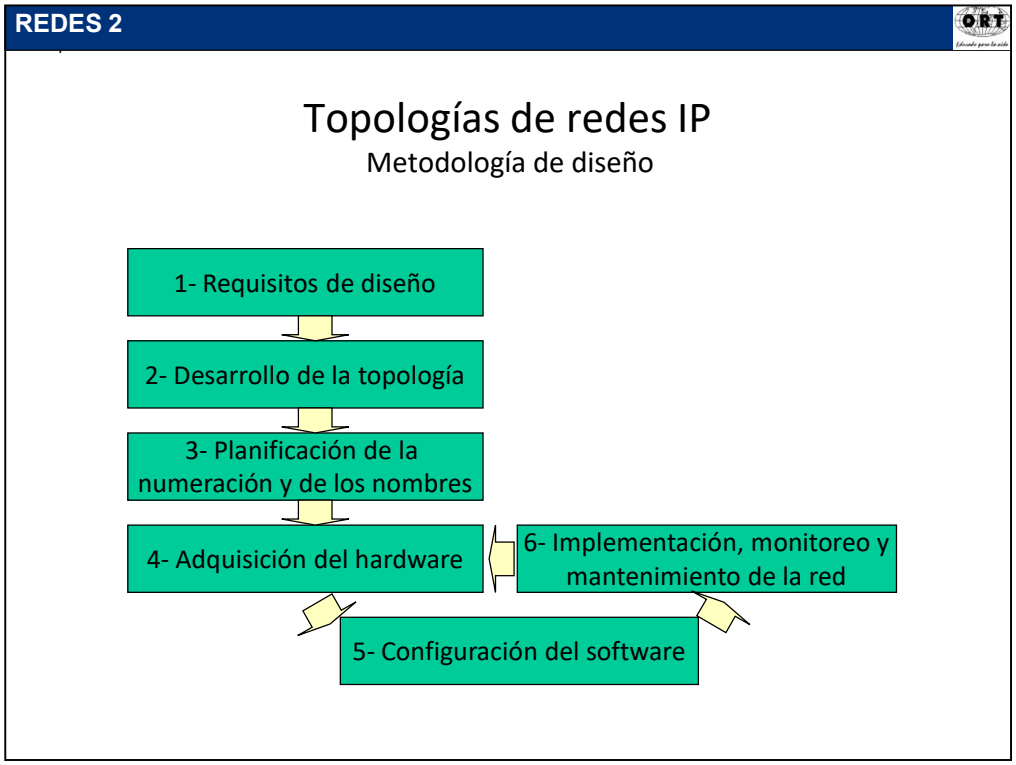
Topologías de redes IP y enrutamiento

Ing. José Restaino
Ing. Alvaro Sánchez



Metodología en etapas

La planificación y el diseño de la red pueden seguir una metodología en etapas como se muestra en la figura.

Las tres primeras se ejecutan una vez y sirven de base para el funcionamiento futuro de la red. Las restantes tres se aplican reiteradas veces para ajustar y desarrollar la red.

Requisitos de diseño - Primeramente se deben analizar las funcionalidades que se requieren. Ancho de banda, topología (acceso de diversos lugares remotos a un lugar central, red mallada, etc.), servicios (datos, multimedia).

Desarrollo de la topología - Empleo de un modelo jerárquico para el desarrollo de la topología general. De este modo, mediante el empleo de "capas" de red, se obtienen flexibilidad y escalabilidad. Según el modelo jerárquico, la red comprende tres capas (layers) al menos: core layer, distribution layer y access layer. El core provee conectividad entre lugares remotos a gran velocidad, y rara vez tiene hosts directamente conectados a él. En distribución se da servicio a múltiples LANs en un entorno de campus, normalmente constituyendo el "campus backbone" basado en FDDI, Fast Ethernet o ATM, e implementando las políticas de seguridad, de convenciones de nombres, etc. En el acceso, generalmente encontramos las LANs o grupos de ellas (Ethernet o Token Ring), que permiten la conectividad de los usuarios con la red, y en la cual se hallan la gran mayoría de los hosts y servidores.

Planificación de la numeración y de los nombres - Consiste en el diseño del plan de numeración y la asignación de bloques de direcciones a las diferentes porciones de la red, de modo de facilitar su administración y hacer escalable la asignación. Del mismo modo se debe planificar el esquema de denominaciones de máquinas, con prefijos comunes, para aplicarlo en toda la organización.

Adquisición del hardware - Selección del hardware a adquirir según necesidades de CPU, RAM, Bus, conmutación, tipos de interfaces y cantidades, etc. Se debe tener en cuenta también la capacidad de gestión.

Configuración del software - Definición de access lists, características de servicio proxy, encolamiento, compresión, etc. Inicialmente se debe poder determinar si los protocolos a emplear serán ruteables, si será posible gestionar remotamente los dispositivos y de qué manera se tendrá conocimiento de lo que hay conectado a la red. Finalmente se deberán configurar los servicios de proxy, las rutas estáticas y el filtrado en la capa de acceso, y las características de compresión, control de congestión y gestión en la capa de distribución.

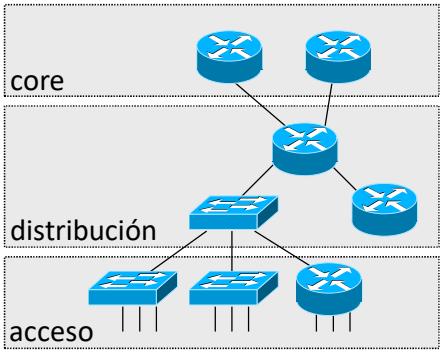
Implementación, monitoreo y mantenimiento de la red - En la última etapa de procede a la implementación. Siempre que sea posible se deberán probar las funcionalidades previamente en ambiente de laboratorio. La implantación deberá ejecutarse en etapas, de modo de minimizar el impacto al usuario. Finalmente, se deberá monitorear el estado de la red a efectos de prever posibles necesidades de

cambios y/o crecimiento.

Topologías de redes IP

Modelo jerárquico

En redes IP es posible distinguir al menos tres servicios lógicos: backbone o core, distribución o agregación, y accesos.



⇐ Backbone o core: provee conectividad de alta performance a distintas partes de la red.

⇐ Distribución: aplica las políticas de permisos y filtros.

⇐ Acceso: permite acceso a recursos y conectividad local.

Modelo de diseño jerárquico

Los diseños de red tienden s seguir uno de dos modelos de diseño: mallado o jerárquico.

En un diseño mallado todos los routers desempeñan funciones similares, la topología es chata (flat) y no hay especialización o división de tareas. La red crece en forma desordenada y su comportamiento es difícilmente previsible.

En una estructura jerárquica cada capa tiene funciones específicas, lo cual permite:

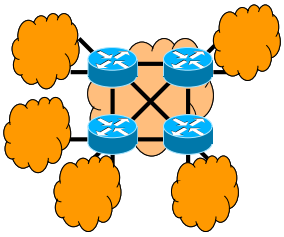
- *Escalabilidad* - permite crecer mucho más manteniendo el control y la facilidad de gestión, porque la funcionalidad está localizada y los potenciales problemas se pueden reconocer más fácilmente.
- *Facilidad de implementación* - las funciones están definidas claramente en cada capa lo que facilita la implementación.
- *Facilidad de troubleshooting* - el aislamiento de los problemas es sencillo por cada capa está bien definida, y la segmentación de la red para reducir el alcance de cada problema es fácil.
- *Predecibilidad* - el comportamiento es más predecible y se puede modelar para su análisis.
- *Soporte de protocolos* - la integración de protocolos y aplicaciones es sencillo porque la red está organizada lógicamente.
- *Gestionabilidad* - Por todo lo anterior es más fácil la gestión.

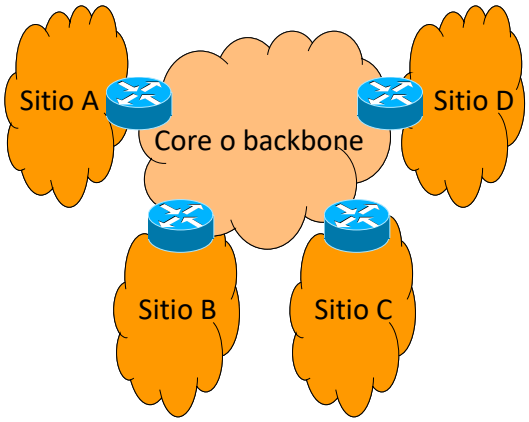
Topologías de redes IP

Backbone

Transporte optimizado entre sitios remotos:

- Caminos redundantes
- Balance de carga
- Rápida convergencia
- Uso eficiente del ancho de banda





Gestión de ancho de banda

- Colas de prioridad, ajuste del largo para evitar descartes
- Routing metrics, ajuste de cada ruta
- Terminación de sesiones locales, servicios de proxy

Optimización de trayectos

- Mejora de convergencia mediante temporizadores y parámetros ajustables
- Empleo de ancho de banda, carga, retardo, etc. para decisiones de ruteo

Priorización de trafico

- Selección de prioridad para cada tipo de trafico

Balance de carga

- Enlaces adicionales con reparto de carga gestionado por paquetes o por destinos
- Balance para trafico bridged (cada destino-un enlace serie evita tener que reordenar)

Caminos alternativos

- Por costos se emplea solo en caso de aplicaciones “mission-critical”
- Enlaces redundantes terminados en routers múltiples

Acceso PSTN

- empleo de conectividad WAN

Encapsulamiento (tunneling)

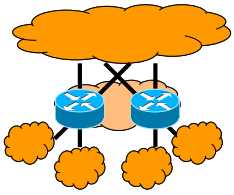
- paquetes de un sistema transportados por otro

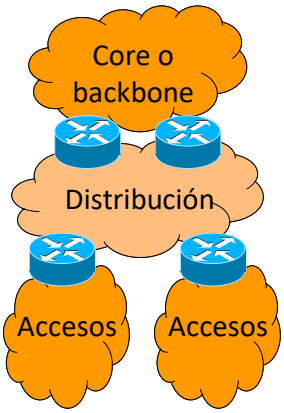
Topologías de redes IP

Distribución o Agregación

Conectividad basada en políticas:

- Control de acceso a los servicios
- Definición de métricas
- Control de publicaciones de rutas





Filtrado de áreas y servicios

- Empleo de "access lists" según dirección de red, protocolo y servicio

Políticas

- Regulación del acceso de grupos y protocolos al backbone
- Contención de broadcasts

Redistribución de información de routing

- Protocolos de routing de IP pueden intercambiar información
- Similarmente ISO IGRP e IS-IS

Traducción de protocolos

- Efectividad limitada en ciertos casos (Ethernet - Token Ring) por funcionalidades diferentes de cada red
- Traducción SDLLC (Token Ring/LLC2 a SNA/SDLC)

Servicio de gateway

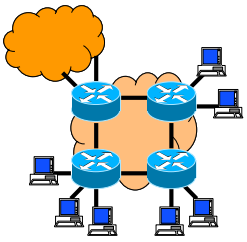
- Compatibilización de redes diversas

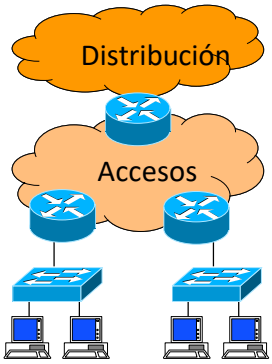
Topologías de redes IP

Accesos

Conexión de grupos de trabajo a backbones:

- Segmentación lógica
- Agrupamiento de usuarios según intereses
- Aislamiento de broadcasts
- Distribución de servicios
- Control de acceso de usuarios





Segmentación

- Implementación de subredes IP, áreas DECnet, etc., para disminuir congestión
- Contención de broadcasts

Capacidad de broadcast y multicast

- Routers pueden permitir el pasaje de broadcasts y multicasts
- Multicast requiere empleo de protocolos como IGRP y son preferibles a broadcasts

Servicios de nombres, proxy y cache local

- Respuestas locales a solicitudes de resolución de nombres (NetBIOS, DNS, etc.)
- Respuestas locales a exploradores Source Route y a pollings
- Respuestas locales a ARP

Seguridad de acceso

- Control de acceso al backbone
- Control de salida del backbone

Descubrimiento de routers

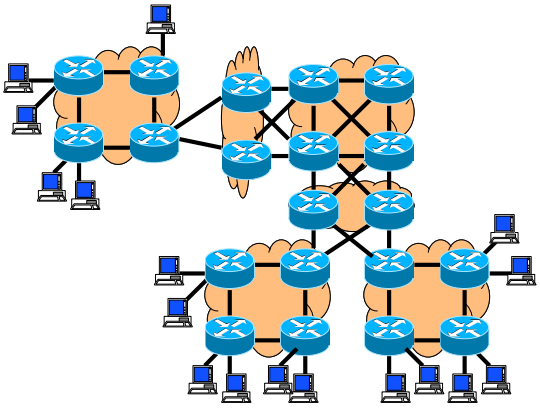
- soporte de protocolos de descubrimiento de routers para optimización de rutas (ES-IS, IRDP, Proxy ARP, RIP)

Direccionamiento con "helpers"

- Helper addressing y access lists permiten encaminar broadcasts a ciertos servidores

Topologías de redes IP

Ejemplo



Topologías de redes IP

Recomendaciones

- Cada capa del modelo jerárquico sirve para controlar broadcasts o acceso mediante listas
- No mallar las capas de distribución o de acceso
- No conectar hosts al backbone de modo de aumentar su confiabilidad, facilitar la gestión del tráfico y la planificación del crecimiento
- Los grupos de trabajo de las LANs deben tener “buen comportamiento” (regla 80/20), para lo cual se deben colocar los servidores en los grupos adecuados

Repaso de enrutamiento

- *Ruteo*: es el proceso de decidir cómo enviar un paquete de un lugar a otro.
- *Protocolo de ruteo*: Es un conjunto de reglas que gobiernan el intercambio de información entre routers que permita decir el envío de los paquetes por los mejores caminos.
- Los routers deben enviar paquetes provenientes de una interfaz de entrada a una interfaz de salida. El proceso se llama conmutación de paquetes.

9

Funciones principales

Los routers son dispositivos de capa 3. Extraen los paquetes de las tramas que reciben, deciden el encaminamiento de los mismos mediante el análisis de su cabecera y en particular de las direcciones lógicas, y los encapsulan en tramas para su envío. Las funciones principales son:

- *Enrutamiento (Routing)* - Aprendizaje de la topología lógica de la red. Cada dispositivo tiene direcciones lógicas que permiten que sean alcanzados individualmente en algunos casos y como parte de grupos en otros casos. Los routers entienden varios esquemas diferentes de direccionamiento y regularmente intercambian información topológica con los demás routers. La función de routing consiste en el aprendizaje y actualización de la topología de la red. Esa información de registra en una o varias tablas (tabla topológica, tabla de enrutamiento, etc.).
- *Conmutación (Switching o Forwarding)* - Recepción de paquetes que ingresan por una interfaz de entrada (inbound interface) y retrasmisión de los mismos por una interfaz de salida (outbound interface).

