BNG Juniper - PPPoE

WZTECH®
networks

Revisão 1
22/09/2023

WZTECH®
networks

1. Introdução

Este documento produzido pela WZTECH Networks tem como objetivo documentar as configurações de BNG nos roteadores do fabricante Juniper para o modelo de conexão utilizando o protocolo PPPoE. Todas as informações contidas neste documento foram validadas no roteador MX204 utilizando o JunOS versão 21.4R3-S4. A versão atual recomendada deve ser sempre validada com a WZTECH antes de subir o BNG em produção.

2. Configuração Geral no BNG para ativar o serviço de Subscriber (PPPoE)

Por default o serviço de BNG não fica ativo nos roteadores:

```
admin@MX204-LAB-WZTECH> show system subscriber-management statistics
subscriber-management not enabled
command not supported
```

É necessário ativar o serviço com o comando:

```
set system services subscriber-management enable
```

Este comando habilita o serviço de BNG no MX

```
set system configuration-database max-db-size 314572800
```

Este commando ajusta o tamanho da memória compartilhada do BNG. No caso do MX204 e MX10003 a recomendação é 314572800 (314MB de memória)

Quando é feito o commit é gerado um warning informando que é obrigatório reiniciar a caixa para ativar o serviço de BNG:

```
    warning: Chassis configuration for subscriber-management has been changed. A system reboot is mandatory.  Please
reboot the system NOW. Continuing without a reboot might result in unexpected system behavior.
commit complete
```

Se não for feito o reboot, mesmo com o comando aplicado o output printado acima vai continuar da mesma forma e o serviço de BNG continuará sem funcionar.

Quando o BNG é reiniciado com as configurações a caixa a partir deste momento terá o serviço de subscriber-management ativo. Para validar que está ativo:

```
admin@MX204-LAB-WZTECH> show system subscriber-management statistics
Session Manager started @ Thu Jul 20 13:55:45 2023
Session Manager cleared @ Thu Jul 20 13:55:45 2023
------------------------------------------------------------
                    Packet Statistics
------------------------------------------------------------
I/O Statistics:
------------------------------------------------------------
    Rx Statistics
        packets                         : 0
    Tx Statistics
        packets                         : 0
  Layer 3 Statistics
    Rx Statistics
        packets                         : 0
    Tx Statistics
        packets                         : 0
```

O BNG mostra o output com linhas de estatísticas quando o serviço está ativo.

3. Deletar Configurações Default do MX - Traceoptions DHCP

```
set system processes dhcp-service traceoptions file dhcp_logfile
set system processes dhcp-service traceoptions file size 10m
set system processes dhcp-service traceoptions level all
set system processes dhcp-service traceoptions flag packet
```

Por default o MX vem com a configuração de traceoptions para fazer debug do protocolo DHCP. Como o BNG terá o DHCPv6 como serviço para os assinantes (IA_NA e/ou IA_PD) e não apenas para obter algum IPv6 local

é recomendado deletar essa configuração de traceoptions para não ficar consumindo recursos desnecessários da Routing Engine. O traceoptions pode ser configurado quando for necessário para troubleshooting.

```
[edit]
admin@MX204-LAB-WZTECH# delete system processes dhcp-service traceoptions

[edit]
admin@MX204-LAB-WZTECH# commit and-quit
commit complete
Exiting configuration mode
```

4. Licenças

Por default o BNG vem com uma licença básica que permite até 10 conexões de assinantes no equipamento:

```
admin@MX204-LAB-WZTECH> show system license
License usage:
                              Licenses     Licenses    Licenses    Expiry
  Feature name                    used    installed      needed
  subscriber-accounting              1            0           1    29 days
  subscriber-authentication          1            0           1    29 days
  subscriber-address-assignment      1            0           1    29 days
  service-dc                         1            0           1    29 days
  scale-subscriber                   2           10           0    permanent
  scale-l2tp                         0         1000           0    permanent
  l2tp-inline-lns                    1            0           1    29 days

Licenses installed: none
```

É necessário instalar todas as licenças de BNG para habilitar os serviços. As licenças são instaladas pela WZTECH, sendo elas:

S-SA-FP – Licença que ativa serviço de subscriber
S-SM-FP – Licença que ativa serviço de CoA e serviços dinâmicos
S-SA-64K – Licença que ativa 64K assinantes no BNG. Neste caso cada assinante mesmo que esteja utilizando IPv4 + IPv6 WAN (NDRA ou IA_NA) + IPv6 LAN (PD) conta uma licença apenas.:

Exemplo de um usuário conectado com as licenças instaladas:

```
admin@MX204-LAB-WZTECH> show subscribers
Interface                      IP Address/VLAN ID                  User Name                       LS:RI
demux0.3221225503               200                                                            default:default
pp0.3221225504                 100.64.10.1                         wztech3                    default:default
*                              2090::
*                              1010:ee4:4000::/64
*                              2804:ee4:8000::/64
pp0.3221225504                 2090::                                                         default:default
*                              1010:ee4:4000::/64

admin@MX204-LAB-WZTECH> show system license
License usage:
                              Licenses     Licenses    Licenses    Expiry
  Feature name                    used    installed      needed
  subscriber-accounting              1            1           0    permanent
  subscriber-authentication          1            1           0    permanent
  subscriber-address-assignment      1            1           0    permanent
  subscriber-vlan                    0            1           0    permanent
  subscriber-ip                      0            1           0    permanent
  service-dc                         0            1           0    permanent
  service-accounting                 0            1           0    permanent
  service-qos                        0            1           0    permanent
  service-ancp                       0            1           0    permanent
  service-cbsp                       0            1           0    permanent
  scale-subscriber                   1        64000           0    permanent
  scale-l2tp                         0         1000           0    permanent
  l2tp-inline-lns                    0            1           0    permanent
```

Está sendo consumida apenas uma licença de assinante das 64K e o usuário no exemplo tem um endereço IPv4, um endereço WAN IA_NA, um prefixo NDRA alocado para a WAN caso seja solicitado pela ONU e um prefixo IA_PD.

Com todas as licenças ativadas o BNG fica desta forma:

```
admin@MX204-LAB-WZTECH> show system license
License usage:
                              Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  subscriber-accounting                 1            1           0    permanent
  subscriber-authentication             1            1           0    permanent
  subscriber-address-assignment         1            1           0    permanent
  subscriber-vlan                       0            1           0    permanent
  subscriber-ip                         0            1           0    permanent
  service-dc                            0            1           0    permanent
  service-accounting                    0            1           0    permanent
  service-qos                           0            1           0    permanent
  service-ancp                          0            1           0    permanent
  service-cbsp                          0            1           0    permanent
  scale-subscriber                      2        64000           0    permanent
  scale-l2tp                            0         1000           0    permanent
  l2tp-inline-lns                       0            1           0    permanent

Licenses installed:
  License identifier: E400662843
  License version: 4
  Features:
    scale-subscriber-64k - Subscriber Tier 32K - 64K
      permanent

  License identifier: E401171420
  License version: 4
  Features:
    service-dc       - Service Definition Capability
      permanent
    service-accounting - Per Service Accounting
      permanent
    service-qos      - Dynamic QOS Policy
      permanent
    service-ancp     - ANCP Based QOS Adjustment
      permanent
    service-cbsp     - Cell Based Shaping and Policing
      permanent

  License identifier: E408338859
  License version: 4
  Features:
    subscriber-accounting - Per Subscriber Radius Accounting
      permanent
    subscriber-authentication - Per Subscriber Radius Authentication
      permanent
    subscriber-address-assignment - Radius/SRC Address Pool Assignment
      permanent
    subscriber-vlan  - Dynamic Auto-sensed Vlan
      permanent
    subscriber-ip    - Dynamic and Static IP
      permanent
    l2tp-inline-lns  - L2TP Inline LNS
      permanent
```


Obs: É possível ver ao invés de "permanent" o valor "invalid" na linha scale-subscriber. Isto pode acontecer porque por default o JunOS monitora o uso da licença de assinantes e se o uso chegar em 90% do valor licenciado, por default o BNG vai ligar um modo trial por 30 dias permitindo qualquer quantidade de conexões e não limitará mais no valor da licença. Isto é o comportamento default para minimizar qualquer impacto em rede de produção caso seja extrapolado o valor licenciado do equipamento. Neste caso ao invés de "permanent" no valor da coluna Expiry começará um contador de 30 dias e quando terminar os 30 dias ficará com o valor "invalid". Dentro dos 30 dias qualquer quantidade de usuários será aceita no BNG. Depois dos 30 dias o valor invalid permanecerá e o BNG limitará na quantidade de usuários licenciados no valor real da licença não dando mais a possibilidade de ser extrapolado o valor licenciado.

Caso queira voltar o estado para permanent é necessário deletar e ativar as licenças novamente.

Caso não queira este comportamento default pode-se configurar o BNG para que ele não permita em momento nenhum mais conexões do que já está licenciado. Isto pode ser feito com o comando:

set system services subscriber-management enforce-strict-scale-limit-license

Este comportamento está documentado pela Juniper no seguinte link:

https://supportportal.juniper.net/s/article/Subscriber-Management-Scale-Subscriber-license-starts-showing-expiry-when-subscribers-are-reaching-license-limit?language=en_US

5. Configuração das Interfaces Físicas e Lógicas

As interfaces que receberão as conexões dos usuários podem ser configuradas com "flexible-vlan-tagging" para que suporte tanto conexões com um tag de VLAN que a Juniper chama de Service VLAN (SVLAN) ou com dois tags de VLAN no modelo stacked que a Juniper chama de Customer VLAN (CVLAN).

No modelo SVLAN geralmente cada OLT possui uma VLAN distinta de uplink e todos os usuários da mesma OLT usam esta mesma VLAN de Uplink para chegar no BNG.

Já no modelo CVLAN geralmente cada OLT possui uma VLAN distinta de uplink e cada usuário desta OLT possui um segundo tag de VLAN individual de forma que o par de VLANs na rede identifica o assinante e no BNG chega as vlan's empilhadas (SVLAN/CVLAN).

No modelo SVLAN a identificação do assinante deve utilizar algum outro parâmetro como usuário, MAC, Circuit-ID, etc.

Exemplo de configuração de uma interface para suportar modelo SVLAN e modelo CVLAN.

```
set interfaces xe-0/1/0 description CONEXOES_PPPOE
set interfaces xe-0/1/0 flexible-vlan-tagging

set interfaces xe-0/1/0 auto-configure vlan-ranges dynamic-profile SVLAN-DYNAMIC-PROFILE accept pppoe
set interfaces xe-0/1/0 auto-configure vlan-ranges dynamic-profile SVLAN-DYNAMIC-PROFILE ranges any

set interfaces xe-0/1/0 auto-configure stacked-vlan-ranges dynamic-profile CVLAN-DYNAMIC-PROFILE accept pppoe
set interfaces xe-0/1/0 auto-configure stacked-vlan-ranges dynamic-profile CVLAN-DYNAMIC-PROFILE ranges 2-4094,any

set interfaces xe-0/1/0 auto-configure remove-when-no-subscribers
```

O "flexible-vlan-tagging" habilita a interface a suportar pacotes com 1 tag de VLAN quanto pacotes com 2 tags (stacked). Com a configuração de flexible-vlan-tagging automaticamente o JunOS já muda o MTU da interface para suportar 8 bytes a mais. Neste caso o MTU sobe de 1514 que é o default para 1522. Caso haja necessidade por algum motivo de alterar o MTU da interface pode ser configurado:

```
set interfaces xe-0/1/0 mtu 9192
```

É possível configurar cada SVLAN ou SVLAN/CVLAN individualmente na interface. Este é um modelo que na prática fica inviável para configurar o BNG pois cada VLAN ou conjunto de VLAN's (Stacked) teria que ter configuração manual na interface do BNG. Em virtude disso a Juniper criou o modelo chamado auto-configure. Com este modelo é possível de forma dinâmica habilitar quais SVLAN's ou SVLAN/CVLAN's podem chegar no equipamento e automaticamente é criado subinterfaces (unit's) com identificadores dinâmicos sem que esta configuração tenha que ser feita de forma manual.

```
set interfaces xe-0/1/0 auto-configure vlan-ranges dynamic-profile SVLAN-DYNAMIC-PROFILE accept pppoe
set interfaces xe-0/1/0 auto-configure vlan-ranges dynamic-profile SVLAN-DYNAMIC-PROFILE ranges any
```

A configuração destas duas linhas está chamando no modelo auto-configure uma profile dinâmica de nome SVLAN-DYNAMIC-PROFILE. Também está definindo que para chamar esta profile dinâmica SVLAN-DYNAMIC-PROFILE o filtro é VLANs com 1 tag (vlan-ranges) com qualquer tag (ranges any). Também está permitindo pacotes pppoe serem aceitos para este range de VLAN configurado (accept pppoe).

```
set interfaces xe-0/1/0 auto-configure stacked-vlan-ranges dynamic-profile CVLAN-DYNAMIC-PROFILE accept pppoe
set interfaces xe-0/1/0 auto-configure stacked-vlan-ranges dynamic-profile CVLAN-DYNAMIC-PROFILE ranges 2-4094,any
```

A configuração destas duas linhas está chamando no modelo auto-configure uma profile dinâmica de nome CVLAN-DYNAMIC-PROFILE. Também está definindo que para chamar esta profile dinâmica CVLAN-

DYNAMIC-PROFILE o filtro é vlan's stacked (stacked-vlan-ranges) com qualquer VLAN outer (VLAN da OLT) sendo o range 2 a 4094 (2-4094) e a VLAN do usuário podendo ser qualquer uma (any). Também está permitindo pacotes pppoe serem aceitos para este range de CVLAN configurado (accept pppoe).

```
set interfaces xe-0/1/0 auto-configure remove-when-no-subscribers
```

Esta configuração de remove-when-no-subscribers fala para o BNG que quando uma conexão PPPoE for desconectada e não houver mais nenhum outro usuário que esteja utilizando a interface de camada 2 (demux0 por exemplo) é para o BNG deletar a interface dinâmica de camada 2. Caso esta linha não seja configurada quando um usuário conectar por exemplo no modelo CVLAN onde é criado uma interface demux0.<unit> para cada assinante e o assinante desconectar a interface demux0.<unit> permanecerá criada na caixa e quando houver uma próxima tentativa de conexão deste usuário o BNG apenas irá processar novamente a parte do assinante e não de VLAN. Apesar de otimizar de certa forma os recursos de VLAN NÃO é recomendado que o BNG seja configurado sem o remove-when-no-subscribers. Desta forma o BNG vai garantir que se não houver nenhuma conexão utilizando a interface ele automaticamente limpará a interface de camada 2 (VLAN) que não tem nenhum usuário conectado. Caso o comando "remove-when-no-subscribers" não esteja ativo e por algum motivo fiquem interfaces demux0.<unit> em desuso ativas no BNG a única forma de deletar estas interfaces será de forma manual:

Comando para deletar uma interface demux que não tem assinantes conectados no BNG:

```
admin@MX204-LAB-WZTECH> clear auto-configuration interfaces demux0.3221226299
```

As configurações de SVLAN e CVLAN são independentes e não interferem entre si. É possível ter uma SVLAN 300 chegando no BNG (1 tag de VLAN apenas) e outra vlan 300 chegando de uma ONU que usa o modelo CVLAN. Neste caso a SVLAN será a 300 com a CVLAN sendo a VLAN do assinante.

Caso seja configurado overlapping de VLAN's na interface o MX não vai deixar comitar:

```
[edit interfaces]
  'xe-0/1/0'
    Range 2-4,400-500 overlaps with range 2-4,300-400
error: configuration check-out failed

[edit interfaces]
  'xe-0/1/0'
    Range 1-3,any overlaps with range 2-4,300-400
error: configuration check-out failed

[edit interfaces]
  'xe-0/1/0'
    Range 1-5,any overlaps with range 2-4,300-400
error: configuration check-out failed

[edit interfaces]
  'xe-0/1/0'
    Range 2-4094,300-400 overlaps with range 2-4094,1-4094
error: configuration check-out failed

[edit interfaces]
  'xe-0/1/0'
    Range 200-200 overlaps with range 1-4094 in another profile under same interface
error: configuration check-out failed
```

No modelo auto-configure é necessário ser invocado uma primeira dynamic-profile chamada de VLAN Profile. Esta dynamic-profile é responsável por tratar os pacotes em camada 2 (SVLAN ou CVLAN).

Quando as configurações são manuais e não é utilizado o modelo auto-configure não é necessário chamar dynamic-profiles de VLAN pois como as subinterfaces (units) são criadas manualmente com as suas devidas configurações de underlying-interfaces a dynamic-profile de VLAN não faz sentido. Neste modelo manual de configuração é invocado diretamente a dynamic-profile da camada do assinante.

6. VLAN Profiles (SVLAN-DYNAMIC-PROFILE e/ou CVLAN-DYNAMIC-PROFILE)

O conceito de profiles dinâmicas na Juniper (dynamic-profiles) serve para trabalhar como um template de forma dinâmica onde o BNG com o auxílio de variáveis cria internamente os recursos necessários para o funcionamento do serviço, seja ele VLAN, PPPoE ou IPoE.

Anteriormente na interface física foi invocado no modelo auto-configure estas dynamic-profiles de VLAN's. Abaixo é feito a configuração destas dynamic-profiles de VLAN's:

```
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" vlan-id "$junos-vlan-id"
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" demux-options underlying-
interface "$junos-interface-ifd-name"
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe access-
concentrator CONCENTRADOR-PPPOE
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe duplicate-
protection
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe dynamic-profile
SUBSCRIBER-PROFILE
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe short-cycle-
protection


set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" vlan-tags outer "$junos-
stacked-vlan-id"
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" vlan-tags inner "$junos-vlan-
id"
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" demux-options underlying-
interface "$junos-interface-ifd-name"
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe access-
concentrator CONCENTRADOR-PPPOE
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe duplicate-
protection
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe dynamic-profile
SUBSCRIBER-PROFILE
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe short-cycle-
protection
```

As linhas acima estão criando as duas profiles dinâmicas (SVLAN-DYNAMIC-PROFILE e CVLAN-DYNAMIC-PROFILE) e está sendo definido uma interface chamada demux0 para ser utilizada como interface de camada 2. A interface demux0 com a sua subinterface (unit) que no modelo auto-configure é gerado de forma dinâmica é a interface para tratar os pacotes de camada 2 do usuário. Para cada tag de VLAN no modelo SVLAN ou para cada conjunto de tag's de vlan outer+inner do modelo CVLAN é criado uma interface demux0.<unit>. Isto significa que se o modelo utilizado for SVLAN todos os usuários que conectarem na mesma SVLAN estarão ancorados na mesma interface demux0.<unit> visto que para a mesma SVLAN é criada apenas uma interface demux0.<unit>. Esta unit será criada de forma dinâmica e é explicado mais abaixo.

Exemplo:

```
admin@MX204-LAB-WZTECH> show subscribers
Interface                   IP Address/VLAN ID                  User Name                       LS:RI
demux0.3221225914            200                                                               default:default
pp0.3221225915              192.168.4.60                        wztech2                         default:default
pp0.3221225916              192.168.4.61                        wztech2                         default:default
```

Neste caso existem duas conexões PPPoE (duas interfaces pp0.<unit>) e ambas as conexões estão ancoradas na interface demux0.3221225914. Esta unit 3221225914 foi criada dinamicamente no JunOS para a VLAN 200. Qualquer próxima conexão da VLAN 200 sempre utilizará esta interface demux0.3221225914. Caso seja feito uma conexão com a VLAN 300 ou um conjunto de VLAN's no modelo stacked será criada uma interface demux0 com um novo unit para esta nova SVLAN/CVLAN.

Exemplo:

```
demux0.3221225904     0x8100.300 0x8100.400                                         default:default
pp0.3221225905        192.168.4.1                         wztech2                   default:default
*                     2804:ee4:8000::/64
demux0.3221225906      200                                                          default:default
pp0.3221225907        192.168.4.2                         wztech3                   default:default
*                     2002::
*                     1010:ee4:4000::/64
*                     2804:ee4:8000:1::/64
pp0.3221225907        2002::                                                        default:default
*                     1010:ee4:4000::/64
```

No exemplo acima foi criada uma interface demux0.3221225904 para uma conexão CVLAN onde a SVLAN é 300 e a CVLAN é 400 e uma outra interface demux0.3221225906 para a SVLAN 200.

Todas as conexões novas com a VLAN 200 serão ancoradas na interface demux0.3221225906 e se houver uma nova conexão CVLAN usando a VLAN outer 300 e a inner 400 esta nova conexão será ancorada na interface demux0.3221225904.

Existem vários controles que são feitos diretamente na interface demux0.<unit> como por exemplo o número máximo de conexões. Se for configurado via RADIUS ou localmente que o número máximo de conexões é 1 este controle é feito na interface lógica demux0.<unit>.

Este modelo de utilizar a interface demux0 que é uma interface nativa do BNG para multiplexar e demultiplexar as conexões é o modelo mais recomendado pois o BNG trata todas as SVLAN's ou CVLAN's em um único ponto (interface demux0).

Existe um outro modelo pouco usado onde na configuração da dynamic-profile de SVLAN ou CVLAN ao invés de utilização da interface demux0 é apontado a variável "$junos-interface-ifd-name". Exemplo:

```
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces "$junos-interface-ifd-name" unit "$junos-interface-unit" vlan-id
"$junos-vlan-id"
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces "$junos-interface-ifd-name" unit "$junos-interface-unit" demux-
options underlying-interface "$junos-interface-ifd-name"
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces "$junos-interface-ifd-name" unit "$junos-interface-unit" family
pppoe access-concentrator CONCENTRADOR-PPPOE
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces "$junos-interface-ifd-name" unit "$junos-interface-unit" family
pppoe duplicate-protection
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces "$junos-interface-ifd-name" unit "$junos-interface-unit" family
pppoe dynamic-profile SUBSCRIBER-PROFILE
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces "$junos-interface-ifd-name" unit "$junos-interface-unit" family
pppoe short-cycle-protection
```

Neste caso está sendo configurado para que o JunOS não ancore a conexão do usuário na interface demux0 mas na interface da variável "$junos-interface-ifd-name". Esta variável é uma referência à interface física onde o usuário chegou no BNG.

Neste modelo o usuário quando conecta fica ancorado na interface física:

```
admin@MX204-LAB-WZTECH> show subscribers
Interface                   IP Address/VLAN ID                  User Name                       LS:RI
xe-0/1/0.3221225900          200                                                               default:default
pp0.3221225901              192.168.4.51                        wztech2                         default:default
pp0.3221225902              192.168.4.52                        wztech2                         default:default
```

Caso esteja em uma interface agregada será ancorado na interface agregada. Abaixo outro exemplo com um usuário ancorado na interface agregada ae0.

```
admin@MX204-LAB-WZTECH> show subscribers
Interface                   IP Address/VLAN ID                  User Name                       LS:RI
ae0.3221225611               200                                                               default:default
pp0.3221225612              100.64.10.41                        wztech3                         default:default
*                           1010:ee4:4000:8::/64
*                           2804:ee4:8000:28::/64
pp0.3221225612              1010:ee4:4000:8::/64                                              default:default
```

O problema neste modelo é que os controles feitos em camada 2 passam a não ser mais em um ponto central no BNG (interface demux0) mas sim por interface. Se for feito por exemplo a configuração de número máximo de conexões este controle estará na interface física de forma que se houver por exemplo conexão utilizando a VLAN 200 em 3 interfaces físicas distintas do BNG cada interface terá o seu controle individual. Este modelo apesar de funcional não é o mais recomendado. É recomendado o uso da interface demux0.

A seguir explicação de cada linha da configuração da dynamic-profile de SVLAN:

6.1. SVLAN Profile - VLAN-ID

```
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" vlan-id "$junos-vlan-id"
```

A variável "$junos-interface-unit" orienta o JunOS a criar uma subinterface (unit) com ID dinâmico e é obrigatória na configuração.
A variável "$junos-vlan-id" não é obrigatória na configuração, mas ainda recomendada pela Juniper e serve para definir internamente no software a VLAN do usuário.

6.2. Underlying-Interface

```
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" demux-options underlying-interface "$junos-interface-ifd-name"
```

A configuração de demux-options underlying-interface "$junos-interface-ifd-name" não é obrigatória e orienta o JunOS a interface física onde a interface demux0 criada para a conexão deve ser ancorada (underlying-interface). Em versões mais novas do JunOS automaticamente isso já é feito sem a necessidade desta configuração, mas ainda é recomendado pela Juniper esta linha.

6.3. Access-Concentrator Name

```
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe access-concentrator CONCENTRADOR-PPPOE
```

A configuração de access-concentrator não é obrigatória. Se não for definido o MX para o protocolo PPPoE (family pppoe) utilizará o nome do hostname (set system host-name) configurado no BNG para sinalizar o nome do concentrador na conexão PPPoE:

O nome do concentrador é enviado no PADO do BNG para o usuário:

```
> Frame 5: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)
> Juniper Ethernet
> Ethernet II, Src: JuniperN_fb:44:27 (20:d8:0b:fb:44:27), Dst: HuaweiTe_d7:a1:15 (d8:10:9f:d7:a1:15)
> 802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 300
> 802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 400
v PPP-over-Ethernet Discovery
    0001 .... = Version: 1
    .... 0001 = Type: 1
    Code: Active Discovery Offer (PADO) (0x07)
    Session ID: 0x0000
    Payload Length: 52
  v PPPoE Tags
      AC-Name: MX204-LAB-WZTECH
      Host-Uniq: c5070000
      AC-Cookie: 5914e29bbd68c587042f615c53ea53fc
```

6.4. Duplicate-Protection

```
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe duplicate-protection
```

A configuração de duplicate-protection não é obrigatória, mas altamente recomendada. Por default o BNG para a família de protocolos PPPoE (family pppoe) aceita mais de uma conexão PPPoE caso o MAC do usuário ou ONU esteja duplicado. Esta configuração de duplicate-protection garante que o BNG não vai aceitar uma segunda conexão PPPoE caso o MAC Address já esteja em uso em outra conexão.

Caso seja habilitado o PPPoE Session Lockout (short cycle protection) torna-se ainda mais importante esta configuração haja vista que caso o BNG detecte algum MAC Address fazendo atividades consideradas maliciosas para o equipamento caso existam mais conexões utilizando o mesmo MAC Address todas elas serão penalizadas. Então o recomendado é sempre deixar ligado o duplicate-protection.

6.5. Dynamic-Profile do Assinante ou Dynamic-Profile do Cliente

```
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe dynamic-profile
SUBSCRIBER-PROFILE
```

Na VLAN profile (SVLAN-DYNAMIC-PROFILE) está sendo apontado para a familia de protocolos PPPoE (family pppoe) a profile dinâmica do assinante SUBSCRIBER-PROFILE. Esta Subscriber Profile é também chamada pela Juniper de profile dinâmica do cliente (Dynamic Client Profile) processa o que é inerente ao protocolo utilizado pelo usuário na conexão, no nosso caso PPPoE. É nesta dynamic profile que é instanciado a interface PPPoE do assinante. Esta configuração é obrigatória.

6.6. PPPoE Lockout (Short Cycle Protection)

```
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces "$junos-interface-ifd-name" unit "$junos-interface-unit" family
pppoe short-cycle-protection
```

A configuração de PPPoE short-cycle-protection não é obrigatória, mas altamente recomendada. Este mecanismo possui um algoritmo que protege a parte de Control Plane do BNG em casos de ataques com pacotes PADI, conexões e desconexões em tempo curto e outros eventos que o BNG considera perigosos no protocolo PPPoE que possam after o Control Plane do equipamento. Este controle é individual por assinante (MAC) diferentemente do DDoS Protection onde os controles são gerais.

Exemplo de eventos que trigam a criação da criação do lockout:

1. Conetar/Desconectar rapidamente (mesmo que com usuário e senha corretos)
2. Erro de senha na conexão PPPoE

Caso no algoritmo de Short Cycle Protection seja considerado que o assinante trigou um cenário considerado perigoso o BNG vai bloquear o MAC Address do assinante e dar sequência no algoritmo de controle e bloqueio do assinante dentro do contexto da funcionalidade de short-cycle-protection.

Caso o usuário tenha sido autenticado sem a configuração de short-cycle-protection ele ficará com o estado de "Off" no BNG para a funcionalidade de short-cycle-protection:

```
admin@MX204-LAB-WZTECH> show pppoe lockout
demux0.3221225606 Index 536871098
Device: xe-0/1/0, VLAN: 200
  Short Cycle Protection: Off,
```

Short Cycle Protection Off significando que a funcionalidade está desabilitada para o usuário.

Quando a funcionalidade está ligada para o assinante:

```
admin@MX204-LAB-WZTECH> show pppoe lockout
demux0.3221225612 Index 536871104
Device: xe-0/1/0, VLAN: 200
  Short Cycle Protection: mac-address,
  Lockout Time (sec):  Min: 1, Max: 300
    Total clients in lockout: 0
    Total clients in lockout grace period: 0
```

Quando um assinante é penalizado, ele começa com um bloqueio de 1 segundo e caso haja novamente um próximo evento ele é bloqueado por 2 segundos e caso haja um novo evento o BNG vai bloquear o MAC por 4 segundos e assim sucessivamente. O tempo de bloqueio é exponencial podendo chegar por default até 300 segundos (5 minutos). Este tempo pode ser mudado. Exemplo para configurar o tempo máximo de bloqueio em 120 segundos:

```
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe short-cycle-
protection lockout-time-max 120
```

Durante o tempo do bloqueio o BNG não vai processar nenhum pacote PPPoE deste assinante que está com o MAC Address bloqueado.

```
admin@MX204-LAB-WZTECH> show pppoe lockout
Device: xe-0/1/0, VLAN: 200
  Short Cycle Protection: mac-address,
```

```
  Lockout Time (sec):  Min: 1, Max: 300
    Total clients in lockout: 0
    Total clients in lockout grace period: 1
  Client Address                    Current    Elapsed    Next
    8C:47:BE:52:91:FB                     0          0       2
```

Neste caso acima existiu um evento de bloqueio (lockout) no BNG para o assinante, porém neste momento ele não está bloqueado (Current está com o valor 0) e caso haja um novo evento de bloqueio o MAC será bloqueado por 2 segundos.

```
admin@MX204-LAB-WZTECH> show pppoe lockout
Device: xe-0/1/0, VLAN: 200
  Short Cycle Protection: mac-address,
  Lockout Time (sec):  Min: 1, Max: 300
    Total clients in lockout: 1
    Total clients in lockout grace period: 0
  Client Address                    Current    Elapsed    Next
    8C:47:BE:52:91:FB                    16          7      32
```

Neste exemplo acima o assinante está bloqueado com um bloqueio de 16 segundos (Current: 16) e já se passaram 7 segundos que ele foi bloqueado (Elapsed: 7). Caso o assinante gere um próximo evento considerado perigoso no algoritmo do short-cycle-protection o bloqueio será 32 segundos (Next: 32).

Depois dos 16 segundos o usuário volta a ficar com Current e Elapsed com valor 0 (Não tem bloqueio) e enquanto o Current estiver com valor maior que 0 o BNG não processará pacotes PPPoE deste MAC.

Caso nenhum novo evento considerado perigoso pelo algoritmo do short-cycle-protection aconteça com este assinante no BNG durante 15 minutos o evento de lockout é deletado. Havendo um novo evento o processo começa novamente com o tempo de bloqueio sendo incrementado exponencialmente: 1, 2, 4, 8, 16, 32, 64, 128, 256, 300 segundos (valor default máximo).

Para filtrar o estado de lockout de um assinante específico pode-se fazer pela interface L2 (demux0.<unit> por exemplo) caso o usuário esteja conectado:


```
admin@MX204-LAB-WZTECH> show pppoe lockout demux0.3221225624
  Lockout Time (sec):  Min: 1, Max: 300
    Total clients in lockout: 0
    Total clients in lockout grace period: 1
  Client Address                    Current    Elapsed    Next
    8C:47:BE:52:91:FB                     0          0      32
```

Importante: Mesmo que o assinante não esteja conectado e a interface L2 tenha sido deletada em virtude da configuração de "remove-when-no-subscribers" caso o short-cycle-protection esteja configurado o BNG ainda mantém este estado dos assinantes que não estão conectados. Neste caso para filtrar um assinante não conectado este filtro tem que ser feito pela SVLAN ou SVLAN/CVLAN + interface física ou agregada do assinante.

Exemplo:

```
admin@MX204-LAB-WZTECH> show pppoe lockout vlan-identifier device-name xe-0/1/0 vlan-id 200
  Lockout Time (sec):  Min: 1, Max: 300
    Total clients in lockout: 0
    Total clients in lockout grace period: 1
  Client Address                    Current    Elapsed    Next
    8C:47:BE:52:91:FB                     0          0      64
```

```
admin@MX204-LAB-WZTECH> show pppoe lockout vlan-identifier vlan-id 400 svlan-id 300 device-name xe-0/1/0
  Lockout Time (sec):  Min: 1, Max: 300
    Total clients in lockout: 0
    Total clients in lockout grace period: 0
```

Para deletar um lockout de um assinante pode-se limpar usando a interface underlying (demux0.<unit>), o MAC-Address, VLAN, etc:

Exemplos:

```
admin@MX204-LAB-WZTECH> clear pppoe lockout vlan-identifier vlan-id 200 device-name xe-0/1/0
```

```
admin@MX204-LAB-WZTECH> clear pppoe lockout underlying-interfaces demux0.3221225627

admin@MX204-LAB-WZTECH> clear pppoe lockout mac-address 8C:47:BE:52:91:FB
```

A seguir explicação de cada linha da configuração da dynamic-profile de CVLAN:

```
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" vlan-tags outer "$junos-stacked-vlan-id"
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" vlan-tags inner "$junos-vlan-id"
```

6.7. CVLAN Profile - VLAN-TAGS

A variável "$junos-interface-unit" orienta o JunOS a criar uma subinterface (unit) com ID dinâmico e é obrigatória na configuração.
As configurações de vlan-tags com as variáveis "$junos-stacked-vlan-id" e "$junos-vlan-id" são obrigatórias e servem para orientar o JunOS a alocar internamente as VLAN's SVLAN e CVLAN do usuário.

```
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" demux-options underlying-interface "$junos-interface-ifd-name"
```

Mesma explicação da profile SVLAN-DYNAMIC-PROFILE

```
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe access-concentrator CONCENTRADOR-PPPOE
```

Mesma explicação da profile SVLAN-DYNAMIC-PROFILE

```
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe duplicate-protection
```

Mesma explicação da profile SVLAN-DYNAMIC-PROFILE

```
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe dynamic-profile SUBSCRIBER-PROFILE
```

Mesma explicação da profile SVLAN-DYNAMIC-PROFILE

```
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe short-cycle-protection
```

7. Profile do Assinante (Subscriber Profile ou Client Profile) – PPPoE (DYNAMIC PROFILE SUBSCRIBER-PROFILE)

Conforme visto anteriormente as profiles dinâmicas de VLAN também chamadas de VLAN Profiles chamam a profile do assinante (Subscriber Profile também chamada pela Juniper de Client Profile). É nesta subscriber dynamic-profile onde são definidos vários dos parâmetros do protocolo PPPoE e do assinante.

A seguir o exemplo da configuração da profile dinâmica do assinante (subscriber profile):

```
set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults input-filter PREDEFINED-IPV4-IN
set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults output-filter PREDEFINED-IPV4-OUT
set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults input-ipv6-filter PREDEFINED-IPV6-IN
set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults output-ipv6-filter PREDEFINED-IPV6-OUT
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" interface "$junos-interface-name"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options rib "$junos-ipv6-rib" access route $junos-framed-route-ipv6-address-prefix qualified-next-hop "$junos-interface-name"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options rib "$junos-ipv6-rib" access route $junos-framed-route-ipv6-address-prefix metric "$junos-framed-route-ipv6-cost"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options rib "$junos-ipv6-rib" access route $junos-framed-route-ipv6-address-prefix preference "$junos-framed-route-ipv6-distance"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options rib "$junos-ipv6-rib" access route $junos-framed-route-ipv6-address-prefix tag "$junos-framed-route-ipv6-tag"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options access route $junos-framed-route-ip-address-prefix next-hop "$junos-framed-route-nexthop"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options access route $junos-framed-route-ip-address-prefix metric "$junos-framed-route-cost"
```

```
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options access route $junos-framed-route-ip-address-prefix preference "$junos-framed-route-distance"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options access route $junos-framed-route-ip-address-prefix tag "$junos-framed-route-tag"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" actual-transit-statistics
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" ppp-options chap
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" ppp-options pap
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet rpf-check
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet filter input "$junos-input-filter"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet filter output "$junos-output-filter"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet unnumbered-address "$junos-loopback-interface"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 rpf-check
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 filter input "$junos-input-ipv6-filter"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 filter output "$junos-output-ipv6-filter"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 unnumbered-address "$junos-loopback-interface"
set dynamic-profiles SUBSCRIBER-PROFILE protocols router-advertisement interface "$junos-interface-name" dns-server-address $junos-ipv6-dns-server-address
set dynamic-profiles SUBSCRIBER-PROFILE protocols router-advertisement interface "$junos-interface-name" prefix $junos-ipv6-ndra-prefix
```

Antes de detalharmos a profile dinâmica do assinante "SUBSCRIBER-PROFILE" vamos primeiramente detalhar o conceito de firewall filter.

7.1. Firewall Filters

No BNG da Juniper existe o conceito de firewall filter. Estas firewall filters são politicas para fazer controles de protocolos e portas, policiamento de tráfego, desvio de tráfego para um CGNAT por exemplo e outras funções. Elas podem ser aplicadas nas interfaces definidas manualmente e podem também ser aplicadas de forma dinâmica nas interfaces criadas dinamicamente no modelo auto-configure. No caso do BNG elas podem fazer o controle de protocolos e portas originadas do usuário e destinadas ao usuário, controle de banda (policer) do tráfego originado do usuário e destinado ao usuário e pode também por exemplo fazer desvio de tráfego IPv4 para um CGNAT.

Para cada conexão PPPoE no BNG é possível enviar firewall filter de input para endereços IPv4 (family inet filter input), firewall filter de output para endereços IPv4 (family inet filter output), firewall filter de input para endereços IPv6 (family inet6 filter input) e firewall filter de output para endereços IPv6 (family inet6 filter output). O filtro é aplicado individualmente em cada família de protocolos (IPv4 ou IPv6) e em cada sentido (input ou output). No caso do sentido input ou output é do ponto de vista do BNG. Input é o tráfego originado do assinante. Output é o tráfego destinado ao assinante.

Exemplo de uma firewall filter IPv4 (inet) criada no BNG chamada PREDEFINED-IPV4-IN:

```
set firewall family inet filter PREDEFINED-IPV4-IN interface-specific
set firewall family inet filter PREDEFINED-IPV4-IN term POLICER then policer 2Mbps
set firewall family inet filter PREDEFINED-IPV4-IN term POLICER then next term
set firewall family inet filter PREDEFINED-IPV4-IN term FILTRO-PADRAO-IN filter FILTRO-PADRAO-IPV4-IN
```

A seguir o detalhamento deste exemplo de firewall filter IPv4 (family inet):

```
set firewall family inet filter PREDEFINED-IPV4-IN interface-specific
```

Esta firewall filter tem a informação de interface-specific. No caso de PPPoE é obrigatório que tenha a configuração de interface-specific. Esta configuração faz com que o MX instancie individualmente a mesma firewall filter para cada interface onde ela é aplicada e mantenha controles de banda e contadores em cada interface onde ela é aplicada.

Como no BNG cada usuário que pegar o mesmo filtro vai precisar de um controle individual de banda e contadores é obrigatório o interface-specific. Se a firewall filter for criada sem o interface-specific o usuário não vai conectar.

```
set firewall family inet filter PREDEFINED-IPV4-IN term POLICER then policer 2Mbps
set firewall family inet filter PREDEFINED-IPV4-IN term POLICER then next term
```

Depois, na firewall filter IPv4 é definido um termo chamado "POLICER" onde é instruído o BNG a fazer um policiamento de tráfego de acordo com os parâmetros da policer de nome "2Mbps" e por fim ler o próximo termo (next term). Ao final do processamento de cada termo após executada a ação configurada não há sequência no processamento dos demais termos da firewall filter. Se não for configurado o "next term" o firewall vai simplesmente aceitar o tráfego e policiar em 2Mbps e não vai dar sequência nos próximos termos. Desta forma está sendo informado ao BNG que após policiar o tráfego com os valores da policer chamado 2Mbps é para o BNG ao invés de parar de ler a firewall filter seguir avaliando o próximo termo (next term).

```
set firewall policer 2Mbps logical-interface-policer
set firewall policer 2Mbps if-exceeding bandwidth-limit 2m
set firewall policer 2Mbps if-exceeding burst-size-limit 250k
set firewall policer 2Mbps then discard
```

```
set firewall policer 2Mbps logical-interface-policer
```

Esta policer chamada "2Mbps" está configurada com o parâmetro "logical-interface-policer". O "logical-interface-policer" permite que as famílias de protocolos IPv4 e IPv6 compartilhem a mesma banda caso a firewall filter de ambas as famílias apontem para a mesma policer. Se não for configurado o "logical-interface-policer" cada família de protocolos (IPv4 e IPv6) terá sua banda individual.

```
set firewall policer 2Mbps if-exceeding bandwidth-limit 2m
set firewall policer 2Mbps if-exceeding burst-size-limit 256k
set firewall policer 2Mbps then discard
```

Está sendo configurado na policer de nome "2Mbps" que a banda limite do usuário é 2Mbits/s com burst de 256Kbytes. Como recomendação geral considerar como burst o valor da banda multiplicado por 12,5%.

Exemplo: 2Mbps (2048000) * 12,5% = 256000 (256Kbytes)

```
set firewall family inet filter PREDEFINED-IPV4-IN term FILTRO-PADRAO-IN filter FILTRO-PADRAO-IN-IPV4
```

Por fim na firewall filter IPv4 PREDEFINED-IPV4-IN é criado um último termo chamado FILTRO-PADRAO-IN invocando uma outra firewall filter chamada "FILTRO-PADRAO-IN-IPV4". Este modelo é uma forma de configuração onde ao invés de fazer toda a configuração em toda firewall filter e o arquivo de configuração ficar muito grande, é feito na firewall filter primária apenas o básico da configuração e o que é comum a todos apenas invoca o nome desta segunda firewall filter dentro da primeira.

```
set firewall family inet filter FILTRO-PADRAO-IPV4-IN interface-specific
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DESCARTA-PORTAS-INPUT from destination-port 1900
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DESCARTA-PORTAS-INPUT from destination-port 25
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DESCARTA-PORTAS-INPUT then discard
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from protocol udp
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from source-port 53
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from source-port 161
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from source-port 123
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from source-port 1900
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from source-port 111
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from source-port 137
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from source-port 10001
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION then discard
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term BYPASS-LOOPBACK-LOCAL from destination-address 20.20.20.20/32
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term BYPASS-LOOPBACK-LOCAL then accept
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term BYPASS-TRAFEGO-LOCAL from destination-address 200.225.230.0/24
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term BYPASS-TRAFEGO-LOCAL from destination-address 200.225.231.0/24
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term BYPASS-TRAFEGO-LOCAL from destination-address 200.225.232.0/24
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term BYPASS-TRAFEGO-LOCAL from destination-address 200.225.233.0/24
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term BYPASS-TRAFEGO-LOCAL then accept
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DESVIA-TRAFEGO-CGNAT from source-address 100.64.0.0/10
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DESVIA-TRAFEGO-CGNAT then next-ip 172.17.17.2/32
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term ACCEPT then accept
```

Esta nova firewall filter invocada no final da firewall filter PREDEFINED-IPV4-IN é processada também.

```
set firewall family inet filter FILTRO-PADRAO-IPV4-IN interface-specific
```

Esta firewall filter chamada dentro da principal também precisa ter o interface-specific.

```
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DESCARTA-PORTAS-INPUT from destination-port 1900
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DESCARTA-PORTAS-INPUT from destination-port 25
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DESCARTA-PORTAS-INPUT then discard
```

O termo DESCARTA-PORTAS-INPUT o BNG vai bloquear (discard) todo tráfego originado do usuário na familia IPv4 (inet) onde as portas de destino forem 1900 (SSDP) e 25 (SMTP não autenticado)

```
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from protocol udp
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from source-port 53
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from source-port 161
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from source-port 123
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from source-port 1900
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from source-port 111
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from source-port 137
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION from source-port 10001
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DROP-AMPLIFICATION then discard
```

No termo DROP-AMPLIFICATION o BNG vai bloquear todo tráfego UDP IPv4 originado do usuário se as portas de origem forem 53 (DNS), 161 (SNMP), 123 (NTP), 1900 (SSDP), 111 (PORTMAP), 127 (NETBIOS) e 10001 (Service Discovery Ubiquiti).

Este tipo de tráfego é comumente utilizado em ataques de amplificação e é recomendado que esteja sempre bloqueado.

```
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term BYPASS-LOOPBACK-LOCAL from destination-address 20.20.20.20/32
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term BYPASS-LOOPBACK-LOCAL then accept
```

No termo BYPASS-LOOPBACK-LOCAL o BNG simplesmente aceita os pacotes destinados ao IP de Loopback do BNG. Esta ação se faz necessário pois posteriormente há um termo que pega todo o tráfego dos assinantes onde a rede de origem é 100.64/10 e desvia para um CGNAT. Neste caso as respostas de ping dos usuários para o BNG (echo-reply) também seriam desviadas para o CGNAT e não seria possível fazer ping do BNG para os assinantes. Com esta ação os pacotes destinados ao IP de loopback do BNG simplesmente são aceitos e processados neste termo.


```
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term BYPASS-TRAFEGO-LOCAL from destination-address 200.225.230.0/24
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term BYPASS-TRAFEGO-LOCAL from destination-address 200.225.231.0/24
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term BYPASS-TRAFEGO-LOCAL from destination-address 200.225.232.0/24
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term BYPASS-TRAFEGO-LOCAL from destination-address 200.225.233.0/24
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term BYPASS-TRAFEGO-LOCAL then accept
```

O termo BYPASS-TRAFEGO-LOCAL também está permitindo tráfego que não deve passar pelo CGNAT. Neste caso por exemplo devem ser definidas as redes de CDN internas e tráfego que serão roteados diretamente pelo BNG sem passar pelo CGNAT.

```
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DESVIA-TRAFEGO-CGNAT from source-address 100.64.0.0/10
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DESVIA-TRAFEGO-CGNAT then next-ip 172.17.17.2/32
```

O próximo termo dá match na rede 100.64.0.0/10 (RFC 6598) que é a rede reservada para IP's privados que passarão pelo CGNAT e como ação é feito um desvio do tráfego para o next-ip 172.17.17.2. Quando for feita a configuracão de next-ip para CGNAT é importante lembrar que esse PBR de tráfego feito na firewall filter chamado pela Juniper de FBF (Filter Based Forwarding) não triga protocolo ARP. Isto significa que se não houver entrada ARP aprendida para o IP do next-ip quando chegar um pacote no MX este pacote irá ser descartado e o MX não vai gerar um ARP Request pois FBF não triga ARP Request.

Neste caso pode-se criar uma entrada ARP estática para o IP do next-ip ou pode-se também configurar uma rota estática do IP do next-ip para ele mesmo. Esse "trick" faz com que o MX gere ARP Request para o next-ip caso ele não tenha entrada ARP se chegar um pacote na caixa e este pacote precisar ser desviado para esse next-ip. Isto é documentado pela Juniper na seguinte URL:

https://kb.juniper.net/InfoCenter/index?page=content&id=KB31274&cat=JUNOS_PLATFORM&actp=LIST

Outro modelo que pode ser utilizado para desvio do tráfego dos assinantes IPv4 com IP's privados para uma estrutura de CGNAT no BNG é utilizando VRF. Ao invés de usar o next-ip pode-se jogar o tráfego dentro de uma VRF e a comunicação do BNG com o CGNAT ocorre dentro da VRF:

```
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DESVIA-TRAFEGO-CGNAT from source-address 100.64.0.0/10
set firewall family inet filter FILTRO-PADRAO-IPV4-IN term DESVIA-TRAFEGO-CGNAT then routing-instance VR-NAT44

set routing-instances VR-NAT44 routing-options static route 100.64.0.0/10 next-table inet.0
set routing-instances VR-NAT44 routing-options static route 0.0.0.0/0 next-hop 177.69.8.66
set routing-instances VR-NAT44 description "VR para CGN de NAT44"
set routing-instances VR-NAT44 instance-type virtual-router
set routing-instances VR-NAT44 interface ae0.100
```

Neste caso o trafégo do assinante quando chegar da rede 10.64.0.0/10 no BNG será desviado para uma VRF de nome VR-NAT44. Na VRF é feito a comunicação com o CGNAT e quando o tráfego voltar do CGNAT para o BNG na VRF o tráfego será novamente roteado para a tabela global (inet.0) já que o assinante está conectado na tabela global (inet.0).

```
set firewall family inet filter FILTRO-PADRAO-IPV4-IN then accept
```

E por último qualquer outro tipo de tráfego que chegar no BNG que não tenha que ser redirecionado para o CGNAT vai dar match neste último termo e ser liberado (por exemplo o tráfego dos usuários que pegam endereço IP público).

Com o entendimento básico do conceito de firewall filter vamos voltar no detalhamento da profile do assinante SUBSCRIBER-PROFILE:

7.2. Subscriber Profile - Variáveis Pré-Definidas

```
set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults input-filter PREDEFINED-IPV4-IN
```

A configuração acima não é obrigatória, mas a falta dela em alguns casos pode fazer com que o usuário não conecte. A função das predefined-variable-defaults na Juniper é aplicar configurações padrões quando o RADIUS não envia uma informação obrigatória. Posteriormente na configuração da SUBSCRIBER-PROFILE há uma linha que habilita o BNG a receber filtro IPv4 de input do RADIUS. A partir do momento que é habilitado este recebimento é obrigatório que o usuário tenha uma firewall filter de input IPv4 (seja recebida por RADIUS ou seja preenchendo através da variavel predefined chamada input-filter).

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet filter input "$junos-input-filter"
```

Caso o RADIUS não envie esta firewall filter de IPv4 de input para o usuario o BNG vai aplicar a firewall filter IPv4 de input chamada PREDEFINED-IPV4-IN neste assinante. Se não for configurado na profile do assinante (SUBSCRIBER-PROFILE) que esta firewall filter de input é obrigatória (family inet filter input "$junos-input-filter") esta linha não tem sentido e não será utilizada.

Por outro lado, se a filter de input está configurada como obrigatória, se o RADIUS não enviar o AVP e não estiver configurado a variável predefined input-filter o assinante não conectará.

```
set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults output-filter PREDEFINED-IPV4-OUT
```

Esta configuração também não é obrigatória e tem o mesmo comportamento e a mesma explicação da predefined-variable-default input-filter. A única diferença é que ela é o nome da firewall filter que será aplicada para a familia IPv4 no sentido de OUTPUT (tráfego destinado ao usuário) caso o RADIUS não mande o atributo desta firewall filter.

A seguir vamos detalhar o conteúdo dessa firewall filter PREDEFINED-IPV4-OUT:

```
set firewall family inet filter PREDEFINED-IPV4-OUT interface-specific
set firewall family inet filter PREDEFINED-IPV4-OUT term FILTRO-PADRAO-OUT filter FILTRO-PADRAO-IPV4-OUT
set firewall family inet filter PREDEFINED-IPV4-OUT term POLICER then policer 2Mbps

set firewall family inet filter PREDEFINED-IPV4-OUT interface-specific
```

Primeiramente a firewall filter tem o interace-specific que é obrigatório para firewall filters de usuários no BNG já explicado anteriormente.

```
set firewall family inet filter PREDEFINED-IPV4-OUT term FILTRO-PADRAO-OUT filter FILTRO-PADRAO-IPV4-OUT
```

Este termo chamado FILTRO-PADRAO-OUT invoca uma nova firewall filter chamada FILTRO-PADRAO-IPV4-OUT. Neste momento o BNG não processa mais a próxima linha (termo POLICER). O BNG vai processar o filtro FILTRO-PADRAO-IPV4-OUT completamente e se não houver nenhum match nesse filtro ele volta para continuar processando a próxima linha do filtro original PREDEFINED-IPV4-OUT

```
set firewall family inet filter FILTRO-PADRAO-IPV4-OUT interface-specific
set firewall family inet filter FILTRO-PADRAO-IPV4-OUT term BLOQUEIA-PORTAS-OUT from destination-port 0-1023
set firewall family inet filter FILTRO-PADRAO-IPV4-OUT term BLOQUEIA-PORTAS-OUT then discard
```

```
set firewall family inet filter FILTRO-PADRAO-IPV4-OUT interface-specific
```

Interface-specific é obrigatório em todo filtro de usuário conforme já detalhado anteriormente.

```
set firewall family inet filter FILTRO-PADRAO-IPV4-OUT term BLOQUEIA-PORTAS-OUT from destination-port 0-1023
set firewall family inet filter FILTRO-PADRAO-IPV4-OUT term BLOQUEIA-PORTAS-OUT then discard
```

O termo BLOQUEIA-PORTAS-OUT bloqueia (discard) todas as portas baixas (0 a 1023) dos protocolos UDP e TCP (visto que não foi mencionado o protocolo). A ideia desse termo é garantir que todo tráfego em portas baixas (portas usadas para serviços) não chegue no assinante e o BNG descarte esse tráfego.

Como não tem mais nenhum termo posterior a este no filtro FILTRO-PADRAO-IPV4-OUT o BNG volta a processar a próxima linha do filtro PREDEFINED-IPV4-OUT:

```
set firewall family inet filter PREDEFINED-IPV4-OUT term POLICER then policer 2Mbps
```

Neste caso é feito um policiamento de tráfego com o conteúdo da policer de nome 2Mbps.

```
set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults input-ipv6-filter PREDEFINED-IPV6-IN
```

Esta configuração também não é obrigatória e tem o mesmo comportamento e a mesma explicação da predefined-variable-default input-filter. A diferença é que ela é o nome da firewall filter que será aplicada para a familia IPv6 no sentido de INPUT (qualquer tráfego IPv6 originado do usuário) caso o RADIUS não mande o atributo desta firewall filter.

Exemplo da firewall filter de IPv6 chamada PREDEFINED-IPV6-IN:

```
set firewall family inet6 filter PREDEFINED-IPV6-IN interface-specific
set firewall family inet6 filter PREDEFINED-IPV6-IN term DHCPV6POLICER from next-header udp
set firewall family inet6 filter PREDEFINED-IPV6-IN term DHCPV6POLICER from source-port 546
set firewall family inet6 filter PREDEFINED-IPV6-IN term DHCPV6POLICER from destination-port 547
set firewall family inet6 filter PREDEFINED-IPV6-IN term DHCPV6POLICER then policer DHCPPOLICER
set firewall family inet6 filter PREDEFINED-IPV6-IN term DHCPV6POLICER then next term
set firewall family inet6 filter PREDEFINED-IPV6-IN term POLICER then policer 2Mbps
set firewall family inet6 filter PREDEFINED-IPV6-IN term POLICER then next term
set firewall family inet6 filter PREDEFINED-IPV6-IN term FILTRO-PADRAO-IPV6-IN filter FILTRO-PADRAO-IPV6-IN

set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN interface-specific
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term DESCARTA-PORTAS-INPUT-TCP from next-header tcp
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term DESCARTA-PORTAS-INPUT-TCP from destination-port 25
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term DESCARTA-PORTAS-INPUT-TCP then discard
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term DESCARTA-PORTAS-INPUT-UDP from next-header udp
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term DESCARTA-PORTAS-INPUT-UDP from destination-port 1900
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term DESCARTA-PORTAS-INPUT-UDP then discard
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term DROP-AMPLIFICATION from next-header udp
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term DROP-AMPLIFICATION from source-port 53
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term DROP-AMPLIFICATION from source-port 1900
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term DROP-AMPLIFICATION from source-port 10001
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term DROP-AMPLIFICATION from source-port 137
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term DROP-AMPLIFICATION from source-port 123
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term DROP-AMPLIFICATION from source-port 161
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term DROP-AMPLIFICATION from source-port 111
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term DROP-AMPLIFICATION then discard
set firewall family inet6 filter FILTRO-PADRAO-IPV6-IN term ACCEPT then accept
```

```
set firewall policer DHCPPOLICER logical-interface-policer
set firewall policer DHCPPOLICER if-exceeding-pps pps-limit 4
set firewall policer DHCPPOLICER if-exceeding-pps packet-burst 1
set firewall policer DHCPPOLICER then discard
```

A explicação destes filtros é a mesma já dada anteriormente para a familia IPv4 (inet).

A diferença do filtro IPv6 para o IPv4 é que ele é feito na família IPv6 (inet6) e ao invés de definir o protocolo com o parametro protocol no IPv6 é utilizado o parametro next-header para definir o protocolo.

Importante: Na firewall filter IPv6 associada com o assinante é recomendado antes de policiar o tráfego todo criar um termo para limitar a quantidade de pacotes por segundo DHCPv6 enviados do assinante para o BNG já que no caso de DHCP IA_NA e/ou DHCP IA_PD os pacotes são todos processados pela Routing Engine e caso haja ataques e/ou comportamentos anômalos já vistos em ONU's com problemas de firmware o BNG vai limitar na PFE (Data Plane) em aproximadamente 5 pacotes por segundo DHCPv6 vindo da ONU para a Routing Engine. No exemplo acima o termo criado é o termo DHCPV6POLICER.

```
set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults output-ipv6-filter PREDEFINED-IPV6-OUT
```

Esta configuração também não é obrigatória e tem o mesmo comportamento e a mesma explicação da predefined-variable-default output-filter. A diferença é que ela é o nome da firewall filter que será aplicada para a familia IPv6 no sentido de OUTPUT (tráfego destinado ao usuário) caso o RADIUS não mande o atributo desta firewall filter.

```
set firewall family inet6 filter PREDEFINED-IPV6-OUT interface-specific
set firewall family inet6 filter PREDEFINED-IPV6-OUT term FILTRO-PADRAO-OUT filter FILTRO-PADRAO-IPV6-OUT
set firewall family inet6 filter PREDEFINED-IPV6-OUT term POLICER then policer 2Mbps

set firewall family inet6 filter FILTRO-PADRAO-IPV6-OUT interface-specific
set firewall family inet6 filter FILTRO-PADRAO-IPV6-OUT term BLOQUEIA-PORTAS-OUT from next-header tcp
set firewall family inet6 filter FILTRO-PADRAO-IPV6-OUT term BLOQUEIA-PORTAS-OUT from next-header udp
set firewall family inet6 filter FILTRO-PADRAO-IPV6-OUT term BLOQUEIA-PORTAS-OUT from destination-port 0-1023
set firewall family inet6 filter FILTRO-PADRAO-IPV6-OUT term BLOQUEIA-PORTAS-OUT then discard
```

A firewall filter inet6 (IPv6) é similar à firewall filter inet (IPv4). A diferença é que é utilizado o parametro next-header no lugar de protocol.

7.3. Routing-Instance - Junos-Interface-Name

```
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" interface "$junos-interface-name"
```

A configuração acima da profile do assinante é obrigatória e faz com que o BNG habilite o funcionamento da interface PPPoE do assinante (pp0.<unit>) no modelo de routing-instance. Routing-instance na Juniper é o mesmo conceito de VRF. Qualquer usuário sempre vai usar routing-instance. Mesmo que não seja enviado VRF pelo RADIUS o usuário estará utilizando uma routing-instance chamada "default". Desta forma é obrigatório que seja configurado esta linha para que o usuário consiga conectar.

7.4. IPv6 - Access-Routes

```
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options rib "$junos-ipv6-rib"
access route $junos-framed-route-ipv6-address-prefix qualified-next-hop "$junos-interface-name"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options rib "$junos-ipv6-rib"
access route $junos-framed-route-ipv6-address-prefix metric "$junos-framed-route-ipv6-cost"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options rib "$junos-ipv6-rib"
access route $junos-framed-route-ipv6-address-prefix preference "$junos-framed-route-ipv6-distance"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options rib "$junos-ipv6-rib"
access route $junos-framed-route-ipv6-address-prefix tag "$junos-framed-route-ipv6-tag"
```

A configuração acima não é obrigatória. Ela habilita o funcionamento de access routes para o protocolo IPv6. Access-routes são rotas enviadas via RADIUS usando o AVP Framed-IPv6-Route. Se não for feito a configuração acima não será possível enviar rotas IPv6 para o BNG utilizando o AVP Framed-IPv6-Route. Qualquer outro atributo para envio de prefixo ou pool para o assinante não depende da configuração acima. A configuração acima é necessária estritamente para o caso de envio de rotas utilizando o AVP Framed-IPv6-Route. Há a possibilidade do envio de atributos da rota como métrica (metric), preferencia (preference) e tag

(tag). O BNG vai colocar como next-hop desta rota sempre a interface pp0.<unit> do usuario (qualified-next-hop "$junos-interface-name").

Este AVP pode ser preenchido de formas diferentes no RADIUS. Para nossa documentação todo atributo de RADIUS mostrados nos exemplos foram configurados no software FreeRADIUS versão 3.0.13.

Exemplo:

Framed-IPv6-Route = "2020:2020::/64"

Quando um usuário se conectar o RADIUS vai enviar o prefixo 2020:2020::/64 para o assinante. Neste caso não é obrigatório definir o gateway no AVP pois o FreeRADIUS vai adicionar o valor :: no gateway e metric 1 na métrica automaticamente.

Caso queira enviar além do prefixo parâmetros da rota como métrica, tag e preferência é necessário na frente do prefixo definir um gateway (pode ser utilizado sempre o valor :: pois o BNG vai descartar qualquer valor de gateway enviado e vai criar a rota apontando para a interface pp0.<unit> do usuario), depois o valor de métrica, depois o parâmetro tag com o devido valor de tag e por ultimo o parametro pref com o devido valor de preferência.

Exemplo do AVP com todas as definições:

Framed-IPv6-Route = "2020:2020::/64 :: 20 tag 10 pref 3"

```
admin@MX204-LAB-WZTECH> show route 2020:2020::/64

inet6.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

2020:2020::/64     *[Access/13] 00:02:28, metric 20, tag 10
                       Private unicast

admin@MX204-LAB-WZTECH>
```

Neste caso a rota 2020:2020::/64 foi instalada no BNG para o assinante com métrica 20 e tag 10. Toda rota enviada pelo RADIUS utilizando este AVP Framed-IPv6-Route sendo prefixo de host /128 ou de rede é instalada no BNG como tipo access. Todos os prefixos IPv6 atribuídos aos assinantes instalados pelo RADIUS (utilizando os AVP's Framed-IPv6-Pool, ERX-IPv6-Delegated-Pool-Name, Framed-IPv6-Prefix, Delegated-IPv6-Prefix) ou obtidos localmente no BNG, caso o endereço seja /128 ele será instalado como access-internal. Caso o prefixo seja menor que /128 ele será instalado como access. Estas definições de como o prefixo é instalado (access ou access-internal) podem ser utilizadas posteriormente em políticas de exportação de rotas utilizando protocolo de roteamento dinâmico.

Caso o AVP seja configurado no RADIUS com sintaxe errada e o BNG não consiga processar o AVP ele será descartado. O usuário se conectará mas não receberá a rota IPv6.

7.5. IPv4 - Access-Routes

```
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options access route $junos-framed-route-ip-address-prefix next-hop "$junos-framed-route-nexthop"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options access route $junos-framed-route-ip-address-prefix metric "$junos-framed-route-cost"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options access route $junos-framed-route-ip-address-prefix preference "$junos-framed-route-distance"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options access route $junos-framed-route-ip-address-prefix tag "$junos-framed-route-tag"
```

As definições de access route não são obrigatórias. Elas têm o propósito também de receber as rotas IPv4 pelo RADIUS com as devidas definições de tag, distancia e métrica. Se não for configurado as definições de "access route" caso o RADIUS envie o atributo Framed-Route esta rota não será instalada no BNG.

O funcionamento é exatamente o mesmo do IPv6. O nome do atributo no RADIUS é Framed-Route:

Framed-Route = "200.0.0.0/24"

Desta forma no AVP o usuário vai receber uma rota com a rede 200.0.0.0/24. Neste caso não é obrigatório definir o gateway no AVP pois o FreeRADIUS vai adicionar o valor 0.0.0.0 no gateway e metric 1 na metrica automaticamente.

Framed-Route = "200.0.0.0/24 0.0.0.0 20 tag 10 pref 100"

Caso queira enviar além da rede os parâmetros da rota como métrica, tag e preferência é necessário na frente do prefixo definir um gateway (pode ser utilizado sempre o valor 0.0.0.0 pois o BNG vai descartar qualquer valor de gateway enviado e vai criar a rota apontando para a interface pp0.<unit> do usuario), depois o valor de métrica, depois o parametro tag com o devido valor de tag e por ultimo o parametro pref com o devido valor de preferência.

```
admin@MX204-LAB-WZTECH> show route 200.0.0.0/24

inet.0: 9 destinations, 9 routes (9 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

200.0.0.0/24       *[Access/13] 00:10:29, metric 20, tag 10
                        Private unicast
```

No exemplo acima a rota 200.0.0.0/24 foi instalada para o assinante com métrica 20 e tag 10. Toda rota enviada pelo RADIUS utilizando este AVP Framed-Route sendo rota de host /32 ou de rede é instalada no BNG como tipo access.

Caso o AVP seja configurado no RADIUS com sintaxe errada e o BNG não consiga processar o AVP ele será descartado. O usuário se conectará mas não receberá a rota IPv4.

Importante: Para alocar um endereço fixo IPv4 para um usuário pelo RADIUS utilizando o AVP Framed-IP-Address não é necessário configuração de "access route". Esta configuração de "access route" é apenas necessária envio de rotas IPv4 através do AVP Framed-Route. O endereço IP recebido pelo Framed-IP-Address é instalado internamente no BNG como tipo access-internal:

Framed-IP-Address = 80.80.80.80

```
admin@MX204-LAB-WZTECH> show route 80.80.80.80

inet.0: 9 destinations, 9 routes (9 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

80.80.80.80/32     *[Access-internal/12] 00:05:09
                        Private unicast
```

7.6. Actual-Transit-Statistics - Accounting Acurado

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" actual-transit-statistics
```

Esta configuração não é obrigatória, mas é recomendada pela Juniper. Com esta configuração o BNG faz uma contabilização de pacotes e bytes de forma mais acurada. Neste caso o BNG despreza a contabilização de pacotes descartados por firewall filters, pacotes de controle, bytes de overhead, etc e envia para o RADIUS apenas a contabilização de bytes e pacotes que realmente usados pelo assinante que passaram pelo BNG. O propósito é ter uma contabilização mais adequada para o tráfego contabilizando apenas o que de fato que foi utilizado pelo usuário. Para que as informações de bytes e pacotes sejam reportadas para o RADIUS é necessário que seja configurado a opção volume-time na configuração do radius-server. Exemplo:

```
set access profile ACCESS-PROFILE accounting statistics volume-time
```

Com a configuração do volume-time o BNG mostra que os dados de pacotes e bytes estão sendo contabilizados para o usuário:

```
admin@MX204-LAB-WZTECH> show subscribers accounting-statistics interface pp0.3221225496
Session ID: 35
```

```
Interface: pp0.3221225496
Accounting Statistics
   Input bytes: 125842
   Input packets: 1630
   Output bytes: 33156
   Output packets: 662
IPv6
   Input bytes: 400
   Input packets: 5
   Output bytes: 320
   Output packets: 4
```

Também a partir do momento é que é ligado o volume-time na configuração o BNG passa a enviar no Accounting para o RADIUS alguns AVP's IPv4 e IPv6 de contadores de pacotes e bytes:

(11) Acct-Input-Octets = 3360
(11) Acct-Output-Octets = 2192
(11) Acct-Input-Packets = 40
(11) Acct-Output-Packets = 29
(11) ERX-Input-Gigapkts = 0
(11) ERX-Output-Gigapkts = 0
(11) Acct-Output-Gigawords = 0
(11) Acct-Input-Gigawords = 0

(11) ERX-IPv6-Acct-Input-Octets = 0
(11) ERX-IPv6-Acct-Output-Octets = 0
(11) ERX-IPv6-Acct-Input-Packets = 0
(11) ERX-IPv6-Acct-Output-Packets = 0
(11) ERX-IPv6-Acct-Input-Gigawords = 0
(11) ERX-IPv6-Acct-Output-Gigawords = 0

Para monitorar a banda do usuário não é necessário nem a configuração de actual-transit-statistics nem a configuração de volume-time. Sempre é possível monitorar a banda em bps e pps tanto pela interface demux0.<unit> quanto pela interface pp0.<unit> sendo que na interface pp0.<unit> é possível ver a banda do IPv4 e IPv6 separadas:

```
monitor interface demux0.3221225501

Next='n', Quit='q' or ESC, Freeze='f', Thaw='t', Clear='c', Interface='i'
MX204-LAB-WZTECH                  Seconds: 30                 Time: 09:26:28
                                                            Delay: 0/0/0
Interface: demux0.3221225501, Enabled, Link is Up
Flags:
Encapsulation: ENET2
VLAN-Tag [ 0x8100.200 ]
Remote statistics:
  Input bytes:                    1581158 (1330224 bps)              [1551135]
  Output bytes:                 129769169 (103108960 bps)          [129755737]
  Input packets:                   31579 (3360 pps)                    [31199]
  Output packets:                  89539 (8877 pps)                    [89408]
Traffic statistics:
  Input bytes:                    1581158                            [1551135]
  Output bytes:                 129769169                          [129755737]
  Input packets:                   31579                               [31199]
  Output packets:                  89539                               [89408]

monitor interface pp0.3221225502

Next='n', Quit='q' or ESC, Freeze='f', Thaw='t', Clear='c', Interface='i'
MX204-LAB-WZTECH                  Seconds: 21                 Time: 09:26:26
                                                            Delay: 0/0/0
Interface: pp0.3221225502, Enabled, Link is Up
Flags: Point-To-Point
Encapsulation: PPPoE
Remote statistics:
  Input bytes:                     743248 (412312 bps)                [713413]
  Output bytes:                  73112167 (57955384 bps)            [73098941]
  Input packets:                   17126 (1157 pps)                    [16738]
  Output packets:                  50500 (4989 pps)                    [50381]
IPv6 statistics:
  Input bytes:                         0 (0 bps)                          [0]
  Output bytes:                        0 (0 bps)                          [0]
```

```
  Input packets:                          0 (0 pps)                          [0]
  Output packets:                         0 (0 pps)                          [0]
Traffic statistics:
  Input bytes:                       743248                              [713413]
  Output bytes:                    73112167                            [73098941]
  Input packets:                      17126                               [16738]
  Output packets:                     50500                               [50381]
Protocol: inet, MTU: 1492, Flags: 0x20000000
```

7.7. Autenticação PPP - PAP/CHAP

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" ppp-options chap
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" ppp-options pap
```

As duas linhas acima definem qual o tipo de autenticação que será utilizado no protocolo PPP. Pelo menos uma das opções (pap ou chap) deve ser habilitada. Recomendado habilitar as duas. Se não for configurado nem PAP nem CHAP o assinante vai se conectar sem se autenticar no RADIUS. O BNG vai enviar para o RADIUS apenas o Accounting.

Se for configurado ambas as opções (PAP e CHAP) o BNG vai enviar CHAP para a ONU na negociação da autenticação. Se ela aceitar com o ACK vai ser utilizado CHAP da ONU até o BNG e do BNG até o RADIUS Server. Se a ONU não aceitar CHAP o BNG tenta negociar PAP. Se a ONU aceitar PAP vai ser PAP da ONU até o BNG e PAP do BNG até o RADIUS.

No protocolo PAP o usuário e senha é enviado em texto claro até o BNG e do BNG para o radius é crifado no campo User-Password com a secret do radius.

Já no protocolo CHAP a senha do usuário é cifrada da ONU até o BNG e os AVP's que autenticam o usuário no RADIUS são CHAP-Password e CHAP-Challenge. Não é enviado User-Password na autenticação para o RADIUS. Neste caso o RADIUS tem que suportar autenticação CHAP.

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet rpf-check
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet filter input "$junos-
input-filter"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet filter output "$junos-
output-filter"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet unnumbered-address
"$junos-loopback-interface"
```

Este bloco acima de configurações são configurações aplicadas para a familia inet (IPv4):

7.8. IPv4 - Anti-Spoofing - RPF-Check

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet rpf-check
```

Esta configuração de rpf-check habilitada na familia inet habilita o recurso de anti-spoof do BNG na interface pp0.<unit> para a familia IPv4. Não é obrigatória, mas recomendável. Por default se um usuário tentar gerar pacotes com endereços IPv4 diferentes do que foi alocado para ele estes pacotes são permitidos. Quando habilita o rpf-check o BNG passa a usar o mecanismo de RPF (Reverse Path Forwarding) e neste caso para que um pacote seja permitindo pela interface do usuário é necessário que o endereço IP de origem do pacote seja conhecido por aquela interface pp0.<unit>. Caso o endereço IPv4 não seja conhecido por aquela interface o pacote é descartado.

7.9. IPv4 - Firewall Filters - INPUT/OUTPUT

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet filter input "$junos-
input-filter"
```

Esta configuração de filter input "$junos-input-filter" já mencionada em partes anteriormente habilita o BNG a receber o atributo ERX-Ingress-Policy-Name (Vendor 4874 / Atributo 10) do RADIUS. Ela não é obrigatória, mas sem ela o assinante não terá firewall filter aplicada de input no protocolo IPv4 (a não ser no cenário de uso de profile de serviço com variáveis dinâmicas). Com esta configuração feita no BNG é obrigatório que o RADIUS envie o AVP ERX-Ingress-Policy-Name com o nome da firewall filter IPv4 que deve ser associada ao usuário no sentido de INPUT. Esta firewall filter é definida em "firewall family inet filter".

