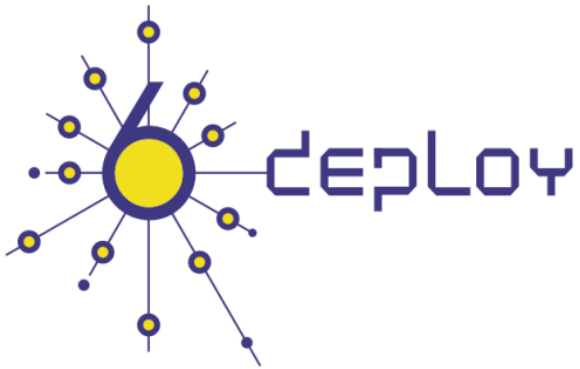
IPv6 Avanzado
Ruteo
LACNIC XVIII / LACNOG 2012
Montevideo
28 Octubre 2012



Alvaro Vives (alvaro.vives@consulintel.es)

Agenda

1. Encaminamiento con IPv6

PRÁCTICA: Encaminamiento

1. Encaminamiento con IPv6

1.1 Conceptos de Encaminamiento
1.2 Encaminamiento Estático
1.3 RIP
1.4 OSPF
1.5 IS-IS
1.6 BGP

1.1 Conceptos de Encaminamiento

Visión General Encaminamiento

- Los encaminadores deben saber como llegar al destino final de los paquetes que se le reenvían
- Las rutas estáticas no son adecuadas para redes medianas ni grandes
  - Tampoco para las pequeñas si se producen cambios en la topología de red
- Los protocolos de encaminamiento proporcionan un método automático de generar las tablas de encaminamiento
  - Tienen en cuenta cambio de la topología de red

Tipos de protocolos de encaminamiento

- Atendiendo al ámbito:
  - IGP (Interior Border Gateway)
  - EGP (Exterior Border Gateway)

- En los de tipo IGP
  - Atendiendo a la metodología de propagación
    - Vector Distancia
    - Estado de Enlace
  - Atendiendo al tipo de rutas que propagan
    - Classful
    - Classless

Criterios de selección IGP

- La selección de uno u otro depende de varios factores:
  - Topología de la intrared
  - Tipos de rutas a propagar
  - Tiempo de convergencia
  - Criterio de cálculo de métricas de la ruta.
  - Escalabilidad
  - Seguridad

Protocolos IGP

	VD	LS	Classful	Classless	Seguridad
RIPv1	X		X		
RIPv2	X			X	
IGRP	X		X		
EIGRP	X			X	X
OSPF		X		X	X
IS-IS		X		X	

Protocolos EGP

- No hay muchas alternativas
- BGP
  - El estándar “de facto”

IGP vs. EGP

IGP	EGP
Descubrimiento automático de Vecinos	Vecinos son configurados específicamente
Confianza en la información de los enrutadores que corren el IGP	Conexión a Redes Externas
Prefijos van a todos los enrutadores que corren el IGP	Define fronteras administrativas
Conecta enrutadores dentro de una AS	Conecta sistemas autónomos
Lleva sólo las direcciones de infraestructura del ISP	Lleva los prefijos de los clientes
ISPs tratan de mantener el tamaño de las tablas del IGP bajo para eficiencia y estabilidad	Lleva los prefijos del Internet
	EGPs son independientes de la topología de la red del ISP

Encaminamiento IPv6

- Mismo mecanismo CIDR “longest-prefix match” que actualmente en IPv4
- Cambios mínimos respecto de los protocolos existentes para encaminado en IPv4 (gestión de direcciones mayores)
  - Unicast: **RIP, OSPF, IS-IS, BGP4+, …**
  - Multicast: **MOSPF, PIM, …**
- Se puede utilizar la cabecera de routing con direcciones unicast para encaminar paquetes a través de regiones concretas
  - Por ejemplo, para la selección de proveedores, políticas, prestaciones, etc.

Router ID

- Los protocolos de routing dinámicos requieren un **router ID** que identifique cada uno de los participantes
- Se usa un **número entero de 32 bits**
- En IPv4 servía el “formato IPv4”: a.b.c.d
- Para IPv6 también sirve y se usan las mismas reglas para definirlo:
  - De forma explícita: router-id a.b.c.d
  - Si no, se busca la mayor dirección IPv4 configurada en las interfaces de loopback (up/up)
  - Si no, la mayor dirección IPv4 de cualquier interfaz no loopback (up/up)

1.2 Encaminamiento Estático

Encaminamiento Estático (1)

- Hay escenarios donde el encaminamiento estático es el adecuado
- Se puebla la tabla de rutas de manera manual
- La información solamente cambiará si se hace de manera manual
- Ventajas: sencillez y rapidez de configuración, no hay necesidad de aprender nada complicado
- Desventajas: No es escalable, no reacciona ante cambios en la red, requiere conocimientos
- Es muy normal utilizar un entorno **híbrido**, con rutas estáticas y dinámicas

Encaminamiento Estático (2)

- El uso y sintaxis de rutas estáticas con IPv6 es similar al de IPv4
- En Cisco IOS, por ejemplo:

```
ipv6 route prefix/length{outgoing interface [next-
  hop-address] | next-hop-address } [admin-distance]
```

- Sin embargo existen algunas diferencias:

1. Como dirección next-hop se puede usar cualquiera del router vecino, incluida la link-local
2. Si se usa la link-local como next-hop, hay que configurar tanto la interfaz de salida como la dirección de link-local

1.3 RIP

RIPng (1)

- RIP para IPv6 o RIPng esta definido en el RFC2080: RIPng for IPv6
- Basado en RIPv2, RIPng es muy parecido al usado para IPv4
  - Vector distancia
  - Actualizaciones periódicas
  - No se establecen vecinos
  - Máximo 15 hops
  - Split-horizon
  - Se usa UDP (521) para enviar los mensajes RIP
  - La métrica usada es la misma

RIPng (2)

- RIPng extiende RIPv1 y RIPv2 para soportar
  - Direcciones de 128 bits (Next Hop)
  - Encaminamiento de prefijos IPv6, prefijo/longitud
  - Uso de la dirección FF02::9, del grupo multicast all-RIP-routers, como la dirección destino de los mensajes de update de RIP
  - Se puede usar IPsec para ofrecer autenticación, RIPng no lo soporta

