Сертификация Huawei

HCIA-Routing&Switching

ПРОМЕЖУТОЧНЫЙ УРОВЕНЬ

Сетевые технологии и устройства Huawei

Руководство по лабораторным работам

Huawei Technologies Co.,Ltd

Сертификация Huawei

HCIA-Routing&Switching
Сетевые технологии и устройства Huawei

Руководство по лабораторным работам: промежуточный уровень

Версия 2.5

Система сертификации Huawei

Благодаря мощной и профессиональной системе технической подготовки и сертификации, в соответствии с требованиями клиентов различных уровней ИКТ компания Huawei стремится предоставить клиентам аутентичную, профессиональную сертификацию и удовлетворяет потребности в развитии качеств инженеров, способных поддерживать работу корпоративных сетей в условиях постоянно меняющейся среды ИКТ. Портфель сертификатов Huawei в области технологий маршрутизации и коммутации (R&S) состоит из трех уровней и позволяет содействовать развитию и проверке навыков и знаний клиентов в области технологий маршрутизации и коммутации.

Уровень сертификации Huawei Certified Network Associate (HCIA) подтверждает навыки и знания инженеров IP-сетей по внедрению и поддержке малых и средних корпоративных сетей. Сертификация HCIA предоставляет богатую техническую базу навыков и знаний для создания таких корпоративных сетей, а также возможность внедрения услуг и функций в рамках существующих корпоративных сетей для эффективной поддержки отраслевой деятельности.

Сертификация HCIA охватывает базовые навыки работы с TCP/IP, маршрутизацией, коммутацией и соответствующими сетевыми IP-технологиями и продуктами передачи данных Huawei, а также навыки эксплуатации и управления универсальной платформой маршрутизации (VRP).

Сертификация Huawei Certified Network Professional (HCIP-R&S) предназначена для инженеров по корпоративным сетям, занимающихся проектированием и техническим обслуживанием, а также для специалистов, желающих углубленно изучить технологии маршрутизации, коммутации, эффективности и оптимизации сети. HCIP-R&S состоит из трех блоков, включая внедрение корпоративной сети маршрутизации и коммутации (IERS), улучшение производительности корпоративной сети (IENP) и реализацию инженерного проекта корпоративной сети (IEEP), которая, в свою очередь, включает в себя передовые принципы технологии маршрутизации и коммутации IPv4, безопасность сети, высокий уровень доступности и QoS, а также применение таких технологий в продукции Huawei.

Сертификация Huawei Certified Internet Expert (HCIE-R&S) позволяет инженерам овладеть разнообразными знаниями о сетевых IP-технологиях и навыками техобслуживания, диагностики и устранения неисправностей оборудования Huawei, а также глубокими знаниями в сфере планирования, проектирования и оптимизации крупномасштабных IP-сетей.

Условные обозначения

Маршрутизатор

Коммутатор

Межсетевой экран

Облако

Канал Ethernet

Последовательный канал

СОДЕРЖАНИЕ

Модуль 1 Ethernet и VLAN

Лабораторная работа 1-1 Конфигурация интерфейса и канала Ethernet

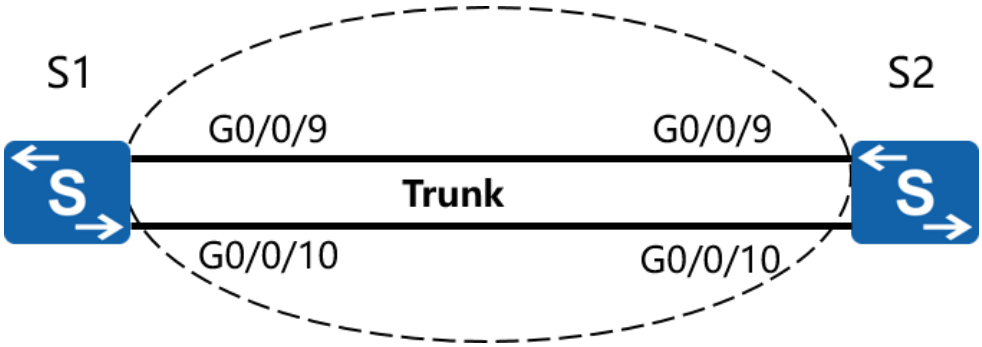
Цели обучения

В ходе данной лабораторной работы вам необходимо выполнить следующие задания:

- Ручная установка скорости линии на интерфейсе.
- Настройка агрегации каналов в ручном режиме.
- Настройка агрегации каналов в статическом режиме LACP.
- Управление приоритетом интерфейсов в статическом режиме LACP.

Топология

Рис. 1-1 Топология агрегации канала Ethernet



Сценарий

Администратору существующей корпоративной сети поступил запрос на повышение эффективности соединения между коммутаторами за счет подготовки коммутаторов к поддержке агрегации каналов перед установкой агрегации каналов вручную, причем необходимо настроить среду между коммутаторами в качестве смежных каналов.

Задания

Шаг 1 Выполнение основных настроек на коммутаторах Ethernet

По умолчанию на интерфейсах коммутатора Huawei включено автосогласование. Скорости G0/0/9 и G0/0/10 на S1 и S2 должны быть установлены вручную.

Измените имя системы и просмотрите подробную информацию для G0/0/9 и G0/0/10 на S1.

```
<Quidway>system-view
[Quidway]sysname S1
[S1]display interface GigabitEthernet 0/0/9
GigabitEthernet0/0/9 current state : UP
Line protocol current state : UP
```

Description:
Switch Port, Link-type : trunk(negotiated),
PVID : 1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is d0d0-4ba6-aab0
Current system time: 2016-11-23 14:18:37
Port Mode: COMMON COPPER
Speed : 1000, Loopback: NONE
Duplex: FULL, Negotiation: ENABLE
Mdi : AUTO, Flow-control: DISABLE
Last 300 seconds input rate 256 bits/sec, 0 packets/sec
Last 300 seconds output rate 912 bits/sec, 0 packets/sec
Input peak rate 13976 bits/sec, Record time: 2016-11-22 14:59:12
Output peak rate 13976 bits/sec, Record time: 2016-11-22 14:59:12

Input: 8802 packets, 1242101 bytes
  Unicast: 854, Multicast: 7017
  Broadcast: 931, Jumbo: 0
  Discard: 0, Pause: 0
  Frames: 0

  Total Error: 0
  CRC: 0, Giants: 0
  Jabbers: 0, Fragments: 0
  Runts: 0, DropEvents: 0
  Alignments: 0, Symbols: 0
  Ignoreds: 0

Output: 53495 packets, 7626413 bytes
  Unicast: 231, Multicast: 49564
  Broadcast: 3700, Jumbo: 0
  Discard: 0, Pause: 0

  Total Error: 0
  Collisions: 0, ExcessiveCollisions: 0
  Late Collisions: 0, Deferreds: 0
  Buffers Purged: 0

    Input bandwidth utilization threshold : 80.00%
    Output bandwidth utilization threshold: 80.00%
    Input bandwidth utilization : 0%
    Output bandwidth utilization : 0%
[S1]display interface GigabitEthernet 0/0/10
GigabitEthernet0/0/10 current state : UP
Line protocol current state : UP
Description:
Switch Port, Link-type : trunk(negotiated),
PVID : 1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is d0d0-4ba6-aab0
Current system time: 2016-11-23 14:22:22
Port Mode: COMMON COPPER
Speed : 1000, Loopback: NONE
Duplex: FULL, Negotiation: ENABLE
Mdi : AUTO, Flow-control: DISABLE
Last 300 seconds input rate 72 bits/sec, 0 packets/sec
Last 300 seconds output rate 1024 bits/sec, 0 packets/sec

```
Input peak rate 14032 bits/sec, Record time: 2016-11-22 14:59:12
Output peak rate 14032 bits/sec, Record time: 2016-11-22 14:59:12

Input:  7025 packets, 786010 bytes
  Unicast:                0,  Multicast:              7025
  Broadcast:              0,  Jumbo:                     0
  Discard:                0,  Pause:                     0
  Frames:                 0

  Total Error:            0
  CRC:                      0,  Giants:                  0
  Jabbers:                0,  Fragments:               0
  Runts:                    0,  DropEvents:              0
  Alignments:             0,  Symbols:                 0
  Ignoreds:               0

Output:  54507 packets, 7979793 bytes
  Unicast:              150,  Multicast:            49709
  Broadcast:           4648,  Jumbo:                   0
  Discard:                0,  Pause:                    0

  Total Error:            0
  Collisions:             0,  ExcessiveCollisions:     0
  Late Collisions:        0,  Deferreds:               0
  Buffers Purged:         0

    Input bandwidth utilization threshold : 80,00%
    Output bandwidth utilization threshold: 80,00%
    Input bandwidth utilization   :     0%
    Output bandwidth utilization :      0%
```

Для скорости G0/0/9 и G0/0/10 на S1 установите значение 100 Мбит/с. Перед изменением скорости интерфейса отключите автосогласование.

```
[S1]interface GigabitEthernet 0/0/9
[S1-GigabitEthernet0/0/9]undo negotiation auto
[S1-GigabitEthernet0/0/9]speed 100
[S1-GigabitEthernet0/0/9]quit
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]undo negotiation auto
[S1-GigabitEthernet0/0/10]speed 100
```

Для скорости G0/0/9 и G0/0/10 на S2 установите значение 100 Мбит/с.

```
<Quidway>system-view
[Quidway]sysname S2
[S2]interface GigabitEthernet 0/0/9
[S2-GigabitEthernet0/0/9]undo negotiation auto
[S2-GigabitEthernet0/0/9]speed 100
[S2-GigabitEthernet0/0/9]quit
[S2]interface GigabitEthernet 0/0/10
[S2-GigabitEthernet0/0/10]undo negotiation auto
[S2-GigabitEthernet0/0/10]speed 100
```

Убедитесь, что на S1 установлены скорости G0/0/9 и G0/0/10.

```
[S1]display interface GigabitEthernet 0/0/9
```

```
GigabitEthernet0/0/9 current state : UP
Line protocol current state : UP
Description:
Switch Port, Link-type : trunk(negotiated),
PVID :       1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is d0d0-4ba6-aab0
Current system time: 2016-11-23 14:29:45
Port Mode: COMMON COPPER
Speed : 100,       Loopback: NONE
Duplex: FULL,      Negotiation: DISABLE
Mdi     : AUTO,     Flow-control: DISABLE
……output omit……

[S1]display interface GigabitEthernet 0/0/10
GigabitEthernet0/0/10 current state : UP
Line protocol current state : UP
Description:
Switch Port, Link-type : trunk(negotiated),
PVID :       1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is d0d0-4ba6-aab0
Current system time: 2016-11-23 14:32:53
Port Mode: COMMON COPPER
Speed : 100,       Loopback: NONE
Duplex: FULL,      Negotiation: DISABLE
Mdi     : AUTO,     Flow-control: DISABLE
……output omit……
```

Шаг 2 Настройка агрегации канала вручную

Создайте Eth-Trunk 1 на S1 и S2. Удалите конфигурацию по умолчанию с G0/0/9 и G0/0/10 на S1 и S2, а затем добавьте G0/0/9 и G0/0/10 в Eth-Trunk 1.

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]quit
[S1]interface GigabitEthernet 0/0/9
[S1-GigabitEthernet0/0/9]eth-trunk 1
[S1-GigabitEthernet0/0/9]quit
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]eth-trunk 1

[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]quit
[S2]interface GigabitEthernet 0/0/9
[S2-GigabitEthernet0/0/9]eth-trunk 1
[S2-GigabitEthernet0/0/9]quit
[S2]interface GigabitEthernet 0/0/10
[S2-GigabitEthernet0/0/10]eth-trunk 1
```

Проверьте конфигурацию 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: 8
Operate status: up                 Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
```

```
PortName                      Status      Weight
GigabitEthernet0/0/9          Up          1
GigabitEthernet0/0/10         Up          1

[S2]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: 8
Operate status: up                Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
PortName                      Status      Weight
GigabitEthernet0/0/9          Up          1
GigabitEthernet0/0/10         Up          1
```

Строки, выделенные серым цветом, указывают на то, что Eth-Trunk работает правильно.

Шаг 3 Конфигурирование агрегации каналов в статическом режиме LACP

Удалите настройки с G0/0/9 и G0/0/10 на S1 и S2.

```
[S1]interface GigabitEthernet 0/0/9
[S1-GigabitEthernet0/0/9]undo eth-trunk
[S1-GigabitEthernet0/0/9]quit
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]undo eth-trunk

[S2]interface GigabitEthernet 0/0/9
[S2-GigabitEthernet0/0/9]undo eth-trunk
[S2-GigabitEthernet0/0/9]quit
[S2]interface GigabitEthernet 0/0/10
[S2-GigabitEthernet0/0/10]undo eth-trunk
```

Создайте Eth-Trunk 1 и установите режим балансировки нагрузки Eth-Trunk в качестве статического режима LACP.

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]mode lacp
[S1-Eth-Trunk1]quit
[S1]interface GigabitEthernet 0/0/9
[S1-GigabitEthernet0/0/9]eth-trunk 1
[S1-GigabitEthernet0/0/9]quit
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]eth-trunk 1

[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]mode lacp
[S2-Eth-Trunk1]quit
[S2]interface GigabitEthernet 0/0/9
[S2-GigabitEthernet0/0/9]eth-trunk 1
[S2-GigabitEthernet0/0/9]interface GigabitEthernet 0/0/10
[S2-GigabitEthernet0/0/10]eth-trunk 1
```

Убедитесь, что на двух каналах включен статический режим LACP.

```
[S1]display eth-trunk
Eth-Trunk1's state information is:
Local:
```

```
LAG ID: 1                         WorkingMode: LACP
Preempt Delay: Disabled           Hash arithmetic: According to SIP-XOR-DIP
System Priority: 32768            System ID: d0d0-4ba6-aab0
Least Active-linknumber: 1        Max Active-linknumber: 8
Operate status: up                Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName              Status     PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/9       Selected   100M     32768   1      289     10111100   1
GigabitEthernet0/0/10      Selected   100M     32768   2      289     10111100   1

Partner:
--------------------------------------------------------------------------------
ActorPortName              SysPri     SystemID        PortPri PortNo PortKey PortState
GigabitEthernet0/0/9       32768      d0d0-4ba6-ac20  32768   1      289     10111100
GigabitEthernet0/0/10      32768      d0d0-4ba6-ac20  32768   2      289     10111100
```

Установите приоритет системы на S1 равным 100, чтобы S1 оставался Actor.

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

Установите приоритет интерфейса и определите активные каналы на S1.

```
[S1]interface GigabitEthernet 0/0/9
[S1-GigabitEthernet0/0/9]lacp priority 100
[S1-GigabitEthernet0/0/9]quit
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]lacp priority 100
```

Проверьте конфигурацию Eth-Trunk.

```
[S1]display    eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                         WorkingMode: LACP
Preempt Delay: Disabled           Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100              System ID: d0d0-4ba6-aab0
Least Active-linknumber: 1        Max Active-linknumber: 8
Operate status: up                Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName              Status     PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/9       Selected   100M     100     1      289     10111100   1
GigabitEthernet0/0/10      Selected   100M     100     2      289     10111100   1
Partner:
--------------------------------------------------------------------------------
ActorPortName              SysPri     SystemID        PortPri PortNo PortKey PortState
GigabitEthernet0/0/9       32768      d0d0-4ba6-ac20  32768   1      289     10111100
GigabitEthernet0/0/10      32768      d0d0-4ba6-ac20  32768   2      289     10111100

[S2]display    eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                         WorkingMode: LACP
Preempt Delay: Disabled           Hash arithmetic: According to SIP-XOR-DIP
System Priority: 32768            System ID: d0d0-4ba6-ac20
Least Active-linknumber: 1        Max Active-linknumber: 8
Operate status: up                Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
```

```
ActorPortName              Status     PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/9       Selected 100M       32768       1       289       10111100      1
GigabitEthernet0/0/10      Selected 100M       32768       2       289       10111100      1

Partner:
------------------------------------------------------------------------------
ActorPortName              SysPri     SystemID            PortPri PortNo PortKey PortState
GigabitEthernet0/0/9       100        d0d0-4ba6-aab0      100     1      289     10111100
GigabitEthernet0/0/10      100        d0d0-4ba6-aab0      100     2      289     10111100
```

Окончательная конфигурация

```
[S1]display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S1
#
 lacp priority 100
#
interface Eth-Trunk1
 mode lacp
#
interface GigabitEthernet0/0/9
 eth-trunk 1
 lacp priority 100
 undo negotiation auto
 speed 100
#
interface GigabitEthernet0/0/10
 eth-trunk 1
 lacp priority 100
 undo negotiation auto
 speed 100
#
return

[S2]display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S2
#
interface Eth-Trunk1
 mode lacp
#
interface GigabitEthernet0/0/9
 eth-trunk 1
 undo negotiation auto
 speed 100
#
interface GigabitEthernet0/0/10
 eth-trunk 1
 undo negotiation auto
 speed 100
#
return
```

Лабораторная работа 1-2 Конфигурация VLAN

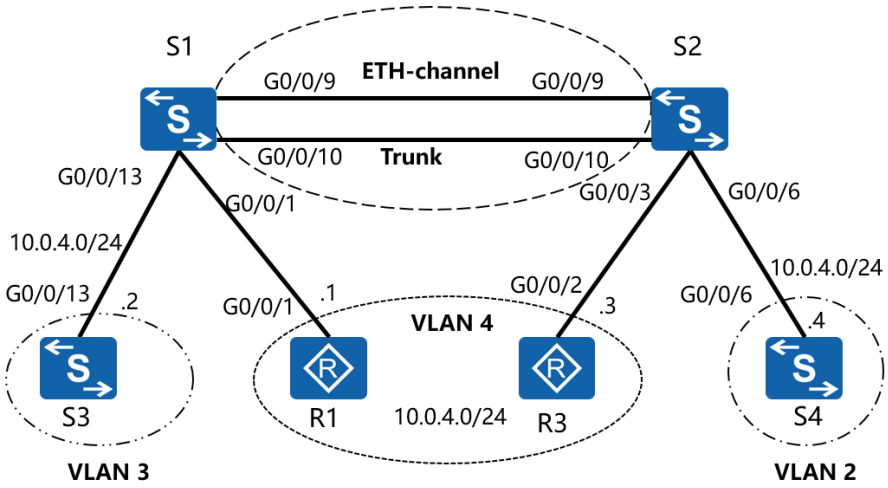
Цели обучения

В ходе данной лабораторной работы вам необходимо выполнить следующие задания:

- Назначение интерфейсов портов в качестве портов доступа и магистральных портов.
- Создание VLAN.
- Настройка тегирования VLAN для портов с использованием типа связи гибридного порта.
- Настройка VLAN по умолчанию для интерфейса с помощью идентификатора VLAN порта.

Топология

Рис. 1-2 Топология VLAN



Сценарий

В настоящее время корпоративная сеть работает в одном широковещательном домене. Это приводит к тому, что большой объем трафика передается на все узлы сети. Требуется, чтобы администратор попытался контролировать поток трафика на канальном уровне путем внедрения решения VLAN. Решения VLAN должны применяться к коммутаторам S1 и S2.

Задания

Шаг 1 Подготовка среды

Если вы еще не произвели настройку устройства, начните с шага 1, а затем перейдите к шагу 2. Для тех, кто продолжает предыдущие лабораторные работы, необходимо начать с шага 2.

Установите соединение по каналу Eth-trunk между S1 и S2.

```
<Quidway>system-view
```

```
[Quidway]sysname S1
[S1]interface Eth-trunk 1
[S1-Eth-Trunk1]mode lacp
[S1-Eth-Trunk1]quit
[S1]interface GigabitEthernet0/0/9
[S1-Gigabitethernet0/0/9]eth-trunk 1
[S1-Gigabitethernet0/0/9]interface GigabitEthernet0/0/10
[S1-Gigabitethernet0/0/10]eth-trunk 1
```

На S2 добавьте интерфейсы к Eth-Trunk с помощью представления Eth-Trunk.

```
<Quidway>system-view
[Quidway]sysname S2
[S2]interface eth-trunk 1
[S2-Eth-Trunk1]mode lacp
[S2-Eth-Trunk1]trunkport GigabitEthernet 0/0/9
[S2-Eth-Trunk1]trunkport GigabitEthernet 0/0/10
```

Шаг 2 Отключение неиспользуемых интерфейсов и установка магистрали VLAN

Неиспользуемые интерфейсы должны быть отключены для обеспечения точности результатов тестирования. В данной лабораторной работе необходимо отключить интерфейсы Ethernet 0/0/1 и Ethernet 0/0/7 на S3, Ethernet0/0/1 и Ethernet0/0/14 на S4.

```
<Quidway>system-view
Enter system view, return user view with Ctrl+Z.
[Quidway]sysname S3
[S3]interface Ethernet 0/0/1
[S3-Ethernet0/0/1]shutdown
[S3-Ethernet0/0/1]quit
[S3]interface Ethernet 0/0/7
[S3-Ethernet0/0/7]shutdown
[Quidway]sysname S4
[S4]interface Ethernet 0/0/1
[S4-Ethernet0/0/1]shutdown
[S4-Ethernet0/0/1]quit
[S4]interface Ethernet 0/0/14
[S4-Ethernet0/0/14]shutdown
```

По умолчанию для типа соединения интерфейса порта коммутатора установлено значение hybrid. Настройте port link-type для Eth-Trunk 1 в режиме trunk port. Кроме того, разрешите использование всех VLAN через trunk port.

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]port link-type trunk
[S1-Eth-Trunk1]port trunk allow-pass vlan all
[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]port link-type trunk
[S2-Eth-Trunk1]port trunk allow-pass vlan all
```

Шаг 3 Конфигурирование VLAN

Используйте S3, R1, R3 и S4 в качестве хостов, не поддерживающих VLAN. Существует два метода создания VLAN и два метода для привязки интерфейсов к созданным VLAN. Для демонстрации этих двух методов используются S1 и S2. Все интерфейсы, связанные с хостами, должны быть настроены как порты доступа (access port).