Para ejecutar el enrutamiento, el router efectúa tres análisis mayores:

- Interpretación del esquema de direccionamiento. Para decidir cómo proceder lo primero es ver si se es capaz de entender el direccionamiento lógico (TCP/IP, IPX, DEC, etc.).
- Búsqueda de un registro en la tabla de enrutamiento para la dirección lógica analizada. Si no se encuentra un registro que indique qué hacer con esa dirección, los routers descartan el paquete y pueden devolver un mensaje de error al origen (paquete ICMP). En general, la tabla de enrutamiento contiene entradas para diversas direcciones y una entrada adicional genérica (ruta por defecto o default) que se aplicará a todas las direcciones que no tienen una entrada específica.
- Una vez encontrada una coincidencia en la tabla (lo cual incluye el caso de una ruta por defecto), se debe elegir la interfaz de salida del paquete. Para ello se utiliza un mecanismo de ponderación de cada interfaz llamado esquema de métricas, que permite evaluarlas y seleccionar la más adecuada. Diversos parámetros se pueden aplicar para calcular la métrica: ancho de banda, retardo (delay), confiabilidad, peso administrativo (que puede representar cualquier variable que el administrador considere adecuada), etc. Una vez elegida la interfaz de salida, el router arma una trama para enviar el paquete al próximo dispositivo de la red (next-hop device).

Protocolos de enrutamiento y enrutables

- Protocolos enrutados: Son protocolos que se emplean para transmitir los datos de usuario. Ejemplos IP o IPX.
- Protocolos de enrutamiento: Son los que actualizan la información que permite encaminar los paquetes de los protocolos enrutados a través de la red. Entre estos protocolos tenemos IGRP, RIP, EIGRP, OSPF, IS-IS.

Tabla de ruteo

- *En función de la tabla de ruteo, se van a enviar los paquetes a su destino.*
- *La tabla de ruteo está compuesta por los campos red de destino, próximo salto y métrica*

```
r2>sho ip route
 10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O IA    10.0.0.2/32 [110/3] via 192.168.1.9, 00:01:04, FastEthernet1/0
C       10.0.0.3/32 is directly connected, Loopback0
O       10.0.0.1/32 [110/2] via 192.168.1.9, 00:01:04, FastEthernet1/0
B       10.0.100.0/24 [200/0] via 10.0.0.2, 00:00:16
S       10.0.200.0/24 [1/0] via 192.168.1.14
     192.168.1.0/30 is subnetted, 4 subnets
C       192.168.1.8 is directly connected, FastEthernet1/0
C       192.168.1.12 is directly connected, FastEthernet1/1
O IA    192.168.1.0 [110/3] via 192.168.1.9, 00:01:04, FastEthernet1/0
O       192.168.1.4 [110/2] via 192.168.1.9, 00:01:04, FastEthernet1/0
```

11

Información de enrutamiento

En la tabla de enrutamiento se encuentra la mayor parte de la información necesaria para decidir el enrutamiento de los paquetes. Cada entrada incluye:

Cómo fue aprendida la ruta. El método puede ser manual o dinámico (automático, mediante protocolo de enrutamiento).

Destino lógico expresado como red, subred o host.

Distancia administrativa, una medida de la confiabilidad del mecanismo de aprendizaje. Las rutas manuales son preferidas a las dinámicas. Los protocolos con métricas sofisticadas son preferidos a los protocolos con métricas simples.

Métrica, una medida del costo de la ruta. Si más de una interfaz tienen igual métrica es posible hacer balance de carga, es decir, repartir los paquetes entre ellas, enviando uno por vez por cada una (método de round-robin).

Dirección lógica del next-hop (próximo router) en el camino hacia el destino.

Antigüedad del registro de la entrada (aging). La información debe ser refrescada periódicamente para asegurar su actualización.

Interfaz por la cual se aprendió la ruta y por la cual saldrá el paquete hacia el next-hop.

Valores de distancia administrativa por defecto:

Origen de la ruta	Distancia administrativa por defecto
Interfaz conectada	0
Ruta estática hacia una interfaz	0
Ruta estática hacia next-hop	0
EIGRP summaries	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP v1, v2	120
EGP	140
External EIGRP	170
Internal BGP	200
Desconocido	255

Criterios de decisión

1- Ruta más específica

2- Distancia administrativa

3- Métrica

Enrutamiento

Algoritmo de decisión I

Algoritmo de selección de rutas

Se verá a continuación el algoritmo de decisión que permite seleccionar rutas para ingresarlas en la tabla de enrutamiento y elegir la mejor de acuerdo con los criterios usuales de enrutamiento.

Definiciones - Distancia Administrativa

La Distancia Administrativa es un valor numérico que indica la confiabilidad de la fuente de información (administrador o protocolo) por el cual se conoce la ruta. A menor distancia administrativa, mayor es la confiabilidad. Los routers normalmente tienen valores por defecto definidos previamente.

Distancia Administrativa

Interfaz directamente conectada 0
Ruta estática* 1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route 5
External Border Gateway Protocol (BGP) 20
Internal EIGRP 90
IGRP 100
OSPF 110
Intermediate System-to-Intermediate System (IS-IS) 115
Routing Information Protocol (RIP) 120
Exterior Gateway Protocol (EGP) 140
On Demand Routing (ODR) 160
External EIGRP 170
Internal BGP 200
Desconocida** 255

* Una ruta estática que apunta a la direccion de un next hop, tiene distancia administrativa 1. En cambio, si apunta a una interfaz de salida, tiene distancia administrativa 0.

** Si la distancia administrativa es 255, en router considera que la fuente de información no es creíble, y no instala la ruta en la tabla de enrutamiento.

Enrutamiento

Algoritmo de decisión II

Definiciones - Métrica

La métrica es un parámetro o conjunto de parámetros que permite evaluar la conveniencia de una ruta en relación con las demás rutas dirigidas a los mismos destinos. La métrica depende del protocolo.

Ejemplos:

En RIP, nº de routers que deben ser atravesados para alcanzar un destino (nº de hops).

En EIGRP, una combinación de varios parámetros (hasta 4) que en general se reducen a mínimo ancho de banda en el trayecto y mínimo retardo acumulado.

En OSPF, el costo, que normalmente se implementa como el menor ancho de banda en el trayecto.

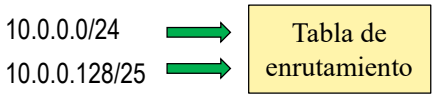
En BGP, un conjunto de parámetros que se aplican en un estricto orden de prioridades, de modo que se intenta evaluar con el primero, y si no es posible diferenciar las rutas por el mismo, se intenta con el segundo, y así sucesivamente.

Enrutamiento

Algoritmo de decisión III

Rutas a destinos diferentes

1- Rutas dirigidas a rangos de direcciones diferentes, aún cuando los rangos coincidan parcialmente, se consideran rutas a destinos diferentes. Ejemplo: 10.0.0.0 / 24 y 10.0.0.128 / 25 se consideran dirigidas a destinos diferentes, aún cuando el segundo rango está incluido en el primero. Todas las rutas diferentes se incluyen en la tabla de enrutamiento.



Si para un destino hay más de una ruta posible, con prefijos de diferente longitud, se prefiere la ruta de prefijo mayor (la más específica). Ejemplo: para alcanzar el destino 10.0.0.195, la ruta 10.0.0.128 / 25 es preferible a la ruta 10.0.0.0 / 24.

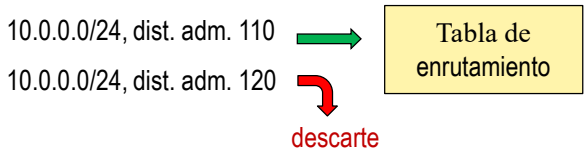
Enrutamiento

Algoritmo de decisión IV

Rutas a los mismos destinos

2- Si se reciben dos o más rutas dirigidas a los mismos destinos (exactamente al mismo rango de direcciones), se sigue el siguiente algoritmo de selección:

a) Se analiza la Distancia Administrativa, o confiabilidad de la fuente de información (administrador o protocolo de enrutamiento). Si hay una ruta con menor Distancia Administrativa que las demás, se elige dicha ruta.

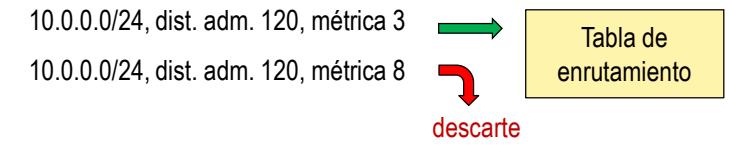


Enrutamiento

Algoritmo de decisión IV

Rutas a los mismos destinos

b) Si la Distancia Administrativa no permite decidir (más de una ruta con el menor valor de dicho parámetro), se analiza la métrica de las rutas. Si hay una ruta con menor métrica que las demás, se elige dicha ruta.



Enrutamiento

Algoritmo de decisión IV

Rutas a los mismos destinos

c) Si la métrica no permite decidir (más de una ruta con el mismo valor de dicho parámetro), según el protocolo que se emplee, en general se incluyen varias de las rutas de igual métrica (normalmente hasta 6), para utilizarlas en lo que se llama "balance de carga".

El balance de carga consiste en utilizar las rutas en forma alternada.

Criterios de decisión - Ejemplo

Se quiere encaminar paquetes IP con destino la IP: **192.168.70.190**

Y se reciben las siguientes rutas:

Ruta	Distancia Adm.	Métrica
192.168.0.0/16	90	6540
192.168.0.0/16	100	2345
192.168.0.0/17	110	6590
192.168.0.0/17	90	8796
192.168.0.0/18	100	7896
192.168.0.0/18	110	2341

¿Qué ruta se utilizará?

Criterios de decisión - Ejercicio

Un router recibe las rutas:

Destinos	Métrica	Dist. Administrativa	Next hop
172.16.0.0/18	2543	120	20.0.0.1
172.16.128.0/18	3665	90	20.0.0.2
172.16.0.0/16	2345	110	20.0.0.3
172.16.0.0/16	7643	110	20.0.0.4
0.0.0.0/0	9483	90	20.0.0.5

Debe encaminar paquetes IP a la dirección 172.16.193.1, por lo cual enviará todos los paquetes al next hop:

1)20.0.0.1
2)20.0.0.2
3)20.0.0.3
4)20.0.0.4

Distancia Administrativa

Ruta	Distancia Administrativa
Directamente conectada	0
Ruta estática a interface de salida	0
Ruta estática al *next hop*	1
EIGRP *summary route*	5
BGP externo	20
EIGRP interno	90
OSPF	110
RIP V1, V2	120
EIGRP externo	170
BGP interno	200

Enrutamiento estático

El administrador ingresa las rutas manualmente a diferencia del dinámico donde las rutas y los cambios topológicos se agregan automáticamente.

Router (config) # ip route network mask {address | interface}
[distance] [permanent]

*Comando **ip route***	*Descripción*
network	Dirección IP destino
mask	Máscara
address	Dirección IP del próximo salto
interface	Nombre de la interfaz de salida que será usada para alcanzar el destino
distance	Distancia administrativa
permanent	Especifica que la ruta no se quitará aún cuando caiga la interfaz de salida

22

Rutas estáticas

Son configuradas manualmente por el administrador de la red.

Son útiles en redes pequeñas, y en los casos como el de la figura en el cual hay un solo camino para alcanzar la red stub (red que tiene una sola salida).

Ejemplo:

ip route 192.168.3.0 255.255.255.0 192.54.2.1

ip route - identifica el comando de ruta estática

192.54.2.0 - dirección del rango

255.255.255..0 - máscara (en conjunto con una dirección del rango permite especificar el rango completo de direcciones)

192.54.2.1 - dirección ip del próximo salto (next-hop) en el camino al destino

Protocolo Classful

No intercambia la máscara en la información de ruteo

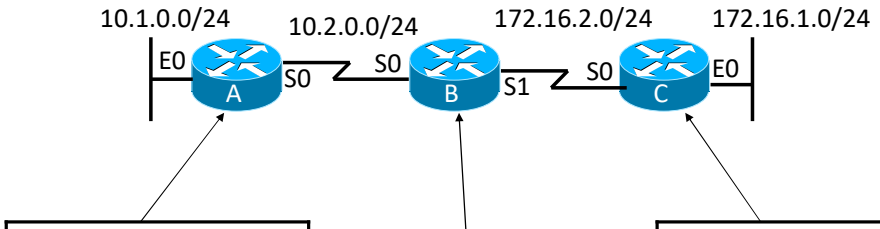


Tabla de ruteo de A		
10.1.0.0	E0	0
10.2.0.0	S0	0
172.16.0.0	S0	2

Tabla de ruteo de B		
10.0.0.0	S0	1
10.2.0.0	S0	0
172.16.2.0	S1	0
172.16.0.0	S1	1

Tabla de ruteo de C		
10.0.0.0	S0	2
172.16.2.0	S0	0
172.16.1.0	E0	0

23

Classful

Los protocolos Classful no transportan la máscara de red por lo cual las rutas no pueden viajar en forma más específica que la clase a la cual pertenecen. Ejemplos: RIP v1, IGRP.

Al hacer subredes, todas las interfaces de los routers y todas las subredes deben tener la misma máscara. Cuando se intercambian rutas con redes distintas (con prefijos diferentes al local), la información de subredes no puede propagarse, porque se desconoce la máscara de las subredes de esa otra red. En consecuencia, las rutas se sumarizan en la frontera de las redes en forma automática por parte de los protocolos classful.