RIPv2 vs. RIPng

RIPv2	RIPng
Mensajes RIP usan IPv4/UDP	Mensajes RIP usan IPv6/UDP
Puerto UDP: 520	Puerto UDP: 521
Puede efectuar sumarización automática	No disponible
Dirección Mulitcast usada para updates: 224.0.0.9	Dirección Multicast usada para updates: ff02::9
Autentificación: específica de RIP	Autentificación: IPv6 AH/ESP
Vector Distancia, distancia administrativa por defecto 120, soporta VLSM	
Usa split horizon y poison reverse	
Métrica cuenta de saltos, 16 saltos significan infinito	
Actualizaciones completas periódicamente cada 30 segundos (ligeramente variable), sirve para saber que el vecino sigue “vivo”	

RIPng (3)

- RIPng es sólo para IPv6
  - En un entorno de doble-pila, si se usa RIP harán falta dos procesos distintos: RIPv2 (IPv4) y RIPng (IPv6)
- Cuando habilitemos RIPng en una interfaz, al igual que para RIPv1 y RIPv2, el proceso RIP hará tres cosas:

1. Enviar actualizaciones RIP por esa interfaz
2. Procesar las actualizaciones RIP recibidas en esa interfaz
3. Anunciar las rutas “conectadas” de esa interfaz

- RIPng utiliza la direcciones link-local como next-hop

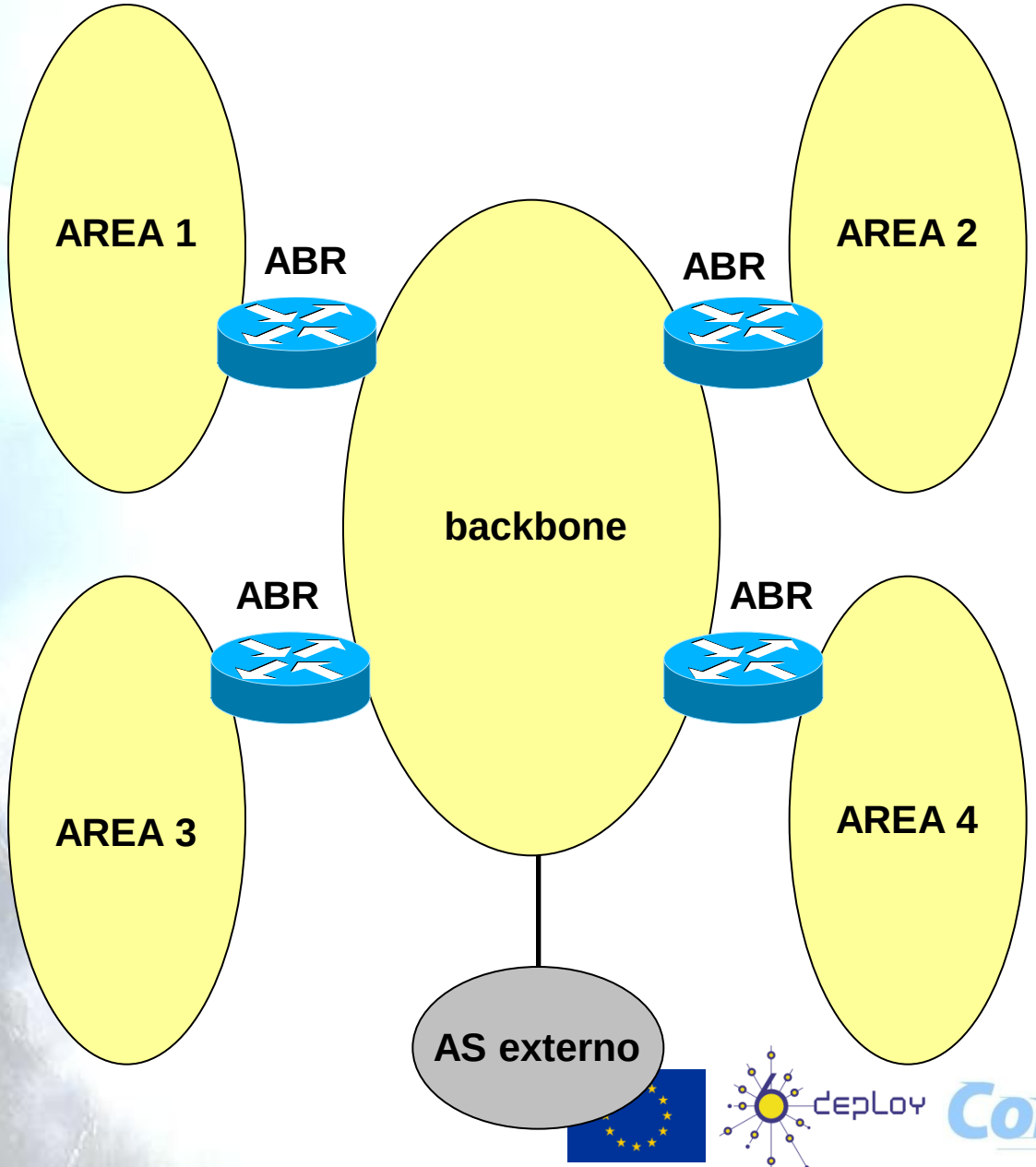
1.4 OSPF

Visión General OSPF (1)

- Protocolo de encaminamiento IGP de tipo “link-state” que intenta dar solución a las necesidades más avanzadas de los Sistemas Autónomos más exigentes:
  - soporte VLSM (Variable Length Subnet Masking)
  - autenticación
  - rápida convergencia cuando se producen cambios en la topología de la red
  - propagación de rutas por medio de multicast
  - consideración del ancho de banda en la elección de la mejor ruta

- Se divide la red en varias áreas, todas conectadas al área de backbone, para una mejor escalabilidad

Visión General OSPF (2)



Visión General OSPF (3)

- OSPF utiliza el protocolo Hello para determinar:
  - Qué interfaces recibirán los LSAs
  - Qué otros encaminadores vecinos existen
  - Si los encaminadores vecinos siguen activos (keepalive)
- Los encaminadores envían LSAs (Link-State Advertisements) a todos los encaminadores de la misma unidad jerárquica por medio de una dirección multicast e incluyen entre otros:
  - Prefijo de red
  - Máscara de red
  - Tipo de red
  - Encaminadores conectados
  - Etc.
- Todos construyen la misma base de datos topológica a partir de los LSAs recibidos
  - Se obtiene la nueva tabla de rutas a partir de la nueva topología.

