lacnic
lacnog 2018

30

24/28 SETIEMBRE 2018
ROSARIO•ARGENTINA

Despliegue de IPv6 en Redes xDSL y algunas cosas más...

Ariel S. Weher

Usual Suspect / Well-Known Guilty / Anti NAT Activist / Networking Gardener / Virtualization Chef

ariel@weher.net | @arielweher

CC BY SA

“Usted puede hacer una transición planificada y cuidadosa a IPv6 , o puede hacerlo de urgencia y con pánico.

Pero debe saber muy bien que la urgencia y el pánico siempre son más caros.”

Martin Levy

Hurricane Electric

Lo que vamos a aprender hoy

Modos de funcionamiento de los CPE's

Router

Segmenta a Capa 3 el puerto WAN (ATM) y los puertos LAN (bridge ethernet). Se activa Source NAT para los paquetes que llegan desde la LAN y se permite que el CPE obtenga direccionamiento IP desde la interfaz WAN.

En caso de ser necesario, la interface WAN puede utilizar algún tipo de encapsulamiento PPP o bien PPP over Ethernet (PPPoE).

Bridge

RFC1483 y RFC2684 describen dos métodos de multiplexación para los paquetes que viajan sobre ATM.

Básicamente este modo de funcionamiento transforma el CPE en un bridge transparente entre los datos contenidos en el PVC ATM + AAL5 (generalmente Ethernet) y las tramas ethernet que se reciben desde los puertos "LAN" del equipo.

El cliente es responsable de los detalles de Capa 3.

Plan de direccionamiento

Inicialmente el RIR nos va a ofrecer un /32.

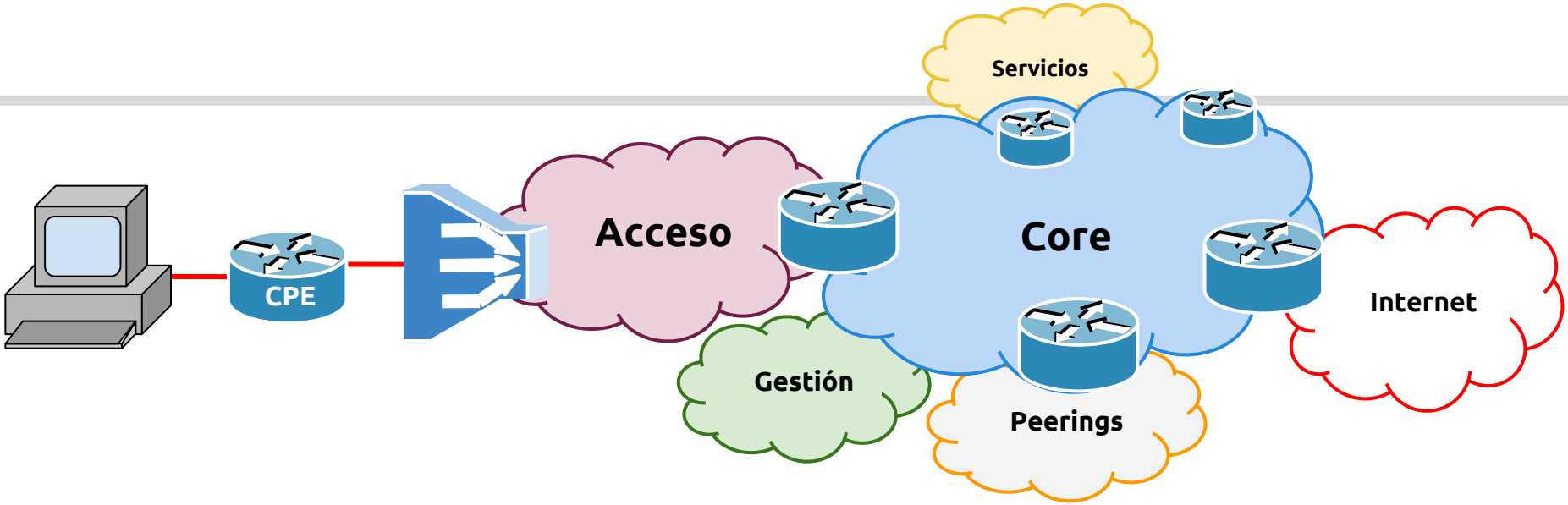
Generalmente se puede obtener un prefijo más grande sin demasiadas complicaciones.

- **Todo cliente obtiene un /48** *(RFC 6177)*.
  - /48 dinámico.
    - Asignado desde un pool configurado en el BNG.
    - Permite la agregación de prefijos en la red.
  - /48 fijo.
    - Asignado desde el provisioning.
    - Aumenta la cantidad de prefijos de la red.
    - Obliga a mantener esquemas de redistribución en los protocolos de ruteo o una solución de mobility.

Algunas best practices para conectarse al mundo IPv6 nativo

- En caso de ruteo estático, usar la default hacia 2000::/3.
  - Evitar los nexthop con direcciones de link local.
    - `ipv6 route 2000::/3 2001:db8::1`
- Mantener sesiones de BGP separadas para IPv4 e IPv6.
- Muchas reglas de seguridad para IPv4 también aplican:
  - BGP maxas-limit & ttl-security
  - Bogonsv6: http://bit.ly/Filterv6atxSP
  - uRPF.
  - RTBH: (100::/64) RFC 6666.
  - Control Plane Policing.
  - ICMPv6 Filtering: RFC 4890.
  - Network Ingress Filtering: BCP38.

