

Implementación de IOS de la Función iBGP PE-CE

Contenido

[Introducción](#)

[Antecedentes](#)

[Implementar iBGP PE-CE](#)

[Atributo de ruta del cliente BGP](#)

[Configurar](#)

[Nuevo Comando](#)

[Análisis detallado de ATTR_SET](#)

[Gestión de próximo salto](#)

[RD](#)

[Función iBGP PE-CE con Local-AS](#)

[Reglas para el Intercambio de Rutas entre Diferentes Sitios VRF](#)

[Reflexión de CE a CE VRF-Lite](#)

[Cisco IOS anterior en el router PE](#)

[Siguiendo salto-auto para eBGP en VRF](#)

Introducción

Este documento describe cómo se implementa el protocolo de gateway fronterizo interno (iBGP) entre la función de borde del proveedor (PE) y borde del cliente (CE) en Cisco IOS®.

Antecedentes

Hasta la nueva función PE-CE de iBGP, no se admitía oficialmente el iBGP entre PE y CE (por lo tanto en una interfaz de routing y reenvío virtual (VRF) en el router PE). Una excepción es iBGP en las interfaces VRF en una configuración CE de VRF múltiple (VRF-Lite). La motivación para implementar esta función es:

- El cliente desea tener un único número de sistema autónomo (ASN) en los varios sitios del VRF, sin la implementación de protocolo de gateway fronterizo externo (eBGP) con as-override.
- El cliente desea proporcionar una reflexión de ruta interna hacia los routers CE, actuando como si el núcleo del proveedor de servicios (SP) fuera un reflector de ruta transparente (RR).

Con esta función, los sitios del VRF pueden tener el mismo ASN que el núcleo SP. Sin embargo,

en caso de que el ASN de los sitios VRF sean diferentes al ASN del núcleo SP, se puede hacer que aparezca igual con el uso de la función Local-Autonomous System (AS).

Implementar iBGP PE-CE

Estas son las dos partes principales para que esta función funcione:

- Se agregó un nuevo atributo ATTR_SET al protocolo BGP para llevar los atributos BGP VPN a través del núcleo SP de una manera transparente.
- Haga del router PE un RR para las sesiones iBGP hacia los routers CE en el VRF y como un RR hacia los vecinos VPNv4 (otros routers PE o RR).

El nuevo atributo ATTR_SET permite al SP llevar todos los atributos BGP del cliente de una manera transparente y no interfiere con los atributos SP y las políticas BGP. Estos atributos son la lista de clústeres, las preferencias locales, las comunidades, etc.

Atributo de ruta del cliente BGP

ATTR_SET es el nuevo atributo BGP utilizado para transportar los atributos BGP VPN del cliente SP. Es un atributo transitorio opcional. En este atributo, se pueden transportar todos los atributos BGP del cliente del mensaje de actualización BGP, excepto los atributos MP_REACH y MP_UNREACH.

El atributo ATTR_SET tiene este formato:

```
+-----+
| Attr Flags (O|T) Code = 128 |
+-----+
| Attr. Length (1 or 2 octets) |
+-----+
| Origin AS (4 octets) |
+-----+
| Path Attributes (variable) |
+-----+
```

Los indicadores de atributo son los indicadores de atributo BGP normales (consulte RFC 4271). La longitud del atributo indica si la longitud del atributo es uno o dos octetos. El propósito del campo AS de origen es evitar la fuga de una ruta originada en un AS para filtrarse a otro AS sin la manipulación adecuada del AS_PATH. El campo Path Attributes de longitud variable lleva los atributos BGP VPN que se deben transportar a través del núcleo SP.

En el router PE de salida, los atributos BGP VPN se introducen en este atributo. En el router PE de ingreso, estos atributos se extraen del atributo, antes de que el prefijo BGP se envíe al router CE. Este atributo proporciona el aislamiento de los atributos BGP entre la red SP y la VPN del cliente y viceversa. Por ejemplo, el atributo de lista de clústeres de reflexión de ruta SP no se ve ni se considera dentro de la red VPN. Pero también, el atributo de la lista del clúster de reflexión de ruta VPN no se ve ni se considera dentro de la red SP.

Observe la Figura 1 para ver la propagación de un prefijo BGP del cliente a través de la red SP.

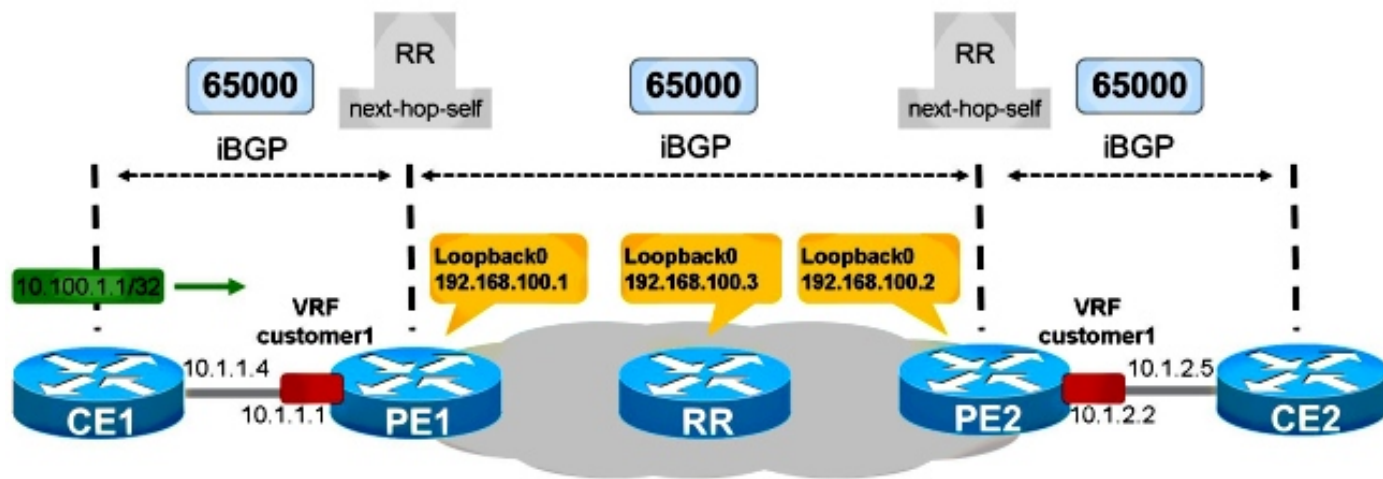


Figure 1

CE1 y CE2 están en el mismo AS que la red SP: 65000. PE1 tiene iBGP configurado hacia CE1. PE1 refleja la trayectoria del prefijo 10.100.1.1/32 hacia el RR en la red SP. El RR refleja el trayecto iBGP hacia los routers PE como siempre. PE2 refleja la trayectoria hacia CE2.

