Динамическая маршрутизация на коммутаторах SNR

В рамках данной темы планируется написание цикла статей. Сегодня мы расскажем о динамической маршрутизации, которая используется практически в каждой более-менее крупной сети, будь то сеть предприятия или сеть провайдера.

В данной статье мы рассмотрим следующие вопросы:

- Что такое динамическая маршрутизация и для чего она используется.
- Протоколы динамической маршрутизации на коммутаторах SNR.
- Протокол OSPF и примеры настройки протокола OSPF на коммутаторах SNR.

Динамическая маршрутизация

Использование статической маршрутизации оправдано только в случае небольшого количества подсетей и полной уверенности в том, что конфигурация сети не будет меняться, ведь в случае изменений в сети необходимо реконфигурировать все маршруты вручную. Здесь и поможет применение одного (а то и нескольких) протоколов динамической маршрутизации, которые позволяют автоматически выстраивать и перестраивать маршруты в сети в случае аварий, при масштабировании сети, а также балансировке трафика.

OSPF

OSPF - протокол динамической маршрутизации, который описан в RFC_2328(V2) и RFC_5340(V3). Он используется для обмена маршрутной информацией в пределах одной автономной системы. OSPF является наиболее распространенным протоколом маршрутизации, который поддерживается практически любым оборудованием, в том числе и L2+ и L3 коммутаторами SNR. Транспортным протоколом для OSPF выступает протокол IP.

OSPF работает поверх протокола IP и использует мультикаст-адреса для обмена маршрутной информацией. Данные о маршрутах в протоколе OSPF передаются в виде сообщений LSA (Link State Advertisement). Маршрутизаторы OSPF хранят информацию о всех маршрутах сети в базе состояния каналов LSDB и выбирают из неё лучшие.

Полностью теорию работы в рамках этой статьи мы рассматривать не будем, OSPF довольно популярный протокол и о нем написано очень много материалов, которые можно легко найти в сети. Например здесь или здесь. Однако для понимания конфигурации нам потребуются некоторые понятия. Рассмотрим их дальше.

Типы маршрутизаторов в OSPF

Для начала необходимо обозначить какие типы маршрутизаторов бывают:

- Internal router - маршрутизатор, у которого все стыковочные интерфейсы находятся в одной зоне. Такой маршрутизатор не обменивается маршрутной информацией с другими AS и имеет одну LSDB.
- Area border router (ABR) - маршрутизатор, который находится на границе с магистральной зоной, и служит шлюзом для трафика, который проходит между зонами. Хотя бы один интерфейс такого маршрутизатора должен находиться в магистральной зоне. Для каждой зоны ABR имеет отдельную LSDB.
- Backbone router - магистральный маршрутизатор. Хотя бы один интерфейс такого маршрутизатора должен находиться в магистральной зоне. Внутренний маршрутизатор, у которого есть интерфейсы, принадлежащие нулевой зоне, тоже будет считаться магистральным. Может быть как ABR, так и не быть им.
- AS boundary router (ASBR) - такой маршрутизатор может обмениваться маршрутами с маршрутизаторами в других AS, или маршрутизаторами, использующими другой протокол маршрутизации. ASBR может быть в любом месте AS и являться как магистральным, так и внутренним или пограничным.

Типы зон OSPF

Разделение AS на зоны OSPF может снизить загрузку CPU маршрутизаторов, сократить размер LSDB и сократить количество пакетов LSA.

Зоны бывают следующих типов:

- Backbone (Area 0) - Магистральная зона OSPF. Это обычная зона, через которую происходят все взаимодействия между другими зонами.
- Normal - Зона с номером отличным от 0. Такой тип устанавливается по умолчанию, если в конфигурации не указан иной.
- Stub - Маршрутизаторы в такой зоне не принимают информацию об External-маршрутах, но принимают маршруты из других зон. Маршрутизатор в Stub-зоне не может выступать в качестве ASBR. Чтобы передавать трафик за границу AS, будет использован маршрут по умолчанию, транслируемый от ASR. Для настройки такого типа зон используется команда **area X stub**.
- Totally Stub - Stub-зона, которая принимает только маршрут по умолчанию. Для настройки такого типа зон используется команда **area X stub no-summary**.
- NSSA - Stub-зона, но маршрутизатор в такой зоне может выступать в качестве ASBR. Для трансляции External маршрутов используется LSA Type 7, которые трансформируются в LSA Type 5 на ASR. Для настройки такого типа зон используется команда **area X nssa**.
- Totally NSSA - Totally stub зона, но в ней может находиться ASBR. Имеет только маршрут по умолчанию. Для настройки такого типа зон используется команда **area X nssa no-summary**.