Algunas formas de plantear la red



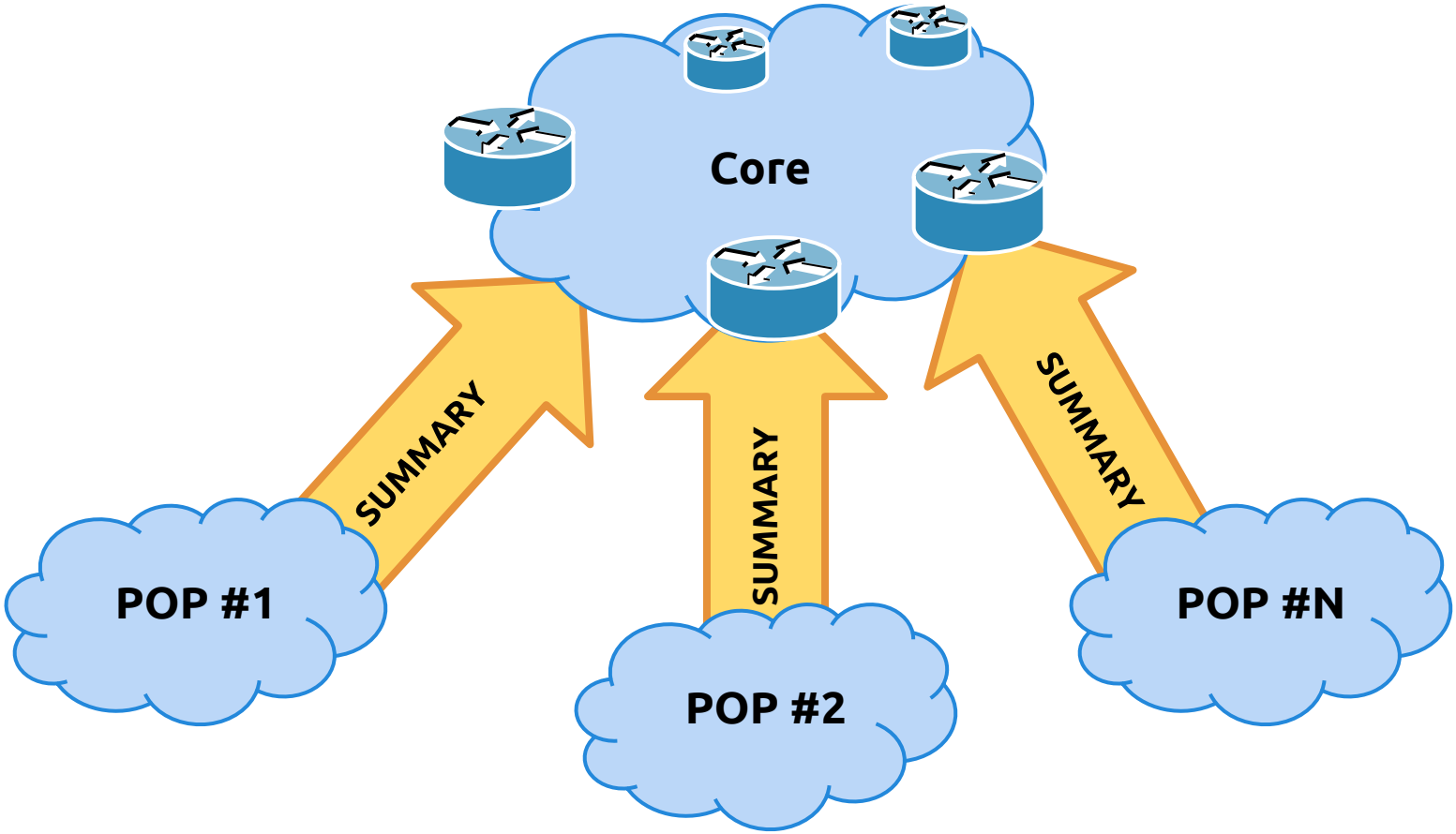
Dual Stack Nativo

- Dual Stack en todos los routers.
- IGP IPv6 dedicado, no se comparte con ningún cliente.
- Todos BNG corren BGP.
- Solo los BGP Next-Hop y links de core están en el IGP.
- Route Reflectors para escalar.

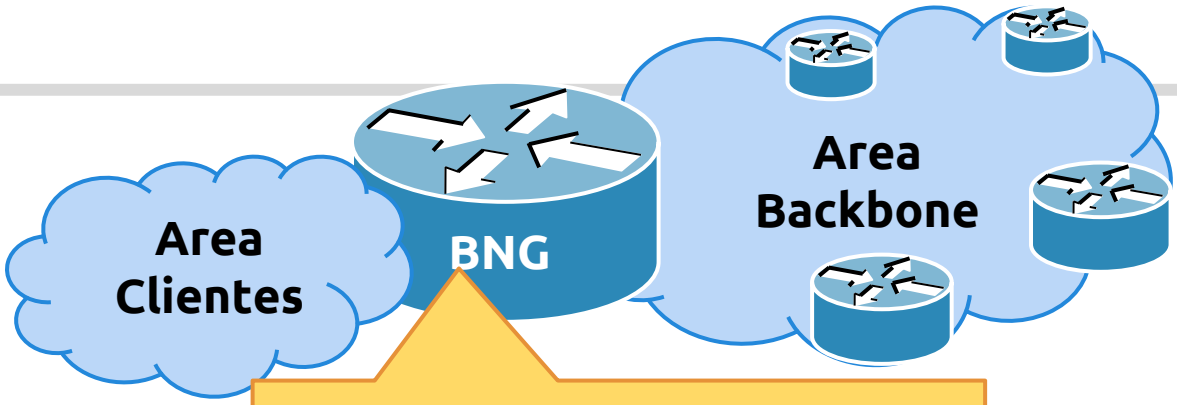
Dual Stack c/MPLS

- Solo los PE corren BGP.
- Se usa MPLS para transportar datos entre los BGP Next-Hop.
- No hay configuraciones de IPv6 en el Core.
- IPv6 disponible sólo en los PE y Route Reflectors.

Agregación de prefijos:



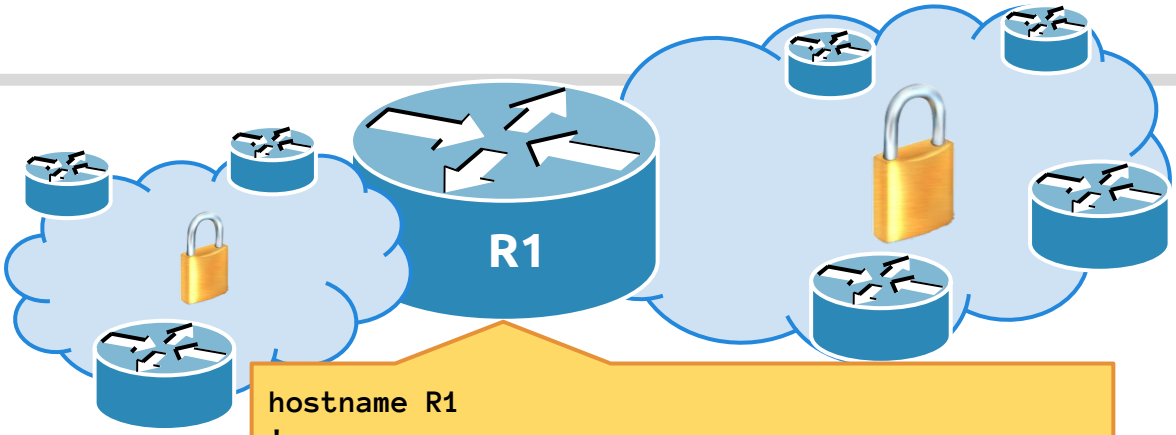
Agregación de prefijos: OSPFv3




```
hostname BNG
!
interface GigabitEthernet0/0
 description Area Backbone
 [...]
 ipv6 address 2001:DB8::/64 eui-64
 ipv6 ospf 10 area 0
!
interface GigabitEthernet0/1
 description Area Clientes
 [...]
 ipv6 address 2001:DB8:8000::/64 eui-64
 ipv6 ospf 10 area 20
!
ipv6 router ospf 100
 [...]
 area 20 range 2001:DB8:8000::/33
```

- Para mantener la estabilidad de la red evitar redistribuir las estáticas en el IGP del Core.
- Incluir las interfaces del lado de los clientes en un área diferente
- Sumarizar los prefijos de los clientes utilizando un *area range*.