Para que esto funcione correctamente, debe:

- Tener código en PE1 y PE2 que tenga soporte para la función iBGP PE-CE
- Configure PE1 y PE2 para realizar la reflexión de ruta en su sesión BGP hacia sus respectivos routers CE
- Tenga next-hop-self en los routers PE para la sesión BGP hacia sus routers CE
- Asegúrese de que cada sitio VPN utiliza diferentes distinguidores de rutas (RD)

Configurar

Consulte la Figura 1.

Esta es la configuración necesaria para PE1 y PE2:

```

PE1

vrf definition customer1
rd 65000:1
route-target export 1:1
route-target import 1:1
!
address-family ipv4
exit-address-family

router bgp 65000
bgp log-neighbor-changes
neighbor 192.168.100.3 remote-as 65000
neighbor 192.168.100.3 update-source Loopback0
!

```

```
address-family vpnv4
 neighbor 192.168.100.3 activate
 neighbor 192.168.100.3 send-community extended
exit-address-family
!
address-family ipv4 vrf customer1
 neighbor 10.1.1.4 remote-as 65000
 neighbor 10.1.1.4 activate
 neighbor 10.1.1.4 internal-vpn-client
 neighbor 10.1.1.4 route-reflector-client
 neighbor 10.1.1.4 next-hop-self
exit-address-family
```

PE2

```
vrf definition customer1
 rd 65000:2
 route-target export 1:1
 route-target import 1:1
!
address-family ipv4
exit-address-family
```

```
router bgp 65000
 bgp log-neighbor-changes
 neighbor 192.168.100.3 remote-as 65000
 neighbor 192.168.100.3 update-source Loopback0
!
address-family vpnv4
 neighbor 192.168.100.3 activate
 neighbor 192.168.100.3 send-community extended
exit-address-family
!
address-family ipv4 vrf customer1
 neighbor 10.1.2.5 remote-as 65000
 neighbor 10.1.2.5 activate
 neighbor 10.1.2.5 internal-vpn-client
 neighbor 10.1.2.5 route-reflector-client
 neighbor 10.1.2.5 next-hop-self
exit-address-family
```

Nota: Si el PE no tiene el comando `neighbor <internal-CE> internal-vpn-client` para el vecino CE, no propaga los prefijos del CE hacia los routers SP RR/PE.

Nota: Si el PE no es el RR en el VRF, no propaga los prefijos de los routers RR/PE hacia el router CE.

Nuevo Comando

Hay un nuevo comando, `neighbor <internal-CE> internal-vpn-client`, para hacer que esta función funcione. Se debe configurar en el router PE solamente para la sesión iBGP hacia los routers CE.

Nota: La función CE de VRF múltiple de iBGP PE-CE (VRF-Lite) aún se admite sin el comando `neighbor <internal-CE> internal-vpn-client`.

Nota: Cuando se configura el comando `neighbor <internal-CE> internal-vpn-client`, los

comandos `neighbor <internal-CE> route-reflector-client` y `neighbor <internal-CE> next-hop-self` también se colocan automáticamente en la configuración. Cuando se eliminan uno de los comandos `neighbor <internal-CE> route-reflector-client` y `neighbor <internal-CE> next-hop-self` (o ambos) y se realiza una recarga, se vuelven a colocar automáticamente en la configuración.

Análisis detallado de ATTR_SET

Consulte la Figura 1.

Este es el prefijo anunciado por CE1:

```
CE1#show bgp ipv4 unicast 10.100.1.1/32
BGP routing table entry for 10.100.1.1/32, version 2
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
    4
  Refresh Epoch 1
  Local
    0.0.0.0 from 0.0.0.0 (10.100.1.1)
      Origin IGP, metric 0, localpref 100, weight 32768, valid, sourced, local, best
      rx pathid: 0, tx pathid: 0x0
```

Cuando PE1 recibe el prefijo BGP 10.100.1.1/32 de CE1, lo almacena dos veces:

```
PE1#show bgp vpnv4 unicast all 10.100.1.1/32
BGP routing table entry for 65000:1:10.100.1.1/32, version 21
Paths: (2 available, best #1, table customer1)
  Advertised to update-groups:
    5
  Refresh Epoch 1
  Local, (Received from ibgp-pece RR-client)
    10.1.1.4 (via vrf customer1) from 10.1.1.4 (10.100.1.1)
      Origin IGP, metric 0, localpref 200, valid, internal, best
      mpls labels in/out 18/nolabel
      rx pathid: 0, tx pathid: 0x0
  Refresh Epoch 1
  Local, (Received from ibgp-pece RR-client), (ibgp sourced)
    10.1.1.4 (via vrf customer1) from 10.1.1.4 (10.100.1.1)
      Origin IGP, localpref 100, valid, internal
      Extended Community: RT:1:1
      mpls labels in/out 18/nolabel
      rx pathid: 0, tx pathid: 0
```

La primera trayectoria es la trayectoria real en PE1, porque se recibe de CE1.

La segunda trayectoria es la trayectoria que se anuncia hacia los routers RR/PE. Está marcado con **origen ibgp**. Contiene el atributo ATTR_SET. Observe que esta ruta tiene uno o más destinos de ruta (RT) conectados a ella.

