

Условные обозначения



Маршрутизатор



L3 Коммутатор



L2 Коммутатор



Облако



Ethernet канал



Последовательная связь

Спецификация лабораторной работы

Чтобы гарантировать, что конфигурация, данная в этой лабораторной работе, поддерживается на всех устройствах, рекомендуется использовать следующие модели устройств и версии VRP:

Identifier	Device Model	VRP version
R1	AR 2220E	Version 5.160 (AR2200 V200R007C00SPC600)
R2	AR 2220E	Version 5.160 (AR2200 V200R007C00SPC600)
R3	AR 2220E	Version 5.160 (AR2200 V200R007C00SPC600)
S1	S5720-36C-EI-AC	Version 5.160 (S5720 V200R008C00SPC500)
S2	S5720-36C-EI-AC	Version 5.160 (S5720 V200R008C00SPC500)
S3	S3700-28TP-EI-AC	Version 5.70 (S3700 V100R006C05)
S4	S3700-28TP-EI-AC	Version 5.70 (S3700 V100R006C05)

Содержание

МОДУЛЬ 1 Ethernet И VLAN	1
LAB 1-1 Интерфейс Ethernet и конфигурация ссылок.....	1
LAB 1-2 VLAN конфигурация.....	11
LAB 1-3 GVRP конфигурация.....	21
LAB 1-4 VLAN маршрутизация.....	33
LAB 1-5 Конфигурация 3 уровня коммутации.....	41
MODULE 2 Конфигурация WAN предприятия.....	55
LAB 2-1 Конфигурация HDLC и PPP	55
LAB 2-2 Настройка Frame Relay на границе клиента	72
LAB 2-3 Установка клиентской сессии PPPoE.....	93
MODULE 3 Реализация IP-безопасности	102
LAB 3-1 Фильтрация корпоративных данных с помощью списков управления доступом.....	102
LAB 3-2 Перевод сетевых адресов	113
LAB 3-3 Создание локальных решений AAA.....	124
LAB 3-4 Защита трафика с помощью IPsec VPN.....	133
LAB 3-5 Поддержка динамической маршрутизации с помощью GRE	146
MODULE 4 Создание сетей IPv6.....	157
LAB 4-1 Внедрение сетей и решений IPv6	157

Module 1 Ethernet и VLAN

Lab 1-1 Интерфейс Ethernet и конфигурация ссылок

Цели обучения

В результате этой лабораторной вы должны выполнить следующие задачи:

- Вручную установите скорость линии на интерфейсе.
- Конфигурация агрегации ссылок в ручном режиме.
- Конфигурация агрегации ссылок с использованием статического режима LACP.
- Управление приоритетом интерфейсов в статическом режиме LACP.

Топология

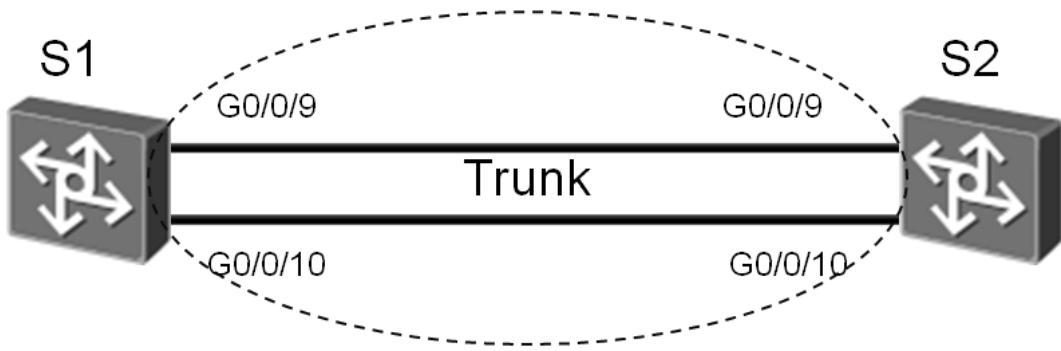


Рисунок 1.1 топология агрегации Ethernet-ссылок

Сценарий

В качестве сетевого администратора существующей сети предприятия было предложено более эффективно использовать соединения между коммутаторами, подготовив коммутаторы для поддержки агрегации ссылок до создания агрегации ручного соединения, для которой среда между коммутаторами должна быть сконфигурирована как ссылки участника.

Задачи

Шаг 1 Выполнение базовой настройки коммутаторов Ethernet

Автоматическое согласование включено на интерфейсах коммутатора Huawei по умолчанию. Скорость G0/0/9 и G 0/0/10 на S1 и S2 устанавливаются 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%

```

Установите скорость для G0/0/9 и G0/0/10 на S1 до 100 Мб/с. Перед тем как установить скорость 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

```

Установите скорость G0/0/9 и G0/0/10 на S2 до 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

```

Подтвердите, что скорость G0/0/9 и G0/0/10 установлены на 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 14:29:45
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 ссылок вручную

Создайте Eth-Trunk 1 на S1 и S2. Удалите конфигурацию по умолчанию из G0/0/9 и G0/0/10 на S1 и S2, и далее добавьте G0/0/9 и G0/0/10 для 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
```

Серые линии в приведенной выше информации указывают на то, что Eth-Trunk работает правильно.

Шаг 3 Настройка агрегации ссылок в статическом режиме LACP

Удалите конфигурации из 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 для Eth-Trunk в статистическом режиме 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
```

Проверьте, что статический режим LACP был включен на этих двух ссылках.

```
[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 до 100

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

Установите приоритет интерфейса и определите активные ссылки 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
```

Lab 1-2 Конфигурация VLAN

Цели обучения

В результате этой лабораторной вы должны выполнить следующие задачи:

- Назначить интерфейсы: сделать access и второй trunk порты
- Создание VLAN.
- Настройте VLAN-Теги по портам, используя тип связи гибридного порта.
- Настройте VLAN по умолчанию для интерфейса с помощью идентификатора порта VLAN.

Топология

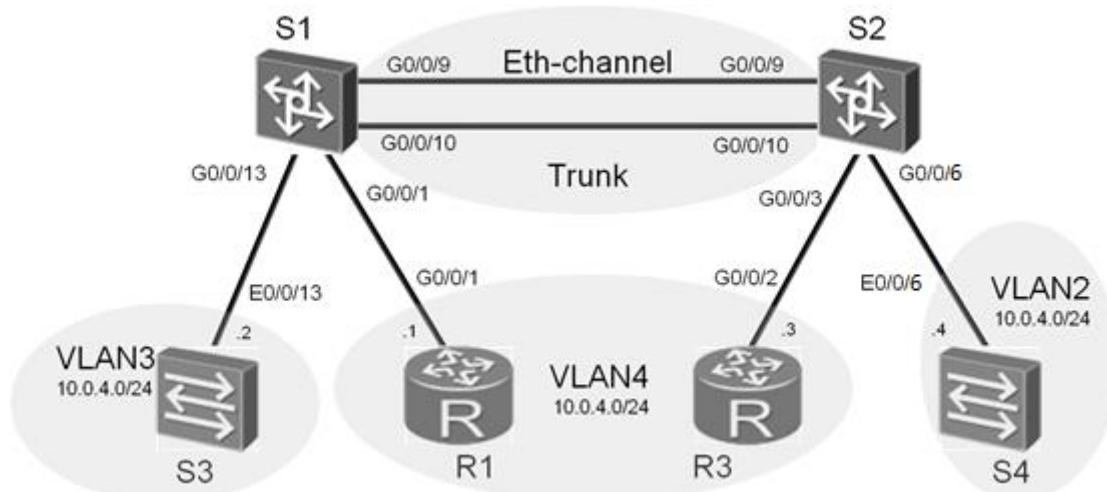


Рисунок 1.2 топология VLAN

Сценарий

Сеть предприятия в настоящее время работает в одном широковещательном домене, что приводит к тому, что большой объем трафика заливается во все сетевые узлы. Требуется, чтобы администратор попытался контролировать поток трафика на уровне канала, внедряя решения VLAN. Решения VLAN должны применяться к коммутаторам S1 и S2.

Задачи

Шаг 1 Подготовка среды

Если вы начинаете этот раздел с не настроенного устройства, начните здесь, а затем перейдите к шагу 2. Для тех, кто продолжает работать в предыдущих лабораториях, начните с шага 2.

Установите связь 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, используя представление 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 Отключите неиспользуемые интерфейсы и установите VLAN trunk

Неиспользуемые интерфейсы должны быть отключены для обеспечения точности результатов теста. В этой лабораторной интерфейсы Ethernet 0/0/1 и Ethernet 0/0/7 на S3, Ethernet0/0/1 и Ethernet0/0/14 на S4 необходимо закрыть.

```
<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
```

Тип ссылки интерфейса порта коммутатора по умолчанию является гибридным. Настройте тип соединения порта для Eth-Trunk 1, чтобы создать порт соединительной линии. Кроме того, разрешить использование всех VLANs по порту соединительной линии.

```
[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 **Настройка Vlan**

Используйте S3, R1, R3 и S4 как хосты, не поддерживающие VLAN. Существует два способа со-зования VLANs (виртуальных локальных сетей), а для демонстрации этих двух методов используются два метода привязки интерфейсов к созданным VLAN, S1 и S2. Все интерфейсы, связанные с хостами, должны быть настроены как порты доступа.

На S1, связать интерфейс Gigabit Ethernet 0/0/13 с VLAN 3, и интерфейса Gigabit Ethernet 0/0/1 с VLAN 4.

На S2 связать интерфейс Gigabit Ethernet 0/0/3 с VLAN 4 и 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

```

Проверьте, что конфигурация VLAN была 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     TG:Eth-Trunk1 (U)

4  common     UT:GE0/0/3 (U)
               TG:Eth-Trunk1 (U)

...output omitted...

```

Выделенные записи подтверждают привязку интерфейсов к каждой созданной VLAN. Все VLAN разрешены по trunk порту (TG) Eth-Trunk 1.

Шаг 4 Настройте IP-адресацию для каждой VLAN

Настройте IP-адреса на хостах, R1, S3, R3 и S4 как часть соответствующих VLAN. Интерфейсы физических портов на коммутаторах не могут быть настроены с IP-адресами, 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 Проверьте конфигурацию, проверив подключение

Используйте команду **ping**. R1 и R3 в VLAN 4 должны быть способны связываться друг с другом. Устройства в других VLAN должны быть недоступны для связи.

```
[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

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

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

Шаг 6 Настройка гибридного интерфейса

Используйте тип соединения с гибридным портом, чтобы можно было управлять тегами VLAN на уровне интерфейса порта. Мы будем использовать гибридные порты, чтобы разрешить помеченому блоку данных из VLAN 4 принимать VLAN 2 и наоборот.

Установите тип соединения интерфейса Gigabit Ethernet 0/0/1 для порта S1, Gigabit Ethernet 0/0/3 и 0/0/6 для S2 в качестве гибридных портов. Кроме того, установите гибридные порты для отключения всех данных, связанных с VLAN 2 и 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
```

Команда **port hybrid pvid vlan** гарантирует, что фреймы, полученные от хоста, помечены соответствующим тегом VLAN. Фреймы, полученные от VLAN 2 или 4, будут немаркированы на интерфейсе перед пересылкой на хост.

Используйте команду ping, чтобы убедиться, 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 S4 в VLAN 2 и так же доступен ли 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 с гибридным портом данные, исходящие из VLAN 4, теперь могут быть приняты VLAN 2 и наоборот, а также не могут достичь адреса узла 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
```

Lab 1-3 Конфигурация GVRP

Цели обучения

В результате этой лабораторной вы должны выполнить следующие задачи:

- Конфигурация GVRP.
- Настройка режима регистрации GVRP.

Топология

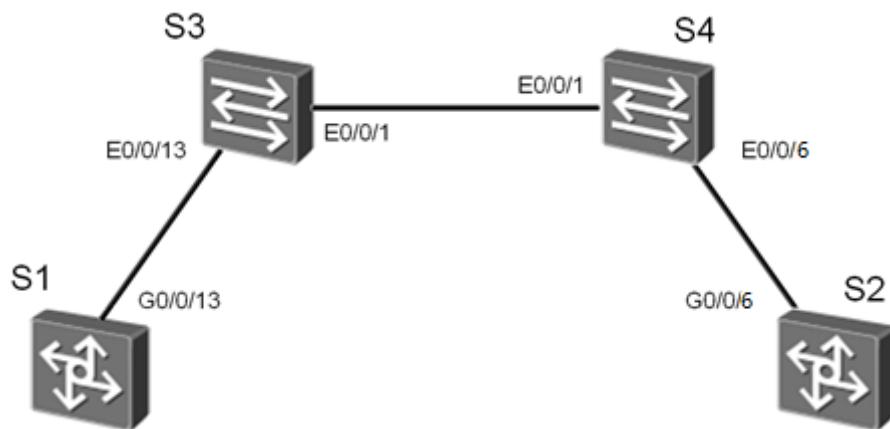


Рисунок 1.3 топология GVRP

Сценарий

Сеть предприятия содержит несколько коммутаторов, которые, как ожидается, будут регулярно управляться. VLAN должны применяться и удаляться по мере необходимости на всех коммутаторах, однако это, как правило, трудоемкая задача для администратора, и часто ошибки конфигурации возникают из-за человеческой ошибки. Администратор хочет упростить процесс управления VLAN и попросил включить GVRP на всех коммутаторах и установить режим регистрации на интерфейсах.

Задачи

Шаг 1 Подготовка среды

Если вы начинаете этот раздел с не настроенного устройства, начните здесь, а за-тем перейдите к шагу 3. Для тех, кто продолжает работать в предыдущих лабора-ториях, начните с шага 2.

