IPv4/IPv6 Dual Stack на коммутаторах SNR

Введение

В прошлой статье мы поговорили про теоретическую часть протокола IPv6, а также познакомились с его базовыми настройками на коммутаторах доступа SNR. Теперь мы затронем более практические для операторов вещи - DHCPv6 и Dual Stack. Не секрет, что никто не предоставляет абонентам только IPv6-адрес, это всегда идет в связке с IPv4-адресом. Об этом и поговорим.

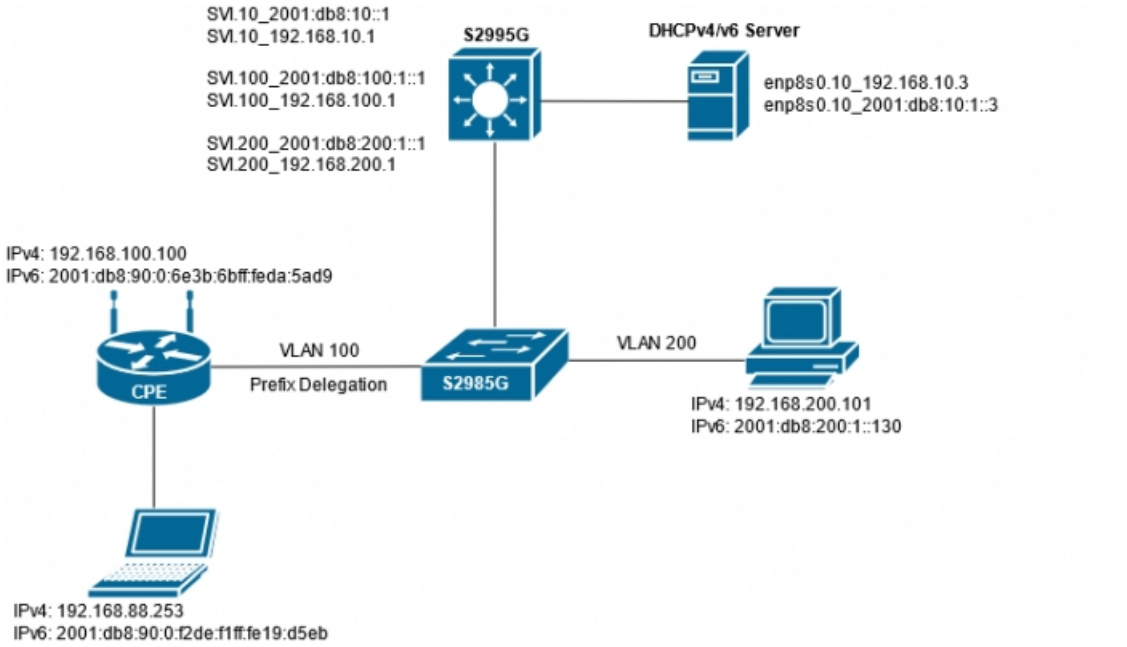
Описание стенда Dual Stack

На тестовом стенде мы разберем настройки коммутаторов SNR для авторизации IPv6-абонентов с использованием опций 37 (remote-id), 38 (subscriber-id), безопасность и конфигурацию DHCP-сервера для выдачи IPv6-адресов.

Еще раз отметим, что все управляемые коммутаторы доступа SNR, от FastEthernet-моделей, таких как SNR-S2962-24T, до гигабитных коммутаторов с 10G-аплинками (SNR-S2989G-24TX), поддерживают одинаковый функционал и имеют одинаковые настройки в части IPv6.

Наш стенд будет представлять из себя:

- Домашний Wi-Fi-маршрутизатор (CPE).
- Коммутатора доступа (SNR-S2985G-24TC).
- Коммутатор агрегации третьего уровня (SNR-S2995G-24FX).
- DHCPv4/v6-сервер (ISC-DHCP).



Рассмотрим стенд Dual Stack. Коммутатор доступа SNR-S2985G-24TC будет использоваться для подключения абонентов, как через домашний Wi-Fi-маршрутизатор, методом Prefix Delegation, так и напрямую. Для выделения IPv6-префикса и IPv6-адресов будут использоваться опции 37 (remote-id) и 38 (subscriber-id). Для выделения IPv4-адресов будем использовать классическую опцию 82.