Autenticación OSPFv3

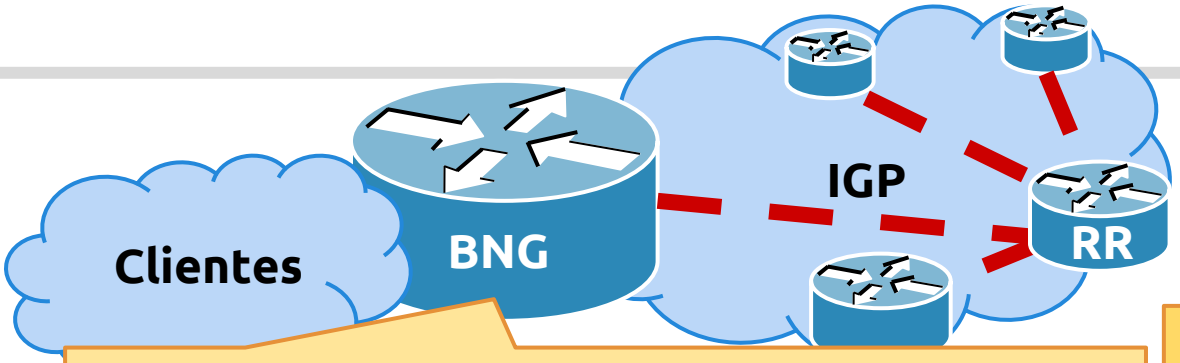



```
hostname R1
!
interface GigabitEthernet0/0
 [...]
 ipv6 address 2001:DB8::/64 eui-64
 ipv6 ospf 10 area 0
 ipv6 ospf authentication ipsec spi 1024 sha1
dd3e1646c4be8b3e252eab3607e99fb464050cf5
```

Para obtener la clave SHA-1:

```
usuario@linuxbox:~$ dd if=/dev/urandom count=1024 | sha1sum
1024+0 records in
1024+0 records out
524288 bytes (524 kB) copied, 0.0405063 s, 12.9 MB/s
dd3e1646c4be8b3e252eab3607e99fb464050cf5  -
```

Agregación de prefijos: BGP



BGP Route Reflector

```
[...]
ipv6 route 2001:DB8:8000/35 null0 250 tag 100
!
router bgp 65530
 [...]
 address-family ipv6
  redistribute static route-map PrefijosLocales
  exit address-family
!
ipv6 prefix-list prefijoschicos permit 2001:DB8::/32 ge 36
!
route-map PrefijosLocales deny 10
 match ipv6 address prefix-list prefijoschicos
route-map PrefijosLocales permit 20
 match tag 100
 set community no-export additive
route-map PrefijosLocales deny 1000
```

Prefijos para delegar. Evita flapping

Nuestras redes con máscara ≥ /36

Evita propagación de redes desagregadas al core

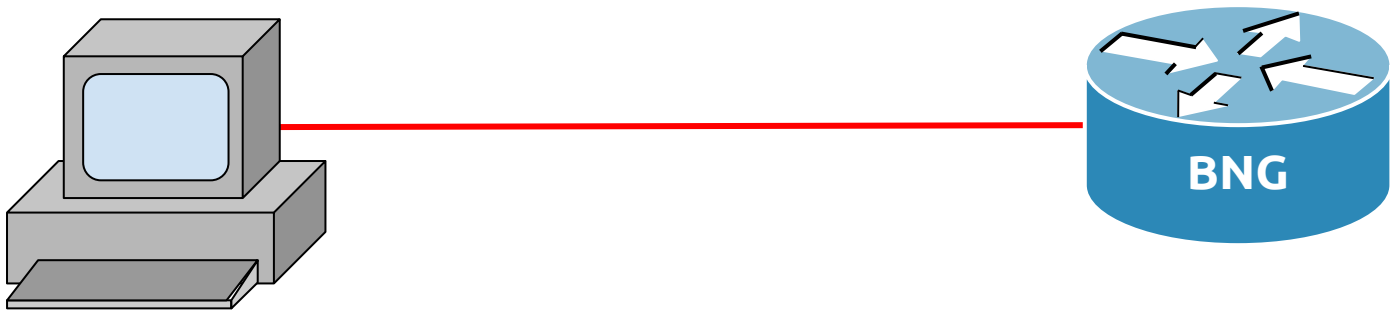
Evita propagación desagregada al mundo

lacnic
lacnog 2018
30
24/28 SETIEMBRE 2018
ROSARIO • ARGENTINA

Dual Stack

Hosts Individuales:

- **ND RA para ruta por defecto.**
  - DHCPv6 no propaga esta opción como en DHCPv4.
- **DHCPv6 para aprender servidores DNS.**
  - RFC 6106 DNS over RA Options no está en todas las implementaciones.
- **SLAAC para configuración de direcciones.**
- Cada subred obtiene un /64.
- Una subred por cliente (VLAN o PPPoE).
- Agregación de rutas por POP o por PE.



Hosts Individuales: SLAAC Ejemplo de Configuración:

```
hostname BNG
!
ipv6 dhcp pool ClienteMetroVLAN200
 dns-server 2001:DB8:8::4
 domain-name lacnog.org
!
interface GigabitEthernet0/0.200
 description Acceso Metro Ethernet
 encapsulation dot1Q 200
 ipv6 address 2001:DB8:8200::1/64
 ipv6 nd other-config-flag
 ipv6 nd router-preference High
 no ipv6 nd ra suppress
 ipv6 nd ra interval 5
 ipv6 dhcp server ClienteMetroVLAN200
```

Un pool por cliente...

Hosts Individuales: DHCPv6 Ejemplo de Configuración:

```
hostname BNG
!
ipv6 dhcp pool ClienteMetroVLAN100
 address prefix 2001:DB8:2100::/64 lifetime 30 10
 dns-server 2001:DB8:8::4
 domain-name lacnog.org
!
interface GigabitEthernet0/0.100
 description Acceso Metro Ethernet
 encapsulation dot1Q 100
 ipv6 address 2001:DB8:2100::1/64
 ipv6 nd prefix 2001:DB8:2100::/64 no-advertise
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd router-preference high
 ipv6 nd cache-limit <numero máx de clientes>
 no ipv6 unreachables
 ipv6 dhcp server ClienteMetroVLAN100
 ipv6 verify unicast source reachable-via rx
```

La máscara podría no ser necesariamente un /64...

RECORDAR: DHCPv6 no tiene opción de default gateway.