```
<Quidway>system-view  
[Quidway]sysname S1  
[S1]interface GigabitEthernet 0/0/9  
[S1-GigabitEthernet0/0/9]shutdown  
[S1-GigabitEthernet0/0/9]quit  
[S1]interface GigabitEthernet 0/0/10  
[S1-GigabitEthernet0/0/10]shutdown
```

```
<Quidway>system-view  
[Quidway]sysname S2  
[S2]interface GigabitEthernet 0/0/9  
[S2-GigabitEthernet0/0/9]shutdown  
[S2-GigabitEthernet0/0/9]quit  
[S2]interface GigabitEthernet 0/0/10  
[S2-GigabitEthernet0/0/10]shutdown
```

```
<Quidway>system-view  
[Quidway]sysname S3  
[S3-Ethernet0/0/7]shutdown
```

```
<Quidway>system-view  
[Quidway]sysname S4  
[S4-Ethernet0/0/14]shutdown
```

Шаг 2 Удаление предыдущей конфигурации

Удалите неиспользуемые VLAN и отключите интерфейс Eth-Trunk на S1 и S2. Удалите VLAN 1 на S3 и S4 и вызовите интерфейс Ethernet 0/0/1 на S3.

```
[S1]undo vlan batch 2 to 4  
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 Eth-Trunk 1  
[S1-Eth-Trunk1]shutdown
```

```

[S2]undo vlan batch 2 to 4
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 Eth-Trunk 1
[S2-Eth-Trunk1]shutdown
[S2-Eth-Trunk1]quit
[S2]interface GigabitEthernet 0/0/6
[S2-GigabitEthernet0/0/6]undo port hybrid vlan 2 4

[S3]interface Ethernet 0/0/1
[S3-Ethernet0/0/1]undo shutdown
[S3-Ethernet0/0/1]quit
[S3]undo interface Vlanif 1
Info: This operation may take a few seconds. Please wait for a moment...succeeded.

[S4]interface Ethernet 0/0/1
[S4-Ethernet0/0/1]undo shutdown
[S4-Ethernet0/0/1]quit
[S4]undo interface Vlanif 1
Info: This operation may take a few seconds. Please wait for a moment...succeeded.

```

Шаг 3 Настройте trunk каналы между коммутаторами

```

[S1]interface GigabitEthernet 0/0/13
[S1-Gigabitethernet0/0/13]port link-type trunk
[S1-Gigabitethernet0/0/13]port trunk allow-pass vlan all

[S3]interface Ethernet 0/0/13
[S3-Ethernet0/0/13]port link-type trunk
[S3-Ethernet0/0/13]port trunk allow-pass vlan all
[S3-Ethernet0/0/13]quit
[S3]interface Ethernet 0/0/1
[S3-Ethernet0/0/1]port link-type trunk
[S3-Ethernet0/0/1]port trunk allow-pass vlan all

[S2]interface GigabitEthernet 0/0/6
[S2-Gigabitethernet0/0/6]port link-type trunk
Warning: This command will delete VLANs on this port. Continue?[Y/N]:y
[S2-Gigabitethernet0/0/6]port trunk allow-pass vlan all

[S4]interface Ethernet 0/0/6
[S4-Ethernet0/0/6]port link-type trunk

```

```
[S4-Ethernet0/0/6]port trunk allow-pass vlan all  
[S4-Ethernet0/0/6]quit  
[S4]interface Ethernet 0/0/1  
[S4-Ethernet0/0/1]port link-type trunk  
[S4-Ethernet0/0/1]port trunk allow-pass vlan all
```

Шаг 4 Включить GVRP на всех соответствующих интерфейсах

```
[S1]vcmp role silent  
[S1]gvrp  
[S1]interface GigabitEthernet 0/0/13  
[S1-GigabitEthernet0/0/13]gvrp
```

```
[S3]gvrp  
[S3]interface Ethernet 0/0/13  
[S3-Ethernet0/0/13]gvrp  
[S3-Ethernet0/0/13]quit  
[S3]interface Ethernet 0/0/1  
[S3-Ethernet0/0/1]gvrp
```

```
[S2]vcmp role silent  
[S2]gvrp  
[S2]interface GigabitEthernet 0/0/6  
[S2-Gigabitethernet0/0/6]gvrp
```

```
[S4]gvrp  
[S4]interface Ethernet0/0/6  
[S4-Ethernet0/0/6]gvrp  
[S4-Ethernet0/0/6]quit  
[S4]interface Ethernet 0/0/1  
[S4-Ethernet0/0/1]gvrp
```

Создайте VLAN 100 на S1, VLAN 200 на S2 и VLAN 2 на S1, S2, S3 и S4.

```
[S1]vlan batch 2 100  
[S2]vlan batch 2 200  
[S3]vlan 2  
[S4]vlan 2
```

Выполните команду **display gvrp statistics** на S3 и S4 для просмотра статистики GVRP.

```
[S3]display gvrp statistics  
GVRP statistics on port Ethernet0/0/1  
GVRP status : Enabled
```

```

GVRP registrations failed      : 0
GVRP last PDU origin         : e028-6120-36f0
GVRP registration type       : Normal
GVRP statistics on port Ethernet0/0/13
GVRP status                  : Enabled
GVRP registrations failed    : 0
GVRP last PDU origin         : d0d0-4ba6-aab0
GVRP registration type       : Normal

```

```

[S4]display gvrp statistics
GVRP statistics on port Ethernet0/0/1
GVRP status                  : Enabled
GVRP registrations failed    : 0
GVRP last PDU origin         : e028-6120-3660
GVRP registration type       : Normal
GVRP statistics on port Ethernet0/0/6
GVRP status                  : Enabled
GVRP registrations failed    : 0
GVRP last PDU origin         : d0d0-4ba6-ac20
GVRP registration type       : Normal

```

Тип регистрации устанавливается как обычно по умолчанию. Используйте команду **display vlan для проверки конфигурации VLAN на S3 и S4.**

```

[S3]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:Eth0/0/1(U)  Eth0/0/2(D)      Eth0/0/3(D)      Eth0/0/4(D)
                           Eth0/0/5(D)      Eth0/0/6(D)      Eth0/0/7(D)      Eth0/0/8(D)
                           Eth0/0/9(D)      Eth0/0/10(D)     Eth0/0/11(D)     Eth0/0/12(D)
                           Eth0/0/13(U)     Eth0/0/14(D)     Eth0/0/15(D)     Eth0/0/16(D)
                           Eth0/0/17(D)     Eth0/0/18(D)     Eth0/0/19(D)     Eth0/0/20(D)
                           Eth0/0/21(D)     Eth0/0/22(D)     Eth0/0/23(D)     Eth0/0/24(D)
                           GE0/0/1(D)      GE0/0/2(D)      GE0/0/3(D)      GE0/0/4(D)
2  common   TG:Eth0/0/1(U)  Eth0/0/13(U)
100 dynamic TG:Eth0/0/13(U)

```

```
200 dynamic TG:Eth0/0/1 (U)
```

...output omitted...

```
[S4]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:Eth0/0/1 (U)	Eth0/0/2 (D)	Eth0/0/3 (D)	Eth0/0/4 (D)
		Eth0/0/5 (D)	Eth0/0/7 (D)	Eth0/0/8 (D)	Eth0/0/9 (D)
		Eth0/0/10 (D)	Eth0/0/11 (D)	Eth0/0/12 (D)	Eth0/0/13 (D)
		Eth0/0/14 (D)	Eth0/0/15 (D)	Eth0/0/16 (D)	Eth0/0/17 (D)
		Eth0/0/18 (D)	Eth0/0/19 (D)	Eth0/0/20 (D)	Eth0/0/21 (D)
		Eth0/0/22 (D)	Eth0/0/23 (D)	Eth0/0/24 (D)	GE0/0/1 (D)
		GE0/0/2 (D)	GE0/0/3 (D)	GE0/0/4 (D)	

```
2 common TG:Eth0/0/1 (U) Eth0/0/6 (U)
```

```
100 dynamic TG:Eth0/0/1 (U)
```

```
200 dynamic TG:Eth0/0/6 (U)
```

...output omitted...

S3 и S4 изучают VLAN 100 и VLAN 200 динамично, но только в одном направлении. VLAN 2 была статически определена. Создайте VLAN 200 на S1 и VLAN 100 на S2 для включения двухстороннего распространения.

```
[S1]vlan 200
```

```
[S2]vlan 100
```

Запустите команду **display vlan для проверки конфигурации.**

```
[S3]display vlan
```

...output omitted...

```
VID Type Ports
```

1	common	UT:Eth0/0/1 (U)	Eth0/0/2 (D)	Eth0/0/3 (D)	Eth0/0/4 (D)
		Eth0/0/5 (D)	Eth0/0/6 (D)	Eth0/0/7 (D)	Eth0/0/8 (D)
		Eth0/0/9 (D)	Eth0/0/10 (D)	Eth0/0/11 (D)	Eth0/0/12 (D)
		Eth0/0/13 (U)	Eth0/0/14 (D)	Eth0/0/15 (D)	Eth0/0/16 (D)
		Eth0/0/17 (D)	Eth0/0/18 (D)	Eth0/0/19 (D)	Eth0/0/20 (D)
		Eth0/0/21 (D)	Eth0/0/22 (D)	Eth0/0/23 (D)	Eth0/0/24 (D)
		GE0/0/1 (D)	GE0/0/2 (D)	GE0/0/3 (D)	GE0/0/4 (D)

```

2 common TG:Eth0/0/1(U) Eth0/0/13(U)
100 dynamic TG:Eth0/0/1(U) Eth0/0/13(U)
200 dynamic TG:Eth0/0/1(U) Eth0/0/13(U)
...output omitted...

[S4]display vlan
...output omitted...
VID Type Ports
-----
1 common UT:Eth0/0/1(U) Eth0/0/2(D) Eth0/0/3(D) Eth0/0/4(D)
          Eth0/0/5(D) Eth0/0/7(D) Eth0/0/8(D) Eth0/0/9(D)
          Eth0/0/11(D) Eth0/0/12(D) Eth0/0/10(D) Eth0/0/13(D)
          Eth0/0/14(D) Eth0/0/15(D) Eth0/0/16(D) Eth0/0/17(D)
          Eth0/0/18(D) Eth0/0/19(D) Eth0/0/20(D) Eth0/0/21(D)
          Eth0/0/22(D) Eth0/0/23(D) Eth0/0/24(U) GE0/0/1(D)
          GE0/0/2(D) GE0/0/3(D) GE0/0/4(D)

2 common TG:Eth0/0/1(U) Eth0/0/6(U)
100 dynamic TG:Eth0/0/1(U) Eth0/0/6(U)
200 dynamic TG:Eth0/0/1(U) Eth0/0/6(U)
...output omitted...

```

Выделенные записи указывают интерфейсы, которые были добавлены в VLAN100 и VLAN200 на обоих S3 и S4.

Шаг 5 Изменение типа регистрации для интерфейсов

Изменение типа регистрации для Ethernet 0/0/1 на S3 к фиксированному. Те же действия выполнить для Ethernet 0/0/1 на S4.

```
[S3]interface Ethernet 0/0/1
[S3-Ethernet0/0/1]gvrp registration fixed
```

Запустить команду **display gvrp statistics** на S3 и S4 для того, чтобы увидеть изменения.

```
[S3]display gvrp statistics interface Ethernet 0/0/1
GVRP statistics on port Ethernet0/0/1
  GVRP status : Enabled
  GVRP registrations failed : 11
  GVRP last PDU origin : e028-6120-36f0
  GVRP registration type : Fixed
```

Тип регистрации GVRP проверяется как фиксированный на интерфейсе Ethernet 0/0/1. Динамическим VLAN не разрешается регистрироваться на этом интерфейсе.

Выполните команду **display vlan** для просмотра эффекта фиксированного типа регистрации.

```
[S3]display vlan  
...output omitted...  
VID Type Ports  
-----1 common  
    UT:Eth0/0/1(U) Eth0/0/2(D)     Eth0/0/3(D)     Eth0/0/4(D)  
        Eth0/0/5(D)   Eth0/0/6(D)     Eth0/0/7(D)     Eth0/0/8(D)  
        Eth0/0/9(D)   Eth0/0/10(D)    Eth0/0/11(D)    Eth0/0/12(D)  
        Eth0/0/13(U)  Eth0/0/14(D)    Eth0/0/15(D)    Eth0/0/16(D)  
        Eth0/0/17(D)  Eth0/0/18(D)    Eth0/0/19(D)    Eth0/0/20(D)  
        Eth0/0/21(D)  Eth0/0/22(D)    Eth0/0/23(D)    Eth0/0/24(D)  
        GE0/0/1(D)    GE0/0/2(D)     GE0/0/3(D)     GE0/0/4(D)  
2    common  TG:Eth0/0/1(U)  Eth0/0/13(U)  
100 dynamic TG:Eth0/0/13(U)  
200 dynamic TG:Eth0/0/13(U)  
...output omit...
```

Выделенные записи показывают, что интерфейс Ethernet 0/0/1 не регистрирует динамиче-ские VLAN 100 и 200.

