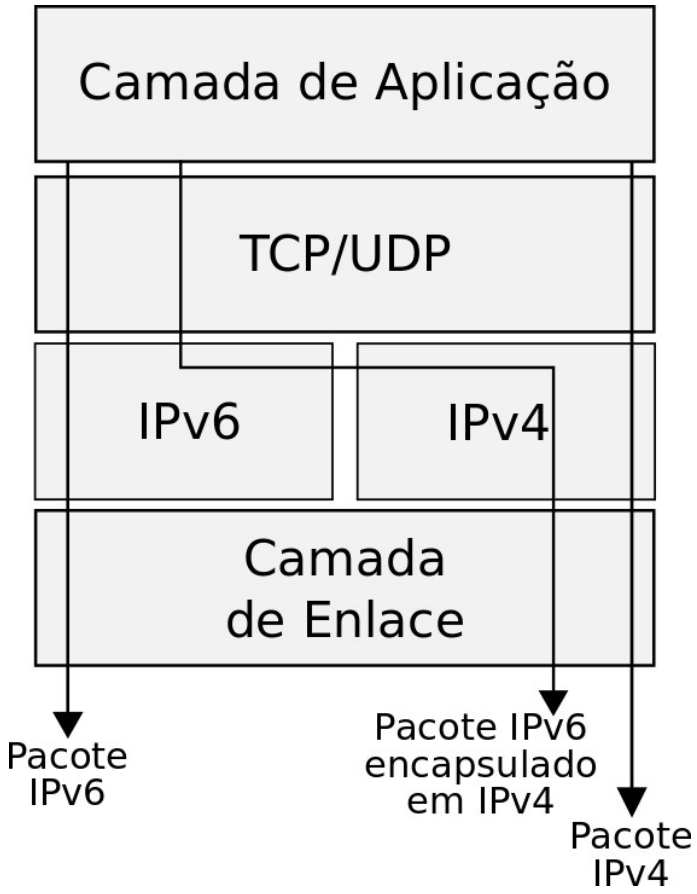
Enrutamiento IPv6

Módulo 8

Consideraciones importantes

- IPv4 e IPv6 → Capa de Red
- Dos redes diferentes
  - Planificación
  - Soporte
  - *Troubleshooting*
  - Arquitectura de los equipos
  - ...



Consideraciones importantes

Características fundamentales de las direcciones IP

- Identificación
  - Unívoca
  - Comandos: host, nslookup, dig...
- Localización
  - Enrutamiento y encaminamiento entre el origen y el destino
  - Comandos: mtr -4/-6, traceroute(6), tracert(6)...

¿Cómo funciona el router?

Ejemplo:

1. El router recibe una trama Ethernet;
2. Verifica la información del Ethertype que indica que el protocolo de capa superior transportado es IPv6;
3. Se procesa el encabezado IPv6 y se analiza la dirección de destino;
4. El router busca en la tabla de enrutamiento *unicast* (RIB - *Router Information Base*) si hay alguna entrada a la red de destino;
   - Visualización de la RIB:
     show ip(v6) route → Cisco/Quagga
     show route (table inet6) → Juniper

¿Cómo funciona el router?

5. *Longest Match* - Busca la entrada más específica. Ejemplo:

- La IP de destino es 2001:0DB8:0010:0010::0010
- El router tiene la siguiente información en su tabla de rutas:
    - 2001:DB8::/32 vía interfaz A
    - 2001:DB8::/40 vía interfaz B
    - 2001:DB8:10::/48 vía interfaz C
- Los tres prefijos engloban la dirección de destino, pero el router siempre preferirá el más específico, en este caso el /48;

6. Una vez identificado el prefijo más específico, el router decrementa el *Hop-Limit*, arma la trama Ethernet de acuerdo con la interfaz y envía el paquete.

¿Cómo funciona el router?

¿Qué pasa si hay más de un camino para el mismo prefijo?

- Se utiliza una tabla de preferencias predefinida.
  - Número entero comprendido entre 0 y 255 asociado a cada ruta; cuanto menor sea su valor más confiable será la ruta;
  - Evalúa si está conectado directamente, si la ruta fue aprendida a través del protocolo de enrutamiento externo o interno;
  - Tiene significado local, no puede ser anunciado por los protocolos de enrutamiento;
  - Su valor puede ser modificado en caso que sea necesario priorizar un determinado protocolo.

¿Qué pasa si el valor de la tabla de preferencias también es el mismo?

Tabla de Enrutamiento

- El proceso de selección de rutas es idéntico en IPv4 e IPv6, pero las tablas de rutas son independientes.
    - Hay una RIB IPv4 y otra IPv6.
- A través de mecanismos de optimización, las mejores rutas se agregan a la tabla de encaminamiento
    - FIB - *Forwarding Information Base;*
    - La FIB se crea a partir de la RIB;
    - Al igual que la RIB, la FIB también está duplicada.
- En los routers que tienen arquitectura distribuida el proceso de selección de rutas y el encaminamiento de los paquetes son funciones diferentes.

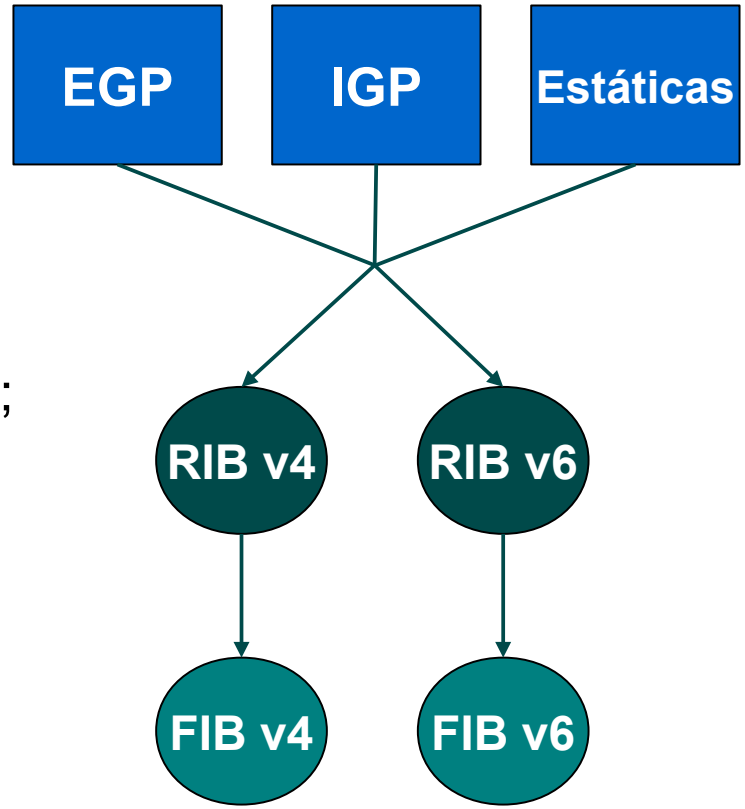
Tabla de Enrutamiento

- Son las informaciones recibidas por los protocolos de enrutamiento que "alimentan" la RIB, la cual a su vez “alimenta” la FIB.

- Los Protocolos de Enrutamiento se dividen en dos grupos:

  - **Interno (IGP)** - Protocolos que distribuyen la información de los routers dentro de Sistemas Autónomos. Ejemplo: OSPF; IS-IS; RIP.

  - **Externo (EGP)** - Protocolos que distribuyen la información entre Sistemas Autónomos. Ejemplo: BGP-4.



Ruta por defecto

- Cuando un router no encuentra una entrada en la tabla de rutas para una determinada dirección, ese router utiliza una ruta por defecto.
- Los servidores, estaciones de trabajo, *firewalls*, etc. solo conocen las redes directamente conectadas a una interfaz.
  - Para llegar a un destino que no esté directamente conectado deberán usar la ruta por defecto hacia otro que sí conozcan.
- ¿Todo el mundo necesita tener una ruta por defecto?

Ruta por defecto

- DFZ (*Default Free Zone*) - Concepto que existe entre los operadores. Es una región de Internet que no tiene ruta por defecto.
- Los routers DFZ no tienen ruta por defecto, tienen la tabla BGP completa.
- ¿Los AS que tienen la tabla completa deben tener ruta *por defecto*?
- La tabla completa muestra todas las entradas de red del mundo.
  - Los routers deben procesar información del mundo entero en tiempo real;
  - Problemas de escalabilidad futura.

Ruta por defecto

- Si hay tabla completa y ruta por defecto, ¿se utiliza la ruta por defecto?
- Ejemplo:
  - Imagine una red comprometida por un *malware*;
  - La máquina contaminada “barrerá” Internet intentando contaminar otras máquinas, incluso IPs que no están asignadas y que no están en la tabla completa;
  - Si hay ruta por defecto, su router va a encaminar ese tráfico no válido hacia adelante;
  - Este es uno de los motivos para utilizar DFZ;
  - Sugerencia: Crear una ruta por defecto y apuntar hacia Null0 o DevNull, deshabilitando el envío de mensajes '*ICMP unreachable*'.
- La ruta por defecto en IPv4 es 0.0.0.0/0 y en IPv6 ::/0.

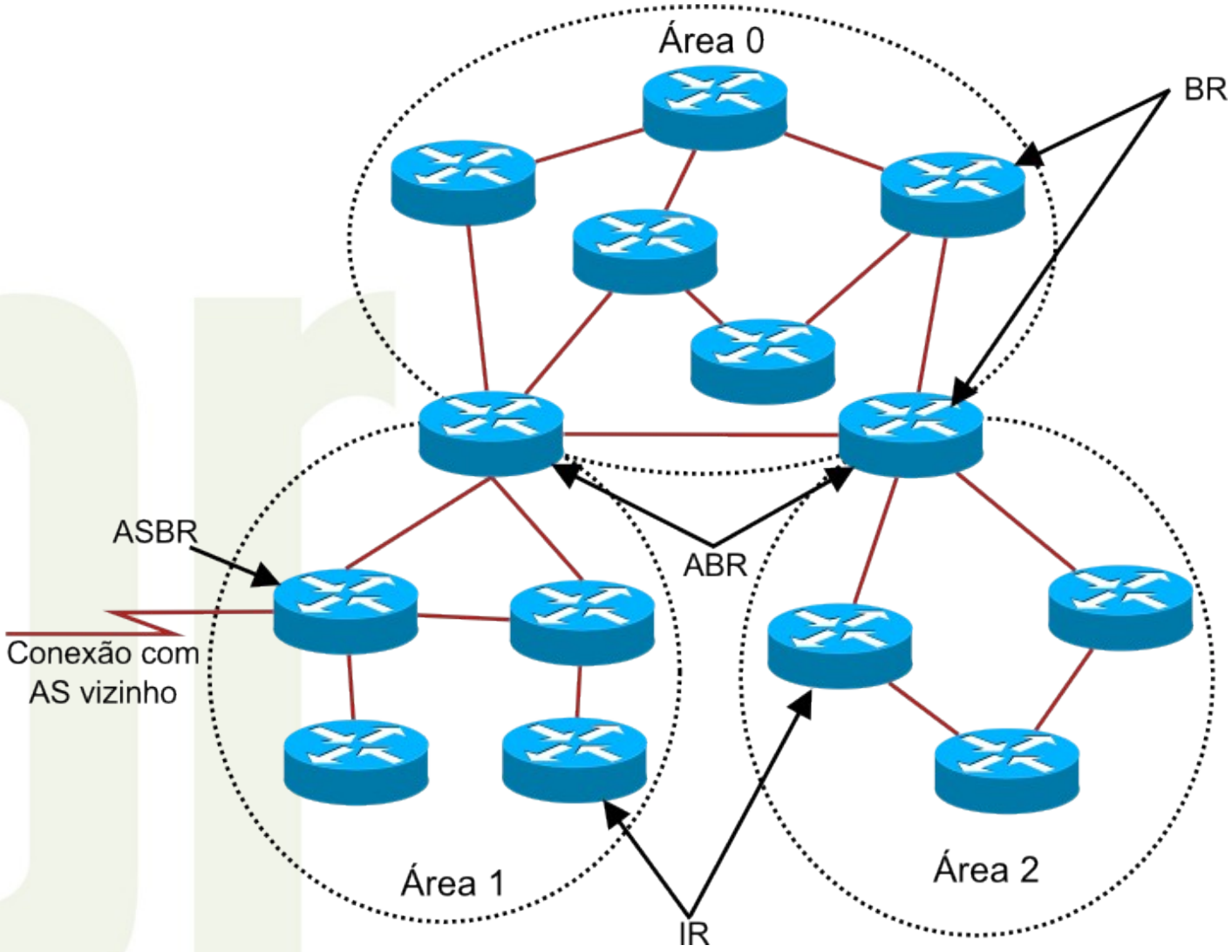
Protocolos de Enrutamiento Interno

- Hay dos opciones principales para trabajar con el enrutamiento interno:
  - OSPF
  - IS-IS
    - protocolos tipo *Link-State*;
    - consideran la información de estado y envían actualizaciones de manera optimizada;
    - trabajan con estructura jerárquica.
- Tercera opción
  - RIP
- El protocolo de enrutamiento interno solo debe ser habilitado en las interfaces necesarias.

OSPFv3

- *Open Shortest Path First version 3* (OSPFv3) – Protocolo IGP de tipo *link-state*
  - Los routers describen su estado actual a lo largo del AS enviando LSAs (*flooding*)
- Utiliza el algoritmo del camino más corto de Dijkstra
- Agrupa los routers en áreas
- Basado en el protocolo OSPFv2
- Protocolo específico para IPv6
  - En un ambiente IPv4+IPv6 es necesario utilizar OSPFv2 (IPv4) y OSPFv3 (IPv6).

Routers OSPFv3



OSPFv3

Semejanzas entre OSPFv2 y OSPFv3

- Tipos básicos de paquetes
  - Hello, DBD, LSR, LSU, LSA
- Mecanismos para descubrimiento de vecinos y formación de adyacencias
- Tipos de interfaces
  - *point-to-point*, *broadcast*, NBMA, *point-to-multipoint* y enlaces virtuales
- Lista de estados y eventos de las interfaces
- Algoritmo de selección del *Designated Router* y del *Backup Designated Router*
- Envío y edad de las LSAs
- AREA_ID y ROUTER_ID continúan siendo de 32 bits

OSPFv3

Diferencias entre OSPFv2 y OSPFv3

- OSPFv3 funciona por enlace, y no por subred
- Se eliminó la información de direccionamiento
- Se agregó limitación de alcance para *flooding*
- En OSPFv3 no es necesario crear el “routing process” explícitamente. Al habilitar OSPFv3 en una interfaz se creará el proceso.
- OSPFv3 se debe habilitar en cada interfaz y no globalmente.
- Se pueden configurar varios prefijos en una interfaz.

OSPFv3

Diferencias entre OSPFv2 y OSPFv3 (Cont.)