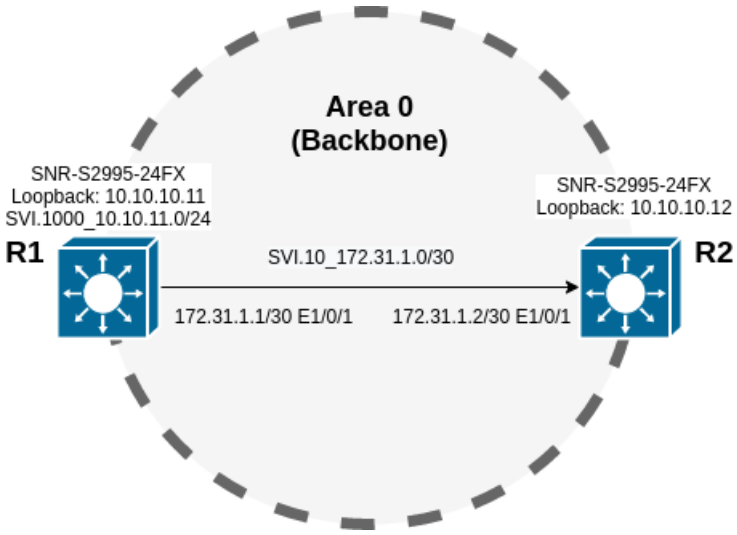
Базовая настройка OSPF

В качестве первого примера рассмотрим случай, если у нас всего одна магистральная зона (Area 0).

Допустим, у нас имеются коммутаторы SNR-S2995G-24FX, которые используются на уровне агрегации в сети оператора связи. На R1 терминируются клиенты с подсетью 10.10.11.0/24, которую мы хотим анонсировать и передать на BRAS, а также хотим, чтобы между коммутаторами была L3-связность.

Для такой ситуации оправдано применение протокола OSPF, т.к. количество коммутаторов и подсетей будет расти в будущем. Сложность масштабируемости и настройки статической адресации также будут быстро увеличиваться. В случае применения OSPF нам необходимо лишь выполнить первоначальную настройку и в будущем OSPF будет самостоятельно анонсировать добавленные подсети (добавленные на SVI подсети будут иметь тип Connected. Для того, чтобы OSPF перекладывал маршруты из Connected в OSPF, необходимо применить команду **redistribute connected**. Это мы рассмотрим во втором примере данной статьи).

В нашем примере схема будет выглядеть следующим образом:



Конфигурация R1:

```
conf t
vlan 10;3000
interface vlan 10
 ip address 172.31.1.1 255.255.255.252
!
interface vlan 1000
 ip address 10.10.11.1 255.255.255.0
!
interface Loopback1
 ip address 10.10.10.11 255.255.255.255
!
```

```
interface E1/0/1
 switchport access vlan 10
!
router ospf 1
 ospf router-id 10.10.10.11
 network 172.31.1.0/30 area 0
 network 10.10.11.0/24 area 0
 network 10.10.10.11/32 area 0
end
```

Конфигурация R2:

```
conf t
vlan 10
interface vlan 10
 ip address 172.31.1.2 255.255.255.252
!
interface Loopback1
 ip address 10.10.10.12 255.255.255.255
!
interface E1/0/1
 switchport access vlan 10
!
router ospf 1
 ospf router-id 10.10.10.12
 network 172.31.1.0/30 area 0
 network 10.10.10.12/32 area 0
end
```

После применения конфигурации, приведенной выше, коммутаторы устанавливают OSPF-соседство, IP-адреса Loopback-интерфейсов и подсети с SVI 3000 с R1 передаются на R2. Начинается процесс установления соединения, который должен пройти через следующие этапы:

1. DOWN - начальное состояние;
2. Init - после отправки Hello другому коммутатору, он ожидает от другого коммутатора свой hello. В этот момент он находится в состоянии Init;
3. Full - когда коммутаторы получили всю информацию и LSDB синхронизирована, оба коммутатора переходят в состояние fully adjacent (FULL).