OSPF IPv6 (1)

- La versión 3 OSPF, para IPv6 (RFC2740), extiende la versión 2 de OSPF (RFC2328) para soportar el encaminamiento de prefijos IPv6 y las direcciones de 128 bits
- OSPFv3 es solo-IPv6, en un entorno doble-pila hará falta ejecutar dos instancias distintas para IPv4 (OSPFv2) e IPv6 (OSPFv3)

- Nuevas características:
  - Se ejecuta directamente sobre IPv6
  - Se distribuyen prefijos IPv6
  - Nuevos tipos de LSA
  - Utiliza direcciones Multicast:
    - ALLSPFRouters (FF02::5)
    - ALLDRouters (FF02::6)

OSPF IPv6 (2)

- Puesto que en IPv6 una interfaz de red puede tener más de una dirección, los LSAs en OSPFv3 difieren de los de la versión para IPv4

Código	LSA	Link-State ID
1	Router LSA	Originating router ID of the router. En IPv6 no tienen información de la dirección de red y son independientes del protocolo de red.
2	Network LSA	Interface IP address of the DR En IPv6 no tienen información de la dirección de red y son independientes del protocolo de red.
3	Interarea-prefix LSAs for ABRs	Destination network number. En IPv6 se expresa como prefijo, longitud de prefijo.
4	Interarea-router LSAs for ASBRs	Router ID of AS boundary router
5	Autonomous system external LSAs	Redistributing routes from another AS. En IPv6 se expresa como prefijo, longitud de prefijo y la ruta por defecto, de longitud 0.
8	Link LSA	Local-link flooding scope. Informa de las direcciones link-local de todos los encaminadores del segmento de red
9	Intra-Area-Prefix LSA	Describes association to the router LSA.

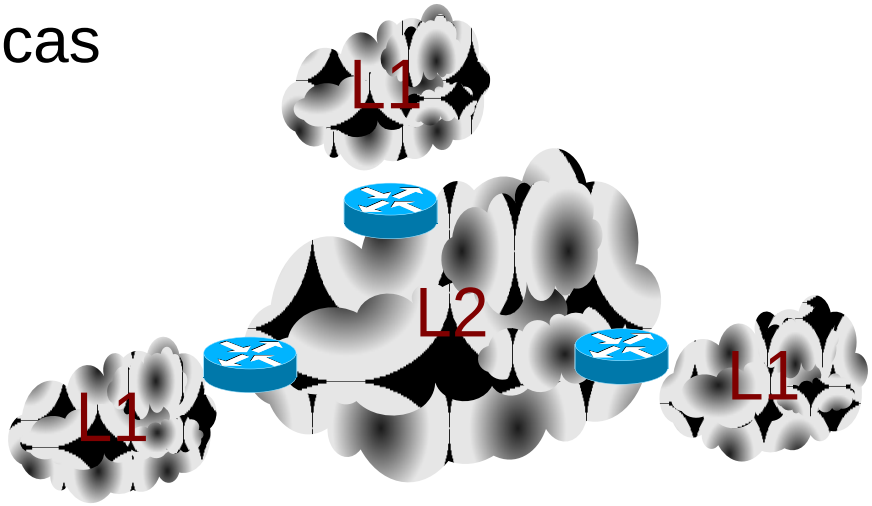
7.5 IS-IS

Visión General IS-IS (1)

- IS-IS es un protocolo de encaminamiento OSI
- Diseñado para soportar el protocolo CLNP
  - Protocolo de la capa de red similar a IP
- Se ha extendido para soportar también IPv4 y IPv6 (RFC5308)

Visión General IS-IS (2)

- Características
  - Encaminamiento jerárquico
  - Soporte “classless”
  - Uso de direcciones multicast
  - Autenticación mediante password
  - Soporte de múltiples métricas
  - Cálculo SPF local



Visión General IS-IS (3)

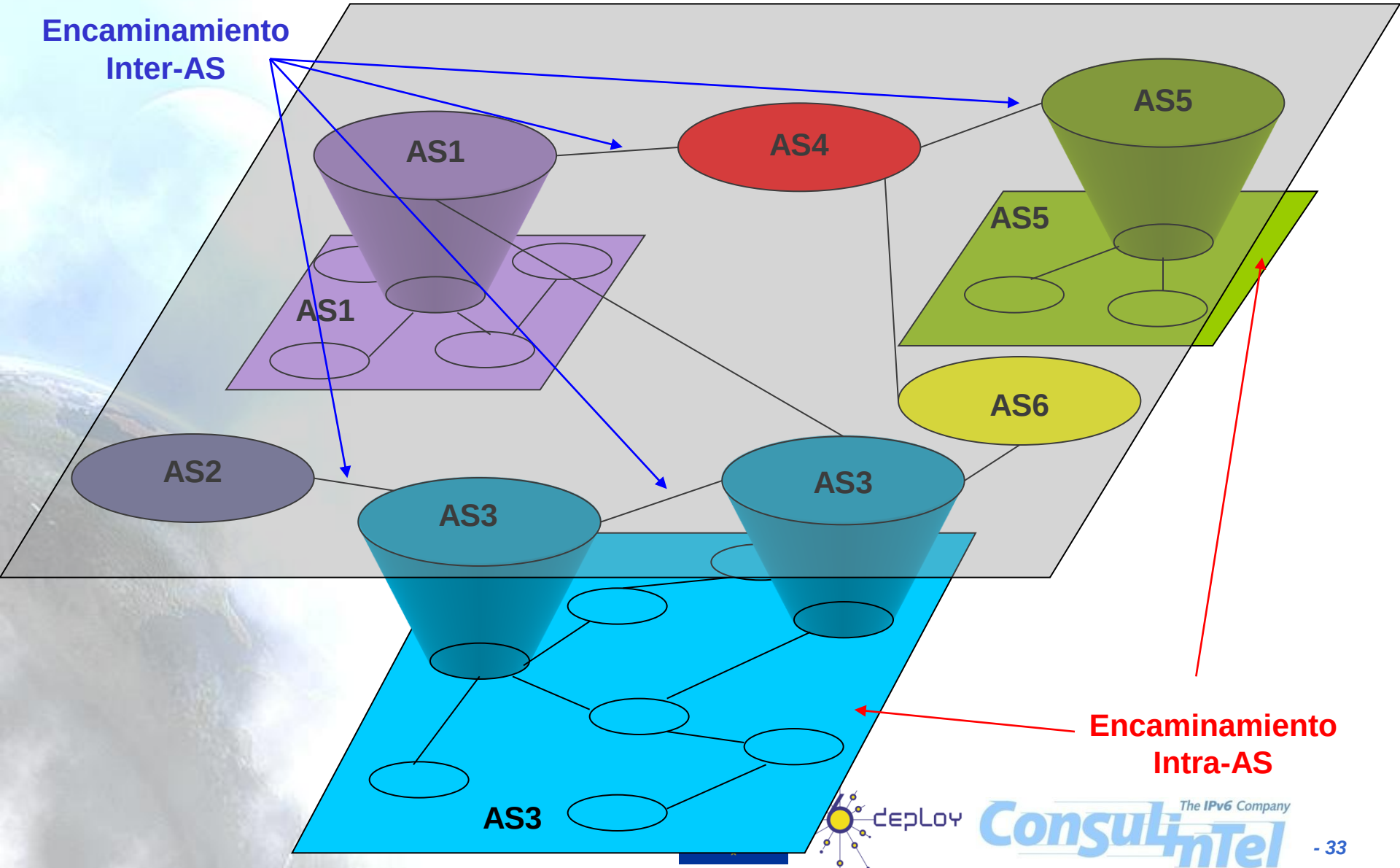
- Se basa en dos niveles jerárquicos (backbone y stub)
- Se envían LSP (Link State Packets)
- La información se envía mediante TLVs (Tag / Lenght / Value)
- Se definen dos nuevos TLVs para IPv6:
  - IPv6 Reachability
  - IPv6 Interface Address
- Se define un nuevo identificador de red para IPv6:
  - IPv6 NLPID