En el (router) cliente:

```
interface GigabitEthernet0/0
 [...]
 ipv6 address dhcp
 ipv6 address autoconfig default
 ipv6 enable
 ipv6 nd ra suppress
```

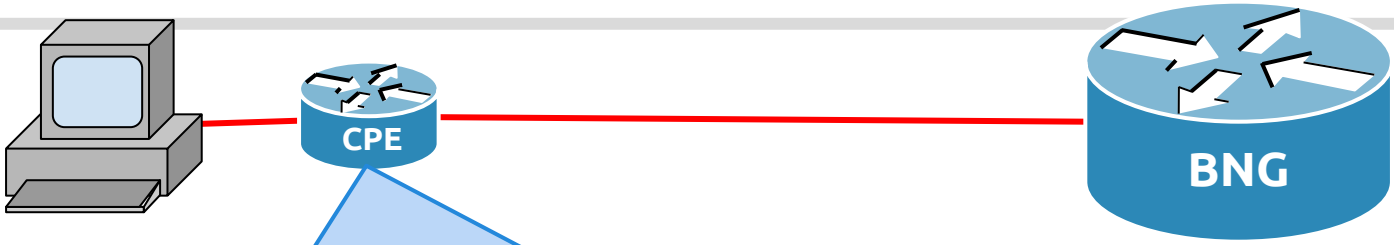
Hosts Individuales: DHCPv6-Relay Ejemplo de Configuración:

```
hostname BNG
!
interface GigabitEthernet0/0.100
 description Acceso Metro Ethernet
 encapsulation dot1Q 100
 ipv6 address 2001:DB8:2100::1/64
 ipv6 nd prefix 2001:DB8:2100::/64 no-autoconfig
 ipv6 nd managed-config-flag
 ipv6 nd router-preference High
 ipv6 dhcp relay destination 2001:DB8:3::4
 ipv6 dhcp relay source-interface Loopback0
 ipv6 verify unicast source reachable-via rx
```

Esto desactiva la publicación del prefijo para que se pueda asignar la dirección mediante DHCPv6.

El request DHCPv6 del cliente será enviado dentro de otro request DHCPv6 con el source interface definido en el comando o bien con la interfaz más cercana al destino según la RIB

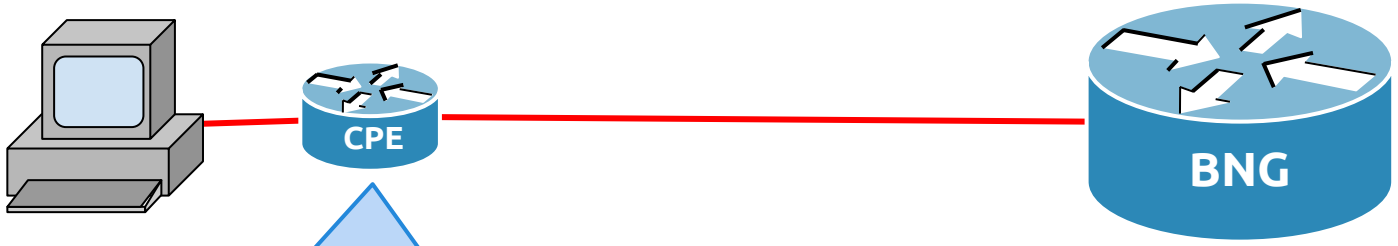
Prefix Delegation en CPE: Ejemplo de Configuración *(1/2)*:




```
hostname CPE
!
ipv6 unicast-routing
ipv6 cef
!
interface Loopback0
 ipv6 address PrefijoDelegado ::1/64
!
interface FastEthernet0/0
 description Link al Cliente
 ipv6 address PrefijoDelegado ::1:0:0:0:1/64
!
interface FastEthernet0/1
 description Link al BNG
 ipv6 enable
 ipv6 nd autoconfig default-route
 ipv6 dhcp client pd PrefijoDelegado
 ipv6 nd ra supress
```

En esta 'variable' se almacena el prefijo de red obtenido por el BNG, y luego se reemplaza en la configuración de las interfaces.

Prefix Delegation en CPE: Ejemplo de Configuración *(2/2)*:

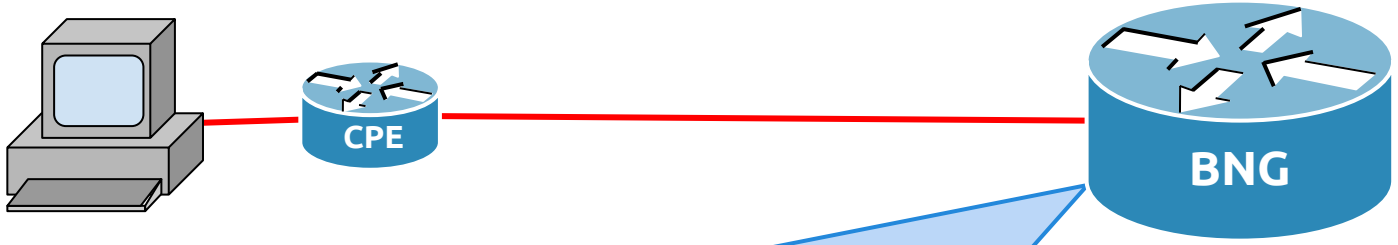



```
hostname CPE
!
ipv6 dhcp pool Inside
 import dns-server
 import domain-name
 import information refresh
!
interface FastEthernet0/0
 ipv6 nd other-config-flag
 ipv6 nd ra interval 4 3
 ipv6 dhcp server Inside
```

Importar configuraciones adquiridas desde el BNG en el DHCPv6 Local

Configurar el pool en cada interface

Prefix Delegation en CPE: Ejemplo de Configuración




```
hostname BNG
!
ipv6 dhcp pool Clientes
 prefix-delegation 2001:DB8:8300::/48 00030001CA04068A0008
 prefix-delegation pool OtroPool
 prefix-delegation pool OtroPool lifetime 1800 600
 dns-server 2001:DB8:8::4
 domain-name lacnog.org
!
ipv6 dhcp database <url>
!
ipv6 route 2001:DB8:A000::/35 Null0 tag 100
ipv6 local pool OtroPool 2001:DB8:A000::/35 48
```

DUID

Delegar prefijo fijo a cliente conocido.

Delegar dinámicamente al resto.

Setear de manera acorde, evitar los defaults (30 y 3.5 días)

Agregación de ruta para publicaciones.

Pool para clientes dinámicos. Delegar /48's desde el /35.