PE1 anuncia el prefijo como se muestra aquí:

```
PE1#show bgp vpnv4 unicast all neighbors 192.168.100.3 advertised-routes
BGP table version is 7, local router ID is 192.168.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

```
Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 65000:1 (default for vrf customer1)
*>i 10.100.1.1/32  10.1.1.4          0    200    0 i
```

Total number of prefixes 1

Así es como el RR ve la trayectoria:

```
RR#show bgp vpnv4 un all 10.100.1.1/32
BGP routing table entry for 65000:1:10.100.1.1/32, version 10
Paths: (1 available, best #1, no table)
Advertised to update-groups:
 3
Refresh Epoch 1
Local, (Received from a RR-client)
 192.168.100.1 (metric 11) (via default) from 192.168.100.1 (192.168.100.1)
  Origin IGP, localpref 100, valid, internal, best
  Extended Community: RT:1:1
  Originator: 10.100.1.1, Cluster list: 192.168.100.1
  ATTR_SET Attribute:
  Originator AS 65000
  Origin IGP
  Aspath
  Med 0
  LocalPref 200
  Cluster list
  192.168.100.1,
  Originator 10.100.1.1
mpls labels in/out nlabel/18
rx pathid: 0, tx pathid: 0x0
```

Observe que la preferencia local de este prefijo de unidifusión VPNv4 en el núcleo es 100. En ATTR_SET, se almacena la preferencia local original de 200. Sin embargo, esto es transparente para el RR en el núcleo SP.

En PE2, verá el prefijo como se muestra aquí:

```
PE2#show bgp vpnv4 unicast all 10.100.1.1/32
BGP routing table entry for 65000:1:10.100.1.1/32, version 5
Paths: (1 available, best #1, no table)
Not advertised to any peer
Refresh Epoch 2
Local
 192.168.100.1 (metric 21) (via default) from 192.168.100.3 (192.168.100.3)
  Origin IGP, localpref 100, valid, internal, best
  Extended Community: RT:1:1
  Originator: 10.100.1.1, Cluster list: 192.168.100.3, 192.168.100.1
  ATTR_SET Attribute:
  Originator AS 65000
  Origin IGP
  Aspath
  Med 0
  LocalPref 200
  Cluster list
  192.168.100.1,
  Originator 10.100.1.1
```

```

mpls labels in/out nolabel/18
rx pathid: 0, tx pathid: 0x0
BGP routing table entry for 65000:2:10.100.1.1/32, version 6
Paths: (1 available, best #1, table customer1)
Advertised to update-groups:
 1
Refresh Epoch 2
Local, imported path from 65000:1:10.100.1.1/32 (global)
 192.168.100.1 (metric 21) (via default) from 192.168.100.3 (192.168.100.3)
  Origin IGP, metric 0, localpref 200, valid, internal, best
  Originator AS(ibgp-pece): 65000
  Originator: 10.100.1.1, Cluster list: 192.168.100.1
mpls labels in/out nolabel/18
rx pathid:0, tx pathid: 0x0

```

La primera trayectoria es la recibida del RR, con ATTR_SET. Observe que el RD es 65000:1, el origen RD. La segunda trayectoria es la ruta importada desde la tabla VRF con RD 65000:1. Se ha eliminado ATTR_SET.

Esta es la ruta tal como se ve en CE2:

```

CE2#show bgp ipv4 unicast 10.100.1.1/32
BGP routing table entry for 10.100.1.1/32, version 10
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
Local
 10.1.2.2 from 10.1.2.2 (192.168.100.2)
  Origin IGP, metric 0, localpref 200, valid, internal, best
  Originator: 10.100.1.1, Cluster list: 192.168.100.2, 192.168.100.1
  rx pathid: 0, tx pathid: 0x0

```

Observe que el salto siguiente es **10.1.2.2**, que es PE2. La lista de clústeres contiene routers PE1 y PE2. Estos son los RR que importan dentro de la VPN. El SP RR (10.100.1.3) no está en la lista de clústeres.

La preferencia local de 200 se ha conservado dentro de la VPN a través de la red SP.

El comando **debug bgp vpnv4 unicast updates** muestra la actualización propagada en la red SP:

```

PE1#
BGP(4): Revise route installing 1 of 1 routes for 10.100.1.1/32 -> 10.1.1.4
(customer1) to customer1 IP table
BGP(4): 192.168.100.3 NEXT_HOP changed SELF for ibgp rr-client pe-ce net
65000:1:10.100.1.1/32,
BGP(4): 192.168.100.3 Net 65000:1:10.100.1.1/32 from ibgp-pece 10.1.1.4 format
ATTR_SET
BGP(4): (base) 192.168.100.3 send UPDATE (format) 65000:1:10.100.1.1/32, next
192.168.100.1, label 16, metric 0, path Local, extended community RT:1:1
BGP: 192.168.100.3 Next hop is our own address 192.168.100.1
BGP: 192.168.100.3 Route Reflector cluster loop; Received cluster-id 192.168.100.1
BGP: 192.168.100.3 RR in same cluster. Reflected update dropped

RR#
BGP(4): 192.168.100.1 rcvd UPDATE w/ attr: nexthop 192.168.100.1, origin i, localpref
100, originator 10.100.1.1, clusterlist 192.168.100.1, extended community RT:1:1,
[ATTR_SET attribute: originator AS 65000, origin IGP, aspath , med 0, localpref 200,
cluster list 192.168.100.1 , originator 10.100.1.1]
BGP(4): 192.168.100.1 rcvd 65000:1:10.100.1.1/32, label 16
RT address family is not configured. Can't create RTC route

```

```
BGP(4): (base) 192.168.100.1 send UPDATE (format) 65000:1:10.100.1.1/32, next
192.168.100.1, label 16, metric 0, path Local, extended community RT:1:1
```

