TEMA 4

-Direccionamiento IP

-Protocolos de encaminamiento.

-RIP, IGRP,OSPF,EIGRP.

Direccionamiento IP y división en subredes 1/6

Propósito de las direcciones IP

• Cada nodo que utiliza el conjunto de protocolos TCP/IP tiene una dirección lógica distinta de 32 bits. Esta dirección se denomina dirección IP y se especifica en formato decimal separado por puntos de 32 bits. Las interfaces del router se deben configurar con una dirección IP si el protocolo IP se debe enrutar hacia o desde la interfaz .

• Cada red de una empresa tiene una dirección; los hosts que residen en esa red comparten la misma dirección de red, pero cada host se identifica por medio de la dirección única de host en la red.

Direccionamiento IP y división en subredes 2/6

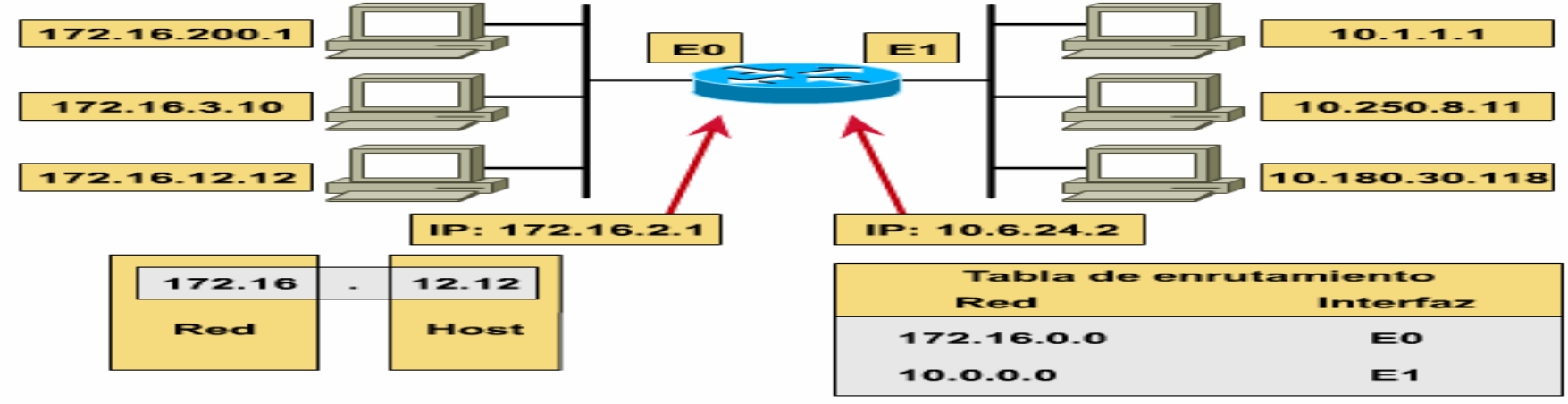
Rol de la red del host en una red enrutada

• Cada dispositivo o interfaz debe tener un número de host que no tenga sólo ceros en el campo de host. Una dirección de host de sólo unos está reservada para un broadcast IP hacia esa red. Un valor de host de 0 significa "esta red" o "el cable en sí mismo" (por ej., 172.16.0.0).

• La tabla de enrutamiento contiene entradas para las direcciones de red o de cable. Por lo general, no contiene información acerca de los hosts.

• Una dirección IP y una máscara de subred en una interfaz cumplen tres propósitos:

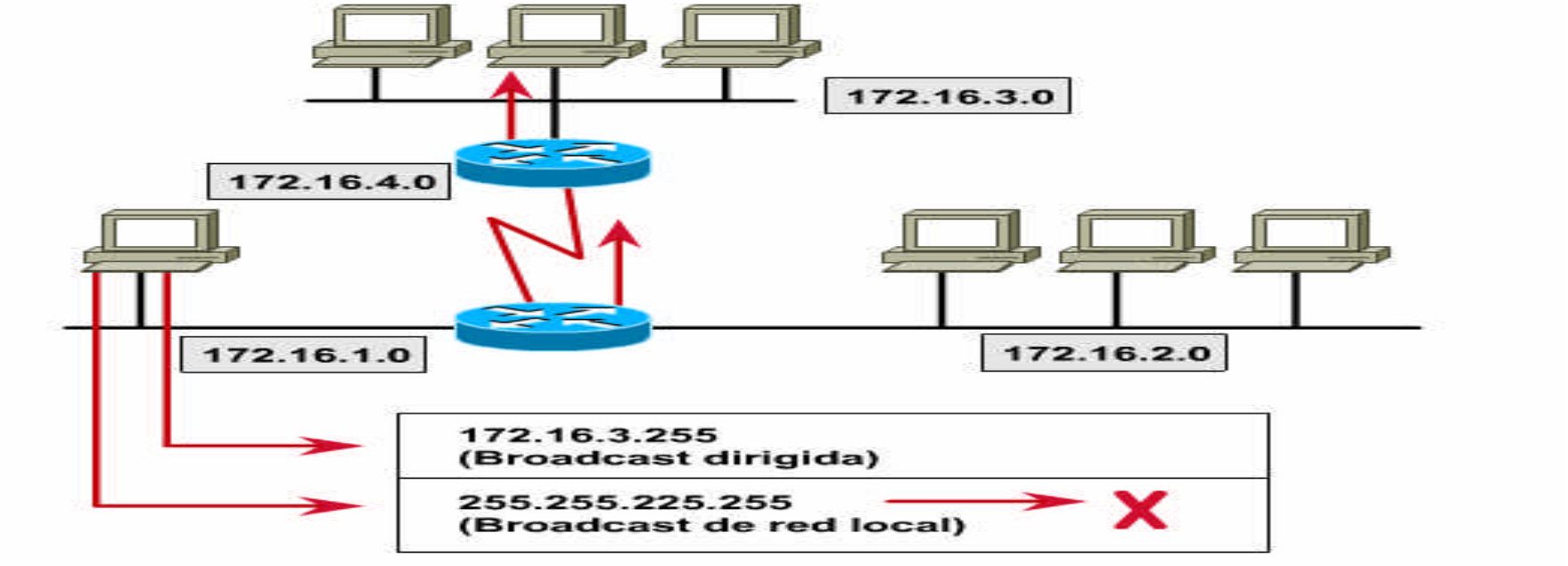
1. Permiten que el sistema procese la recepción y transmisión de paquetes.
2. Especifican la dirección local del dispositivo.
3. Especifican un intervalo de direcciones que comparten el cable con el dispositivo.



