Порог определяет минимальную пропускную способность Eth-Trunk и настраивается с помощью команды **least active-linknumber**.
- Верхний порог: если количество активных портов достигает этого порогового значения, пропускная способность Eth-Trunk не увеличивается, даже при увеличении числа каналов в состоянии Up. Верхний порог обеспечивает доступность сети и настраивается с помощью команды **max active-linknumber**.

Включите функцию внеочередного занятия линии.

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]lacp preempt enable
```

В режиме LACP при выходе из строя активного канала система выбирает резервный канал с наивысшим приоритетом, чтобы заменить неисправный. Если включена функция внеочередного занятия линии, то после восстановления неисправный канал может снова получить статус активного канала, если он имеет более высокий приоритет, чем резервный канал. Функцию внеочередного занятия линии можно включить с помощью команды **lacp preempt enable**. По умолчанию эта функция отключена.

Выведите на экран статус текущего Eth-Trunk.

```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                               WorkingMode: STATIC
```



```
Preempt Delay Time: 30      Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100        System ID: 4c1f-cc33-7359
Least Active-linknumber: 2  Max Active-linknumber: 2
Operate status: up         Number Of Up Port In Trunk: 2
```

ActorPortName	Status	PortType	PortPri	PortNo	PortKey	PortState	Weight
GigabitEthernet0/0/10	Unselect	1GE	40000	11	305	10100000	1
GigabitEthernet0/0/11	Selected	1GE	32768	12	305	10111100	1
GigabitEthernet0/0/12	Selected	1GE	32768	13	305	10111100	1

Partner:

ActorPortName	SysPri	SystemID	PortPri	PortNo	PortKey	PortState
GigabitEthernet0/0/10	32768	4c1f-ccc1-4a02	32768	11	305	10110000
GigabitEthernet0/0/11	32768	4c1f-ccc1-4a02	32768	12	305	10111100
GigabitEthernet0/0/12	32768	4c1f-ccc1-4a02	32768	13	305	10111100

GigabitEthernet0/0/11 и GigabitEthernet0/0/12 находятся в активном состоянии.

Отключите GigabitEthernet0/0/12, чтобы смоделировать неисправность канала.

```
[S1]interface GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12]shutdown
[S1]display eth-trunk 1
```

Eth-Trunk1's state information is:

Local:

```
LAG ID: 1      WorkingMode: STATIC
Preempt Delay Time: 30      Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100        System ID: 4c1f-cc33-7359
Least Active-linknumber: 2  Max Active-linknumber: 2
Operate status: up         Number Of Up Port In Trunk: 2
```

ActorPortName	Status	PortType	PortPri	PortNo	PortKey	PortState	Weight
GigabitEthernet0/0/10	Selected	1GE	40000	11	305	10111100	1
GigabitEthernet0/0/11	Selected	1GE	32768	12	305	10111100	1
GigabitEthernet0/0/12	Unselect	1GE	32768	13	305	10100010	1

Partner:

ActorPortName	SysPri	SystemID	PortPri	PortNo	PortKey	PortState
GigabitEthernet0/0/10	32768	4c1f-ccc1-4a02	32768	11	305	10111100
GigabitEthernet0/0/11	32768	4c1f-ccc1-4a02	32768	12	305	10111100
GigabitEthernet0/0/12	0	0000-0000-0000 0		0	0	10100011

GigabitEthernet 0/0/10 стал активным.

Отключите GigabitEthernet 0/0/11, чтобы смоделировать неисправность канала.

```
[S1]interface GigabitEthernet 0/0/11
[S1-GigabitEthernet0/0/11]shutdown
```

```
[S1]display eth-trunk 1
```

Eth-Trunk1's state information is:

Local:

```
LAG ID: 1      WorkingMode: STATIC
Preempt Delay Time: 30      Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100        System ID: 4c1f-cc33-7359
```

```
Least Active-linknumber: 2      Max Active-linknumber: 2
Operate status: down          Number Of Up Port In Trunk: 0
```

ActorPortName	Status	PortType	PortPri	PortNo	PortKey	PortState	Weight
GigabitEthernet0/0/10	Unselect	1GE	40000	11	305	10100000	1
GigabitEthernet0/0/11	Unselect	1GE	32768	12	305	10100010	1
GigabitEthernet0/0/12	Unselect	1GE	32768	13	305	10100010	1

Partner:

ActorPortName	SysPri	SystemID	PortPri	PortNo	PortKey	PortState
GigabitEthernet0/0/10	32768	4c1f-ccc1-4a02	32768	11	305	10110000
GigabitEthernet0/0/11	0	0000-0000-0000 0	0	0	0	10100011
GigabitEthernet0/0/12	0	0000-0000-0000 0	0	0	0	10100011

В качестве нижнего порога количества активных каналов настроено значение 2. Таким образом, Eth-Trunk отключен. Хотя GigabitEthernet0/0/10 стал активным, он все еще имеет статус Unselect.

Шаг 4 Измените режим балансировки нагрузки.

Включите порты, отключенные на предыдущем шаге.

```
[S1]inter GigabitEthernet 0/0/11
[S1-GigabitEthernet0/0/11]undo shutdown
[S1-GigabitEthernet0/0/11]quit
[S1]inter GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12]undo shutdown
```

Подождите около 30 секунд и проверьте статус Eth-Trunk 1.

```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                      WorkingMode: STATIC
Preempt Delay Time: 30         Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100           System ID: 4c1f-cc33-7359
Least Active-linknumber: 2     Max Active-linknumber: 2
Operate status: down          Number Of Up Port In Trunk: 0
```

ActorPortName	Status	PortType	PortPri	PortNo	PortKey	PortState	Weight
GigabitEthernet0/0/10	Unselect	1GE	40000	11	305	10100000	1
GigabitEthernet0/0/11	Selected	1GE	32768	12	305	10100010	1
GigabitEthernet0/0/12	Selected	1GE	32768	13	305	10100010	1

Partner:

ActorPortName	SysPri	SystemID	PortPri	PortNo	PortKey	PortState
GigabitEthernet0/0/10	32768	4c1f-ccc1-4a02	32768	11	305	10110000
GigabitEthernet0/0/11	0	0000-0000-0000 0	0	0	0	10100011
GigabitEthernet0/0/12	0	0000-0000-0000 0	0	0	0	10100011

Функция внеочередного занятия линии включена на Eth-Trunk. Таким образом, GigabitEthernet0/0/11 и GigabitEthernet0/0/12 становятся активными, потому что имеют более высокий приоритет, чем GigabitEthernet0/0/10. В результате GigabitEthernet0/0/10 получает статус Unselect. Кроме того, для обеспечения стабильности канала время внеочередного занятия линии по умолчанию составляет

30 секунд. Таким образом, внеочередное занятие линии происходит через 30 секунд после включения портов.

Измените режим балансировки нагрузки Eth-Trunk на балансировку нагрузки на основе IP-адреса назначения.

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]load-balance dst-ip
```

Чтобы обеспечить правильную балансировку нагрузки между физическими каналами Eth-Trunk и избежать перегрузки каналов, настройте режим балансировки нагрузки Eth-Trunk с помощью команды **load-balance**. Балансировка нагрузки работает только для исходящего трафика. Поэтому режимы балансировки нагрузки для портов на разных сторонах виртуального канала могут отличаться.

----Конец

3.3.3 Проверка

Подробности данной операции здесь не приводятся.

3.3.4 Справочные конфигурации

Конфигурация на S1

```
#
sysname S1
#
lacp priority 100
#
interface Eth-Trunk1
 mode lacp
 least active-linknumber 2
 load-balance dst-ip
 lacp preempt enable
 max active-linknumber 2
#
interface GigabitEthernet0/0/10
 eth-trunk 1
 lacp priority 40000
#
interface GigabitEthernet0/0/11
 eth-trunk 1
#
interface GigabitEthernet0/0/12
 eth-trunk 1
#
return
```

Конфигурация на S2

```
#
sysname S2
#
interface Eth-Trunk1
 mode lacp
```

```
#  
interface GigabitEthernet0/0/10  
eth-trunk 1  
#  
interface GigabitEthernet0/0/11  
eth-trunk 1  
#  
interface GigabitEthernet0/0/12  
eth-trunk 1  
#  
return
```

3.3.5 Вопросы

1. Какие требования предъявляются к значениям параметров **least active-linknumber** и **max active-linknumber**?

3.4 Лабораторная работа 4. Связь между VLAN

3.4.1 Общая информация

3.4.1.1 О лабораторной работе

Для минимизации широковещательных доменов реализуется разделение VLAN на уровне 2. Для обеспечения связи между VLAN компания Huawei предлагает различные технологии. Наиболее часто используются следующие две технологии:

- Подинтерфейс терминирования dot1q: такие подинтерфейсы являются логическими интерфейсами уровня 3. Подобно интерфейсу VLANIF, после настройки подинтерфейса терминирования dot1q и его IP-адреса устройство добавляет соответствующую запись MAC-адреса и устанавливает флаг передачи уровня 3 для реализации связи между VLAN на уровне 3. Подинтерфейс терминирования dot1q применяется в сценариях, где к порту Ethernet уровня 3 подключается несколько VLAN.
- Интерфейс VLANIF: интерфейсы VLANIF — это логические интерфейсы уровня 3. После настройки интерфейса VLANIF и его IP-адреса устройство добавляет MAC-адрес и VID интерфейса VLANIF в таблицу MAC-адресов и устанавливает флаг передачи уровня 3 для записи MAC-адреса. Когда MAC-адрес пункта назначения пакета совпадает с записью, пакет передается на уровень 3 для реализации связи уровня 3 между сетями VLAN.

В этой лабораторной работе вам предлагается два способа конфигурирования связи между VLAN.

3.4.1.2 Цели

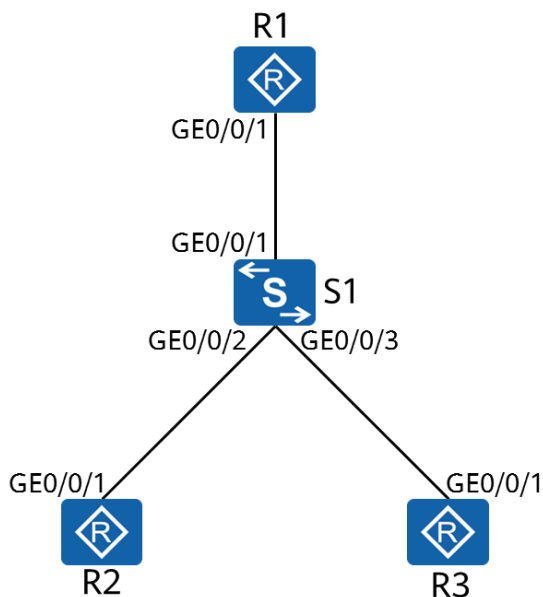
Лабораторная работа помогает получить практические навыки по изучению следующих тем:

- Использование подинтерфейсов терминирования dot1q для реализации связи между VLAN
- Использование интерфейсов VLANIF для реализации связи между VLAN
- Процесс передачи данных между VLAN

3.4.1.3 Топология сети

Маршрутизаторы R2 и R3 принадлежат к разным VLAN. Для их взаимодействия необходимы интерфейсы VLANIF и подинтерфейсы терминирования dot1q.

Рис. 3-4 Топология сети для реализации связи между VLAN, используемая в данной лабораторной работе



1. Смоделируйте пользователей терминалов на R2 и R3 и назначьте интерфейсам IP-адреса 192.168.2.1/24 и 192.168.3.1/24.
2. Назначьте в качестве адресов шлюзов R2 и R3 адреса 192.168.2.254 и 192.168.3.254 соответственно.
3. На S1 назначьте GigabitEtherneto/0/2 и GigabitEtherneto/0/3 для VLAN 2 и VLAN 3 соответственно.

3.4.2 Лабораторная работа

3.4.2.1 План работы

1. Настройка подинтерфейсов терминирования dot1q для реализации связи между VLAN.
2. Настройка интерфейсов VLANIF для реализации связи между VLAN.

3.4.2.2 Процедура конфигурирования

Шаг 1 Настройте основные параметры устройств.

Присвойте имена маршрутизаторам R1, R2, R3 и S1.

Подробности данной операции здесь не приводятся.

Настройте IP-адреса и шлюзы для R2 и R3.

```

<R2> system-view
Enter system view, return user view with Ctrl+Z.
[R2] interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1] ip address 192.168.2.1 24
[R2-GigabitEthernet0/0/1] quit
  
```

```
[R2]ip route-static 0.0.0.0 0 192.168.2.254
```

Настройте маршрут по умолчанию (эквивалентный шлюзу) для устройства.

```
<R3>system-view
```

Enter system view, return user view with Ctrl+Z.

```
[R3]interface GigabitEthernet 0/0/1
```

```
[R3-GigabitEthernet0/0/1]ip address 192.168.3.1 24
```

```
[R3-GigabitEthernet0/0/1]quit
```

```
[R3]ip route-static 0.0.0.0 0 192.168.3.254
```

На S1 назначьте R2 и R3 в разные VLAN.

```
[S1]vlan batch 2 3
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S1]interface GigabitEthernet 0/0/2
```

```
[S1-GigabitEthernet0/0/2]port link-type access
```

```
[S1-GigabitEthernet0/0/2]port default vlan 2
```

```
[S1-GigabitEthernet0/0/2]quit
```

```
[S1]interface GigabitEthernet 0/0/3
```

```
[S1-GigabitEthernet0/0/3]port link-type access
```

```
[S1-GigabitEthernet0/0/3]port default vlan 3
```

Шаг 2 Настройте подинтерфейсы терминирования dot1q для реализации связи между VLAN.

Настройте магистральный порт на S1.

```
[S1]interface GigabitEthernet 0/0/1
```

```
[S1-GigabitEthernet0/0/1]port trunk allow-pass vlan 2 3
```

Канал между S1 и R1 должен разрешать прохождение пакетов из VLAN 2 и VLAN 3, потому что R1 должен удалять теги VLAN из пакетов, которыми обмениваются эти VLAN.

Настройте подинтерфейс терминирования dot1q на маршрутизаторе R1.

```
[R1]interface GigabitEthernet 0/0/1,2
```

После создания подинтерфейса осуществляется переход в режим конфигурирования подинтерфейса. В этом примере цифра 2 указывает номер подинтерфейса.

Рекомендуется, чтобы номер подинтерфейса совпадал с идентификатором VLAN.

```
[R1-GigabitEthernet0/0/1.2]dot1q termination vid 2
```

Команда **dot1q termination vid *vlan-id*** позволяет настраивать идентификатор VLAN для выполнения терминирования Dot1q на подинтерфейсе.

В этом примере, когда GigabitEthernet0/0/1 получает данные с тегами VLAN 2, он передает данные подинтерфейсу 2 для терминирования VLAN и последующей обработки. Данные, отправленные с подинтерфейса 2, также помечаются тегами VLAN 2.

```
[R1-GigabitEthernet0/0/1.2]arp broadcast enable
```

Подинтерфейсы, выполняющие удаление тегов VLAN, не могут пересылать широковещательные пакеты и автоматически отбрасывают их при получении. Чтобы такие подинтерфейсы могли пересылать широковещательные пакеты, необходимо

включить функцию широковещательной передачи ARP с помощью команды **arp broadcast enable**. На некоторых устройствах эта функция включена по умолчанию.

```
[R1-GigabitEthernet0/0/1,2]ip address 192.168.2.254 24
[R1-GigabitEthernet0/0/1,2]quit
[R1]interface GigabitEthernet 0/0/1,3
[R1-GigabitEthernet0/0/1,3]dot1q termination vid 3
[R1-GigabitEthernet0/0/1,3]arp broadcast enable
[R1-GigabitEthernet0/0/1,3]ip address 192.168.3.254 24
[R1-GigabitEthernet0/0/1,3]quit
```

Проверьте связь между VLAN.

```
<R2>ping 192.168.3.1
  PING 192.168.3.1: 56 data bytes, press CTRL_C to break
    Reply from 192.168.3.1: bytes=56 Sequence=1 ttl=254 time=60 ms
    Reply from 192.168.3.1: bytes=56 Sequence=2 ttl=254 time=40 ms
    Reply from 192.168.3.1: bytes=56 Sequence=3 ttl=254 time=110 ms
    Reply from 192.168.3.1: bytes=56 Sequence=4 ttl=254 time=70 ms
    Reply from 192.168.3.1: bytes=56 Sequence=5 ttl=254 time=100 ms

  --- 192.168.3.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/76/110 ms

<R2>tracert 192.168.3.1
  traceroute to 192.168.3.1(192.168.3.1), max hops: 30 ,packet length: 40,press CTRL_C to break

  1 192.168.2.254 30 ms 50 ms 50 ms

  2 192.168.3.1 70 ms 60 ms 60 ms
VLAN 2 and VLAN 3 can communicate with each other.
```

Шаг 3 Настройте интерфейсы VLANIF для реализации связи между VLAN.

Удалите конфигурацию, созданную на предыдущем шаге.

```
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]undo port trunk allow-pass vlan 2 3
[S1-GigabitEthernet0/0/1]undo port link-type
[R1]undo interface GigabitEthernet 0/0/1.2
[R1]undo interface GigabitEthernet 0/0/1.3
```

Создайте интерфейс VLANIF на коммутаторе S1.

```
[S1]interface Vlanif 2
```

С помощью команды **interface vlanif *vlan-id*** можно создать интерфейс VLANIF и перейти в режим конфигурирования интерфейса VLANIF. Перед настройкой интерфейса VLANIF необходимо создать VLAN.

```
[S1-Vlanif2]ip address 192.168.2.254 24
[S1-Vlanif2]quit
[S1]interface Vlanif 3
[S1-Vlanif3]ip address 192.168.3.254 24
[S1-Vlanif3]quit
```

Проверьте связь между VLAN.

```
<R2>ping 192.168.3.1
PING 192.168.3.1: 56 data bytes, press CTRL_C to break
  Reply from 192.168.3.1: bytes=56 Sequence=1 ttl=254 time=100 ms
  Reply from 192.168.3.1: bytes=56 Sequence=2 ttl=254 time=50 ms
  Reply from 192.168.3.1: bytes=56 Sequence=3 ttl=254 time=50 ms
  Reply from 192.168.3.1: bytes=56 Sequence=4 ttl=254 time=60 ms
  Reply from 192.168.3.1: bytes=56 Sequence=5 ttl=254 time=70 ms
--- 192.168.3.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 50/66/100 ms

<R2>tracert 192.168.3.1

tracert to 192.168.3.1(192.168.3.1), max hops: 30 ,packet length: 40,press CTRL_C to break

 1 192.168.2.254 40 ms 30 ms 20 ms

 2 192.168.3.1 40 ms 30 ms 40 ms
Связь между VLAN 2 и VLAN 3 успешно осуществляется.
```

----Конец

3.4.3 Проверка

Подробности данной операции здесь не приводятся.

3.4.4 Справочные конфигурации

Конфигурация на S1

```
#
sysname S1
#
vlan batch 2 to 3
#
interface Vlanif2
 ip address 192.168.2.254 255.255.255.0
#
interface Vlanif3
 ip address 192.168.3.254 255.255.255.0
#
interface GigabitEthernet0/2
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/3
 port link-type access
 port default vlan 3
#
return
```

Конфигурация на R2

```
#
sysname R2
#
interface GigabitEthernet0/0/1
ip address 192.168.2.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.2.254
#
return
```

Конфигурация на R3

```
#
sysname R3
#
interface GigabitEthernet0/0/1
ip address 192.168.3.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.254
#
return
```

3.4.5 Вопросы

1. Какие настройки необходимо выполнить на S1, если маршрутизатору R2 требуется доступ к сети, подключенной к маршрутизатору R1?
2. Когда интерфейс VLANIF начнет работать в качестве интерфейса уровня 3?

4

Основы сетевой безопасности и доступа к сети

4.1 Лабораторная работа 1. Настройка ACL

4.1.1 Общая информация

4.1.1.1 О лабораторной работе

Список контроля доступа (Access Control List, ACL) — это набор правил, разрешающих или запрещающих доступ. В каждом правиле определяется условие сопоставления пакетов. Это может быть адрес источника, адрес пункта назначения или номер порта.

ACL — это механизм фильтрации пакетов на основе правил. Пакеты, соответствующие списку ACL, обрабатываются на основе политики, определенной в ACL.

4.1.1.2 Цели

Лабораторная работа помогает получить практические навыки по изучению следующих тем:

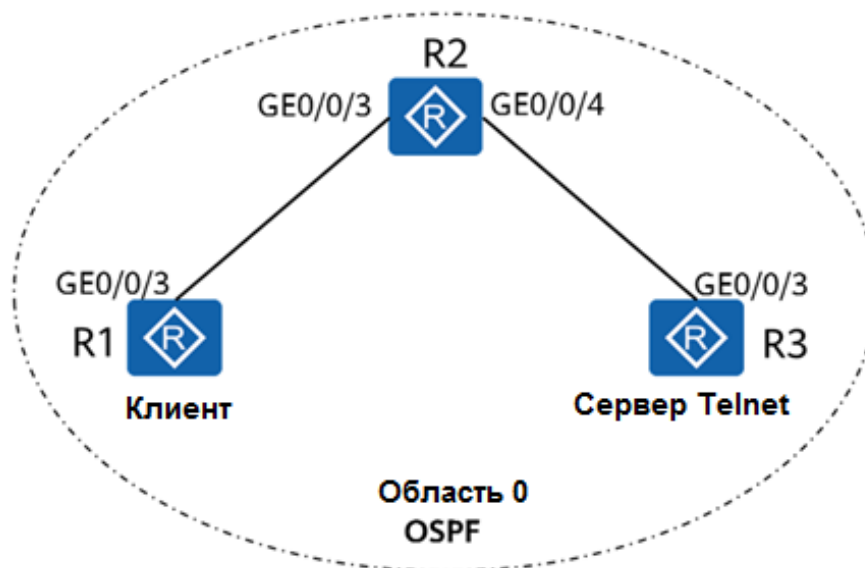
- Настройка списков ACL
- Применение ACL на интерфейсе
- Основные методы фильтрации трафика

4.1.1.3 Топология сети

В сети, показанной на схеме, маршрутизатор R3 выполняет функции сервера, маршрутизатор R1 выполняет функции клиента, и они доступны для связи. Физические интерфейсы, соединяющие R1 и R2, имеют IP-адреса 10.1.2.1/24 и 10.1.2.2/24 соответственно, а физические интерфейсы, соединяющие R2 и R3, — IP-адреса 10.1.3.2/24 и 10.1.3.1/24. Кроме того, на маршрутизаторе R1 созданы два логических интерфейса LoopBack 0 и LoopBack 1 для имитации двух пользователей-клиентов. Два интерфейса имеют IP-адреса 10.1.1.1/24 и 10.1.4.1/24 соответственно.

Один пользователь (LoopBack 1 на R1) должен удаленно управлять R3. Для гарантии того, что вход в R3 будет разрешен только пользователю, который соответствует политике безопасности, можно настроить Telnet на сервере, задать защиту паролем и сконфигурировать ACL.

Рис. 4-1 Топология сети для конфигурирования ACL, используемая в данной лабораторной работе



4.1.2 Лабораторная работа

4.1.2.1 План работы

1. Настройка IP-адресов.
2. Настройка OSPF для обеспечения возможности сетевого подключения.
3. Создание ACL на основе необходимого трафика.
4. Настройка фильтрации трафика.

4.1.2.2 Процедура конфигурирования

Шаг 1 Настройте IP-адреса.

Настройте IP-адреса для маршрутизаторов R1, R2 и R3.