Для защиты от нелегитимных DHCP-серверов и подмены IP-адреса, в случае с IPv4 будет использоваться DHCP snooping binding. Коммутаторы SNR имеют несколько механизмов защиты протокола IPv6. Например, Security RA блокирует RA-сообщения от недоверенных портов. ND Security позволяет влиять на автоматическое изучение ND-записей (аналог ARP Security). В нашем примере будет использоваться SAVI (Source Address Validation Improvement), который включает в себя ND Snooping, DHCPv6 Snooping и RA Snooping. Мы будем защищаться от нелегитимных DHCP-серверов и источников RA-сообщений с помощью trust-портов. Выдаваемые IPv6-адреса и префиксы будут привязываться к binding-таблице. Мы также будем задавать максимальное количество адресов на порт.

Коммутатор агрегации SNR-2995G-24FX, в качестве IPv6-роутера, будет рассылать RA-сообщения с M-флагом в своем сегменте сети, чтобы клиенты могли знать, каким образом формировать их IPv6-адрес. Также, на SNR-2995G-24FX будут присутствовать L3-интерфейсы в клиентских VLAN, с которых он будет осуществлять релей в VLAN DHCP-сервера.

Сервер ISC-DHCP будет выделять адреса и префиксы согласно классам.

Настройка и проверка стенда

Далее будут приведены минимально необходимые конфигурации с пояснениями некоторых настроек. Некоторые из них были описаны в прошлой статье.

Настройка коммутатора SNR-S2985G-24TC

```
ip dhcp snooping enable
ip dhcp snooping vlan 100;200
 ip dhcp snooping binding enable
!
 ip dhcp snooping information enable
 ip dhcp snooping information option subscriber-id format hex
!
savi enable
 savi ipv6 dhcp-slaac enable
 savi check binding probe mode
!
ipv6 dhcp snooping vlan 100;200
ipv6 dhcp snooping remote-id option #включаем добавление опции 37
ipv6 dhcp snooping subscriber-id option #включаем добавление опции 38
ipv6 dhcp snooping mode relay #задаем отправку опций в RELAY-FORWARD сообщениях
!
vlan 1;100;200
!
Interface Ethernet1/0/1
 switchport access vlan 100
 ip dhcp snooping binding user-control
 ip dhcp snooping binding user-control max-user 10
 savi ipv6 check source ip-address mac-address #включаем проверку IP и MAC адресов
 savi ipv6 binding num 10
!
Interface Ethernet1/0/2
 switchport access vlan 200
 ip dhcp snooping binding user-control
 ip dhcp snooping binding user-control max-user 10
 savi ipv6 check source ip-address mac-address
 savi ipv6 binding num 10
!
Interface Ethernet1/0/24
 switchport mode trunk
 switchport trunk allowed vlan 100;200
 ip dhcp snooping trust
 ipv6 dhcp snooping trust #назначаем trust-порт для DHCPv6 пакетов
 ipv6 nd snooping trust #назначаем trust-порт для ND-RA пакетов
```

Настройка коммутатора SNR-2995G-24FX

```
service dhcp
!
ip forward-protocol udp bootps
!
service dhcpv6
!
vlan 1;10;100;200
!
Interface Ethernet1/0/1
 switchport mode trunk
 switchport trunk allowed vlan 100;200
!
Interface Ethernet1/0/12
 switchport mode trunk
 switchport trunk allowed vlan 10
!
interface Vlan10
```

```
 ipv6 address 2001:db8:10:1::1/64
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan100
 ipv6 address 2001:db8:100:1::1/64
 no ipv6 nd suppress-ra #разрешаем рассылать RA-сообщения с этого L3-интерфейса
 ipv6 nd min-ra-interval 60 #задаем минимальный интервал рассылки RA
 ipv6 nd max-ra-interval 120 #задаем максимальный интервал рассылки RA
 ipv6 nd managed-config-flag #задаем M-флаг
 ipv6 nd prefix 2001:db8:100:1::/64 2592000 604800 no-autoconfig #отключаем A-флаг в RA-сообщениях
 ip address 192.168.100.1 255.255.255.0
 ip helper-address 192.168.10.3
 ipv6 dhcp relay destination 2001:db8:10:1::3
!
interface Vlan200
 ipv6 address 2001:db8:200:1::1/64
 no ipv6 nd suppress-ra
 ipv6 nd min-ra-interval 60
 ipv6 nd max-ra-interval 120
 ipv6 nd managed-config-flag
 ipv6 nd prefix 2001:db8:200:1::/64 2592000 604800 no-autoconfig
 ip address 192.168.200.1 255.255.255.0
 ip helper-address 192.168.10.3
 ipv6 dhcp relay destination 2001:db8:10:1::3
```