- Cambios en la autenticación
- Identificación de vecinos mediante Router Ids
- Soporte explícito para múltiples instancias en cada enlace
- Uso de direcciones *link-local*
- Utiliza direcciones *multicast* (*AllSPFRouters* **FF02::5** y *AllDRouters* **FF02::6**)

IS-IS

- *Intermediate System to Intermediate System* (IS-IS) - Protocolo IGP de tipo *link-state*
- Originalmente desarrollado para funcionar sobre el protocolo CLNS
  - *Integrated IS-IS* permite enrutar tanto IP como OSI
  - Utiliza NLPID para identificar el protocolo de red utilizado
- Trabaja en dos niveles
  - L2 = Backbone
  - L1 = Stub
  - L2/L1= Interconexión L2 y L1

IS-IS

- No se ha desarrollado una nueva versión para trabajar con IPv6. Solo se han agregado nuevas funcionalidades a la versión ya existente

- Dos nuevos TLVs para
  - *IPv6 Reachability*
  - *IPv6 Interface Address*

- Se crea una nueva familia de direcciones (“address family”) para soportar Ipv6.

- Nuevo identificador de capa de red
  - IPv6 NLPID

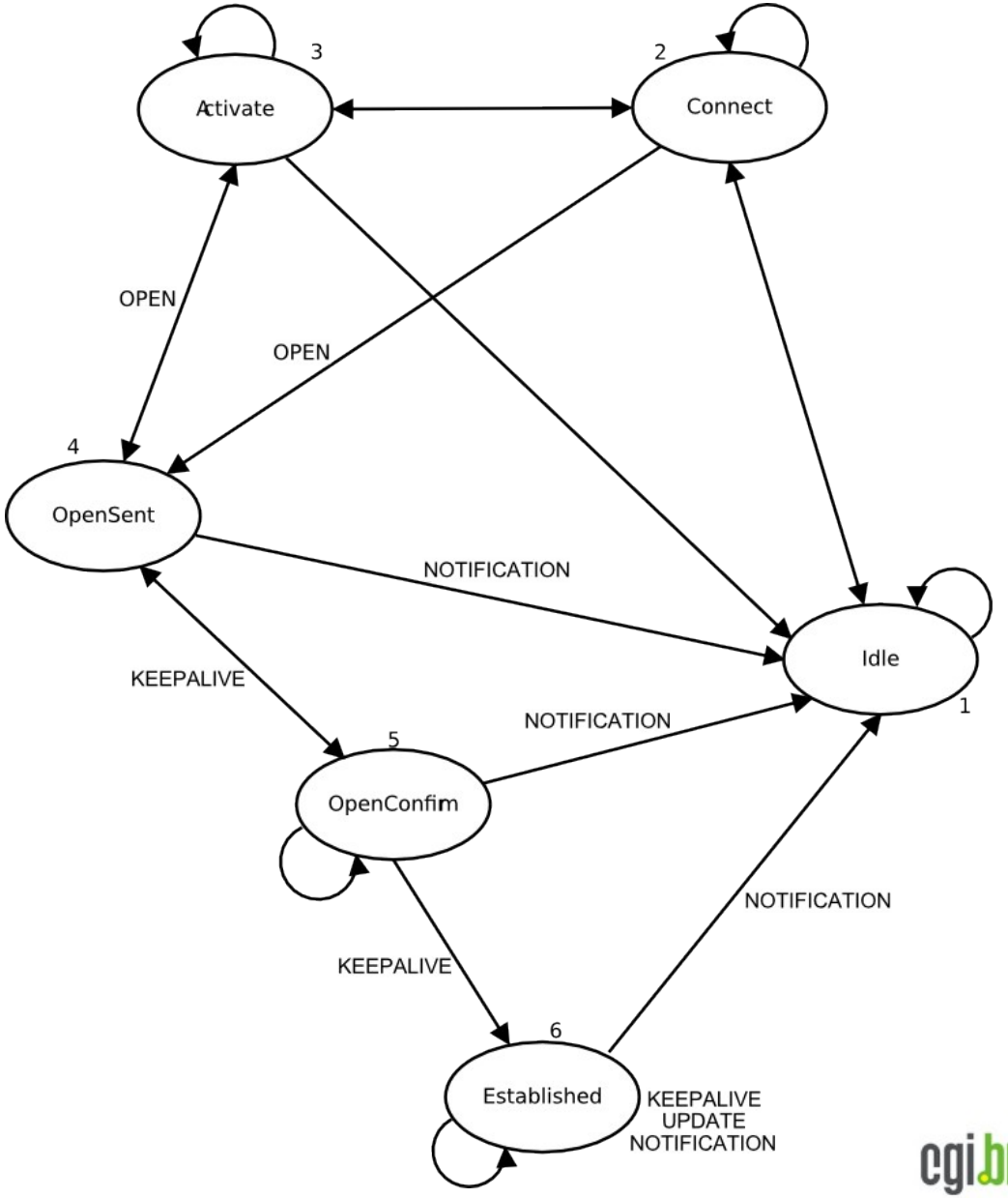
- El proceso de establecimiento de vecindades no cambia

Protocolo de Enrutamiento Externo

- En la actualidad el protocolo de enrutamiento externo por defecto es *Border Gateway Protocol* versión 4 (BGP-4).
    - protocolo de tipo *path vector.*
- Los routers BGP intercambian información de enrutamiento entre ASs vecinos.
    - con esta información diseñan un grafo de conectividad entre los AS.

BGP

- Puerto TCP 179
- Cuatro tipos de mensajes:
  - *Open*
  - *Update*
  - *Keepalive*
  - *Notification*
- Dos tipos de conexión:
  - eBGP
  - iBGP
- Funcionamiento representado por una Máquina de Estados.



Atributos BGP

- El criterio de selección entre diferentes atributos BGP varía de implementación a implementación.

- Los atributos BGP se dividen en categorías y subcategorías.

ORIGIN	Bien conocido	Obligatorio
AS_PATH	Bien conocido	Obligatorio
NEXT_HOP	Bien conocido	Obligatorio
MULTI_EXIT_DISC	Opcional	No transitivo
LOCAL_PREF	Bien conocido	Discrecional
ATOMIC_AGGREGATE	Bien conocido	Discrecional
AGGREGATOR	Opcional	Transitivo

BGP Multiprotocolo

- *Multiprotocol* BGP (MP-BGP) – Extensión de BGP para soportar múltiples protocolos de red o familias de direcciones.
    - El soporte para MP-BGP es fundamental para realizar el enrutamiento externo IPv6, ya que no existe una versión específica de BGP para esta tarea.

- Se introdujeron dos nuevos atributos:
    - *Multiprotocol Reachable NLRI* (MP_REACH_NLRI) – Transporta el conjunto de destinos alcanzables junto con la información del *next-hop;*
    - *Multiprotocol Unreachable NLRI* (MP_UNREACH_NLRI) – Transporta el conjunto de destinos inalcanzables;
    - Estos atributos son opcionales y no transitivos.

Tabla BGP

- La información sobre las rutas de Internet se encuentra en la tabla BGP.
- En los routers de borde esta información se replica hacia la RIB y la FIB, IPv4 e IPv6.
    - Tabla Global IPv4 → ~300.000 entradas
    - Tabla Global IPv6 → ~2.500 entradas
- La duplicidad de esta información implica más espacio, más memoria y más procesamiento.
    - Agregación de rutas
    - Evitar el anuncio innecesario de rutas
    - Limitar el número de rutas recibidas de otros AS
        - Importante en IPv4
        - Fundamental en IPv6

Establecimiento de sesiones BGP

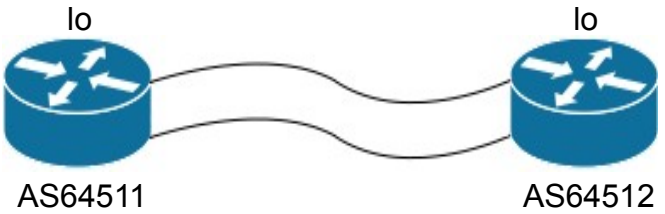
- Una sesión BGP se establece entre dos routers en base a una conexión TCP.
  - puerto TCP 179;
  - conexión IPv4 o IPv6.
- Interfaz *loopback*
  - interfaz lógica;
  - no “caen”.

Establecimiento de sesiones BGP

iBGP entre *loopbacks*

- Es fundamental establecer sesiones iBGP utilizando la interfaz *loopback*.
  - a través de la IP de la interfaz real:
    - si el *link* se interrumpe, la sesión también se interrumpirá.
  - por medio de la IP de la interfaz *loopback*:
    - más estabilidad;
    - las IP de las interfaces *loopback* serán aprendidas a través del protocolo IGP.
    - si el *link* se interrumpe, la sesión puede ser establecida por otro camino.

Establecimiento de sesiones BGP



eBGP entre *loopbacks*

- Balanceo
  - Por ejemplo:
    - Hay dos routers y cada router representa un AS:
    - Ambos están conectados mediante dos *links;*
    - Utilizando la IP de las interfaces reales:
      - Se necesitarán dos sesiones BGP;
      - Eventualmente con políticas diferentes.
    - Utilizando la IP de las interfaces *loopback*
      - Se establece una única sesión BGP;
      - Se crea una ruta estática para la IP de la interfaz *loopback* del vecino a través de cada *link.*

Establecimiento de sesiones BGP

eBGP entre *loopbacks*

- Seguridad
  - La utilización de interfaces *loopbacks* en sesiones eBGP no es necesaria solo para asegurar el balanceo.
  - Establecer sesiones eBGP utilizando la IP de la interfaz facilita mucho los ataques contra la infraestructura.
  - Es recomendable establecer eBGP entre *loopbacks* aunque haya un único *enlace*.

Decisiones de enrutamiento

- Los routers toman decisiones de acuerdo con la información que conocen.
- Esta información es recibida y enviada a otros routers a través de los protocolos de enrutamiento interno y externo.
  - Los routers solo anuncian la mejor ruta que conocen para un determinado destino.
- Esta información se utiliza para influenciar el tráfico de entrada y de salida del AS.

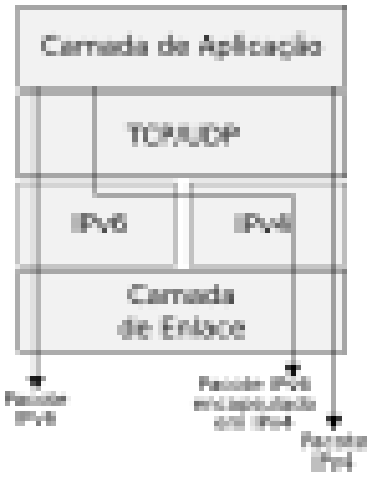
En este módulo presentaremos algunas características básicas sobre el funcionamiento de los mecanismos de enrutamiento, tanto interno (IGP) como externo (EGP), siempre destacando los principales cambios en relación con IPv6. Hablaremos sobre los protocolos de enrutamiento RIP, OSPF, IS-IS y BGP.

nic.br Núcleo de Información e Coordenação do Ponto BR

ceptro.br IPv6.br

Consideraciones importantes

- IPv4 e IPv6 → Capa de Red
- Dos redes diferentes
  - Planificación
  - Soporte
  - *Troubleshooting*
  - Arquitectura de los equipos
  - ...

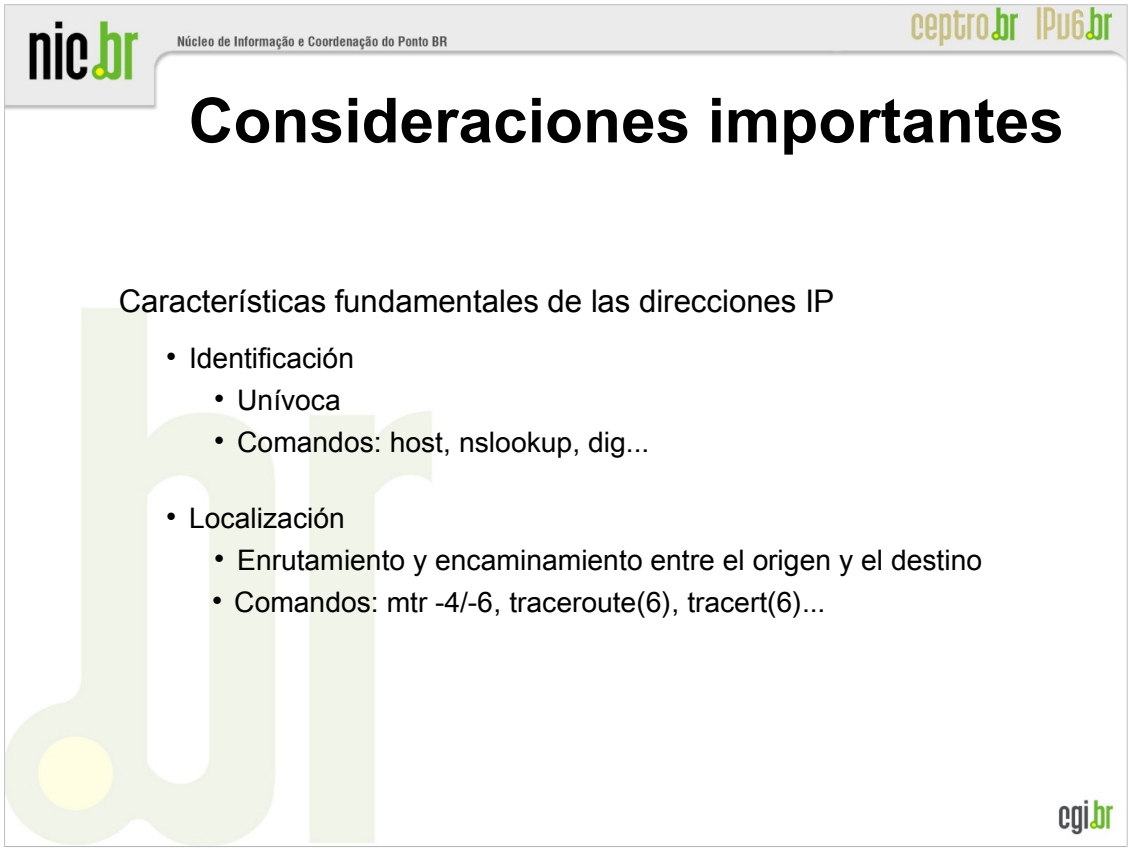


egi.br

IPv4 e IPv6 son protocolos de Capa de Red, de manera que ésta es la única capa directamente afectada por la implementación de IPv6, sin necesidad de modificar el funcionamiento de las demás.

Sin embargo, es necesario comprender que se trata de dos Capas de Red distintas e independientes. Esto implica algunas consideraciones importantes:

- Cómo actuar en la planificación y estructuración del as redes:
  - Migrar toda la estructura a doble pila; migrar solo las áreas críticas; mantener dos estructuras diferentes, una IPv4 y otra IPv6; etc.
  - En las redes con doble pila algunas configuraciones deben ser duplicadas, como por ejemplo la del DNS, *el firewall* y los protocolos de enrutamiento.
- Para el soporte y resolución de problemas será necesario si las fallas se encuentran en la conexión de la red IPv4 o de la red IPv6;
- Los nuevos equipos y aplicaciones deben soportar las funcionalidades de los dos protocolos.