Настройте интерфейс Ethernet 0/0/1 на S3, чтобы использовать запрещенный тип регистрации. Те же действия выполните для Ethernet 0/0/1 на S4.

```
[S3]interface Ethernet 0/0/1  
[S3-Ethernet0/0/1]gvrp registration forbidden  
  
[S4]interface Ethernet 0/0/1  
[S4-Ethernet0/0/1]gvrp registration forbidden
```

Запустите команду **display gvrp statistics** для того, чтобы увидеть изменения на GVRP.

```
[S3]display gvrp statistics interface Ethernet 0/0/1  
GVRP statistics on port Ethernet0/0/1  
  GVRP status           : Enabled  
  GVRP registrations failed : 18  
  GVRP last PDU origin   : 5489-98ec-f012  
  GVRP registration type : Forbidden
```

Тип регистрации GVRP запрещен на интерфейсе Ethernet 0/0/1.

Запустить команду **display vlan** для того, чтобы просмотреть эффект запрещенной регистрации.

```
[S3]display vlan  
The total number of vlans is : 4  
...output omitted...  
VID Type Ports  
1 common UT:Eth0/0/1 (U)---Eth0/0/2 (D)---Eth0/0/3 (D)---Eth0/0/4 (D)---  
    Eth0/0/5 (D)    Eth0/0/6 (D)    Eth0/0/7 (D)    Eth0/0/8 (D)  
    Eth0/0/9 (D)    Eth0/0/10 (D)   Eth0/0/11 (D)   Eth0/0/12 (D)  
    Eth0/0/13 (U)   Eth0/0/14 (D)   Eth0/0/15 (D)   Eth0/0/16 (D)  
    Eth0/0/17 (D)   Eth0/0/18 (D)   Eth0/0/19 (D)   Eth0/0/20 (D)  
    Eth0/0/21 (D)   Eth0/0/22 (D)   Eth0/0/23 (D)   Eth0/0/24 (D)  
    GE0/0/1 (D)     GE0/0/2 (D)     GE0/0/3 (D)     GE0/0/4 (D)  
2  common TG:Eth0/0/13 (U)  
100 dynamic TG:Eth0/0/13 (U)  
200 dynamic TG:Eth0/0/13 (U)
```

Запрещенный режим позволяет только VLAN1 проходить через интерфейс Ethernet 0/0/1, все остальные VLANS ограничены.

Финальная конфигурация

```
[S1]display current-configuration  
#  
!Software Version V200R008C00SPC500  
sysname S1  
#  
vcmp role silent  
#  
vlan batch 2 100 200  
#  
gvrp  
#  
interface GigabitEthernet0/0/9  
shutdown  
#  
interface GigabitEthernet0/0/10  
shutdown  
#  
interface GigabitEthernet0/0/13  
port link-type trunk
```

```
port trunk allow-pass vlan 2 to 4094
gvrp
#
return

[S2]display current-configuration
#
!Software Version V200R008C00SPC500
sysname S2
#
vcmp role silent
vlan batch 2 100 200
#
gvrp
#
interface GigabitEthernet0/0/6
port link-type trunk
port trunk allow-pass vlan 2 to 4094
gvrp
#
interface GigabitEthernet0/0/9
shutdown
#
interface GigabitEthernet0/0/10
shutdown
#
return

[S3]display current-configuration
#
!Software Version V100R006C05
sysname S3
#
vlan batch 2
#
gvrp
#interface Ethernet0/0/1
port link-type trunk
port trunk allow-pass vlan 2 to 4094
gvrp
gvrp registration forbidden
#
```

```
interface Ethernet0/0/7
shutdown
#
interface Ethernet0/0/13
port link-type trunk
port trunk allow-pass vlan 2 to 4094
gvrp
#
return

[S4]display current-configuration
#
!Software Version V100R006C05
sysname S4
#
vlan batch 2
#
gvrp
#
interface Ethernet0/0/1
port link-type trunk
port trunk allow-pass vlan 2 to 4094
gvrp
gvrp registration forbidden
#
interface Ethernet0/0/6
port link-type trunk
port trunk allow-pass vlan 2 to 4094
gvrp
#
interface Ethernet0/0/14
shutdown
#
return
```

Lab 1-4 Маршрутизация VLAN

Цель работы

В результате этой лабораторной вы должны выполнить следующие задачи:

- Создание trunk интерфейса для маршрутизации VLAN.
- Настройка подинтерфейсов на одном физическом интерфейсе.
- Включение сообщений ARP для трансляции между VLANs.

Топология

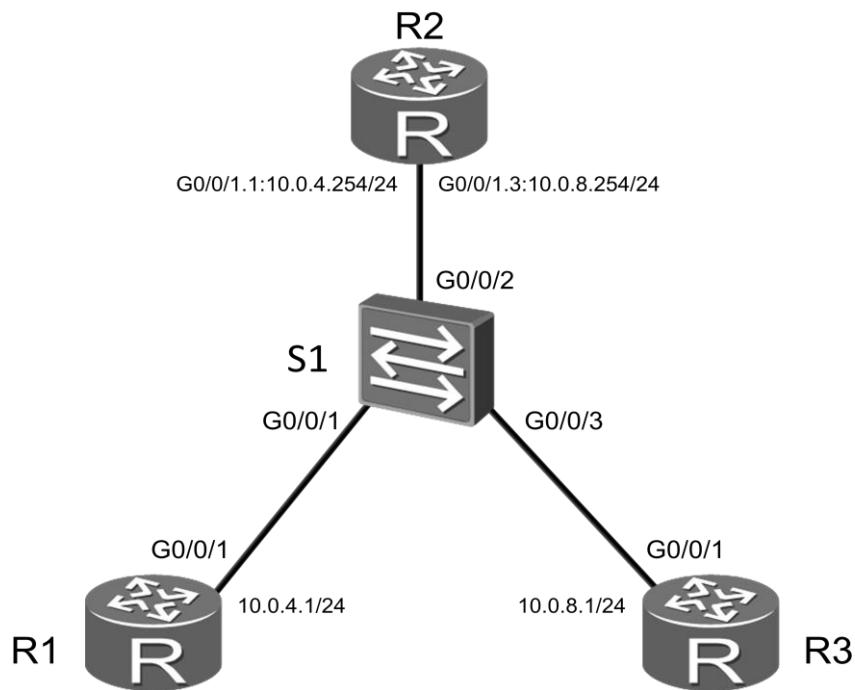


Рисунок 1.4 топология маршрутизации VLAN с помощью коммутатора уровня 2.

Сценарий

Реализация VLAN в корпоративной сети привела к тому, что группы пользователей

были изолированы от других пользователей, которые являются частью разных подсетей. В качестве сетевого администратора вам была предоставлена задача обеспечения того, чтобы домены широковещательной передачи поддерживались и в то же время обеспечивая связь между рассоединенными пользователями.

Задачи

Шаг 1 Подготовка среды

Если вы начинаете этот раздел с не настроенного устройства, начинайте здесь, а затем переходите к шагу 3. Для тех, кто продолжает работать в предыдущих лабораториях, начинайте с шага 2.

Настройте название системы для R1, R3 и S1. Настройте IP-адрес 10.0.4.1/24 на интерфейс 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 Очистка предыдущей конфигурации

Удалите IP-адрес 10.0.4.3 из R3 и отключите интерфейсы коммутатора между S1 и S3 и S2 и S4 соответственно.

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

```
[S1]undo gvrp  
Warning: All information about the GVRP will be deleted . Continue?[Y/N]:y  
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```

[S1]interface GigabitEthernet 0/0/13
[S1-GigabitEthernet0/0/13]undo port trunk allow-pass vlan 2 to 4094
[S1-GigabitEthernet0/0/13]shutdown
[S1-GigabitEthernet0/0/13]quit
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]undo port hybrid vlan 2 4
[S1-GigabitEthernet0/0/1]quit
[S1]undo vlan batch 2 100 200
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]undo gvrp
Warning: All information about the GVRP will be deleted . Continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment...done.
[S2]interface GigabitEthernet 0/0/6
[S2-GigabitEthernet0/0/6]undo port trunk allow-pass vlan 2 to 4094
[S2-GigabitEthernet0/0/6]shutdown
[S2-GigabitEthernet0/0/6]quit
[S2]interface GigabitEthernet 0/0/3
[S2-GigabitEthernet0/0/3]undo port hybrid vlan 2 4
[S2-GigabitEthernet0/0/3]quit
[S2]undo vlan batch 2 100 200
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.

[S3]undo gvrp
Warning: All information about the GVRP will be deleted . Continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment...done.
[S3]interface Ethernet 0/0/13
[S3-Ethernet0/0/13]undo port trunk allow-pass vlan 2 to 4094
[S3-Ethernet0/0/13]port link-type hybrid
[S3-Ethernet0/0/13]quit
[S3]interface Ethernet 0/0/1
[S3-Ethernet0/0/1]undo port trunk allow-pass vlan 2 to 4094
[S3-Ethernet0/0/1]quit
[S3]undo vlan 2

[S4]undo gvrp
Warning: All information about the GVRP will be deleted . Continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment...done.
[S4]interface Ethernet 0/0/6
[S4-Ethernet0/0/6]undo port trunk allow-pass vlan 2 to 4094

```

```
[S4-Ethernet0/0/6]port link-type hybrid  
[S4-Ethernet0/0/6]quit  
[S4]interface Ethernet 0/0/1  
[S4-Ethernet0/0/1]undo port trunk allow-pass vlan 2 to 4094  
[S4-Ethernet0/0/1]quit  
[S4]undo vlan 2
```

Шаг 3 Настройка IP-адреса для R3

Настройка IP-адреса в сетевом диапазоне 10.0.8.0/24 на интерфейсе R1 Gigabit Ethet-net 0/0/1

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

Шаг 4 Установка сетей VLAN

Создайте VLAN 4 и 8 на S1, настройте интерфейс Gigabit Ethernet 0/0/1, который должен принадлежать VLAN 4, а интерфейс Gigabit Ethernet 0/0/3 должен принадлежать 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
```

Установите интерфейс Gigabit Ethernet 0/0/2 в качестве соединительной линии для VLAN 4 и 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 5 Настройте маршрутизацию VLAN через подинтерфейс R2

Настройте под-интерфейсы GigabitEthernet0 / 0 / 1.1 и GigabitEthernet0 / 0 / 1.3, чтобы действовать как шлюз VLAN 4 и действовать как шлюз 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 соединение 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

--- 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
```

Проверьте соединение между R1 и R3 снова.

```
<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

```

Финальная 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
```

Lab 1-5 Настройка коммутации уровня 3

Цель работы

В результате этой лабораторной вы должны выполнить следующие задачи:

- Конфигурация интерфейсов VLAN.
- Установление маршрутизации VLAN на одном коммутаторе
- Выполните маршрутизацию VLAN по каналу Ethernet Trunk.
- Выполните динамическую маршрутизацию между интерфейсами VLAN с использованием OSPF.

Топология

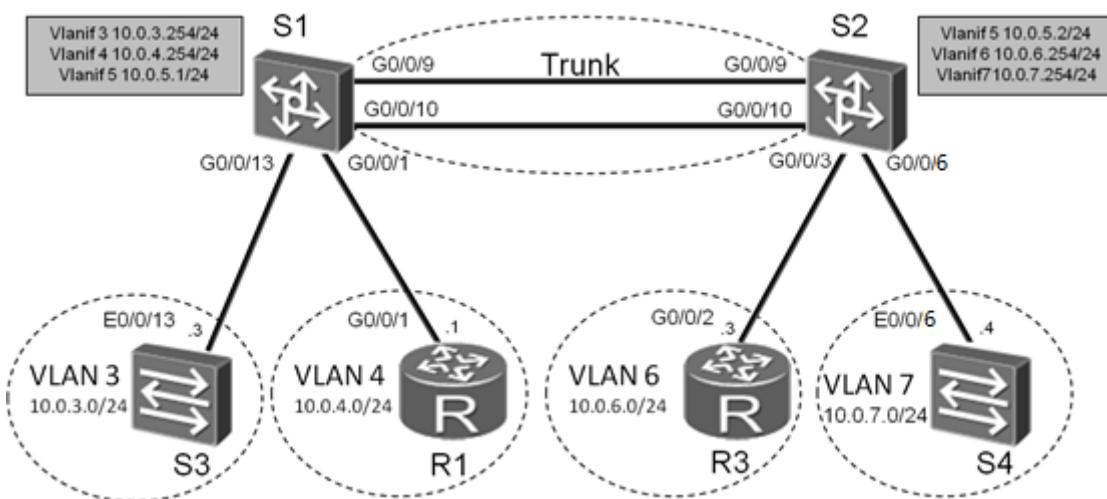


Рисунок 1.5 топология коммутации уровня 3

Сценарий

Внедрение коммутаторов 3 уровня в сеть дало возможности для оптимизации текущей конфигурации маршрутизации VLAN. Администратору сети была поручена реализация маршрутизации VLAN с использованием только переключателей 3 уровня для поддержки связи между VLAN в сети, отображаемой в схеме. Сети VLAN должны иметь возможность взаимодействия между VLAN. Кроме того, ожидается, что S1 и S2 будут

взаимодействовать через 3 уровня , для которого требуется поддержка протокола маршрутизации.

Задачи

Шаг 1 Подготовка среды

Если вы начинаете этот раздел с не настроенного устройства, начинайте здесь, а затем переходите к шагу 3. Для тех, кто продолжает работать в предыдущих лабораториях, начинайте с шага 2.

Настройте R1 с адресом 10.0.4.1/24 на интерфейсе Gigabit Ethernet 0/0/1. Установите Eth-Trunk под 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 Ethernet 0/0/7  
[S3-Ethernet0/0/7]shutdown
```

```
<Quidway>system-view  
[Quidway]sysname S4  
[S4]interface Ethernet 0/0/14  
[S4-Ethernet0/0/14]shutdown
```

Шаг 2 **Очистка предыдущей конфигурации**

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
```

Повторно включите интерфейс Eth-Trunk между S1 и S2

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

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

Шаг 3 Configure VLAN 3 through to VLAN 7 for S1 and 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.
```

Проверьте, что VLAN были 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 Установите ссылку Eth-Trunk между S1 и S2 с PVID 5

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

Запустите 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 могут быть назначены Vlanif, где Vlanif1 является общим (немаркированным) Vlanif. Интерфейсы Ethernet 0/0/13 S3 и Ethernet 0/0/6 S4 должны быть связаны с общей VLAN1. R1 уже должен быть настроен с адресом 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 соединения между VLAN 3 и VLAN 4

Проверьте соединение между VLAN 3 и VLAN 4

```
<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 соединение 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  
  
--- 10.0.6.3 ping statistics ---  
5 packet(s) transmitted  
0 packet(s) received  
100.00% packet loss
```

Сбой подключения между R1 и R3. Используйте команду **tracert** для устранения неисправности:

```
[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 выходным данным команды, R1 отправил пакеты данных на адрес назначения 10.0.6.3, но шлюз в 10.0.4.254 отвечает, что сеть недоступна.

Проверьте, недоступна 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        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
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
```

Согласно выходному сигналу команды S1 не имеет маршрута к сегменту сети 10.0.6.0, поскольку сегмент сети напрямую не подключен к S1. Кроме того, для рекламы маршрутов не настроен протокол статического маршрута или динамической маршрутизации.