Exemplo:

```
set firewall family inet filter 100M-IPV4-IN interface-specific
set firewall family inet filter 100M-IPV4-IN term POLICER then policer 20Mbps
set firewall family inet filter 100M-IPV4-IN term POLICER then next term
set firewall family inet filter 100M-IPV4-IN term FILTRO-PADRAO-IN filter FILTRO-PADRAO-IPV4-IN

set firewall policer 20Mbps logical-interface-policer
set firewall policer 20Mbps if-exceeding bandwidth-limit 20m
set firewall policer 20Mbps if-exceeding burst-size-limit 2m
set firewall policer 20Mbps then discard
```

Exemplo de definição no RADIUS:

ERX-Ingress-Policy-Name = 100M-IPV4-IN

Caso o RADIUS não envie o AVP com o nome da firewall filter existente no BNG o BNG tentará alocar a firewall filter definida na variavel predefined chamada input-filter:

```
set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults input-filter PREDEFINED-IPV4-IN
```

Caso esteja variável não esteja configurada o usuário não vai se conectar.

Caso não seja configurado no BNG a family inet filter input significa que não é esperado que o RADIUS envie o atributo. Desta forma não fará diferença o RADIUS enviar ou não o atributo e não fará diferença ter ou não a configuração da variável predefinida input-filter. O usuário vai conectar e vai navegar sem nenhum filtro e sem nenhum controle de banda. O único caso onde estes controles serão ativados sem esta configuração utilizando o modelo de variáveis dinâmicas enviando os atributos de policer pelo radius. Isto será detalhado posteriormente.

Importante: Se for enviado pelo RADIUS um nome de firewall que não exista no BNG o assinante NÃO vai se conectar. O BNG nao deixa o assinante se conectar pois nao tem o filtro que está sendo enviado. Neste caso a variável predefinida não vai atuar pois o RADIUS mandou o AVP com um nome e esse nome não existe.

Quando a firewall filter é de fato ativada no usuário ela é exibida em IPv4 Input Filter no output do comando show subscribers. Exemplo:

```
admin@MX204-LAB-WZTECH> show subscribers user-name wztech3 extensive
Type: PPPoE
User Name: wztech3
IP Address: 80.80.80.80
IP Netmask: 255.255.255.255
Primary DNS Address: 8.8.8.8
Secondary DNS Address: 8.8.4.4
IPv6 Address: 4444:ee4:4000:100::
IPv6 Prefix: 1010:ee4:4000::/64
Domain name server inet6: 2001:4860:4860::8888 2001:4860:4860::8844
IPv6 User Prefix: 2804:ee4:8000:a::/64
Logical System: default
Routing Instance: default
Interface: pp0.3221225637
Interface type: Dynamic
Underlying Interface: demux0.3221225636
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 11
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 207
Session ID: 207
PFE Flow ID: 260
VLAN Id: 200
Login Time: 2023-08-11 22:25:54 -03
IPv6 Address Pool: _DAPV6
IPv6 Framed Interface Id: c96d:72cc:dbbd:7bea
IPv4 Input Filter Name: 100M-IPV4-IN-pp0.3221225637-in
IPv4 Output Filter Name: 100M-IPV4-OUT-pp0.3221225637-out
IPv6 Input Filter Name: 100M-IPV6-IN-pp0.3221225637-in
IPv6 Output Filter Name: 100M-IPV6-OUT-pp0.3221225637-out
Accounting interval: 0
```

```
Dynamic configuration:
  junos-framed-route-ip-address-prefix: 200.0.0.0/32
      junos-framed-route-nexthop: 0.0.0.0
          junos-framed-route-cost: 20
          junos-framed-route-tag: 10
      junos-framed-route-ipv6-address-prefix: 2020:2020::/128
          junos-framed-route-ipv6-nexthop: ::
          junos-framed-route-ipv6-cost: 20
          junos-framed-route-ipv6-tag: 10
  junos-input-filter: 100M-IPV4-IN
  junos-input-ipv6-filter: 100M-IPV6-IN
  junos-ipv6-ndra-prefix: 2804:ee4:8000:a::/64
  junos-output-filter: 100M-IPV4-OUT
  junos-output-ipv6-filter: 100M-IPV6-OUT
```

A firewall filter sendo exibida em Dynamic configuration não significa que está ativa. Apenas significa que foi recebida pelo RADIUS.

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet filter output "$junos-output-filter"
```

Mesma explicação e funcionamento da filter input. Neste caso como é filter output com a variável "$junos-output-filter" é a firewall filter que vai ser utilizada no sentido output do BNG (tráfego destinado ao assinante). Neste caso no RADIUS é utilizado o AVP ERX-Egress-Policy-Name (Vendor 4874 / Atributo 11).

Exemplo de configuração no RADIUS e BNG:

ERX-Egress-Policy-Name = 100M-IPV4-OUT

```
set firewall family inet filter 100M-IPV4-OUT interface-specific
set firewall family inet filter 100M-IPV4-OUT term FILTRO-PADRAO-OUT filter FILTRO-PADRAO-IPV4-OUT
set firewall family inet filter 100M-IPV4-OUT term POLICER then policer 100Mbps

set firewall policer 100Mbps logical-interface-policer
set firewall policer 100Mbps if-exceeding bandwidth-limit 100m
set firewall policer 100Mbps if-exceeding burst-size-limit 12m
set firewall policer 100Mbps then discard
```

7.10. IPv4 - Unnumbered Loopback Interface

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet unnumbered-address "$junos-loopback-interface"
```

Esta configuração é obrigatória para a alocação de endereço IPv4. Esta definição fala para o protocolo PPP na negociação da camada IPCP qual o endereço IP do BNG. A configuração de unnumbered-address "$junos-loopback-interface" informa ao BNG que é para ele herdar o endereço IPv4 da interface loopback unit 0 para esta negociação. Neste caso é obrigatório que a interface loopback tenha um endereço IPv4 configurado na unit 0. Exemplo:

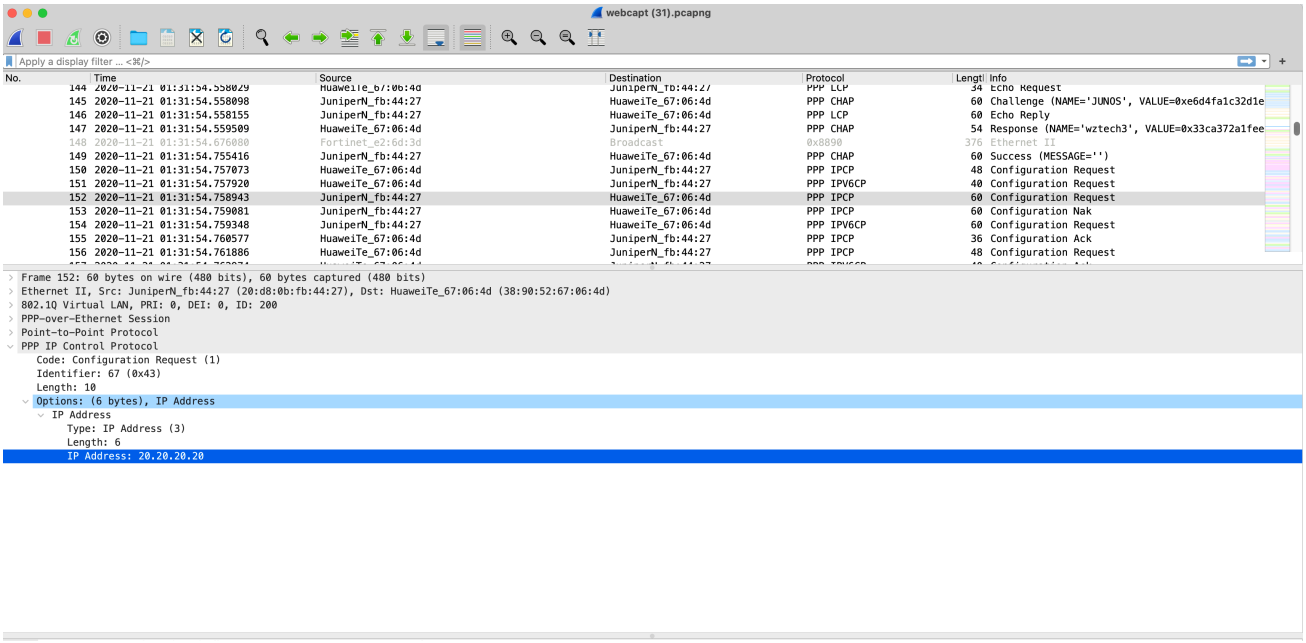
```
set interfaces lo0 unit 0 family inet address 20.20.20.20/32
```

Caso queira informar um outro endereço IP na negociação do IPCP pode-se configurar diretamente o endereço IPv4 ao invés de configurar unnumbered-address:

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet address 30.30.30.30
```

De todas as formas alguma das duas opções tem que ser configurada pois sem esta configuração o assinante não vai se conectar.

Exemplo da negociação do endereço IPv4 do BNG no IPCP do protocolo PPP:



O BNG informou o endereço IPv4 à ONU.

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 rpf-check
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 filter input "$junos-input-ipv6-filter"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 filter output "$junos-output-ipv6-filter"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 unnumbered-address "$junos-loopback-interface"
```

O bloco de configuração acima é para o protocolo IPv6 (family inet6):

7.11. IPv6 - Anti-Spoofing - RPF-Check

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 rpf-check
```

Mesmo funcionamento e explicação do rpf-check da familia inet. O único ponto de atenção a essa configuração para IPv6 é no caso do uso de VRF. Caso vá ser feito uso de VRF no BNG utilizando o AVP ERX-Virtual-Router-Name o rpf-check para inet6 precisa ser desativado senão os endereços IPv6 não serão alocados na VRF.

7.12. IPv6 - Firewall Filters - INPUT/OUTPUT

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 filter input "$junos-input-ipv6-filter"
```

Mesmo funcionamento e explicação da family inet filter input. Neste caso é a configuração do BNG para receber firewal filter de input para a familia de protocolo IPv6 (family inet6) com o AVP ERX-IPv6-Ingress-Policy-Name (Vendor 4874 / Atributo 106) do RADIUS.

Exemplo de configuracão do RADIUS e BNG:

ERX-IPv6-Ingress-Policy-Name = 100M-IPV6-IN

```
set firewall family inet6 filter 100M-IPV6-IN interface-specific
set firewall family inet6 filter 100M-IPV6-IN term POLICER then policer 20Mbps
set firewall family inet6 filter 100M-IPV6-IN term POLICER then next term
set firewall family inet6 filter 100M-IPV6-IN term FILTRO-PADRAO-IPV6-IN filter FILTRO-PADRAO-IPV6-IN

set firewall policer 20Mbps logical-interface-policer
set firewall policer 20Mbps if-exceeding bandwidth-limit 20m
set firewall policer 20Mbps if-exceeding burst-size-limit 2m
set firewall policer 20Mbps then discard
```

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 filter output "$junos-output-ipv6-filter"
```

Mesmo funcionamento e explicação da family inet6 filter output. Neste caso está habilitando o BNG para receber a firewall filter do protocolo IPv6 para ser aplicada no sentido output (tráfego destinado ao usuário). O AVP enviado pelo RADIUS para este caso é o ERX-IPv6-Egress-Policy-Name (Vendor 4874 / Atributo 107).

Exemplo de configuração no RADIUS e BNG:

ERX-IPv6-Egress-Policy-Name = 100M-IPV6-OUT

```
set firewall family inet6 filter 100M-IPV6-OUT interface-specific
set firewall family inet6 filter 100M-IPV6-OUT term FILTRO-PADRAO-OUT filter FILTRO-PADRAO-IPV6-OUT
set firewall family inet6 filter 100M-IPV6-OUT term POLICER then policer 100Mbps

set firewall policer 100Mbps logical-interface-policer
set firewall policer 100Mbps if-exceeding bandwidth-limit 100m
set firewall policer 100Mbps if-exceeding burst-size-limit 12m
set firewall policer 100Mbps then discard
```

7.13. IPv6 - Unnumbered Loopback Interface

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 unnumbered-address "$junos-loopback-interface"
```

Mesmo funcionamento e explicação da family inet. Esta configuração é obrigatória para a alocação de endereço IPv6. A diferença é que no caso do IPV6CP o BNG não informa este endereço na negociação, mas um outro parâmetro chamado Interface Identifier. De todas as formas se não houver um endereço IPv6 na unit 0 da interface loopback o usuário não vai receber endereços IPv6.

Exemplo da configuração da interface loopback:

```
set interfaces lo0 unit 0 family inet6 address 2001:1291::2/128
```

Caso queira informar um outro endereço IP na negociação do IPV6CP pode-se configurar diretamente o endereço IPv6 ao invés de configurar unnumbered-address: Exemplo:

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 address 3030:1291::2/128
```

7.14. IPv6 - NDRA (SLAAC)

A seguir as configurações para habilitar o protocolo NDRA/SLAAC.

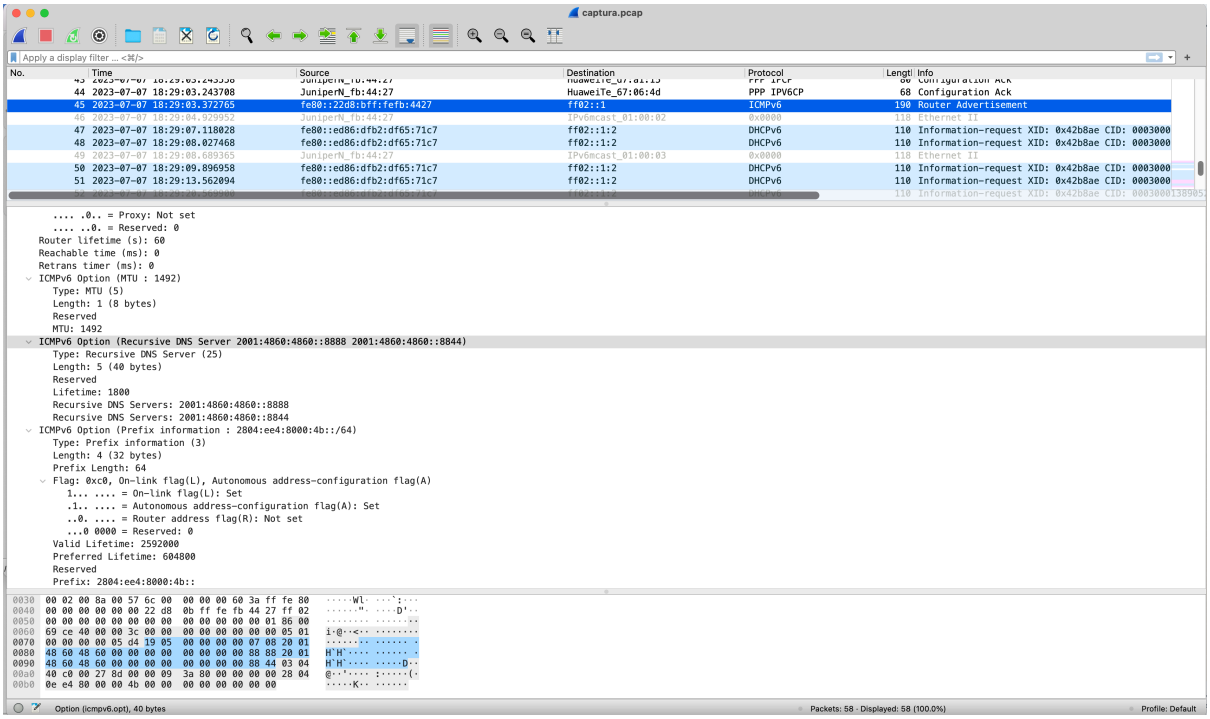
```
set dynamic-profiles SUBSCRIBER-PROFILE protocols router-advertisement interface "$junos-interface-name" dns-server-address $junos-ipv6-dns-server-address
set dynamic-profiles SUBSCRIBER-PROFILE protocols router-advertisement interface "$junos-interface-name" prefix $junos-ipv6-ndra-prefix
```

Esta configuração de "protocols router-advertisement" na profile do assinante SUBSCRIBER-PROFILE habilita o SLAAC. No BNG o modelo para a ONU pegar IPv6 na WAN é através de NDRA (SLAAC) ou DHCP IA_NA. É um ou outro. Existe uma forma de funcionamento dos dois em conjunto mas não há suporte oficial pelo fabricante e tem algumas considerações haja vista que alguns atributos de RADIUS para os dois casos são os mesmos.

```
set dynamic-profiles SUBSCRIBER-PROFILE protocols router-advertisement interface "$junos-interface-name" dns-server-address $junos-ipv6-dns-server-address
```

A configuração acima faz com que o BNG envie nas mensagens de ICMPv6 Router Advertisement os DNS's IPv6 configurados no BNG. Se não for configurado esta linha, nas mensagens de ICMPv6 RA não serão informados os DNS's IPv6 para a conexão WAN. No caso por exemplo de uma ONU como bridge onde não existe o processo de DHCPv6 IA_PD o usuário vai se conectar com NDRA ele não vai receber DNS sem essa linha para o protocolo IPv6.

DNS's informados no RA:



Importante: Com a variavel $junos-ipv6-dns-server-address configurada é obrigatório que o BNG encontre os DNS's SLAAC para serem enviados nas mensagens de Router Advertisement. Normalmente estes DNS's são definidos na access-profile que está autenticando o usuário:

Exemplo:


```
set access profile ACCESS-PROFILE domain-name-server-inet6 2001:4860:4860::8888
set access profile ACCESS-PROFILE domain-name-server-inet6 2001:4860:4860::8844
```

Se os DNS's IPv6 não forem encontrados pelo BNG, o usuário não vai se conectar em IPv6. No BNG vai aparecer o prefixo NDRA alocado, mas na ONU o usuário não se conecta.

O detalhamento de todas as opções para o BNG encontrar os DNS's que serão enviados para o usuário no NDRA encontra-se neste documento no item de DNS NDRA da access profile.

```
set dynamic-profiles SUBSCRIBER-PROFILE protocols router-advertisement interface "$junos-interface-name" prefix $junos-ipv6-ndra-prefix
```

Esta configuração da variável $junos-ipv6-ndra-prefix instrui o BNG que ele deverá começar a advertir o prefixo SLAAC informado pelo RADIUS (caso seja recebido o prefixo pelo RADIUS através do AVP Framed-IPv6-Prefix ou o Pool através do AVP Framed-IPv6-Pool) e caso não seja recebido nada pelo RADIUS que o BNG deve fazer a alocação de um prefixo do pool configurado em [access address-assignment neighbor-discovery-router-advertisement] para o assinante:

```
set access address-assignment neighbor-discovery-router-advertisement POOL-V6-NDRA
```

Neste caso existe um pool IPv6 chamado POOL-V6-NDRA:

```
set access address-assignment pool POOL-V6-NDRA family inet6 prefix 2804:0ee4:8000::/48
set access address-assignment pool POOL-V6-NDRA family inet6 range RANGE-PARA-NDRA prefix-length 64
```

Desta forma, com a configuração acima caso o RADIUS não envie um pool NDRA ou não envie um prefixo NDRA o BNG vai alocar um prefixo de tamanho 64 (prefix-lenght /64) para o assinante do prefixo /48 configurado no pool POOL-V6-NDRA e o BNG vai fazer o Router Advertisement deste prefixo para o assinante.

No BNG ele aceita configurar o pool NDRA com prefixos de tamanho menores que /64 (até /127) porém na ONU geralmente só vai aceitar prefixos /64 ou maiores para fazer o processo do EUI-64 local senão o usuário não conecta. Este comportamento vai depender da implementação da ONU.

No modelo de ONU testado quando é enviado um prefixo maior que /64 (/56 por exemplo) a ONU não conecta. Existe a configuração para ser derivados prefixos /64 a partir de um prefixo maior recebido. Se for o caso de configurar prefixos maiores que /64 no BNG para o usuário é necessário validar com o fabricante da ONU o comportamento esperado.

Caso seja deletado a configuração geral de [protocols router-advertisement] da subscriber profile do assinante (SUBSCRIBER-PROFILE) o BNG não faz mais NDRA nem de forma automática usando o prefixo apontado em [access address-assignment neighbor-discovery-router-advertisement] e nem utilizando o pool ou prefixo NDRA caso tenha sido recebido por RADIUS. Neste cenário a ONU obrigatoriamente precisa pedir o IP de WAN via DHCPv6 IA_NA. No modelo de DHCP IA_NA na WAN é altamente recomendado que esta configuração de [protocolos router-advertisement] seja deletado da subscriber profile. Desta forma, os atributos de RADIUS Framed-IPv6-Pool e Framed-IPv6-Prefix serão usados para o DHCP IA_NA tanto para envio das informações para o BNG quanto do BNG para o RADIUS no processo de Accounting haja vista que o NDRA foi desabilitado.

Quando a configuração do [protocols router-advertisement] está ativa mas foi desativado/deletado a configuração do [prefix $junos-ipv6-ndra-prefix] significa que a caixa ainda está suportando NDRA e vai fazer Router Advertisement na conexão PPPoE, porém não há um prefixo automático para ser feito o Router Advertisement de forma automática e também não é possível ser recebido este prefixo ou pool por RADIUS. Neste caso o comportamento de como vai ser alocado o IP vai depender de como a ONU está configurada.

Quando a configuração do [protocols router-advertisement] está ativa com a configuração correta de [prefix $junos-ipv6-ndra-prefix] mas foi desativado/deletado a configuração do [access address-assignment neighbor-discovery-router-advertisement] significa que a caixa ainda está suportando NDRA e vai fazer Router Advertisement, porém não há um prefixo default para ser feito o Router Advertisement de forma automática. Desta forma, caso venha o prefixo NDRA ou pool NDRA do RADIUS será feito o Router Advertisement deste prefixo ou pool recebido pelo RADIUS. Se o RADIUS não enviar nenhum prefixo ou pool NDRA o comportamento de como vai ser alocado o IP vai depender de como a ONU está configurada. Algumas ONU's podem neste caso fazer o DHCPv6 Solicit e outras não e este comportamento vai depender do firmware da ONU.

8. Service Profile com Variáveis Dinâmicas

Além das profiles dinâmicas de VLAN (VLAN Profile) e profiles dinâmicas de assinante (Subscriber Profile ou Client Profile) o BNG suporta também profiles dinâmicas de serviços (Service Profile).

A service profile é um tipo de dynamic profile que pode ser enviada pelo RADIUS onde os atributos de banda, burst e outros parâmetros podem ser enviados diretamente pelo RADIUS de forma dinâmica.

Neste modelo a subscriber profile do assinante não pode ter nenhuma configuração relacionado à filter, visto que esta parte de configuração de firewall filter será configurada na Service Profile que será enviada pelo protocolo RADIUS.

Neste modelo a VLAN do assinante está associada a uma VLAN Profile que por sua vez chama uma Subscriber Profile (que não tem mais nenhuma configuração relacionada à firewall filter). Todas as configurações abaixo são removidas da Subscriber Profile quando vai ser utilizado o modelo de Service Profile:

```
- set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults input-filter PREDEFINED-IPV4-IN
- set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults output-filter PREDEFINED-IPV4-OUT
- set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults input-ipv6-filter PREDEFINED-IPV6-IN
- set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults output-ipv6-filter PREDEFINED-IPV6-OUT
- set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet filter input "$junos-
input-filter"
- set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet filter output "$junos-
output-filter"
```

```
- set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 filter input "$junos-
input-ipv6-filter"
- set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 filter output "$junos-
output-ipv6-filter"
```

Exemplo de da configuração da Subscriber Profile nova que será usada em conjunto com a Service Profile enviada pelo RADIUS:

```
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" interface "$junos-
interface-name"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options rib
"$junos-ipv6-rib" access route $junos-framed-route-ipv6-address-prefix qualified-next-hop "$junos-interface-name"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options rib
"$junos-ipv6-rib" access route $junos-framed-route-ipv6-address-prefix metric "$junos-framed-route-ipv6-cost"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options rib
"$junos-ipv6-rib" access route $junos-framed-route-ipv6-address-prefix preference "$junos-framed-route-ipv6-distance"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options rib
"$junos-ipv6-rib" access route $junos-framed-route-ipv6-address-prefix tag "$junos-framed-route-ipv6-tag"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options access
route $junos-framed-route-ip-address-prefix next-hop "$junos-framed-route-nexthop"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options access
route $junos-framed-route-ip-address-prefix metric "$junos-framed-route-cost"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options access
route $junos-framed-route-ip-address-prefix preference "$junos-framed-route-distance"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options access
route $junos-framed-route-ip-address-prefix tag "$junos-framed-route-tag"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO interfaces pp0 unit "$junos-interface-unit" actual-transit-statistics
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO interfaces pp0 unit "$junos-interface-unit" ppp-options chap
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO interfaces pp0 unit "$junos-interface-unit" ppp-options pap
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO interfaces pp0 unit "$junos-interface-unit" family inet rpf-check
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO interfaces pp0 unit "$junos-interface-unit" family inet unnumbered-
address "$junos-loopback-interface"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO interfaces pp0 unit "$junos-interface-unit" family inet6 rpf-check
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO interfaces pp0 unit "$junos-interface-unit" family inet6 unnumbered-
address "$junos-loopback-interface"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO protocols router-advertisement interface "$junos-interface-name" dns-
server-address $junos-ipv6-dns-server-address
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO protocols router-advertisement interface "$junos-interface-name"
prefix $junos-ipv6-ndra-prefix
```


Configuração da Service Profile que será enviada pelo RADIUS utilizando o AVP ERX-Service-Activate (Vendor 4874 / Atributo 65):

```
set dynamic-profiles SERVICE-PROFILE variables BANDWIDTH-IN mandatory
set dynamic-profiles SERVICE-PROFILE variables BANDWIDTH-OUT mandatory
set dynamic-profiles SERVICE-PROFILE variables BURST-IN default-value 2m
set dynamic-profiles SERVICE-PROFILE variables BURST-OUT default-value 2m
set dynamic-profiles SERVICE-PROFILE variables POLICER-IN uid
set dynamic-profiles SERVICE-PROFILE variables POLICER-OUT uid
set dynamic-profiles SERVICE-PROFILE variables FILTERv4-IN uid
set dynamic-profiles SERVICE-PROFILE variables FILTERv4-OUT uid
set dynamic-profiles SERVICE-PROFILE variables FILTERv6-IN uid
set dynamic-profiles SERVICE-PROFILE variables FILTERv6-OUT uid
set dynamic-profiles SERVICE-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet filter input "$FILTERv4-IN"
set dynamic-profiles SERVICE-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet filter output "$FILTERv4-
OUT"
set dynamic-profiles SERVICE-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 filter input "$FILTERv6-IN"
set dynamic-profiles SERVICE-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 filter output "$FILTERv6-
OUT"
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" interface-specific
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term POLICER then policer "$POLICER-IN"
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term POLICER then next term
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term DESCARTA-PORTAS-INPUT from
destination-port 1900
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term DESCARTA-PORTAS-INPUT from
destination-port 25
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term DESCARTA-PORTAS-INPUT then discard
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term DROP-AMPLIFICATION from protocol udp
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term DROP-AMPLIFICATION from source-port
53
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term DROP-AMPLIFICATION from source-port
161
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term DROP-AMPLIFICATION from source-port
123
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term DROP-AMPLIFICATION from source-port
1900
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term DROP-AMPLIFICATION from source-port
111
```

```
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term DROP-AMPLIFICATION from source-port
137
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term DROP-AMPLIFICATION from source-port
10001
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term DROP-AMPLIFICATION then discard
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term BYPASS-LOOPBACK-LOCAL from
destination-address 20.20.20.20/32
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term BYPASS-LOOPBACK-LOCAL then accept
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term BYPASS-TRAFEGO-LOCAL from
destination-address 200.225.230.0/24
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term BYPASS-TRAFEGO-LOCAL from
destination-address 200.225.231.0/24
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term BYPASS-TRAFEGO-LOCAL from
destination-address 200.225.232.0/24
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term BYPASS-TRAFEGO-LOCAL from
destination-address 200.225.233.0/24
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term BYPASS-TRAFEGO-LOCAL from
destination-address 20.20.20.20/32
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term BYPASS-TRAFEGO-LOCAL then accept
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term DESVIA-TRAFEGO-CGNAT from source-
address 100.64.0.0/10
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term DESVIA-TRAFEGO-CGNAT then next-ip
172.17.17.2/32
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-IN" term ACCEPT then accept
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-OUT" interface-specific
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-OUT" term BLOQUEIA-PORTAS-OUT from
destination-port 0-1023
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-OUT" term BLOQUEIA-PORTAS-OUT then discard
set dynamic-profiles SERVICE-PROFILE firewall family inet filter "$FILTERv4-OUT" term 1 then policer "$POLICER-OUT"
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" interface-specific
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DHCPV6POLICER from next-header udp
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DHCPV6POLICER from source-port 546
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DHCPV6POLICER from destination-port
547
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DHCPV6POLICER then policer
DHCPPOLICER
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DHCPV6POLICER then next term
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term POLICER then policer "$POLICER-IN"
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term POLICER then next term
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DESCARTA-PORTAS-INPUT-TCP from
next-header tcp
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DESCARTA-PORTAS-INPUT-TCP from
destination-port 25
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DESCARTA-PORTAS-INPUT-TCP then
discard
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DESCARTA-PORTAS-INPUT-UDP from
next-header udp
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DESCARTA-PORTAS-INPUT-UDP from
destination-port 1900
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DESCARTA-PORTAS-INPUT-UDP then
discard
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DROP-AMPLIFICATION from next-header
udp
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DROP-AMPLIFICATION from source-port
53
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DROP-AMPLIFICATION from source-port
1900
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DROP-AMPLIFICATION from source-port
10001
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DROP-AMPLIFICATION from source-port
137
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DROP-AMPLIFICATION from source-port
123
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DROP-AMPLIFICATION from source-port
161
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DROP-AMPLIFICATION from source-port
111
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term DROP-AMPLIFICATION then discard
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-IN" term ACCEPT then accept
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-OUT" interface-specific
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-OUT" term BLOQUEIA-PORTAS-OUT from next-
header tcp
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-OUT" term BLOQUEIA-PORTAS-OUT from next-
header udp
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-OUT" term BLOQUEIA-PORTAS-OUT from
destination-port 0-1023
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-OUT" term BLOQUEIA-PORTAS-OUT then discard
set dynamic-profiles SERVICE-PROFILE firewall family inet6 filter "$FILTERv6-OUT" term 1 then policer "$POLICER-OUT"
set dynamic-profiles SERVICE-PROFILE firewall policer "$POLICER-IN" filter-specific
set dynamic-profiles SERVICE-PROFILE firewall policer "$POLICER-IN" logical-interface-policer
set dynamic-profiles SERVICE-PROFILE firewall policer "$POLICER-IN" if-exceeding bandwidth-limit "$BANDWIDTH-IN"
set dynamic-profiles SERVICE-PROFILE firewall policer "$POLICER-IN" if-exceeding burst-size-limit "$BURST-IN"
set dynamic-profiles SERVICE-PROFILE firewall policer "$POLICER-IN" then discard
```

```
set dynamic-profiles SERVICE-PROFILE firewall policer "$POLICER-OUT" filter-specific
set dynamic-profiles SERVICE-PROFILE firewall policer "$POLICER-OUT" logical-interface-policer
set dynamic-profiles SERVICE-PROFILE firewall policer "$POLICER-OUT" if-exceeding bandwidth-limit "$BANDWIDTH-OUT"
set dynamic-profiles SERVICE-PROFILE firewall policer "$POLICER-OUT" if-exceeding burst-size-limit "$BURST-OUT"
set dynamic-profiles SERVICE-PROFILE firewall policer "$POLICER-OUT" then discard

set firewall policer DHCPPOLICER logical-interface-policer
set firewall policer DHCPPOLICER if-exceeding-pps pps-limit 4
set firewall policer DHCPPOLICER if-exceeding-pps packet-burst 1
set firewall policer DHCPPOLICER then discard
```

As configurações de firewall filter neste modelo são as mesmas existentes nas firewall filters IPv4 e IPv6 dos assinantes já detalhadas neste documento. A diferença neste caso é que ao invés de existir a firewall filter configurada estaticamente no BNG elas são configuradas dentro da Service Profile e os valores serão preenchidos dinamicamente com as informações enviadas pelo RADIUS.

A primeira parte da configuração da Service Profile são as variáveis (variables):

```
set dynamic-profiles SERVICE-PROFILE variables BANDWIDTH-IN mandatory
set dynamic-profiles SERVICE-PROFILE variables BANDWIDTH-OUT mandatory
set dynamic-profiles SERVICE-PROFILE variables BURST-IN default-value 2m
set dynamic-profiles SERVICE-PROFILE variables BURST-OUT default-value 2m
set dynamic-profiles SERVICE-PROFILE variables POLICER-IN uid
set dynamic-profiles SERVICE-PROFILE variables POLICER-OUT uid
set dynamic-profiles SERVICE-PROFILE variables FILTERv4-IN uid
set dynamic-profiles SERVICE-PROFILE variables FILTERv4-OUT uid
set dynamic-profiles SERVICE-PROFILE variables FILTERv6-IN uid
set dynamic-profiles SERVICE-PROFILE variables FILTERv6-OUT uid
```

O RADIUS manda o atributo ERX-Service-Activate para ativar o serviço do usuário:

```
wztech3  Cleartext-Password := "wztech3"
        ERX-Service-Activate:1 = "SERVICE-PROFILE(2m,4m)"
```

No atributo ERX-Service-Activate (Vendor 4874 / Atributo 65) primeiro vem o nome da dynamic service profile que será ativada no usuário e entre parêntesis é definido os valores das variáveis configuradas no BNG.

Os valores das variáveis são recebidos e são preenchidos pelo BNG na ordem que as variáveis estão definidas na configuração.

No exemplo da configuração acima das variables a primeira variável é BANDWIDTH-IN. Neste caso o primeiro valor enviado pelo RADIUS (2m) preencherá esta variável. O segundo valor enviado pelo RADIUS (4m) preencherá a próxima variável configurada (BANDWIDTH-OUT) e assim por diante.

O valor "mandatory" na frente da variável exige que o RADIUS mande o valor para preencher esta variável.

O valor "default-value" é o valor local definido no BNG para preencher a variável caso o RADIUS não mande nenhuma informação. Se a variável tiver a configuração de "mandatory" + "default-value" e o RADIUS não mandar o valor para preencher esta variável o BNG não irá preencher a variável com o default-value, ou seja, "mandatory" significa que obrigatoriamente o RADIUS terá que enviar o valor. O BNG só preenche a variável com os dados informados como default-value caso não tenha a configuração de "mandatory".

Para as variaveis do tipo UID se for enviado algum valor pelo RADIUS o BNG apenas vai pegar o valor da variável enviado pelo RADIUS e usar para identificar este nome internamente. Caso seja enviado estes nomes das variáveis UID pelo RADIUS é necessário que o valor enviado pelo RADIUS tenha pelo menos 2 caracteres. Não há nenhuma mudança de comportamento no BNG enviando estes valores. As variáveis que não são valores numéricos e são nomes utilizados na configuração obrigatoriamente precisam ter o parâmetro uid. Caso não for configurado o uid o assinante não vai se conectar.

Importante: É recomendado deixar as variáveis de banda primeiro na configuração, depois as variáveis de burst e por fim as variáveis UID haja vista que se for colocado primeiro as variáveis de UID ou BURST e por ultimo as variáveis de banda, obrigatoriamente no RADIUS vai ter que ser preenchido o valor de todas as variáveis pois o BNG nesse caso precisa ler o valor das últimas variáveis que são obrigatórias.

Exemplo:

Se a configuração do BNG ficar desta forma:

```
set dynamic-profiles SERVICE-PROFILE variables BURST-IN default-value 2m
set dynamic-profiles SERVICE-PROFILE variables BURST-OUT default-value 2m
set dynamic-profiles SERVICE-PROFILE variables POLICER-IN uid
set dynamic-profiles SERVICE-PROFILE variables POLICER-OUT uid
set dynamic-profiles SERVICE-PROFILE variables FILTERv4-IN uid
set dynamic-profiles SERVICE-PROFILE variables FILTERv4-OUT uid
set dynamic-profiles SERVICE-PROFILE variables FILTERv6-IN uid
set dynamic-profiles SERVICE-PROFILE variables FILTERv6-OUT uid
set dynamic-profiles SERVICE-PROFILE variables BANDWIDTH-IN mandatory
set dynamic-profiles SERVICE-PROFILE variables BANDWIDTH-OUT mandatory
```

Neste caso o BNG está esperando uma lista com 10 valores (10 variáveis) e os valores 9 e 10 são obrigatórios. Não adianta colocar no RADIUS apenas dois valores pois o BNG os colocaria apenas na posição 1 (BURST-IN) e 2 (BURST-OUT) e aguardaria o preenchimento da lista até os valores 9 (BANDWIDTH-IN) e 10 (BANDWIDTH-OUT) e como não foi enviado estes valores o usuário não se conectará.

Neste caso também não funciona colocar uma lista no RADIUS sem valor para preencher os campos. Exemplo:

wztech3 Cleartext-Password := "wztech3"
        ERX-Service-Activate:1 = "SERVICE-PROFILE(,,,,,,,,2m,4m)"

Este modelo acima também não funciona. Para funcionar no BNG as variáveis utilizando o exemplo de configuração mostrado no BNG no RADIUS precisaria preencher os 10 campos. Exemplo:

wztech3 Cleartext-Password := "wztech3"
        ERX-Service-Activate:1 = "SERVICE-
PROFILE(VALOR1,VALOR2,VALOR3,VALOR4,VALOR5,VALOR6,200k,100k,2m,4m)"

A única forma onde não é preciso preencher no RADIUS os valores de todas as variáveis é colocando as variáveis de BANDWIDTH primeiro, depois Burst e por fim as variáveis de UID pois desta forma os campos 1 (BANDWIDTH-IN) e 2 (BANDWIDTH-OUT) que são obrigatórios já são enviados e os demais o BNG preenche (Burst o BNG preenche caso não seja enviado pelo RADIUS com o valor default-value local) e as demais variáveis usa o mesmo nome da variável local configurada para preencher internamente no BNG os valores:

Exemplo:

```
admin@MX204-LAB-WZTECH> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.3221225894
Interface type: Dynamic
Underlying Interface: xe-0/1/0
Dynamic Profile Name: SVLAN-DYNAMIC-PROFILE
Dynamic Profile Version: 1
State: Active
Session ID: 624
PFE Flow ID: 596
VLAN Id: 200
Login Time: 2023-08-08 20:14:01 -03

Type: PPPoE
User Name: wztech3
IP Address: 100.64.10.66
IP Netmask: 255.255.255.255
Primary DNS Address: 8.8.8.8
Secondary DNS Address: 8.8.4.4
IPv6 Address: 2090::4
IPv6 Prefix: 1010:ee4:4000:f::/64
Domain name server inet6: 2001:4860:4860::8888 2001:4860:4860::8844
IPv6 User Prefix: 2804:ee4:8000:79::/64
Logical System: default
Routing Instance: default
Interface: pp0.3221225895
Interface type: Dynamic
Underlying Interface: demux0.3221225894
```

```
Dynamic Profile Name: SUBSCRIBER-PROFILE-SEM-FILTRO
Dynamic Profile Version: 17
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 625
Session ID: 625
PFE Flow ID: 598
VLAN Id: 200
Login Time: 2023-08-08 20:14:01 -03
Service Sessions: 1
IP Address Pool: POOL-IP-01
IPv6 Address Pool: NOVO-IA_NA
IPv6 Framed Interface Id: 9d35:bbe8:3c3e:31df
Accounting interval: 0
Dynamic configuration:
  junos-ipv6-ndra-prefix: 2804:ee4:8000:79::/64

   Service Session ID: 626
   Service Session Name: SERVICE-PROFILE
   Service Session Version: 15
   State: Active
   Family: inet, inet6
   Service session type: Service-Profile
   IPv4 Input Filter Name: FILTERv4-IN_UID1523-pp0.3221225895-in
   IPv4 Output Filter Name: FILTERv4-OUT_UID1525-pp0.3221225895-out
   IPv6 Input Filter Name: FILTERv6-IN_UID1526-pp0.3221225895-in
   IPv6 Output Filter Name: FILTERv6-OUT_UID1527-pp0.3221225895-out
   Service Activation time: 2023-08-08 20:14:02 -03
   Dynamic configuration:
     BANDWIDTH-IN: 2m
     BANDWIDTH-OUT: 4m
     BURST-IN: 2m
     BURST-OUT: 2m
     FILTERv4-IN: FILTERv4-IN_UID1523
     FILTERv4-OUT: FILTERv4-OUT_UID1525
     FILTERv6-IN: FILTERv6-IN_UID1526
     FILTERv6-OUT: FILTERv6-OUT_UID1527
     POLICER-IN: POLICER-IN_UID1522
     POLICER-OUT: POLICER-OUT_UID1524

Type: DHCP
Domain name server inet: 8.8.8.8 8.8.4.4
IPv6 Address: 2090::4
IPv6 Prefix: 1010:ee4:4000:f::/64
Domain name server inet6: 2001:4860:4860::8888 2001:4860:4860::8844
Logical System: default
Routing Instance: default
Interface: pp0.3221225895
Interface type: Static
Underlying Interface: pp0.3221225895
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 627
Session ID: 627
Underlying Session ID: 625
PFE Flow ID: 598
Login Time: 2023-08-08 20:14:06 -03
DHCPV6 Options: len 115
00 01 00 0a 00 03 00 01 38 90 52 67 06 4d 00 03 00 28 00 9f
9e 6f 00 00 00 00 00 00 00 00 05 00 18 20 90 00 00 00 00
00 00 00 00 00 00 00 00 00 04 ff ff ff ff ff ff ff ff 00 08
00 02 00 00 00 06 00 02 00 17 00 19 00 29 00 9f 97 67 00 00
00 00 00 00 00 00 00 1a 00 19 ff ff ff ff ff ff ff ff 40 10
10 0e e4 40 00 00 0f 00 00 00 00 00 00 00 00
DHCPV6 Header: len 4
01 3a 40 65
IPv6 Address Pool: NOVO-IA_NA
IPv6 Delegated Address Pool: POOL-V6-PD-2
```


É possível ver a configuração dinâmica ativa no BNG com o seguinte comando:

```
admin@MX204-LAB-WZTECH> show dynamic-profile session service-id 626
SERVICE-PROFILE {
    interfaces {
        pp0 {
            unit 3221225895 {
                family {
                    inet {
                        filter {
                            input FILTERv4-IN_UID1523;
                            output FILTERv4-OUT_UID1525;
```

```
                    }
                }
                inet6 {
                    filter {
                        input FILTERv6-IN_UID1526;
                        output FILTERv6-OUT_UID1527;
                    }
                }
            }
        }
    }
}
firewall {
    family {
        inet {
            filter FILTERv4-IN_UID1523 {
                interface-specific;
                term POLICER {
                    then {
                        policer POLICER-IN_UID1522;
                        next term;
                    }
                }
                term DESCARTA-PORTAS-INPUT {
                    from {
                        destination-port 1900;
                        destination-port 25;
                    }
                    then discard;
                }
                term DROP-AMPLIFICATION {
                    from {
                        protocol udp;
                        source-port 53;
                        source-port 161;
                        source-port 123;
                        source-port 1900;
                        source-port 111;
                        source-port 137;
                        source-port 10001;
                    }
                    then discard;
                }
                term BYPASS-LOOPBACK-LOCAL {
                    from {
                        destination-address {
                            20.20.20.20/32;
                        }
                    }
                    then accept;
                }
                term BYPASS-TRAFEGO-LOCAL {
                    from {
                        destination-address {
                            200.225.230.0/24;
                            200.225.231.0/24;
                            200.225.232.0/24;
                            200.225.233.0/24;
                            20.20.20.20/32;
                        }
                    }
                    then accept;
                }
                term DESVIA-TRAFEGO-CGNAT {
                    from {
                        source-address {
                            100.64.0.0/10;
                        }
                    }
                    then next-ip 172.17.17.2/32;
                }
                term ACCEPT {
                    then accept;
                }
            }
            filter FILTERv4-OUT_UID1525 {
                interface-specific;
                term BLOQUEIA-PORTAS-OUT {
                    from {
                        destination-port 0-1023;
                    }
                    then discard;
                }
```

```
                term 1 {
                    then policer POLICER-OUT_UID1524;
                }
            }
        }
        inet6 {
            filter FILTERv6-IN_UID1526 {
                interface-specific;
                term DHCPV6POLICER {
                    from {
                        next-header udp;
                        source-port 546;
                        destination-port 547;
                    }
                    then {
                        policer DHCPPOLICER;
                        next term;
                    }
                }
                term POLICER {
                    then {
                        policer POLICER-IN_UID1522;
                        next term;
                    }
                }
                term DESCARTA-PORTAS-INPUT-TCP {
                    from {
                        next-header tcp;
                        destination-port 25;
                    }
                    then discard;
                }
                term DESCARTA-PORTAS-INPUT-UDP {
                    from {
                        next-header udp;
                        destination-port 1900;
                    }
                    then discard;
                }
                term DROP-AMPLIFICATION {
                    from {
                        next-header udp;
                        source-port 53;
                        source-port 1900;
                        source-port 10001;
                        source-port 137;
                        source-port 123;
                        source-port 161;
                        source-port 111;
                    }
                    then discard;
                }
                term ACCEPT {
                    then accept;
                }
            }
            filter FILTERv6-OUT_UID1527 {
                interface-specific;
                term BLOQUEIA-PORTAS-OUT {
                    from {
                        next-header tcp;
                        next-header udp;
                        destination-port 0-1023;
                    }
                    then discard;
                }
                term 1 {
                    then policer POLICER-OUT_UID1524;
                }
            }
        }
    }
    policer POLICER-IN_UID1522 {
        filter-specific;
        logical-interface-policer;
        if-exceeding {
            bandwidth-limit 2m;
            burst-size-limit 2m;
        }
        then discard;
    }
    policer POLICER-OUT_UID1524 {
        filter-specific;
```

```
            logical-interface-policer;
            if-exceeding {
                bandwidth-limit 4m;
                burst-size-limit 2m;
            }
            then discard;
        }
    }
}

admin@MX204-LAB-WZTECH>
```

Neste caso para mostrar a configuração da Service Profile deve-se utilizar o service-id e não o client-id. O service-id é mostrado no assinante apenas quando se está fazendo uso de Service Profile. No comando "show dynamic-profile session client-id <Session-Id>" também são mostradas todas as informações da Service Profile.

Independente da configuração de "versioning" (que está detalhada neste documento) estar habilitada ou não o comando "show dynamic-profile session" vai funcionar e vai mostrar o conteúdo da dynamic-profile ativada.

Importante: Neste modelo de service profile com variáveis dinâmicas como os dados de firewall filter estão diretamente na dynamic-profile qualquer mudança feita na dynamic-profile como mudança nos filtros da parte de firewall filter, mudança de next-ip de CGNAT, etc.. não são refletidas em tempo real no BNG. É necessário desconectar o usuário para valer a nova versão desta dynamic-profile. Já quando é usado apenas a profile estática (subscriber profile) com as firewall filters enviadas pelo RADIUS qualquer mudança feita nas firewall filters locais sofrem efeito imediato no BNG não sendo necessário desconectar os assinantes pois esta configuração das firewall filters ficam fora da dynamic-profile.

O único caso em que as valores da service profile com variaveis dinâmicas é alterado completamente (policers, next-ip, etc) em tempo real é quando é utilizando o CoA com o Service-Deactivate e Service-Activate. Neste caso a mudança acontece em tempo real independente da configuração de "versioning" estar ativada ou não.

Caso a service profile seja configurada erroneamente com as configurações de firewall filter, a firewall filter será ativada (seja sendo recebida por RADIUS ou seja local através das predefined-variables) e as configurações dinâmicas apesar de serem recebidas não serão ativadas.

Com o modelo de Service Profile caso o serviço RADIUS fique fora e o provedor queira permitir as conexões sem validar a autenticação [authentication order radius none] o assinante vai se conectar normalmente e vai ficar ativo sem nenhum filtro e vai navegar sem nenhum controle.

É possível configurar um modelo onde caso o serviço RADIUS pare de funcionar com o uso de Service Profile seja ativado um filtro padrão. Neste modelo todos os assinantes vão utilizar a subscriber profile padrão SUBSCRIBER-PROFILE (que tem configurações de filtros e predefined-variables):

```
set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults input-filter PREDEFINED-IPV4-IN
set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults output-filter PREDEFINED-IPV4-OUT
set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults input-ipv6-filter PREDEFINED-IPV6-IN
set dynamic-profiles SUBSCRIBER-PROFILE predefined-variable-defaults output-ipv6-filter PREDEFINED-IPV6-OUT
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" interface "$junos-interface-name"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options rib "$junos-ipv6-rib"
access route $junos-framed-route-ipv6-address-prefix qualified-next-hop "$junos-interface-name"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options rib "$junos-ipv6-rib"
access route $junos-framed-route-ipv6-address-prefix metric "$junos-framed-route-ipv6-cost"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options rib "$junos-ipv6-rib"
access route $junos-framed-route-ipv6-address-prefix preference "$junos-framed-route-ipv6-distance"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options rib "$junos-ipv6-rib"
access route $junos-framed-route-ipv6-address-prefix tag "$junos-framed-route-ipv6-tag"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options access route $junos-
framed-route-ip-address-prefix next-hop "$junos-framed-route-nexthop"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options access route $junos-
framed-route-ip-address-prefix metric "$junos-framed-route-cost"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options access route $junos-
framed-route-ip-address-prefix preference "$junos-framed-route-distance"
set dynamic-profiles SUBSCRIBER-PROFILE routing-instances "$junos-routing-instance" routing-options access route $junos-
framed-route-ip-address-prefix tag "$junos-framed-route-tag"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" actual-transit-statistics
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" ppp-options chap
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" ppp-options pap
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet rpf-check
```

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet filter input "$junos-
input-filter"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet filter output "$junos-
output-filter"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet unnumbered-address
"$junos-loopback-interface"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 rpf-check
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 filter input "$junos-
input-ipv6-filter"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 filter output "$junos-
output-ipv6-filter"
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 unnumbered-address
"$junos-loopback-interface"
set dynamic-profiles SUBSCRIBER-PROFILE protocols router-advertisement interface "$junos-interface-name" dns-server-
address $junos-ipv6-dns-server-address
set dynamic-profiles SUBSCRIBER-PROFILE protocols router-advertisement interface "$junos-interface-name" prefix $junos-
ipv6-ndra-prefix
```

Também precisa existir no BNG configurado a subscriber profile para ser utilizada em conjunto com a Service Profile chamada SUBSCRIBER-PROFILE-SEM-FILTRO:

```
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" interface "$junos-
interface-name"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options rib
"$junos-ipv6-rib" access route $junos-framed-route-ipv6-address-prefix qualified-next-hop "$junos-interface-name"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options rib
"$junos-ipv6-rib" access route $junos-framed-route-ipv6-address-prefix metric "$junos-framed-route-ipv6-cost"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options rib
"$junos-ipv6-rib" access route $junos-framed-route-ipv6-address-prefix preference "$junos-framed-route-ipv6-distance"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options rib
"$junos-ipv6-rib" access route $junos-framed-route-ipv6-address-prefix tag "$junos-framed-route-ipv6-tag"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options access
route $junos-framed-route-ip-address-prefix next-hop "$junos-framed-route-nexthop"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options access
route $junos-framed-route-ip-address-prefix metric "$junos-framed-route-cost"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options access
route $junos-framed-route-ip-address-prefix preference "$junos-framed-route-distance"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO routing-instances "$junos-routing-instance" routing-options access
route $junos-framed-route-ip-address-prefix tag "$junos-framed-route-tag"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO interfaces pp0 unit "$junos-interface-unit" actual-transit-statistics
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO interfaces pp0 unit "$junos-interface-unit" ppp-options chap
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO interfaces pp0 unit "$junos-interface-unit" ppp-options pap
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO interfaces pp0 unit "$junos-interface-unit" family inet rpf-check
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO interfaces pp0 unit "$junos-interface-unit" family inet unnumbered-
address "$junos-loopback-interface"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO interfaces pp0 unit "$junos-interface-unit" family inet6 rpf-check
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO interfaces pp0 unit "$junos-interface-unit" family inet6 unnumbered-
address "$junos-loopback-interface"
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO protocols router-advertisement interface "$junos-interface-name" dns-
server-address $junos-ipv6-dns-server-address
set dynamic-profiles SUBSCRIBER-PROFILE-SEM-FILTRO protocols router-advertisement interface "$junos-interface-name"
prefix $junos-ipv6-ndra-prefix
```

No RADIUS os usuários que não estiverem utilizando serviço com variáveis dinâmicas serão autenticados normalmente e podem receber os atributos de Firewall filter:

```
wztech3  Cleartext-Password := "wztech3"
         ERX-IPv6-Ingress-Policy-Name = 100M-IPV6-IN,
         ERX-IPv6-Egress-Policy-Name = 100M-IPV6-OUT,
         ERX-Ingress-Policy-Name = 100M-IPV4-IN,
         ERX-Egress-Policy-Name = 100M-IPV4-OUT
```

Caso o RADIUS não responda, se o authentication-order da access profile tiver também a configuração de "none" o BNG vai aceitar estas autenticações e vai ativar para o usuário as firewall filters configuradas nas predefined-variables da subscriber Profile SUBSCRIBER-PROFILE.

Já para os usuários que precisam receber os valores dinâmicos é configurado no RADIUS da seguinte forma:

```
wztech3  Cleartext-Password := "wztech3"
         ERX-Client-Profile-Name = "SUBSCRIBER-PROFILE-SEM-FILTRO",
         ERX-Service-Activate:1 = "SERVICE-PROFILE(2m,2m)"
```

Neste caso apesar do usuário ter chegado no RADIUS utilizando a subscriber profile "SUBSCRIBER-PROFILE" o RADIUS está mudando a subscriber profile do assinante para uma nova chamada "SUBSCRIBER-PROFILE-SEM-FILTRO" que é uma subscriber profile que não possui nenhuma configuração de filtro haja vista que também está sendo enviado para o assinante o AVP ERX-Service-Activate para ativação do serviço com variáveis dinâmicas. Desta forma o usuário não terá que receber nenhuma firewall filter do RADIUS.

Caso o RADIUS fique fora e o BNG libere as autenticações com a configuração do [authentication-order none]. os assinantes vão continuar usando a profile de serviço SUBSCRIBER-PROFILE original haja vista que não existe RADIUS disponível para mudar essa subscriber profile e neste caso serão utilizados os filtros configurados nas variáveis predefined-variables normalmente.

9. Versioning

Por default o BNG não possui configuração de versioning ativada e é recomendado que seja ativado através do comando:

```
set system dynamic-profile-options versioning
```

O versioning apesar de não ser obrigatório é importante e recomendado pois por default não é possível fazer alterações nas dynamic-profiles com os assinantes conectados pois eles estão fazendo uso da dynamic-profile e o BNG não aceita mudar a configuração já que ela está em uso. Exemplo:

```
admin@MX204-LAB-WZTECH# deactivate protocols router-advertisement

[edit dynamic-profiles SUBSCRIBER-PROFILE]
admin@MX204-LAB-WZTECH# commit check
error: Cannot modify dynamic-profile-option versioning, dynamic profile is configured.
configuration check succeeds

[edit dynamic-profiles SUBSCRIBER-PROFILE]
```

Neste caso para mexer na configuração de alguma dynamic-profile seja ela VLAN Profile, Subscriber Profile ou Service Profile precisaria derrubar todos os assinantes que estão fazendo uso daquela determinada profile. Com a configuração de versioning habilitada o BNG mantém até 10 versoes diferentes da dynamic-profile configurada. Desta forma, quando há modificação na configuração da dynamic-profile os assinantes que estavam com a configuração antiga continuam utilizando aquela versão de configuração e os novos assinantes serão ativados com a nova versão da configuração. A partir do momento que os assinantes que estão utilizando alguma versão de configuração antiga desconectar e conectar novamente eles vão se conectar utilizando a última versão de configuração no BNG. Com a configuração de versioning ligada é possível ver a versão atual de cada dynamic-profile ativa para o assinante. Exemplo de um assinante conectado:

```
admin@MX204-LAB-WZTECH> show subscribers user-name wztech3 extensive
Type: PPPoE
User Name: wztech3
IP Address: 192.168.60.89
IP Netmask: 255.255.255.255
IPv6 Prefix: 1011:ee4:4000:19::/64
Domain name server inet6: 2070::1 2070::2
IPv6 User Prefix: 2904:ee4:8000:21::/64
Logical System: default
Routing Instance: default
Interface: pp0.3221225747
Interface type: Dynamic
Underlying Interface: demux0.3221225745
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 1
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 330
Session ID: 330
PFE Flow ID: 358
VLAN Id: 200
Login Time: 2023-09-12 16:05:22 -03
IP Address Pool: POOL-IP-06
IPv6 Address Pool: POOL-V6-NDRA-1
IPv6 Delegated Address Pool: POOL-V6-PD-2
IPv6 Framed Interface Id: 6c40:1155:d291:c539
IPv4 Input Filter Name: 100M-IPV4-IN-pp0.3221225747-in
IPv4 Output Filter Name: 100M-IPV4-OUT-pp0.3221225747-out
```

```
IPv6 Input Filter Name: 100M-IPV6-IN-pp0.3221225747-in
IPv6 Output Filter Name: 100M-IPV6-OUT-pp0.3221225747-out
Accounting interval: 0
Dynamic configuration:
  junos-input-filter: 100M-IPV4-IN
  junos-input-ipv6-filter: 100M-IPV6-IN
  junos-ipv6-ndra-prefix: 2904:ee4:8000:21::/64
  junos-output-filter: 100M-IPV4-OUT
  junos-output-ipv6-filter: 100M-IPV6-OUT
```

O usuário está utilizando a Subscriber Profile SUBSCRIBER-PROFILE na versão 1 (Dynamic Profile Version: 1).

Com o comando abaixo vemos todas as versões que existem para a dynamic-profile SUBSCRIBER-PROFILE e quais estão em uso no BNG:

```
admin@MX204-LAB-WZTECH> show dynamic-profile profile-name SUBSCRIBER-PROFILE
Profile Name               Version Number        In use
SUBSCRIBER-PROFILE              1                    Yes
SUBSCRIBER-PROFILE              2                    No
```

Com o comando a seguir conseguimos olhar exatamente a configuração da versão que está ativada no assinante:

```
admin@MX204-LAB-WZTECH> show dynamic-profile session client-id 330
SUBSCRIBER-PROFILE {
    predefined-variable-defaults {
        input-filter {
            PREDEFINED-IPV4-IN;
        }
        output-filter {
            PREDEFINED-IPV4-OUT;
        }
        input-ipv6-filter {
            PREDEFINED-IPV6-IN;
        }
        output-ipv6-filter {
            PREDEFINED-IPV6-OUT;
        }
    }
    routing-instances {
        default {
            interface pp0.3221225747;
            routing-options {
                rib inet6.0 {
                    access {
                        route NONE {
                            metric NONE;
                            preference NONE;
                            tag NONE;
                        }
                    }
                }
                access {
                    route NONE {
                        metric NONE;
                        preference NONE;
                        tag NONE;
                    }
                }
            }
        }
    }
    interfaces {
        pp0 {
            unit 3221225747 {
                ppp-options {
                    chap;
                    pap;
                    mtu 1300;
                }
                family {
                    inet {
                        rpf-check;
                        filter {
                            input 100M-IPV4-IN;
                            output 100M-IPV4-OUT;
                        }
                        unnumbered-address lo0.0;
```

```
                }
                inet6 {
                    rpf-check;
                    filter {
                        input 100M-IPV6-IN;
                        output 100M-IPV6-OUT;
                    }
                    unnumbered-address lo0.0;
                }
            }
        }
    }
    protocols {
        router-advertisement {
            interface pp0.3221225747 {
                max-advertisement-interval 60;
                min-advertisement-interval 40;
                dns-server-address NONE;
                prefix 2904:ee4:8000:21::/64;
            }
        }
    }
}

admin@MX204-LAB-WZTECH>
```

O valor 330 do client-id é o "Session ID" da sessão. Este Session ID é o identificador da interface pp0.<unit> do assinante. O Session-ID da interface pp0 vai também no Accounting Radius:

(7) Received Accounting-Request Id 138 from 192.168.1.248:56458 to 192.168.1.236:1813 length 615
(7) User-Name = "wztech3"
(7) Acct-Status-Type = Start
(7) Acct-Session-Id = "330"

Também é possível obter este Session ID com o comando abaixo:

```
admin@MX204-LAB-WZTECH> show network-access aaa subscribers username wztech3
Logical system/Routing instance   Client type    Session-ID     Session uptime    Accounting
default:default                   pppoe          330            00:21:14          on/time
```

É possível também ver a versão da VLAN Profile (dynamic-profile da interface L2):

```
admin@MX204-LAB-WZTECH> show subscribers interface demux0.3221225745 extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.3221225745
Interface type: Dynamic
Underlying Interface: ae0
Dynamic Profile Name: SVLAN-DYNAMIC-PROFILE
Dynamic Profile Version: 1
State: Active
Session ID: 328
PFE Flow ID: 355
VLAN Id: 200
Login Time: 2023-09-12 16:05:22 -03
```

A interface demux0.3221225745 é a interface L2 onde a interface pp0 está ativa. Ela é mostrada como Underlying Interface no usuário:

```
admin@MX204-LAB-WZTECH> show subscribers user-name wztech3 extensive
Type: PPPoE
User Name: wztech3
IP Address: 192.168.60.89
IP Netmask: 255.255.255.255
IPv6 Prefix: 1011:ee4:4000:19::/64
Domain name server inet6: 2070::1 2070::2
IPv6 User Prefix: 2904:ee4:8000:21::/64
Logical System: default
Routing Instance: default
Interface: pp0.3221225747
Interface type: Dynamic
Underlying Interface: demux0.3221225745
```

```
admin@MX204-LAB-WZTECH> show subscribers interface demux0.3221225745 extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.3221225745
Interface type: Dynamic
Underlying Interface: ae0
Dynamic Profile Name: SVLAN-DYNAMIC-PROFILE
Dynamic Profile Version: 1
State: Active
Session ID: 328
PFE Flow ID: 355
VLAN Id: 200
Login Time: 2023-09-12 16:05:22 -03
```

Neste exemplo o assinante está utilizando VLAN Profile SVLAN-DYNAMIC-PROFILE com a versão 1.

```
admin@MX204-LAB-WZTECH> show dynamic-profile profile-name SVLAN-DYNAMIC-PROFILE
Profile Name               Version Number        In use
SVLAN-DYNAMIC-PROFILE      1                     Yes
SVLAN-DYNAMIC-PROFILE      2                     No
```

Conforme o comando acima existem usuários neste momento utilizando a versão 1 e não existem usuários no BNG utilizando a vesão 2 da VLAN Profile SVLAN-DYNAMIC-PROFILE.

Para ver a configuração exata da versão que está aplicada no assinante deve-se utilizar o Session ID da interface L2 (demux):

```
admin@MX204-LAB-WZTECH> show dynamic-profile session client-id 328
SVLAN-DYNAMIC-PROFILE {
    interfaces {
        demux0 {
            unit 3221225745 {
                demux-options {
                    underlying-interface ae0;
                }
                family {
                    pppoe {
                        access-concentrator CONCENTRADOR-PPPOE;
                        duplicate-protection;
                        dynamic-profile SUBSCRIBER-PROFILE;
                        short-cycle-protection;
                    }
                }
            }
        }
    }
}
```

O Session ID da interface L2 não é enviado no RADIUS Accounting

Importante: Mesmo que a configuração de versioning não esteja habilitada no BNG o comando "show dynamic-profile session" vai mostrar o que está ativado para o usuário. Neste caso sempre será a mesma configuração para todos os assinantes que estão usando esta dynamic-profile pois sem o versioning não há versões diferentes da configuração. Já no comando que mostra as versões da dynamic-profile o BNG vai apontar que o versioning não está ativado:

```
admin@MX204-LAB-WZTECH> show dynamic-profile profile-name SUBSCRIBER-PROFILE
Invalid argument: Dynamic profile versioning not enabled.
```

Para ativar ou desativar a configuração de "versioning" não podem ter dynamic-profiles ativas no BNG. Caso exista alguma dynamic-profile configurada e ativa elas devem ser desativadas com o comando:

```
deactivate dynamic-profiles
```

Para desativar as dynamic-profiles não podem existir usuários conectados fazendo uso da mesma. Neste caso precisa primeiro desabilitar a interface física onde estes usuários estão chegando no BNG. Exemplo:

```
set interface ae0 disable
```

Depois de desabilitado a interface física e ter feito o commit no BNG é possível fazer "deactivate dynamic-profiles".

Com as dynamic-profiles desativadas ai sim é possível ativar ou desativar a configuração de versioning:

```
set system dynamic-profile-options versioning
```

Após ativado o versioning é possível ativar novamente as dynamic-profiles:

```
activate dynamic-profiles
```

10. Configurações de Access

Terminado o processo de encadeamento de auto-configure, vlan-profile e subscriber-profile o BNG precisa avaliar algumas outras definições para dar sequência no estabelecimento da conexão no protocolo PPPoE do assinante como por exemplo como o assinante será autenticado e se for autenticado quais as definições de RADIUS Server, endereçamento que será entregue, etc. Algumas dessas definições ficam em [access] na configuração do BNG.

10.1. Access-Profile

A access-profile é uma definição de alguns parâmetros do acesso, sendo o principal deles a definição do processo de autenticação (se é para ser usado RADIUS ou não) e se for utilizado RADIUS as definições dos servidores RADIUS. Também pode ser definido na access profile quais servidores DNS's serão entregues para o usuário na conexão PPPoE dentre outros parâmetros.

Importante: Existe na configuração da access profile a configuração de address-assignment onde é possível definir o pool IPv4 e IPv6 do assinante porém esta configuração apesar de aparecer como opção na access profile NÃO é suportada atualmente para o cenário de BNG.

A chamada ao access profile é obrigatória para que o BNG defina o processo de autenticação e outros parâmetros e esta chamada pode ser feita em pontos de configuração diferentes do BNG sendo os principais destacados neste documento:

10.1.1. Precedência da access-profile no BNG

10.1.1.1. aaa-options

aaa-options é uma opção para definir a access profile que será utilizada para uma determinada Subscriber Profile. Caso seja definida uma aaa-options dentro de uma Subscriber Profile e esta aaa-options contenha uma access profile, esta access profile tem precedência sobre qualquer outra access profile definida (seja em domain map ou seja global). A partir deste momento não será mais avaliado nada configurado em domain map e nem access profile global.

Exemplo de configuração de aaa-options na subscriber profile:

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" ppp-options aaa-options AAA-OPTIONS-1
```

Dentro da Subscriber Profile é definido uma aaa-options chamada AAA-OPTIONS-1

```
set access aaa-options AAA-OPTIONS-1 access-profile ACCESS-PROFILE-2
```

Dentro de access é definido a aaa-options de nome AAA-OPTIONS-1 e dentro dessa AAA-OPTIONS é invocado a access-profile chamada ACCESS-PROFILE-2

```
set access profile ACCESS-PROFILE-2 authentication-order radius
set access profile ACCESS-PROFILE-2 domain-name-server-inet 8.8.8.8
set access profile ACCESS-PROFILE-2 domain-name-server-inet 8.8.4.4
set access profile ACCESS-PROFILE-2 domain-name-server-inet6 2001:4860:4860::8888
set access profile ACCESS-PROFILE-2 domain-name-server-inet6 2001:4860:4860::8844
set access profile ACCESS-PROFILE-2 radius authentication-server 192.168.1.102
set access profile ACCESS-PROFILE-2 radius accounting-server 192.168.1.102
set access profile ACCESS-PROFILE-2 radius options calling-station-id-format mac-address
set access profile ACCESS-PROFILE-2 radius-server 192.168.1.102 secret "$9$cgdrMX7Nbg4Z7NqfTz6/"
```

```
set access profile ACCESS-PROFILE-2 radius-server 192.168.1.102 source-address 192.168.1.248
set access profile ACCESS-PROFILE-2 accounting order radius
set access profile ACCESS-PROFILE-2 accounting address-change-immediate-update
set access profile ACCESS-PROFILE-2 accounting statistics volume-time
```

Na access-profile ACCESS-PROFILE-2 está sendo definido que a autenticação será feita pelo protocolo RADIUS, está sendo definido os servidores DNS's IPv4 e IPv6 que serão entregues na conexão PPPoE e também está sendo definido na access-profile as configurações dos servidores RADIUS que farão a autenticação e accounting das conexões. O detalhamento destas configurações será apresentado posteriormente.

10.1.1.2. domain-map

A access profile definida em Domain MAP é processada caso não haja uma definição de access profile em aaa-options. Domain map é um modelo onde pode ser definido access-profile baseado no dominio do usuario enviado para ser autenticado. Exemplo:

```
set access domain map wztech access-profile NONE
set access domain map ngxservices access-profile ACCESS-PROFILE
```

No exemplo acima foi criado um domain map para o dominio wztech e outro domain map para o dominio ngxservices. Qualquer usuário na conexão PPPoE que tiver o dominio wztech (Ex.: joao@wztech) o BNG processará a access-profile de nome NONE e qualquer usuário na conexão PPPoE que tiver o dominio ngxservices (Ex.: maria@ngxservices) o BNG processará a access-profile de nome ACCESS-PROFILE.

```
set access profile NONE authentication-order none
set access profile NONE domain-name-server-inet 8.8.8.8
set access profile NONE domain-name-server-inet 8.8.4.4
set access profile NONE domain-name-server-inet6 2001:4860:4860::8888
set access profile NONE domain-name-server-inet6 2001:4860:4860::8844
```

No exemplo acima a access profile NONE está configurada com o authentication order "none". Isto significa que não é para o BNG fazer autenticação em servidores externos e é para aceitar qualquer usuário e senha que der match nesta access-profile. Também está configurado nesta access-profile os servidores DNS's IPv4 e IPv6 que serão entregues na conexão PPPoE.