Notar que

- El router A aprende la 172.16.0.0 pero no aprende la 172.16.2.0/24 y la 172.16.2.0/24
- El router C aprende la 10.0.0.0 pero no aprende la 10.2.0.0/24 y la 10.1.0.0/24

Protocolo Classless

Intercambia la máscara en la información de ruteo

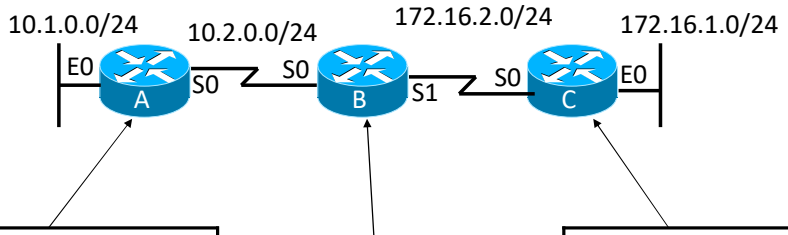


Tabla de ruteo de A		
10.1.0.0	E0	0
10.2.0.0	S0	0
172.16.2.0	S0	1
172.16.1.0	S0	2

Tabla de ruteo de B		
10.1.0.0	S0	1
10.2.0.0	S0	0
172.16.2.0	S1	0
172.16.1.0	S1	1

Tabla de ruteo de C		
10.1.0.0	S0	2
10.2.0.0	S0	1
172.16.2.0	S0	0
172.16.1.0	E0	0

24

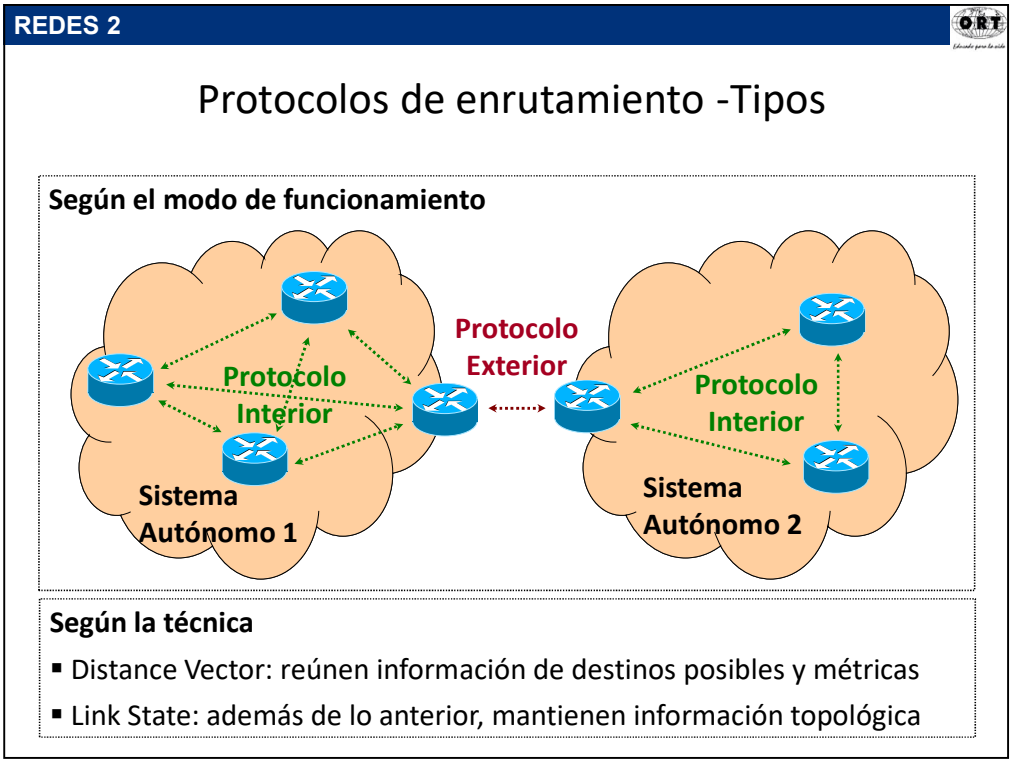
Classless

En el caso de los protocolos classless cada anuncio porta la máscara correspondiente.

Adicionalmente, no requieren que las máscaras de las diferentes subredes sean la misma, permitiendo el funcionamiento en modo Variable Length Subnet Mask (VLSM).

Ejemplos: RIP v2, EIGRP, OSPF, IS-IS, BGP.

En este caso sí se aprenden las rutas que antes no se aprendian



Tipos de protocolos

Según el modo de funcionamiento

- *End System-End System* - Se incluyen protocolos como IP, IPX, CLNP, DECnet Phase IV y V, AppleTalk, Xerox Network System, Banyan,etc. Corresponden a los protocolos ruteados.
- *End System-Intermediate System* - Protocolos que comunican DTE con router, y publican las tablas de direcciones del DTE.
- *Intermediate System-Intermediate System* - Efectúan el enrutamiento, publican tablas de los routers y optimizan rutas. Pueden clasificarse en:
    - *Protocolos interiores (Intra Domain)* - Procuran el intercambio de información detallada en un ámbito llamado *sistema autónomo o dominio de enrutamiento*, a los efectos de seleccionar rutas óptimas.
    - *Protocolos exteriores (Inter Domain)* - Permiten el intercambio de información de accesibilidad entre sistemas autónomos. El volumen de información es más reducido que en el caso anterior, lo cual tiene dos consecuencias, por un lado las decisiones pueden no ser óptimas, pero por otro lado, hacen tolerable el tráfico de información de enrutamiento generado.

Según la técnica

- Distance Vector- corresponden a la primera generación de protocolos, son aptos para redes pequeñas y medianas.
- Link State – corresponden a la segunda generación, se desempeñan bien en redes medianas y grandes.

Convergencia

- La rapidez para reconfigurar la red una vez que hay una modificación, se llama velocidad de convergencia. Para ello, algunos protocolos emplean técnicas especiales como guardar las tablas de los vecinos para recalcular todas la rutas inmediatamente que se conoce un cambio.

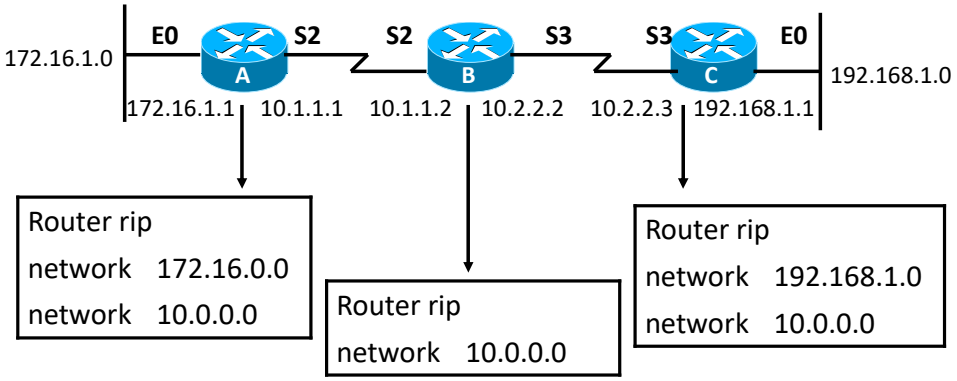
Convergencia

- Es la etapa en la cual los routers de una red actualizan la información de enrutamiento de la misma, luego de cambios tales como:
  - Nueva ruta
  - Cambio de estado de una ruta existente
- El tiempo de convergencia es afectado por:
  - Mecanismos de actualización (como temporizadores de hold-down)
  - Tamaño de la tabla topológica
  - Algoritmo utilizado para el recálculo
  - Tipo de medio

RIP

- Es un protocolo de vector distancia
- Los saltos son usados como métrica para seleccionar un camino
- Máximo de saltos (hop) 15
- Las *updates* (actualizaciones) son periódicas cada 30 segundos
- Es capaz de balancear tráfico entre 6 caminos de igual métrica
- RIPv1 (*classful routing protocol*) no envía la máscara en los *updates*
- RIPv2 (*classless routing protocol*) envía la máscara

Configuración de RIP



- Router(config)# router rip
- Router(config-router) # network network-number

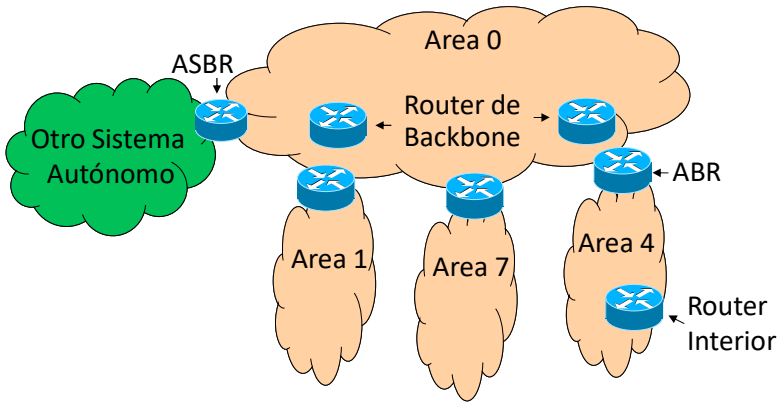
Fuente: Curso BSCI de Cisco Systems

28

Características de OSPF

- Protocolo de estado de enlace
- Rápida convergencia
- Soporta máscara de subred con longitud variable (VLSM)
- Procesa actualizaciones eficientemente
- Soporta redes grandes
- Como métrica utiliza el ancho de banda (BW)
- Soporta múltiples caminos de igual métrica

Arquitectura de redes con OSPF



Terminología de OSPF

- Neighbors (vecinos): Dos routers que tienen interfaces sobre una red común
- Link state (estado de enlace): Es el estado de un enlace entre dos routers vecinos. El *link state* es anunciado por los routers en un paquete especial llamado anuncio *Link State* (LSA)
- Costo: Es el valor asignado a un link
- Sistema Autónomo: Está formado por un grupo de routers que intercambian información de ruteo por medio de un protocolo de ruteo común
- Área: Un grupo de routers y redes que tienen la misma identificación de área. Cada router dentro de un área tiene la misma información del estado de los enlaces (link-state)

31

Fuente: Curso BSCI 642-801 de Cisco Systems

Terminología de OSPF

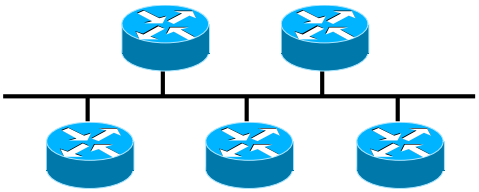
- Hello: Paquetes usados por OSPF para establecer y mantener la relación entre sus vecinos
- Neighborship database: Es una lista de todos sus vecinos con los cuales un router ha establecido comunicación bidireccional
- Link-state database: También conocida como tabla topológica. Contiene los estados de los enlaces de todos los routers en la red. Ésta nos muestra la topología de la red. Todos los routers dentro de un área tienen idénticas link-state databases. Esta base es armada con los LSA generados por todos los routers de una red.
- Tabla de ruteo: Es generada cuando el Algoritmo SPF (shortest path first) es ejecutado sobre la tabla topológica. Cada tabla de ruteo es propia de cada router

32

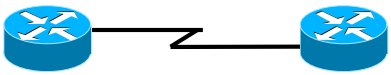
Fuente: Curso BSCI 642-801 de Cisco Systems

Topologías de OSPF

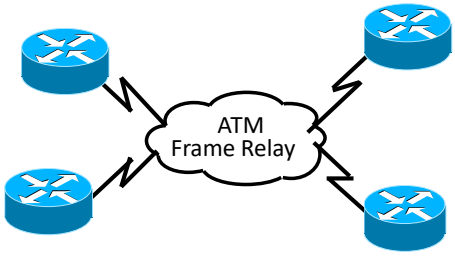
Topología de broadcast multiacceso



Topología punto a punto



Topología de multiacceso no broadcast (NBMA)



33

Fuente: Curso BSCI 642-801 de Cisco Systems

Contenido de los paquetes de Hello

- Router ID: Es un número de 32 bit único que identifica cada router dentro del sistema autónomo. La dirección IP más alta de las interfaces activas dentro de un router es la escogida por defecto (Este valor puede modificarse creando una interface de loopback). Esta identificación también es usada cuando se designan los routers DR (router designado) y BDR (backup del router designado).
- Intervalos Hello y dead: Por defecto los *hello* son cada 10 segundos y el intervalo de *dead* es de cuatro *hello* no escuchados.
- Neighbors: Los vecinos con los cuales se ha establecido comunicación bidireccional.
- Área ID: Para que dos routers se comuniquen deben poseer un segmento en común y las respectivas interfaces en el segmento deben pertenecer a la misma área.

Contenido de los paquetes de Hello

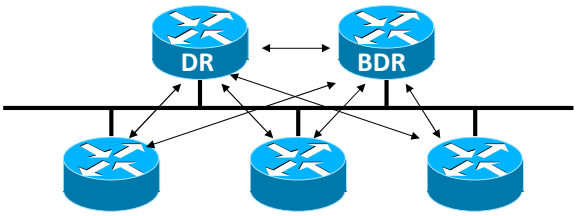
- Prioridad de router: Es un número de 8 bits que indica la prioridad de un router para ser designado como DR o BDR.
- Dirección IP de DR y BDR: Si se conocen estas IP serán especificadas para cada red.
- Password de autenticación: Si está habilitada, todos los routers pares deben tener la misma password de autenticación.
- Bandera de área *Stub*: Dos routers deben estar de acuerdo sobre la bandera de área *stub* en los paquetes de *hello*. Un área es stub si tiene sólo una vía de acceso al backbone.

Métrica de las interfaces

Tipo de interfaz	Ancho de banda en bits/segundo	Ancho de banda en bytes/segundo	Costo de Interfaz de OSPF
Ethernet	1G	128M	1
Ethernet	100M	12.5M	10
Ethernet	10M	1.25M	100
Módem	2M	256K	500
Módem	1M	128K	1000
Módem	500K	62.5K	2000
Módem	250K	31.25K	4000
Módem	125K	15625	8000
Módem	62500	7812	16000

Designated Router y Backup Designated Router

Sólo para lan

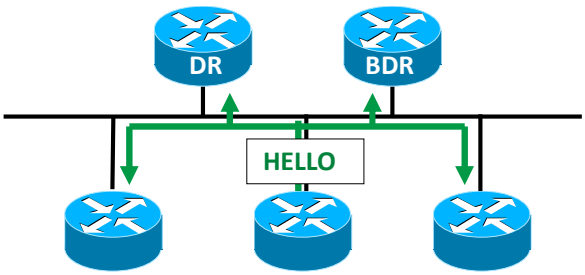


- Los paquetes de *Hello* son los empleados para elegir un Designated Router (DR) y un Backup Designated Router (BDR) para cada segmento.
- Cada router establece una adyacencia con el DR y BDR e intercambiará información de estado de enlaces sólo con ellos.
- Esto reduce tráfico de ruteo: El DR y BDR actúan como punto central de contacto para intercambiar información de estado de enlaces.
- Se logra la sincronización de estado de enlace: cada DR y BDR se asegura que los otros routers sobre la red tienen la misma información sobre el estado de la red.
- El BDR solo actuará si el DR falla.

37

Fuente: Curso BSCI 642-801 de Cisco Systems

Elección del DR y del BDR

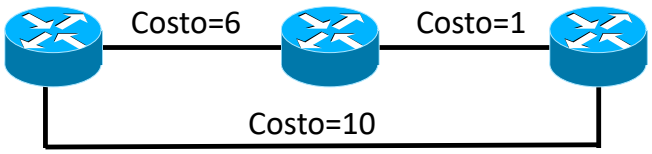


- El router con mayor valor de prioridad es el DR.
- El que contenga el segundo valor de prioridad es el BDR
- La prioridad por defecto es 1. En caso de igual prioridad la ID de router es usada.
- Un router con prioridad 0 no puede ser elegido como DR o BDR
- Si posteriormente un router con más alta prioridad entra a la red el DR y BDR no serán cambiados; sólo cambiarán si alguno cae.
- Para determinar si el DR esta caído, el BDR prende un temporizador el cual terminado, BDR asumirá la función de retransmisor de LSAs del DR.