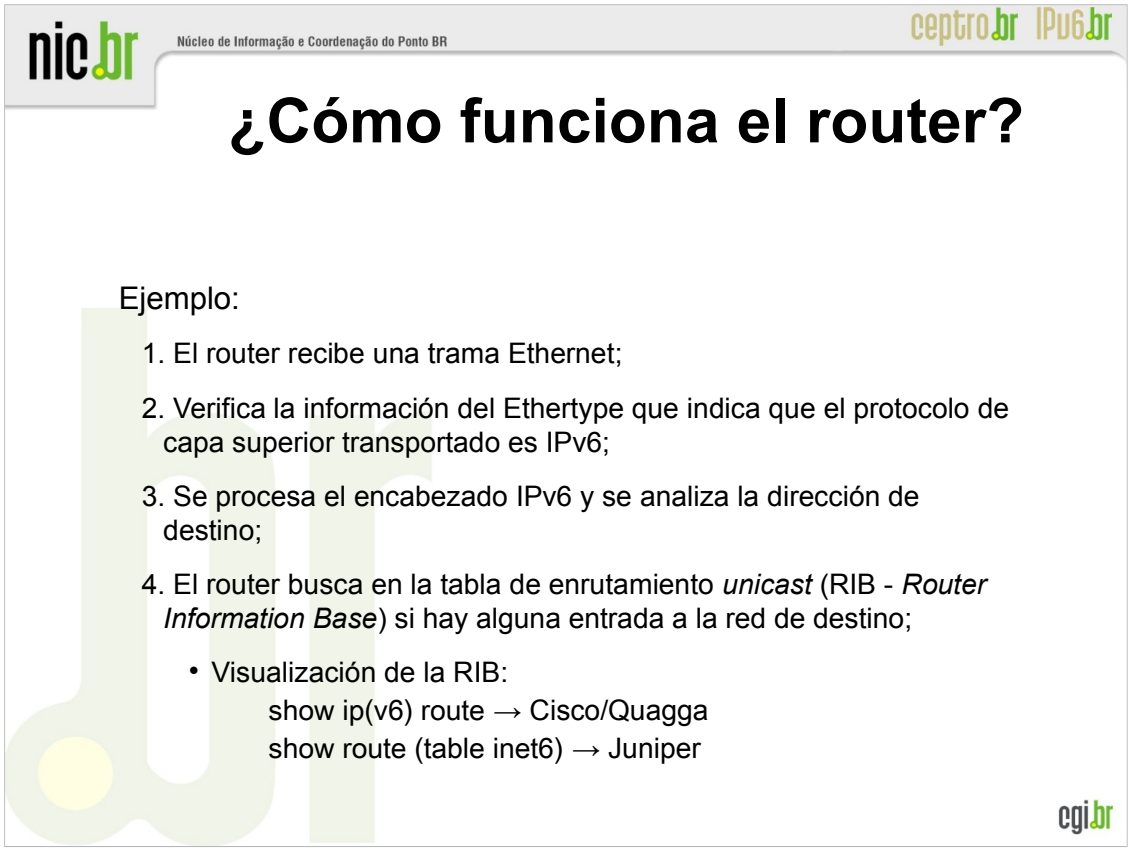


La Capa de Red está asociada principalmente a dos características:

- **Identificación** – Debe garantizar que cada dispositivo de la red sea identificado de manera unívoca, sin posibilidad de error. En otras palabras, la dirección IP debe ser única en a nivel mundial. Utilizando el comando host en las plataformas UNIX, o nslookup en las plataformas Windows, se puede verificar la identificación de un servicio, por ejemplo. En las redes con doble pila los nodos se identifican por las dos direcciones.

- **Localización** – Indica cómo llegar al destino, decidiendo el encaminamiento de los paquetes en base al direccionamiento; ocurre de la misma manera tanto en IPv4 como en IPv6. Podemos verificar esta funcionalidad utilizando comandos como *mtr -4* y *-6*, o *traceroute (traceroute6)*, o *tracert (tracert6)*. Estos comandos muestran la identificación y la localización de un nodo.

La unión de estas dos características en la Capa de Red resulta en una semántica sobrecargada. Esto se evidencia en aspectos tales como la agregación de rutas, agravando el problema del crecimiento de la tabla de enrutamiento global. Una forma de impedir esto consiste en separar las funciones de localización e identificación.



También es importante comprender el funcionamiento básico de un router y de qué manera procesa los paquetes recibidos y toma las decisiones de encaminamiento. Consideremos el siguiente ejemplo:

- El router recibe una trama Ethernet a través de su interfaz de red;
- Verifica la información del Ethertype que indica que el protocolo de capa superior transportado es IPv6;
- Se procesa el encabezado IPv6 y se analiza la dirección de destino;
- El router busca en la tabla de enrutamiento *unicast* (RIB - *Router Information Base*) si hay alguna entrada a la red de destino;
-

  Visualización de la RIB IPv6:

  Cisco/Quagga → show ipv6 route
  Juniper → show route table inet6

  Visualización de la RIB IPv4:

  Cisco/Quagga → show ip route
  Juniper → show route

nic.br Núcleo de Información e Coordenação do Ponto BR ceptro.br IPv6.br

¿Cómo funciona el router?

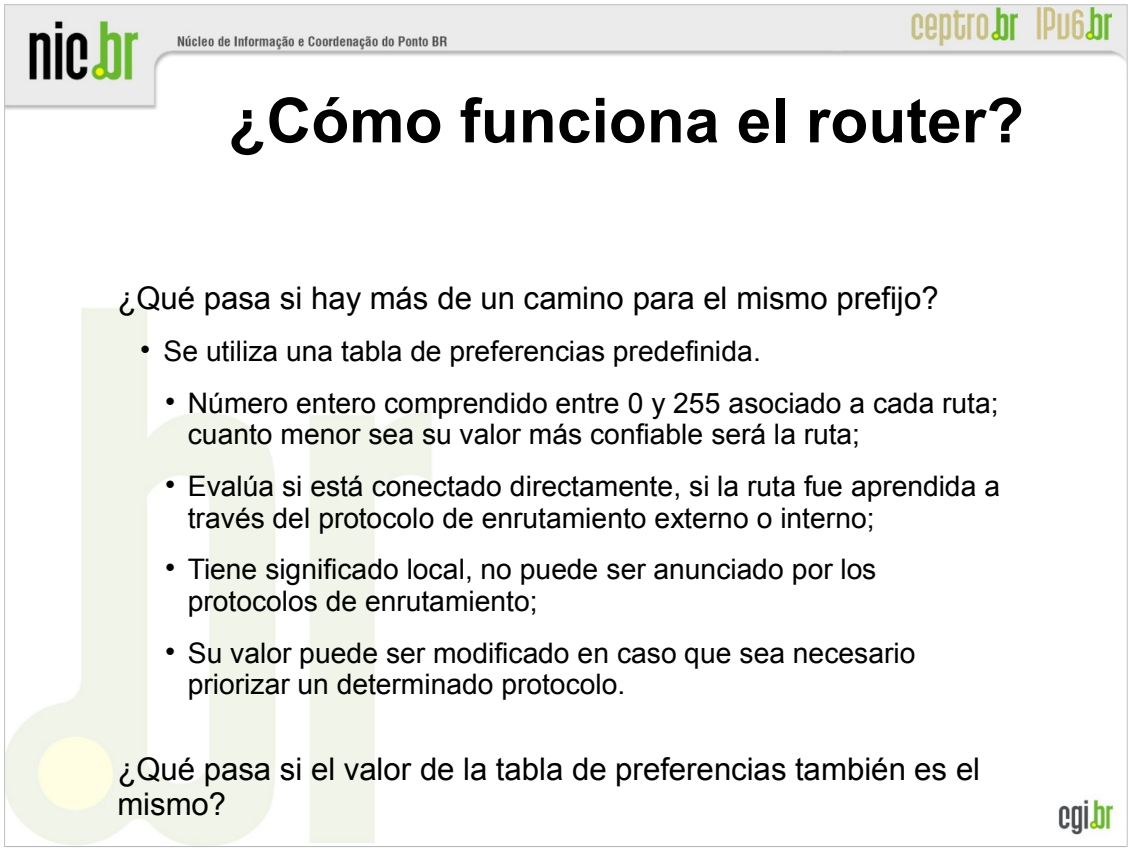
5. *Longest Match* - Busca la entrada más específica. Ejemplo:

- La IP de destino es 2001:0DB8:0010:0010::0010
- El router tiene la siguiente información en su tabla de rutas:
  - 2001:DB8::/32 vía interfaz A
  - 2001:DB8::/40 vía interfaz B
  - 2001:DB8:10::/48 vía interfaz C
- Los tres prefijos engloban la dirección de destino, pero el router siempre preferirá el más específico, en este caso el /48;

6. Una vez identificado el prefijo más específico, el router decrementa el *Hop-Limit*, arma la trama Ethernet de acuerdo con la interfaz y envía el paquete.

cgi.br

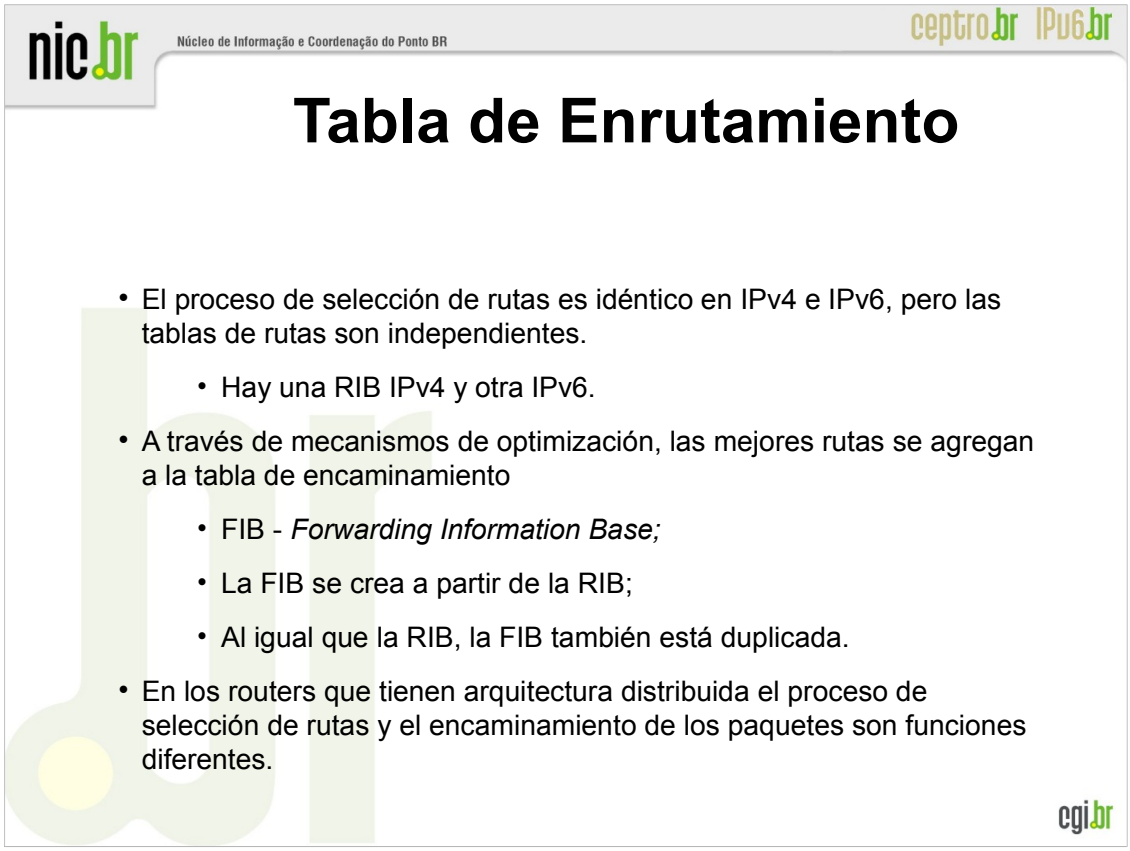
- *Longest Match* - Busca la entrada más específica. Ejemplo:
  - La IP de destino es 2001:0DB8:0010:0010::0010
  - El router tiene la siguiente información en su tabla de rutas:
  - 2001:DB8::/32 vía interfaz A
  - 2001:DB8::/40 vía interfaz B
  - 2001:DB8:10::/48 vía interfaz C
- Los tres prefijos engloban la dirección de destino, pero el router siempre preferirá el más específico, en este caso el /48;
- Una vez identificado el prefijo más específico, el router decrementa el *Hop-Limit*, arma la trama Ethernet de acuerdo con la interfaz y envía el paquete.



Si el router encuentra más de un camino para el mismo destino con el mismo valor de *longest match*, éste una tabla de preferencias predefinida (concepto de *Distancia Administrativa* de Cisco).

Los valores de esta tabla son números enteros comprendidos entre 0 y 255 asociados a cada ruta; cuanto menor es su valor más confiable es la ruta; Los valores se asignan evaluando si la ruta está conectada directamente, si fue aprendida a través del protocolo de enrutamiento externo o interno, etc. Estos valores solo tienen significado local, no pueden ser anunciados por los protocolos de enrutamiento y, si fuera necesario, pueden ser modificados para priorizar un determinado protocolo.

En caso que en la tabla de preferencias también se encuentre el mismo valor, hay equipos e implementaciones que por defecto realizan el balanceo de carga.



El proceso de selección de rutas es idéntico en IPv4 e IPv6, pero las tablas de rutas son independientes. Por ejemplo: Hay una RIB IPv4 y otra IPv6.

Para optimizar el envío de paquetes hay mecanismos que agregan solo las mejoras rutas a otra tabla, la tabla de encaminamiento (FIB - *Forwarding Information Base*). Un ejemplo de este mecanismo es el CEF (*Cisco Express Forwarding*) de Cisco.

La FIB se crea a partir de la RIB y, al igual que la RIB, también está duplicada si la red está configurada con doble pila. Es así que hay más información para almacenar y procesar.

En los routers que tienen arquitectura distribuida el proceso de selección de rutas y el encaminamiento de los paquetes son funciones diferentes.