На S1 свяжите интерфейс Gigabit Ethernet 0/0/13 с VLAN 3, а интерфейс Gigabit Ethernet 0/0/1 — с VLAN 4.

На S2 свяжите интерфейс Gigabit Ethernet 0/0/3 с VLAN4, а интерфейс Gigabit Ethernet 0/0/6 — с VLAN 2.

```
[S1]interface GigabitEthernet0/0/13
[S1-GigabitEthernet0/0/13]port link-type access
[S1-GigabitEthernet0/0/13]quit
[S1]interface GigabitEthernet0/0/1
[S1-GigabitEthernet0/0/1]port link-type access
[S1-GigabitEthernet0/0/1]quit
[S1]vlan 2
[S1-vlan2]vlan 3
[S1-vlan3]port GigabitEthernet0/0/13
[S1-vlan3]vlan 4
[S1-vlan4]port GigabitEthernet0/0/1
[S2]vlan batch 2 to 4
[S2]interface GigabitEthernet 0/0/3
[S2-GigabitEthernet0/0/3]port link-type access
[S2-GigabitEthernet0/0/3]port default vlan 4
[S2-GigabitEthernet0/0/3]quit
[S2]interface GigabitEthernet 0/0/6
[S2-GigabitEthernet0/0/6]port link-type access
[S2-GigabitEthernet0/0/6]port default vlan 2
```

Убедитесь, что конфигурация VLAN правильно применена к S1 и S2.

```
<S1>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:GE0/0/2(U)   GE0/0/3(U)        GE0/0/4(U)        GE0/0/5(U)
                       GE0/0/6(D)      GE0/0/7(D)        GE0/0/8(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(U)     GE0/0/22(U)       GE0/0/23(U)       GE0/0/24(D)
                       Eth-Trunk1(U)
2     common     TG:Eth-Trunk1(U)
3     common     UT:GE0/0/13(U)
                 TG:Eth-Trunk1(U)
4     common     UT:GE0/0/1(U)
                 TG:Eth-Trunk1(U)
…output omitted…
<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(U)        GE0/0/4(U)        GE0/0/5(U)
                      GE0/0/7(D)      GE0/0/8(D)        GE0/0/11(U)       GE0/0/12(U)
                GE0/0/13(U)     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)
                Eth-Trunk1(U)
2     common    UT:GE0/0/6(U)
                TG:Eth-Trunk1(U)
3     common    UT:GE0/0/13(U)
                TG:Eth-Trunk1(U)
4     common    UT:GE0/0/1(U)
                TG:Eth-Trunk1(U)
…output omitted…
```

Выделенные записи подтверждают привязку интерфейсов к каждой созданной VLAN. Разрешено использование всех VLAN через магистральный (TG) порт Eth-Trunk 1.

Шаг 4 Настройка IP-адресации для каждой VLAN

Настройте IP-адреса на хостах, R1, S3, R3 и S4 как часть соответствующих VLAN. Невозможно произвести настройку IP-адресов для физических интерфейсов портов на коммутаторах, поэтому настройте собственный интерфейс управления Vlanif1 с IP-адресом для коммутатора.

```
<Huawei>system-view
[Huawei]sysname R1
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.4.1 24
[S3]interface vlanif 1
[S3-vlanif1]ip address 10.0.4.2 24
<Huawei>system-view
[Huawei]sysname R3
[R3]interface GigabitEthernet0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.0.4.3 24
[S4]interface vlanif 1
[S4-vlanif1]ip address 10.0.4.4 24
```

Шаг 5 Проверка конфигурации путем проверки подключения

Воспользуйтесь командой **ping**. R1 и R3 в VLAN 4 должны иметь возможность передачи данных друг другу. Устройства в другой VLAN не должны взаимодействовать друг с другом.

```
[R1]ping 10.0.4.3
  PING 10.0.4.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.3: bytes=56 Sequence=1 ttl=255 time=6 ms
    Reply from 10.0.4.3: bytes=56 Sequence=2 ttl=255 time=2 ms
    Reply from 10.0.4.3: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 10.0.4.3: bytes=56 Sequence=4 ttl=255 time=2 ms
    Reply from 10.0.4.3: bytes=56 Sequence=5 ttl=255 time=2 ms
  --- 10.0.4.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 2/2/6 ms
[R1]ping 10.0.4.4
  PING 10.0.4.4: 56  data bytes, press CTRL_C to break
```

```
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
  --- 10.0.4.4 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
100.00% packet loss
```

Вы можете попробовать настроить передачу данных между R1 и S3, а также R3 и S4.

Шаг 6 Конфигурирование гибридного интерфейса

Используйте тип соединения гибридного порта, чтобы обеспечить возможность тщательного управления тегированием VLAN на уровне интерфейса порта. Для обеспечения приема тегированных кадров VLAN 2 из VLAN 4 и наоборот мы будем использовать гибридные порты.

Установите тип соединения порта интерфейса порта Gigabit Ethernet 0/0/1 порта S1 и интерфейсы Gigabit Ethernet 0/0/3 и 0/0/6 S2 в качестве гибридных портов. Дополнительно на гибридных портах произведите отмену тегирования всех кадров, связанных с VLAN 2 и VLAN 4.

```
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]undo port default vlan
[S1-GigabitEthernet0/0/1]port link-type hybrid
[S1-GigabitEthernet0/0/1]port hybrid untagged vlan 2 4
[S1-GigabitEthernet0/0/1]port hybrid pvid vlan 4

[S2]interface GigabitEthernet 0/0/3
[S2-GigabitEthernet0/0/3]undo port default vlan
[S2-GigabitEthernet0/0/3]port link-type hybrid
[S2-GigabitEthernet0/0/3]port hybrid untagged vlan 2 4
[S2-GigabitEthernet0/0/3]port hybrid pvid vlan 4
[S2-GigabitEthernet0/0/3]quit
[S2]interface GigabitEthernet 0/0/6
[S2-GigabitEthernet0/0/6]undo port default vlan
[S2-GigabitEthernet0/0/6]port link-type hybrid
[S2-GigabitEthernet0/0/6]port hybrid untagged vlan 2 4
[S2-GigabitEthernet0/0/6]port hybrid pvid vlan 2
```

Выполнение команды **port hybrid pvid vlan** гарантирует, что кадры, полученные от хоста, будут маркированы тегом соответствующей VLAN. Для кадров, полученных от VLAN 2 или VLAN 4, будет отменено тегирование на интерфейсе до того, как они будут перенаправлены на хост.

С помощью команды ping убедитесь, что R3 в VLAN 4 все еще доступен.

```
<R1>ping 10.0.4.3
  PING 10.0.4.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.3: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.4.3: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.4.3: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.4.3: bytes=56 Sequence=4 ttl=255 time=10 ms
    Reply from 10.0.4.3: bytes=56 Sequence=5 ttl=255 time=1 ms
  --- 10.0.4.3 ping statistics ---
    5 packet(s) transmitted
```

```
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 1/2/10 ms
```

Используйте команду ping, чтобы проверить, доступен ли теперь S4 в VLAN 2 из R1 в VLAN 4.

```
<R1>ping 10.0.4.4
  PING 10.0.4.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.4: bytes=56 Sequence=1 ttl=255 time=41 ms
    Reply from 10.0.4.4: bytes=56 Sequence=2 ttl=254 time=2 ms
    Reply from 10.0.4.4: bytes=56 Sequence=3 ttl=254 time=3 ms
    Reply from 10.0.4.4: bytes=56 Sequence=4 ttl=254 time=2 ms
    Reply from 10.0.4.4: bytes=56 Sequence=5 ttl=254 time=2 ms
  --- 10.0.4.4 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 2/10/41 ms
```

При использовании типа соединения гибридного порта кадры из VLAN 4 теперь могут приниматься VLAN 2 и наоборот, хотя по-прежнему не могут достичь адреса хоста 10.0.4.2 в VLAN 3.

Окончательная конфигурация

```
[R1]display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.0.4.1 255.255.255.0
#
return

[S3]display current-configuration
#
!Software Version V100R006C05
 sysname S3
#
interface Vlanif1
 ip address 10.0.4.2 255.255.255.0
#
interface Ethernet0/0/1
 shutdown
#
interface Ethernet0/0/7
 shutdown
#
return

[S1]display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S1
```

```
#
 vlan batch 2 to 4
#
 lacp priority 100
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 mode lacp
#
interface GigabitEthernet0/0/1
port link-type hybrid
 port hybrid pvid vlan 4
 port hybrid untagged vlan 2 4
#
interface GigabitEthernet0/0/9
undo negotiation auto
 speed 100
 eth-trunk 1
 lacp priority 100
#
interface GigabitEthernet0/0/10
undo negotiation auto
 speed 100
 eth-trunk 1
 lacp priority 100
#
interface GigabitEthernet0/0/13
 port link-type access
 port default vlan 3
#
return

[S2]display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S2
#
 vlan batch 2 to 4
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 mode lacp
#
interface GigabitEthernet0/0/3
port link-type hybrid
 port hybrid pvid vlan 4
 port hybrid untagged vlan 2 4
#
interface GigabitEthernet0/0/9
undo negotiation auto
 speed 100
 eth-trunk 1
#
```

```
interface GigabitEthernet0/0/10
undo negotiation auto
 speed 100
 eth-trunk 1
#
interface GigabitEthernet0/0/6
port link-type hybrid
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2 4
#
return

[R3]display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
interface GigabitEthernet0/0/2
 ip address 10.0.4.3 255.255.255.0
#
return

[S4]display current-configuration
#
!Software Version V100R006C05
 sysname S4
#
interface Vlanif1
 ip address 10.0.4.4 255.255.255.0
#
interface Ethernet0/0/1
 shutdown
#
interface Ethernet0/0/14
 shutdown
#
return
```

Лабораторная работа 1-3 Маршрутизация VLAN

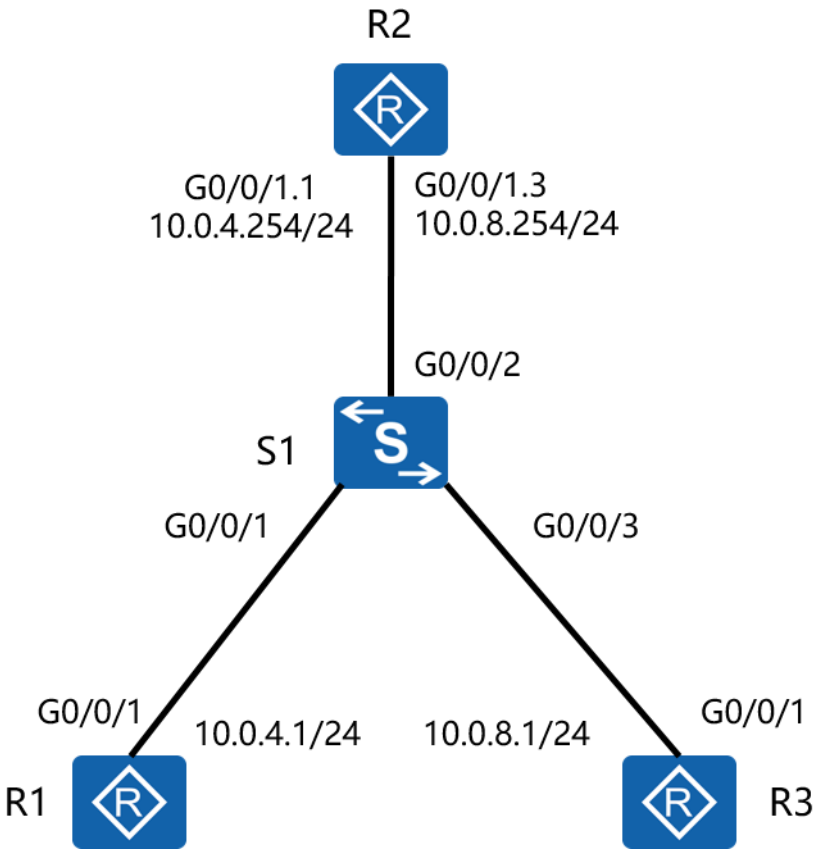
Цели обучения

В ходе данной лабораторной работы вам необходимо выполнить следующие задания:

- Создание магистрального интерфейса для маршрутизации VLAN.
- Конфигурирование субинтерфейсов на одном физическом интерфейсе.
- Включение сообщений ARP для трансляции между VLAN.

Топология

Рис. 1-3 Топология маршрутизации VLAN с помощью коммутатора уровня 2



Сценарий

Внедрение VLAN в корпоративной сети привело к изоляции групп пользователей от других пользователей, которые являются частью разных подсетей. Как администратору сети вам было поручено обеспечить поддержку широковещательных доменов, одновременно обеспечивая связь между разрозненными пользователями.

Задания

Шаг 1 Подготовка среды

Если вы еще не произвели настройку устройства, начните с шага 1, а затем перейдите к шагу 3. Для тех, кто продолжает предыдущие лабораторные работы, необходимо начать с шага 2.

Настройте имя системы для R1, R3 и S1. Настройте IP-адрес 10.0.4.1/24 на интерфейсе Gigabit Ethernet 0/0/1.

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.4.1 24
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
<Quidway>system-view
[Quidway]sysname S1
```

Шаг 2 Конфигурирование IP-адресов для R3

Настройте IP-адрес в диапазоне сети 10.0.8.0/24 на интерфейсе R1 Gigabit Ethernet 0/0/1.

```
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]ip address 10.0.8.1 24
```

Шаг 3 Установка двух VLAN

Создайте VLAN 4 и VLAN 8 на S1, настройте интерфейс Gigabit Ethernet 0/0/1 для подключения к VLAN 4, а интерфейс Gigabit Ethernet 0/0/3 для подключения к VLAN 8.

```
[S1]vlan batch 4 8
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]port link-type access
[S1-GigabitEthernet0/0/1]port default vlan 4
[S1-GigabitEthernet0/0/1]quit
[S1]interface GigabitEthernet0/0/3
[S1-GigabitEthernet0/0/3]port link-type access
[S1-GigabitEthernet0/0/3]port default vlan 8
[S1-GigabitEthernet0/0/3]quit
```

Настройте интерфейс Gigabit Ethernet 0/0/2 в качестве магистрального канала для VLAN 4 и VLAN 8.

```
[S1]interface GigabitEthernet0/0/2
[S1-GigabitEthernet0/0/2]port link-type trunk
[S1-GigabitEthernet0/0/2]port trunk allow-pass vlan 4 8
```

Шаг 4 Настройка маршрутизации VLAN через субинтерфейс R2

Сконфигурируйте субинтерфейсы GigabitEthernet0/0/1.1 и GigabitEthernet0/0/1.3 для работы в качестве шлюза VLAN 4, а также в качестве шлюза VLAN 8.

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet0/0/1.1
[R2-GigabitEthernet0/0/1.1]ip address 10.0.4.254 24
[R2-GigabitEthernet0/0/1.1]dot1q termination vid 4
[R2-GigabitEthernet0/0/1.1]arp broadcast enable
```

```
[R2-GigabitEthernet0/0/1.1]quit
[R2]interface GigabitEthernet0/0/1.3
[R2-GigabitEthernet0/0/1.3]ip address 10.0.8.254 24
[R2-GigabitEthernet0/0/1.3]dot1q termination vid 8
[R2-GigabitEthernet0/0/1.3]arp broadcast enable
```

Проверьте связь между R1 и R3.

```
<R1>ping 10.0.8.1
  PING 10.0.8.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
  --- 10.0.8.1 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

Настройте маршрут по умолчанию на R1 и R3.

```
[R1]ip route-static 0.0.0.0 0.0.0.0 10.0.4.254
[R3]ip route-static 0.0.0.0 0.0.0.0 10.0.8.254
```

Снова проверьте связь между R1 и R3.

```
<R1>ping 10.0.8.1
  PING 10.0.8.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.8.1: bytes=56 Sequence=1 ttl=254 time=10 ms
    Reply from 10.0.8.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 10.0.8.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 10.0.8.1: bytes=56 Sequence=4 ttl=254 time=10 ms
    Reply from 10.0.8.1: bytes=56 Sequence=5 ttl=254 time=1 ms
  --- 10.0.8.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/4/10 ms
[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

        10.0.4.0/24  Direct  0    0           D   10.0.4.254      GigabitEthernet0/0/1.1
      10.0.4.254/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1.1
      10.0.4.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1.1
        10.0.8.0/24  Direct  0    0           D   10.0.8.254      GigabitEthernet0/0/1.3
      10.0.8.254/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1.3
      10.0.8.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1.3
        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
```

Окончательная конфигурация

```
[R1]display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.0.4.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 10.0.4.254
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$dD#}P<HzJ;Xs%X>hOkm!,.+Iq61QK`K6tI}cc-;k_o`C.+L,%$%$
user-interface vty 0 4
#
return

[R2]display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/1.1
 dot1q termination vid 4
 ip address 10.0.4.254 255.255.255.0
 arp broadcast enable
#
interface GigabitEthernet0/0/1.3
 dot1q termination vid 8
 ip address 10.0.8.254 255.255.255.0
 arp broadcast enable
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$|nRPL^hr2IXi7LHDID!/,.*%.8%h;3:,hXO2dk#ikaWI.*(,%$%$
user-interface vty 0 4
#
return
[R3]dis current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
interface GigabitEthernet0/0/1
 ip address 10.0.8.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 10.0.8.254
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$W|$)M5D}v@bY^gK\;>QR,.*d;8Mp>|+EU,:~D~8b59~..*g,%$%$
```

```
user-interface vty 0 4
#
return
[S1]display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S1
#
 vlan batch 4 8
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 4
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 4 8
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 8
#
user-interface con 0
user-interface vty 0 4
#
return
```

Лабораторная работа 1-4 Конфигурирование коммутации уровня 3

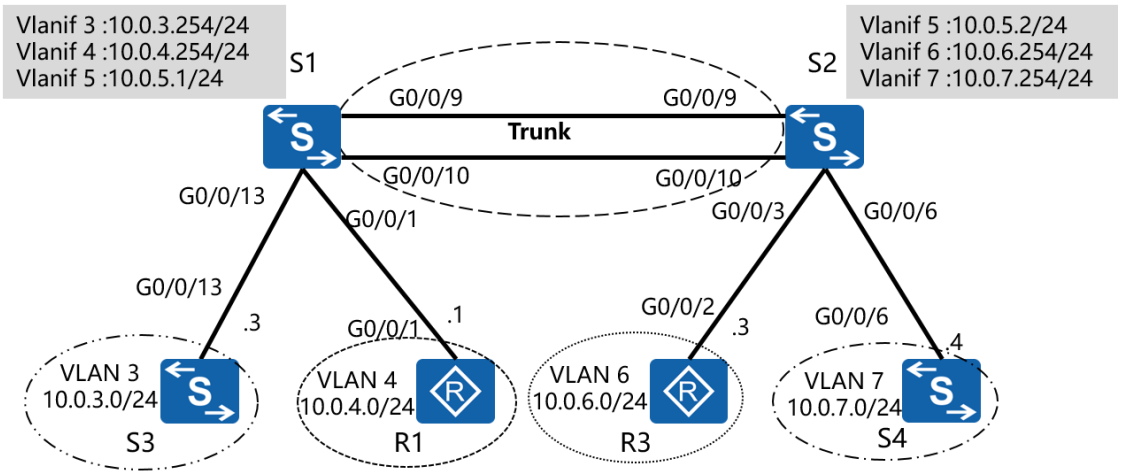
Цели обучения

В ходе данной лабораторной работы вам необходимо выполнить следующие задания:

- Конфигурация интерфейсов VLAN.
- Настройка маршрутизации VLAN на одном коммутаторе.
- Реализация маршрутизации VLAN по каналу Ethernet Trunk.
- Выполнение динамической маршрутизации между интерфейсами VLAN с помощью OSPF.

Топология

Рис. 1-4 Топология коммутации уровня 3



Сценарий

Введение коммутаторов уровня 3 в корпоративную сеть открыло возможности для оптимизации текущей конфигурации маршрутизации VLAN. Администратору сети было поручено реализовать маршрутизацию VLAN с использованием только коммутаторов уровня 3 для поддержки связи между VLAN в сети, как показано в топологии. VLAN должны поддерживать связь друг с другом. Кроме того, ожидается, что S1 и S2 будут обмениваться данными на уровне 3, для которого требуется поддержка протокола маршрутизации.

Задания

Шаг 1 Подготовка среды

Если вы еще не произвели настройку устройства, начните с шага 1, а затем перейдите к шагу 3. Для тех, кто продолжает предыдущие лабораторные работы, необходимо начать с шага 2.

Настройте IP-адрес 10.0.4.1/24 для R1 на интерфейсе Gigabit Ethernet 0/0/1. Установите соединение по каналу Eth-trunk между S1 и S2. Отключите все ненужные интерфейсы на S1 и S2 до S3 и S4.

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.4.1 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3

<Quidway>system-view
[Quidway]sysname S1
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]mode lacp
[S1-Eth-Trunk1]port link-type trunk
[S1-Eth-Trunk1]port trunk allow-pass vlan all
[S1-Eth-Trunk1]quit
[S1]interface GigabitEthernet 0/0/9
[S1-GigabitEthernet0/0/9]eth-trunk 1
[S1-GigabitEthernet0/0/9]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]eth-trunk 1

<Quidway>system-view
[Quidway]sysname S2
[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]mode lacp
[S2-Eth-Trunk1]port link-type trunk
[S2-Eth-Trunk1]port trunk allow-pass vlan all
[S2-Eth-Trunk1]quit
[S2]interface GigabitEthernet 0/0/9
[S2-GigabitEthernet0/0/9]eth-trunk 1
[S2-GigabitEthernet0/0/9]interface GigabitEthernet 0/0/10
[S2-GigabitEthernet0/0/10]eth-trunk 1

<Quidway>system-view
[Quidway]sysname S3
[S3]interface GigabitEthernet 0/0/7
[S3-GigabitEthernet0/0/7]shutdown

<Quidway>system-view
[Quidway]sysname S4
[S4]interface GigabitEthernet 0/0/14
[S4-GigabitEthernet0/0/14]shutdown
```

Шаг 2 Удаление предыдущих конфигураций

Удалите конфигурацию маршрутизации VLAN и субинтерфейсы на устройствах.