38

Fuente: Curso BSCI 642-801 de Cisco Systems

Elección de rutas

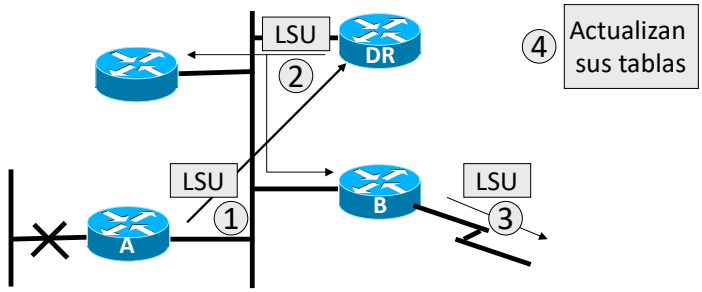


- Cuando un router tiene completa la *link-state database*, está listo para crear su tabla de ruteo y rutear tráfico.
- En los routers Cisco la métrica utilizada es el BW.
- Para calcular el menor costo a un destino, el protocolo *link-state* utiliza el algoritmo de Dijkstra. Usando como entrada la *link-state database*, el algoritmo de Dijkstra construye la tabla de ruteo paso a paso (esta tabla será única para cada router).
- Para minimizar los problemas de intermitencia (flapeo) de rutas cada vez que una LSU es recibida, el router espera un período antes de recalcular su tabla de ruteo (por defecto 5 segundos).

39

Fuente: Curso BSCI 642-801 de Cisco Systems

Actualización de la información de ruteo

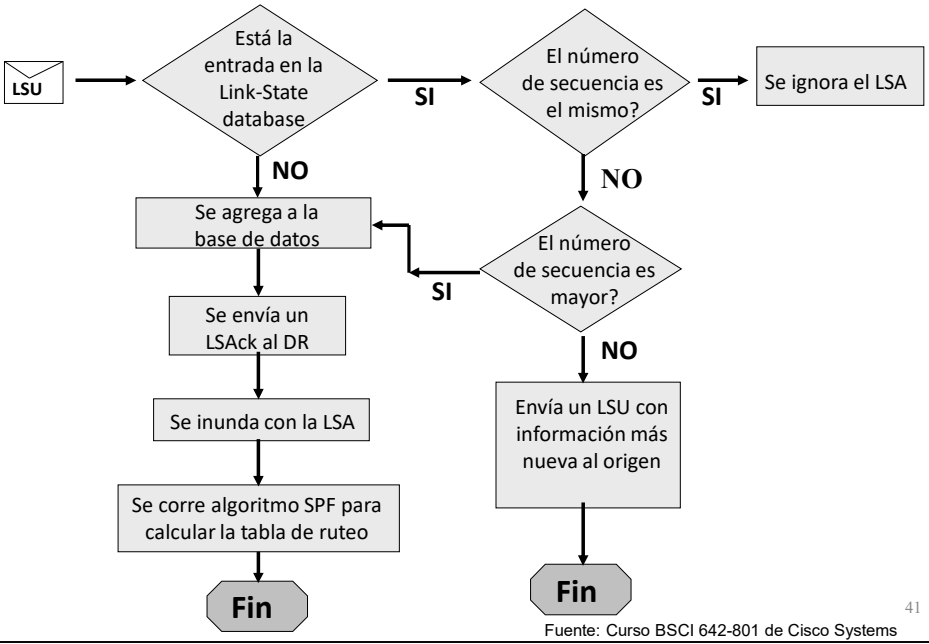


- Router A detecta el cambio y envía un paquete LSU incluyendo el LSA actualizado (lo envía a la 224.0.0.6 es decir al DR y BDR)
- El DR manda un acuse de recibo al router A. Y luego envía el LSU por medio de multicast (224.0.0.5) a los otros vecinos de la ethernet. Estos últimos acusarán también el recibo.
- Si uno de los routers que recibe el LSU está conectado a otra red, éste tendrá a su vez que reenviar el LSU por sus otras interfaces (router B).
- Cada router que recibe el LSU actualizará su base link-state y luego de los 5s correrá el algoritmo SPF recalculando su tabla de ruteo.

40

Fuente: Curso BSCI 642-801 de Cisco Systems

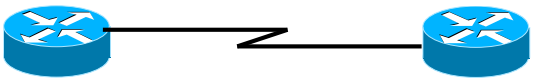
Actualización de la información de ruteo



41

Fuente: Curso BSCI 642-801 de Cisco Systems

Vecinos con enlaces punto a punto

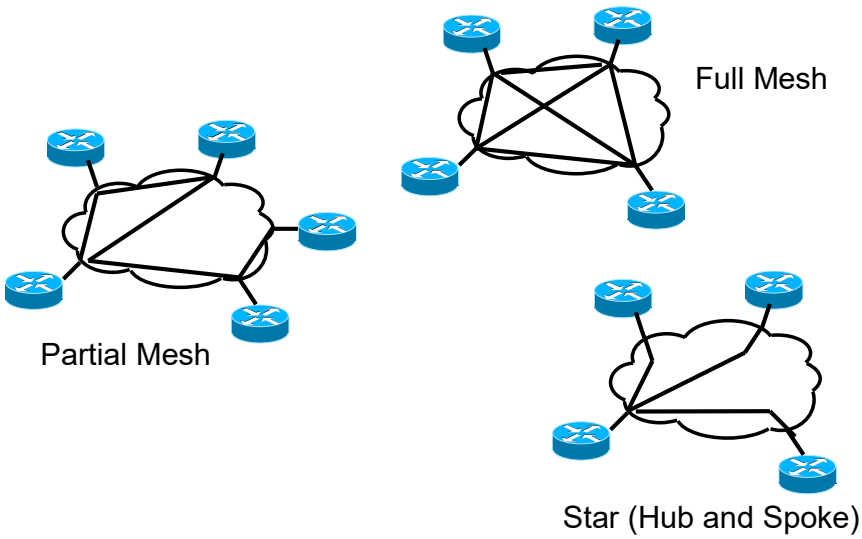


- Los routers detectan dinámicamente sus vecinos por medio de paquetes de Hello
- Las adyacencias son automáticas
- Los paquetes de OSPF son siempre enviados como multicast (224.0.0.5)

42

Fuente: Curso BSCI 642-801 de Cisco Systems

Topologías Non Broadcast Multiple Access (NBMA)



43

Fuente: Curso BSCI 642-801 de Cisco Systems

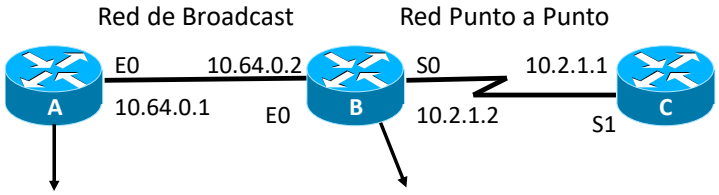
Modos de operación en topologías NBMA

- Multiacceso no broadcast (NMBA)
  - En este modo de operación OSPF simula un medio de broadcast. Aquí los routers intercambian actualizaciones con sus vecinos y eligen un DR y un BDR.
  - Este modo es usado particularmente en redes fully-meshed
- Punto a multipunto
  - Aquí los enlaces se tratan como una colección de enlaces punto a punto.
  - Esto puede ser usado en redes fully-meshed o partially-meshed

44

Fuente: Curso BSCI 642-801 de Cisco Systems

Configuración en routers internos




```
Interface Ethernet0
ip address 10.64.0.1 255.255.255.0
!
router ospf 1
network 10.64.0.0   0.0.0.255 area 0
```

```
Interface Ethernet0
ip address 10.64.0.2 255.255.255.0
!
Interface Serial0
ip address 10.2.1.2 255.255.255.0
!
router ospf 1
network 10.2.1.0   0.0.0.255 area 0
network 10.64.0.0   0.0.0.255 area 0
```

45

Fuente: Curso BSCI 642-801 de Cisco Systems

Configuración opcional

Router ID:
router (config)# interface loopback <number>
router (config-if)# ip address 172.16.1.1 255.255.255.255

Prioridad del router:
router (config-if)# ip ospf priority <number> (del 0 al 255))

Costo de interfaz de salida:
router (config-if)# ip ospf cost <cost> (de 1 65535)

Configuración en NBMA

Para modo non.broadcast
router (config)# interface Serial0
router (config-if)# ip address 10.1.1.1 255.255.255.0
router (config-if)#encapsulation frame-relay
router (config-if)#ip ospf network non-broadcast
router (config)# router ospf 1
router (config-router)#network 10.1.1.0 0.0.0.255 area0
router (config-router)#neighbor 10.1.1.2
router (config-router)#neighbor 10.1.1.3
router (config-router)#neighbor 10.1.1.4

Para modo point-to-multipoint
router (config-if)#ip ospf network point-to-multipoint
Y no se configuran los neighbors

47

Fuente: Curso BSCI 642-801 de Cisco Systems

Verificación del funcionamiento

show ip protocols (Verifica que OSPF está configurado)

show ip route (Muestra todas las rutas aprendidas por el router)

show ip ospf interface (Muestra ID de área e información de adyacencias)

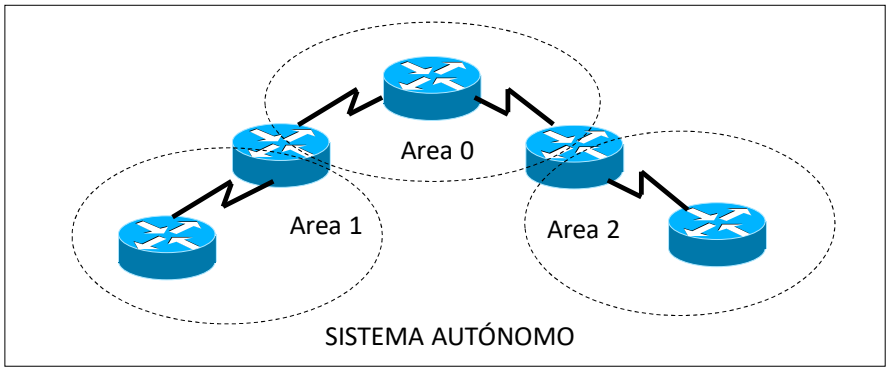
show ip ospf (Muestra temporizadores de OSPF y estadísticas)

show ip ospf neighbor detail (Muestra información de DR, BDR y vecinos)

show ip ospf database (Muestra la link-state base de datos)

Fuente: Curso BSCI 642-801 de Cisco Systems

Ruteo jerárquico (múltiples áreas)



- Consiste en áreas interconectadas por el área 0
- Minimiza el tráfico por actualizaciones de ruteo
- Reduce la frecuencia de recálculos de SPF (se calcula por área)
- Reduce la tabla de ruteo (resúmenes de rutas entre áreas)

49

Fuente: Curso BSCI 642-801 de Cisco Systems

Tipos de routers en OSPF

Routers internos: Son los routers que tienen todas sus interfaces en una misma área (estos tienen idéntica database y una sola copia del algoritmo de ruteo).

Routers de backbone: Estos routers tienen al menos una interfaz en el área 0. Mantienen información de ruteo de la misma forma que los internos.

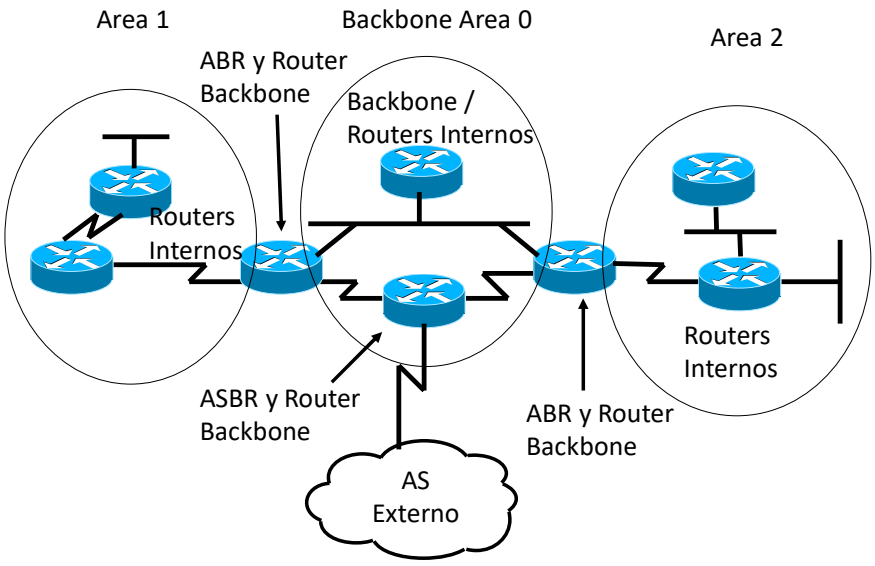
Routers de área borde (ABR): Son los que tienen interfaces en distintas áreas. Estos mantienen link-state databases para cada área a la que está conectado. Este rutea tráfico entre áreas. ABR es el encargado de resumir información de rutas y enviarla dentro del backbone.

Router de límite de AS (ASBR): Routers que tienen al menos una interfaz dentro de una red externa.

50

Fuente: Curso BSCI 642-801 de Cisco Systems

Tipos de routers en OSPF



51

Fuente: Curso BSCI 642-801 de Cisco Systems

Tipos de anuncios de estado de enlace (LSA)

- Tipo 1: Router link entry (se propagan sólo dentro de un área). Contienen información del estado de los enlaces que se encuentran en el área.
- Tipo 2: Network link entry (se propagan sólo dentro de un área). Son enviados por el DR y contienen cuales son sus vecindades.
- Tipo 3 y 4: Summary link entry (se propagan inter áreas). Los LSA tipo 3 contienen un resumen de todas las redes, y los tipo 4 se envía desde el ABR al ASBR indicando el costo desde el ABR al ASBR
- Tipo 5: AS external link entry (rutas externas). Contienen información de rutas inyectadas desde otro AS.

52

Fuente: Curso BSCI 642-801 de Cisco Systems

OSPF
Anuncios (Link State Advertisements)

Tipos de anuncios

Tipo 1: todo router los genera acerca de sus links. Se propagan sólo dentro de la misma área donde se generan.

Tipo 2: los origina el DR acerca de él y de todos los routers conectados a él. Se propagan sólo dentro de la misma área donde se generan.

Tipos de anuncios

Tipo 1: todo router los genera acerca de sus links. Se propagan sólo dentro de la misma área donde se generan.