```
set access profile ACCESS-PROFILE authentication-order radius
set access profile ACCESS-PROFILE domain-name-server-inet 8.8.8.8
set access profile ACCESS-PROFILE domain-name-server-inet 8.8.4.4
set access profile ACCESS-PROFILE domain-name-server-inet6 2001:4860:4860::8888
set access profile ACCESS-PROFILE domain-name-server-inet6 2001:4860:4860::8844
set access profile ACCESS-PROFILE radius authentication-server 192.168.1.236
set access profile ACCESS-PROFILE radius accounting-server 192.168.1.236
set access profile ACCESS-PROFILE radius options calling-station-id-format mac-address
set access profile ACCESS-PROFILE radius-server 192.168.1.236 secret "$9$cgdrMX7Nbg4Z7NqfTz6/"
set access profile ACCESS-PROFILE radius-server 192.168.1.236 source-address 192.168.1.248
set access profile ACCESS-PROFILE accounting order radius
set access profile ACCESS-PROFILE accounting address-change-immediate-update
set access profile ACCESS-PROFILE accounting statistics volume-time
```

Na access-profile ACCESS-PROFILE está sendo definido que a autenticação será feita pelo protocolo RADIUS, está sendo definido os servidores DNS's IPv4 e IPv6 que serão entregues na conexão PPPoE e também está sendo definido na access-profile as configurações dos servidores RADIUS que farão a autenticação e accounting das conexões.

Existem alguns valores que podem ser utilizados dentro de domain map ao invés do domínio do usuario que possuem funções específicas:

default: Dá match em qualquer domínio que não foi definido previamente nas configurações de domain map. Exemplo:

```
set access domain map wztech access-profile NONE
set access domain map ngxservices access-profile ACCESS-PROFILE
set access domain map default access-profile ACCESS-PROFILE-2
```

No exemplo acima usuários com o dominio @wztech serão direcionados para a access profile NONE, usuários com o domínio ngxservices serão direcionados para a access profile ACCESS-PROFILE e usuários com qualquer outro domínio serão direcionados para a access profile ACCESS-PROFILE-2

none: Dá match em qualquer usuário que não possui domínio no usuario (Ex.: wztech). Neste caso como o usuário não possui domínio junto do usuário não há domínio a ser definido na configuração de domain map. O valor "none" dará match em qualquer usuário sem domínio.

*: O valor asterisco pode ser utilizado para ajudar na definição da access-profile. Exemplo:

```
set access domain map wztech* access-profile ACCESS-PROFILE-2
```

Neste caso qualquer usuario @wztech com qualquer sufixo irá dar match nesta definição (Ex: user1@wztech.com.br, user2@wztech, user3@wztech.net.br).

Dentro do domain map é possível definir um pool IPv4 para ser alocado para o usuário. Caso não seja enviado o pool através do protocolo RADIUS o pool do domain map será escolhido. Atualmente é suportado apenas definição do pool IPv4. Não é suportado definição de pool IPv6 dentro do domain map. Exemplo desta configuração:

```
set access domain map none access-profile ACCESS-PROFILE
set access domain map none address-pool POOL-IP-03
```

Neste caso está sendo definido o pool IPv4 POOL-IP-03 para este domain map. Este pool é definido em [access address-assignment pool]:

```
set access address-assignment pool POOL-IP-03 family inet network 192.168.10.0/24
set access address-assignment pool POOL-IP-03 family inet range RANGE low 192.168.10.1
set access address-assignment pool POOL-IP-03 family inet range RANGE high 192.168.10.254
```

10.1.1.3. Global (access-profile)

Por fim caso não seja encontrada uma access profile definida em aaa-options ou em domain map o BNG avaliará qual a access-profile global que está definida. Exemplo:

```
set access-profile ACCESS-PROFILE-2
```

Neste caso será processado a ACCESS-PROFILE-2 para definir o processo de autenticação.

Importante: Nesta ordem de precedência aaa-options, domain map e global caso por exemplo o(s) RADIUS Server(s) configurados em aaa-options parem de funcionar o BNG não tentará buscar os RADIUS servers configurados em domain map. A partir do momento que foi configurado em um ponto da configuração com precedência maior será sempre utilizado os RADIUS neste ponto da configuração.

Importante: Existe uma opção para definir a access profile diretamente na interface na configuração de auto-configure dentro da VLAN Profile porém esta definição só é processada em caso de autenticação da interface VLAN e não vale para a autenticação do usuário. Exemplo deste tipo de configuração:

```
set interfaces ae0 auto-configure vlan-ranges access-profile ACCESS-PROFILE
```

Com esta configuração caso seja habilitado autenticação da VLAN que é um mecanismo para autenticar a interface VLAN antes de autenticar o usuário será utilizado essa access profile para autenticar a VLAN. A autenticação do usuário vai buscar a access profile configurada em algum dos outros pontos mencionados anteriormente seguindo a precedência já detalhada.

10.1.2. Detalhamento dos itens configurados na access profile:

10.1.2.1. DNS's IPv4 e IPv6

```
set access profile ACCESS-PROFILE domain-name-server-inet 8.8.8.8
set access profile ACCESS-PROFILE domain-name-server-inet 8.8.4.4
```

```
set access profile ACCESS-PROFILE domain-name-server-inet6 2001:4860:4860::8888
set access profile ACCESS-PROFILE domain-name-server-inet6 2001:4860:4860::8844
```

Os servidores DNS que serão entregues para o usuário podem ser definidos em alguns lugares diferentes no BNG. É comum e recomendado que eles sejam configurados na access profile que está autenticando o assinante, porém eles podem ser definidos em outros pontos da configuração no BNG e há uma precedência para serem lidas estas configurações. A seguir um detalhamento com as opções que podem ser usadas para envio dos DNS's:

10.1.2.1.1. DNS IPv4 no PPPoE

Os DNS's IPv4 que serão entregues na conexão PPPoE são processados de acordo com a lista abaixo. Se o BNG encontrar o DNS no item 1 ele já usa esta informação para entregar para o usuário. Caso ele não encontre ele vai para o próximo item seguindo a lista abaixo de precedência até o final.

1. Protocolo RADIUS. Exemplo dos AVP's no RADIUS:

ERX-Primary-Dns = 8.8.8.8
ERX-Secondary-Dns = 8.8.4.4

Caso seja recebido os DNS's pelo protocolo RADIUS através dos atributos ERX-Primary-Dns (Vendor 4874 / Atributo 4) e ERX-Secondary-Dns (Vendor 4874 / Atributo 5) o BNG vai usar estas informações.

2. xauth-attributes do pool IPv4 alocado para o usuário. Exemplo:

```
set access address-assignment pool POOL-IP-03 family inet xauth-attributes primary-dns 8.8.8.8
set access address-assignment pool POOL-IP-03 family inet xauth-attributes secondary-dns 8.8.4.4
```

Caso não venha nenhum atributo do RADIUS este será o próximo ponto que o BNG avaliará os DNS's que serão entregues na negociação IPCP do protocolo PPPoE para o assinante.

3. access profile que autenticou o usuário. Exemplo:

```
set access profile ACCESS-PROFILE domain-name-server-inet 8.8.8.8
set access profile ACCESS-PROFILE domain-name-server-inet 8.8.4.4
```

O próximo ponto que o BNG procura os DNS's é na access profile que autenticou o usuário.

4. access - global

```
set access domain-name-server-inet 8.8.8.8
set access domain-name-server-inet 8.8.4.4
```

Por fim é procurado os DNS's configurados globalmente em access.

Caso o BNG não ache nenhum DNS IPv4 configurado ele vai deixar o usuário conectar sem DNS. Neste caso depende da implementação da ONU de como entregar DNS's IPv4 ao usuário. Algumas ONU's alocam DNS's IPv4 já pré-configurados no firmware quando não recebe nada do BNG (Google, Cloudflare, etc).

10.1.2.1.2. DNS's IPv6 entregues no Router Advertisement (SLAAC)

A seguir a ordem de processamento para envio dos DNS's IPv6 que serão enviado no SLAAC (Router Advertisement) - Estes DNS's recebidos no RA (Router Advertisement) geralmente são usados pela ONU para resolução de nome local e também será utilizado em casos onde a ONU está em modo bridge e um assinante faz a conexão SLAAC sem existir DHCPv6. A seguir a precedência para 3 modelos de configuração diferentes da subscriber profile:

10.1.2.1.2.1. Configuração de DNS estático na Subscriber Profile do usuário

```
set dynamic-profiles SUBSCRIBER-PROFILE protocols router-advertisement interface "$junos-interface-name" dns-server-address 2001:4860:4860::8888
```

```
set dynamic-profiles SUBSCRIBER-PROFILE protocols router-advertisement interface "$junos-interface-name" dns-server-address 2001:4860:4860::8844
```

Caso exista esta configuração estática de DNS IPv6 na configuração do NDRA sempre será enviado estes DNS's no Router Advertisement para o assinante. Neste caso mesmo que o RADIUS envie os AVP's de DNS o BNG não aceitará os DNS's informados por RADIUS. Não há outro ponto que o BNG vai procurar DNS neste caso.

10.1.2.1.2.2. dns-server-address não configurado na Subscriber Profile:

Caso não seja configurado dns-server-address na subscriber profile o BNG não enviará nenhum DNS no Router Advertisement. Neste caso mesmo que o RADIUS envie os AVP's de DNS o BNG não aceitará os DNS's informados pelo RADIUS.

10.1.2.1.2.3. dns-server-address configurado apontando para variavel $junos-ipv6-dns-server-address. Exemplo:

```
set dynamic-profiles SUBSCRIBER-PROFILE protocols router-advertisement interface "$junos-interface-name" dns-server-address $junos-ipv6-dns-server-address
```

Este modelo é o recomendado. Neste caso foi habilitado no BNG para que o BNG procure os DNS's que serão enviados no Router Advertisement seguindo a ordem de precedência abaixo:

1. RADIUS. Exemplo dos AVP's no RADIUS:

ERX-Ipv6-Primary-Dns = 2001:4860:4860::8888
ERX-Ipv6-Secondary-Dns = 2001:4860:4860::8844

Caso seja recebido os DNS's pelo protocolo RADIUS utilizando os AVP's ERX-Ipv6-Primary-Dns (Vendor 4874 / Atributo 47) e ERX-Ipv6-Secondary-Dns (Vendor 4874 / Atributo 48) o BNG vai usar estas informações e vai enviar estes DNS's no ICMPv6 Router Advertisement

2. access-profile que autenticou o assinante: Exemplo:

```
set access profile ACCESS-PROFILE domain-name-server-inet6 2001:4860:4860::8888
set access profile ACCESS-PROFILE domain-name-server-inet6 2001:4860:4860::8844
```

Caso não seja recebido nenhum DNS por RADIUS o BNG vai procurar os DNS's configurados na access profile que autenticou o usuário

3. global - access:

```
set access domain-name-server-inet6 2080::1
set access domain-name-server-inet6 2080::2
```

Por último o BNG vai procurar os DNS's configurados globalmente em [access] para envio no Router Advertisement.

Com esta configuração do dns-server-address apontando para variavel $junos-ipv6-dns-server-address caso o BNG não tenha nenhum DNS para enviar na conexão PPPoE o assinante não conecta visto que a variável $junos-ipv6-dns-server-address exige que exista DNS IPv6 para ser enviado no RA.

10.1.2.1.3. DNS's IPv6 enviados no DHCPv6 Advertise

A seguir a ordem de processamento para envio dos DNS's IPv6 que serão enviado no DHCPv6 (Advertise). Estes DNS's recebidos na ONU pelo DHCPv6 Advertise geralmente são usados pela ONU para envio ao usuário final (portas LAN da ONU) que está ligado na ONU juntamente com o prefixo PD enviado. A implementação do DNS IPv6 que será entregue ao usuário depende da ONU. Existem modelos de ONU que caso não recebam os DNS's IPv6 no DHCPv6 Advertise envia para o usuário os DNS's recebidos no ICMPv6 RA. Neste caso depende da implementação de DNS na ONU.

1. RADIUS. Exemplo dos AVP's no RADIUS:

ERX-Ipv6-Primary-Dns = 2001:4860:4860::8888
ERX-Ipv6-Secondary-Dns = 2001:4860:4860::8844

Caso seja recebido os DNS's pelo protocolo RADIUS o BNG vai usar estas informações e vai enviar estes DNS's no DHCPv6 Advertise

2. dhcp-attributes no pool do PD:

```
set access address-assignment pool POOL-V6-PD family inet6 dhcp-attributes dns-server 2001:4860:4860::8888
set access address-assignment pool POOL-V6-PD family inet6 dhcp-attributes dns-server 2001:4860:4860::8844
```

Caso não seja recebido os AVP's do RADIUS de DNS o BNG vai procurar em segundo lugar os DNS's configurados no pool PD do assinante. Mesmo que o assinante não solicite IA_PD no DHCPv6 Solicit, por default, como é configurado o delegated-pool no DHCPv6 server do BNG esse pool é associado internamente no BNG ao usuário e fica disponível para entregar os prefixos IPv6 caso seja enviado IA_PD. Neste caso mesmo que o usuário não envie solicitação de IA_PD o BNG vai enviar os DNS's configurados no pool de PD (inet6 dhcp-attributes dns-server) associado com o usuário.

3. dhcp-attributes no pool de WAN:

```
set access address-assignment pool POOL-V6-NDRA family inet6 dhcp-attributes dns-server 2040::1
set access address-assignment pool POOL-V6-NDRA family inet6 dhcp-attributes dns-server 2040::2

set access address-assignment pool NOVO-IA_NA family inet6 dhcp-attributes dns-server 1414::1
set access address-assignment pool NOVO-IA_NA family inet6 dhcp-attributes dns-server 1414::2
```

Em terceiro lugar o BNG vai procurar os DNS's configurados no POOL de WAN IPv6 que foi alocado para a ONU (seja ele SLAAC ou DHCP IA_NA). Caso seja alocado tanto prefixo WAN SLAAC quanto prefixo na WAN IA_NA será entregue o DNS configurado no pool de IA_NA

4. access profile que autenticou usuario:

```
set access profile ACCESS-PROFILE domain-name-server-inet6 2001:4860:4860::8888
set access profile ACCESS-PROFILE domain-name-server-inet6 2001:4860:4860::8844
```

Em quarto lugar o BNG vai procurar os DNS's configurados na access profile que autenticou o usuário

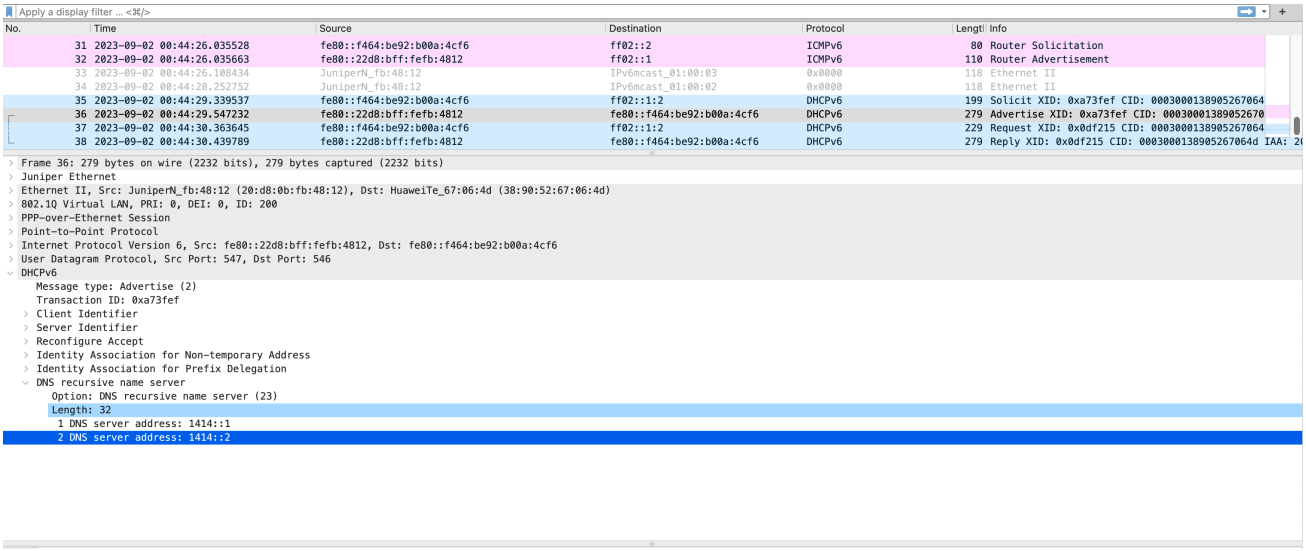
5. global - access:

```
set access domain-name-server-inet6 2080::1
set access domain-name-server-inet6 2080::2
```

Por último o BNG vai procurar os DNS's configurados globalmente em [access] para envio no DHCPv6 Advertise.

Caso o BNG não ache os DNS's para serem enviados no DHCPv6 Advertise o BNG vai alocar o prefixo para o usuário normalmente, porém a ONU não vai receber o DNS no DHCP Avertise.

Os DNS's no DHCPv6 Advertise são enviados pelo BNG de forma global dentro do DHCP Advertise:



Existe uma opção para configurar os DNS's para serem enviados como suboption dentro do DHCP IA_NA ou DHCP IA_PD chamada [multi-address-embedded-option-response] porém não é recomendado utilizar este modelo em virtude de incompatibilidade com o firmware de muitos modelos de ONU's.

Este modelo é documentado pela Juniper na seguinte URL:

https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-sessions/topics/topic-map/dns-address-subscriber-management.html#id-overriding-how-the-dns-server-address-is-returned-in-a-dhcpv6-multiple-address-environment

Importante: Configurar domain-name-server (sem inet) tem o mesmo efeito que a configuração com o inet [set access profile ACCESS-PROFILE domain-name-server]. Se ambas as configurações estiverem ativas os valores com inet terão precedência.

10.1.2.2. RADIUS para Autenticação e Accounting do Assinante

```
set access profile ACCESS-PROFILE authentication-order radius
```

O authentication-order na access profile informa qual é a ordem do processo de autenticação. Se estiver só radius significa que o BNG tentará fazer a autenticação pelo protocolo RADIUS e caso os servidores RADIUS definidos não estejam respondendo o usuário não se autenticará.

O authentication-order "none" orienta o BNG para que não haja autenticação. Qualquer autenticação será aceita.

É possível configurar primeiramente o radius e depois none. Exemplo:

```
set access profile ACCESS-PROFILE authentication-order radius
set access profile ACCESS-PROFILE authentication-order none
```

Neste caso primeiramente o BNG tentará fazer a autenticação utilizando protocolo RADIUS e caso os servidores RADIUS não respondam o BNG passará para o próximo mecanismo de autenticação que é "none" e nesse caso vai liberar qualquer usuário sem autenticação.

Neste caso precisa da definição das firewall filters pré definidas (predefined-variable-defaults) pois caso o RADIUS não esteja disponível não serão recebidas as firewall filters e o BNG precisa aplicar alguma firewall filter no assinante e neste caso ele vai usar a firewall filter pré-definida na configuração da Subscriber Profile.

Existe uma outra opção do authentication-order que é a opção "password". É possível para cenario de testes configurar autenticação local "password" e criar usuarios locais para teste na access-profile. Exemplo:

```
set access profile ACCESS-PROFILE authentication-order password
set access profile ACCESS-PROFILE subscriber wztech-local password "$9$UFHPQ1IcvWx9AWx7-ws.PfTQnApBcyK"
set access profile ACCESS-PROFILE subscriber wztech-local framed-pool POOL-IP-03
```

Neste caso é possível fazer uma autenticação local com o usuário wztech-local e com a senha definida local para efeitos de testes. O BNG não suporta volume grande de usuários locais. Este cenário é apenas para testes e validação local no BNG sem depender dos servidores RADIUS.

```
set access profile ACCESS-PROFILE radius-server 192.168.1.236 secret "$9$cgdrMX7Nbg4Z7NqfTz6/"
set access profile ACCESS-PROFILE radius-server 192.168.1.236 source-address 192.168.1.248

set access profile ACCESS-PROFILE radius-server 192.168.1.102 secret "$9$cgdrMX7Nbg4Z7NqfTz6/"
set access profile ACCESS-PROFILE radius-server 192.168.1.102 source-address 192.168.1.248
```

Acima são definidos os servidores RADIUS com as devidas chaves de segurança (secret) que farão a encriptação da senha do usuário. Caso a autenticação do usuário na access profile seja utilizado RADIUS é obrigatório configurar os servidores RADIUS para que haja autenticação do usuário.

A configuração de "source-address" altera qual o endereço IP de origem que será enviado nos pacotes RADIUS bem como o AVP "NAS-IP-Address" enviado para o RADIUS. É recomendado que o BNG tenha conectividade com os servidores RADIUS utilizando a interface loopback e que este endereço de source-address seja o IP da interface loopback (lo0).

Estas definições de radius-server podem ser feitas tanto na access profile que está autenticando o usuário quanto globalmente em [access radius-server].

Se forem definidas configurações globais de radius em [access radius-server] estes radius servers podem ser apontados na configuração da access profile (desde que não haja nenhuma definição de radius-server na access profile em questão).

Exemplo:


```
set access radius-server 192.168.1.236 secret "$9$uzJxBhreK8N-weKJDikPf"
set access radius-server 192.168.1.102 secret "$9$nO0S9u1REyvMXREwgoJDj"

set access profile ACCESS-PROFILE authentication-order radius
…
set access profile ACCESS-PROFILE radius authentication-server 192.168.1.236
set access profile ACCESS-PROFILE radius accounting-server 192.168.1.236
…
set access profile ACCESS-PROFILE accounting order radius
set access profile ACCESS-PROFILE accounting address-change-immediate-update
set access profile ACCESS-PROFILE accounting statistics volume-time
```

Neste caso, a access profile ACCESS-PROFILE está invocando os radius-servers e fará uso dos mesmos, visto que não há nenhuma definição de radius-server dentro da access profile.

Para efeito de CoA ou Disconnect Request com esta configuração acima o BNG também vai aceitar requisições de CoA/Disconnect Request de qualquer IP de radius-server globalmente definido, mesmo que não esteja sendo especificado como authentication-server ou accounting-server.

A partir do momento que for criada alguma entrada de radius-server dentro da access profile que está autenticando o assinante as entradas globais (access radius-server) passam a não valer mais e não são mais válidas para autenticação, accounting, CoA ou Disconnect-Request. Neste caso passa a valer as definições de radius-servers que foram criadas dentro da access profile.

Exemplo:

```
set access radius-server 192.168.1.236 secret "$9$uzJxBhreK8N-weKJDikPf"
set access radius-server 192.168.1.102 secret "$9$nO0S9u1REyvMXREwgoJDj"

set access profile ACCESS-PROFILE authentication-order radius
…
set access profile ACCESS-PROFILE radius authentication-server 192.168.1.236
set access profile ACCESS-PROFILE radius accounting-server 192.168.1.236
```

```
…
set access profile ACCESS-PROFILE radius-server 192.168.1.103 secret "$9$FAik6tO1IceK81IVYgoGU"
…
set access profile ACCESS-PROFILE accounting order radius
set access profile ACCESS-PROFILE accounting address-change-immediate-update
set access profile ACCESS-PROFILE accounting statistics volume-time
```

Como foi feita uma definição de radius-server dentro da access profile do usuário as chamadas aos radius externos definidos (radius authentication-server 192.168.1.236 e radius accounting-server 192.168.1.236) não funcionam mais pois agora o BNG considera as entradas de radius-server locais na access-profile para autenticação, accounting, Disconnect-Request e CoA. Neste caso toda a configuração global de radius-server é ignorada completamente pelo BNG para esta access profile.

Importante: No caso de configurar o mesmo RADIUS-SERVER dentro da access profile e global vale o mesmo conceito. O IP global será descartado e não tem valor nenhum para o BNG.

Em resumo:

Se as definições de radius-server estiverem presentes na access profile o BNG não vai avaliar mais globalmente
Se as definições de radius-server estiverem apenas globalmente em [access] o BNG vai usar estas informações
Se as definições de radius-server estiverem presentes tanto globalmente em [access] quanto na access profile que está autenticando o usuário o BNG vai olhar apenas os radius-servers da access profile.

```
set access profile ACCESS-PROFILE radius authentication-server 192.168.1.236
set access profile ACCESS-PROFILE radius authentication-server 192.168.1.102
```

Acima são as configurações de quais servidores RADIUS (já definidos anteriormente) que farão a autenticação (authentication-server) dos assinantes caso a access profile esteja invocando o protocolo RADIUS com o [authentication-order radius].

Por default o mecanismo de redundancia dos RADIUS Servers é um mecanismo chamado "direct" pela Juniper. As autenticações e os accountings serão sempre enviados para o primeiro RADIUS Server configurado em authentication-server no caso de autenticação e accounting-server no caso de accounting. Caso este servidor RADIUS não responda as autenticações ou accounting é enviado os pacotes para o próximo RADIUS definido.

Este comportamento default pode ser alterado para um outro algoritmo chamado "round-robin". Esta configuração pode ser feita individualmente tanto para o processo de autenticação quanto para o processo de accounting:

```
set access profile ACCESS-PROFILE radius options client-authentication-algorithm round-robin
set access profile ACCESS-PROFILE radius options client-accounting-algorithm round-robin
```

No algoritmo round-robin é enviado um pacote para cada servidor. Não há garantia que o accounting vai ser enviado para o mesmo servidor da autenticação. Não é guardado este estado no BNG. Apenas será enviado um pacote para um servidor e outro pacote para outro de forma que seja feito um balanceamento das autenticações e bilhetagem.

Não existe hoje disponível um modelo de configuração de peso onde o BNG envie um volume maior de requisições para um servidor e um outro volume menor para outro servidor. No caso de balanceamento atualmente é suportado apenas o mecanismo round-robin.

O BNG nao fica enviando por conta própria pacotes de testes no protocolo RADIUS para validar o estado do Servidor Radius (se está UP ou Down). O mecanismo de redundância dos radius servers é descrito a seguir:

No caso do algoritmo direct, que é o default do BNG, a autenticação é enviada para o primeiro radius-server da lista. Se o primeiro radius-server não responder, a autenticação é enviada para o segundo RADIUS Server. Não é possível configurar prioridade nos radius-servers definidos. A lista é sequencial do primeiro servidor até o último.

Por default se nao for configurado parametros de timeout e retry nos radius servers o tempo default de timeout são 3 segundos e o número de retry (novas tentativas) também é 3 (tanto para autenticação como para

accounting). Estes parametros podem ser configurados também individualmente para authentication e accounting (accounting-timeout, authentication-timeout, accounting-retry, authentication-retry).

Se o RADIUS Server que recebeu a autenticação não responder a esta tentativa de autenticação seguido de mais três tentativas (3 retries) o BNG já envia a mesma autenticação que falhou neste radius server para o próximo radius-server configurado no BNG.

Para o servidor que não respondeu a autenticação seguido dos 3 retries é criado um timer no BNG chamado timeout-grace que por default é de 10 segundos.

Este valor pode ser alterado globalmente no MX com a seguinte configuração:

```
set access radius-options timeout-grace 20
```

Enquanto isso o radius server que não respondeu a autenticação seguida de 3 retries ainda está com o estado UP no BNG:

```
admin@MX204-LAB-WZTECH> show network-access aaa radius-servers
  Profile: ACCESS-PROFILE
    Server address: 192.168.1.236
      Authentication port: 1812
      Preauthentication port: 1812
      Accounting port: 1813
      Status: UP
  Profile: ACCESS-PROFILE-2
    Server address: 192.168.1.102
      Authentication port: 1812
      Preauthentication port: 1812
      Accounting port: 1813
      Status: UP
```

Todas as novas autenticações que ainda estão chegando no BNG seguem o fluxo normalmente dependendo do algoritmo configurado (direct ou round-robin) e consideram o RADIUS Server que não respondeu a autenticação normal no processo haja vista que ele ainda possui o estado como UP no BNG. Caso este radius server não responda estas novas autenticações seguidas dos 3 retries da mesma forma estas autenticações também serão comutadas para o próximo radius server da lista.

Todas as autenticações que chegam no BNG validam ser o timer do timeout-grace criado de 10 segundos já expirou. Se o timer estiver expirado o servidor radius vai para DOWN (O accounting não é usado para declarar um servidor RADIUS como DOWN. Apenas os pacotes de autenticação).

```
admin@MX204-LAB-WZTECH> show network-access aaa radius-servers
  Profile: ACCESS-PROFILE
    Server address: 192.168.1.236
      Authentication port: 1812
      Preauthentication port: 1812
      Accounting port: 1813
      Status: DOWN ( 60 seconds )
    Server address: 192.168.1.102
      Authentication port: 1812
      Preauthentication port: 1812
      Accounting port: 1813
      Status: UP
```

Quando o RADIUS vai para o BNG inicia um novo timer chamado revert-interval para este servidor RADIUS. Este timer é o tempo que o servidor no estado DOWN não vai ser utilizado para nenhuma autenticação ou accounting. As requisições não serão mais enviadas para este servidor neste tempo que por default é de 60 segundos. Este tempo pode ser alterado com a seguinte configuração:

```
set access profile ACCESS-PROFILE radius options revert-interval 120
```

Depois desse tempo do revert-interval o servidor fica UP novamente (não há uma validação do BNG para saber se o servidor radius voltou ou não). O BNG coloca o servidor novamente como UP e caso ele não tenha voltado a responder vai seguir o mesmo fluxo já descrito anteriormente.

Durante o periodo do timeout-grace (que por default são 10 segundos), este servidor RADIUS que está com o timer do timeout-grace rodando no BNG (em virtude de não ter respondido a alguma autenticação), caso ele responda a qualquer autenticação antes do timer expirar, o timer é deletado internamente no BNG e o servidor não vai para DOWN e a próxima autenticação vai iniciar o fluxo novamente. A ideia do timeout-grace é tentar dar uma sobrevida para o servidor RADIUS em casos rápidos de instabilidade.

Se o próximo servidor da lista também não responder a autenticação que foi chaveada para ele e este servidor for o último da lista disponível (os outros servidores estiverem DOWN) ele também vai ficar com o estado UP pelo periodo do grace-timeout e quando o grace-timeout terminar ao invés do estado ficar DOWN ele vai ficar com o estado de UNREACHABLE pois ele é o ultimo servidor da lista e não tem mais nenhum outro servidor RADIUS para responder as requisições de autenticação:

```
admin@MX204-LAB-WZTECH> show network-access aaa radius-servers
  Profile: ACCESS-PROFILE
    Server address: 192.168.1.236
      Authentication port: 1812
      Preauthentication port: 1812
      Accounting port: 1813
      Status: DOWN ( 36 seconds )
    Server address: 192.168.1.102
      Authentication port: 1812
      Preauthentication port: 1812
      Accounting port: 1813
      Status: UNREACHABLE
```

Quando chegar alguma próxima autenticação no BNG os servidores com o estado DOWN não vão receber estas autenticações até que termine o tempo do revert-interval para ficarem UP novamente, porém, o servidor RADIUS que estava com o estado UNREACHABLE muda para UP instantaneamente para que sempre exista algum servidor RADIUS que possa receber as requisições de autenticação:

```
admin@MX204-LAB-WZTECH> show network-access aaa radius-servers
  Profile: ACCESS-PROFILE
    Server address: 192.168.1.236
      Authentication port: 1812
      Preauthentication port: 1812
      Accounting port: 1813
      Status: DOWN ( 15 seconds )
    Server address: 192.168.1.102
      Authentication port: 1812
      Preauthentication port: 1812
      Accounting port: 1813
      Status: UP
```


Assim que os outros servidores ficarem UP novamente em virtude do término do timer revert-interval as requisições novamente poderão ser enviadas para eles.

```
set access profile ACCESS-PROFILE radius accounting-server 192.168.1.236
set access profile ACCESS-PROFILE radius accounting-server 192.168.1.102
```

Acima são as configurações de quais servidores RADIUS (já definidos anteriormente) farão a bilhetagem (accounting-server) das conexões dos usuários caso a access profile esteja configurada com o accounting. Esta configuração é feita da seguinte forma:

```
set access profile ACCESS-PROFILE accounting order radius
```

Caso não seja configurado accounting na access profile o usuário vai autenticar, porém não vai haver bilhetagem das autenticações.

Por default quando o JunOS vai se comunicar a primeira vez com os RADIUS Servers configurados seja porque o MX está inicializando ou porque é uma nova configuração no BNG, caso o accounting esteja configurado na access profile, o MX envia um pacote inicial de Accounting chamado Accounting-On para o RADIUS Server.

(1) Received Accounting-Request Id 1 from 192.168.1.248:62536 to 192.168.1.236:1813 length 74
(1) Acct-Status-Type = Accounting-On
(1) Acct-Session-Id = "\000\000\000"
(1) Event-Timestamp = "Sep 2 2023 15:11:24 EDT"

(1) Acct-Delay-Time = 0
(1) Acct-Authentic = RADIUS
(1) NAS-IP-Address = 192.168.1.248
(1) NAS-Identifier = "MX204-LAB-WZTECH"

Caso o RADIUS Server responda este pacote de Accounting-On BNG mostrará que este pacote foi respondido colocando o valor ACK:

```
admin@MX204-LAB-WZTECH> show network-access aaa accounting
  Profile               Logical System        Routing Instance      Acct-On-Response
  ACCESS-PROFILE        default               default               ACK
```

Caso o RADIUS não responda o Accounting-On o estado do Acct-On-Response ficará como PENDING:

```
admin@MX204-LAB-WZTECH> show network-access aaa accounting
  Profile               Logical System        Routing Instance      Acct-On-Response
  ACCESS-PROFILE        default               default               PENDING
```

Importante: É obrigatório que algum RADIUS Server do processo de Accounting responda o Accounting-On. Caso não seja respondido o BNG NÃO deixará de fazer o accounting do assinante com as mensagens de Accounting-Start, Accounting-Stop, Accounting-Update, etc.. porém o BNG vai continuar o tempo todo enviando estas mensagens de Accounting-On para os RADIUS Servers até que seja respondido. A ideia do Accounting-On é uma mensagem para informar aos RADIUS Servers que o BNG está iniciando então qualquer tabela de sessão existente com aquele NAS pode ser deletada por completo pois a caixa está começando um novo ciclo e não há motivos para ter sessões ativas para aquele NAS.

Quando o MX é reiniciado ou desligado ele também envia o Accounting-Off para os RADIUS sinalizando que a caixa está parando:

(0) Received Accounting-Request Id 63 from 192.168.1.248:54320 to 192.168.1.236:1813 length 74
(0) Acct-Status-Type = Accounting-Off
(0) Acct-Session-Id = "\000\000\000"
(0) Event-Timestamp = "Sep 2 2023 15:08:54 EDT"
(0) Acct-Delay-Time = 0
(0) Acct-Authentic = RADIUS
(0) NAS-IP-Address = 192.168.1.248
(0) NAS-Identifier = "MX204-LAB-WZTECH"

Não há atualmente comando para desabilitar o envio de Accounting-On e/ou Accounting-Off do MX. É obrigatório que os RADIUS Servers respondam estas mensagens.

```
set access profile ACCESS-PROFILE radius options calling-station-id-delimiter :
set access profile ACCESS-PROFILE radius options calling-station-id-format mac-address
set access profile ACCESS-PROFILE radius options calling-station-id-format vlan
```

Dentro do processo de autenticação e accounting, por default o BNG não envia o AVP Calling-Station-Id. Alguns provedores querem receber este campo com o MAC Address do usuário por exemplo para fazer controle de sessão no RADIUS baseado no MAC. Neste caso é possível configurar o que será enviado no AVP Calling-Station-Id. No exemplo acima está sendo configurado que neste AVP será enviado o MAC-Address do assinante (mac-address) e também a VLAN do usuário (vlan). Também está configurado que o delimitador que delimitará os valores dos dois campos será o símbolo **:** (dois pontos). A seguir como chegará o AVP Calling-Station-Id no RADIUS:

(5) Calling-Station-Id = "38-90-52-67-06-4d:200"

Neste caso foi enviado o MAC + o delimitador + a VLAN do usuário que é a VLAN 200.

O MAC Address neste caso é sempre enviado com o delimitador sendo o hiffen (-). Não é suportado mudar o delimitador do MAC Address ou de qualquer outro campo. Apenas é suportado mudar o delimitador que delimita as informações que serão enviadas no atributo.

A seguir um exemplo de um Access-Request sendo enviado do BNG para o RADIUS:

(16) Received Access-Request Id 188 from 192.168.1.248:49784 to 192.168.1.236:1812 length 258
(16) User-Name = "wztech3"
(16) Service-Type = Framed-User
(16) Framed-Protocol = PPP
(16) CHAP-Password = 0x2d2d06bdb4dcba377e6db57c9b7ccf64d2
(16) CHAP-Challenge = 0xc99f174ad5d576b1f6c81bcb6d26059bd90d332a09925deb1ffe05b4
(16) Chargeable-User-Identity = 0x00
(16) Acct-Session-Id = "79"
(16) Calling-Station-Id = "38-90-52-67-06-4d:200"
(16) ERX-Dhcp-Mac-Addr = "3890.5267.064d"
(16) NAS-Identifier = "MX204-LAB-WZTECH"
(16) NAS-Port = 0
(16) NAS-Port-Id = "ae0.demux0.3221225541:200"
(16) NAS-Port-Type = Ethernet
(16) ERX-Client-Profile-Name = "SUBSCRIBER-PROFILE:"
(16) ERX-Pppoe-Description = "pppoe 38:90:52:67:06:4d"
(16) NAS-IP-Address = 192.168.1.248

O MAC Address do usuário também é enviado nos campos ERX-Dhcp-Mac-Addr (Vendor 4874 / Atributo 56) e no campo ERX-Pppoe-Description (Vendor 4874 / Atributo 24).

```
set access profile ACCESS-PROFILE accounting address-change-immediate-update
```

Quando o usuário faz a conexão PPPoE, caso o BNG possua configuração de SLAAC ele já aloca para o assinante um prefixo NDRA independente do usuário enviar o Router Solicit ou não. Consequentemente esse prefixo NDRA alocado para o usuário é enviado no Accounting-Start para os RADIUS Servers. Após a conexão PPPoE ser estabelecida dependendo da configuração da ONU ela pode enviar o DHCPv6 Solicit requisitando IPv6 para a WAN e/ou LAN (DHCP IA_NA e/ou DHCP IA_PD). Quando isso acontece o Accounting-Start já foi enviado para o RADIUS e o RADIUS não recebeu os prefixos IPv6 que foram alocados para o assinante através do protocolo DHCPv6 haja vista que isso é um processo posterior ao momento do estabelecimento do túnel PPPoE. Neste caso a configuração acima se torna obrigatória. Ela informa ao BNG que qualquer mudança de endereço do assinante no BNG (seja um novo endereço adicionado ao usuário ou um endereço que foi removido do usuário) será gerado um Accounting-Update para o RADIUS atualizando as informações.

Exemplo abaixo do comportamento de uma ONU configurada como SLAAC na WAN + DHCP PD na LAN:

(8) Received Accounting-Request Id 146 from 192.168.1.248:49784 to 192.168.1.236:1813 length 592
(8) User-Name = "wztech3"
(8) Acct-Status-Type = Start
(8) Acct-Session-Id = "30"
(8) Event-Timestamp = "Sep 2 2023 16:08:40 EDT"
(8) Acct-Delay-Time = 0
(8) Service-Type = Framed-User
(8) Framed-Protocol = PPP
(8) Filter-Id = "IPV4-ingress:100M-IPV4-IN-pp0.3221225501-in"
(8) Filter-Id = "IPV4-egress:100M-IPV4-OUT-pp0.3221225501-out"
(8) Filter-Id = "IPV6-ingress:100M-IPV6-IN-pp0.3221225501-in"
(8) Filter-Id = "IPV6-egress:100M-IPV6-OUT-pp0.3221225501-out"
(8) Attr-26.4874.177 = 0x506f72742073706565643a20323030303030306b
(8) Framed-IPv6-Prefix = 2804:ee4:8000:5::/64
(8) Framed-IPv6-Pool = "POOL-V6-NDRA"
(8) Framed-Interface-Id = f94a:118c:8940:1d21
(8) Acct-Authentic = RADIUS
(8) Calling-Station-Id = "38-90-52-67-06-4d:200"
(8) ERX-Dhcp-Mac-Addr = "3890.5267.064d"

(8) ERX-Egress-Policy-Name = "100M-IPV4-OUT"
(8) Framed-IP-Address = 192.168.10.7
(8) Framed-IP-Netmask = 255.255.255.255
(8) ERX-Ingress-Policy-Name = "100M-IPV4-IN"
(8) NAS-Identifier = "MX204-LAB-WZTECH"
(8) NAS-Port = 0
(8) NAS-Port-Id = "ae0.demux0.3221225500:200"
(8) NAS-Port-Type = Ethernet
(8) ERX-IPv6-Ingress-Policy-Name = "100M-IPV6-IN"
(8) ERX-IPv6-Egress-Policy-Name = "100M-IPV6-OUT"
(8) ERX-Virtual-Router-Name = "default:default"
(8) ERX-Pppoe-Description = "pppoe 38:90:52:67:06:4d"
(8) Attr-26.4874.210 = 0x00000004
(8) NAS-IP-Address = 192.168.1.248

No Accounting-Start foi informado o prefixo NDRA (Framed-IPv6-Prefix) porém não há o AVP Delegated-IPv6-Prefix.

Assim que a ONU negocia o prefixo IPv6 de PD o BNG manda um novo Accounting (Update) atualizando as informações:

(9) Received Accounting-Request Id 147 from 192.168.1.248:49784 to 192.168.1.236:1813 length 616
(9) User-Name = "wztech3"
(9) Acct-Status-Type = Interim-Update
(9) Acct-Session-Id = "30"
(9) Event-Timestamp = "Sep 2 2023 16:08:45 EDT"
(9) Acct-Session-Time = 5
(9) Acct-Delay-Time = 0
(9) Service-Type = Framed-User
(9) Framed-Protocol = PPP
(9) Filter-Id = "IPV4-ingress:100M-IPV4-IN-pp0.3221225501-in"
(9) Filter-Id = "IPV4-egress:100M-IPV4-OUT-pp0.3221225501-out"
(9) Filter-Id = "IPV6-ingress:100M-IPV6-IN-pp0.3221225501-in"
(9) Filter-Id = "IPV6-egress:100M-IPV6-OUT-pp0.3221225501-out"
(9) Attr-26.4874.177 = 0x506f72742073706565643a2032303030303030306b
(9) Framed-IPv6-Prefix = 2804:ee4:8000:5::/64
(9) Delegated-IPv6-Prefix = 2804:ee4:4000::/64
(9) Framed-IPv6-Pool = "NOVO-IA_NA"
(9) Framed-Interface-Id = f94a:118c:8940:1d21
(9) Acct-Authentic = RADIUS
(9) Calling-Station-Id = "38-90-52-67-06-4d:200"
(9) ERX-Dhcp-Mac-Addr = "3890.5267.064d"
(9) ERX-Egress-Policy-Name = "100M-IPV4-OUT"
(9) Framed-IP-Address = 192.168.10.7
(9) Framed-IP-Netmask = 255.255.255.255
(9) ERX-Ingress-Policy-Name = "100M-IPV4-IN"
(9) NAS-Identifier = "MX204-LAB-WZTECH"
(9) NAS-Port = 0
(9) NAS-Port-Id = "ae0.demux0.3221225500:200"
(9) NAS-Port-Type = Ethernet
(9) ERX-IPv6-Ingress-Policy-Name = "100M-IPV6-IN"
(9) ERX-IPv6-Egress-Policy-Name = "100M-IPV6-OUT"
(9) ERX-Virtual-Router-Name = "default:default"
(9) ERX-Pppoe-Description = "pppoe 38:90:52:67:06:4d"
(9) Attr-26.4874.210 = 0x00000200
(9) NAS-IP-Address = 192.168.1.248

O atributo 210 do Vendor 4874 é o atributo Acct-Request-Reason. Neste caso foi enviado o valor 0x0200 que significa que o Acconting-Update foi enviado em virtude de mudança de endereço do usuário:

26-210	Acct-Request-Reason	Reason for sending an Accounting-Request message.	integer: 4-octet • 0x0001 = Acct-Start-Ack; that is, receipt of an Acct response for the Acct-Start message 0x0002 = Periodic/Timed interval interim 0x0004 = IP active 0x0008 = IP inactive 0x0010 = IPv6 active 0x0020 = IPv6 inactive 0x0040 = Session active 0x0080 = Session inactive 0x0100 = Line speed change 0x0200 = Address assignment change 0x0400 = Completion of processing of CoA request	No

Todos os AVP's RADIUS suportados pelo BNG tanto IETF quanto atributos VSA estão documentados pela Juniper na seguinte URL:

https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-sessions/topics/topic-map/radius-std-attributes-vsas-support.html

```
set access profile ACCESS-PROFILE accounting statistics volume-time
```

Com a configuração do volume-time o BNG passa a contabilizar pacotes e bytes do assinante. Já detalhado anteriormente no documento.

```
set access profile ACCESS-PROFILE session-options strip-user-name delimiter "@"
```

Esta configuração pode ser útil em cenários onde o ISP quer remover o domínio do usuário antes de enviar a autenticação para os servidores RADIUS. Neste caso se for enviado por exemplo a autenticação do usuário user1@wztech.com.br o BNG vai fazer a remoção "strip" do dominio para enviar Access-Request e Accounting-Request para o radius e no RADIUS chegará apenas user1 como usuário.

```
set access profile ACCESS-PROFILE accounting update-interval 720
```

Esta configuração acima habilita o Interim-Update. Por default o BNG vai gerar o Accounting-Start quando o assinante se conecta e o Accounting-Stop quando o assinante se desconecta. A configuração acima faz com que o BNG a cada 12 horas (720 minutos) gere um novo Interim-Update para o RADIUS. O Interim-Update pode ser útil em casos em que é desejável que em um período (24 horas por exemplo) sempre vai ter as informações do usuário conectado mesmo que ele fique um tempo longo sem se desconectar. O ponto de atenção é o volume de requisições geradas. Caso habilitado deve ser ajustado o update-interval para um valor que não onere o BNG nem os servidores RADIUS. Exemplo de um Accounting-Update:

(67) Received Accounting-Request Id 239 from 192.168.1.248:63120 to 192.168.1.236:1813 length 621
(67) User-Name = "wztech3"

```
(67)  Acct-Status-Type = Interim-Update
(67)  Acct-Session-Id = "371"
(67)  Event-Timestamp = "Sep 14 2023 16:56:18 EDT"
(67)  Acct-Session-Time = 4200
(67)  Acct-Delay-Time = 0
(67)  Service-Type = Framed-User
(67)  Framed-Protocol = PPP
(67)  Filter-Id = "IPV4-ingress:100M-IPV4-IN-pp0.3221225614-in"
(67)  Filter-Id = "IPV4-egress:100M-IPV4-OUT-pp0.3221225614-out"
(67)  Filter-Id = "IPV6-ingress:100M-IPV6-IN-pp0.3221225614-in"
(67)  Filter-Id = "IPV6-egress:100M-IPV6-OUT-pp0.3221225614-out"
(67)  Attr-26.4874.177 = 0x506f72742073706565643a2032303030303030306b
(67)  Framed-IPv6-Prefix = 2904:ee4:8000:17::/64
(67)  Delegated-IPv6-Prefix = 1010:ee4:4000:6::/64
(67)  Framed-IPv6-Pool = "POOL-V6-NDRA-1"
(67)  Framed-Interface-Id = f146:b9b1:6e45:32d7
(67)  Acct-Authentic = RADIUS
(67)  Calling-Station-Id = "38-90-52-67-06-4d:200"
(67)  ERX-Dhcp-Mac-Addr = "3890.5267.064d"
(67)  ERX-Egress-Policy-Name = "100M-IPV4-OUT"
(67)  Framed-IP-Address = 192.168.60.1
(67)  Framed-IP-Netmask = 255.255.255.255
(67)  ERX-Ingress-Policy-Name = "100M-IPV4-IN"
(67)  NAS-Identifier = "MX204-LAB-WZTECH"
(67)  NAS-Port = 0
(67)  NAS-Port-Id = "ae0.demux0.3221225605:200"
(67)  NAS-Port-Type = Ethernet
(67)  ERX-IPv6-Ingress-Policy-Name = "100M-IPV6-IN"
(67)  ERX-IPv6-Egress-Policy-Name = "100M-IPV6-OUT"
(67)  ERX-Virtual-Router-Name = "default:default"
(67)  ERX-Pppoe-Description = "pppoe 38:90:52:67:06:4d"
(67)  Attr-26.4874.210 = 0x00000002
(67)  NAS-IP-Address = 192.168.1.248
```

O atributo 210 do Vendor 4874 é o atributo Acct-Request-Reason. Neste caso foi enviado o valor 0x0002 que significa que o Acconting-Update foi enviado em virtude de update periódico configurado.

```
set access profile ACCESS-PROFILE radius-server 192.168.1.236 max-outstanding-requests 2000
set access profile ACCESS-PROFILE radius-server 192.168.1.102 max-outstanding-requests 2000
```

Por default no MX cada servidor radius tem uma fila (outstanding-requests) que são armazenadas as autenticações e accountings que estão sendo processados. Funciona como uma espécie de um buffer. Esta fila possui um limite máximo de 2000 requisições por servidor RADIUS e por default esta fila tem o tamanho de 1000 requisições. Enquanto uma requisição de autenticação ou accounting não é respondido esta requisição fica nesta fila. Quando o servidor radius responde a requisição esta entrada é removida.

Se o servidor radius estiver lento para responder as requisições de autenticação e/ou accounting esta fila pode chegar no limite e o BNG começará a descartar requisições de autenticações e accounting gerando instabilidade no ambiente.

A seguir o comando mostrando que a fila dos radius servers da access profile ACCESS-PROFILE estão configurados com 2000 requisições. Este comando mostra o volume atual de requisições na fila, qual o pico e se chegou a bater o limite.

```
admin@MX204-LAB-WZTECH> show network-access aaa statistics radius
Outstanding Requests
  RADIUS Server     Profile              Configured   Current   Peak   Exceeded
  192.168.1.236     ACCESS-PROFILE             2000         0      1          0
                    ACCESS-PROFILE-2           1000         0      0          0
  192.168.1.102     ACCESS-PROFILE             2000         0      1          0
```

```
                    ACCESS-PROFILE-2           1000          0       0           0
```

Existem outros comandos que podem ajudar no processo de análise dos servidores radius em casos de problemas e que mostram detalhes dos pacotes enviados para os servidores radius:

```
admin@MX204-LAB-WZTECH> show network-access aaa radius-servers detail
  Profile: ACCESS-PROFILE
    Server address: 192.168.1.236
      Authentication port: 1812
      Preauthentication port: 1812
      Accounting port: 1813
      Status: UP
    Server address: 192.168.1.102
      Authentication port: 1812
      Preauthentication port: 1812
      Accounting port: 1813
      Status: UP
  Profile: ACCESS-PROFILE-2
    Server address: 192.168.1.102
      Authentication port: 1812
      Preauthentication port: 1812
      Accounting port: 1813
      Status: UP

RADIUS Servers
  192.168.1.236
    Last Round Trip Time: 0
    Authentication requests: 17
    Authentication rollover requests: 0
    Authentication retransmissions: 15
    Accepts: 12
    Rejects: 0
    Challenges: 0
    Authentication malformed responses: 0
    Authentication bad authenticators: 0
    Authentication requests pending: 0
    Authentication request timeouts: 20
    Authentication unknown responses: 0
    Authentication packets dropped: 0
    Preauthentication requests: 0
    Preauthentication rollover requests: 0
    Preauthentication retransmissions: 0
    Preauthentication accepts: 0
    Preauthentication rejects: 0
    Preauthentication challenges: 0
    Preauthentication malformed responses: 0
    Preauthentication bad authenticators: 0
    Preauthentication requests pending: 0
    Preauthentication request timeouts: 0
    Preauthentication unknown responses: 0
    Preauthentication packets dropped: 0
    Accounting start requests: 12
    Accounting interim requests: 14
    Accounting stop requests: 11
    Accounting rollover requests: 0
    Accounting retransmissions: 30
    Accounting start responses: 12
    Accounting interim responses: 14
    Accounting stop responses: 10
    Accounting malformed responses: 0
    Accounting bad authenticators: 0
    Accounting requests pending: 0
    Accounting request timeouts: 40
    Accounting unknown responses: 0
    Accounting packets dropped: 0
    Dynamic request change of authorization: 0
    Dynamic request disconnect: 0
    Dynamic request unknown: 0
    Dynamic request malformed: 0
    Dynamic request bad authenticators: 0
    Dynamic request invalid length: 0
  192.168.1.102
    Last Round Trip Time: 0
    Authentication requests: 16
    Authentication rollover requests: 5
    Authentication retransmissions: 48
    Accepts: 0
    Rejects: 0
    Challenges: 0
    Authentication malformed responses: 0
    Authentication bad authenticators: 0
```

```
    Authentication requests pending: 0
    Authentication request timeouts: 64
    Authentication unknown responses: 0
    Authentication packets dropped: 0
    Preauthentication requests: 0
    Preauthentication rollover requests: 0
    Preauthentication retransmissions: 0
    Preauthentication accepts: 0
    Preauthentication rejects: 0
    Preauthentication challenges: 0
    Preauthentication malformed responses: 0
    Preauthentication bad authenticators: 0
    Preauthentication requests pending: 0
    Preauthentication request timeouts: 0
    Preauthentication unknown responses: 0
    Preauthentication packets dropped: 0
    Accounting start requests: 0
    Accounting interim requests: 0
    Accounting stop requests: 1
    Accounting rollover requests: 10
    Accounting retransmissions: 60
    Accounting start responses: 0
    Accounting interim responses: 0
    Accounting stop responses: 0
    Accounting malformed responses: 0
    Accounting bad authenticators: 0
    Accounting requests pending: 0
    Accounting request timeouts: 80
    Accounting unknown responses: 0
    Accounting packets dropped: 0
    Dynamic request change of authorization: 0
    Dynamic request disconnect: 0
    Dynamic request unknown: 0
    Dynamic request malformed: 0
    Dynamic request bad authenticators: 0
    Dynamic request invalid length: 0
```

```
admin@MX204-LAB-WZTECH> show network-access aaa statistics authentication detail
Authentication module statistics
  Requests received: 28
  Accepts: 12
  Rejects: 0
    RADIUS authentication failures: 0
      Queue request deleted: 0
      Malformed reply: 0
      No server configured: 0
      Access Profile configuration not found: 0
      Unable to create client record: 0
      Unable to create client request: 0
      Unable to build authentication request: 0
      No available server: 0
      Unable to create handle: 0
      Unable to queue request: 0
      Invalid credentials: 0
      Malformed request: 0
      License unavailable: 0
      Redirect requested: 0
      Internal failure: 0
    Local authentication failures: 0
    LDAP lookup failures: 0
  Challenges: 0
  Timed out requests: 16
```



```
admin@MX204-LAB-WZTECH> show network-access aaa statistics accounting detail
Accounting module statistics
  Requests received: 57
  Accounting request failures: 0
  Accounting request success: 57
    Account on requests: 20
    Accounting start requests: 12
    Accounting interim requests: 14
    Accounting stop requests: 12
  Timed out requests: 20
  Accounting response failures: 0
  Accounting response success: 37
    Account on responses: 1
    Accounting start responses: 12
    Accounting interim responses: 14
    Accounting stop responses: 10
  Accounting rollover requests: 10
  Accounting unknown responses: 0
  Accounting radius pending requests: 0
```

```
  Accounting malformed responses: 0
  Accounting retransmissions: 90
  Accounting bad authenticators: 0
  Accounting packets dropped: 0
  Accounting backup record creation requests: 0
  Accounting backup request replay success: 0
  Accounting backup request failures: 0
  Accounting backup request success: 0
  Accounting backup timeouts: 0
  Accounting backup in-flight requests: 0
  Accounting backup responses success: 0
  Accounting backup radius requests: 0
  Accounting backup radius responses: 0
  Accounting backup radius timeouts: 0
  Accounting backup radius pending requests: 0
  Accounting backup radius retransmissions: 0
  Accounting backup malformed responses: 0
  Accounting backup bad authenticators: 0
  Accounting backup responses dropped: 0
  Accounting backup rollover requests: 0
  Accounting backup unknown responses: 0
```

10.1.2.3. RADIUS CoA / Disconnect-Request

Depois que o usuário se conecta no BNG é possível enviar requisições para desconectar um usuário conectado (Disconnect-Request) e é possível também alterar os parâmetros de um usuário conectado sem que ele seja desconectado (CoA - Change of Authorization).

Em ambos os casos ao invés do BNG enviar pacotes para os radius servers quem inicia esta comunicação enviando mensagens para o BNG é o servidor RADIUS.

Por default, para processar mensagens de Disconnect-Request ou CoA o BNG espera receber estas mensagens na porta 3799 do protocolo UDP:

```
admin@MX204-LAB-WZTECH> show system connections | match 3799
udp46      0      0  *.3799                                 *.*
udp4       0      0  *.3799                                 *.*
```

Importante: Há a possibilidade de especificar em [access] as configurações de radius-disconnect-port e radius-disconnect <client>. Estas configurações são obsoletas e não mudam nenhum comportamento do BNG.

Já foi detalhado anteriormente na explicação das configurações dos radius-servers a precedência destas definições. Caso haja alguma definição na access profile do usuário o BNG não fará a leitura dos radius-servers globais [access radius-server].

Para o Disconnect-Request ou CoA funcionar basta apenas que o radius-server que vai enviar estas mensagens esteja definido ou na access profile do usuário ou globalmente (caso não existam definições de radius-servers na access profile). Mesmo que o radius-server que vai enviar as mensagens de Disconnect-Request ou CoA não esteja configurado na lista do authentication-server ou accounting-server ou até mesmo o authentication order da access profile esteja configurado como "none", apenas com o radius-server estando definido é o suficiente para o BNG permitir mensagens de Disconnect-Request ou CoA deste servidor.

Caso seja necessário trocar a porta do Disconnect-Request/CoA no BNG pode-se alterar a porta utilizando a configuração a seguir:

```
set access profile ACCESS-PROFILE radius-server 192.168.1.236 dynamic-request-port 1700
set access profile ACCESS-PROFILE radius-server 192.168.1.236 secret "$9$cgdrMX7Nbg4Z7NqfTz6/"
set access profile ACCESS-PROFILE radius-server 192.168.1.236 source-address 192.168.1.248
set access profile ACCESS-PROFILE radius-server 192.168.1.102 dynamic-request-port 1700
set access profile ACCESS-PROFILE radius-server 192.168.1.102 secret "$9$apGHmf5F9Cuf5hrevLX"
set access profile ACCESS-PROFILE radius-server 192.168.1.102 source-address 192.168.1.248
```

A definição deve ser aplicada em todos os radius-server definidos na acess profile do usuário ou globalmente (caso os radius-servers não tenham sido definidos na access profile).

Neste caso o BNG aceitará tanto mensagens do tipo Disconnect-Request quanto mensagens CoA (Change of Authorization).

Em ambos os casos para que o servidor RADIUS envie mensagens de Disconnect-Request ou CoA é necessário que seja o AVP User-Name ou o AVP Acct-Session-ID na requisição. O BNG utilizará esta informação para encontrar a sessão do assinante.

Table 1: Identification Attributes

Attribute	Description
User-Name [RADIUS attribute 1]	Subscriber username.
Acct-Session-ID [RADIUS attribute 44]	Specific subscriber session.

Caso seja utilizado o User-Name na requisição e existam mais conexões com o mesmo usuário o BNG processará a ação do Disconnect-Request ou CoA apenas para o primeiro assinante conectado. Os demais não sofrerão nenhuma modificação. Caso exista no múltiplas conexões com o mesmo User-Name é recomendado o uso do atributo Acct-Session-ID para fazer as modificações no assinante.

```
admin@MX204-LAB-WZTECH> show network-access aaa subscribers username wztech2
Logical system/Routing instance   Client type    Session-ID     Session uptime    Accounting
default:default                   pppoe          1141           00:01:50          on/volume+time
default:default                   pppoe          1144           00:00:55          on/volume+time
```

Exemplo de sucesso com software FreeRadius gerando o Disconnect-Request tanto com User-Name quanto com Acct-Session-ID:

```
[root@freeradius-mist ~]# echo "User-Name=wztech3" | radclient -x 192.168.1.248:1700 disconnect rad1u5
Sent Disconnect-Request Id 241 from 0.0.0.0:45520 to 192.168.1.248:1700 length 29
        User-Name = "wztech3"
Received Disconnect-ACK Id 241 from 192.168.1.248:1700 to 0.0.0.0:0 length 20
```

```
[root@freeradius-mist ~]# echo "Acct-Session-ID=1141" | radclient -x 192.168.1.248:1700 disconnect rad1u5
Sent Disconnect-Request Id 133 from 0.0.0.0:52428 to 192.168.1.248:1700 length 26
        Acct-Session-Id = "1141"
Received Disconnect-ACK Id 133 from 192.168.1.248:1700 to 0.0.0.0:0 length 20
```

O Acct-Session-ID é enviado do BNG para o RADIUS quando o assinante se conecta. O atributo é enviado tanto no Access-Request quanto no Accounting-Request:

```
(1) Received Access-Request Id 2 from 192.168.1.248:51852 to 192.168.1.236:1812 length 254
(1)   User-Name = "wztech3"
(1)   Service-Type = Framed-User
(1)   Framed-Protocol = PPP
(1)   CHAP-Password = 0x009e8a50957dea974dd56784e058880eab
(1)   CHAP-Challenge = 0x7abdb909cddbb01af872ed0fe5cb70cde88e111e4f7c6c
(1)   Chargeable-User-Identity = 0x00
(1)   Acct-Session-Id = "704"
(1)   Calling-Station-Id = "38-90-52-67-06-4d:200"
(1)   ERX-Dhcp-Mac-Addr = "3890.5267.064d"
(1)   NAS-Identifier = "MX204-LAB-WZTECH"
(1)   NAS-Port = 0
(1)   NAS-Port-Id = "ae0.demux0.3221225616:200"
(1)   NAS-Port-Type = Ethernet
(1)   ERX-Client-Profile-Name = "SUBSCRIBER-PROFILE:"
(1)   ERX-Pppoe-Description = "pppoe 38:90:52:67:06:4d"
(1)   NAS-IP-Address = 192.168.1.248
```

Este Session-ID também pode ser obtido no BNG com o comando abaixo:

```
admin@MX204-LAB-WZTECH> show network-access aaa subscribers username wztech3
Logical system/Routing instance   Client type    Session-ID     Session uptime    Accounting
default:default                   pppoe          704            00:08:06          on/volume+time
Service name              Service type   Quota          Accounting
SERVICE-PROFILE-2(20m,20m) -na-          -na-           off
```

É o Session-ID da sessão PPPoE (704).

Pode ser obtido também detalhando as informações do usuário:

```
admin@MX204-LAB-WZTECH> show subscribers vlan-id 200 extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.3221225942
Interface type: Dynamic
Underlying Interface: xe-0/1/0
Dynamic Profile Name: SVLAN-DYNAMIC-PROFILE
Dynamic Profile Version: 1
State: Active
Session ID: 703
PFE Flow ID: 664
VLAN Id: 200
Login Time: 2023-08-08 21:49:17 -03

Type: PPPoE
User Name: wztech3
IP Address: 100.64.10.78
IP Netmask: 255.255.255.255
Primary DNS Address: 8.8.8.8
Secondary DNS Address: 8.8.4.4
IPv6 Address: 2090::4
IPv6 Prefix: 1010:ee4:4000:f::/64
Domain name server inet6: 2001:4860:4860::8888 2001:4860:4860::8844
IPv6 User Prefix: 2804:ee4:8000:85::/64
Logical System: default
Routing Instance: default
Interface: pp0.3221225943
Interface type: Dynamic
Underlying Interface: demux0.3221225942
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 17
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 704
Session ID: 704
PFE Flow ID: 666
VLAN Id: 200
Login Time: 2023-08-08 21:49:17 -03
Service Sessions: 1
IP Address Pool: POOL-IP-01
IPv6 Address Pool: NOVO-IA_NA
IPv6 Framed Interface Id: 509c:8a7:e622:1507
Accounting interval: 0
Dynamic configuration:
  junos-ipv6-ndra-prefix: 2804:ee4:8000:85::/64

   Service Session ID: 707
   Service Session Name: SERVICE-PROFILE-2
   Service Session Version: 1
   State: Active
   Family: inet, inet6
   Service session type: Service-Profile
   IPv4 Input Filter Name: FILTERv4-IN_UID1682-pp0.3221225943-in
   IPv4 Output Filter Name: FILTERv4-OUT_UID1684-pp0.3221225943-out
   IPv6 Input Filter Name: FILTERv6-IN_UID1685-pp0.3221225943-in
   IPv6 Output Filter Name: FILTERv6-OUT_UID1686-pp0.3221225943-out
   Service Activation time: 2023-08-08 21:52:19 -03
   Dynamic configuration:
     BANDWIDTH-IN: 20m
     BANDWIDTH-OUT: 20m
     BURST-IN: 2m
     BURST-OUT: 2m
     FILTERv4-IN: FILTERv4-IN_UID1682
     FILTERv4-OUT: FILTERv4-OUT_UID1684
     FILTERv6-IN: FILTERv6-IN_UID1685
```

```
    FILTERv6-OUT: FILTERv6-OUT_UID1686
    POLICER-IN: POLICER-IN_UID1681
    POLICER-OUT: POLICER-OUT_UID1683
```

É o Session-Id da interface PPPoE. Não é o Session-Id da interface VLAN.

Caso o BNG não tenha o Session-Id local instalado ou não aceite a requisição ele devolverá um NACK:

```
[root@freeradius-mist ~]# echo "Acct-Session-ID=1141" | radclient -x 192.168.1.248:1700 disconnect rad1u5
Sent Disconnect-Request Id 208 from 0.0.0.0:45649 to 192.168.1.248:1700 length 26
      Acct-Session-Id = "1141"
Received Disconnect-NAK Id 208 from 192.168.1.248:1700 to 0.0.0.0:0 length 26
      Error-Cause = Session-Context-Not-Found
            (0)   -: Expected Disconnect-ACK got Disconnect-NAK
```

Outra opção que pode ser utilizada é o CoA (Change of Authorization). Neste caso ao invés de apenas desconectar uma sessão é possível adicionar, deletar e/ou atualizar os serviços dos usuários.

O CoA só fará esta mudança caso o usuário esteja utilizando Service Profile com variáveis dinâmicas. Não é suportado atualmente fazer mudanças em um usuário conectado caso ele esteja utilizando Subscriber Profile padrão. Neste documento há o detalhamento do funcionamento da Service Profile com variáveis dinâmicas.

A seguir um exemplo de um usuário configurado no RADIUS para receber a Service Profile configurada no BNG com variáveis dinâmicas:

Configuração no FreeRADIUS:

```
wztech3  Cleartext-Password := "wztech3"
                ERX-Service-Activate:1 = "SERVICE-PROFILE(2m,2m)"
```

Está sendo enviado o AVP ERX-Service-Activate (Vendor 4874 / Atributo 65) no momento da autenticação.

O usuário conecta e recebe os valores dinâmicos especificados no RADIUS:

```
admin@MX204-LAB-WZTECH> show subscribers vlan-id 200 extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.3221225945
Interface type: Dynamic
Underlying Interface: xe-0/1/0
Dynamic Profile Name: SVLAN-DYNAMIC-PROFILE
Dynamic Profile Version: 1
State: Active
Session ID: 708
PFE Flow ID: 668
VLAN Id: 200
Login Time: 2023-08-08 22:07:21 -03

Type: PPPoE
User Name: wztech3
IP Address: 100.64.10.79
IP Netmask: 255.255.255.255
Primary DNS Address: 8.8.8.8
Secondary DNS Address: 8.8.4.4
IPv6 Address: 2090::4
IPv6 Prefix: 1010:ee4:4000:f::/64
Domain name server inet6: 2001:4860:4860::8888 2001:4860:4860::8844
IPv6 User Prefix: 2804:ee4:8000:86::/64
Logical System: default
Routing Instance: default
Interface: pp0.3221225946
Interface type: Dynamic
Underlying Interface: demux0.3221225945
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 17
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 709
```

```
Session ID: 709
PFE Flow ID: 670
VLAN Id: 200
Login Time: 2023-08-08 22:07:21 -03
Service Sessions: 1
IP Address Pool: POOL-IP-01
IPv6 Address Pool: NOVO-IA_NA
IPv6 Framed Interface Id: 95a2:bf14:5697:e51
Accounting interval: 0
Dynamic configuration:
  junos-ipv6-ndra-prefix: 2804:ee4:8000:86::/64

   Service Session ID: 710
   Service Session Name: SERVICE-PROFILE
   Service Session Version: 1
   State: Active
   Family: inet, inet6
   Service session type: Service-Profile
   IPv4 Input Filter Name: FILTERv4-IN_UID1688-pp0.3221225946-in
   IPv4 Output Filter Name: FILTERv4-OUT_UID1690-pp0.3221225946-out
   IPv6 Input Filter Name: FILTERv6-IN_UID1691-pp0.3221225946-in
   IPv6 Output Filter Name: FILTERv6-OUT_UID1692-pp0.3221225946-out
   Service Activation time: 2023-08-08 22:07:21 -03
   Dynamic configuration:
     BANDWIDTH-IN: 2m
     BANDWIDTH-OUT: 4m
     BURST-IN: 2m
     BURST-OUT: 2m
     FILTERv4-IN: FILTERv4-IN_UID1688
     FILTERv4-OUT: FILTERv4-OUT_UID1690
     FILTERv6-IN: FILTERv6-IN_UID1691
     FILTERv6-OUT: FILTERv6-OUT_UID1692
     POLICER-IN: POLICER-IN_UID1687
     POLICER-OUT: POLICER-OUT_UID1689

admin@MX204-LAB-WZTECH>
```

A seguir é enviado um comando de CoA do radius server para deletar o serviço atual do usuário. É necessário que o nome do serviço seja exatamente o mesmo que está instalado atualmente no BNG. Neste caso é enviado o AVP ERX-Service-Deactivate (Vendor 4874 / Atributo 66)

```
[root@freeradius-mist freeradius]# echo "User-Name=wztech3,ERX-Service-Deactivate = \"SERVICE-PROFILE\"" | radclient -x 192.168.1.248:3799 coa rad1u5
Sent CoA-Request Id 119 from 0.0.0.0:44952 to 192.168.1.248:3799 length 52
      User-Name = "wztech3"
      ERX-Service-Deactivate = "SERVICE-PROFILE "
Received CoA-ACK Id 119 from 192.168.1.248:3799 to 0.0.0.0:0 length 20
[root@freeradius-mist freeradius]#
```

Como o serviço dinâmico do usuário foi desativado ele ficou sem nenhuma Service Profile ativa. Neste caso o BNG deixa o usuário navegar sem nenhum controle de banda e filtros.

Posteriormente é ativado uma nova Service Profile com variáveis dinâmicas que está configurada no BNG chamada SERVICE-PROFILE-2:

```
[root@freeradius-mist freeradius]# echo "User-Name=wztech3,ERX-Service-Activate:1 = \"SERVICE-PROFILE-2(2m,10m)\"" | radclient -x 192.168.1.248:3799 coa rad1u5
Sent CoA-Request Id 139 from 0.0.0.0:59924 to 192.168.1.248:3799 length 63
      User-Name = "wztech3"
      ERX-Service-Activate:1 = "SERVICE-PROFILE-2(2m,10m)"
Received CoA-ACK Id 139 from 192.168.1.248:3799 to 0.0.0.0:0 length 20
```

O usuário passou a ter a nova Service Profile enviada no CoA ativada:

```
admin@MX204-LAB-WZTECH> show subscribers vlan-id 200 extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.3221225945
Interface type: Dynamic
Underlying Interface: xe-0/1/0
```

```
Dynamic Profile Name: SVLAN-DYNAMIC-PROFILE
Dynamic Profile Version: 1
State: Active
Session ID: 708
PFE Flow ID: 668
VLAN Id: 200
Login Time: 2023-08-08 22:07:21 -03