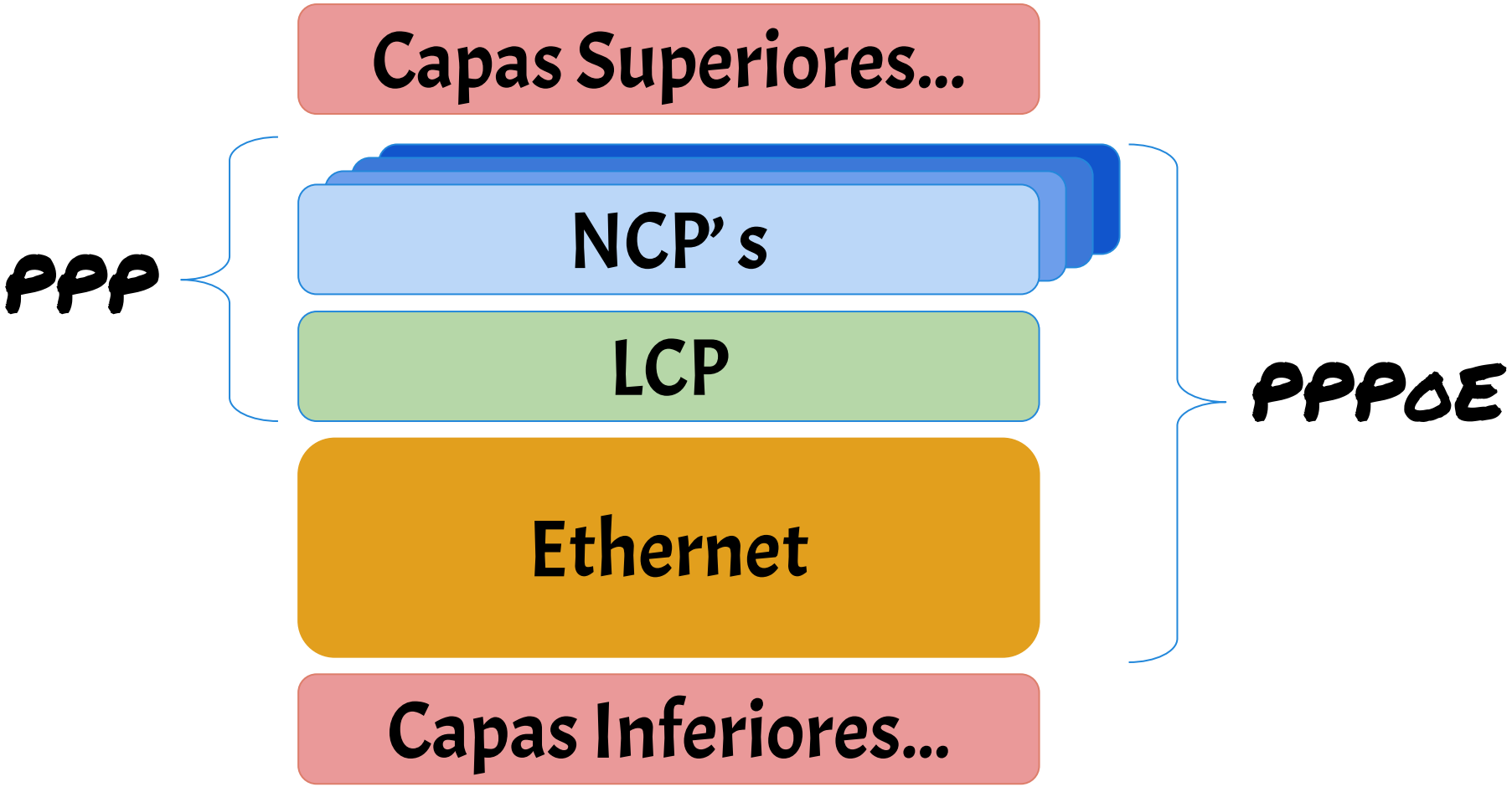
Algunas consideraciones:

- Las rutas estáticas hacia los prefijos delegados pueden perderse en caso del flapeo de la interface o bien si el BNG es reiniciado.
- Un router puede restablecer las rutas estáticas leyendo la base de datos de bindings.
- Bulk Leasequery (RFC 5460) establece una forma de restablecer los leases desde un servidor DHCPv6.
  - `ipv6 dhcp-relay bulk-lease retry <num>`

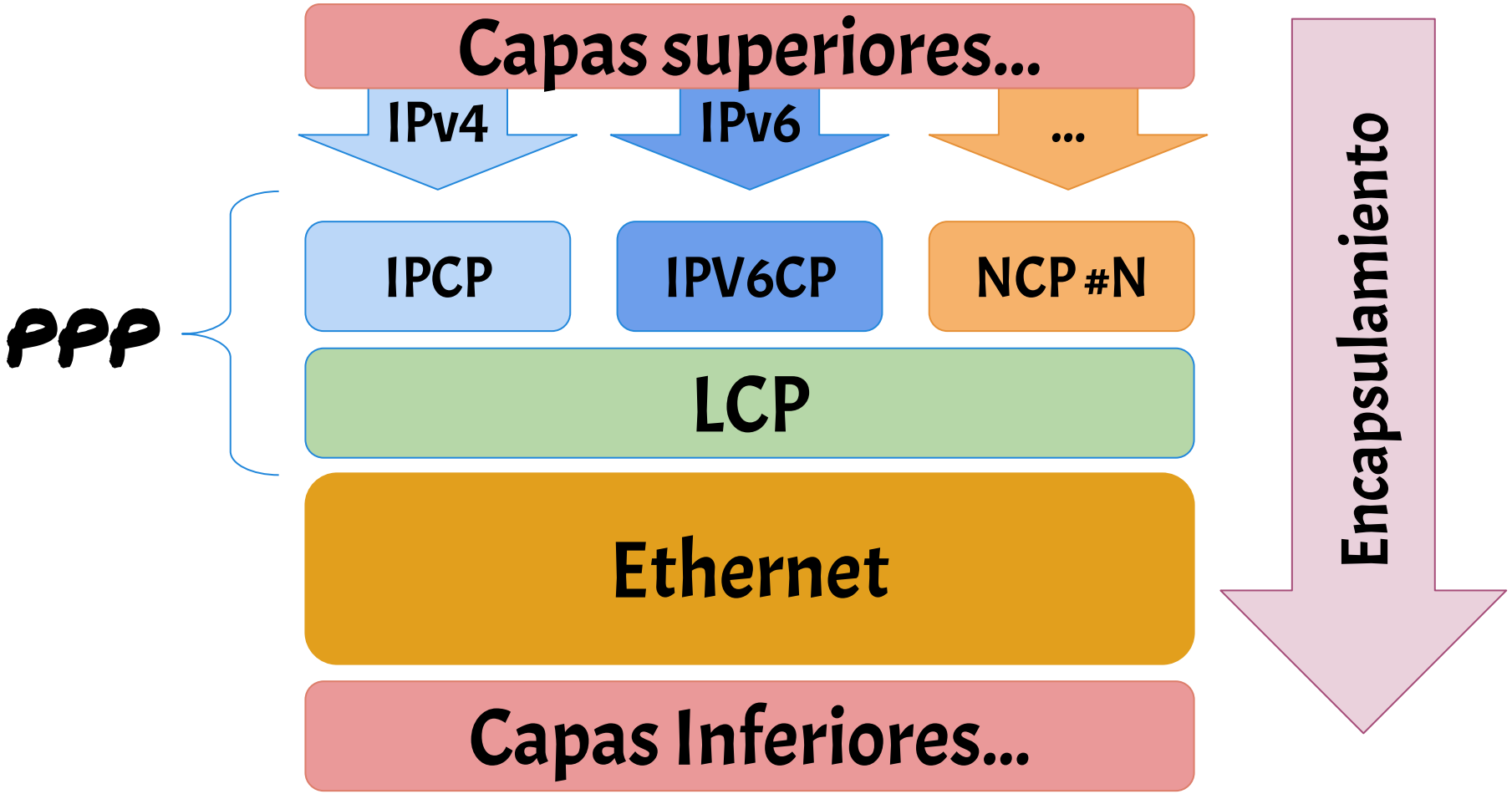
lacnic
lacnog 2018
30
24/28 SETIEMBRE 2018
ROSARIO • ARGENTINA