7.6 BGP

Visión General de BGP (1)

- Sistema Autónomo (AS):
  - Conjunto de redes con políticas de enrutamiento comunes
  - El mismo protocolo de enrutamiento
  - Usualmente bajo el control administrativo de la misma entidad
- El encaminamiento en Internet se hace a dos niveles
  - Intra-AS => IGP
    - La gestión de cada AS es local, lo cual incluye el tipo de protocolo de encaminamiento usado
  - Inter-AS => EGP
    - Requiere una estandarización para que todos los ASs sean alcanzados por todos.
      - BGP estándar “de facto”

Visión General de BGP (2)



Visión General de BGP (3)

- BGP “Border Gateway Protocol”
  - estándar “de facto”
- Se basa en el PVP (Path Vector Protocol)
  - Similar al Distance Vector
  - Cada encaminador frontera envía a sus vecinos (“peerings”) la ruta completa a un destino, no solo la distancia
  - El camino (path) es una secuencia de ASs hasta el destino
    - Ejemplo: Path(X,Z)=X, Y1, Y2, Y3, Y5, Z

Visión General de BGP (4)

- Se utiliza TCP para el intercambio de mensajes BGP
  - OPEN – abre una conexión TCP
  - UPDATE – anuncia o confirma un nuevo camino
  - KEEPALIVE – en ausencia de UPDATES sirve para mantener abierta la conexión TCP y como ACK de un mensaje OPEN
  - NOTIFICATION – informa de errores en mensajes precedentes y para cerrar conexiones

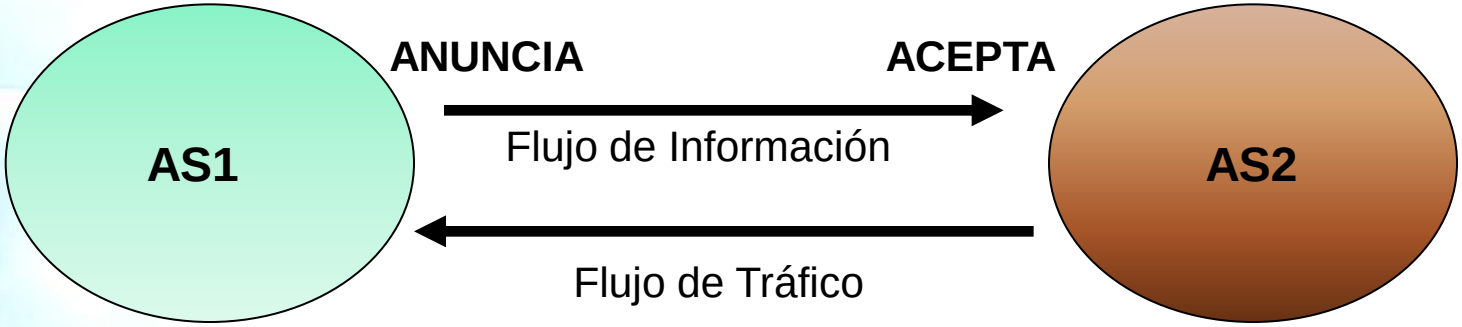
Definiciones BGP

- **AS Vecinos (Neighbors)** – ASs con los que se intercambia información de enrutamiento directamente
- **Anunciar (Announce)** – enviar información de enrutamiento a un vecino
- **Aceptar (Accept)** – recibir y utilizar información de enrutamiento enviada por un vecino
- **Originar (Originate)** – insertar información de enrutamiento en anuncios externos (usualmente como resultado de un IGP)
- **Vecinos (Peers)** – enrutadores, en AS vecinos o dentro del mismo AS, con los se intercambia información de políticas y enrutamiento

Flujo de Información y Tráfico (1)

