Redes de Datos 2
1º Parcial
02/05/2022

Solución

Esta es una posible solución a las preguntas planteadas. Por razones didácticas normalmente contiene bastante más información que la mínima necesaria para responder la pregunta.

Pregunta 1 (3 puntos)

a) Explique por qué se incorporan en IPv6 mecanismos de autoconfiguración.

Dada la cantidad de bits de las direcciones IPv6 (128) en comparación con las de IPv4 (32), la configuración manual en IPv6 es más engorrosa y sujeta a errores, por lo que en IPv6 se agregan mecanismos de autoconfiguración para facilitar la tarea a los administradores. Estos mecanismos (en particular SLAAC) se agregan a la posibilidad de configuración manual y a la configuración por DHCP que siguen existiendo como en IPv4.

b) Explique el mecanismo de autoconfiguración llamado SLAAC (Stateless Address Auto Configuration), indicando los pasos que realiza un equipo para autoconfigurarse.

El mecanismos SLAAC prevé que un equipo pueda autoconfigurar los datos necesarios para conectarse a una red (dirección IP, prefijo, ruta por defecto, servidores de DNS). Es una configuración sin estado en la red, a diferencia de lo que sucede cuando esos parámetros se asignan por DHCP.
En la configuración de direcciones mediante DHCP, el servidor DHCP debe conservar el estado de las direcciones asignadas, los tiempos de asignación y la identificación del equipo al que se asignaron. Por esto la asignación por DHCP se llama stateful.
En la autoconfiguración SLAAC, cada enrutador de la red enviará mensajes RA (Router Advertisement, ICMPv6) indicando que tanto las direcciones IP (bandera M) como los otros parámetros (DNS) (bandera O) se obtienen a partir del mensaje RA. En este caso ambas banderas estarán en 0 y el RA incluirá en la opción Prefix Information el prefijo asignado a los equipos de esa LAN.
La secuencia de eventos cuando un equipo se conecta a la red es:

i. *Se crea un Identificador de Interfaz (IID) de 64 bits de forma aleatoria o usando el mecanismo EUI-64*
ii. *Se concatena el prefijo fe80::/10 definido para direcciones link-local al IID conformando una dirección IPv6 de alcance local*
iii. *Se realiza la verificación de unicidad usando el mecanismo DAD consistente en enviar un mensaje de Neighbor Solicitation con destino a la dirección Solicited Node correspondiente a la IP generada. Si la IP es única no debería ser respondido. Si es respondido, entonces hay que volver al paso i. generando un nuevo IID.*
iv. *Se configura la IP generada en la interfaz*
v. *Se envía un Router Solicitation a la dirección multicast asociada a "todos los routers".*
vi. *El router responde con un Router Advertisement (si no hay respuesta habrá que pasar a un mecanismo stateful) conteniendo las banderas M=0, O=0, opción Prefix Information.*
vii. *La bandera M=0 indica que las direcciones se deben configurar a partir del prefijo indicado. Por tanto se concatena el prefijo indicado en el RA con el IID generado en (i). y se obtiene una dirección IPv6.*

viii. *Mediante DAD se verifica la unicidad de esa IP y posteriormente se configura en la interfaz*
ix. *La ruta por defecto se configura usando como próximo salto la IP link-local del router obtenida del RA.*
x. *La bandera O=0, indica que el DNS debe configurarse a partir de la información de RA, por lo que éste debería incluir la opción RDNSS con la IP del servidor DNS a utilizar. El DNS también se puede obtener de la configuración de IPv4 si el equipo es dual-stack o configurarse por DHCP (en ese caso O sería 1).*

Pregunta 2 (3 puntos)

a) Explique qué son los identificadores de interfaz y para qué se utilizan en IPv6.

Los identificadores de interfaz son los 64 bits menos significativos de una dirección IPv6 y se definen para cada interfaz de cada equipo. Concatenándolos con un prefijo se conforman direcciones IPv6. Se pueden elegir manualmente, aleatoriamente o utilizando el mecanismo EUI-64. Estos IIDs concatenados con un prefijo fe80:: permiten generar automáticamente direcciones link-local o concatenados con un prefijo global permiten generar automáticamente direcciones globales.

b) Explique cómo se pueden generar usando el mecanismo EUI-64.