Ejemplo:

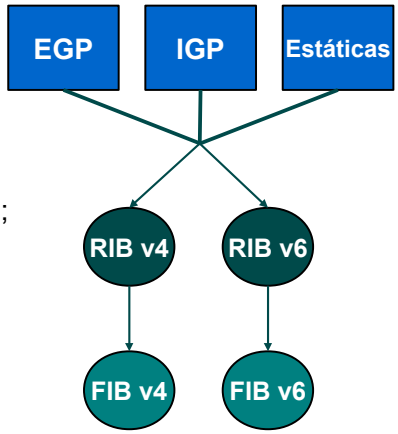
- Routers 7600 de Cisco: La RIB reside en el módulo de enrutamiento central y la FIB en las placas de las interfaces.
- Routers Juniper de la serie M: El *Router Engine* es responsable por la RIB, mientras que la FIB también reside en las placas de las interfaces (*Packet Forwarding Engine* - PFE).

nic.br Núcleo de Información e Coordenação do Ponto BR

ceptro.br IPv6.br

Tabla de Enrutamiento

- Son las informaciones recibidas por los protocolos de enrutamiento que "alimentan" la RIB, la cual a su vez “alimenta” la FIB.
- Los Protocolos de Enrutamiento se dividen en dos grupos:
  - **Interno (IGP)** - Protocolos que distribuyen la información de los routers dentro de Sistemas Autónomos. Ejemplo: OSPF; IS-IS; RIP.
  - **Externo (EGP)** - Protocolos que distribuyen la información entre Sistemas Autónomos. Ejemplo: BGP-4.



cgi.br

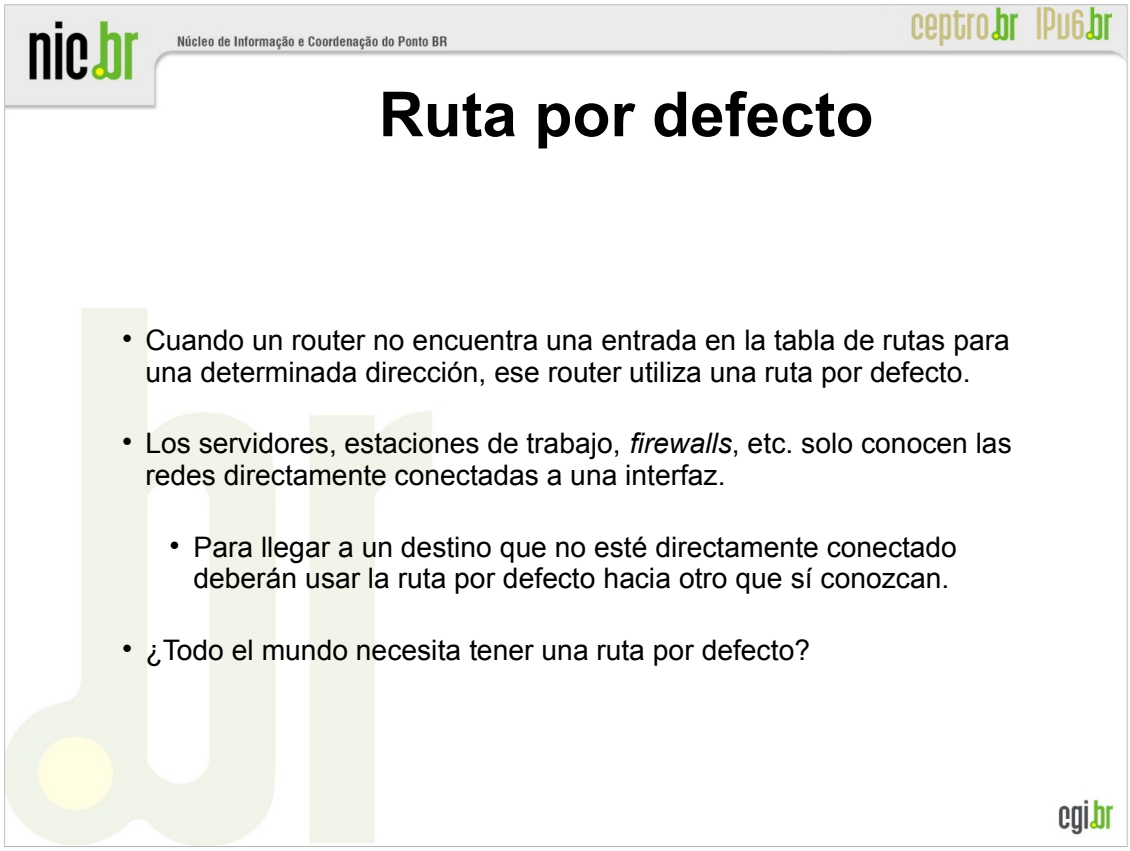
Es el mecanismo de enrutamiento que permite el encaminamiento de paquetes de datos entre dos dispositivos cualquiera conectados a Internet.

Para actualizar la información que utilizan los routers para encontrar el mejor camino disponible en el encaminamiento de los paquetes hasta su destino se utilizan los protocolos de enrutamiento. Son las informaciones recibidas por los protocolos de enrutamiento que "alimentan" la RIB, la cual a su vez "alimenta la FIB.

Estos protocolos se dividen en dos grupos:

Interno (IGP) - Protocolos que distribuyen la información de los routers dentro de Sistemas Autónomos. Como ejemplo de estos protocolos podemos mencionar: OSPF, IS-IS y RIP.

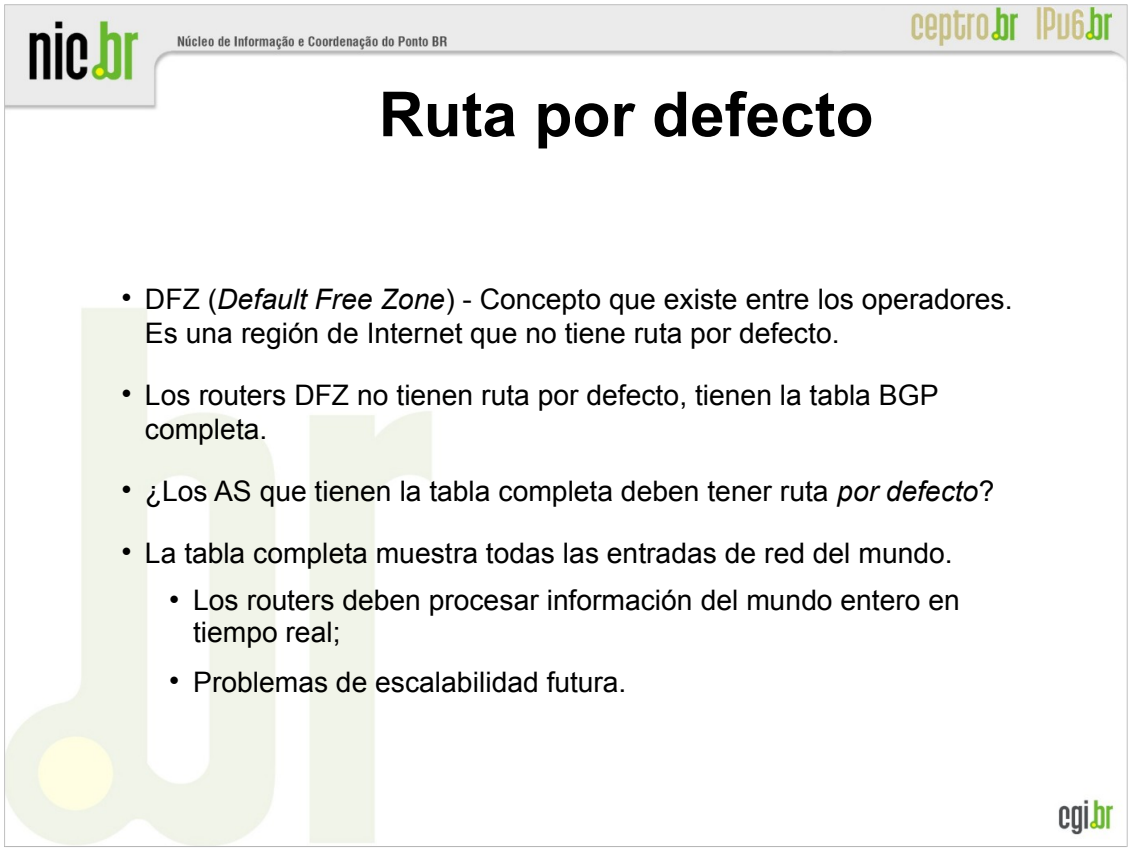
- **Externo (EGP)** - Protocolos que distribuyen la información entre Sistemas Autónomos. Como ejemplo podemos mencionar el protocolo BGP-4.



Si el router recibe un paquete cuya dirección de destino no esté explícitamente listada en la tabla de rutas, éste utilizará su ruta *por defecto.*

*Naturalmente, los s*ervidores y estaciones de trabajo necesitan una ruta *por defecto*. Estos dispositivos no son equipos de red; solo conocen las redes directamente conectadas a sus interfaces. Para llegar a un destino que no esté directamente conectado deberán usar la ruta por defecto hacia otro que sí conozcan.

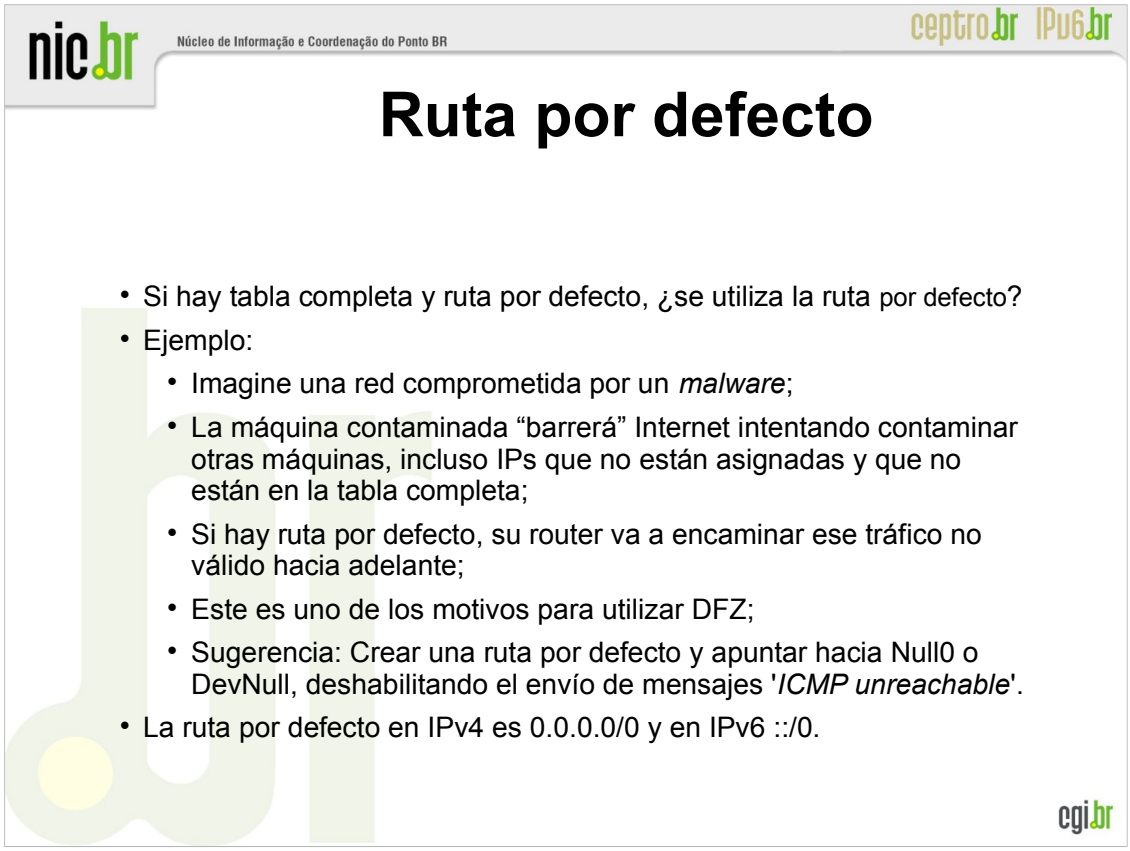
Aquí surge la siguiente pregunta: ¿Todo el mundo necesita tener una ruta por defecto?



Entre los operadores existe un concepto que delimita una región de Internet sin ruta por defecto, la DFZ (*Default Free Zone*).

Un AS que tiene la tabla completa no necesita tener ruta por defecto, ya que la tabla completa muestra las entradas d red de todo el mundo.

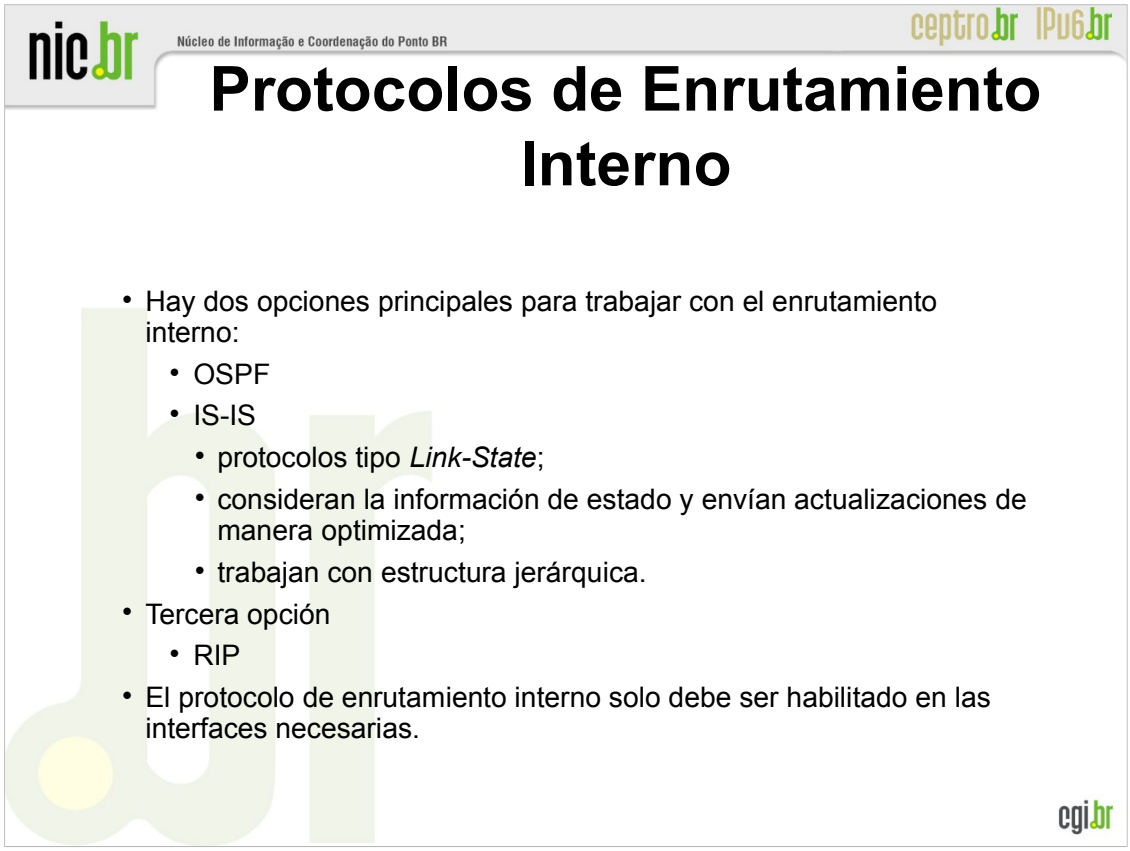
Este modelo es bueno y funcional, pero puede acarrear algunos problemas. Los routers deben procesar información del mundo entero en tiempo real; también pueden surgir problemas de escalabilidad futura.



El uso de ruta por defecto por parte de los routers que tienen tabla completa puede ocasionar algunos problemas.