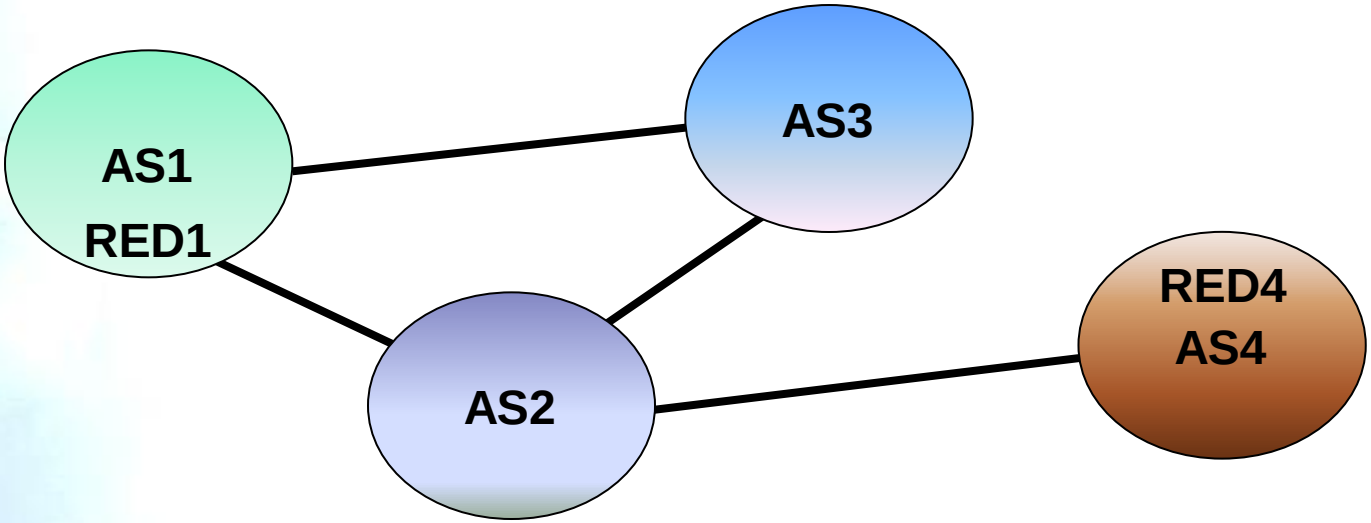
- El flujo de tráfico ocurre en la dirección opuesta al flujo de la información de enrutamiento
  - Filtrado de información de enrutamiento a la salida inhibirá el flujo de tráfico hacia adentro
  - Filtrado de la información de enrutamiento a la entrada inhibirá el flujo de tráfico hacia fuera

Flujo de Información y Tráfico (2)



- AS2 aprende cómo llegar a AS1
- AS2 también debe anunciar su información para que AS1 sepa cómo llegar
- Para que haya comunicación, ambos deben anunciarse

Flujo de Información y Tráfico (3)



- Para que red RED1 en AS1 puede enviar tráfico hacia red RED4 en AS4:

1. AS4 debe originar y anunciar RED4 hacia AS2
2. AS2 debe aceptar RED4 desde AS4
3. AS2 debe anunciar RED4 hacia AS1 o AS3
4. AS1 debe aceptar RED4 desde AS2 o AS3

- Para que los paquetes fluyan en la otra dirección, AS1 debe implementar políticas similares.

Routing Explícito vs. Por Defecto

- Por defecto:
  - Simple, barata (en términos de ciclos, memoria, ancho de banda)
  - Poca granularidad (juega con las métricas)
- Explícito (zona libre de ruta por defecto):
  - Más difícil, compleja, alto costo, alta granularidad
- Híbrido:
  - Minimiza la complejidad y dificultad
  - Provee granularidad adecuada
  - Requiere conocimientos de filtros

Atributos BGP

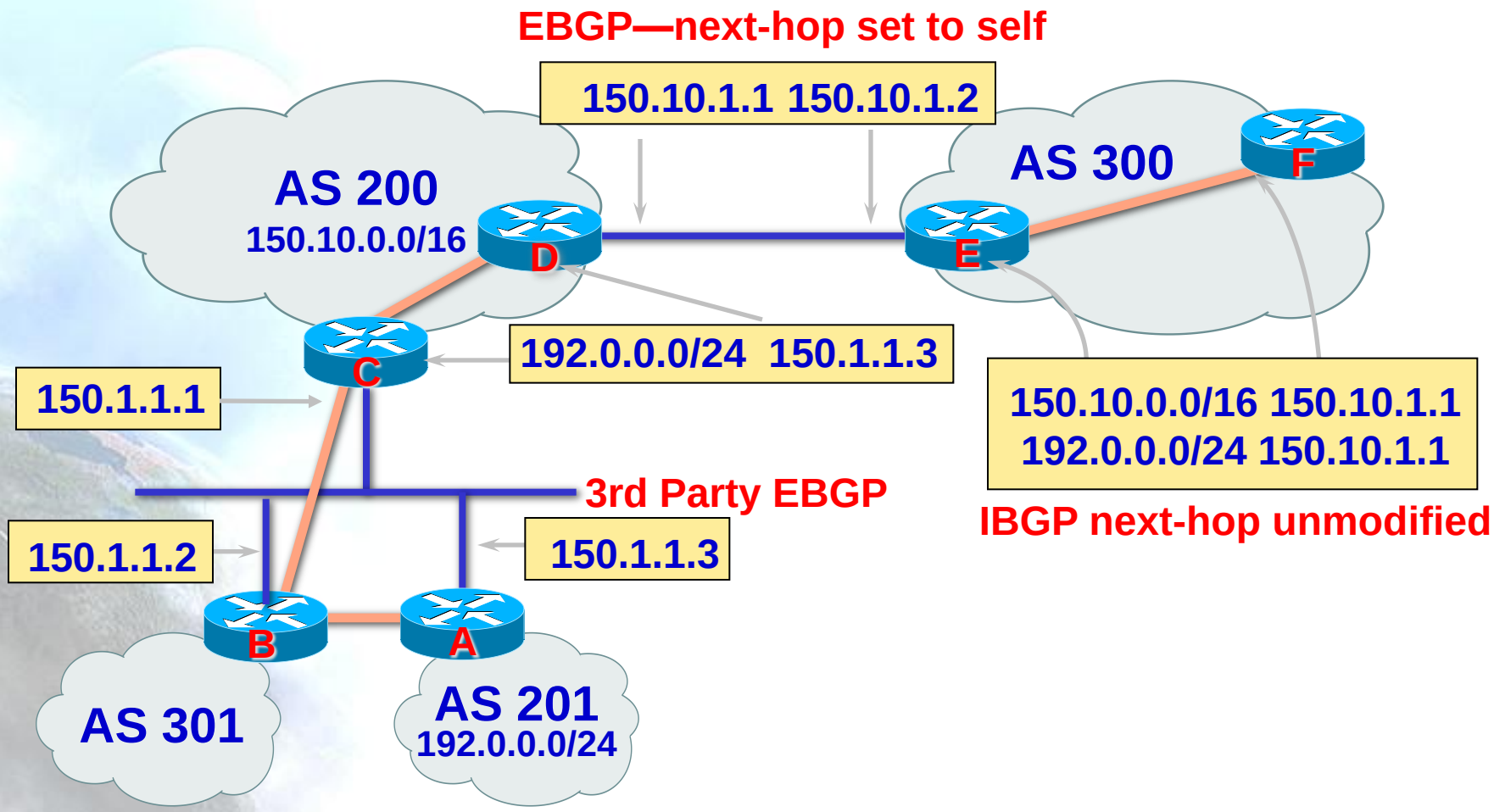
- Atributos:
  - 1: ORIGIN
  - 2: AS-PATH
  - 3: NEXT-HOP
  - 4: MED
  - 5: LOCAL_PREF
  - 6: ATOMIC_AGGREGATE
  - 7: AGGREGATOR
  - 8: COMMUNITY
  - 9: ORIGINATOR_ID
  - 10: CLUSTER_LIST
  - 14: MP_REACH_NLRI
  - 15: MP_UNREACH_NLRI