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

[R2]undo interface GigabitEthernet 0/0/1.1
[R2]undo interface GigabitEthernet 0/0/1.3
```

```
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]undo ip address
[R3-GigabitEthernet0/0/1]quit
[R3]undo ip route-static 0.0.0.0 0

[S1]undo vlan batch 4 8
Warning: The configurations of the VLAN will be deleted. Continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1]interface GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]undo port trunk allow-pass vlan 4 8
[S1-GigabitEthernet0/0/2]quit
[S1]interface GigabitEthernet 0/0/13
[S1-GigabitEthernet0/0/13]undo shutdown

[S2]interface GigabitEthernet0/0/6
[S2-GigabitEthernet0/0/6]undo shutdown
```

Re-enable the Eth-Trunk interface between S1 and S2

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]undo shutdown

[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]undo shutdown
```

Шаг 3 Конфигурирование VLAN 3 – VLAN 7 для S1 и S2

```
[S1]vlan batch 3 to 7
Info: This operation may take a few seconds. Please wait for a moment...done.

[S2]vlan batch 3 to 7
Info: This operation may take a few seconds. Please wait for a moment...done.
```

Убедитесь, что VLAN созданы.

```
[S1]display vlan
The total number of vlans is : 6
…output omitted…
VID  Type    Ports
--------------------------------------------------------------------------------
1    common  UT:GE0/0/1(U)     GE0/0/2(D)     GE0/0/3(U)     GE0/0/4(U)
                GE0/0/5(U)     GE0/0/6(D)     GE0/0/7(D)     GE0/0/8(D)
                GE0/0/11(D)    GE0/0/12(D)    GE0/0/13(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(U)    GE0/0/22(U)
                GE0/0/23(U)    GE0/0/24(D)    Eth-Trunk1(U)
3    common  TG:Eth-Trunk1(U)
4    common  TG:Eth-Trunk1(U)
5    common  TG:Eth-Trunk1(U)
6    common  TG:Eth-Trunk1(U)
7    common  TG:Eth-Trunk1(U)
…output omitted…

[S2]display vlan
The total number of vlans is : 6
```

```
…output omitted…
VID  Type      Ports
--------------------------------------------------------------------------------
1    common    UT:GE0/0/1(U)     GE0/0/2(D)     GE0/0/3(U)     GE0/0/4(U)
                GE0/0/5(U)     GE0/0/6(D)     GE0/0/7(D)     GE0/0/8(D)
                GE0/0/11(U)    GE0/0/12(U)    GE0/0/13(U)    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)    Eth-Trunk1(U)
3    common    TG:Eth-Trunk1(U)
4    common    TG:Eth-Trunk1(U)
5    common    TG:Eth-Trunk1(U)
6    common    TG:Eth-Trunk1(U)
7    common    TG:Eth-Trunk1(U)
…output omitted…
```

Шаг 4 Установка соединения Eth-Trunk между S1 и S2 с помощью PVID 5

Добавьте интерфейсы Gigabit Ethernet 0/0/1 и 0/0/13 S1 к VLAN 4 и VLAN 3 соответственно. Для S2 добавьте интерфейсы Gigabit Ethernet 0/0/3 и G0/0/6 к VLAN 6 и VLAN 7 соответственно.

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]port trunk pvid vlan 5
[S1-Eth-Trunk1]quit
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]port link-type access
[S1-GigabitEthernet0/0/1]port default vlan 4
[S1-GigabitEthernet0/0/1]quit
[S1]interface GigabitEthernet 0/0/13
[S1-GigabitEthernet0/0/13]port link-type access
[S1-GigabitEthernet0/0/13]port default vlan 3

[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]port trunk pvid vlan 5
[S2-Eth-Trunk1]quit
[S2]interface GigabitEthernet 0/0/3
[S2-GigabitEthernet0/0/3]port link-type access
[S2-GigabitEthernet0/0/3]port default vlan 6
[S2-GigabitEthernet0/0/3]quit
[S2]interface GigabitEthernet 0/0/6
[S2-GigabitEthernet0/0/6]port link-type access
[S2-GigabitEthernet0/0/6]port default vlan 7
```

Выполните команду **display vlan** для просмотра конфигурации.

```
<S1>display vlan
The total number of vlans is : 6
…output omit…
VID  Type      Ports
--------------------------------------------------------------------------------
1    common    UT:GE0/0/2(D)     GE0/0/3(U)     GE0/0/4(U)     GE0/0/5(U)
                GE0/0/6(D)     GE0/0/7(D)     GE0/0/8(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(U)    GE0/0/22(U)    GE0/0/23(U)    GE0/0/24(D)
TG:Eth-Trunk1(U)
```

```
3      common    UT:GE0/0/13(U)
TG:Eth-Trunk1(U)
4      common    UT:GE0/0/1(U)
TG:Eth-Trunk1(U)
5      common    UT:Eth-Trunk1(U)
6      common    TG:Eth-Trunk1(U)
7      common    TG:Eth-Trunk1(U)
…output omit…

<S2>display vlan
The total number of vlans is : 6
…output omit…
VID  Type      Ports
--------------------------------------------------------------------------------
1      common   UT:GE0/0/1(U)        GE0/0/2(D)        GE0/0/4(U)        GE0/0/5(U)
                  GE0/0/6(D)        GE0/0/7(D)        GE0/0/8(D)        GE0/0/11(U)
                  GE0/0/12(U)       GE0/0/13(U)       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)
               TG:Eth-Trunk1(U)
3      common    TG:Eth-Trunk1(U)
4      common    TG:Eth-Trunk1(U)
5      common    TG:Eth-Trunk1(U)
6      common    UT:GE0/0/3(U)
TG:Eth-Trunk1(U)
7      common    UT:GE0/0/6(U)
TG:Eth-Trunk1(U)
…output omit…
```

Шаг 5 Настройка адресов шлюза для VLAN на S1 и S2

Настройте IP-адреса для Vlanif3, Vlanif4 и Vlanif5 на S1, а также для Vlanif5, Vlanif6 и Vlanif7 на S2.

```
[S1]interface Vlanif 3
[S1-Vlanif3]ip address 10.0.3.254 24
[S1-Vlanif3]interface Vlanif 4
[S1-Vlanif4]ip address 10.0.4.254 24
[S1-Vlanif4]interface Vlanif 5
[S1-Vlanif5]ip address 10.0.5.1 24
[S2]interface Vlanif 5
[S2-Vlanif5]ip address 10.0.5.2 24
[S2-Vlanif5]interface Vlanif 6
[S2-Vlanif6]ip address 10.0.6.254 24
[S2-Vlanif6]interface Vlanif 7
[S2-Vlanif7]ip address 10.0.7.254 24
```

Шаг 6 IP-адресация и маршруты по умолчанию для R1, R3, S3 и S4

IP-адреса на коммутаторе должны быть назначены Vlanif, где Vlanif1 — это обычный Vlanif (без тегов). Интерфейсы Ethernet 0/0/13 S3 и Ethernet 0/0/6 S4 должны быть связаны с общей VLAN1. Для R1 должен быть предварительно настроен адрес 10.0.4.1/24.

```
[R1]ip route-static 0.0.0.0 0.0.0.0 10.0.4.254
```

```
[S3]interface Vlanif 1
[S3-Vlanif1]ip address 10.0.3.3 24
[S3-Vlanif1]quit
[S3]ip route-static 0.0.0.0 0.0.0.0 10.0.3.254

[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.0.6.3 24
[R3-GigabitEthernet0/0/2]quit
[R3]ip route-static 0.0.0.0 0.0.0.0 10.0.6.254

[S4]interface Vlanif 1
[S4-Vlanif1]ip address 10.0.7.4 24
[S4-Vlanif1]quit
[S4]ip route-static 0.0.0.0 0.0.0.0 10.0.7.254
```

Шаг 7 Проверка подключения между VLAN 3 и VLAN 4

Проверьте связь между S3 и R1.

```
<R1>ping 10.0.3.3
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.3.3: bytes=56 Sequence=1 ttl=254 time=37 ms
    Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=253 time=2 ms
    Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=253 time=10 ms
    Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=253 time=3 ms
    Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=253 time=2 ms

  --- 10.0.3.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/10/37 ms
```

Проверьте связь между R3 и R1.

```
<R1>ping 10.0.6.3
  PING 10.0.6.3: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
  --- 10.0.6.3 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

Сбой связи между R1 и R3. Для устранения сбоя используйте команду **tracert**:

```
[R1]tracert 10.0.6.3
traceroute to 10.0.6.3(10.0.6.3), max hops: 30 ,packet length: 40,press CTRL_C to break
 1 10.0.4.254 17 ms  4 ms  4 ms
 2  *  *  *
```

Согласно результату выполнения команды, R1 отправил пакеты данных по адресу назначения 10.0.6.3, но шлюз на 10.0.4.254 отвечает, что сеть недоступна.

Проверьте, доступна ли сеть на шлюзе (S1).

```
[S1]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

10.0.3.0/24         Direct0   0           D   10.0.3.254  Vlanif3
10.0.3.254/32       Direct0   0           D   127.0.0.1       InLoopBack0
10.0.4.0/24         Direct0   0           D   10.0.4.254  Vlanif4
10.0.4.254/32       Direct0   0           D   127.0.0.1       InLoopBack0
10.0.5.0/24         Direct0   0           D   10.0.5.1        Vlanif5
10.0.5.1/32         Direct0   0           D   127.0.0.1       InLoopBack0
127.0.0.0/8         Direct0   0           D   127.0.0.1       InLoopBack0
127.0.0.1/32        Direct0   0           D   127.0.0.1       InLoopBack0
```

Согласно результату выполнения команды, у S1 нет маршрута до сегмента сети 10.0.6.0, поскольку сегмент сети не связан напрямую с S1. Кроме того, для объявления маршрутов не были настроены статический маршрут или протокол динамической маршрутизации.

Шаг 8 Включение OSPF на S1 и S2

```
[S1]ospf
[S1-ospf-1]area 0
[S1-ospf-1-area-0.0.0.0]network 10.0.0.0 0.255.255.255

[S2]ospf
[S2-ospf-1]area 0
[S2-ospf-1-area-0.0.0.0]network 10.0.0.0 0.255.255.255
```

После настройки дождитесь, пока S1 и S2 обменяются маршрутами OSPF, и заполните базу данных состояний каналов, а затем просмотрите итоговую таблицу маршрутизации S1.

```
[S1]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
10.0.3.0/24         Direct 0    0           D   10.0.3.254      Vlanif3
10.0.3.254/32       Direct 0    0           D   127.0.0.1       InLoopBack0
10.0.4.0/24         Direct 0    0           D   10.0.4.254      Vlanif4
10.0.4.254/32       Direct 0    0           D   127.0.0.1       InLoopBack0
10.0.5.0/24         Direct 0    0           D   10.0.5.1        Vlanif5
10.0.5.1/32         Direct 0    0           D   127.0.0.1       InLoopBack0
10.0.6.0/24         OSPF 10   2           D   10.0.5.2        Vlanif5
10.0.7.0/24         OSPF 10   2           D   10.0.5.2        Vlanif5
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
```

S1 распознал два маршрута с помощью OSPF. Проверьте связь между R1 и R3.

```
[R1]ping 10.0.6.3
```

```
  PING 10.0.6.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.6.3: bytes=56 Sequence=1 ttl=253 time=11 ms
    Reply from 10.0.6.3: bytes=56 Sequence=2 ttl=253 time=1 ms
    Reply from 10.0.6.3: bytes=56 Sequence=3 ttl=253 time=10 ms
    Reply from 10.0.6.3: bytes=56 Sequence=4 ttl=253 time=1 ms
    Reply from 10.0.6.3: bytes=56 Sequence=5 ttl=253 time=1 ms
  --- 10.0.6.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/4/11 ms
[R1]ping 10.0.7.4
  PING 10.0.7.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.7.4: bytes=56 Sequence=1 ttl=253 time=30 ms
    Reply from 10.0.7.4: bytes=56 Sequence=2 ttl=252 time=2 ms
    Reply from 10.0.7.4: bytes=56 Sequence=3 ttl=252 time=3 ms
    Reply from 10.0.7.4: bytes=56 Sequence=4 ttl=252 time=2 ms
    Reply from 10.0.7.4: bytes=56 Sequence=5 ttl=252 time=2 ms
  --- 10.0.7.4 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/7/30 ms
```

Окончательная конфигурация

```
[R1]display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.0.4.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 10.0.4.254
#
return

[S1]display current-configuration
!Software Version V200R008C00SPC500
#
sysname S1
#
vlan batch 3 to 7
#
interface Vlanif3
 ip address 10.0.3.254 255.255.255.0
#
interface Vlanif4
 ip address 10.0.4.254 255.255.255.0
#
interface Vlanif5
 ip address 10.0.5.1 255.255.255.0
#
interface Eth-Trunk1
```

```
 port link-type trunk
port trunk pvid vlan 5
 port trunk allow-pass vlan 2 to 4094
 mode lacp
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 4
#
interface GigabitEthernet0/0/9
 eth-trunk 1
#
interface GigabitEthernet0/0/10
 eth-trunk 1
#
interface GigabitEthernet0/0/13
 port link-type access
 port default vlan 3
#
ospf 1
 area 0.0.0.0
  network 10.0.0.0 0.255.255.255
#
return

[S2]display current-configuration
!Software Version V200R008C00SPC500
#
sysname S2
#
vlan batch 3 to 7
#
interface Vlanif5
 ip address 10.0.5.2 255.255.255.0
#
interface Vlanif6
 ip address 10.0.6.254 255.255.255.0
#
interface Vlanif7
 ip address 10.0.7.254 255.255.255.0
#
interface Eth-Trunk1
 port link-type trunk
port trunk pvid vlan 5
 port trunk allow-pass vlan 2 to 4094
 mode lacp
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 6
#
interface GigabitEthernet0/0/6
 port link-type access
 port default vlan 7
#
```

```
interface GigabitEthernet0/0/9
 eth-trunk 1
#
interface GigabitEthernet0/0/10
 eth-trunk 1
#
ospf 1
 area 0.0.0.0
  network 10.0.0.0 0.255.255.255
#
return
```

```
[S3]display current-configuration
#
!Software Version V100R006C05
 sysname S3
#
interface Vlanif1
 ip address 10.0.3.3 255.255.255.0
#
interface GigabitEthernet0/0/7
 shutdown
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.3.254
#
return
```

```
[S4]display current-configuration
#
!Software Version V100R006C05
 sysname S4
#
interface Vlanif1
 ip address 10.0.7.4 255.255.255.0
#
interface GigabitEthernet0/0/14
 shutdown
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.7.254
#
return
```

Модуль 2 Конфигурирование корпоративной WAN

Лабораторная работа 2-1 Конфигурация HDLC и PPP

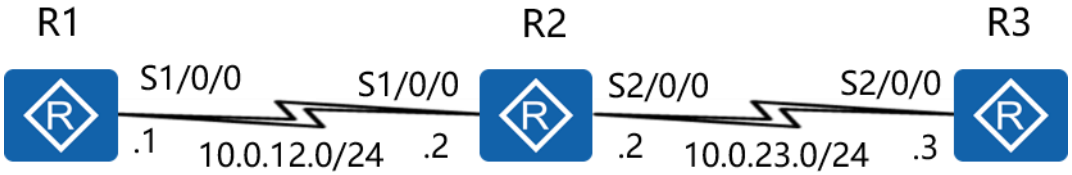
Цели обучения

В ходе данной лабораторной работы вам необходимо выполнить следующие задания:

- Настройка инкапсуляции HDLC в качестве протокола уровня последовательного канала.
- Изменение скорости передачи тактовой частоты DCE по последовательному каналу.
- Настройка инкапсуляции PPP в качестве протокола уровня последовательного канала.
- Реализация аутентификации PAP по каналу PPP.
- Реализация аутентификации CHAP по каналу PPP.

Топология

Рис. 2-1 Топология конфигурации HDLC и PPP



Сценарий

По мере расширения корпоративного бизнеса было создано несколько филиалов, которые должны стать частью административного домена компании. Требуются решения WAN. Вам, как сетевому администратору компании, было поручено установить решения HDLC и PPP на пограничном маршрутизаторе для передачи данных по сети некого поставщика услуг, возможно, MPLS, однако вам не раскрыли подробности, поскольку сеть поставщика услуг остается за рамками вашей задачи. R2 является пограничным маршрутизатором, расположенным в штаб-квартире, а R1 и R3 расположены в филиалах. Штаб-квартира и филиалы должны быть установлены в качестве единого административного домена. Используйте HDLC и PPP на каналах WAN и установите аутентификацию в качестве простой меры безопасности.

Задания

Шаг 1 Подготовка среды

Если вы еще не произвели настройку устройства, начните с шага 1, а затем перейдите к шагу 3. Для тех, кто продолжает предыдущие лабораторные работы, необходимо начать с шага 2.

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
```

```
[Huawei]sysname R1

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
```

Шаг 2 Удаление предыдущих конфигураций

Удалите статические маршруты к R2 и отключите интерфейсы Ethernet, чтобы избежать создания альтернативных маршрутов. Удалите все ненужные конфигурации VLAN.

```
[R1]undo ip route-static 0.0.0.0 0
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]shutdown

[R3]undo ip route-static 0.0.0.0 0
[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]shutdown

[S1]undo interface Vlanif 3
[S1]undo interface Vlanif 5
[S1]undo vlan batch 3 5 to 7
Warning: The configurations of the VLAN will be deleted. Continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]undo port default vlan
[S1-GigabitEthernet0/0/1]quit
[S1]undo ospf 1
Warning: The OSPF process will be deleted. Continue? [Y/N]:y

[S2]undo interface Vlanif 5
[S2]undo interface Vlanif 7
[S2]undo vlan batch 3 to 5 7
Warning: The configurations of the VLAN will be deleted. Continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment...done.
[S2]interface GigabitEthernet 0/0/3
[S2-GigabitEthernet0/0/3]undo port default vlan
[S2-GigabitEthernet0/0/3]quit
[S2]undo ospf 1
Warning: The OSPF process will be deleted. Continue? [Y/N]:y

[S3]undo interface Vlanif 1

[S4]undo interface Vlanif 1
```

Шаг 3 Настройка IP-адресации последовательного интерфейса для R1, R2 и R3

```
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ip address 10.0.12.1 24

[R2]interface Serial 1/0/0
[R2-Serial1/0/0]ip address 10.0.12.2 24
[R2-Serial1/0/0]quit
```

```
[R2]interface Serial 2/0/0
[R2-Serial2/0/0]ip address 10.0.23.2 24

[R3]interface Serial 2/0/0
[R3-Serial2/0/0]ip address 10.0.23.3 24
```

Шаг 4 Включение протокола HDLC на последовательных интерфейсах

```
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]link-protocol hdlc
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]link-protocol hdlc
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y
[R2-Serial1/0/0]quit
[R2]interface Serial 2/0/0
[R2-Serial2/0/0]link-protocol hdlc
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y
[R3]interface Serial 2/0/0
[R3-Serial2/0/0]link-protocol hdlc
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y
```

После включения HDLC на последовательных интерфейсах просмотрите статус последовательного интерфейса. В качестве примера используется отображаемая информация для R1.

```
[R1]display interface Serial1/0/0
Serial1/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2016-3-10 11:25:08
Description:HUAWEI, AR Series, Serial1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 10.0.12.1/24
Link layer protocol is nonstandard HDLC
Last physical up time     : 2016-3-10 11:23:55
Last physical down time : 2016-3-10 11:23:55
Current system time: 2016-3-10 11:25:46
Physical layer is synchronous, Baudrate is 64000 bps
Interface is DCE, Cable type is V24, Clock mode is DCECLK
Last 300 seconds input rate 3 bytes/sec 24 bits/sec 0 packets/sec
Last 300 seconds output rate 3 bytes/sec 24 bits/sec 0 packets/sec

Input: 100418 packets, 1606804 bytes
  Broadcast:                0,  Multicast:                0
  Errors:                   0,  Runts:                    0
  Giants:                   0,  CRC:                      0

  Alignments:               0,  Overruns:                 0
  Dribbles:                 0,  Aborts:                   0
  No Buffers:               0,  Frame Error:              0

Output: 100418 packets, 1606830 bytes
  Total Error:              0,  Overruns:                 0
  Collisions:               0,  Deferred:                 0
  No Buffers:               0
DCD=UP DTR=UP DSR=UP RTS=UP CTS=UP
    Input bandwidth utilization   : 0.06%
```

```
Output bandwidth utilization : 0.06%
```

Убедившись, что физическое состояние и состояние протокола интерфейса установлено в значении Up, проверьте связь подключенного напрямую канала.

```
 <R2>ping 10.0.12.1
   PING 10.0.12.1: 56  data bytes, press CTRL_C to break
     Reply from 10.0.12.1: bytes=56 Sequence=1 ttl=255 time=44 ms
     Reply from 10.0.12.1: bytes=56 Sequence=2 ttl=255 time=39 ms
     Reply from 10.0.12.1: bytes=56 Sequence=3 ttl=255 time=39 ms
     Reply from 10.0.12.1: bytes=56 Sequence=4 ttl=255 time=40 ms
     Reply from 10.0.12.1: bytes=56 Sequence=5 ttl=255 time=39 ms
   --- 10.0.12.1 ping statistics ---
     5 packet(s) transmitted
     5 packet(s) received
     0.00% packet loss
round-trip min/avg/max = 39/40/44 ms

[R2]ping 10.0.23.3
   PING 10.0.23.3: 56  data bytes, press CTRL_C to break
     Reply from 10.0.23.3: bytes=56 Sequence=1 ttl=255 time=44 ms
     Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=255 time=39 ms
     Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=255 time=39 ms
     Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=255 time=40 ms
     Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=255 time=39 ms

   --- 10.0.23.3 ping statistics ---
     5 packet(s) transmitted
     5 packet(s) received
     0.00% packet loss
     round-trip min/avg/max = 39/40/44 ms
```

Шаг 5 Настройка OSPF

Включите протокол маршрутизации OSPF для объявления удаленных сетей R1 и R3.