Como ejemplo, imagina la siguiente situación: una red ha sido comprometida por un malware. La máquina contaminada “barrerá” Internet intentando contaminar otras máquinas, incluso IPs que no están asignadas y que no están en la tabla completa; Si hay ruta por defecto, su router va a encaminar ese tráfico no válido hacia adelante; Este es uno de los motivos para utilizar DFZ. Una sugerencia para solucionar este problema es crear una ruta por defecto y apuntar hacia Null0 o DevNull. También hay que deshabilitar el envío de mensajes 'ICMP unreachable': ya que cuando un router descarta un paquete envía un mensaje 'ICMP unreachable' pero si el destino no es válido no es necesario avisar al origen, esto solo consumirá CPU innecesariamente.

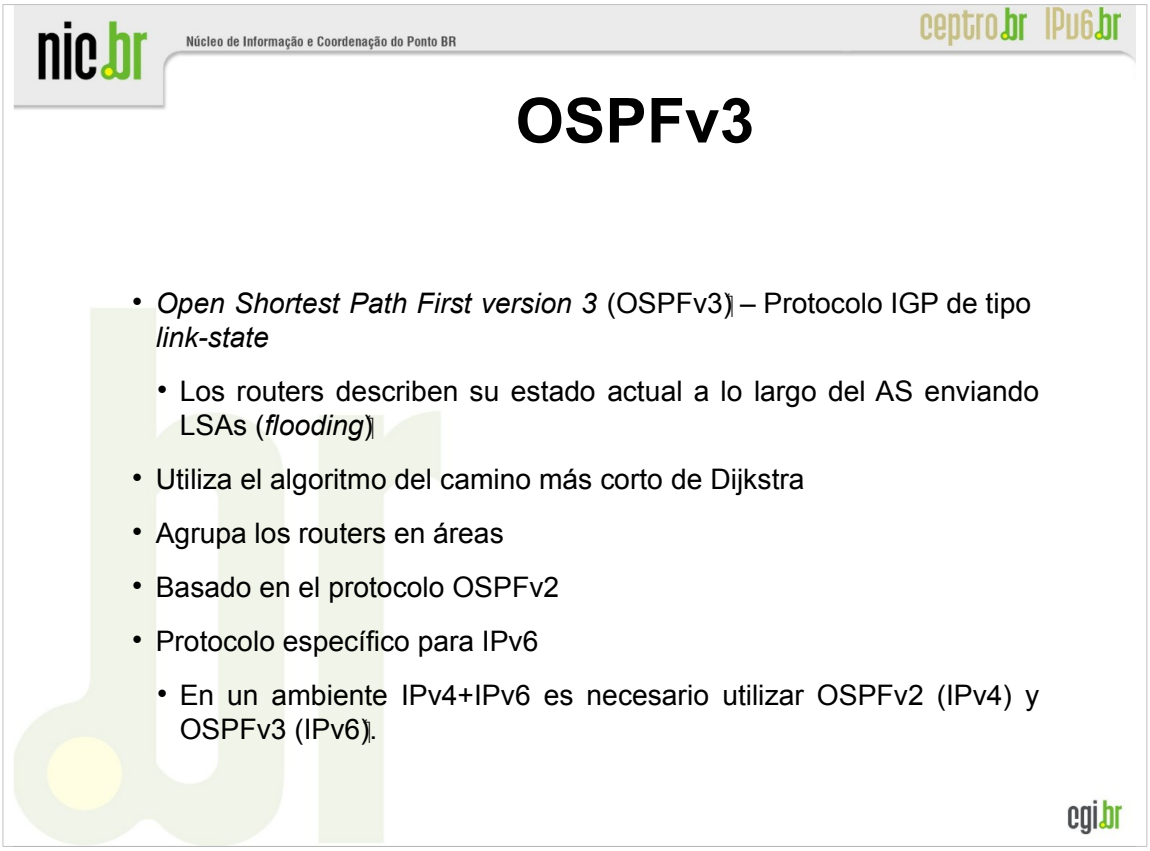
La ruta por defecto en IPv4 es 0.0.0.0/0 y en IPv6 ::/0.



Hoy en día hay dos opciones principales para trabajar con enrutamiento interno, OSPF e IS-IS. Estos dos protocolos son de tipo *Link-State*, es decir, consideran la información de estado del enlace y envían actualizaciones en forma optimizada solo cuando se producen cambios de estado. También permiten trabajar con estructura jerárquica, separando la red por regiones. Esto es un punto fundamental para IPv6.

Otra opción es el protocolo RIP (*Routing Information Protocol*). Éste es un protocolo de tipo Vector de Distancia (Bellman-Ford), de fácil implementación y de funcionamiento sencillo, pero presenta algunas limitaciones como el hecho de enviar su tabla de estados periódicamente sin importar si hay o no cambios en la red.

Es importante que el protocolo de enrutamiento interno se habilite solamente en las interfaces donde sea necesario. Aunque parezca obvio, hay quienes lo configuran equivocadamente haciendo que los routers queden intentando establecer relaciones de vecindad con otros AS.

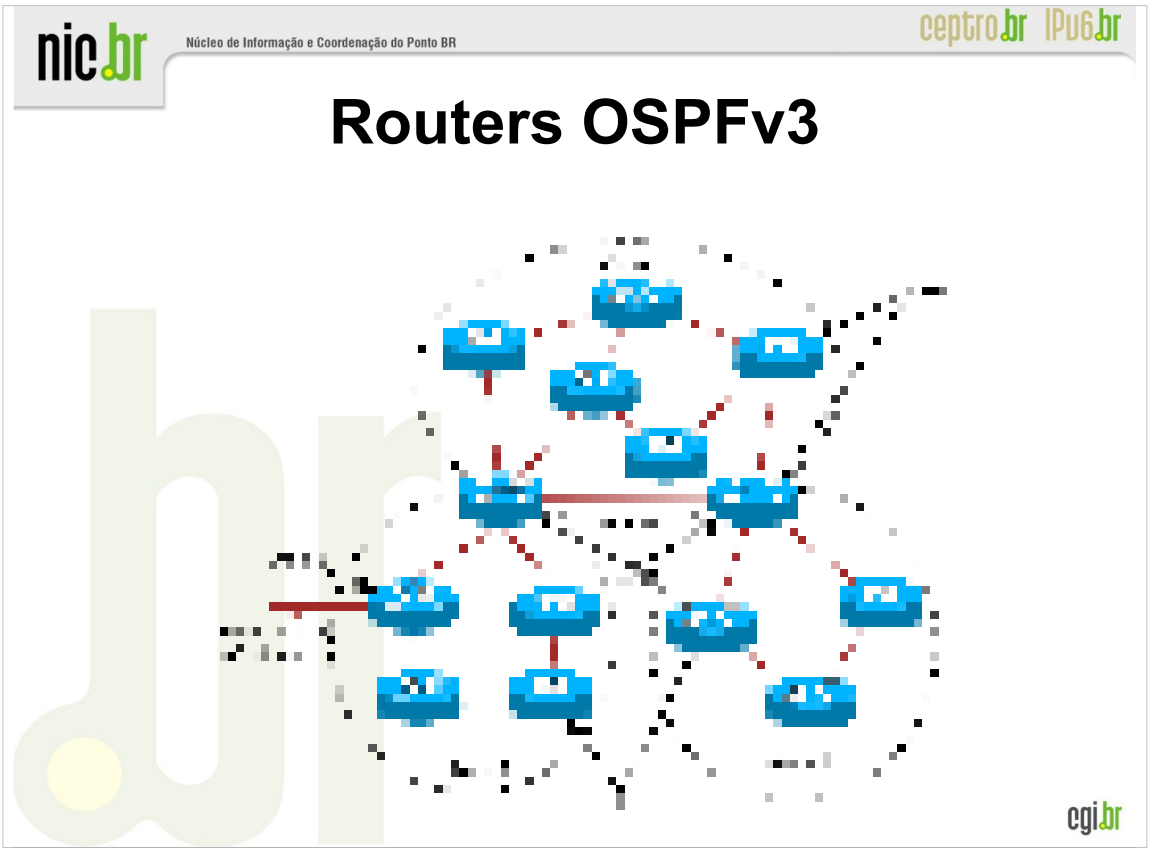


OSPF es un protocolo de tipo *link-state* donde, a través del proceso de *flooding* (inundación), los routers envían *Link State Advertisements* (LSA) describiendo su estado actual a lo largo del AS. El *flooding* consiste en el envío de un LSA por todas las interfaces de salida del router, de modo que todos los routers que reciben un LSA también lo envían por todas sus interfaces. De este modo, el conjunto de los LSAs de todos los routers forma una base de datos del estado del enlace, donde cada router que participa del AS tiene una base de datos idéntica. Con la información de esta basede datos, el router, a través del protocolo OSPF, construye un mapa de la red que será utilizado para determinar un árbol de caminos más cortos dentro de toda la subred, teniendo al propio nodo como raíz. Utiliza el algoritmo de Dijkstra para escoger el mejor camino y permite agrupar los routers en áreas.

OSPF se puede configurar para trabajar de forma jerárquica, dividiendo los routers de un AS en diferentes áreas. A cada una de estas áreas se atribuye un identificador único (Area-ID) de 32 bits y todos los routers de una misma área mantienen base de datos de estado separada, de modo que la topología de una área se desconoce fuera de la misma, reduciendo así la cantidad de trafico de enrutamiento entre las partes del AS. El área *backbone* es la responsable de distribuir la información de enrutamiento entre las áreas *nonbackbone* y se iidentifica mediante el ID 0 (o 0.0.0.0). En los AS en los cuales no hay esta división, generalmente el área *backbone* es la única que se configura.

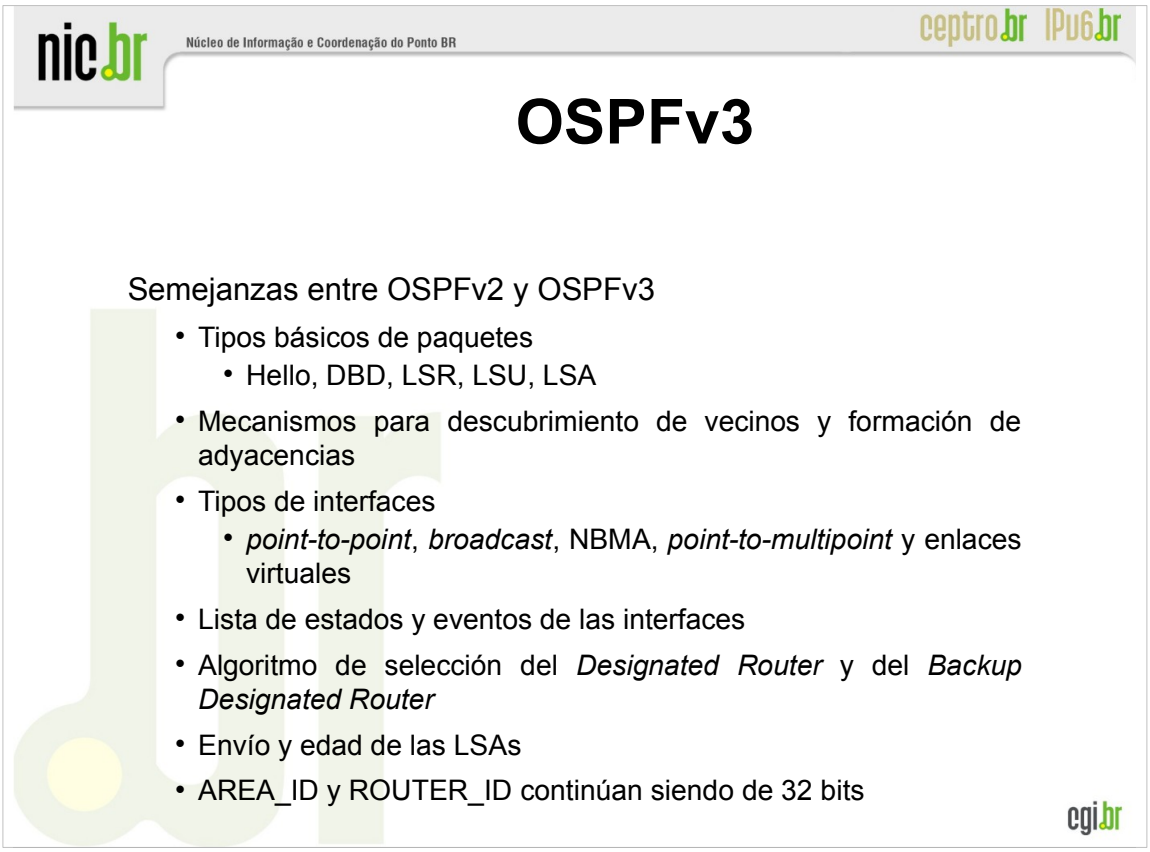
A pesar de que está basado en la versión de OSPFv2 que se utiliza en las redes IPv4, OSPFv3 es un protocolo específico para IPv6. Por lo tanto, en las redes con doble pila es necesario utilizar OSPFv2 para realizar el enrutamiento IPv4 y OSPFv3 para realizar el enrutamiento IPv6.