Type: PPPoE
User Name: wztech3
IP Address: 100.64.10.79
IP Netmask: 255.255.255.255
Primary DNS Address: 8.8.8.8
Secondary DNS Address: 8.8.4.4
IPv6 Address: 2090::4
IPv6 Prefix: 1010:ee4:4000:f::/64
Domain name server inet6: 2001:4860:4860::8888 2001:4860:4860::8844
IPv6 User Prefix: 2804:ee4:8000:86::/64
Logical System: default
Routing Instance: default
Interface: pp0.3221225946
Interface type: Dynamic
Underlying Interface: demux0.3221225945
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 17
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 709
Session ID: 709
PFE Flow ID: 670
VLAN Id: 200
Login Time: 2023-08-08 22:07:21 -03
Service Sessions: 1
IP Address Pool: POOL-IP-01
IPv6 Address Pool: NOVO-IA_NA
IPv6 Framed Interface Id: 95a2:bf14:5697:e51
Accounting interval: 0
Dynamic configuration:
  junos-ipv6-ndra-prefix: 2804:ee4:8000:86::/64

   Service Session ID: 712
   Service Session Name: SERVICE-PROFILE-2
   Service Session Version: 1
   State: Active
   Family: inet, inet6
   Service session type: Service-Profile
   IPv4 Input Filter Name: FILTERv4-IN_UID1694-pp0.3221225946-in
   IPv4 Output Filter Name: FILTERv4-OUT_UID1696-pp0.3221225946-out
   IPv6 Input Filter Name: FILTERv6-IN_UID1697-pp0.3221225946-in
   IPv6 Output Filter Name: FILTERv6-OUT_UID1698-pp0.3221225946-out
   Service Activation time: 2023-08-08 22:11:02 -03
   Dynamic configuration:
     BANDWIDTH-IN: 2m
     BANDWIDTH-OUT: 10m
     BURST-IN: 2m
     BURST-OUT: 2m
     FILTERv4-IN: FILTERv4-IN_UID1694
     FILTERv4-OUT: FILTERv4-OUT_UID1696
     FILTERv6-IN: FILTERv6-IN_UID1697
     FILTERv6-OUT: FILTERv6-OUT_UID1698
     POLICER-IN: POLICER-IN_UID1693
     POLICER-OUT: POLICER-OUT_UID1695
```

Se for enviado uma nova chamada de CoA ativando a mesma Service Profile com novos valores ou outra Service Profile configurada o BNG sem deletar a Service Profile antiga, o BNG vai ativar mais de um serviço para o usuário e comportamento do serviço para o usuário passa a ser inesperado. Tem que deixar apenas um serviço ativo:

Exemplo de ativação indevida de um segundo serviço:

```
[root@freeradius-mist freeradius]# echo "User-Name=wztech3,ERX-Service-Activate:1 = \"SERVICE-PROFILE-2(40m,40m)\"" | radclient -x 192.168.1.248:3799 coa rad1u5
Sent CoA-Request Id 127 from 0.0.0.0:49159 to 192.168.1.248:3799 length 64
      User-Name = "wztech3"
      ERX-Service-Activate:1 = "SERVICE-PROFILE-2(40m,40m)"
Received CoA-ACK Id 127 from 192.168.1.248:3799 to 0.0.0.0:0 length 20
```

```
[root@freeradius-mist freeradius]#
```

Um novo serviço foi ativado sem desativar o serviço antigo:

```
admin@MX204-LAB-WZTECH> show subscribers vlan-id 200 extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.3221225945
Interface type: Dynamic
Underlying Interface: xe-0/1/0
Dynamic Profile Name: SVLAN-DYNAMIC-PROFILE
Dynamic Profile Version: 1
State: Active
Session ID: 708
PFE Flow ID: 668
VLAN Id: 200
Login Time: 2023-08-08 22:07:21 -03

Type: PPPoE
User Name: wztech3
IP Address: 100.64.10.79
IP Netmask: 255.255.255.255
Primary DNS Address: 8.8.8.8
Secondary DNS Address: 8.8.4.4
IPv6 Address: 2090::4
IPv6 Prefix: 1010:ee4:4000:f::/64
Domain name server inet6: 2001:4860:4860::8888 2001:4860:4860::8844
IPv6 User Prefix: 2804:ee4:8000:86::/64
Logical System: default
Routing Instance: default
Interface: pp0.3221225946
Interface type: Dynamic
Underlying Interface: demux0.3221225945
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 17
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 709
Session ID: 709
PFE Flow ID: 670
VLAN Id: 200
Login Time: 2023-08-08 22:07:21 -03
Service Sessions: 2
IP Address Pool: POOL-IP-01
IPv6 Address Pool: NOVO-IA_NA
IPv6 Framed Interface Id: 95a2:bf14:5697:e51
Accounting interval: 0
Dynamic configuration:
  junos-ipv6-ndra-prefix: 2804:ee4:8000:86::/64

   Service Session ID: 712
   Service Session Name: SERVICE-PROFILE-2
   Service Session Version: 1
   State: Active
   Family: inet, inet6
   Service session type: Service-Profile
   IPv4 Input Filter Name: FILTERv4-IN_UID1694-pp0.3221225946-in
   IPv4 Output Filter Name: FILTERv4-OUT_UID1696-pp0.3221225946-out
   IPv6 Input Filter Name: FILTERv6-IN_UID1697-pp0.3221225946-in
   IPv6 Output Filter Name: FILTERv6-OUT_UID1698-pp0.3221225946-out
   Service Activation time: 2023-08-08 22:11:02 -03
   Dynamic configuration:
     BANDWIDTH-IN: 2m
     BANDWIDTH-OUT: 10m
     BURST-IN: 2m
     BURST-OUT: 2m
     FILTERv4-IN: FILTERv4-IN_UID1694
     FILTERv4-OUT: FILTERv4-OUT_UID1696
     FILTERv6-IN: FILTERv6-IN_UID1697
     FILTERv6-OUT: FILTERv6-OUT_UID1698
     POLICER-IN: POLICER-IN_UID1693
     POLICER-OUT: POLICER-OUT_UID1695

   Service Session ID: 713
   Service Session Name: SERVICE-PROFILE-2
   Service Session Version: 1
   State: Active
   Family: inet, inet6
   Service session type: Service-Profile
   IPv4 Input Filter Name: FILTERv4-IN_UID1700-pp0.3221225946-in
```

```
   IPv4 Output Filter Name: FILTERv4-OUT_UID1702-pp0.3221225946-out
   IPv6 Input Filter Name: FILTERv6-IN_UID1703-pp0.3221225946-in
   IPv6 Output Filter Name: FILTERv6-OUT_UID1704-pp0.3221225946-out
   Service Activation time: 2023-08-08 22:13:58 -03
   Dynamic configuration:
     BANDWIDTH-IN: 40m
     BANDWIDTH-OUT: 40m
     BURST-IN: 2m
     BURST-OUT: 2m
     FILTERv4-IN: FILTERv4-IN_UID1700
     FILTERv4-OUT: FILTERv4-OUT_UID1702
     FILTERv6-IN: FILTERv6-IN_UID1703
     FILTERv6-OUT: FILTERv6-OUT_UID1704
     POLICER-IN: POLICER-IN_UID1699
     POLICER-OUT: POLICER-OUT_UID1701

admin@MX204-LAB-WZTECH>
```

É possível enviar a desativação de uma Service Profile juntamente com a ativação de uma nova Service Profile. A seguir enviaremos esta requisição através de CoA. No caso da desativação o BNG vai desativar todas as Service Profiles que estão ativadas para o usuário com o nome que está sendo enviado na requisição.

No exemplo a seguir o BNG vai desativar as duas Service Profiles estão ativas com o mesmo nome e vai ativar apenas um serviço novo:

```
[root@freeradius-mist freeradius]# echo "Acct-Session-ID=709,ERX-Service-Deactivate = \"SERVICE-PROFILE-2\",ERX-Service-Activate:1 = \"DYNAMIC-SERVICE-PROFILE(100m,100m)\"" | radclient -x 192.168.1.248:3799 coa rad1u5
Sent CoA-Request Id 140 from 0.0.0.0:53196 to 192.168.1.248:3799 length 85
        Acct-Session-Id = "709"
        ERX-Service-Deactivate = "SERVICE-PROFILE-2"
        ERX-Service-Activate:1 = "SERVICE-PROFILE(100m,100m)"
Received CoA-ACK Id 140 from 192.168.1.248:3799 to 0.0.0.0:0 length 20
[root@freeradius-mist freeradius]#
```



```
admin@MX204-LAB-WZTECH> show subscribers vlan-id 200 extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.3221225945
Interface type: Dynamic
Underlying Interface: xe-0/1/0
Dynamic Profile Name: SVLAN-DYNAMIC-PROFILE
Dynamic Profile Version: 1
State: Active
Session ID: 708
PFE Flow ID: 668
VLAN Id: 200
Login Time: 2023-08-08 22:07:21 -03

Type: PPPoE
User Name: wztech3
IP Address: 100.64.10.79
IP Netmask: 255.255.255.255
Primary DNS Address: 8.8.8.8
Secondary DNS Address: 8.8.4.4
IPv6 Address: 2090::4
IPv6 Prefix: 1010:ee4:4000:f::/64
Domain name server inet6: 2001:4860:4860::8888 2001:4860:4860::8844
IPv6 User Prefix: 2804:ee4:8000:86::/64
Logical System: default
Routing Instance: default
Interface: pp0.3221225946
Interface type: Dynamic
Underlying Interface: demux0.3221225945
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 17
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 709
Session ID: 709
PFE Flow ID: 670
VLAN Id: 200
Login Time: 2023-08-08 22:07:21 -03
Service Sessions: 1
```

```
IP Address Pool: POOL-IP-01
IPv6 Address Pool: NOVO-IA_NA
IPv6 Framed Interface Id: 95a2:bf14:5697:e51
Accounting interval: 0
Dynamic configuration:
  junos-ipv6-ndra-prefix: 2804:ee4:8000:86::/64

   Service Session ID: 714
   Service Session Name: SERVICE-PROFILE
   Service Session Version: 1
   State: Active
   Family: inet, inet6
   Service session type: Service-Profile
   IPv4 Input Filter Name: FILTERv4-IN_UID1706-pp0.3221225946-in
   IPv4 Output Filter Name: FILTERv4-OUT_UID1708-pp0.3221225946-out
   IPv6 Input Filter Name: FILTERv6-IN_UID1709-pp0.3221225946-in
   IPv6 Output Filter Name: FILTERv6-OUT_UID1710-pp0.3221225946-out
   Service Activation time: 2023-08-08 22:18:41 -03
   Dynamic configuration:
     BANDWIDTH-IN: 100m
     BANDWIDTH-OUT: 100m
     BURST-IN: 2m
     BURST-OUT: 2m
     FILTERv4-IN: FILTERv4-IN_UID1706
     FILTERv4-OUT: FILTERv4-OUT_UID1708
     FILTERv6-IN: FILTERv6-IN_UID1709
     FILTERv6-OUT: FILTERv6-OUT_UID1710
     POLICER-IN: POLICER-IN_UID1705
     POLICER-OUT: POLICER-OUT_UID1707

admin@MX204-LAB-WZTECH>
```

Neste caso o BNG deletou todos os serviços que estavam ativos com o nome SERVICE-PROFILE-2 e ativou um novo serviço SERVICE-PROFILE com a banda enviada na requisição CoA.

Importante: Neste serviço de dynamic service profile com variáveis dinâmicas não há AVP's enviados no Accounting para o RADIUS que informe o nome da Dynamic-Profile nem informação dos valores preenchidos nas variáveis como Banda, Burst, etc... Estas informações não são enviadas via Accounting para o RADIUS.

Existe um VSA chamado ERX-Service-Update (Vendor 4874 / Atributo 180) que tem como propósito apenas atualizar os valores do serviço atualmente já instalado.

Existe um outro VSA chamado ERX-Client-Profile-Name (Vendor 4874 / Atributo 174). Este AVP pode ser enviado pelo RADIUS quando o usuário se conecta e ele não é suportado em mensagens CoA. Se por algum motivo há a necessidade de trocar a dynamic-profile do assinante pode ser utilizado este atributo. Neste caso é enviado a nova subscriber profile que o usuário deverá ser associado. Exemplo:

ERX-Client-Profile-Name = "SUBSCRIBER-PROFILE-2"

O usuário vai conectar utilizando a Subscriber Profile "SUBSCRIBER-PROFILE" e quando ele se conectar o RADIUS vai enviar uma nova subscriber profile chamada "SUBSCRIBER-PROFILE-2"

Neste caso há uma dynamic-profile no BNG chamada SUBSCRIBER-PROFILE-2 com configurações de filtros e IPv6 diferentes:

```
admin@MX204-LAB-WZTECH> show subscribers vlan-id 200 extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.3221225493
Interface type: Dynamic
Underlying Interface: xe-0/1/0
Dynamic Profile Name: SVLAN-DYNAMIC-PROFILE
Dynamic Profile Version: 1
State: Active
Session ID: 27
PFE Flow ID: 58
VLAN Id: 200
Login Time: 2023-08-09 10:02:45 -03

Type: PPPoE
User Name: wztech3
```

```
IP Address: 100.64.10.3
IP Netmask: 255.255.255.255
Primary DNS Address: 8.8.8.8
Secondary DNS Address: 8.8.4.4
IPv6 Address: 2090::4
IPv6 Prefix: 1010:ee4:4000::/64
Domain name server inet6: 2001:4860:4860::8888 2001:4860:4860::8844
IPv6 User Prefix: 2804:ee4:8000:2::/64
Logical System: default
Routing Instance: default
Interface: pp0.3221225494
Interface type: Dynamic
Underlying Interface: demux0.3221225493
Dynamic Profile Name: SUBSCRIBER-PROFILE-2
Dynamic Profile Version: 2
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 28
Session ID: 28
PFE Flow ID: 60
VLAN Id: 200
Login Time: 2023-08-09 10:02:45 -03
IP Address Pool: POOL-IP-01
IPv6 Address Pool: NOVO-IA_NA
IPv6 Framed Interface Id: 75b2:482b:6264:c55f
IPv4 Input Filter Name: 5M-Ingress-v4-pp0.3221225494-in
IPv4 Output Filter Name: 5M-Egress-v4-pp0.3221225494-out
IPv6 Input Filter Name: 5M-Ingress-v6-pp0.3221225494-in
IPv6 Output Filter Name: 5M-Egress-v6-pp0.3221225494-out
Accounting interval: 0
```

Ao invés do assinante pegar as configurações da subscriber profile SUBSCRIBER-PROFILE ele pegou as configurações da subscriber profile enviada pelo RADIUS (SUBSCRIBER-PROFILE-2).

As estatísticas de mensagens CoA e Disconnect-Request podem ser obtidas no BNG de forma global com o comando abaixo:

```
admin@MX204-LAB-WZTECH> show network-access aaa statistics dynamic-requests
Dynamic-requests module statistics
  Requests received: 0
  Processed successfully: 0
  Initial validation successful: 0
  Error: 0
  Silently dropped: 0
Bulk-CoA Transactions
    Received: 0
    Success: 0
    Timeout: 0
    Transaction mismatch: 0
    No services: 0
    Service not found: 0
    Service already active: 0
    Execution failure: 0
    Logout in progress: 0
    Max services exceeded: 0
    Max requests exceeded: 0
    Max concurrent CoAs exceeded: 0
    Extensible services errors: 0
```

Estas estatísticas também podem ser obtidas dentro do radius-server que enviou as mensagens:

```
admin@MX204-LAB-WZTECH> show network-access aaa radius-servers detail
  Profile: ACCESS-PROFILE
    Server address: 192.168.1.236
      Authentication port: 1812
      Preauthentication port: 1812
      Accounting port: 1813
      Status: UP

RADIUS Servers
  192.168.1.236
    Last Round Trip Time: 0
    Authentication requests: 17
    Authentication rollover requests: 0
    Authentication retransmissions: 15
    Accepts: 12
    Rejects: 0
    Challenges: 0
```

```
    Authentication malformed responses: 0
    Authentication bad authenticators: 0
    Authentication requests pending: 0
    Authentication request timeouts: 20
    Authentication unknown responses: 0
    Authentication packets dropped: 0
    Preauthentication requests: 0
    Preauthentication rollover requests: 0
    Preauthentication retransmissions: 0
    Preauthentication accepts: 0
    Preauthentication rejects: 0
    Preauthentication challenges: 0
    Preauthentication malformed responses: 0
    Preauthentication bad authenticators: 0
    Preauthentication requests pending: 0
    Preauthentication request timeouts: 0
    Preauthentication unknown responses: 0
    Preauthentication packets dropped: 0
    Accounting start requests: 12
    Accounting interim requests: 14
    Accounting stop requests: 11
    Accounting rollover requests: 0
    Accounting retransmissions: 30
    Accounting start responses: 12
    Accounting interim responses: 14
    Accounting stop responses: 10
    Accounting malformed responses: 0
    Accounting bad authenticators: 0
    Accounting requests pending: 0
    Accounting request timeouts: 40
    Accounting unknown responses: 0
    Accounting packets dropped: 0
    Dynamic request change of authorization: 0
    Dynamic request disconnect: 0
    Dynamic request unknown: 0
    Dynamic request malformed: 0
    Dynamic request bad authenticators: 0
    Dynamic request invalid length: 0
```

10.1.2.4. Limite de Sessão por Usuário


```
set access profile ACCESS-PROFILE session-limit-per-username 1
```

Neste documento há o detalhamento do controle da quantidade de conexões na mesma interface L2 (VLAN Interface), porém o BNG suporta também fazer o controle da quantidade de conexões dos assinantes que estão utilizando o mesmo login (usuário na conexão PPPoE). Este controle é feito dentro da access profile criando tabelas internamente. Como o limite é na access profile caso seja autenticado um login já existente no BNG através de outra access profile o BNG não fará esta limitação pois o controle é no nivel da access profile. Se houver uma segunda autenticação com um login já existente no BNG na mesma access profile o BNG vai bloquear esta segunda tentativa de autenticação com este usuário e a autenticação não será enviada para os servidores radius.

Para ver estatísticas desse processo de controle de sessão por usuário na access profile o comando abaixo mostra estas informações:

```
admin@MX204-LAB-WZTECH> show network-access aaa statistics session-limit-per-username
  Total blocked requests: 9
  Total usernames exceeding session limit: 1
  Total usernames: 1
```

10.1.3. Address-Assigment - Alocação de Endereços IP aos assinantes

A configuração dos pools de endereços que serão alocados para os assinantes é feita em [access address-assigment]. Tanto os pools de endereços IPv4 e IPv6 são configurados em [access address-assigment] e o BNG pode alocar os endereços aos assinantes usando os atributos recebidos pelo protocolo RADIUS e também utilizando os pools configurados localmente.

10.1.3.1. Alocação de endereços IPv4

A seguir o detalhamento da entrega dos endereços IPv4 para os assinantes baseado na precedência listada a seguir:

1. Em primeiro lugar o BNG dá preferência pelo endereço IP atribuído ao usuário através do AVP Framed-IP-Address. Caso o RADIUS mande este AVP com um endereço IPv4 este IP será atribuído ao assinante na conexão PPPoE.

2. Em segundo lugar o BNG dá preferência para o atributo Framed-Pool. Caso tenha sido enviado o atributo Framed-Pool com um nome de um pool configurado no BNG este será o pool que o BNG vai usar para alocar IP's para o assinante. No caso do servidor RADIUS enviar os AVP's Framed-IP-Address e Framed-Pool o BNG alocará o IP enviado no AVP Framed-IP-Address visto que ele tem precedência.

Caso o RADIUS envie o AVP Framed-Pool com um nome de pool que não existe configurado no BNG este AVP será descartado e o BNG vai usar o próximo mecanismo para alocar o endereço IP para o usuário.

Importante: Caso o RADIUS envie o AVP Framed-Pool para o usuário com um nome de pool correto que existe configurado no BNG, porém no pool não existe mais endereços IP's livres para serem alocados, o assinante não vai pegar endereço IP e o BNG não vai procurar um próximo pool. O único caso que o BNG vai procurar um próximo pool é quando o pool informado pelo RADIUS está encadeado ou "conectado" com um outro pool em uma cadeia de pools através da configuração de link.

Exemplo:

```
set access address-assignment pool POOL-IP-01 link POOL-IP-02
set access address-assignment pool POOL-IP-01 family inet network 100.64.10.0/24
set access address-assignment pool POOL-IP-01 family inet range RANGE low 100.64.10.1
set access address-assignment pool POOL-IP-01 family inet range RANGE high 100.64.10.254
set access address-assignment pool POOL-IP-02 link POOL-IP-03
set access address-assignment pool POOL-IP-02 family inet network 100.65.10.0/24
set access address-assignment pool POOL-IP-02 family inet range RANGE low 100.65.10.1
set access address-assignment pool POOL-IP-02 family inet range RANGE high 100.65.10.254
set access address-assignment pool POOL-IP-03 family inet network 192.168.10.0/24
set access address-assignment pool POOL-IP-03 family inet range RANGE low 192.168.10.1
set access address-assignment pool POOL-IP-03 family inet range RANGE high 192.168.10.254
```

Neste caso se for enviado pelo RADIUS o AVP Framed-Pool com o nome Framed-Pool = "POOL-IP-01". Se não houver mais endereços IP livres no pool POOL-IP-01 para ser entregue ao assinante o BNG vai tentar alocar endereços IP do pool POOL-IP-02 que é o pool "conectado" com o pool POOL-IP-01. Caso não exista endereços IP livres no POOL-IP-02 o BNG vai procurar endereços IP livres no pool POOL-IP-03, visto que, o pool POOL-IP-02 está "conectado" com o POOL-IP-03.

Com a configuração de pools acima no BNG caso o RADIUS envie um nome de pool que não é o primeiro da cadeia a busca por endereços IP se dará de forma diferente. Exemplo:

Se o RADIUS enviar o AVP Framed-Pool = "POOL-IP-02" o BNG vai tentar primeiramente alocar endereços IP livres do pool POOL-IP-02. Caso o BNG não encontre endereços IP livre neste pool ele vai procurar endereços IP livre no primeiro pool da cadeia de pools (POOL-IP-01) e caso não encontre ai sim ele vai procurar endereços IP livres no pool conectado com o pool POOL-IP-02 que no caso da configuração seria o POOL-IP-03.

O algoritmo completo para alocação dos endereços IP nos pools no BNG está descrito pela Juniper na seguinte URL:

https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-sessions/topics/topic-map/address-assignment-pools-subscriber-management.html

3. Em terceiro lugar o BNG dá preferência para o pool configurado no domain map (caso exista domain map configurado para o usuário). Exemplo:

```
set access domain map none access-profile ACCESS-PROFILE
set access domain map none address-pool POOL-IP-04
```

```
set access address-assignment pool POOL-IP-04 family inet network 192.168.11.0/24
set access address-assignment pool POOL-IP-04 family inet range RANGE low 192.168.11.1
set access address-assignment pool POOL-IP-04 family inet range RANGE high 192.168.11.254
```

O funcionamento de domain map já está detalhado neste documento.

Caso no domain map seja configurado um pool que não exista no BNG o BNG vai descartar esta configuração e vai dar sequência no próximo recurso para a busca do endereço IP que é a busca global.

4. Em quarto lugar e por último caso nenhuma das três formas anteriores tenha sido configurada, o BNG vai procurar endereços IP livre para o usuário no pool que chamaremos de pool DEFAULT. Por padrão o pool DEFAULT é o primeiro pool configurado no BNG em [access address-assignment].

Exemplo:

```
set access address-assignment pool POOL-IP-05 family inet network 192.168.12.0/24
set access address-assignment pool POOL-IP-05 family inet range RANGE low 192.168.12.1
set access address-assignment pool POOL-IP-05 family inet range RANGE high 192.168.12.254
set access address-assignment pool POOL-IP-04 family inet network 192.168.11.0/24
set access address-assignment pool POOL-IP-04 family inet range RANGE low 192.168.11.1
set access address-assignment pool POOL-IP-04 family inet range RANGE high 192.168.11.254
set access address-assignment pool POOL-IP-01 link POOL-IP-02
set access address-assignment pool POOL-IP-01 family inet network 100.64.10.0/24
set access address-assignment pool POOL-IP-01 family inet range RANGE low 100.64.10.1
set access address-assignment pool POOL-IP-01 family inet range RANGE high 100.64.10.254
set access address-assignment pool POOL-IP-02 link POOL-IP-03
set access address-assignment pool POOL-IP-02 family inet network 100.65.10.0/24
set access address-assignment pool POOL-IP-02 family inet range RANGE low 100.65.10.1
set access address-assignment pool POOL-IP-02 family inet range RANGE high 100.65.10.254
set access address-assignment pool POOL-IP-03 family inet network 192.168.10.0/24
set access address-assignment pool POOL-IP-03 family inet range RANGE low 192.168.10.1
set access address-assignment pool POOL-IP-03 family inet range RANGE high 192.168.10.254
```

Neste caso o primeiro pool IPv4 configurado no BNG é o pool POOL-IP-05. Desta forma o BNG vai procurar endereços IP livres neste pool e caso exista vai alocar um endereço IPv4 para o assinante:

```
admin@MX204-LAB-WZTECH> show subscribers
Interface                   IP Address/VLAN ID                  User Name                       LS:RI
demux0.3221225472            200                                                               default:default
pp0.3221225473              192.168.12.1                        wztech3                         default:default
*                           2090::
*                           2804:ee4:4000::/64
pp0.3221225473              2090::                                                              default:default
*                           2804:ee4:4000::/64

admin@MX204-LAB-WZTECH> show subscribers user-name wztech3 extensive
Type: PPPoE
User Name: wztech3
IP Address: 192.168.12.1
IP Netmask: 255.255.255.255
IPv6 Address: 2090::
IPv6 Prefix: 2804:ee4:4000::/64
Domain name server inet6: 2070::1 2070::2
Logical System: default
Routing Instance: default
Interface: pp0.3221225473
Interface type: Dynamic
Underlying Interface: demux0.3221225472
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 1
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 2
Session ID: 2
PFE Flow ID: 30
VLAN Id: 200
Login Time: 2023-09-04 12:21:05 -03
IP Address Pool: POOL-IP-05
IPv6 Address Pool: NOVO-IA_NA
IPv6 Delegated Address Pool: _DAPV6
IPv6 Framed Interface Id: d0f7:b2fd:c2f4:b59d
IPv4 Input Filter Name: 100M-IPV4-IN-pp0.3221225473-in
IPv4 Output Filter Name: 100M-IPV4-OUT-pp0.3221225473-out
IPv6 Input Filter Name: 100M-IPV6-IN-pp0.3221225473-in
IPv6 Output Filter Name: 100M-IPV6-OUT-pp0.3221225473-out
Accounting interval: 0
Dynamic configuration:
  junos-input-filter: 100M-IPV4-IN
```

```
  junos-input-ipv6-filter: 100M-IPV6-IN
  junos-output-filter: 100M-IPV4-OUT
  junos-output-ipv6-filter: 100M-IPV6-OUT
```

Neste processo, caso não existam mais endereços IPv4 livres neste pool configurado o BNG não dará sequência na procura e o assinante não vai pegar IPv4.

Importante: O pool DEFAULT é o primeiro pool configurado enquanto ele não é desativado ou deletado. A partir do momento que o pool DEFAULT é desativado ou deletado da configuração o BNG vai setar como pool DEFAULT o próximo pool ativo existente na configuração.

No exemplo de configuração acima caso o pool POOL-IP-05 seja deletado ou desativado a partir do momento que a configuração for "commitada" no JunOS o JunOS vai definir o POOL-IP-04 como pool DEFAULT. Mesmo que o pool POOL-IP-05 volte a ser ativado ou configurado novamente em primeiro lugar na configuração (antes dos demais pools) o JunOS vai manter o POOL-IP-04 como sendo o pool DEFAULT. Caso aconteça a desativação ou deleção do POOL-IP-04 o BNG vai setar o pool POOL-IP-01 como sendo o DEFAULT e o processo segue sequencialmente desta forma. Caso todos os pool's sejam deletados ou o MX seja reiniciado será setado como DEFAULT o primeiro pool configurado novamente.

Algumas informações importantes na configuração do pool IPv4:

```
set access address-assignment pool POOL-IP-06 family inet network 192.168.60.0/24
```

Neste modelo de configuração serão alocados do IP (192.168.60.1) ao último (192.168.60.255). O IP de rede do pool não é alocado para os usuários. Caso o IP de rede seja definido dentro da configuração de range ele passará a ser entregue para os usuários.

É possível configurar no pool a exclusão de alguns endereços para não serem entregues aos usuários. Exemplo:

```
set access address-assignment pool POOL-IP-06 family inet network 192.168.60.0/24
set access address-assignment pool POOL-IP-06 family inet excluded-address 192.168.12.255
```


Neste caso o endereço 192.168.12.255 não será entregue para o usuário. Apenas será entregue os endereços 192.168.12.1 ao 192.168.12.254. O IP de rede do pool não é entregue aos assinantes e é excluído automaticamente pelo BNG do processo de alocação.

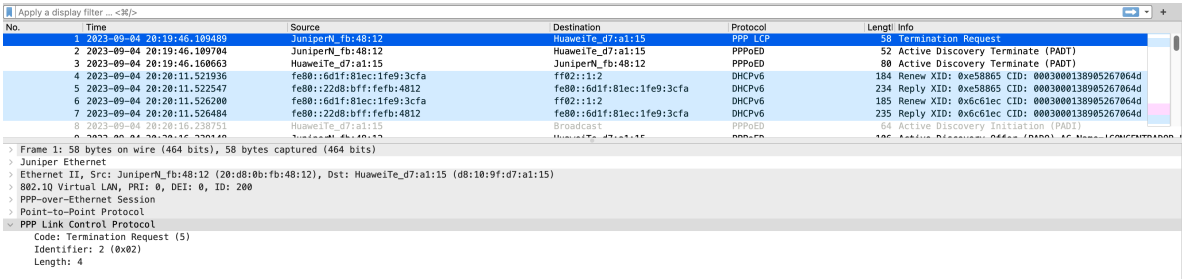
Outra opção é a configuração de range. É possível definir um pool com uma rede (network), porém apenas um range dentro do pool será entregue aos usuários. Exemplo:

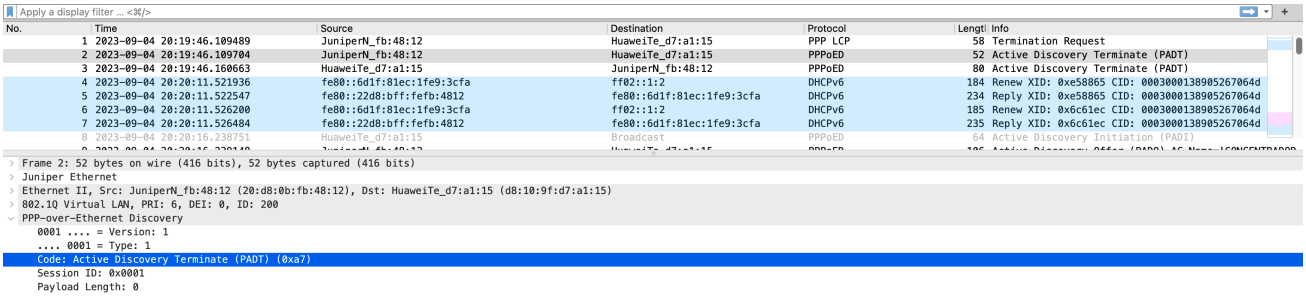
```
set access address-assignment pool POOL-IP-05 family inet network 192.168.12.0/24
set access address-assignment pool POOL-IP-05 family inet range RANGE low 192.168.12.0
set access address-assignment pool POOL-IP-05 family inet range RANGE high 192.168.12.100
```

Neste caso os endereços que serão entregues aos assinantes serão do endereço 192.168.12.0 ao endereço 192.168.12.100.

Caso um pool seja desabilitado ou deletado, todos os usuários que estão usando endereços IP desde pool receberão uma mensagem de PADT no protocolo PPPoE informando a esta ONU que a sessão não está mais disponível e o assinante é desconectado:

Primeiramente o BNG envia um Termination Request no LCP do túnel PPP:





Em seguida o BNG envia um PADT para terminar o túnel PPPoE.

Quando o pool é criado no BNG o JunOS não cria uma rota automaticamente para este pool na tabela de rotas. Caso estas redes precisem ser exportadas para protocolos de roteamento é necessário criar a rota manualmente no JunOS de forma estática ou como rota agregada (aggregate).

Hold down e Active Drain

Existem duas opções que podem ser configuradas no pool que tem funções diferentes quando o pool é utilizado para PPPoE e quando o pool é utilizado pelo protocolo DHCP. O detalhamento do funcionamento para o protocolo DHCP será feito posteriormente.

Importante: Estas configurações de hold-down e active-drain só fazem sentido em pools que estão encadeados com outros pool's. Caso os pools não estejam encadeados através da configuração de link caso seja configurado hold-down ou active-drain em um pool que o BNG usaria para entregar os endereços IP o BNG não fará a procura do próximo pool e o usuário não vai receber endereço nenhum. Esta configuração é recomendada apenas em pools que estejam encadeados com a configuração de "link", sejam eles IPv4, SLAAC, IA_NA ou IA_PD.

No caso do protocolo PPPoE:

Active Drain

```
set access address-assignment pool POOL-IP-03 active-drain
```

Quando é necessário remover um pool do BNG, quando o pool é desativado ou deletado o BNG envia um pacote PPPoE PADT e faz a desconexão de forma abrupta dos assinante conectados que estão utilizando este pool. O comando active-drain em um pool que está sendo utilizado pelo protocolo PPPoE tem o mesmo efeito que desativar ou deletar um determinado pool. O BNG vai enviar o PADT para todos os assinantes que estão utilizando este determinado pool e desconectar os assinantes. Neste caso o active-drain já vai drenar todos os assinantes do pool imediatamente.

Hold Down:

```
set access address-assignment pool POOL-IP-03 hold-down
```

Quando é necessário remover um pool do BNG e é desejado que esta remoção não gere impacto nos assinantes que estão utilizando este determinado pool a funcionalidade de hold-down vai ajudar neste cenário. Quando o hold-down é configurado no pool, todos os assinantes que estão conectados neste pool permanecem conectados e não há uma desconexão ativa destes usuários, porém, este pool não vai aceitar mais nenhuma alocação de endereço IP nova. À medida que os assinantes que estão utilizando este pool forem desconectando e conectando novamente eles vão receber endereços IP de outro pool. Desta forma, o pool vai sendo liberado até não ter mais nenhuma conexão utilizando o mesmo e desta forma não há impacto nos assinantes.

Exemplo de utilização do hold-down no PPPoE:

Vamos supor que a política do provedor é de que um assinante pode ficar no máximo 3 dias conectado sem desconectar a sessão PPPoE. Caso não haja uma desconexão do assinante dentro de 3 dias o BNG vai desconectar o assinante automaticamente. Para que isso aconteça pode ser configurado no BNG o client-session-timeout na access profile do assinante:

```
set access profile ACCESS-PROFILE session-options client-session-timeout 4320 (4320 minutos)
```

Ou pode ser enviado por RADIUS o atributo IETF Session-Timeout = 259200 (259200 segundos ou 4320 minutos)

O provedor possui 3 pools encadeados na configuração com a configuração de link:

```
set access address-assignment pool POOL-IP-01 link POOL-IP-02
set access address-assignment pool POOL-IP-01 family inet network 100.64.10.0/24
set access address-assignment pool POOL-IP-01 family inet range RANGE low 100.64.10.1
set access address-assignment pool POOL-IP-01 family inet range RANGE high 100.64.10.254
set access address-assignment pool POOL-IP-02 link POOL-IP-03
set access address-assignment pool POOL-IP-02 family inet network 100.65.10.0/24
set access address-assignment pool POOL-IP-02 family inet range RANGE low 100.65.10.1
set access address-assignment pool POOL-IP-02 family inet range RANGE high 100.65.10.254
set access address-assignment pool POOL-IP-03 family inet network 192.168.10.0/24
set access address-assignment pool POOL-IP-03 family inet range RANGE low 192.168.10.1
set access address-assignment pool POOL-IP-03 family inet range RANGE high 192.168.10.254
```

A partir do momento que for configurado o active-drain em um dos pool's que estão encadeados como por exemplo o pool POOL-IP-02 os assinantes que estão utilizando o pool POOL-IP-02 vão permanecer até no máximo 3 dias (tempo máximo da sessão) e depois de no máximo 3 dias não haverá mais nenhum assinante fazendo uso deste pool. Desta forma poderá ser removido do BNG sem gerar impacto nos assinantes:

```
set access address-assignment pool POOL-IP-01 link POOL-IP-02
set access address-assignment pool POOL-IP-01 family inet network 100.64.10.0/24
set access address-assignment pool POOL-IP-01 family inet range RANGE low 100.64.10.1
set access address-assignment pool POOL-IP-01 family inet range RANGE high 100.64.10.254
set access address-assignment pool POOL-IP-02 link POOL-IP-03
set access address-assignment pool POOL-IP-02 active-drain
set access address-assignment pool POOL-IP-02 family inet network 100.65.10.0/24
set access address-assignment pool POOL-IP-02 family inet range RANGE low 100.65.10.1
set access address-assignment pool POOL-IP-02 family inet range RANGE high 100.65.10.254
set access address-assignment pool POOL-IP-03 family inet network 192.168.10.0/24
set access address-assignment pool POOL-IP-03 family inet range RANGE low 192.168.10.1
set access address-assignment pool POOL-IP-03 family inet range RANGE high 192.168.10.254
```

Neste caso será mostrado no comando que mostra as estatísticas do pool que ele se encontra no estado de drain e desta forma não será mais utilizado para alocação de IPs. O comando abaixo mostra as estatísticas da utilização do pool. Caso ele esteja encadeado com outros pools será mostrado a estatística em conjunta com todos os pools que estão encadeados.

```
admin@MX204-LAB-WZTECH> show network-access aaa statistics address-assignment pool POOL-IP-01
Address assignment statistics
  Pool Name: POOL-IP-01
    Link Name: POOL-IP-02
    Out of Memory: 0
    Out of Addresses: 0
    Address total: 254
    Addresses in use: 1
    Address Usage (percent): 0
    Pool drain configured: no
  Pool Name: POOL-IP-02
    Link Name: POOL-IP-03
    Out of Memory: 0
    Out of Addresses: 0
    Address total: 254
    Addresses in use: 0
    Address Usage (percent): 0
    Pool drain configured: yes
  Pool Name: POOL-IP-03
    Out of Memory: 0
    Out of Addresses: 0
    Address total: 254
    Addresses in use: 1
    Address Usage (percent): 0
    Pool drain configured: no
  Pool Name: (all pools in chain)
```

```
    Out of Memory: 0
    Out of Addresses: 0
    Address total: 762
    Addresses in use: 2
    Address Usage (percent): 0
    Pool drain configured: no
```

Conforme mostrado acima no conjunto de pools encadeados o POOL-IP-03 está em "drain" e também é mostrado as estatísticas do uso dos pools individuais e também de forma geral com a soma de todos os pools encadeados: quantidade de IP's, endereços IP em uso, percentual de utilização dos pools, etc...

Outro comando que mostra todos os assinantes que estão fazendo uso do pool com o seu devido MAC é o comando a seguir:

```
admin@MX204-LAB-WZTECH> show network-access address-assignment pool POOL-IP-06
IP address/prefix       Hardware address     Host/User      Type
192.168.60.1           D8:10:9F:D7:A1:15    wztech2        pppoe
192.168.60.2           38:90:52:67:06:4D    wztech3        pppoe
```

É possível configurar o BNG para gerar eventos de TRAP SNMP quando a utilização de algum pool IPv4 chegar em um determinado threshold e gerar outro TRAP SNMP quando for normalizado:

```
set access address-assignment high-utilization 85
set access address-assignment abated-utilization 75
```

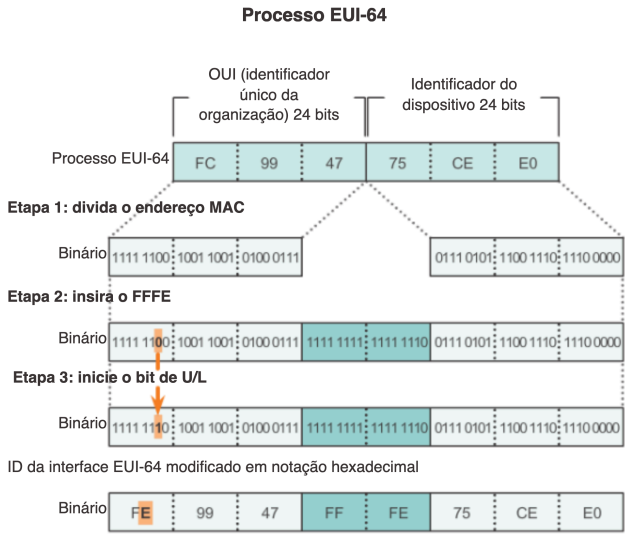
Neste caso quando a utilização do pool chegar a 85% será gerado um trap SNMP e quando a utilização voltar para um valor abaixo de 75% será gerado um novo trap SNMP informando da normalização. Caso a utilização do pool chegue em 100% independente desta configuração será gerado um evento de syslog:

```
Sep  4 16:02:31  MX204-LAB-WZTECH authd[11673]: pool POOL-IP-04 is out of addresses
```

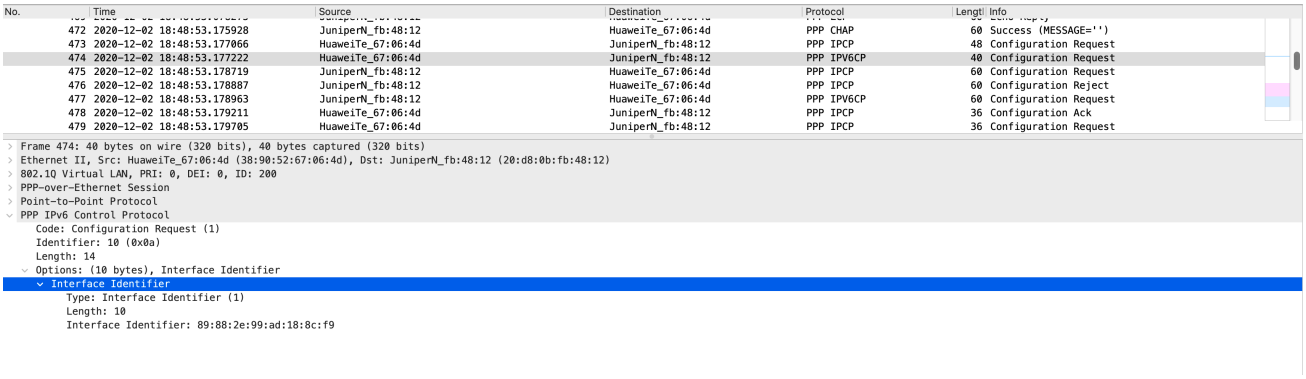
10.1.3.2. IPv6 - SLAAC - Funcionamento e Alocação de Prefixos

Na conexão PPPoE, a ONU pode alocar o prefixo IPv6 de WAN de algumas formas diferentes. Uma destas formas é através do mecanismo SLAAC (Stateless Auto Address Configuration) que a Juniper também chama de NDRA (Neighbor Discovery Router Advertisement).

O mecanismo SLAAC na conexão PPPoE segue a mesma lógica do mecanismo SLAAC utilizado em redes locais para entrega do endereço IPv6 de forma stateless. O BNG faz o anúncio através de mensagens ICMPv6 Router Advertisement do prefixo de rede (primeiros 64 bits do endereço IPv6) e o host usa o mecanismo chamado EUI-64 para calcular os últimos 64 bits para compor o endereço IPv6 de 128 bits. O mecanismo IEEE EUI-64 usa um endereço MAC de 48 bits (físico ou virtual) como base para gerar os 64 bits finais do prefixo:



Estes últimos 64 bits que serão utilizados pela ONU para o IP de WAN são informados no protocolo PPPoE na negociação do protocolo no IPV6CP (IPv6 Control Protocol) como o Interface Identifier:



Neste caso, na ONU usada nos testes gera um Interface Identifier virtual a cada conexão e não utiliza o MAC Address da interface WAN. Este comportamento depende da implementação da ONU.

O Interface Identifier da ONU negociado na conexão PPPoE pode ser encontrado na sessão do assinante no campo IPv6 Framed Interface Id:

```
admin@MX204-LAB-WZTECH> show subscribers user-name wztech3 extensive
Type: PPPoE
User Name: wztech3
IP Address: 192.168.60.43
IP Netmask: 255.255.255.255
IPv6 Prefix: 2804:ee4:4000:24::/64
Domain name server inet6: 2070::1 2070::2
IPv6 User Prefix: 2905:ee4:8000::/64
Logical System: default
Routing Instance: default
Interface: pp0.3221225614
Interface type: Dynamic
Underlying Interface: demux0.3221225597
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 1
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 165
Session ID: 165
PFE Flow ID: 202
VLAN Id: 200
Login Time: 2023-09-09 14:28:45 -03
IP Address Pool: POOL-IP-06
IPv6 Address Pool: POOL-V6-NDRA-2
IPv6 Delegated Address Pool: _DAPV6
IPv6 Framed Interface Id: 8988:2e99:ad18:8cf9
IPv4 Input Filter Name: 100M-IPV4-IN-pp0.3221225614-in
IPv4 Output Filter Name: 100M-IPV4-OUT-pp0.3221225614-out
IPv6 Input Filter Name: 100M-IPV6-IN-pp0.3221225614-in
IPv6 Output Filter Name: 100M-IPV6-OUT-pp0.3221225614-out
Accounting interval: 0
Dynamic configuration:
  junos-input-filter: 100M-IPV4-IN
  junos-input-ipv6-filter: 100M-IPV6-IN
  junos-ipv6-ndra-prefix: 2905:ee4:8000::/64
  junos-output-filter: 100M-IPV4-OUT
  junos-output-ipv6-filter: 100M-IPV6-OUT
```

E pode ser obtido no RADIUS Accounting através do atributo Framed-Interface-Id:

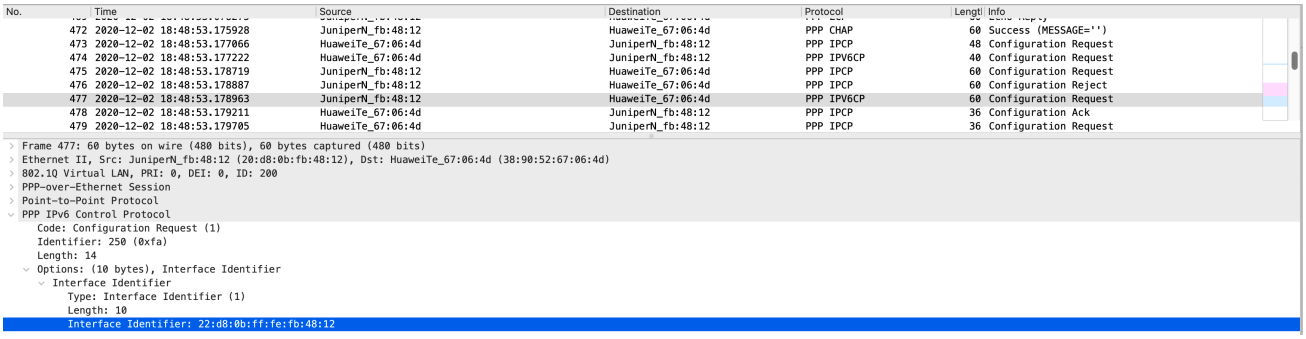
(10) Received Accounting-Request Id 3 from 192.168.1.248:54435 to 192.168.1.236:1813 length 595
(10) User-Name = "wztech3"
(10) Acct-Status-Type = Start
(10) Acct-Session-Id = "165"
(10) Event-Timestamp = "Sep 9 2023 13:28:46 EDT"
(10) Acct-Delay-Time = 0
(10) Service-Type = Framed-User
(10) Framed-Protocol = PPP

(10) Filter-Id = "IPV4-ingress:100M-IPV4-IN-pp0.3221225614-in"
(10) Filter-Id = "IPV4-egress:100M-IPV4-OUT-pp0.3221225614-out"
(10) Filter-Id = "IPV6-ingress:100M-IPV6-IN-pp0.3221225614-in"
(10) Filter-Id = "IPV6-egress:100M-IPV6-OUT-pp0.3221225614-out"
(10) Attr-26.4874.177 = 0x506f72742073706565643a2032303030303030306b
(10) Framed-IPv6-Prefix = 2905:ee4:8000::/64
(10) Framed-IPv6-Pool = "POOL-V6-NDRA-2"
(10) Framed-Interface-Id = 8988:2e99:ad18:8cf9
(10) Acct-Authentic = RADIUS
(10) Calling-Station-Id = "38-90-52-67-06-4d:200"
(10) ERX-Dhcp-Mac-Addr = "3890.5267.064d"
(10) ERX-Egress-Policy-Name = "100M-IPV4-OUT"
(10) Framed-IP-Address = 192.168.60.43
(10) Framed-IP-Netmask = 255.255.255.255
(10) ERX-Ingress-Policy-Name = "100M-IPV4-IN"
(10) NAS-Identifier = "MX204-LAB-WZTECH"
(10) NAS-Port = 0
(10) NAS-Port-Id = "ae0.demux0.3221225597:200"
(10) NAS-Port-Type = Ethernet
(10) ERX-IPv6-Ingress-Policy-Name = "100M-IPV6-IN"
(10) ERX-IPv6-Egress-Policy-Name = "100M-IPV6-OUT"
(10) ERX-Virtual-Router-Name = "default:default"
(10) ERX-Pppoe-Description = "pppoe 38:90:52:67:06:4d"
(10) Attr-26.4874.210 = 0x00000004
(10) NAS-IP-Address = 192.168.1.248

Desta forma, para pingar a ONU basta pingar o prefixo (primeiros 64 bits) + o Interface Id (últimos 64 bits):

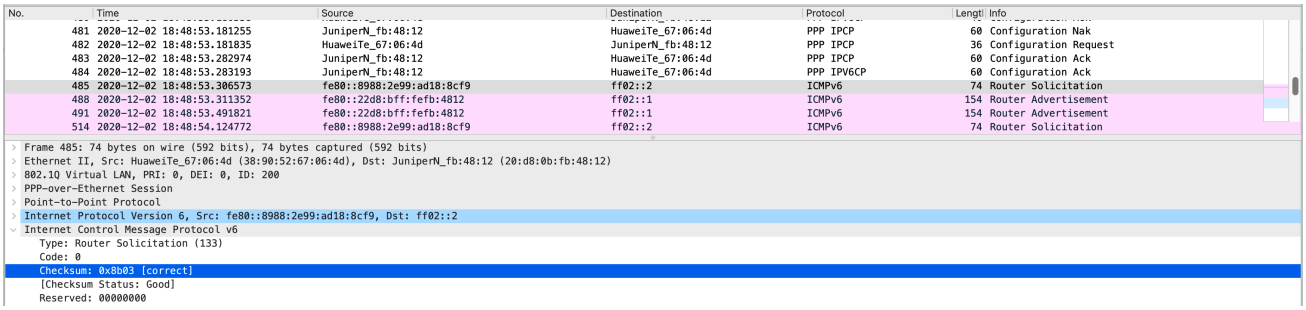
```
admin@MX204-LAB-WZTECH> ping 2905:ee4:8000::8988:2e99:ad18:8cf9
PING6(56=40+8+8 bytes) 2090::1 --> 2905:ee4:8000:0:8988:2e99:ad18:8cf9
16 bytes from 2905:ee4:8000:0:8988:2e99:ad18:8cf9, icmp_seq=0 hlim=64 time=2.560 ms
16 bytes from 2905:ee4:8000:0:8988:2e99:ad18:8cf9, icmp_seq=1 hlim=64 time=2.128 ms
16 bytes from 2905:ee4:8000:0:8988:2e99:ad18:8cf9, icmp_seq=2 hlim=64 time=2.145 ms
16 bytes from 2905:ee4:8000:0:8988:2e99:ad18:8cf9, icmp_seq=3 hlim=64 time=2.079 ms
16 bytes from 2905:ee4:8000:0:8988:2e99:ad18:8cf9, icmp_seq=4 hlim=64 time=2.092 ms
--- 2905:ee4:8000::8988:2e99:ad18:8cf9 ping6 statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/std-dev = 2.079/2.201/2.560/0.181 ms
```

O BNG informou à ONU o Interface Identifier sendo o EUI-64 do MAC Address da interface física onde a demux0 foi instalada.




```
admin@MX204-LAB-WZTECH> show interfaces ae0 extensive | match hardware
  Current address: 20:d8:0b:fb:48:12, Hardware address: 20:d8:0b:fb:48:12
```

Após a negociação das mensagens do protocolo PPP a ONU envia uma mensagem de ICMPv6 Router Solicit para o BNG dentro do túnel PPPoE:

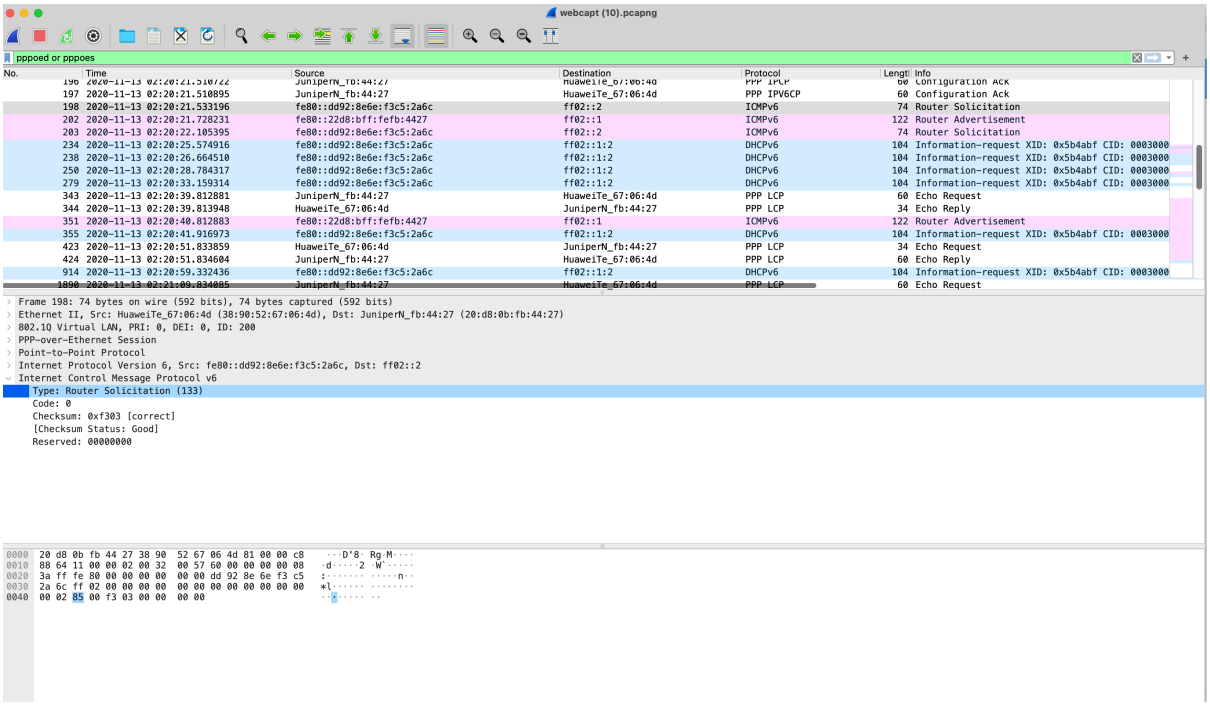


Nesta mensagem de ICMPv6 Router Solicit (Type 133) o endereço IPv6 de origem é o endereço de link-local onde é usado o prefixo fe80:: + Interface Identifier (64 bits finais gerados dinamicamente pela ONU) e o endereço IPv6 de destino é o endereço ff02::2. Este endereço de destino é um endereço de multicast do IPv6 onde todos os roteadores do enlance local respondem com o Router Advertisement.

Importante: Mesmo que o BNG não responda às mensagens Router Solicit (caso haja filtro no BNG para não receber estas mensagens), de todas as formas, o BNG envia de forma espontânea um primeiro Router Advertisement assim que o assinante conecta e fica enviando de forma espontânea mensagens de Router Advertisement com os atributos necessários. Desta forma, geralmente, não há nenhum impacto em filtrar as mensagens de Router Solicit no BNG e deixar que apenas o BNG envie mensagens de Router Advertisement espontaneamente. Neste caso este filtro pode ser feito na firewall filter que será aplicada na lo0 para proteção do Control Plane do BNG (Routing Engine) ou pode ser feito também na firewall filter do assinante. Em qualquer um dos dois modelos os pacotes de Router Solicit serão descartados na PFE (Data Plane) e não chegarão na Routing Engine. Como os pacotes estão sendo bloqueados na PFE não será mais possível capturar estes pacotes com o comando "monitor traffic" pois este comando captura os pacotes que estão chegando na Routing Engine (Controle Plane).

A seguir exemplo de configuração de um termo de bloqueio de pacotes ICMPv6 Router Solicit das ONU's:

```
.....
set firewall family inet6 filter PROTEGE-RE term BLOQUEIA-RS from next-header icmp6
set firewall family inet6 filter PROTEGE-RE term BLOQUEIA-RS from icmp-type router-solicit
set firewall family inet6 filter PROTEGE-RE term BLOQUEIA-RS then discard
.....
```



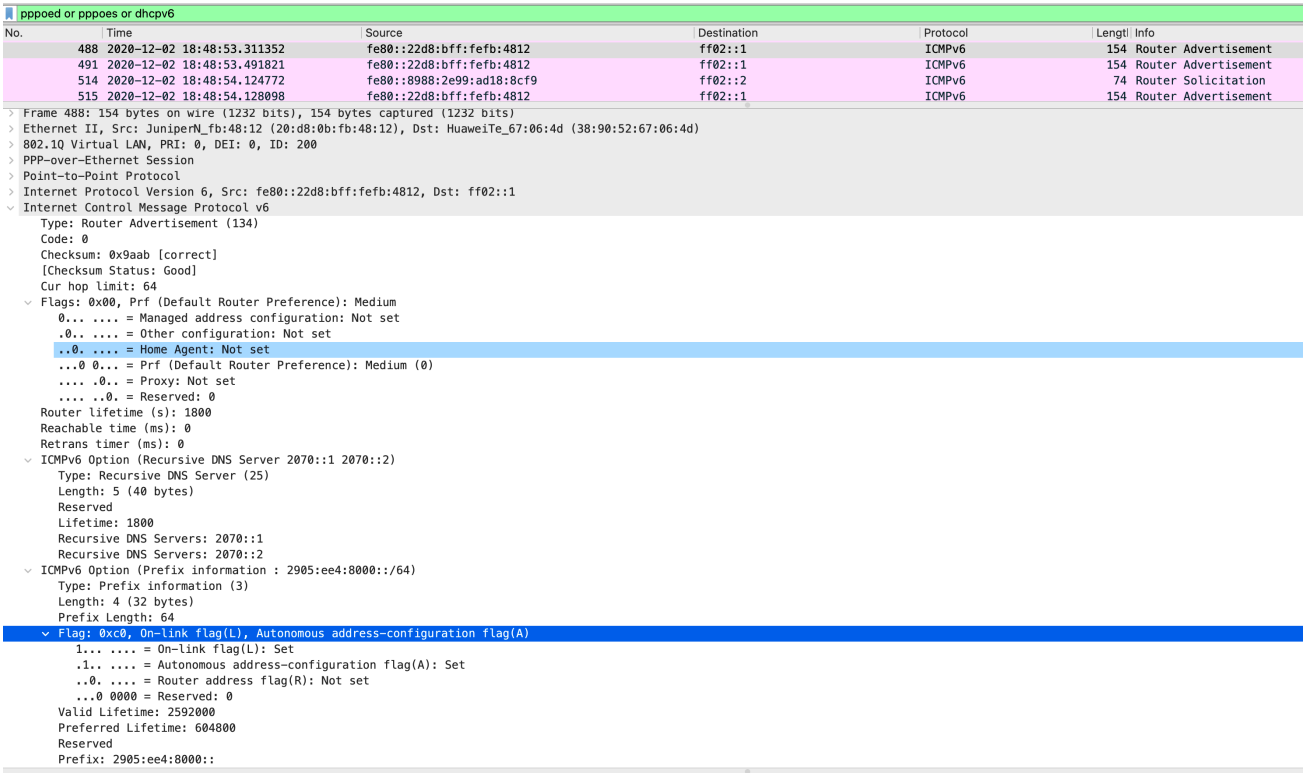
Nesta captura feita na ONU é possível ver que as mensagens de Router Solicit estão sendo bloqueadas pois não estão sendo respondidas e o BNG continua enviando Router Advertisement de forma espontânea.

Por outro lá há a possibilidade de configurar o BNG para não mais enviar mensagens de RA de forma espontânea. Desta forma o BNG apenas vai apenas responder a requisições de Router Solicit. Caso a ONU neste cenário não faça novos Router Solicit periodicamente para renovar os atributos enviados no RA o prefixo IPv6 na ONU vai parar de funcionar:

```
set system services subscriber-management overrides no-unsolicited-ra
```

Importante: Este comando desabilita globalmente o envio de RA de forma espontânea no BNG e só deve ser utilizada em algum caso específico avaliado junto com a Juniper e o fabricante da ONU em casos específicos.

O BNG envia o ICMPv6 Router Advertisement (type 134) para a ONU:



Na mensagem de Router Advertisement é comum ser enviado o prefixo, os DNS's, juntamente com as flag's da mensagem de Router Advertisement e também as flag's do prefixo.

As flag's M (Managed Address Configuration) e O (Other configuration) da mensagem Router Advertisement por default no BNG são enviadas com valor 0.

M (Managed Address Configuration) informa à ONU onde ela deve obter o prefixo IPv6 sendo: 0 do próprio Router Advertisement e 1 através de DHCPv6.

O (Other configuration) informa à ONU onde ela deve obter as demais configurações como DNS e domínio de DNS: 0 do próprio Router Advertisement e 1 através de DHCPv6.

Resumo do resultado da combinação destas flags na mensagem de Router Advertisement:

M = 0, O = 0: Tudo Stateless - ONU obtém prefixo IPv6 e demais configurações como DNS e sufixo de DNS através das informações enviadas no RA apenas. Não deve ser utilizado DHCPv6 neste caso - Este modelo também é chamado de Stateless Autoconfig e é o default do BNG.

M = 0, O = 1 : ONU obtém prefixo IPv6 da mensagem de RA e as demais configurações de DNS e sufixo de DNS devem ser obtidas pelo protocolo DHCPv6. Este modelo é chamado de DHCPv6 stateless

M = 1, O = 0 : ONU obtém tanto o prefixo IPv6 quanto as demais configurações de DNS e sufixo de domínio através do protocolo DHCPv6. Este modelo é chamado de DHCPv6 stateful

M = 1, O = 1 : ONU obtém tanto o prefixo IPv6 quanto as demais configurações de DNS e sufixo de domínio através do protocolo DHCPv6. Como a flag M está setada a ONU vai obrigatoriamente ter que fazer a chamada no servidor DHCPv6 para obter o prefixo IPv6 e DNS. A flag O neste caso fica redundante já que o servidor DHCPv6 retorna todas as informações.

Importante: A implementação destas flags na ONU e o seu funcionamento podem variar de fabricante para fabricante e depende do código de firmware implementado.

Diferentemente do protocolo IPv4 onde o default gateway é enviado no protocolo DHCP, no protocolo IPv6 não existe até este momento suporte oficial para envio do default gateway através do protocolo DHCPv6. No protocolo IPv6 o default gateway é instalado nos clientes através também das mensagens de Router Advertisement. Por default a flag R do prefixo (Router Address Flag) não é setada (fica com valor 0) nas mensagens de Router Advertisement. Desta forma o host que está recebendo as mensagens de Router Advertisement vai instalar como default gateway o endereço IPv6 de origem do pacote de Router Advertisement:

WAN Information	
MAC Address:	38:90:52:67:06:4D
VLAN:	200
Policy:	Use the specified value
Priority:	0
Enable NPTv6:	Disable
DNS Servers:	2070::1,2070::2
Prefix:	2804:ee4:4000:24::/64
Prefix Acquisition Mode:	PrefixDelegation
Prefix Preferred Lifetime:	86400 s
Prefix Valid Lifetime:	86400 s
Remaining Lifetime of the Prefix:	82335 s
IP Address:	2905:ee4:8000:0:8988:2e99:ad18:8cf9
Acquisition Mode of the IP Address:	AutoConfigured
Status of the IP Address:	Preferred
Preferred Lifetime of the IP Address:	604800 s
Valid Lifetime of the IP Address:	2592000 s
Remain Lifetime of the IP Address:	2591548 s
Default Gateway:	fe80::22d8:bff:fefb:4812
DS-Lite AFTR Name:	
Peer IP Address of the DS-Lite Channel:	
Online Duration (dd:hh:mm:ss):	00:01:07:50

Neste caso a ONU instalou como default gateway o endereço fe80::22d8:bff:fefb:4812 que é o endereço IPv6 de origem enviado na mensagem de RA do BNG para a ONU. Mesmo que o BNG esteja enviando um prefixo global IPv6 na mensagem de RA (2905:ee4:8000::/64) a ONU vai instalar o default gateway com o endereço de

link local do BNG. Este é o comportamento padrão do protocolo IPv6 e pode ser mudado alterando a flag Router Address Flag. Em geral não é recomendado mudar estas flags no BNG.

Timers do Router Advertisement:

Após o envio da primeira mensagem de RA do BNG para a ONU o BNG vai ficar enviando periodicamente mensagens de RA na conexão PPPoE. Estas mensagens usam alguns parâmetros para definir a periodicidade que serão enviadas:

max-advertisement-interval: Tempo máximo que o BNG vai considerar para enviar a próxima mensagem de RA para a ONU depois da última mensagem enviada. Por default na Juniper este tempo é de 10 minutos (600 segundos).

Este valor pode ser alterado na Subscriber Profile. O valor máximo permitido é de 1800 segundos.

```
set dynamic-profiles SUBSCRIBER-PROFILE protocols router-advertisement interface "$junos-interface-name" max-advertisement-interval 1000
```

min-advertisement-interval: Tempo mínimo que o BNG vai considerar para enviar a próxima mensagem de RA para a ONU depois da última mensagem enviada. Por default na Juniper este tempo é 1/3 (um terço) do valor configurado como max-advertisement-interval. Como o max-advertisement-interval por default é 10 minutos este valor fica em 200 segundos (um terço de 600 segundos).

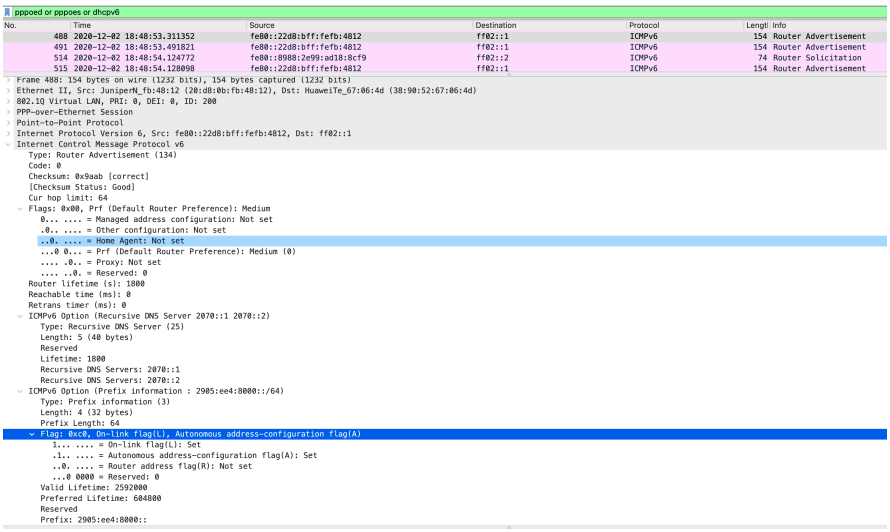
Este valor pode ser alterado na Subscriber Profile. O valor máximo permitido em segundos para ser configurado é 3/4 (três quartos) o valor configurado em max-advertisement-interval.