PPPoE

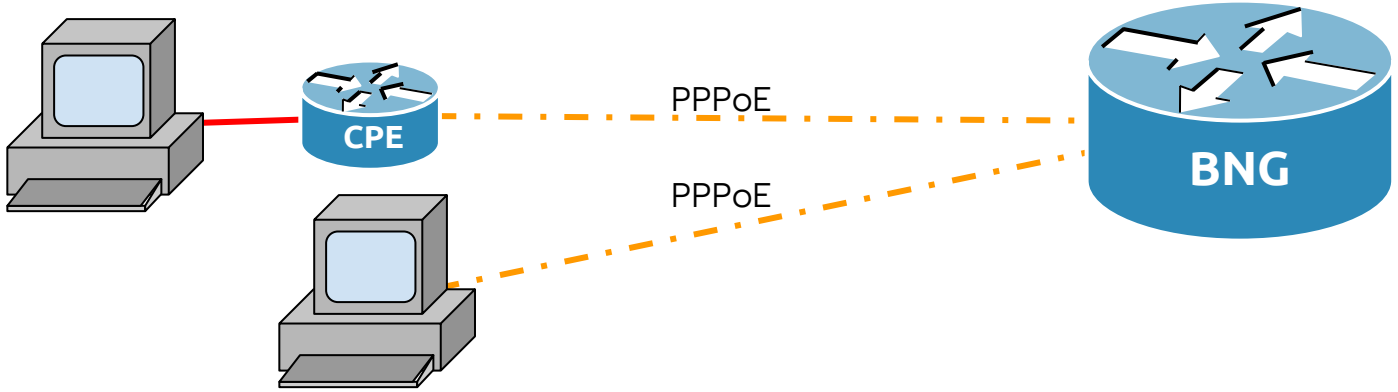
Stack PPPoE


Capas Superiores...
PPP
NCP's
LCP
PPPoE
Ethernet
Capas Inferiores...

En el Stack PPPoE, cada NCP es independiente y opcional...



Acceso IPv6 mediante PPPoE:

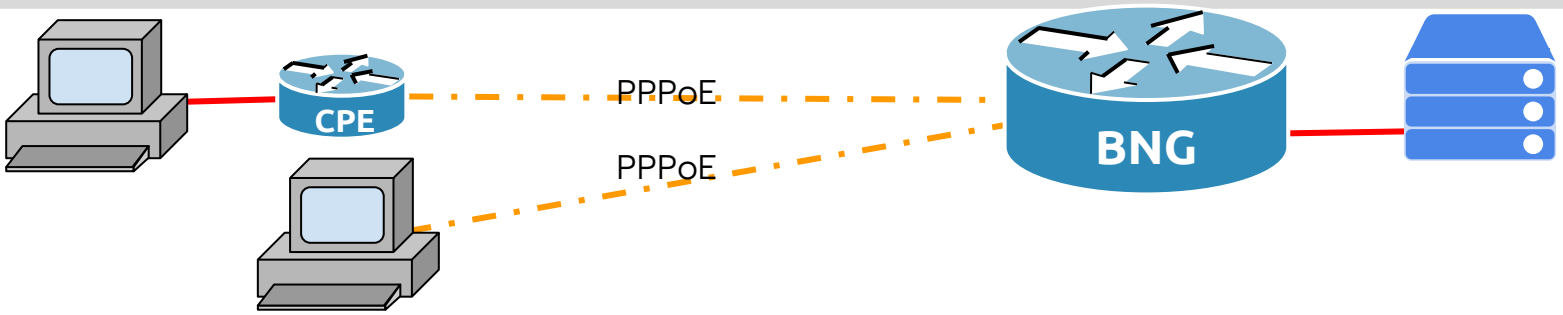


- Cada sesión de PPPoE es una subred, por lo que necesita un /64 asignado.
- El router CPE necesita Prefix Delegation para distribuir el servicio a los equipos que residen detrás de el.
- Habitualmente se utiliza algún servidor de AAA con algún backend de base de datos para validar al usuario:
  - RADIUS (el más usado).
  - TACACS+.
  - DIAMETER.

Acceso IPv6 mediante PPPoE con direccionamiento local:

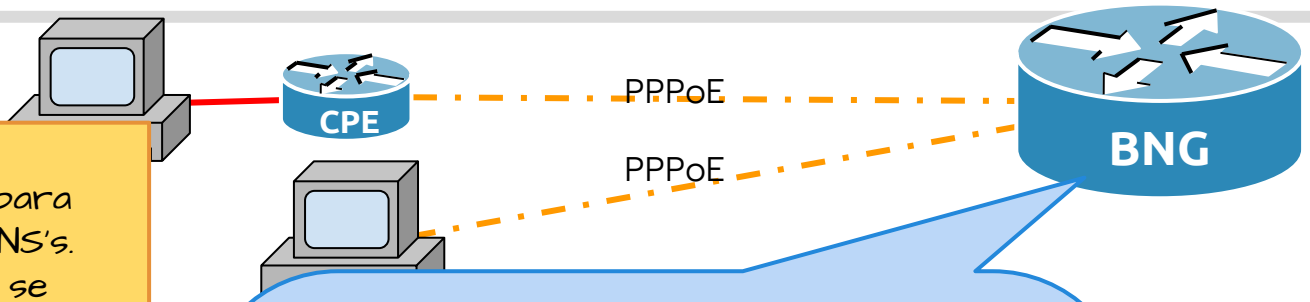
- Es la opción más simple y no requiere servidores de AAA.
- Generalmente no permite validación de usuario más allá de las opciones Remote ID / Subscriber ID (DHCPv6 Option 37/38).
- Se configura un pool de prefijos para el enlace entre el CPE y el BNG.
- Se agrega un pool de prefijos más grandes para delegar a los clientes.

Acceso IPv6 mediante PPPoE con direccionamiento centralizado:



- En el caso de RADIUS utiliza atributos específicamente creados para la provisión de este servicio:
  - Para definir estáticamente el vínculo entre el BNG y el CPE:
    - `Framed-IPv6-Prefix`
  - Para elegir el direccionamiento entre el BNG y el CPE desde un pool:
    - `Framed-IPv6-Pool`
  - Para designar los prefijos delegados:
    - `Delegated-IPv6-Prefix`

Direccionamiento entre el BNG y el CPE desde un pool local:



Requerido para entregar DNS's. Ignorar si se entregan DNS's en IPv4.

```
ipv6 dhcp pool Servicios
 dns-server 2001:DB8:8::4
 domain-name lacnog.org
!
interface Virtual-Template6
 mtu 1480
 peer default ipv6 pool PPPoELinks
 ipv6 enable
 ipv6 nd other-config-flag
 no ipv6 nd ra suppress
 ppp authentication chap pap
 ipv6 nd ra interval 5
 ipv6 dhcp server Servicios
!
ipv6 local pool PPPoELinks 2001:DB8:C000::/48 64
ipv6 route 2001:DB8:C000::/48 Null0 tag 100
```

Local Pool para direccionamiento entre BNG y CPE.