```
[R1]ospf 1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network  10.0.12.0 0.0.0.255

[R2]ospf 1
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network  10.0.12.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network  10.0.23.0 0.0.0.255

[R3]ospf 1
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network  10.0.23.0 0.0.0.255
```

После завершения настройки убедитесь, что все маршруты были распознаны. Убедитесь, что соответствующие маршруты были распознаны RIP.

```
<R1>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

10.0.12.0/24        Direct  0    0           D   10.0.12.1       Serial1/0/0
10.0.12.1/32        Direct  0    0           D   127.0.0.1       Serial1/0/0
10.0.12.255/32      Direct  0    0           D   127.0.0.1       Serial1/0/0
10.0.23.0/24        OSPF    10   3124        D   10.0.12.2       Serial1/0/0
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 R1 выполните команду **ping** для проверки подключения между R1 и R3.

```
<R1>ping 10.0.23.3
  PING 10.0.23.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.23.3: bytes=56 Sequence=1 ttl=254 time=44 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=254 time=39 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=254 time=39 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=254 time=40 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=254 time=39 ms

  --- 10.0.23.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 39/40/44 ms
```

Шаг 6 Управление последовательным соединением

Проверьте тип кабеля, подключенного к последовательному интерфейсу, состояние интерфейса и тактовую частоту, затем измените тактовую частоту.

```
<R1>display interface Serial1/0/0
Serial1/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2016-03-10 11:25:08
Description:HUAWEI, AR Series, Serial1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 10.0.12.1/24
Link layer protocol is nonstandard HDLC
Last physical up time     : 2016-03-10 11:23:55
Last physical down time : 2016-03-10 11:23:55
Current system time: 2016-03-10 11:51:12
Physical layer is synchronous, Baudrate is 64000 bps
Interface is DCE, Cable type is V35, Clock mode is DCECLK1
Last 300 seconds input rate 5 bytes/sec 40 bits/sec 0 packets/sec
Last 300 seconds output rate 2 bytes/sec 16 bits/sec 0 packets/sec
…output omit…
```

В приведенной выше информации показано, что S1/0/0 на R1 подключается к кабелю DCE, а тактовая частота составляет 64000 бит/с. DCE управляет тактовой частотой и полосой пропускания.

Измените тактовую частоту на канале между R1 и R2 на 128000 бит/с. Данная операция должна быть выполнена на DCE, R1.

```
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]baudrate 128000
```

После завершения настройки проверьте состояние последовательного интерфейса.

```
<R1>display interface Serial1/0/0
Serial1/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2016-03-10 11:25:08
Description:HUAWEI, AR Series, Serial1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 10.0.12.1/24
Link layer protocol is nonstandard HDLC
Last physical up time     : 2016-03-10 11:23:55
Last physical down time : 2016-03-10 11:23:55
Current system time: 2016-03-10 11:54:19
Physical layer is synchronous, Baudrate is 128000 bps
Interface is DCE, Cable type is V35, Clock mode is DCECLK1
Last 300 seconds input rate 6 bytes/sec 48 bits/sec 0 packets/sec
Last 300 seconds output rate 4 bytes/sec 32 bits/sec 0 packets/sec
…output omit…
```

Шаг 7 Конфигурирование PPP на последовательных интерфейсах

Настройте PPP между R1 и R2, а также R2 и R3. На обоих концах канала должен использоваться один и тот же режим инкапсуляции. При использовании различных режимов инкапсуляции на интерфейсах может отобразиться состояние «Down».

```
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]link-protocol ppp
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]link-protocol ppp
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y
[R2-Serial1/0/0]quit
[R2]interface Serial 2/0/0
[R2-Serial2/0/0]link-protocol ppp
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y
[R3]interface Serial 2/0/0
[R3-Serial2/0/0]link-protocol ppp
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y
```

После завершения настройки проверьте подключение канала.

```
<R2>ping 10.0.12.1
  PING 10.0.12.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.12.1: bytes=56 Sequence=1 ttl=255 time=22 ms
    Reply from 10.0.12.1: bytes=56 Sequence=2 ttl=255 time=27 ms
    Reply from 10.0.12.1: bytes=56 Sequence=3 ttl=255 time=27 ms
    Reply from 10.0.12.1: bytes=56 Sequence=4 ttl=255 time=27 ms
    Reply from 10.0.12.1: bytes=56 Sequence=5 ttl=255 time=27 ms

  --- 10.0.12.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 22/26/27 ms
<R2>ping 10.0.23.3
  PING 10.0.23.3: 56  data bytes, press CTRL_C to break
```

```
    Reply from 10.0.23.3: bytes=56 Sequence=1 ttl=255 time=35 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=255 time=40 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=255 time=40 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=255 time=40 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=255 time=40 ms

  --- 10.0.23.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 35/39/40 ms
```

При сбое операции **ping** проверьте статус интерфейса и правильность типа протокола уровня канала.

```
<R1>display interface Serial1/0/0
Serial1/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2016-03-10 12:35:41
Description:HUAWEI, AR Series, Serial1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 10.0.12.1/24
Link layer protocol is PPP
LCP opened, IPCP opened
Last physical up time     : 2016-03-10 11:57:20
Last physical down time : 2016-03-10 11:57:19
Current system time: 2016-03-10 13:38:03
Physical layer is synchronous, Baudrate is 128000 bps
Interface is DCE, Cable type is V35, Clock mode is DCECLK1
Last 300 seconds input rate 7 bytes/sec 56 bits/sec 0 packets/sec
Last 300 seconds output rate 4 bytes/sec 32 bits/sec 0 packets/sec
…output omit…
```

Шаг 8 Проверка изменений записей маршрутизации

После завершения настройки PPP маршрутизаторы устанавливают соединения на уровне канала. Локальное устройство отправляет маршрут на одноранговое устройство. Маршрут содержит IP-адрес интерфейса и 32-битную маску.

Ниже в качестве примера приводится R2, для которого можно увидеть маршруты к R1 и R3.

```
[R2]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

10.0.12.0/24        Direct  0    0           D   10.0.12.2       Serial1/0/0
10.0.12.1/32        Direct  0    0           D   10.0.12.1       Serial1/0/0
10.0.12.2/32        Direct  0    0           D   127.0.0.1       Serial1/0/0
10.0.12.255/32      Direct  0    0           D   127.0.0.1       Serial1/0/0
10.0.23.0/24        Direct  0    0           D   10.0.23.2       Serial2/0/0
10.0.23.2/32        Direct  0    0           D   127.0.0.1       Serial2/0/0
10.0.23.3/32        Direct  0    0           D   10.0.23.3       Serial2/0/0
```

```
10.0.23.255/32  Direct  0  0        D      127.0.0.1       Serial2/0/0
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
```

Подумайте о происхождении и функциях этих двух маршрутов. Проверьте следующее:

Существуют ли эти два маршрута при инкапсуляции HDLC?

Могут ли R1 и R2 обмениваться данными с использованием HDLC или PPP, когда IP-адреса интерфейсов S1/0/0 на R1 и R2 расположены в разных сегментах сети?

Шаг 9 Включение аутентификации PAP между R1 и R2

Настройте аутентификацию PAP с R1 в качестве аутентификатора PAP PPP.

```
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ppp authentication-mode pap
[R1-Serial1/0/0]quit
[R1]aaa
[R1-aaa]local-user huawei password cipher huawei123
 info: A new user added
[R1-aaa]local-user huawei service-type ppp
```

Настройте аутентификацию PAP с помощью R2 в качестве аутентифицированного устройства PAP.

```
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]ppp pap local-user huawei password cipher huawei123
```

После того, как R2 отправляет запрос аутентификации на R1, R1 отправляет ответное сообщение на R2, совершая запрос R2 на использование аутентификации PAP, после чего R2 отправляет свой пароль на R1.

После завершения настройки проверьте связь между R1 и R2.

```
<R1>debugging ppp pap packet
<R1>terminal debugging
<R1>display debugging
PPP PAP packets debugging switch is on
<R1>system-view
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]shutdown
[R1-Serial1/0/0]undo shutdown

Mar 10 2016 14:44:22.440.1+00:00 R1 PPP/7/debug2:
  PPP Packet:
      Serial1/0/0 Input   PAP(c023) Pkt, Len 22
      State ServerListen, code Request(01), id 1, len 18
      Host Len:   6   Name:huawei
[R1-Serial1/0/0]
Mar 10 2016 14:44:22.440.2+00:00 R1 PPP/7/debug2:
  PPP Packet:
      Serial1/0/0 Output PAP(c023) Pkt, Len 52
      State WaitAAA, code Ack(02), id 1, len 48
      Msg Len: 43   Msg:Welcome to use Access ROUTER, Huawei Tech.
[R1-Serial1/0/0]return
```

```
<R1>undo debugging all
Info: All possible debugging has been turned off
```

Шаг 10 Включение аутентификации CHAP между R2 и R3

Настройте R3 в качестве аутентификатора. После того, как R2 отправляет запрос аутентификации на R3, R3 отправляет ответное сообщение на R2, совершая запрос R2 на использование аутентификации CHAP, после чего вызов отправляется на R3.

```
[R3]interface Serial 2/0/0
[R3-Serial2/0/0]ppp authentication-mode chap
[R3-Serial2/0/0]quit
[R3]aaa
[R3-aaa]local-user huawei password cipher huawei123
 info: A new user added
[R3-aaa]local-user huawei service-type ppp
[R3-aaa]quit
[R3]interface Serial 2/0/0
[R3-Serial2/0/0]shutdown
[R3-Serial2/0/0]undo shutdown
```

На R3 появится следующая информация:

```
Dec 10 2013 15:06:00+00:00 R3 %%01PPP/4/PEERNOCHAP(l)[5]:On the interface Serial2/0/0, authentication failed and
PPP link was closed because CHAP was disabled on the peer.
[R3-Serial2/0/0]
Dec 10 2013 15:06:00+00:00 R3 %%01PPP/4/RESULTERR(l)[6]:On the interface Serial2/0/0, LCP negotiation failed
because the result cannot be accepted.
```

Выделенные цветом выходные данные указывают на то, что аутентификация не может быть инициализирована.

Сконфигурируйте R2 в качестве клиента CHAP.

```
[R2]interface Serial 2/0/0
[R2-Serial2/0/0]ppp chap user huawei
[R2-Serial2/0/0]ppp chap password cipher huawei123
```

После завершения настройки интерфейс переходит в состояние Up. Результат выполнения команды ping:

```
<R2>ping 10.0.23.3
  PING 10.0.23.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.23.3: bytes=56 Sequence=1 ttl=255 time=35 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=255 time=41 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=255 time=41 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=255 time=41 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=255 time=41 ms
  --- 10.0.23.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 35/39/41 ms
```

Шаг 11 Отладка PPP CHAP

Выполните команду отладки, чтобы просмотреть согласование соединения PPP между R2 и R3. Соединение PPP устанавливается с использованием CHAP. Отключите интерфейс Serial 2/0/0 на R2, выполните команду отладки и включите Serial 2/0/0 на R2.

```
[R2]interface Serial 2/0/0
[R2-Serial2/0/0]shutdown
```

Выполните команды **debugging ppp chap all** и **terminal debugging** для отображения информации по отладке.

```
[R2-Serial2/0/0]return
<R2>debugging ppp chap all
<R2>terminal debugging
Info: Current terminal debugging is on.
<R2>display debugging
PPP CHAP packets debugging switch is on
PPP CHAP events debugging switch is on
PPP CHAP errors debugging switch is on
PPP CHAP state change debugging switch is on
```

Выполните принудительную аутентификацию CHAP для инициализации на S2/0/0 R2.

```
<R2>system-view
Enter system view, return user view with Ctrl+Z.
[R2]interface Serial 2/0/0
[R2-Serial2/0/0]undo shutdown
```

На экране появится следующая информация об отладке:

```
Mar 10 2016 09:10:38.700.1+00:00 R2 PPP/7/debug2:
  PPP State Change:
      Serial2/0/0 CHAP : Initial --> ListenChallenge
[R2-Serial2/0/0]
Mar 10 2016 09:10:38.710.1+00:00 R2 PPP/7/debug2:
  PPP Packet:
      Serial2/0/0 Input    CHAP(c223) Pkt, Len 25
      State ListenChallenge, code Challenge(01), id 1, len 21
      Value_Size:    16    Value: fc 9b 56 e1 53 e3 a6 26 1b 54 e5 e2 a1 ed 90 87
      Name:
[R2-Serial2/0/0]
Mar 10 2016 09:10:38.710.2+00:00 R2 PPP/7/debug2:
  PPP Event:
      Serial2/0/0 CHAP Receive Challenge Event
      state ListenChallenge
[R2-Serial2/0/0]
Mar 10 2016 09:10:38.710.3+00:00 R2 PPP/7/debug2:
  PPP Packet:
      Serial2/0/0 Output CHAP(c223) Pkt, Len 31
      State ListenChallenge, code Response(02), id 1, len 27
      Value_Size:    16    Value: f9 54    1 69 30 59 a0 af 52 a1 1d de 85 77 27 6b
      Name: huawei
[R2-Serial2/0/0]
Mar 10 2016 09:10:38.710.4+00:00 R2 PPP/7/debug2:
  PPP State Change:
      Serial2/0/0 CHAP : ListenChallenge --> SendResponse
[R2-Serial2/0/0]
Mar 10 2016 09:10:38.720.1+00:00 R2 PPP/7/debug2:
  PPP Packet:
      Serial2/0/0 Input    CHAP(c223) Pkt, Len 20
      State SendResponse, code SUCCESS(03), id 1, len 16
      Message: Welcome to .
```

```
[R2-Serial2/0/0]
Mar 10 2016 09:10:38.720.2+00:00 R2 PPP/7/debug2:
  PPP Event:
      Serial2/0/0 CHAP Receive Success Event
      state SendResponse
[R2-Serial2/0/0]
Mar 10 2016 09:10:38.720.3+00:00 R2 PPP/7/debug2:
  PPP State Change:
      Serial2/0/0 CHAP : SendResponse --> ClientSuccess
```

Выделенная информация об отладке описывает ключевое поведение CHAP. Отключите процесс отладки.

```
[R2-Serial2/0/0]return
<R2>undo debugging all
Info: All possible debugging has been turned off
```

Дополнительные упражнения: анализ и проверка

Почему уровень безопасности протокола аутентификации с косвенным согласованием PPP (CHAP) выше, чем у протокола простой проверки подлинности PPP (PAP)?

Окончательная конфигурация

```
[R1]display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei password cipher %$%$B:%I)Io0H8)[%SB[idM3C/!#%$%$
 local-user huawei service-type ppp
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode pap
 ip address 10.0.12.1 255.255.255.0
 baudrate 128000
#
ospf 1
 area 0.0.0.0
  network 10.0.12.0 0.0.0.255
#
return

[R2]display current-configuration
[V200R007C00SPC600]
#
 sysname R2
```

```
#
interface Serial1/0/0
 link-protocol ppp
 ppp pap local-user huawei password cipher %$%$u[hr6d<JVHR@->T7xr1<$.iv%$%$
 ip address 10.0.12.2 255.255.255.0
#
interface Serial2/0/0
 link-protocol ppp
 ppp chap user huawei
 ppp chap password cipher %$%$e{5h)gh"/Uz0mUC%vEx3$4<m%$%$
 ip address 10.0.23.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.0.12.0 0.0.0.255
  network 10.0.23.0 0.0.0.255
#
return

[R3]display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei password cipher %$%$fZsyUk1=O=>:L4'ytgR~D*Im%$%$
 local-user huawei service-type ppp
#
interface Serial2/0/0
 link-protocol ppp
 ppp authentication-mode chap
 ip address 10.0.23.3 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.0.23.0 0.0.0.255
#
return
```

Лабораторная работа 2-2 Настройка сеанса клиента PPPoE

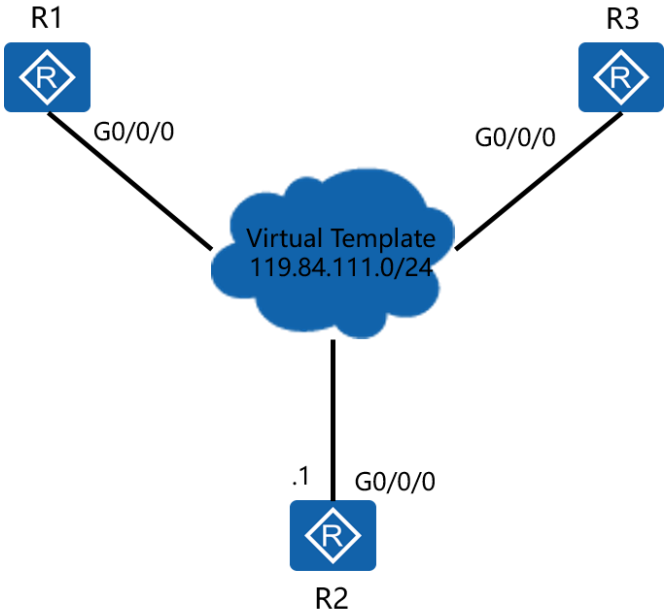
Цели обучения

В ходе данной лабораторной работы вам необходимо выполнить следующие задания:

- Настройка интерфейса номеронабирателя для PPPoE.
- Аутентификация клиента по PPPoE.

Топология

Рис. 2-2 Топология клиента и сервера PPPoE



Сценарий

Предприятие подписывается на (обычно высокоскоростную) услугу DSL от поставщика услуг, посредством которой поддерживаются услуги WAN. R1 и R3 являются корпоративными пограничными маршрутизаторами различных офисов, которые устанавливают соединение с поставщиком услуг через сервер PPPoE (R2). Предприятию необходимо установить номеронабиратель PPPoE на пограничных маршрутизаторах, чтобы хосты в локальной сети могли прозрачно получать доступ к внешним ресурсам через сеть поставщика услуг посредством PPPoE.

Задания

Шаг 1 Подготовка среды

Если вы еще не произвели настройку устройства, начните с шага 1, а затем перейдите к шагу 3. Для тех, кто продолжает предыдущие лабораторные работы, необходимо начать с шага 2.

```
<Huawei>system-view
```

```
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
```

Шаг 2 Удаление предыдущих конфигураций

Отключите последовательные интерфейсы, чтобы избежать маршрутизации по сети Frame Relay.

```
[R1]interface Serial 2/0/0
[R1-Serial2/0/0]shutdown
[R3]interface Serial 1/0/0
[R3-Serial1/0/0]shutdown
```

Шаг 3 Конфигурирование сервера PPPoE

Сервер PPPoE не является частью корпоративной сети, однако он необходим для аутентификации пограничных маршрутизаторов R1 и R3 предприятия.

```
[R2]ip pool pool1
Info: It's successful to create an IP address pool.
[R2-ip-pool-pool1]network 119.84.111.0 mask 255.255.255.0
[R2-ip-pool-pool1]gateway-list 119.84.111.254
[R2-ip-pool-pool1]quit
[R2]interface Virtual-Template 1
[R2-Virtual-Template1]ppp authentication-mode chap
[R2-Virtual-Template1]ip address 119.84.111.254 255.255.255.0
[R2-Virtual-Template1]remote address pool pool1
[R2-Virtual-Template1]quit
```

Привяжите виртуальный шаблон к интерфейсу Gigabit Ethernet 0/0/0.

```
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]pppoe-server bind virtual-template 1
[R2-GigabitEthernet0/0/0]quit
```

Настройте аутентифицированного пользователя PPPoE.

```
[R2]aaa
[R2-aaa]local-user huawei1 password cipher huawei123
Info: Add a new user.
[R2-aaa]local-user huawei1 service-type ppp
[R2-aaa]local-user huawei2 password cipher huawei123
Info: Add a new user.
[R2-aaa]local-user huawei2 service-type ppp
[R2-aaa]quit
```

Шаг 4 Конфигурирование клиента PPPoE

Сконфигурируйте R1 в качестве клиента PPPoE, для которого необходимо создать интерфейс номеронабирателя, и включите аутентификацию PPP. Имя пользователя и пароль PPP должны совпадать с настроенными на сервере PPPoE.

```
[R1]dialer-rule
[R1-dialer-rule]dialer-rule 1 ip permit
[R1-dialer-rule]quit
[R1]interface Dialer 1
[R1-Dialer1]dialer user user1
[R1-Dialer1]dialer-group 1
[R1-Dialer1]dialer bundle 1
[R1-Dialer1]ppp chap user huawei1
[R1-Dialer1]ppp chap password cipher huawei123
[R1-Dialer1]dialer timer idle 300
[R1-Dialer1]dialer queue-length 8
[R1-Dialer1]ip address ppp-negotiate
[R1-Dialer1]quit
```

Привяжите номеронабиратель PPPoE к исходящему интерфейсу.

```
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]pppoe-client dial-bundle-number 1
[R1-GigabitEthernet0/0/0]quit
```

Настройте статический маршрут по умолчанию к серверу PPPoE.

```
[R1]ip route-static 0.0.0.0 0.0.0.0 Dialer 1
```

Сконфигурируйте R3 в качестве клиента PPPoE, для которого необходимо создать интерфейс номеронабирателя, и включите аутентификацию PPP. Имя пользователя и пароль PPP должны совпадать с настроенными на сервере PPPoE.

```
[R3]dialer-rule
[R3-dialer-rule]dialer-rule 1 ip permit
[R3-dialer-rule]quit
[R3]interface Dialer 1
[R3-Dialer1]dialer user user2
[R3-Dialer1]dialer-group 1
[R3-Dialer1]dialer bundle 1
[R3-Dialer1]ppp chap user huawei2
[R3-Dialer1]ppp chap password cipher huawei123
[R3-Dialer1]dialer timer idle 300
[R3-Dialer1]dialer queue-length 8
[R3-Dialer1]ip address ppp-negotiate
[R3-Dialer1]quit
```

Привяжите номеронабиратель PPPoE к исходящему интерфейсу.

```
[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]pppoe-client dial-bundle-number 1
[R3-GigabitEthernet0/0/0]quit
```

Настройте статический маршрут по умолчанию к серверу PPPoE.

```
[R3]ip route-static 0.0.0.0 0.0.0.0 Dialer 1
```

Шаг 5 Проверка результатов конфигурации

Выполните команду **display pppoe-server session all** для просмотра статуса и информации о конфигурации.

```
<R2>display pppoe-server session all
SID Intf                      State OIntf       RemMAC          LocMAC
1   Virtual-Template1:0       UP    GE0/0/0     00e0.fc03.d0ae  00e0.fc03.7516
```

```
2    Virtual-Template1:1          UP          GE0/0/0          00e0.fc03.aedd    00e0.fc03.7516
```

Согласно отображаемой информации, состояние сеанса нормальное.