```
set dynamic-profiles SUBSCRIBER-PROFILE protocols router-advertisement interface "$junos-interface-name" min-advertisement-interval 750
```

Com estes dois parâmetros o BNG calcula internamente um momento entre o tempo mínimo e o tempo máximo e envia a mensagem de RA para a ONU saber que o BNG está ativo e que o prefixo ainda é válido. Não há um tempo exato para o envio do RA. O BNG garante que vai enviar a mensagem entre o tempo mínimo e máximo considerando o melhor momento internamente no equipamento. Por default a mensagem será enviada entre 200 e 600 segundos após o último RA.

Importante: Diferentemente dos LCP Updates do protocolo PPP onde o MX envia estes updates diretamente pelo data plane (PFE), os Router Advertisement enviados pelo MX são gerados pela Routing-Engine e eles podem ser vistos na captura de tráfego na Routing Engine com o comando "monitor traffic interface" tanto na interface física quanto na interface pp0 do assinante. Desta forma é importante tomar cuidado em mudar estes valores pois caso seja configurado tempos muito curtos para o envio do RA pode haver sobrecarga na Routing Engine.

Outro timer enviado no RA foi o Router Lifetime:

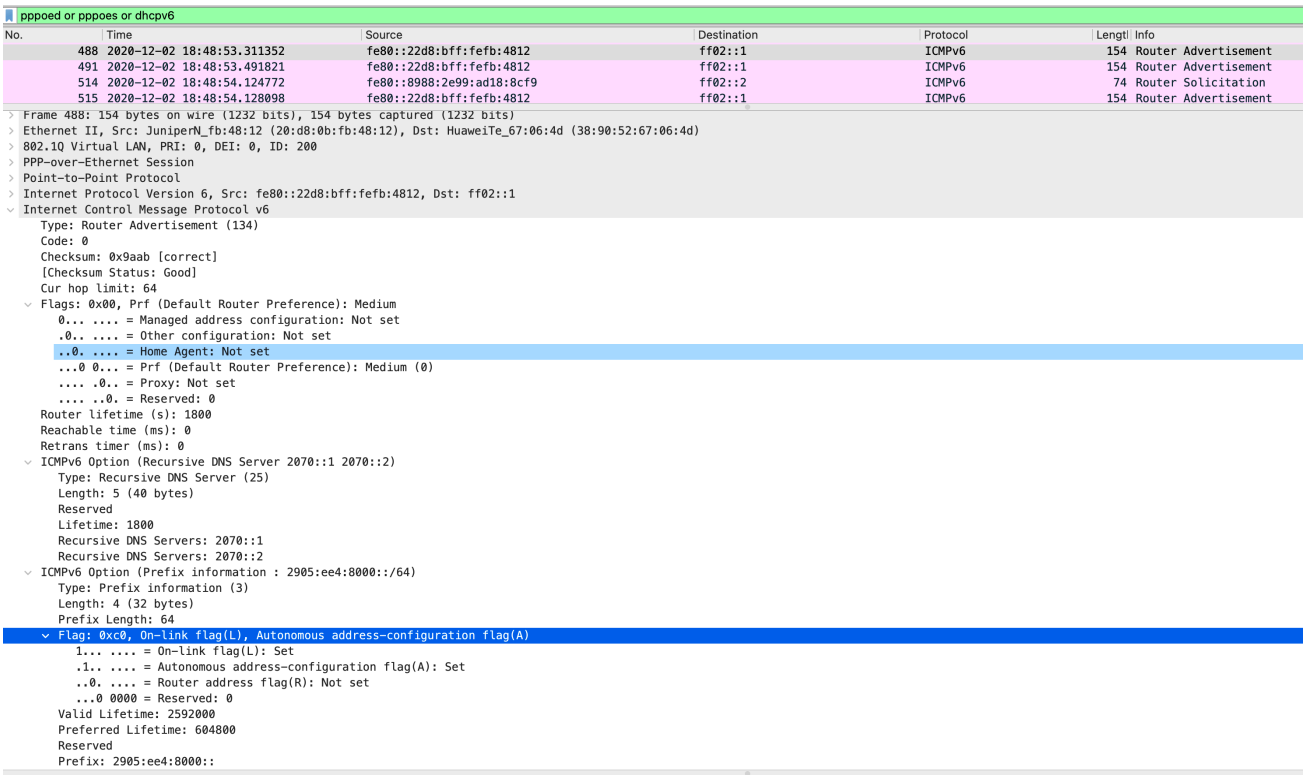


O Router lifetime em segundos é tempo máximo que a ONU pode ter esse roteador (BNG) que está gerando o RA como default gateway. Na Juniper este tempo se refere ao parâmetro default-lifetime que por default é 3 vezes o valor do parâmetro max-advertisement-interval. Como o tempo default do max-advertisement-interval é 600 segundos por default o default-lifetime é 1800 segundos. Ele pode ser alterado na Subscriber Profile e o tempo máximo suportado é de 9000 segundos (duas horas e meia):

```
set dynamic-profiles SUBSCRIBER-PROFILE protocols router-advertisement interface "$junos-interface-name" default-lifetime 9000
```

Se for configurado o default-lifetime com um valor igual ou maior que o max-advertisement-interval o BNG envia no RA o Router lifetime com o valor configurado. Se for configurado um valor menor que o max-advertisement-interval o BNG vai enviar o valor do Router lifetime sendo três vezes o valor do max-advertisement-interval. Isto porque não faz sentido o default gateway não ser mais válido na ONU antes de ter um próximo RA para atualizar esta entrada como válida. O ideal é manter o Router lifetime pelo menos 3 vezes o valor máximo do RA pois caso alguma mensagem de RA seja perdida a ONU ainda consegue atualizar as informações locais não desativando o BNG como gateway IPv6.

No RA também são enviados os DNS's IPv6 configurados para SLAAC em Recursive DNS Server (RDNSS):

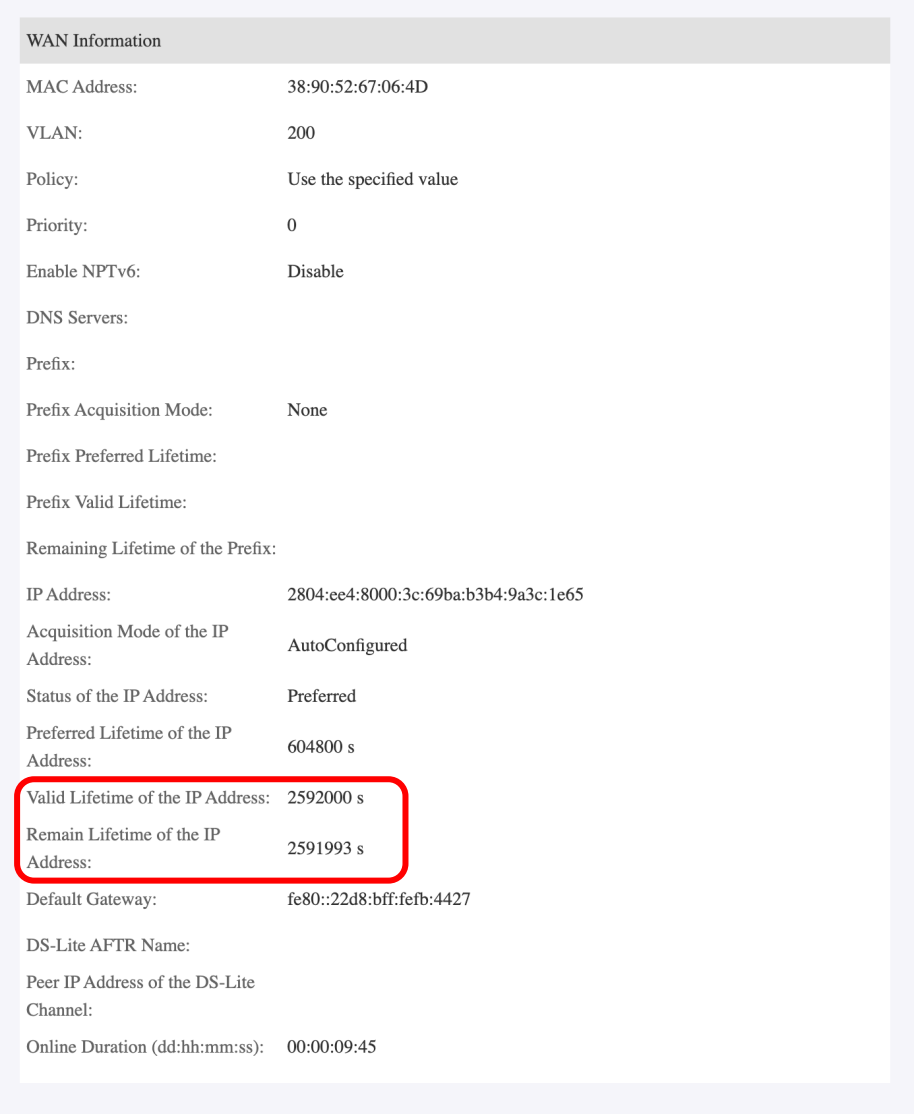


O detalhamento do funcionamento dos DNS's IPv6 no SLAAC já foi detalhado neste documento.

No RA é enviado o prefixo do assinante (geralmente /64) em Prefix Information e alguns timers do prefixo.

Valid Lifetime e Preferred Lifetime: Por default o BNG envia o Valid Lifetime com o valor de 2592000 segundos e o Preferred Lifetime com o valor de 604800 segundos.

Os dois são timers padronizados no protocolo IPv6 e definem por quanto tempo a ONU pode ficar com este prefixo ativo localmente caso não seja recebido um novo RA. Na ONU utilizada nos testes é considerado sempre o valor de Valid Lifetime para renovação do prefixo e sempre que chega um novo RA este tempo é renovado:



WAN Information	
MAC Address:	38:90:52:67:06:4D
VLAN:	200
Policy:	Use the specified value
Priority:	0
Enable NPTv6:	Disable
DNS Servers:	
Prefix:	
Prefix Acquisition Mode:	None
Prefix Preferred Lifetime:	
Prefix Valid Lifetime:	
Remaining Lifetime of the Prefix:	
IP Address:	2804:ee4:8000:3c:69ba:b3b4:9a3c:1e65
Acquisition Mode of the IP Address:	AutoConfigured
Status of the IP Address:	Preferred
Preferred Lifetime of the IP Address:	604800 s
Valid Lifetime of the IP Address:	2592000 s
Remain Lifetime of the IP Address:	2591993 s
Default Gateway:	fe80::22d8:bff:fefb:4427
DS-Lite AFTR Name:	
Peer IP Address of the DS-Lite Channel:	
Online Duration (dd:hh:mm:ss):	00:00:09:45

Nesse caso o último RA recebido foi há 7 segundos visto que o Remain Lifetime of the IP Address é 7 segundos menor que o valor total do Valid LifeTime. Em geral, não há necessidade de mudança destes valores no BNG.

As estatísticas dos RA's e RS's enviados e recebidos no BNG podem ser obtidos através do comando "show ipv6 router-advertisement"

```
admin@MX204-LAB-WZTECH> show ipv6 router-advertisement
Interface: pp0.3221225598
  Advertisements sent: 60, last sent 0:00:11 ago
  Solicits received: 2, last received 5:40:39 ago
  Advertisements received: 0
Interface: pp0.3221225600
  Advertisements sent: 63, last sent 0:03:42 ago
  Solicits received: 2, last received 5:40:39 ago
  Advertisements received: 0
Interface: pp0.3221225614
  Advertisements sent: 36, last sent 0:01:42 ago
  Solicits received: 2, last received 2:57:06 ago
  Advertisements received: 0
```

```
admin@MX204-LAB-WZTECH> show ipv6 router-advertisement interface pp0.3221225598
Interface: pp0.3221225598
  Advertisements sent: 60, last sent 0:00:27 ago
  Solicits received: 2, last received 5:40:55 ago
  Advertisements received: 0
```

Como os Router Advertisement e Router Solicit são todos recebidos dentro do protocolo PPPoE. Caso a interface pp0 do usuário não exista mais em virtude de desconexão todas estas estatísticas de router-advertisement e router solicit para esta interface serão perdidas.

A seguir o detalhamento da entrega dos endereços IPv6 SLAAC para o assinante quando o BNG está configurado com NDRA:

1. Em primeiro lugar o BNG dá preferência pelo prefixo IPv6 de NDRA recebido através do AVP Framed-IPv6-Prefix no protocolo RADIUS. Caso o RADIUS mande este AVP com um prefixo IPv6 ele será atribuído ao assinante na conexão PPPoE.

2. Em segundo lugar o BNG dá preferência para o atributo Framed-IPv6-Pool. Caso tenha sido enviado o atributo Framed-IPv6-Pool com um nome de pool configurado no BNG este será o pool que o BNG vai usar para alocar prefixos para o usuário. Caso o RADIUS envie os AVP's Framed-IPv6-Prefix e Framed-IPv6-Pool o BNG alocará o prefixo enviado no AVP Framed-IPv6-Prefix visto que ele tem precedência.

Caso o RADIUS envie o AVP Framed-IPv6-Pool com um nome de pool que não existe configurado no BNG este AVP será descartado e o BNG vai alocar um prefixo do pool configurado para NDRA em [access address-assignment neighbor-discovery-router-advertisement] caso exista pool configurado.

Importante: Caso o RADIUS envie o AVP Framed-IPv6-Pool para o assinante com um nome de pool correto que existe no BNG, porém no pool não existem mais prefixos livres para serem alocados, o assinante não vai pegar endereço IPv6 e o BNG não vai procurar um próximo pool. O único caso que o BNG vai procurar um próximo pool é quando o pool informado pelo RADIUS está encadeado ou "conectado" com um outro pool em uma cadeia de pools através da configuração de link. Exemplo:

```
set access address-assignment pool POOL-V6-NDRA-1 link POOL-V6-NDRA-2
set access address-assignment pool POOL-V6-NDRA-1 family inet6 prefix 2904:0ee4:8000::/64
set access address-assignment pool POOL-V6-NDRA-1 family inet6 range RANGE-PARA-NDRA prefix-length 64
set access address-assignment pool POOL-V6-NDRA-2 link POOL-V6-NDRA-3
set access address-assignment pool POOL-V6-NDRA-2 family inet6 prefix 2905:0ee4:8000::/64
set access address-assignment pool POOL-V6-NDRA-2 family inet6 range RANGE-PARA-NDRA prefix-length 64
set access address-assignment pool POOL-V6-NDRA-3 family inet6 prefix 2906:0ee4:8000::/64
set access address-assignment pool POOL-V6-NDRA-3 family inet6 range RANGE-PARA-NDRA prefix-length 64
```

Neste caso se for enviado pelo RADIUS o AVP Framed-IPv6-Pool com o nome Framed-IPv6-Pool = "POOL-V6-NDRA-1", se não houver mais prefixos IPv6 livres neste pool para serem entregues ao assinante o BNG vai tentar alocar endereços IP do pool POOL-V6-NDRA-2 que é o pool conectado com o pool POOL-V6-NDRA-1. Caso não existam prefixos livres no POOL-V6-NDRA-2 o BNG vai procurar prefixos livres no pool POOL-V6-NDRA-3 visto que o pool POOL-V6-NDRA-2 está conectado com o POOL-V6-NDRA-3.

Com a configuração de pools acima no BNG caso o RADIUS envie um nome de pool que não é o primeiro da cadeia a busca por endereços IP se dará de forma diferente e o comportamento é o mesmo já detalhado para pool IPv4 neste cenário.

3. Em terceiro lugar e por último caso nenhuma das duas formas anteriores sejam enviadas pelo RADIUS o BNG vai procurar prefixos livres para o assinante no pool configurado em [access address-assignment neighbor-discovery-router-advertisement] caso o NDRA esteja configurado no BNG.

O prefixo SLAAC do usuário aparece na sessão como "IPv6 User Prefix":

```
admin@MX204-LAB-WZTECH> show subscribers user-name wztech3 extensive
Type: PPPoE
User Name: wztech3
IP Address: 192.168.60.43
IP Netmask: 255.255.255.255
IPv6 Prefix: 2804:ee4:4000:24::/64
Domain name server inet6: 2070::1 2070::2
IPv6 User Prefix: 2905:ee4:8000::/64
Logical System: default
Routing Instance: default
Interface: pp0.3221225614
Interface type: Dynamic
```

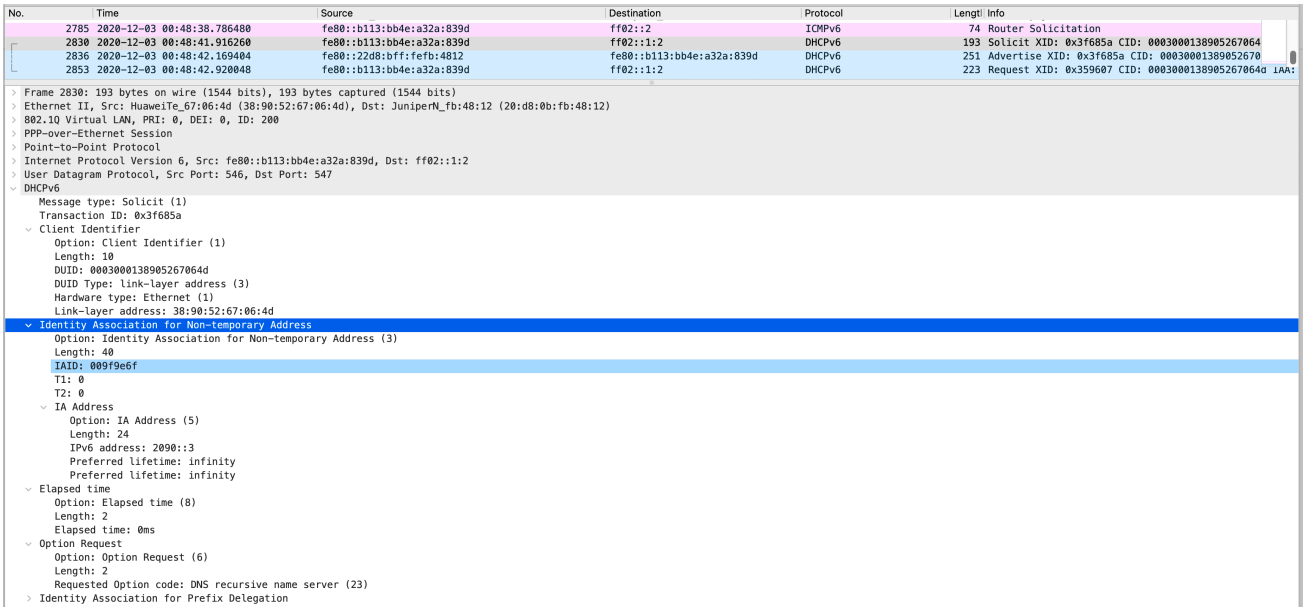
```
Underlying Interface: demux0.3221225597
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 1
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 165
Session ID: 165
PFE Flow ID: 202
VLAN Id: 200
Login Time: 2023-09-09 14:28:45 -03
IP Address Pool: POOL-IP-06
IPv6 Address Pool: POOL-V6-NDRA-2
IPv6 Delegated Address Pool: _DAPV6
IPv6 Framed Interface Id: 8988:2e99:ad18:8cf9
IPv4 Input Filter Name: 100M-IPV4-IN-pp0.3221225614-in
IPv4 Output Filter Name: 100M-IPV4-OUT-pp0.3221225614-out
IPv6 Input Filter Name: 100M-IPV6-IN-pp0.3221225614-in
IPv6 Output Filter Name: 100M-IPV6-OUT-pp0.3221225614-out
Accounting interval: 0
Dynamic configuration:
  junos-input-filter: 100M-IPV4-IN
  junos-input-ipv6-filter: 100M-IPV6-IN
  junos-ipv6-ndra-prefix: 2905:ee4:8000::/64
  junos-output-filter: 100M-IPV4-OUT
  junos-output-ipv6-filter: 100M-IPV6-OUT
```

O funcionamento do hold-down e active-drain em um pool SLAAC tem funcionamento similar ao pool IPv4 usado para PPPoE. O active-drain vai enviar PADT em todas as conexões PPPoE que estão fazendo uso daquele pool e os assinantes serão desconectados de forma abrupta. No caso de hold-down no pool os assinantes conectados que já estão utilizando o pool configurado com hold-down vão continuar recebendo RA's normalmente com prefixo já alocado no pool. As novas conexões não receberão RA do pool que está com hold-down e o BNG vai procurar o próximo pool disponível que está encadeado com o pool que foi configurado com hold-down.

Importante: Caso o pool NDRA em uso seja deletado do usuário o BNG vai enviar PADT para as conexões PPPoE forçando todas as ONU's fazerem novas conexões PPPoE no BNG.

10.1.3.3. IPv6 - DHCPv6 IA_NA e IA_PD - Funcionamento e Alocação de Prefixos

Outra forma da ONU obter o endereçamento na WAN é através do protocolo DHCPv6. Neste caso é enviado uma requisição de DHCP IA_NA para obtenção do endereço IP de WAN:



Neste caso a ONU fez o Router Solicit porém o BNG não está configurado com NDRA e a ONU fez a requisição de DHCPv6 (DHCPv6 Solicit).

Da mesma forma que acontece no SLAAC a requisição de DHCPv6 Solicit é enviada com o endereço IP de origem sendo o endereço de link-local da ONU (prefixo fe80:: + últimos 64 bits negociados no Interface Identifier) e o endereço IPv6 de destino é o IP de multicast **ff02::1:2**. Este endereço é reservado que agentes relay e servidores DHCPv6 respondam requisições DHCP feitas em link-local. Apenas servidores DHCPv6 e relay's de DHCPv6 responderão a estas requisições.

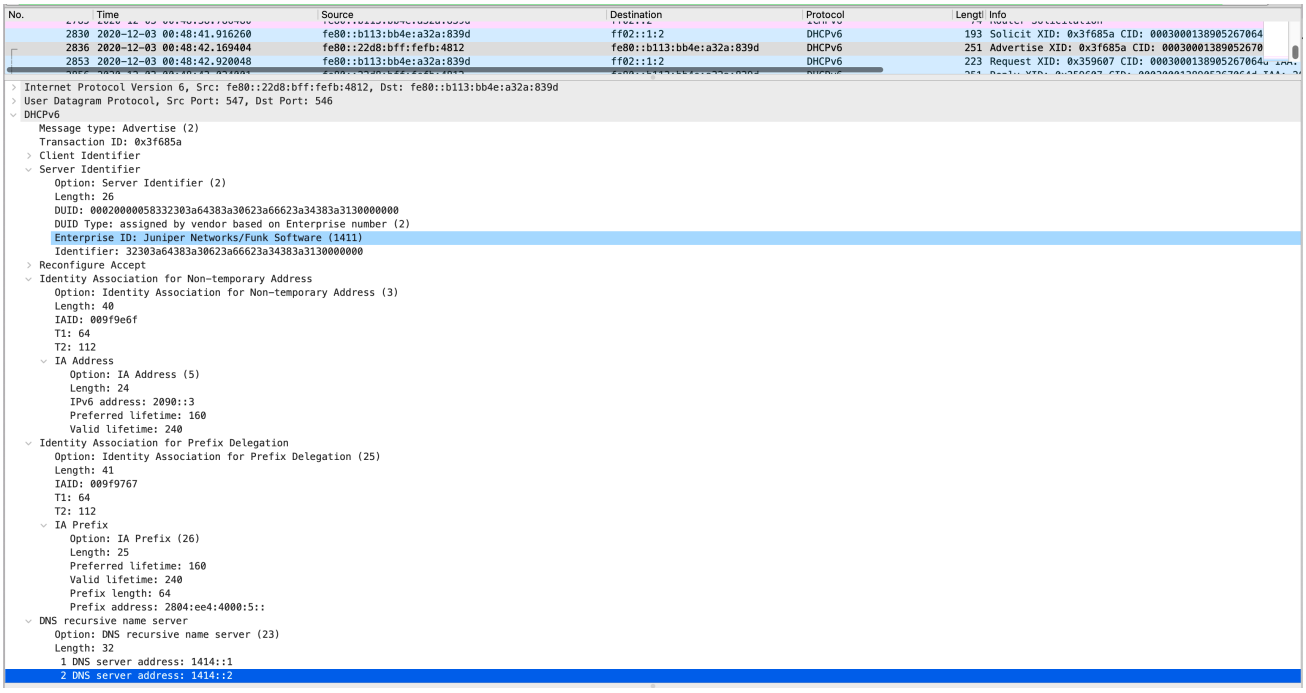
No caso da requisição de DHCP (DHCP Solicit) é utilizado o protocolo UDP onde a porta de origem é 546 e a porta de destino é 547.

Neste exemplo como a ONU também está configurada para receber o prefixo PD para entrega na LAN ela enviou o DHCP Solicit com o IA_NA (Identity Association for Non-Temporary Address) e também enviou o IA_PD na requisição (Identify Association for Prefix Delegation). Na requisição de DHCPv6 Solicit também é possível ver que a ONU envia o Option Request solicitando também os DNS's Recursivos (DNS recursive name server).

Importante: O BNG não suporta envio individual de DHCP Solicit para IA_NA e outro DHCP Solicit para PD. Caso a ONU vá fazer alocação de IP na WAN através de IA_NA e na LAN através de IA_PD é obrigatório que o DHCP Solicit seja uma mensagem só enviando as duas opções na mesma requisição. O BNG suporta o DHCP Renew do IA_NA e do IA_PD em requisições separadas mas a requisição dos prefixos tem que ser enviadas no mesmo DHCP Solicit.

Como o BNG está configurado com os devidos pool's DHCP de IA_NA e IA_PD ele vai enviar a resposta para a ONU:

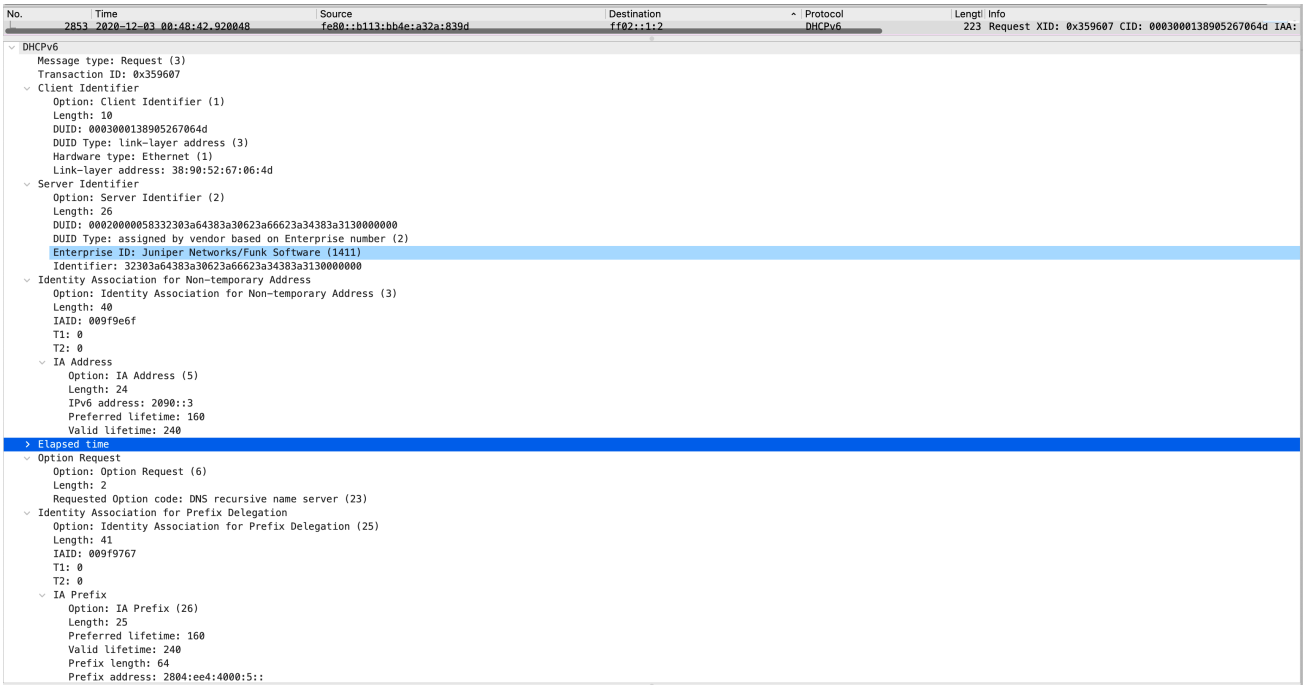
A resposta é enviada no DHCP Advertise:



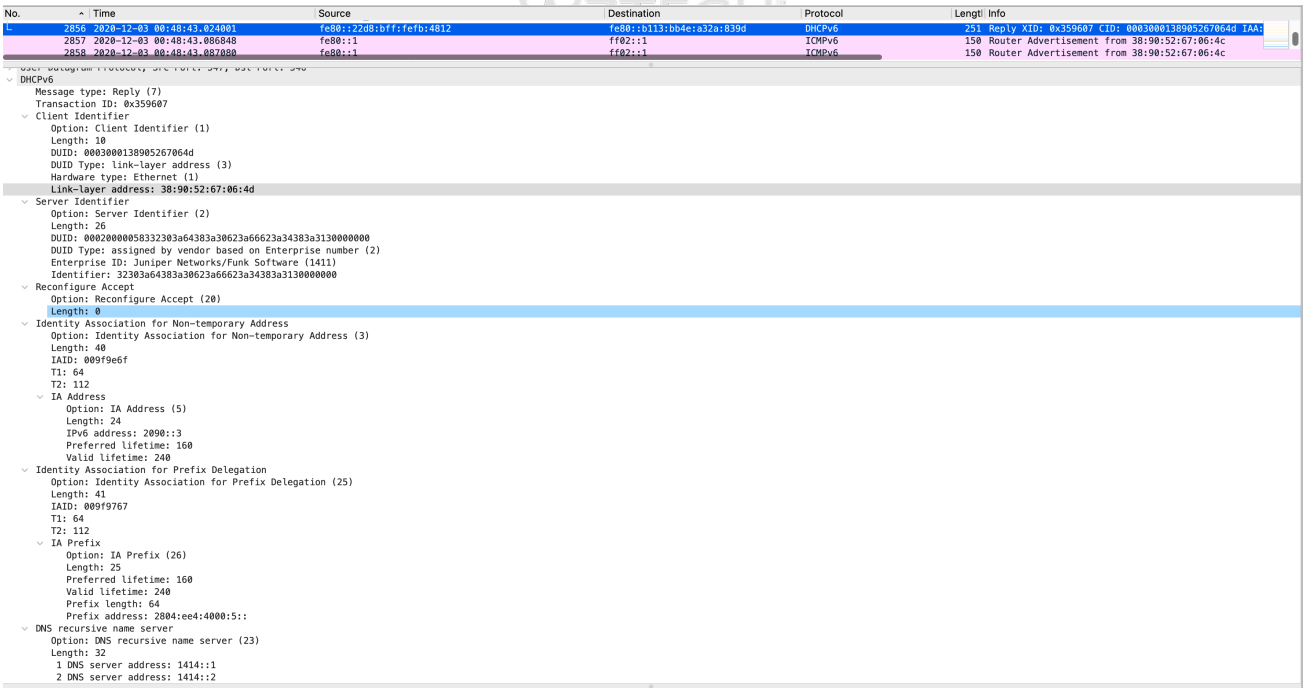
O DHCPv6 Advertise é enviado do BNG para a ONU com o source IP do pacote sendo o IP de link-local do BNG e o destino sendo o IP de link-local da ONU (comunicação unicast).

No DHCPv6 Advertise o BNG envia as informações de DNS requisitadas (DNS recursive name server), envia as informações do prefixo solicitado de IA_NA (Identity Association for Non-temporary Address) com os devidos valores de T1, T2, Preferred Lifetime e Valid lifetime e também envia as informações do prefixo de IA_PD com o prefixo entregue, tamanho do prefixo, Preferred lifetime, Validlifetime, T1 e T2.

Após a ONU dar aceite nestas informações enviadas ela envia a mensagem de DHCPv6 Request para o endereço de multicast ff02::1:2 confirmando que aceitou estas informações enviadas pelo DHCPv6 Server:



E por fim o BNG envia o DHCP Reply para a ONU através dos endereços de link-local (comunicação unicast).



Este fluxo das 4 mensagens de DHCP no IPv6 é chamado de SARR (Solicit, Advertise, Request, Reply).

Para que o BNG responda a requisições DHCP o primeiro passo é habilitar o serviço de DHCPv6 no BNG. Esta configuração é feita em [system services dhcp-local-server]:

```
set system services dhcp-local-server dhcpv6 group DHCPV6 interface pp0.0
```

Este comando acima está habilitando o serviço de DHCP no protocolo IPv6 (dhcpv6), está criando um grupo chamado DHCPV6 e as configurações são feitas neste grupo. É recomendado fazer as configurações utilizando grupos e não de forma geral em [system services dhcp-local-server dhcpv6]. Na configuração de grupos é possível fazer filtros do que será processado. No exemplo acima no grupo DHCPV6 está configurado a interface pp0.0. Neste caso este grupo só vale para requisições DHCPv6 feitas através da interface pp0. Caso seja feito uma requisição DHCPv6 através de qualquer outra interface do BNG não será processado por este grupo.

Apenas com a configuração acima habilitando o DHCPv6 Server na interface pp0 o BNG já consegue receber requisições DHCPv6. Caso seja requisitado um prefixo IA_NA o BNG vai avaliar se o RADIUS enviou os AVP's Framed-IPv6-Prefix ou Framed-IPv6-Pool. Caso o RADIUS não tenha enviado nenhum destes AVP's o BNG vai procurar um pool que tenha o prefix-lenght como /128. Para IA_NA é obrigatório que o tamanho do prefixo entregue seja /128. Este pool é configurado em [access address-assignment]:

Exemplo:

```
set access address-assignment pool POOL-IA_NA-1 family inet6 prefix 2090::/64
set access address-assignment pool POOL-IA_NA-1 family inet6 range RANGE prefix-length 128
set access address-assignment pool POOL-IA_NA-1 family inet6 excluded-address 2090::1
```

Este pool IA_NA foi configurado com tamanho /64 e deve ser alocados prefixos de tamanho /128 para os assinantes (caso não seja configurado, o prefix-length por default no BNG já é /128 para pool's IPv6). Também está sendo informado que o endereço IPv6 2090::1 não deve ser entregue aos usuários já que no caso de IA_NA *é obrigatório que o MX tenha um endereço IP do pool local configurado na interface loopback.* Desta forma, este endereço não pode fazer parte do pool.

O endereço IP que faz parte do pool IA_NA configurado na interface loopback deve obrigatoriamente possuir as configurações de preferred e primary. Exemplo da interface loopback configurada para IPv6:

```
set interfaces lo0 unit 0 family inet6 address 2001:1291::2/128
set interfaces lo0 unit 0 family inet6 address 2090::1/128 primary
set interfaces lo0 unit 0 family inet6 address 2090::1/128 preferred
```

Importante: Caso o pool utilizado por IA_NA seja enviado pelo RADIUS através do AVP Framed-IPv6-Pool o MX não exige que a interface loopback tenha um endereço dentro desse pool. Esta obrigatoriedade existe quando o pool IA_NA é buscado localmente sem ser informado pelo protocolo RADIUS. Para IA_PD não é necessário que a loopback tenha endereço IP participante do pool.

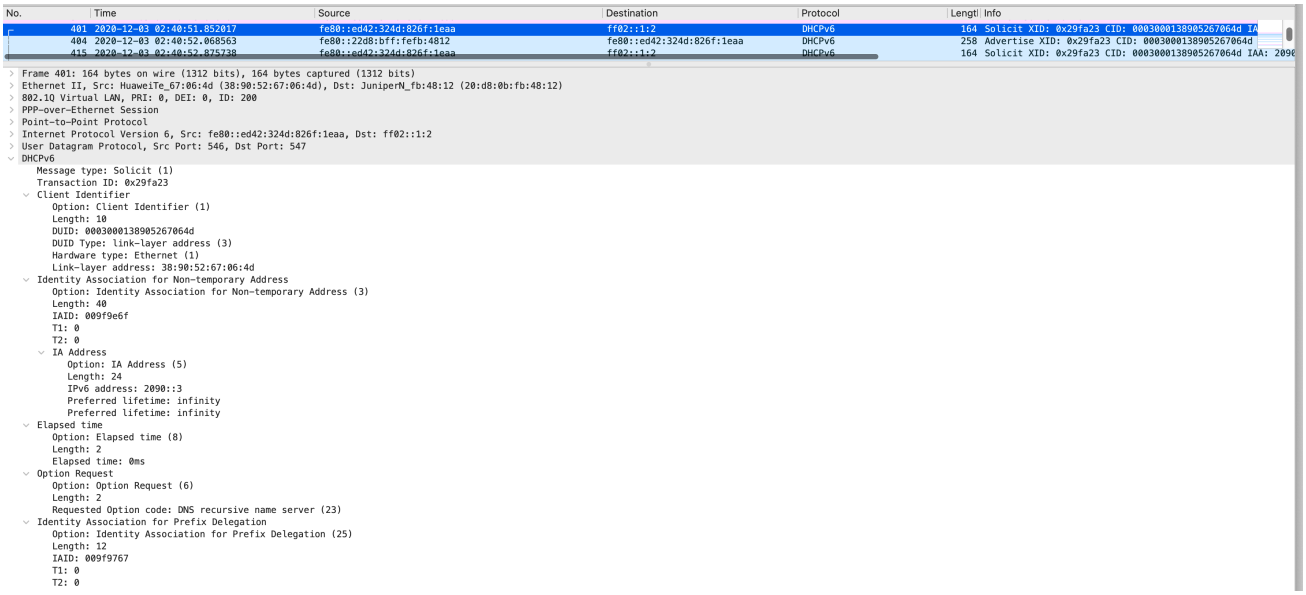
```
set system services dhcp-local-server dhcpv6 group DHCPV6 overrides delegated-pool POOL-V6-PD-1
```

Nesta configuração acima no grupo DHCPV6 do DHCPv6 Server está sendo associado um pool para PD (delegated-pool). Diferentemente do IA_NA caso o RADIUS não envie atributos de ERX-IPv6-Delegated-Pool-Name ou Delegated-IPv6-Prefix o DHCPv6 server não vai tentar achar um pool de PD automaticamente na lista de pool's em [address-assignment pool]. Este pool deve ser configurado de forma explicita com o [overrides delegated-pool]. No exemplo de configuração acima caso não seja enviado os AVP's do RADIUS o BNG vai atribuir aos assinantes prefixos IA_PD do pool POOL-V6-PD-1. Este pool é configurado em [access address-assignment]:

```
set access address-assignment pool POOL-V6-PD-1 family inet6 prefix 2804:0ee4:4000:0000:0000:0000:0000:0000/48
set access address-assignment pool POOL-V6-PD-1 family inet6 range prefix-range prefix-length 64
```

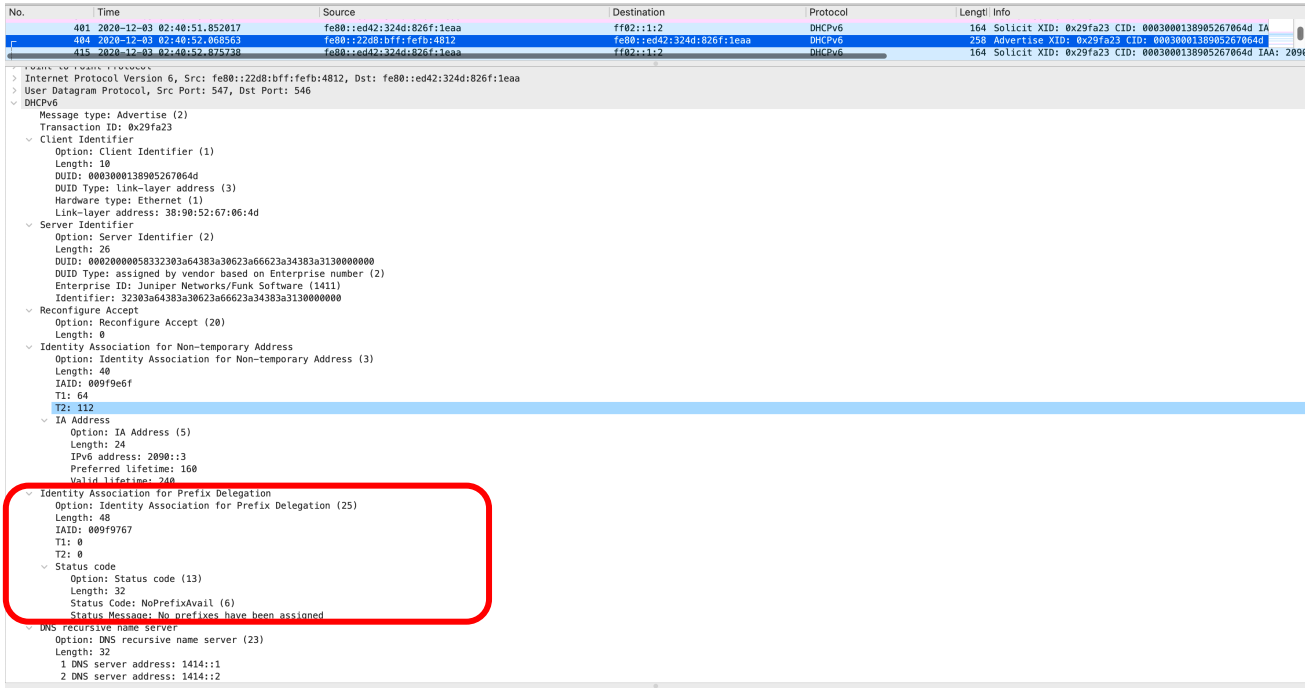
Este pool PD está sendo configurado como /48 e está sendo informado que os prefixos serão entregues aos assinantes com tamanho /64.

Quando o BNG recebe as requisições de DHCPv6 ele precisa devolver tudo que foi solicitado pela ONU.



Neste exemplo a ONU solicitou tanto IA_NA quanto IA_PD, ou seja, para a WAN a ONU vai alocar um prefixo IPv6 recebido através de IA_NA e para a LAN a ONU vai entregar endereços IPv6 do prefixo IPv6 PD recebido.

Caso o BNG não tenha como responder um prefixo para IA_NA ou para IA_PD ele vai informar na resposta:



Neste caso o BNG informou no DHCPv6 Advertise um prefixo para IA_NA e informou também na resposta do DHCPv6 Advertise que não há prefixos disponíveis para IA_PD. Como a ONU está esperando receber os dois prefixos ela manda o DHCP Solicit novamente e fica neste processo e não termina o SARR.

No BNG como não foi concluído o processo do SARR e o BIND (que é a entrada criada no BNG para tratar as mensagens de DHCP) fica no estado de SELECTING haja vista que a ONU não concluiu o fluxo completo do DHCP:

```
admin@MX204-LAB-WZTECH> show dhcpv6 server binding
Prefix                  Session Id  Expires  State     Interface    Client DUID
2090::3/128             121         86379    SELECTING pp0.3221225568 LL0x1-38:90:52:67:06:4d
```

```
admin@MX204-LAB-WZTECH> show dhcpv6 server binding detail

Session Id:  121
     Client IPv6 Address:                  2090::3/128
     Lease Expires:                        2023-09-12 12:02:12 -03
     Lease Expires in:                     86372 seconds
     Preferred Lease Expires:              2023-09-12 12:02:12 -03
     Preferred Lease Expires in:           86372 seconds
     Client DUID:                          LL0x1-38:90:52:67:06:4d
     State:                                SELECTING(DHCPV6_LOCAL_SERVER_STATE_CLIENT_SELECTING)
     Lease Start:                          2023-09-11 12:02:12 -03
     Last Packet Received:                 2023-09-11 12:02:28 -03
     Incoming Client Interface:            pp0.3221225568
     Client Pool Name:                     POOL-IA_NA-1
     Client Id Length:                     10
     Client Id:                            /0x00030001/0x38905267/0x064d
```

Importante: A ONU tem que confirmar o prefixo enviado com um DHCP Request (informando o prefixo recebido) e por fim o DHCPv6 server do BNG tem que enviar um DHCP Reply confirmando a alocação do bloco. Como a ONU não recebeu o PD ela fica retransmitindo esse DHCP Solicit e recebendo o DHCP Advertise com o mesmo resultado e como a ONU não termina o processo o BNG deleta o bind depois de 120 segundos (mesmo que chegue novo DHCP Solicit ele não atualiza esse timer do bind). Se o bind ficar no estado SELECTING por 120 segundos ele será deletado e o próximo pacote que chegar na caixa com DHCP Solicit vai criar um novo bind. Durante esse período em que o bind fica no estado de SELECTING não há conectividade do BNG com o assinante. Os prefixos só ficarão ativos no BNG quando a entrada mudar para o estado BOUND.

Caso o processo seja concluído corretamente com o SARR (Solicit, Advertise, Request e Reply) o bind ficará no estado BOUND:

```
admin@MX204-LAB-WZTECH> show dhcpv6 server binding
Prefix                  Session Id  Expires  State    Interface    Client DUID
2090::3/128             118         86367    BOUND    pp0.3221225565 LL0x1-38:90:52:67:06:4d
2804:ee4:4000:5::/64    118         86367    BOUND    pp0.3221225565 LL0x1-38:90:52:67:06:4d

admin@MX204-LAB-WZTECH> show dhcpv6 server binding detail

Session Id:  118
     Client IPv6 Address:                  2090::3/128
     Lease Expires:                        2023-09-12 12:00:09 -03
     Lease Expires in:                     86396 seconds
     Preferred Lease Expires:              2023-09-12 12:00:09 -03
     Preferred Lease Expires in:           86396 seconds
     Client IPv6 Prefix:                   2804:ee4:4000:5::/64
     Lease Expires:                        2023-09-12 12:00:09 -03
     Lease Expires in:                     86396 seconds
     Preferred Lease Expires:              2023-09-12 12:00:09 -03
     Preferred Lease Expires in:           86396 seconds
     Client DUID:                          LL0x1-38:90:52:67:06:4d
     State:                                BOUND(DHCPV6_LOCAL_SERVER_STATE_BOUND)
     Lease Start:                          2023-09-11 12:00:09 -03
     Last Packet Received:                 2023-09-11 12:00:10 -03
     Incoming Client Interface:            pp0.3221225565
     Client Pool Name:                     POOL-IA_NA-1
     Client Prefix Pool Name:              POOL-V6-PD
     Client Id Length:                     10
     Client Id:                            /0x00030001/0x38905267/0x064d
```

Neste caso foi criado um bind com ambos os prefixos (IA_NA e IA_PD) pois a ONU requisitou os dois prefixos e o BNG respondeu corretamente a ambos no DHCP Advertise.

Importante: O bind está associado à interface pp0 do assinante. Caso a conexão PPPoE caia, automaticamente, todos os binds associados àquela interface pp0.<unit> serão removidos.

Exemplo do usuário conectado usando IA_NA para a WAN + IA_PD para a LAN:

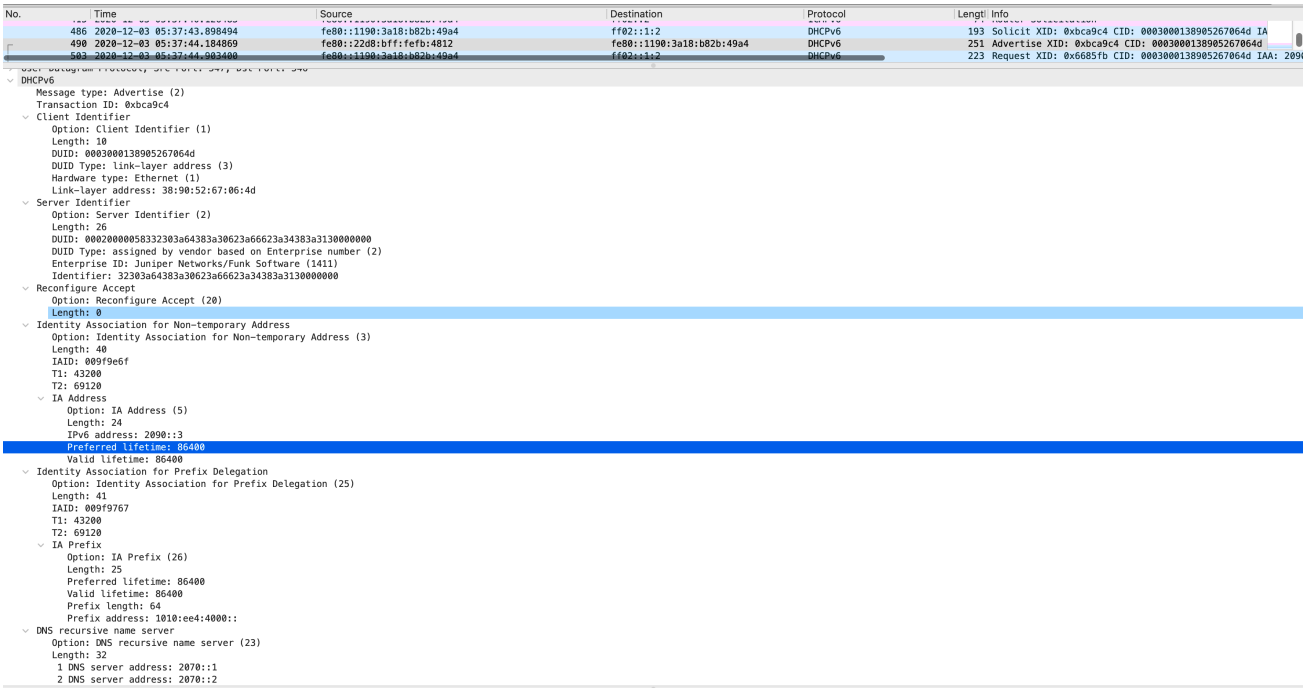
```
admin@MX204-LAB-WZTECH> show subscribers user-name wztech3
Interface                   IP Address/VLAN ID                  User Name                       LS:RI
pp0.3221225581              192.168.60.21                       wztech3                 default:default
*                           2090::3
*                           1010:ee4:4000::/64

admin@MX204-LAB-WZTECH> show subscribers user-name wztech3 extensive
Type: PPPoE
```

```
User Name: wztech3
IP Address: 192.168.60.21
IP Netmask: 255.255.255.255
IPv6 Address: 2090::3
IPv6 Prefix: 1010:ee4:4000::/64
Domain name server inet6: 2070::1 2070::2
Logical System: default
Routing Instance: default
Interface: pp0.3221225581
Interface type: Dynamic
Underlying Interface: demux0.3221225580
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 2
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 133
Session ID: 133
PFE Flow ID: 169
VLAN Id: 200
Login Time: 2023-09-11 13:08:55 -03
IP Address Pool: POOL-IP-06
IPv6 Address Pool: POOL-IA_NA-1
IPv6 Delegated Address Pool: _DAPV6
IPv6 Framed Interface Id: 8902:d2d3:6e25:6791
IPv4 Input Filter Name: 100M-IPV4-IN-pp0.3221225581-in
IPv4 Output Filter Name: 100M-IPV4-OUT-pp0.3221225581-out
IPv6 Input Filter Name: 100M-IPV6-IN-pp0.3221225581-in
IPv6 Output Filter Name: 100M-IPV6-OUT-pp0.3221225581-out
Accounting interval: 0
Dynamic configuration:
  junos-input-filter: 100M-IPV4-IN
  junos-input-ipv6-filter: 100M-IPV6-IN
  junos-output-filter: 100M-IPV4-OUT
  junos-output-ipv6-filter: 100M-IPV6-OUT
```

O endereço IA_NA aparece na sessão como IPv6 Address. O prefixo de PD aparece na sessão como IPv6 Prefix.

Detalhamento do Funcionamento do Lease no DHCP:

Na mensagem de DHCP Advertise o BNG informa à ONU alguns parâmetros relacionados ao prefixo IPv6:



Valid lifetime, Preferred lifetime, T1 e T2. Estes parâmetros são padronizados no protocolo DHCP e possuem as seguintes funções:

Valid lifetime: Tempo máximo que o prefixo recebido pode ficar instalado no cliente DHCP que recebeu o prefixo. Por default o BNG envia o valor sendo 86400 segundos (um dia). Caso o cliente DHCP não renove o

lease dentro destes 86400 segundos ao término deste tempo o cliente deve obrigatoriamente remover este prefixo. O BNG ao término do tempo do Valid lifetime também deletará o bind criado e o assinante perderá todos os endereços IP que foram entregues pelo DHCP através desse bind:

```
admin@MX204-LAB-WZTECH> show dhcpv6 server binding detail

Session Id:  130
     Client IPv6 Address:                  2090::4/128
     Lease Expires:                        2023-08-09 13:41:32 -03
     Lease Expires in:                     2 seconds
     Preferred Lease Expires:              2023-08-09 13:40:12 -03
     Preferred Lease Expires in:           0 seconds
     Client IPv6 Prefix:                   1010:ee4:4000::/64
     Lease Expires:                        2023-08-09 13:41:32 -03
     Lease Expires in:                     2 seconds
     Preferred Lease Expires:              2023-08-09 13:40:12 -03
     Preferred Lease Expires in:           0 seconds
     Client DUID:                          LL0x1-38:90:52:67:06:4d
     State:                                BOUND(DHCPV6_LOCAL_SERVER_STATE_BOUND)
     Lease Start:                          2023-08-09 13:36:27 -03
     Last Packet Received:                 2023-08-09 13:37:32 -03
     Incoming Client Interface:            pp0.3221225567
     Client Pool Name:                     NOVO-IA_NA
     Client Prefix Pool Name:              POOL-V6-PD-2
     Client Id Length:                     10
     Client Id:                            /0x00030001/0x38905267/0x064d
```

No exemplo acima o bind estava com apenas 2 segundos para expirar

```
admin@MX204-LAB-WZTECH> show dhcpv6 server binding
```

Depois de 2 segundos ele expirou e não foram encontrados mais bindings no BNG.

```
admin@MX204-LAB-WZTECH> show subscribers vlan-id 200
Interface                      IP Address/VLAN ID                  User Name                       LS:RI
demux0.3221225566               200                                                            default:default
pp0.3221225567                 100.64.10.27                        wztech3                     default:default
*                              2804:ee4:8000:1a::/64
```

Em virtude do bind ser removido o usuário perdeu os endereços IPv6 que o mesmo possuía na sessão.

O tempo máximo do lease (Valid lifetime) pode ser alterado no BNG dentro da configuração do pool através das configurações max-lease-time ou valid-lifetime. As duas opções têm o mesmo efeito e alteram o tempo máximo de lease enviado pelo DHCP Server na mensagem de Advertise. É uma opção ou outra. Caso seja configurado as duas o BNG não deixa fazer o commit da configuracão.

```
set access address-assignment pool POOL-IA_NA-1 family inet6 dhcp-attributes maximum-lease-time 240
set access address-assignment pool POOL-IA_NA-1 family inet6 dhcp-attributes valid-lifetime 240
```

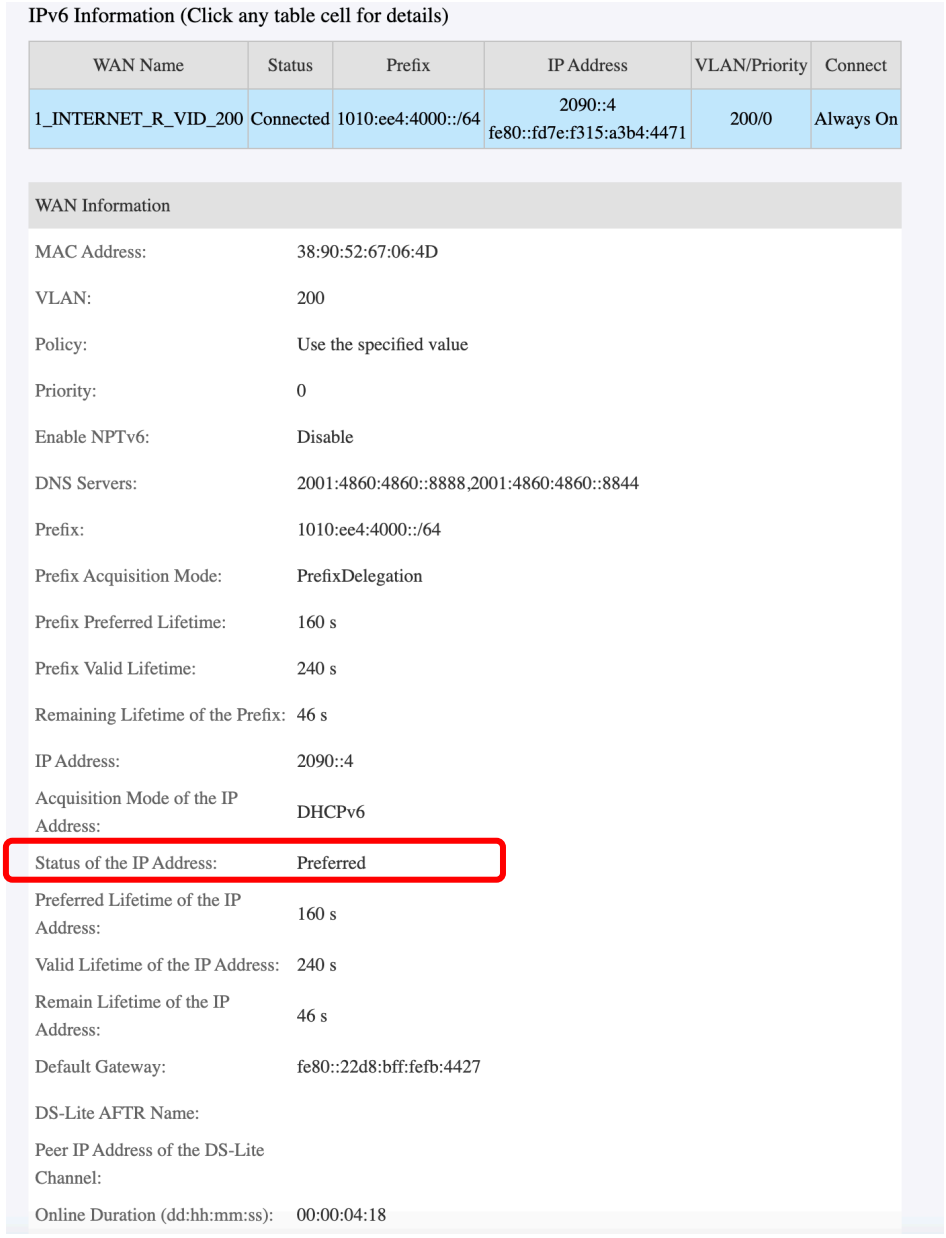
Preferred lifetime: Por default o BNG envia o valor também de Preferred lifetime sendo 86400 segundos (um dia). Caso o prefixo não seja renovado pela ONU após o término do tempo do Preferred Lifetime, é recomendado no protocolo DHCP que este prefixo não seja mais utilizado para novas conexões e apenas continue funcionando aceitando pacotes das conexões já estabelecidas. Porém, na prática, a implementação geral do protocolo nos clientes DHCP é de que o Preferred Lifetime funciona como o Valid lifetime, ou seja, mesmo que o Preferred lifetime expire, enquanto não expirar o Valid lifetime o prefixo é utilizado normalmente para conexões existentes ou novas. *No BNG caso o cliente não renove o prefixo até que termine o tempo do Preferred lifetime o "bind" vai continuar normal no estado de BOUND e funcionando normalmente. O bind só será deletado caso expire o tempo de Valid lifetime:*

```
admin@MX204-LAB-WZTECH> show dhcpv6 server binding detail

Session Id:  130
     Client IPv6 Address:                  2090::4/128
     Lease Expires:                        2023-08-09 13:41:32 -03
     Lease Expires in:                     2 seconds
     Preferred Lease Expires:              2023-08-09 13:40:12 -03
     Preferred Lease Expires in:           0 seconds
     Client IPv6 Prefix:                   1010:ee4:4000::/64
     Lease Expires:                        2023-08-09 13:41:32 -03
     Lease Expires in:                     2 seconds
     Preferred Lease Expires:              2023-08-09 13:40:12 -03
```

```
    Preferred Lease Expires in:          0 seconds
    Client DUID:                         LL0x1-38:90:52:67:06:4d
    State:                               BOUND(DHCPV6_LOCAL_SERVER_STATE_BOUND)
    Lease Start:                         2023-08-09 13:36:27 -03
    Last Packet Received:                2023-08-09 13:37:32 -03
    Incoming Client Interface:           pp0.3221225567
    Client Pool Name:                    NOVO-IA_NA
    Client Prefix Pool Name:             POOL-V6-PD-2
    Client Id Length:                    10
    Client Id:                           /0x00030001/0x38905267/0x064d

admin@MX204-LAB-WZTECH>
```

No exemplo acima o Preferred Lease já expirou e o bind continua como BOUND.

Na ONU usada nos testes, mesmo já havendo terminando o tempo de Preferred lifetime do prefixo o estado do prefixo ainda permanece como "Preferred", ou seja, será utilizado de forma geral.



IPv6 Information (Click any table cell for details)

WAN Name	Status	Prefix	IP Address	VLAN/Priority	Connect
1_INTERNET_R_VID_200	Connected	1010:ee4:4000::/64	2090::4 fe80::fd7e:f315:a3b4:4471	200/0	Always On

WAN Information	
MAC Address:	38:90:52:67:06:4D
VLAN:	200
Policy:	Use the specified value
Priority:	0
Enable NPTv6:	Disable
DNS Servers:	2001:4860:4860::8888,2001:4860:4860::8844
Prefix:	1010:ee4:4000::/64
Prefix Acquisition Mode:	PrefixDelegation
Prefix Preferred Lifetime:	160 s
Prefix Valid Lifetime:	240 s
Remaining Lifetime of the Prefix:	46 s
IP Address:	2090::4
Acquisition Mode of the IP Address:	DHCPv6
Status of the IP Address:	Preferred
Preferred Lifetime of the IP Address:	160 s
Valid Lifetime of the IP Address:	240 s
Remain Lifetime of the IP Address:	46 s
Default Gateway:	fe80::22d8:bff:fefb:4427
DS-Lite AFTR Name:	
Peer IP Address of the DS-Lite Channel:	
Online Duration (dd:hh:mm:ss):	00:00:04:18

O tempo do preferred-lifetime pode ser alterado com o comando abaixo:

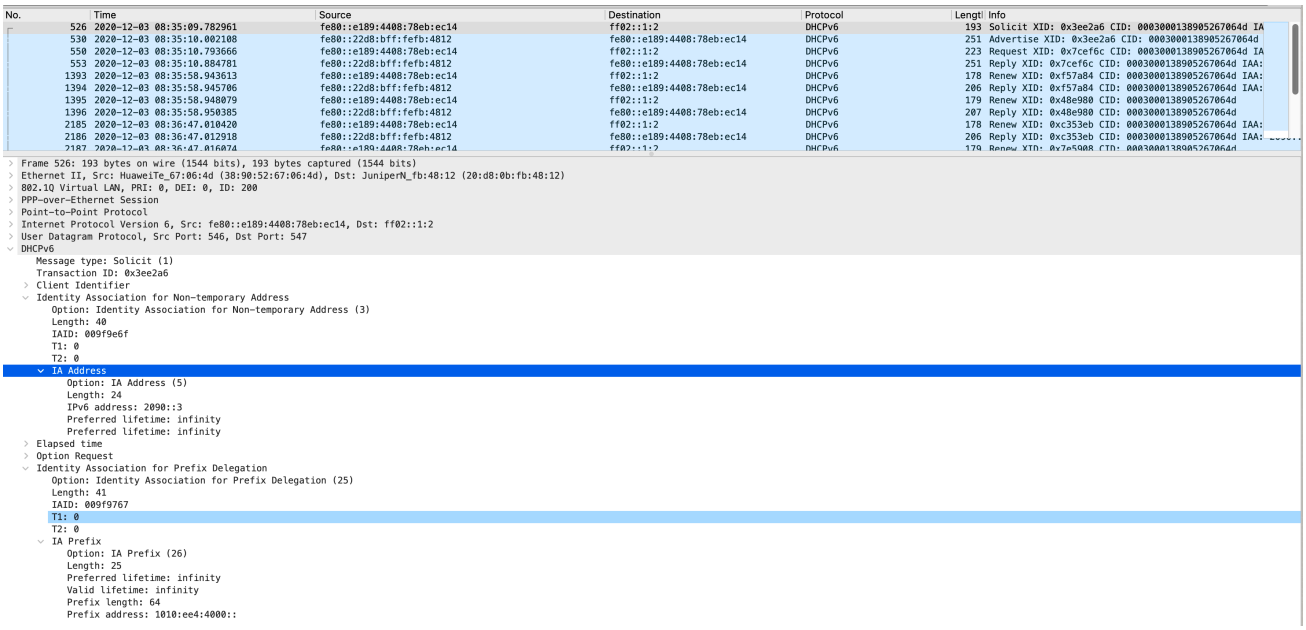
```
set access address-assignment pool POOL-IA_NA-1 family inet6 dhcp-attributes preferred-lifetime 180
```

O preferred-lifetime não pode ser configurado em conjunto com o maximum-lease-time. Apenas pode ser configurado em conjunto com o valid-lifetime.

Caso seja alterado o valor de Preferred Lifetime os valores de T1 e T2 serão calculados baseados no valor do Preferred Lifetime.

T1 e T2: Por default quando é entregue um prefixo para o assinante, além do Valid lifetime e o Preferred lifetime é informado também em segundos o valor T1 e T2. O valor T1 chamado de Renewal Time é por default 50% do tempo máximo do Lease e o valor T2 chamado de Rebinding Time é por default 80% do tempo máximo do Lease. Caso o valor do Preferred lifetime seja alterado, os valores de T1 e T2 serão calculados em cima do Preferred e não mais do Valid lifetime.

Vamos tomar um exemplo de uma requisição da ONU para obter endereços IA_NA e IA_PD:

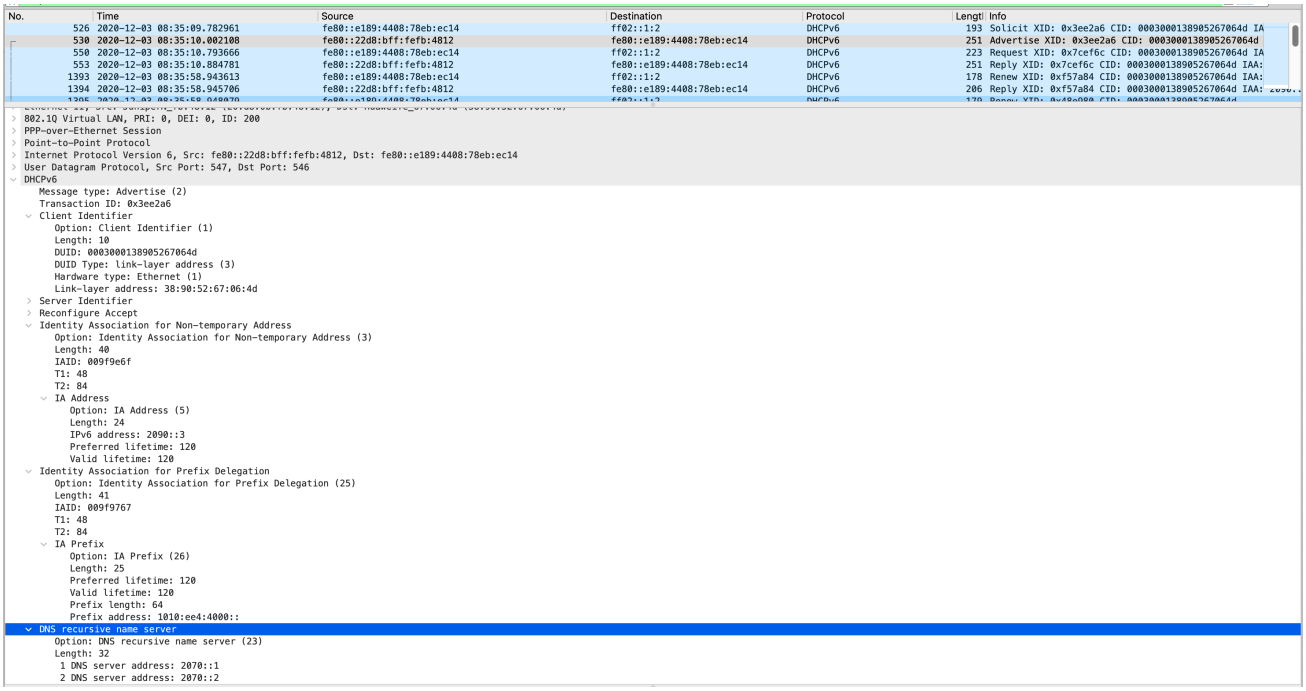


A ONU enviou o DHCP Solicit requisitando IP IA_NA e prefixo IA_PD.

No BNG temos dois pool's configurados que serão utilizados para entregar os endereços: um pool para IA_NA (prefix-length /128) e outro pool para IA_PD (prefix-length /64):