Direccionamiento IP y división en subredes 3/6

Rol de las direcciones de broadcast en una red enrutada

IP soporta el broadcast. Se pretende que los mensajes sean vistos por todos los hosts de la red.
La dirección de broadcast se forma utilizando sólo unos en una parte de la dirección IP.
El software Cisco IOS soporta dos tipos de broadcasts: broadcasts dirigidos y broadcasts inundados. Los broadcasts dirigidos hacia una red/subred específica son autorizados y retransmitidos por el router. Estos broadcasts dirigidos contienen sólo unos en la parte de la dirección correspondiente al host. (Configuración en router: **ip direct broadcast**).
Los broadcasts inundados (255.255.255.255) no se propagan, sino que se consideran broadcasts locales (sólo se transmiten localmente).



Direccionamiento IP y división en subredes 5/6

Direcciones IP especiales

Dirección	Significado	Ejemplo
255.255.255.255	Broadcast a todos los nodos de la red local	
0.0.0.0	Identifica a cualquier host o red. (configuraciones de rutas por defecto)	
Host a ceros	Identifica una red (o subred)	147.156.0.0
Host a unos	Broadcast en la red (o subred)	147.156.255.255
Red a ceros	Identifica un host en esa red (o subred)	0.0.1.25
127.0.0.1	Loopback. Cliente y servidor están en la misma máquina.	
224.0.0.1	Todos los hosts multicast	

Direccionamiento IP y división en subredes 6/6

Direcciones IP reservadas y privadas (RFC 1918)

Red o rango	Uso
127.0.0.0	**Reservado (fin clase A)**
128.0.0.0	**Reservado (ppio. Clase B)**
191.255.0.0	**Reservado (fin clase B)**
192.0.0.0	**Reservado (ppio. Clase C)**
224.0.0.0	**Reservado (ppio. Clase D)**
240.0.0.0 – 255.255.255.254	**Reservado (clase E)**
10.0.0.0	**Privado**
172.16.0.0 – 172.31.0.0	**Privado**
192.168.0.0 – 192.168.255.0	**Privado**

Rol del DNS en las configuraciones del router 1/5

-El comando *ip address*

Se utiliza para establecer la dirección de red lógica de una interfaz.

-El comando *ip* *netmask-format*

Router (config-if) #

Se utiliza para especificar el formato de las máscaras de red para un línea específica

-El comando *term ip* *netmask-format*

Router #

Para especificar el formato de las máscaras de red para la sesión actual.

Opciones:

- **número de bits (bit-count)**
- **decimal separado por puntos (opción por defecto)**
- **hexadecimal**

Comando
`Router(config-if)# ip address ip-address subnet-mask`

- **Asigna una dirección y una máscara de subred**
- **Inicia el procesamiento IP en una interfaz**

Rol del DNS en las configuraciones del router 2/5

El comando ip host

• **Crea una entrada estática que relaciona el nombre de host con la dirección del mismo en el archivo de configuración del router.**

Comando
`Router(config)# ip host nombre[número de puerto tcp] dirección[dirección]...`

El comando `ip host`	Descripción
`nombre`	cualquier nombre que prefiera para describir el destino
`número de puerto tcp`	número de opción que identifica el puerto TCP que se debe utilizar cuando se usa el nombre de host con un comando connect o telnet EXEC. La opción por defecto es puerto 23
`dirección`	Dirección o direcciones IP con las que se puede llegar al dispositivo

Rol del DNS en las configuraciones del router 3/5

¿Cómo asignar nombres de dominio a las direcciones IP?