Más información:
- RFC 5340 - *OSPF for IPv6*



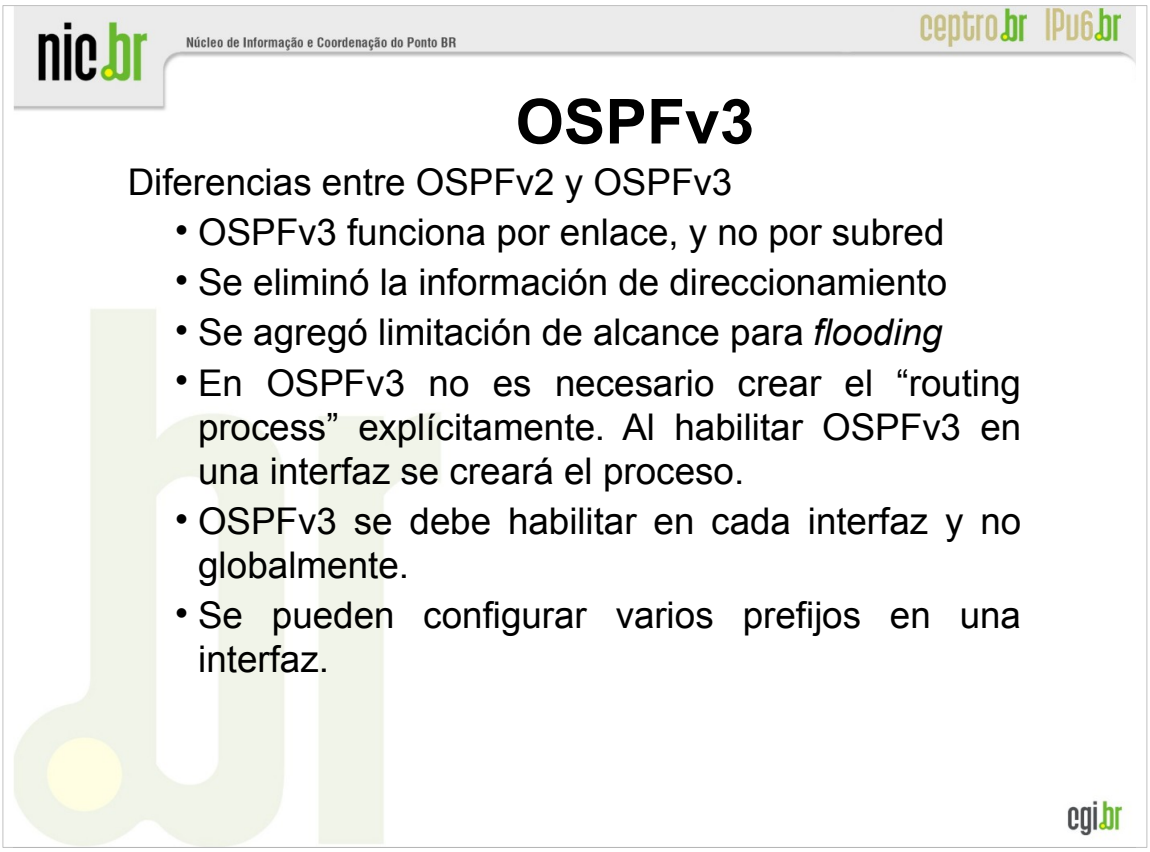
Los routers OSPF se pueden clasificar de la siguiente manera:

- *Internal Router* (IR) – Routers que solo se relacionan con vecinos OSPF de una misma área;
- *Area Border Router* (ABR) – Routers que conectan una o más áreas al *backbone*. Estos poseen múltiples copias de las bases de datos de estado, una para cada área, y son responsables por condensar la información de estas áreas y enviarla al *backbone*;
- *Backbone Router* (BR) – Routers que pertenecen al área *backbone*. Un ABR es siempre un BR, ya que todas sus áreas están directamente conectadas al *backbone* o conectadas vía *virtual link* - túnel que conecta una área al *backbone* pasando a través de otra área; y
- *Autonomous System Border Router* (ASBR) – Routers que intercambian información de enrutamiento con routers de otro AS y distribuyen las rutas recibidas dentro su propio AS.



OSPFv3 todavía incluye algunas características de OSPFv2:

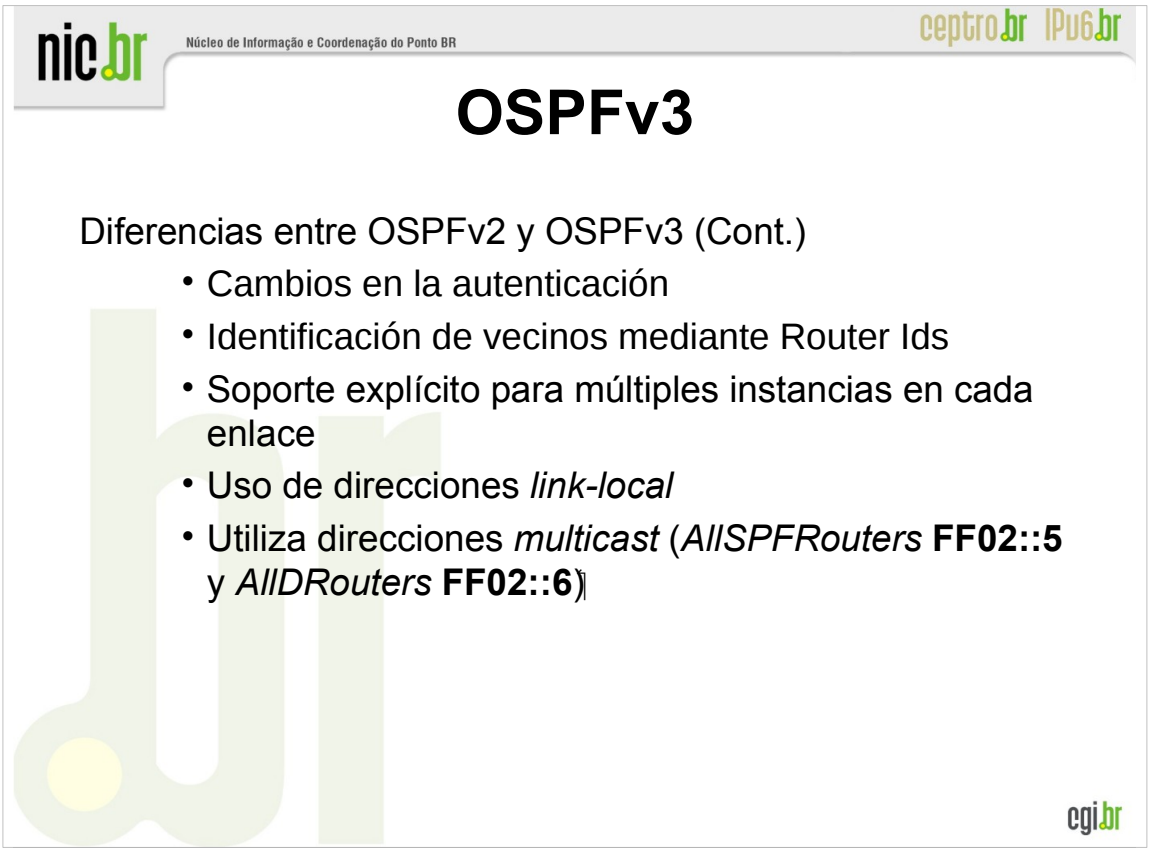
- Tipos básicos de paquetes
  - Hello, DBD (Database descriptor), LSR (Link state request), LSU (Link state update), LSA (Link state advertisement)
- Mecanismos para descubrimiento de vecinos y formación de adyacencias
- Tipos de interfaces
  - *point-to-point*, *broadcast*, NBMA (Non-broadcast multiple access), *point-to-multipoint* y enlaces virtuales
- Lista de estados y eventos de las interfaces
- Algoritmo de selección del *Designated Router* y del *Backup Designated Router*
- Envío y edad de las LSAs
- AREA_ID y ROUTER_ID continúan siendo de 32 bits



1. Protocol processing per-link, not per-subnet:
IPv6 uses the term "link" instead of "subnet" or "network" to define a medium used to communicate between nodes at the link layer. Multiple IP subnets can be assigned to a single link, and two nodes can communicate with each other even if they do not share a common IP subnet.

2. Removal of addressing semantics:
IPv6 addresses are not present in OSPF packets, except in Link-State Update (LSU) packets.
Router and Network LSAs do not contain network addresses, but only contains topology information.
OSPF Router ID, Area ID and Link-State IDs remain at 32-bits size- they cannot be assigned IPv6 addresses.
Neighboring routers are identified by Router IDs only.

3. Addition of Flooding scope:
There are three seperate scopes for flooding LSAs:
Link-local scope- LSA is flooded only on local link and no further.
Area scope- LSA is flooded in a single OSPF area.
AS scope- LSA is flooded throughout the routing domain.

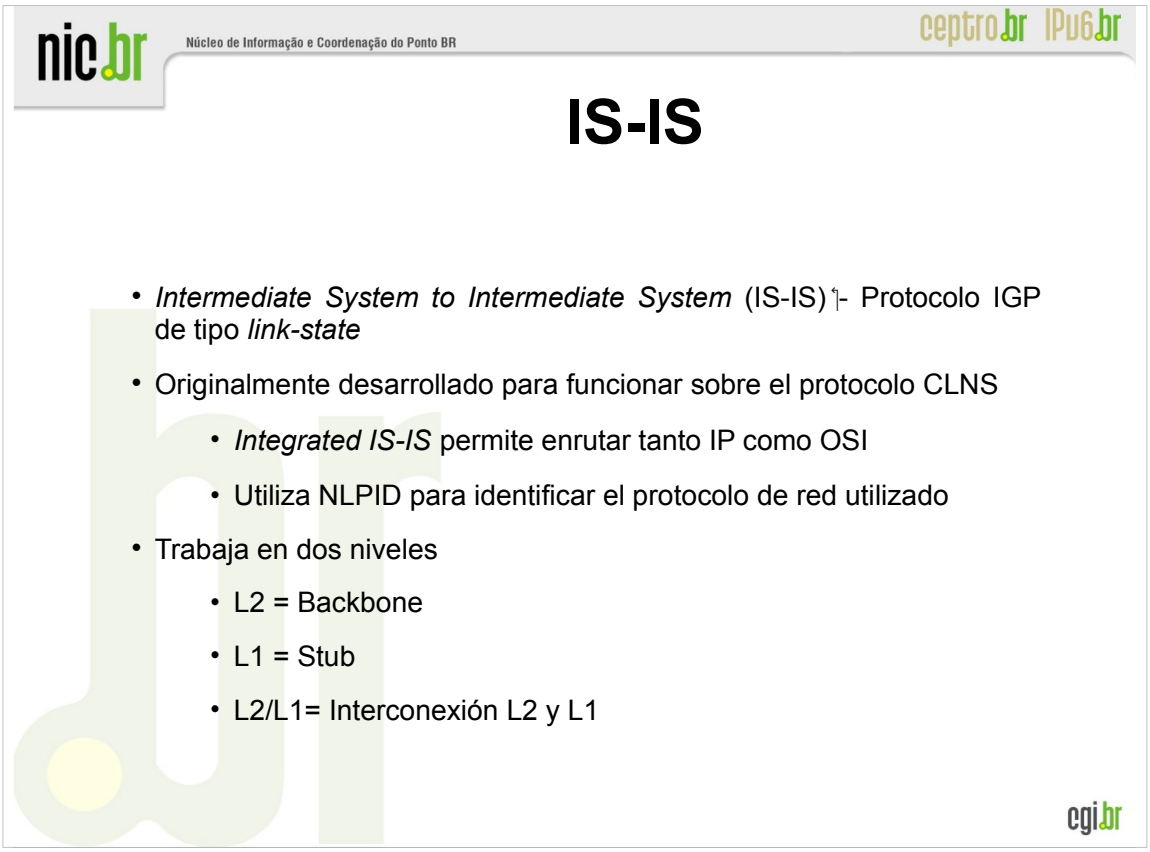


Authentication changes:
In OSPFv3, Authentication for OSPF has been removed. OSPFv3 relies on IPv6 Authentication Header (AH) and Encapsulating Security Payload (ESP) to ensure integrity and authentication/confidentiality of routing exchanges.

Identifying neighbors by Router ID:
Neighboring routers on a given link are always identified by a Router ID. This behaviour is valid for neighbors on point-to-point, virtual-links, broadcast, NBMA and point-to-multipoint links.

Explicit support for multiple instances per link:
Providers may run different OSPF domains and would like to keep it seperate even though if they have one or more links in common, can use multiple instances on the same link.
If someone wants a single link in more than one area can use multiple instances on the same link.
Multiple instances on the single link can be achieved using "Instance ID" contained in the OSPF packet header.

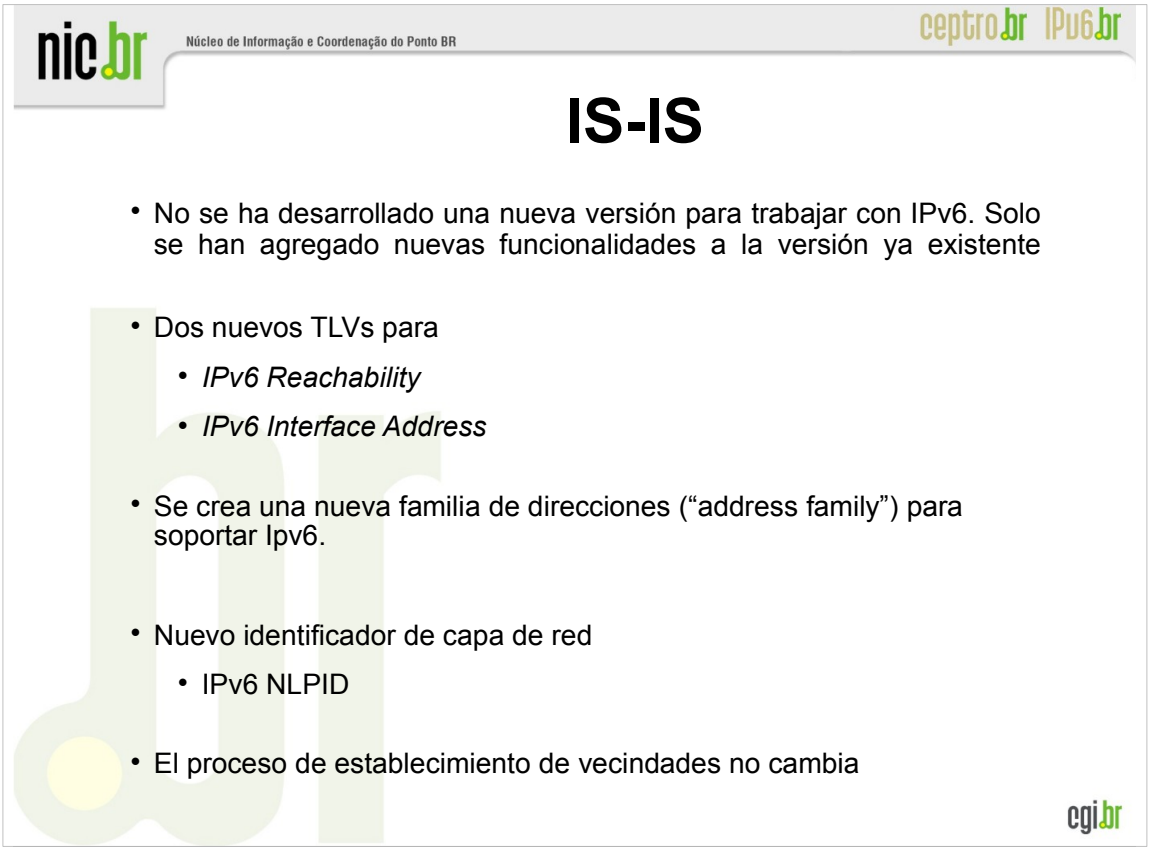
Use of Link-local addresses:
OSPFv3 requires that every interface has a link-local address from the range FE80/10. A router uses the link-local address as next-hop during packet forwarding for the neighbors attached to its links.



Al igual que OSFP, *Intermediate System to Intermediate System* (IS-IS) es un protocolo IGP de tipo *link-state*, que utiliza el algoritmo de Dijkistra para calcular las rutas.

IS-IS fue originalmente desarrollado para funcionar sobre el protocolo CLNS (Connectionless Network Service) (OSI equivalent to IP), pero la versión *Integrated IS-IS* permite enrutar tanto paquetes de red IP como OSI. Para ello se utiliza un identificador de protocolo, el NLPID (Network layer protocol identifier), para informar qué protocolo de red está siendo utilizado.

Al igual que OSPF, IS-IS también permite trabajar la red de manera jerárquica, actuando con los routers en dos niveles, L1 (Stub) y L2 (Backbone), además de los routers que integran esas áreas, L2/L1.