```
set access address-assignment pool POOL-IA_NA-1 family inet6 prefix 2090::/64
set access address-assignment pool POOL-IA_NA-1 family inet6 range RANGE prefix-length 128
set access address-assignment pool POOL-IA_NA-1 family inet6 dhcp-attributes valid-lifetime 120
set access address-assignment pool POOL-IA_NA-1 family inet6 dhcp-attributes t1-percentage 40
set access address-assignment pool POOL-IA_NA-1 family inet6 dhcp-attributes t2-percentage 70
set access address-assignment pool POOL-IA_NA-1 family inet6 excluded-address 2090::1

set system services dhcp-local-server dhcpv6 group DHCPV6 overrides delegated-pool POOL-V6-PD-1

set access address-assignment pool POOL-V6-PD-1 family inet6 prefix 1010:0ee4:4000:0000:0000:0000:0000:0000/48
set access address-assignment pool POOL-V6-PD-1 family inet6 range prefix-range prefix-length 64
set access address-assignment pool POOL-V6-PD-1 family inet6 dhcp-attributes valid-lifetime 300
set access address-assignment pool POOL-V6-PD-1 family inet6 dhcp-attributes t1-percentage 20
set access address-assignment pool POOL-V6-PD-1 family inet6 dhcp-attributes t2-percentage 40
```

Importante: Como existem tempos diferentes de valid-lifetime nos dois pool's que terão prefixos sendo entregues ao assinante o BNG vai usar os parâmetros do pool que tiver o menor tempo de valid-lifetime. Neste caso o pool POOL-IA_NA-1 tem o menor tempo de valid-lifetime e os valores de Valid lifetime, Preferred lifetime, T1 e T2 serão obtidos deste pool e serão enviados à ONU para ambos os prefixos.

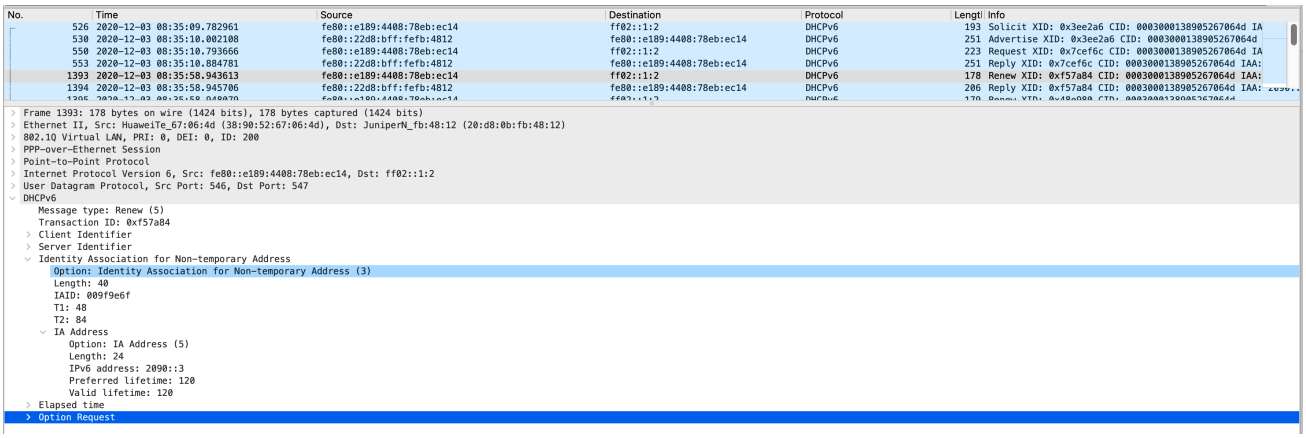


Neste exemplo acima às 08:35:10 o BNG no DHCP Advertise enviou um Valid Lifetime de 120 segundos, o Preferred Lifetime de 120 segundos (haja vista que não foi configurado valor diferente para Preferred Lifetime), T1 foi enviado com 40% dos 120 segundos (48 segundos) e T2 foi enviado com 70% dos 120 segundos (84 segundos) visto que estes percentuais de T1 e T2 foram configurados.

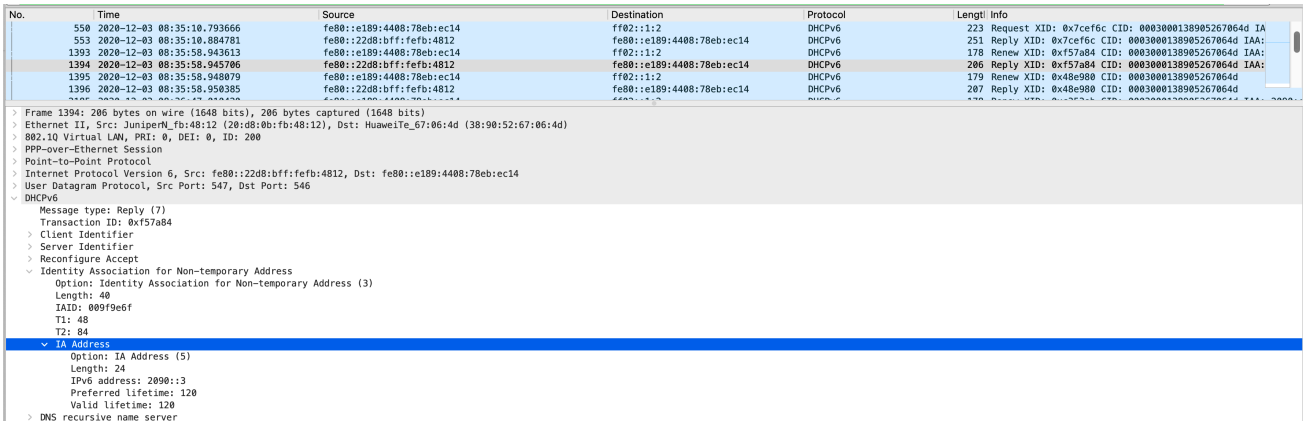
Os tempos T1 (Renew) e T2 (Rebinding) informam ao cliente DHCP que sendo atingido o tempo T1 ele deve fazer uma renovação do lease (Renew) com o Servidor DHCP que lhe concedeu o endereço IP. Caso não haja respostas do servidor DHCP no tempo T2 (Rebinding) o cliente DHCP deve fazer um Rebind. O rebind é uma requisição para toda a rede a fim de que qualquer servidor DHCP renove seu o lease ou conceda um novo endereço caso não seja possível fazer a renovação. Caso o cliente DHCP não tenha respostas até o término do tempo do Valid Lifetime o prefixo não poderá mais ser utilizado.

Às 08:35:58 (48 segundos depois do Advertise que é o tempo de T1) a ONU enviou o Renew do IA_NA e do IA_PD:

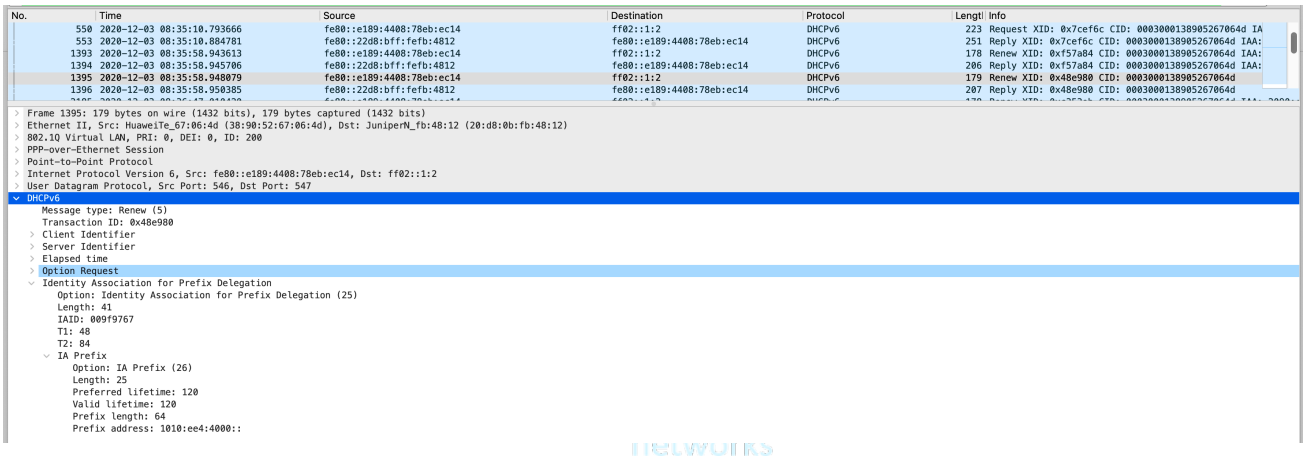
Renew do IA_NA:



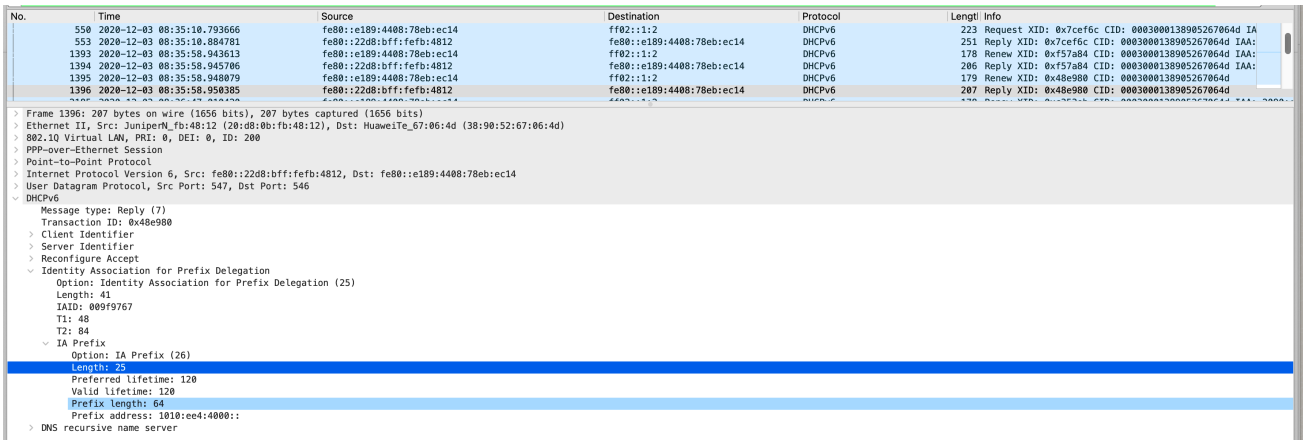
O BNG respondeu com o Reply do IA_NA:



Renew do IA_PD também 48 segundos depois do Advertise que é o tempo de T1:



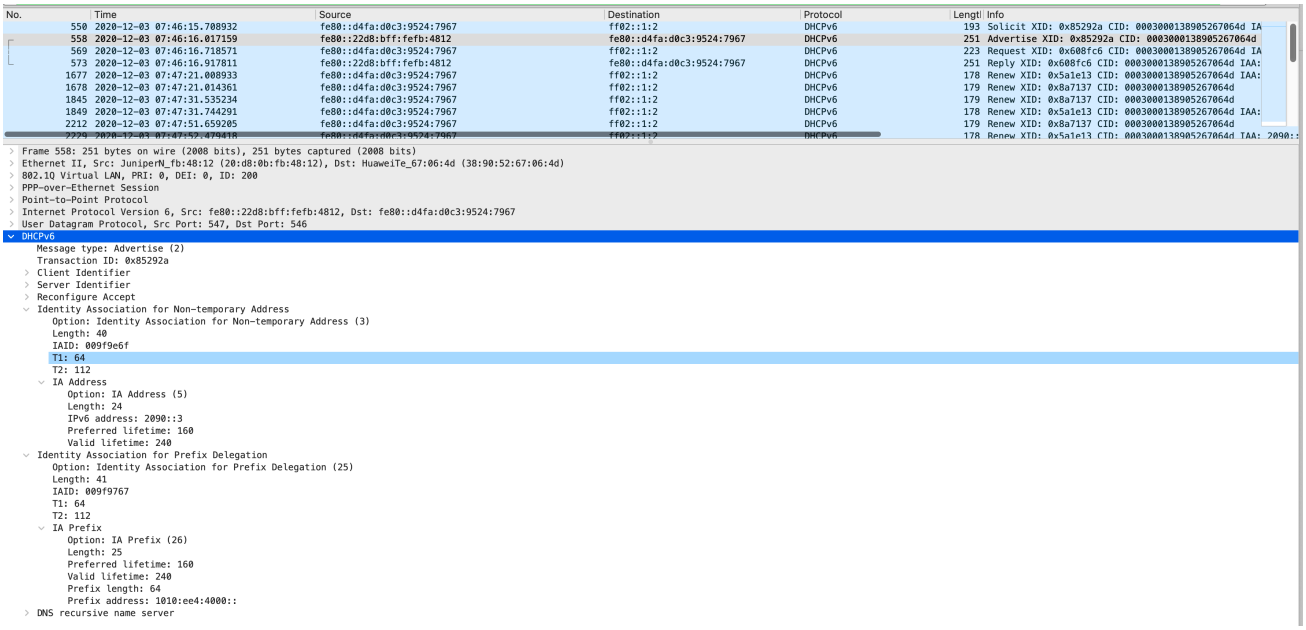
E o BNG respondeu o Renew do IA_PD com Reply:



Desta forma a ONU vai sempre tentar renovar o lease do IA_NA e do IA_PD no tempo T1.

Abaixo um outro exemplo de outro lease entregue pelo BNG. Configuração do BNG:

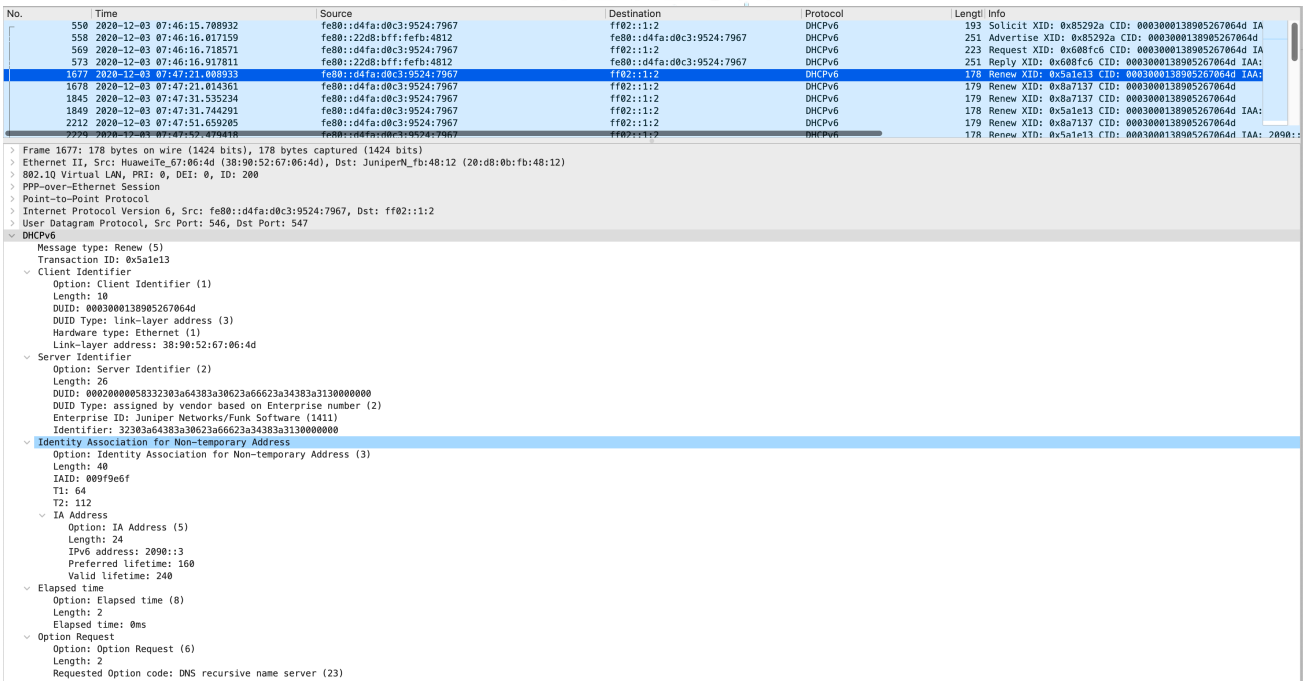
```
set access address-assignment pool POOL-IA_NA-1 family inet6 prefix 2090::/64
set access address-assignment pool POOL-IA_NA-1 family inet6 range RANGE prefix-length 128
set access address-assignment pool POOL-IA_NA-1 family inet6 dhcp-attributes valid-lifetime 240
set access address-assignment pool POOL-IA_NA-1 family inet6 dhcp-attributes preferred-lifetime 160
set access address-assignment pool POOL-IA_NA-1 family inet6 dhcp-attributes t1-percentage 40
set access address-assignment pool POOL-IA_NA-1 family inet6 dhcp-attributes t2-percentage 70
set access address-assignment pool POOL-IA_NA-1 family inet6 excluded-address 2090::1
```



Foi entregue o Lease com Valid Lifetime de 240, Preferred Lifetime de 160, T1 sendo 40% do Preferred Lifetime (visto que ele está configurado) e T2 sendo 70% do tempo do Preferred Lifetime (visto que ele está configurado).

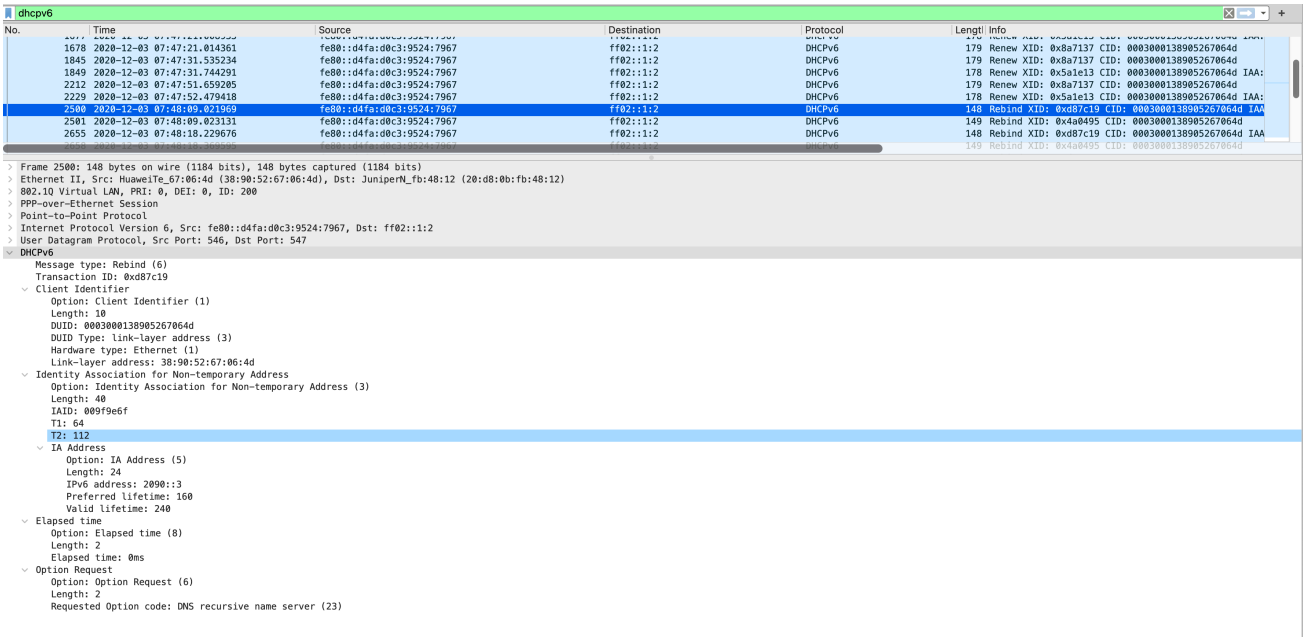
O Advertise foi enviado para o usuario no horario 07:46:16.

Às 07:47:21 (64 segundos depois do lease ser entregue à ONU que é o tempo T1) a ONU faz o DHCP Renew para o IA_NA e IA_PD:

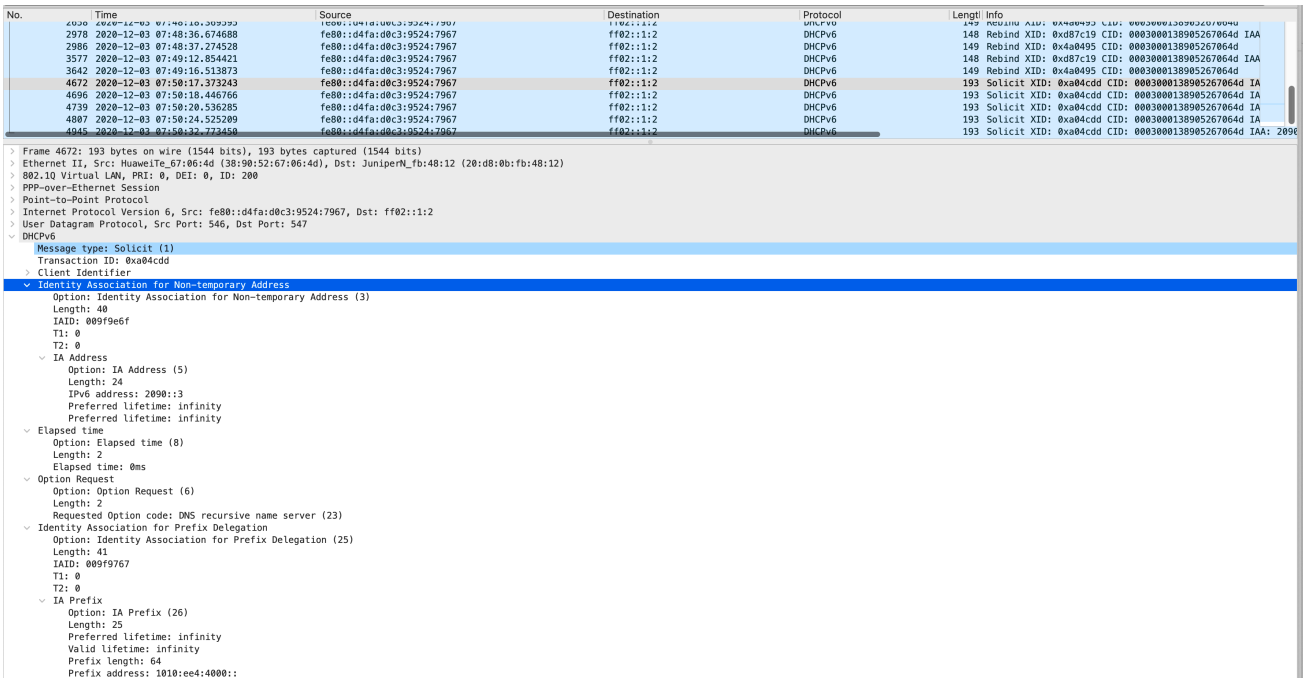


Como não são obtidas respostas, a ONU faz novos envios de Renew às 07:47:31, 07:47:51 e 07:47:52. (Estes novos Renew podem NÃO ser gerados e vai depender da implementação do protocolo DHCP no cliente).

Às 07:48:09 (112 segundos depois do lease ser entregue à ONU que é o tempo T2) a ONU faz o DHCP Rebind para o IA_NA e IA_PD:



Às 07:50:17, depois de 240 segundos (Valid lifetime entregue no lease para a ONU) o prefixo é removido da ONU e esta começa novamente a tentar obter novo endereço IP enviando mensagens de DHCP Solicit:



Este é o processo normal de funcionamento do lease no protocolo DHCPv6.

É possível também configurar os valores de T1 e T2 sem usar percentual. Neste caso é configurado valores absolutos. Exemplo:

```
set access address-assignment pool POOL-IA_NA-1 family inet6 dhcp-attributes t1-renewal-time 100
set access address-assignment pool POOL-IA_NA-1 family inet6 dhcp-attributes t2-rebinding-time 130
```

Outra opção que existe para ser configurado dentro do pool no caso de uso com o protocolo DHCP é o parâmetro grace-period. Neste caso, o BNG, após o tempo do Valid Lifetime, dá ainda esse tempo para que a ONU consiga fazer o Renew. Exemplo da configuração:

```
set access address-assignment pool POOL-IA_NA-1 family inet6 dhcp-attributes grace-period 100
```

Depois que terminar o tempo máximo do lease no bind caso ele não seja renovado através do DHCP Renew ao invés do bind ser deletado o BNG adiciona o tempo do grace-period ao tempo de expiração do bind e aguarda mais esse tempo para ver se a ONU vai conseguir renovar o bind:

```
admin@MX204-LAB-WZTECH> show dhcpv6 server binding
Prefix                  Session Id  Expires  State    Interface    Client DUID
2090::4/128             143         100      BOUND    pp0.3221225576 LL0x1-38:90:52:67:06:4d
1010:ee4:4000::/64      143         100      BOUND    pp0.3221225576 LL0x1-38:90:52:67:06:4d
```

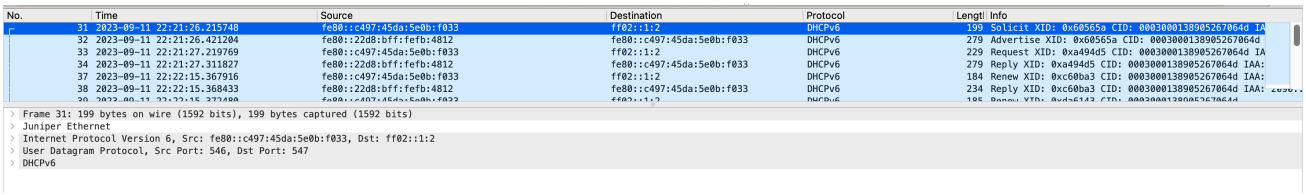
Caso não seja renovado o bind dentro desse período de tempo adicional o bind será removido.

Todas as mensagens de DHCPv6 são processadas no BNG pela Routing-Engine e os pacotes podem ser capturados com o comando "monitor traffic". Exemplo:

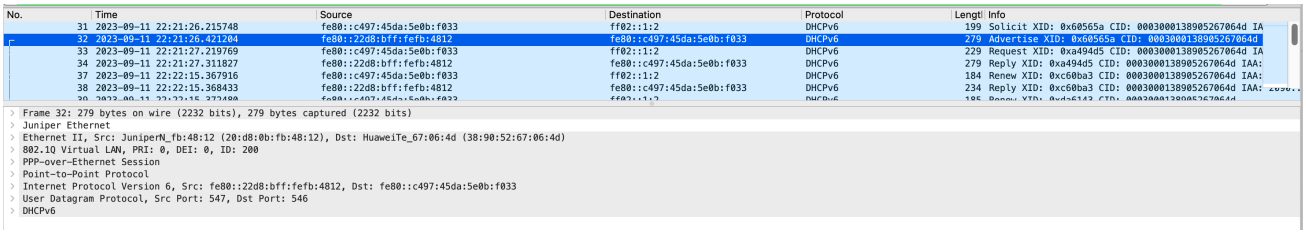
```
admin@MX204-LAB-WZTECH> monitor traffic interface ae0 size 1500 no-resolve no-domain-names write-file
/var/tmp/sniffer.pcap
Address resolution is OFF.
Listening on ae0, capture size 1500 bytes
88 packets received by filter
0 packets dropped by kernel

admin@MX204-LAB-WZTECH>
```

Neste caso estão sendo capturados todos os pacotes que estão chegando na Routing Engine através da interface ae0 (*caso sejam feitos filtros com "matching" alguns pacotes podem não ser mostrados no arquivo pcap para o protocolo DHCPv6).* Pacotes com tamanho de até 1500 bytes serão capturados e o resultado será gravado em um arquivo no formato PCAP em /var/tmp/sniffer.pcap. Este arquivo pcap pode ser aberto por softwares como wireshark ou tcpdump.

Quando é feito esta captura, para os pacotes DHCPv6 onde o destino é o próprio MX no arquivo PCAP não são mostradas as camadas Ethernet, 802.1Q, PPPoE e PPP. Exemplo:



Já nos pacotes enviados pelo MX estas camadas são gravadas no arquivo pcap:



Importante: Os pacotes estão todos sendo encapsulados em cima do protocolo PPPoE. Neste caso é apenas uma restrição do MX para capturar estas informações quando os pacotes de DHCPv6 são destinados à Routing Engine.

Diferentemente do SLAAC onde o Router Advertisement é um pacote gerado de forma espontânea pelo BNG, sendo possível ser feito o bloqueio do Router Solicit no MX, no protocolo DHCPv4 ou DHCPv6 não há a possibilidade do BNG gerar mensagens de forma espontânea a não ser casos muito específicos como o caso da funcionalidade "reconfigure" do DHCP Server. O BNG vai esperar as mensagens DHCP Solicit, Renew ou Rebind chegarem para enviar as respostas de Advertise ou Reply. Desta forma, não é possível bloquear pacotes de DHCPv6 para a Routing Engine. Há funcionalidades no BNG para minimizar possíveis impactos em caso de flooding de pacotes DHCPv4 ou DHCPv6 para o plano de controle como DDoS Protection, DHCP Short Cycle Protection e PPPoE Short Cycle Protection, porém é recomendado que os clientes que fazem uso de DHCP

tenham em suas firewall filters um termo fazendo policiamento da quantidade de pacotes DHCPv4 ou DHCPv6, para que em casos de ataques ou comportamentos anômalos na rede o BNG aplique este limite por assinante na PFE. Este termo chamado de DHCPV6POLICER já foi detalhado neste documento.

A seguir o detalhamento da entrega dos endereços IPv6 IA_NA para o assinante quando o BNG precisa fazer a entrega de IA_NA em virtude de ter recebido DHCP Solicit com IA_NA:

1. Em primeiro lugar o BNG dá preferência pelo prefixo IPv6 de IA_NA recebido através do AVP Framed-IPv6-Prefix no protocolo RADIUS. Lembrando que para IA_NA o prefixo deve ser /128. Caso o RADIUS mande este AVP com um prefixo IPv6 /128 este prefixo será atribuído ao assinante e este prefixo será informado para a ONU na mensagem de DHCP Advertise. O AVP Framed-IPv6-Prefix é o mesmo utilizado para NDRA. Neste caso para que o Framed-IPv6-Prefix funcione corretamente como IA_NA é recomendado que não exista configuração de NDRA.

2. Em segundo lugar o BNG dá preferência para o atributo Framed-IPv6-Pool. Caso tenha sido enviado o atributo Framed-IPv6-Pool com um nome de um pool IA_NA configurado no BNG este será o pool que o BNG vai usar para alocar endereços para a ONU. Neste caso não é obrigatório que este pool tenha um endereço IP na interface loopback configurado como primary/preferred. Caso o RADIUS envie os AVP's Framed-IPv6-Prefix e Framed-IPv6-Pool o BNG alocará o prefixo enviado no AVP Framed-IPv6-Prefix visto que ele tem precedência. O AVP Framed-IPv6-Pool também é o mesmo atributo utilizado no BNG para NDRA. Neste caso para utilização do AVP com IA_NA é recomendado que o NDRA não esteja ativo no BNG.

Importante: Caso o NDRA esteja configurado juntamente com IA_NA e IA_PD o resultado da alocação dos prefixos vai depender da configuração da ONU e configuração do BNG. Também podem existir problemas para identificação do endereço de WAN da ONU no RADIUS. Este modelo não é suportado oficialmente pela Juniper em virtude de possíveis falhas no processo de rastreamento do endereço de WAN em casos de solicitações judiciais. Os modelos suportados oficialmente para IPv6 são NDRA + IA_PD, IA_NA + IA_PD ou apenas IA_PD.

Caso o RADIUS envie o AVP Framed-IPv6-Pool com um nome de pool IA_NA que não existe configurado no BNG este AVP será descartado e o BNG vai alocar um prefixo do pool IA_NA DEFAULT.

Importante: Caso o RADIUS envie o AVP Framed-IPv6-Pool para o assinante com um nome de pool correto que existe no BNG, porém no pool não existe mais prefixos livres para serem alocados, a ONU não vai pegar endereço IP e o BNG não vai procurar um próximo pool. O único caso que o BNG vai procurar um próximo pool é quando o pool informado pelo RADIUS está encadeado ou "conectado" com um outro pool em uma cadeia de pools através da configuração de link. Este detalhamento do encadeamento dos pools segue o mesmo processo já detalhado para pools IPv4.

3. Em terceiro lugar caso nenhuma das duas formas anteriores sejam enviadas por RADIUS o BNG vai procurar endereços livres para o assinante no pool IA_NA DEFAULT. Este pool IA_NA DEFAULT é o pool que está configurado para entrega de endereços /128 e possui um endereço IPv6 do pool configurado na interface lo0. Este endereço do pool na interface lo0 deve estar com as configurações de primary e preferred e não podem existir outros endereços IPv6 configurados como primary e preferred na interface lo0.

A seguir o detalhamento da entrega dos endereços IPv6 IA_PD para o assinante quando o BNG precisa fazer a entrega de prefixos PD em virtude de ter recebido DHCP Solicit com IA_PD:

1. Em primeiro lugar o BNG dá preferência pelo prefixo IPv6 de IA_PD recebido através do AVP Delegated-IPv6-Prefix no protocolo RADIUS. Para prefixos PD o BNG suporta configurar prefixos de qualquer tamanho, porém é recomendado o uso de prefixos /64 para que a ONU consiga entregar o prefixo PD na LAN também através de SLAAC. Para envio de prefixos diferentes de /64 deve ser avaliado o suporte da ONU com as suas devidas configurações. Caso o RADIUS mande este AVP com um prefixo IPv6 /64 este prefixo será atribuído ao assinante e este prefixo será informado no DHCP Advertise.

2. Em segundo lugar o BNG dá preferência para o atributo ERX-IPv6-Delegated-Pool-Name (Vendor 4874 / Atributo 161). Caso tenha sido enviado o atributo ERX-IPv6-Delegated-Pool-Name com o nome de

um pool IA_PD configurado no BNG este será o pool que o BNG vai usar para alocar prefixos para o assinante. Caso o RADIUS envie os AVP's Delegated-IPv6-Prefix e ERX-IPv6-Delegated-Pool-Name o BNG alocará o prefixo enviado no AVP Delegated-IPv6-Prefix visto que ele tem precedência.

Caso o RADIUS envie o AVP ERX-IPv6-Delegated-Pool-Name com um nome de pool que não existe configurado no BNG o assinante NÃO vai conectar.

Importante: Caso o RADIUS envie o AVP ERX-IPv6-Delegated-Pool-Name *para o assinante com um nome de pool correto que existe no BNG, porém no pool não existe mais prefixos livres para serem alocados, o assinante não vai conseguir fazer a conexão IPv6 e o BNG não vai procurar um próximo pool. O único caso que o BNG vai procurar um próximo pool é quando o pool informado pelo RADIUS está encadeado ou "conectado" com um outro pool em uma cadeia de pools através da configuração de link. Este detalhamento do encadeamento dos pools com a ordem de busca segue o mesmo processo já detalhado para pools IPv4.*

No caso de pools encadeados pode-se obter as estatísticas dos pool's encadeados da mesma forma que acontece com os pool's IPv4:

```
admin@MX204-LAB-WZTECH> show network-access aaa statistics address-assignment pool POOL-V6-PD-1
Address assignment statistics
  Pool Name: POOL-V6-PD-1
    Link Name: POOL-V6-PD-2
    Out of Memory: 0
    Out of Addresses: 4
    Address total: 1
    Addresses in use: 1
    Address Usage (percent): 100
    Pool drain configured: no
  Pool Name: POOL-V6-PD-2
    Link Name: POOL-V6-PD-3
    Out of Memory: 0
    Out of Addresses: 0
    Address total: 1
    Addresses in use: 1
    Address Usage (percent): 100
    Pool drain configured: no
  Pool Name: POOL-V6-PD-3
    Out of Memory: 0
    Out of Addresses: 0
    Address total: 1
    Addresses in use: 1
    Address Usage (percent): 100
    Pool drain configured: no
  Pool Name: (all pools in chain)
    Out of Memory: 0
    Out of Addresses: 4
    Address total: 3
    Addresses in use: 3
    Address Usage (percent): 100
    Pool drain configured: no
```

3. Em terceiro lugar caso nenhuma das duas formas anteriores sejam enviadas pelo RADIUS, o BNG vai procurar prefixos livres para o assinante no pool especificado na configuração de [overrides delegated-pool]. Este pool é o pool DEFAULT de PD.

Caso algum pool IPv6 chegue no limite de utilização será gerado um evento no log (arquivo messages):

```
Sep 12 09:39:30  MX204-LAB-WZTECH authd[19564]: pool POOL-V6-PD-3 is out of addresses
Sep 12 09:39:30  MX204-LAB-WZTECH authd[19564]: pool POOL-IA_NA-2 is out of addresses
```

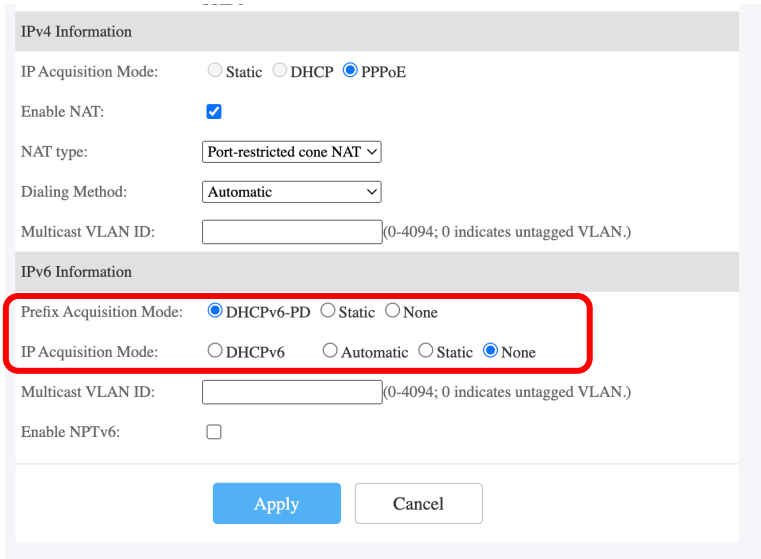
É possível também configurar para que o MX gere trap SNMP no caso de uso do pool IPv6 acima de um determinado threshold:

```
set access address-assignment high-utilization-v6 85
set access address-assignment abated-utilization-v6 75
```

Neste caso se o uso de algum pool IPv6 chegar em 85% de utilização será gerado um trap SNMP e quando a utilização retornar abaixo de 75% será gerado novo trap SNMP.

É possível configurar a ONU para fazer apenas DHCP IA_PD. Neste caso a ONU não vai obter o endereço IPv6 de WAN nem via SLAAC nem via DHCPv6 IA_NA. Ela apenas vai obter o endereço de PD com a requisição DHCPv6 IA_PD.

Exemplo de configuração da ONU para esse cenário:



O endereço de WAN que a ONU alocará neste depende da implementação de firmware da ONU. No caso da ONU que foi utilizada nos testes, esta faz o processo de EUI-64 do MAC Address e reserva estes 64 bits do prefixo para ser o endereço local de WAN e este endereço não vai ser entregue na LAN. Neste modelo de ONU não foi utilizado o Interface-Id para alocar este endereço local.

A ONU recebeu o prefixo 1010:ee4:4000:6::/64:

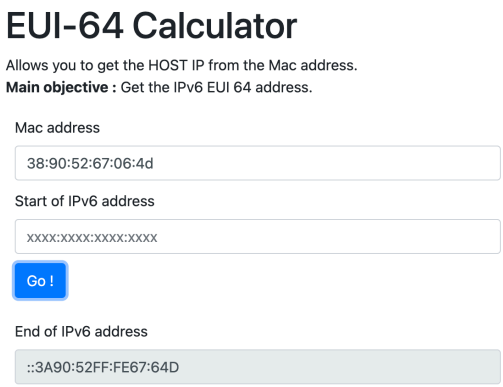
```
admin@MX204-LAB-WZTECH> show dhcpv6 server binding
Prefix                  Session Id  Expires  State    Interface    Client DUID
1010:ee4:4000:6::/64    372         258      BOUND    pp0.3221225614 LL0x1-38:90:52:67:06:4d
```

O MAC Address da ONU é o MAC 38:90:52:67:06:4d:

Quando geramos tráfego a partir da ONU:

```
16:49:16.150630  In IP6 1010:ee4:4000:6:3a90:52ff:fe67:64d > 2008:1212::1: ICMP6, echo request, seq 0, length 64
16:49:16.150775 Out PPPoE  [ses 1]IP6 2008:1212::1 > 1010:ee4:4000:6:3a90:52ff:fe67:64d: [|icmp6]
16:49:17.151219  In IP6 1010:ee4:4000:6:3a90:52ff:fe67:64d > 2008:1212::1: ICMP6, echo request, seq 1, length 64
16:49:17.151376 Out PPPoE  [ses 1]IP6 2008:1212::1 > 1010:ee4:4000:6:3a90:52ff:fe67:64d: [|icmp6]
```

A ONU está saindo com o prefixo PD recebido (64 bits) + EUI-64 do MAC Address (64 bits):



A ferramenta disponível na URL abaixo calcula o EUI-64 a partir de um MAC Address:

https://eui64-calc.princelle.org/

Hold down e Active Drain - DHCPv6

Quando é necessário remover um pool usado pelo protocolo DHCPv4 ou DHCPv6 do BNG e é desejado que esta remoção não gere impacto nos assinantes que estão utilizando este determinado pool existem duas funcionalidades que auxiliam neste cenário:

Hold Down:

```
set access address-assignment pool POOL-IA_NA-1 hold-down
```

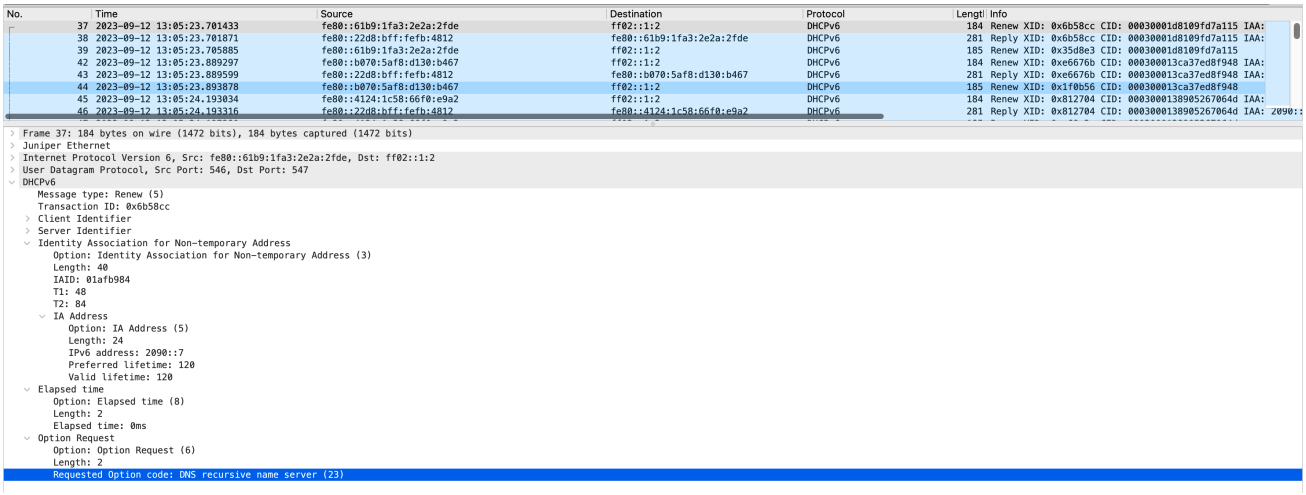
Quando o hold-down é configurado, todos os assinantes que estão conectados fazendo uso deste pool permanecem fazendo uso do mesmo e as mensagens de Renew para renovação do bind já criado continuam sendo respondidas normalmente pelo BNG, porém, este pool não vai aceitar mais nenhuma alocação nova. Para qualquer novo DHCP Solicit ou Rebind o BNG não vai mais considerar este pool e vai procurar outro pool na cadeia de pools. À medida que os assinantes que estão utilizando este pool forem desconectando e conectando eles vão receber endereços IP de outro pool. Desta forma, o pool vai sendo liberado até não ter mais nenhuma conexão.

Active Drain

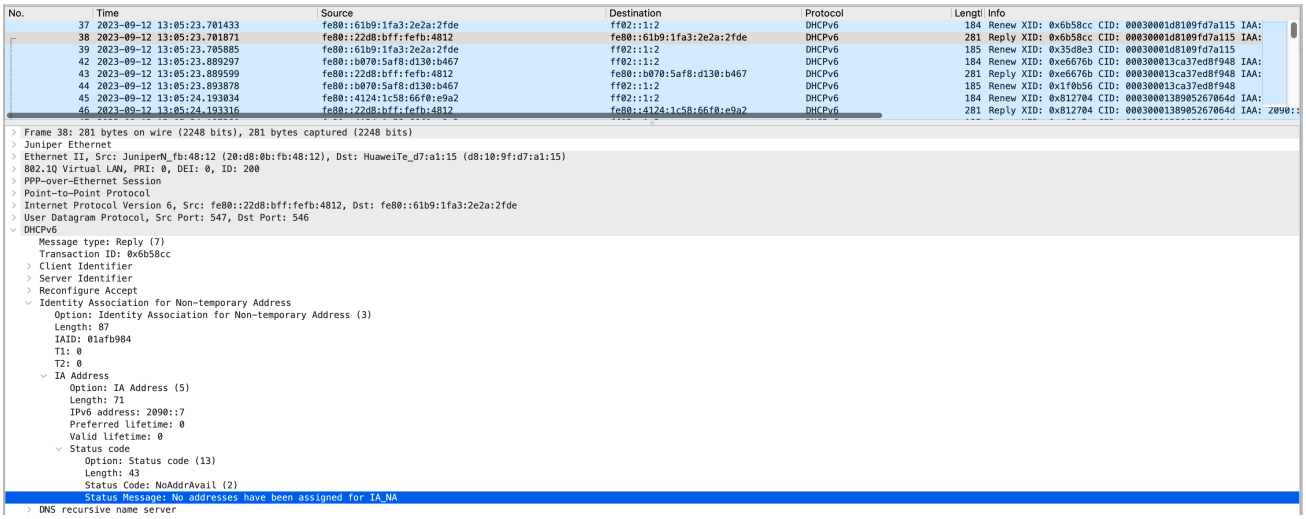
```
set access address-assignment pool POOL-IA_NA-1 active-drain
```

Diferentemente do que acontece com pools IPv4 utilizados pelo PPPoE, o active-drain em pools que estão sendo utilizados pelo protocolo DHCP tem comportamento diferente. O comando active-drain em um pool usado no DHCPv4 ou DHCPv6 faz com que quando a ONU tentar renovar o lease com o Renew o BNG vai rejeitar o Renew informando que o bind não é mais valido e a ONU vai gerar um novo DHCP Solicit. Neste caso, o pool com o comando active-drain não será mais escolhido para entrega de prefixos. O processo de active-drain não é tão abrupto como é o caso de pools IPv4 para o PPPoE. Os usuários continuam funcionando normalmente usando o pool que está com active-drain até que façam o Renew do endereço e neste momento o BNG rejeita o Renew e a ONU vai solicitar um novo prefixo:

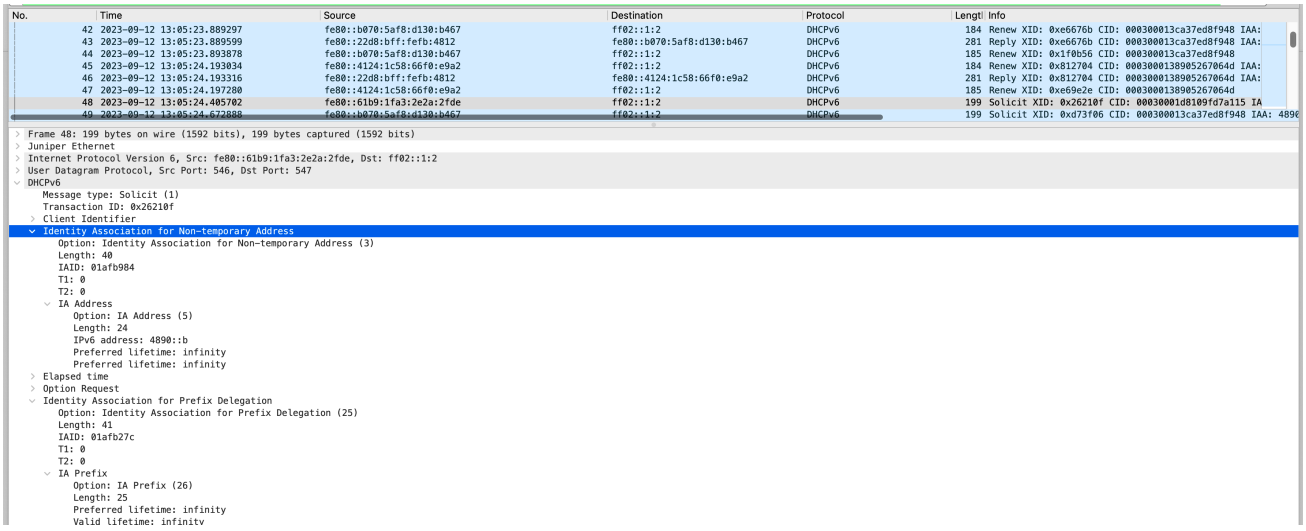
A seguir um exemplo da ONU fazendo o Renew com o pool DHCP configurado com Active Drain:



Resposta do BNG:



BNG informa que o bind não é mais valido. Neste caso a ONU solicita um novo prefixo:



Importante: O uso do active-drain ou hold-down para pools DHCP é muito importante caso vá ser feito a remoção de um pool utilizado pelo protocolo DHCP, pois caso o pool seja deletado com os usuários conectados a sessão PPPoE do usuário vai continuar conectada com o pool IPv4 funcionando porém os prefixos IPv6 deixarão de funcionar pois

todos os bindings serão removidos e só voltarão a funcionar quando a ONU tentar fazer Renew, que pode ser depois de horas ou dias dependendo do tempo máximo do lease entregue. Neste cenário para o usuário obter o IPv6 imediatamente novamente teria que desconectar a sessão PPPoE visto que os endereços estão todos associados à conexão PPPoE.

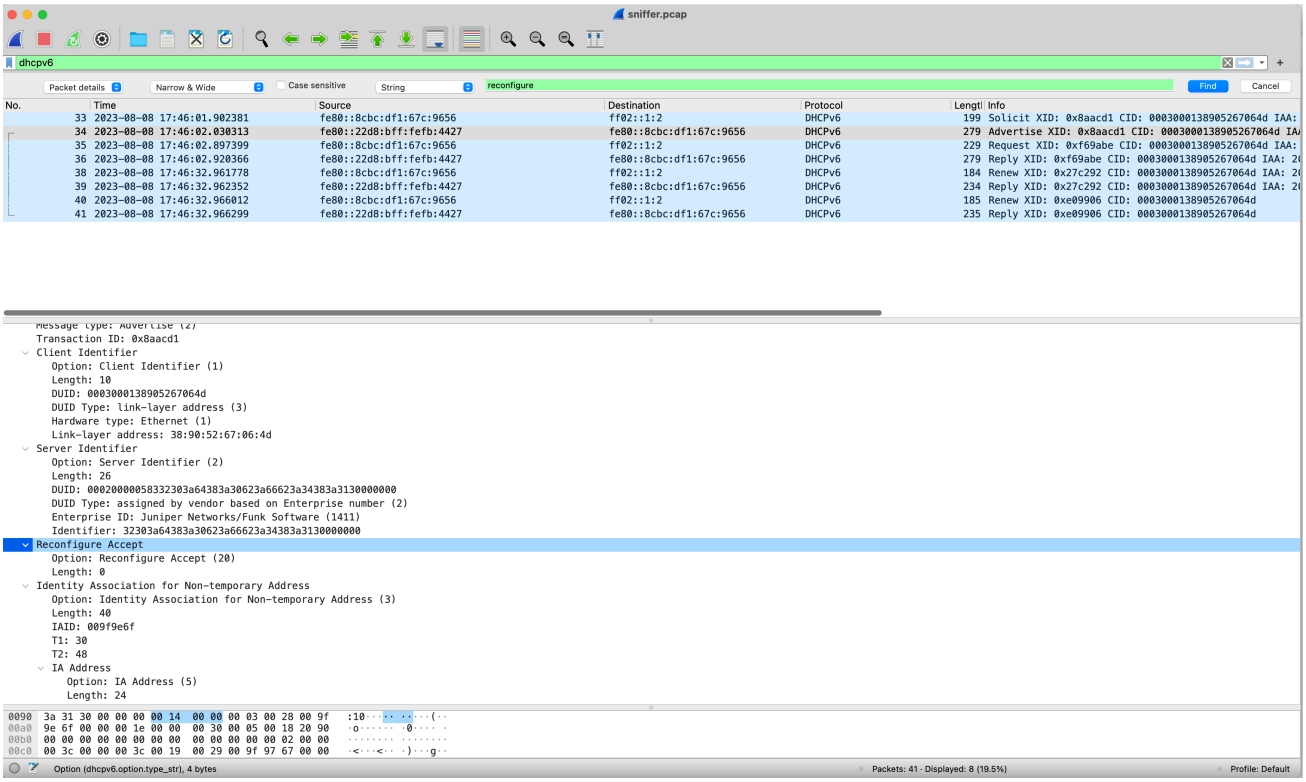
Configurações Opcionais no DHCP Local Server do BNG:

Além das configurações básicas já mencionadas no servidor DHCP Local do BNG algumas configurações opcionais podem ser configuradas:

```
set system services dhcp-local-server dhcpv6 group DHCPV6 reconfigure
```

A opção de "reconfigure" no DHCP Server auxilia a minimizar possíveis impactos caso hajam mudanças no BNG relacionados à configuração de DHCP. Por default o BNG só responde requisições dos usuários, seja DHCP Solicit, Renew ou Rebind. Quando é habilitado o "reconfigure" se houver por exemplo mudança de endereço do pool DHCP o "reconfigure" faz com que o BNG gere mensagens do tipo "forcenew". Se os clientes suportarem o "reconfigure" eles tentarão fazer o renew/rebind do lease DHCP para não ficar com o serviço indisponível. O "reconfigure" depende do cliente DHCP suportar esta funcionalidade. O Reconfigure é informado na negociação do DHCP com a mensagem "Reconfigure Accept".

Nesse caso o BNG está informando que suporta Reconfigure:



A ONU que usamos nos testes não suporta a opção de "Reconfigure".

RFC's relacionadas com esta funcionalidade:

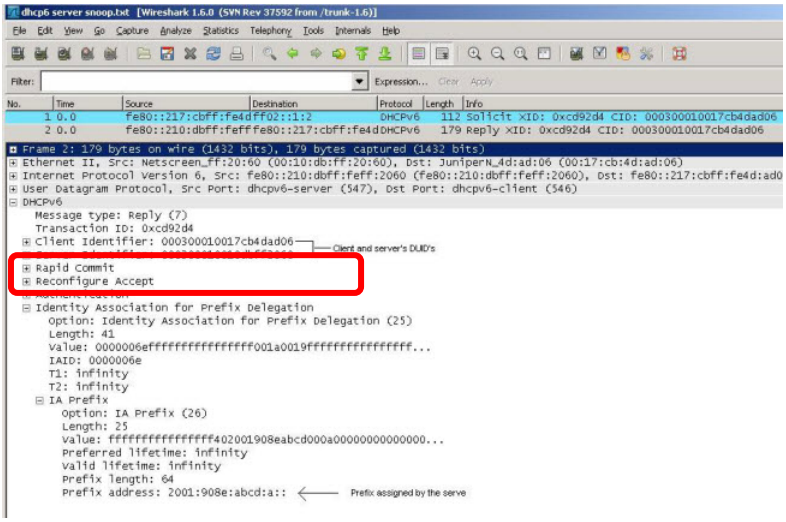
RFC 3203, DHCP Reconfigure Extension for DHCPv4
RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

```
set system services dhcp-local-server dhcpv6 group DHCPV6 overrides rapid-commit
```

Rapid Commit é outra configuração que pode ser habilitada no DHCPv6 server no BNG. Se o BNG e o cliente DHCP suportarem, ao invés da ONU trocar 4 mensagens DHCPv6 com o BNG serão trocadas apenas duas:

Ao invés do SARR (Solicit, Advertise, Request, Reply) as mensagens trocadas são apenas Solicit/Reply:

O cliente DHCP deve sinalizar no DHCP Solicit que suporta rapid-commit:



Obs: Esta é uma captura de um equipamento mostrando que o mesmo suporta "Reconfigure" e "Rapid Commit".

Também é visto que as mensagens de DHCPv6 foram apenas DHCP Solicit e DHCP Reply.

DHCP Lockout ou DHCP Short Cycle Protection

Outra opção que pode ser configurada no servidor DHCP no BNG é o DHCP Short Cycle Protection. O mecanismo é similar à funcionalidade PPPoE Short Cycle Protection, porém, ao invés de ficar detectando eventos de curta duração nos pacotes do protocolo PPPoE o mecanismo fica avaliando comportamentos no protocolo DHCP que podem ser considerados críticos para a Routing Engine como: muitas negociações no DHCP em tempos muito curtos ou muitos eventos de Solicit do mesmo usuário em tempos curtos. Caso o BNG considere o evento perigoso será criado a entrada de lockout para DHCP e será feito o bloqueio do recebimento de qualquer mensagem DHCP no BNG daquele MAC.

O detalhamento do algoritmo e eventos que trigam o mecanismo é detalhado pela Juniper na seguinte URL:

https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-sessions/topics/topic-map/dhcp-short-cycle-protection.html

Por padrão o DHCP Short Cycle Protection não é habilitado. Para ser habilitado ele deve ser configurado com o tempo mínimo e o tempo máximo que um assinante pode ficar bloqueado para envio de pacotes DHCP:

```
set system services dhcp-local-server dhcpv6 group DHCPV6 short-cycle-protection lockout-min-time 2
set system services dhcp-local-server dhcpv6 group DHCPV6 short-cycle-protection lockout-max-time 300
```

Abaixo o comando para ver as entradas de lockout criadas para DHCPv6:

```
admin@MX204-LAB-WZTECH> show dhcpv6 server lockout-entries
Index     Key                          State    Expire(s)  Elapsed(s)    Count
0         default/00 03 00 01 d8 10 9f d7 a1 15/ Grace 177 723       1
1         default/00 03 00 01 3c a3 7e d8 f9 48/ Grace 178 722       1
2         default/00 03 00 01 38 90 52 67 06 4d/ Grace 178 722       1
```

Comando para mostrar os DHCPv6 bindings criados:

```
admin@MX204-LAB-WZTECH> show dhcpv6 server binding
Prefix                  Session Id  Expires  State    Interface    Client DUID
1011:ee4:4000:b::/64    292         86399    BOUND    pp0.3221225711 LL0x1-38:90:52:67:06:4d
1011:ee4:4000:a::/64    293         86399    BOUND    pp0.3221225710 LL0x1-3c:a3:7e:d8:f9:48
```

```
1011:ee4:4000:9::/64    291         86398    BOUND    pp0.3221225709 LL0x1-d8:10:9f:d7:a1:15
```

Comando para filtrar uma entrada de lockout específica de um Cliente DHCP (DUID):

```
admin@MX204-LAB-WZTECH> show dhcpv6 server lockout-entries | match "d8 10 9f d7 a1 15"
0         default/00 03 00 01 d8 10 9f d7 a1 15/ Grace 36 864        1
```

Neste caso há uma entrada criada para o cliente DHCP DUID LL0X1-d8:10:96

Para ver uma entrada de lockout do DHCP com os detalhes é necessário especificar o index da entrada que é o número identificador que fica no início da linha:

```
admin@MX204-LAB-WZTECH> show dhcpv6 server lockout-entries
Index     Key                          State    Exipre(s)  Elapsed(s)    Count
0         default/00 01 00 01 27 66 07 7c 8c 47 be 52 91 fb/ Grace 891 9 1

admin@MX204-LAB-WZTECH> show dhcpv6 server lockout-entries index 0

    Index:                              0
    Lockout count:                      1
    State:                              Grace
    Key:                                default/00 01 00 01 27 66 07 7c 8c 47 be 52 91 fb/
    Expires:                            2023-08-08 09:40:17 -03
    Expires in:                         170
    Min lockout time:                   2
    Next lockout time:                  4
    Lockout reason:                     194
```

Nest caso não há bloqueio pois o State está "Grace".

```
admin@MX204-LAB-WZTECH> show dhcpv6 server lockout-entries index 0

    Index:                              0
    Lockout count:                      6
    State:                              Lockout
    Key:                                default/00 01 00 01 27 66 07 7c 8c 47 be 52 91 fb/
    Expires:                            2023-08-08 09:41:33 -03
    Expires in:                         64
    Min lockout time:                   2
    Next lockout time:                  128
    Lockout reason:                     194
```

Neste caso acima o cliente está bloqueado para fazer DHCP (State: Lockout) e o estado de bloqueio vai expirar em 64 segundos (Expires in: 64). Se houver um próximo bloqueio, este durará 128 segundos (Next lockout time: 128). O tempo de bloqueio é exponencial entre o valor mínimo e o máximo configurado da mesma forma que acontece no PPPoE Short Cycle Protection já detalhado neste documento.

Importante: O Expires in quando o usuário não está bloqueado (State: Grace) fica em 900 segundos (que é o tempo máximo que esta entrada fica ativa no BNG) e vai decrementando desde que não haja um novo evento considerado de risco pelo algoritmo do BNG. Quando chegar em 0 a entrada é removida.

Para limpar um lockout de DHCP:

```
admin@MX204-LAB-WZTECH> clear dhcpv6 server lockout-entries index 0

admin@MX204-LAB-WZTECH> clear dhcpv6 server lockout-entries all
```

Todas as regras e normas para que um CPE IPv6 funcione de forma adequada estão sugeridas no documento disponível no site ipv6ready.org: *https://www.ipv6ready.org/docs/CE_Router_Conformance.pdf*

10.1.4. Address-Protection

```
set access address-protection
```

O mecanismo address-protection não vem ativado por default e pode ser ativado através de um comando global em [access]. Este comando não é obrigatório mas é altamente recomendado. O mecanismo de address-protection serve para evitar duplicação de uso de endereço IPv4 ou IPv6 no BNG.

Sem o address-protection o BNG deixa por exemplo dois dois assinantes se conectarem com o mesmo prefixo enviado pelo RADIUS. Com a configuração de address-protection um próximo usuário que tentar se conectar no BNG com o mesmo endereço de um assinante já conectado não vai ser conseguir.

É possível mudar o comportamento do address-protection para que neste caso de duplicidade de endereço o BNG aceite a nova conexão e desconecte a conexão antiga:

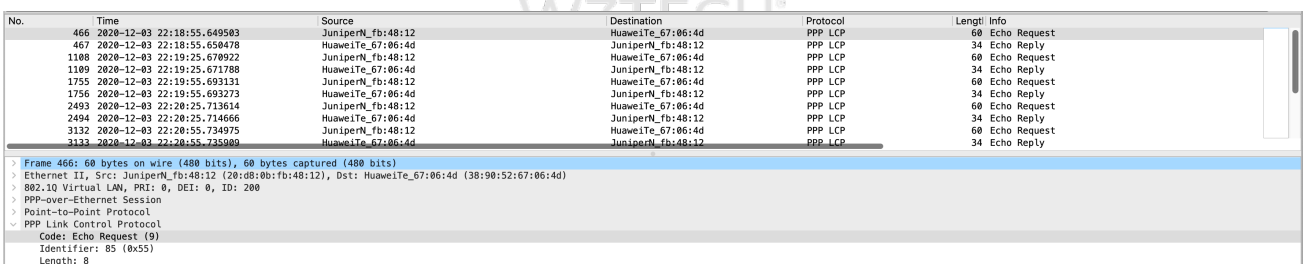
```
set access address-protection reassign-on-match
```

Para prefixos NDRA recebidos do RADIUS o mecanismo address-protection possui as seguintes ações:

- Se o prefixo recebido pelo RADIUS existir em um pool local ele é removido do pool caso esteja disponível
- Se o prefixo já estiver em uso o usuário não conecta

11. PPPoE Keepalive

Por default, na conexão PPPoE o BNG faz um keepalive no protocolo PPP de 30 em 30 segundos para verificar se a ONU está ativa ainda. Os pacotes a seguir foram capturados diretamente na ONU:



Estes keepalive's (LCP Requests) são gerados no BNG pela PFE, bem como a resposta enviada para o BNG também é processada pela PFE (Data Plane). Desta forma não é possível capturar estes pacotes através do comando "monitor traffic" visto que o comando "monitor traffic" vai capturar os pacotes que chegam no control plane (Routing Engine).

Para considerar que a sessão PPPoE caiu o BNG precisa enviar e não receber respostas destes pacotes de keepalive por 3 vezes (down-count = 3) e para considerar que a sessão está UP precisa receber apenas um pacote de keepalive (up-count = 1). Não existe opção para mudar estes valores de down-count ou up-count. É possível apenas ajustar caso seja necessário o intervalo do keepalive gerado pelo BNG. Esta configuração é feita na Subscriber Profile:

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" keepalives interval 50
```

Na configuração acima está sendo alterado o tempo do keepalive no BNG para o intervalo de 50 segundos. Qualquer valor configurado maior que 600 segundos é aceito pela CLI mas é aplicado 600 segundos na PFE (Packet Fowarding Engine).

12. Limite da Quantidade de Conexões PPPoE no BNG

Já foi mostrado neste documento a funcionalidade onde o BNG faz o controle de login simultâneo. Neste caso, o controle é feito dentro da access profile controla a quantidade de conexões com o mesmo login (usuário PPPoE).

É possível também limitar a quantidade de conexões PPPoE que podem ser criadas na interface VLAN assinante. Esta configuração pode ser aplicada em alguns lugares diferentes no JunOS e geralmente é feito na VLAN Profile:

```
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe max-sessions 1
```

Outra opção é enviar o AVP ERX-Max-Clients-Per-Interface (Vendor 4874 / Atributo 143) através do protocolo RADIUS:

```
wztech3  Cleartext-Password := "wztech3"
         ERX-Max-Clients-Per-Interface = 1
```

É possível configurar o BNG para que ele não aceite que o RADIUS envie este atributo fazendo esta modificação nas interfaces L2. Desta forma o AVP vindo do RADIUS não terá efeito nenhum no BNG:

```
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe max-sessions-vsa-ignore
```

A interface pp0.<unit> (PPPoE) do usuário se ancora (Underlying-Interface) na interface demux0.<unit> que é a interface Layer 2:

```
admin@MX204-LAB-WZTECH> show subscribers user-name wztech3 extensive
Type: PPPoE
User Name: wztech3
IP Address: 192.168.60.113
IP Netmask: 255.255.255.255
IPv6 Prefix: 1011:ee4:4000:31::/64
Domain name server inet6: 2070::1 2070::2
IPv6 User Prefix: 2904:ee4:8000:2f::/64
Logical System: default
Routing Instance: default
Interface: pp0.3221225795
Interface type: Dynamic
Underlying Interface: demux0.3221225794
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 3
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 396
Session ID: 396
PFE Flow ID: 413
VLAN Id: 200
Login Time: 2023-09-12 18:06:29 -03
IP Address Pool: POOL-IP-06
IPv6 Address Pool: POOL-V6-NDRA-1
IPv6 Delegated Address Pool: POOL-V6-PD-2
IPv6 Framed Interface Id: d23:493b:d93e:49c4
IPv4 Input Filter Name: 100M-IPV4-IN-pp0.3221225795-in
IPv4 Output Filter Name: 100M-IPV4-OUT-pp0.3221225795-out
IPv6 Input Filter Name: 100M-IPV6-IN-pp0.3221225795-in
IPv6 Output Filter Name: 100M-IPV6-OUT-pp0.3221225795-out
Accounting interval: 0
Dynamic configuration:
  junos-input-filter: 100M-IPV4-IN
  junos-input-ipv6-filter: 100M-IPV6-IN
  junos-ipv6-ndra-prefix: 2904:ee4:8000:2f::/64
  junos-output-filter: 100M-IPV4-OUT
  junos-output-ipv6-filter: 100M-IPV6-OUT
```

A interface demux0.<unit> que é a interface L2 se ancora (Underlying-Interface) na interface física (et, xe, ae, etc...):

```
admin@MX204-LAB-WZTECH> show interfaces demux0.3221225794
  Logical interface demux0.3221225794 (Index 536871323) (SNMP ifIndex 200000411)
    Flags: Up VLAN-Tag [ 0x8100.200 ]  Encapsulation: ENET2
    Demux:
      Underlying interface: ae0 (Index 130)
    Link:
```

```
      xe-0/1/0
      xe-0/1/2
    Bandwidth: 0
    Input packets : 279
    Output packets: 145
    Protocol pppoe
      Dynamic Profile: SUBSCRIBER-PROFILE,
      Service Name Table: None,
      Max Sessions: 32000, Max Sessions VSA Ignore: Off,
      Duplicate Protection: Off, Short Cycle Protection: mac-address,
      Direct Connect: Off,
      AC Name: CONCENTRADOR-PPPOE
      Addresses
```

Este controle de sessões é ativado na interface L2.

No exemplo abaixo temos duas conexões PPPoE chegando no BNG pela SVLAN 200:

```
admin@MX204-LAB-WZTECH> show subscribers vlan-id 200
Interface                   IP Address/VLAN ID                  User Name                       LS:RI
pp0.3221225796              192.168.60.114                      wztech2                   default:default
*                           1011:ee4:4000:32::/64
*                           2904:ee4:8000:30::/64
pp0.3221225795              192.168.60.113                      wztech3                   default:default
*                           1011:ee4:4000:31::/64
*                           2904:ee4:8000:2f::/64
demux0.3221225794            200                                                          default:default
```

Como é criada apenas uma interface demux0.<unit> por SVLAN ou SVLAN+CVLAN todos os usuários estão ancorados na mesma interface demux0.3221225794:

```
admin@MX204-LAB-WZTECH> show subscribers client-type pppoe vlan-id 200 extensive | match "User Name|Under"
User Name: wztech3
Underlying Interface: demux0.3221225794
User Name: wztech2
Underlying Interface: demux0.3221225794
```

O limite de sessões é ativado em cima da interface L2. Por default o BNG ativa o limite de conexões por interface demux0.<unit> em 32.000:

```
admin@MX204-LAB-WZTECH> show interfaces demux0.3221225794
  Logical interface demux0.3221225794 (Index 536871323) (SNMP ifIndex 200000411)
    Flags: Up VLAN-Tag [ 0x8100.200 ]  Encapsulation: ENET2
    Demux:
      Underlying interface: ae0 (Index 130)
    Link:
      xe-0/1/0
      xe-0/1/2
    Bandwidth: 0
    Input packets : 541
    Output packets: 411
    Protocol pppoe
      Dynamic Profile: SUBSCRIBER-PROFILE,
      Service Name Table: None,
      Max Sessions: 32000, Max Sessions VSA Ignore: Off,
      Duplicate Protection: Off, Short Cycle Protection: mac-address,
      Direct Connect: Off,
      AC Name: CONCENTRADOR-PPPOE
      Addresses
```

```
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe max-sessions 1
```

A partir do momento que é configurado manualmente o max-sessions na VLAN Profile esta configuração só vai valer na interface demux0.<unit> a partir do momento que a interface demux0.<unit> for criada novamente. Neste caso é necessário que todos os usuários sejam desconectados. A configuração de "versioning" neste caso não vai ajudar pois é necessário que a interface seja criada novamente.

Após os usuários se desconectarem e a interface L2 ser criada novamente será mostrado o Max Sessions com o valor novo configurado:

```
admin@MX204-LAB-WZTECH> show interfaces demux0.3221225806
  Logical interface demux0.3221225806 (Index 536871336) (SNMP ifIndex 200000424)
    Flags: Up VLAN-Tag [ 0x8100.200 ]  Encapsulation: ENET2
```

```
    Demux:
      Underlying interface: ae0 (Index 130)
    Link:
      xe-0/1/0
      xe-0/1/2
    Bandwidth: 0
    Input packets : 27
    Output packets: 16
    Protocol pppoe
      Dynamic Profile: SUBSCRIBER-PROFILE,
      Service Name Table: None,
      Max Sessions: 1, Max Sessions VSA Ignore: Off,
      Duplicate Protection: Off, Short Cycle Protection: mac-address,
      Direct Connect: Off,
      AC Name: CONCENTRADOR-PPPOE
      Addresses
```

Outra forma de alterar o limite de sessões por interface L2 é através do protocolo RADIUS. Caso exista a configuração local no BNG e também no RADIUS o RADIUS tem precedência.

No caso do protocolo RADIUS não é necessário que os assinantes que estão fazendo uso da interface demux0.<unit> se desconectem para que o AVP tenha efeito. A partir do momento que um assinante da SVLAN ou CLAN+SVLAN se conectar e o RADIUS enviar o atributo ERX-Max-Clients-Per-Interface este atributo vai modificar a quantidade máxima de sessões da interface demux0.<unit> instantaneamente.

Exemplo:

Temos dois assinantes conectados na SVLAN 200 e logo os dois assinantes estão fazendo uso da mesma interface demux0.<unit>:

```
admin@MX204-LAB-WZTECH> show subscribers client-type pppoe vlan-id 200 extensive | match "User Name|Under"
User Name: wztech2
Underlying Interface: demux0.3221225823
User Name: wztech3
Underlying Interface: demux0.3221225823
```


Não há nenhuma configuração de max-sessions localmente no BNG logo a interface demux0.3221225823 tem o limite de 32.000 sessões:

```
admin@MX204-LAB-WZTECH> show interfaces demux0.3221225823
  Logical interface demux0.3221225823 (Index 536871353) (SNMP ifIndex 200000441)
    Flags: Up VLAN-Tag [ 0x8100.200 ]  Encapsulation: ENET2
    Demux:
      Underlying interface: ae0 (Index 130)
    Link:
      xe-0/1/0
      xe-0/1/2
    Bandwidth: 0
    Input packets : 402
    Output packets: 260
    Protocol pppoe
      Dynamic Profile: SUBSCRIBER-PROFILE,
      Service Name Table: None,
      Max Sessions: 32000, Max Sessions VSA Ignore: Off,
      Duplicate Protection: Off, Short Cycle Protection: mac-address,
      Direct Connect: Off,
      AC Name: CONCENTRADOR-PPPOE
      Addresses

admin@MX204-LAB-WZTECH> show pppoe underlying-interfaces demux0.3221225823
demux0.3221225823 Index 536871353
  State: Dynamic, Dynamic Profile: SUBSCRIBER-PROFILE,
  Max Sessions: 32000, Max Sessions VSA Ignore: Off,
  Active Sessions: 2,
  Service Name Table: None,
  Duplicate Protection: Off, Short Cycle Protection: mac-address,
  Direct Connect: Off,
  AC Name: CONCENTRADOR-PPPOE,
```

A partir do momento que um terceiro assinante (wztech4) conecta e o RADIUS envia o AVP ERX-Max-Clients-Per-Interface = 1 o controle de sessões para a interface demux0.<unit>, ou seja, a VLAN 200 passa a ser 1:

RADIUS:

(0) Sent Access-Accept Id 1 from 192.168.1.236:1812 to 192.168.1.248:56458 length 0
(0) ERX-Max-Clients-Per-Interface = 1

```
admin@MX204-LAB-WZTECH> show interfaces demux0.3221225823
  Logical interface demux0.3221225823 (Index 536871353) (SNMP ifIndex 200000441)
    Flags: Up VLAN-Tag [ 0x8100.200 ]  Encapsulation: ENET2
    Demux:
      Underlying interface: ae0 (Index 130)
    Link:
      xe-0/1/0
      xe-0/1/2
    Bandwidth: 0
    Input packets : 883
    Output packets: 726
    Protocol pppoe
      Dynamic Profile: SUBSCRIBER-PROFILE,
      Service Name Table: None,
      Max Sessions: 32000, Max Sessions VSA Ignore: Off,
      Duplicate Protection: Off, Short Cycle Protection: mac-address,
      Direct Connect: Off,
      AC Name: CONCENTRADOR-PPPOE
      Addresses
```

```
admin@MX204-LAB-WZTECH> show pppoe underlying-interfaces demux0.3221225823
demux0.3221225823 Index 536871353
  State: Dynamic, Dynamic Profile: SUBSCRIBER-PROFILE,
  Max Sessions: 1, Max Sessions VSA Ignore: Off,
  Active Sessions: 2,
  Service Name Table: None,
  Duplicate Protection: Off, Short Cycle Protection: mac-address,
  Direct Connect: Off,
  AC Name: CONCENTRADOR-PPPOE,
```

Importante: O comando "show interfaces demux0.<unit>" continua mostrando o valor máximo. No caso do envio do atributo pelo protocolo RADIUS ele é refletido apenas no output do comando "show pppoe underlying-interfaces demux0.<unit>". Neste caso a interface demux0.3221225823 teve o limite de sessões alterado para 1.

Importante: As conexões ativas na interface demux0.<unit> não são removidas quando o valor ativado pelo protocolo RADIUS é menor do que a quantidade de conexões atuais ancoradas nesta interface, porém não é aceito nenhuma conexão nova (inclusive a própria conexão que ativou o parâmetro no BNG) até que estas conexões estejam dentro do limite da interface demux0.<unit>.

No modelo CVLAN já que cada assinante possui um par de VLAN's (Outer + Inner), limitar a quantidade de conexões em 1 é comum e recomendado visto que neste cenário cada interface pp0.<unit> terá a sua interface demux0.<unit>.

Se a configuração da VLAN Profile estiver usando o modelo de configuração com a variável $junos-interface-ifd-name no nome da interface ao invés da interface demux0 o BNG vai criar uma interface Layer 2 associada à interface física para cada SVLAN ou SVLAN+CVLAN. Exemplo:

```
admin@MX204-LAB-WZTECH> show subscribers
Interface                   IP Address/VLAN ID                User Name                LS:RI
xe-0/1/0.3221225900          200                                                       default:default
pp0.3221225901              192.168.4.51                      wztech2                  default:default
pp0.3221225902              192.168.4.52                      wztech2                  default:default
```

Neste caso, os controles de max-sessions serão feitos nas interfaces Layer2 associadas à interface física. Caso a mesma SVLAN seja utilizada em interfaces físicas distintas cada interface física terá o seu controle separado. Este modelo de configuração não é recomendado. É recomendado o uso da interface demux0.

13. SNMP para Interfaces PPPoE:

Por padrão o MX não faz as coletas internamente de SNMP para os assinantes PPPoE. O comportamento padrão do JunOS é não ativar MIB SNMP para a interface pp0 e nem para a interface demux0. Desta forma, por padrão não é possível coletar dados como bytes, pacotes e outros contadores das interfaces demux0 e pp0.

Caso haja necessidade de obter informações de bytes e pacotes nas interfaces demux0 ou pp0 é necessário ativar a configuração de interface-mib.