Atributos BGP: AS_PATH

- El atributo AS_PATH esta compuesto por varias partes entre ellas AS_Seq (AS Sequence) que es una lista de Nºs de AS por donde hay que pasar para llegar al prefijo asociado
- BGP usa el AS-PATH para dos funciones claves

1. Elegir la mejor ruta hacia un prefijo (AS_PATH más corto / con menos ASNs)
2. Prevenir bucles de routing: se ignoran rutas recibidas que incluyan mi propio ASN

Atributos BGP: NEXT_HOP



eBGP

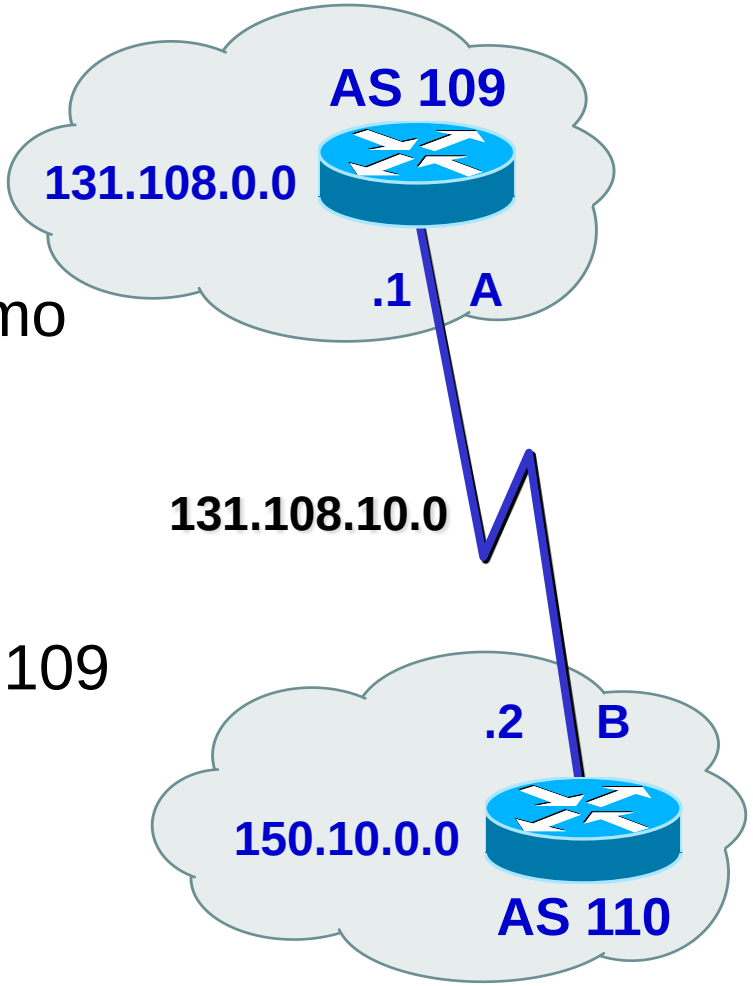
eBGP – External BGP

- Entre routers en AS diferentes
- Usualmente con conexión directa
- Con next-hop apuntando a si mismo
- Se modifica el AS_PATH
- Router B

```
router bgp 110
    neighbor 131.108.10.1 remote-as 109
```

- Router A

```
router bgp 109
    neighbor 131.108.10.2 remote-as 110
```



iBGP

iBGP – Internal BGP

- Vecinos en el mismo AS
- No se modifica el Next-hop ni el AS_PATH
- No necesariamente con conexión directa
- No anuncia otras rutas aprendidas por iBGP
- Se pueden usar direcciones de loopback (alcanzables) para peering
- Router B:

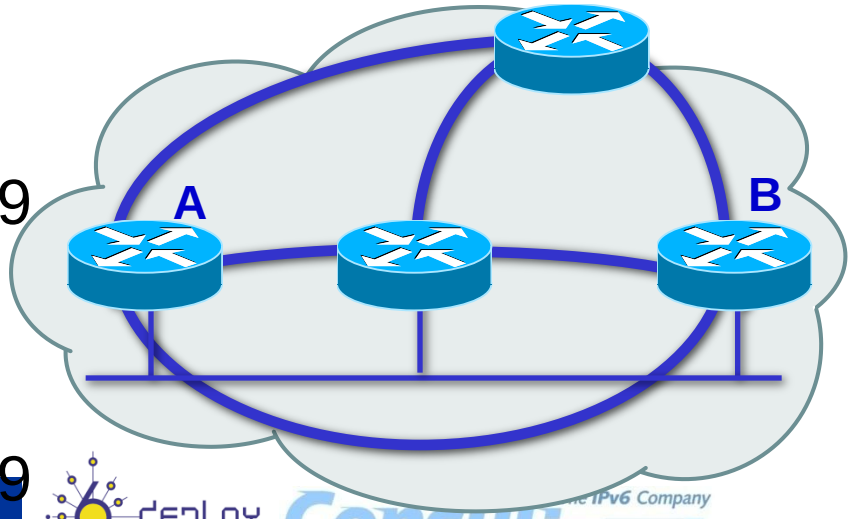
router bgp 109

neighbor 131.108.30.2 remote-as 109

- Router A:

router bgp 109

neighbor 131.108.20.1 remote-as 109



BGP para IPv6 (BGP4+) (1)