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.1.2.1 24
[R1-GigabitEthernet0/0/3]quit
[R1]interface LoopBack 0
[R1-LoopBack0]ip address 10.1.1.1 24
[R1-LoopBack0]quit
[R1]interface LoopBack 1
[R1-LoopBack1]ip address 10.1.4.1 24
[R1-LoopBack1]quit
```

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 10.1.2.2 24
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
```



```
[R2-GigabitEthernet0/4]ip address 10.1.3.2 24
[R2-GigabitEthernet0/4]quit
```

```
[R3]interface GigabitEthernet0/3
[R3-GigabitEthernet0/3]ip address 10.1.3.1 24
[R3-GigabitEthernet0/3]quit
```

Шаг 2 Настройте OSPF для обеспечения возможности сетевого подключения.

Настройте OSPF на маршрутизаторах R1, R2 и R3 и назначьте их в область 0, чтобы обеспечить возможность подключения.

```
[R1]ospf
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.1.1.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0]network 10.1.2.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0]network 10.1.4.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0]return
```

```
[R2]ospf
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.1.2.2 0.0.0.0
[R2-ospf-1-area-0.0.0.0]network 10.1.3.2 0.0.0.0
[R2-ospf-1-area-0.0.0.0]return
```

```
[R3]ospf
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.1.3.1 0.0.0.0
[R3-ospf-1-area-0.0.0.0]return
```

Выполните команду ping на маршрутизаторе R3, чтобы проверить возможность подключения к сети.

```
<R3>ping 10.1.1.1
PING 10.1.1.1: 56 data bytes, press CTRL_C to break
  Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=254 time=40 ms
  Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=254 time=40 ms
  Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=254 time=20 ms
  Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=254 time=40 ms
  Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=254 time=30 ms
--- 10.1.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 20/34/40 ms

<R3>ping 10.1.2.1
PING 10.1.2.1: 56 data bytes, press CTRL_C to break
  Reply from 10.1.2.1: bytes=56 Sequence=1 ttl=254 time=30 ms
  Reply from 10.1.2.1: bytes=56 Sequence=2 ttl=254 time=30 ms
  Reply from 10.1.2.1: bytes=56 Sequence=3 ttl=254 time=30 ms
  Reply from 10.1.2.1: bytes=56 Sequence=4 ttl=254 time=30 ms
```

```
Reply from 10.1.2.1: bytes=56 Sequence=5 ttl=254 time=50 ms
--- 10.1.2.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 30/34/50 ms

<R3>ping 10.1.4.1
PING 10.1.4.1: 56 data bytes, press CTRL_C to break
Reply from 10.1.4.1: bytes=56 Sequence=1 ttl=254 time=50 ms
Reply from 10.1.4.1: bytes=56 Sequence=2 ttl=254 time=30 ms
Reply from 10.1.4.1: bytes=56 Sequence=3 ttl=254 time=40 ms
Reply from 10.1.4.1: bytes=56 Sequence=4 ttl=254 time=30 ms
Reply from 10.1.4.1: bytes=56 Sequence=5 ttl=254 time=30 ms
--- 10.1.4.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 30/36/50 ms
```

Шаг 3 Сконфигурируйте R3 в качестве сервера.

Включите функцию Telnet на R3, установите для уровня пользователя значение 3 и задайте для входа пароль — Huawei@123.

```
[R3]telnet server enable
```

Команда **telnet server enable** позволяет включить службу Telnet.

```
[R3]user-interface vty 0 4
```

Команда **user-interface** позволяет перейти в режим интерфейса одного или нескольких пользователей.

Пользовательский интерфейс терминала виртуального типа (Virtual Type Terminal, VTY) осуществляет управление и мониторинг входа пользователей в систему с помощью Telnet или SSH.

```
[R3-ui-vty0-4]user privilege level 3
[R3-ui-vty0-4]set authentication password cipher
Warning: The "password" authentication mode is not secure, and it is strongly recommended to use "aaa" authentication mode.
Enter Password(<8-128>):Huawei@123
Confirm password:Huawei@123
[R3-ui-vty0-4]quit
```

Шаг 4 Настройте ACL на основе необходимого трафика.

Способ 1. Настройте ACL на интерфейсе VTY маршрутизатора R3, чтобы разрешить вход с R1 в R3 через Telnet, используя IP-адрес LoopBack 1.

Настройте ACL на R3.

```
[R3]acl 3000
[R3-acl-adv-3000]rule 5 permit tcp source 10.1.4.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port eq 23
[R3-acl-adv-3000]rule 10 deny tcp source any
[R3-acl-adv-3000]quit
```

Выполните фильтрацию трафика на интерфейсе VTY маршрутизатора R3.

```
[R3]user-interface vty 0 4
[R3-ui-vty0-4]acl 3000 inbound
```

Выведите на экран конфигурацию ACL на R3.

```
[R3]display acl 3000
```

Команда **display acl** позволяет вывести на экран конфигурацию ACL.

```
Advanced ACL 3000, 2 rules
```

Создан расширенный ACL. Он имеет номер 3000 и содержит два правила.

```
Acl's step is 5
```

Правила ACL пронумерованы с шагом 5.

```
rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet
```

Правило 5 разрешает прохождение соответствующего трафика. Если пакетов, соответствующих правилу, нет, поле **matches** не отображается.

```
rule 10 deny tcp
```

Способ 2. Настройте ACL на физическом интерфейсе маршрутизатора R2, чтобы разрешить вход с R1 в R3 через Telnet, используя IP-адрес физического интерфейса.

Настройте ACL на R2.

```
[R2]acl 3001
[R2-acl-adv-3001]rule 5 permit tcp source 10.1.4.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port eq 23
[R2-acl-adv-3001]rule 10 deny tcp source any
[R2-acl-adv-3001]quit
```

Выполните фильтрацию трафика на интерфейсе GE0/0/3 маршрутизатора R3.

```
[R2]interface GigabitEthernet0/0/3
[R2-GigabitEthernet0/0/3]traffic-filter inbound acl 3001
```

Выведите на экран конфигурацию ACL на R2.

```
[R2]display acl 3001
Advanced ACL 3001, 2 rules
Acl's step is 5
rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet (21 matches)
```

Правило 5 разрешает прохождение соответствующего трафика. Поле **matches** показывает 21 соответствие пакетов правилу.

```
rule 10 deny tcp (1 matches)
```

----Конец

4.1.3 Проверка

Протестируйте доступ через Telnet и проверьте конфигурацию ACL.

1. На маршрутизаторе R1 подключитесь через Telnet к серверу, используя указанный IP-адрес источника 10.1.1.1.

```
<R1>telnet -a 10.1.1.1 10.1.3.1
```

Команда **telnet** позволяет использовать протокол Telnet для входа на другое устройство.

-а *source-ip-address*: определяет IP-адрес источника. Пользователи могут связываться с сервером, используя указанный IP-адрес.

```
Press CTRL_] to quit telnet mode
Trying 10.1.3.1 ...
Error: Can't connect to the remote host
```

2. На маршрутизаторе R1 подключитесь через Telnet к серверу, используя указанный IP-адрес источника 10.1.4.1.

```
<R1>telnet -a 10.1.4.1 10.1.3.1
Press CTRL_] to quit telnet mode
Trying 10.1.3.1 ...
Connected to 10.1.3.1 ...

Login authentication

Password:
<R3>quit
```

4.1.4 Справочные конфигурации (Способ 1)

Конфигурация на R1

```
#
sysname R1
#
interface GigabitEthernet0/0/3
ip address 10.1.2.1 255.255.255.0
#
interface LoopBack0
ip address 10.1.1.1 255.255.255.0
#
interface LoopBack1
ip address 10.1.4.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 10.1.1.1 0.0.0.0
network 10.1.2.1 0.0.0.0
network 10.1.4.1 0.0.0.0
#
return
```

Конфигурация на R2

```
#
sysname R2
#
interface GigabitEthernet0/0/3
ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet0/0/4
ip address 10.1.3.2 255.255.255.0
#
```

```
ospf 1
 area 0.0.0.0
  network 10.1.2.2 0.0.0.0
  network 10.1.3.2 0.0.0.0
#
return
```

Конфигурация на R3

```
#
 sysname R3
#
acl number 3000
 rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet
 rule 10 deny tcp
#
interface GigabitEthernet0/0/3
 ip address 10.1.3.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.3.1 0.0.0.0
#
telnet server enable
#
user-interface vty 0 4
 acl 3000 inbound
 authentication-mode password
 user privilege level 3
 set authentication password cipher %^%#Z5)H#8cE(YJ6YZ:=}c-;trp&784i>HtKl~pLnn>2zL16cs<6E}xj.FmK5(8%^%#
#
return
```

4.1.5 Справочные конфигурации (Способ 2)

Конфигурация на R1

```
#
 sysname R1
#
interface GigabitEthernet0/0/3
 ip address 10.1.2.1 255.255.255.0
#
interface LoopBack0
 ip address 10.1.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.1.4.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.1 0.0.0.0
  network 10.1.2.1 0.0.0.0
  network 10.1.4.1 0.0.0.0
#
return
```

Конфигурация на R2

```
#
 sysname R2
#
acl number 3001
 rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet
 rule 10 deny tcp
#
interface GigabitEthernet0/0/3
 ip address 10.1.2.2 255.255.255.0
 traffic-filter inbound acl 3001
#
interface GigabitEthernet0/0/4
 ip address 10.1.3.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.2.2 0.0.0.0
  network 10.1.3.2 0.0.0.0
#
return
```

Конфигурация на R3

```
#
 sysname R3
#
interface GigabitEthernet0/0/3
 ip address 10.1.3.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.3.1 0.0.0.0
#
telnet server enable
#
user-interface vty 0 4
 authentication-mode password
 user privilege level 3
 set authentication password cipher %^%#Z5)H#8cE(YJ6YZ:='}c-,trp&784i>HtKl~pLnn>2zL16cs<6E}xj.FmK5(8%^%#
#
return
```

4.1.6 Вопросы

R3 выполняет функции как сервера Telnet, так и FTP-сервера, IP-адрес LoopBack 0 на R1 должен использоваться только для доступа к службе FTP, а IP-адрес LoopBack 1 на R1 должен использоваться для удаленного управления R3 через Telnet.

Настройте ACL в соответствии с приведенными требованиями.

4.2 Лабораторная работа 2. Настройка локального механизма AAA

4.2.1 Общая информация

4.2.1.1 О лабораторной работе

Аутентификация, авторизация и учет (AAA) — механизм управления сетевой безопасностью.

AAA предоставляет следующие функции:

- Аутентификация: проверка наличия у пользователей разрешения на доступ к сети.
- Авторизация: проверка полномочий пользователей на использование определенных услуг.
- Учет: регистрация сетевых ресурсов, используемых пользователями.

Пользователи могут использовать одну или несколько служб безопасности, предоставляемых AAA. Например, если компании требуется аутентификация сотрудников, которые обращаются к определенным сетевым ресурсам, то сетевому администратору необходимо только настроить сервер аутентификации. Если компания также хочет регистрировать операции, выполняемые сотрудниками в сети, необходимо настроить сервер учета.

Таким образом, механизм AAA будет разрешать сотрудникам использовать определенные ресурсы и записывать их операции. Механизм AAA получил широкое применение, поскольку отличается хорошей масштабируемостью и упрощает централизованное управление пользовательской информацией. Реализовать AAA можно с помощью нескольких протоколов. В реальных условиях чаще всего используется протокол RADIUS.

В этой лабораторной работе вам предлагается настроить локальный механизм AAA для управления и контроля ресурсов, используемых удаленными пользователями Telnet.

4.2.1.2 Цели

Лабораторная работа помогает получить практические навыки по изучению следующих тем:

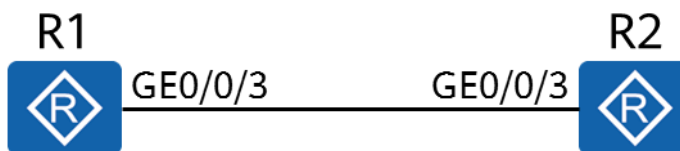
- Настройка локального механизма AAA
- Процедура создания домена
- Процедура создания локального пользователя
- Управление пользователями на основе домена

4.2.1.3 Топология сети

Маршрутизатор R1 выполняет функции клиента, а R2 — функции сетевого устройства. Необходим контроль доступа к ресурсам на R2. Следовательно, нужно настроить локальную аутентификацию AAA на маршрутизаторах R1 и R2 и управлять

пользователями на основе доменов, а также настроить уровни полномочий для аутентифицированных пользователей.

Рис. 4-2 Топология сети для конфигурирования локального механизма AAA, используемая в данной лабораторной работе



4.2.2 Лабораторная работа

4.2.2.1 План работы

1. Настройка схемы AAA.
2. Создание домена и применение к нему схемы AAA.
3. Настройка локальных пользователей.

4.2.2.2 Процедура конфигурирования

Шаг 1 Настройте основные параметры устройств.

Присвойте имена маршрутизаторам R1 и R2.

Подробности данной операции здесь не приводятся.

Настройте IP-адреса для маршрутизаторов R1 и R2.

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.0.12.1 24
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 10.0.12.2 24
```

Шаг 2 Настройте схему AAA.

Настройте схемы аутентификации и авторизации.

```
[R2-aaa]aaa
Перейдите в режим AAA.
[R2-aaa]authentication-scheme datacom
Info: Create a new authentication scheme.
Создайте схему аутентификации с названием datacom.
[R2-aaa-authen-datacom]authentication-mode local
Задайте в качестве режима аутентификации локальную аутентификацию.
[R2-aaa-authen-datacom]quit
[R2-aaa]authorization-scheme datacom
Info: Create a new authorization scheme.
Создайте схему авторизации с названием datacom.
[R2-aaa-author-datacom]authorization-mode local
Задайте в качестве режима авторизации локальную авторизацию.
[R2-aaa-author-datacom]quit
```


Устройство, выполняющее функции сервера AAA, называется локальным сервером AAA, который может выполнять аутентификацию и авторизацию, но не учет.

Локальному серверу AAA требуется база данных локальных пользователей, содержащая имя пользователя, пароль и информацию об авторизации локальных пользователей. Локальный сервер AAA быстрее и дешевле, чем удаленный сервер AAA, но имеет меньшую емкость хранилища.

Шаг 3 Создайте домен и примените к нему схему AAA.

```
[R2]aaa  
[R2-aaa]domain datacom
```

Устройства управляют пользователями на основе доменов. Домен — это группа пользователей. Каждый пользователь принадлежит к домену. Конфигурация AAA для домена применяется к пользователям в домене. Создайте домен с именем datacom.

```
[R2-aaa-domain-datacom]authentication-scheme datacom  
Схема аутентификации с названием datacom используется для пользователей в домене.  
[R2-aaa-domain-datacom]authorization-scheme datacom  
Схема авторизации с названием datacom используется для пользователей в домене.
```

Шаг 4 Настройте локальных пользователей.

Создайте локального пользователя и настройте для него пароль.

```
[R2-aaa]local-user hcia@datacom password cipher HCIA-Datcom  
Info: Add a new user.
```

Если в имени пользователя содержится разделитель в виде символа @, то строка символов перед символом @ — это имя пользователя, а строка символов после символа @ — имя домена. Если в имени пользователя нет разделителя в виде символа @, вся символьная строка представляет собой имя пользователя, а для домена используется имя по умолчанию.

Настройте параметры для локального пользователя, такие как тип доступа и уровень полномочий.

```
[R2-aaa]local-user hcia@datacom service-type telnet
```

Команда **local-user service-type** позволяет настроить тип доступа для локального пользователя. После настройки типа доступа пользователь сможет успешно войти в систему, только применив настроенный тип доступа. Если в качестве типа доступа было указано telnet, пользователь не сможет получить доступ к устройству через веб-страницу. Для одного пользователя можно настроить несколько типов доступа.

```
[R2-aaa]local-user hcia@datacom privilege level 3
```

Для локального пользователя настроен уровень полномочий. Этому пользователю будут доступны только команды, предоставляемые указанным уровнем полномочий, и команды более низкого уровня полномочий.

Шаг 5 Включите функцию telnet на R2.

```
[R2]telnet server enable  
На устройстве включена функция сервера Telnet. На некоторых устройствах эта функция включена по умолчанию.  
[R2]user-interface vty 0 4  
[R2-ui-vty0-4]authentication-mode aaa
```

Команда **authentication-mode** позволяет настроить режим аутентификации для доступа к пользовательскому интерфейсу. По умолчанию режим аутентификации на пользовательском интерфейсе VTY не настроен. Для интерфейса входа в систему необходимо настроить режим аутентификации. В противном случае пользователи не смогут выполнять вход в устройство.

Шаг 6 Проверьте конфигурацию.

Выполните вход с R1 на R2 через Telnet.

```
<R1>telnet 10.0.12.2
Press CTRL_] to quit telnet mode
Trying 10.0.12.2 ...
Connected to 10.0.12.2 ...

Login authentication

Username:hcia@datacom
Password:
<R2>
```

С маршрутизатора R1 можно выполнить вход в систему R2.

Выведите на экран список пользователей, подключенных к R2.

```
[R2]display users
```

User-Intf	Delay	Type	Network Address	AuthenStatus	AuthorcmdFlag
129 VTY 0	00:02:43	TEL	10.0.12.1	pass	

```
Username : hcia@datacom
```

----Конец

4.2.3 Проверка

Подробности данной операции здесь не приводятся.

4.2.4 Справочные конфигурации

Конфигурация на R1

```
#
sysname R1
#
interface GigabitEthernet0/0/3
ip address 10.0.12.1 255.255.255.0
#
return
```

Конфигурация на R2

```
#
sysname R2
#
aaa
authentication-scheme datacom
authorization-scheme datacom
```

```
domain datacom
 authentication-scheme datacom
 authorization-scheme datacom
 local-user hcia@datacom password irreversible-
 cipher %^%#.}hB'1"=&=:FWx!Ust(3s^<.[Z}kEc/>==P56gUVU*cE^]5@|8/O5FC$9A%^%#
 local-user hcia@datacom privilege level 3
 local-user hcia@datacom service-type telnet
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.2 255.255.255.0
#
telnet server enable
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 15
#
return
```

4.2.5 Вопросы

Вопросы по этой теме не предоставляются.

4.3 Лабораторная работа 3. Настройка NAT

4.3.1 Общая информация

4.3.1.1 О лабораторной работе

Преобразование сетевых адресов (Network Address Translation, NAT) — механизм, позволяющий преобразовать IP-адрес в заголовке IP-пакета в другой IP-адрес. В качестве плана транзитной сети NAT позволяет повторно использовать адреса, чтобы решить проблему нехватки IPv4-адресов. Помимо этого, NAT дает следующие преимущества:

- Обеспечивает защиту частных сетей от внешних атак.
- Обеспечивает и контролирует связь между частными и общедоступными сетями.

С помощью данной лабораторной работы вы научитесь настраивать механизм NAT и поймете принцип его работы.

4.3.1.2 Цели

Лабораторная работа помогает получить практические навыки по изучению следующих тем:

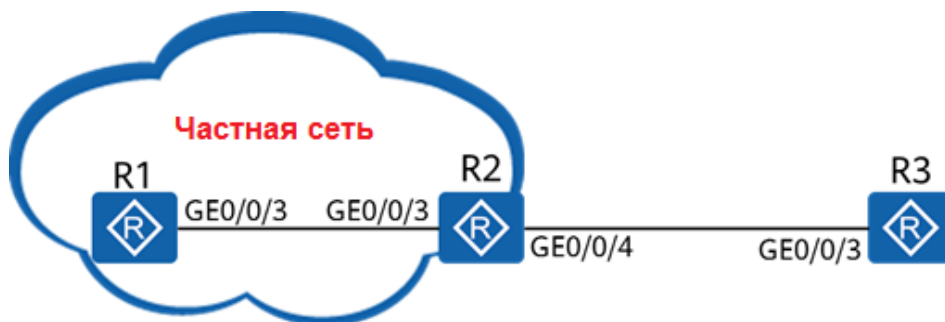
- Настройка динамического NAT
- Настройка Easy IP
- Настройка NAT-сервера

4.3.1.3 Топология сети

Для решения проблемы нехватки адресов IPv4 предприятия, как правило, используют частные адреса IPv4. Однако корпоративная сеть должна предоставлять доступ сотрудникам к общедоступной сети и услуги внешним пользователям. В этом случае необходимо настроить NAT в соответствии с приведенными выше требованиями.

1. Сеть между маршрутизаторами R1 и R2 является интрасетью и использует частные адреса IPv4.
2. R1 выполняет функции клиента, а R2 является шлюзом для R1 и граничным маршрутизатором, подключенным к общедоступной сети.
3. R3 имитирует общедоступную сеть.

Рис. 4-3 Топология сети для конфигурирования NAT, используемая в данной лабораторной работе



4.3.2 Лабораторная работа

4.3.2.1 План работы

1. Настройка динамического NAT.
2. Настройка Easy IP.
3. Настройка сервера NAT.

4.3.2.2 Процедура конфигурирования

Шаг 1 Настройте основные параметры.

Настройте IP-адреса и маршруты.

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3]ip address 192.168.1.1 24
[R1-GigabitEthernet0/0/3]quit
[R1]ip route-static 0.0.0.0 0 192.168.1.254
```

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 192.168.1.254 24
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ip address 1.2.3.4 24
[R2-GigabitEthernet0/0/4]quit
[R2]ip route-static 0.0.0.0 0 1.2.3.254
```

```
[R3]interface GigabitEthernet 0/0/3
[R3-GigabitEthernet0/0/3]ip address 1.2.3.254 24
```

Настройте функцию Telnet на маршрутизаторах R1 и R3 для последующей проверки.

```
[R1]user-interface vty 0 4
[R1-ui-vty0-4]authentication-mode aaa
[R1-ui-vty0-4]quit
[R1]aaa
[R1-aaa]local-user test password irreversible-cipher Huawei@123
Info: Add a new user.
[R1-aaa]local-user test service-type telnet
[R1-aaa]local-user test privilege level 15
```

```
[R3]user-interface vty 0 4
[R3-ui-vty0-4]authentication-mode aaa
[R3-ui-vty0-4]quit
[R3]aaa
[R3-aaa]local-user test password irreversible-cipher Huawei@123
Info: Add a new user.
[R3-aaa]local-user test service-type telnet
[R3-aaa]local-user test privilege level 15
[R3-aaa]quit
```

Проверьте возможность установления связи.

```
[R1]ping 1.2.3.254
PING 1.2.3.254: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- 1.2.3.254 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss
```

```
[R2]ping 1.2.3.254
PING 1.2.3.254: 56 data bytes, press CTRL_C to break
Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=255 time=40 ms
Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=255 time=20 ms
Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=255 time=20 ms
Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=255 time=20 ms
Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=255 time=20 ms

--- 1.2.3.254 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 20/24/40 ms
```

У маршрутизатора R1 нет связи с R3, потому что на R3 не настроен маршрут к адресу 192.168.1.0/24.

Более того, на R3 нельзя настраивать маршруты в частные сети.

Шаг 2 Предприятие получает общедоступные IP-адреса в диапазоне от 1.2.3.10 до 1.2.3.20, поэтому ему требуется функция динамического NAT.

Настройте пул адресов NAT.

```
[R2]nat address-group 1 1.2.3.10 1.2.3.20
```

С помощью команды **nat address-group** можно настроить пул адресов NAT. В данном примере пул адресов имеет номер 1. Пул адресов должен быть набором последовательных IP-адресов. При достижении внутренними пакетами данных границы частной сети частные IP-адреса источников будут преобразовываться в общедоступные IP-адреса.

Настройте ACL.