Se for configurado o interface-mib na VLAN Profile as interfaces demux dos usuarios aparecerão na consulta SNMP e será contabilizado todos os pacotes e bytes das interfaces demux0.<unit>:

```
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 interface-mib
```

Caso haja necessidade de contabilizar pacotes e bytes nas interfaces pp0 dos assinantes é necessário ativar o interface-mib na Subscriber Profile:

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 interface-mib
```

Caso o interface-mib seja ativado na VLAN Profile e na Subscriber Profile o BNG vai disponibilizar as informações de bytes e pacotes tanto da interface demux0 quanto da interface pp0 do assinante.

O comportamento do MX por default é NÃO gerar traps SNMP quando as interfaces demux0 e pp0 dos assinantes ficam UP e Down. Caso queira deixar explícito esta configuração:

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" no-traps
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" no-traps
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" no-traps
```

Caso por algum motivo específico seja necessário gerar traps SNMP para estas interfaces é necessário configurar:

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" traps
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" traps
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" traps
```

Importante: A configuração de traps só funciona em conjunto com a configuração de interface-mib.

Por padrão, o BNG vai logar as traps SNMP no arquivo messages. Caso seja necessário o envio das trap's SNMP para um servidor externo:

```
set snmp trap-group SERVIDORSNMPTRAP version v2
set snmp trap-group SERVIDORSNMPTRAP targets 172.17.17.2
```

Caso exista a configuração de interface-mib na VLAN Profile e/ou Subscriber Profile o BNG vai disponibilizar todos os contadores por interface (pp0.<unit> ou demux0.<unit>) e na árvore de interfaces quando for feito o SNMP Walk no BNG vai aparecer todas estas interfaces:

```
admin@MX204-LAB-WZTECH> show snmp mib walk ifEntry | match "pp|demux"
ifDescr.507   = pp0
ifDescr.519   = demux0
ifDescr.564   = demux0.2147483718
ifDescr.200000507 = demux0.3221225881
ifDescr.200000509 = pp0.3221225882
ifDescr.200000510 = pp0.3221225883
ifDescr.200000511 = pp0.3221225884
```

É possível configurar no BNG filtro para que algumas interfaces sejam removidas do SNMP Walk:

`set snmp filter-interfaces interfaces pp0*` - Tira todas as interfaces pp0.<unit> do SNMP
`set snmp filter-interfaces interfaces demux0*` - Tira todas as interfaces demux0.<unit> do SNMP
`set snmp filter-interfaces all-internal-interfaces` - Tira todas as interfaces internas usadas pelo MX para comunicações internas do SNMP

Lembrando que neste modelo de filtro de interfaces, de todas as formas, com a configuração de interface-mib feita no BNG a caixa vai criar estas interfaces internamente e vai popular os dados. O comando de filter-interfaces apenas está filtrando estas interfaces para elas não sejam disponibilizados no protocolo SNMP. Para o BNG não ficar gerando a informação internamente a configuração de interface-mib não pode ser habilitada.

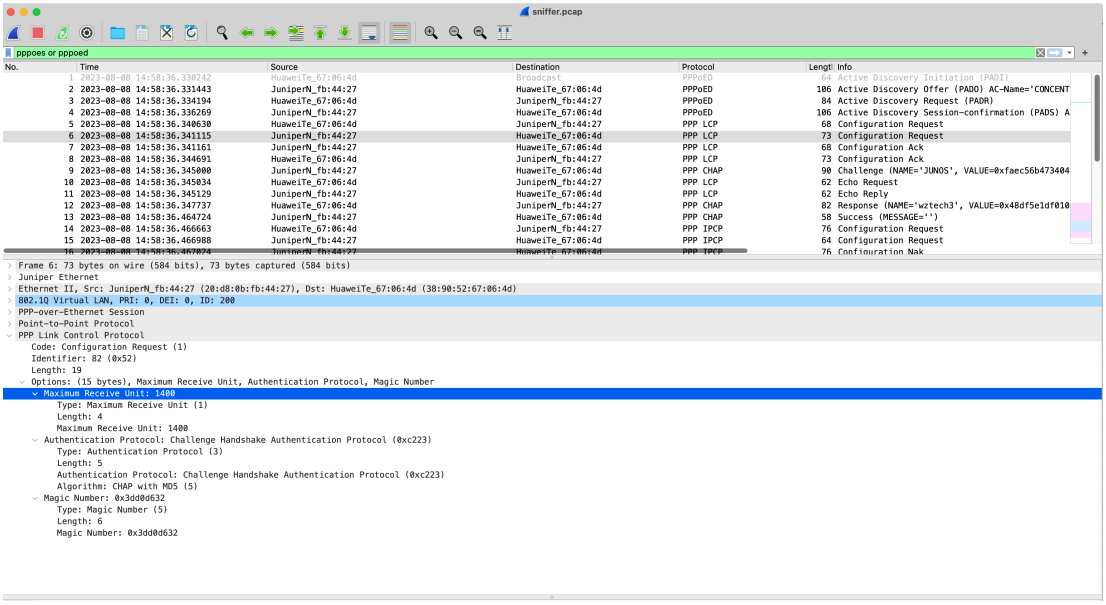
14. Ajuste de MTU/MRU e TCP MSS

No protocolo PPPoE dentro do protocolo PPP LCP é informado entre a ONU e o BNG o tamanho máximo de Payload do protocolo PPP (MRU: Maximum Receive Unit). Por default o BNG negocia este valor de MRU em 1492 bytes. Este valor de 1492 é 1500 bytes do padrão Ethernet menos 6 bytes do cabeçalho PPPoE menos 2 bytes do protocolo PPP. A ONU geralmente também negocia um valor de MRU de 1492. O menor valor entre os lados vai prevalecer deve prevalecer entre as partes.

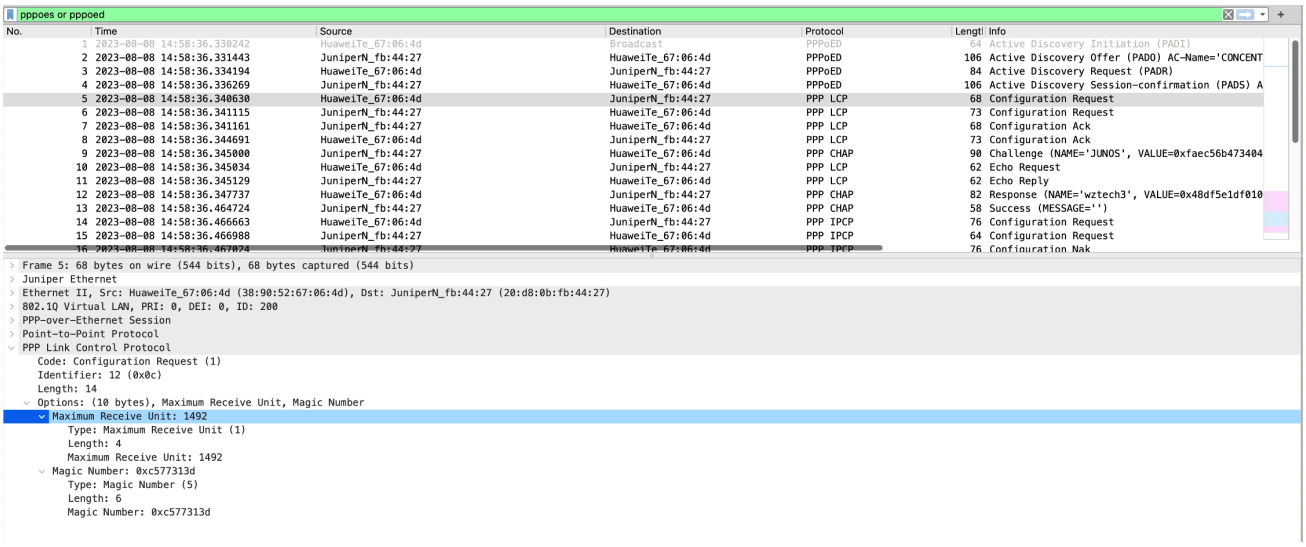
É possível mudar este valor no BNG configurando o MRU ou o MTU dentro da Subscriber Profile. Ambas as configurações geram o mesmo efeito:

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" ppp-options mru 1400
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" ppp-options mtu 1400
```

A seguir o MRU informado pelo BNG à ONU:



A seguir o MRU informado pela ONU ao BNG:



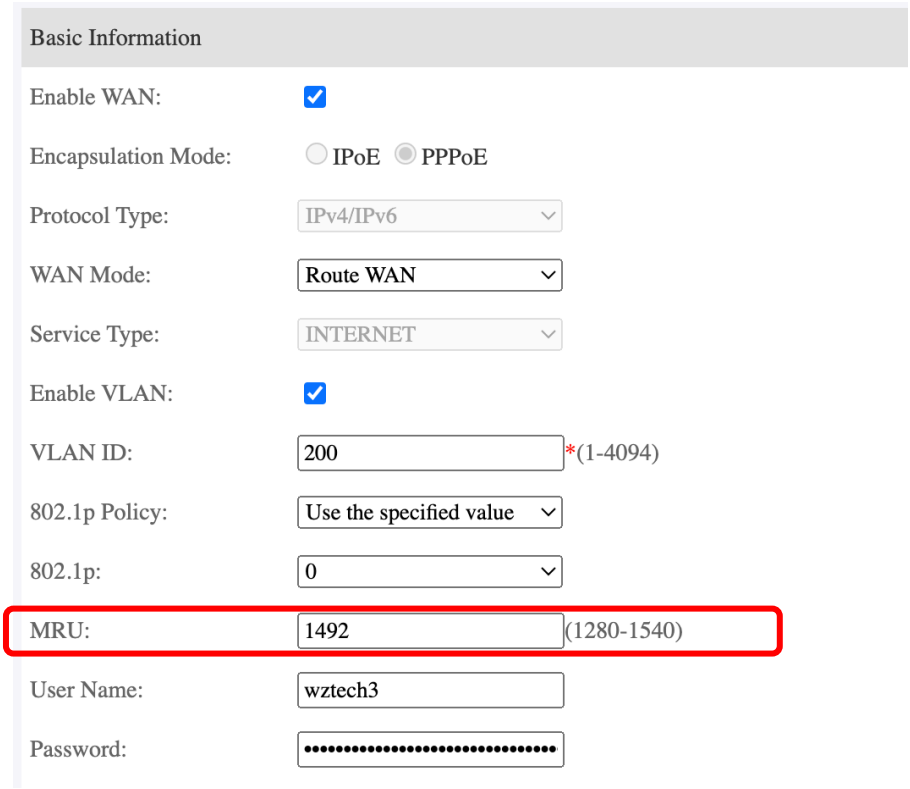
Deve ser utilizado na comunicação o menor valor de MRU.

Como o MRU é o tamanho máximo de Payload que pode ser transportado no protocolo PPP o TCP MSS no BNG e na ONU é ajustado baseado neste menor valor. A ONU utilizada nos testes negocia o TCP MSS sendo 60 bytes a menos que o menor valor de MRU.

12:11:23.452262 IP 192.168.4.29.56210 > 172.17.17.2.24: Flags [S], seq 2433292295, win 64240, options [mss 1340,nop,wscale 8,nop,nop,sackOK], length 0
12:11:23.452272 IP 172.17.17.2.24 > 192.168.4.29.56210: Flags [R.], seq 0, ack 1, win 0, length 0

Importante: Se for configurado um valor de PPP MRU ou PPP MTU fora do range que a ONU pode não conectar no protocolo PPPoE.

A ONU utilizada nos testes aceita o range de 1280 a 1540 para MRU:



No caso do envio de um valor de 1000 de MRU por parte do BNG a ONU gera um Terminate na negociação do protocolo PPPoE.

Caso não seja possível ajustar os valores de tamanho de pacotes no protocolo PPP pode-se mudar o TCP MSS para IPv4 (inet) e IPv6 (inet6) no BNG. Caso o valor do TCP MSS configurado no BNG seja maior que o TCP MSS calculado pela ONU em virtude do MRU, vai prevalecer o MSS calculado pela ONU.

A configuração de TCP MSS no BNG é feita na Subscriber Profile em cada família de protocolos (inet para IPV4 e inet6 para IPv6):

```
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet tcp-mss 1300
set dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 tcp-mss 1300
```

INET:

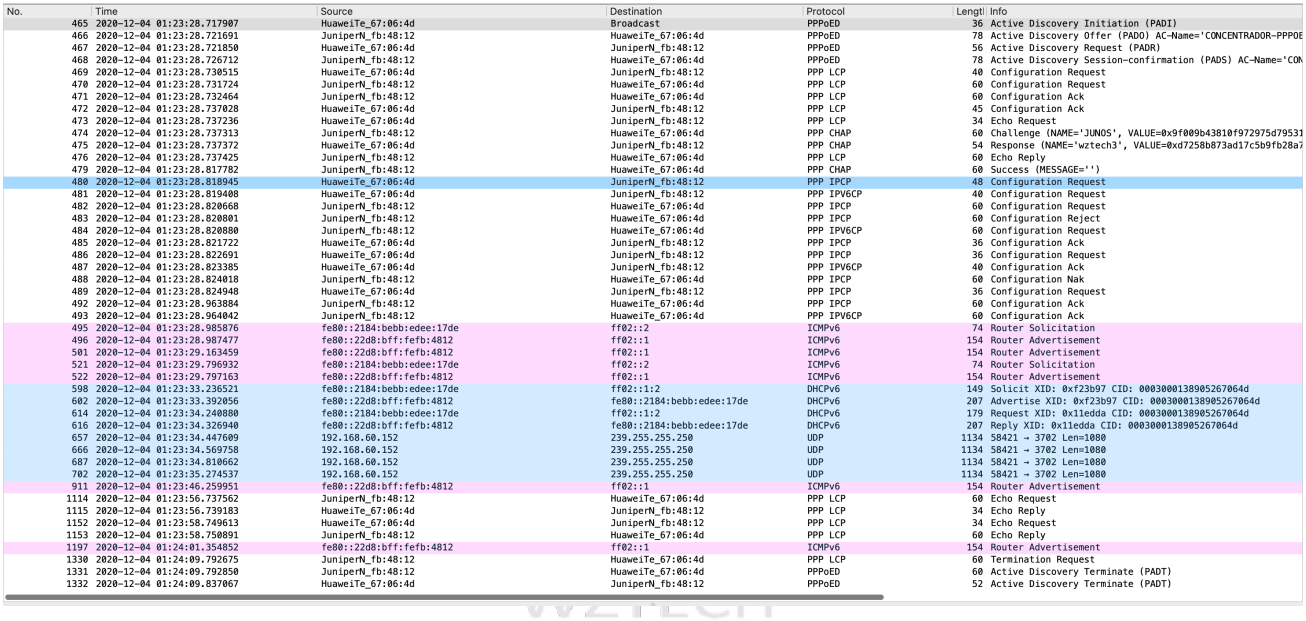
18:41:03.592515 IP 192.168.4.24.52897 > 172.17.17.2.24: Flags [S], seq 3087622203, win 64800, options [mss 1300,nop,wscale 8,nop,nop,sackOK], length 0
18:41:03.592544 IP 172.17.17.2.24 > 192.168.4.24.52897: Flags [R.], seq 0, ack 3087622204, win 0, length 0

INET6:

18:53:26.148732 IP6 2804:ee4:8000:1b:6c91:c40:2a96:10ff.59400 > 2008:1212::2.24: Flags [S], seq 2430542446, win 65320, options [mss 1300,nop,wscale 8,nop,nop,sackOK], length 0
18:53:26.148743 IP6 2008:1212::2.24 > 2804:ee4:8000:1b:6c91:c40:2a96:10ff.59400: Flags [R.], seq 0, ack 1, win 0, length 0

15. PADO Delay

Antes de falarmos do PADO Delay será mostrado o fluxo de uma conexão PPPoE:



No.	Time	Source	Destination	Protocol	Lengt	Info
465	2020-12-04 01:23:28.717907	HuaweiTe_67:06:4d	Broadcast	PPPoED	36	Active Discovery Initiation (PADI)
466	2020-12-04 01:23:28.721691	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPPoED	78	Active Discovery Offer (PADO) AC-Name='CONCENTRADOR-PPPOE
467	2020-12-04 01:23:28.721850	HuaweiTe_67:06:4d	JuniperN_fb:48:12	PPPoED	56	Active Discovery Request (PADR)
468	2020-12-04 01:23:28.726712	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPPoED	78	Active Discovery Session-confirmation (PADS) AC-Name='CON
469	2020-12-04 01:23:28.730515	HuaweiTe_67:06:4d	JuniperN_fb:48:12	PPP LCP	40	Configuration Request
470	2020-12-04 01:23:28.731724	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPP LCP	60	Configuration Request
471	2020-12-04 01:23:28.732464	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPP LCP	60	Configuration Ack
472	2020-12-04 01:23:28.737028	HuaweiTe_67:06:4d	JuniperN_fb:48:12	PPP LCP	45	Configuration Ack
473	2020-12-04 01:23:28.737236	HuaweiTe_67:06:4d	JuniperN_fb:48:12	PPP LCP	34	Echo Request
474	2020-12-04 01:23:28.737313	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPP CHAP	60	Challenge (NAME='JUNOS', VALUE=0x9f009b43810f972975d79531
475	2020-12-04 01:23:28.737372	HuaweiTe_67:06:4d	JuniperN_fb:48:12	PPP CHAP	54	Response (NAME='wztech3', VALUE=0xd7258b873ad17c5b9fb28a7
476	2020-12-04 01:23:28.737425	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPP LCP	60	Echo Reply
479	2020-12-04 01:23:28.817782	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPP CHAP	60	Success (MESSAGE='')
480	2020-12-04 01:23:28.818945	HuaweiTe_67:06:4d	JuniperN_fb:48:12	PPP IPCP	48	Configuration Request
481	2020-12-04 01:23:28.819408	HuaweiTe_67:06:4d	JuniperN_fb:48:12	PPP IPV6CP	40	Configuration Request
482	2020-12-04 01:23:28.820668	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPP IPCP	60	Configuration Request
483	2020-12-04 01:23:28.820801	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPP IPCP	60	Configuration Reject
484	2020-12-04 01:23:28.820880	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPP IPV6CP	60	Configuration Request
485	2020-12-04 01:23:28.821722	HuaweiTe_67:06:4d	JuniperN_fb:48:12	PPP IPCP	36	Configuration Ack
486	2020-12-04 01:23:28.822691	HuaweiTe_67:06:4d	JuniperN_fb:48:12	PPP IPCP	36	Configuration Request
487	2020-12-04 01:23:28.823385	HuaweiTe_67:06:4d	JuniperN_fb:48:12	PPP IPV6CP	40	Configuration Ack
488	2020-12-04 01:23:28.824018	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPP IPCP	60	Configuration Nak
489	2020-12-04 01:23:28.824948	HuaweiTe_67:06:4d	JuniperN_fb:48:12	PPP IPCP	36	Configuration Request
492	2020-12-04 01:23:28.963884	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPP IPCP	60	Configuration Ack
493	2020-12-04 01:23:28.964042	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPP IPV6CP	60	Configuration Ack
495	2020-12-04 01:23:28.985876	fe80::2184:bebb:edee:17de	ff02::2	ICMPv6	74	Router Solicitation
496	2020-12-04 01:23:28.987477	fe80::22d8:bff:fefb:4812	ff02::1	ICMPv6	154	Router Advertisement
501	2020-12-04 01:23:29.163459	fe80::22d8:bff:fefb:4812	ff02::1	ICMPv6	154	Router Advertisement
521	2020-12-04 01:23:29.796932	fe80::2184:bebb:edee:17de	ff02::2	ICMPv6	74	Router Solicitation
522	2020-12-04 01:23:29.797163	fe80::22d8:bff:fefb:4812	ff02::1	ICMPv6	154	Router Advertisement
598	2020-12-04 01:23:33.236521	fe80::2184:bebb:edee:17de	ff02::1:2	DHCPv6	149	Solicit XID: 0xf23b97 CID: 000300013890526706 4d
602	2020-12-04 01:23:33.392056	fe80::22d8:bff:fefb:4812	fe80::2184:bebb:edee:17de	DHCPv6	207	Advertise XID: 0xf23b97 CID: 000300013890526706 4d
614	2020-12-04 01:23:34.240880	fe80::2184:bebb:edee:17de	ff02::1:2	DHCPv6	179	Request XID: 0x11edda CID: 000300013890526706 4d
616	2020-12-04 01:23:34.326940	fe80::22d8:bff:fefb:4812	fe80::2184:bebb:edee:17de	DHCPv6	207	Reply XID: 0x11edda CID: 000300013890526706 4d
657	2020-12-04 01:23:34.447609	192.168.60.152	239.255.255.250	UDP	1134	58421 → 3702 Len=1080
666	2020-12-04 01:23:34.569758	192.168.60.152	239.255.255.250	UDP	1134	58421 → 3702 Len=1080
687	2020-12-04 01:23:34.810662	192.168.60.152	239.255.255.250	UDP	1134	58421 → 3702 Len=1080
702	2020-12-04 01:23:35.274537	192.168.60.152	239.255.255.250	UDP	1134	58421 → 3702 Len=1080
911	2020-12-04 01:23:46.259951	fe80::22d8:bff:fefb:4812	ff02::1	ICMPv6	154	Router Advertisement
1114	2020-12-04 01:23:56.737562	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPP LCP	60	Echo Request
1115	2020-12-04 01:23:56.739183	HuaweiTe_67:06:4d	JuniperN_fb:48:12	PPP LCP	34	Echo Reply
1152	2020-12-04 01:23:58.749613	HuaweiTe_67:06:4d	JuniperN_fb:48:12	PPP LCP	34	Echo Request
1153	2020-12-04 01:23:58.750891	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPP LCP	60	Echo Reply
1197	2020-12-04 01:24:01.354852	fe80::22d8:bff:fefb:4812	ff02::1	ICMPv6	154	Router Advertisement
1330	2020-12-04 01:24:09.792675	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPP LCP	60	Termination Request
1331	2020-12-04 01:24:09.792850	JuniperN_fb:48:12	HuaweiTe_67:06:4d	PPPoED	60	Active Discovery Terminate (PADT)
1332	2020-12-04 01:24:09.837067	HuaweiTe_67:06:4d	JuniperN_fb:48:12	PPPoED	52	Active Discovery Terminate (PADT)

1. Cliente PPPoE (geralmente a ONU) vai conectar na rede e envia uma mensagem de PPPoE PADI para toda a rede (MAC de Broadcast ff:ff:ff:ff:ff:ff) procurando por concentradores PPPoE ativos: Pacote 465.

2. Os concentradores PPPoE ativos na rede que recebem o PADI devolvem um PADO para o cliente. Neste caso é pacote Unicast onde o MAC de destino é o cliente: Pacote 466

3. O cliente envia um PADR Unicast para o MAC Address do concentrador informando que vai estabelecer a conexão PPPoE com este concentrador: Pacote 467

4. O concentrador confirma a conexão através do pacote PADS Unicast para o cliente: Pacote 468

5. A partir deste momento são negociados parâmetros no protocolo PPP como MRU, Protocolo de autenticação (PAP, CHAP) nos pacotes de PPP LCP: Pacotes 469 a 473

6. Em seguida é feito a autenticação no protocolo PPP (CHAP ou PAP): Pacotes 474 a 479

7. Depois são negociados os endereços e DNS IPv4 nas mensagens PPP IPCP e o prefixo IPv6 NDRA e DNS IPv6 NDRA nas mensagens PPP IPV6CP: Pacotes 480 a 493

8. Por fim no estabelecimento do túnel PPPoE são negociados os endereços IPv6 através do protocolo DHCPv6 (IA_NA e/ou IA_PD) caso a ONU esteja configurada para fazer DHCPv6. Pacotes 598 a 616

9. Em caso de término de conexão é gerado enviado o pacote PADT de quem está solicitando o término da conexão. No exemplo foi o BNG que desconectou o assinante: Pacotes 1331 a 1332

PADO Delay é um mecanismo para fazer redundância de BNG onde a requisição do assinante (PADI) chega em mais de um BNG já que esta requisição é Broadcast (MAC ff:ff:ff:ff:ff:ff). Neste caso um BNG (principal)

responde com o PADO imediatamente e um outro BNG (backup) é configurado com um delay na resposta do PADO (delay de 5 segundos por exemplo). Desta forma, a ONU em virtude de ter recebido o PADO do BNG principal automaticamente já deu sequência no estabelecimento do túnel PPPoE com este BNG.

Quando o BNG backup responder o PADO a ONU simplesmente vai descartar este pacote já que ela não está mais esperando respostas visto que já deu sequência no estabelecimento do túnel PPPoE com o BNG principal. Por outro lado como a ONU não respondeu ao BNG backup ele deletou a interface demux0.<unit> criada e também não deu sequência no processo.

Caso aconteça do BNG principal parar de responder, quando a ONU enviar o PADI para a rede e o BNG backup responder (mesmo com atraso) a ONU vai utilizar este BNG para estabelecer o túnel PPPoE.

Configuração do PADO Delay:

```
set protocols pppoe service-name-tables PADO-DELAY service any delay 5
```

É criado uma service-name-table chamada PADO-DELAY com delay de 5 segundos. Esta service-name-table é associada à profile CVLAN ou SVLAN:

```
set dynamic-profiles SVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe service-name-table
PADO-DELAY
set dynamic-profiles CVLAN-DYNAMIC-PROFILE interfaces demux0 unit "$junos-interface-unit" family pppoe service-name-table
PADO-DELAY
```

Desta forma quando chegar um PADI, ao invés do BNG responder imediatamente, ele responderá o PADO com o delay de 5 segundos:

19:02:21.019680 In PPPoE PADI [Service-Name] [Host-Uniq UTF8]
19:02:25.947930 Out PPPoE PADO [AC-Name "CONCENTRADOR-PPPOE"] [Host-Uniq UTF8] [Service-Name] [AC-Cookie UTF8]

16. VRF (Virtual Routing Instances)

O BNG Juniper suporta o modelo de VRF (Virtual Router Instances) onde é possível ter assinantes conectados em uma tabela de roteamento e outros assinantes conectados em outra tabela de roteamento. O MX não suporta o uso de Logical Systems para o serviço de BNG.

O uso de VRF's pode ser utilizado por exemplo no cenário onde clientes estão inadimplentes e precisam ser bloqueados. Neste cenário é possível configurar um assinante com sua VRF e quando ele se conectar ele será ativado nesta tabela de roteamento diferente.

No modelo de VRF é suportado o `instance-type virtual-router` e também o `instance-type vrf`

No cenário de VRF, toda a configuração de BNG até que o usuário se autentique é feito globalmente. Não é possível configurar uma interface física por exemplo com auto-configure dentro da VRF. Toda a configuração de interfaces físicas com auto-configure, VLAN Profile, Subscriber Profile, Service Profile, Access, Access profile, Firewall Filters, etc... é feito globalmente da mesma forma já detalhada neste documento e o BNG precisa alcançar o servidor RADIUS que fará a autenticação do assinante também utilizando a tabela de roteamento global (inet.0).

A partir do momento que a autenticação do usuário chegar no servidor RADIUS o RADIUS enviará o AVP ERX-Virtual-Router-Name (Vendor 4874 / Atributo 1) informando qual o nome da VRF que o usuário deve ser ancorado. Exemplo:

```
wztech3  Cleartext-Password := "wztech3"
         ERX-Virtual-Router-Name = VRF-PROVEDOR-1
```

Para que um assinante consiga ser associado a uma VRF é obrigatório que esta VRF possua uma interface loopback e também que esta VRF possua as configurações necessárias para entrega dos endereços IPv4 e IPv6 [access address-assignment pool], [access address-assignment neighbor-discovery-router-advertisement] (no caso de uso de NDRA) e [system services dhcp-local-server dhcpv6] (no caso de uso de DHCPv6).

As configurações de DHCPv6 Server precisam existir dentro da VRF para que seja fornecido endereços IA_NA e/ou IA_PD através do protocolo DHCPv6.

A configuração de NDRA (neighbor-discovery-router-advertisement) precisa existir dentro da VRF no caso de uso de NDRA (SLAAC).

O BNG não herda nenhuma configuração global de alocação de endereços. Estas configurações precisam ser feitas dentro da VRF.

Exemplo da configuração de uma VRF:

```
set routing-instances VRF-PROVEDOR-1 instance-type virtual-router
set routing-instances VRF-PROVEDOR-1 system services dhcp-local-server dhcpv6 group DHCPV6-VRF reconfigure
set routing-instances VRF-PROVEDOR-1 system services dhcp-local-server dhcpv6 group DHCPV6-VRF overrides rapid-commit
set routing-instances VRF-PROVEDOR-1 system services dhcp-local-server dhcpv6 group DHCPV6-VRF overrides delegated-pool
VRF-POOL-V6-PD
set routing-instances VRF-PROVEDOR-1 system services dhcp-local-server dhcpv6 group DHCPV6-VRF interface pp0.0
set routing-instances VRF-PROVEDOR-1 access address-assignment neighbor-discovery-router-advertisement VRF-POOL-V6-NDRA
set routing-instances VRF-PROVEDOR-1 access address-assignment pool VRF-POOL-IP-01 family inet network 100.64.10.0/24
set routing-instances VRF-PROVEDOR-1 access address-assignment pool VRF-POOL-V6-IA_NA family inet6 prefix
8000:0ee4:9000::/64
set routing-instances VRF-PROVEDOR-1 access address-assignment pool VRF-POOL-V6-IA_NA family inet6 range RANGE-01-IA_NA
prefix-length 128
set routing-instances VRF-PROVEDOR-1 access address-assignment pool VRF-POOL-V6-NDRA family inet6 prefix
8002:0ee4:8000::/48
set routing-instances VRF-PROVEDOR-1 access address-assignment pool VRF-POOL-V6-NDRA family inet6 range RANGE-01-NDRA
prefix-length 64
set routing-instances VRF-PROVEDOR-1 access address-assignment pool VRF-POOL-V6-PD family inet6 prefix
8003:0ee4:4000:0000:0000:0000:0000:0000/48
set routing-instances VRF-PROVEDOR-1 access address-assignment pool VRF-POOL-V6-PD family inet6 range RANGE-01-PD prefix-
length 64
set routing-instances VRF-PROVEDOR-1 interface lo0.1

set interfaces lo0 unit 1 family inet address 30.30.30.30/32
set interfaces lo0 unit 1 family inet6 address 2001:1291::2/128
set interfaces lo0 unit 1 family inet6 address 8000:ee4:9000::/128 primary
set interfaces lo0 unit 1 family inet6 address 8000:ee4:9000::/128 preferred
```

Os mesmos requisitos globais de [access address-assignment] já detalhados neste documento valem também para a VRF. Exemplos:

- No caso do IA_NA é obrigatório que a loopback dentro da VRF tenha um endereço IP que faça parte do pool
- Os requisitos de tamanho de prefixo para IA_NA e IA_PD são os mesmos requisitos globais

Importante: Para uso de IPv6 na VRF é obrigatório que a configuração de rpf-check para a family inet6 na Subscriber Profile seja desativada ou deletada. Caso ela esteja ativa não será fornecido endereços IPv6 para o assinante:

```
deactivate dynamic-profiles SUBSCRIBER-PROFILE interfaces pp0 unit "$junos-interface-unit" family inet6 rpf-check
```

Todos os AVP's para alocação de endereços e pools IPv4, prefixos e pools IPv6 já detalhados neste documento são suportados na VRF. Exemplo dos AVP's: Framed-IP-Address, Framed-Pool, Framed-IPv6-Pool, Framed-IPv6-Prefix, Framed-Route, Framed-IPv6-Route, Delegated-IPv6-Prefix, ERX-IPv6-Delegated-Pool-Name, etc...

Neste caso os AVP's têm ação local dentro da VRF. Se o RADIUS estiver enviando por exemplo o AVP ERX-IPv6-Delegated-Pool-Name, este pool deve existir dentro da VRF. Da mesma forma, se for enviado o AVP Framed-IP-Address será alocado um IPv4 para o assinante dentro da VRF e assim por diante. O comportamento de todos os AVP's dentro da VRF bem como a precedência para alocação dos endereços IPv4 e IPv6 é o mesmo já detalhado neste documento. Se por exemplo for enviado o AVP Framed-Pool com um nome de pool que não existe dentro da VRF o BNG vai tentar alocar endereços IPv4 do pool DEFAULT.

Também é suportado dentro da VRF o uso dos AVP's para envio de serviço dinâmico (ERX-Service-Activate, ERX-Service-Deactivate) e CoA/Disconnect-Request. No CoA/Disconnect-Request não é necessário enviar o nome da VRF na requisição de CoA/Disconnect-Request. O conteúdo dos AVP's o mesmo já detalhado.

Exemplo do usuário wztech3 conectado na tabela global (sem o uso de VRF):

```
admin@MX204-LAB-WZTECH> show subscribers user-name wztech3
Interface                   IP Address/VLAN ID                  User Name                       LS:RI
pp0.3221225569              192.168.60.8                        wztech3                 default:default
*                           1010:ee4:4000::/64
*                           2904:ee4:8000:7::/64
```

Na informação de RI (Routing Instance) é mostrado que o usuário está conectado na Routing Instance default (inet.0).

Quando o usuário está conectado em alguma VRF o nome da VRF é mostrado no usuário:

```
admin@MX204-LAB-WZTECH> show subscribers user-name wztech3
Interface                   IP Address/VLAN ID                  User Name                       LS:RI
pp0.3221225571              100.64.10.4                         wztech3                 default:VRF-PROVEDOR-1
*                           8003:ee4:4000:1::/64
*                           8002:ee4:8000:3::/64
```

Neste caso o usuário recebeu pelo RADIUS o AVP ERX-Virtual-Router-Name = VRF-PROVEDOR-1 e o BNG instalou a conexão PPPoE na VRF enviada pelo RADIUS.

É possível criar um modelo de configuração utilizando VRF onde cada interface física (ou range de VLAN's de uma interface física) utiliza um RADIUS diferente para autenticar os assinantes e cada RADIUS autentica os assinantes específicos da sua VRF. Exemplo:

```
set interfaces ae0 description INTERFACE-ACESSO
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 auto-configure vlan-ranges dynamic-profile SVLAN-DYNAMIC-PROFILE-1 accept pppoe
set interfaces ae0 auto-configure vlan-ranges dynamic-profile SVLAN-DYNAMIC-PROFILE-1 ranges 2-999
set interfaces ae0 auto-configure vlan-ranges dynamic-profile SVLAN-DYNAMIC-PROFILE-2 accept pppoe
set interfaces ae0 auto-configure vlan-ranges dynamic-profile SVLAN-DYNAMIC-PROFILE-2 ranges 1000-1999
set interfaces ae0 auto-configure remove-when-no-subscribers
set interfaces ae0 mtu 1522

set dynamic-profiles SVLAN-DYNAMIC-PROFILE-1 interfaces demux0 unit "$junos-interface-unit" vlan-id "$junos-vlan-id"
set dynamic-profiles SVLAN-DYNAMIC-PROFILE-1 interfaces demux0 unit "$junos-interface-unit" demux-options underlying-
interface "$junos-interface-ifd-name"
set dynamic-profiles SVLAN-DYNAMIC-PROFILE-1 interfaces demux0 unit "$junos-interface-unit" family pppoe access-
concentrator CONCENTRADOR-PPPOE
set dynamic-profiles SVLAN-DYNAMIC-PROFILE-1 interfaces demux0 unit "$junos-interface-unit" family pppoe dynamic-profile
SUBSCRIBER-PROFILE-RADIUS-1

set dynamic-profiles SVLAN-DYNAMIC-PROFILE-2 interfaces demux0 unit "$junos-interface-unit" vlan-id "$junos-vlan-id"
set dynamic-profiles SVLAN-DYNAMIC-PROFILE-2 interfaces demux0 unit "$junos-interface-unit" demux-options underlying-
interface "$junos-interface-ifd-name"
set dynamic-profiles SVLAN-DYNAMIC-PROFILE-2 interfaces demux0 unit "$junos-interface-unit" family pppoe access-
concentrator CONCENTRADOR-PPPOE
set dynamic-profiles SVLAN-DYNAMIC-PROFILE-2 interfaces demux0 unit "$junos-interface-unit" family pppoe dynamic-profile
SUBSCRIBER-PROFILE-RADIUS-2


set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 predefined-variable-defaults input-filter PREDEFINED-IPV4-IN
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 predefined-variable-defaults output-filter PREDEFINED-IPV4-OUT
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 predefined-variable-defaults input-ipv6-filter PREDEFINED-IPV6-IN
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 predefined-variable-defaults output-ipv6-filter PREDEFINED-IPV6-OUT
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 routing-instances "$junos-routing-instance" interface "$junos-interface-
name"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 routing-instances "$junos-routing-instance" routing-options rib "$junos-
ipv6-rib" access route $junos-framed-route-ipv6-address-prefix qualified-next-hop "$junos-interface-name"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 routing-instances "$junos-routing-instance" routing-options rib "$junos-
ipv6-rib" access route $junos-framed-route-ipv6-address-prefix metric "$junos-framed-route-ipv6-cost"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 routing-instances "$junos-routing-instance" routing-options rib "$junos-
ipv6-rib" access route $junos-framed-route-ipv6-address-prefix preference "$junos-framed-route-ipv6-distance"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 routing-instances "$junos-routing-instance" routing-options rib "$junos-
ipv6-rib" access route $junos-framed-route-ipv6-address-prefix tag "$junos-framed-route-ipv6-tag"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 routing-instances "$junos-routing-instance" routing-options access route
$junos-framed-route-ip-address-prefix next-hop "$junos-framed-route-nexthop"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 routing-instances "$junos-routing-instance" routing-options access route
$junos-framed-route-ip-address-prefix metric "$junos-framed-route-cost"
```

```
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 routing-instances "$junos-routing-instance" routing-options access route
$junos-framed-route-ip-address-prefix preference "$junos-framed-route-distance"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 routing-instances "$junos-routing-instance" routing-options access route
$junos-framed-route-ip-address-prefix tag "$junos-framed-route-tag"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 interfaces pp0 unit "$junos-interface-unit" actual-transit-statistics
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 interfaces pp0 unit "$junos-interface-unit" ppp-options chap
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 interfaces pp0 unit "$junos-interface-unit" ppp-options pap
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 interfaces pp0 unit "$junos-interface-unit" ppp-options aaa-options AAA-
OPTIONS-RADIUS-1
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 interfaces pp0 unit "$junos-interface-unit" family inet rpf-check
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 interfaces pp0 unit "$junos-interface-unit" family inet filter input
"$junos-input-filter"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 interfaces pp0 unit "$junos-interface-unit" family inet filter output
"$junos-output-filter"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 interfaces pp0 unit "$junos-interface-unit" family inet unnumbered-
address "$junos-loopback-interface"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 interfaces pp0 unit "$junos-interface-unit" family inet6 rpf-check
deactivate dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 interfaces pp0 unit "$junos-interface-unit" family inet6 rpf-
check
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 interfaces pp0 unit "$junos-interface-unit" family inet6 filter input
"$junos-input-ipv6-filter"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 interfaces pp0 unit "$junos-interface-unit" family inet6 filter output
"$junos-output-ipv6-filter"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 interfaces pp0 unit "$junos-interface-unit" family inet6 unnumbered-
address "$junos-loopback-interface"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 protocols router-advertisement interface "$junos-interface-name" dns-
server-address $junos-ipv6-dns-server-address
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-1 protocols router-advertisement interface "$junos-interface-name" prefix
$junos-ipv6-ndra-prefix

set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 predefined-variable-defaults input-filter PREDEFINED-IPV4-IN
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 predefined-variable-defaults output-filter PREDEFINED-IPV4-OUT
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 predefined-variable-defaults input-ipv6-filter PREDEFINED-IPV6-IN
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 predefined-variable-defaults output-ipv6-filter PREDEFINED-IPV6-OUT
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 routing-instances "$junos-routing-instance" interface "$junos-interface-
name"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 routing-instances "$junos-routing-instance" routing-options rib "$junos-
ipv6-rib" access route $junos-framed-route-ipv6-address-prefix qualified-next-hop "$junos-interface-name"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 routing-instances "$junos-routing-instance" routing-options rib "$junos-
ipv6-rib" access route $junos-framed-route-ipv6-address-prefix metric "$junos-framed-route-ipv6-cost"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 routing-instances "$junos-routing-instance" routing-options rib "$junos-
ipv6-rib" access route $junos-framed-route-ipv6-address-prefix preference "$junos-framed-route-ipv6-distance"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 routing-instances "$junos-routing-instance" routing-options rib "$junos-
ipv6-rib" access route $junos-framed-route-ipv6-address-prefix tag "$junos-framed-route-ipv6-tag"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 routing-instances "$junos-routing-instance" routing-options access route
$junos-framed-route-ip-address-prefix next-hop "$junos-framed-route-nexthop"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 routing-instances "$junos-routing-instance" routing-options access route
$junos-framed-route-ip-address-prefix metric "$junos-framed-route-cost"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 routing-instances "$junos-routing-instance" routing-options access route
$junos-framed-route-ip-address-prefix preference "$junos-framed-route-distance"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 routing-instances "$junos-routing-instance" routing-options access route
$junos-framed-route-ip-address-prefix tag "$junos-framed-route-tag"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 interfaces pp0 unit "$junos-interface-unit" actual-transit-statistics
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 interfaces pp0 unit "$junos-interface-unit" ppp-options chap
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 interfaces pp0 unit "$junos-interface-unit" ppp-options pap
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 interfaces pp0 unit "$junos-interface-unit" ppp-options aaa-options AAA-
OPTIONS-RADIUS-3
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 interfaces pp0 unit "$junos-interface-unit" family inet rpf-check
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 interfaces pp0 unit "$junos-interface-unit" family inet filter input
"$junos-input-filter"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 interfaces pp0 unit "$junos-interface-unit" family inet filter output
"$junos-output-filter"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 interfaces pp0 unit "$junos-interface-unit" family inet unnumbered-
address "$junos-loopback-interface"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 interfaces pp0 unit "$junos-interface-unit" family inet6 rpf-check
deactivate dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 interfaces pp0 unit "$junos-interface-unit" family inet6 rpf-
check
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 interfaces pp0 unit "$junos-interface-unit" family inet6 filter input
"$junos-input-ipv6-filter"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 interfaces pp0 unit "$junos-interface-unit" family inet6 filter output
"$junos-output-ipv6-filter"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 interfaces pp0 unit "$junos-interface-unit" family inet6 unnumbered-
address "$junos-loopback-interface"
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 protocols router-advertisement interface "$junos-interface-name" dns-
server-address $junos-ipv6-dns-server-address
set dynamic-profiles SUBSCRIBER-PROFILE-RADIUS-2 protocols router-advertisement interface "$junos-interface-name" prefix
$junos-ipv6-ndra-prefix

set access aaa-options AAA-OPTIONS-RADIUS-1 access-profile ACCESS-PROFILE-RADIUS-1
set access aaa-options AAA-OPTIONS-RADIUS-2 access-profile ACCESS-PROFILE-RADIUS-2

set access profile ACCESS-PROFILE-RADIUS-1 authentication-order radius
set access profile ACCESS-PROFILE-RADIUS-1 domain-name-server-inet6 1070::1
```

```
set access profile ACCESS-PROFILE-RADIUS-1 domain-name-server-inet6 1070::2
set access profile ACCESS-PROFILE-RADIUS-1 radius authentication-server 192.168.1.236
set access profile ACCESS-PROFILE-RADIUS-1 radius authentication-server 192.168.1.102
set access profile ACCESS-PROFILE-RADIUS-1 radius accounting-server 192.168.1.236
set access profile ACCESS-PROFILE-RADIUS-1 radius accounting-server 192.168.1.102
set access profile ACCESS-PROFILE-RADIUS-1 radius-server 192.168.1.236 secret "$9$cgdrMX7Nbg4Z7NqfTz6/"
set access profile ACCESS-PROFILE-RADIUS-1 radius-server 192.168.1.236 source-address 192.168.1.248
set access profile ACCESS-PROFILE-RADIUS-1 radius-server 192.168.1.102 secret "$9$6oNwC0IEhrMWxEhs4aZji"
set access profile ACCESS-PROFILE-RADIUS-1 radius-server 192.168.1.102 source-address 192.168.1.248
set access profile ACCESS-PROFILE-RADIUS-1 accounting order radius
set access profile ACCESS-PROFILE-RADIUS-1 accounting address-change-immediate-update

set access profile ACCESS-PROFILE-RADIUS-2 authentication-order radius
set access profile ACCESS-PROFILE-RADIUS-2 domain-name-server-inet6 2070::1
set access profile ACCESS-PROFILE-RADIUS-2 domain-name-server-inet6 2070::2
set access profile ACCESS-PROFILE-RADIUS-2 radius authentication-server 192.168.2.236
set access profile ACCESS-PROFILE-RADIUS-2 radius authentication-server 192.168.2.102
set access profile ACCESS-PROFILE-RADIUS-2 radius accounting-server 192.168.2.236
set access profile ACCESS-PROFILE-RADIUS-2 radius accounting-server 192.168.2.102
set access profile ACCESS-PROFILE-RADIUS-2 radius-server 192.168.2.236 secret "$9$cgdrMX7Nbg4Z7NqfTz6/"
set access profile ACCESS-PROFILE-RADIUS-2 radius-server 192.168.2.236 source-address 192.168.1.248
set access profile ACCESS-PROFILE-RADIUS-2 radius-server 192.168.2.102 secret "$9$6oNwC0IEhrMWxEhs4aZji"
set access profile ACCESS-PROFILE-RADIUS-2 radius-server 192.168.2.102 source-address 192.168.1.248
set access profile ACCESS-PROFILE-RADIUS-2 accounting order radius
set access profile ACCESS-PROFILE-RADIUS-2 accounting address-change-immediate-update

set routing-instances VRF-PROVEDOR-A instance-type vrf
set routing-instances VRF-PROVEDOR-A system services dhcp-local-server dhcpv6 group DHCPV6-PROVEDOR-A interface pp0.0
overrides delegated-pool PD-POOL-PROVEDOR-A
set routing-instances VRF-PROVEDOR-A access address-assignment neighbor-discovery-router-advertisement POOL-V6-WAN-PROV-A
set routing-instances VRF-PROVEDOR-A access address-assignment pool POOL-PROVEDOR-A family inet network 172.44.0.0/16
set routing-instances VRF-PROVEDOR-A access address-assignment pool POOL-V6-WAN-PROV-A family inet6 prefix
2804:04e4:0000:0000:0000:0000:0000:0000/48
set routing-instances VRF-PROVEDOR-A access address-assignment pool POOL-V6-WAN-PROV-A family inet6 range ndra-range
prefix-length 64
set routing-instances VRF-PROVEDOR-A access address-assignment pool PD-POOL-PROVEDOR-A family inet6 prefix
2804:04e4:4000:0000:0000:0000:0000:0000/48
set routing-instances VRF-PROVEDOR-A access address-assignment pool PD-POOL-PROVEDOR-A family inet6 range RANGE-PD
prefix-length 64
set routing-instances VRF-PROVEDOR-A interface lo0.1
set routing-instances VRF-PROVEDOR-A route-distinguisher 1.1.1.1:1
set routing-instances VRF-PROVEDOR-A vrf-target target:1:1

set routing-instances VRF-PROVEDOR-B instance-type vrf
set routing-instances VRF-PROVEDOR-B system services dhcp-local-server dhcpv6 group DHCPV6-PROVEDOR-B interface pp0.0
overrides delegated-pool PD-POOL-PROVEDOR-B
set routing-instances VRF-PROVEDOR-B access address-assignment neighbor-discovery-router-advertisement POOL-V6-WAN-PROV-B
set routing-instances VRF-PROVEDOR-B access address-assignment pool POOL-PROVEDOR-B family inet network 172.25.0.0/16
set routing-instances VRF-PROVEDOR-B access address-assignment pool POOL-V6-WAN-PROV-B family inet6 prefix
2805:04e4:0000:0000:0000:0000:0000:0000/48
set routing-instances VRF-PROVEDOR-B access address-assignment pool POOL-V6-WAN-PROV-B family inet6 range ndra-range
prefix-length 64
set routing-instances VRF-PROVEDOR-B access address-assignment pool PD-POOL-PROVEDOR-B family inet6 prefix
2805:04e4:4000:0000:0000:0000:0000:0000/48
set routing-instances VRF-PROVEDOR-B access address-assignment pool PD-POOL-PROVEDOR-B family inet6 range RANGE-PD
prefix-length 64
set routing-instances VRF-PROVEDOR-B interface lo0.2
set routing-instances VRF-PROVEDOR-B route-distinguisher 2.2.2.2:1
set routing-instances VRF-PROVEDOR-B vrf-target target:2:2

set interfaces lo0 unit 1 family inet address 1.1.1.1/32
set interfaces lo0 unit 1 family inet6 address 1804:04e4:c000:0000:0000:0000:0000:0001/128

set interfaces lo0 unit 2 family inet address 2.2.2.2/32
set interfaces lo0 unit 2 family inet6 address 1805:04e4:8000:0000:0000:0000:0000:0001/128
```

Neste caso, na interface ae0 o range de VLAN's 2 a 999 chama a VLAN Profile SVLAN-DYNAMIC-PROFILE-1 e o range de VLAN's 1000 a 1999 chama a VLAN Profile SVLAN-DYNAMIC-PROFILE-2. Cada VLAN Profile chama uma Subscriber Profile diferente e cada Subscriber Profile está configurada com um aaa-options diferente. No aaa-options é especificado a access profile diferente para cada Subscriber Profile e dentro de cada access profile são especificados RADIUS distintos. Com esse modelo é possível separar totalmente o BNG com VRF's em mais de um ambiente onde cada ambiente tem o seu RADIUS específico para autenticar os seus assinantes.

17. Comandos Úteis - Sessões PPPoE

```
admin@MX204-LAB-WZTECH> show subscribers
Interface                   IP Address/VLAN ID                  User Name                       LS:RI
```

```
demux0.3221225562                200                                                    default:default
pp0.3221225571                   100.64.10.4                          wztech3           default:VRF-PROVEDOR-1
*                                8003:ee4:4000:1::/64
*                                8002:ee4:8000:3::/64
pp0.3221225571                   8003:ee4:4000:1::/64                                   default:VRF-PROVEDOR-1
pp0.3221225573                   192.168.60.9                         wztech2           default:default
*                                1011:ee4:4000:7::/64
*                                2904:ee4:8000:8::/64
pp0.3221225574                   192.168.60.10                        wztech4           default:default
*                                1011:ee4:4000:8::/64
*                                2904:ee4:8000:9::/64
pp0.3221225573                   1011:ee4:4000:7::/64                                   default:default
pp0.3221225574                   1011:ee4:4000:8::/64                                   default:default
```

O comando acima mostra todos os assinantes conectados com o usuário, interface pp0 e VRF.

```
admin@MX204-LAB-WZTECH> show subscribers summary port

Interface           Count
ae0: xe-0/1/0       3
ae0: xe-0/1/2       3

Total Subscribers: 3
```

O comando acima mostra o sumário de assinantes por porta física do BNG

```
admin@MX204-LAB-WZTECH> show subscribers summary

Subscribers by State
   Active: 7
   Total: 7

Subscribers by Client Type
   DHCP: 3
   VLAN: 1
   PPPoE: 3
   Total: 7
```


O comando acima mostra um sumário da quantidade de conexões ativas no BNG por protocolo. Para efeito de licença um usuário pode ter uma interface VLAN, uma interface PPPoE, um prefixo SLAAC e dois prefixos DHCPv6 (IA_NA e IA_PD) e nas licenças será contado apenas uma licença usada em scale-subscriber.

```
admin@MX204-LAB-WZTECH> show subscribers user-name wztech3
Interface                        IP Address/VLAN ID                   User Name                 LS:RI
pp0.3221225571                   100.64.10.4                          wztech3           default:VRF-PROVEDOR-1
*                                8003:ee4:4000:1::/64
*                                8002:ee4:8000:3::/64
```

O comando acima filtra um assinante baseado no login (user-name)

```
admin@MX204-LAB-WZTECH> show network-access aaa subscribers username wztech3
Logical system/Routing instance   Client type    Session-ID     Session uptime    Accounting
default:VRF-PROVEDOR-1            pppoe          231            00:08:58          on/time
```

Também é possível filtrar o login com o comando acima. Neste caso é mostrado de forma resumida com o Session-ID, uptime e se está ligado Accounting para o usuário.

```
admin@MX204-LAB-WZTECH> show subscribers vlan-id 200
Interface                        IP Address/VLAN ID                   User Name                 LS:RI
pp0.3221225571                   100.64.10.4                          wztech3           default:VRF-PROVEDOR-1
*                                8003:ee4:4000:1::/64
*                                8002:ee4:8000:3::/64
demux0.3221225562                200                                                    default:default
```

O comando acima mostra o filtro de um assinante baseado na SVLAN

```
admin@MX204-LAB-WZTECH> show subscribers stacked-vlan-id 300 vlan-id 400
Interface                        IP Address/VLAN ID                   User Name                 LS:RI
demux0.3221225474                0x8100.300 0x8100.400                                  default:default
pp0.3221226282                   192.168.4.5                          wztech2           default:default
```

O comando acima mostra o filtro de um assinante baseado na SVLAN / CVLAN

```
admin@MX204-LAB-WZTECH> show subscribers address 100.64.10.10
Interface                   IP Address/VLAN ID                  User Name                LS:RI
pp0.3221225601              100.64.10.10                        wztech3                  default:VRF-PROVEDOR-1
*                           8003:ee4:4000:7::/64
*                           8002:ee4:8000:9::/64
```

O comando acima filtra um assinante baseado no endereço IPv4:

```
admin@MX204-LAB-WZTECH> show system subscriber-management route prefix 100.64.10.10

Route:  100.64.10.10/32
     Routing-instance:          default:VRF-PROVEDOR-1
     Kernel rt-table id :       7
     Family:                    AF_INET
     Route Type:                Access-internal
     Protocol Type:             Unspecified
     Interface:                 pp0.3221225601
     Interface index:           199
     Internal Interface index:  199
     Route index:               77
     Next-Hop index:            642
     Reference-count:           1
     L2 Address:                38:90:52:67:06:4d
     Flags:                     0x0
```

Este comando acima também pode ser utilizado para filtrar o assinante baseado no endereço IPv4

Para achar o assinante baseado em um prefixo IPv6 pode-se utilizar os passos a seguir:

```
admin@MX204-LAB-WZTECH> show route 8003:ee4:4000:7::100

VRF-PROVEDOR-1.inet6.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

8003:ee4:4000:7::/64
                   *[Access/13] 00:02:06
                       Private unicast
```


É feita uma busca na tabela de rotas pelo endereço IPv6 e é obtido o prefixo do assinante.

```
admin@MX204-LAB-WZTECH> show system subscriber-management route prefix 8003:ee4:4000:7::/64

Route:  8003:ee4:4000:7::/64
     Routing-instance:          default:VRF-PROVEDOR-1
     Kernel rt-table id :       7
     Family:                    AF_INET6
     Route Type:                Access
     Protocol Type:             Unspecified
     Interface:                 pp0.3221225601
     Interface index:           199
     Internal Interface index:  204
     Route index:               81
     Next-Hop index:            642
     Reference-count:           1
     L2 Address:                be:7c:45:e4:aa:e1
     Flags:                     0x0
```

Com base no prefixo é possível achar qual é a interface PPPoE do assinante

```
admin@MX204-LAB-WZTECH> show subscribers interface pp0.3221225601
Interface                   IP Address/VLAN ID                  User Name                LS:RI
pp0.3221225601              8003:ee4:4000:7::/64                                         default:VRF-PROVEDOR-1
pp0.3221225601              100.64.10.10                        wztech3                  default:VRF-PROVEDOR-1
*                           8003:ee4:4000:7::/64
*                           8002:ee4:8000:9::/64
```

Com base na interface é possível achar o assinante.

Com base no prefixo é possível também achar o binding DHCPv6 caso este prefixo tenha sido entregue por DHCPv6:

```
admin@MX204-LAB-WZTECH> show dhcpv6 server binding routing-instance VRF-PROVEDOR-1 8003:ee4:4000:7::/64
Prefix                  Session Id  Expires  State    Interface    Client DUID
8003:ee4:4000:7::/64    252         85984    BOUND    pp0.3221225601 LL0x1-38:90:52:67:06:4d
```

Também é possível achar um binding DHCPv6 do assinante pela interface PPPoE:

```
admin@MX204-LAB-WZTECH> show dhcpv6 server binding interface pp0.3221225601
Prefix                  Session Id  Expires  State    Interface    Client DUID
8003:ee4:4000:7::/64    252         85943    BOUND    pp0.3221225601 LL0x1-38:90:52:67:06:4d
```

Este comando acima não funciona quando o assinante está dentro de VRF.

Com a interface pp0 é possível filtrar o assinante. Com o extensive será mostrado várias informações do assinante (DHCP e PPPoE):

```
admin@MX204-LAB-WZTECH> show subscribers interface pp0.3221225601 extensive
Type: DHCP
IPv6 Prefix: 8003:ee4:4000:7::/64
Domain name server inet6: 2080::1 2080::2
Logical System: default
Routing Instance: VRF-PROVEDOR-1
Interface: pp0.3221225601
Interface type: Static
Underlying Interface: pp0.3221225601
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: jnpr :252
Session ID: 252
Underlying Session ID: 248
PFE Flow ID: 199
Login Time: 2023-09-13 17:55:48 -03
DHCPV6 Options: len 71
00 01 00 0a 00 03 00 01 38 90 52 67 06 4d 00 08 00 02 00 00
00 06 00 02 00 17 00 19 00 29 00 9f 97 67 00 00 00 00 00 00
00 00 00 1a 00 19 ff ff ff ff ff ff ff ff 40 10 10 0e e4 40
00 00 01 00 00 00 00 00 00 00 00 00
DHCPV6 Header: len 4
01 dc ee 8c
IPv6 Address Pool: VRF-POOL-V6-NDRA
IPv6 Delegated Address Pool: VRF-POOL-V6-PD

Type: PPPoE
User Name: wztech3
IP Address: 100.64.10.10
IP Netmask: 255.255.255.255
Primary DNS Address: 8.8.8.8
Secondary DNS Address: 8.8.4.4
IPv6 Prefix: 8003:ee4:4000:7::/64
Domain name server inet6: 2070::1 2070::2
IPv6 User Prefix: 8002:ee4:8000:9::/64
Logical System: default
Routing Instance: VRF-PROVEDOR-1
Interface: pp0.3221225601
Interface type: Dynamic
Underlying Interface: demux0.3221225600
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 2
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 248
Session ID: 248
PFE Flow ID: 199
VLAN Id: 200
Login Time: 2023-09-13 17:55:44 -03
IP Address Pool: VRF-POOL-IP-01
IPv6 Address Pool: VRF-POOL-V6-NDRA
IPv6 Framed Interface Id: bc7c:45d6:5de4:aae1
IPv4 Input Filter Name: 100M-IPV4-IN-pp0.3221225601-in
IPv4 Output Filter Name: 100M-IPV4-OUT-pp0.3221225601-out
IPv6 Input Filter Name: 100M-IPV6-IN-pp0.3221225601-in
IPv6 Output Filter Name: 100M-IPV6-OUT-pp0.3221225601-out
Accounting interval: 0
Dynamic configuration:
  junos-input-filter: 100M-IPV4-IN
  junos-input-ipv6-filter: 100M-IPV6-IN
  junos-ipv6-ndra-prefix: 8002:ee4:8000:9::/64
  junos-output-filter: 100M-IPV4-OUT
  junos-output-ipv6-filter: 100M-IPV6-OUT
```

O comando acima vai mostrar as informações PPPoE e DHCP do assinante.

```
admin@MX204-LAB-WZTECH> show subscribers user-name wztech3 extensive
Type: PPPoE
User Name: wztech3
IP Address: 100.64.10.10
IP Netmask: 255.255.255.255
Primary DNS Address: 8.8.8.8
Secondary DNS Address: 8.8.4.4
IPv6 Prefix: 8003:ee4:4000:7::/64
Domain name server inet6: 2070::1 2070::2
IPv6 User Prefix: 8002:ee4:8000:9::/64
Logical System: default
Routing Instance: VRF-PROVEDOR-1
Interface: pp0.3221225601
Interface type: Dynamic
Underlying Interface: demux0.3221225600
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 2
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 248
Session ID: 248
PFE Flow ID: 199
VLAN Id: 200
Login Time: 2023-09-13 17:55:44 -03
IP Address Pool: VRF-POOL-IP-01
IPv6 Address Pool: VRF-POOL-V6-NDRA
IPv6 Framed Interface Id: bc7c:45d6:5de4:aae1
IPv4 Input Filter Name: 100M-IPV4-IN-pp0.3221225601-in
IPv4 Output Filter Name: 100M-IPV4-OUT-pp0.3221225601-out
IPv6 Input Filter Name: 100M-IPV6-IN-pp0.3221225601-in
IPv6 Output Filter Name: 100M-IPV6-OUT-pp0.3221225601-out
Accounting interval: 0
Dynamic configuration:
  junos-input-filter: 100M-IPV4-IN
  junos-input-ipv6-filter: 100M-IPV6-IN
  junos-ipv6-ndra-prefix: 8002:ee4:8000:9::/64
  junos-output-filter: 100M-IPV4-OUT
  junos-output-ipv6-filter: 100M-IPV6-OUT
```


O comando acima mostra várias informações de um assinante: Firewall Filter ativada para IPv4 (IPv4 Input/Output Filter), IPv6 (IPv6 Input/Output Filter), Pool IPv4 (IP Address Pool), Pool IPv6 de WAN (IPv6 Address Pool), VLAN (Vlan Id), Session ID, MAC Address, Subscriber Profile (Dynamic Profile Name), Interface L2 (Underlying Interface), Interface PPPoE (Interface), Routing Instance, Prefixo SLAAC (IPv6 User Prefix), Prefixo PD (IPv6 Prefix), endereço IPv4 (IP Address), etc...

```
admin@MX204-LAB-WZTECH> show interfaces pp0.3221225601 extensive
  Logical interface pp0.3221225601 (Index 536871111) (SNMP ifIndex 200000199) (Generation 172)
    Flags: Up Point-To-Point Encapsulation: PPPoE
    PPPoE:
      State: SessionUp, Session ID: 1,
      Session AC name: CONCENTRADOR-PPPOE, Remote MAC address: 38:90:52:67:06:4d,
      Underlying interface: demux0.3221225600 (Index 536871109)
      Ignore End-Of-List tag: Disable
    Link:
      xe-0/1/0.32767
      xe-0/1/2.32767
    Traffic statistics:
     Input  bytes  :                26118
     Output bytes  :                28708
     Input  packets:                  332
     Output packets:                  278
     IPv6 transit statistics:
     Input  bytes  :                23772
     Output bytes  :                28790
     Input  packets:                  263
     Output packets:                  209
    Local statistics:
     Input  bytes  :                  372
     Output bytes  :                 4586
     Input  packets:                    4
     Output packets:                   35
    Transit statistics:
     Input  bytes  :                25746                    0 bps
     Output bytes  :                24122                    0 bps
     Input  packets:                  328                    0 pps
     Output packets:                  243                    0 pps
```

```
    IPv6 transit statistics:
     Input  bytes  :                23400                    0 bps
     Output bytes  :                24204                    0 bps
     Input  packets:                  259                    0 pps
     Output packets:                  174                    0 pps
  Keepalive settings: Interval 30 seconds, Up-count 3, Down-count 3
  LCP state: Opened
  NCP state: inet: Opened, inet6: Opened, iso: Not-configured, mpls: Not-configured
  CHAP state: Success
  PAP state: Closed
    Protocol inet, MTU: 1300
    Max nh cache: 0, New hold nh limit: 0, Curr nh cnt: 0, Curr new hold cnt: 0, NH drop cnt: 0
    Generation: 0, Route table: 7
      Flags: uRPF, Unnumbered
      Donor interface: lo0.1 (Index 330)
      RPF Failures: Packets: 0, Bytes: 0
      Input Filters: 100M-IPV4-IN-pp0.3221225601-in
      Output Filters: 100M-IPV4-OUT-pp0.3221225601-out
      Addresses, Flags: Is-Primary
        Destination: Unspecified, Local: 30.30.30.30, Broadcast: Unspecified, Generation: 0
    Protocol inet6, MTU: 1300
    Max nh cache: 0, New hold nh limit: 0, Curr nh cnt: 0, Curr new hold cnt: 0, NH drop cnt: 0
    Generation: 0, Route table: 7
      Flags: Unnumbered
      Donor interface: lo0.1 (Index 330)
      Input Filters: 100M-IPV6-IN-pp0.3221225601-in
      Output Filters: 100M-IPV6-OUT-pp0.3221225601-out
      Addresses, Flags: Primary Preferred Is-Default Is-Primary
        Destination: Unspecified, Local: 8000:ee4:9000::
    Generation: 230
      Addresses, Flags: Is-Primary
        Destination: Unspecified, Local: 8000:ee4:9000::
    Generation: 0
        Destination: Unspecified, Local: fe80::22d8:bff:fefb:4812
    Generation: 0
```

O comando acima mostra informações da interface do assinante como bytes e pacotes trafegados, intervalo do keepalive, mecanismo de autenticação que foi usado (PAP ou CHAP), MTU negociado para IPv4 e IPv6 etc.

```
admin@MX204-LAB-WZTECH> show pppoe interfaces pp0.3221225584 detail
pp0.3221225584 Index 536871089
  State: Session Up, Session ID: 3, Type: Dynamic,
  Service name: <empty>, Remote MAC address: 38:90:52:67:06:4D,
  Session AC name: CONCENTRADOR-PPPOE,
  Session uptime: 00:02:29 ago,
  Dynamic Profile: SUBSCRIBER-PROFILE,
  Underlying interface: demux0.3221225577 Index 536871080
```

O comando acima mostra o nome do AC Name enviado no PADO, O MAC do assinante, a Subscriber Profile do assinante e a interface L2 (Underlying Interface).

```
admin@MX204-LAB-WZTECH> show interfaces demux0.3221225577 extensive
  Logical interface demux0.3221225577 (Index 536871080) (SNMP ifIndex 200000168) (Generation 141)
    Flags: Up VLAN-Tag [ 0x8100.200 ]  Encapsulation: ENET2
    Demux:
      Underlying interface: ae0 (Index 130)
    Link:
      xe-0/1/0
      xe-0/1/2
    Bandwidth: 0
    Traffic statistics:
     Input  bytes  :                73483
     Output bytes  :               111327
     Input  packets:                 1421
     Output packets:                 1438
    Local statistics:
     Input  bytes  :                 3018
     Output bytes  :                 1008
     Input  packets:                   69
     Output packets:                   15
    Transit statistics:
     Input  bytes  :                70465                    0 bps
     Output bytes  :               110319                    0 bps
     Input  packets:                 1352                    0 pps
     Output packets:                 1423                    0 pps
    Protocol pppoe
      Dynamic Profile: SUBSCRIBER-PROFILE,
      Service Name Table: None,
      Max Sessions: 32000, Max Sessions VSA Ignore: Off,
```

```
      Duplicate Protection: Off, Short Cycle Protection: mac-address,
      Direct Connect: Off,
      AC Name: CONCENTRADOR-PPPOE
    Generation: 0, Route table: 65535
      Addresses, Flags: None
        Destination: Unspecified, Local: Unspecified, Broadcast: Unspecified, Generation: 0
```

O comando acima mostra se está habilitado Duplicate Protection na conexão, quantidade máxima de sessões permitidas, se está ignorando o VSA de limite de sessão do RADIUS, se está usando alguma Service Name Table, etc.

```
admin@MX204-LAB-WZTECH> show pppoe underlying-interfaces demux0.3221225577 extensive
demux0.3221225577 Index 536871080
  State: Dynamic, Dynamic Profile: SUBSCRIBER-PROFILE,
  Max Sessions: 32000, Max Sessions VSA Ignore: Off,
  Active Sessions: 3,
  Service Name Table: None,
  Duplicate Protection: Off, Short Cycle Protection: mac-address,
  Direct Connect: Off,
  AC Name: CONCENTRADOR-PPPOE,
  PacketType                      Sent         Received
    PADI                             0                6
    PADO                             6                0
    PADR                             0                6
    PADS                             6                0
    PADT                             3                3
    Service name error               0                0
    AC system error                  0                0
    Generic error                    0                0
    Malformed packets                0                0
    Unknown packets                  0                0
  Lockout Time (sec):  Min: 1, Max: 300
    Total clients in lockout: 0
    Total clients in lockout grace period: 0
```

O comando acima mostra também as informações de quantidade máxima de sessões, quantidade de conexões PPPoE ancoradas nesta interface L2, se o Short Cycle Protection está ativado e mostra principalmente estatísticas e erros da negociação do protocolo PPPoE (PADI, PADO, etc...)

```
admin@MX204-LAB-WZTECH> show subscribers vlan-id 200 extensive
 Type: PPPoE
User Name: wztech2
IP Address: 192.168.60.18
IP Netmask: 255.255.255.255
Primary DNS Address: 8.8.8.8
Secondary DNS Address: 8.8.4.4
IPv6 Prefix: 1011:ee4:4000:f::/64
Domain name server inet6: 2070::1 2070::2
IPv6 User Prefix: 2904:ee4:8000:11::/64
Logical System: default
Routing Instance: default
Interface: pp0.3221225603
Interface type: Dynamic
Underlying Interface: demux0.3221225600
 Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 2
MAC Address: d8:10:9f:d7:a1:15
State: Active
Radius Accounting ID: 250
Session ID: 250
PFE Flow ID: 201
VLAN Id: 200
Login Time: 2023-09-13 17:55:44 -03
IP Address Pool: POOL-IP-06
IPv6 Address Pool: POOL-V6-NDRA-1
IPv6 Delegated Address Pool: POOL-V6-PD-2
IPv6 Framed Interface Id: 95a:990b:e307:cba9
IPv4 Input Filter Name: PREDEFINED-IPV4-IN-pp0.3221225603-in
IPv4 Output Filter Name: PREDEFINED-IPV4-OUT-pp0.3221225603-out
IPv6 Input Filter Name: PREDEFINED-IPV6-IN-pp0.3221225603-in
IPv6 Output Filter Name: PREDEFINED-IPV6-OUT-pp0.3221225603-out
Accounting interval: 0
Dynamic configuration:
  junos-ipv6-ndra-prefix: 2904:ee4:8000:11::/64

Type: PPPoE
User Name: wztech4
IP Address: 192.168.60.17
```

```
IP Netmask: 255.255.255.255
Primary DNS Address: 8.8.8.8
Secondary DNS Address: 8.8.4.4
IPv6 Prefix: 1011:ee4:4000:e::/64
Domain name server inet6: 2070::1 2070::2
IPv6 User Prefix: 2904:ee4:8000:10::/64
Logical System: default
Routing Instance: default
Interface: pp0.3221225602
Interface type: Dynamic
Underlying Interface: demux0.3221225600
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 2
MAC Address: 3c:a3:7e:d8:f9:48
State: Active
Radius Accounting ID: 249
Session ID: 249
PFE Flow ID: 200
VLAN Id: 200
Login Time: 2023-09-13 17:55:44 -03
IP Address Pool: POOL-IP-06
IPv6 Address Pool: POOL-V6-NDRA-1
IPv6 Delegated Address Pool: POOL-V6-PD-2
IPv6 Framed Interface Id: b075:8ba9:2d4a:a84f
IPv4 Input Filter Name: PREDEFINED-IPV4-IN-pp0.3221225602-in
IPv4 Output Filter Name: PREDEFINED-IPV4-OUT-pp0.3221225602-out
IPv6 Input Filter Name: PREDEFINED-IPV6-IN-pp0.3221225602-in
IPv6 Output Filter Name: PREDEFINED-IPV6-OUT-pp0.3221225602-out
Accounting interval: 0
Dynamic configuration:
  junos-ipv6-ndra-prefix: 2904:ee4:8000:10::/64

Type: PPPoE
User Name: wztech3
IP Address: 100.64.10.10
IP Netmask: 255.255.255.255
Primary DNS Address: 8.8.8.8
Secondary DNS Address: 8.8.4.4
IPv6 Prefix: 8003:ee4:4000:7::/64
Domain name server inet6: 2070::1 2070::2
IPv6 User Prefix: 8002:ee4:8000:9::/64
Logical System: default
Routing Instance: VRF-PROVEDOR-1
Interface: pp0.3221225601
Interface type: Dynamic
Underlying Interface: demux0.3221225600
Dynamic Profile Name: SUBSCRIBER-PROFILE
Dynamic Profile Version: 2
MAC Address: 38:90:52:67:06:4d
State: Active
Radius Accounting ID: 248
Session ID: 248
PFE Flow ID: 199
VLAN Id: 200
Login Time: 2023-09-13 17:55:44 -03
IP Address Pool: VRF-POOL-IP-01
IPv6 Address Pool: VRF-POOL-V6-NDRA
IPv6 Framed Interface Id: bc7c:45d6:5de4:aae1
IPv4 Input Filter Name: 100M-IPV4-IN-pp0.3221225601-in
IPv4 Output Filter Name: 100M-IPV4-OUT-pp0.3221225601-out
IPv6 Input Filter Name: 100M-IPV6-IN-pp0.3221225601-in
IPv6 Output Filter Name: 100M-IPV6-OUT-pp0.3221225601-out
Accounting interval: 0
Dynamic configuration:
  junos-input-filter: 100M-IPV4-IN
  junos-input-ipv6-filter: 100M-IPV6-IN
  junos-ipv6-ndra-prefix: 8002:ee4:8000:9::/64
  junos-output-filter: 100M-IPV4-OUT
  junos-output-ipv6-filter: 100M-IPV6-OUT

Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.3221225600
Interface type: Dynamic
Underlying Interface: ae0
Dynamic Profile Name: SVLAN-DYNAMIC-PROFILE
Dynamic Profile Version: 2
State: Active
Session ID: 247
PFE Flow ID: 197
VLAN Id: 200
Login Time: 2023-09-13 17:55:44 -03
```

O comando acima mostra na SVLAN do usuário ou SVLAN+CVLAN qual é a VLAN Profile que está em uso e a versão.

```
admin@MX204-LAB-WZTECH> show network-access aaa subscribers session-id 248 detail
Type: pppoe
Username: wztech3
Stripped username: wztech3
AAA Logical system/Routing instance: default:default
Target Logical system/Routing instance: default:VRF-PROVEDOR-1
Access-profile: ACCESS-PROFILE
Session ID: 248
Accounting Session ID: 248
Multi Accounting Session ID: 0
IP Address: 100.64.10.10
Authentication State: AuthStateActive
Accounting State: Acc-Interim-Sent
Provisioning Type: None
```

Com o comando acima sabendo o session-id do assinante é possível saber qual a access profile que foi usada para autenticar o usuário. O Session ID pode ser obtido dentro da sessão do usuário (show subscriber username <username> extensive).

```
admin@MX204-LAB-WZTECH> show firewall templates-in-use
                  Dynamic Subscribers Reference Counts
Filter Template                                 Reference Count
----------------                                ----------------
100M-IPV4-IN                                    1
100M-IPV4-OUT                                   1
PREDEFINED-IPV4-IN                              2
PREDEFINED-IPV4-OUT                             2
100M-IPV6-IN                                    1
100M-IPV6-OUT                                   1
PREDEFINED-IPV6-IN                              2
PREDEFINED-IPV6-OUT                             2
```

O comando acima mostra o uso das firewall filters locais criadas no BNG.

```
admin@MX204-LAB-WZTECH> clear network-access aaa subscriber username wztech3

admin@MX204-LAB-WZTECH> clear network-access aaa subscriber session-id 225

admin@MX204-LAB-WZTECH> clear pppoe sessions pp0.3221225579
```

Os comandos acima são formas diferentes de fazer desconexão de um assinante (baseado no login, no session-id e na interface pp0)

```
admin@MX204-LAB-WZTECH> clear pppoe sessions
Clear all PPPoE sessions? [yes,no] (no) yes
```

O comando acima desconecta todos os assinantes do BNG

18. Troubleshooting - Comandos Úteis

Além de todos os comandos já detalhados no documento alguns comandos adicionais podem auxiliar em casos de análise de problemas dos assinantes no BNG:

Os pacotes esperados (PADI, DHCPv6, ICMPv6 RA/RS, etc) estão chegando no BNG na interface de acesso?