- La versión actual de BGP es la versión 4, i.e. BGP4
  - –BGP4 (BGP para IPv4) se describe en RFC4271

- Las Extensiones Multiprotocolo para BGP [RFC4760], i.e. BGP4+, permiten usar BGP4 con diferentes familias de direcciones (address family), tales como IPv6 y Multicast

BGP para IPv6 (BGP4+) (2)

- Las extensiones multiprotocolo para BGP para IPv6 soportan las mismas funcionalidades y características que BGP para IPv4
  - –Las extensiones para IPv6 incluyen el soporte para
    - •La familia de direcciones IPv6 (IPv6 address family) y la network layer reachability information (NLRI)
    - •El atributo de next hop (el router siguiente en el camino hacia el destino), que ahora usa direcciones iPv6

- Las extensiones multiprotocolo para BGP para IPv6 Multicast soportan las mismas funcionalidades y características que BGP para IPv4 Multicast
  - –Las extensiones para IPv6 Multicat incluyen el soporte para
    - •La familia de direcciones IPv6 Multicast (IPv6 Multicast address family) y la network layer reachability information (NLRI)
    - •El atributo de next hop (el router siguiente en el camino hacia el destino), que ahora usa direcciones iPv6 Multicast

Características de BGP4+ (1)

- Los únicos componentes de información de BGP que son específicos para IPv4 son los atributos
  1. NEXT_HOP (expresado como una direcion IPv4)
  2. AGGREGATOR (contiene una direcion IPv4)
  3. NLRI (expresado como prefijos de direciones IPv4)
- RFC4760 asume que cualquier router BGP (incluyendo los que soportan el mismo RFC4760) tiene una dirección IPv4 (la cual se usará, entre otras cosas en el atributo de AGGREGATOR)

Características de BGP4+ (2)

- Se definen dos nuevos atributos opcionales y no-transitivos (permite compatibilidad hacia atrás)
  - **Multiprotocol Reachable NLRI (MP_REACH_NLRI)**, contiene la información de los destinos alcanzables, asi como la información de next hop usada para hacer el reenvió (forwarding) hacia esos destinos
  - **Multiprotocol Unreachable NLRI (MP_UNREACH_NLRI)**, contiene la información de los destinos inalcanzables
- Cada atributo contiene una o más triplas:
  - **AFI** (Address Family Information)
  - **NEXT_HOP** Information (debe ser de la misma address family)
  - **NLRI** Network Layer Reachability Information (independiente del protocolo)

BGP Doble-pila (1)

- Se tendrán dos RIBs (Routing Information Base), una para cada versión de IP
- Ejemplo de configuración, incluyendo filtros de prefijos IPv4 e IPv6:

```
ip prefix-list <name> permit|deny <ipv4 address>

ipv6 prefix-list <name> permit|deny <ipv6 address>
```

BGP Doble-pila (2)

```
router bgp 10
no bgp default ipv4-unicast
neighbor 2001:db8:1:1019::1 remote-as 20
neighbor 172.16.1.2 remote-as 30
!
address-family ipv4
neighbor 172.16.1.2 activate
neighbor 172.16.1.2 prefix-list ipv4-ebgp in
neighbor 172.16.1.2 prefix-list v4out out
network 172.16.0.0
exit-address-family
!
address-family ipv6
neighbor 2001:db8:1:1019::1 activate
neighbor 2001:db8:1:1019::1 prefix-list ipv6-ebgp in
neighbor 2001:db8:1:1019::1 prefix-list v6out out
network 2001:db8::/32
exit-address-family
```

BGP Doble-pila (3)

```
!
ip prefix-list ipv4-ebgp permit 0.0.0.0/0 le 32
!
ip prefix-list v4out permit 172.16.0.0/16
!
ipv6 prefix-list ipv6-ebgp permit ::/0 le 128
!
ipv6 prefix-list v6out permit 2001:db8::/32
```

Filtrado prefijos BGP (1)

- El filtrado de prefijos enviados y recibidos es una práctica común y recomendada
- El ISP o proveedor de tránsito solo debe permitir recibir anuncio de prefijos que sabe pertenecen a sus clientes
- **Bogon filtering**: filtrado de prefijos no asignados o reservados:
  - [RFC5156] Indica prefijos especiales que no debe aparecer en Internet, por lo tanto deben filtrarse: documentación, ULA, link-local, 6bone, ORCHID, etc.
  - [RFC4291] Establece que las asignaciones de direcciones globales se hace desde el 2000::/3
  - IANA da detalles más específicos:

http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xml

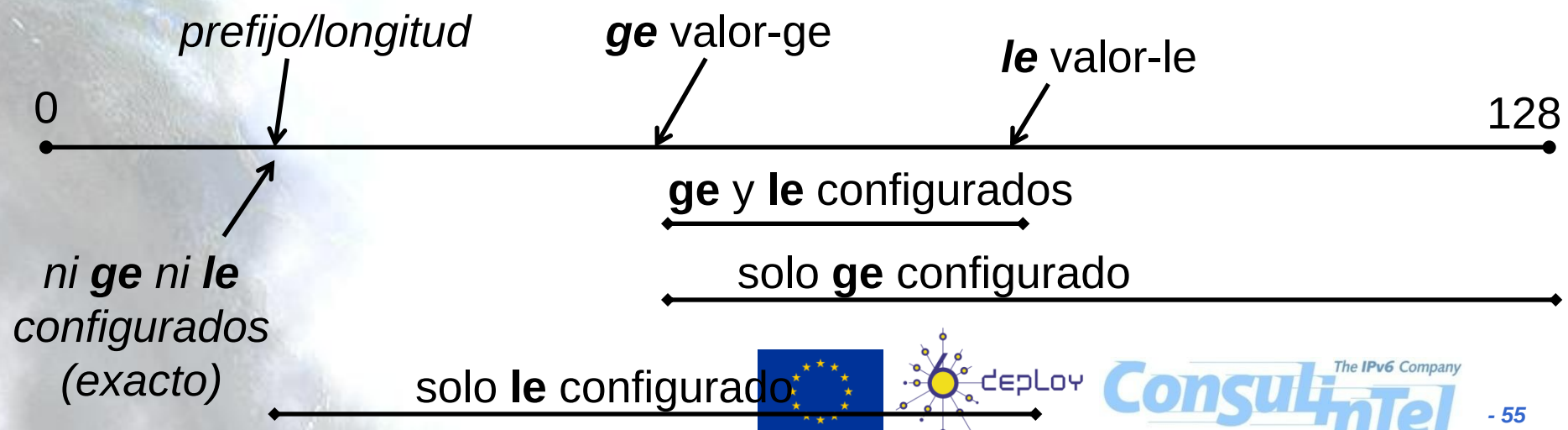
Filtrado prefijos BGP (2)