La IEEE define un mecanismo para generar los IID (64 bits) a partir de la dirección MAC/802. (48 bits) de una interfaz.
El mecanismo consiste en tomar los 3 bytes más significativos de la dirección MAC (los bytes que identifican el fabricante), concatenarlos con dos bytes con el valor FFFE y concatenarlos con los 3 bytes menos significativos de la dirección MAC. Además se invierte el valor del bit 2 del primer byte.
Dado que las direcciones MAC se supone que son únicas para cada interfaz, este mecanismo genera IIDs únicos para cada interfaz.

Pregunta 3 (6 puntos)

a) En el protocolo OSPF, ¿cuáles son las funciones del enrutador designado (DR)?
¿En qué redes se utiliza?
El enrutador designado se utiliza en las redes multiacceso (broadcast o NBMA), como por ejemplo las redes 802.3 (Ethernet) u 802.11
Sus funciones son:
- Generación e inundación del LSA tipo network que representa en el grafo a la red multiacceso
- Ser adyacente con todos los enrutadores de la red multiacceso, y de esa forma minimizar la cantidad de adyacencias (cada enrutador de la red multiacceso es adyacente solo con el DR)

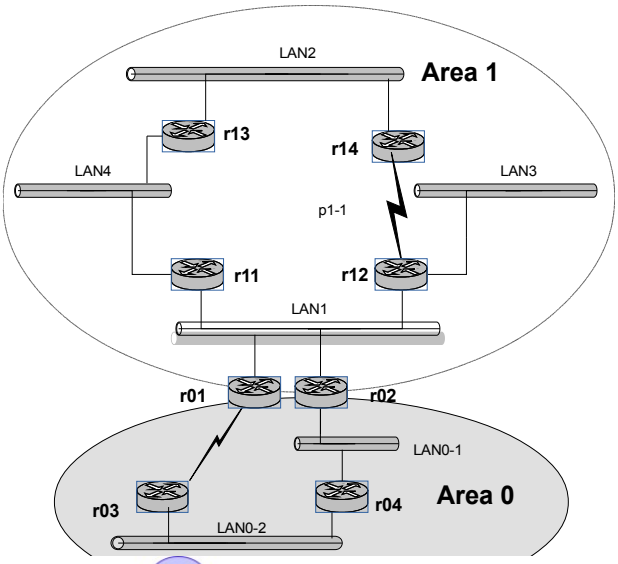
b) Explique cómo funciona el mecanismo de descubrimiento de vecinos mediante Hello, y cómo se realiza la elección del DR en OSPF
El descubrimiento de vecinos en OSPF se basa en el envío periódico de paquetes Hello por parte de todos los enrutadores que hablan OSPF. Los vecinos son descubiertos cuando recibo sus paquetes Hello. (una vez descubierto el vecino el enrutador lo agrega en la lista de vecinos de sus paquetes Hello, para de esta manera confirmarle al otro enrutador que la comunicación es bidireccional)
En las redes multiacceso también se utilizan los paquetes Hello para la elección del enrutador designado (DR). El paquete Hello tiene un campo para indicar el router-id del DR (y del BDR). Si no hay un DR elegido, el enrutador con mayor prioridad se convierte en DR, poniendo su router-id en el campo correspondiente de los paquetes Hello enviados, y los demás lo

aceptarán poniéndo también este valor en sus mensajes de Hello. En caso de empate en las prioridades se elige en función del router-id. En cambio si ya hay un DR elegido (los paquetes Hello recibidos ya tienen el router-id del DR) entonces se acepta aunque tengamos mayor prioridad