```
[R2]acl 2000
[R2-acl-basic-2000]rule 5 permit source any
```

Настройте динамический NAT на GigabitEthernet0/0/4 маршрутизатора R2.

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]nat outbound 2000 address-group 1
```

Команда **nat outbound** позволяет установить привязку ACL к пулу адресов NAT. IP-адреса пакетов, соответствующих списку ACL, будут преобразовываться в адреса из пула адресов. Если в пуле достаточно адресов, можно добавить аргумент **no-pat**, чтобы включить однозначное преобразование адресов. В этом случае будут преобразовываться только IP-адреса пакетов данных, а порты преобразовываться не будут.

Проверьте возможность установления связи.

```
[R1]ping 1.2.3.254
PING 1.2.3.254: 56 data bytes, press CTRL_C to break
  Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=254 time=60 ms
  Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=254 time=20 ms
  Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=254 time=30 ms
  Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=254 time=30 ms
  Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=254 time=20 ms

--- 1.2.3.254 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
round-trip min/avg/max = 20/32/60 ms
```

Выполните вход с R1 на R3 через Telnet, чтобы смоделировать трафик TCP.

```
<R1>telnet 1.2.3.254
Press CTRL_] to quit telnet mode
Trying 1.2.3.254 ...
Connected to 1.2.3.254 ...

Login authentication

Username:test
Password:
<R3>
```

Выведите на экран таблицу сеансов NAT на R2.

```
[R2]display nat session all
NAT Session Table Information:
  Protocol      : TCP(6)
  SrcAddr  Port Vpn  : 192.168.1.1      62185      //IP-адрес и порт источника перед преобразованием
NAT                                                     //IP-адрес источника после преобразования NAT
  DestAddr Port Vpn  : 1.2.3.254      23
  NAT-Info
  New SrcAddr   : 1.2.3.11
  New SrcPort   : 49149      //Порт источника после преобразования NAT
  New DestAddr  : ----
  New DestPort  : ----

Total : 1
```

Несмотря на то, что R3 не имеет маршрута к R1, он передает данные на преобразованный адрес источника 1.2.3.11. После получения данных R2 преобразует

адрес источника в адрес R1 на основе данных в таблице сеансов NAT и передает данные. Таким образом, R1 может инициировать доступ к R3.

Шаг 3 Если IP-адрес GigabitEthernet0/0/4 на R2 назначается динамически (например, через DHCP или PPPoE), необходимо настроить Easy IP.

Удалите конфигурацию, созданную на предыдущем шаге.

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]undo nat outbound 2000 address-group 1
```

Настройте Easy IP.

```
[R2-GigabitEthernet0/0/1]nat outbound 2000
```

Проверьте возможность установления связи.

```
[R1]ping 1.2.3.254
  PING 1.2.3.254: 56 data bytes, press CTRL_C to break
    Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=254 time=30 ms

--- 1.2.3.254 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 30/30/30 ms
```

Выполните вход с R1 на R3 через Telnet, чтобы смоделировать трафик TCP.

```
[R2]display nat session all
NAT Session Table Information:
  Protocol      : TCP(6)
  SrcAddr  Port Vpn  : 192.168.1.1    58546           //IP-адрес и порт источника перед
преобразованием NAT
  DestAddr Port Vpn  : 1.2.3.4      23
  NAT-Info
  New SrcAddr   : 1.2.3.4    //IP-адрес источника после преобразования NAT, то есть, адрес GigabitEthernet
0/0/4 на R2
  New SrcPort   : 49089      //Порт источника после преобразования NAT
  New DestAddr  : ----
  New DestPort  : ----

Total : 1
```

Шаг 4 R3 должен предоставлять сетевые услуги (в данном примере telnet) для пользователей в общедоступной сети. Поскольку R3 не имеет общедоступного IP-адреса, необходимо настроить сервер NAT на исходящем интерфейсе R2.

Настройте сервер NAT на R2.

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4] nat server protocol tcp global current-interface 2323 inside 192.168.1.1 telnet
```

Команда **nat server** позволяет определить таблицу сопоставления внутренних серверов, чтобы внешние пользователи могли получать доступ к внутренним

серверам через преобразование адресов и портов. Можно настроить внутренний сервер так, чтобы пользователи внешней сети могли инициировать доступ к внутреннему серверу. Когда хост во внешней сети отправляет запрос на соединение на общедоступный адрес (глобальный адрес) внутреннего сервера NAT, сервер NAT преобразует адрес назначения, содержащийся в запросе, в частный адрес (внутренний адрес) и пересылает запрос на сервер в частной сети.

Выполните вход с R3 на R1 через Telnet.

```
<R3>telnet 1.2.3.4 2323
Press CTRL_] to quit telnet mode
Trying 1.2.3.4 ...
Connected to 1.2.3.4 ...

Login authentication

Username:test
Password:
<R1>
```

Выведите на экран таблицу сеансов NAT на R2.

```
[R2]display nat session all
      Protocol      : TCP(6)
      SrcAddr  Port Vpn  : 1.2.3.254      61359
      DestAddr Port Vpn  : 1.2.3.4        2323           //IP-адрес и порт назначения перед преобразованием
NAT
      NAT-Info
      New SrcAddr      : ----
      New SrcPort       : ----
      New DestAddr     : 192.168.1.1       //IP-адрес назначения после преобразования NAT, то есть, IP-адрес маршрутизатора R1
      New DestPort     : 23                //Порт назначения после преобразования NAT
Total : 1
```

----Конец

4.3.3 Проверка

Подробности данной операции здесь не приводятся.

4.3.4 Справочные конфигурации

Конфигурация на R1

```
#
sysname R1
#
aaa
local-user test password irreversible-
cipher %^%#y'BJ=em]VY(E%IH!+,f-[!n*L`HU#H=vlVzMJR'^+^U3qWRm%&:Kd't7ol$%^%#
local-user test privilege level 3
local-user test service-type telnet
```

```
#
interface GigabitEthernet0/0/3
 ip address 192.168.1.1 255.255.255.0
#
telnet server enable
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
#
user-interface vty 0 4
 authentication-mode aaa
#
return
```

Конфигурация на R2

```
#
 sysname R2
#
acl number 2000
 rule 5 permit
#
 nat address-group 1 1.2.3.10 1.2.3.20
#
interface GigabitEthernet0/0/3
 ip address 192.168.1.254 255.255.255.0
#
interface GigabitEthernet0/0/4
 ip address 1.2.3.4 255.255.255.0
 nat server protocol tcp global current-interface 2323 inside 192.168.1.1 telnet
 nat outbound 2000
#
return
```

Конфигурация на R3

```
#
 sysname R3
#
aaa
local-user test password irreversible-cipher %^%#s<LQ(8-ZC6FNGG1#)n=.GgU|@)n`Z'n%$43+2>7,l>#XBkfcu{-
3y+o: `UD%^%#
 local-user test privilege level 15
 local-user test service-type telnet
#
interface GigabitEthernet0/0/3
 ip address 1.2.3.254 255.255.255.0
#
telnet server enable
#
user-interface vty 0 4
 authentication-mode aaa
#
return
```



4.3.5 Вопросы

1. После настройки сервера NAT должны ли порты назначения до преобразования соответствовать портам назначения после преобразования?

5

Конфигурирование основных сетевых служб

5.1 Лабораторная работа 1. Настройка FTP

5.1.1 Общая информация

5.1.1.1 О лабораторной работе

Для управления файлами используются несколько режимов, включая протокол передачи файлов (File Transfer Protocol, FTP), простейший протокол передачи файлов (Trivial File Transfer Protocol, TFTP) и безопасный протокол передачи файлов (Secure File Transfer Protocol, SFTP). Вам необходимо выбрать один, исходя из требований к обслуживанию и безопасности.

Устройство может работать как сервер или как клиент.

- Если устройство выполняет функции сервера, то для управления файлами можно получить к нему доступ с клиента и передавать файлы между клиентом и устройством.
- Если устройство работает как клиент, то для управления и передачи файлов можно получить доступ к другому устройству (серверу) с устройства.

5.1.1.2 Цели

Лабораторная работа помогает получить практические навыки по изучению следующих тем:

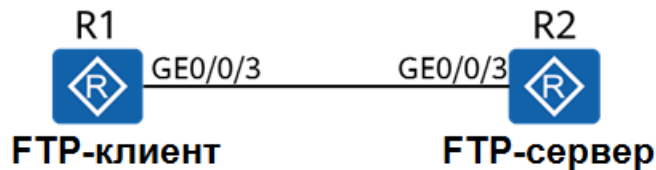
- Установление FTP-соединения
- Настройка параметров FTP-сервера
- Процедура передачи файлов на FTP-сервер

5.1.1.3 Топология сети

Необходимо на R1 выполнить операции с конфигурационным файлом R2.

R1 функционирует как FTP-клиент, а R2 — как FTP-сервер.

Рис. 5-1 Топология сети для конфигурирования FTP, используемая в данной лабораторной работе



5.1.2 Лабораторная работа

5.1.2.1 План работы

1. Настройка функции и параметров FTP-сервера.
2. Настройка локальных пользователей FTP.
3. Вход в систему FTP-сервера с FTP-клиента.
4. Выполнение операций с файлами в FTP-клиенте.

5.1.2.2 Процедура конфигурирования

Шаг 1 Настройте основные параметры устройств.

Задайте имена устройствам.

Подробности данной операции здесь не приводятся.

Настройте IP-адреса устройств.

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.0.12.1 24
```

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 10.0.12.2 24
[R2-GigabitEthernet0/0/3]quit
```

Сохраните конфигурационный файл для последующей проверки.

```
<R1>save test1.cfg
Are you sure to save the configuration to test1.cfg? (y/n)[n]:y
It will take several minutes to save configuration file, please wait.....
Configuration file had been saved successfully
Note: The configuration file will take effect after being activated
```

```
<R2>save test2.cfg
Are you sure to save the configuration to test2.cfg? (y/n)[n]:y
It will take several minutes to save configuration file, please wait.....
Configuration file had been saved successfully
Note: The configuration file will take effect after being activated
```

Выведите на экран текущий список файлов.

```
<R1>dir
Directory of flash:/
```

Idx	Attr	Size(Byte)	Date	Time(LMT)	FileName
0	-rw-	126,538,240	Jul 04 2016	17:57:22	ar651c- v300r019c00Sspc100.cc
1	-rw-	23,963	Feb 21 2020	09:22:53	mon_file.txt
2	-rw-	721	Feb 21 2020	10:14:33	vrpcfg.zip
3	drw-	-	Jul 04 2016	18:51:04	CPM_ENCRYPTED_FOLDER
4	-rw-	783	Jul 10 2018	14:46:16	default_local.cer
5	-rw-	0	Sep 11 2017	00:00:54	brdxpon_snmp_cfg.efs
6	drw-	-	Sep 11 2017	00:01:22	update
7	drw-	-	Sep 11 2017	00:01:48	shelldir
8	drw-	-	Feb 20 2020	21:33:16	localuser
9	drw-	-	Sep 15 2017	04:35:52	dhcp
10	-rw-	509	Feb 21 2020	10:18:31	private-data.txt
11	-rw-	2,686	Dec 19 2019	15:05:18	mon_lpu_file.txt
12	-rw-	3,072	Dec 18 2019	18:15:54	Boot_LogFile
13	-rw-	1,390	Feb 21 2020	10:18:30	test1.cfg

510,484 KB total available (386 448 KB free)

```
<R2>dir
Directory of flash:/
```

Idx	Attr	Size(Byte)	Date	Time(LMT)	FileName
0	-rw-	126,538,240	Jul 04 2016	17:57:22	ar651c- v300r019c00Sspc100.cc
1	-rw-	11,405	Feb 21 2020	09:21:53	mon_file.txt
2	-rw-	809	Feb 21 2020	10:14:10	vrpcfg.zip
3	drw-	-	Jul 04 2016	18:51:04	CPM_ENCRYPTED_FOLDER
4	-rw-	782	Jul 10 2018	14:48:14	default_local.cer
5	-rw-	0	Oct 13 2017	15:36:32	brdxpon_snmp_cfg.efs
6	drw-	-	Oct 13 2017	15:37:00	update
7	drw-	-	Oct 13 2017	15:37:24	shelldir
8	drw-	-	Feb 20 2020	20:51:34	localuser
9	drw-	-	Oct 14 2017	11:27:04	dhcp
10	-rw-	1,586	Feb 21 2020	10:16:51	test2.cfg
11	-rw-	445	Feb 21 2020	10:16:52	private-data.txt
12	-rw-	4,096	Aug 06 2019	11:19:08	Boot_LogFile

510,484 KB total available (386 464 KB free)
The configuration files of the two devices are saved successfully.

Шаг 2 Настройте функцию и параметры FTP-сервера на R2.

```
[R2]ftp server enable
Info: Succeeded in starting the FTP server
```

Команда **ftp server enable** позволяет включить функцию FTP-сервера. По умолчанию эта функция отключена.

К необязательным параметрам конфигурации относятся номер порта FTP-сервера, IP-адрес источника FTP-сервера и максимальное время простоя FTP-подключений.

Шаг 3 Настройте локальных пользователей FTP.

```
[R2]aaa
[R2-aaa]local-user ftp-client password irreversible-cipher Huawei@123
Info: Add a new user.
[R2-aaa]local-user ftp-client service-type ftp
[R2-aaa]local-user ftp-client privilege level 15
```

Был определен уровень пользователя. Чтобы гарантировать успешное установление соединения, пользователю необходимо настроить уровень 3 или выше.

```
[R2-aaa]local-user ftp-client ftp-directory flash:/
```

Определен авторизованный каталог пользователя FTP. Этот каталог должен быть настроен. В противном случае пользователь FTP не сможет войти в систему.

Шаг 4 Выполните вход в систему FTP-сервера с FTP-клиента.

Выполните вход в FTP-клиент.

```
<R1>ftp 10.0.12.2
Trying 10.0.12.2 ...

Press CTRL+K to abort
Connected to 10.0.12.2.
220 FTP service ready.
User(10.0.12.2:(none)):ftp-client
331 Password required for ftp-client.
Enter password:
230 User logged in.

[R1-ftp]
You have logged in to the file system of R2.
```

Шаг 5 Выполните операции в файловой системе на R2.

Настройте режим передачи.

```
[R1-ftp]ascii
200 Type set to A.
```

Файлы могут передаваться в режиме ASCII или двоичном режиме.

Режим ASCII используется для передачи простых текстовых файлов, а двоичный режим используется для передачи файлов приложений, таких как системное программное обеспечение, изображения, видеофайлы, сжатые файлы и файлы баз данных. Загружаемый файл конфигурации представляет собой текстовый файл. Поэтому необходимо установить режим ASCII. По умолчанию для передачи файлов используется режим ASCII. Эта операция показана только с целью обучения.

Загрузите конфигурационный файл.

```
[R1-ftp]get test2.cfg
200 Port command okay.
150 Opening ASCII mode data connection for test2.cfg.
226 Transfer complete.
FTP: 961 byte(s) received in 0.220 second(s) 4.36Kbyte(s)/sec.
```

Удалите конфигурационный файл.

```
[R1-ftp]delete test2.cfg
```



```
Warning: The contents of file test2.cfg cannot be recycled. Continue? (y/n)[n]:y
250 DELE command successful.
```

Выгрузите конфигурационный файл.

```
[R1-ftp]put test1.cfg
200 Port command okay.
150 Opening ASCII mode data connection for test1.cfg.
226 Transfer complete.
FTP: 875 byte(s) sent in 0.240 second(s) 3.64Kbyte(s)/sec.
```

Закройте FTP-соединение.

```
[R1-ftp]bye
221 Server closing.

<R1>
```

----Конец

5.1.3 Проверка

Выведите на экран файловые каталоги маршрутизаторов R1 и R2.

```
<R1>dir
Directory of flash:/

Idx  Attr   Size(Byte)    Date   Time(LMT)    FileName
  0  -rw-   126,538,240   Jul 04 2016 17:57:22  ar651c- v300r019c00Sspc100.cc
  1  -rw-      23,963    Feb 21 2020 09:22:53  mon_file.txt
  2  -rw-       721    Feb 21 2020 10:14:33  vrpcfg.zip
  3  drw-        -    Jul 04 2016 18:51:04  CPM_ENCRYPTED_FOLDER
  4  -rw-       783    Jul 10 2018 14:46:16  default_local.cer
  5  -rw-        0    Sep 11 2017 00:00:54  brdxpon_snmp_cfg.efs
  6  drw-        -    Sep 11 2017 00:01:22  update
  7  drw-        -    Sep 11 2017 00:01:48  shelldir
  8  drw-        -    Feb 20 2020 21:33:16  localuser
  9  drw-        -    Sep 15 2017 04:35:52  dhcp
 10  -rw-     1,586    Feb 21 2020 10:26:10  test2.cfg
 11  -rw-       509    Feb 21 2020 10:18:31  private-data.txt
 12  -rw-     2,686   Dec 19 2019 15:05:18  mon_lpu_file.txt
 13  -rw-     3,072   Dec 18 2019 18:15:54  Boot_LogFile
 14  -rw-     1,390    Feb 21 2020 10:18:30  test1.cfg

510,484 KB total available (386 444 KB free)
```

```
<R2>dir
Directory of flash:/

Idx  Attr   Size(Byte)    Date Time(LMT)    FileName
  0  -rw-   126,538,240   Jul 04 2016 17:57:22  ar651c- v300r019c00Sspc100.cc
  1  -rw-     11,405    Feb 21 2020 09:21:53  mon_file.txt
  2  -rw-       809    Feb 21 2020 10:14:10  vrpcfg.zip
  3  drw-        -    Jul 04 2016 18:51:04  CPM_ENCRYPTED_FOLDER
  4  -rw-       782    Jul 10 2018 14:48:14  default_local.cer
```




5	-rw-	0	Oct 13 2017 15:36:32	brdxpon_snmp_cfg.efs
6	drw-	-	Oct 13 2017 15:37:00	update
7	drw-	-	Oct 13 2017 15:37:24	shelldir
8	drw-	-	Feb 20 2020 20:51:34	localuser
9	drw-	-	Oct 14 2017 11:27:04	dhcp
10	-rw-	1,390	Feb 21 2020 10:25:42	test1.cfg
11	-rw-	445	Feb 21 2020 10:16:52	private-data.txt
12	-rw-	4,096	Aug 06 2019 11:19:08	Boot_LogFile

510,484 KB total available (386 464 KB free)

5.1.4 Справочные конфигурации

Конфигурация на R1

```
#
sysname R1
#
interface GigabitEthernet0/0/3
ip address 10.0.12.1 255.255.255.0
#
return
```

Конфигурация на R2

```
#
sysname R2
#
aaa
local-user ftp-client password irreversible-
cipher %^%#XqV;f=C;/1!sQ6LA+Ow8GBO;W%oHBfo`>p(`[SpV]J%Amom!na3:4RvFv@%^%#
local-user ftp-client privilege level 15
local-user ftp-client ftp-directory flash:/
local-user ftp-client service-type ftp
#
interface GigabitEthernet0/0/3
ip address 10.0.12.2 255.255.255.0
#
ftp server enable
#
user-interface vty 0 4
authentication-mode aaa
user privilege level 15
#
return
```

5.1.5 Вопросы

1. В активном или пассивном режиме работает FTP по умолчанию?

5.2 Лабораторная работа 2. Конфигурирование DHCP

5.2.1 Общая информация

5.2.1.1 О лабораторной работе

Протокол динамической настройки узла (Dynamic Host Configuration Protocol, DHCP) позволяет хостам в сети автоматически получать IP-адреса и другие настройки, обеспечивая динамическое конфигурирование и унифицированное управление IP-адресами. Это упрощает развертывание и горизонтальное масштабирование даже для небольших сетей.

Протокол DHCP определен в стандарте RFC 2131 и использует режим связи клиент/сервер. Клиент (DHCP-клиент) запрашивает конфигурационную информацию у сервера (DHCP-сервера), и сервер отправляет нужные клиенту настройки.

DHCP поддерживает динамическое и статическое назначение IP-адресов.

- Динамическое назначение: DHCP назначает клиенту IP-адрес на определенный срок (это называется арендой адреса). Такой механизм применяется в сценариях, когда хосты временно подключаются к сети, а количество свободных IP-адресов меньше общего количества хостов.
- Статическое назначение: DHCP назначает клиентам постоянные IP-адреса из настроенного диапазона. По сравнению с ручной настройкой IP-адреса статическое назначение DHCP позволяет предотвратить ошибки, которые могут возникнуть в результате неправильных действий при ручной настройке, и обеспечивает унифицированное обслуживание и управление.

5.2.1.2 Цели

Лабораторная работа помогает получить практические навыки по изучению следующих тем:

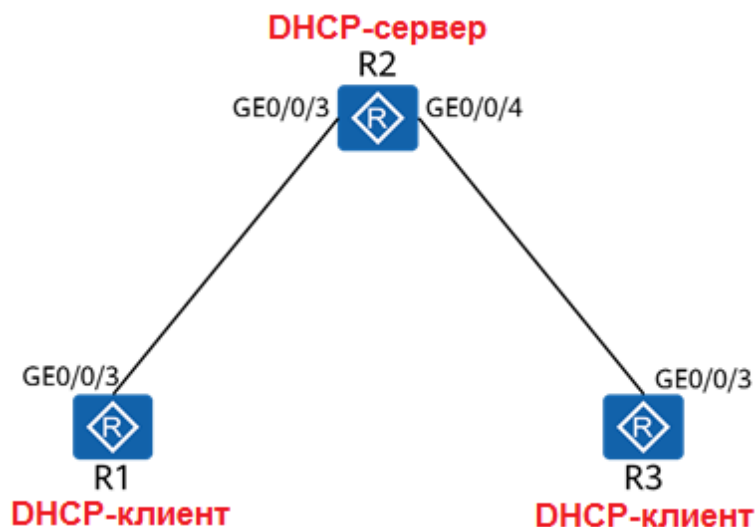
- Настройка пула адресов интерфейса на DHCP-сервере.
- Настройка глобального пула адресов на DHCP-сервере.
- Использование DHCP для статического назначения IP-адресов.

5.2.1.3 Топология сети

Чтобы оптимизировать использование IP-адресов, предприятие планирует развернуть DHCP в сети.

1. Для этого необходимо настроить маршрутизаторы R1 и R3 в качестве DHCP-клиентов.
2. А также необходимо настроить маршрутизатор R2 в качестве DHCP-сервера для назначения IP-адресов R1 и R3.

Рис. 5-2 Топология сети для конфигурирования DHCP, используемая в данной лабораторной работе



5.2.2 Лабораторная работа

5.2.2.1 План работы

1. Настройка DHCP-сервера.
2. Настройка DHCP-клиентов.

5.2.2.2 Процедура конфигурирования

Шаг 1 Настройте основные параметры.

Настройте на маршрутизаторе R2 адреса интерфейсов.

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3] ip address 10.0.12.2 24
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ip address 10.0.23.2 24
[R2-GigabitEthernet0/0/4]quit
```

Шаг 2 Включите функцию DHCP.

```
[R1]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
```

Команду **dhcp enable** необходимо выполнять перед выполнением других команд, связанных с DHCP, независимо от того, предназначены эти команды для DHCP-серверов или DHCP-клиентов.

```
[R2]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
```

```
[R3]dhcp enable
```

Info: The operation may take a few seconds. Please wait for a moment.done.

Шаг 3 Настройте пул адресов.

Настройте пул IP-адресов на GE 0/0/3 маршрутизатора R2 для назначения IP-адреса маршрутизатору R1.

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]dhcp select interface
```

Команда **dhcp select interface** позволяет интерфейсу использовать пул адресов интерфейса. Без выполнения этой команды вам не удастся настроить параметры, относящиеся к пулу адресов интерфейса.

```
[R2-GigabitEthernet0/0/3]dhcp server dns-list 10.0.12.2
```

Команда **dhcp server dns-list** позволяет настраивает адреса DNS-серверов для пула адресов интерфейса. Можно настроить до восьми адресов DNS-серверов. Эти IP-адреса разделяются пробелами.