Tipo 2: los origina el DR acerca de él y de todos los routers conectados a él. Se propagan sólo dentro de la misma área donde se generan.

Tipo 3: los origina un ABR, y los envía a un área conectada a él (puede ser el backbone) para informar sobre destinos fuera del área. Puede ser una ruta default siempre que sea interna al sistema autónomo. Se propagan entre diferentes áreas comunes (áreas no stub ni totally stubby).

Tipo 4: ídem al 3, pero el destino anunciado no es una red sino un ASBR. Se propagan entre diferentes áreas comunes.

Tipo 5: los origina un ASBR acerca de rutas externas al sistema autónomo. Se propagan entre diferentes áreas comunes.

Tipo 6: exclusivos de Multicast OSPF (MOSPF), anuncia destinos de clase D.

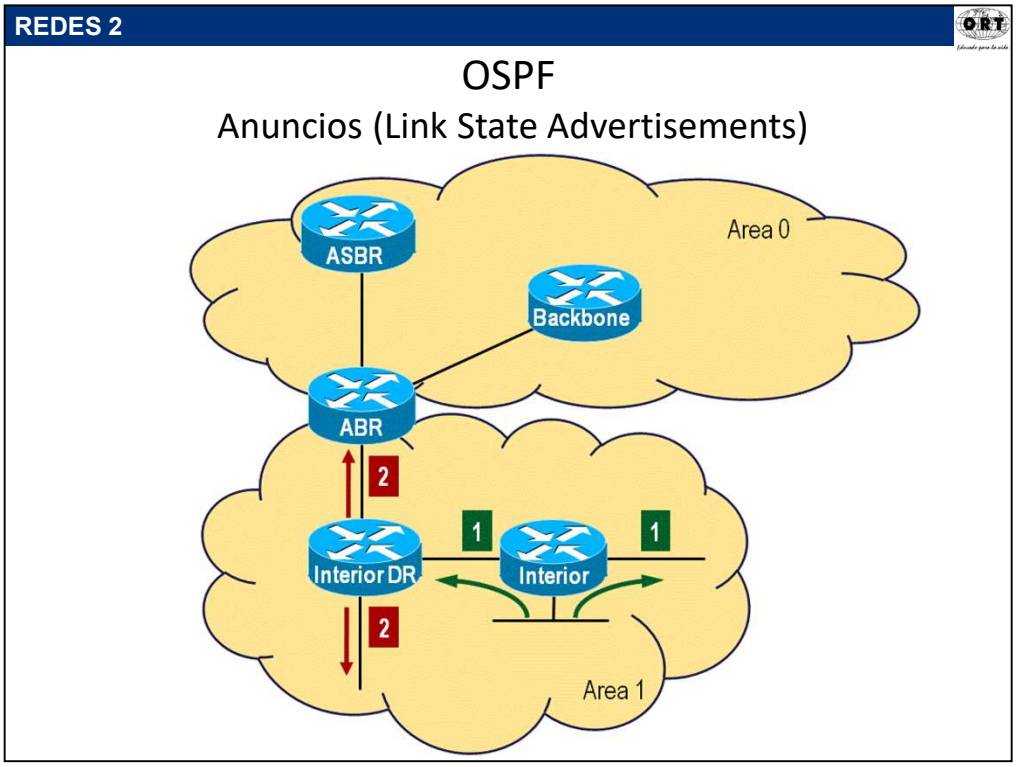
Tipo 7: originados por un ASBR en un área no tan stubby (No So Stubby Area, NSSA) y se propagan sólo en el NSSA en que se originan.

Tipo 8: permiten transportar información de BGP a través de un dominio OSPF.

Tipo 9: LSA con cabecera estándar y con contenido específico de una aplicación, con el fin de propagar información de dicha aplicación a través del dominio ospf. Tiene alcance local en el enlace.

Tipo 10: ídem al 9, pero el alcance se extiende a toda el área.

Tipo 11: ídem al 9, pero el alcance se extiende a todo el dominio ospf.



Tipos de anuncios

Tipo 1: todo router los genera acerca de sus links. Se propagan sólo dentro de la misma área donde se generan.

Tipo 2: los origina el DR acerca de él y de todos los routers conectados a él. Se propagan sólo dentro de la misma área donde se generan.

Tipo 3: los origina un ABR, y los envía a un área conectada a él (puede ser el backbone) para informar sobre destinos fuera del área. Puede ser una ruta default siempre que sea interna al sistema autónomo. Se propagan entre diferentes áreas comunes (áreas no stub ni totally stubby).

Tipo 4: ídem al 3, pero el destino anunciado no es una red sino un ASBR. Se propagan entre diferentes áreas comunes.

Tipo 5: los origina un ASBR acerca de rutas externas al sistema autónomo. Se propagan entre diferentes áreas comunes.

Tipo 6: exclusivos de Multicast OSPF (MOSPF), anuncia destinos de clase D.

Tipo 7: originados por un ASBR en un área no tan stubby (No So Stubby Area, NSSA) y se propagan sólo en el NSSA en que se originan.

Tipo 8: permiten transportar información de BGP a través de un dominio OSPF.

Tipo 9: LSA con cabecera estándar y con contenido específico de una aplicación, con el fin de propagar información de dicha aplicación a través del dominio ospf. Tiene alcance local en el enlace.

Tipo 10: ídem al 9, pero el alcance se extiende a toda el área.

Tipo 11: ídem al 9, pero el alcance se extiende a todo el dominio ospf.

OSPF
Anuncios (Link State Advertisements)

Tipos de anuncios

Tipo 3: los origina un ABR, y los envía a un área conectada a él (puede ser el backbone) para informar sobre destinos fuera del área. Puede ser una ruta default siempre que sea interna al sistema autónomo. Se propagan entre diferentes áreas comunes (áreas no stub ni totally stubby).

Tipo 4: ídem al 3, pero el destino anunciado no es una red sino un ASBR. Se propagan entre diferentes áreas comunes.

Tipo 5: los origina un ASBR acerca de rutas externas al sistema autónomo. Se propagan entre diferentes áreas comunes.

Tipos de anuncios

Tipo 1: todo router los genera acerca de sus links. Se propagan sólo dentro de la misma área donde se generan.

Tipo 2: los origina el DR acerca de él y de todos los routers conectados a él. Se propagan sólo dentro de la misma área donde se generan.

Tipo 3: los origina un ABR, y los envía a un área conectada a él (puede ser el backbone) para informar sobre destinos fuera del área. Puede ser una ruta default siempre que sea interna al sistema autónomo. Se propagan entre diferentes áreas comunes (áreas no stub ni totally stubby).

Tipo 4: ídem al 3, pero el destino anunciado no es una red sino un ASBR. Se propagan entre diferentes áreas comunes.

Tipo 5: los origina un ASBR acerca de rutas externas al sistema autónomo. Se propagan entre diferentes áreas comunes.

Tipo 6: exclusivos de Multicast OSPF (MOSPF), anuncia destinos de clase D.

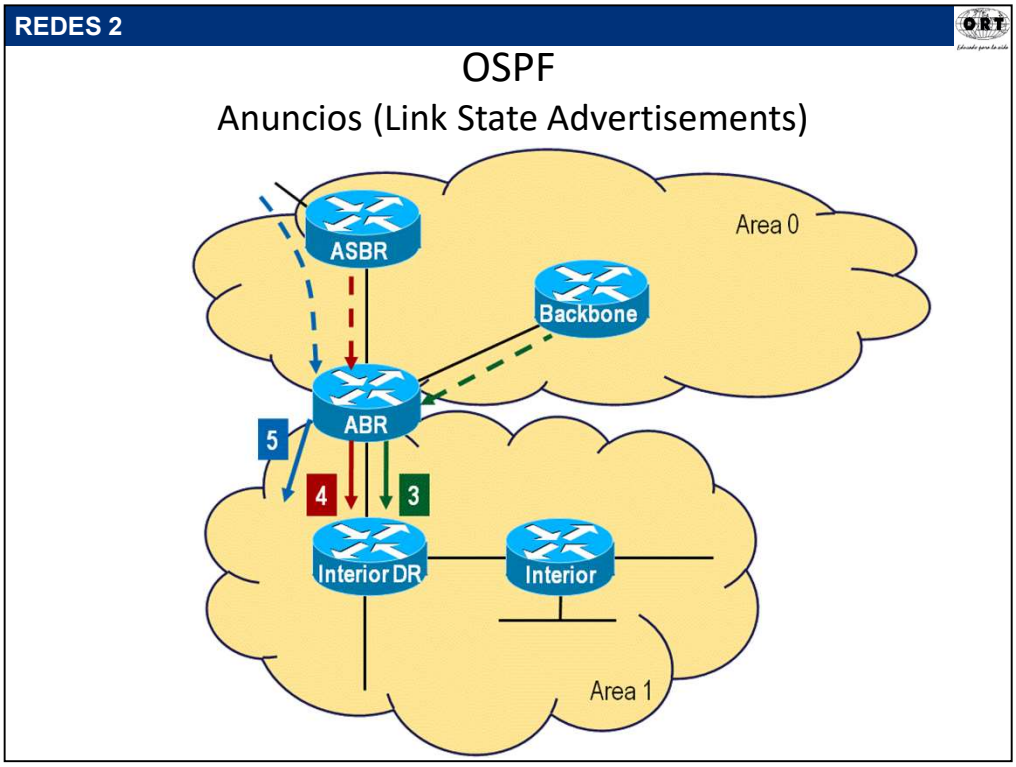
Tipo 7: originados por un ASBR en un área no tan stubby (No So Stubby Area, NSSA) y se propagan sólo en el NSSA en que se originan.

Tipo 8: permiten transportar información de BGP a través de un dominio OSPF.

Tipo 9: LSA con cabecera estándar y con contenido específico de una aplicación, con el fin de propagar información de dicha aplicación a través del dominio ospf. Tiene alcance local en el enlace.

Tipo 10: ídem al 9, pero el alcance se extiende a toda el área.

Tipo 11: ídem al 9, pero el alcance se extiende a todo el dominio ospf.



Tipos de anuncios

Tipo 1: todo router los genera acerca de sus links. Se propagan sólo dentro de la misma área donde se generan.

Tipo 2: los origina el DR acerca de él y de todos los routers conectados a él. Se propagan sólo dentro de la misma área donde se generan.

Tipo 3: los origina un ABR, y los envía a un área conectada a él (puede ser el backbone) para informar sobre destinos fuera del área. Puede ser una ruta default siempre que sea interna al sistema autónomo. Se propagan entre diferentes áreas comunes (áreas no stub ni totally stubby).

Tipo 4: ídem al 3, pero el destino anunciado no es una red sino un ASBR. Se propagan entre diferentes áreas comunes.

Tipo 5: los origina un ASBR acerca de rutas externas al sistema autónomo. Se propagan entre diferentes áreas comunes.

Tipo 6: exclusivos de Multicast OSPF (MOSPF), anuncia destinos de clase D.

Tipo 7: originados por un ASBR en un área no tan stubby (No So Stubby Area, NSSA) y se propagan sólo en el NSSA en que se originan.

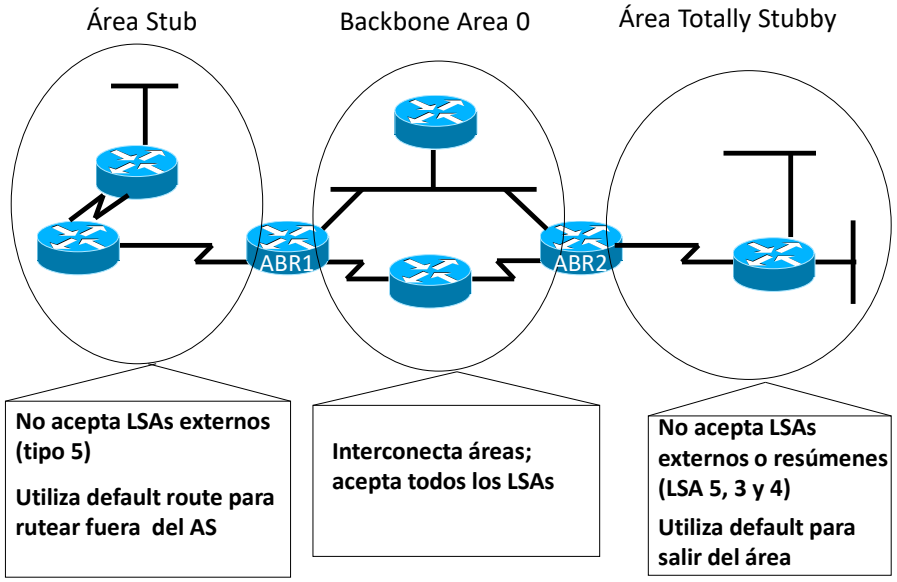
Tipo 8: permiten transportar información de BGP a través de un dominio OSPF.

Tipo 9: LSA con cabecera estándar y con contenido específico de una aplicación, con el fin de propagar información de dicha aplicación a través del dominio ospf. Tiene alcance local en el enlace.

Tipo 10: ídem al 9, pero el alcance se extiende a toda el área.

Tipo 11: ídem al 9, pero el alcance se extiende a todo el dominio ospf.