На нашем стенде мы будем запускать два экземпляра сервера ISC-DHCP - DHCPv4 и DHCPv6. По этой причине и файлов конфигураций будет два. Конфигурационный файл для DHCPv4 уже был описан в статье.

ISC-DHCP-Server. /etc/dhcp/dhcpd4.conf:

```
default-lease-time 120;
max-lease-time 240;
if exists agent.remote-id {log ( info, concat(
     "Switch MAC: ", binary-to-ascii(16, 8, ":", option agent.remote-id),
    " Switch port: ", binary-to-ascii(10, 8, ".", option agent.circuit-id)
  ));
}
class "sw1-1" {
match if binary-to-ascii(16, 8, ":", suffix(option agent.remote-id ,6))="f8:f0:82:78:5:ba"
and
binary-to-ascii(10, 8,"", suffix(option agent.circuit-id, 1))="1";
}
class "sw1-2" {
match if binary-to-ascii(16, 8, ":", suffix(option agent.remote-id ,6))="f8:f0:82:78:5:ba"
and
binary-to-ascii(10, 8,"", suffix(option agent.circuit-id, 1))="2";
}
shared-network test{
    subnet 192.168.10.0 netmask 255.255.255.0 {}
    subnet 192.168.100.0 netmask 255.255.255.0 {
       option subnet-mask 255.255.255.0;
       option routers 192.168.100.253;
       authoritative;
       default-lease-time 120;
       max-lease-time 240;
            pool {range 192.168.100.100 192.168.100.130; allow members of "sw1-1";}
    }
    subnet 192.168.200.0 netmask 255.255.255.0 {
       option subnet-mask 255.255.255.0;
       option routers 192.168.200.253;
       authoritative;
       default-lease-time 120;
       max-lease-time 240;
            pool {range 192.168.200.100 192.168.200.130; allow members of "sw1-2";}
}
}
```

Приступим к конфигурационному файлу для DHCPv6, здесь уже появляются новые элементы, требующие пояснений.

ISC-DHCP-Server. /etc/dhcp/dhcpd6.conf:

```
default-lease-time 120;
max-lease-time 240;
#Делаем наглядный разделитель с перечислением распознанных опций, например:
#Remote-ID: f8-f0-82-78-05-ba | Subscriber-ID: vlan200+Ethernet1/0/2
log(info, (concat(
"Remote-ID: ", (substring(v6relay(1, option dhcp6.remote-id), 4, 17)),
" | Subscriber-ID: ", v6relay(1, option dhcp6.subscriber-id)
    )));
#Создаем класс "sw1-1", который сверяет DHCPv6-RELAY опции 37 и 38.
class "sw1-1" {
        match if(
                (substring (v6relay(1, option dhcp6.remote-id), 4, 17) = "f8-f0-82-78-05-ba") and
               (v6relay(1, option dhcp6.subscriber-id) = "vlan100+Ethernet1/0/1")
);
}
class "sw1-2" {
        match if(
                (substring (v6relay(1, option dhcp6.remote-id), 4, 17) = "f8-f0-82-78-05-ba") and
                (v6relay(1, option dhcp6.subscriber-id) = "vlan200+Ethernet1/0/2")
);
}
subnet6 2001:db8:100:1::/64 {
pool6 {
#Задаем диапазон префиксов, выдаваемых CPE.
        prefix6 2001:db8:80:: 2001:db8:90:: /56;
        range6 2001:db8:100:1::100 2001:db8:100:1::130;
        option dhcp6.name-servers 2001:db8:10:1::88;
        option dhcp6.domain-search "domain.example";
        allow members of "sw1-1";
}
}
subnet6 2001:db8:200:1::/64 {
pool6 {
        range6 2001:db8:200:1::100 2001:db8:200:1::130;
        option dhcp6.name-servers 2001:db8:10:1::88;
        option dhcp6.domain-search "domain.example";
        allow members of "sw1-2";
}
}
subnet6 2001:db8:10:1::/64 {}
```