```
PE2#
```

```
BGP(4): 192.168.100.3 rcvd UPDATE w/ attr: nexthop 192.168.100.1, origin i, localpref
100, originator 10.100.1.1, clusterlist 192.168.100.3 192.168.100.1, extended community
RT:1:1, [ATTR_SET attribute: originator AS 65000, origin IGP, aspath , med 0, localpref
200, cluster list 192.168.100.1 , originator 10.100.1.1]
```

```
BGP(4): 192.168.100.3 rcvd 65000:1:10.100.1.1/32, label 16
```

```
RT address family is not configured. Can't create RTC route
```

```
BGP(4): Revise route installing 1 of 1 routes for 10.100.1.1/32 -> 192.168.100.1
```

```
(customer1) to customer1 IP table
```

```
BGP(4): 10.1.2.5 NEXT_HOP is set to self for net 65000:2:10.100.1.1/32,
```

Nota: PE1 recibió su propia actualización de RR y luego la descartó. Esto se debe a que PE1 y PE2 están en el mismo grupo de actualización en RR.

Nota: Si desea volcar el mensaje de actualización completo en hexadecimal, utilice la palabra clave **detail** para el comando **debug BGP updates**.

```
PE2# debug bgp vpnv4 unicast updates detail
```

```
BGP updates debugging is on with detail for address family: VPNv4 Unicast
```

```
PE2#
```

```
BGP(4): 192.168.100.3 rcvd UPDATE w/ attr: nexthop 192.168.100.1, origin i,
localpref 100, originator 10.100.1.1, clusterlist 192.168.100.3 192.168.100.1,
extended community RT:1:1, [ATTR_SET attribute: originator AS 65000, origin IGP,
aspath , med 0, localpref 200, cluster list 192.168.100.1 , originator 10.100.1.1]
```

```
BGP(4): 192.168.100.3 rcvd 65000:1:10.100.1.1/32, label 17
```

```
RT address family is not configured. Can't create RTC route
```

```
BGP: 192.168.100.3 rcv update length 125
```

```
BGP: 192.168.100.3 rcv update dump: FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF
```

```
0090 0200 00
```

```
PE2#00 7980 0E21 0001 800C 0000 0000 0000 0000 0000 C0A8 6401 0078 0001 1100 00FD E800
0000 010A 6401 0140 0101 0040 0200 4005 0400 0000 64C0 1008 0002 0001 0000 0001 800A
08C0 A864 03C0 A864 0180 0904 0A64 0101 C080 2700 00FD E840 0101 0040 0200 8004 0400
0000 0040 0504 0000 00C8 800A 04C0 A864 0180 0904 0A64 0101
```

```
BGP(4): Revise route installing 1 of 1 routes for 10.100.1.1/32 -> 192.168.100.1
```

```
(customer1) to customer1 IP table
```

```
BGP(4): 10.1.2.5 NEXT_HOP is set to self for net 65000:2:10.100.1.1/32,
```

Gestión de próximo salto

Para esta función, se debe configurar Next-hop-self en los routers PE. La razón de esto es que normalmente el salto siguiente se transporta sin cambios con iBGP. Sin embargo, aquí hay dos redes independientes: la red VPN y la red SP, que ejecutan protocolos de gateway interior (IGP) independientes. Por lo tanto, la métrica IGP no se puede comparar fácilmente y usar para el mejor cálculo de trayectoria entre las dos redes. El enfoque elegido por RFC 6368 es tener el salto siguiente-auto obligatorio para la sesión iBGP hacia el CE, lo que evita el problema descrito anteriormente por completo. Una ventaja es que los sitios VRF pueden ejecutar diferentes IGP con este enfoque.

RD

RFC 6368 menciona que se recomienda que diferentes sitios VRF de la misma VPN utilicen

diferentes RD (únicos). En Cisco IOS, esto es obligatorio para esta función.

Función iBGP PE-CE con Local-AS

Consulte la Figura 2. El cliente VPN1 tiene ASN 65001.

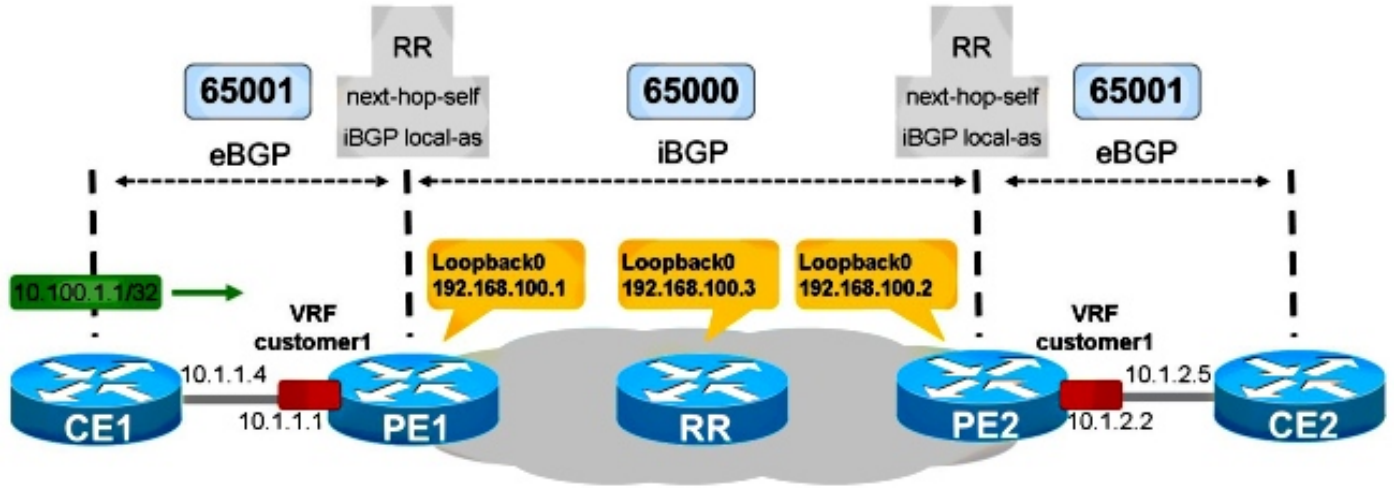


Figure 2

CE1 está en AS 65001. Para hacer este BGP interno desde el punto de vista de PE1, necesita la función local-as de iBGP.

CE1