Para tratar el enrutamiento IPv6 no se definió una nueva versión del IS-IS sino que solo se agregaron nuevas funcionalidades a la versión ya existente.

Se agregaron dos nuevas TLVs (*Type-Length-Values*):

- **IPv6 Reachability** (type 236) – Transporta información de las redes accesibles;
- **IPv6 Interface Address** (type 232) – Indica las direcciones IP de la interfaz que está transmitiendo el paquete.

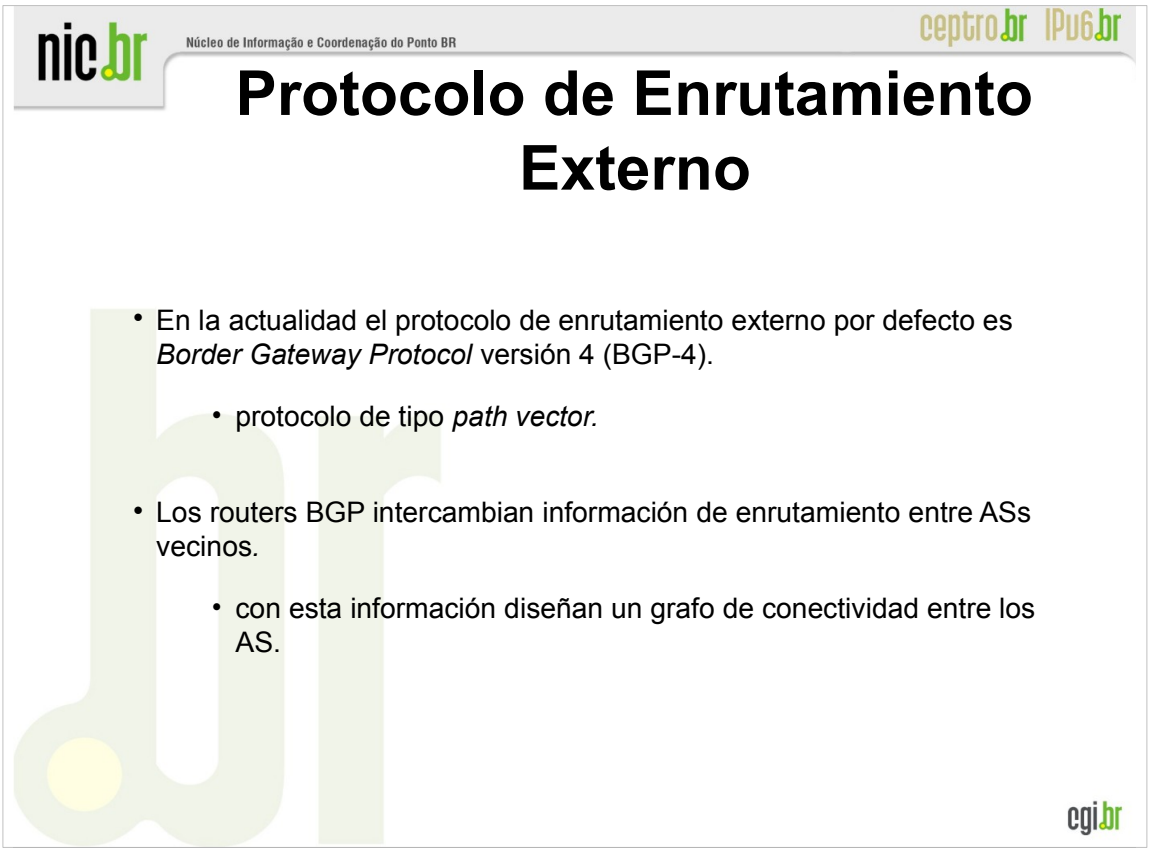
También se agregó un nuevo identificador de la capa de red

- **IPv6 NLPID** – Su valor es 142.

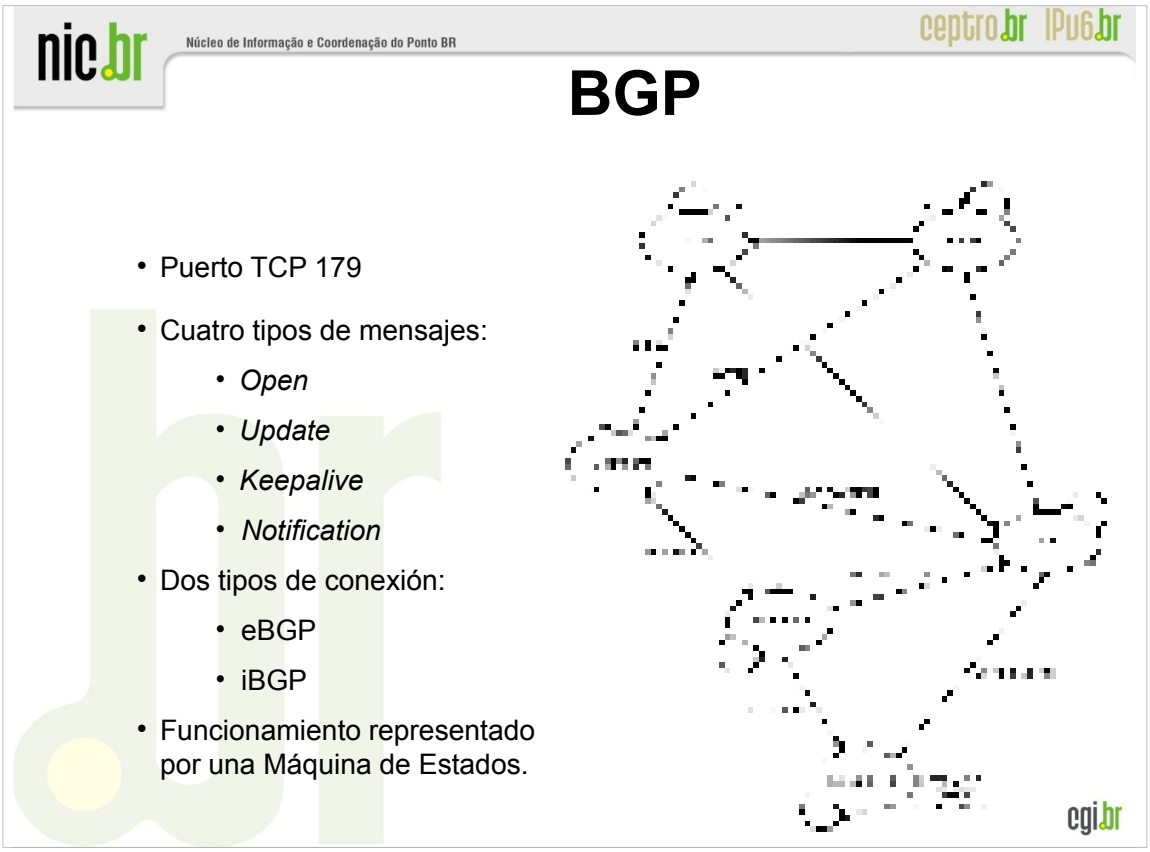
El proceso de establecimiento de vecindades no cambia.

Más información:

- RFC 1195 - *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- RFC 5308 - *Routing IPv6 with IS-IS*



En la actualidad el protocolo de enrutamiento externo por defecto es *Border Gateway Protocol* versión 4 (BGP-4). Se trata de un protocolo de tipo *path vector*, en el cual los routers BGP intercambian información de enruramiento entre ASs vecinos diseñando un grafo de conectividad entre los mismso.



BGP es un protocolo extremamente simple basado en sesiones TCP escuchando en el puerto 179.

Para intercambiar información y mantener el estado de la conexión TCP se utilizan cuatro tipos de mensajes BGP:

- *Open* – Enviado por los dos vecinos luego del establecimiento de la conexión TCP, lleva la información necesaria para el establecimiento de la sesión BGP (ASN, versión de BGP, etc);
- *Update* – Usado para transferir la información de enrutamiento entre los vecinos BGP, la cual se utilizará para construir el grafo que describe la relación entre varios ASs;
- *Keepalive* – Se envían frecuentemente para evitar que la conexión TCP expire;
- *Notification* – Se envía cuando se detecta un error, cerrando la conexión BGP inmediatamente después de su envío.

Usted puede establecer dos tipos de conexión BGP:

- externa (eBGP) – conexión entre dos AS vecinos;
- interna (iBGP) – conexión entre routers dentro de un mismo AS. Establecer el iBGP es muy importante para mantener una visión consistente de las rutas externas en todos los routers de un AS.

El funcionamiento de BGP se puede representar mediante una Máquina de Estados Finitos. Para quien no están familiarizado con el protocolo BGP, al verificar que el estado de una conexión está “Active” o “Established”, puede tener la falsa impresión de que la conexión está “activa” o “establecida”, pero en general, en BGP, cuando hay “palabras” representando el estado, significa que la sesión BGP todavía no está bien. La sesión estará efectivamente establecida cuando se observe el número de prefijos que se está recibiendo del vecino. Esos nombres representan estados intermedios de la sesión BGP. Identificar eses estados ayuda en el análisis y resolución de problemas.

Más información:
RFC 4271 - *A Border Gateway Protocol 4* (BGP-4)
RFC 4760 - *Multiprotocol Extensions for* BGP-4

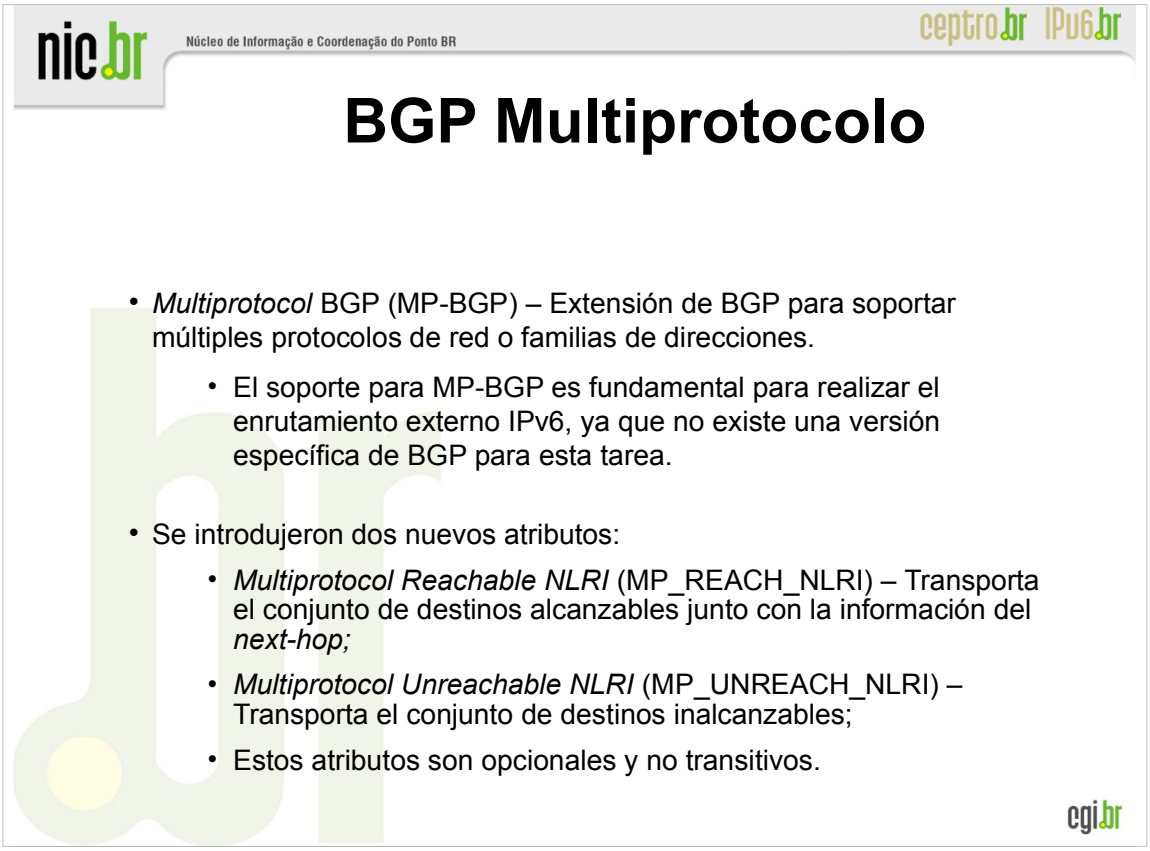
A pesar de que la RFC sobre BGP recomienda algunos puntos, el criterio de selección entre diferentes atributos BGP puede variar de implementación a implementación. Sin embargo, la mayor parte de las implementaciones sigue los mismos estándares.

Los atributos BGP se pueden dividir en dos grandes categorías:

- **Bien conocidos** (*Well-known*) – Son atributos definidos en la especificación original del protocolo BGP. Estos se subdividen en otras dos categorías:
  - **Obligatorios** (*Mandatory*) – Siempre deben estar presentes en los mensajes tipo UPDATE y deben ser obligatoriamente reconocidos por todas las implementaciones del protocolo;
  - **Discrecional** (*Discretionary*) – No deben obligatoriamente estar presentes en todos los mensajes UPDATE.
- **Opcionales** (*Optional*) – No son obligatoriamente soportados por todas las implementaciones de BGP. Estos se subdividen en otras dos categorías:
  - **Transitivos** (Transitive) – Deben ser re-transmitidos en los mensajes UPDATE;
  - **No Transitivos** (*Non-transitive*) – No deben ser re-transmitidos.

La RFC sobre BGP contiene los siguientes atributos:

- *ORIGIN* – Es bien conocido y obligatorio Indica si el camino fue aprendido vía IGP o EGP;
- *AS_PATH* - Es bien conocido y obligatorio. Indica el camino para llegar a un destino, listando los ASN por los cuales se debe pasar;
- *NEXT_HOP* – Es bien conocido y obligatorio. Indica la dirección IP de la interfaz del siguiente router;
- *MULTI_EXIT_DISC* – Es opcional y no transitivo. Indica a los vecinos BGP externos cuál es el mejor camino para una determinada ruta del propio AS, influenciándolos, así como cuál camino se debe seguir en caso que el AS posea diferentes puntos de entrada;
- *LOCAL_PREF* – Es bien conocido y discrecional. Indica un camino de salida preferencial para una determinada ruta destinada a una red externa al AS;
- *ATOMIC_AGGREGATE* – Es bien conocido y discrecional. Indica si caminos más específicos se agregaron en menos específicos.
- *AGGREGATOR* - Es opcional y transitivo. Indica el ASN del último router que formó una ruta agregada, seguido por su propio ASN y dirección IP.



Se definieron extensiones para BGP-4 con la intención de habilitarlo para que transporte información de enrutamiento de múltiples protocolo de Capa de Red (ex., IPv6, IPX, L3VPN, etc.). Para realizar el enrutamiento externo IPv6 es fundamental el soporte para MP-BGP, ya que no existe una versión específica de BGP para tratar esta tarea.