Настройте глобальный пул адресов.

```
[R2]ip pool GlobalPool
Info: It's successful to create an IP address pool.
# Создайте пул IP-адресов с названием GlobalPool.
[R2-ip-pool-GlobalPool]network 10.0.23.0 mask 24
```

Команда **network** позволяет указать сетевой адрес для глобального пула адресов.

```
[R2-ip-pool-GlobalPool]dns-list 10.0.23.2
[R2-ip-pool-GlobalPool]gateway-list 10.0.23.2
```

Команда **gateway-list** позволяет настроить адрес шлюза для DHCP-клиента. После того, как R3 получает IP-адрес, он генерирует маршрут по умолчанию с адресом следующего перехода 10.0.23.2.

```
[R2-ip-pool-GlobalPool]lease day 2 hour 2
```

Команда **lease** позволяет настроить аренду IP-адресов в глобальном пуле IP-адресов. Если срок аренды имеет значение **unlimited**, значит, он не ограничен. По умолчанию аренда IP-адресов составляет один день.

```
[R2-ip-pool-GlobalPool]static-bind ip-address 10.0.23.3 mac-address 00e0-fc6f-6d1f
```

Команда **static-bind** позволяет установить привязку IP-адреса в глобальном пуле адресов к MAC-адресу клиента. 00e0-fc6f-6d1f — это MAC-адрес GigabitEthernet0/0/3 на маршрутизаторе R3. Чтобы вывести на экран MAC-адрес GigabitEthernet0/0/3, можно выполнить команду **display interface GigabitEthernet0/0/3** на маршрутизаторе R3. После выполнения команды R3 получит постоянный IP-адрес 10.0.23.3.

```
[R2-ip-pool-GlobalPool]quit
```

Шаг 4 Включите функцию DHCP-сервера на GigabitEthernet 0/0/4 маршрутизатора R2 для назначения IP-адреса маршрутизатору R3.

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]dhcp select global
```

Команда **dhcp select global** позволяет интерфейсу использовать глобальный пул адресов. После получения запроса от DHCP-клиента интерфейс ищет в глобальном пуле адресов доступный IP-адрес и назначает его DHCP-клиенту.

Шаг 5 Настройте DHCP-клиенты.

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3] ip address dhcp-alloc
```

```
[R3]interface GigabitEthernet 0/0/3
[R3-GigabitEthernet0/0/3] ip address dhcp-alloc
```

----Конец

5.2.3 Проверка

5.2.3.1 Вывод на экран IP-адресов и маршрутов R1 и R3

```
[R1]display ip interface brief
Interface                               IP Address/Mask      Physical  Protocol
GigabitEthernet0/0/3                   10.0.12.254/24       up        up
Здесь представлена только основная информация. Из командного вывода видно, что R1 получил IP-адрес.
```

```
[R1]display dns server
```

Type:

D:Dynamic S:Static

No.	Type	IP Address
1	D	10.0.12.2

Здесь представлена только основная информация. Из командного вывода видно, что R1 получил DNS-адрес.

```
[R1]display ip routing-table
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
0.0.0.0/0	Unr	60	0	D	10.0.12.2	GigabitEthernet0/0/3

Здесь представлена только основная информация. Из командного вывода видно, что R1 получил маршрут по умолчанию.

```
[R3]display ip interface brief
Interface                               IP Address/Mask      Physical  Protocol
GigabitEthernet0/0/3                   10.0.23.3/24         up        up
```

Здесь представлена только основная информация. Из командного вывода видно, что R3 получил постоянный IP-адрес.

```
[R3]display dns server
```

Type:

D:Dynamic S:Static

No.	Type	IP Address
1	D	2.23.0.10

Здесь представлена только основная информация. Из командного вывода видно, что R3 получил DNS-адрес.

```
[R3]display ip routing-table
```

Route Flags: R - relay, D - download to fib

Routing Tables: Public

Destinations : 8 Routes : 8



Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
0.0.0.0/0	Unr	60	0	D	10.0.23.2	GigabitEthernet0/0/3

Здесь представлена только основная информация. Из командного вывода видно, что R3 получил маршрут по умолчанию.

5.2.3.2 Вывод на экран информации о назначении адресов на R2

```
[R2]display ip pool name GlobalPool
```

Pool-name	: GlobalPool						
Pool-No	: 1						
Lease	: 2 Days 2 Hours 0 Minutes						
Domain-name	: -						
DNS-servero	: 10.0.23.2						
NBNS-servero	: -						
Netbios-type	: -						
Position	: Local	Status	: Unlocked				
Gateway-o	: 10.0.23.2						
Mask	: 255.255.255.0						
VPN instance	: --						

Start	End	Total	Used	Idle(Expired)	Conflict	Disable
10.0.23.1	10.0.23.254	253	1	252(0)	0	0

Команда **display ip pool** позволяет вывести на экран информацию о настройках пула адресов, включая имя, аренду, статус блокировки и статус IP-адреса.

```
[R2]display ip pool interface GigabitEthernet0/0/4
```

Pool-name	: GigabitEthernet0/0/4						
Pool-No	: 0						
Lease	: 1 Days 0 Hours 0 Minutes						
Domain-name	: -						
DNS-servero	: 10.0.12.2						
NBNS-servero	: -						
Netbios-type	: -						
Position	: Interface	Status	: Unlocked				
Gateway-o	: 10.0.12.2						
Mask	: 255.255.255.0						
VPN instance	: --						

Start	End	Total	Used	Idle(Expired)	Conflict	Disable
10.0.12.1	10.0.12.254	253	1	252(0)	0	0

После настройки пула адресов интерфейса он получает имя интерфейса. Назначенный адрес шлюза является IP-адресом интерфейса и не может быть изменен.

5.2.4 Справочные конфигурации

Конфигурация на R1

```
#
sysname R1
#
```

```
dhcp enable
#
interface GigabitEthernet0/0/3
 ip address dhcp-alloc
#
return
```

Конфигурация на R2

```
#
 sysname R2
#
dhcp enable
#
ip pool GlobalPool
 gateway-list 10.0.23.2
 network 10.0.23.0 mask 255.255.255.0
 static-bind ip-address 10.0.23.3 mac-address a008-6fe1-0c47
 lease day 2 hour 2 minute 0
 dns-list 10.0.23.2
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.2 255.255.255.0
 dhcp select interface
 dhcp server dns-list 10.0.12.2
#
interface GigabitEthernet0/0/4
 ip address 10.0.23.2 255.255.255.0
 dhcp select global
#
return
```

Конфигурация на R3

```
#
 sysname R3
#
dhcp enable
#
interface GigabitEthernet0/0/3
 ip address dhcp-alloc
#
return
```

5.2.5 Вопросы

1. В чем разница между глобальным пулом адресов и пулом адресов интерфейса?
2. Как определить глобальный пул адресов для DHCP-клиента, если существует несколько глобальных пулов адресов?

6

Создание WLAN

6.1 Общая информация

6.1.1 О лабораторной работе

К основным недостаткам проводных локальных сетей можно отнести дороговизну создания и расширения, а также отсутствие мобильности сетевых устройств. Чтобы удовлетворить растущий спрос на портативность и мобильность устройств, необходимо использовать технологии беспроводной локальной сети (WLAN). В настоящее время WLAN является наиболее экономичным и удобным режимом сетевого доступа. Технология WLAN обеспечивает пользователям возможность свободного перемещения в зоне ее покрытия, устраняя ограничения проводных сетей.

В этой лабораторной работе вы научитесь конфигурировать WLAN с помощью контроллера доступа (AC) и точек доступа Fit AP.

6.1.2 Цели

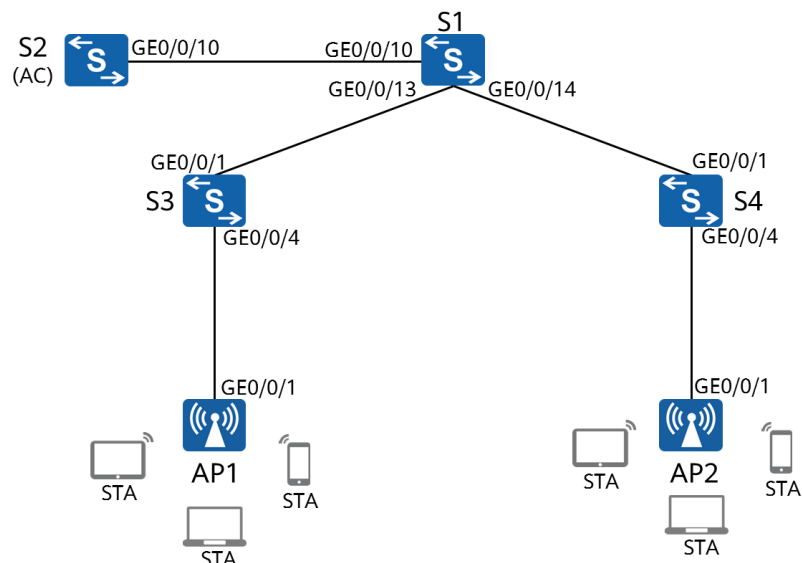
Лабораторная работа помогает получить практические навыки по изучению следующих тем:

- Процедура аутентификации точек доступа
- Процедура настройки профилей WLAN
- Процесс настройки основных параметров WLAN

6.1.3 Топология сети

1. Коммутатор S2 должен поддерживать функцию WLAN-AC. Если коммутатор не поддерживает функцию WLAN-AC, то вместо него можно использовать обычный контроллер доступа (AC). В данном случае функции AC выполняет коммутатор S2.
2. AC развернут в режиме «Out-of-path» (вне пути прохождения трафика) и находится в той же сети уровня 2, что и точки доступа (AP).
3. AC и S1 работают как DHCP-серверы. AC назначает IP-адреса AP, а S1 назначает IP-адреса станциям (STA).
4. Служебные данные передаются напрямую.

Рис. 6-1 Топология сети для создания WLAN, используемая в данной лабораторной работе



6.1.4 Планирование данных

Предприятию необходимо создать WLAN, чтобы обеспечить мобильность рабочих мест для сотрудников.

Табл. 6-1 Планирование данных AC

Элемент	Конфигурация
VLAN для управления AP	VLAN100
Сервисная VLAN	VLAN101
DHCP-сервер	AC выполняет функции DHCP-сервера, который назначает IP-адреса AP. S1 выполняет функции DHCP-сервера, который назначает IP-адреса STA. По умолчанию для STA используется адрес шлюза 192.168.101.254.
Пул IP-адресов для AP	192.168.100.1–192.168.100.253/24
Пул IP-адресов для STA	192.168.101.1–192.168.101.253/24
IP-адрес интерфейса-источника AC	VLANIF100: 192.168.100.254/24
Группа AP	Имя: ap-group1 Ссылочные профили: профиль VAP HCIA-WLAN и профиль регулирующего домена default

Элемент	Конфигурация
Профиль регулирующего домена	Имя: default
	Код страны: CN
Профиль SSID	Имя: HCIA-WLAN
	Имя SSID: HCIA-WLAN
Профиль безопасности	Имя: HCIA-WLAN
	Политика безопасности: WPA-WPA2+PSK+AES
	Пароль: HCIA-Datcom
Профиль VAP	Имя: HCIA-WLAN
	Режим передачи: прямая передача
	Сервисная VLAN: VLAN 101
	Ссылочные профили: профиль SSID HCIA-WLAN и профиль безопасности HCIA-WLAN

6.2 Лабораторная работа

6.2.1 План работы

1. Настройка подключения к проводной сети.
2. Настройка точек доступа и перевод их в режим онлайн.
 - (1) Создание групп точек доступа и добавление точек доступа с одинаковой конфигурацией в одну группу для унифицированной настройки.
 - (2) Настройка системных параметров контроллера доступа, включая код страны и интерфейс-источник, используемый контроллером для связи с точками доступа.
 - (3) Настройка режима аутентификации AP и импорт AP для выхода точек доступа в сеть.
3. Настройка параметров сервисов WLAN и передача конфигурации точкам доступа, чтобы обеспечить доступ STA к WLAN.

6.2.2 Процедура конфигурирования

Шаг 1 Настройте основные параметры устройства.

Присвойте имена устройствам (назовите S2 в топологии **AC**).

Подробности данной операции здесь не приводятся.

Отключите ненужные порты между S1 и AC. Этот шаг можно выполнять только в среде, описанной в *Руководстве по выполнению лабораторных работ для подготовки к сертификации HCIA-Datcom V1.0*.

```
[S1] interface GigabitEthernet 0/0/11
[S1-GigabitEthernet0/0/11] shutdown
[S1-GigabitEthernet0/0/11] quit
[S1] interface GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12] shutdown
[S1-GigabitEthernet0/0/12] quit
```

Включите функцию PoE на портах S3 и S4, подключенных к точкам доступа.

```
[S3] interface GigabitEthernet 0/0/4
[S3-GigabitEthernet0/0/4] poe enable
```

Команда **poe enable** позволяет включить функцию PoE на порте. При подключении к порту питаемого устройства (PD), порт обнаруживает его и обеспечивает ему подачу питания. По умолчанию функция PoE включена. Таким образом, эту команду, как правило, выполнять не требуется, она приводится только с целью обучения.

```
[S4] interface GigabitEthernet 0/0/4
[S4-GigabitEthernet0/0/4] poe enable
```

Шаг 2 Настройте параметры проводной сети.

Настройте VLAN.

```
[S1] vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1] interface GigabitEthernet 0/0/13
[S1-GigabitEthernet0/0/13] port link-type trunk
[S1-GigabitEthernet0/0/13] port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/13] quit
[S1] interface GigabitEthernet 0/0/14
[S1-GigabitEthernet0/0/14] port link-type trunk
[S1-GigabitEthernet0/0/14] port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/14] quit
[S1] interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10] port link-type trunk
[S1-GigabitEthernet0/0/10] port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/10] quit
```

```
[AC] vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[AC] interface GigabitEthernet 0/0/10
[AC-GigabitEthernet0/0/10] port link-type trunk
[AC-GigabitEthernet0/0/10] port trunk allow-pass vlan 100 101
[AC-GigabitEthernet0/0/10] quit
```

```
[S3] vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[S3] interface GigabitEthernet 0/0/1
[S3-GigabitEthernet0/0/1] port link-type trunk
```

```
[S3-GigabitEthernet0/0/1]port trunk allow-pass vlan 100 101
[S3-GigabitEthernet0/0/1]quit
[S3]interface GigabitEthernet 0/0/4
[S3-GigabitEthernet0/0/4]port link-type trunk
[S3-GigabitEthernet0/0/4]port trunk pvid vlan 100
[S3-GigabitEthernet0/0/4]port trunk allow-pass vlan 100 101
[S3-GigabitEthernet0/0/4]quit
```

```
[S4]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[S4]interface GigabitEthernet0/0/1
[S4-GigabitEthernet0/0/1] port link-type trunk
[S4-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 101
[S4-GigabitEthernet0/0/1]quit
[S4]interface GigabitEthernet0/0/4
[S4-GigabitEthernet0/0/4] port link-type trunk
[S4-GigabitEthernet0/0/4] port trunk pvid vlan 100
[S4-GigabitEthernet0/0/4] port trunk allow-pass vlan 100 to 101
[S4-GigabitEthernet0/0/4]quit
```

Настройте IP-адреса интерфейсов.

```
[S1]interface Vlanif 101
[S1-Vlanif101]ip address 192.168.101.254 24
```

Шлюз для STA

```
[S1-Vlanif101]quit
[S1]interface LoopBack 0
[S1-LoopBack0] ip address 10.0.1.1 32
```

Эта операция показана только с целью обучения.

```
[S1-LoopBack0]quit
```

```
[AC]interface Vlanif 100
[AC-Vlanif100]ip address 192.168.100.254 24
```

Настройте DHCP.

```
[S1]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[S1]ip pool sta
Info:It's successful to create an IP address pool.
IP address pool for STAs
[S1-ip-pool-sta]network 192.168.101.0 mask 24
[S1-ip-pool-sta]gateway-list 192.168.101.254
[S1-ip-pool-sta]quit
[S1]interface Vlanif 101
[S1-Vlanif101]dhcp select global
[S1-Vlanif101]quit
```

```
[AC]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[AC]ip pool ap
Info: It is successful to create an IP address pool.
```

```
IP address pool for APs
[AC-ip-pool-ap]network 192.168.100.254 mask 24
[AC-ip-pool-ap]gateway-list 192.168.100.254
[AC-ip-pool-ap]quit
[AC]interface Vlanif 100
[AC-Vlanif100]dhcp select global
[AC-Vlanif100]quit
```

S1 является DHCP-сервером для STA, а AC — DHCP-сервером для AP.

Шаг 3 Настройте параметры точек доступа для выхода в сеть.

Создайте группу AP и назовите ее ap-group1.

```
[AC]wlan
[AC-wlan-view]ap-group name ap-group1
Info: This operation may take a few seconds. Please wait for a moment.done.
[AC-wlan-ap-group-ap-group1]quit
```

Создайте профиль регулирующего домена и настройте код страны AC в профиле.

```
[AC]wlan
[AC-wlan-view]regulatory-domain-profile name default
```

Профиль регулирующего домена предоставляет конфигурации кода страны, калибровочного канала и калибровочной полосы пропускания для точки доступа.

Профиль регулирующего домена по умолчанию называется **default**. Таким образом, на экране отображается профиль по умолчанию.

```
[AC-wlan-regulate-domain-default]country-code cn
Info: The current country code is same with the input country code.
```

Код страны определяет страну, в которой развернуты AP. В разных странах требуются разные атрибуты радиосвязи AP, включая мощность передачи и поддерживаемые каналы. Правильная конфигурация кода страны гарантирует, что атрибуты радиосвязи точек доступа будут соответствовать местным законам и правилам. По умолчанию установлен код страны CN.

```
[AC-wlan-regulate-domain-default]quit
```

Установите привязку профиля регулирующего домена к группе AP.

```
[AC]wlan
[AC-wlan-view]ap-group name ap-group1
[AC-wlan-ap-group-ap-group1]regulatory-domain-profile default
Warning: Modifying the country code will clear channel, power and antenna gain configurations of the radio and reset the AP. Continue?[Y/N]:y
```

Команда **regulatory-domain-profile** в режиме группы точек доступа используется для установления привязки профиля регулирующего домена к AP или группе AP. По умолчанию профиль регулирующего домена **default** привязан только к группе AP, а к AP не привязан. В профиле регулирующего домена по умолчанию задан код страны CN. Следовательно, калибровочные каналы 2,4 ГГц включают в себя каналы 1, 6 и 11, а калибровочные каналы 5 ГГц — каналы 149, 153, 157, 161 и 165. Этот шаг и предыдущий шаг можно пропустить.

```
[AC-wlan-ap-group-ap-group1]quit
```

Укажите интерфейс-источник на AC для установления туннелей CAPWAP.

```
[AC]capwap source interface Vlanif 100
```

Команда **capwap source interface** позволяет настроить интерфейс, используемый AC для установления туннелей CAPWAP с точками доступа.

Импортируйте точки доступа в AC и добавьте их в группу AP с именем **ap-group1**.

Добавление AP в AC может осуществляться следующими способами:

- Ручная настройка: предварительная настройка MAC-адресов и серийных номеров (SN) AP на AC. При подключении точек доступа контроллер доступа определяет, соответствуют ли их MAC-адреса и серийные номера предварительно сконфигурированным, и устанавливает с ними соединения.
- Автоматическое обнаружение: AC автоматически обнаруживает подключенные AP и, если для AP используется режим без аутентификации или аутентификации по MAC-адресу или SN, и MAC-адреса или SN содержатся в белом списке, устанавливает с ними соединения.
- Ручное подтверждение: в режиме аутентификации AP по MAC-адресам или серийным номерам, а MAC-адрес или SN подключенной AP не включен в белый список на AC, AC добавляет AP в список неавторизованных AP. Для выхода AP в сеть можно ручную подтвердить ее подлинность.

```
[AC]wlan
```

```
[AC-wlan-view]ap auth-mode mac-auth
```

Команда **ap auth-mode** используется для настройки режима аутентификации AP. Только аутентифицированные точки доступа могут подключаться к сети. Для аутентификации используются следующие режимы: аутентификация по MAC-адресу, аутентификация по SN и режим без аутентификации. В качестве режима аутентификации AP по умолчанию используется аутентификация по MAC-адресу.

Примечание: информация о MAC-адресе и серийном номере точки доступа приводится на упаковке устройства.

```
[AC-wlan-view]ap-id 0 ap-mac 60F1-8A9C-2B40
```

Команда **ap-id** используется для добавления AP или перехода в режим конфигурирования AP.

Аргумент **ap-mac** определяет аутентификацию по MAC-адресу, а аргумент **ap-sn** определяет аутентификацию по SN.

В режиме AP можно ввести **ap-id**, чтобы перейти в режим соответствующей AP.

```
[AC-wlan-ap-o]ap-name ap1
```

Командой **ap-name** можно указать имя AP. Имена AP должны быть уникальными. Если имя точки доступа не указано, то именем по умолчанию является MAC-адрес точки доступа.

```
[AC-wlan-ap-o]ap-group ap-group1
```

Команда **ap-group** позволяет настроить группу AP. AC передает конфигурацию точкам доступа. Например, при добавлении точки доступа AP1 в группу ap-group1 она получит настройки профиля регулирующего домена, профиля радиосвязи и профиля VAP, которые имеют привязку к группе ap-group1. По умолчанию точки доступа не

добавлены в группы. При добавлении AP в группу или изменении настроек группы AP контроллер доступа автоматически передаст конфигурацию группы, и AP автоматически перезапустится, чтобы присоединиться к группе.

```
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain
configurations of the radio, Whether to continue? [Y/N]:y //Введите y для подтверждения.
Info: This operation may take a few seconds. Please wait for a moment.. done.
[AC-wlan-ap-o]quit
[AC-wlan-view]ap-id 1 ap-mac B4FB-F9B7-DE40
[AC-wlan-ap-1]ap-name ap2
[AC-wlan-ap-1]ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain
configurations of the radio, Whether to continue? [Y/N]:y //Введите y для подтверждения.
Info: This operation may take a few seconds. Please wait for a moment.. done.
[AC-wlan-ap-1]quit
```

Выведите на экран информацию о текущей AP.

```
[AC]wlan
[AC-wlan-view]display ap all
Info: This operation may take a few seconds. Please wait for a moment..done.
Total AP information:
nor : normal          [2]

-----
ID   MAC                Name Group   IP                Type              State  STA  Uptime
-----
0    00e0-fc25-0edo ap1   ap-group1     192.168.100.206   AirEngine5760    nor   0    30M:4S
1    00e0-fc0f-07ao ap2   ap-group1     192.168.100.170   AirEngine5760    nor   0    31M:31S
-----
Total: 2
```

Команда **display ap** позволяет вывести на экран информацию о точке доступа, включая IP-адрес, модель (AirEngine5760), статус (normal) и продолжительность работы точки доступа в сети.

Кроме того, можно указать в команде параметр **by-state state** или **by-ssid ssid** для фильтрации AP, находящихся в определенном состоянии или использующих указанный SSID.

Из командного вывода видно, что две точки доступа работают в нормальном режиме. (Более подробное описание других состояний приводится в разделе 6.6 Приложение.)

Шаг 4 Настройте параметры сервисов WLAN.

Создайте профиль безопасности **HCIA-WLAN** и настройте политику безопасности.