Tipos de áreas



No acepta LSAs externos (tipo 5)

Utiliza default route para rutear fuera del AS

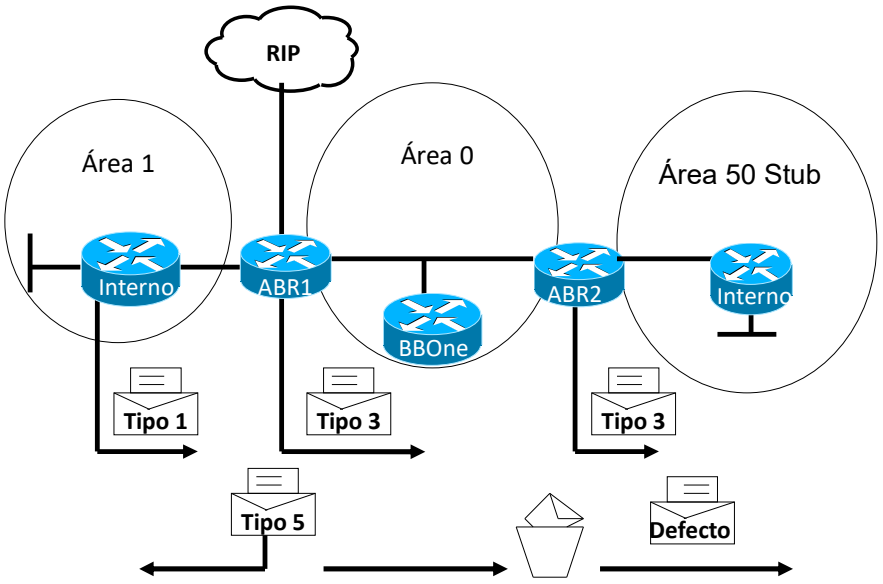
Interconecta áreas; acepta todos los LSAs

No acepta LSAs externos o resúmenes (LSA 5, 3 y 4)

Utiliza default para salir del área

Fuente: Curso BSCI 642-801 de Cisco Systems

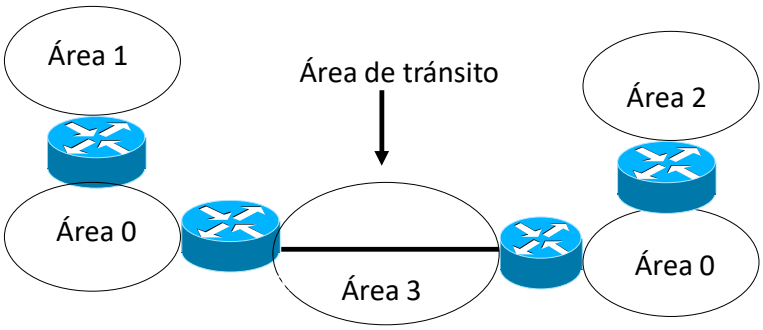
Inundación de LSUs a múltiples áreas



58

Fuente: Curso BSCI 642-801 de Cisco Systems

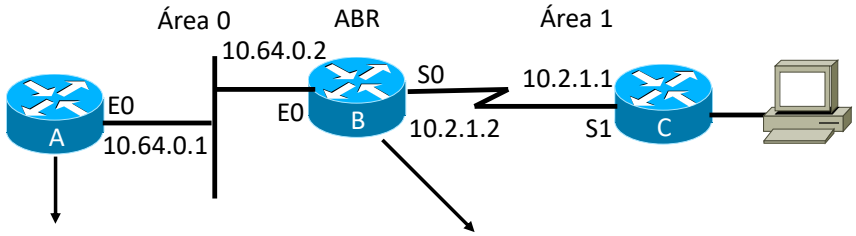
Conexión de dos áreas de backbone



Los enlaces virtuales proveen un camino para llegar al backbone o interconectar backbones separados

Fuente: Curso BSCI 642-801 de Cisco Systems

Configuración de ABR



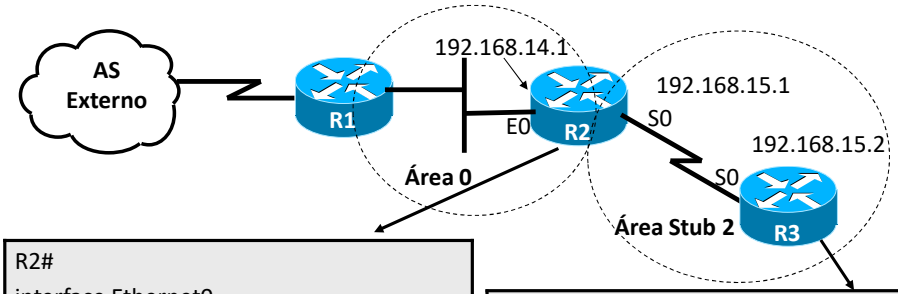

```
Interface Ethernet0
ip address 10.64.0.1 255.255.255.0
!
router ospf 77
network 10.64.0.0  0.0.0.255 area 0
```

```
Interface Ethernet0
ip address 10.64.0.2 255.255.255.0
!
Interface Serial0
ip address 10.2.1.2 255.255.255.252
!
router ospf 77
network 10.2.1.2   0.0.0.3 area 1
network 10.64.0.0   0.0.0.255 area 0
```

60

Fuente: Curso BSCI 642-801 de Cisco Systems

Configuración de área stub




```
R2#
interface Ethernet0
 ip address 192.168.14.1  255.255.255.0
interface Serial0
 ip address 192.168.15.1 255.255.255.252

router ospf 100
 network 192.168.14.0  0.0.0.255 area 0
 network 192.168.15.0  0.0.0.3 area 2
 area 2 stub
```

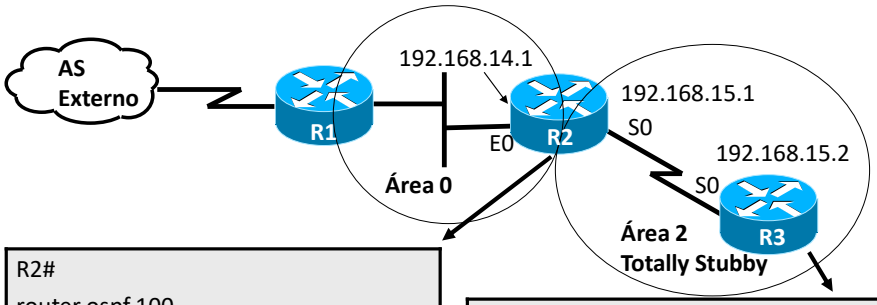
```
R3#
interface Serial 0
 ip address 192.168.15.2
255.255.255.252

router ospf 100
 network 192.168.15.0  0.0.0.3 area 2
 area 2 stub
```

61

Fuente: Curso BSCI 642-801 de Cisco Systems

Configuración de área totally stubby



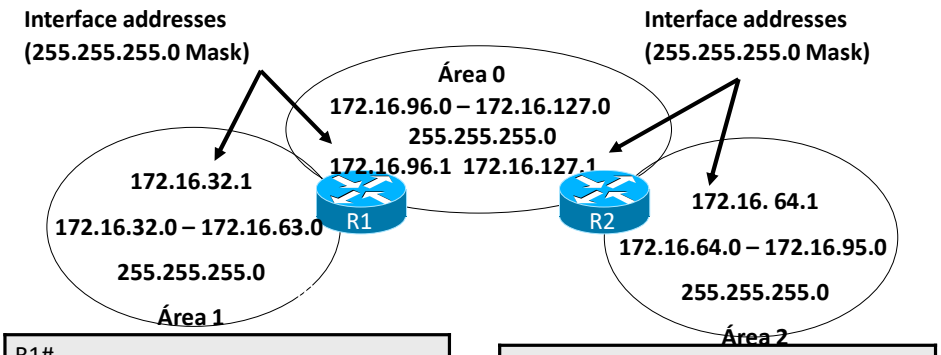

```
R2#
router ospf 100
network 192.168.14.0  0.0.0.255 area 0
network 192.168.15.0  0.0.0.3 area 2
area 2 stub no-summary
```

```
R3#
router ospf 100
network 192.168.15.0  0.0.0.3 area 2
area 2 stub
```

62

Fuente: Curso BSCI 642-801 de Cisco Systems

Ejemplo de resúmen de rutas




```
R1#
router ospf 100
network 172.16.32.1  0.0.0.255 area 1
network 172.16.96.1 0.0.0.255 area 0
area 0 range 172.16.96.0  255.255.224.0
area 1 range 172.16.32.0  255.255.224.0
```

```
R2#
router ospf 100
network 172.16.64.1  0.0.0.255 area 2
network 172.16.127.1 0.0.0.255 area 0
area 0 range 172.16.96.0  255.255.224.0
area 2 range 172.16.64.0  255.255.224.0
```

63

Fuente: Curso BSCI 642-801 de Cisco Systems

Visualización de la configuración

show ip ospf border-routers (Lista los ABRs en el AS)

show ip ospf virtual-link (Muestra el estado de los link virtuales)

show ip ospf process-id (Muestra estadística sobre cada área a la cual el router esta conectado)

show ip ospf database (Muestra el contenido de la tabla de OSPF)

Fuente: Curso BSCI 642-801 de Cisco Systems

Características de ISIS

ISIS, protocolo desarrollado y estandarizado por la ISO

- Protocolo de rápida convergencia
- Utilizado como IGP
- Altamente estable
- Utiliza de manera eficiente los recursos que utiliza (ancho de banda, memoria y procesador)

Es utilizado en redes extensas de ISPs

- Implementación mas simple que OSPF
- Implantación directa de IPv6 (a diferencia de OSPF)
- Inicialmente el gobierno de EEUU exigió a los ISP utilizar un protocolo que soportara los estándares ISO e IP
- Resulto ser muy estable y no hubo motivos para cambiarlo

Niveles en ISIS

Es un protocolo de estado de enlace que utiliza el algoritmo de Dijkstra (SPF)

- A diferencia de OSPF, donde un router puede pertenecer a varias áreas, en ISIS un router pertenece a un área determinada
- Se tienen dos niveles de ruteo
  - ***Nivel 1 (L1)*** Mantienen la información topológica de todos los nodos de la misma área; para acceder a una red de otra área se debe de acceder realizar a traves de un router L1L2
  - ***Nivel 2 (L2)*** Se intercambian prefijos de diferentes áreas

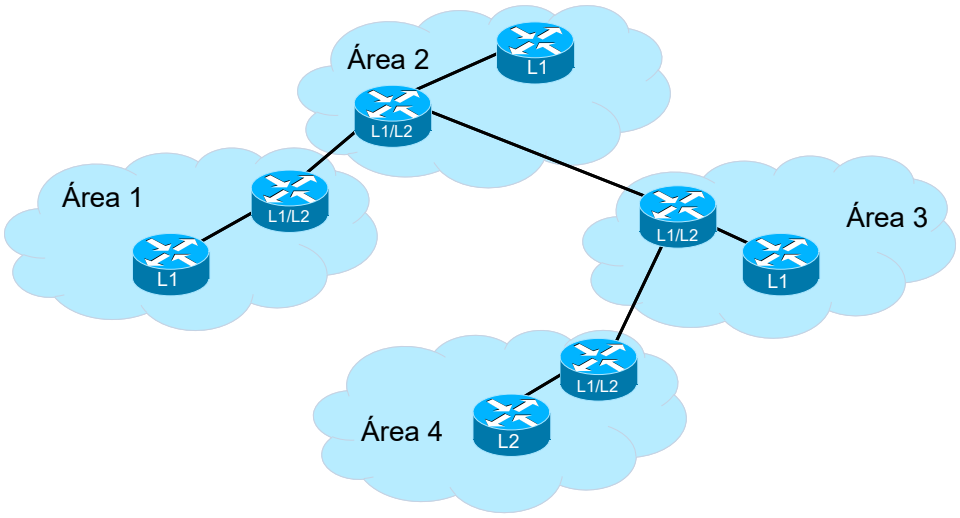
66

Niveles en ISIS

Los routers se configuran como L1, L2 o L1/L2

- L1 intercambian LSPs para construir la topología del área local
- L2 intercambian LSPs para construir la topología entre áreas
- L1/L2, sirven como frontera entre los dominios L1 y L2

Niveles en ISIS



Direccionamiento OSI NSAP

Los routers se identificaran con una dirección NSAP

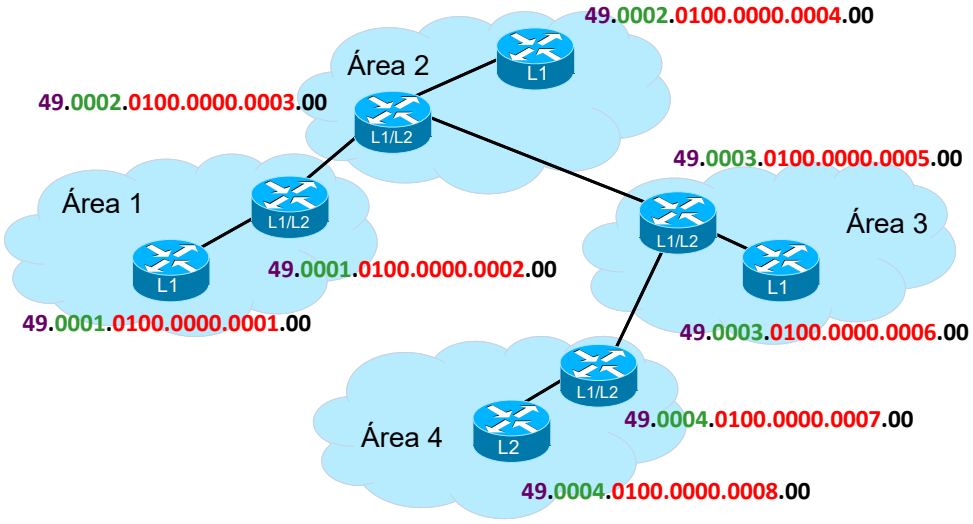
- Direccionamiento de Area: campo variable
- System ID: Identificador del nodo dentro del área
- NSEL: Identificador del servicio

Valores típicos

- Direccionamiento de Area
  - AFI = 49 (direcciones administradas localmente); direcciónes CLNS privadas
  - Area ID (un byte) Identifica el area en la cual se encuentra el equipo
- System ID
  - Tipicamente se agrega la dirección de loopback en formato de 6 bytes (wwwx.xxyy.yzzz)
- NSEL
  - Siempre igual a 0

69

Niveles en ISIS



L1, L2 y L1/L2

- L1 son análogos a los routers internos de OSPF
  - Cada área L1 esta compuesta por routers L1 y L1/L2
  - Cada router L1 mantiene una version de la tabla topologica de su área
- L1/L2 son análogos a los routers ABR de OSPF
  - Cada router L1/L2, mantiene una versión de la tabla topologica L1 de su área y la tabla topologica L2
  - Los routers L1/L2, advierten la ruta por defecto a los routers L1
- L2 son análogos a los routers de backbone de OSPF
  - Cada área L2 esta compuesta por routers L2 y L1/L2
  - Cada router L2, mantiene una versión de la tabla topologica L2

Paquetes en ISIS

- El intercambio de PDUs se realiza directamente sobre la trama Ethernet
- ISIS fue realizado solo para soportar el protocolo CLNP (Connectionless Network Protocol), el mismo pudo ser extendido a IPv4 y a IPv6 los TLVs
- Los TLVs, se intercambian dentro de los LSPs y son los encargados de transportar la información intercambiada por el protocolo de ruteo
- Ejemplos de TLV, Área, neighbors ISIS, rutas redistribuidas

Paquetes en ISIS

```
▷ Frame 4: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▷ IEEE 802.3 Ethernet
▷ Logical-Link Control
▽ ISO 10589 ISIS InTRA Domain Routeing Information Exchange Protocol
    Intra Domain Routing Protocol Discriminator: ISIS (0x83)
    PDU Header Length: 27
    Version (==1): 1
    System ID Length: 0
    PDU Type           : L1 HELLO (R:000)
    Version2 (==1): 1
    Reserved (==0): 0
    Max.AREAs: (0==3): 0
  ▽ ISIS HELLO
      Circuit type             : Level 1 and 2, reserved(0x00 == 0)
      System-ID {Sender of PDU} : 1000.0000.1001
      Holding timer: 30
      PDU length: 1497
      Priority                 : 64, reserved(0x00 == 0)
      System-ID {Designated IS} : 1000.0000.1001.04
    ▽ Protocols Supported (1)
        NLPID(s): IP (0xcc)
    ▽ Area address(es) (4)
        Area address (3): 49.0001
    ▽ IP Interface address(es) (4)
        IPv4 interface address: 192.168.0.5 (192.168.0.5)
    ▽ Restart Signaling (3)
      ▷ Restart Signaling Flags: 0x00
```