Для каждого протокола будем запускать отдельный экземпляр ISC-DHCP с соответствующим файлом конфигурации:

```
/usr/sbin/dhcpd -4 -d -cf /etc/dhcp/dhcpd4.conf enp8s0.10
/usr/sbin/dhcpd -6 -d -cf /etc/dhcp/dhcpd6.conf enp8s0.10
```

Проверим, корректно ли отрабатывают технологии DHCP Snooping и SAVI на одном коммутаторе доступа одновременно:

```
ip dhcp snooping static binding count:0, dynamic binding count:2
MAC                IP address          Interface           Vlan ID   Flag
-------------------------------------------------------------------------
6c-3b-6b-da-5a-d8   192.168.100.100     Ethernet1/0/1       100       DOL
f0-de-f1-19-d5-eb   192.168.100.101     Ethernet1/0/2       200       DOL
-------------------------------------------------------------------------
SNR-S2985G-24T-UPS#sh savi ipv6 check source binding
Static binding count: 0
Dynamic binding count: 4
Binding count: 2
MAC               IP                                  VLAN Port            Type    State     Expires
-------------------------------------------------------------------------------------------------------
6c-3b-6b-da-5a-d8  fe80::6e3b:6bff:feda:5ad8              100  Ethernet1/0/1    slaac   BOUND     14008
6c-3b-6b-da-5a-d8  2001:db8:90::/56                       100  Ethernet1/0/1    dhcp    BOUND     83
```

```
f0-de-f1-19-d5-eb  fe80::f2de:f1ff:fe19:d5eb          200  Ethernet1/0/2    slaac   BOUND     5
f0-de-f1-19-d5-eb  2001:db8:100:1::130                200  Ethernet1/0/2    dhcp    BOUND     94
-----------------------------------------------------------------------------------------------------------
```

Для порта Ethernet1/0/1 в VLAN 100 видим выданный CPE префикс. Для порта Ethernet1/0/2 в VLAN 200 - IPv6-адрес, полученный stateful методом.

Посмотрим как выглядят полученные сетевые реквизиты на одном из клиентов:

```
[root@manjaro ~]$ ip add show enp3s0
2: enp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether f0:de:f1:19:d5:eb brd ff:ff:ff:ff:ff:ff
   inet 192.168.200.101/24 brd 192.168.200.255 scope global dynamic noprefixroute enp3s0
      valid_lft 170sec preferred_lft 170sec
   inet6 2001:db8:200:1::130/128 scope global dynamic noprefixroute
      valid_lft 76sec preferred_lft 31sec
   inet6 fe80::f2de:f1ff:fe19:d5eb/64 scope link noprefixroute
      valid_lft forever preferred_lft forever
```

Проверим информацию о маршрутах:

```
[root@manjaro ~]$ ip -4 route
default via 192.168.200.1 dev enp3s0 proto dhcp metric 20100
192.168.200.0/24 dev enp3s0 proto kernel scope link src 192.168.200.101 metric 100
[root@manjaro ~]$ ip -6 route
::1 dev lo proto kernel metric 256 pref medium
2001:db8:200:1::130 dev enp3s0 proto kernel metric 100 pref medium
2001:db8:200:1::/64 dev enp3s0 proto ra metric 100 pref medium
fe80::/64 dev enp3s0 proto kernel metric 100 pref medium
default via fe80::faf0:82ff:fe7a:2afb dev enp3s0 proto ra metric 20100 pref medium
```

Как и было описано в первой статье, шлюзом по умолчанию для IPv6-хоста является link-local адрес маршрутизатора, от которого было получено RA-сообщение.

Заключение

Подведем итог. Мы рассмотрели один из сценариев настройки Dual Stack на коммутаторах SNR, делается это довольно просто. На тестовом стенде проверили работоспособность одновременного использования IPv4, IPv6 и связанных с ними технологий. Если статья вызовет достаточный интерес, то можно будет ожидать третью часть про настройку IPv6-маршрутизации на коммутаторах агрегации и ядра SNR.

По всем вопросам, в том числе предоставления скидок, вы можете обратиться к вашему менеджеру. Напоминаем, что у нас есть Telegram-канал, а также обновленная база знаний.