```
[AC-wlan-view]security-profile name HCIA-WLAN
[AC-wlan-sec-prof-HCIA-WLAN]security wpa-wpa2 psk pass-phrase HCIA-Datcom aes
```

Команда **security psk** используется для настройки аутентификации и шифрования с помощью общего ключа (Pre-Shared Key, PSK) WPA/WPA2.

В настоящее время используются как WPA, так и WPA2. Пользовательские терминалы могут быть аутентифицированы посредством WPA или WPA2. PSK настроено значение **HCIA-Datcom**. Для шифрования пользовательских данных используется алгоритм AES.

```
[AC-wlan-sec-prof-HCIA-WLAN]quit
```

Создайте профиль SSID **HCIA-WLAN** и задайте имя SSID **HCIA-WLAN**.

```
[AC]wlan
[AC-wlan-view]ssid-profile name HCIA-WLAN
SSID profile HCIA-WLAN is created.
[AC-wlan-ssid-prof-HCIA-WLAN]ssid HCIA-WLAN
The SSID name is set to HCIA-WLAN.
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-ssid-prof-HCIA-WLAN]quit
```

Создайте профиль VAP **HCIA-WLAN**, настройте режим передачи данных и сервисную VLAN и примените профиль безопасности и профиль SSID к профилю VAP.

```
[AC]wlan
[AC-wlan-view]vap-profile name HCIA-WLAN
```

Команда **vap-profile** позволяет создавать профили VAP.

В профиле VAP можно настроить режим передачи данных и привязку профиля SSID, профиля безопасности и профиля трафика.

```
[AC-wlan-vap-prof-HCIA-WLAN]forward-mode direct-forward
```

Команда **forward-mode** позволяет настроить режим передачи данных в профиле VAP. По умолчанию установлен режим прямой передачи данных.

```
[AC-wlan-vap-prof-HCIA-WLAN]service-vlan vlan-id 101
```

Команда **service-vlan** позволяет настроить сервисную VLAN для VAP. После обращения STA к WLAN пользовательские данные, передаваемые AP, будут содержать тег **service-VLAN**.

```
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-HCIA-WLAN]security-profile HCIA-WLAN
Security profile HCIA-WLAN is bound.
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-HCIA-WLAN]ssid-profile HCIA-WLAN
SSID profile HCIA-WLAN is bound.
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-HCIA-WLAN]quit
```

Установите привязку профиля VAP к группе AP и примените конфигурацию профиля VAP **HCIA-WLAN** к радиомодулю 0 и радиомодулю 1 точек доступа в группе AP.

```
[AC]wlan
[AC-wlan-view]ap-group name ap-group1
[AC-wlan-ap-group-ap-group1]vap-profile HCIA-WLAN wlan 1 radio all
```

Команда **vap-profile** позволяет установить привязку профиля VAP к радиомодулю. После выполнения этой команды все конфигурации в VAP, включая настройки профилей, привязанных к VAP, будут переданы радиомодулям точек доступа.

```
Info: This operation may take a few seconds, please wait...done.
[AC-wlan-ap-group-ap-group1]quit
```

----Конец

6.3 Проверка

1. С помощью STA попробуйте подключиться к WLAN с SSID **HCIA-WLAN**.
Посмотрите IP-адрес, полученный STA, и выполните проверку связи с помощью команды ping с IP-адресом (10.0.1.1) порта LoopBacko на S1.
2. После подключения STA к AC выполните команду **display station all** на AC, чтобы проверить информацию STA.

6.4 Справочные конфигурации

Конфигурация на S1

```
#
sysname S1
#
vlan batch 100 to 101
#
dhcp enable
#
ip pool sta
 gateway-list 192.168.101.254
 network 192.168.101.0 mask 255.255.255.0
#
interface Vlanif101
 ip address 192.168.101.254 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/10
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/12
#
interface GigabitEthernet0/0/13
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/14
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
return
```

Конфигурация на контроллере доступа

```
#
sysname AC
#
vlan batch 100 to 101
#
```

```
dhcp enable
#
ip pool ap
 gateway-list 192.168.100.254
 network 192.168.100.0 mask 255.255.255.0
#
interface Vlanif100
 ip address 192.168.100.254 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/10
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
wlan
 security-profile name HCIA-WLAN
  security wpa-wpa2 psk pass-phrase %^%#V-rr;CTW$X%,nJ/ojcmO!tRQ(pt;^8IN,z1||UU)%^%# aes
 ssid-profile name HCIA-WLAN
  ssid HCIA-WLAN
 vap-profile name HCIA-WLAN
  service-vlan vlan-id 101
  ssid-profile HCIA-WLAN
  security-profile HCIA-WLAN
 ap-group name ap-group1
  radio 0
   vap-profile HCIA-WLAN wlan 1
  radio 1
   vap-profile HCIA-WLAN wlan 1
  radio 2
   vap-profile HCIA-WLAN wlan 1
 ap-id 0 type-id 75 ap-mac 60f1-8a9c-2b40 ap-sn 21500831023GJ9022622
 ap-name ap1
 ap-group ap-group1
 ap-id 1 type-id 75 ap-mac b4fb-f9b7-de40 ap-sn 21500831023GJ2001889
 ap-name ap2
 ap-group ap-group1
 provision-ap
#
return
```

Конфигурация на S3

```
#
sysname S3
#
vlan batch 100 to 101
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
```

```
return
```

Конфигурация на S4

```
#
sysname S4
#
vlan batch 100 to 101
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
return
```

6.5 Вопросы

1. Какое влияние на доступ STA к S1 в текущей сети будут оказывать настройки порта GigabitEthernet0/0/10 контроллера доступа, запрещающие прохождение пакетов из VLAN 101? Почему? Что изменится, если будет использоваться туннельная передача?
2. Какие операции необходимо выполнить на AC, чтобы назначить STA, подключенные к AP1 и AP2, к разным VLAN?

6.6 Приложение

Статус AP	Описание
commit-failed	После перехода AP в режим онлайн на AC она не может получить сервисные конфигурации WLAN.
committing	После перехода AP в режим онлайн на AC она получает сервисные конфигурации WLAN.
config	AP получает сервисные конфигурации WLAN при переходе в режим онлайн на AC.
config-failed	При переходе AP в режим онлайн на AC она не может получить сервисные конфигурации WLAN.
download	AP находится в процессе обновления.
fault	AP не может перейти в режим онлайн.
idle	AP находится в процессе инициализации перед установлением соединения между ней и контроллером доступа в первый раз.

Статус AP	Описание
name-conflicted	Конфликт имен двух AP.
normal	AP работает исправно.
standby	AP находится в нормальном состоянии на резервном AC.
unauth	AP не аутентифицирована.

7

Создание сети IPv6

7.1 Общая информация

7.1.1 О лабораторной работе

Интернет-протокол версии 6 (Internet Protocol Version 6, IPv6), также называемый интернет-протоколом следующего поколения (IP Next Generation, IPng), был разработан сообществом IETF (Internet Engineering Task Force) для решения проблем, с которыми столкнулась предыдущая версия IPv4.

IPv6 имеет следующие преимущества перед IPv4:

- Практически бесконечное адресное пространство
- Иерархическая структура адресов
- Автоматическая настройка
- Упрощенный заголовок пакета
- Высокий уровень безопасности
- Обеспечение мобильности
- Расширенные функции QoS

В этом разделе описываются методы настройки сети IPv6, которые помогут вам понять основные принципы назначения адресов IPv6.

7.1.2 Цели

Лабораторная работа помогает получить практические навыки по изучению следующих тем:

- Настройка статических адресов IPv6
- Настройка сервера DHCPv6
- Настройка адресов без отслеживания состояния
- Настройка статических маршрутов IPv6
- Способы просмотра информации IPv6

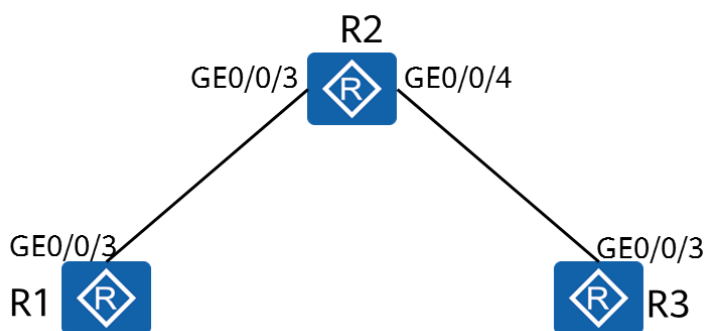
7.1.3 Топология сети

Предприятию требуется развернуть IPv6 в своей сети.

1. Настройте статические IPv6-адреса двум интерфейсам маршрутизатора R2.

2. Настройте автоконфигурацию адреса без отслеживания состояния на GigabitEthernet0/0/3 маршрутизатора R1.
3. Настройте IPv6-адрес для GigabitEthernet0/0/3 маршрутизатора R3 с помощью DHCPv6.

Рис. 7-1 Топология сети для создания сети IPv6, используемая в данной лабораторной работе



7.2 Лабораторная работа

7.2.1 План работы

1. Настройка статических адресов IPv6.
2. Настройка сервера DHCPv6.
3. Настройка назначения адресов IPv6 без отслеживания состояния.
4. Вывод на экран адресов IPv6.

7.2.2 Процедура конфигурирования

Шаг 1 Настройте основные параметры устройств.

Задайте имена устройствам.

Подробности данной операции здесь не приводятся.

Шаг 2 Настройте функции IPv6 на устройствах и интерфейсах.

Включите IPv6 глобально.

```
[R1]ipv6
```

С помощью команды **ipv6** можно настроить устройство на передачу одноадресных пакетов IPv6, включая отправку и получение локальных пакетов IPv6.

```
[R2]ipv6
```

```
[R3]ipv6
```

Включите IPv6 на интерфейсе.

```
[R1]interface GigabitEthernet 0/0/3
```

Команда **ipv6 enable** позволяет включить функцию IPv6 на интерфейсе.

```
[R1-GigabitEthernet0/0/3]ipv6 enable  
[R1-GigabitEthernet0/0/3]quit
```

```
[R2]interface GigabitEthernet 0/0/3  
[R2-GigabitEthernet0/0/3]ipv6 enable  
[R2-GigabitEthernet0/0/3]quit  
[R2]interface GigabitEthernet 0/0/4  
[R2-GigabitEthernet0/0/4]ipv6 enable  
[R2-GigabitEthernet0/0/4]quit
```

```
[R3]interface GigabitEthernet 0/0/3  
[R3-GigabitEthernet0/0/3]ipv6 enable  
[R3-GigabitEthernet0/0/3]quit
```

Шаг 3 Настройте локальный адрес канала (link-local address) для интерфейса и проверьте конфигурацию.

Настройте на интерфейсе автоматическое генерирование локального адреса канала (link-local address).

```
[R1]interface GigabitEthernet 0/0/3
```

Команда **ipv6 address auto link-local** позволяет включить функцию генерирования локального адреса канала (link-local address) на интерфейсе.

Для каждого интерфейса можно настроить только один локальный адрес канала (link-local address). Рекомендуется использовать функцию автоматического генерирования локального адреса канала (link-local address) во избежание конфликтов этих адресов. После настройки глобального IPv6-адреса одноадресной рассылки интерфейс автоматически сгенерирует локальный адрес канала (link-local address).

```
[R1-GigabitEthernet0/0/3]ipv6 address auto link-local  
[R1-GigabitEthernet0/0/3]quit
```

```
[R2]interface GigabitEthernet 0/0/3  
[R2-GigabitEthernet0/0/3]ipv6 address auto link-local  
[R2-GigabitEthernet0/0/3]quit  
[R2]interface GigabitEthernet 0/0/4  
[R2-GigabitEthernet0/0/4]ipv6 address auto link-local  
[R2-GigabitEthernet0/0/4]quit
```

```
[R3]interface GigabitEthernet 0/0/3  
[R3-GigabitEthernet0/0/3]ipv6 address auto link-local  
[R3-GigabitEthernet0/0/3]quit
```

Выведите на экран IPv6-статус интерфейса и проверьте возможность подключения.



```
<R1>display ipv6 interface GigabitEthernet 0/0/3
GigabitEthernet0/0/3 current state : UP
IPv6 protocol current state : UP //Физический статус и статус протокола — Up.
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE4D:355 //Локальный адрес канала (link-local address) для
интерфейса сгенерирован.
No global unicast address configured
Joined group address(es):
  FF02::1:FF4D:355
  FF02::2
  FF02::1
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
```

```
<R2>display ipv6 interface GigabitEthernet 0/0/3
GigabitEthernet0/0/3 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE12:6486
No global unicast address configured
Joined group address(es):
  FF02::1:FF12:6486
  FF02::2
  FF02::1
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
```

```
<R2>display ipv6 interface GigabitEthernet 0/0/4
GigabitEthernet0/0/4 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE12:6487
No global unicast address configured
Joined group address(es):
  FF02::1:FF12:6487
  FF02::2
  FF02::1
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
```

```
<R3>display ipv6 interface GigabitEthernet 0/0/3
GigabitEthernet0/0/4 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE3C:5133
No global unicast address configured
Joined group address(es):
```



```
FF02::1:FF3C:5133
FF02::2
FF02::1
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
```

Проверьте сетевое соединение между маршрутизаторами R1 и R2.

```
<R1>ping ipv6 FE80::2E0:FCFF:FE12:6486 -i GigabitEthernet 0/0/3
PING FE80::2E0:FCFF:FE12:6486 : 56 data bytes, press CTRL_C to break
Reply from FE80::2E0:FCFF:FE12:6486
bytes=56 Sequence=1 hop limit=64 time = 90 ms
Reply from FE80::2E0:FCFF:FE12:6486
bytes=56 Sequence=2 hop limit=64 time = 10 ms
Reply from FE80::2E0:FCFF:FE12:6486
bytes=56 Sequence=3 hop limit=64 time = 20 ms
Reply from FE80::2E0:FCFF:FE12:6486
bytes=56 Sequence=4 hop limit=64 time = 10 ms
Reply from FE80::2E0:FCFF:FE12:6486
bytes=56 Sequence=5 hop limit=64 time = 30 ms

--- FE80::2E0:FCFF:FE12:6486 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 10/32/90 ms
```

При проверке связи с локальным адресом канала (link-local address) посредством команды ping необходимо указать интерфейс-источник или IPv6-адрес источника.

Шаг 4 Настройте статические IPv6-адреса на R2.

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ipv6 address 2000:0012::2 64
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ipv6 address 2000:0023::2 64
[R2-GigabitEthernet0/0/4]quit
```

Шаг 5 Настройте функцию сервера DHCPv6 на R2 и настройте R3 для получения IPv6-адресов через DHCPv6.

Настройте функцию сервера DHCPv6.

```
[R2]dhcp enable
[R2]dhcpv6 pool pool1
An IPv6 address pool named pool1 is created.
[R2-dhcpv6-pool-pool1]address prefix 2000:0023::/64
The IPv6 address prefix is configured.
[R2-dhcpv6-pool-pool1]dns-server 2000:0023::2
The IP address of the DNS server is specified.
[R2-dhcpv6-pool-pool1]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]dhcpv6 server pool1
```

```
[R2-GigabitEthernet0/0/4]quit
```

Настройте функцию клиента DHCPv6.

```
[R3]dhcp enable
```

Info: The operation may take a few seconds. Please wait for a moment.done.

```
[R3]interface GigabitEthernet 0/0/3
```

```
[R3-GigabitEthernet0/0/3]ipv6 address auto dhcp
```

```
[R3-GigabitEthernet0/0/3]quit
```

Выведите на экран адрес клиента и информацию о DNS-сервере.

```
[R3]display ipv6 interface brief
```

*down: administratively down

(l): loopback

(s): spoofing

Interface	Physical	Protocol
GigabitEthernet0/0/3	up	up

[IPv6 Address] 2000:23::1

```
[R3]display dns server
```

Type:

D:Dynamic S:Static

No configured ip dns servers.

No.	Type	IPv6 Address	Interface Name
1	D	2000:23::2	-

GigabitEthernet0/0/3 на маршрутизаторе R3 получил глобальный IPv6-адрес одноадресной рассылки.

Посмотрите, настроен ли сервер DHCPv6 для передачи информации о шлюзе клиентам?

В данном случае сервер DHCPv6 не передает клиенту адрес шлюза IPv6.

Когда настроен режим DHCPv6 с отслеживанием состояния, клиенты DHCPv6 получают маршрут по умолчанию IPv6-шлюза с помощью команды **ipv6 address auto global default**. Если настроен режим DHCPv6 без отслеживания состояния, то с помощью этой команды клиенты DHCPv6 получают глобальный IPv6-адрес одноадресной рассылки и маршрут по умолчанию к IPv6-шлюзу. С помощью команды **undo ipv6 nd ra halt** убедитесь, что на интерфейсе удаленного устройства, подключенного к локальному устройству, была включена функция отправки пакетов RA.

Настройте сервер DHCPv6 для передачи адресов шлюза клиентам.

```
[R2]interface GigabitEthernet 0/0/4
```

```
[R2-GigabitEthernet0/0/4]undo ipv6 nd ra halt
```

Команда **undo ipv6 nd ra halt** позволяет системе отправлять пакеты RA. По умолчанию интерфейсы маршрутизатора не отправляют пакеты RA.

```
[R2-GigabitEthernet0/0/4]ipv6 nd autoconfig managed-address-flag
```

Команда **ipv6 nd autoconfig managed-address-flag** используется для установки флага управляемой конфигурации адресов (флаг M) в сообщениях RA, указывающего, должны или нет хосты использовать автоконфигурацию с отслеживанием состояния для получения адресов. По умолчанию флаг не установлен.

- Если флаг M установлен, хост получает IPv6-адрес посредством автоконфигурации с отслеживанием состояния.

- Если флаг M не установлен, хост использует автоконфигурацию без отслеживания состояния для получения IPv6-адреса, то есть хост генерирует IPv6-адрес на основе информации о префиксе в пакете RA.

```
[R2-GigabitEthernet0/0/4]ipv6 nd autoconfig other-flag
```

Команда **ipv6 nd autoconfig other-flag** устанавливает флаг другой конфигурации (флаг O) в сообщениях RA. По умолчанию флаг не установлен.

- Если флаг O установлен, хост использует автоконфигурацию с отслеживанием состояния для получения других параметров конфигурации (за исключением IPv6-адреса), в том числе продолжительность работы маршрутизатора, время доступности соседа, интервал повторной передачи и PMTU.
- Если флаг O не установлен, хост может получить настройки параметров (за исключением IPv6-адреса), в том числе продолжительность работы маршрутизатора, время доступности соседа, интервал повторной передачи и PMTU, посредством автоконфигурации без отслеживания состояния. Это означает, что устройство маршрутизации анонсирует эти конфигурации с помощью сообщений RA подключенным хостам.

```
[R2-GigabitEthernet0/0/4]quit
```

Настройте клиент на получение маршрута по умолчанию посредством сообщений RA.

```
[R3]interface GigabitEthernet 0/0/3
```

```
[R3-GigabitEthernet0/0/3] ipv6 address auto global default
```

Выведите на экран маршруты R3.

```
[R3]display ipv6 routing-table
```

Routing Table : Public

Destinations : 4 Routes : 4

Destination	::	PrefixLength	: 0
NextHop	: FE80::A2F4:79FF:FE5A:CDAE	Preference	: 64
Cost	: 0	Protocol	: Unr
RelayNextHop	::	TunnelID	: 0x0
Interface	: GigabitEthernet0/0/3	Flags	: D
Destination	:::1	PrefixLength	: 128
NextHop	:::1	Preference	: 0
Cost	: 0	Protocol	: Direct
RelayNextHop	::	TunnelID	: 0x0
Interface	: InLoopBack0	Flags	: D
Destination	: 2000:23::1	PrefixLength	: 128
NextHop	:::1	Preference	: 0
Cost	: 0	Protocol	: Direct
RelayNextHop	::	TunnelID	: 0x0
Interface	: GigabitEthernet0/0/3	Flags	: D
Destination	: FE80::	PrefixLength	: 10
NextHop	::	Preference	: 0
Cost	: 0	Protocol	: Direct
RelayNextHop	::	TunnelID	: 0x0
Interface	: NULL0	Flags	: D

Шаг 6 Настройте R1 для получения IPv6-адреса в режиме без отслеживания состояния.

Включите RA на GigabitEthernet0/0/3 маршрутизатора R2.

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]undo ipv6 nd ra halt
```

Включите функцию автоконфигурации адреса без отслеживания состояния на GigabitEthernet0/0/3 маршрутизатора R1.

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3]ipv6 address auto global
```

Выведите на экран конфигурацию IP-адреса маршрутизатора R1.

```
[R1]display ipv6 interface brief
```

```
*down: administratively down
```

```
(l): loopback
```

```
(s): spoofing
```

Interface	Physical	Protocol
GigabitEthernet0/0/3	up	up

```
[IPv6 Address] 2000:12::2E0:FCFF:FE4D:355
```

GigabitEthernet0/0/3 маршрутизатора R1 генерирует глобальный IPv6-адрес одноадресной рассылки на основе префикса IPv6-адреса, полученного из сообщения RA, которое отправил маршрутизатор R2, и локально сгенерированного идентификатора интерфейса.

Шаг 7 Настройте статический маршрут IPv6.

Настройте статический маршрут на маршрутизаторе R1, чтобы обеспечить соединение между GigabitEthernet0/0/3 на маршрутизаторе R1 и GigabitEthernet0/0/3 на маршрутизаторе R3.

```
[R1]ipv6 route-static 2000:23::64 2000:12::2
```

```
Info: The destination address and mask of the configured static route mismatched, and the static route 2000:23::/64 was generated.
```

Проверьте возможность установления связи.

```
[R1]ping ipv6 2000:23::1
```

```
PING 2000:23::1 : 56 data bytes, press CTRL_C to break
```

```
Reply from 2000:23::1
```

```
bytes=56 Sequence=1 hop limit=63 time = 20 ms
```

```
Reply from 2000:23::1
```

```
bytes=56 Sequence=2 hop limit=63 time = 20 ms
```

```
Reply from 2000:23::1
```

```
bytes=56 Sequence=3 hop limit=63 time = 30 ms
```

```
Reply from 2000:23::1
```

```
bytes=56 Sequence=4 hop limit=63 time = 20 ms
```

```
Reply from 2000:23::1
```

```
bytes=56 Sequence=5 hop limit=63 time = 30 ms
```

```
--- 2000:23::1 ping statistics ---
```

```
5 packet(s) transmitted
```

```
5 packet(s) received
```

```
0.00% packet loss
```

```
round-trip min/avg/max = 20/24/30 ms
```

R1 имеет статический маршрут к сети 2000:23::/64. R3 получает маршрут по умолчанию через DHCPv6. Следовательно, GigabitEthernet0/0/3 на R1 и GigabitEthernet0/0/3 на R3 могут взаимодействовать друг с другом.

Выведите на экран информацию о соседях IPv6.

```
[R1]display ipv6 neighbors
-----
IPv6 Address      : 2000:12::2
Link-layer        : 00e0-fc12-6486          State      : STALE
Interface         : GE0/0/3                Age        : 8
VLAN              : -                      CEVLAN     : -
VPN name          :                      Is Router  : TRUE
Secure FLAG       : UN-SECURE

IPv6 Address      : FE80::2E0:FCFF:FE12:6486
Link-layer        : 00e0-fc12-6486          State      : STALE
Interface         : GE0/0/3                Age        : 8
VLAN              : -                      CEVLAN     : -
VPN name          :                      Is Router  : TRUE
Secure FLAG       : UN-SECURE
-----
Total: 2          Dynamic: 2          Static: 0
```

----Конец

7.3 Проверка

Подробности данной операции здесь не приводятся.