Paquetes en ISIS

```
▷ Frame 21: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface 0
▷ IEEE 802.3 Ethernet
▷ Logical-Link Control
▽ ISO 10589 ISIS InTRA Domain Routeing Information Exchange Protocol
    Intra Domain Routing Protocol Discriminator: ISIS (0x83)
    PDU Header Length: 33
    Version (==1): 1
    System ID Length: 0
    PDU Type           : L2 CSNP (R:000)
    Version2 (==1): 1
    Reserved (==0): 0
    Max.AREAs: (0==3): 0
  ▽ ISO 10589 ISIS Complete Sequence Numbers Protocol Data Unit
      PDU length: 115
      Source-ID:    1000.0000.0001.00
      Start LSP-ID: 0000.0000.0000.00-00
      End LSP-ID: ffff.ffff.ffff.ff-ff
    ▽ LSP entries (80)
      ▽ LSP-ID: 1000.0000.0001.00-00, Sequence: 0x00000006, Lifetime:   812s, Checksum: 0xcc16
          LSP-ID:             : 1000.0000.0001.00-00
          LSP Sequence Number : 0x00000006
          Remaining Lifetime  : 812s
          LSP checksum        : 0xcc16
      ▷ LSP-ID: 1000.0000.0001.02-00, Sequence: 0x00000002, Lifetime:   807s, Checksum: 0x0683
      ▷ LSP-ID: 1000.0000.0002.00-00, Sequence: 0x00000009, Lifetime:   936s, Checksum: 0xf57f
      ▷ LSP-ID: 1000.0000.0002.02-00, Sequence: 0x00000002, Lifetime:   950s, Checksum: 0x0780
      ▷ LSP-ID: 1000.0000.1001.00-00, Sequence: 0x00000007, Lifetime:  1148s, Checksum: 0xe62c
```

Ejemplo de Tabla topológica

```
uvv2xxx1#sho isis database

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
uvv2xxx1.00-00      * 0x0000000A   0xF603        925               0/0/0
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
ort2xxx1.00-00        0x0000000A   0xC41A        575               0/0/0
ort2xxx1.02-00        0x00000006   0xFD87        837               0/0/0
ort2xxx2.00-00        0x0000000D   0xED83        513               0/0/0
ort2xxx2.02-00        0x00000005   0x0183        205               0/0/0
uvv2xxx1.00-00      * 0x0000000D   0xB4AB        920               0/0/0
```

Ejemplo de Tabla topológica

```
ort2xxx2#sho isis database uvv2xxx1.00-00 detail


IS-IS Level-2 LSP uvv2xxx1.00-00
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
uvv2xxx1.00-00        0x0000000C   0x9FD5        246               0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  Hostname: uvv2xxx1
  Router ID:    10.0.1.1
  IP Address:   10.0.1.1
  Metric: 10         IS-Extended ort2xxx2.02
  Metric: 1          IP 10.0.1.1/32
  Metric: 10         IP 192.168.0.8/30
  Metric: 10         IP 192.168.0.12/30
  Metric: 10         IP 192.168.0.16/30
  Metric: 10         IP 192.168.0.24/30
  Metric: 10         IP 192.168.0.28/30
```

Ejemplo de Tabla de ruteo

```
ort2xxx2#sho ip route isis
     10.0.0.0/32 is subnetted, 3 subnets
i L2    10.0.1.1 [115/11] via 192.168.0.17, FastEthernet0/0
i L2    10.0.0.1 [115/21] via 192.168.0.17, FastEthernet0/0
     192.168.0.0/30 is subnetted, 6 subnets
i L2    192.168.0.8 [115/20] via 192.168.0.17, FastEthernet0/0
i L2    192.168.0.12 [115/20] via 192.168.0.17, FastEthernet0/0
i L2    192.168.0.4 [115/20] via 192.168.0.17, FastEthernet0/0
i L2    192.168.0.24 [115/20] via 192.168.0.17, FastEthernet0/0
i L2    192.168.0.28 [115/20] via 192.168.0.17, FastEthernet0/0
```

Observación, el SPF para obtener la tabla de ruteo, se realiza de manera independiente para la tabla topologica L1 y para la L2

Paquetes en ISIS

- Los Links en ISIS pueden ser configurados de dos formas, como point to point o como broadcast
  - Broadcast: para uso en una LAN
  - Point to point para otras topologías
- Broadcast
  - Los LSP se envian a una direccion IP destino de multicast
  - Se elije un router como designado al igual que en OSPF; en este caso se llama DIS en lugar de DR
    - Solo routers con adjacencias son elegibles como DIS
    - El router que tenga mas prioridad (0-127)
    - El router que tenga system ID mayor en caso de que todos tengan igual prioridad
- Point to Point
  - Los LSP se envian a una direccion IP destino de unicast

Vecindades en ISIS

- Ejemplo

```
ort2xxx2#sho isis nei

System Id      Type Interface IP Address      State Holdtime Circuit Id
uvv2xxx1       L2   Fa0/0     192.168.0.17    UP    26       ort2xxx2.02
```

Configuración en ISIS

- Paso 1: Definir las áreas que se van a configurar y en función de esto planificar las direcciones NET a configurar
- Paso 2: Configurar el proceso de ruteo ISIS
- Paso 3: Configurar la dirección NET asignada
- Step 4: Habilitar las interfaces que van a participar del protocolo de ruteo
- Configuraciones opcionales, como por ejemplo autenticación de las vecindades, sumarización, modificación de metricas asociadas a los enlaces, etc.
- Repetir a partir del paso 2 en cada router

Configuración en ISIS

- Ejemplo

```
router isis
 net 49.0002.0100.0000.0002.00
 is-type level-1
!
interface Loopback0
 ip address 10.0.0.2 255.255.255.255
 ip router isis
 isis metric 1
!
interface FastEthernet0/0
 ip address 192.168.0.18 255.255.255.252
 ip router isis
```

Cuadro comparativo de protocolos de ruteo

Protocolo	Interior o Exterior	DV o LS	Jerarquía requerida	Métrica
OSPF	Interior	LS	Sí	Costo
EIGRP	Interior	DV Avanzado	No	Compuesto
BGP	Exterior	DV Avanzado	No	Camino de vectores o atributos

Fuente: Curso BSCI de Cisco Systems

Cuestionario

1- Qué características presentan las zonas de Acceso, Distribución y Backbone de una red IP?
2- Qué grado de redundancia se prevé en la conectividad de cada una de las zonas anteriores?
3- Qué información emplea para enrutar un router?
4- Qué criterios se emplean para seleccionar rutas y en qué orden de prioridad?
5- En qué consisten los classless updates y qué ventajas tienen ante los classful updates?
6- Qué problemas plantean los protocolos de enrutamiento Distance Vector y qué soluciones se aplican?
7- Cómo logran los protocolos Link State evitar los loops de enrutamiento?
8- Qué es la convergencia de una red que usa un protocolo de enrutamiento?
9- Cómo son desde el punto de vista de la convergencia los distintos protocolos?
10- Qué diferencia presenta RIPv2 respecto de RIP?
11- Qué características presenta OSPF?
12- Qué características presenta un área stub en OSPF? Y un área totally stubby?
13- Por qué no es necesario elegir DR y BDR en un enlace punto a punto cuando se emplea OSPF?
14- Para qué sirve la delimitación de áreas en OSPF?
15- Qué similitudes y diferencias presentan ISIS y OSPF?
16- Cómo pueden interconectarse áreas en ISIS?

IPv6

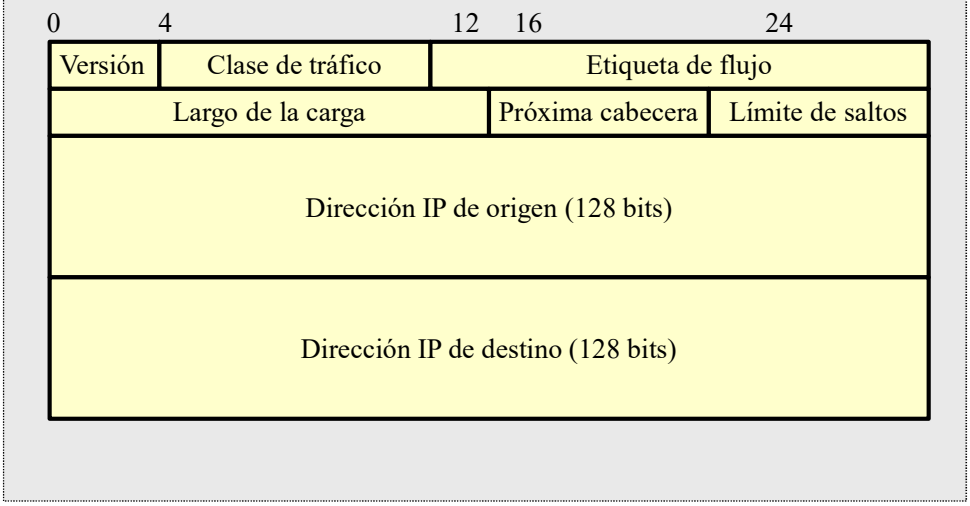
Cuál es el tamaño del espacio de IPv6?:

2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456

= 3.4×10^{38} aprox.

- Implica 6.7×10^{17} direcciones/mm² de la superficie terrestre
- Cantidad de átomos de todos los seres vivos terrestres: 10^{41}
- IPv4 no alcanza para tener una dirección por habitante

IPv6

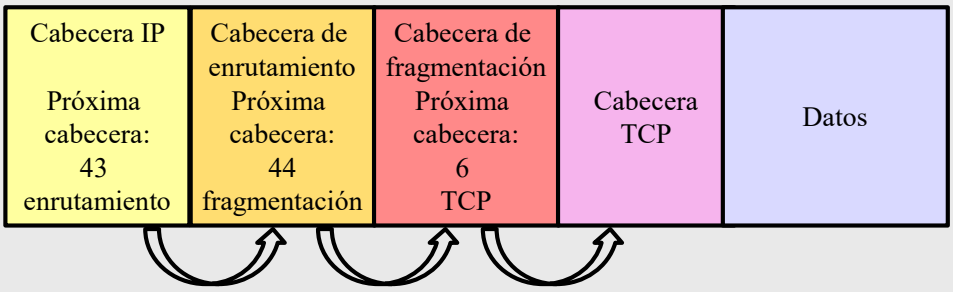


Versión: Versión de IP (6).
Clase de tráfico : Indica la prioridad del paquete.
Etiqueta de flujo: Permite un tratamiento especial para paquetes con requisitos de retardos.
Largo de la carga: Cantidad de bytes total en el paquete, con un máximo de 65535.
Próxima cabecera: Indica la siguiente cabecera.
Límite de saltos: Corresponde al antiguo tiempo de vida de IPv4.
Direcciones: Direcciones de nivel 3 de origen y de destino.

IPv6

Cabeceras de extensión

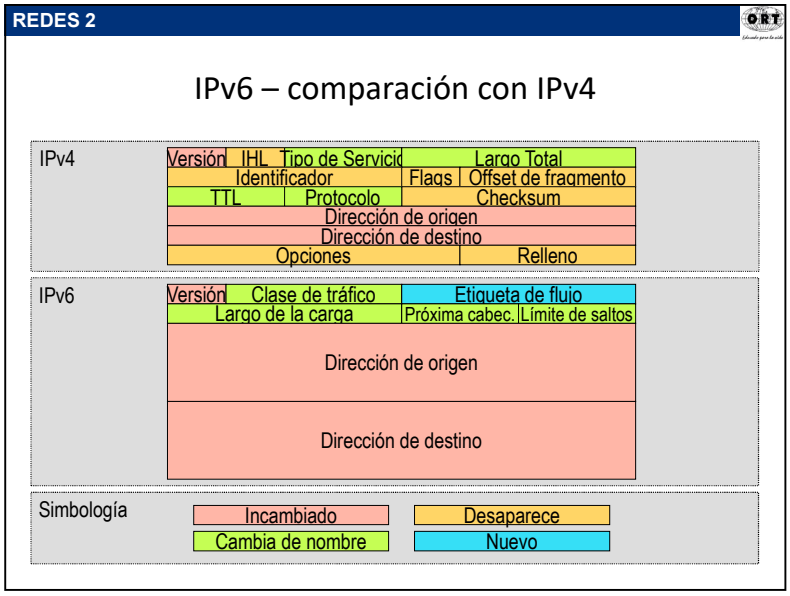
Funcionamiento de “próxima cabecera”:



Cabeceras de extensión

Cabeceras definidas hasta el momento:

- Autenticación (AH de IPSec)
- Encriptamiento (ESP de IPSec)
- Enrutamiento
- Fragmentación
- Opciones para el destino
- Opciones para el próximo salto



Resumen de modificaciones

Incremento del tamaño de cabecera de 32 a 40 bytes

Incremento del tamaño de las direcciones de 32 a 128 bits

Eliminación del checksum

Eliminación de campos de fragmentación y de offset

Cabecera de largo fijo, pero posibilidad de cabeceras adicionales (de extensión)

Nuevo campo de etiqueta de flujo

Alineación de 64 bits

IPv6

Direccionamiento

Representaciones:

- Preferida 2000:0:0:0:2C:FF:2001:010F
- Comprimida 2000::2C:FF:2001:010F
- Compatible IPv4 0:0:0:0:0:0:192.168.10.1 ó 0::192.168.10.1

Tipos de direcciones:

- Unicast: Identifican una única interfaz
  - Globales
  - Enlace local
  - Sitio local
- Anycast: Identifican un grupo de interfaces, los paquetes dirigidos a ellas se entregan a la más próxima
- Multicast : Identifican un grupo de interfaces, los paquetes dirigidos a ellas se entregan a todas ellas
- Reservadas

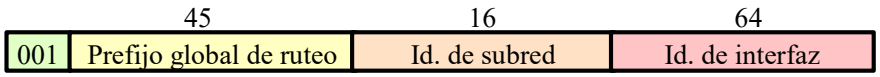
IPv6

Direccionamiento

Prefijos para cada tipo de direcciones:

Tipo	Prefijo
Unicast globales	001
Unicast enlace local	1111 1110 10
Unicast sitio local	1111 1110 11
Anycast	El mismo que las unicast
Multicast	1111 1111
Reservadas	El resto de direcciones (87.5%)

Direcciones globales unicast (RFC 3587):