```
router bgp 65001
  bgp log-neighbor-changes
  network 10.100.1.1 mask 255.255.255.255
  neighbor 10.1.1.1 remote-as 65001
```

PE1

```
router bgp 65000
  bgp log-neighbor-changes
  neighbor 192.168.100.3 remote-as 65000
  neighbor 192.168.100.3 update-source Loopback0
  !
  address-family vpnv4
  neighbor 192.168.100.3 activate
  neighbor 192.168.100.3 send-community extended
  exit-address-family
  !
  address-family ipv4 vrf customer1
  neighbor 10.1.1.4 remote-as 65001
  neighbor 10.1.1.4 local-as 65001
  neighbor 10.1.1.4 activate
  neighbor 10.1.1.4 internal-vpn-client
  neighbor 10.1.1.4 route-reflector-client
  neighbor 10.1.1.4 next-hop-self
  exit-address-family
```

PE2 y CE2 se configuran de manera similar.

PE1 ve el prefijo BGP como se muestra aquí:

```
PE1#show bgp vpnv4 unicast all 10.100.1.1/32
BGP routing table entry for 65000:1:10.100.1.1/32, version 41
Paths: (2 available, best #1, table customer1)
  Advertised to update-groups:
    5
  Refresh Epoch 1
  Local, (Received from ibgp-pece RR-client)
    10.1.1.4 (via vrf customer1) from 10.1.1.4 (10.100.1.1)
      Origin IGP, metric 0, localpref 200, valid, internal, best
      mpls labels in/out 18/nolabel
      rx pathid: 0, tx pathid: 0x0
  Refresh Epoch 1
  Local, (Received from ibgp-pece RR-client), (ibgp sourced)
    10.1.1.4 (via vrf customer1) from 10.1.1.4 (10.100.1.1)
      Origin IGP, localpref 100, valid, internal
      Extended Community: RT:1:1
      mpls labels in/out 18/nolabel
      rx pathid: 0, tx pathid: 0
```

El prefijo es un BGP interno.

PE2 ve esto:

```
PE2#show bgp vpnv4 unicast all 10.100.1.1/32
BGP routing table entry for 65000:1:10.100.1.1/32, version 33
Paths: (1 available, best #1, no table)
  Not advertised to any peer
  Refresh Epoch 5
  Local
    192.168.100.1 (metric 21) (via default) from 192.168.100.3 (192.168.100.3)
      Origin IGP, localpref 100, valid, internal, best
      Extended Community: RT:1:1
      Originator: 10.100.1.1, Cluster list: 192.168.100.3, 192.168.100.1
      ATTR_SET Attribute:
        Originator AS 65001
        Origin IGP
        Aspath
        Med 0
        LocalPref 200
        Cluster list
        192.168.100.1,
        Originator 10.100.1.1
      mpls labels in/out nolabel/18
      rx pathid: 0, tx pathid: 0x0
  BGP routing table entry for 65000:2:10.100.1.1/32, version 34
  Paths: (1 available, best #1, table customer1)
  Advertised to update-groups:
    5
  Refresh Epoch 2
  Local, imported path from 65000:1:10.100.1.1/32 (global)
    192.168.100.1 (metric 21) (via default) from 192.168.100.3 (192.168.100.3)
      Origin IGP, metric 0, localpref 200, valid, internal, best
      Originator AS(ibgp-pece): 65001
      Originator: 10.100.1.1, Cluster list: 192.168.100.1
      mpls labels in/out nolabel/18
      rx pathid: 0, tx pathid: 0x0
```

El AS de origen es 65001, que es el AS utilizado cuando el prefijo se envía de PE2 a CE2. Por lo tanto, se preserva el AS y también la preferencia local en este ejemplo.

```

CE2#show bgp ipv4 unicast 10.100.1.1/32
BGP routing table entry for 10.100.1.1/32, version 3
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
Local
  10.1.2.2 from 10.1.2.2 (192.168.100.2)
    Origin IGP, metric 0, localpref 200, valid, internal, best
    Originator: 10.100.1.1, Cluster list: 192.168.100.2, 192.168.100.1
    rx pathid: 0, tx pathid: 0x0

```

Usted ve **Local** en lugar de una trayectoria AS. Esto significa que es una ruta BGP interna originada en AS 65001, que también es el ASN configurado del router CE2. Todos los atributos BGP se han tomado del atributo ATTR_SET. Esto se ajusta a las reglas del caso 1 en la siguiente sección.

Reglas para el Intercambio de Rutas entre Diferentes Sitios VRF

El ATTR_SET contiene el AS de origen del VRF de origen. Este AS de origen es verificado por el PE remoto, cuando elimina ATTR_SET antes de enviar el prefijo al router CE.

Caso 1: Si el AS de origen coincide con el AS configurado para el router CE, los atributos BGP se toman del atributo ATTR_SET cuando el PE importa la trayectoria en el VRF de destino.

Caso 2: Si el AS de origen no coincide con el AS configurado para el router CE, el conjunto de atributos para la trayectoria construida se toma como se muestra aquí:

1. Los atributos de trayectoria se establecen en los atributos contenidos en el atributo ATTR_SET.
2. Los atributos específicos de iBGP se descartan (LOCAL_PREF, ORIGINATOR y CLUSTER_LIST).
3. El número **AS de origen** contenido en el atributo ATTR_SET se antepone al AS_PATH y sigue las reglas que se aplican a un peering BGP externo entre los AS de origen y de destino.
4. Si el sistema autónomo asociado con el VRF es el mismo que el sistema autónomo del proveedor VPN y el atributo AS_PATH de la ruta VPN no está vacío, se antepone al atributo AS_PATH de la ruta VRF.

Consulte la Figura 3. CE1 y PE1 tienen el AS 65000 y se configuran con la función PE-CE de iBGP. CE2 tiene ASN 65001. Esto significa que hay eBGP entre PE2 y CE2.

Figure 3

PE2 ve la ruta de la siguiente manera:

```

PE2#show bgp vpvv4 unicast all 10.100.1.1/32
BGP routing table entry for 65000:1:10.100.1.1/32, version 43
Paths: (1 available, best #1, no table)
Not advertised to any peer
Refresh Epoch 6
Local
  192.168.100.1 (metric 21) (via default) from 192.168.100.3 (192.168.100.3)
  Origin IGP, localpref 100, valid, internal, best
  Extended Community: RT:1:1
  Originator: 10.100.1.1, Cluster list: 192.168.100.3, 192.168.100.1
  ATTR_SET Attribute:
    Originator AS 65000
    Origin IGP
    Aspath
    Med 0
    LocalPref 200
    Cluster list
    192.168.100.1,
    Originator 10.100.1.1
  mpls labels in/out nolabel/17
  rx pathid: 0, tx pathid: 0x0
BGP routing table entry for 65000:2:10.100.1.1/32, version 44
Paths: (1 available, best #1, table customer1)
Advertised to update-groups:
  6
Refresh Epoch 6
Local, imported path from 65000:1:10.100.1.1/32 (global)
  192.168.100.1 (metric 21) (via default) from 192.168.100.3 (192.168.100.3)
  Origin IGP, metric 0, localpref 200, valid, internal, best
  Originator AS(ibgp-pece): 65000
  Originator: 10.100.1.1, Cluster list: 192.168.100.1
  mpls labels in/out nolabel/17
  rx pathid: 0, tx pathid: 0x0

```

Este es el prefijo como se ve en CE2:

```

CE2#show bgp ipv4 unicast 10.100.1.1/32
BGP routing table entry for 10.100.1.1/32, version 5
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
65000
  10.1.2.2 from 10.1.2.2 (192.168.100.2)
  Origin IGP, localpref 100, valid, external, best
  rx pathid: 0, tx pathid: 0x0

```

Este es el caso 2. El número **AS de origen** contenido en el atributo ATTR_SET se antepone al AS_PATH por PE2 y sigue las reglas que se aplican a un peering eBGP entre el AS de origen y de destino. PE2 ignora los atributos específicos de iBGP cuando crea la ruta que se anunciará a CE2. Por lo tanto, la preferencia local es 100 y no 200 (como se ve en el atributo ATTR_SET).

Reflexión de CE a CE VRF-Lite

Consulte la Figura 4.

Figure 4

La figura 4 muestra un router CE adicional, CE3, conectado a PE1. CE1 y CE3 están conectados a PE1 en la misma instancia de VRF: customer1. Esto significa que CE1 y CE3 son routers CE de

VRF múltiple (también conocidos como VRF-Lite) de PE1. PE1 se coloca como salto siguiente cuando anuncia los prefijos de CE1 a CE3. En el caso de que no se desee este comportamiento, podría configurar **neighbor 10.1.3.6 next-hop-inalterado** en PE1. Para configurar esto, debe quitar **neighbor 10.1.3.6 next-hop-self** en PE1. Luego, CE3 ve que las rutas de CE1 con CE1 son el salto siguiente para esos prefijos BGP. Para hacer que esto funcione, necesita las rutas para esos saltos siguientes BGP en la tabla de ruteo de CE3. Necesita un protocolo de routing dinámico (IGP) o rutas estáticas en CE1, PE1 y CE3 para asegurarse de que los routers tengan una ruta para las demás direcciones IP de salto siguiente. Sin embargo, hay un problema con esta configuración.

La configuración en PE1 es:

```
router bgp 65000
!
address-family ipv4 vrf customer1
neighbor 10.1.1.4 remote-as 65000
neighbor 10.1.1.4 activate
neighbor 10.1.1.4 internal-vpn-client
neighbor 10.1.1.4 route-reflector-client
neighbor 10.1.1.4 next-hop-self
neighbor 10.1.3.6 remote-as 65000
neighbor 10.1.3.6 activate
neighbor 10.1.3.6 internal-vpn-client
neighbor 10.1.3.6 route-reflector-client
neighbor 10.1.3.6 next-hop-unchanged
exit-address-family
```

El prefijo de CE1 se ve bien en CE3:

```
CE3#show bgp ipv4 unicast 10.100.1.1
BGP routing table entry for 10.100.1.1/32, version 9
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
Local
 10.1.1.4 from 10.1.3.1 (192.168.100.1)
  Origin IGP, metric 0, localpref 200, valid, internal, best
  Originator: 10.100.1.1, Cluster list: 192.168.100.1
  rx pathid: 0, tx pathid: 0x0
```

Sin embargo, el prefijo de CE2 se ve en CE3 como se muestra aquí:

```
CE3#show bgp ipv4 unicast 10.100.1.2
BGP routing table entry for 10.100.1.2/32, version 0
Paths: (1 available, no best path)
Not advertised to any peer
Refresh Epoch 1
Local
 192.168.100.2 (inaccessible) from 10.1.3.1 (192.168.100.1)
  Origin IGP, metric 0, localpref 100, valid, internal
  Originator: 10.100.1.2, Cluster list: 192.168.100.1, 192.168.100.2
  rx pathid: 0, tx pathid: 0
```

El siguiente salto BGP es **192.168.100.2**, la dirección IP de loopback de PE2. PE1 no reescribió el siguiente salto BGP a sí mismo cuando anunció el prefijo 10.100.1.2/32 a CE3. Esto hace que este prefijo no sea utilizable en CE3.

Por lo tanto, en el caso de una combinación de la función PE-CE de iBGP a través de MPLS-VPN

y VRF-Lite iBGP, debe asegurarse de que siempre tenga next-hop-self en los routers PE.

No puede conservar el salto siguiente cuando un router PE es un RR que refleja las rutas iBGP de un CE a otro CE a través de las interfaces VRF localmente en el PE. Cuando ejecuta el PE-CE iBGP a través de una red VPN MPLS, debe utilizar **internal-vpn-client** para las sesiones iBGP hacia los routers CE. Cuando tiene más de un CE local en un VRF en un router PE, debe mantener **next-hop-self** para esos peers BGP.

Puede observar route-maps para configurar el siguiente salto en sí mismo para los prefijos recibidos de otros routers PE, pero no para los prefijos reflejados de otros routers CE conectados localmente. Sin embargo, actualmente no se soporta establecer el siguiente salto en sí mismo en un route-map saliente. Esta configuración se muestra aquí:

```
router bgp 65000

address-family ipv4 vrf customer1
neighbor 10.1.1.4 remote-as 65000
neighbor 10.1.1.4 activate
neighbor 10.1.1.4 internal-vpn-client
neighbor 10.1.1.4 route-reflector-client
neighbor 10.1.1.4 next-hop-self
neighbor 10.1.3.6 remote-as 65000
neighbor 10.1.3.6 activate
neighbor 10.1.3.6 internal-vpn-client
neighbor 10.1.3.6 route-reflector-client
neighbor 10.1.3.6 route-map NH-setting out
exit-address-family

ip prefix-list PE-loopbacks seq 10 permit 192.168.100.0/24 ge 32
!

route-map NH-setting permit 10
description set next-hop to self for prefixes from other PE routers
match ip route-source prefix-list PE-loopbacks
set ip next-hop self
!

route-map NH-setting permit 20
description advertise prefixes with next-hop other than the prefix-list in
route-map entry 10 above
!
```

Sin embargo, esto no se admite:

```
PE1(config)#route-map NH-setting permit 10
PE1(config-route-map)# set ip next-hop self
% "NH-setting" used as BGP outbound route-map, set use own IP/IPv6 address for the nexthop not supported
```

Cisco IOS anterior en el router PE

Si PE1 ejecuta el software Cisco IOS más antiguo que carece de la función iBGP PE-CE, PE1 nunca se establece como el salto siguiente para los prefijos iBGP reflejados. Esto significa que el prefijo BGP reflejado (10.100.1.1/32) de CE1 (10.100.1.1) a CE2 -a través de PE1- tendría CE1 (10.1.1.4) como salto siguiente.

```
CE3#show bgp ipv4 unicast 10.100.1.1
BGP routing table entry for 10.100.1.1/32, version 32
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
Local
  10.1.1.4 from 10.1.3.1 (192.168.100.1)
    Origin IGP, metric 0, localpref 200, valid, internal, best
    Originator: 10.100.1.1, Cluster list: 192.168.100.1
    rx pathid: 0, tx pathid: 0x0
```

El prefijo de CE2 (10.100.1.2/32) se ve con PE2 como el salto siguiente, porque PE1 no realiza el salto siguiente-self para este prefijo tampoco:

```
CE3#show bgp ipv4 unicast 10.100.1.2
BGP routing table entry for 10.100.1.2/32, version 0
Paths: (1 available, no best path)
Not advertised to any peer
Refresh Epoch 1
Local
  192.168.100.2 (inaccessible) from 10.1.3.1 (192.168.100.1)
    Origin IGP, localpref 100, valid, internal
    Originator: 10.100.1.2, Cluster list: 192.168.100.1, 192.168.100.3, 192.168.100.2
    ATTR_SET Attribute:
      Originator AS 65000
      Origin IGP
      Aspath
      Med 0
      LocalPref 100
      Cluster list
      192.168.100.2,
      Originator 10.100.1.2
    rx pathid: 0, tx pathid: 0
```

Para que la función iBGP PE-CE funcione correctamente, todos los routers PE para la VPN donde la función está habilitada deben tener el código para soportar la función y tener la función habilitada.

Siguiente salto-auto para eBGP en VRF

Consulte la Figura 5.

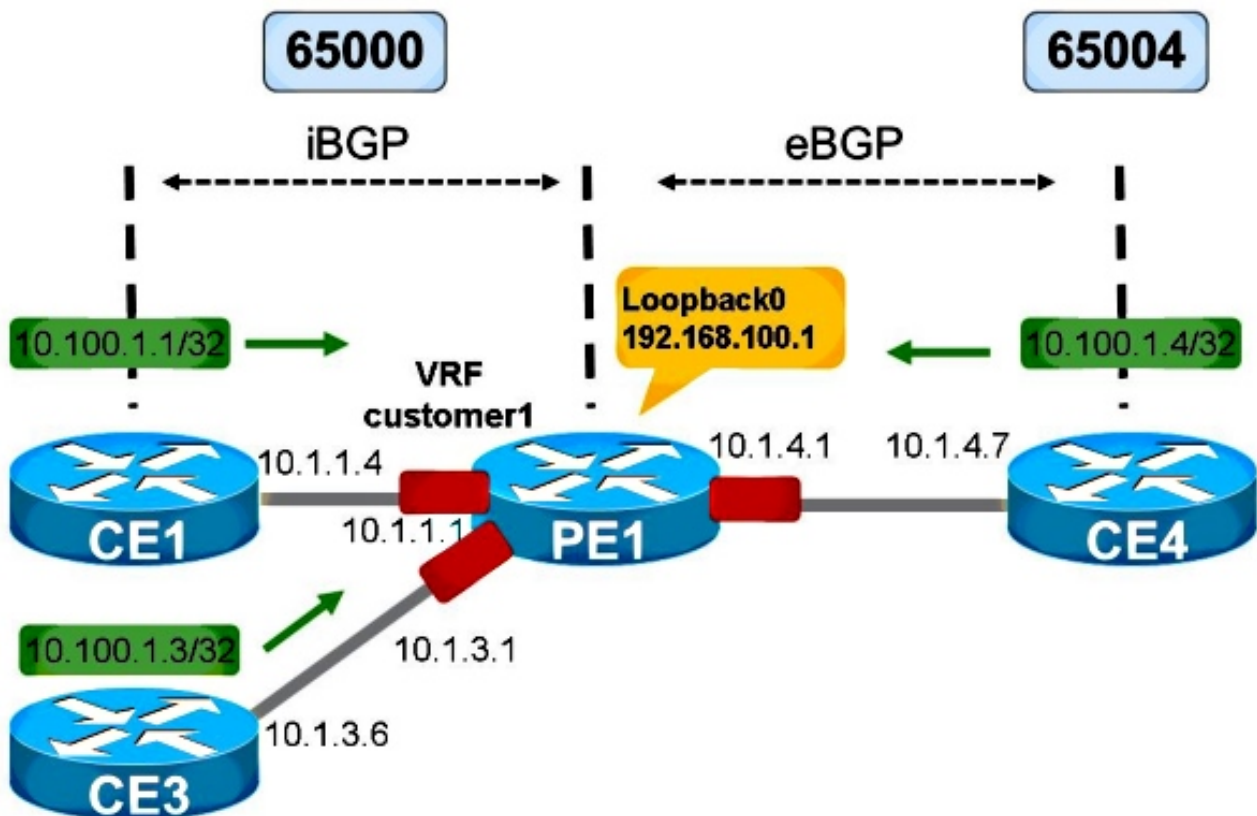


Figure 5

La figura 5 muestra una configuración de VRF-Lite. La sesión de PE1 hacia CE4 es eBGP. La sesión de PE1 hacia CE3 sigue siendo iBGP.

Para los prefijos eBGP, el siguiente salto siempre se configura en sí mismo cuando anuncia los prefijos hacia un vecino iBGP en el VRF. Esto es independientemente del hecho si la sesión hacia el vecino iBGP a través de VRF tiene establecido o no next-hop-self.

En la Figura 5, CE3 ve los prefijos de CE4 con PE1 como el salto siguiente.