c) Explique las semejanzas y diferencias con el mecanismo de descubrimiento de vecinos del protocolo IS-IS (por ejemplo manejo de prioridades, manejo de DR y respaldo, protocolo sobre el que se transporta, información enviada, etc)
Ambos protocolos utilizan un mecanismo basado en el envío periódico de paquetes de descubrimiento (Hello en OSPF, IIH PDU en IS-IS). Para los enlaces punto a punto en ambos los vecinos son adyacentes si coinciden los parámetros, y en ambos se elige un enrutador específico (enrutador designado en OSPF, IS designado en IS-IS) para ser adyacente con los demás nodos si se trata de una red multiacceso.
Como diferencias vistas en clase podemos notar que en IS-IS hay diferentes "Hello" para nivel 1 y nivel 2 (y un enrutador que sea L12 tendrá que formar adyacencias en ambos niveles), que en IS-IS no se elige un enrutador designado de respaldo (BDR), que en IS-IS un nuevo enrutador con mayor prioridad es automáticamente elegido como DIS (en OSPF si ya hay un DR elegido, este no se cambia al ingresar un nuevo enrutador a la red) y que como todos los paquetes IS-IS, los paquetes de "Hello" no utilizan IP para su transporte

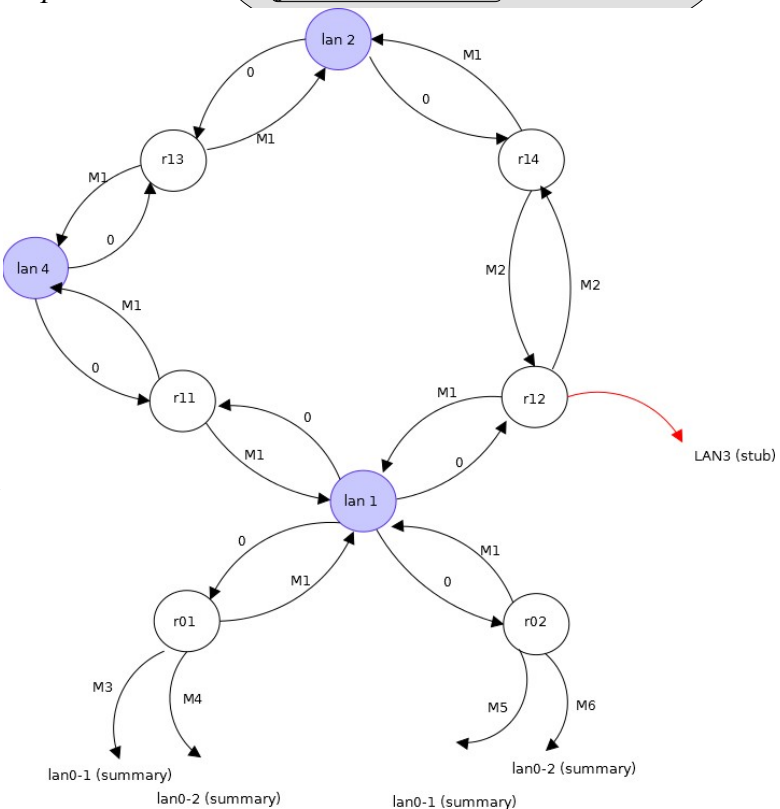
Pregunta 4 (7 puntos)

La red de la figura es dual stack (IPv4 e IPv6). Como protocolo de enrutamiento se utiliza OSPF (v2 y v3). Los enrutadores y áreas son los indicados. Las redes son todas Gigabit Ethernet excepto los enlaces punto a punto r14-r12 y r01-r03.



a) Esquematice la topología vista por un enrutador del área 1. ¿Cambia dicha topología según si se trata de OSPFv2 u OSPFv3? Justifique.

En el siguiente diagrama se observa una posible representación de la topología observada por los enrutadores del área 1.



Se asumió que los enlaces punto a punto no son numerados (si lo fueran aparecen redes stub en los enrutadores correspondientes), y que la métrica que cada enrutador calcula para las redes LAN es igual (M1). LAN3 fue representada, pero no forma parte de la topología sino que en IPv4 aparece como un link STUB en r12, y en IPv6 aparece como un LSA tipo Intra-Area Prefix.