Estes pacotes podem ser capturados com o comando:

```
admin@MX204-LAB-WZTECH> monitor traffic interface ae0 no-resolve no-domain-names size 1500
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is OFF.
Listening on ae0, capture size 1500 bytes

18:41:32.707193 Out PPPoE  [ses 3]IP6 fe80::22d8:bff:fefb:4812 > ff02::1: ICMP6, router advertisement, length 88
18:41:40.759798 Out PPPoE  [ses 2]IP6 fe80::22d8:bff:fefb:4812 > ff02::1: ICMP6, router advertisement, length 88
18:41:45.838685  In PPPoE PADI [Service-Name] [Host-Uniq UTF8]
18:41:45.839112 Out PPPoE PADO [AC-Name "CONCENTRADOR-PPPOE"] [Host-Uniq UTF8] [Service-Name] [AC-Cookie UTF8]
18:41:45.842768  In PPPoE PADR [Service-Name] [Host-Uniq UTF8] [AC-Cookie UTF8]
```

```
18:41:45.848095 Out PPPoE PADS [ses 1] [Service-Name] [Host-Uniq UTF8] [AC-Name "CONCENTRADOR-PPPOE"] [AC-Cookie UTF8]
18:41:45.852370  In PPPoE  [ses 1]LCP, Conf-Request (0x01), id 46, length 16
18:41:45.852880 Out PPPoE  [ses 1]LCP, Conf-Request (0x01), id 237, length 21
18:41:45.852936 Out PPPoE  [ses 1]LCP, Conf-Ack (0x02), id 46, length 16
18:41:45.856595  In PPPoE  [ses 1]LCP, Conf-Ack (0x02), id 237, length 21
18:41:45.856916 Out PPPoE  [ses 1]CHAP, Challenge (0x01), id 189, Value
b78fba3a3699029fb0ef8a54281059c401f8599e3075e2753bcbd9f51d63, Name JUNOS
18:41:45.856939  In PPPoE  [ses 1]LCP, Echo-Request (0x09), id 0, length 10
18:41:45.857046 Out PPPoE  [ses 1]LCP, Echo-Reply (0x0a), id 0, length 10
18:41:45.859218  In PPPoE  [ses 1]CHAP, Response (0x02), id 189, Value 77e8564623f982056917d24318a91c5d, Name wztech3
18:41:45.939444 Out PPPoE  [ses 1]CHAP, Success (0x03), id 189, Msg
18:41:45.941524  In PPPoE  [ses 1]IPCP, Conf-Request (0x01), id 33, length 24
18:41:45.941527  In PPPoE  [ses 1]IP6CP, Conf-Request (0x01), id 14, length 16
18:41:45.941892 Out PPPoE  [ses 1]IPCP, Conf-Request (0x01), id 120, length 12
18:41:45.941931 Out PPPoE  [ses 1]IPCP, Conf-Nack (0x03), id 33, length 24
18:41:45.942064 Out PPPoE  [ses 1]IP6CP, Conf-Request (0x01), id 134, length 16
18:41:45.943479  In PPPoE  [ses 1]IPCP, Conf-Ack (0x02), id 120, length 12
18:41:45.943804  In PPPoE  [ses 1]IPCP, Conf-Request (0x01), id 34, length 24
18:41:45.944135  In PPPoE  [ses 1]IP6CP, Conf-Ack (0x02), id 134, length 16
```

Para uma análise mais completa, os pacotes podem ser gravados em formato pcap e escritos em um arquivo. O arquivo pode ser baixado e analisado nos programas wireshark ou tcpdump:

```
admin@MX204-LAB-WZTECH> monitor traffic interface ae0 no-resolve no-domain-names size 1500 write-file
/var/tmp/sniffer.pcap
Address resolution is OFF.
Listening on ae0, capture size 1500 bytes

60 packets received by filter
0 packets dropped by kernel

admin@MX204-LAB-WZTECH> file list /var/tmp/sniffer.pcap detail
-rw-r--r--  1 admin wheel       9033 Sep 13 18:49 /var/tmp/sniffer.pcap
total files: 1
```

Os servidores RADIUS estão respondendo corretamente e não há fila de autenticação ou accounting?

```
admin@MX204-LAB-WZTECH> show network-access aaa radius-servers
  Profile: ACCESS-PROFILE
    Server address: 192.168.1.236
      Authentication port: 1812
      Preauthentication port: 1812
      Accounting port: 1813
      Status: UP
    Server address: 192.168.1.102
      Authentication port: 1812
      Preauthentication port: 1812
      Accounting port: 1813
      Status: UP

admin@MX204-LAB-WZTECH> show network-access aaa radius-servers detail | match pending
    Authentication requests pending: 0
    Preauthentication requests pending: 0
    Accounting requests pending: 0
    Authentication requests pending: 0
    Preauthentication requests pending: 0
    Accounting requests pending: 0
```

O RADIUS está respondendo a requisição do usuário que está tentando autenticar? O RADIUS está enviando Access-Accept? Quais AVP's estão sendo enviados do RADIUS para o BNG?

Esta análise pode ser feita capturando os pacotes para os servidores RADIUS:

```
admin@MX204-LAB-WZTECH> show route 192.168.1.236

inet.0: 9 destinations, 9 routes (9 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.1.0/24     *[Direct/0] 10:24:40
                    >  via xe-0/1/1.0
```

O servidor RADIUS está sendo conhecido no MX pela interface xe-0/1/1.

```
admin@MX204-LAB-WZTECH> monitor traffic interface xe-0/1/1 size 1500 no-resolve no-domain-names matching "host
192.168.1.236" write-file /var/tmp/snifferradius.pcap
```

```
Address resolution is OFF.
Listening on fxp0, capture size 1500 bytes

1381 packets received by filter
0 packets dropped by kernel

admin@MX204-LAB-WZTECH> file list /var/tmp/snifferradius.pcap detail
-rw-r--r--  1 admin wheel       5865 Sep 13 18:53 /var/tmp/snifferradius.pcap
total files: 1
```

Caso o RADIUS esteja respondendo ou a requisição não esteja sendo enviada para o RADIUS pode-se fazer um debug no BNG:

```
set system processes general-authentication-service traceoptions file general.log
set system processes general-authentication-service traceoptions file size 10m
set system processes general-authentication-service traceoptions file files 5
set system processes general-authentication-service traceoptions flag all
```

Este comando vai ligar o traceoptions (debug) no processo general-autentication-service capturando todas as flags disponíveis. Vão ser gerados até 5 arquivos de no máximo 10MB. Caso chegue nesse limite os eventos serão rotacionados. O nome do arquivo gerado será general.log. Estes arquivos são gerados no diretório /var/log.

```
admin@MX204-LAB-WZTECH> file list /var/log detail | match general.log
-rw-r-----  1 root  wheel     278241 Sep 13 19:05 general.log
-rw-r--r--  1 root  wheel        768 Sep 13 18:58 general.log_enc
```

Para limpar um arquivo de log pode-se dar o comando "clear log":

```
admin@MX204-LAB-WZTECH> clear log general.log

admin@MX204-LAB-WZTECH> show log general.log
Sep 13 19:05:37 MX204-LAB-WZTECH clear-log[44881]: logfile cleared
```

O arquivo general.log gerado é um arquivo de debug com várias entradas:

```
Sep 13 19:08:18 MX204-LAB-WZTECH clear-log[44993]: logfile cleared
Sep 13 19:08:24.320344 Process/Dispatch Client Message
Sep 13 19:08:24.320376 New Process/Dispatch Client Message
Sep 13 19:08:24.320402 authd_tlv_build_list_from_struct username l =1 offset =56
Sep 13 19:08:24.320420 authd_tlv_build_list_from_struct profile l =1 offset =57
Sep 13 19:08:24.320437 authd_tlv_build_list_from_struct password l =1 offset =58
Sep 13 19:08:24.320454 authd_auth_aaa_msg_create: num_of_tlvs:0 tot_num_of_tlv:0
Sep 13 19:08:24.320468 authd_auth_aaa_msg_create username:() profile:()
Sep 13 19:08:24.320482 Process Request
Sep 13 19:08:24.320502 SEQ RecvClientMsg:jpppd-client session-id:334 Opcode:4929, Subcode:0 (ACCESS_REQUEST)
Sep 13 19:08:24.320520 Taking a client snapshot, session-id:334
Sep 13 19:08:24.320542 getSubscriberAaaOptionsName
Sep 13 19:08:24.320560 authd_build_req_attr_list_from_sdb_data: The request list is from sdb
Sep 13 19:08:24.320576 Taking a client snapshot, session-id:334
Sep 13 19:08:24.320589 authd_build_req_attr_list_from_sdb_data: The request list is from aaa_msg
Sep 13 19:08:24.320608  Performing domain-map check for session:334 with username:wztech3
Sep 13 19:08:24.320624 domain parse-direction:RtoL, domain-delimiter: "@" username:wztech3 domain to map:
Sep 13 19:08:24.320639  Performing domain-map check for session:334 with username:wztech3
Sep 13 19:08:24.320654 no configured sub-domain, using un-qualified domain:none
Sep 13 19:08:24.320670 Domain map lookup results for user:wztech3, parsed domain:, mapped domain:NONE, session-id:334,
qualified:none
Sep 13 19:08:24.320696 findSession AST-Table couldn't find the session-id:334
Sep 13 19:08:24.320711 Finding a client snapshot session-id:334
Sep 13 19:08:24.320797 createSubscriberSession session-id:334
Sep 13 19:08:24.320813 Taking a client snapshot, session-id:334
Sep 13 19:08:24.320830 createSubscriberSession UserName (wztech3) for session-id:334 from SDB
Sep 13 19:08:24.320848 createSubscriberSession SDB_CLIENT_SESSION_TYPE is 64
Sep 13 19:08:24.320874 AaaService::RoutingContext::ctor/default, ls default, ri default, tn null
Sep 13 19:08:24.320891 AaaService::RoutingContext::ctor/default, ls default, ri default, tn null
Sep 13 19:08:24.320908 Creating SubscriberASTEntry for session-id:334, session name:wztech3
Sep 13 19:08:24.320948 fillSessionDBAttributes: attr type 10005
Sep 13 19:08:24.320965 fillSessionDBAttributes: attr type 10169
Sep 13 19:08:24.320979 fillSessionDBAttributes: attr type 10076
Sep 13 19:08:24.321005 fillSessionDBAttributes: attr type 10081
Sep 13 19:08:24.321021 fillSessionDBAttributes: attr type 10185
Sep 13 19:08:24.321038 fillSessionDBAttributes: session-id:334, ifdName: ae0
Sep 13 19:08:24.321058 initialize: Found Bbe Flow Id 274 in SDB for session-id:334
Sep 13 19:08:24.321077 initialize: : Found the access-profile in the SDB for session-id:334 access-profile: ACCESS-
PROFILE, tn_name
Sep 13 19:08:24.321093 ActiveSessionTable::ActiveSessionTableEntry::setAccessProfileName: ACCESS-PROFILE
```

```
Sep 13 19:08:24.321110 initialize: Bbe Domain Id found in the SDB for session-id:334
Sep 13 19:08:24.321126 initialize: PhyIfdName found in the SDB for session-id:334
Sep 13 19:08:24.321144 initialize: InterfaceName found in the SDB for session-id:334
Sep 13 19:08:24.321164 initialize: aaa ls:default aaa ri:default; target ls:default target ri: default
Sep 13 19:08:24.321181 AaaService::RoutingContext::assign, ls default, ri default, tn null
Sep 13 19:08:24.321198 setTargetRoutingContextdefault:default
Sep 13 19:08:24.321212 AaaService::RoutingContext::assign, ls default, ri default, tn null
Sep 13 19:08:24.321228 setRoutingContext: Access Profile Name is <ACCESS-PROFILE> on LR/RI:default:default
Sep 13 19:08:24.321250 authd_build_radius_nas_port_and_id: nas-port-id-format order is disabled
Sep 13 19:08:24.321263 authd_build_req_attr_list_from_sdb_data: The request list is from aaa_msg
Sep 13 19:08:24.321278 Taking a client snapshot, session-id:334
```

Com é um arquivo de debug é possível analisar linha a linha para tentar identificar indícios de problemas ou também tentar filtrar por erros, timeouts, radius, etc... Exemplo:

```
admin@MX204-LAB-WZTECH> show log general.log | match timeout
Sep 13 19:00:06.224041 RadiusServer: server[0] used for last request - 192.168.1.236 timeout
Sep 13 19:00:06.224072 RadiusServer: 192.168.1.236 timeout (g:10, r:120)
Sep 13 19:00:06.224085 RadiusServer: marking current time for initial timeout for 192.168.1.236
Sep 13 19:00:06.224113 RadiusServer: 192.168.1.102 timeout (g:10, r:120)
Sep 13 19:00:06.224124 RadiusServer: marking current time for initial timeout for 192.168.1.102
Sep 13 19:00:06.224145 Radius result is CLIENT_REQ_TIMEOUT
Sep 13 19:00:06.224158 authd_radius_acctg_callback Result is :(CLIENT_REQ_TIMEOUT) reply_code:((null)) 0 session-id:270
Sep 13 19:00:06.224813 RadiusServer: server[0] used for last request - 192.168.1.236 timeout
```

Muito importante também avaliar os logs que estão sendo gerados no arquivo messages. Este é o arquivo de log principal do MX e fica no diretório /var/log:

```
admin@MX204-LAB-WZTECH> show log messages | match radius
Sep 12 09:00:37  MX204-LAB-WZTECH authd[19564]: AUTHD_RADIUS_SERVER_STATUS_CHANGE: Status of radius server 192.168.1.236
set to ALIVE (profile ACCESS-PROFILE)
Sep 12 09:00:44  MX204-LAB-WZTECH authd[19564]: AUTHD_RADIUS_SERVER_STATUS_CHANGE: Status of radius server 192.168.1.102
set to UNREACHABLE (profile ACCESS-PROFILE)
Sep 12 09:01:14  MX204-LAB-WZTECH authd[19564]: AUTHD_RADIUS_SERVER_STATUS_CHANGE: Status of radius server 192.168.1.102
set to ALIVE (profile ACCESS-PROFILE)
Sep 12 09:01:38  MX204-LAB-WZTECH authd[19564]: AUTHD_RADIUS_SERVER_STATUS_CHANGE: Status of radius server 192.168.1.236
set to DEAD (profile ACCESS-PROFILE)
```


Também pode ser ligado o debug do daemon de DHCP no MX caso o problema esteja relacionado com o protocolo DHCP dentro do túnel PPPoE:

```
set system processes dhcp-service traceoptions file dhcp_logfile
set system processes dhcp-service traceoptions file size 10m
set system processes dhcp-service traceoptions file files 5
set system processes dhcp-service traceoptions level all
set system processes dhcp-service traceoptions flag all
```

Os arquivos serão gravados ambém no diretório /var/log:

```
admin@MX204-LAB-WZTECH> file list detail /var/log | match dhcp_logfile
-rw-r-----  1 root  wheel     778637 Sep 13 21:37 dhcp_logfile
```

```
admin@MX204-LAB-WZTECH> show log dhcp_logfile
Jul 20 16:27:35.937818 [MSTR][DEBUG] jdhcpd_dns_write_resolv: open fp file name /etc/resolv.conf, fp_tmp file name
/var/tmp/resolv_tmp.conf
Jul 20 16:27:36.163537 [MSTR][DEBUG][default:default][CLN][INET6][fxp0.0] dhcpv6_client_proto_start: new client table
entry created for ifindex 9
Jul 20 16:27:36.163980 [MSTR][DEBUG][default:default][CLN][INET6][fxp0.0][SID=0] dhcpv6_client_reload_config: Rapid
commit is not configured
Jul 20 16:27:36.164008 [MSTR][DEBUG] dhcpv6_client_reload_config: update_ra_cfg not changed
Jul 20 16:27:36.165764 [MSTR][DEBUG][default:default][CLN][INET6][fxp0.0][SID=0] dhcpv6_client_subscribe_ra: Subscribing
RA. ra_server_len = 0
Jul 20 16:27:36.165914 [MSTR][DEBUG][default:default][CLN][INET6][fxp0.0][SID=0] dhcpv6_client_subscribe_ra: RPD RA add
failed (Unknown error: -1)
Jul 20 16:27:36.166061 [MSTR][DEBUG][default:default][CLN][INET6][fxp0.0][SID=0] jdhcp_v6_client_pdu_send: Preparing to
send 1 PDU
Jul 20 16:27:36.166931 [MSTR][DEBUG] dhcpv6_packet_info_new: PACKET - Allocated new v6 packet 0x552da80
Jul 20 16:27:36.166959 [MSTR][DEBUG][default:default][CLN][INET6][fxp0.0][SID=0] jdhcp_v6_client_pdu_send: Vendor Id =
Juniper:mx204:BM749 Size 19
Jul 20 16:27:36.166977 [MSTR][DEBUG][default:default][CLN][INET6][fxp0.0][SID=0] jdhcp_v6_client_pdu_send:
Dump of 1 PDU to be sent

Jul 20 16:27:36.170571 [MSTR][INFO] [default:default][CLN][INET6][fxp0.0] >>>>>>>>>> Decode message from == ::/0
<<<<<<<<<<
Jul 20 16:27:36.171951 [MSTR][INFO] [default:default][CLN][INET6][fxp0.0] --[ msgtype == DHCPV6-SOLICIT ]----------------
----------
```

```
Jul 20 16:27:36.171984 [MSTR][INFO] [default:default][CLN][INET6][fxp0.0] --[ len == 75 ]--
Jul 20 16:27:36.172002 [MSTR][INFO] [default:default][CLN][INET6][fxp0.0] --[ xid == 21576e ]--
Jul 20 16:27:36.173522 [MSTR][INFO] [default:default][CLN][INET6][fxp0.0] --[ OPTION_CLIENTID
Jul 20 16:27:36.173563 [MSTR][INFO] [default:default][CLN][INET6][fxp0.0]       OPTION code   1, len  10, data 00 03 00
01 20 d8 0b fb 4a 1e ]--
Jul 20 16:27:36.173582 [MSTR][INFO] [default:default][CLN][INET6][fxp0.0] --[ OPTION_VENDOR_CLASS
Jul 20 16:27:36.173607 [MSTR][INFO] [default:default][CLN][INET6][fxp0.0]       OPTION code  16, len  25, data 00 00 05
83 00 13 4a 75 6e 69 70 65 72 3a 6d 78 32 30 34 3a 42 4d 37 34 39 ]--
Jul 20 16:27:36.173623 [MSTR][INFO] [default:default][CLN][INET6][fxp0.0] --[ OPTION_IA_NA
Jul 20 16:27:36.173659 [MSTR][INFO] [default:default][CLN][INET6][fxp0.0]       OPTION code   3, len  12, iaid 0, T1
4294967295, T2 4294967295 ]--
Jul 20 16:27:36.173676 [MSTR][INFO] [default:default][CLN][INET6][fxp0.0] --[ OPTION_OPT_REQ
Jul 20 16:27:36.173694 [MSTR][INFO] [default:default][CLN][INET6][fxp0.0]       OPTION code   6, len   8, data 00 11 00
3b 00 3c 00 38 ]--
Jul 20 16:27:36.173711 [MSTR][DEBUG][default:default][CLN][INET6][fxp0.0] dhcpv6_option_parse:     Parsing suboptions of
OPTION_IA_NA - Start
Jul 20 16:27:36.173727 [MSTR][DEBUG][default:default][CLN][INET6][fxp0.0] dhcpv6_option_parse:     Parsing suboptions of
OPTION_IA_NA - Done
Jul 20 16:27:36.173743 [MSTR][DEBUG][default:default][CLN][INET6][fxp0.0] dhcpv6_packet_decode: dhcpv6 pkt parsing - End
Jul 20 16:27:36.173831 [MSTR][DEBUG] dhcpv6_packet_free: PACKET - Freeing v6 packet 0x552da80
Jul 20 16:27:36.174042 [MSTR][DEBUG][default:default][CLN][INET][fxp0.0] jdhcpd_client_proto_start: new client table
entry created for ifindex 9
Jul 20 16:27:36.174114 [MSTR][DEBUG][default:default][CLN][INET][fxp0.0][SID=0] jdhcpd_client_pdu_send: Preparing to send
0 PDU
Jul 20 16:27:36.174131 [MSTR][DEBUG] jdhcpd_packet_info_new: PACKET - Allocated new v4 packet 0x54e9390
Jul 20 16:27:36.174159 [MSTR][DEBUG][default:default][CLN][INET][fxp0.0][SID=0] jdhcpd_client_pdu_send:
```

Como é um arquivo de debug (traceoptions) é necessário fazer a análise em cima do arquivo.

Importante: A partir do momento que for feito o troubleshooting é necessário desativar o traceoptions pois este é um processo que vai exigir muito processamento da Routing Engine e deve ficar sempre desativado no equipamento no dia a dia e deve ser utilizado com cautela.

```
admin@MX204-LAB-WZTECH> configure
Entering configuration mode

[edit]
admin@MX204-LAB-WZTECH# deactivate system processes general-authentication-service

[edit]
admin@MX204-LAB-WZTECH# deactivate system processes dhcp-service

[edit]
admin@MX204-LAB-WZTECH# commit and-quit
commit complete
Exiting configuration mode

admin@MX204-LAB-WZTECH>
```

19. Firewall Filter Routing Engine (Loopback)

Conforme já mencionado anteriormente o MX possui a PFE (Packet Forwarding Engine) que é o plano de encaminhamento de pacotes e onde é comutado todos os pacotes que passam pelo equipamento. Também existe no MX o plano de controle (Routing Engine) que é responsável por tratar pacotes de administração, processar os pacotes dos protocolos de roteamento dinâmico, gerência e também os pacotes de controle dos protocolos utilizados no serviço de BNG (PPPoE, DHCPv6, ICMPv6, etc.). Neste caso não são pacotes que passam pelo equipamento mas sim pacotes destinados ao próprio roteador.

É altamente recomendado que a Routing-Engine tenha configurações de proteção liberando apenas os recursos necessários que precisam se comunicar com o roteador como SSH, ICMP, DHCP, BGP etc., minimizando assim a exposição do equipamento a ataques que possam gerar impacto no serviço que está no equipamento.

No MX para que seja feito um filtro de proteção à Routing Engine é necessário que esta firewall firewall seja aplicada na interace lo0 que é a interface loopback. Neste caso os pacotes destinados ao MX antes de chegarem na Routing Engine serão avaliados na PFE e caso não sejam permitidos serão descartados.

A seguir são colocados exemplos de firewall filter IPv4 e IPv6 para serem aplicadas na interface loopback do BNG. Cada ambiente tem suas particularidades e a firewall filter deve ser ajustada para ficar mais ou menos restritiva de acordo com cada ambiente. Alguns termos dos exemplos também podem não se aplicar ao ambiente e dependendo do ambiente pode ser removido e dependendo do ambiente talvez seja necessário a

adição de outros termos para tratar outros protocolos. As firewall filters a seguir são exemplos e o provedor deve avaliar internamente as necessidades do ambiente. Os endereços IPv4 e IPv6 usados nos exemplos são fictícios. Os endereços corretos do ambiente devem ser usados na configuração da firewall filter.

Firewall Filter Loopback - IPv4

```
set firewall policer limit-icmp if-exceeding bandwidth-limit 5m
set firewall policer limit-icmp if-exceeding burst-size-limit 15k
set firewall policer limit-icmp then discard

set firewall policer limit-traceroute if-exceeding bandwidth-limit 1m
set firewall policer limit-traceroute if-exceeding burst-size-limit 625k
set firewall policer limit-traceroute then discard

set policy-options prefix-list dns-addresses apply-path "system name-server <*>"

set policy-options prefix-list ntp-addresses apply-path "system ntp server <*>"

set policy-options prefix-list bgp-peers apply-path "protocols bgp group <*> neighbor <*>"

set policy-options prefix-list bgp-peers-vpn apply-path "routing-instances <*> protocols bgp group <*> neighbor <*>"

set policy-options prefix-list tacacs-addresses apply-path "system tacplus-server <*>"

set policy-options prefix-list radius-addresses apply-path "access radius-server <*>"

set policy-options prefix-list radius-addresses-access-profile apply-path "access profile <*> radius-server <*>"

set policy-options prefix-list interfaces-addresses apply-path "interfaces <*> unit <*> family inet address <*>"


set policy-options prefix-list ssh-addresses 200.233.196.24/29
set policy-options prefix-list ssh-addresses 200.233.174.134/32
set policy-options prefix-list ssh-addresses 192.168.1.0/24

set policy-options prefix-list snmp-addresses 200.233.196.24/29
set policy-options prefix-list snmp-addresses 200.233.174.134/32
set policy-options prefix-list snmp-addresses 192.168.1.0/24

set firewall family inet filter PROTEGE-RE-IPV4 term icmp from protocol icmp
set firewall family inet filter PROTEGE-RE-IPV4 term icmp then policer limit-icmp
set firewall family inet filter PROTEGE-RE-IPV4 term icmp then accept

set firewall family inet filter PROTEGE-RE-IPV4 term ssh from source-prefix-list ssh-addresses
set firewall family inet filter PROTEGE-RE-IPV4 term ssh from protocol tcp
set firewall family inet filter PROTEGE-RE-IPV4 term ssh from port ssh
set firewall family inet filter PROTEGE-RE-IPV4 term ssh then accept

set firewall family inet filter PROTEGE-RE-IPV4 term snmp from source-prefix-list snmp-addresses
set firewall family inet filter PROTEGE-RE-IPV4 term snmp from protocol udp
set firewall family inet filter PROTEGE-RE-IPV4 term snmp from port snmp
set firewall family inet filter PROTEGE-RE-IPV4 term snmp then accept

set firewall family inet filter PROTEGE-RE-IPV4 term dns from source-prefix-list dns-addresses
set firewall family inet filter PROTEGE-RE-IPV4 term dns from protocol udp
set firewall family inet filter PROTEGE-RE-IPV4 term dns from protocol tcp
set firewall family inet filter PROTEGE-RE-IPV4 term dns from port domain
set firewall family inet filter PROTEGE-RE-IPV4 term dns then accept

set firewall family inet filter PROTEGE-RE-IPV4 term ntp from source-prefix-list ntp-addresses
set firewall family inet filter PROTEGE-RE-IPV4 term ntp from protocol udp
set firewall family inet filter PROTEGE-RE-IPV4 term ntp from protocol tcp
set firewall family inet filter PROTEGE-RE-IPV4 term ntp from port ntp
set firewall family inet filter PROTEGE-RE-IPV4 term ntp then accept

set firewall family inet filter PROTEGE-RE-IPV4 term bgp from source-prefix-list bgp-peers
set firewall family inet filter PROTEGE-RE-IPV4 term bgp from source-prefix-list bgp-peers-vpn
set firewall family inet filter PROTEGE-RE-IPV4 term bgp from protocol tcp
set firewall family inet filter PROTEGE-RE-IPV4 term bgp from port bgp
set firewall family inet filter PROTEGE-RE-IPV4 term bgp then accept

set firewall family inet filter PROTEGE-RE-IPV4 term tacacs from source-prefix-list tacacs-addresses
set firewall family inet filter PROTEGE-RE-IPV4 term tacacs from protocol tcp
set firewall family inet filter PROTEGE-RE-IPV4 term tacacs from port 49
set firewall family inet filter PROTEGE-RE-IPV4 term tacacs then accept

set firewall family inet filter PROTEGE-RE-IPV4 term bfd from protocol udp
set firewall family inet filter PROTEGE-RE-IPV4 term bfd from source-port 49152-65535
set firewall family inet filter PROTEGE-RE-IPV4 term bfd from destination-port 3784-3785
set firewall family inet filter PROTEGE-RE-IPV4 term bfd from destination-port 4784
```

```
set firewall family inet filter PROTEGE-RE-IPV4 term bfd from destination-port 6784
set firewall family inet filter PROTEGE-RE-IPV4 term bfd then accept

set firewall family inet filter PROTEGE-RE-IPV4 term ldp from protocol udp
set firewall family inet filter PROTEGE-RE-IPV4 term ldp from protocol tcp
set firewall family inet filter PROTEGE-RE-IPV4 term ldp from port 646
set firewall family inet filter PROTEGE-RE-IPV4 term ldp then accept

set firewall family inet filter PROTEGE-RE-IPV4 term radius from source-prefix-list radius-addresses
set firewall family inet filter PROTEGE-RE-IPV4 term radius from source-prefix-list radius-addresses-access-profile
set firewall family inet filter PROTEGE-RE-IPV4 term radius from protocol tcp
set firewall family inet filter PROTEGE-RE-IPV4 term radius from protocol udp
set firewall family inet filter PROTEGE-RE-IPV4 term radius from port 1812
set firewall family inet filter PROTEGE-RE-IPV4 term radius from port 1813
set firewall family inet filter PROTEGE-RE-IPV4 term radius then accept

set firewall family inet filter PROTEGE-RE-IPV4 term ospf from protocol ospf
set firewall family inet filter PROTEGE-RE-IPV4 term ospf then accept

set firewall family inet filter PROTEGE-RE-IPV4 term rsvp from protocol rsvp
set firewall family inet filter PROTEGE-RE-IPV4 term rsvp then accept

set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-udp from destination-prefix-list interfaces-
addresses
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-udp from protocol udp
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-udp from ttl 1
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-udp from destination-port 33435-33450
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-udp then policer limit-traceroute
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-udp then accept

set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-icmp from destination-prefix-list interfaces-
addresses
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-icmp from protocol icmp
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-icmp from ttl 1
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-icmp from icmp-type echo-request
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-icmp from icmp-type timestamp
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-icmp from icmp-type time-exceeded
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-icmp then policer limit-traceroute
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-icmp then accept

set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-tcp from destination-prefix-list interfaces-
addresses
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-tcp from protocol tcp
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-tcp from ttl 1
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-tcp then policer limit-traceroute
set firewall family inet filter PROTEGE-RE-IPV4 term accept-traceroute-tcp then accept

set firewall family inet filter PROTEGE-RE-IPV4 term discard then discard


set interfaces lo0 unit 0 family inet filter input PROTEGE-RE-IPV4
```

Firewall Filter Loopback - IPv6

```
set firewall policer limit-icmp-v6 if-exceeding bandwidth-limit 5m
set firewall policer limit-icmp-v6 if-exceeding burst-size-limit 15k
set firewall policer limit-icmp-v6 then discard

set firewall policer limit-traceroute-v6 if-exceeding bandwidth-limit 1m
set firewall policer limit-traceroute-v6 if-exceeding burst-size-limit 625k
set firewall policer limit-traceroute-v6 then discard

set policy-options prefix-list dns-addresses apply-path "system name-server <*>"

set policy-options prefix-list ntp-addresses apply-path "system ntp server <*>"

set policy-options prefix-list bgp-peers apply-path "protocols bgp group <*> neighbor <*>"

set policy-options prefix-list tacacs-addresses apply-path "system tacplus-server <*>"

set policy-options prefix-list radius-addresses apply-path "access radius-server <*>"

set policy-options prefix-list radius-addresses-access-profile apply-path "access profile <*> radius-server <*>"

set policy-options prefix-list ssh-addresses-v6 2804:2804::0/64

set policy-options prefix-list snmp-addresses-v6 2805:2804::0/64


set firewall family inet6 filter PROTEGE-RE-IPV6 term bloqueia-ra from next-header icmp6
set firewall family inet6 filter PROTEGE-RE-IPV6 term bloqueia-ra from icmp-type router-solicit
```

```
set firewall family inet6 filter PROTEGE-RE-IPV6 term bloqueia-ra from icmp-type router-advertisement
set firewall family inet6 filter PROTEGE-RE-IPV6 term bloqueia-ra then discard

set firewall family inet6 filter PROTEGE-RE-IPV6 term dhcp from next-header udp
set firewall family inet6 filter PROTEGE-RE-IPV6 term dhcp from destination-port 546
set firewall family inet6 filter PROTEGE-RE-IPV6 term dhcp from destination-port 547
set firewall family inet6 filter PROTEGE-RE-IPV6 term dhcp then accept

set firewall family inet6 filter PROTEGE-RE-IPV6 term icmp from next-header icmp6
set firewall family inet6 filter PROTEGE-RE-IPV6 term icmp from icmp-type echo-request
set firewall family inet6 filter PROTEGE-RE-IPV6 term icmp from icmp-type echo-reply
set firewall family inet6 filter PROTEGE-RE-IPV6 term icmp then policer limit-icmp-v6
set firewall family inet6 filter PROTEGE-RE-IPV6 term icmp then accept

set firewall family inet6 filter PROTEGE-RE-IPV6 term ssh from source-prefix-list ssh-addresses-v6
set firewall family inet6 filter PROTEGE-RE-IPV6 term ssh from next-header tcp
set firewall family inet6 filter PROTEGE-RE-IPV6 term ssh from port ssh
set firewall family inet6 filter PROTEGE-RE-IPV6 term ssh then accept

set firewall family inet6 filter PROTEGE-RE-IPV6 term snmp from source-prefix-list snmp-addresses-v6
set firewall family inet6 filter PROTEGE-RE-IPV6 term snmp from next-header udp
set firewall family inet6 filter PROTEGE-RE-IPV6 term snmp from port snmp
set firewall family inet6 filter PROTEGE-RE-IPV6 term snmp then accept

set firewall family inet6 filter PROTEGE-RE-IPV6 term dns from source-prefix-list dns-addresses
set firewall family inet6 filter PROTEGE-RE-IPV6 term dns from next-header udp
set firewall family inet6 filter PROTEGE-RE-IPV6 term dns from next-header tcp
set firewall family inet6 filter PROTEGE-RE-IPV6 term dns from port domain
set firewall family inet6 filter PROTEGE-RE-IPV6 term dns then accept

set firewall family inet6 filter PROTEGE-RE-IPV6 term ntp from source-prefix-list ntp-addresses
set firewall family inet6 filter PROTEGE-RE-IPV6 term ntp from next-header udp
set firewall family inet6 filter PROTEGE-RE-IPV6 term ntp from next-header tcp
set firewall family inet6 filter PROTEGE-RE-IPV6 term ntp from port ntp
set firewall family inet6 filter PROTEGE-RE-IPV6 term ntp then accept

set firewall family inet6 filter PROTEGE-RE-IPV6 term bgp from source-prefix-list bgp-peers
set firewall family inet6 filter PROTEGE-RE-IPV6 term bgp from source-prefix-list bgp-peers-vpn
set firewall family inet6 filter PROTEGE-RE-IPV6 term bgp from next-header tcp
set firewall family inet6 filter PROTEGE-RE-IPV6 term bgp from port bgp
set firewall family inet6 filter PROTEGE-RE-IPV6 term bgp then accept

set firewall family inet6 filter PROTEGE-RE-IPV6 term tacacs from source-prefix-list tacacs-addresses
set firewall family inet6 filter PROTEGE-RE-IPV6 term tacacs from next-header tcp
set firewall family inet6 filter PROTEGE-RE-IPV6 term tacacs from port 49
set firewall family inet6 filter PROTEGE-RE-IPV6 term tacacs then accept

set firewall family inet6 filter PROTEGE-RE-IPV6 term bfd from next-header udp
set firewall family inet6 filter PROTEGE-RE-IPV6 term bfd from source-port 49152-65535
set firewall family inet6 filter PROTEGE-RE-IPV6 term bfd from destination-port 3784-3785
set firewall family inet6 filter PROTEGE-RE-IPV6 term bfd from destination-port 4784
set firewall family inet6 filter PROTEGE-RE-IPV6 term bfd from destination-port 6784
set firewall family inet6 filter PROTEGE-RE-IPV6 term bfd then accept

set firewall family inet6 filter PROTEGE-RE-IPV6 term radius from source-prefix-list radius-addresses
set firewall family inet6 filter PROTEGE-RE-IPV6 term radius from source-prefix-list radius-addresses-access-profile
set firewall family inet6 filter PROTEGE-RE-IPV6 term radius from next-header tcp
set firewall family inet6 filter PROTEGE-RE-IPV6 term radius from next-header udp
set firewall family inet6 filter PROTEGE-RE-IPV6 term radius from port 1812
set firewall family inet6 filter PROTEGE-RE-IPV6 term radius from port 1813
set firewall family inet6 filter PROTEGE-RE-IPV6 term radius then accept

set firewall family inet6 filter PROTEGE-RE-IPV6 term discard then discard


set interfaces lo0 unit 0 family inet6 filter input PROTEGE-RE-IPV6
```

20. DDoS Protection

O mecanismo de DDoS Protection também é um mecanismo para proteção do plano de Controle do MX onde o roteador possui limiares (thresholds) padrões configurados para mitigar altos volumes de pacotes (permitidos) destinados à Routing Engine. Estes controles podem ser feitos no nível da PFE, FPC, Routing Engine, etc, e depende do modelo e arquitetura do equipamento.

Figure 1: Policer Hierarchy for PPPoE Packets

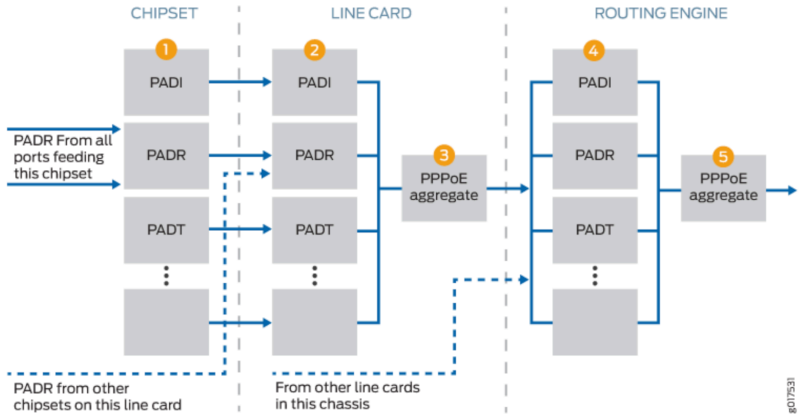
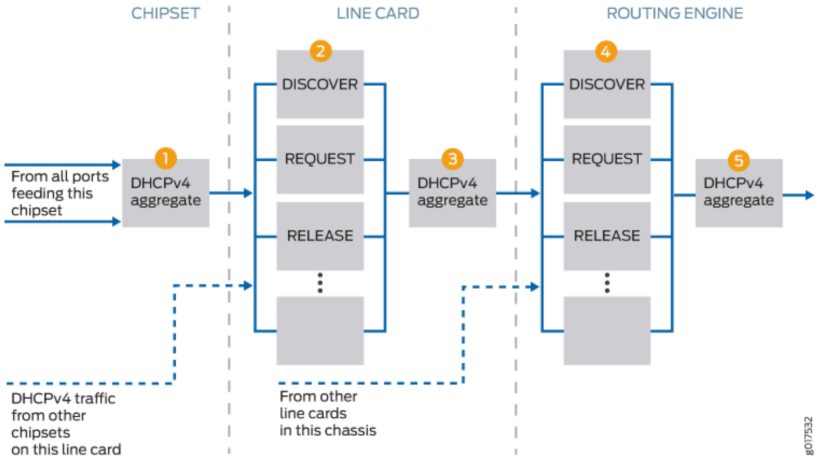


Figure 2: Policer Hierarchy for DHCPv4 Packets



O comando abaixo mostra os valores padrões para o protocolo PPPoE e DHCPv6 para o roteador MX204. Para pacotes PADI por exemplo o MX possui um limite padrão de 500 pacotes por segundo que são aceitos na FPC 0. Caso o valor de pacotes PADI ultrapasse o valor de 500 pacotes por segundo será considerada uma violação e o mecanismo de DDoS Protection vai policiar este tráfego específico limitando a 500pps. Já para o protocolo PPPoE como um todo (independente do tipo do pacote) há um limite agregado total na FPC de 2500 pacotes por segundo. Caso este volume seja atingido na FPC o MX fará o policiamento dos pacotes de PPPoE limitando o fluxo para a Routing Engine em 2500 pacotes por segundo. Neste caso será gerado uma violação.

```
admin@MX204-LAB-WZTECH> show ddos-protection protocols pppoe
Packet types: 9, Modified: 0, Received traffic: 4, Currently violated: 0
Currently tracked flows: 0, Total detected flows: 0
* = User configured value

Protocol Group: PPPoE

  Packet type: aggregate (Aggregate for all PPPoE control traffic)
    Aggregate policer configuration:
      Bandwidth:          2500 pps
      Burst:              2500 packets
      Recover time:       300 seconds
      Enabled:            Yes
    System-wide information:
      Aggregate bandwidth is never violated
      Received:  1050               Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 1 pps
    Routing Engine information:
      Bandwidth: 2500 pps, Burst: 2500 packets, enabled
      Aggregate policer is never violated
      Received:  1050               Arrival rate:     0 pps
```

```
    Dropped:   0                  Max arrival rate: 1 pps
      Dropped by individual policers: 0
  FPC slot 0 information:
    Bandwidth: 100% (2500 pps), Burst: 100% (2500 packets), enabled
    Hostbound queue 255
    Aggregate policer is never violated
    Received:  1050               Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 1 pps
      Dropped by individual policers: 0
      Dropped by flow suppression:    0

Packet type: padi (PPPoE PADI)
  Individual policer configuration:
    Bandwidth:        500 pps
    Burst:            500 packets
    Priority:         Low
    Recover time:     300 seconds
    Enabled:          Yes
    Bypass aggregate: No
  Flow detection configuration:
    Flow detection system is off
    Detection mode: Automatic  Detect time:  3 seconds
    Log flows:      Yes        Recover time: 60 seconds
    Timeout flows:  No         Timeout time: 300 seconds
    Flow aggregation level configuration:
      Aggregation level   Detection mode  Control mode  Flow rate
      Subscriber          Automatic       Drop          10 pps
      Logical interface   Automatic       Drop          10 pps
      Physical interface  Automatic       Drop          500 pps
  System-wide information:
    Bandwidth is never violated
    Received:  695                Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
  Routing Engine information:
    Bandwidth: 500 pps, Burst: 500 packets, enabled
    Policer is never violated
    Received:  695                Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 0 information:
    Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
    Hostbound queue 2
    Policer is never violated
    Received:  695                Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
      Dropped by flow suppression:  0

Packet type: pado (PPPoE PADO)
  Individual policer configuration:
    Bandwidth:        0 pps
    Burst:            0 packets
    Priority:         Low
    Recover time:     300 seconds
    Enabled:          Yes
    Bypass aggregate: No
  Flow detection configuration:
    Flow detection system is off
    Detection mode: Automatic  Detect time:  3 seconds
    Log flows:      Yes        Recover time: 60 seconds
    Timeout flows:  No         Timeout time: 300 seconds
    Flow aggregation level configuration:
      Aggregation level   Detection mode  Control mode  Flow rate
      Subscriber          Automatic       Drop          10 pps
      Logical interface   Automatic       Drop          10 pps
      Physical interface  Automatic       Drop          0  pps
  System-wide information:
    Bandwidth is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
  Routing Engine information:
    Bandwidth: 0 pps, Burst: 0 packets, enabled
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 0 information:
    Bandwidth: 100% (0 pps), Burst: 100% (0 packets), enabled
    Hostbound queue 3
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
```

```
      Dropped by flow suppression:  0

  Packet type: padr (PPPoE PADR)
    Individual policer configuration:
      Bandwidth:        500 pps
      Burst:            500 packets
      Priority:         Medium
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    Flow detection configuration:
      Flow detection system is off
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      Yes        Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          500 pps
    System-wide information:
      Bandwidth is never violated
      Received:  179                Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Bandwidth: 500 pps, Burst: 500 packets, enabled
      Policer is never violated
      Received:  179                Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
    FPC slot 0 information:
      Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
      Hostbound queue 3
      Policer is never violated
      Received:  179                Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
        Dropped by flow suppression:  0

  Packet type: pads (PPPoE PADS)
    Individual policer configuration:
      Bandwidth:        0 pps
      Burst:            0 packets
      Priority:         Low
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    Flow detection configuration:
      Flow detection system is off
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      Yes        Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          0  pps
    System-wide information:
      Bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Bandwidth: 0 pps, Burst: 0 packets, enabled
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
    FPC slot 0 information:
      Bandwidth: 100% (0 pps), Burst: 100% (0 packets), enabled
      Hostbound queue 3
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
        Dropped by flow suppression:  0

  Packet type: padt (PPPoE PADT)
    Individual policer configuration:
      Bandwidth:        1000 pps
      Burst:            1000 packets
      Priority:         High
      Recover time:     300 seconds
      Enabled:          Yes
```

```
    Bypass aggregate: No
  Flow detection configuration:
    Flow detection system is off
    Detection mode: Automatic  Detect time:  3 seconds
    Log flows:      Yes        Recover time: 60 seconds
    Timeout flows:  No         Timeout time: 300 seconds
    Flow aggregation level configuration:
      Aggregation level   Detection mode  Control mode  Flow rate
      Subscriber          Automatic       Drop          10 pps
      Logical interface   Automatic       Drop          10 pps
      Physical interface  Automatic       Drop          1000 pps
  System-wide information:
    Bandwidth is never violated
    Received:  176                 Arrival rate:     0 pps
    Dropped:   0                   Max arrival rate: 0 pps
  Routing Engine information:
    Bandwidth: 1000 pps, Burst: 1000 packets, enabled
    Policer is never violated
    Received:  176                 Arrival rate:     0 pps
    Dropped:   0                   Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 0 information:
    Bandwidth: 100% (1000 pps), Burst: 100% (1000 packets), enabled
    Hostbound queue 3
    Policer is never violated
    Received:  176                 Arrival rate:     0 pps
    Dropped:   0                   Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
      Dropped by flow suppression:  0

Packet type: padm (PPPoE PADM)
  Individual policer configuration:
    Bandwidth:        0 pps
    Burst:            0 packets
    Priority:         Low
    Recover time:     300 seconds
    Enabled:          Yes
    Bypass aggregate: No
  Flow detection configuration:
    Flow detection system is off
    Detection mode: Automatic  Detect time:  3 seconds
    Log flows:      Yes        Recover time: 60 seconds
    Timeout flows:  No         Timeout time: 300 seconds
    Flow aggregation level configuration:
      Aggregation level   Detection mode  Control mode  Flow rate
      Subscriber          Automatic       Drop          10 pps
      Logical interface   Automatic       Drop          10 pps
      Physical interface  Automatic       Drop          0  pps
  System-wide information:
    Bandwidth is never violated
    Received:  0                   Arrival rate:     0 pps
    Dropped:   0                   Max arrival rate: 0 pps
  Routing Engine information:
    Bandwidth: 0 pps, Burst: 0 packets, enabled
    Policer is never violated
    Received:  0                   Arrival rate:     0 pps
    Dropped:   0                   Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 0 information:
    Bandwidth: 100% (0 pps), Burst: 100% (0 packets), enabled
    Hostbound queue 3
    Policer is never violated
    Received:  0                   Arrival rate:     0 pps
    Dropped:   0                   Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
      Dropped by flow suppression:  0

Packet type: padn (PPPoE PADN)
  Individual policer configuration:
    Bandwidth:        0 pps
    Burst:            0 packets
    Priority:         Low
    Recover time:     300 seconds
    Enabled:          Yes
    Bypass aggregate: No
  Flow detection configuration:
    Flow detection system is off
    Detection mode: Automatic  Detect time:  3 seconds
    Log flows:      Yes        Recover time: 60 seconds
    Timeout flows:  No         Timeout time: 300 seconds
    Flow aggregation level configuration:
      Aggregation level   Detection mode  Control mode  Flow rate
      Subscriber          Automatic       Drop          10 pps
```

```
      Logical interface   Automatic       Drop          10 pps
      Physical interface  Automatic       Drop          0  pps
  System-wide information:
    Bandwidth is never violated
    Received:  0                    Arrival rate:     0 pps
    Dropped:   0                    Max arrival rate: 0 pps
  Routing Engine information:
    Bandwidth: 0 pps, Burst: 0 packets, enabled
    Policer is never violated
    Received:  0                    Arrival rate:     0 pps
    Dropped:   0                    Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 0 information:
    Bandwidth: 100% (0 pps), Burst: 100% (0 packets), enabled
    Hostbound queue 3
    Policer is never violated
    Received:  0                    Arrival rate:     0 pps
    Dropped:   0                    Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
      Dropped by flow suppression:  0

Packet type: padse (PPPoE Session)
  Individual policer configuration:
    Bandwidth:        500 pps
    Burst:            500 packets
    Priority:         High
    Recover time:     300 seconds
    Enabled:          Yes
    Bypass aggregate: No
  Flow detection configuration:
    Flow detection system is off
    Detection mode: Automatic  Detect time:  3 seconds
    Log flows:      Yes        Recover time: 60 seconds
    Timeout flows:  No         Timeout time: 300 seconds
    Flow aggregation level configuration:
      Aggregation level   Detection mode  Control mode  Flow rate
      Subscriber          Automatic       Drop          10 pps
      Logical interface   Automatic       Drop          10 pps
      Physical interface  Automatic       Drop          500 pps
  System-wide information:
    Bandwidth is never violated
    Received:  0                    Arrival rate:     0 pps
    Dropped:   0                    Max arrival rate: 0 pps
  Routing Engine information:
    Bandwidth: 500 pps, Burst: 500 packets, enabled
    Policer is never violated
    Received:  0                    Arrival rate:     0 pps
    Dropped:   0                    Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 0 information:
    Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
    Hostbound queue 2
    Policer is never violated
    Received:  0                    Arrival rate:     0 pps
    Dropped:   0                    Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
      Dropped by flow suppression:  0
```

As violações caso existam podem ser obtidas com o comando:

```
admin@MX204-LAB-WZTECH> show ddos-protection protocols violations
Packet types: 241, Currently violated: 0

admin@MX204-LAB-WZTECH> show ddos-protection protocols pppoe violations
Packet types: 9, Currently violated:
```

Para analisar o estado de um tipo de pacote específico (PADI por exemplo) pode ser dado o comando especificando o tipo do pacote:

```
admin@MX204-LAB-WZTECH> show ddos-protection protocols pppoe padi
Currently tracked flows: 0, Total detected flows: 0
* = User configured value
Protocol Group: PPPoE

  Packet type: padi (PPPoE PADI)
    Individual policer configuration:
      Bandwidth:        500 pps
      Burst:            500 packets
      Priority:         Low
      Recover time:     300 seconds
```

```
    Enabled:          Yes
    Bypass aggregate: No
  Flow detection configuration:
    Flow detection system is off
    Detection mode: Automatic  Detect time:  3 seconds
    Log flows:      Yes        Recover time: 60 seconds
    Timeout flows:  No         Timeout time: 300 seconds
    Flow aggregation level configuration:
      Aggregation level   Detection mode  Control mode  Flow rate
      Subscriber          Automatic       Drop          10 pps
      Logical interface   Automatic       Drop          10 pps
      Physical interface  Automatic       Drop          500 pps
  System-wide information:
    Bandwidth is never violated
    Received:  695                 Arrival rate:     0 pps
    Dropped:   0                   Max arrival rate: 0 pps
  Routing Engine information:
    Bandwidth: 500 pps, Burst: 500 packets, enabled
    Policer is never violated
    Received:  695                 Arrival rate:     0 pps
    Dropped:   0                   Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 0 information:
    Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
    Hostbound queue 2
    Policer is never violated
    Received:  695                 Arrival rate:     0 pps
    Dropped:   0                   Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
      Dropped by flow suppression:  0
```

Isso vale também para o protocolo DHCPv6 por exemplo:

```
admin@MX204-LAB-WZTECH> show ddos-protection protocols dhcpv6 solicit
Currently tracked flows: 0, Total detected flows: 0
* = User configured value
Protocol Group: DHCPv6

  Packet type: solicit (DHCPv6 SOLICIT)
    Individual policer configuration:
      Bandwidth:          500 pps
      Burst:              500 packets
      Priority:           Low
      Recover time:       300 seconds
      Enabled:            Yes
      Bypass aggregate: No
    Flow detection configuration:
      Flow detection system is off
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      Yes        Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          500 pps
    System-wide information:
      Bandwidth is never violated
      Received:  56                  Arrival rate:     0 pps
      Dropped:   0                   Max arrival rate: 0 pps
    Routing Engine information:
      Bandwidth: 500 pps, Burst: 500 packets, enabled
      Policer is never violated
      Received:  56                  Arrival rate:     0 pps
      Dropped:   0                   Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
    FPC slot 0 information:
      Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
      Hostbound queue 0
      Policer is never violated
      Received:  56                  Arrival rate:     0 pps
      Dropped:   0                   Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
        Dropped by flow suppression:  0
```

Caso a violação não se repita por 300 segundos ela será removida do BNG.

É possível desabilitar ou ajustar os controles de DDoS Protection de forma global ou individual por protocolo ou pelo tipo do pacote tanto no nível da FPC quanto no nível da Routing Engine:

```
set system ddos-protection global disable-routing-engine
set system ddos-protection global disable-fpc
```

Com os comandos acima está sendo desabilitado o controle de DDoS Protection globalmente no BNG para qualquer protocolo tanto no nível da FPC quanto no nível da Routing-Engine.

```
set system ddos-protection protocols pppoe aggregate disable-routing-engine
set system ddos-protection protocols pppoe aggregate disable-fpc
```

Com os comandos acima está sendo desabilitado o controle de DDoS Protection para o protocolo PPPoE de forma agregada (PADI, PADO, PADR, etc) no BNG tanto no nível da FPC quanto no nível da Routing-Engine.

```
set system ddos-protection protocols pppoe padi disable-fpc
set system ddos-protection protocols pppoe padi disable-routing-engine
```

Com os comandos acima está sendo desabilitado o controle de DDoS Protection para o protocolo PPPoE apenas nos pacotes PADI. O controle está sendo desabilitado tanto no nível da FPC quanto no nível da Routing-Engine.

```
set system ddos-protection protocols dhcpv6 solicit bandwidth 2000
```

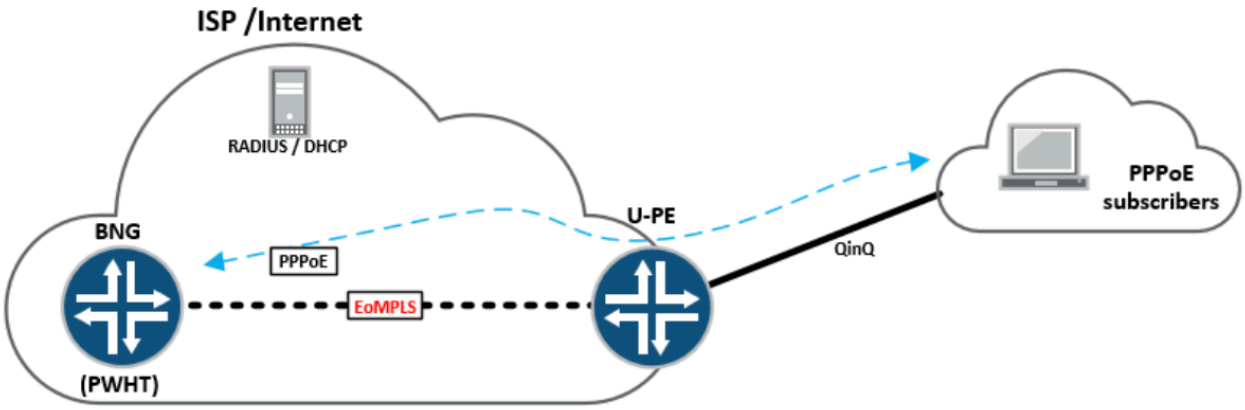
No comando acima está sendo alterado o limite de pacotes por segundo de DHCPv6 Solicit que por default é 500 pacotes por segundo para 2000 pacotes por segundo.

```
admin@MX204-LAB-WZTECH> show ddos-protection protocols dhcpv6 solicit
Currently tracked flows: 0, Total detected flows: 0
* = User configured value
Protocol Group: DHCPv6

  Packet type: solicit (DHCPv6 SOLICIT)
    Individual policer configuration:
      Bandwidth:            2000 pps*
      Burst:                500 packets
      Priority:             Low
      Recover time:         300 seconds
      Enabled:              Yes
      Bypass aggregate: No
    Flow detection configuration:
      Flow detection system is off
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      Yes        Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          500 pps
    System-wide information:
      Bandwidth is never violated
      Received:  56                  Arrival rate:     0 pps
      Dropped:   0                   Max arrival rate: 0 pps
    Routing Engine information:
      Bandwidth: 2000 pps, Burst: 500 packets, enabled
      Policer is never violated
      Received:  56                  Arrival rate:     0 pps
      Dropped:   0                   Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
    FPC slot 0 information:
      Bandwidth: 100% (2000 pps), Burst: 100% (500 packets), enabled
      Hostbound queue 0
      Policer is never violated
      Received:  56                  Arrival rate:     0 pps
      Dropped:   0                   Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
        Dropped by flow suppression:  0
```

Importante: Não é recomendado desabilitar o DDoS Protection e nem alterar os valores default. Os valores têm se mostrado satisfatórios e eficazes para proteger o BNG no dia a dia nos provedores.

21. PWHT (Pseudowire Headend Termination) - BNG

É possível terminar conexões dos assinantes PPPoE sem necessitar que o tráfego chegue em Layer 2 no BNG. Nesto caso a conexão PPPoE é terminada no BNG através de um Pseudowire (conexão virtual L2 em cima do protocolo MPLS). Este Pseudowire (PW) pode ser terminado em cima de um circuito VPWS que na Juniper é chamado de l2circuit ou através de circuito VPLS:



Neste modelo todo o tráfego PPPoE do assinante é transportado por MPLS até o BNG e o BNG faz uso de interfaces ps (Pseudo Subscriber) para ancorar o l2circuit. A interface ps passa a ser a interface onde a interface de camada 2 (demux0) será ancorada e não mais na interface física. A seguir os passos para configurar o PWHT no BNG com a explicação:

```
set chassis fpc 0 pic 0 tunnel-services bandwidth 200g
```

As interfaces ps são encoradas em uma interface física chamada lt (Logical Tunnel). Por default esta interface não é ativada no MX. Para que ela seja ativada é preciso do comando acima. Ela é ativada no nível da PIC da placa (FPC). No caso do MX204 existem duas PIC's. Na PIC0 estão as interfaces de 40/100G e na PIC1 estão as interfaces de 1/10G. Para o MX204 a configuração de tunnel-services deve ser ativada a PIC0 e deve ser configurado o bandwidth para 200G. Este é o valor máximo suportado de banda passando na interface lt.

Quando a interface lt é ativada ela passa a existir no MX. Não é necessário reboot nem bounce da PIC:

```
admin@MX204-LAB-WZTECH> show interfaces terse | match lt-
lt-0/0/0                up    up
lt-0/0/0.32767          up    up
```

Depois é necessário fazer a configuração no MX informando qual a quantidade de interfaces ps que podem ser criadas. Por default não é permitido a criação de nenhuma interface ps.

```
set chassis pseudowire-service device-count 7000
```

Neste caso está sendo informado que o MX vai suportar a criação de até 7000 interfaces ps.

O próximo passo é a criação das interfaces ps:

```
set interfaces ps0 description VLAN200
set interfaces ps0 anchor-point lt-0/0/0
set interfaces ps0 flexible-vlan-tagging
set interfaces ps0 auto-configure stacked-vlan-ranges dynamic-profile CVLAN-DYNAMIC-PROFILE accept pppoe
set interfaces ps0 auto-configure stacked-vlan-ranges dynamic-profile CVLAN-DYNAMIC-PROFILE ranges 1-4094,any
set interfaces ps0 auto-configure vlan-ranges dynamic-profile SVLAN-DYNAMIC-PROFILE accept pppoe
set interfaces ps0 auto-configure vlan-ranges dynamic-profile SVLAN-DYNAMIC-PROFILE ranges any
set interfaces ps0 auto-configure remove-when-no-subscribers
set interfaces ps0 mtu 9192
set interfaces ps0 no-gratuitous-arp-request
set interfaces ps0 unit 0 encapsulation ethernet-ccc
```

A configuração de anchor-point informa qual interface física que a interface ps utilizará. No caso do MX204 deve ser utilizado sempre a interface lt-0/0/0 (que está ancorada na PIC0).

As configurações de auto-configure e MTU são exatamente as mesmas das interfaces físicas (já detalhado neste documento).

É obrigatório ter a configuração de encapsulation ethernet-ccc na interface ps.

Neste caso no BNG é configurado um l2circuit para um PE:

```
set protocols l2circuit neighbor 2.2.2.2 interface ps0.0 virtual-circuit-id 200
set protocols l2circuit neighbor 2.2.2.2 interface ps0.0 mtu 9192
set protocols l2circuit neighbor 2.2.2.2 interface ps0.0 encapsulation-type ethernet
```

O l2circuit é configurado para o PE com o encapsulation-type ethernet. Tem equipamentos que sinalizam ethernet-vlan como encapsulation-type e esta configuração precisa ser ajustada. O l2circuit configurado acima está associado à interface ps0.

Importante: A interface ps suporta múltiplas VLAN's. Caso o l2circuit esteja transportando várias VLAN's todas serão aceitas na mesma interface ps onde o l2circuito está usando.

Abaixo é criado uma outra interface ps (ps1) que será utilizada por outro l2circuit.

```
set interfaces ps1 description VLAN200
set interfaces ps1 anchor-point lt-0/0/0
set interfaces ps1 flexible-vlan-tagging
set interfaces ps1 auto-configure stacked-vlan-ranges dynamic-profile CVLAN-DYNAMIC-PROFILE accept pppoe
set interfaces ps1 auto-configure stacked-vlan-ranges dynamic-profile CVLAN-DYNAMIC-PROFILE ranges 1-4094,any
set interfaces ps1 auto-configure vlan-ranges dynamic-profile SVLAN-DYNAMIC-PROFILE accept pppoe
set interfaces ps1 auto-configure vlan-ranges dynamic-profile SVLAN-DYNAMIC-PROFILE ranges any
set interfaces ps1 auto-configure remove-when-no-subscribers
set interfaces ps1 mtu 9192
set interfaces ps1 no-gratuitous-arp-request
set interfaces ps1 unit 0 encapsulation ethernet-ccc
```



```
set protocols l2circuit neighbor 2.2.2.2 interface ps1.0 virtual-circuit-id 300
set protocols l2circuit neighbor 2.2.2.2 interface ps1.0 mtu 9192
set protocols l2circuit neighbor 2.2.2.2 interface ps1.0 encapsulation-type ethernet
```

Neste caso o assinante vai chegar no modelo SVLAN+CVLAN utilizando a VLAN 300 como VLAN Outer.

Do lado do PE também é feito a configuração do l2circuit associado à interface l2 por onde o tráfego das VLAN's dos usuários chegarão:

Configuração no agregador (QFX-5120-48Y):

```
set interfaces ae0 description AGGREGACAO-ACESSO
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 mtu 9192
set interfaces ae0 encapsulation flexible-ethernet-services
set interfaces ae0 aggregated-ether-options link-speed 10g
set interfaces ae0 aggregated-ether-options lacp active
set interfaces ae0 aggregated-ether-options lacp periodic fast
set interfaces ae0 unit 200 encapsulation vlan-ccc
set interfaces ae0 unit 200 vlan-id 200
set interfaces ae0 unit 300 encapsulation vlan-ccc
set interfaces ae0 unit 300 vlan-id 300

set protocols l2circuit neighbor 1.1.1.1 interface ae0.200 virtual-circuit-id 200
set protocols l2circuit neighbor 1.1.1.1 interface ae0.200 mtu 9192
set protocols l2circuit neighbor 1.1.1.1 interface ae0.200 encapsulation-type ethernet
set protocols l2circuit neighbor 1.1.1.1 interface ae0.300 virtual-circuit-id 300
set protocols l2circuit neighbor 1.1.1.1 interface ae0.300 mtu 9192
set protocols l2circuit neighbor 1.1.1.1 interface ae0.300 encapsulation-type ethernet
```

Status dos 2 l2circuit no MX:

```
admin@MX204-LAB-WZTECH> show l2circuit connections
Layer-2 Circuit Connections:
```

```
Legend for connection status (St)
EI -- encapsulation invalid      NP -- interface h/w not present
MM -- mtu mismatch               Dn -- down
EM -- encapsulation mismatch     VC-Dn -- Virtual circuit Down
CM -- control-word mismatch      Up -- operational
VM -- vlan id mismatch           CF -- Call admission control failure
OL -- no outgoing label          IB -- TDM incompatible bitrate
NC -- intf encaps not CCC/TCC    TM -- TDM misconfiguration
BK -- Backup Connection          ST -- Standby Connection
CB -- rcvd cell-bundle size bad  SP -- Static Pseudowire
LD -- local site signaled down   RS -- remote site standby
RD -- remote site signaled down  HS -- Hot-standby Connection
XX -- unknown

Legend for interface status
Up -- operational
Dn -- down
Neighbor: 2.2.2.2
    Interface                 Type  St     Time last up          # Up trans
    ps0.0(vc 200)             rmt   Up     Sep 15 12:13:26 2023           1
      Remote PE: 2.2.2.2, Negotiated control-word: Yes (Null)
      Incoming label: 16, Outgoing label: 16
      Negotiated PW status TLV: No
      Local interface: ps0.0, Status: Up, Encapsulation: ETHERNET
      Flow Label Transmit: No, Flow Label Receive: No
    ps1.0(vc 300)             rmt   Up     Sep 15 08:36:30 2023           1
      Remote PE: 2.2.2.2, Negotiated control-word: Yes (Null)
      Incoming label: 17, Outgoing label: 17
      Negotiated PW status TLV: No
      Local interface: ps1.0, Status: Up, Encapsulation: ETHERNET
      Flow Label Transmit: No, Flow Label Receive: No
```

Os dois l2circuit estão UP, cada um usando uma interface ps.

```
admin@MX204-LAB-WZTECH> show subscribers summary port

Interface           Count
ps0: lt-0/0/0       2
ps1: lt-0/0/0       1

Total Subscribers: 3

admin@MX204-LAB-WZTECH>
```


Neste caso temos 3 assinantes conectados. Dois na interface ps0 e um assinante na interface ps1.

```
admin@MX204-LAB-WZTECH> show subscribers
Interface                   IP Address/VLAN ID                  User Name                LS:RI
demux0.3221226016           0x8100.300 0x8100.400                                        default:default
pp0.3221226017              192.168.60.1                        wztech3                  default:default
*                           1010:ee4:4000:1::/64
*                           2904:ee4:8000:3::/64
pp0.3221226017              1010:ee4:4000:1::/64                                         default:default
demux0.3221226020            200                                                         default:default
pp0.3221226021              192.168.60.2                        wztech2                  default:default
*                           1011:ee4:4000:2::/64
*                           2904:ee4:8000:4::/64
pp0.3221226021              1011:ee4:4000:2::/64                                         default:default
pp0.3221226023              192.168.60.3                        wztech4                  default:default
*                           1011:ee4:4000:3::/64
*                           2904:ee4:8000:5::/64
pp0.3221226023              1011:ee4:4000:3::/64                                         default:default

admin@MX204-LAB-WZTECH> show interfaces demux0.3221226016
  Logical interface demux0.3221226016 (Index 536871861) (SNMP ifIndex 200000949)
    Flags: Up VLAN-Tag [ 0x8100.300 0x8100.400 ]  Encapsulation: ENET2
    Demux:
      Underlying interface: ps1 (Index 155)
    Bandwidth: 0
    Input packets : 54
    Output packets: 68
    Protocol pppoe
      Dynamic Profile: SUBSCRIBER-PROFILE,
      Service Name Table: None,
      Max Sessions: 32000, Max Sessions VSA Ignore: Off,
      Duplicate Protection: On, Short Cycle Protection: mac-address,
      Direct Connect: Off,
      AC Name: CONCENTRADOR-PPPOE
      Addresses
```

No caso do uso de interface ps a interface demux0 aparece utilizado esta interface como Underlying Interface.

Os mesmos comandos para fazer captura de tráfego na interface física funcionam na interface ps0 para capturar os pacotes PPPoE (PADI, PADO, ICMPv6 Router Solicit, DHCPv6 Solicit, etc...) vindos através de um l2circuit.