Убедимся, что соседство установилось и подсети R1 доступны через R2 и наоборот:

```
R1#sh ip ospf neighbor

OSPF process 1:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.12       1   Full/DR         00:00:31    172.31.1.2      Vlan10
```

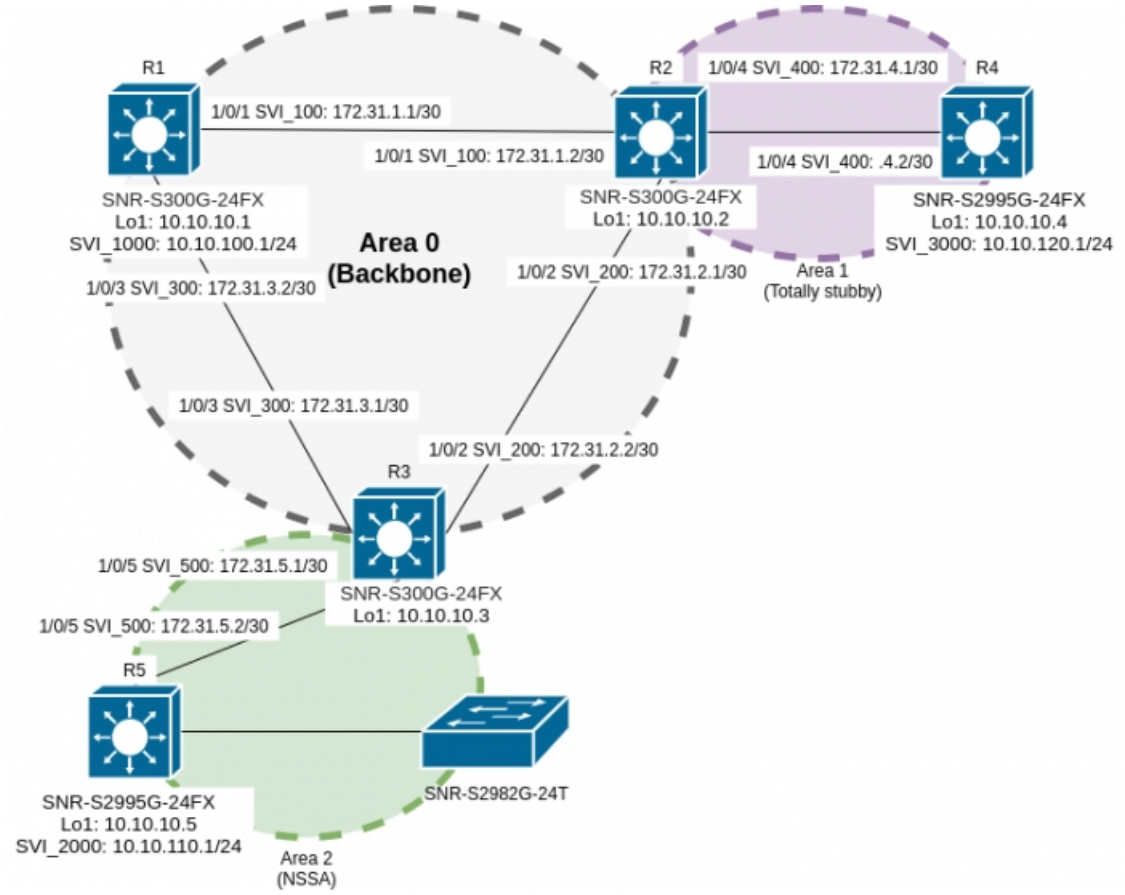
Как мы видим, соседство установилось и был выбран DR. В нашем случае, R2.

```
R2#sh ip ospf neighbor

OSPF process 1:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.11       1   Full/Backup     00:00:33    172.31.1.1      Vlan10

R2#sh ip route ospf
O       10.10.10.11/32 [110/2] via 172.31.1.1, Vlan10, 00:04:56  tag:0
O       10.10.11.0/24 [110/2] via 172.31.1.1, Vlan10, 00:01:24  tag:0
Total routes are : 2 item(s)
```

То же мы видим и на R2. Адрес Loopback1 и клиентская подсеть доступны с R2.

Настройка OSPF с использованием нескольких зон

Производительность коммутаторов ограничена. Размеры LSDB могут достигать размеров в тысячи маршрутов, при этом коммутатор тратит много ресурсов на просмотр своей таблицы маршрутизации, а если учесть, что помимо OSPF коммутатор должен обрабатывать и другие задачи, загрузка CPU может достигать критически высоких значений, что скажется на производительности коммутатора. В таких случаях целесообразно применение деления на зоны, которые помогут уменьшить количество маршрутов в LSDB, тем самым снизив нагрузку на CPU. Давайте рассмотрим пример использования NSSA и Totally Stubby area на следующей схеме:



R1:

```
vlan 1;100;300;1000
Interface Ethernet1/0/1
 description R2
 switchport discard packet untag
 switchport mode trunk
 switchport trunk allowed vlan 100
!
Interface Ethernet1/0/3
 description R3
 switchport discard packet untag
 switchport mode trunk
 switchport trunk allowed vlan 300
!
interface Vlan100
 ip address 172.31.1.1 255.255.255.252
!
interface Vlan300
 ip address 172.31.3.2 255.255.255.252
!
interface Vlan1000
 ip address 10.10.100.1 255.255.255.0
!
interface Loopback1
 ip address 10.10.10.1 255.255.255.255
!
router ospf 1
 ospf router-id 10.10.10.1
 passive-interface Vlan1000
 network 172.31.1.0/30 area 0
 network 172.31.3.0/30 area 0
 redistribute connected
!
```

R2:

```
vlan 1;100;200;400
!
Interface Ethernet1/0/1
 description R1
 switchport discard packet untag
 switchport mode trunk
 switchport trunk allowed vlan 100
!
Interface Ethernet1/0/2
 description R3
 switchport discard packet untag
 switchport mode trunk
 switchport trunk allowed vlan 200
!
Interface Ethernet1/0/4
 description R4
 switchport discard packet untag
 switchport mode trunk
 switchport trunk allowed vlan 400
!
interface Vlan100
 ip address 172.31.1.2 255.255.255.252
!
interface Vlan200
 ip address 172.31.2.1 255.255.255.252
!
interface Vlan400
 ip address 172.31.4.1 255.255.255.252
!
interface Loopback1
 ip address 10.10.10.2 255.255.255.255
!
router ospf 1
 ospf router-id 10.10.10.2
 area 1 stub no-summary
 network 172.31.1.0/30 area 0
 network 172.31.2.0/30 area 0
 network 172.31.4.0/30 area 1
 redistribute connected
!
```

R3:

```
vlan 1;200;300;500
!
Interface Ethernet1/0/2
 description R2
 switchport discard packet untag
 switchport mode trunk
 switchport trunk allowed vlan 200
!
Interface Ethernet1/0/3
 description R1
 switchport discard packet untag
 switchport mode trunk
 switchport trunk allowed vlan 300
!
Interface Ethernet1/0/5
 description R5
 switchport discard packet untag
 switchport mode trunk
 switchport trunk allowed vlan 500
!
interface Vlan200
 ip address 172.31.2.2 255.255.255.252
!
interface Vlan300
 ip address 172.31.3.1 255.255.255.252
!
```

```
interface Vlan500
 ip address 172.31.5.1 255.255.255.252
!
interface Loopback1
 ip address 10.10.10.3 255.255.255.255
!
router ospf 1
 ospf router-id 10.10.10.3
 area 2 nssa default-information-originate
 network 172.31.2.0/30 area 0
 network 172.31.3.0/30 area 0
 network 172.31.5.0/30 area 2
 redistribute connected
!
```

R4:

```
vlan 1;400;3000
!
interface Vlan400
 ip address 172.31.4.2 255.255.255.252
!
interface Vlan3000
 ip address 10.10.120.1 255.255.255.0
!
Interface Ethernet1/0/4
 description R2
 switchport discard packet untag
 switchport mode trunk
 switchport trunk allowed vlan 400
!
interface Loopback1
 ip address 10.10.10.4 255.255.255.255
!
router ospf 1
 ospf router-id 10.10.10.4
 passive-interface Vlan3000
 area 1 stub
 network 10.10.10.4/32 area 1
 network 10.10.120.0/24 area 1
 network 172.31.4.0/30 area 1
!
```

R5:

```
vlan 1;500;2000
!
Interface Ethernet1/0/5
 description R3
 switchport discard packet untag
 switchport mode trunk
 switchport trunk allowed vlan 500;2000
!
interface Vlan500
 ip address 172.31.5.2 255.255.255.252
!
interface Vlan2000
 ip address 10.10.110.1 255.255.255.0
!
interface Loopback1
 ip address 10.10.10.5 255.255.255.255
!
router ospf 1
 ospf router-id 10.10.10.5
 passive-interface Vlan2000
 area 2 nssa
 network 172.31.5.0/30 area 2
 redistribute connected
!
```

На данной схеме приведена сеть, в которой используется как Totally stubby (R2-R4), так и NSSA (R3-R5) зоны.

Внешние маршруты других зон в NSSA (R5) будут заменены на маршрут по умолчанию.