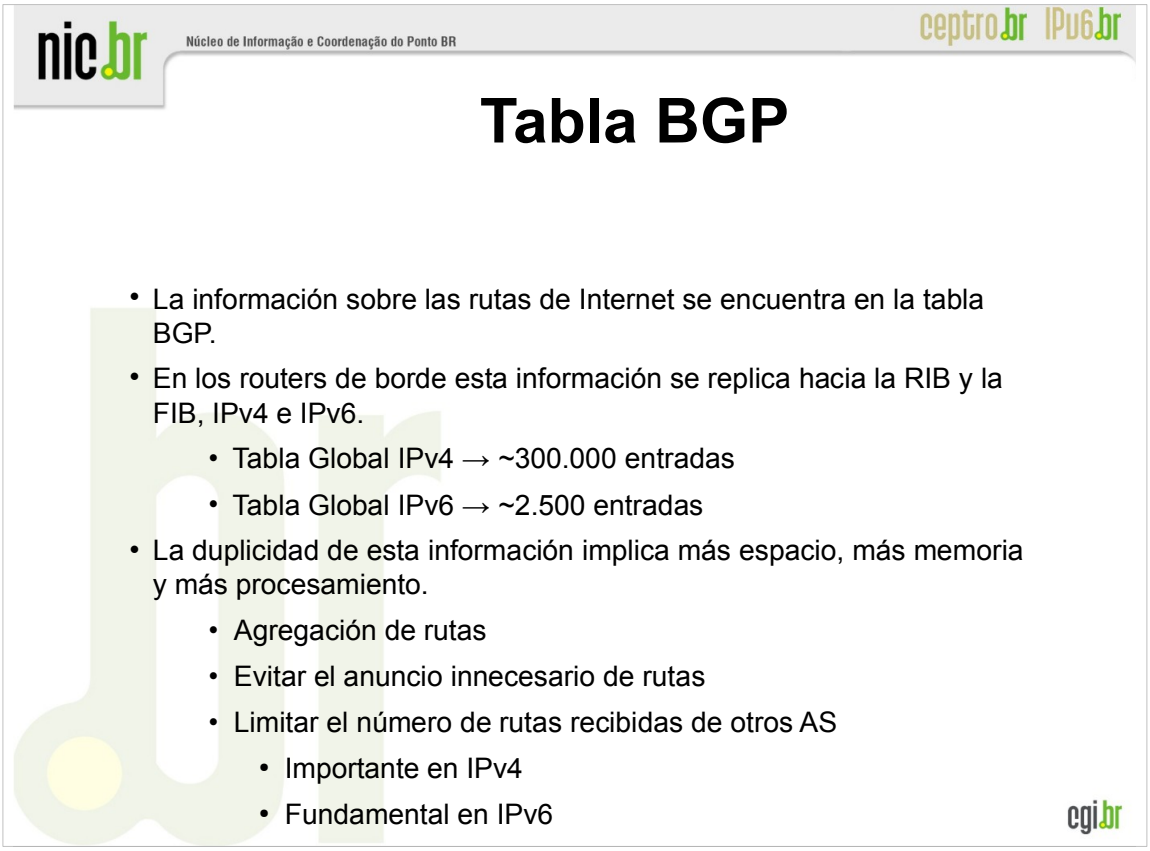
Para que BGP pueda trabajar con la información de enrutamiento de diversos protocolos se introdujeron dos nuevos atributos:

- *Multiprotocol Reachable NLRI (Network layer reachability information)* (MP_REACH_NLRI): Transporta el conjunto de destinos alcanzables junto con la información del *next-hop;*
- *Multiprotocol Unreachable NLRI* (MP_UNREACH_NLRI): Transporta el conjunto de destinos inalcanzables.

Estos atributos son opcionales y no transitivos; en caso que un router BGP no soporte MBGP, debe ignorar esta información y no transferirla a sus vecinos.

Más información:

- RFC 2545 - *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
- RFC 4760 - *Multiprotocol Extensions for BGP-4*

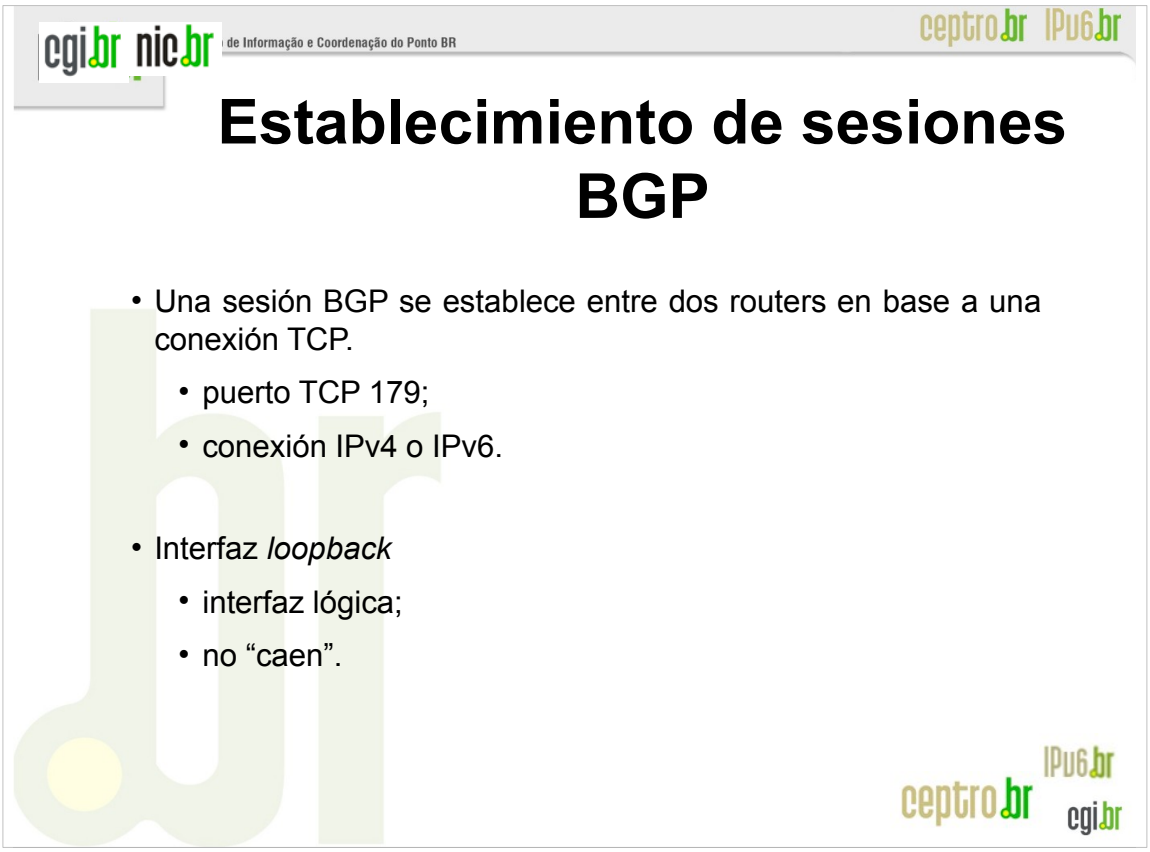


La información sobre las rutas de Internet se encuentra en la tabla BGP. En los routers de borde, los cuales se ocupan de la comunicación entre ASs, esta información se replica hacia la RIB y la FIB, IPv4 e IPv6.

La tabla global IPv4 hoy tiene aproximadamente 300.000 entradas. La tabla IPv6 tiene aproximadamente 2.500 entradas. La duplicidad de esta información en las arquitecturas distribuidas implica la necesidad de contar con más espacio para almacenamiento, más memoria y más capacidad de procesamiento, tanto en el módulo central como en las placas de las interfaces.

Esto también implica otro aspecto importante, la necesidad de establecer un plan de direccionamiento jerárquico para minimizar la tabla de rutas y optimizar el enrutamiento, evitando el anuncio de rutas innecesarias y desagregadas.

Los AS también pueden controlar los anuncios que reciben de sus vecinos BGP. Por ejemplo, es posible limitar el tamaño de los prefijos recibidos entre /20 y /24 IPv4, y entre /32 y /48 IPv6. Sin embargo, recuerde que se pueden anunciar hasta 31 prefijos IPv4 (considerando anuncios entre un /20 y un /24) y 131.071 prefijos IPv6 (considerando anuncios entre un /32 y un /48), de este modo hay quienes también controlan la cantidad de prefijos que reciben de sus vecinos BGP a través de comandos como `maximum-prefix` (Cisco) y `maximum-prefixes` (Juniper). Prestar atención a este tema es muy importante en las redes IPv4, pero en las redes IPv6 es fundamental.



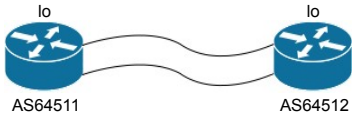
Una sesión BGP se establece entre dos routers en base a una conexión TCP, utilizando como estándar el puerto TCP 179, precisándose para ello conectividad IP, ya sea IPv4 o IPv6.

Una forma de establecer esa comunicación es a través de interfaces *loopback*. Éstas son interfaces lógicas, como la “null0”, es decir, “no caen” a no ser que se apague el router o que la interfaz se desconfigure.

Por sus características, es fundamental que las sesiones iBGP se establezcan utilizando la interfaz *loopback*. En caso que la sesión sea establecida a través de la IP de la interfaz física, real, si el *enlace* se interrumpe la sesión también se interrumpirá. Si se establece a través del a interfaz *loopback*, la sesión podrá ser restablecida por otro camino aprendido a través de los protocolos IGP.

El uso de interfaces *loopback* en el establecimiento de las sesiones iBGP proporcionan mayor estabilidad a los sistemas autónomos.

Establecimiento de sesiones BGP



eBGP entre *loopbacks*

- Balanceo
  - Por ejemplo:
    - Hay dos routers y cada router representa un AS:
    - Ambos están conectados mediante dos *links;*
    - Utilizando la IP de las interfaces reales:
      - Se necesitarán dos sesiones BGP;
      - Eventualmente con políticas diferentes.
    - Utilizando la IP de las interfaces *loopback*
      - Se establece una única sesión BGP;
      - Se crea una ruta estática para la IP de la interfaz *loopback* del vecino a través de cada *link*.

También se recomienda utilizar interfaces *loopback* para establecer sesiones eBGP. Uno de los propósitos de establecer este tipo de conexión es garantizar el balanceo.

Consideremos el siguiente ejemplo:

- Hay dos routers – cada uno de los cuales representa un AS – conectados a través de dos enlaces;
- Si en esta comunicación se utiliza la IP de las interfaces reales será necesario establecer dos sesiones BGP para cada sesión, eventualmente habrá una política diferente. Eso puede ocasionar complicaciones innecesarias.
- Utilizar las interfaces *loopback* simplifica este proceso. En ese caso, solo se necesitaría una sesión BGP y la creación de rutas estáticas apuntando a la IP de la *loopback* del vecino a través de cada enlace.

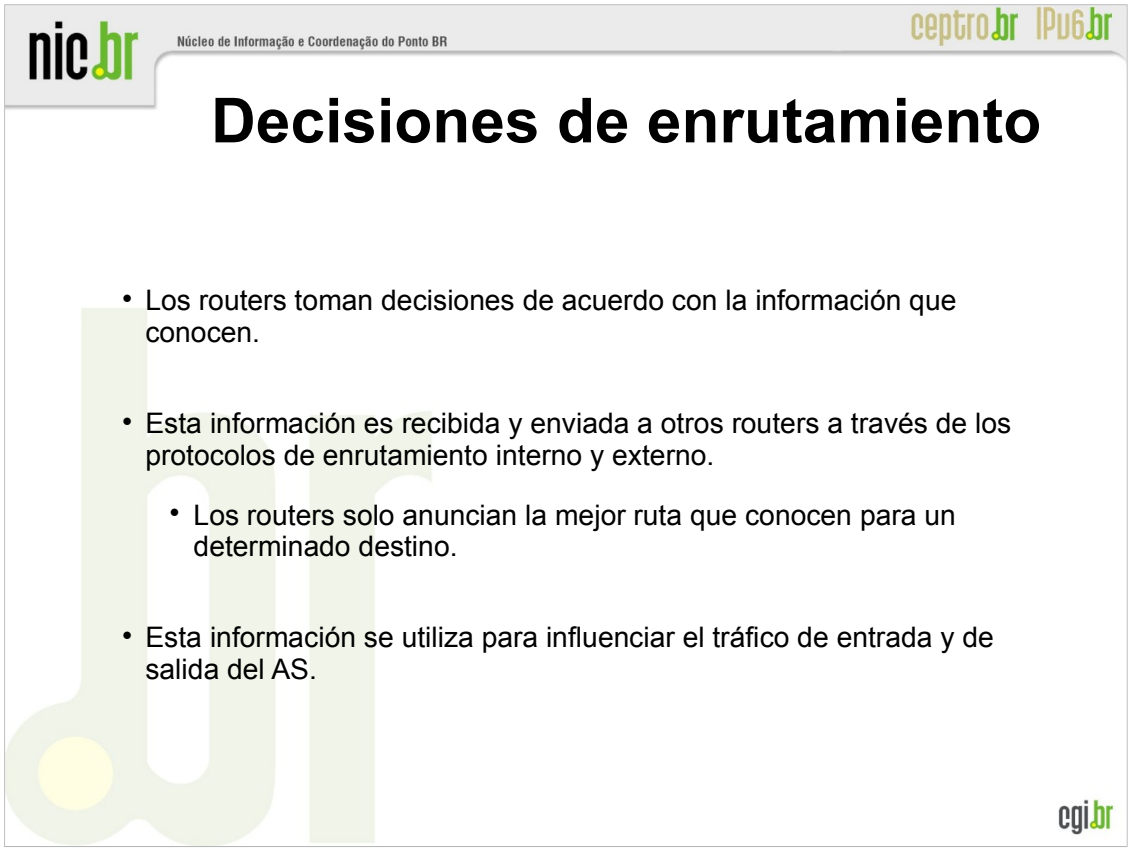
Establecimiento de sesiones BGP

eBGP entre *loopbacks*

- Seguridad
  - La utilización de interfaces *loopbacks* en sesiones eBGP no es necesaria solo para asegurar el balanceo.
  - Establecer sesiones eBGP utilizando la IP de la interfaz facilita mucho los ataques contra la infraestructura.
  - Es recomendable establecer eBGP entre *loopbacks* aunque haya un único *enlace*.

Hay quienes sostienen que el uso de interfaz *loopback* solo es realmente necesaria para garantizar el balanceo de tráfico. Esa práctica también ayuda en relación con los temas de seguridad.

Establecer sesiones eBGP utilizando la IP de la interfaz puede facilitar los ataques contra la infraestructura de un AS. Por eso es recomendable trabajar sesiones eBGP entre *loopbacks* aunque exista un único *enlace*.



Los routers toman decisiones de acuerdo con la información que conocen. Esta información es recibida y enviada a otros routers a través de los protocolos de enrutamiento interno y externo.

Al enviar su información, los routers solo anuncian la mejor ruta que conocen para un determinado destino. Esta información se utilizará para influenciar el tráfico de entrada y de salida del AS.