Проверьте интерфейс номеронабирателя R1 и R3 и убедитесь, что они оба могут получить IP-адрес от сервера PPPoE.

```
<R1>display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
The number of interface that is UP in Physical is 7
The number of interface that is DOWN in Physical is 4
The number of interface that is UP in Protocol is 5
The number of interface that is DOWN in Protocol is 6

Interface                   IP Address/Mask      Physical   Protocol
Cellular0/0/0               unassigned           down       down
Cellular0/0/1               unassigned           down       down
Dialer1                     119.84.111.253/32    up         up(s)
GigabitEthernet0/0/0        unassigned           up         down
…output omitted…
<R3>display ip interface brief
…output omitted…
Interface                   IP Address/Mask      Physical   Protocol
Cellular0/0/0               unassigned           down       down
Cellular0/0/1               unassigned           down       down
Dialer1                     119.84.111.252/32    up         up(s)
GigabitEthernet0/0/0        unassigned           up         down
…output omitted…
```

Окончательная конфигурация

```
[R1]display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei password cipher %$%$B:%l)Io0H8)[%SB[idM3C/!#%$%$
 local-user huawei service-type ppp
#
interface Dialer1
 link-protocol ppp
 ppp chap user huawei1
 ppp chap password cipher %$%$A8E~UjX}@;bhCL*C4w#<%"Ba%$%$
 ip address ppp-negotiate
 dialer user user1
```

```
 dialer bundle 1
 dialer queue-length 8
 dialer timer idle 300
 dialer-group 1
#
interface GigabitEthernet0/0/0
 pppoe-client dial-bundle-number 1
#
dialer-rule
 dialer-rule 1 ip permit
#
ip route-static 0.0.0.0 0.0.0.0 Dialer1
#
return
```

```
[R2]dis current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
ip pool pool1
 gateway-list 119.84.111.254
 network 119.84.111.0 mask 255.255.255.0
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei1 password cipher %$%$MjCY6,a82N4W`]F]3LMAKG9+%$%$
 local-user huawei1 service-type ppp
 local-user huawei2 password cipher %$%$Ctq55RX:]R,8Jc13{|,)KH!m%$%$
 local-user huawei2 service-type ppp
#
interface Virtual-Template1
 ppp authentication-mode chap
 remote address pool pool1
 ip address 119.84.111.254 255.255.255.0
#
interface GigabitEthernet0/0/0
 pppoe-server bind Virtual-Template 1
#
return
```

```
[R3]display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
aaa
```

```
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei password cipher %$%$fZsyUk1=O=>:L4'ytgR~D*Im%$%$
 local-user huawei service-type ppp
#
interface Dialer1
 link-protocol ppp
 ppp chap user huawei2
 ppp chap password cipher %$%$0f8(;^]1NS:q;SPo8TyP%.Ei%$%$
 ip address ppp-negotiate
 dialer user user2
 dialer bundle 1
 dialer queue-length 8
 dialer timer idle 300
 dialer-group 1
#
interface GigabitEthernet0/0/0
 pppoe-client dial-bundle-number 1
#
dialer-rule
 dialer-rule 1 ip permit
#
ip route-static 0.0.0.0 0.0.0.0 Dialer1
#
return
```

Модуль 3 Реализация IP-безопасности

Лабораторная работа 3-1 Фильтрация корпоративных данных с помощью списков управления доступом

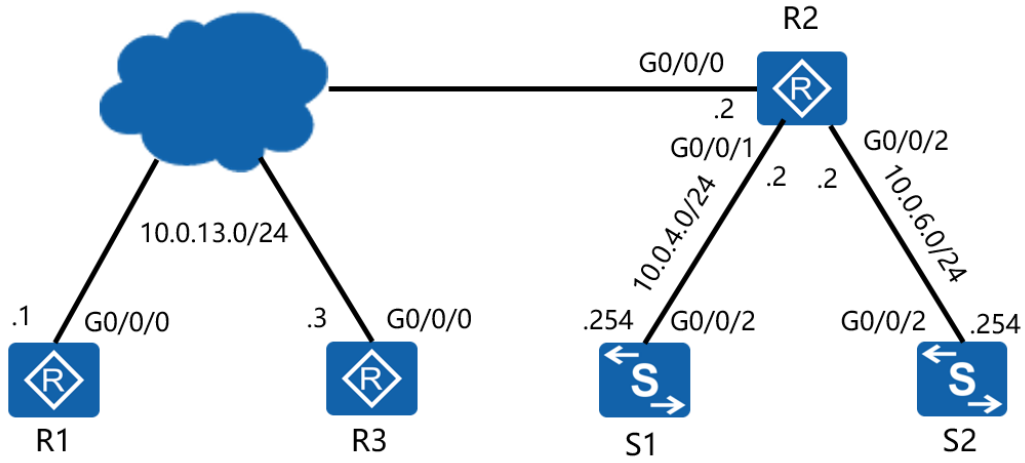
Цели обучения

В ходе данной лабораторной работы вам необходимо выполнить следующие задания:

- Создание стандартного ACL для реализации исходной фильтрации.
- Создание расширенного ACL для реализации расширенной фильтрации.

Топология

Рис. 3-1 Фильтрация данных корпоративной сети с помощью списков управления доступом



Сценарий

Предположим, что вы являетесь сетевым администратором компании, имеющей три сети, принадлежащие трем объектам. R2 развернут на границе сети для основного объекта, а R1 и R3 развернуты на границе остальных объектов. Маршрутизаторы взаимодействуют посредством подключения к частной WAN. Компании необходимо контролировать доступ сотрудников к услугам telnet и FTP. Только R1 объекта имеет разрешение на доступ к серверу telnet на основном объекте. Только R3 объекта имеет разрешение на доступ к серверу FTP.

Задания

Шаг 1 Подготовка среды

Если вы еще не произвели настройку устройства, начните с шага 1, а затем перейдите к шагу 3. Для тех, кто продолжает предыдущие лабораторные работы, необходимо начать с шага 2.

```
[Huawei]sysname R1
```

```
[Huawei]sysname R2
[Huawei]sysname R3

[Huawei]sysname S1
[S1]vlan 4
[S1-vlan4]quit
[S1]interface vlanif 4
[S1-Vlanif4]ip address 10.0.4.254 24

[Huawei]sysname S2
[S2]vlan 6
[S2-vlan6]quit
[S2]interface vlanif 6
[S2-Vlanif6]ip address 10.0.6.254 24
```

Шаг 2 Удаление предыдущих конфигураций

Удалите текущую сеть, объявленную в OSPF, интерфейсы номеронабирателя PPPoE, а также конфигурацию виртуального шаблона сервера PPPoE из R2.

```
[R1]ospf
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]undo network 10.0.0.0 0.255.255.255
[R1-ospf-1-area-0.0.0.0]quit
[R1-ospf-1]quit
[R1]undo ip route-static 0.0.0.0 0
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]undo pppoe-client dial-bundle-number 1
[R1]interface Dialer 1
[R1-Dialer1]undo dialer user
[R1]undo interface Dialer 1
[R1]dialer-rule
[R1-dialer-rule]undo dialer-rule 1

[R2]ospf
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]undo network 10.0.0.0 0.255.255.255
[R2-ospf-1-area-0.0.0.0]quit
[R2-ospf-1]quit
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]undo pppoe-server bind
 Warning:All PPPoE sessions on this interface will be deleted, continue?[Y/N]:y
[R2-GigabitEthernet0/0/0]quit
[R2]undo interface Virtual-Template 1
[R2]undo ip pool pool1
[R2]aaa
[R2-aaa]undo local-user huawei1
[R2-aaa]undo local-user huawei2

[R3]ospf
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]undo network 10.0.0.0 0.255.255.255
[R3-ospf-1-area-0.0.0.0]quit
[R3-ospf-1]quit
[R3]undo ip route-static 0.0.0.0 0
[R3]interface GigabitEthernet 0/0/0
```

```
[R3-GigabitEthernet0/0/0]undo pppoe-client dial-bundle-number 1
[R3-GigabitEthernet0/0/0]quit
[R3]interface Dialer 1
[R3-Dialer1]undo dialer user
[R3-Dialer1]quit
[R3]undo interface Dialer 1
[R3]dialer-rule
[R3-dialer-rule]undo dialer-rule 1
```

Шаг 3 Конфигурирование IP-адресации

Сконфигурируйте адресацию для 10.0.13.0/24. Сети 10.0.4.0/24 и 10.0.6.0/24 показаны в топологии на рис. 3-3.

```
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]ip address 10.0.13.1 24

[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ip address 10.0.13.2 24
[R2-GigabitEthernet0/0/0]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.0.4.2 24
[R2-GigabitEthernet0/0/1]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2]ip address 10.0.6.2 24
[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]ip address 10.0.13.3 24
```

Установите магистрали VLAN на S1 и S2. Для интерфейса GigabitEthernet 0/0/2 на S1 должен быть предварительно настроен тип соединения порта.

```
[S1]interface GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]port link-type trunk
[S1-GigabitEthernet0/0/2]port trunk allow-pass vlan all
[S1-GigabitEthernet0/0/2]port trunk pvid vlan 4
[S1-GigabitEthernet0/0/2]quit

[S2]interface GigabitEthernet 0/0/2
[S2-GigabitEthernet0/0/2]port link-type trunk
[S2-GigabitEthernet0/0/2]port trunk allow-pass vlan all
[S2-GigabitEthernet0/0/2]port trunk pvid vlan 6
[S2-GigabitEthernet0/0/2]quit
```

Шаг 4 Настройка OSPF для включения межсетевого взаимодействия

Настройте OSPF для R1, R2 и R3. Убедитесь, что все они являются частью одной и той же области OSPF, и объявите о созданных сетях.

```
[R1]ospf
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255

[R2]ospf
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.4.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.6.0 0.0.0.255

[R3]ospf
```

```
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255
```

Настройте статический маршрут на S1 и S2, установите nexthop в качестве шлюза частной сети.

```
[S1]ip route-static 0.0.0.0 0.0.0.0 10.0.4.2
[S2]ip route-static 0.0.0.0 0.0.0.0 10.0.6.2
```

Убедитесь, что существует маршрут от R1 и R3 до S1 и S2.

```
<R1>ping 10.0.4.254
  PING 10.0.4.254: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.254: bytes=56 Sequence=1 ttl=253 time=2 ms
    Reply from 10.0.4.254: bytes=56 Sequence=2 ttl=253 time=10 ms
    Reply from 10.0.4.254: bytes=56 Sequence=3 ttl=253 time=1 ms
    Reply from 10.0.4.254: bytes=56 Sequence=4 ttl=253 time=2 ms
    Reply from 10.0.4.254: bytes=56 Sequence=5 ttl=253 time=2 ms

  --- 10.0.4.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 1/3/10 ms

<R1>ping 10.0.6.254
  PING 10.0.6.254: 56  data bytes, press CTRL_C to break
    Reply from 10.0.6.254: bytes=56 Sequence=1 ttl=253 time=10 ms
    Reply from 10.0.6.254: bytes=56 Sequence=2 ttl=253 time=2 ms
    Reply from 10.0.6.254: bytes=56 Sequence=3 ttl=253 time=2 ms
    Reply from 10.0.6.254: bytes=56 Sequence=4 ttl=253 time=10 ms
    Reply from 10.0.6.254: bytes=56 Sequence=5 ttl=253 time=2 ms

  --- 10.0.6.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/5/10 ms

<R3>ping 10.0.4.254
  PING 10.0.4.254: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.254: bytes=56 Sequence=1 ttl=253 time=10 ms
    Reply from 10.0.4.254: bytes=56 Sequence=2 ttl=253 time=2 ms
    Reply from 10.0.4.254: bytes=56 Sequence=3 ttl=253 time=2 ms
    Reply from 10.0.4.254: bytes=56 Sequence=4 ttl=253 time=10 ms
    Reply from 10.0.4.254: bytes=56 Sequence=5 ttl=253 time=2 ms

  --- 10.0.4.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 2/5/10 ms
<R3>ping 10.0.6.254
  PING 10.0.6.254: 56  data bytes, press CTRL_C to break
    Reply from 10.0.6.254: bytes=56 Sequence=1 ttl=253 time=10 ms
    Reply from 10.0.6.254: bytes=56 Sequence=2 ttl=253 time=2 ms
    Reply from 10.0.6.254: bytes=56 Sequence=3 ttl=253 time=2 ms
```

```
    Reply from 10.0.6.254: bytes=56 Sequence=4 ttl=253 time=10 ms
    Reply from 10.0.6.254: bytes=56 Sequence=5 ttl=253 time=2 ms

  --- 10.0.6.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/5/10 ms
```

Шаг 5 Настройка фильтров с использованием списков управления доступом

Настройте S1 в качестве сервера telnet.

```
[S1]telnet server enable
[S1]user-interface vty 0 4
[S1-ui-vty0-4]protocol inbound all
[S1-ui-vty0-4]authentication-mode password
[S1-ui-vty0-4]set authentication password cipher huawei123
```

Настройте S2 в качестве сервера FTP.

```
[S2]ftp server enable
[S2]aaa
[S2-aaa]local-user huawei password cipher huawei123
[S2-aaa]local-user huawei privilege level 3
[S2-aaa]local-user huawei service-type ftp
[S2-aaa]local-user huawei ftp-directory flash:/
```

Настройте список управления доступом на R2, чтобы разрешить R1 доступ к серверу telnet, а R3 — доступ к FTP-серверу.

```
[R2]acl 3000
[R2-acl-adv-3000]rule 5 permit tcp source 10.0.13.1 0.0.0.0 destination 10.0.4.254 0.0.0.0 destination-port eq 23
[R2-acl-adv-3000]rule 10 permit tcp source 10.0.13.3 0.0.0.0 destination 10.0.6.254 0.0.0.0 destination-port range 20 21
[R2-acl-adv-3000]rule 15 permit ospf
[R2-acl-adv-3000]rule 20 deny ip source any
[R2-acl-adv-3000]quit
```

Примените ACL к интерфейсу Gigabit Ethernet 0/0/0 маршрутизатора R2.

```
[R2]interface GigabitEthernet0/0/0
[R2-GigabitEthernet0/0/0]traffic-filter inbound acl 3000
```

Проверьте результаты списка управления доступом в сети.

```
<R1>telnet 10.0.4.254
  Press CTRL_] to quit telnet mode
  Trying 10.0.4.254 ...
  Connected to 10.0.4.254 ...
Login authentication
Password:
Info: The max number of VTY users is 5, and the number
      of current VTY users on line is 1.
<S1>
```

Примечание: используйте команду quit для выхода из сеанса telnet.

```
<R1>ftp 10.0.6.254
Trying 10.0.6.254 ...
```

```
Press CTRL+K to abort
Error: Failed to connect to the remote host.
```

Примечание: ответ на соединение FTP может занять некоторое время (около 60 секунд).

```
<R3>telnet 10.0.4.254
  Press CTRL_] to quit telnet mode
  Trying 10.0.4.254 ...
  Error: Can't connect to the remote host

<R3>ftp 10.0.6.254
Trying 10.0.6.254 ...
Press CTRL+K to abort
Connected to 10.0.6.254.
220 FTP service ready.
User(10.0.6.254:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[R3-ftp]
```

Примечание: для закрытия соединения FTP используется команда bye.

Дополнительные упражнения: анализ и проверка

Почему для FTP в списке управления доступом должны быть определены два порта?

Нужно ли развертывать стандартный ACL и расширенный ACL рядом с исходной или целевой сетью и почему?

Окончательная конфигурация

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei password cipher %$%$B:%I)Io0H8)[%SB[idM3C/!#%$%$
 local-user huawei service-type ppp
#
interface GigabitEthernet0/0/0
 ip address 10.0.13.1 255.255.255.0
#
ospf 1 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.13.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
```

```
 set authentication password cipher %$%$dD#}P<HzJ;Xs%X>hOkm!,.+Iq61QK`K6tI}cc-;k_o`C.+L,%$%$
user-interface vty 0 4
#
return
<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
acl number 3000
 rule 5 permit tcp source 10.0.13.1 0 destination 10.0.4.254 0 destination-port eq telnet
 rule 10 permit tcp source 10.0.13.3 0 destination 10.0.6.254 0 destination-port range ftp-data ftp
rule 15 permit ospf
 rule 20 deny ip
#
interface GigabitEthernet0/0/0
 ip address 10.0.13.2 255.255.255.0
 traffic-filter inbound acl 3000
#
interface GigabitEthernet0/0/1
 ip address 10.0.4.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.0.6.2 255.255.255.0
#
ospf 1 router-id 10.0.2.2
 area 0.0.0.0
  network 10.0.4.0 0.0.0.255
  network 10.0.6.0 0.0.0.255
  network 10.0.13.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$|nRPL^hr2IXi7LHDID!/,.*%.8%h;3:,hXO2dk#ikaWI.*(,%$%$
user-interface vty 0 4
#
return


<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
interface GigabitEthernet0/0/0
 ip address 10.0.13.3 255.255.255.0
#
ospf 1 router-id 10.0.3.3
 area 0.0.0.0
  network 10.0.13.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$W|$)M5D}v@bY^gK\;>QR,.*d;8Mp>|+EU,:~D~8b59~..*g,%$%$
user-interface vty 0 4
```

```
#
return


<S1>display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S1
#
 vlan batch 3 to 4
#
interface Vlanif4
 ip address 10.0.4.254 255.255.255.0
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 4
 port trunk allow-pass vlan 2 to 4094
#
ip route-static 0.0.0.0 0.0.0.0 10.0.4.2
#
user-interface con 0
user-interface vty 0 4
authentication-mode password
 set authentication password cipher N`C55QK<`=/Q=^Q`MAF4<1!!
Protocol inbound all
#
return
<S2>dis current-configuration
#
!Software Version V200R008C00SPC500
 sysname S2
#
 FTP server enable
#
 vlan batch 6
#
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
 local-user huawei password cipher N`C55QK<`=/Q=^Q`MAF4<1!!
Local-user huawei privilege level 3
 local-user huawei ftp-directory flash:/
 local-user huawei service-type ftp
#
interface Vlanif6
 ip address 10.0.6.254 255.255.255.0
#
interface GigabitEthernet0/0/2
 port link-type trunk
```

```
 port trunk pvid vlan 6
 port trunk allow-pass vlan 2 to 4094
#
ip route-static 0.0.0.0 0.0.0.0 10.0.6.2
#
user-interface con 0
user-interface vty 0 4
#
return
```

Лабораторная работа 3-2 Преобразование сетевых адресов

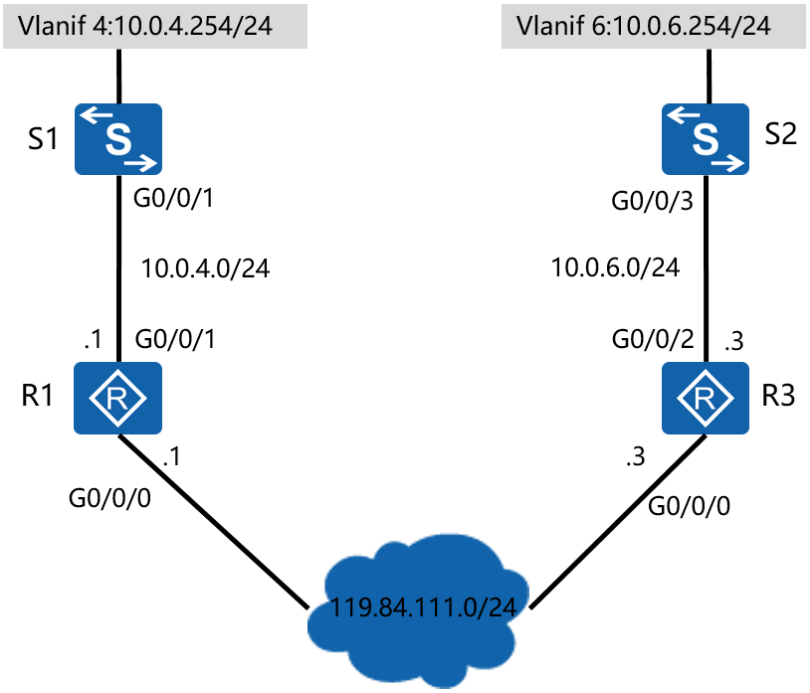
Цели обучения

В ходе данной лабораторной работы вам необходимо выполнить следующие задания:

- Преобразование сетевых адресов (NAT).
- Конфигурирование Easy IP.

Топология

Рис. 3-2 Топология преобразования сетевых адресов



Сценарий

Для сохранения адресации в офисах корпоративной сети внедрена частная адресация внутри компании. Тем не менее, пользователям требуются средства для маршрутизации между этими частными сетями и доменом общедоступной сети. R1 и R3 представляют собой пограничные маршрутизаторы филиалов предприятия; сети филиалов необходим доступ к общедоступной сети. Администратору сети предлагается настроить решения динамического NAT, чтобы разрешить R1 выполнение преобразования адресов. Решение easyIP NAT должно применяться к R3.

Задания

Шаг 1 Подготовка среды

Если вы еще не произвели настройку устройства, начните с шага 1, а затем перейдите к шагу 3. Для тех, кто продолжает предыдущие лабораторные работы, необходимо начать с шага 2.