7.4 Справочные конфигурации

Конфигурация на R1

```
#
sysname R1
#
ipv6
#
interface GigabitEthernet0/0/3
ipv6 enable
ipv6 address auto link-local
ipv6 address auto global
#
ipv6 route-static 2000:23:: 64 2000:12::2
#
return
```

Конфигурация на R2

```
#
```

```
sysname R2
#
ipv6
#
dhcp enable
#
dhcpv6 pool pool1
address prefix 2000:23::/64
dns-server 2000:23::2
#
interface GigabitEthernet0/0/3
ipv6 enable
ipv6 address 2000:12::2/64
ipv6 address auto link-local
undo ipv6 nd ra halt
interface GigabitEthernet0/0/4
#
ipv6 enable
ipv6 address 2000:23::2/64
ipv6 address auto link-local
undo ipv6 nd ra halt
ipv6 nd autoconfig managed-address-flag
dhcpv6 server pool1
#
return
```

Конфигурация на R3

```
#
sysname R3
#
ipv6
#
dhcp enable
#
interface GigabitEthernet0/0/3
ipv6 enable
ipv6 address auto link-local
ipv6 address auto global default
ipv6 address auto dhcp
#
return
```

7.5 Вопросы

1. Почему интерфейс-источник должен быть указан на шаге 3 (для проверки связи между локальными адресами канала), но не должен быть указан на шаге 7 (для проверки связи между адресами GUA)?
2. Объясните, в чем отличие между конфигурацией адреса с отслеживанием состояния и конфигурацией адреса без отслеживания состояния?

8

Основы сетевого программирования и автоматизации

8.1 Общая информация

8.1.1 О лабораторной работе

С помощью этой лабораторной работы вы поймете, как использовать Python telnetlib.

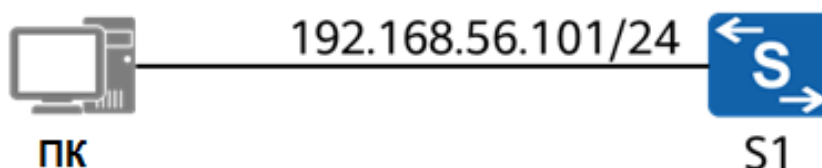
8.1.2 Цели

- Изучение базового синтаксиса языка Python
- Использование telnetlib

8.1.3 Топология сети

У компании есть коммутатор с IP-адресом управления 192.168.56.101/24. Необходимо написать сценарий автоматизации для просмотра текущего конфигурационного файла устройства.

Рис. 8-1 Топология сети для сетевого программирования и автоматизации, используемая в данной лабораторной работе



8.2 Лабораторная работа

8.2.1 План работы

1. Настройка параметров Telnet: установка пароля Telnet, включение Telnet и настройка разрешения на доступ через Telnet.

2. Компиляция сценария Python: вызов модуля telnetlib для входа в устройство и проверка конфигурации.

8.2.2 Процедура конфигурирования

Шаг 1 Настройте Telnet на коммутаторе.

Задайте пароль для входа Telnet.

```
[Huawei]user-interface vty 0 4
[Huawei-ui-vty0-4]authentication-mode password
[Huawei-ui-vty0-4]set authentication password simple Huawei@123
[Huawei-ui-vty0-4]protocol inbound telnet
[Huawei-ui-vty0-4]user privilege level 15
```

Перед использованием сценария Python для входа в устройство через Telnet необходимо задать пароль Telnet и включить функцию Telnet на устройстве. Установите пароль **Huawei@123** для входа Telnet.

Включите службу Telnet, чтобы разрешить доступ через Telnet.

```
[Huawei]telnet server enable
Info: The Telnet server has been enabled.
```

Войдите с ПК в коммутатор через Telnet с помощью командного интерфейса.

```
C:\Users\XXX>telnet 192.168.56.101
Login authentication

Password:
Info: The max number of VTY users is 5, and the number of current VTY users on line is 1.           The
current login time is 2020-01-15 21:12:57.
<Huawei>
```

Функции Telnet сконфигурированы корректно.

Шаг 2 Напишите код на языке Python.

```
import telnetlib
import time

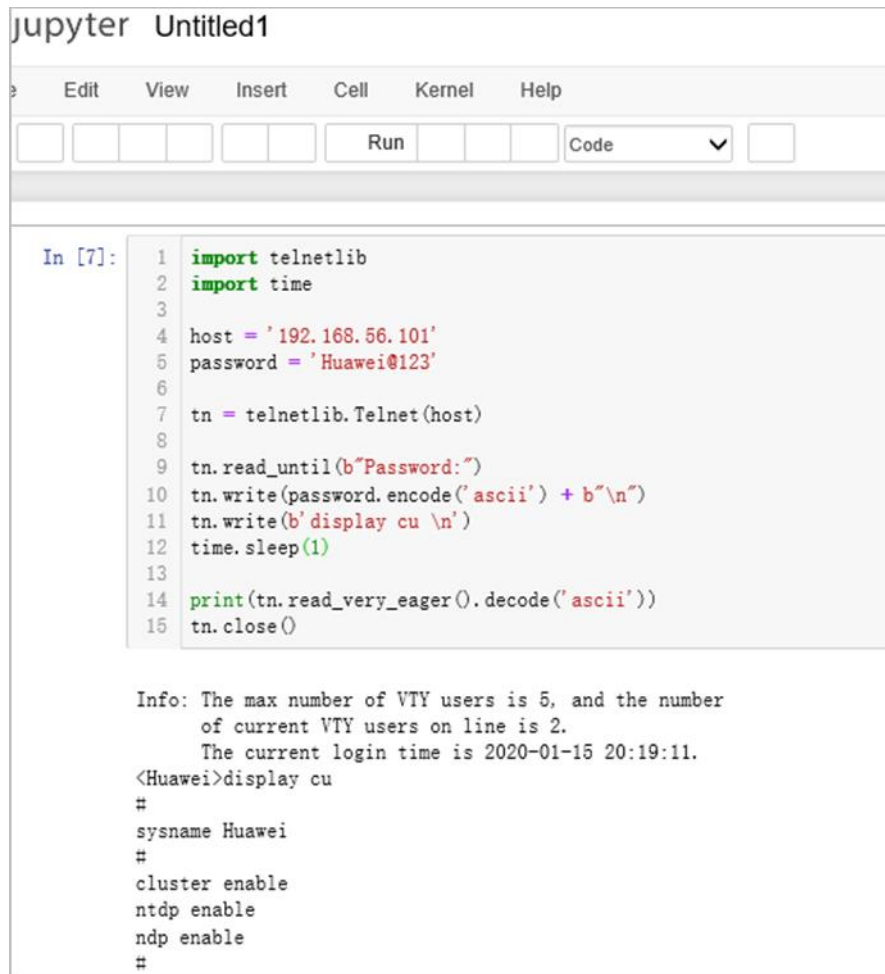
host = '192.168.56.101'
password = 'Huawei@123'

tn = telnetlib.Telnet(host)

tn.read_until(b"Password:")
tn.write(password.encode('ascii') + b"\n")
tn.write(b'display cu \n')
time.sleep(1)

print(tn.read_very_eager().decode("ascii"))
tn.close()
```

Сценарий Python вызывает модуль telnetlib для входа в коммутатор S1, выполняет команду **display current-configuration** и выводит на экран результаты выполнения команды.

Шаг 3 Запустите компилятор.

```
In [7]: 1 import telnetlib
2 import time
3
4 host = '192.168.56.101'
5 password = 'Huawei@123'
6
7 tn = telnetlib.Telnet(host)
8
9 tn.read_until(b'Password:~')
10 tn.write(password.encode('ascii') + b'\n')
11 tn.write(b'display cu \n')
12 time.sleep(1)
13
14 print(tn.read_very_eager().decode('ascii'))
15 tn.close()
```

Info: The max number of VTY users is 5, and the number
of current VTY users on line is 2.
The current login time is 2020-01-15 20:19:11.

<Huawei>display cu

sysname Huawei

cluster enable
ntdp enable
ndp enable
#

В этой лабораторной среде используется компилятор Jupyter Notebook. Но можно использовать и другие компиляторы.

Шаг 4 Командный вывод выглядит следующим образом:

```
Info: The max number of VTY users is 5, and the number
of current VTY users on line is 2.
The current login time is 2020-01-15 20:19:11.
<Huawei>display cu
#
sysname Huawei
#
cluster enable
ntdp enable
ndp enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
```

```
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
interface Vlanif1
 ip address 192.168.56.101 255.255.255.0
---- More ----
```

----Конец

8.2.3 Интерпретация кода

Шаг 1 Имортируйте модуль.

```
import telnetlib
import time
```

Импортируйте модули telnetlib и time. Python предоставляет оба модуля, и установка их не требуется.

В этом разделе описаны общие классы и методы Telnetlib, используемого в качестве клиента, в том числе read_until, read_very_eager() и write() в классе Telnet. Дополнительные методы Telnet см. в официальном документе для telnetlib, который опубликован на странице <https://docs.python.org/3/library/telnetlib.html#telnet-example>.

По умолчанию Python выполняет весь код последовательно без интервалов. При использовании Telnet для передачи коммутатору команд конфигурирования коммутатор может не отвечать вовремя или выходные данные команды могут быть неполными. В этом случае можно использовать метод sleep в модуле time, чтобы вручную приостановить работу программы.

Шаг 2 Войдите в устройство.

Вызовите несколько методов класса Telnet в модуле telnetlib для входа в S1.

```
host = '192.168.56.101'
password = 'Huawei@123'
tn = telnetlib.Telnet(host)
```

Создайте две переменные. host и password — это адрес и пароль для входа в устройство соответственно, которые совпадают с адресом и паролем, настроенными на устройстве. В этом примере для входа используется только пароль Telnet. Следовательно, указывать имя пользователя не требуется.

telnetlib.Telnet() указывает, что вызывается метод Telnet() в классе telnetlib. Этот метод содержит параметры для входа, включая IP-адрес и номер порта. Если информация о порте не указана, по умолчанию используется порт 23.

В этом примере `tn = telnetlib.Telnet(host)` означает, что осуществляется вход в устройство с номером хоста `192.168.56.101`, и для `tn` устанавливается значение `telnetlib.Telnet(host)`.

```
tn.read_until(b"Password:")
```

При входе в устройство с адресом `192.168.56.101` через Telnet отображается следующая информация:

```
<TelnetClient>telnet 192.168.56.101
Trying 192.168.56.101 ...
Press CTRL+K to abort
Connected to 192.168.56.101 ...
```

Login authentication

```
Password:
```

Примите во внимание, что программа не знает, какую информацию требуется считывать. Поэтому используется `read_until()` — чтение до тех пор, пока не будет найдена заданная в скобках строка.

В этом примере `tn.read_until(b"Password:")` указывает, что чтение данных осуществляется до строки «Password:». Буква «b» перед «Password:» указывает, что код Unicode по умолчанию в Python3 изменен на байты. Это требование функции к входным данным. Более подробную информацию см. в официальном документе для `telnetlib`. Если этот параметр не передается, программа сообщает об ошибке.

```
tn.write(password.encode('ascii') + b"\n")
```

После того, как в коде отображается `Password:`, программа вводит пароль. Этот параметр был определен и используется в качестве пароля для входа в Telnet. Для записи пароля используйте `write()`.

В этом примере `tn.write (password.encode('ascii') + b"\n")` состоит из двух частей: `password.encode('ascii')` и `b"\n"`. `password.encode('ascii')`. Это указывает, что символьная строка `Huawei@123`, используемая в качестве пароля, имеет тип кодировки ASCII.

«+» обозначает, что символьные строки до и после символа будут объединены.

`\n` — символ новой строки, который эквивалентен нажатию клавиши Enter.

Следовательно, код в этой строке эквивалентен вводу пароля `Huawei@123` и нажатию Enter.

Шаг 3 Выполните команды конфигурирования.

После входа в устройство через Telnet используйте сценарий Python для выполнения команд.

```
tn.write(b'display cu \n')
```

`write()` используется для ввода команд, которые необходимо выполнить на устройстве. Команда **display cu** — это сокращенная форма команды **display current-configuration**, которая выводит на экран текущую конфигурацию устройства.

```
time.sleep(1)
```

`time.sleep(1)` используется для приостановки выполнения программы на одну секунду, чтобы дождаться предоставления коммутатором данных перед выполнением последующего кода. Если время ожидания не указано, программа непосредственно выполняет следующую строку кода. В результате происходит сбой чтения данных.

```
print(tn.read_very_eager().decode('ascii'))
```

`print()` указывает, что содержимое в скобках отображается на консоли.

`tn.read_very_eager()` указывает на чтение как можно большего количества данных.

`.decode('ascii')` указывает, что считанные данные декодируются в ASCII.

Код в этом примере позволяет отображать выводимые данные с S1 в течение одной секунды на консоли после выполнения команды **display cu**.

Шаг 4 Закройте сеанс.

```
tn.close()
```

Для закрытия сеанса используется метод `close()`. Количество соединений VTY на устройстве ограничено. Таким образом, после выполнения сценариев необходимо закрывать сеансы.

----Конец

8.3 Проверка

Подробности данной операции здесь не приводятся.

8.4 Справочные конфигурации

Подробная информация здесь не приводится.

8.5 Вопросы

1. Как с помощью `telnetlib` настроить параметры устройства, например, IP-адрес интерфейса управления устройством?
2. Как сохранить файл конфигурации в локальный каталог?

9

Конфигурирование кампусной сети

9.1 Справочная информация

Рекомендуемые команды и документация, представленные в настоящем документе, приводятся только в справочных целях. В реальных условиях их выбор зависит от модели и версии используемого вами продукта.

Рекомендуемые документы:

1. Документация по продуктам AR600 и AR6000
2. Документация по Ethernet-коммутаторам серий S2720, S5700 и S6700
3. Документация по контроллеру беспроводного доступа (AC и Fit AP)
4. Стандартная архитектура и типовые примеры применения кампусной сети

Справочные ссылки:

1. <http://support.huawei.com/>
2. <http://e.huawei.com/>

9.2 Общая информация

9.2.1 О лабораторной работе

Повсеместное развертывание сетей связи является неотъемлемой частью развития информационного общества. В качестве основы при создании сети связи всегда используются кампусные сети. Кампусы есть повсюду, включая фабрики, административные здания и государственные учреждения, торговые центры, офисные здания, образовательные комплексы и парки. Согласно статистике, 90% городских жителей работают и живут в кампусах, 80% валового внутреннего продукта (ВВП) создается в кампусах, и каждый человек 18 часов в день проводит в кампусе. При строительстве любого объекта кампусной сети придается очень важное значение. Как инфраструктура, обеспечивающая подключение к цифровому миру, она играет ключевую роль для реализации повседневной работы, исследований и разработок, производства и управления операциями.

В этой лабораторной работе вы создадите кампусную сеть, чтобы понять общие технологии и их применение в кампусных сетях.

9.2.2 Цели

Лабораторная работа помогает получить практические навыки по изучению следующих тем:

- Общие концепции и архитектура кампусной сети
- Наиболее распространенные сетевые технологии
- Жизненный цикл кампусных сетей
- Основные этапы кампусной сети: планирование и проектирование, развертывание и внедрение, эксплуатация и техобслуживание, а также оптимизация
- Процесс реализации проекта кампусной сети

9.2.3 Топология сети

В офисном здании необходимо создать сеть. Офисное здание имеет шесть этажей. В настоящее время в эксплуатацию введены три этажа: холл с рецепцией на первом этаже, административный отдел и кабинет генерального директора на втором этаже, отдел исследований и разработок и отдел маркетинга на третьем этаже. Аппаратный зал с основным оборудованием располагается на первом этаже, а на каждом из других этажей оборудовано небольшое помещение для размещения сетевых устройств.

Сформируйте проектную группу для завершения строительства сети.

9.3 Задачи лабораторной работы

9.3.1 Сбор и анализ требований

Определите, какую информацию необходимо получить от компании? Укажите не менее пяти требований.

Например: количество терминалов, которые будут подключаться к корпоративной сети.

1. _____
2. _____
3. _____
4. _____
5. _____

Проанализируйте собранные требования.

1. Бюджет проекта
Бюджет ограничен. Проект необходимо реализовать с минимальными затратами.

2. Типы подключаемых терминалов
Будет осуществляться развертывание как проводных, так и беспроводных терминалов.

3. Количество терминалов
Первый этаж: 10 проводных терминалов и 100 беспроводных терминалов
Второй и третий этажи: 200 проводных терминалов и 50 беспроводных терминалов

4. Режим управления сетью
Унифицированное управление сетью с помощью SNMP.

5. Объем сетевого трафика и темпы роста
Большая часть трафика — это внутренний трафик. Скорость проводного доступа должна быть 100 Мбит/с. Других особых требований нет.

6. Требования к доступности
Необходимо реализовать резервирование определенных компонентов сети уровня 3 и поддержку возможностей аварийного переключения.

7. Требования к безопасности
Необходимо реализовать контроль сетевого трафика.

8. Режим доступа в Интернет
Для подключения к Интернету граничные устройства кампусной сети должны использовать статические IP-адреса.

9. Требования к расширению сети
При вводе в эксплуатацию других этажей существующие устройства не должны требовать замены.

9.3.2 Планирование и проектирование

Задача 1. Выбор устройства и проектирование физической топологии (опционально)

Исходные данные

В следующей таблице приведено общее количество терминалов в сети.

Этаж	Первый этаж	Второй этаж	Третий этаж	Другие этажи (зарезервированное количество)
Проводные терминалы	10	200	200	500
Беспроводные терминалы	100	50	50	200
Примечания	Гостевые беспроводные терминалы + серверы	Компьютеры + мобильные телефоны		

Трафик с беспроводных терминалов — это трафик доступа в Интернет. Скорость доступа каждого клиента составляет 2 Мбит/с.

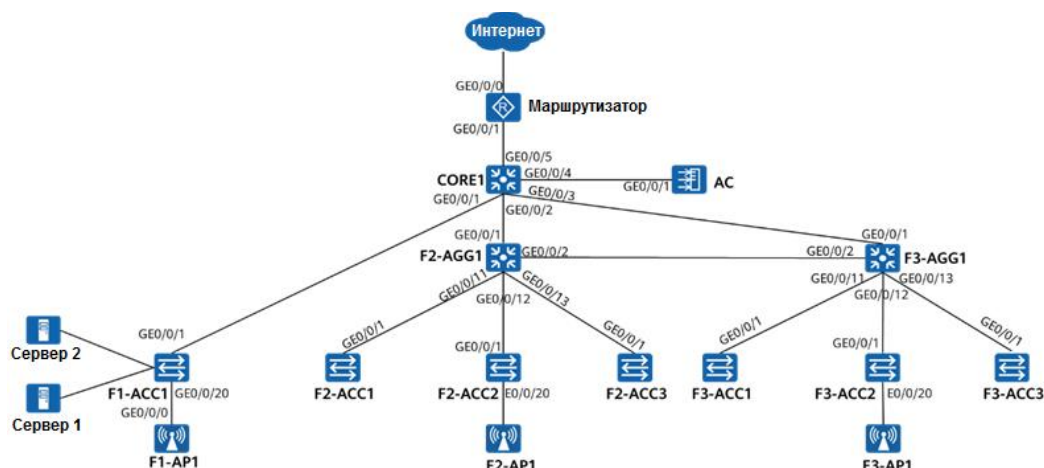
Убедитесь, что на компьютерах реализуется скорость 100 Мбит/с, а на серверах — 1000 Мбит/с.

Для повышения качества беспроводного доступа на каждом этаже требуется не менее трех двухдиапазонных точек доступа.

Задача

Разработайте физическую топологию сети в такой последовательности: уровень доступа, уровень агрегации, уровень ядра сети и выходная область, а затем выберите необходимые устройства.

Справочное решение



Далее в таблице приводятся интерфейсы устройств с соответствующими номерами.

Устройство	Интерфейсы
F2-ACC1, F2-ACC2, F2-ACC3, F3-ACC1, F3-ACC2 и F3-ACC3	Eo/o/1–Eo/o/222 GEo/o/1–GEo/o/2
F1-ACC1, F2-AGG1, F3-AGG1 и CORE1	GEo/o/1–GEo/o/24
AC	GEo/o/1–GEo/o/8
F1-AP1, F2-AP1 и F3-AP1	GEo/o/0–GEo/o/1
Маршрутизатор	GEo/o/0–GEo/o/2

ПРИМЕЧАНИЕ

Процесс проектирования сети и топологии по указанным выше требованиям подробно описывается в учебном пособии по сертификации HCIA-Datcom «Практическая реализация проектов кампусной сети». В этом документе эта информация не приводится. В реальной сети разворачивается большое количество коммутаторов доступа и точек доступа. Для удобства организации сети и последующего тестирования в этом документе используется упрощенная топология сети.

Задача 2. Сетевое проектирование уровня 2

Исходные данные

- Создание VLAN на базе проводной сети:
 - Порты коммутатора доступа GEo/o/1–GEo/o/10 в помещении с основным оборудованием подключены к серверам и назначены в одну и ту же VLAN.
 - На втором этаже F2-ACC2 подключен к офису генерального директора, а другие коммутаторы подключены к административному отделу. Два отдела принадлежат к разным VLAN.

- На третьем этаже порты Eo/o/1–Eo/o/10 F3-ACC1 и F3-ACC3 принадлежат отделу маркетинга, а Eo/o/11–Eo/o/20 — отделу исследований и разработок.
- Порты Eo/o/1–Eo/o/19 F3-ACC2 принадлежат отделу маркетинга.
- Создание VLAN на базе беспроводной сети:
 - Беспроводные терминалы на разных этажах должны быть назначены в разные VLAN.
 - На каждом этаже должна быть своя VLAN управления беспроводной сетью.

ПРИМЕЧАНИЕ

Необходимо зарезервировать VLAN для организации связи между устройствами и VLAN для управления устройствами.

Задача

Заполните таблицу планирования сети уровня 2 на основе существующей информации и требований.

Идентификатор VLAN	Описание
Например, 1	VLAN управления устройствами уровня 2

Справочное решение

Идентификатор VLAN	Описание
1	VLAN управления устройствами уровня 2 на первом этаже
2	VLAN управления устройствами уровня 2 на втором этаже
3	VLAN управления устройствами уровня 2 на третьем этаже
100	VLAN для серверов
101	VLAN для офиса генерального директора
102	VLAN для административного отдела
103	VLAN для отдела маркетинга
104	VLAN для отдела исследований и разработок (R&D)
105	VLAN для беспроводных терминалов на первом этаже
106	VLAN для беспроводных терминалов на втором этаже
107	VLAN для беспроводных терминалов на третьем этаже
201	VLAN для организации связи между F2-AGG1 и CORE1
202	VLAN для связи между F3-AGG1 и CORE1
203	VLAN для организации связи между F2-AGG1 и F3-AGG1
204	VLAN для организации связи между CORE1 и маршрутизатором
205	VLAN управления беспроводной сетью на первом этаже
206	VLAN управления беспроводной сетью на втором этаже
207	VLAN управления беспроводной сетью на третьем этаже

Задача 3. Сетевое проектирование уровня 3

Исходные данные

- Диапазон адресов в сети 192.168.0.0/16. При этом предъявляются следующие требования:
 - Первый этаж:
 - Серверы используют статические IP-адреса. Назначение IP-адресов беспроводным станциям и точкам доступа осуществляет CORE1 через DHCP. Шлюз находится на CORE1.
 - Управляющие IP-адреса коммутаторов доступа являются статическими IP-адресами, а шлюз находится на CORE1.
 - Второй и третий этажи:

- IP-адреса всех проводных терминалов, беспроводных терминалов и беспроводных точек доступа назначаются коммутатором агрегации соответствующего этажа посредством DHCP. Шлюз развернут на коммутаторах агрегации.
- Управляющие IP-адреса коммутаторов доступа являются статическими IP-адресами, а шлюз находится на коммутаторе агрегации соответствующего этажа.
- OSPF используется во всей сети для обеспечения связи между сервисными сетями. Все терминалы выходят в Интернет через маршрутизатор.