Для Totally stubby-зоны (R4) все маршруты будут заменены на маршрут по умолчанию.

Для анонса сетей, находящихся в Totally stubby зоне, необходимо указать их в Router OSPF.

Для анонса адресов Loopback в Area 0 используем команду **redistribute connected**. Это позволит нам не только упростить конфигурацию, но и сократить количество маршрутов, которые будут анонсироваться в другие типы зон, так как такие маршруты будут считаться External.

Для того, чтобы коммутаторы не искали соседей за SVI, на котором находятся клиентские подсети, применим команду **passive-interface**. Для R2 также применим команду **redistribute connected metric-type 1** для того, чтобы увидеть разницу в типе метрик.

Посмотрим на таблицу маршрутов OSPF для маршрутизатора R1:

```
R1#sh ip route ospf
O E1    10.10.10.2/32 [110/21] via 172.31.1.2, Vlan100, 00:01:52  tag:0
O E2    10.10.10.3/32 [110/20] via 172.31.3.1, Vlan300, 00:01:52  tag:0
O IA    10.10.10.4/32 [110/3] via 172.31.1.2, Vlan100, 00:01:53  tag:0
O E2    10.10.10.5/32 [110/20] via 172.31.3.1, Vlan300, 00:01:52  tag:0
O E2    10.10.110.0/24 [110/20] via 172.31.3.1, Vlan300, 00:01:52  tag:0
O IA    10.10.120.0/24 [110/3] via 172.31.1.2, Vlan100, 00:01:53  tag:0
O       172.31.2.0/30 [110/2] via 172.31.1.2, Vlan100, 00:01:53  tag:0
                      [110/2] via 172.31.3.1, Vlan300, 00:01:53  tag:0
O IA    172.31.4.0/30 [110/2] via 172.31.1.2, Vlan100, 00:01:53  tag:0
O IA    172.31.5.0/30 [110/2] via 172.31.3.1, Vlan300, 00:01:53  tag:0
Total routes are : 10 item(s)
```

В данной таблице мы видим все маршруты, которые анонсируются на R1 путем OSPF. Маршруты до Loopback-адресов R2, R3 и R5 анонсируются как "E" (LSA Type 5), то есть, получены путем перекладывания маршрутов из другого протокола маршрутизации (в нашем случае из connected). Цифра 1 или 2 после буквы "E" показывает на тип метрики. 1 тип увеличивает метрику маршрута при расчете SPF, а 2 тип нет:

```
R1#sh ip route 10.10.10.2/32
Routing entry for 10.10.10.2/32
  Known via "ospf", distance 110, metric 21, best
  Last update 00:07:52 ago
  * 172.31.1.2, via Vlan100


R1#sh ip route 10.10.10.3/32
Routing entry for 10.10.10.3/32
  Known via "ospf", distance 110, metric 20, best
  Last update 01:32:18 ago
  * 172.31.3.1, via Vlan300
```

Давайте посмотрим на таблицу маршрутизации OSPF на R2 и R4:

```
R2#sh ip route ospf
O E2    10.10.10.1/32 [110/20] via 172.31.1.1, Vlan100, 02:09:49  tag:0
O E2    10.10.10.3/32 [110/20] via 172.31.2.2, Vlan200, 02:09:14  tag:0
O       10.10.10.4/32 [110/2] via 172.31.4.2, Vlan400, 00:13:54  tag:0
O E2    10.10.10.5/32 [110/20] via 172.31.2.2, Vlan200, 00:02:44  tag:0
O E2    10.10.100.0/24 [110/20] via 172.31.1.1, Vlan100, 00:11:24  tag:0
O E2    10.10.110.0/24 [110/20] via 172.31.2.2, Vlan200, 00:02:48  tag:0
O       10.10.120.0/24 [110/2] via 172.31.4.2, Vlan400, 01:53:08  tag:0
O       172.31.3.0/30 [110/2] via 172.31.1.1, Vlan100, 03:15:38  tag:0
                      [110/2] via 172.31.2.2, Vlan200, 03:15:38  tag:0
O IA    172.31.5.0/30 [110/2] via 172.31.2.2, Vlan200, 02:44:01  tag:0
Total routes are : 10 item(s)
```

```
R4#sh ip route ospf
O*IA    0.0.0.0/0 [110/2] via 172.31.4.1, Vlan400, 02:17:02  tag:0
Total routes are : 1 item(s)
```

Здесь мы наглядно видим зачем в принципе используются Totally stub - зоны. Вместо десятков