Шаг 8 Включить 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 конфигурации подождите, пока S1 и S2 обменяют OSPF маршрутами и завершат базу данных состояния канала, затем просмотрите результатирующую 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 изучил два маршрута с использованием OSPF. Проверьте соединение 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
```

Финальная 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 Ethernet0/0/7
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 Ethernet0/0/14
    shutdown
#
    ip route-static 0.0.0.0 0.0.0.0 10.0.7.254
#
return
```

Модуль 2 Конфигурация WAN предприятия

Lab 2-1 HDLC и PPP конфигурация

Цель работы

В результате этой лабораторной вы должны выполнить следующие задачи:

- Установите инкапсуляцию HDLC в качестве протокола уровня последовательной связи.
- Измените скорость передачи данных DCE на серийный канал.
- Установите инкапсуляцию PPP в качестве протокола последовательного уровня канала.
- Реализация аутентификации PAP на PPP-ссылке.
- Реализация аутентификации CHAP на ссылке PPP.

Топология

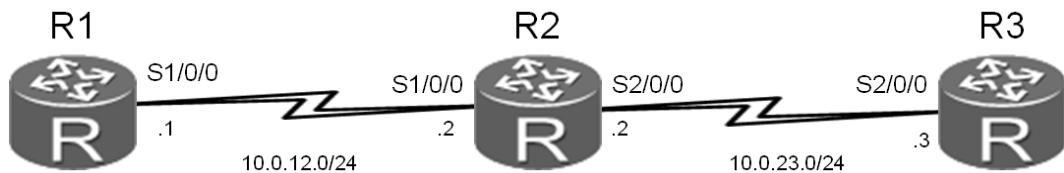


Рисунок 2.1 топология конфигурации HDLC и PPP

Сценарий

В качестве расширяющегося корпоративного бизнеса было создано несколько филиалов, которые должны быть частью административной сферы компании. WAN решения необходимы и как администратор сети компания, которой вы были поставлены задачи по созданию HDLC и PPP решений на пограничном маршрутизаторе, которые будут перенесены на некоторые сети поставщика услуг, возможно MPLS, однако детали этого не были выявлены для вас, поскольку сеть поставщика услуг остается вне сферы действия вашей задачи. R2 — это пограничный маршрутизатор, расположенный в штаб-квартире, а R1

R3 — в филиалах. Штаб-квартира и филиалы должны быть созданы в качестве единого административного домена. Используйте HDLC и PPP в связях WAN и устанавливайте аутентификацию как простую меру безопасности.

Задачи

Шаг 1 Подготовка среды

Если вы начинаете этот раздел с не настроенного устройства, начинайте здесь, а затем переходите к шагу 3. Для тех, кто продолжает работать в предыдущих лабораториях, начинайте 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 Очистка предыдущей конфигурации

Удалите статические маршруты до R2 и отключите интерфейсы Ethernet, чтобы избежать создания альтернативных маршрутов. Удалите ненужную конфигурацию 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 серийных интерфейсах просмотрите состояние серийного интерфейса. В качестве примера следует использовать отображаемую информацию 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%
```

Проверьте подключение подключенной связи после проверки того, что физический статус и статус протокола интерфейса - up.

```
<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 RIPv2

Включите протокол маршрутизации RIP для рекламы удаленных сетей R1 и R3.

```
[R1]rip
```

```
[R1-rip-1]version 2  
[R1-rip-1]network 10.0.0.0
```

```
[R2]rip  
[R2-rip-1]version 2  
[R2-rip-1]network 10.0.0.0
```

```
[R3]rip  
[R3-rip-1]version 2  
[R3-rip-1]network 10.0.0.0
```

**После завершения настройки убедитесь, что все маршруты были изучены.
Убедитесь, что соответствующие маршруты изучены с помощью 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     RIP     100   1        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 запустите команду **ping для проверки соединения 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 подключением

Просмотрите тип кабеля, подключенного к последовательному интерфейсу, состоянию интерфейса и тактовой частоте, и 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...
```

Предыдущая информация показывает, что S1/0/0 на R1 подключается к кабелю DCE, а тактовая частота составляет 64000 бит/с. DCE управляет тактовой частотой и пропускной способностью.

Измените тактовую частоту на канале между R1 и R2 до 128000 бит/с. Эта операция должна выполняться на DCE, R1.

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

После завершения конфигурации просмотрите 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 Настройка PPP на последовательных интерфейсах

Настройте PPP между R1 и R2, а также R2 и R3. Оба конца связи должны использовать один и тот же режим инкапсуляции. Если используются различные режимы инкапсуляции, интерфейсы могут отображаться как "вниз".

```
[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
```

По завершении конфигурации подключите тестовую ссылку.

```
<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

```

Если операция **ping завершилась неудачно, проверьте состояние интерфейса и правильный ли тип 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...

```

Step 8 Проверьте изменения записи маршрутизации

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

Следующая информация использует R2 в качестве примера, 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 двух маршрутов. Проверьте следующие пункты:

Если используется инкапсуляция HDLC, существуют ли эти два маршрута?

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

Шаг 9 Включить аутентификацию PAP между R1 и R2

Настройте аутентификацию PAP с помощью R1 в качестве аутентификатора PPP PAP.

```

[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 R2, действующим как устройство, прошедшее аутентификацию PAP.

```

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

```

После того как R2 отправит запрос аутентификации в R1, R1 отправляет ответное сообщение в R2, запрашивая R2 использовать аутентификацию PAP, после чего R2 отправит свой пароль в R1.

После завершения конфигурации проверьте соединение 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 Включить аутентификацию CHAP между R2 и R3

Настройте R3 как аутентификатор. После того как R2 отправит запрос аутентификации в R3, R3 отправит ответное сообщение в R2, запросив R2, чтобы использовать аутентификацию CHAP, по-сле 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 отображается следующая информация.

```
Dec 10 2013 15:06:00+00:00 R3 %%01PPP/4/PEERNOCHAP(1) [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(1) [6]:On the interface Serial2/0/0, LCP
negotiation failed because the result cannot be accepted.
```

Выделенный вывод указывает, что аутентификация не может инициализироваться.

Настройте R2 как клиент CHAP.

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

По завершении настройки интерфейс переходит в состояние Up. Вывод команды ping выглядит следующим образом:

```
<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

Запустите команду `debug`, чтобы просмотреть согласование PPP-соединения между R2 и R3. Соединение PPP устанавливается с использованием CHAP. Отключите интерфейс Serial 2/0/0 на R2, запустите команду отладки и включите Serial 2/0/0 на R2.

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

Запустите команды **debugging ppp chap all** и **terminal debugging**, чтобы отобразить отладочную информацию.

```
[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 из 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
```

Отображается 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 отображает ключевое режим 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 протокол аутентификации подписи PPP Challenge (CHAP) более безопасен, чем протокол проверки подлинности протокола PPP (PAP)?

Финальная 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  
#  
rip 1  
version 2  
network 10.0.0.0  
#  
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
```

```

#
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
#
rip 1
version 2
network 10.0.0.0
#
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
#
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
#
rip 1
version 2
network 10.0.0.0
#
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
#
return
```

Lab 2-2 Настройка протокола Frame Relay в CE-маршрутизаторе

Цель работы

В результате этой лабораторной вы должны выполнить следующие задачи:

- Конфигурация интерфейсов frame relay в CE-маршрутизаторе.
- Установка RIP со схемой подключения узлов hub and spoke.
- Установка OSPF со схемой подключения узлов hub and spoke без возможности широковещания.
- Настройка интерфейса frame relay в тех случаях когда используется OSPF сеть типа точка-многоточка.

Топология

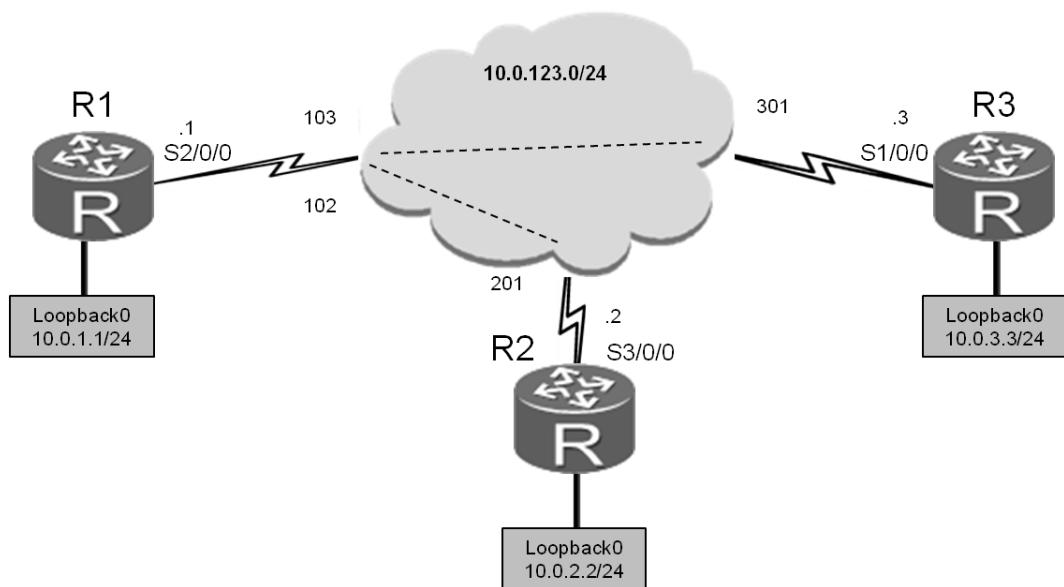


Рисунок 2.2 Лабораторная топология для конфигурации frame relay

Сценарий

Сеть предприятия имеет существующие виртуальные схемы ретрансляции кадров между штаб-квартирой и некоторыми филиалами. Недавнее изменение в оборудовании требует, чтобы ретрансляция кадров VC была восстановлена.

Виртуальные цепи были предоставлены поставщиком услуг на момент первого внедрения службы, и задача администратора заключается в реализации конфигурации Frame Relay на пограничных маршрутизаторах для головного офиса и филиалов. Администратор должен настроить Frame Relay на соединениях WAN и выполнить сопоставление между локальными DLCI и IP-адресами.

Задачи

Шаг 1 Подготовка среды

Если вы начинаете этот раздел с не настроенного устройства, начинайте здесь, а затем переходите к шагу 3. Для тех, кто продолжает работать в предыдущих лабораториях, начинайте 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 Очистка предыдущей конфигурации

Отключите последовательные интерфейсы, используемые для установления сетей HDLC и PPP.

```
[R1]interface Serial 1/0/0  
[R1-Serial1/0/0]shutdown  
  
[R2]interface Serial 1/0/0  
[R2-Serial1/0/0]shutdown  
[R2-Serial1/0/0]interface Serial 2/0/0  
[R2-Serial2/0/0]shutdown  
  
[R3]interface Serial 2/0/0  
[R3-Serial2/0/0]shutdown
```

Шаг 3 Гарантировать инкапсуляцию frame relay

Задайте основные параметры, в том числе IP-адреса. Вручную определите сопоставление между узлом и DLCI. Функция обратного ARP должна быть отключена. Убедитесь, что параметр широ-ковещания используется в команде fr map, чтобы разрешить рекламу сети на кольцевом интерфейсе с помощью RIP.