Задача

Заполните таблицу планирования сети уровня 3 на основе существующей информации и требований.

IP-сеть	Метод назначения адреса, шлюз	Режим маршрутизации	Описание сети
192.168.1.0/24	DHCP; 192.168.1.254	OSPF	Сеть управления устройствами уровня 2

Справочное решение

IP-сеть	Метод назначения адреса, шлюз	Режим маршрутизации	Описание сети
192.168.1.0/24	Статические адреса; CORE1	Маршрут по умолчанию, направленный на CORE1	Сеть управления устройствами уровня 2 на первом этаже
192.168.2.0/24	Статические адреса; F2-AGG1	Маршрут по умолчанию, направленный на F2-AGG1	Сеть управления устройствами уровня 2 на втором этаже
192.168.3.0/24	Статические адреса; F3-AGG	Маршрут по умолчанию, направленный на F3-AGG	Сеть управления устройствами уровня 2 на третьем этаже
192.168.100.0/24	Статические адреса; CORE1	Анонсирование в OSPF через шлюзовые устройства	Сеть серверов
192.168.101.0/24	Назначение выполняет F2-AGG1 посредством DHCP; F2-AGG1		Сеть офиса генерального директора
192.168.102.0/24			Сеть административного отдела
192.168.103.0/24	Назначение выполняет F3-AGG1 посредством DHCP; F3-AGG1		Сеть отдела маркетинга
192.168.104.0/24			Сеть отдела исследований и разработок
192.168.105.0/24	Назначение выполняет CORE1 посредством DHCP; CORE1		Сеть беспроводных терминалов на первом этаже
192.168.106.0/24	Назначение выполняет F2-AGG1 посредством DHCP; F2-AGG1		Сеть беспроводных терминалов на втором этаже
192.168.107.0/24	Назначение выполняет F3-AGG1 посредством DHCP; F3-AGG1		Сеть беспроводных терминалов на третьем этаже

IP-сеть	Метод назначения адреса, шлюз	Режим маршрутизации	Описание сети
192.168.201.0/30	Статические адреса; шлюз не требуется	Включены OSPF и отношения соседства, маршрутизатор анонсирует маршрут по умолчанию	Сеть для организации связи между F2-AGG1 и CORE1
192.168.202.0/30			Сеть для организации связи между F3-AGG1 и CORE1
192.168.203.0/30			Сеть для организации связи между F2-AGG1 и F3-AGG1
192.168.204.0/30			Сеть для организации связи между CORE1 и маршрутизатором
192.168.205.0/24	Назначение выполняет CORE1 посредством DHCP; CORE1	Анонсирование в OSPF через шлюзовые устройства	Сеть управления беспроводной сетью на первом этаже
192.168.206.0/24	Назначение выполняет F2-AGG1 посредством DHCP; F2-AGG1		Сеть управления беспроводной сетью на втором этаже
192.168.207.0/24	Назначение выполняет F3-AGG1 посредством DHCP; F3-AGG1		Сеть управления беспроводной сетью на третьем этаже

Задача 4. Проектирование WLAN

Исходные данные

- АС управляет всеми точками доступа унифицированным образом и имеет ограниченную скорость передачи данных.
 - Точки доступа на первом этаже зарегистрированы на уровне 2.
 - Все точки доступа на втором и третьем этажах регистрируются в АС на уровне 3. Шлюзом АС является CORE1.
- Для каждого этажа создается SSID.
 - Используется политика безопасности WPA-WPA2+PSK+AES.
 - У каждого этажа свой SSID и отдельный пароль.

Задача

Заполните таблицу планирования сети WLAN на основе имеющейся информации и требований.

Элемент	WLAN на первом этаже	WLAN на втором этаже	WLAN на третьем этаже
VLAN для управления AP			
Сервисная VLAN			
DHCP-сервер			
IP-адрес интерфейса-источника контроллера доступа			
Группа AP			
Профиль регулирующего домена			
Профиль SSID			
Профиль безопасности			
Профиль VAP			
Другие настройки			

Справочное решение

Элемент	WLAN на первом этаже	WLAN на втором этаже	WLAN на третьем этаже
VLAN для управления AP	VLAN205	VLAN206	VLAN207
Сервисная VLAN	VLAN105	VLAN106	VLAN107
DHCP-сервер	CORE1 назначает IP-адреса для AP и STA.	F2-AGG1 назначает IP-адреса для AP и STA.	F3-AGG1 назначает IP-адреса для AP и STA.
IP-адрес интерфейса-источника контроллера доступа	VLANIF205: 192.168.205.253/24		
Группа AP	Имя: WLAN-F1 Профиль VAP: WLAN-F1	Имя: WLAN-F2 Профиль VAP: WLAN-F2	Имя: WLAN-F3 Профиль VAP: WLAN-F3

Элемент	WLAN на первом этаже	WLAN на втором этаже	WLAN на третьем этаже
	Профиль регулирующего домена: default	Профиль регулирующего домена: default	Профиль регулирующего домена: default
Профиль регулирующего домена	Имя: default Код страны: CN		
Профиль SSID	Имя: WLAN-F1 Имя SSID: WLAN-F1	Имя профиля: WLAN-F2 Имя SSID: WLAN-F2	Имя профиля: WLAN-F3 Имя SSID: WLAN-F3
Профиль безопасности	Имя: WLAN-F1 Политика безопасности: WPA-WPA2+PSK+AES Пароль: WLAN@Guest123	Имя: WLAN-F2 Политика безопасности: WPA-WPA2+PSK+AES Пароль: WLAN@Employee2	Имя: WLAN-F3 Политика безопасности: WPA-WPA2+PSK+AES Пароль: WLAN@Employee3
Профиль VAP	Имя: WLAN-F1 Режим передачи: прямая передача Сервисная VLAN: VLAN: 105 Профили: Профиль SSID: WLAN-F1 Профиль безопасности: WLAN-F1	Имя: WLAN-F2 Режим передачи: прямая передача Сервисная VLAN: 106 Профили: Профиль SSID: WLAN-F2 Профиль безопасности: WLAN-F2	Имя: WLAN-F3 Режим передачи: прямая передача Сервисная VLAN: VLAN: 107 Профили: Профиль SSID: WLAN-F3 Профиль безопасности: WLAN-F3

Задача 5. Проектирование сетевой безопасности и выхода в Интернет

Исходные данные

- Гостевому SSID не разрешен доступ во внутреннюю сеть компании.
- Только беспроводные терминалы могут подключаться к сети Интернет.
- Маршрутизатор использует статический IP-адрес для подключения к сети Интернет. Оператор связи назначает маршрутизатору IP-адреса из диапазона 1.1.1.1–1.1.1.10 (с 24-битной маской). IP-адрес следующего перехода маршрутизатора для доступа к сети Интернет — 1.1.1.254.
- Веб-сервер на предприятии должен предоставлять услуги для внешних пользователей. Частный IP-адрес веб-сервера — 192.168.100.1, а номер порта — 80. В целях обеспечения безопасности сервера сопоставление NAT реализуется только для веб-служб.

Задача

Заполните таблицу планирования сетевой безопасности и выхода в Интернет на основе имеющейся информации и требований.

Требование	Реализация

Справочное решение

Требование	Реализация
Контроль доступа гостей к интрасети	Настройка фильтрации трафика или политики прохождения трафика на CORE1.
Контроль выхода в Интернет	Настройка NAT на маршрутизаторе и отключение трансляции адресов для определенных сетей.
Сопоставление веб-серверов	Настройка NAT-сервера на интерфейсе маршрутизатора.

Задача 6. Проектирование управления сетью

Исходные данные

- SNMPv3 используется для связи с NMS, а для повышения уровня безопасности настроены аутентификация и шифрование.
- Все устройства, кроме маршрутизатора и AC, взаимодействуют с NMS, имеющей адрес 192.168.100.2/24, через VLAN управления.
- Маршрутизаторы взаимодействуют с NMS через GE0/0/1.
- AC взаимодействует с NMS через VLANIF 205.
- Все устройства должны иметь функцию отправки аварийных сигналов SNMP в NMS.

Задача

Оптимизируйте конфигурации устройств на этапе развертывания и внедрения на основе приведенных выше требований.

9.3.3 Реализация

Задача 1. Схема конфигурирования

Заполните схему конфигурирования для каждого устройства в соответствии со схемой планирования и проектирования.

Маршрутизатор:

Элемент	Конфигурация
Настройка основных параметров	
Настройка IP-адреса	
OSPF	
Настройка выхода	
Настройка SNMP	
Другие настройки	

CORE1:

Элемент	Конфигурация
Настройка основных параметров	
Настройка VLAN	
Настройка интерфейса VLANIF	
Настройка OSPF	
Настройка DHCP	
Контроль доступа	
Настройка SNMP	
Другие настройки	

F2-AGG1:

Элемент	Конфигурация
Настройка основных параметров	
Настройка VLAN	
Настройка VLAN на интерфейсах	

Элемент	Конфигурация
Настройка интерфейса VLANIF	
Настройка OSPF	
Настройка DHCP	
Настройка SNMP	
Другие настройки	

F3-AGG1:

Элемент	Конфигурация
Настройка основных параметров	
Настройка VLAN	
Настройка VLAN на интерфейсах	
Настройка интерфейса VLANIF	
Настройка OSPF	
Настройка DHCP	
Настройка SNMP	
Другие настройки	

Контроллер доступа (AC):

Элемент	Конфигурация
Настройка основных параметров	
Настройка проводной сети	
Настройка беспроводной сети	
Настройка SNMP	
Другие настройки	

F1-ACC1:

Элемент	Конфигурация
Настройка основных параметров	

Элемент	Конфигурация
Настройка VLAN	
Настройка интерфейса VLANIF	
Настройка параметров маршрутизации	
Настройка SNMP	
Другие настройки	

F2-ACC1:

Элемент	Конфигурация
Настройка основных параметров	
Настройка VLAN	
Настройка интерфейса VLANIF	
Настройка параметров маршрутизации	
Настройка SNMP	
Другие настройки	

F2-ACC2:

Элемент	Конфигурация
Настройка основных параметров	
Настройка VLAN	
Настройка интерфейса VLANIF	
Настройка параметров маршрутизации	
Настройка SNMP	
Другие настройки	

F2-ACC3:

Элемент	Конфигурация
Настройка основных параметров	
Настройка VLAN	

Элемент	Конфигурация
Настройка интерфейса VLANIF	
Настройка параметров маршрутизации	
Настройка SNMP	
Другие настройки	

F3-ACC1:

Элемент	Конфигурация
Настройка основных параметров	
Настройка VLAN	
Настройка интерфейса VLANIF	
Настройка параметров маршрутизации	
Настройка SNMP	
Другие настройки	

F3-ACC2:

Элемент	Конфигурация
Настройка основных параметров	
Настройка VLAN	
Настройка интерфейса VLANIF	
Настройка параметров маршрутизации	
Настройка SNMP	
Другие настройки	

F3-ACC3:

Элемент	Конфигурация
Настройка основных параметров	
Настройка VLAN	
Настройка интерфейса VLANIF	

Элемент	Конфигурация
Настройка параметров маршрутизации	
Настройка SNMP	
Другие настройки	

Конфигурирование

Создайте лабораторную среду и выполните необходимые настройки в соответствии с приведенными выше схемами конфигурирования в течение 40 минут.

Задача 2. Приемка проекта

Вам необходимо определить, какие элементы будут проходить проверку для приемки проекта после завершения настройки устройств. А также вам необходимо определить способы проверки. Укажите не менее пяти требований.

1. _____
2. _____
3. _____
4. _____
5. _____

Справочное решение

1. Проверка возможности беспроводных клиентов обнаруживать беспроводные сигналы и успешно получать доступ к сети.
2. Проверка успешного установления отношений соседства OSPF.
3. Проверка возможности подключения внутри сетей.
4. Проверка связи между сетями.
5. Проверка контроля доступа для гостей, использующих беспроводные терминалы.
6. Проверка контроля доступа к сети Интернет.
7. Проверка возможности NMS управлять сетевыми устройствами.

9.3.4 Эксплуатация и техническое обслуживание сети (O&M)

Задача 1. Организация O&M

Как организовать работы по техническому обслуживанию в будущем после сдачи проекта? Обсудите со своей проектной группой и перечислите не менее пяти пунктов обслуживания.

1. _____
2. _____
3. _____
4. _____
5. _____

Справочное решение

Периодичность техобслуживания	Пункт проверки	Способ проверки	Критерий оценки
Каждый день	Подключение кабелей питания	Осмотр	Кабель питания правильно и надежно подсоединен к соответствующему разъему устройства. Индикатор питания на устройстве постоянно горит (зеленым светом), не мигая.
	Температура устройства	<HUAWEI> display temperature	Температура каждого модуля находится в диапазоне между верхним и нижним пределом.
	Аварийная информация	<HUAWEI> display alarm urgent	Аварийные сигналы регистрируются, а для значительных и наиболее серьезных аварийных сигналов производятся анализ и обработка.
	Загрузка ЦП	<HUAWEI> display cpu- usage	Загрузка ЦП каждого модуля в норме. Если загрузка ЦП часто или постоянно превышает 80%, требуется выяснить причину и принять соответствующие меры.

Периодичность техобслуживания	Пункт проверки	Способ проверки	Критерий оценки
	Использование ресурсов памяти	<HUAWEI> display memory-usage	Использование ресурсов памяти в норме. Если значение параметра Memory Using Percentage превышает 60%, требуется выяснить причину и принять соответствующие меры.
Один раз в неделю	Температура окружающей среды в аппаратном зале	Измерение с помощью прибора	Температура долгосрочной эксплуатации аппаратного зала находится в диапазоне от 0°C до 50°C, а температура кратковременной эксплуатации находится в диапазоне от -5°C до 55°C.
	Относительная влажность окружающей среды в аппаратном зале	Измерение с помощью прибора	Относительная влажность окружающей среды в помещении с оборудованием находится в диапазоне от 10% до 90%.
Один раз в месяц	Положение устройства	Осмотр и измерение с помощью приборов	Устройство размещено на ровной поверхности в хорошо вентилируемом, сухом и чистом помещении.
	Таблица маршрутизации	<HUAWEI> display ip routing-table	На всех устройствах, использующих одинаковый протокол маршрутизации на одном сетевом уровне, количество маршрутов примерно одинаковое.
	Резервное копирование конфигурации	—	Копии конфигурационной информации устройств создаются ежемесячно.
	Смена пароля	—	Смена паролей для входа в устройство производится раз в месяц.

9.3.5 Оптимизация сети

Задача 1. Оптимизация производительности

По мере развития предприятия внутренний трафик, особенно между вторым и третьим этажами, существенно увеличился. Канал между коммутаторами агрегации обладает недостаточной пропускной способностью для передачи такого большого объема трафика. Как оптимизировать работу канала?

Справочное решение

1. Можно добавить физические каналы между F2-AGG1 и F3-AGG1 и настроить агрегацию каналов Ethernet.
2. Можно изменить значения стоимости OSPF и реализовать балансировку нагрузки, чтобы часть трафика передавалась через CORE1.

9.4 Проверка

Подробности данной операции здесь не приводятся.

9.5 Справочные конфигурации

Конфигурация на маршрутизаторе

```
#
sysname Router
#
snmp-agent local-engineid 800007DB03000000000000
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap-hostname nms address 192.168.100.2 udp-port 162 tra
p-paramsname datacom
snmp-agent target-host trap-paramsname datacom v3 securityname test privacy
snmp-agent usm-user v3 test datacom authentication-mode md5 4DE14BB77015FFE895A
65FDE05B8F6E9 privacy-mode aes128 4DE14BB77015FFE895A65FDE05B8F6E9
snmp-agent trap source GigabitEthernet0/0/1
snmp-agent trap enable
snmp-agent
#
acl number 2000
rule 5 permit source 192.168.105.0 0.0.0.255
rule 10 permit source 192.168.106.0 0.0.0.255
rule 15 permit source 192.168.107.0 0.0.0.255
#
nat address-group 1 1.1.1.2 1.1.1.10
#
interface GigabitEthernet0/0/0
ip address 1.1.1.1 255.255.255.0
nat server protocol tcp global current-interface 8080 inside 192.168.100.1 www
nat outbound 2000 address-group 1
```

```
#
interface GigabitEthernet0/0/1
 ip address 192.168.204.1 255.255.255.252
#
ospf 1
 default-route-advertise always
 area 0.0.0.0
  network 192.168.204.0 0.0.0.3
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
return
```

Конфигурация на CORE1

```
#
sysname CORE1
#
vlan batch 100 105 201 to 202 204 to 205
#
dhcp enable
#
acl number 3000
 rule 5 deny ip source 192.168.105.0 0.0.0.255 destination 192.168.0.0 0.0.255.255
 rule 10 permit ip
#
ip pool ap-f1
 gateway-list 192.168.205.254
 network 192.168.205.0 mask 255.255.255.0
 excluded-ip-address 192.168.205.253
#
ip pool sta-f1
 gateway-list 192.168.105.254
 network 192.168.105.0 mask 255.255.255.0
#
interface Vlanif1
 ip address 192.168.1.254 255.255.255.0
#
interface Vlanif100
 ip address 192.168.100.254 255.255.255.0
#
interface Vlanif105
 ip address 192.168.105.254 255.255.255.0
 dhcp select global
#
interface Vlanif201
 ip address 192.168.201.1 255.255.255.252
#
interface Vlanif202
 ip address 192.168.202.1 255.255.255.252
#
interface Vlanif204
 ip address 192.168.204.2 255.255.255.252
#
interface Vlanif205
 ip address 192.168.205.254 255.255.255.0
```

```
dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 105 205
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 201
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 202
#
interface GigabitEthernet0/0/4
 port link-type access
 port default vlan 205
#
interface GigabitEthernet0/0/5
 port link-type access
 port default vlan 204
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.100.0 0.0.0.255
  network 192.168.105.0 0.0.0.255
  network 192.168.205.0 0.0.0.255
  network 192.168.201.0 0.0.0.3
  network 192.168.202.0 0.0.0.3
  network 192.168.204.0 0.0.0.3
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC635139
snmp-agent sys-info version v3
snmp-agent group v3 datcom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
 datcom v3
snmp-agent usm-user v3 test datcom authentication-mode md5 %_#_3UJ'3!M;9]$R@P:G
H1!! privacy-mode des56 %_#_3UJ'3!M;9]$R@P:GH1!!
snmp-agent trap source Vlanif1
snmp-agent trap enable
#
return
```

Конфигурация на F2-AGG1

```
#
sysname F2-AGG1
#
vlan batch 2 101 to 102 106 201 203 206
#
dhcp enable
#
ip pool admin
 gateway-list 192.168.102.254
```

```
network 192.168.102.0 mask 255.255.255.0
#
ip pool ap-f2
gateway-list 192.168.206.254
network 192.168.206.0 mask 255.255.255.0
option 43 sub-option 3 ascii 192.168.205.253
#
ip pool manager
gateway-list 192.168.101.254
network 192.168.101.0 mask 255.255.255.0
#
ip pool sta-f2
gateway-list 192.168.106.254
network 192.168.106.0 mask 255.255.255.0
#
interface Vlanif2
ip address 192.168.2.254 255.255.255.0
#
interface Vlanif101
ip address 192.168.101.254 255.255.255.0
dhcp select global
#
interface Vlanif102
ip address 192.168.102.254 255.255.255.0
dhcp select global
#
interface Vlanif106
ip address 192.168.106.254 255.255.255.0
dhcp select global
#
interface Vlanif201
ip address 192.168.201.2 255.255.255.252
#
interface Vlanif203
ip address 192.168.203.1 255.255.255.252
#
interface Vlanif206
ip address 192.168.206.254 255.255.255.0
dhcp select global
#
interface GigabitEthernet0/0/1
port link-type access
port default vlan 201
#
interface GigabitEthernet0/0/2
port link-type access
port default vlan 203
#
interface GigabitEthernet0/0/11
port link-type trunk
port trunk pvid vlan 2
port trunk allow-pass vlan 2 102
#
interface GigabitEthernet0/0/12
port link-type trunk
```

```
port trunk pvid vlan 2
port trunk allow-pass vlan 2 101 106 206
#
interface GigabitEthernet0/0/13
port link-type trunk
port trunk pvid vlan 2
port trunk allow-pass vlan 2 102
#
ospf 1
area 0.0.0.0
network 192.168.2.0 0.0.0.255
network 192.168.101.0 0.0.0.255
network 192.168.102.0 0.0.0.255
network 192.168.106.0 0.0.0.255
network 192.168.201.0 0.0.0.3
network 192.168.203.0 0.0.0.3
network 192.168.206.0 0.0.0.255
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC070327
snmp-agent sys-info version v3
snmp-agent group v3 datcom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
datcom v3
snmp-agent usm-user v3 test datcom authentication-mode md5 +3V3OM/)GC7M+H\V-;
(!!! privacy-mode des56 +3V3OM/)GC7M+H\V-;!!!
snmp-agent trap source Vlanif2
snmp-agent trap enable
#
return
```

Конфигурация на F3-AGG1

```
#
sysname F3-AGG1
#
vlan batch 3 103 to 104 107 202 to 203 207
#
ip pool ap-f3
gateway-list 192.168.207.254
network 192.168.207.0 mask 255.255.255.0
option 43 sub-option 3 ascii 192.168.205.253
#
ip pool marketing
gateway-list 192.168.103.254
network 192.168.103.0 mask 255.255.255.0
#
ip pool rd
gateway-list 192.168.104.254
network 192.168.104.0 mask 255.255.255.0
#
ip pool sta-f3
gateway-list 192.168.107.254
network 192.168.107.0 mask 255.255.255.0
#
interface Vlanif3
```

```
ip address 192.168.3.254 255.255.255.0
#
interface Vlanif103
ip address 192.168.103.254 255.255.255.0
dhcp select global
#
interface Vlanif104
ip address 192.168.104.254 255.255.255.0
dhcp select global
#
interface Vlanif107
ip address 192.168.107.254 255.255.255.0
dhcp select global
#
interface Vlanif202
ip address 192.168.202.2 255.255.255.252
#
interface Vlanif203
ip address 192.168.203.2 255.255.255.252
#
interface Vlanif207
ip address 192.168.207.254 255.255.255.0
dhcp select global
#
interface GigabitEthernet0/0/1
port link-type access
port default vlan 202
#
interface GigabitEthernet0/0/2
port link-type access
port default vlan 203
#
interface GigabitEthernet0/0/11
port link-type trunk
port trunk pvid vlan 3
port trunk allow-pass vlan 3 103 to 104
#
interface GigabitEthernet0/0/12
port link-type trunk
port trunk pvid vlan 3
port trunk allow-pass vlan 3 103 107 207
#
interface GigabitEthernet0/0/13
port link-type trunk
port trunk pvid vlan 3
port trunk allow-pass vlan 3 103 to 104
#
ospf 1
area 0.0.0.0
network 192.168.3.0 0.0.0.255
network 192.168.103.0 0.0.0.255
network 192.168.104.0 0.0.0.255
network 192.168.107.0 0.0.0.255
network 192.168.202.0 0.0.0.3
network 192.168.203.0 0.0.0.3
```

```
network 192.168.207.0 0.0.0.255
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCCFB0564
snmp-agent sys-info version v3
snmp-agent group v3 datcom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
datcom v3
snmp-agent usm-user v3 test datcom authentication-mode md5 5>5W!8N^H,L8E-@(C*:@
AQ!! privacy-mode des56 5>5W!8N^H,L8E-@(C*:@AQ!!
snmp-agent trap source Vlanif3
snmp-agent trap enable
#
return
```