- En Cisco IOS se puede hacer de dos formas en la configuración de BGP: prefix-list o route-map
- route-map, que también utiliza una prefix-list, es más potente y flexible que prefix-list
- Hay que entender la lógica de ambos métodos:

1. Route-map:
   - route-map decide con **deny/permit** si se filtra o permite la ruta que coincida con el **match**. El deny/permit del prefix-list solo servirá para indicar si no se cumple/sí se cumple el match del route-map
   - **deny all** implícito al final del route-map. Para permitir todo hay que añadir una entrada al route-map con la acción permit pero sin ningún comando match (si no hay mach implica que todo "hace match")

Filtrado prefijos BGP (3)

2. Prefix-list:
   - `ipv6 prefix-list <name> [seq <num>] {deny|permit prefijo/longitud}[ge valor-ge] [le valor-le]`
   - decide con **deny/permit** si se filtra o permite la ruta que coincida con el **prefijo** y el **rango de longitud de prefijos**
   - 1º el prefijo de la ruta debe estar en el rango definido por ***prefijo/longitud*** del comando
   - 2º la longitud del prefijo de la ruta debe estar dentro del rango definido por los parámetros ***longitud, le*** y ***ge***:



Filtrado BGP: prefix-list

```
router bgp <my-as-number>
 neighbor X:X:X:X::X remote-as <neighbor-as>
 !
 address-family ipv6
  neighbor X:X:X:X::X activate
  neighbor X:X:X:X::X prefix-list global_ipv6_in in
  neighbor X:X:X:X::X prefix-list MI_prefijo_1 out
 exit-address-family
!
ipv6 prefix-list MI_prefijo_1 seq 10 permit 2001:db8::/32
ipv6 prefix-list MI_prefijo_1 seq 20 deny ::/0 le 128
!
ipv6 prefix-list global_ipv6_in seq 10 deny 3FFE::/16 le 128
ipv6 prefix-list global_ipv6_in seq 20 permit ::/0 le 48
ipv6 prefix-list global_ipv6_in seq 30 deny ::/0 le 128
!
```

Filtrado BGP: route-map

```
router bgp <my-as-number>
 neighbor X:X:X:X::X remote-as <neighbor-as>
 !
 address-family ipv6
  neighbor X:X:X:X::X activate
  neighbor X:X:X:X::X route-map TRANSITO1_in in
  neighbor X:X:X:X::X route-map TRANSITO1_out out
 exit-address-family
!
ipv6 prefix-list MI_prefijo_1 seq 5 permit 2001:db8::/32
!
ipv6 prefix-list global_ipv6 seq 3 deny 3FFE::/16 le 128
ipv6 prefix-list global_ipv6 seq 35 permit ::/0 le 48
ipv6 prefix-list global_ipv6 seq 40 deny ::/0 le 128
!
route-map TRANSITO1_out permit 10
 match ipv6 address prefix-list MI_prefijo_1
!
route-map TRANSITO1_in permit 10
 match ipv6 address prefix-list global_ipv6
```

Filtrado bogons BGP (1)

- Prefijos a filtrar:

Rutas	Prefijos	Comentario
Default	::/0	
Unspecified Address	::/128	Se pueden agrupar en el prefijo 0000::/8 o mayor
Loopback Address	::1/128	
IPv4-mapped Addresses	::ffff:0.0.0.0/96	
IPv4-compatible Addresses (deprecated)	::/96	
Link-local Addresses	fe80::/10 o mayor	
Site-local Addresses (deprecated)	fec0::/10 o mayor	
Unique-local addresses	fc00::/7 o mayor	
Multicast Addresses	FF00::/8 o mayor	Si no se usa multicast
Documentation addresses	2001:db8::/32 o mayor	
6Bone Addresses (deprecated)	3ffe::/16, 5f00::/8	RFCs 1897,2471,3701
ORCHID	2001:10::/28	RFC 4843

Filtrado bogons BGP (2)

- Ejemplo lista bogon:

```
ipv6 prefix-list global_ipv6_in seq 10 deny 2001:10::/28 le 128
ipv6 prefix-list global_ipv6_in seq 10 deny 3FFE::/16 le 128
ipv6 prefix-list global_ipv6_in seq 10 deny 5f00::/8 le 128
ipv6 prefix-list global_ipv6_in seq 20 deny 2001:db8::/32 le 128
ipv6 prefix-list global_ipv6_in seq 20 deny FC00::/7 le 128
ipv6 prefix-list global_ipv6_in seq 20 deny FEC0::/10 le 128
ipv6 prefix-list global_ipv6_in seq 20 deny FE80::/10 le 128
ipv6 prefix-list global_ipv6_in seq 20 deny 0000::/8 le 128
ipv6 prefix-list global_ipv6_in seq 20 permit 2000::/3 le 48
ipv6 prefix-list global_ipv6_in seq 30 deny ::/0 le 128
```

Seguridad en BGP

- Aparte del filtrado ya visto existen otras medidas de seguridad:
  - Usar claves secretas compartidas en los peerings

```
neighbor <neigh-ipv6-addr> password <shared-pwd>
```

  - Controlar el TTL de los paquetes BGP [RFC5082]

```
neighbor <neigh-ipv6-addr> ttl-security hops 1
```

  - Prevenirse contra AS_PATH largos

```
bgp maxas-limit <number-of-AS-hops>
```

  - Limitar el número de prefijos recibidos

```
neighbor <neigh-ipv6-addr> maximum-prefix <num-prefs>
```

  - Prevenirse contra BGP updates con ASN privado

```
neighbor <neigh-ipv6-addr> remove-private-as
```

Gracias !!

Contacto:

- Alvaro Vives (Consulintel): alvaro.vives@consulintel.es