```
[R1]interface Serial 2/0/0
[R1-Serial2/0/0]link-protocol fr
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y
[R1-Serial2/0/0]ip address 10.0.123.1 24
[R1-Serial2/0/0]undo fr inarp
[R1-Serial2/0/0]fr map ip 10.0.123.2 102 broadcast
[R1-Serial2/0/0]fr map ip 10.0.123.3 103 broadcast
[R1-Serial2/0/0]interface loopback 0
[R1-LoopBack0]ip address 10.0.1.1 24

[R2]interface Serial 3/0/0
[R2-Serial3/0/0]link-protocol fr
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y
[R2-Serial3/0/0]ip address 10.0.123.2 24
[R2-Serial3/0/0]undo fr inarp
[R2-Serial3/0/0]fr map ip 10.0.123.1 201 broadcast
[R2-Serial3/0/0]interface loopback 0
[R2-LoopBack0]ip address 10.0.2.2 24

[R3]interface Serial 1/0/0
[R3-Serial1/0/0]link-protocol fr
Warning: The encapsulation protocol of the link will be changed. Continue? [Y/N]:y
[R3-Serial1/0/0]ip address 10.0.123.3 24
[R3-Serial1/0/0]undo fr inarp
[R3-Serial1/0/0]fr map ip 10.0.123.1 301 broadcast
[R3-Serial1/0/0]interface loopback 0
[R3-LoopBack0]ip address 10.0.3.3 24
```

После настройки IP-адресов проверьте подключение к сети.

```
<R1>ping 10.0.123.2
PING 10.0.123.2: 56 data bytes, press CTRL_C to break
Reply from 10.0.123.2: bytes=56 Sequence=1 ttl=255 time=64 ms
Reply from 10.0.123.2: bytes=56 Sequence=2 ttl=255 time=59 ms
Reply from 10.0.123.2: bytes=56 Sequence=3 ttl=255 time=59 ms
```

```

Reply from 10.0.123.2: bytes=56 Sequence=4 ttl=255 time=59 ms
Reply from 10.0.123.2: bytes=56 Sequence=5 ttl=255 time=59 ms

--- 10.0.123.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 59/60/64 ms

<R1>ping 10.0.123.3
PING 10.0.123.3: 56 data bytes, press CTRL_C to break
Reply from 10.0.123.3: bytes=56 Sequence=1 ttl=255 time=64 ms
Reply from 10.0.123.3: bytes=56 Sequence=2 ttl=255 time=59 ms
Reply from 10.0.123.3: bytes=56 Sequence=3 ttl=255 time=59 ms
Reply from 10.0.123.3: bytes=56 Sequence=4 ttl=255 time=59 ms
Reply from 10.0.123.3: bytes=56 Sequence=5 ttl=255 time=59 ms

--- 10.0.123.3 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 59/60/64 ms

```

Выполните данные команды, чтобы просмотреть информацию об инкапсуляции FR для интерфейсов R1.

```

<R1>display fr interface Serial 2/0/0
Serial2/0/0, DTE, physical up, protocol up

<R1>display fr lmi-info interface Serial 2/0/0
Frame relay LMI statistics for interface Serial2/0/0 (DTE, Q933)
T391DTE = 10 (hold timer 10)
N391DTE = 6, N392DTE = 3, N393DTE = 4
out status enquiry = 180, in status = 178
status timeout = 0, discarded messages = 0

<R1>display fr map-info interface Serial 2/0/0
Map Statistics for interface Serial2/0/0 (DTE)
DLCI = 102, IP 10.0.123.2, Serial2/0/0
create time = 2011/11/16 09:28:49, status = ACTIVE
encapsulation = ietf, vlink = 1, broadcast
DLCI = 103, IP 10.0.123.3, Serial2/0/0
create time = 2011/11/16 09:28:56, status = ACTIVE
encapsulation = ietf, vlink = 2, broadcast

```

Шаг 4 Настройте RIPv2 между R1, R2 и R3

Настройте RIPv2 на R1, R2 и R3. Если вы продолжаете работать в предыдущей лабораторной работе HDLC/PPP, маршруты RIP для сети 10.0.0.0 могут быть уже настроены, однако автоматизация все равно должна быть отключена, чтобы однозначно идентифицировать маршруты одноранговых узлов.

Кроме того, разрыв по горизонтали отключен по умолчанию в сетях frame relay, и поэтому нет необходимости изменять параметры разделения горизонта в этом упражнении.

```
[R1]rip 1  
[R1-rip-1]version 2  
[R1-rip-1]network 10.0.0.0  
[R1-rip-1]undo summary
```

```
[R2]rip 1  
[R2-rip-1]version 2  
[R2-rip-1]network 10.0.0.0  
[R2-rip-1]undo summary
```

```
[R3]rip 1  
[R3-rip-1]version 2  
[R3-rip-1]network 10.0.0.0  
[R3-rip-1]undo summary
```

Просмотрите таблицы маршрутизации на R1, R2 и R3, чтобы проверить изученные маршруты.

```
<R1>display ip routing-table protocol rip  
Route Flags: R - relay, D - download to fib  
-----  
Public routing table : RIP  
Destinations : 2          Routes : 2  
  
RIP routing table status : <Active>  
Destinations : 2          Routes : 2  
  
Destination/Mask   Proto   Pre  Cost      Flags NextHop       Interface  
10.0.2.0/24    RIP     100   1          D   10.0.123.2      Serial2/0/0  
10.0.3.0/24    RIP     100   1          D   10.0.123.3      Serial2/0/0  
  
RIP routing table status : <Inactive>
```

```

Destinations : 0          Routes : 0

<R2>display ip routing-table protocol rip
Route Flags: R - relay, D - download to fib
-----
Public routing table : RIP
Destinations : 2          Routes : 2

RIP routing table status : <Active>
Destinations : 2          Routes : 2

Destination/Mask Proto Pre Cost Flags NextHop Interface
10.0.1.0/24 RIP   100 1      D   10.0.123.1   Serial3/0/0
10.0.3.0/24 RIP   100 2      D   10.0.123.1   Serial3/0/0

RIP routing table status : <Inactive>
Destinations : 0          Routes : 0

[R3]display ip routing-table protocol rip
Route Flags: R - relay, D - download to fib
-----
Public routing table : RIP
Destinations : 2          Routes : 2

RIP routing table status : <Active>
Destinations : 2          Routes : 2

Destination/Mask Proto Pre Cost Flags NextHop Interface
10.0.1.0/24 RIP   100 1      D   10.0.123.1   Serial1/0/0
10.0.2.0/24 RIP   100 2      D   10.0.123.1   Serial1/0/0

RIP routing table status : <Inactive>
Destinations : 0          Routes : 0

```

Убедитесь, что 10.0.3.0 сеть R3 способна достичь 10.0.1.0 сети R1.

```
[R3]ping -a 10.0.3.3 10.0.1.1
PING 10.0.1.1: 56 data bytes, press CTRL_C to break
Reply from 10.0.1.1: bytes=56 Sequence=1 ttl=255 time=68 ms
Reply from 10.0.1.1: bytes=56 Sequence=2 ttl=255 time=63 ms
Reply from 10.0.1.1: bytes=56 Sequence=3 ttl=255 time=63 ms
Reply from 10.0.1.1: bytes=56 Sequence=4 ttl=255 time=63 ms
Reply from 10.0.1.1: bytes=56 Sequence=5 ttl=255 time=63 ms

--- 10.0.1.1 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 63/64/68 ms
```

Выполните тот же тест в сети 10.0.2.2 R2 из сети 10.0.3.3 из R3.

```
<R3>ping -a 10.0.3.3 10.0.2.2
PING 10.0.2.2: 56 data bytes, press CTRL_C to break
Reply from 10.0.2.2: bytes=56 Sequence=1 ttl=254 time=101 ms
Reply from 10.0.2.2: bytes=56 Sequence=2 ttl=254 time=110 ms
Reply from 10.0.2.2: bytes=56 Sequence=3 ttl=254 time=101 ms
Reply from 10.0.2.2: bytes=56 Sequence=4 ttl=254 time=101 ms
Reply from 10.0.2.2: bytes=56 Sequence=5 ttl=254 time=101 ms

--- 10.0.2.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 101/102/110 ms
```

Протокол маршрутизации RIP позволяет установить маршрут между кольцевыми интерфейсами R2 и R3, установленными через R1.

Попробуйте ту же процедуру для сети 10.0.2.2 R2 из S2/0/0 (10.0.123.3) интерфейса R3.

```
[R3]ping 10.0.2.2
PING 10.0.2.2: 56 data bytes, press CTRL_C to break
Request time out
```

```
Request time out
Request time out
Request time out
Request time out

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

Предыдущие результаты теста показывают, что R3 не может связываться с R2 (и наоборот), когда последовательный интерфейс является источником. Проверьте маршруты, чтобы узнать, почему R3 и R2 отключены. Процедура диагностики этой ошибки следующая:

Просмотрите таблицу маршрутизации R3 и проверьте, предназначен ли какой-либо маршрут для IP-адреса 10.0.2.2.

Если есть такой маршрут, узнайте следующий IP-адрес этого маршрута. Затем проверьте, может ли R3 достичь следующего перехода и существует ли сопоставление между IP-адресами уровня 3 и PVC-уровня-2.

Если R3 может перейти к следующему переходу, и существует сопоставление между IP-адресами уровня 3 и PVC-уровня 2, проверьте устройства на маршруте, чтобы определить, есть ли какой-либо маршрут, который может достичь IP-адреса 10.0.2.2, будет ли следующий этап на этом маршруте доступен, и существует ли сопоставление между IP-адресами уровня-3 и PVC-уровня-2.

Если есть маршрут, который может достичь IP-адреса 10.0.2.2, и существует сопоставление между IP-адресами уровня-3 и PVC уровня 2, проверьте R2, чтобы определить, есть ли какой-либо маршрут, который достигает целевого IP-адреса ответа пакетов, и следующий этап этого маршрута достигнут.

Если следующий переход этого маршрута недостижим, и IP-адрес назначения пакетов ответа 10.0.123.3, R2 имеет маршрут, который достигает этого адреса, но нет никакого сопоставления между IP-адресами уровня 3 и PVCs уровня 2.

Ниже приведен вывод команд, используемых в предыдущей процедуре диагностики неисправности.

```
<R3>display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
Destinations : 13      Routes : 13
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.1.0/24	RIP	100	1	D	10.0.123.1	Serial1/0/0
10.0.2.0/24	RIP	100	2	D	10.0.123.1	Serial1/0/0
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	InLoopBack0
10.0.3.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
10.0.123.0/24	Direct	0	0	D	10.0.123.3	Serial1/0/0
10.0.123.1/32	Direct	0	0	D	10.0.123.1	Serial1/0/0
10.0.123.3/32	Direct	0	0	D	127.0.0.1	InLoopBack0
10.0.123.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

<R3>display fr map-info interface Serial 1/0/0

Map Statistics for interface Serial1/0/0 (DTE)

```
DLCI = 301, IP 10.0.123.1, Serial1/0/0
create time = 2011/11/16 09:22:30, status = ACTIVE
encapsulation = ietf, vlink = 1, broadcast
```

<R1>display ip routing-table

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

Routing Tables: Public

Destinations : 14 Routes : 14

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.1.0/24	Direct	0	0	D	10.0.1.1	LoopBack0
10.0.1.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
10.0.1.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
10.0.2.0/24	RIP	100	1	D	10.0.123.2	Serial2/0/0
10.0.3.0/24	RIP	100	1	D	10.0.123.3	Serial2/0/0
10.0.123.0/24	Direct	0	0	D	10.0.123.1	Serial2/0/0
10.0.123.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
10.0.123.2/32	Direct	0	0	D	10.0.123.2	Serial2/0/0
10.0.123.3/32	Direct	0	0	D	10.0.123.3	Serial2/0/0
10.0.123.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0

```
127.255.255.255/32 Direct 0 0 D 127.0.0.1 InLoopBack0  
255.255.255.255/32 Direct 0 0 D 127.0.0.1 InLoopBack0
```

```
<R1>display fr map-info interface Serial 2/0/0  
Map Statistics for interface Serial2/0/0 (DTE)  
DLCI = 102, IP 10.0.123.2, Serial2/0/0  
create time = 2011/11/16 09:28:49, status = ACTIVE  
encapsulation = ietf, vlink = 1, broadcast  
DLCI = 103, IP 10.0.123.3, Serial2/0/0  
create time = 2011/11/16 09:28:56, status = ACTIVE  
encapsulation = ietf, vlink = 2, broadcast
```

```
<R2>display ip routing-table  
Route Flags: R - relay, D - download to fib  
-----  
Routing Tables: Public  
Destinations : 13 Routes : 13  
  
Destination/Mask Proto Pre Cost Flags NextHop Interface  
  
10.0.1.0/24 RIP 100 1 D 10.0.123.1 Serial3/0/0  
10.0.2.0/24 Direct 0 0 D 10.0.2.2 LoopBack0  
10.0.2.2/32 Direct 0 0 D 127.0.0.1 InLoopBack0  
10.0.2.255/32 Direct 0 0 D 127.0.0.1 InLoopBack0  
10.0.3.0/24 RIP 100 2 D 10.0.123.1 Serial3/0/0  
10.0.123.0/24 Direct 0 0 D 10.0.123.2 Serial3/0/0  
10.0.123.1/32 Direct 0 0 D 10.0.123.1 Serial3/0/0  
10.0.123.2/32 Direct 0 0 D 127.0.0.1 InLoopBack0  
10.0.123.255/32 Direct 0 0 D 127.0.0.1 InLoopBack0  
127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0  
127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0  
127.255.255.255/32 Direct 0 0 D 127.0.0.1 InLoopBack0  
255.255.255.255/32 Direct 0 0 D 127.0.0.1 InLoopBack0
```

```
<R2>display fr map-info interface Serial 3/0/0
Map Statistics for interface Serial3/0/0 (DTE)
  DLCI = 201, IP 10.0.123.1, Serial3/0/0
  create time = 2011/11/16 09:21:10, status = ACTIVE
  encapsulation = ietf, vlink = 1, broadcast
```

Вывод состоит в том, что нет PVC, который позволяет R2 достичь IP-адреса 10.0.123.3.

Шаг 5 Измените параметры сети, чтобы включить соединение между R2 и R3

Результаты диагностики сбоя от шага 2 указывают, что отказывает связь, так как нет никакого виртуального канала между интерфейсами frame relay на R2 и R3. Для решения этого настройте PVC Frame relay между интерфейсами на R2 и R3.