La topología es la misma ya sea que se trate de OSPFv2 u OSPFv3 (mismas aristas, mismos vértices) ya que se utiliza la misma representación de los elementos de la red (los nodos son los enrutadores y redes multiacceso, las aristas los links)

b) Indique los LSA (tipo y elemento descripto) que espera que conozcan los enrutadores del área 1 en el caso de OSPFv2.
Esperamos ver 6 LSA de tipo router, correspondiente a los 6 enrutadores que tienen interfaces en el área, 3 LSA de tipo network, correspondientes a las redes multiacceso con más de un enrutador conectado, y LSA de tipo summary correspondientes a las redes externas al área (que en el diagrama mostrado son las correspondientes redes accesibles en el área 0, LAN0-1 y LAN0-2)

c) Para el LSA que describe al enrutador r12, indique la información que lleva dicho LSA. ¿qué diferencias hay entre el LSA para OSPFv2 y OSPFv3?
El LSA de tipo enrutador para r12 incluirá al menos:
- ✔ *Encabezado de LSA conteniendo*
  - *Identificación del enrutador (router-id de 32 bits correspondiente a r12)*
  - *Número de secuencia*
  - *Suma de comprobación*
  - *Tipo (router)*
  - *Edad*
  - *Opciones (solo en IPv6)*
- ✔ *Lista de todos los links e información de cada uno de ellos. R12 tiene 3 links (4 en OSPFv2 si el link punto a punto está numerado):*
  - *Link punto a punto hacia r14. Incluye router-id de r14, y métrica de utilizar dicho link*
  - *Link de tipo tránsito hacia LAN 1. Se identifica LAN1 con el network-id del LSA network correspondiente, incluye la métrica*
  - *Link de tipo STUB correspondiente a LAN3. En OSPFv2 indica red y máscara. En OSPFv3 usa un identificador interno, y la información de direcciones IP se encuentra en otro LSA (de tipo Intra-Area-Prefix) relacionado con este*
  - *En OSPFv2, si el link punto a punto tiene direcciones IP, tendremos un link de tipo STUB para estas IPs (incluyendo red y máscara)*

Las diferencias son las ya notadas, que en OSPFv2 hay un campo de opciones del LSA que no se encuentra en OSPFv3, que los link STUB en OSPFv2 incluyen la información de IP/Máscara, mientras que en OSPFv3 la información de direcciones IP se envía mediante LSAs de tipo Inter-Area-Prefix

Pregunta 5 (7 puntos)

a) ¿Por qué dentro del protocolo BGP se diferencia entre eBGP e iBGP?

El objetivo de eBGP es intercambiar información de prefijos y sus atributos con otros Sistemas Autónomos (AS), mientras que iBGP permite propagar la información aprendida de otros AS dentro del AS local. La diferenciación es importante porque el comportamiento es diferente, por ejemplo, el tipo de atributos intercambiados, local-preference solo se utiliza en sesiones iBGP, el comportamiento por defecto que se utiliza con el atributo

NEXT-HOP (en eBGP por defecto se utiliza para el NEXT-HOP la IP de quien inicia la sesión mientras que para iBGP se preserva el NEXT-HOP aprendido).

Las reglas de propagación de anuncios también son diferentes, lo veremos en las próximas partes, pero básicamente eBGP puede detectar loops de información de ruteo revisando el atributo AS-PATH, mientras que en iBGP no es posible detectar loops.
Si bien normalmente se deshabilita, la sincronización es una regla que no permite considerar un prefijo aprendido por iBGP a menos que se aprenda por el IGP (Interior Gateway Protocol). Esta regla solo aplica al escenario iBGP.

b) ¿En qué se diferencia la configuración de eBGP e iBGP?

La diferencia por excelencia es que el AS del vecino BGP y el AS local coinciden en el caso de iBGP, y son diferentes en eBGP. Luego hay diferencias más sutiles, por ejemplo, los Reflectores de rutas o Confederaciones, solo aplican en sesiones iBGP.

¿En qué se diferencia el comportamiento de eBGP e iBGP?

- *En el comportamiento de redistribución de los prefijos aprendidos, siendo formales del mejor camino aprendido.*
- *Modificación del NEXT-HOP del anuncio al propagarlo, por defecto eBGP lo modifica, iBGP preserva lo aprendido.*
- *Las sesiones iBGP por defecto son multi-hop, los vecinos no tienen porque estar directamente conectados (no impone restricciones al valor de TTL de IP), en eBGP por defecto se asume directamente conectado (TTL=1).*

c) De acuerdo a las reglas del protocolo BGP. ¿Lo que se aprende por una sesión eBGP por que tipo de sesiones BGP se distribuye?