маршрутов для нас доступен всего один - маршрут по умолчанию (для того, чтобы R2 анонсировал только маршрут по умолчанию, используем команду **area 1 stub no-summary**). Несмотря на то, что маршрут всего один, все маршрутизаторы и сети доступны:

```
R4#ping 10.10.10.1
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/13/50 ms
R4#ping 10.10.10.2
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/6/33 ms
R4#ping 10.10.10.3
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.10.10.3, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/6/33 ms
R4#ping 10.10.10.5
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.10.10.5, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/9/33 ms
R4#ping 10.10.100.1
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.10.100.1, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/6/16 ms
R4#ping 10.10.110.1
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.10.110.1, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/6/33 ms
```

R4 не может генерировать LSA Type 5, так как находится в stub-зоне. Адрес Loopback и подсети, подключенные к R4 указаны вручную командой **network**.

Давайте посмотрим что у нас в NSSA на R5:

```
R5#sh ip route ospf
O*N2    0.0.0.0/0 [110/1] via 172.31.5.1, Vlan500, 01:12:47  tag:0
O N2    10.10.10.3/32 [110/20] via 172.31.5.1, Vlan500, 01:12:47  tag:0
O IA    10.10.10.4/32 [110/4] via 172.31.5.1, Vlan500, 00:14:54  tag:0
O IA    10.10.120.0/24 [110/4] via 172.31.5.1, Vlan500, 01:12:48  tag:0
O IA    172.31.1.0/30 [110/3] via 172.31.5.1, Vlan500, 01:12:48  tag:0
O IA    172.31.2.0/30 [110/2] via 172.31.5.1, Vlan500, 01:12:48  tag:0
O IA    172.31.3.0/30 [110/2] via 172.31.5.1, Vlan500, 01:12:48  tag:0
O IA    172.31.4.0/30 [110/3] via 172.31.5.1, Vlan500, 01:12:48  tag:0
Total routes are : 8 item(s)
```

Как мы видим, маршруты, которые были redistribute, на R5 не попали, но они доступны через default, анонсируемый R3. Для того, чтобы R3 передавал информацию о маршруте по умолчанию мы применили команду **area 2 nssa default-information-originate**.

```
R5#ping 10.10.100.1
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.10.100.1, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/6/33 ms
R5#ping 10.10.10.1
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
R5#ping 10.10.120.1
Type ^c to abort.
Sending 5 56-byte ICMP Echos to 10.10.120.1, timeout is 2 seconds.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Так как R5 находится в NSSA, то он может выступать в качестве ASBR, а также перекладывать маршруты из других протоколов маршрутизации. Это значит, что в NSSA могут находится External-маршруты в виде специального LSA Type 7, который может находиться только в NSSA. На границе зоны пограничный коммутатор преобразует LSA Type 7 в LSA Type 5.

Для фильтрации маршрутов можно также воспользоваться функционалом ACL. Например, если на коммутаторе в NSSA-зоне мы хотим принимать только маршрут по умолчанию и маршруты из подсети 172.31.0.0/16, то необходимо создать ACL на R5 типа:

```
access-list 100 permit ip host-source 0.0.0.0 any-destination
access-list 100 permit ip 172.31.0.0 0.0.255.255 any-destination
access-list 100 permit ospf host-source 0.0.0.0 any-destination
access-list 100 permit ospf 172.31.0.0 0.0.255.255 any-destination
access-list 100 deny ospf any-source any-destination
access-list 100 deny ip any-source any-destination
!
router ospf 1
 filter-policy 100
!
```

В таком случае таблица маршрутов будет иметь следующий вид:

```
R5#sh ip route ospf
O*N2    0.0.0.0/0 [110/1] via 172.31.5.1, Vlan500, 00:02:03  tag:0
O IA    172.31.1.0/30 [110/3] via 172.31.5.1, Vlan500, 00:02:04  tag:0
O IA    172.31.2.0/30 [110/2] via 172.31.5.1, Vlan500, 00:02:04  tag:0
O IA    172.31.3.0/30 [110/2] via 172.31.5.1, Vlan500, 00:02:04  tag:0
O IA    172.31.4.0/30 [110/3] via 172.31.5.1, Vlan500, 00:02:04  tag:0
Total routes are : 5 item(s)
```

Количество маршрутов сократилось, но все адреса Loopback и подсетей доступны через маршрут по умолчанию.

Заключение

В данной статье мы рассмотрели принципы работы протокола OSPF и его настройке на коммутаторах SNR. В будущем также планируется выход второй части данной статьи, посвященный протоколу BGP.