```
[Huawei]sysname R1
[R1]inter GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.4.1 24

[Huawei]sysname R3
[R3]interface GigabitEthernet0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.0.6.3 24

[Huawei]sysname S1
[S1]vlan 4
[S1-vlan3]quit
[S1]interface vlanif 4
[S1-Vlanif4]ip address 10.0.4.254 24
[S1-Vlanif4]quit

[Huawei]sysname S2
[S2]vlan 6
[S2-vlan6]quit
[S2]interface vlanif 6
[S2-Vlanif6]ip address 10.0.6.254 24
[S2-Vlanif6]quit
```

Шаг 2 Удаление предыдущих конфигураций

Восстановите соединение с S1 и S2 через Gigabit Ethernet 0/0/1 на R1 и Gigabit Ethernet 0/0/2 на R3. Удалите OSPF со всех маршрутизаторов.

```
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]undo ip address
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]undo shutdown
[R1]undo ospf 1
Warning: The OSPF process will be deleted. Continue? [Y/N]:y

[R2]undo ospf 1
Warning: The OSPF process will be deleted. Continue? [Y/N]:y

[R3-GigabitEthernet0/0/0]undo ip address
[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]undo shutdown
[R3]undo ospf 1
Warning: The OSPF process will be deleted. Continue? [Y/N]:y
```

Удалите статические маршруты, указывающие на R2 в S1 и S2.

```
[S1]undo ip route-static 0.0.0.0 0.0.0.0

[S2]undo ip route-static 0.0.0.0 0.0.0.0
```

Шаг 3 Реализация конфигурирования VLAN для S1 и S2

```
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]port link-type trunk
[S1-GigabitEthernet0/0/1]port trunk pvid vlan 4
[S1-GigabitEthernet0/0/1]port trunk allow-pass vlan all
```

```
[S1-GigabitEthernet0/0/1]quit

[S2]interface GigabitEthernet 0/0/3
[S2-GigabitEthernet0/0/3]port link-type trunk
[S2-GigabitEthernet0/0/3]port trunk pvid vlan 6
[S2-GigabitEthernet0/0/3]port trunk allow-pass vlan all

[R1]interface GigabitEthernet0/0/0
[R1-GigabitEthernet0/0/0]ip address 119.84.111.1 24

[R3]interface GigabitEthernet0/0/0
[R3-GigabitEthernet0/0/0]ip address 119.84.111.3 24
```

Убедитесь, что R1 может достичь как S1, так и R3.

```
<R1>ping 10.0.4.254
  PING 10.0.4.254: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.254: bytes=56 Sequence=1 ttl=255 time=23 ms
    Reply from 10.0.4.254: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 10.0.4.254: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 10.0.4.254: bytes=56 Sequence=4 ttl=254 time=10 ms
    Reply from 10.0.4.254: bytes=56 Sequence=5 ttl=254 time=1 ms

  --- 10.0.4.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 1/7/23 ms

<R1>ping 119.84.111.3
  PING 119.84.111.3: 56  data bytes, press CTRL_C to break
    Reply from 119.84.111.3: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 119.84.111.3: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 119.84.111.3: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 119.84.111.3: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 119.84.111.3: bytes=56 Sequence=5 ttl=255 time=10 ms

  --- 119.84.111.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 1/4/10 ms
```

Шаг 4 Настройка списков управления доступом для R1 и R3

Сконфигурируйте расширенный ACL на R1 и выберите поток данных с источником S1, пунктом назначения R3 для сервисного порта telnet.

```
[R1]acl 3000
[R1-acl-adv-3000]rule 5 permit tcp source 10.0.4.254 0.0.0.0 destination 119.84.111.3 0.0.0.0 destination-port eq 23
[R1-acl-adv-3000]rule 10 permit ip source 10.0.4.0 0.0.0.255 destination any
[R1-acl-adv-3000]rule 15 deny ip
```

Сконфигурируйте стандартный ACL на R3 и выберите поток данных, IP-адрес источника которого — 10.0.6.0/24.

```
[R3]acl 2000
```

```
[R3-acl-basic-2000]rule permit source 10.0.6.0 0.0.0.255
```

Шаг 5 Конфигурирование динамического NAT

Настройте статический маршрут на S1 и S2, установите nexthop в качестве шлюза частной сети.

```
[S1]ip route-static 0.0.0.0 0.0.0.0 10.0.4.1
[S2]ip route-static 0.0.0.0 0.0.0.0 10.0.6.3
```

Настройте динамический NAT на интерфейсе GigabitEthernet0/0/0 R1.

```
[R1]nat address-group 1 119.84.111.240 119.84.111.243
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]nat outbound 3000 address-group 1
```

Настройте R3 в качестве сервера telnet.

```
[R3]telnet server enable
[R3]user-interface vty 0 4
[R3-ui-vty0-4]authentication-mode password
[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>):huawei123
Confirm password:huawei123
[R3-ui-vty0-4]quit
```

Убедитесь, что группа адресов настроена правильно.

```
<R1>display nat address-group
 NAT Address-Group Information:
 ----------------------------------------
 Index    Start-address          End-address
 ----------------------------------------
 1        119.84.111.240    119.84.111.243
 ----------------------------------------
        Total : 1
```

Проверьте подключение к шлюзу удаленного одноранговой узла от внутренней сети.

```
<S1>ping 119.84.111.3
  PING 119.84.111.3: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 119.84.111.3: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 119.84.111.3: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 119.84.111.3: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 119.84.111.3: bytes=56 Sequence=5 ttl=254 time=1 ms

  --- 119.84.111.3 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

Установите соединение telnet с общедоступным адресом удаленного однорангового узла.

```
<S1>telnet 119.84.111.3
Trying 119.84.111.3 ...
Press CTRL+K to abort
Connected to 119.84.111.3 ...

Login authentication

Password:
<R3>
```

Не выходите из сеанса telnet, вместо этого откройте второе окно сеанса для R1 и просмотрите результаты преобразования сеансов ACL и NAT.

```
<R1>display acl 3000
Advanced ACL 3000, 3 rules
Acl's step is 5
rule 5 permit tcp source 10.0.4.254 0 destination 119.84.111.3 0 destination-port eq telnet (1 matches)
rule 10 permit ip source 10.0.4.0 0.0.0.255 (1 matches)
rule 15 deny ip

<R1>display nat session all
  NAT Session Table Information:

     Protocol                    : ICMP(1)
     SrcAddr    Vpn              : 10.0.4.254
     DestAddr   Vpn              : 119.84.111.3
     Type Code IcmpId            : 8    0    44003
     NAT-Info
       New SrcAddr               : 119.84.111.242
       New DestAddr              : ----
       New IcmpId                : 10247

     Protocol                    : TCP(6)
     SrcAddr Port Vpn       : 10.0.4.254         49646
     DestAddr Port Vpn           : 119.84.111.3      23
     NAT-Info
       New SrcAddr               : 119.84.111.242
       New SrcPort               : 10249
       New DestAddr              : ----
       New DestPort              : ----

  Total : 2
```

Время сеанса ICMP составляет всего 20 секунд и, следовательно, может отсутствовать при отображении результатов сеанса NAT. В этом случае для продления периода, в течение которого сохраняются результаты ICMP, используется следующая команда:

```
[R1]firewall-nat session icmp aging-time 300
```

Сконфигурируйте easyIP на интерфейсе Gigabit Ethernet 0/0/0 R3, связав конфигурацию easyIP с ACL 2000, который был настроен ранее.

```
[R3-GigabitEthernet0/0/0]nat outbound 2000
```

Проверьте подключение от S2 к R1 через R3.

```
<S2>ping 119.84.111.1
  PING 119.84.111.1: 56  data bytes, press CTRL_C to break
    Reply from 119.84.111.1: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 119.84.111.1: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 119.84.111.1: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 119.84.111.1: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 119.84.111.1: bytes=56 Sequence=5 ttl=254 time=1 ms

  --- 119.84.111.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 1/1/1 ms

<R3>display acl 2000
Basic ACL 2000, 1 rule
Acl's step is 5
 rule 5 permit source 10.0.6.0 0.0.0.255 (1 matches)

<R3>display nat outbound acl 2000
 NAT Outbound Information: ----------------------------------------------------------------------
Interface                        Acl         Address-group/IP/Interface        Type
----------------------------------------------------------------------
GigabitEthernet0/0/0    2000                        119.84.111.3      easyip
----------------------------------------------------------------------
  Total : 1
```

Окончательная конфигурация

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
firewall-nat session icmp aging-time 300
#
acl number 3000
 rule 5 permit tcp source 10.0.4.254 0 destination 119.84.111.3 0 destination-port eq telnet
 rule 10 permit ip source 10.0.4.0 0.0.0.255
 rule 15 deny ip
#
 nat address-group 1 119.84.111.240 119.84.111.243
#
interface GigabitEthernet0/0/0
 ip address 119.84.111.1 255.255.255.0
 nat outbound 3000 address-group 1
#
interface GigabitEthernet0/0/1
 ip address 10.0.4.1 255.255.255.0
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$dD#}P<HzJ;Xs%X>hOkm!,.+Iq61QK`K6tI}cc-;k_o`C.+L,%$%$
user-interface vty 0 4
#
```

```
return


<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
telnet server enable
#
acl number 2000
 rule 5 permit source 10.0.6.0 0.0.0.255
#
interface GigabitEthernet0/0/0
 ip address 119.84.111.3 255.255.255.0
 nat outbound 2000
#
interface GigabitEthernet0/0/2
 ip address 10.0.6.3 255.255.255.0
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$W|$)M5D}v@bY^gK\;>QR,.*d;8Mp>|+EU,:~D~8b59~..*g,%$%$
user-interface vty 0 4
 authentication-mode password
 set authentication password cipher %$%$7ml|,!ccE$SQ~CZ{GtaE%hO>v}~bVk18p5qq<:UPtI:9hOA%%$%$
#
return

<S1>display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S1
#
 vlan batch 4
#
interface Vlanif4
 ip address 10.0.4.254 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 4
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 4
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/14
 shutdown
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.4.1
#
user-interface con 0
```

```
user-interface vty 0 4
 set authentication password cipher N`C55QK<`=/Q=^Q`MAF4<1!!
#
return
<S2>display current-configuration
#
!Software Version V200R008C00SPC500
 sysname S2
#
 vlan batch 6
#
interface Vlanif6
 ip address 10.0.6.254 255.255.255.0
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 6
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk pvid vlan 6
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/23
 shutdown
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.6.3
#
user-interface con 0
user-interface vty 0 4
#
return
```

Лабораторная работа 3-3 Установка решений локального AAA

Цели обучения

В ходе данной лабораторной работы вам необходимо выполнить следующие задания:

- Конфигурация локального AAA, для которого должны использоваться схемы аутентификации и авторизации.
- Создание домена с именем huawei.
- Реализация уровней привилегий для аутентифицированных пользователей.

Топология

Рис. 3-3 Конфигурация AAA

Сценарий

R1 и R3 были развернуты в сети и должны предоставлять услуги удаленной аутентификации с использованием AAA. Компания требует, чтобы оба маршрутизатора были включены в домен huawei и чтобы услуга telnet была доступна пользователям с ограниченными привилегиями, предоставляемыми после проверки подлинности.

Задания

Шаг 1 Подготовка среды

Если вы еще не произвели настройку устройства, начните с шага 1, а затем перейдите к шагу 3. Для тех, кто продолжает предыдущие лабораторные работы, необходимо начать с шага 2.

```
[Huawei]sysname R1
[R1]interface GigabitEthernet0/0/0
[R1-GigabitEthernet0/0/0]ip address 119.84.111.1 24

[Huawei]sysname R3
[R3]inter GigabitEthernet0/0/0
[R3-GigabitEthernet0/0/0]ip address 119.84.111.3 24
```

Шаг 2 Удаление предыдущих конфигураций

Удалите предыдущую конфигурацию NAT и ACL из R1 и R3.

```
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]undo nat outbound 3000 address-group 1
[R1-GigabitEthernet0/0/0]quit
```

```
[R1]undo nat address-group 1
[R1]undo acl 3000

[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]undo nat outbound 2000
[R3-GigabitEthernet0/0/0]quit
[R3]undo acl 2000
```

Шаг 3 Проверка связи между R1 и R3

```
<R1>ping 119.84.111.3
  PING 119.84.111.3: 56  data bytes, press CTRL_C to break
    Reply from 119.84.111.3: bytes=56 Sequence=1 ttl=255 time=70 ms
    Reply from 119.84.111.3: bytes=56 Sequence=2 ttl=255 time=20 ms
    Reply from 119.84.111.3: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 119.84.111.3: bytes=56 Sequence=4 ttl=255 time=20 ms
    Reply from 119.84.111.3: bytes=56 Sequence=5 ttl=255 time=10 ms

  --- 119.84.111.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 10/26/70 ms
```

Шаг 4 Выполнение конфигурации AAA на R1

Настройте схему аутентификации и схему авторизации на R1. Конфигурация R3 приведена в шаге 5.

```
[R1]aaa
[R1-aaa]authentication-scheme auth1
Info: Create a new authentication scheme.
[R1-aaa-authen-auth1]authentication-mode local
[R1-aaa-authen-auth1]quit
[R1-aaa]authorization-scheme auth2
Info: Create a new authorization scheme.
[R1-aaa-author-auth2]authorization-mode local
[R1-aaa-author-auth2]quit
```

Сконфигурируйте домен *huawei* на R1, затем создайте пользователя и примените для него этот домен.

```
[R1]telnet server enable
[R1]aaa
[R1-aaa]domain huawei
[R1-aaa-domain-huawei]authentication-scheme auth1
[R1-aaa-domain-huawei]authorization-scheme auth2
[R1-aaa-domain-huawei]quit
[R1-aaa]local-user user1@huawei password cipher huawei123
[R1-aaa]local-user user1@huawei service-type telnet
[R1-aaa]local-user user1@huawei privilege level 0
```

Настройте R1 в качестве сервера telnet, используя режим аутентификации AAA.

```
[R1]user-interface vty 0 4
[R1-ui-vty0-4]authentication-mode aaa
```

Убедитесь, что служба telnet на R1 была успешно установлена.

```
<R3>telnet 119.84.111.1
  Press CTRL_] to quit telnet mode
  Trying 119.84.111.1 ...
  Connected to 119.84.111.1 ...

Login authentication

Username:user1@huawei
Password:
<R1>system-view
      ^
Error: Unrecognized command found at '^' position.
<R1>quit
```

Операции ограничены, поскольку привилегии пользователя ограничены уровнем привилегий 0 для user1@huawei.

Шаг 5 Выполнение конфигурации AAA на R3

Сконфигурируйте режим аутентификации *local* на R3, а также режим авторизации *local*.

```
[R3]aaa
[R3-aaa]authentication-scheme auth1
Info: Create a new authentication scheme.
[R3-aaa-authen-auth1]authentication-mode local
[R3-aaa-authen-auth1]quit
[R3-aaa]authorization-scheme auth2
Info: Create a new authorization scheme.
[R3-aaa-author-auth2]authorization-mode local
[R3-aaa-author-auth2]quit
```

Сконфигурируйте домен *huawei* на R3, затем создайте пользователя и примените для него этот домен.

```
[R3]telnet server enable
[R3]aaa
[R3-aaa]domain huawei
[R3-aaa-domain-huawei]authentication-scheme auth1
[R3-aaa-domain-huawei]authorization-scheme auth2
[R3-aaa-domain-huawei]quit
[R3-aaa]local-user user3@huawei password cipher huawei123
[R3-aaa]local-user user3@huawei service-type telnet
[R3-aaa]local-user user3@huawei privilege level 0
```

Настройте службу telnet на R3 для использования режима аутентификации AAA.

```
[R3]user-interface vty 0 4
[R3-ui-vty0-4]authentication-mode aaa
```

Проверьте результаты реализации AAA на интерфейсе vty.

```
<R1>telnet 119.84.111.3
  Press CTRL_] to quit telnet mode
  Trying 119.84.111.1 ...
  Connected to 119.84.111.1 ...

Login authentication

Username:user3@huawei
```

```
Password:
<R3>system-view
      ^
Error: Unrecognized command found at '^' position.
<R3>
```

Операции ограничены, поскольку для привилегий пользователя установлено значение уровня привилегий 0 для *user3@huawei*.

Шаг 6 Просмотр результатов конфигурации AAA

```
<R1>display domain name huawei
  Domain-name                          : huawei
  Domain-state                         : Active
  Authentication-scheme-name     : auth1
  Accounting-scheme-name         : default
  Authorization-scheme-name      : auth2
  Service-scheme-name                  : -
  RADIUS-server-template         : -
  HWTACACS-server-template             : -
  User-group                           : -

<R1>display local-user username user1@huawei
  The contents of local user(s):
  Password                       : **********
  State                          : active
  Service-type-mask          : T
  Privilege level          : 0
  Ftp-directory              : -
  Access-limit               : -
  Accessed-num               : 0
  Idle-timeout               : -
  User-group                 : -

<R3>display domain name huawei

  Domain-name                          : huawei
  Domain-state                         : Active
  Authentication-scheme-name     : auth1
  Accounting-scheme-name         : default
  Authorization-scheme-name            : auth2
  Service-scheme-name                  : -
  RADIUS-server-template         : -
  HWTACACS-server-template             : -
  User-group                           : -

<R3>display local-user username user3@huawei
  The contents of local user(s):
  Password                       : **********
  State                          : active
  Service-type-mask          : T
  Privilege level          : 0
  Ftp-directory              : -
  Access-limit               : -
  Accessed-num               : 0
  Idle-timeout               : -
```

User-group : -

Окончательная конфигурация

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
telnet server enable
#
aaa
 authentication-scheme default
 authentication-scheme auth1
 authorization-scheme default
 authorization-scheme auth2
 accounting-scheme default
 domain default
 domain default_admin
 domain huawei
  authentication-scheme auth1
  authorization-scheme auth2
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei password cipher %$%$B:%I)Io0H8)[%SB[idM3C/!#%$%$
 local-user huawei service-type ppp
 local-user user1@huawei password cipher %$%$^L*5IP'0^A!;R)R*L=LFcXgv%$%$
 local-user user1@huawei privilege level 0
 local-user user1@huawei service-type telnet
#
interface GigabitEthernet0/0/0
 ip address 119.84.111.1 255.255.255.0
 nat outbound 3000 address-group 1    //may remain from previous labs
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$dD#}P<HzJ;Xs%X>hOkm!,.+Iq61QK`K6tI}cc-;k_o`C.+L,%$%$
user-interface vty 0 4
 authentication-mode aaa
#
return



<R3>dis current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
telnet server enable
#
aaa
 authentication-scheme default
 authentication-scheme auth1
 authorization-scheme default
```

```
 authorization-scheme auth2
 accounting-scheme default
 domain default
 domain default_admin
 domain huawei
  authentication-scheme auth1
  authorization-scheme auth2
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
 local-user huawei password cipher %$%$fZsyUk1=O=>:L4'ytgR~D*Im%$%$
 local-user huawei service-type ppp
 local-user user3@huawei password cipher %$%$WQt.;bEsR<8fz3LCiPY,che_%$%$
 local-user user3@huawei privilege level 0
 local-user user3@huawei service-type telnet
#
interface GigabitEthernet0/0/0
 ip address 119.84.111.3 255.255.255.0
 nat outbound 2000      //may remain from previous labs
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$W|$)M5D}v@bY^gK\;>QR,.*d;8Mp>|+EU,:~D~8b59~..*g,%$%$
user-interface vty 0 4
 authentication-mode aaa
#
return
```

Лабораторная работа 3-4 Защита трафика с IPSec VPN

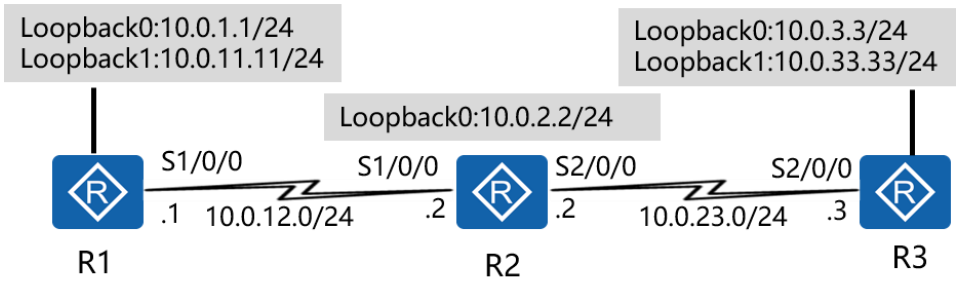
Цели обучения

В ходе данной лабораторной работы вам необходимо выполнить следующие задания:

- Конфигурирование предложения IPSec с использованием набора преобразования esp.
- Конфигурация ACL, используемая для определения «интересного» трафика.
- Конфигурация политики IPSec.
- Привязка политики IPSec к интерфейсу.

Топология

Рис. 3-4 Топология IPSec VPN



Сценарий

В интересах защиты как целостности, так и конфиденциальности данных компании требуется, чтобы связь между офисами предприятия обеспечивала безопасность конкретных частных данных при их передаче по инфраструктуре общедоступной сети. Как сетевому администратору компании, вам было поручено внедрить решения IPSec VPN между пограничным маршрутизатором HQ (R1) и офисом филиала (R3). В настоящее время выбраны только отделы в штаб-квартире, предъявляющие требования к обеспечению безопасности связи в общедоступной сети (R2). Администратор должен установить IPSec, используя туннельный режим между двумя офисами для всего трафика, исходящего из отдела.