Si el mejor camino para un prefijo se aprende por eBGP, este se enseñará tanto a vecinos eBGP como iBGP.

d) De acuerdo a las reglas del protocolo BGP. ¿Lo que se aprende por una sesión iBGP por que tipo de sesiones BGP se distribuye?

Si el mejor camino para un prefijo se aprende por iBGP, este solo se enseñará a vecinos eBGP.

El motivo de esto es prevenir loops de enrutamiento,
- si bien el comportamiento por defecto en iBGP es no alterar el NEXT-HOP aprendido, es posible realizarlo, en particular en el laboratorio vimos el next-hop self. Si lo aprendido por sesiones iBGP se propaga a vecinos iBGP y se tuviera activado next-hop self o se activa una política que modifica el next-hop, fácilmente se puede generar un loop de ruteo.
- ante el withdraw de un prefijo puede generarse un loop de anuncios entre los enrutadores del mismo AS, debido a no tener algún atributo que permita indicar que el anuncio recibido fue a su vez generado por el enrutador que lo está recibiendo

e) De acuerdo a las respuestas anteriores. ¿Qué criterio de diseño hay que elegir dentro de un AS de tránsito respecto a las sesiones de iBGP? Justifique

Todos los equipos en el camino entre el nodo eBGP de ingreso y egreso deben de conocer la información de ruteo para poder encaminar (forwardear) los paquetes entre el router de entrada al AS y el de salida del AS.

Dada la regla explicada en la parte (d), para que todos los enrutadores del sistema autónomo conozcan tanto la información aprendida por eBGP de otros sistemas autónomos como la generada por los propios enrutadores del sistema autónomo necesito tener sesiones iBGP entre todos, lo que se llama full-mesh iBGP. De esta manera puedo trasladar a un AS vecino (AS X) lo aprendido de otro AS vecino (AS Y).

Las arquitecturas con full-mesh iBGP adolece del problema de escala, mantenimiento de cambios cuando crece la cantidad de routers iBGP. Hay dos propuestas para mejorar estos aspectos de escalabilidad, definir reflectores de rutas y jerarquías de reflectores, o confederaciones.

***Nota:** En caso de no ser AS de tránsito, podría no ser necesario el full-mesh, por ejemplo, si se trata de un sistema autónomo stub, alcanza con una ruta por defecto hacia el equipo de frontera.*

Pregunta 6 (5 puntos)

a) Describa la información que llevan los atributos AS_PATH y LOCAL_PREFERENCE; y cómo se utilizan en el protocolo BGP.

El AS_PATH es un atributo obligatorio, bien conocido que contiene la lista de sistemas autónomos (AS) que el anuncio ha atravesado y permite detectar/evitar loops. Puede incluir una lista de ASs o un conjunto de ASs (AS-Set).
Se usa también, en el algoritmo de decisión del mejor camino, para preferir un camino con menor largo de AS_PATH.

El LOCAL_PREFERENCE es un atributo opcional, bien conocido que se utiliza en el algoritmo de decisión del mejor camino para preferir aquellos anuncios cuyo valor de preferencia sea mayor. Permite influenciar la salida de tráfico de mi AS cuando tengo varios caminos hacia un mismo destino, eligiendo convenientemente los valores de preferencia. Su valor se define administrativamente por política. Tiene sentido solamente dentro de mi AS y por tanto se propaga por iBGP, pero no por eBGP.

b) Dentro del proceso de selección de mejor camino en BGP, ¿Cuál de los atributos anteriores se evalúa primero?

Al comparar caminos para un mismo prefijo, se compara primero el valor de LOCAL_PREFERENCE, y solo si estos valores son iguales se avanza llegando eventualmente a comparar las longitudes del AS-PATH. Esto hace que sea más fácil influenciar el "camino de salida" de mi sistema autónomo (manipulando el atributo LOCAL_PREFERENCE dentro del AS) que el tráfico entrante manipulando el largo del AS-PATH

Pregunta 7 (6 puntos)

a) Compare ventajas y desventajas de establecer las sesiones iBGP desde las IP asignadas a interfaces físicas versus establecerlas desde las IP de interfaces de loopback.