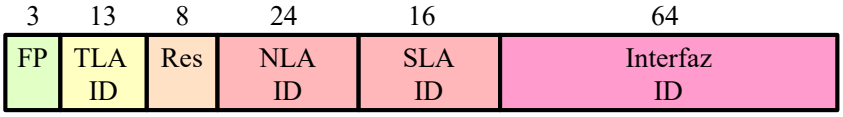
Prefijo global de ruteo: identifica un sitio

- Identificador de subred: identifica una subred dentro de un sitio, permite establecer jerarquías en la estructura de direcciones
- Identificador de interfaz: pueden seguir el formato EUI-64 que permite incluir la información de la dirección MAC

IPv6

Direccionamiento

Direcciones globales unicast agregables:



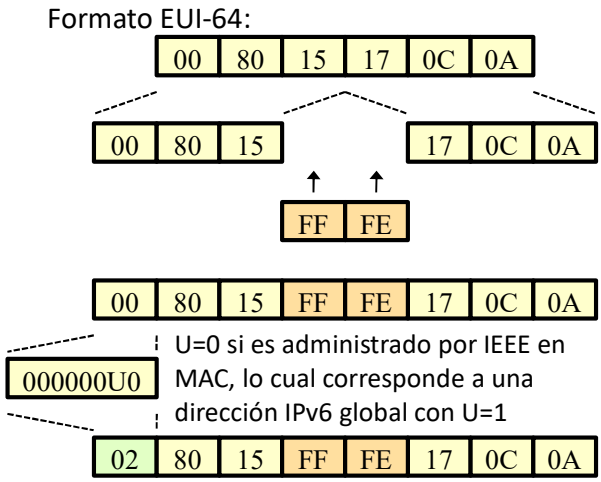
FP:	Prefijo de formato, 001
TLA ID:	Identificación de agregación de nivel superior
Res:	Reservado para uso futuro
NLA ID:	Identificador de agregación de siguiente nivel
SLA ID:	Identificador de agregación de nivel de sitio
Interfaz ID:	Identificador de interfaz

IPv6

Direccionamiento

Identificador de interfaz:

- Puede seguir el formato EUI-64
- Puede generarse seudoaleatoriamente (por seguridad)
- Puede asignarse por DHCP
- Puede configurarse manualmente

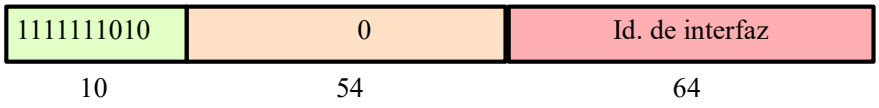


IPv6

Direccionamiento

Direcciones de enlace local:

- Se previeron para direccionar un enlace con fines de autoconfiguración, de descubrimiento de vecindario, o para situaciones en las que no hay routers
- Emplean identificadores de interfaz



IPv6

Direccionamiento

Autoconfiguración stateless:

- El dispositivo no necesita la intervención de un servidor para configurar las direcciones de sus interfaces, aún sin información externa (stateless). Emplea para eso una dirección de enlace local (los primeros bits son 1111 1110 10 y se agregan 54 ceros) que genera a partir de la dirección MAC.
- El dispositivo verifica que la dirección es única en la subred mediante el protocolo ND (envía un mensaje Neighbor Solicitation, y espera para ver si detecta un Neighbor Advertisement que indicaría duplicación de direcciones). Si hubiera duplicación, o bien intenta nuevamente o bien aplica otro método.
- Si no existe duplicación, el dispositivo asigna la dirección a la interfaz, y la emplea para la comunicación local en la subred
- A continuación, el dispositivo intenta contactarse con un router, escuchando algún Router Advertisement o bien enviando un Router Solicitation a efectos de pedir indicación de cómo proseguir. El procedimiento que sigue a esta instancia es el que corresponde a la autoconfiguración stateful

IPv6

Direccionamiento

Autoconfiguración stateful:

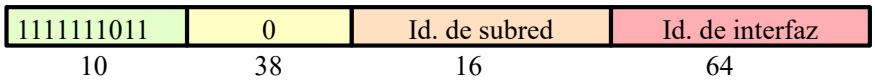
- El router informa al host o bien cuál servidor DHCP está disponible en la subred, o bien cuál es el prefijo de red.
- Si la configuración es stateless, el dispositivo combina el prefijo informado por el router con el identificador obtenido en la etapa anterior.

IPv6

Direccionamiento

Direcciones de sitio local:

- Permiten direccionar dentro de un sitio, sin necesidad de un prefijo global
- No deben ser retransmitidas fuera del sitio
- Emplean un identificador de subred de 16 bits



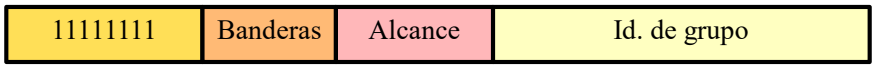
Direcciones especiales:

- Dirección no especificada, se emplea cuando aún no se dispone de de una dirección:
  0:0:0:0:0:0:0:0
- Dirección de loopback para autoenvío: 0:0:0:0:0:0:0:1

IPv6

Direccionamiento

Direcciones de multicast (RFC 3513):

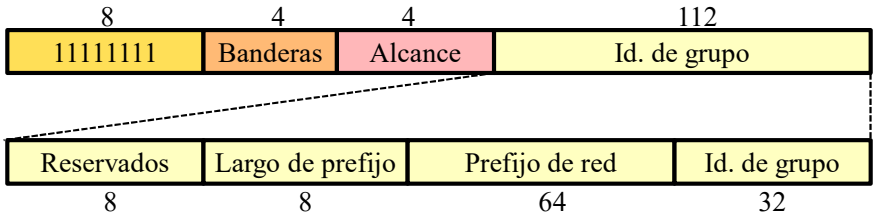


Banderas: sólo se emplea el bit menos significativo, que indica si se trata de grupos permanentes o temporales

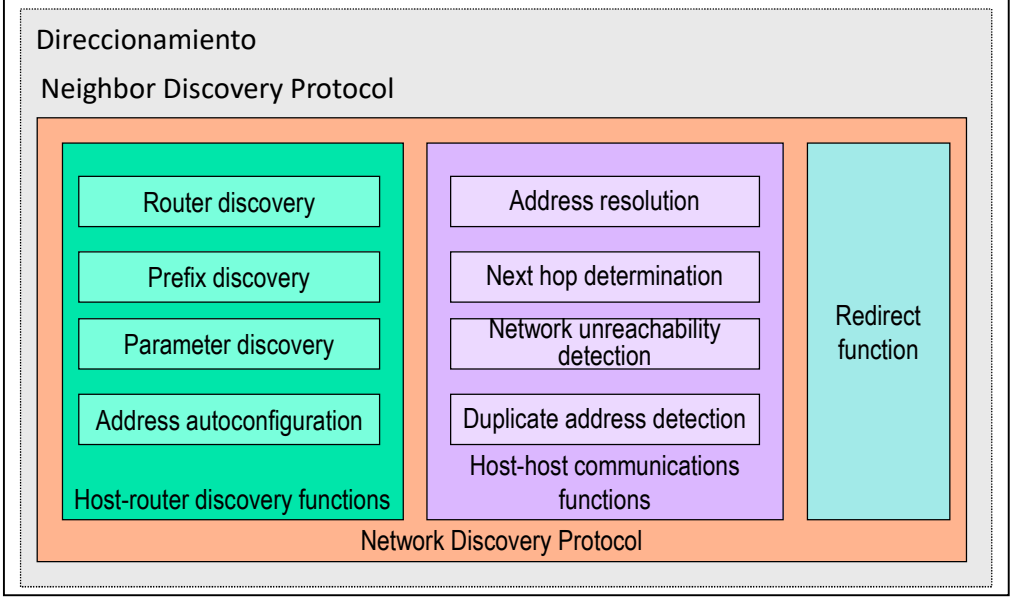
- Alcance:

1 - nodo local 8 - organización local
2 - enlace local B - comunidad local
5 - sitio local E - global

Direcciones de multicast (RFC 3306) globales ruteables:



IPv6


Direccionamiento
Neighbor Discovery Protocol
Router discovery
Prefix discovery
Parameter discovery
Address autoconfiguration
Host-router discovery functions
Address resolution
Next hop determination
Network unreachability detection
Duplicate address detection
Host-host communications functions
Redirect function
Network Discovery Protocol

IPv6

Direccionamiento

Neighbor Discovery Protocol

Mensajes:

- Router Advertisement: el router lo envía regularmente, informa sobre prefijos y parámetros a los hosts
- Router Solicitation: un host lo envía para pedir un RA
- Neighbor Advertisement: el host indica su presencia
- Neighbor Solicitation: el host verifica si existe otro host o solicita un NA
- Redirect: un router indica un mejor ruteo a un host

Configuración de IPv6

Habilitación de IPv6:

Router(config)# ipv6 unicast-routing

Configuración de interfaces:

Router (config-if) # ipv6 address W:X:Y:Z::/prefix

Servidor de nombre accesible por IPv6:

Router (config) # ip nameserver fec0:2:1:1::2

Router (config) # ip nameserver 10.1.40.40

Habilitar IPv6 en una interfaz:

Router (config-if) # ipv6 enable ← Al hacer esto se configura automáticamente con una IPv6 del tipo Local-link de forma FE80::interface-id

Visualización de estado de interfaz IPv6

```
Router1#sh ipv6 interface eth0/0
Ethernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:1E00
  Global unicast address(es):
    2001:DB8::A8BB:CCFF:FE00:1E00, subnet is 2001:DB8::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1E00
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

Configuración de IPv6

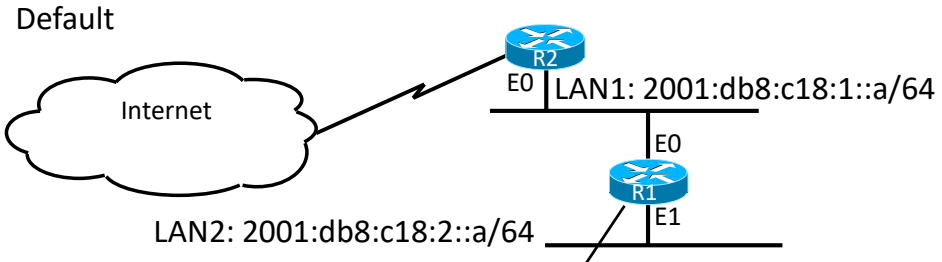
Enrutamiento estático:

ipv6 route ipv6-prefix/prefix-length {ipv6-address | interface-type interface-number} [admin-distance]

Ejemplo:

ipv6 route 2001:db8::/64 2001:db8:0:cc00::1 110

Configuración de IPv6




```
Interface Ethernet 0
 ipv6 address 2001:db8:c18:1::a/64
!
Interface Ethernet 1
 ipv6 address 2001:db8:c18:2::a/64
!
ipv6 route ::/0 <direccion de E0 de R2>
```

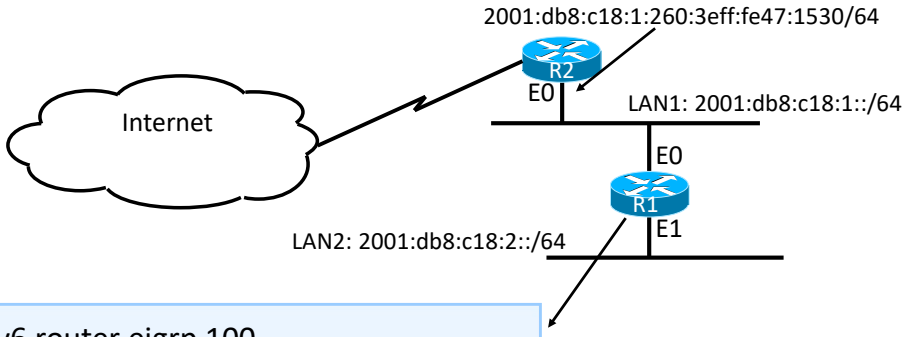
Configuración de IPv6

Protocolos de ruteo dinámico

- IGP
  - RIPng (RFC 2080)
  - Cisco EIGRP for IPv6
  - OSPFv3 (RFC 2740)
  - Integrado IS-ISv6 (draft-ietf-isis-ipv6-06)
- EGP
  - MP-BGP4 (RFC 4760 y RFC 2545)

Configuración de IPv6

Configuración de EIGRP para IPv6



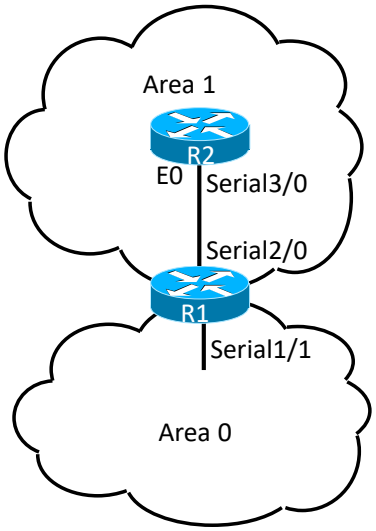

```
ipv6 router eigrp 100
!
Interface Ethernet 0
 ipv6 address 2001:db8:c18:1::/64 eui-64
 ipv6 enable
 ipv6 eigrp 100
```

Configuración de IPv6

Configuración de OSPFv3 para IPv6

```
Router2#
Interface Serial3/0
  ipv6 address 2001:db8:1:1::1/64
  ipv6 ospf 100 area 1
!
Ipv6 router ospf 100
 router-id 2.2.2.2
```

```
Router1#
Interface Serial1/1
  ipv6 address 2001:db8:ffff:1::1/64
  ipv6 ospf 100 area 0
!
Interface Serial2/0
 ipv6 address 2001:db8:1:1::2/64
 ipv6 ospf 100 area 1
!
ipv6 router ospf 100
 router-id 1.1.1.1
```



105

Comando de visualización de rutas de IPv6

```
Router2#sh ipv6 route
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
OI  2001:db8:FFFF:1::/64 [110/2]
     via FE80::2D0:FFFF:FE60:DFFF, POS3/0
C   2001:db8:1:1::/64 [0/0]
     via ::, POS3/0
L   2001:db8:1:1::1/128 [0/0]
     via ::, POS3/0
L   FE80::/10 [0/0]
     via ::, Null0
L   FF00::/8 [0/0]
     via ::, Null0
```

Cuestionario

1- Qué cambios introduce IPv6 respecto de IPv4?

2- Qué mecanismos permiten evitar la configuración manual de las direcciones IPv6 en los hosts?

3- Qué formato tienen las direcciones IPv6?

4- Cuántos bits suelen reservarse para hosts en IPv6?

5- Qué utilidad tiene el protocolo DHCP y cómo funciona?

Investigación

1- Cómo tratan los routers que tienen configurado NAT con sobrecarga (NAT/PAT) a los paquetes de protocolos que no soportan puertos (ICMP por ejemplo)?