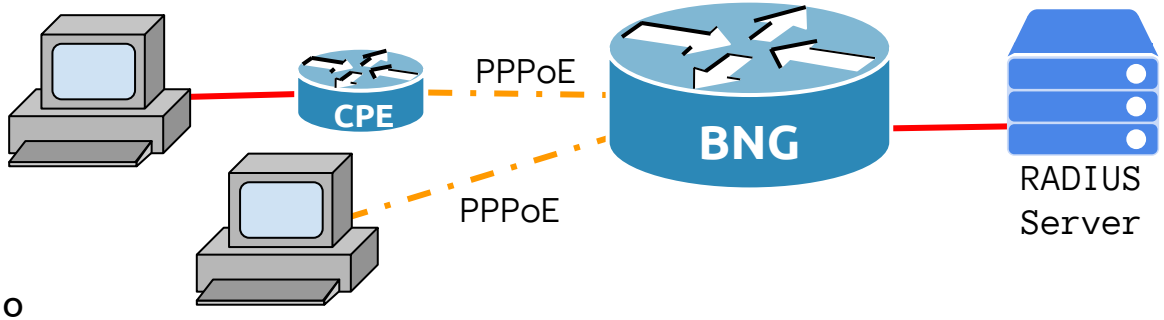
Interface 'unnumbered'

Se entregan subnets /64 desde el /48.

Ruta sumarizada para publicar por BGP.

Direccionamiento entre el BNG y el CPE desde servidor RADIUS:

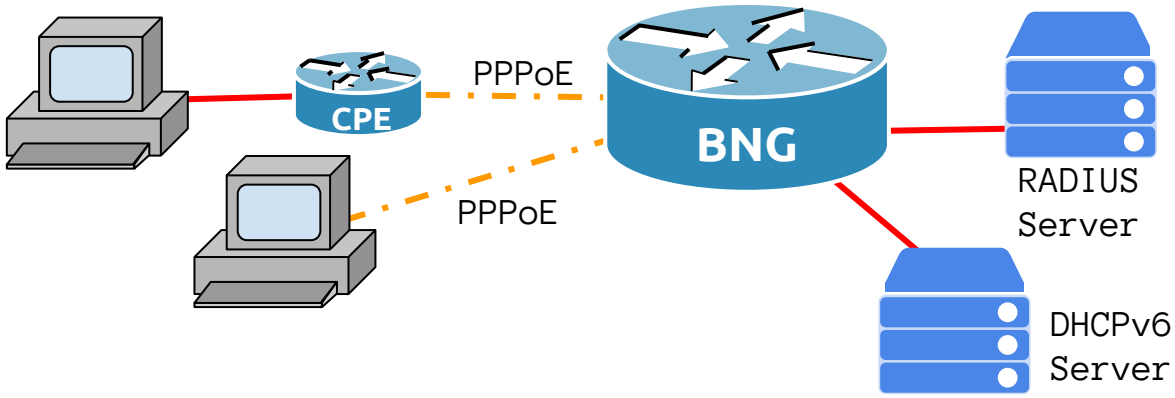
- El atributo ***Framed-IPv6-Pool*** sobreescribe el comando peer default ipv6 pool.
- El atributo ***Framed-IPv6-Prefix*** agrega otro prefijo BNG-CPE.
- Siempre usar configuración local o atributos de RADIUS, pero no ambos.



Archivo *users* de RADIUS:

```
Juan      Cleartext-Password := "sup3rs3cr3t0"
          Service-Type = Framed-User,
          Framed-Protocol = PPP,
          Framed-IPv6-Prefix = "2001:DB8:C000:1::/64“
Pedro     Cleartext-Password := "ind3sc1fr4bl3"
          Service-Type = Framed-User,
          Framed-Protocol = PPP,
          Framed-IPv6-Pool = "PPPoELinks”
```

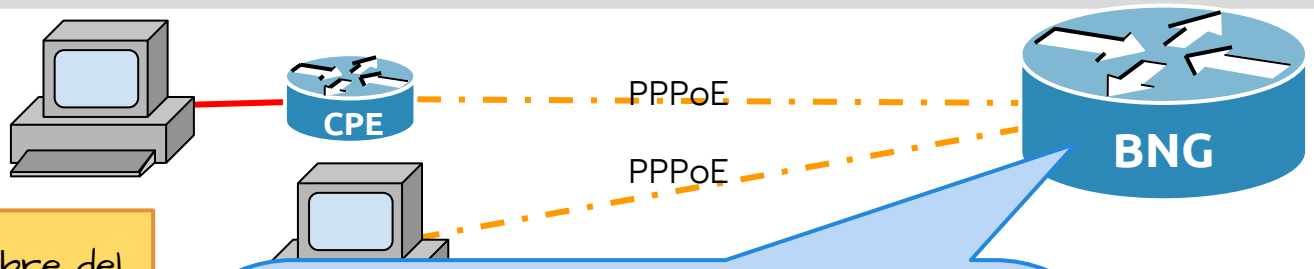
PPPoE: DHCPv6 Prefix Delegation:



Opciones de implementación:

- Prefix Delegation de pool local en el BNG.
- Servidor central de DHCPv6 y DHCPv6 Relay en el BNG.
- Prefix Delegation determinado por atributos de RADIUS (RFC 4818).
- Otras no recomendadas.

Prefix Delegation desde un pool local en el BNG:



Define el nombre del pool local para delegaciones.