Задания

Шаг 1 Подготовка среды

Если вы еще не произвели настройку устройства, начните с шага 1, а затем перейдите к шагу 3. Для тех, кто продолжает предыдущие лабораторные работы, необходимо начать с шага 2.

```
<Huawei>system-view
[Huawei]sysname R1
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ip address 10.0.12.1 24
[R1-Serial1/0/0]interface loopback 0
[R1-LoopBack0]ip address 10.0.1.1 24
```

```
<Huawei>system-view
[Huawei]sysname R2
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]ip address 10.0.12.2 24
[R2-Serial1/0/0]interface serial 2/0/0
[R2-Serial2/0/0]ip address 10.0.23.2 24
[R2-Serial2/0/0]interface loopback 0
[R2-LoopBack0]ip address 10.0.2.2 24
<Huawei>system-view
[Huawei]sysname R3
[R3]interface Serial  2/0/0
[R3-Serial2/0/0]ip address 10.0.23.3 24
[R3-Serial2/0/0]interface loopback 0
[R3-LoopBack0]ip address 10.0.3.3 24
```

Шаг 2 Удаление предыдущих конфигураций

Для предотвращения возникновения альтернативных маршрутов удалите адресацию для интерфейса Gigabit Ethernet 0/0/0 на R1 и R3 и отключите интерфейсы, как показано ниже.

```
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]undo ip address
[R1-GigabitEthernet0/0/0]quit
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]shutdown
[R1-GigabitEthernet0/0/1]quit
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]undo shutdown
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]undo shutdown
[R2]interface Serial 2/0/0
[R2-Serial2/0/0]undo shutdown

[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]undo ip address
[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]shutdown
[R3]interface Serial 2/0/0
[R3-Serial2/0/0]undo shutdown
```

Шаг 3 Настройка дополнительных логических интерфейсов

```
[R1-LoopBack0]interface loopback 1
[R1-LoopBack1]ip address 10.0.11.11 24
[R3-LoopBack0]interface loopback 1
[R3-LoopBack1]ip address 10.0.33.33 24
```

Шаг 4 Настройка OSPF

Используйте IP-адрес Loopback 0 в качестве идентификатора маршрутизатора, используйте процесс OSPF по умолчанию (1) и укажите сегменты общедоступной сети 10.0.12.0/24 и 10.0.23.0/24 в качестве часть области 0 OSPF.

```
[R1]ospf router-id 10.0.1.1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.1.0 0.0.0.255
```

```
[R1-ospf-1-area-0.0.0.0]network 10.0.11.0 0.0.0.255

[R2]ospf router-id  10.0.2.2
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.0.2.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network  10.0.12.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network  10.0.23.0 0.0.0.255

[R3]ospf router-id  10.0.3.3
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network  10.0.23.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network  10.0.3.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network  10.0.33.0 0.0.0.255
```

После завершения конвергенции маршрута OSPF проверьте конфигурацию.

```
<R2>display ospf peer brief
            OSPF Process 1 with Router ID 10.0.2.2
                    Peer Statistic Information
 --------------------------------------------------------------------------------
 Area Id          Interface                        Neighbor id      State
 0.0.0.0          Serial1/0/0                      10.0.1.1         Full
 0.0.0.0          Serial2/0/0                      10.0.3.3         Full
 --------------------------------------------------------------------------------

<R1>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
            Destinations : 17        Routes : 17

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

10.0.1.0/24         Direct0 0           D   10.0.1.1        LoopBack0
10.0.1.1/32         Direct0 0           D   127.0.0.1       LoopBack0
10.0.1.255/32       Direct0 0           D   127.0.0.1       LoopBack0
10.0.2.2/32         OSPF    10   781          D   10.0.12.2       Serial1/0/0
10.0.3.3/32         OSPF    10   2343    D   10.0.12.2       Serial1/0/0
10.0.11.0/24        Direct0 0           D   10.0.11.11      LoopBack1
10.0.11.11/32       Direct0 0           D   127.0.0.1       LoopBack1
10.0.11.255/32      Direct0 0           D   127.0.0.1       LoopBack1
10.0.12.0/24        Direct0 0           D   10.0.12.1       Serial1/0/0
10.0.12.1/32        Direct0 0           D   127.0.0.1       Serial1/0/0
10.0.12.2/32        Direct0 0           D   10.0.12.2       Serial1/0/0
10.0.12.255/32      Direct0 0           D   127.0.0.1       Serial1/0/0
10.0.23.0/24        OSPF    10   2343    D   10.0.12.2       Serial1/0/0
10.0.33.33/32       OSPF    10   2343    D   10.0.12.2       Serial1/0/0
127.0.0.0/8         Direct0 0           D   127.0.0.1       InLoopBack0
127.0.0.1/32        Direct0 0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct0 0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct0 0           D   127.0.0.1       InLoopBack0
```

Если скорость передачи поддерживается на уровне 128000 из лабораторной работы 6-1, стоимость OSPF будет установлена, как показано ниже, и, таким образом, может варьироваться в зависимости от расчета метрики, используемой OSPF.

```
<R3>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 17        Routes : 17

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

10.0.1.1/32         OSPF    10   3124      D   10.0.23.2       Serial2/0/0
10.0.2.2/32         OSPF    10   1562      D   10.0.23.2       Serial2/0/0
10.0.3.0/24         Direct  0    0         D   10.0.3.3        LoopBack0
10.0.3.3/32         Direct  0    0         D   127.0.0.1       LoopBack0
10.0.3.255/32       Direct  0    0         D   127.0.0.1       LoopBack0
10.0.11.11/32       OSPF    10   3124      D   10.0.23.2       Serial2/0/0
10.0.12.0/24        OSPF    10   3124      D   10.0.23.2       Serial2/0/0
10.0.23.0/24        Direct  0    0         D   10.0.23.3       Serial2/0/0
10.0.23.2/32        Direct  0    0         D   10.0.23.2       Serial2/0/0
10.0.23.3/32        Direct  0    0         D   127.0.0.1       Serial2/0/0
10.0.23.255/32      Direct  0    0         D   127.0.0.1       Serial2/0/0
10.0.33.0/24        Direct  0    0         D   10.0.33.33      LoopBack1
10.0.33.33/32       Direct  0    0         D   127.0.0.1       LoopBack1
10.0.33.255/32      Direct  0    0         D   127.0.0.1       LoopBack1
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
```

Шаг 5 Конфигурирование ACL для определения «интересного» трафика

Расширенный ACL создается для определения «интересного» трафика, для которого будет применяться IPSec VPN. Расширенный ACL имеет возможность фильтрования на основе определенных параметров для выборочной фильтрации трафика.

```
[R1]acl 3001
[R1-acl-adv-3001]rule 5 permit ip source 10.0.1.0 0.0.0.255 destination 10.0.3.0 0.0.0.255

[R3]acl 3001
[R3-acl-adv-3001]rule 5 permit ip source 10.0.3.0 0.0.0.255 destination 10.0.1.0 0.0.0.255
```

Шаг 6 Конфигурирование предложения IPSec VPN

Создайте предложение IPSec и войдите в представление предложения IPSec, чтобы указать используемые протоколы безопасности. Убедитесь, что оба узла используют одинаковые протоколы.

```
[R1]ipsec proposal tran1
[R1-ipsec-proposal-tran1]esp authentication-algorithm sha1
[R1-ipsec-proposal-tran1]esp encryption-algorithm 3des

[R3]ipsec proposal tran1
[R3-ipsec-proposal-tran1]esp authentication-algorithm sha1
[R3-ipsec-proposal-tran1]esp encryption-algorithm 3des
```

Выполните команду **display ipsec proposal** для проверки конфигурации.

```
[R1]display ipsec proposal

Number of proposals: 1

IPSec proposal name  :    tran1
  Encapsulation mode :    Tunnel
  Transform          :    esp-new
  ESP protocol       :    Authentication SHA1-HMAC-96
Encryption       3DES

[R3]display ipsec proposal
```

Шаг 7 Создание политики IPSec

Создайте политику IPSec и определите параметры для установления SA.

```
[R1]ipsec   policy P1 10 manual
[R1-ipsec-policy-manual-P1-10]security acl 3001
[R1-ipsec-policy-manual-P1-10]proposal tran1
[R1-ipsec-policy-manual-P1-10]tunnel remote 10.0.23.3
[R1-ipsec-policy-manual-P1-10]tunnel local 10.0.12.1
[R1-ipsec-policy-manual-P1-10]sa spi outbound esp 54321
[R1-ipsec-policy-manual-P1-10]sa spi inbound esp 12345
[R1-ipsec-policy-manual-P1-10]sa string-key outbound esp simple huawei
[R1-ipsec-policy-manual-P1-10]sa string-key inbound esp simple huawei

[R3]ipsec   policy P1 10 manual
[R3-ipsec-policy-manual-P1-10]security acl 3001
[R3-ipsec-policy-manual-P1-10]proposal tran1
[R3-ipsec-policy-manual-P1-10]tunnel remote 10.0.12.1
[R3-ipsec-policy-manual-P1-10]tunnel local 10.0.23.3
[R3-ipsec-policy-manual-P1-10]sa spi outbound esp 12345
[R3-ipsec-policy-manual-P1-10]sa spi inbound esp 54321
[R3-ipsec-policy-manual-P1-10]sa string-key outbound esp simple huawei
[R3-ipsec-policy-manual-P1-10]sa string-key inbound esp simple huawei
```

Выполните команду **display ipsec policy** для проверки конфигурации.

```
<R1>display ipsec policy

==========================================
IPSec policy group: "P1"
Using interface:
==========================================

    Sequence number: 10
    Security data flow: 3001
    Tunnel local    address: 10.0.12.1
    Tunnel remote address: 10.0.23.3
    Qos pre-classify: Disable
    Proposal name:tran1
    Inbound AH setting:
      AH SPI:
      AH string-key:
```

```
    AH authentication hex key:
  Inbound ESP setting:
    ESP SPI: 12345 (0x3039)
    ESP string-key: huawei
    ESP encryption hex key:
    ESP authentication hex key:
  Outbound AH setting:
    AH SPI:
    AH string-key:
    AH authentication hex key:
  Outbound ESP setting:
    ESP SPI: 54321 (0xd431)
    ESP string-key: huawei
    ESP encryption hex key:
    ESP authentication hex key:

<R3>display ipsec policy

==========================================
IPSec policy group: "P1"
Using interface:
==========================================

  Sequence number: 10
  Security data flow: 3001
  Tunnel local    address: 10.0.23.3
  Tunnel remote address: 10.0.12.1
  Qos pre-classify: Disable
  Proposal name:tran1
  Inbound AH setting:
    AH SPI:
    AH string-key:
    AH authentication hex key:
  Inbound ESP setting:
    ESP SPI: 54321 (0xd431)
    ESP string-key: huawei
    ESP encryption hex key:
    ESP authentication hex key:
  Outbound AH setting:
    AH SPI:
    AH string-key:
    AH authentication hex key:
  Outbound ESP setting:
    ESP SPI: 12345 (0x3039)
    ESP string-key: huawei
    ESP encryption hex key:
    ESP authentication hex key:
```

Шаг 8 Применение политик IPSec к интерфейсам

Примените политику к физическому интерфейсу, на котором трафик будет подвергаться обработке IPSec.

```
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ipsec policy P1
```

```
[R3]interface Serial 2/0/0
[R3-Serial2/0/0]ipsec policy P1
```

Шаг 9 Проверка связи между IP-сетями

Убедитесь, что «неинтересный» трафик обходит обработку IPSec.

```
<R1>ping -a 10.0.11.11 10.0.33.33
  PING 10.0.33.33: 56  data bytes, press CTRL_C to break
    Reply from 10.0.33.33: bytes=56 Sequence=1 ttl=254 time=60 ms
    Reply from 10.0.33.33: bytes=56 Sequence=2 ttl=254 time=50 ms
    Reply from 10.0.33.33: bytes=56 Sequence=3 ttl=254 time=50 ms
    Reply from 10.0.33.33: bytes=56 Sequence=4 ttl=254 time=60 ms
    Reply from 10.0.33.33: bytes=56 Sequence=5 ttl=254 time=50 ms
  --- 10.0.33.33 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 50/54/60 ms

<R1>display ipsec statistics esp
 Inpacket count                : 0
 Inpacket auth count           : 0
 Inpacket decap count          : 0
 Outpacket count               : 0
 Outpacket auth count          : 0
 Outpacket encap count         : 0
 Inpacket drop count           : 0
 Outpacket drop count          : 0
 BadAuthLen count              : 0
 AuthFail count                : 0
 InSAAclCheckFail count        : 0
 PktDuplicateDrop count        : 0
 PktSeqNoTooSmallDrop count    : 0
 PktInSAMissDrop count         : 0
```

Обратите внимание, что IPSec VPN будет защищать только «интересный» трафик.

```
<R1>ping -a 10.0.1.1 10.0.3.3
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.3.3: bytes=56 Sequence=1 ttl=255 time=80 ms
    Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=255 time=77 ms
    Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=255 time=77 ms
    Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=255 time=80 ms
    Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=255 time=77 ms
  --- 10.0.3.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 77/78/80 ms

<R1>display ipsec statistics esp
 Inpacket count                : 5
 Inpacket auth count           : 0
 Inpacket decap count          : 0
```

```
Outpacket count                : 5
Outpacket auth count           : 0
Outpacket encap count                : 0
Inpacket drop count            : 0
Outpacket drop count           : 0
BadAuthLen count                     : 0
AuthFail count                       : 0
InSAAclCheckFail count               : 0
PktDuplicateDrop count               : 0
PktSeqNoTooSmallDrop count           : 0
PktInSAMissDrop count                : 0
```

Окончательная конфигурация

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
acl number 3001
 rule 5 permit ip source 10.0.1.0 0.0.0.255 destination 10.0.3.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy P1 10 manual
 security acl 3001
 proposal tran1
 tunnel local 10.0.12.1
 tunnel remote 10.0.23.3
 sa spi inbound esp 12345
 sa string-key inbound esp simple huawei
 sa spi outbound esp 54321
 sa string-key outbound esp simple huawei
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode pap
 ip address 10.0.12.1 255.255.255.0
 ipsec policy P1
 baudrate 128000
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.0.11.11 255.255.255.0
#
ospf 1 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
  network 10.0.11.0 0.0.0.255
  network 10.0.12.0 0.0.0.255
#
```

```
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$dD#}P<HzJ;Xs%X>hOkm!,.+Iq61QK`K6tI}cc-;k_o`C.+L,%$%$
user-interface vty 0 4
 authentication-mode aaa
#
return


<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
interface Serial1/0/0
 link-protocol ppp
 ppp pap local-user huawei password cipher %$%$u[hr6d<JVHR@->T7xr1<$.iv%$%$
 ip address 10.0.12.2 255.255.255.0
#
interface Serial2/0/0
 link-protocol ppp
 ppp chap user huawei
 ppp chap password cipher %$%$e{5h)gh"/Uz0mUC%vEx3$4<m%$%$
 ip address 10.0.23.2 255.255.255.0
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.0
#
ospf 1 router-id 10.0.2.2
 area 0.0.0.0
  network 10.0.12.0 0.0.0.255
  network 10.0.23.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$|nRPL^hr2IXi7LHDID!/,.*%.8%h;3:,hXO2dk#ikaWI.*(,%$%$
user-interface vty 0 4
#
return


<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
acl number 3001
 rule 5 permit ip source 10.0.3.0 0.0.0.255 destination 10.0.1.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy P1 10 manual
 security acl 3001
```

```
 proposal tran1
 tunnel local 10.0.23.3
 tunnel remote 10.0.12.1
 sa spi inbound esp 54321
 sa string-key inbound esp simple huawei
 sa spi outbound esp 12345
 sa string-key outbound esp simple huawei
#
interface Serial2/0/0
 link-protocol ppp
 ppp authentication-mode chap
 ip address 10.0.23.3 255.255.255.0
 ipsec policy P1
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.0
#
interface LoopBack1
 ip address 10.0.33.33 255.255.255.0
#
ospf 1 router-id 10.0.3.3
 area 0.0.0.0
  network 10.0.3.0 0.0.0.255
  network 10.0.23.0 0.0.0.255
  network 10.0.33.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$W|$)M5D}v@bY^gK\;>QR,.*d;8Mp>|+EU,:~D~8b59~..*g,%$%$
user-interface vty 0 4
 authentication-mode aaa
#
return
```

Лабораторная работа 3-5 Поддержка динамической маршрутизации с GRE

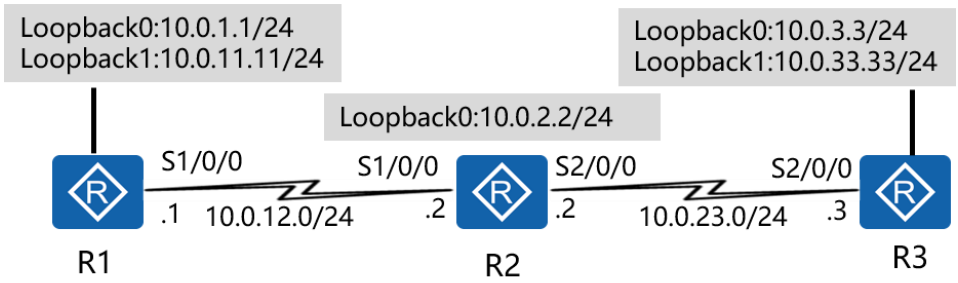
Цели обучения

В ходе данной лабораторной работы вам необходимо выполнить следующие задания:

- Настройка ACL для поддержки инкапсуляции GRE
- Создание туннельного интерфейса для GRE
- Реализация функции keepalive GRE.

Топология

Рис. 3-5 Топология динамической маршрутизации с GRE



Сценарий

Требуется разрешить объявление сетей из других офисов штаб-квартире. После внедрения решений IPSec VPN оказалось, что это сделать невозможно. После проведения ряда консультаций администратору посоветовали внедрить решение GRE в существующей сети IPSec, чтобы корпоративные офисы могли по-настоящему функционировать как единый административный домен.

Задания

Примечание: Перед тем, как приступить к данной лабораторной работе, необходимо выполнить лабораторную работу 3-4.

Шаг 1 Настройка трафика GRE в качестве «интересного» трафика

Перенастройте список управления доступом и установите инкапсуляцию GRE по IPSec.

```
[R1]acl 3001
[R1-acl-adv-3001]rule 5 permit gre source 10.0.12.1 0 destination 10.0.23.3 0

[R3]acl 3001
[R3-acl-adv-3001]rule 5 permit gre source 10.0.23.3 0 destination 10.0.12.1 0
```

Шаг 2 Конфигурирование туннельного интерфейса

Создайте туннельный интерфейс и укажите GRE в качестве типа инкапсуляции. Установите адрес источника туннеля или интерфейс источника и адрес назначения туннеля.

```
[R1]interface Tunnel 0/0/1
[R1-Tunnel0/0/1]ip address 100.1.1.1 24
[R1-Tunnel0/0/1]tunnel-protocol gre
[R1-Tunnel0/0/1]source 10.0.12.1
[R1-Tunnel0/0/1]destination 10.0.23.3
```

```
[R3]interface Tunnel 0/0/1
[R3-Tunnel0/0/1]ip address 100.1.1.2 24
[R3-Tunnel0/0/1]tunnel-protocol gre
[R3-Tunnel0/0/1]source 10.0.23.3
[R3-Tunnel0/0/1]destination 10.0.12.1
```

Шаг 3 Конфигурирование второго процесса OSPF для маршрутизации туннеля

Добавьте сеть с туннельным интерфейсом к процессу OSPF 1 и создайте второй экземпляр OSPF базы данных состояний каналов (процесс 2) для сетей 10.0.12.0 и 10.0.23.0, обязательно удалите эти сети из OSPF 1.

```
[R1]ospf 1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 100.1.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]undo network 10.0.12.0 0.0.0.255
[R1]ospf 2 router-id 10.0.1.1
[R1-ospf-2]area 0
[R1-ospf-2-area-0.0.0.0]network 10.0.12.0 0.0.0.255
```

```
[R3]ospf 1
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 100.1.1.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]undo network 10.0.23.0 0.0.0.255
[R3]ospf 2 router-id 10.0.3.3
[R3-ospf-2]area 0
[R3-ospf-2-area-0.0.0.0]network 10.0.23.0 0.0.0.255
```

OSPF LSDB важны только для локального маршрутизатора, поэтому маршруты от OSPF LSDB 2 R1 и R3 достигают OSPF LSDB 1 R2.

Выполните команду **display interface Tunnel 0/0/1** для проверки конфигурации.

```
<R1>display interface Tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2016-03-17 17:10:16
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 100.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.0.12.1 (Serial1/0/0), destination 10.0.23.3
Tunnel protocol/transport GRE/IP, key disabled
```

```
keepalive disabled
Checksumming of packets disabled
Current system time: 2016-03-17 17:35:39
    Last 300 seconds input rate 0 bytes/sec, 0 packets/sec
    Last 300 seconds output rate 9 bytes/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bytes/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bytes/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    145 packets output, 14320 bytes, 0 drops
    Input bandwidth utilization  : --
Output bandwidth utilization : --

<R3>display interface Tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2016-03-17 17:10:40
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 100.1.1.2/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.0.23.3 (Serial2/0/0), destination 10.0.12.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
Current system time: 2016-03-17 17:36:44
    Last 300 seconds input rate 0 bytes/sec, 0 packets/sec
    Last 300 seconds output rate 9 bytes/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bytes/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bytes/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    162 packets output, 14420 bytes, 15 drops
    Input bandwidth utilization  : --
Output bandwidth utilization : --
```

Шаг 4 Проверка переноса маршрутов посредством GRE

Выполните команду **display ip routing-table** для проверки таблицы маршрутизации IPv4.