Конфигурация на контроллере доступа

```
#
sysname AC
#
vlan batch 205
#
interface Vlanif205
ip address 192.168.205.253 255.255.255.0
#
interface GigabitEthernet0/0/1
port link-type access
port default vlan 205
#
snmp-agent local-engineid 800007DB0300000000000000
snmp-agent group v3 datcom privacy
snmp-agent target-host trap-hostname nms address 192.168.100.2 udp-port 162 trap-paramsname datcom
snmp-agent target-host trap-paramsname datcom v3 securityname %^%#TvWF~zi>Sgp
XL=P81^|^*^,(P&`UR97&h,l'eK8%^%# privacy
snmp-agent trap source Vlanif205
snmp-agent trap enable
snmp-agent
#
ip route-static 0.0.0.0 0.0.0.0 192.168.205.254
#
capwap source interface vlanif205
#
wlan
security-profile name WLAN-F1
security wpa-wpa2 psk pass-phrase %^%#53mQ@x*]z+u72&YdCR7A=11u&USV+g^Qw""O43X>%^%# aes
security-profile name WLAN-F2
security wpa-wpa2 psk pass-phrase %^%#YKB4ZI%zFQxmOS76yLo8],Z41lhJV"S[db(karoX%^%# aes
security-profile name WLAN-F3
security wpa-wpa2 psk pass-phrase %^%#|8)z/PyjU1ssX8Cr(3M=%x\{CP*t,BCahW84sqvK%^%# aes
ssid-profile name WLAN-F1
ssid WLAN-F1
ssid-profile name WLAN-F2
ssid WLAN-F2
ssid-profile name WLAN-F3
ssid WLAN-F3
vap-profile name WLAN-F1
```

```
service-vlan vlan-id 105
ssid-profile WLAN-F1
security-profile WLAN-F1
vap-profile name WLAN-F2
service-vlan vlan-id 106
ssid-profile WLAN-F2
security-profile WLAN-F2
vap-profile name WLAN-F3
service-vlan vlan-id 107
ssid-profile WLAN-F3
security-profile WLAN-F3
ap-group name WLAN-F1
radio 0
vap-profile WLAN-F1 wlan 1
radio 1
vap-profile WLAN-F1 wlan 1
radio 2
vap-profile WLAN-F1 wlan 1
ap-group name WLAN-F2
radio 0
vap-profile WLAN-F2 wlan 2
radio 1
vap-profile WLAN-F2 wlan 2
radio 2
vap-profile WLAN-F2 wlan 2
ap-group name WLAN-F3
radio 0
vap-profile WLAN-F3 wlan 2
radio 1
vap-profile WLAN-F3 wlan 2
radio 2
vap-profile WLAN-F3 wlan 2
ap-id 0 type-id 60 ap-mac 00e0-fcca-2e20 ap-sn 2102354483108B3A413A
ap-name F1-AP1
ap-group WLAN-F1
ap-id 1 type-id 60 ap-mac 00e0-fcfo-7bco ap-sn 210235448310D45A674C
ap-name F2-AP1
ap-group WLAN-F2
ap-id 2 type-id 60 ap-mac 00e0-fcb2-72fo ap-sn 210235448310C73E4033
ap-name F3-AP1
ap-group WLAN-F3
#
return
```

Конфигурация на F1-ACC1

```
#
sysname F1-ACC1
#
vlan batch 100 105 205
#
interface Vlanif1
ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
port link-type trunk
```



```
port trunk allow-pass vlan 100 105 205
#
interface GigabitEthernet0/0/2
port link-type access
port default vlan 100
#
interface GigabitEthernet0/0/3
port link-type access
port default vlan 100
#
interface GigabitEthernet0/0/4
port link-type access
port default vlan 100
#
interface GigabitEthernet0/0/5
port link-type access
port default vlan 100
#
interface GigabitEthernet0/0/6
port link-type access
port default vlan 100
#
interface GigabitEthernet0/0/7
port link-type access
port default vlan 100
#
interface GigabitEthernet0/0/8
port link-type access
port default vlan 100
#
interface GigabitEthernet0/0/9
port link-type access
port default vlan 100
#
interface GigabitEthernet0/0/10
port link-type access
port default vlan 100
#
interface GigabitEthernet0/0/20
port link-type trunk
port trunk pvid vlan 205
port trunk allow-pass vlan 105 205
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC03178D
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 3@^>FD5!85E'A!>CAH"1
U1!! privacy-mode des56 3@^>FD5!85E'A!>CAH"1U1!!
snmp-agent trap source Vlanif1
snmp-agent trap enable
#
```

```
return
```

Конфигурация на F2-ACC1

```
#
sysname F2-ACC1
#
vlan batch 2 102
#
interface Vlanif2
 ip address 192.168.2.1 255.255.255.0
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/4
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/5
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/6
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/7
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/8
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/9
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/10
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/11
 port link-type access
 port default vlan 102
#
```

```
interface Ethernet0/0/12
port link-type access
port default vlan 102
#
interface Ethernet0/0/13
port link-type access
port default vlan 102
#
interface Ethernet0/0/14
port link-type access
port default vlan 102
#
interface Ethernet0/0/15
port link-type access
port default vlan 102
#
interface Ethernet0/0/16
port link-type access
port default vlan 102
#
interface Ethernet0/0/17
port link-type access
port default vlan 102
#
interface Ethernet0/0/18
port link-type access
port default vlan 102
#
interface Ethernet0/0/19
port link-type access
port default vlan 102
#
interface Ethernet0/0/20
port link-type access
port default vlan 102
#
interface Ethernet0/0/21
port link-type access
port default vlan 102
#
interface Ethernet0/0/22
port link-type access
port default vlan 102
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 2
port trunk allow-pass vlan 2 102
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC456509
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
datacom v3
```

```
snmp-agent usm-user v3 test datcom authentication-mode md5 (H\O$K,P78:g;\H&H"Ma+A!!  
+A!! privacy-mode des56 (H\O$K,P78:g;\H&H"Ma+A!!  
snmp-agent trap source Vlanif2  
snmp-agent trap enable  
#  
return
```

Конфигурация на F2-ACC2

```
#  
sysname F2-ACC2  
#  
vlan batch 2 101 106 206  
#  
interface Vlanif1  
#  
interface Vlanif2  
ip address 192.168.2.2 255.255.255.0  
#  
interface Ethernet0/0/1  
port link-type access  
port default vlan 101  
#  
interface Ethernet0/0/2  
port link-type access  
port default vlan 101  
#  
interface Ethernet0/0/3  
port link-type access  
port default vlan 101  
#  
interface Ethernet0/0/4  
port link-type access  
port default vlan 101  
#  
interface Ethernet0/0/5  
port link-type access  
port default vlan 101  
#  
interface Ethernet0/0/6  
port link-type access  
port default vlan 101  
#  
interface Ethernet0/0/7  
port link-type access  
port default vlan 101  
#  
interface Ethernet0/0/8  
port link-type access  
port default vlan 101  
#  
interface Ethernet0/0/9  
port link-type access  
port default vlan 101  
#  
interface Ethernet0/0/10
```

```
port link-type access
port default vlan 101
#
interface Ethernet0/0/11
port link-type access
port default vlan 101
#
interface Ethernet0/0/12
port link-type access
port default vlan 101
#
interface Ethernet0/0/13
port link-type access
port default vlan 101
#
interface Ethernet0/0/14
port link-type access
port default vlan 101
#
interface Ethernet0/0/15
port link-type access
port default vlan 101
#
interface Ethernet0/0/16
port link-type access
port default vlan 101
#
interface Ethernet0/0/17
port link-type access
port default vlan 101
#
interface Ethernet0/0/18
port link-type access
port default vlan 101
#
interface Ethernet0/0/19
port link-type access
port default vlan 101
#
interface Ethernet0/0/20
port link-type trunk
port trunk pvid vlan 206
port trunk allow-pass vlan 106 206
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 2
port trunk allow-pass vlan 2 101 106 206
#
ip route-static 0.0.0.0 0.0.0.0 192.168.2.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCCA5263C
snmp-agent sys-info version v3
snmp-agent group v3 datcom privacy
```

```
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
  datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 RN,<EoK"S8Z3K7.NSN8+
L1!! privacy-mode des56 RN,<EoK"S8Z3K7.NSN8+L1!!
snmp-agent trap source Vlanif2
snmp-agent trap enable
#
return
```

Конфигурация на F2-ACC3

```
#
sysname F2-ACC3
#
vlan batch 2 102
#
interface Vlanif2
  ip address 192.168.2.3 255.255.255.0
#
interface Ethernet0/0/1
  port link-type access
  port default vlan 102
#
interface Ethernet0/0/2
  port link-type access
  port default vlan 102
#
interface Ethernet0/0/3
  port link-type access
  port default vlan 102
#
interface Ethernet0/0/4
  port link-type access
  port default vlan 102
#
interface Ethernet0/0/5
  port link-type access
  port default vlan 102
#
interface Ethernet0/0/6
  port link-type access
  port default vlan 102
#
interface Ethernet0/0/7
  port link-type access
  port default vlan 102
#
interface Ethernet0/0/8
  port link-type access
  port default vlan 102
#
interface Ethernet0/0/9
  port link-type access
  port default vlan 102
#
interface Ethernet0/0/10
```

```
port link-type access
port default vlan 102
#
interface Ethernet0/0/11
port link-type access
port default vlan 102
#
interface Ethernet0/0/12
port link-type access
port default vlan 102
#
interface Ethernet0/0/13
port link-type access
port default vlan 102
#
interface Ethernet0/0/14
port link-type access
port default vlan 102
#
interface Ethernet0/0/15
port link-type access
port default vlan 102
#
interface Ethernet0/0/16
port link-type access
port default vlan 102
#
interface Ethernet0/0/17
port link-type access
port default vlan 102
#
interface Ethernet0/0/18
port link-type access
port default vlan 102
#
interface Ethernet0/0/19
port link-type access
port default vlan 102
#
interface Ethernet0/0/20
port link-type access
port default vlan 102
#
interface Ethernet0/0/21
port link-type access
port default vlan 102
#
interface Ethernet0/0/22
port link-type access
port default vlan 102
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 2
port trunk allow-pass vlan 2 102
```

```
#
ip route-static 0.0.0.0 0.0.0.0 192.168.2.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC6E2774
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
    datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 :S@4*#J%O_-Mg=:>$BB:
7!!! privacy-mode des56 :S@4*#J%O_-Mg=:>$BB:7!!!
snmp-agent trap source Vlanif2
snmp-agent trap enable
#
return
```

Конфигурация на F3-ACC1

```
#
sysname F3-ACC1
#
vlan batch 3 103 to 104
#
interface Vlanif3
    ip address 192.168.3.1 255.255.255.0
#
interface Ethernet0/0/1
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/2
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/3
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/4
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/5
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/6
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/7
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/8
    port link-type access
```



```
port default vlan 103
#
interface Ethernet0/0/9
port link-type access
port default vlan 103
#
interface Ethernet0/0/10
port link-type access
port default vlan 103
#
interface Ethernet0/0/11
port link-type access
port default vlan 104
#
interface Ethernet0/0/12
port link-type access
port default vlan 104
#
interface Ethernet0/0/13
port link-type access
port default vlan 104
#
interface Ethernet0/0/14
port link-type access
port default vlan 104
#
interface Ethernet0/0/15
port link-type access
port default vlan 104
#
interface Ethernet0/0/16
port link-type access
port default vlan 104
#
interface Ethernet0/0/17
port link-type access
port default vlan 104
#
interface Ethernet0/0/18
port link-type access
port default vlan 104
#
interface Ethernet0/0/19
port link-type access
port default vlan 104
#
interface Ethernet0/0/20
port link-type access
port default vlan 104
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 3
port trunk allow-pass vlan 3 103 to 104
#
```

```
ip route-static 0.0.0.0 0.0.0.0 192.168.3.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCCC75F9A
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
    datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 FD5[3#*%a!/W$IOS;(RD
3Q!! privacy-mode des56 FD5[3#*%a!/W$IOS;(RD3Q!!
snmp-agent trap source Vlanif3
snmp-agent trap enable
#
return
```

Конфигурация на F3-ACC2

```
#
sysname F3-ACC2
#
vlan batch 3 103 107 207
#
interface Vlanif3
    ip address 192.168.3.2 255.255.255.0
#
interface MEth0/0/1
#
interface Ethernet0/0/1
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/2
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/3
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/4
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/5
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/6
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/7
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/8
```

```
port link-type access
port default vlan 103
#
interface Ethernet0/0/9
port link-type access
port default vlan 103
#
interface Ethernet0/0/10
port link-type access
port default vlan 103
#
interface Ethernet0/0/11
port link-type access
port default vlan 103
#
interface Ethernet0/0/12
port link-type access
port default vlan 103
#
interface Ethernet0/0/13
port link-type access
port default vlan 103
#
interface Ethernet0/0/14
port link-type access
port default vlan 103
#
interface Ethernet0/0/15
port link-type access
port default vlan 103
#
interface Ethernet0/0/16
port link-type access
port default vlan 103
#
interface Ethernet0/0/17
port link-type access
port default vlan 103
#
interface Ethernet0/0/18
port link-type access
port default vlan 103
#
interface Ethernet0/0/19
port link-type access
port default vlan 103
#
interface Ethernet0/0/20
port link-type trunk
port trunk pvid vlan 207
port trunk allow-pass vlan 107 207
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 3
```

```
port trunk allow-pass vlan 3 103 107 207
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCCF3804A
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
    datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 o=.SBW74%B[6NT]>.>:]
aA!! privacy-mode des56 o=.SBW74%B[6NT]>.>:]aA!!
snmp-agent trap source Vlanif3
snmp-agent trap enable
#
return
```

Конфигурация на F3-ACC3

```
#
sysname F3-ACC3
#
vlan batch 3 103 to 104
#
interface Vlanif3
    ip address 192.168.3.3 255.255.255.0
#
interface Ethernet0/0/1
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/2
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/3
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/4
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/5
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/6
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/7
    port link-type access
    port default vlan 103
#
interface Ethernet0/0/8
```

```
port link-type access
port default vlan 103
#
interface Ethernet0/0/9
port link-type access
port default vlan 103
#
interface Ethernet0/0/10
port link-type access
port default vlan 103
#
interface Ethernet0/0/11
port link-type access
port default vlan 104
#
interface Ethernet0/0/12
port link-type access
port default vlan 104
#
interface Ethernet0/0/13
port link-type access
port default vlan 104
#
interface Ethernet0/0/14
port link-type access
port default vlan 104
#
interface Ethernet0/0/15
port link-type access
port default vlan 104
#
interface Ethernet0/0/16
port link-type access
port default vlan 104
#
interface Ethernet0/0/17
port link-type access
port default vlan 104
#
interface Ethernet0/0/18
port link-type access
port default vlan 104
#
interface Ethernet0/0/19
port link-type access
port default vlan 104
#
interface Ethernet0/0/20
port link-type access
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 3
port trunk allow-pass vlan 3 103 to 104
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC224BC2
```

```
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 P'5R[2VCVEX8"$Y!=87`
1A!! privacy-mode des56 P'5R[2VCVEX8"$Y!=87`1A!!
snmp-agent trap source Vlanif3
snmp-agent trap enable
#
return
```

9.6 Вопросы

1. В этом проекте CORE1, F2-AGG1 и F3-AGG1 образуют физическое кольцо. Однако на этапе планирования и проектирования сети каналы, по которым осуществляется взаимодействие этих трех устройств, были назначены в разные VLAN. Следовательно, петля не формируется. Однако во время лабораторной работы вы обнаружили, что между двумя устройствами отношения соседства не устанавливаются или устанавливаются некорректно. Найдите основную причину и решение.
2. Что нового вы узнали благодаря этой лабораторной работе? Как эти знания смогут помочь вам в дальнейшей учебе или работе?

Справочные ответы на вопросы в лабораторных работах

Huawei VRP и основы конфигурирования

1. Ответ не приводится.
2. Команда **reset saved-configuration** удаляет содержимое файла конфигурации загрузки и отменяет предыдущую конфигурацию. Текущим файлом конфигурации системной загрузки является test.cfg. Таким образом, после выполнения этой команды содержимое файла test.cfg удаляется, а в качестве файла конфигурации загрузки используется файл конфигурации по умолчанию vrpcfg.zip. На шаге 4 текущая конфигурация сохраняется. Таким образом, после перезапуска устройства конфигурация остается неизменной.

Адресация и маршрутизация IPv4

1. Статический маршрут добавляется в таблицу маршрутизации при выполнении следующих условий:
 - a Следующий переход маршрута доступен.
 - b Маршрут является оптимальным маршрутом к сети или хосту назначения.Следовательно, когда следующий переход недоступен, маршрут не добавляется в таблицу IP-маршрутизации.
2. Когда на устройстве Huawei выполняется операция проверки связи ping, устройство определяет интерфейс-источник путем поиска в таблице маршрутизации. IP-адрес интерфейса-источника используется как IP-адрес источника пакетов ICMP.

Маршрутизация OSPF

1. Для возврата пакетов на R1 маршрутизатор R2 будет использовать маршрут R2->R1. После того, как стоимость GigabitEthernet0/0/3 на R1 изменится на 10, стоимость маршрута R1->R2 также будет 10. Следовательно, маршрутом от LoopBack0 на R1 до LoopBack0 на R2 станет маршрут R1->R3->R2. В этом случае R2 не будет знать, что стоимость GigabitEthernet0/0/3 на R1 изменилась на 10, и будет использовать прежнюю стоимость GigabitEthernet0/0/3 на R1 для расчета стоимости маршрута. Таким образом, в качестве маршрута для отправки ответных пакетов будет использоваться маршрут R2->R1.

Основы Ethernet и конфигурирование VLAN

План конфигурирования:

- Создание VLAN для ПК с особыми требованиями.
- Настройка привязки MAC-адресов ПК к сетям VLAN.
- Назначение интерфейсов в сети VLAN для реализации передачи уровня 2.

Процедура конфигурирования:

Создайте сети VLAN.

```
[S1]vlan 10
```

Установите привязку MAC-адреса ПК к VLAN 10.

```
[S1]vlan 10
[S1-vlan10]mac-vlan mac-address 00e0-fc1c-47a7
[S1-vlan10]quit
```

В данном примере ПК имеет MAC-адрес 00e0-fc1c-47a7.

Включите функцию назначения VLAN на основе MAC-адресов

```
[S1]interface gigabitethernet 0/0/1
[S1-GigabitEthernet0/0/1]mac-vlan enable
[S1-GigabitEthernet0/0/1]quit
```

Настройте GE0/0/1, подключенный к S2, в качестве гибридного порта, чтобы разрешить прохождение кадров данных соответствующей VLAN в нетегированном режиме.

```
[S1]interface gigabitethernet 0/0/1
[S1-GigabitEthernet0/0/1]port link-type hybrid
[S1-GigabitEthernet0/0/1]port hybrid untagged vlan 10
[S1-GigabitEthernet0/0/1]quit
```

Настройте GE0/0/2, подключенный к корпоративной сети, для реализации прозрачной передачи пакетов из сетей VLAN, имеющих привязку к MAC-адресам.

```
[S1]interface gigabitethernet 0/0/2
[S1-GigabitEthernet0/0/2]port link-type trunk
[S1-GigabitEthernet0/0/2]port trunk allow-pass vlan 10
[S1-GigabitEthernet0/0/2]quit
```

Протокол связующего дерева (STP)

1. Нет. После получения пакетов BPDU протокола STP все мосты добавляют стоимость локального порта к RPC в блоках BPDU для расчета стоимости корневого маршрута порта. Следовательно, при изменении стоимости GigabitEthernet 0/0/14 на S1 стоимость корневого маршрута S4 не изменится.
2. Необходимо изменить приоритет GigabitEthernet0/0/11 на S1.
3. Нет. Канал между S1 и S2 образует петлю. Следовательно, нужно заблокировать один канал.

Агрегирование каналов Ethernet

1. Наименьшее количество активных каналов должно быть меньше или равно максимальному количеству активных каналов.

Связь между VLAN

1. Необходимо создать интерфейс уровня 3 на S1 для подключения к GigabitEthernet0/0/1 маршрутизатора R1 и настроить маршрут к соответствующей сети.
2. Когда какой-либо физический интерфейс, разрешающий прохождение VLAN, перейдет в активное состояние (Up), соответствующий интерфейс VLANIF также перейдет в активное состояние (Up).

Настройка ACL

План конфигурирования:

- Настройка OSPF для обеспечения возможности сетевого подключения.
- Включение Telnet и FTP на маршрутизаторе R3.
- Настройка расширенного ACL для сопоставления нужного трафика.

Процедура конфигурирования:

Настройте сетевое подключение, Telnet и FTP.

Настройте ACL на R2.

```
[R2] acl 3001
[R2-acl-adv-3001] rule 5 permit tcp source 10.1.2.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port eq 23
[R2-acl-adv-3001] rule 10 permit tcp source 10.1.1.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port range 20 21
[R2-acl-adv-3001] rule 15 deny tcp source any
[R2-acl-adv-3001] quit
```

Примените ACL на GE0/0/3 маршрутизатора R2.

```
[R2] interface GigabitEthernet0/0/3
[R2-GigabitEthernet0/0/3] traffic-filter inbound acl 3001
```

Настройка локального механизма AAA

Ответ не приводится.

Настройка NAT

1. Не должны.

Настройка FTP

1. В активном режиме.

Конфигурирование DHCP

1. Пул адресов интерфейса содержит только IP-адреса в той же подсети, что и интерфейс.
Глобальный пул адресов может содержать IP-адреса в той же подсети, что и интерфейс, или IP-адреса разных подсетей (как в сети ретрансляции DHCP).
2. В сценарии без агента ретрансляции пул IP-адресов в той же подсети, что и интерфейс, выбирается из глобальных пулов адресов, и IP-адреса назначаются клиентам в соответствии с параметрами пула адресов. В сценарии с агентом ретрансляции пул IP-адресов в требуемой подсети выбирается из глобальных пулов адресов на основе подсети, запрошенной агентом ретрансляции, и IP-адреса назначаются клиентам в соответствии с параметрами пула адресов.

Создание WLAN

1. Никакого влияния. Выполняется прямая передача, и данные не проходят через GigabitEthernet0/0/10 контроллера доступа. При туннельной передаче необходимо будет настроить GigabitEthernet0/0/10, чтобы разрешить прохождение пакетов из VLAN 101. В противном случае STA не смогут получить доступ к S1.

2. AP1 и AP2 используют разные профили VAP, и в профилях VAP необходимо настроить разные сервисные VLAN.

Создание сети IPv6

1. Маршрутизатор имеет несколько интерфейсов в сети FE80::/10. Когда IPv6-адрес назначения является локальным адресом канала, интерфейс-источник невозможно будет определить путем запроса таблицы маршрутизации. Таким образом, интерфейс-источник необходимо указать.
2. В режиме с отслеживанием состояния все 128 бит IPv6-адреса интерфейса задает сервер DHCPv6. В режиме без отслеживания состояния 64-битный идентификатор интерфейса создается на основе спецификации EUI-64.

Конфигурирование кампусной сети

1. Хотя функция предотвращения петель реализована на уровне VLAN, физические петли по-прежнему формируются. BPDU STP не содержат теги VLAN. Следовательно, один из каналов между тремя коммутаторами необходимо заблокировать. По этой причине не удастся установить отношения соседства между двумя коммутаторами. На практике предотвращение петель реализовано на уровне VLAN. Таким образом, можно отключить STP на интерфейсах между устройствами.
2. Ответ не приводится.

Основы сетевого программирования и автоматизации

1. Для написания сценария построчной настройки интерфейсов устройств воспользуйтесь функцией write() модуля telnetlib.
2. Подробнее см. стандартную библиотеку Python.