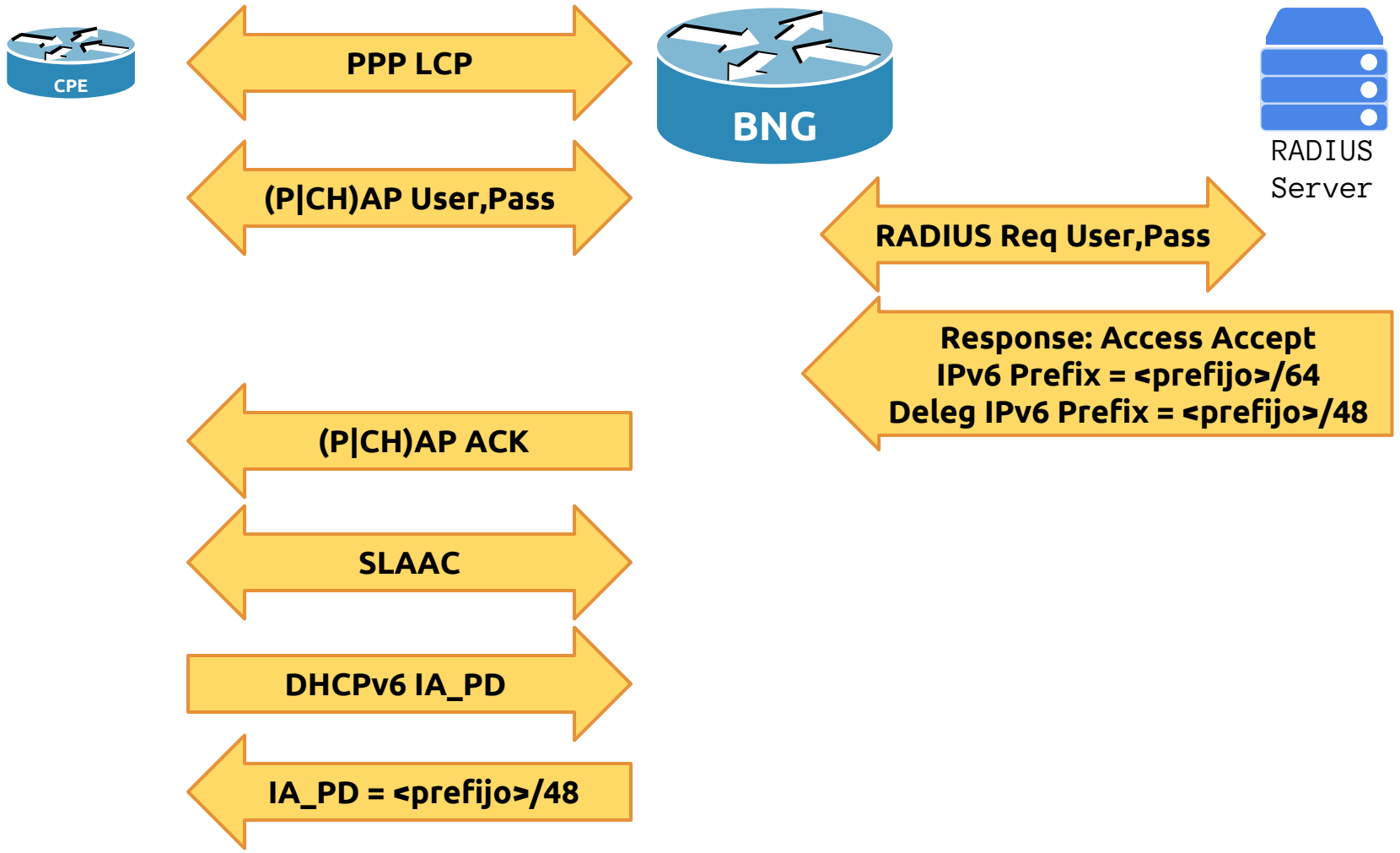
```
ipv6 dhcp pool PPPoE_PD
 prefix-delegation pool IA_PD lifetime 7200 300
 dns-server 2001:DB8:8::4
 domain-name lacnog.org
!
interface Virtual-Template6
 [...]
 peer default ipv6 pool BNG-CPE
 ipv6 enable
 ipv6 nd other-config-flag
 ipv6 nd managed-config-flag
 no ipv6 nd ra suppress
 ipv6 nd ra interval 5
 ipv6 dhcp server PPPoE_PD
!
ipv6 local pool BNG-CPE 2001:DB8:C000::/48 64
ipv6 local pool IA_PD 2001:DB8:E000::/38 48
ipv6 route 2001:DB8:C000::/48 Null0 tag 100
```

Local Pool para direccionamiento entre BNG y CPE.

Ruta sumarizada para publicar por BGP.

Se delegan subnets /48 desde el /38.

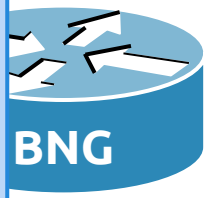
RFC 4818: Diálogos que permiten la asignación de prefijos vía RADIUS:



RFC 4818: Atributo Delegated-IPv6-Prefix

Configuración del BNG:

```
aaa authorization configuration IA_PD group radius
!
ipv6 dhcp pool PPPoE-RADIUS
 prefix-delegation aaa method-list IA_PD lifetime 7200 300
 dns-server 2001:DB8:8::4
 domain-name lacnog.org
!
interface Virtual-Template6
[...]
 ipv6 enable
 ipv6 nd other-config-flag
 no ipv6 nd ra suppress
 ipv6 dhcp server PPPoE-Radius
```



Configuración del usuario de RADIUS:

```
Juan      Cleartext-Password := "sup3rs3cr3t0"
          Service-Type = Framed-User,
          Framed-Protocol = PPP,
          Framed-IPv6-Prefix = "2001:DB8:C000:1::/64“
          Delegated-IPv6-Prefix=”2001:DB8:A001::/48”
```

EEM Applet: Limpiar el prefijo delegado ante un flapping:

```
event manager applet MONITOR-IPV6-DHCP-APP
event syslog pattern "DIALER-6-BIND"
action 1.0 cli command "enable"
action 1.1 cli command "clear ipv6 dhcp client Dialer0"
action 2.0 syslog priority debugging msg "Refreshed DHCP PD lease (Dialer rebind)"
```

lacnic
lacnog 2018

30

24/28 SETIEMBRE 2018
ROSARIO • ARGENTINA

Resumen

Y notas de último momento...

Direccionamiento:

- Cada subred de cliente necesita un /64.
- Clientes con CPE's necesitan un /48 para la red interna.
- En caso de no usar PPPoE necesita un /64 para el link externo contra el BNG.
- Las interfaces externas deben ser provisionadas mediante SLAAC o DHCPv6.
- Las interfaces internas son direccionadas con prefijos delegados.

Seguridad:

- Mantener una VLAN por cliente.
  - 802.1q tunneling (QinQ).
  - Client Isolation en los WAP's.
  - Private VLAN's.
- Tratar de hacer llegar la Capa 3 lo más cerca posible de los clientes.
- Utilizar medidas de seguridad bien conocidas cerca de cliente:
  - uRPF.
  - RA Guard.
  - DHCPv6 Snooping.

Routing:

- Maximizar la agregación de prefijos.
- Mantener el IGP aislado de los clientes.
  - Solamente mantienen la alcanzabilidad de los NextHop de BGP.
- En redes con muchos clientes o puntos de acceso usar BGP se vuelve indispensable.
  - Escalar la red usando Route Reflectors.
- Agregar manualmente en los PE/BNG.
  - Marcar las rutas estáticas null-eadas con un TAG.
  - Redistribuir estáticas en BGP solo si tienen el TAG.

Locación de direcciones y prefijos:

- Mantener una solución redundante de servidores DHCPv6 o RADIUS centralizados.
  - Ocultar prefijos al SLAAC en caso de entregarlos con DHCPv6.
- Usar RA para entregar la ruta por defecto.
- Mantener los CPE's bien controlados.
  - Broadband Forum Technical Report 69 (TR-069).
  - Monitoreo exhaustivo con SNMP.
- Minimizar el uso de túneles y políticas de transición ineficientes.
  - CGN **NO** es una alternativa a IPv6.

Algunas cosas para chequear en casa:

- RFC 7217
  - A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC).
- RFC 6164
  - Using 127-Bit IPv6 Prefixes on Inter-Router Links
- RFC 3971
  - Secure Neighbor Discovery (SeND).
- RFC 6105
  - IPv6 Router Advertisement Guard.
- RFC 6092
  - Recommended Simple Security Capabilities in CPE for providing Residential IPv6 Internet Service.
- BCP 180
  - DHCPv6 Redundancy Deployment Considerations.

Repositorio GitHub con las configuraciones del laboratorio:

https://github.com/aweher/tutorial-ipv6-lacnic

lacnic
lacnog 2018

30

¡Muchas Gracia

24/28 SETIEMBRE 2018
ROSARIO • ARGENTINA

lacnic
lacnog 2018
30