```
[R2]interface Serial 3/0/0
[R2-Serial3/0/0]fr map ip 10.0.123.3 201

[R3]interface Serial 1/0/0
[R3-Serial1/0/0]fr map ip 10.0.123.2 301
```

После того, как сопоставление было настроено между IP-адресами и PVCs, проверьте таблицы отображения IP-адресов-PVC на R2 и R3 и определите сетевое подключение.

```
<R3>display fr lmi-info inter Serial 1/0/0
Frame relay LMI statistics for interface Serial1/0/0 (DTE, Q933)
  T391DTE = 10 (hold timer 10)
  N391DTE = 6, N392DTE = 3, N393DTE = 4
  out status enquiry = 326, in status = 324
  status timeout = 0, discarded messages = 0
```

```
<R3>display fr map-info interface Serial 1/0/0
Map Statistics for interface Serial1/0/0 (DTE)
  DLCI = 301, IP 10.0.123.1, Serial1/0/0
  create time = 2011/11/16 09:22:30, status = ACTIVE
  encapsulation = ietf, vlink = 1, broadcast
  DLCI = 301, IP 10.0.123.2, Serial1/0/0
  create time = 2011/11/16 09:55:23, status = ACTIVE
  encapsulation = ietf, vlink = 2
```

```
<R3>ping 10.0.2.2
PING 10.0.2.2: 56 data bytes, press CTRL_C to break
  Reply from 10.0.2.2: bytes=56 Sequence=1 ttl=254 time=118 ms
```

```
Reply from 10.0.2.2: bytes=56 Sequence=2 ttl=254 time=123 ms
Reply from 10.0.2.2: bytes=56 Sequence=3 ttl=254 time=123 ms
Reply from 10.0.2.2: bytes=56 Sequence=4 ttl=254 time=123 ms
Reply from 10.0.2.2: bytes=56 Sequence=5 ttl=254 time=123 ms

--- 10.0.2.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 118/122/123 ms
```

Шаг 6 Настройте OSPF между R1 и R2

Удалите конфигурации RIP, указанную на шаге 2, и отображение переключателя кадра между R2 и R3, которое было установлено во время шага 3.

```
[R1]undo rip 1
Warning: The RIP process will be deleted. Continue?[Y/N]y
```

```
[R2]interface Serial 3/0/0
[R2-Serial3/0/0]undo fr map ip 10.0.123.3 201
[R2-Serial3/0/0]quit
[R2]undo rip 1
Warning: The RIP process will be deleted. Continue?[Y/N]y
```

```
[R3]interface Serial 1/0/0
[R3-Serial1/0/0]undo fr map ip 10.0.123.2 301
[R3-Serial1/0/0]quit
[R3]undo rip 1
Warning: The RIP process will be deleted. Continue?[Y/N]y
[R3]
```

Настройте OSPF с одной областью на R1, R2 и R3.

```
[R1]ospf 1 router-id 10.0.1.1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.0.0.0 0.255.255.255
```

```
[R2]ospf 1 router-id 10.0.2.2
[R2-ospf-1]area 0
```

```
[R2-ospf-1-area-0.0.0.0]network 10.0.0.0 0.255.255.255
```

```
[R3]ospf 1 router-id 10.0.3.3
```

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

```
[R3-ospf-1-area-0.0.0.0]network 10.0.0.0 0.255.255.255
```

После того, как базовые параметры установлены, OSPF не может установить соседние смежности. При использовании Frame relay для инкапсуляции уровня канала передачи данных OSPF установит тип сети к NBMA по умолчанию. В результате OSPF не поддерживает широковещательные рассылки и поэтому не может автоматически обнаружить соседние узлы.

```
<R3>display ospf interface Serial 1/0/0 verbose
OSPF Process 1 with Router ID 10.0.3.3
    Interfaces

Interface: 10.0.123.3 (Serial1/0/0)
Cost: 1562      State: DR          Type: NBMA        MTU: 1500
Priority: 1
Designated Router: 10.0.123.3
Backup Designated Router: 0.0.0.0
Timers: Hello 30 , Dead 120 , Poll 120 , Retransmit 5 , Transmit Delay 1
    IO Statistics
        Type      Input     Output
        Hello      0         0
        DB Description      0         0
        Link-State Req      0         0
        Link-State Update    0         0
        Link-State Ack      0         0
OpaqueId: 0  PrevState: Waiting
```

Шаг 7 Настройка среды NBMA

Пока R3 является DR, R2 не может установить полное смещение с DR, поскольку R3 недоступен через PVC между R2 и R1. Поэтому DR должен быть установлен на R1. Кроме того, приветствен-ные сообщения OSPF являются одноадресными в сети NBMA. Одноранговые узлы должны быть указаны вручную, чтобы разрешить переадресацию пакетов приветствия.

```
[R1]ospf
```

```
[R1-ospf-1]peer 10.0.123.2
[R1-ospf-1]peer 10.0.123.3
[R1-ospf-1]interface Serial 2/0/0
[R1-Serial2/0/0]ospf dr-priority 255
```

```
[R2]ospf
[R2-ospf-1]peer 10.0.123.1
```

```
[R3]ospf
[R3-ospf-1]peer 10.0.123.1
```

При желании приоритет DR для R2 и R3 может быть установлен в 0 для принудительного освобождения от любых выборов DR.

```
<R1>display ospf interface Serial 2/0/0 verbose
OSPF Process 1 with Router ID 10.0.1.1
    Interfaces

Interface: 10.0.123.1 (Serial2/0/0)
    Cost: 1562      State: DR        Type: NBMA        MTU: 1500
    Priority: 255
    Designated Router: 10.0.123.1
    Backup Designated Router: 10.0.123.3
    Timers: Hello 30 , Dead 120 , Poll 120 , Retransmit 5 , Transmit Delay 1
    IO Statistics
        Type      Input     Output
        Hello     32       32
        DB Description   8        29
        Link-State Req   3        2
        Link-State Update 16      30
        Link-State Ack   20       9
    OpaqueId: 0  PrevState: BDR
Effective cost: 1562, enabled by OSPF Protocol
```

Если R1 не является назначенным маршрутизатором, сбросьте процесс ospf на всех маршрутизаторах с помощью следующей команды и повторите попытку указанной выше команды отображения.

```
<R1>reset ospf process graceful-restart
```

Отобразите таблицу маршрутизации, чтобы подтвердить, что OSPF установлен по сети ретрансляции.

```

<R1>display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
Destinations : 14      Routes : 14

Destination/Mask   Proto Pre Cost     Flags NextHop       Interface
10.0.1.0/24        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  1562      D   10.0.123.2     Serial2/0/0
10.0.3.3/32        OSPF   10  1562      D   10.0.123.3     Serial2/0/0
10.0.123.0/24      Direct 0   0          D   10.0.123.1     Serial2/0/0
10.0.123.1/32      Direct 0   0          D   127.0.0.1      Serial2/0/0
10.0.123.2/32      Direct 0   0          D   10.0.123.2     Serial2/0/0
10.0.123.3/32      Direct 0   0          D   10.0.123.3     Serial2/0/0
10.0.123.255/32    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

```

```

<R1>ping -a 10.0.1.1 10.0.2.2
PING 10.0.2.2: 56 data bytes, press CTRL_C to break
Reply from 10.0.2.2: bytes=56 Sequence=1 ttl=255 time=51 ms
Reply from 10.0.2.2: bytes=56 Sequence=2 ttl=255 time=60 ms
Reply from 10.0.2.2: bytes=56 Sequence=3 ttl=255 time=51 ms
Reply from 10.0.2.2: bytes=56 Sequence=4 ttl=255 time=51 ms
Reply from 10.0.2.2: bytes=56 Sequence=5 ttl=255 time=60 ms

```

```

--- 10.0.2.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 51/54/60 ms

```

Попытки установить соединение между 10.0.2.2 и 10.0.3.3 при использовании типа сети NBMA не удастся, если между R2 и R3 не установлена виртуальная цепь (PVC). В качестве альтернативы можно использовать тип сети многоточечного соединения.

Шаг 8 Установка типа сети OSPF для многоточечного соединения

Конфигурация OSPF может также использовать сеть OSPF «точка - много точек», заменяют сети ретрансляции фреймов вводом с клавиатуры. Сначала вручную удалите пилинг, а затем измените тип сетей на «точка – много точек».

```
[R1]ospf  
[R1-ospf-1]undo peer 10.0.123.2  
[R1-ospf-1]undo peer 10.0.123.3
```

```
[R2]ospf  
[R2-ospf-1]undo peer 10.0.123.1
```

```
[R3]ospf  
[R3-ospf-1]undo peer 10.0.123.1
```

Установите тип сети многоточечного соединения.

```
[R1]interface Serial 2/0/0  
[R1-Serial2/0/0]ospf network-type p2mp
```

```
[R2]interface Serial 3/0/0  
[R2-Serial3/0/0]ospf network-type p2mp
```

```
[R3]interface Serial 1/0/0  
[R3-Serial1/0/0]ospf network-type p2mp
```

После установки типа сети OSPF подождите, пока не будет установлено соседнее отношение, а затем проверьте отношения соседей и направьте информацию о маршруте.

```
<R1>display ospf peer brief  
OSPF Process 1 with Router ID 10.0.1.1  
Peer Statistic Information  
-----  
Area Id      Interface          Neighbor id     State  
0.0.0.0      Serial2/0/0       10.0.2.2        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 : 14      Routes : 14  

-----  

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   1562   D   10.0.123.2  Serial2/0/0  

10.0.3.3/32 OSPF   10   1562   D   10.0.123.3  Serial2/0/0  

10.0.123.0/24 Direct 0   0       D   10.0.123.1  Serial2/0/0  

10.0.123.1/32 Direct 0   0       D   127.0.0.1  Serial2/0/0  

10.0.123.2/32 Direct 0   0       D   10.0.123.2  Serial2/0/0  

10.0.123.3/32 Direct 0   0       D   10.0.123.3  Serial2/0/0  

10.0.123.255/32 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

```

```

<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          Serial3/0/0        10.0.1.1        Full

```

```

<R2>display ip routing-table  

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

-----  

Routing Tables: Public  

Destinations : 14      Routes : 14  

-----  

Destination/Mask Proto Pre Cost Flags NextHop Interface

```

10.0.1.1/32	OSPF	10	1562	D	10.0.123.1	Serial3/0/0
10.0.2.0/24	Direct	0	0	D	10.0.2.2	LoopBack0
10.0.2.2/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.2.255/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.3.3/32	OSPF	10	3124	D	10.0.123.1	Serial3/0/0
10.0.123.0/24	Direct	0	0	D	10.0.123.2	Serial3/0/0
10.0.123.1/32	Direct	0	0	D	10.0.123.1	Serial3/0/0
10.0.123.2/32	Direct	0	0	D	127.0.0.1	Serial3/0/0
10.0.123.3/32	OSPF	10	3124	D	10.0.123.1	Serial3/0/0
10.0.123.255/32	Direct	0	0	D	127.0.0.1	Serial3/0/0
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

<R3>display ospf peer brief

```
OSPF Process 1 with Router ID 10.0.3.3
    Peer Statistic Information
```

Area Id	Interface	Neighbor id	State
0.0.0.0	Serial1/0/0	10.0.1.1	Full

<R3>display ip routing-table

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

Routing Tables: Public

Destinations : 14 Routes : 14

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.1.1/32	OSPF	10	1562	D	10.0.123.1	Serial1/0/0
10.0.2.2/32	OSPF	10	3124	D	10.0.123.1	Serial1/0/0
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
10.0.123.0/24	Direct	0	0	D	10.0.123.3	Serial1/0/0
10.0.123.1/32	Direct	0	0	D	10.0.123.1	Serial1/0/0
10.0.123.2/32	OSPF	10	3124	D	10.0.123.1	Serial1/0/0
10.0.123.3/32	Direct	0	0	D	127.0.0.1	Serial1/0/0

```

10.0.123.255/32 Direct 0 0 D 127.0.0.1 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

```

Выполните тест сетевого соединения на R3 из пункта 10.0.3.3.