```
CE3#show bgp ipv4 unicast 10.100.1.4
BGP routing table entry for 10.100.1.4/32, version 103
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
65004
 10.1.3.1 from 10.1.3.1 (192.168.100.1)
  Origin IGP, metric 0, localpref 100, valid, internal, best
  rx pathid: 0, tx pathid: 0x0
```

Esto ocurre con next-hop-self en PE1 hacia CE3 o sin él.

Si las interfaces en PE1 hacia CE3 y CE4 no están en un VRF, pero en el contexto global, el salto siguiente hacia CE3 sí marca una diferencia.

Sin next-hop-self en PE1 hacia CE3, verá:

```
PE1#show bgp vrf customer1 vpnv4 unicast neighbors 10.1.3.6
```



```
BGP neighbor is 10.1.3.6, vrf customer1, remote AS 65000, internal link
...
For address family: VPNv4 Unicast
Translates address family IPv4 Unicast for VRF customer1
Session: 10.1.3.6
BGP table version 1, neighbor version 1/0
Output queue size : 0
Index 12, Advertise bit 0
Route-Reflector Client
12 update-group member
Slow-peer detection is disabled
Slow-peer split-update-group dynamic is disabled
Interface associated: (none)
```

Aunque el salto siguiente-self está habilitado implícitamente, el resultado no indica esto.

Con next-hop-self en PE1 hacia CE3, verá:

```
PE1#show bgp vrf customer1 vpnv4 unicast neighbors 10.1.3.6
BGP neighbor is 10.1.3.6, vrf customer1, remote AS 65000, internal link
..
For address family: VPNv4 Unicast
...
NEXT_HOP is always this router for eBGP paths
```

Mientras que, si las interfaces hacia CE3 y CE4 están en un contexto global, el salto siguiente para los prefijos desde CE4 es CE4 mismo cuando no se configura next-hop-self:

```
CE3#show bgp ipv4 unicast 10.100.1.4
BGP routing table entry for 10.100.1.4/32, version 124
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
65004
10.1.4.7 from 10.1.3.1 (192.168.100.1)
Origin IGP, metric 0, localpref 100, valid, internal, best
rx pathid: 0, tx pathid: 0x0
```

Para next-hop-self en PE1 hacia CE3:

```
CE3#show bgp ipv4 unicast 10.100.1.4
BGP routing table entry for 10.100.1.4/32, version 125
Paths: (1 available, best #1, table default)
Not advertised to any peer
Refresh Epoch 1
65004
10.1.3.1 from 10.1.3.1 (192.168.100.1)
Origin IGP, metric 0, localpref 100, valid, internal, best
rx pathid: 0, tx pathid: 0x0
```

Esto se hizo en base a RFC 4364.

Si no desea establecer next-hop-self para los prefijos eBGP hacia una sesión iBGP a través de una interfaz VRF, debe configurar **next-hop-inalterado**. El soporte para esto sólo ocurrió con el ID de bug de Cisco [CSCuj11720](#).

```
router bgp 65000
...
address-family ipv4 vrf customer1
```

```
neighbor 10.1.1.4 remote-as 65000
neighbor 10.1.1.4 activate
neighbor 10.1.1.4 route-reflector-client
neighbor 10.1.3.6 remote-as 65000
neighbor 10.1.3.6 activate
neighbor 10.1.3.6 route-reflector-client
neighbor 10.1.3.6 next-hop-unchanged
neighbor 10.1.4.7 remote-as 65004
neighbor 10.1.4.7 activate
exit-address-family
```

Ahora, CE3 ve a CE4 como el salto siguiente para los prefijos anunciados por CE4:

```
CE3#show bgp ipv4 unicast 10.100.1.4
BGP routing table entry for 10.100.1.4/32, version 130
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 3
  65004
    10.1.4.7 from 10.1.3.1 (192.168.100.1)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      rx pathid: 0, tx pathid: 0x0
```

Si intenta configurar la palabra clave **next-hop-inalterada** para la sesión iBGP hacia CE3 en el código del IOS de Cisco antes del Id. de bug de Cisco [CSCuj11720](#), encontrará este error:

```
PE1(config-router-af)# neighbor 10.1.3.6 next-hop-unchanged
%BGP: Can propagate the nexthop only to multi-hop EBGP neighbor
```

Después del Id. de bug Cisco [CSCuj11720](#), la palabra clave **next-hop-inalterado** es válida para vecinos eBGP multisalto y vecinos iBGP VRF-Lite.