```
<R1>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 21        Routes : 21

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.0/24  Direct  0    0           D   10.0.1.1        LoopBack0
        10.0.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
      10.0.1.255/32  Direct  0    0           D   127.0.0.1       LoopBack0
        10.0.2.2/32  OSPF    10   781         D   10.0.12.2       Serial1/0/0
        10.0.3.3/32  OSPF    10   1562        D   100.1.1.2       Tunnel0/0/1
       10.0.11.0/24  Direct  0    0           D   10.0.11.11      LoopBack1
      10.0.11.11/32  Direct  0    0           D   127.0.0.1       LoopBack1
    10.0.11.255/32   Direct  0    0           D   127.0.0.1       LoopBack1
       10.0.12.0/24  Direct  0    0           D   10.0.12.1       Serial1/0/0
```

```
10.0.12.1/32            Direct0  0           D   127.0.0.1       Serial1/0/0
10.0.12.2/32            Direct0  0           D   10.0.12.2       Serial1/0/0
10.0.12.255/32  Direct0  0           D   127.0.0.1       Serial1/0/0
10.0.23.0/24            OSPF     10   2343   D   10.0.12.2       Serial1/0/0
10.0.33.33/32           OSPF     10   1562   D   100.1.1.2       Tunnel0/0/1
100.1.1.0/24            Direct0  0           D   100.1.1.1       Tunnel0/0/1
100.1.1.1/32            Direct0  0           D   127.0.0.1       Tunnel0/0/1
100.1.1.255/32  Direct0  0           D   127.0.0.1       Tunnel0/0/1
127.0.0.0/8             Direct0  0           D   127.0.0.1       InLoopBack0
127.0.0.1/32            Direct0  0           D   127.0.0.1       InLoopBack0
127.255.255.255/32      Direct0  0           D   127.0.0.1       InLoopBack0
255.255.255.255/32      Direct0  0           D   127.0.0.1       InLoopBack0

<R3>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 21        Routes : 21

Destination/Mask Proto Pre  Cost      Flags NextHop         Interface

10.0.1.1/32      OSPF  10   1562      D   100.1.1.1       Tunnel0/0/1
10.0.2.2/32      OSPF  10   1562      D   10.0.23.2       Serial2/0/0
10.0.3.0/24      Direct0  0           D   10.0.3.3        LoopBack0
10.0.3.3/32      Direct0  0           D   127.0.0.1       LoopBack0
10.0.3.255/32           Direct0  0           D   127.0.0.1       LoopBack0
10.0.11.11/32           OSPF     10   1562   D   100.1.1.1       Tunnel0/0/1
10.0.12.0/24            OSPF     10   3124   D   10.0.23.2       Serial2/0/0
10.0.23.0/24            Direct0  0           D   10.0.23.3       Serial2/0/0
10.0.23.2/32            Direct0  0           D   10.0.23.2       Serial2/0/0
10.0.23.3/32            Direct0  0           D   127.0.0.1       Serial2/0/0
10.0.23.255/32  Direct0  0           D   127.0.0.1       Serial2/0/0
10.0.33.0/24            Direct0  0           D   10.0.33.33      LoopBack1
10.0.33.33/32           Direct0  0           D   127.0.0.1       LoopBack1
10.0.33.255/32  Direct0  0           D   127.0.0.1       LoopBack1
100.1.1.0/24            Direct0  0           D   100.1.1.2       Tunnel0/0/1
100.1.1.2/32            Direct0  0           D   127.0.0.1       Tunnel0/0/1
100.1.1.255/32  Direct0  0           D   127.0.0.1       Tunnel0/0/1
127.0.0.0/8     Direct0  0           D   127.0.0.1       InLoopBack0
127.0.0.1/32            Direct0  0           D   127.0.0.1       InLoopBack0
127.255.255.255/32      Direct0  0           D   127.0.0.1       InLoopBack0
255.255.255.255/32      Direct0  0           D   127.0.0.1       InLoopBack0
```

После настройки туннеля GRE маршрутизатор может обмениваться пакетами OSPF через туннель GRE. Удалите статистику IPSec и протестируйте соединение.

```
<R1>reset ipsec statistics esp
[R1]ping -a 10.0.1.1 10.0.3.3
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.3.3: bytes=56 Sequence=1 ttl=255 time=69 ms
    Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=255 time=70 ms
    Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=255 time=68 ms
    Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=255 time=68 ms
    Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=255 time=68 ms
```

```
  --- 10.0.3.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 68/68/70 ms

<R1>display ipsec statistics esp
 Inpacket count                : 8
 Inpacket auth count           : 0
 Inpacket decap count          : 0
 Outpacket count               : 8
 Outpacket auth count          : 0
 Outpacket encap count         : 0
 Inpacket drop count           : 0
 Outpacket drop count          : 0
 BadAuthLen count              : 0
 AuthFail count                : 0
 InSAAclCheckFail count        : 0
 PktDuplicateDrop count        : 0
 PktSeqNoTooSmallDrop count    : 0
 PktInSAMissDrop count         : 0
```

GRE инкапсулирует весь трафик OSPF, включая пакеты hello по IPSec, что подтверждает постепенное увеличение статистики IPSec esp.

Шаг 5 Реализация функции keepalive в туннеле GRE

```
[R1]interface Tunnel 0/0/1
[R1-Tunnel0/0/1]keepalive period 3
```

Убедитесь, что на интерфейсе туннеля включена функция keepalive.

```
<R1>display interface Tunnel 0/0/1
Tunnel0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2016-03-18 09:50:21
Description:HUAWEI, AR Series, Tunnel0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 100.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.0.12.1 (Serial1/0/0), destination 10.0.23.3
Tunnel protocol/transport GRE/IP, key disabled
keepalive enable period 3 retry-times 3
Checksumming of packets disabled
Current system time: 2013-12-18 11:05:49
    Last 300 seconds input rate 0 bytes/sec, 0 packets/sec
    Last 300 seconds output rate 8 bytes/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bytes/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bytes/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    503 packets output, 47444 bytes, 0 drops
    Input bandwidth utilization  : --
Output bandwidth utilization : --
```

Окончательная конфигурация

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
acl number 3001
 rule 5 permit gre source 10.0.12.1 0 destination 10.0.23.3 0
#
ipsec proposal tran1
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy P1 10 manual
 security acl 3001
 proposal tran1
 tunnel local 10.0.12.1
 tunnel remote 10.0.23.3
 sa spi inbound esp 12345
 sa string-key inbound esp simple huawei
 sa spi outbound esp 54321
 sa string-key outbound esp simple huawei
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode pap
 ip address 10.0.12.1 255.255.255.0
 ipsec policy P1
 baudrate 128000
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.0.11.11 255.255.255.0
#
interface Tunnel0/0/1
 ip address 100.1.1.1 255.255.255.0
 tunnel-protocol gre
 keepalive period 3
 source 10.0.12.1
 destination 10.0.23.3
#
ospf 1 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
  network 10.0.11.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
#
ospf 2 router-id 10.0.1.1
 area 0.0.0.0
  network 10.0.12.0 0.0.0.255
#
user-interface con 0
```

```
 authentication-mode password
 set authentication password cipher %$%$dD#}P<HzJ;Xs%X>hOkm!,.+Iq61QK`K6tI}cc-;k_o`C.+L,%$%$
user-interface vty 0 4
 authentication-mode aaa
#
return


<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
interface Serial1/0/0
 link-protocol ppp
 ppp pap local-user huawei password cipher %$%$u[hr6d<JVHR@->T7xr1<$.iv%$%$
 ip address 10.0.12.2 255.255.255.0
#
interface Serial2/0/0
 link-protocol ppp
 ppp chap user huawei
 ppp chap password cipher %$%$e{5h)gh"/Uz0mUC%vEx3$4<m%$%$
 ip address 10.0.23.2 255.255.255.0
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.0
#
ospf 1 router-id 10.0.2.2
 area 0.0.0.0
  network 10.0.2.0 0.0.0.255
  network 10.0.12.0 0.0.0.255
  network 10.0.23.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$|nRPL^hr2IXi7LHDID!/,.*%.8%h;3:,hXO2dk#ikaWI.*(,%$%$
user-interface vty 0 4
#
return


<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
acl number 3001
 rule 5 permit gre source 10.0.23.3 0 destination 10.0.12.1 0
#
ipsec proposal tran1
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy P1 10 manual
 security acl 3001
```

```
 proposal tran1
 tunnel local 10.0.23.3
 tunnel remote 10.0.12.1
 sa spi inbound esp 54321
 sa string-key inbound esp simple huawei
 sa spi outbound esp 12345
 sa string-key outbound esp simple huawei
#
interface Serial2/0/0
 link-protocol ppp
 ppp authentication-mode chap
 ip address 10.0.23.3 255.255.255.0
 ipsec policy P1
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.0
#
interface LoopBack1
 ip address 10.0.33.33 255.255.255.0
#
interface Tunnel0/0/1
 ip address 100.1.1.2 255.255.255.0
 tunnel-protocol gre
 source 10.0.23.3
 destination 10.0.12.1
#
ospf 1 router-id 10.0.3.3
 area 0.0.0.0
  network 10.0.3.0 0.0.0.255
  network 10.0.33.0 0.0.0.255
  network 100.1.1.0 0.0.0.255
#
ospf 2 router-id 10.0.3.3
 area 0.0.0.0
  network 10.0.23.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$W|$)M5D}v@bY^gK\;>QR,.*d;8Mp>|+EU,:~D~8b59~..*g,%$%$
user-interface vty 0 4
 authentication-mode aaa
#
return
```

Модуль 4 Создание сетей IPv6

Лабораторная работа 4-1 Реализация сетей и решений IPv6

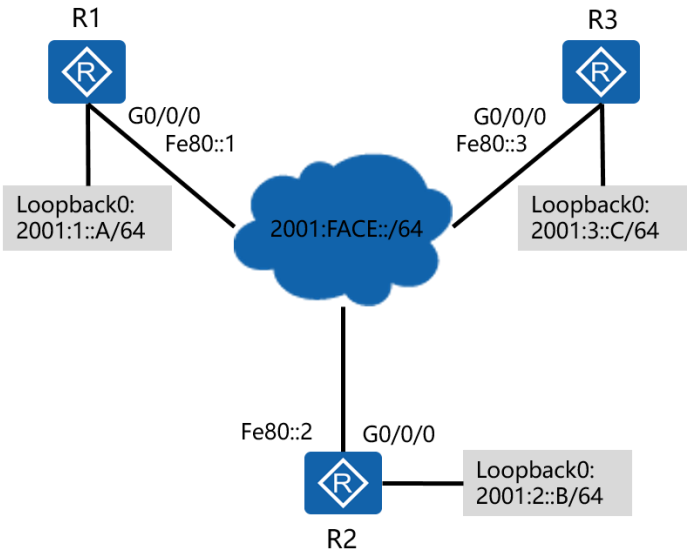
Цели обучения

В ходе данной лабораторной работы вам необходимо выполнить следующие задания:

- Настройка базовой адресации IPv6.
- Настройка протокола маршрутизации OSPFv3.
- Настройка функций сервера DHCPv6.
- Проверка результатов с помощью команд отображения IPv6.

Топология

Рис. 4-1 Топология IPv6



Сценарий

В соответствии с планами развертывания решений для сетей следующего поколения было принято решение о том, что в корпоративной сети необходимо внедрить IPv6 в существующую инфраструктуру. Как администратору, вам было поручено реализовать схему адресации и маршрутизации для IPv6, а также предоставить решения адресации с отслеживанием состояния соединений для IPv6.

Задания

Шаг 1 Подготовка среды

Если вы еще не произвели настройку устройства, начните с шага 1, а затем перейдите к шагу 2. Для тех, кто продолжает предыдущие лабораторные работы, необходимо начать с шага 2.

```
<huawei>system-view
[huawei]sysname R1

<huawei>system-view
[huawei]sysname R2

<huawei>system-view
[huawei]sysname R3
```

Шаг 2 Конфигурирование адресации IPv6

Настройте глобальную адресацию одноадресной передачи IPv6 на интерфейсах loopback и вручную настройте локальную адресацию канала на интерфейсе Gigabit Ethernet 0/0/0 всех маршрутизаторов.

```
[R1]ipv6
[R1]interface loopback 0
[R1-LoopBack0]ipv6 enable
[R1-LoopBack0]ipv6 address 2001:1::A 64
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]ipv6 enable
[R1-GigabitEthernet0/0/0]ipv6 address fe80::1 link-local
[R2]ipv6
[R2]interface loopback 0
[R2-LoopBack0]ipv6 enable
[R2-LoopBack0]ipv6 address 2001:2::B 64
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ipv6 enable
[R2-GigabitEthernet0/0/0]ipv6 address fe80::2 link-local

[R3]ipv6
[R3]interface loopback 0
[R3-LoopBack0]ipv6 enable
[R3-LoopBack0]ipv6 address 2001:3::C 64
[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]ipv6 enable
[R3-GigabitEthernet0/0/0]ipv6 address fe80::3 link-local


<R1>display ipv6 interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::1
  No global unicast address configured
  Joined group address(es):
    FF02::1:FF00:1
    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
```

Интерфейсы IPv6 становятся частью различных групп многоадресной передачи для поддержки автоматической настройки адресов без сохранения состояния (SLAAC). Обнаружение повторяющихся адресов (DAD) при обнаружении сети (ND) проверяет уникальность локального адреса канала.

Шаг 3 Конфигурирование OSPFv3

Включите процесс OSPFv3 и укажите его идентификатор маршрутизатора на R1, R2 и R3. Затем OSPFv3 должен быть включен на интерфейсе.

```
[R1]ospfv3 1
[R1-ospfv3-1]router-id 1.1.1.1
[R1-ospfv3-1]quit
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]ospfv3 1 area 0
[R1-GigabitEthernet0/0/0]quit
[R1]interface loopback 0
[R1-LoopBack0]ospfv3 1 area 0

[R2]ospfv3 1
[R2-ospfv3-1]router-id 2.2.2.2
[R2-ospfv3-1]quit
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ospfv3 1 area 0
[R2-GigabitEthernet0/0/0]quit
[R2]interface loopback 0
[R2-LoopBack0]ospfv3 1 area 0

[R3]ospfv3 1
[R3-ospfv3-1]router-id 3.3.3.3
[R3-ospfv3-1]quit
[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]ospfv3 1 area 0
[R3-GigabitEthernet0/0/0]quit
[R3]interface loopback 0
[R3-LoopBack0]ospfv3 1 area 0
```

Выполните команду **display ospfv3 peer** на R1 и R3, чтобы убедиться, что установлено одноранговое соединение OSPFv3.

```
<R1>display ospfv3 peer
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.0)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
2.2.2.2         1     Full/Backup     00:00:30    GE0/0/0    0
3.3.3.3         1     Full/DROther    00:00:40    GE0/0/0    0
<R3>display ospfv3 peer
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.0)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1         1     Full/DR         00:00:32    GE0/0/0    0
2.2.2.2         1     Full/Backup     00:00:38    GE0/0/0    0
```

Если 1.1.1.1 в данный момент не является DR, для сброса процесса OSPFv3 можно выполнить следующую команду:

```
<R1>reset ospfv3 1 graceful-restart
```

Проверьте подключение к локальному адресу однорангового канала и глобальному адресу одноадресной передачи интерфейса LoopBack 0.

```
<R1>ping ipv6 fe80::3 -i GigabitEthernet 0/0/0
  PING fe80::3 : 56  data bytes, press CTRL_C to break
    Reply from FE80::3
    bytes=56 Sequence=1 hop limit=64  time = 2 ms
    Reply from FE80::3
    bytes=56 Sequence=2 hop limit=64  time = 2 ms
    Reply from FE80::3
    bytes=56 Sequence=3 hop limit=64  time = 11 ms
    Reply from FE80::3
    bytes=56 Sequence=4 hop limit=64  time = 2 ms
    Reply from FE80::3
    bytes=56 Sequence=5 hop limit=64  time = 2 ms
  --- fe80::3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/3/11 ms
<R1>ping ipv6 2001:3::C
  PING 2001:3::C : 56  data bytes, press CTRL_C to break
    Reply from 2001:3::C
    bytes=56 Sequence=1 hop limit=64  time = 11 ms
    Reply from 2001:3::C
    bytes=56 Sequence=2 hop limit=64  time = 6 ms
    Reply from 2001:3::C
    bytes=56 Sequence=3 hop limit=64  time = 2 ms
    Reply from 2001:3::C
    bytes=56 Sequence=4 hop limit=64  time = 2 ms
    Reply from 2001:3::C
    bytes=56 Sequence=5 hop limit=64  time = 6 ms

  --- 2001:3::C ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/5/11 ms
```

Шаг 4 Настройка DHCPv6 для распределения IPv6 адресов

Включите функцию DHCPv6 Server на R2, чтобы устройствам можно было назначать адреса IPv6 с помощью DHCPv6.

```
[R2]dhcp enable
[R2] dhcpv6 duid ll
Warning: The DHCP unique identifier should be globally-unique and stable. Are you sure to change it? [Y/N]y
[R2]dhcpv6 pool pool1
[R2-dhcpv6-pool-pool1]address prefix 2001:FACE::/64
[R2-dhcpv6-pool-pool1]dns-server 2001:444e:5300::1
[R2-dhcpv6-pool-pool1]excluded-address 2001:FACE::1
[R2-dhcpv6-pool-pool1]quit
```

Настройте функции IPv6 на интерфейсе GigabitEthernet 0/0/0.

Включите функцию DHCPv6-сервера на интерфейсе.

```
[R2]interface GigabitEthernet 0/0/0
```

```
[R2-GigabitEthernet0/0/0]ipv6 address 2001:FACE::1 64
[R2-GigabitEthernet0/0/0]dhcpv6 server pool1
```

Включите функцию клиента DHCPv6 на R1 и R3, чтобы устройствам можно было назначать адреса IPv6 с помощью DHCPv6.

```
[R1]dhcp enable
[R1] dhcpv6 duid ll
Warning: The DHCP unique identifier should be globally-unique and stable. Are you sure to change it? [Y/N]y
[R1]interface Gigabitethernet 0/0/0
[R1-GigabitEthernet0/0/0]ipv6 address auto dhcp

[R3]dhcp enable
[R3] dhcpv6 duid ll
Warning: The DHCP unique identifier should be globally-unique and stable. Are you sure to change it? [Y/N]y
[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]ipv6 address auto dhcp
```

Выполните команду **display dhcpv6 pool** на R2 для проверки информации о пуле адресов DHCPv6.

```
<R2>display dhcpv6 pool
DHCPv6 pool: pool1
  Address prefix: 2001:FACE::/64
    Lifetime valid 172800 seconds, preferred 86400 seconds
    2 in use, 0 conflicts
  Excluded-address 2001:FACE::1
  1 excluded addresses
  Information refresh time: 86400
  DNS server address: 2001:444E:5300::1
  Conflict-address expire-time: 172800
  Active normal clients: 2
```

Выполните команду **display ipv6 interface brief** на R1 и R3 для проверки информации об адресе IPv6.

```
[R1]display ipv6 interface brief
*down: administratively down
(l): loopback
(s): spoofing
Interface                  Physical        Protocol
GigabitEthernet0/0/0       up              up
[IPv6 Address] 2001:FACE::2
LoopBack0                  up              up(s)
[IPv6 Address] 2001:1::A

[R3]display ipv6 interface brief
*down: administratively down
(l): loopback
(s): spoofing
Interface                  Physical        Protocol
GigabitEthernet0/0/0       up              up
[IPv6 Address] 2001:FACE::3
LoopBack0                  up              up(s)
[IPv6 Address] 2001:3::C
```

Окончательная конфигурация

```
<R1>display current-configuration
[V200R007C00SPC600]
#
 sysname R1
#
ipv6
#
dhcp enable
#
ospfv3 1
 router-id 1.1.1.1
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ip address 10.0.13.1 255.255.255.0
 ipv6 address FE80::1 link-local
 ospfv3 1 area 0.0.0.0
 ipv6 address auto dhcp
#
interface LoopBack0
 ipv6 enable
 ip address 10.0.1.1 255.255.255.0
 ipv6 address 2001:1::A/64
 ospfv3 1 area 0.0.0.0
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$dD#}P<HzJ;Xs%X>hOkm!,.+Iq61QK`K6tI}cc-;k_o`C.+L,%$%$
user-interface vty 0 4
 authentication-mode aaa
#
return



<R2>display current-configuration
[V200R007C00SPC600]
#
 sysname R2
#
ipv6
#
dhcp enable
#
dhcpv6 pool pool1
 address prefix 2001:FACE::/64
 excluded-address 2001:FACE::1
 dns-server 2001:444E:5300::1
#
ospfv3 1
 router-id 2.2.2.2
#
interface GigabitEthernet0/0/0
```

```
 ipv6 enable
 ip address 10.0.13.2 255.255.255.0
 ipv6 address 2001:FACE::1/64
 ipv6 address FE80::2 link-local
 ospfv3 1 area 0.0.0.0
 traffic-filter inbound acl 3000
 dhcpv6 server pool1
#
interface LoopBack0
 ipv6 enable
 ip address 10.0.2.2 255.255.255.0
 ipv6 address 2001:2::B/64
 ospfv3 1 area 0.0.0.0
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$|nRPL^hr2IXi7LHDID!/,.*%.8%h;3:,hXO2dk#ikaWI.*(,%$%$
user-interface vty 0 4
#
return



<R3>display current-configuration
[V200R007C00SPC600]
#
 sysname R3
#
ipv6
#
dhcp enable
#
ospfv3 1
 router-id 3.3.3.3
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ip address 10.0.13.3 255.255.255.0
 ipv6 address FE80::3 link-local
 ospfv3 1 area 0.0.0.0
 ipv6 address auto dhcp
#
interface LoopBack0
 ipv6 enable
 ip address 10.0.3.3 255.255.255.0
 ipv6 address 2001:3::C/64
 ospfv3 1 area 0.0.0.0
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$W|$)M5D}v@bY^gK\;>QR,.*d;8Mp>|+EU,:~D~8b59~..*g,%$%$
user-interface vty 0 4
 authentication-mode aaa
#
```

```
return
```