```

<R3>ping -a 10.0.3.3 10.0.1.1
PING 10.0.1.1: 56 data bytes, press CTRL_C to break
Reply from 10.0.1.1: bytes=56 Sequence=1 ttl=255 time=60 ms
Reply from 10.0.1.1: bytes=56 Sequence=2 ttl=255 time=51 ms
Reply from 10.0.1.1: bytes=56 Sequence=3 ttl=255 time=50 ms
Reply from 10.0.1.1: bytes=56 Sequence=4 ttl=255 time=60 ms
Reply from 10.0.1.1: bytes=56 Sequence=5 ttl=255 time=51 ms

```

```

--- 10.0.1.1 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 50/54/60 ms

```

```

<R3>ping -a 10.0.3.3 10.0.123.2
PING 10.0.123.2: 56 data bytes, press CTRL_C to break
Reply from 10.0.123.2: bytes=56 Sequence=1 ttl=254 time=110 ms
Reply from 10.0.123.2: bytes=56 Sequence=2 ttl=254 time=101 ms
Reply from 10.0.123.2: bytes=56 Sequence=3 ttl=254 time=101 ms
Reply from 10.0.123.2: bytes=56 Sequence=4 ttl=254 time=110 ms
Reply from 10.0.123.2: bytes=56 Sequence=5 ttl=254 time=101 ms

```

```

--- 10.0.123.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 101/104/110 ms

```

```

<R3>ping -a 10.0.3.3 10.0.2.2
PING 10.0.2.2: 56 data bytes, press CTRL_C to break
Reply from 10.0.2.2: bytes=56 Sequence=1 ttl=254 time=102 ms
Reply from 10.0.2.2: bytes=56 Sequence=2 ttl=254 time=101 ms
Reply from 10.0.2.2: bytes=56 Sequence=3 ttl=254 time=110 ms
Reply from 10.0.2.2: bytes=56 Sequence=4 ttl=254 time=101 ms
Reply from 10.0.2.2: bytes=56 Sequence=5 ttl=254 time=102 ms

```

```
--- 10.0.2.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 101/103/110 ms
```

Финальная конфигурация

```
[R1]display current-configuration
[V200R007C00SPC600]
#
sysname R1
#
interface Serial2/0/0
link-protocol fr
undo fr inarp
fr map ip 10.0.123.2 102 broadcast
fr map ip 10.0.123.3 103 broadcast
ip address 10.0.123.1 255.255.255.0
ospf network-type p2mp
ospf dr-priority 255
#
interface LoopBack0
ip address 10.0.1.1 255.255.255.0
#
ospf 1 router-id 10.0.1.1
area 0.0.0.0
network 10.0.0.0 0.255.255.255
#
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
```

```

#
interface Serial3/0/0
link-protocol fr
undo fr inarp
fr map ip 10.0.123.1 201 broadcast
ip address 10.0.123.2 255.255.255.0
ospf network-type p2mp
#
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 10.0.0.0 0.255.255.255
#
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 Serial1/0/0
link-protocol fr
undo fr inarp
fr map ip 10.0.123.1 301 broadcast
ip address 10.0.123.3 255.255.255.0
ospf network-type p2mp
#
interface LoopBack0
ip address 10.0.3.3 255.255.255.0
#
ospf 1 router-id 10.0.3.3
area 0.0.0.0
network 10.0.0.0 0.255.255.255
#

```

```
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
```

Lab 2-3 Создание клиентской сессии PPPoE

Цель работы

В результате этой лабораторной вы должны выполнить следующие задачи:

- Конфигурация интерфейса Dialer для PPPoE.
- Аутентификация клиента по PPPoE.

Топология

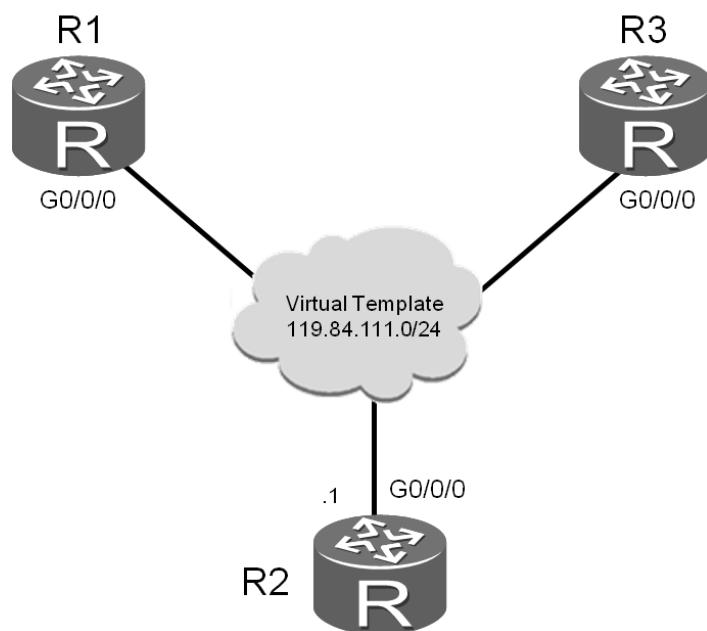


Рисунок 2.3 Сервер PPPoE и клиентская топология

Сценарий

Предприятие подписывается на (как правило, высокоскоростную) услугу DSL от поставщика услуг, по которой поддерживаются службы WAN. R1 и R3 являются корпоративными пограничными маршрутизаторами разных офисов и устанавливают соединение с поставщиком услуг через сервер PPPoE (R2). Предприятие обязано установить на пограничных маршрутизаторах набор PPPoE, позволяющий хостам в локальной сети получать доступ к внешним ресурсам прозрачно через сеть поставщика услуг по протоколу PPPoE.

Задачи

Шаг 1 Подготовка среды

Если вы начинаете эту лабораторную с не настроенного устройства, начинайте здесь, а затем перейдите к шагу 3. Для тех, кто продолжает работу в предыдущих лабораториях, начинайте 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 Очистка предыдущей конфигурации

Отключите последовательные интерфейсы, чтобы избежать маршрутизации через сеть 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 должен позволять корпоративным маршрутизаторам R1 и R3 проходить проверку подлинности.

```
[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
```

Привязать виртуальный шаблон с интерфейсом 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 аутентифицированный 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 Настройка клиента PPPoE

Настройте R1 как клиент PPPoE, для которого необходимо создать интерфейс дайлера, и активировать аутентификацию PPP. Имя пользователя и пароль, прошедшие проверку подлинности 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
```

Свяжите PPPoE Dialer с исходящим интерфейсом

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

Настройка статического маршрута по умолчанию на сервер PPPoE

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

Настройте R3 как клиент PPPoE, для которого необходимо создать интерфейс Dialer, и активировать аутентификацию PPP. Идентифицированное имя пользователя и пароль PPP должны совпадать с именем, установленным 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
```

Свяжите PPPoE Dialer с исходящим интерфейсом

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

Настройка статического маршрута по умолчанию на сервер PPPoE

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

Шаг 5 Проверьте результаты настройки

Выполните команду **display pppoe-server session all** для просмотра информации о состоянии и 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 выведенной на экран информации, состояние сеанса нормально.

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

```
<R1>display ip interface brief
*down: administratively down
^down: standby
(1): 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...

Финальная 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%%%$%
local-user admin service-type http
local-user huawei password cipher %%%B::I)Io0H8) [%SB[idM3C/!#%%%
local-user huawei service-type ppp
#
interface Dialer1
link-protocol ppp
ppp chap user huawei1
ppp chap password cipher %%%A8E~UjX}@;bhCL*C4w#<%"Ba%%%$%
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

Lab 3-1 Фильтрация корпоративных данных с помощью списков управления доступом

Цель работы

В результате этой лабораторной вы должны выполнить следующие задачи:

- Установление базового ACL для реализации фильтрации на основе источников.
- Создание расширенных ACL для реализации расширенной фильтрации.

Топология

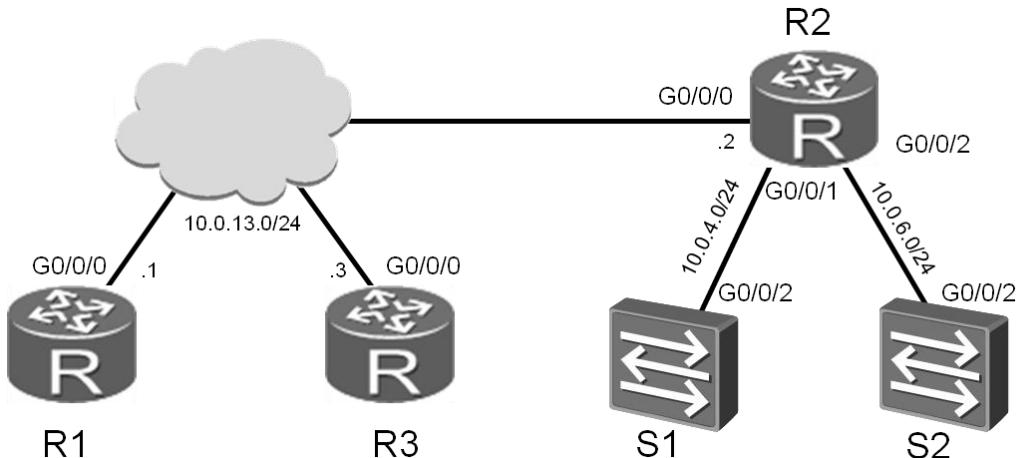


Рисунок 3.1 Фильтрация данных корпоративной сети с помощью списков управления доступом

Сценарий

Предположим, что вы являетесь администратором сети компании, которая имеет три сети, принадлежащие трем объектам. R2 развертывается на границе сети для основного сайта, а R1 и R3 - на границе остальных сайтов. Маршрутизаторы соединены через частное WAN-соединение. Компании необходимо контролировать доступ сотрудников к сервисам telnet и FTP. Только сайт R1 имеет разрешение на доступ к серверу telnet на основном сайте. Только сайт R3 имеет разрешение на доступ к FTP-серверу.

Задачи

Шаг 1 Подготовка среды

Если вы начинаете этот раздел с не конфигурированного устройства, начните здесь, а затем перейдите к шагу 3. Для тех продолжает от предыдущей лабораторной работы, начните 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 Очистите предыдущую конфигурацию

Удалите текущую сеть, объявляемую в OSPF, интерфейс Dialer 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 **Настройка IP-адресации**

Настройте адресацию для 10.0.13.0/24, 10.0.4.0/24 и 10.0.6.0/24 сети как показано в топологии рисунка 7.1.

```
[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 соединительные линии VLAN на S1 и S2. Тип ссылки порта должен уже быть сконфигурирован для интерфейса GigabitEthernet 0/0/2 на S1.

```
[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 Настройте OSPF для включения межсетевой связи

Настройте OSPF для R1, R2 и R3. Гарантируйте, что все являются частью одной и той же области OSPF и объявляют сети, которые были созданы.

```
[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 шлюзе S1 и S2, следующий переход в качестве 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
```

Проверьте, что путь существует 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 помощью списков управления доступом

Настройте S1 как сервер 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 как FTP-сервер.

```
[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 - 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 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: FTP-подключение может занять некоторое время, чтобы ответить (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: команда bye может использоваться для закрытия FTP-соединения

Дополнительное задание: Анализ и проверка

FTP требует, чтобы два порта были определены в списке управления доступом, почему так?

Должен ли базовый ACL и расширенный ACL быть развернут около исходной сети или целевой сети, и почему?

Final Configuration

```
<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
```

Lab 3-2 Преобразование Сетевых Адресов

Цель работы

В результате этой лабораторной вы должны выполнить следующие задачи:

- Трансляция адресов между сетями (NAT).
- Настройка Easy IP.

Топология

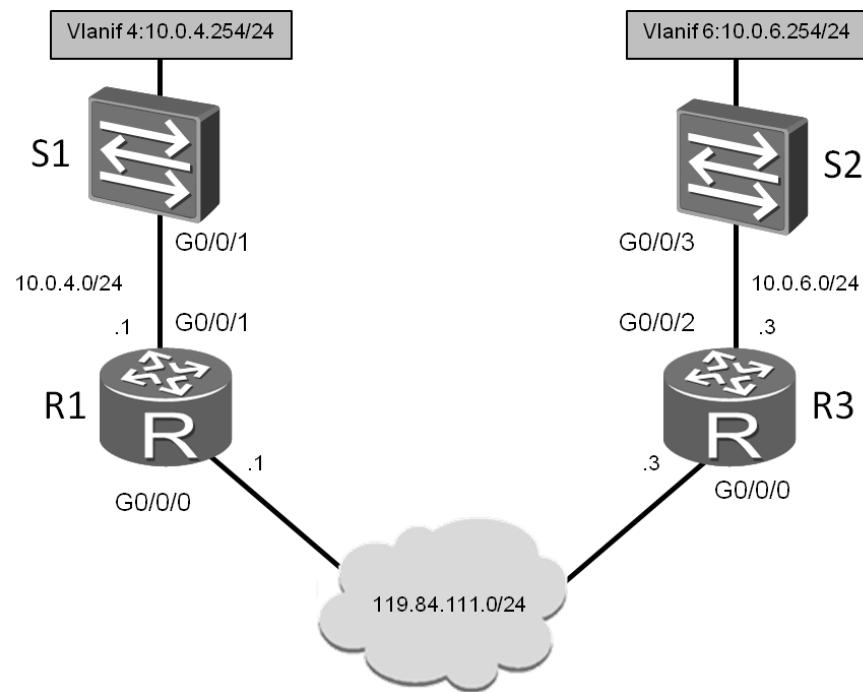


Рис. 3.2 Топология Преобразования Сетевых Адресов

Сценарий

Для сохранения адресации офисы корпоративной сети внедрили внутреннюю частную адресацию. Однако пользователям требуется средства для маршрутизации между этими частными сетями и общим сетевым доменом. R1 и R3 представляют маршрутизаторы края филиалов предпринимательства, доступ потребности филиальной сети к общественной сети. Администратору сети предлагают настроить динамические решения NAT на, чтобы позволить R1 выполнить преобразование адресов. Легкое разрешение IPNAT быть приложенным к R3.

Задачи

Шаг 1 Подготовка среды

Если Вы запускаете этот раздел с не сконфигурированного устройства, начинаете здесь и затем перемещаетесь в шаг 3. Для тех, которые продолжают из предыдущих лабораторной, начните на шаге 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 **Очистите предыдущую конфигурацию**

Повторно установите соединение с S1 и S2 через GigabitEthernet 0/0/1 На R1 и Gigabit Ethernet 0/0/2 на R3. Удалите OSPF из 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 на 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 Реализуйте конфигурацию 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
```

Проверьте, что R1 в состоянии достигнуть и S1 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 Настройте списки управления доступом для R1 и R3

Настройте расширенный ACL на R1 и выберите поток данных с источником S1, назначением R3 и предназначенный для порта сервиса 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

```

Настройте основной 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 Настройка динамического NAT

Настройте статический маршрут на S1 и S2, следующий переход 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

```

Настройка динамического NAT на GigabitEthernet0/0/0 интерфейс P1.

```

[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 как сервер 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 узла из 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 общим адресом удаленного 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 трансляции сеанса ACL и перевода сеанса 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
```

Сеанс ICMP имеет время жизни только 20 секунд и поэтому может не казаться присутствующим при отображении результатов сеанса NAT. В этом случае для

продления периода, в течение которого поддерживаются результаты ICMP, можно использовать следующую команду:

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

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

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

Протестируйте связь от S2 до 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
```

Финальная 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|$)M5D}v@bY^gK\;,>QR,.*d;8Mp>|+EU,:~D~8b59~..*g,%$%
$%
user-interface vty 0 4
  authentication-mode password
  set authentication password cipher %$%$7m1|,!cce$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
```

Lab 3-3 Создание локальных решений AAA

Цель работы

В результате этой лабораторной вы должны выполнить следующие задачи:

- Конфигурация локальных AAA, для которых должны использоваться схемы аутентификации и авторизации.
- Создание домена Huawei
- Реализация уровней привилегий для аутентифицированных пользователей.