	Ventajas	*Desventajas*
Interfaz física	*Configuración en el bloque BGP más simple*	*Recordado que iBGP no tienen por qué estar directamente conectado, cuando hay varios caminos entre los dos vecinos, requiere declarar varias vecindades para obtener el provecho de disponer de varios caminos. Amplia el problema de escala en Full-Mesh iBGP*
Interfaz de loopback	*Permite que independientemente de la cantidad de caminos existente entre los vecinos iBGP, solo se visualice una vecindad, y de delegue la responsabilidad del camino a seguir a lo que decida el IGP.*	*Requiere definir una interfaz de loopback, redistribuir su dirección por el IGP, y que las sesiones iBGP se configuren utilizando dichas direcciones de loopback (update-source).*

b) ¿Qué modificaciones se deben realizar en la configuración de BGP para utilizar como origen las interfaces de loopback?

Por defecto BGP utiliza como origen la dirección IP de la interfaz por la cual alcanza el vecino BGP según su tabla de rutas. Para utilizar como origen la interfaz de loopback debo declararlo en la configuración de la vecindad.

Como ejemplo, siguiendo la sintaxis de la CLI de FRR, requiere ***neigbour A.B.C.D update-source <loopback local>****, donde A.B.C.D es la IP de loopback del vecino (usualmente propagada por IGP) y loopback local es la interfaz de loopback local (se utiliza la dirección IP de dicha interfaz).*

c) ¿Cómo se resuelve la conectividad con las interfaces de loopback de mis vecinos iBGP?

Si bien se podría utilizar rutas estáticas y posiblemente ECMP (Equal cost multipath o balanceo entre rutas con misma métrica), lo usual es activar un protocolo de enrutamiento interior (recordar que en el laboratorio activamos OSPF). De esta manera mientras exista un camino entre las loopback aprendido por el IGP, habrá conectividad entre las loopback y se mantendrá la sesión iBGP. Dicho de otra manera, ante la pérdida de un camino entre

los vecinos BGP, si existe un camino alternativo el IGP lo seleccionará y no habrá pérdida de conectividad de la sesión iBGP.

***Nota**: Mientras converge el protocolo IGP, lo mas probable que se experimenten problemas de conectividad, usualmente los timers por defecto de los IGP suelen ser menores que los de BGP. En caso de ajustarse estos valores, se deben tener en cuenta las interdependencias entre protocolos.*

Actualmente existen protocolos auxiliares como BFD (Bidirecctional Forwarding Detection) que permiten identificar rápidamente la pérdida de conectividad por motivos físicos (por ejemplo, caída de enlaces), y notificar al protocolo de ruteo para que la detección de la pérdida de vecindad sea más rápida (no esperar a que expiren los timers), acelerando la convergencia del protocolo.

d) ¿Por qué podría ser necesario redistribuir las redes WAN (las redes de interconexión con los vecinos) de las diferentes sesiones eBGP dentro del protocolo IGP?

El proceso de selección de mejor camino de BGP no permite considerar una ruta para el cual el next-hop no sea alcanzable, el objetivo de la regla es no generar "agujeros negros", aceptar una ruta que luego no se puede seguir (no se tiene a quien entregar los paquetes para darles tránsito). Como no se considera en el proceso de mejor camino, no se incorpora en la FIB o se propaga a otro vecino (está en la local RIB, pero no en la adj-rib-out).

Recordando que en eBGP por defecto el NEXT-HOP es la IP de origen de la WAN, y que luego en iBGP por defecto no se altera este NEXT-HOP. Se debe encontrar una forma de que se conozcan dentro del sistema autónomo como alcanzar estas WANes. Un de estas alternativas es propagar estas WANes por el IGP, de esta forma se conoce el NEXT-HOP y se pueden considerar esas rutas en el proceso de selección de mejor camino.