Топология



Рисунок 3.3 конфигурация AAA

Сценарий

R1 и R3 были развернуты в сети и должны предоставить сервисы удаленной аутентификации с помощью AAA. Компания требует, чтобы оба маршрутизатора стали частью домена huawei и чтобы услуга telnet была доступна пользователям с ограниченными привилегиями, предоставленными после аутентификации.

Задачи

Шаг 1 Подготовка среды

Если вы начинаете этот раздел с не конфигурированного устройства, начните здесь, а затем перейдите к шагу 3. Для тех, кто продолжает от предыдущей лабораторной, начните 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 Очистка предыдущей конфигурации

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 Проверьте подключение 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 Выполните конфигурацию AAA на R1

Настройте схему аутентификации и схему авторизации на R1. Конфигурацию для R3 можно найти на 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
```

Настройте домен *huawei* на R1, затем создайте пользователя и примените его к этому домену.

```
[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 как сервер telnet, используя режим аутентификации AAA.

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

Проверьте, была ли служба telnet на R1 установлена успешно.

```
<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 пользовательские полномочия ограничены уровнем полномочий 0 для user1@huawei.

Шаг 5 Выполните конфигурацию AAA на R3

Настройте режим аутентификации и авторизации как *local* на R3

```
[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
```

Настройте домен *huawei* на R3, затем создайте пользователя и примените пользователя к этому домену.

```
[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 сервис 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 пользовательские полномочия ограничены уровнем полномочий 0 для *user3@huawei*.

Шаг 6 Наблюдайте за результатами 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       : -
```

Финальная 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
```

Lab 3-4 Защита трафика с помощью IPSec VPN

Цель обучения

В результате этой лабораторной вы должны выполнить следующие задачи:

- Настройка предложения IPSec с помощью набора преобразований esp.
- Конфигурация ACL, используемого для определения интересного трафика.
- Настройка политики IPSec
- Привязка политики IPSec к интерфейсу

Топология

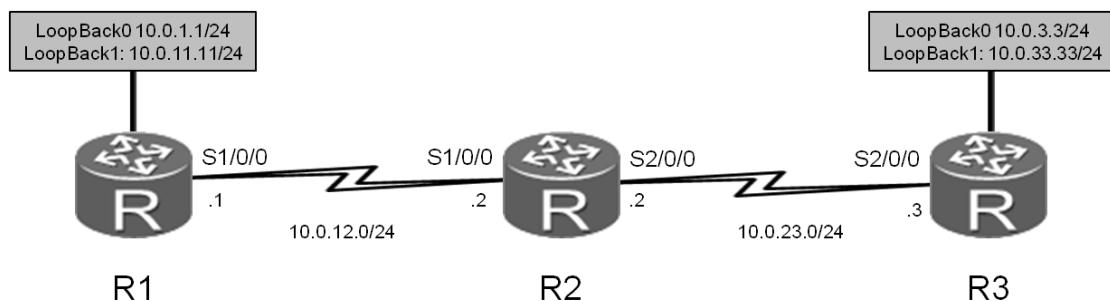


Рисунок 3.4 топология IPSec VPN

Сценарий

В интересах защиты как целостности, так и конфиденциальности данных компании требуется, чтобы связь между офисами предприятия обеспечивала защиту конкретных частных данных по мере их передачи по общедоступной сетевой инфраструктуре. Как администратор сети компании, задача была назначена для реализации решений IPSec VPN между пограничным маршрутизатором HQ (R1) и филиалом (R3). В настоящее время только отдельные отделы в штаб-квартире требуют защищенной связи по общедоступной сети (R2). Администратор должен установить IPSec, используя туннельный режим между двумя офисами для всего трафика, происходящего из отдела.

Задачи

Шаг 1 Подготовка среды

Если вы начинаете этот раздел с не конфигурированного устройства, начните здесь, а затем перейдите к шагу 3. Для тех продолжает от предыдущей лабораторной работы, начните 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 Очистите предыдущую конфигурацию

Удалите адресацию для интерфейса GigabitEthernet 0/0/0 На R1 & R3 и отключите интерфейсы как показано для предотвращения альтернативных маршрутов.

```
[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 Установите дополнительные логические интерфейсы

```
[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 публичной сети 10.0.12.0/24 и 10.0.23.0/24 как часть области OSPF 0.

```
[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 конвертации маршрута OSPF просмотрите 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	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	2343	D	10.0.12.2	Serial1/0/0
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	Direct	0	0	D	127.0.0.1	Serial1/0/0
10.0.12.2/32	Direct	0	0	D	10.0.12.2	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	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	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

Если скорость в бодах будет сохраняться как 128000 из лабораторного 6-1, стоимость OSPF будет установлена как показано, и таким образом может измениться из-за метрического вычисления, используемого 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 Настройте ACL для определения интересного трафика

Для определения интересного трафика, для которого будет применяться IPSec VPN, будет создан расширенный ACL. Расширенный ACL способен фильтровать 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 Настройте предложение IPSec VPN

Создайте предложение IPSec и введите представление предложение 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
```

Number of proposals: 1

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

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 подвергнут 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 Проверьте подключение между IP-сетями

Наблюдайте и проверяйте, 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 только интересный трафик будет защищен IPSec VPN.

```
<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
```

Финальная 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

```

Lab 3-5 Поддержка динамической маршрутизации с GRE

Цель обучения

В результате этой лабораторной вы должны выполнить следующие задачи:

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

Топология

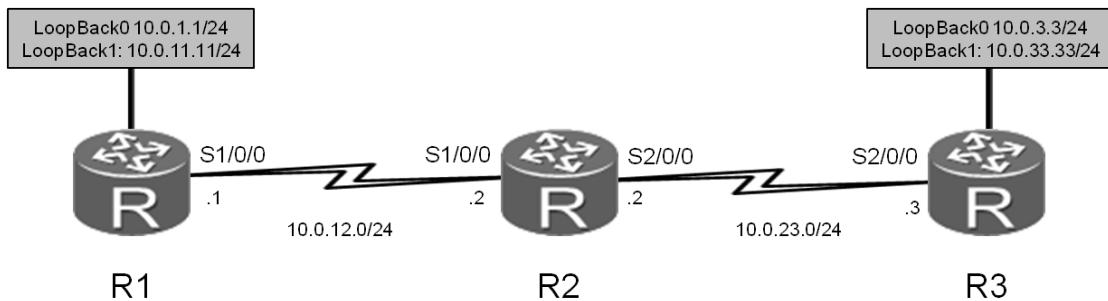


Рисунок 3.5 Динамическая маршрутизация с топологией GRE

Сценарий

Было выдвинуто требование о том, чтобы сети из других отделений рекламировались в штаб-квартире. После реализации решений IPSec VPN было обнаружено, что это невозможно. После некоторых консультаций администратору было рекомендовано внедрить зеленое решение по существующей сети IPSec, чтобы позволить корпоративным офисам действительно работать как единый административный домен.

Задачи

Примечание: Перед выполнением данной лабораторной работы, 3-4 лаб. работы должны быть сделаны

Шаг 1 Установите GRE трафик как интересный трафик

Перенастройте список управления доступом 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 Настройте туннельный интерфейс

Создайте туннельный интерфейс и укажите GRE в качестве типа инкапсуляции. Задайте адрес источника туннеля или исходный интерфейс и задайте 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 Настройте второй процесс OSPF для маршрутизации туннеля

Добавьте сеть туннельного интерфейса к процессу OSPF 1 и создайте второй экземпляр OSPF базы данных состояния канала (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 значимы только для локального маршрутизатора, поэтому позволяя маршрутам от OSPF LSDB 2 R1 и R3 достигать OSPF LSDB 1 R2.

Запустить `display interface Tunnel 0/0/1` чтобы проверить конфигурацию.

```

<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 Убедитесь, что маршруты переносятся через 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       Direct  0   0          D   127.0.0.1      Serial1/0/0
10.0.12.2/32       Direct  0   0          D   10.0.12.2     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	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	Direct	0	0	D	100.1.1.1	Tunnel0/0/1
100.1.1.1/32	Direct	0	0	D	127.0.0.1	Tunnel0/0/1
100.1.1.255/32	Direct	0	0	D	127.0.0.1	Tunnel0/0/1
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

<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	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	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	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
100.1.1.0/24	Direct	0	0	D	100.1.1.2	Tunnel0/0/1
100.1.1.2/32	Direct	0	0	D	127.0.0.1	Tunnel0/0/1
100.1.1.255/32	Direct	0	0	D	127.0.0.1	Tunnel0/0/1
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

После того, как туннель GRE настроен, маршрутизатор может обмениваться пакетами OSPF через туннель. Очистите статистику IPSec и проверьте 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 приветствия по IPSec, постепенное увеличение статистики esp IPSec проверяет это.

Шаг 5 Реализовать функцию поддержки активности на туннеле GRE

```

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

```

Проверьте, что функция поддержки активности была включена на туннельном интерфейсе.

```
<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 : --
```

Финальная 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 trnl
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

Lab 4-1 Внедрение IPv6-сетей и решений

Цель обучения

В результате этой лабораторной вы должны выполнить следующие задачи:

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

Топология

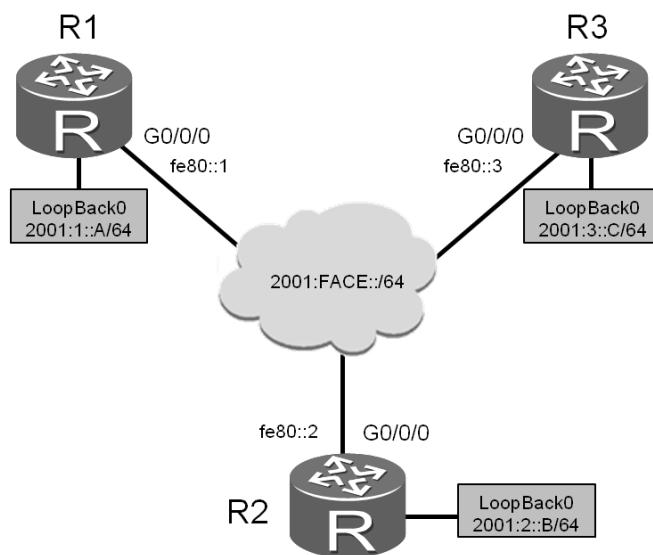


Рисунок 4.1 топология IPv6

Сценарий

В соответствии с планами по развертыванию решений для сетей следующего поколения, было решено, что корпоративная сеть должна реализовать дизайн IPv6 для существующей инфраструктуры. В качестве администратора вам было поручено реализовать схему адресации и маршрутизацию для IPv6, а также предоставить решения с отслеживанием состояния для IPv6.

Задачи

Шаг 1 Подготовка среды

Если Вы запускаете этот раздел с не сконфигурированного устройства, начинаете здесь и затем перемещаетесь в шаг 3. Для тех, которые продолжают из предыдущей лабораторной, начните с шага 2.

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

```
<huawei>system-view  
[huawei]sysname R2
```

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

Шаг 2 Настройка IPv6-адресации

Установите глобальную одноадресную адресацию IPv6 на интерфейсах обратной связи 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 рассылки для поддержки автоматической настройки адресов без состояния (SLAAC). Обнаружение дублирования адреса (DPD) обнаружения сети (ND) проверило, что локальный адрес ссылки уникален.

Шаг 3 Настройте OSPFv3

Включите процесс OSPFv3 и задайте его идентификатор маршрутизатора на R1, R2 и R3. OSPFv3 должен тогда 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 проверить, что пиринг ospfv3 был установлен.

```
<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 не является в настоящее время DR, следующая команда может использоваться для сброса процесса OSPFv3.

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

Проверьте подключение к локальному адресу одноранговой связи и глобальному одноадресному адресу интерфейсной обратной связи 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 Настройте DHCPv6 для распределения IPv6-адресов

Включите функцию сервера DHCPv6 на R2, чтобы устройствам можно было назначить 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 сервера DHCPv6 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 устройства могли получать 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, чтобы проверить информацию 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
(1): 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

```

Финальная 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
```