- Identificar los nombres de host.
- Especificar un servidor de nombre.
- Habilitar DNS.

El comando ip name-server

- Define cuáles son los hosts que pueden suministrar el servicio de denominación.
- Como máximo seis direcciones IP como servidores de nombre por comando.

Comando

```
Router(config)#
ip name-server server-address1[server-address2]...
[server-address6]
```

Rol del DNS en las configuraciones del router 4/5

Habilitación e inhabilitación de DNS en un router

El software Cisco IOS mantiene una memoria caché de asignaciones de nombre a dirección de host para ser utilizada por los comandos EXEC. Esta caché acelera el proceso de conversión de nombres a direcciones.

IP define un esquema de denominación que permite que un dispositivo se identifique a través de su ubicación en IP.

Ejemplo : **ftp.cisco.com** identifica el dominio del Protocolo de Transferencia de Archivos (FTP) para Cisco.

• Habilitado por defecto con una dirección de servidor 255.255.255.255 (broadcast local)

• El comando **no ip domain-lookup** desactiva la conversión de nombres a direcciones en el router.

Comando
`Router(config)# no ip domain-lookup`

Rol del DNS en las configuraciones del router 5/5

El comando show hosts

- Visualiza una lista de la memoria caché de nombres y direcciones de host.

Resultado del comando

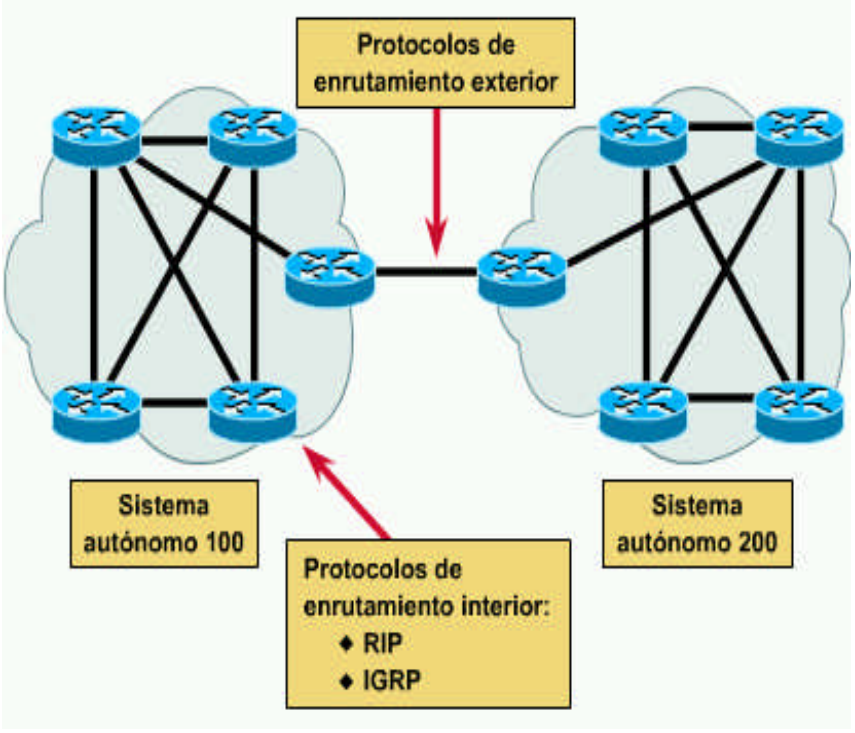
```
Router# show hosts
Default domain is not set
Name/address lookup uses static mappings

Host          Flags          Age     Type     Address(es)
TOKYO         (perm, OK)      5       IP      144.253.100.200   133.3.13.2
                                              133.3.5.1   133.3.10.1
```

El comando show host	Descripción
Host	nombres de los hosts aprendidos
Señalador	descripciones de la forma en que se obtuvo la información y su estado actual
perm	configurado manualmente en una tabla de hosts estática
temp	adquirido a partir del uso del DNS
OK	la entrada es actual
EX	la entrada es antigua, ha expirado
Antigüedad	tiempo medido en horas desde que el software consultó la entrada
Tipo	Campo de protocolo
Dirección(es)	direcciones lógicas asociadas con el nombre del host

Enrutamiento

Enrutamiento interior / Enrutamiento exterior



- **Los protocolos de enrutamiento exterior se utilizan para las comunicaciones entre sistemas autónomos (ej BGP). Los protocolos de enrutamiento interior se utilizan dentro de un mismo sistema autónomo.**

Número de sistema autónomo

- En la configuración de algunos protocolos como IGRP es necesario introducir un número de sistema autónomo.
- Lo forman routers bajo una administración común.
- El Centro de Información de la Red (NIC) asigna un sistema autónomo único a las empresas. Este sistema autónomo equivale a un número de 16 bits.
- El rango reservado por el RFC 1930 para sistemas autónomos privados es del 64512 al 65535.

Conceptos básicos sobre enrutamiento 1/5

Determinación de ruta

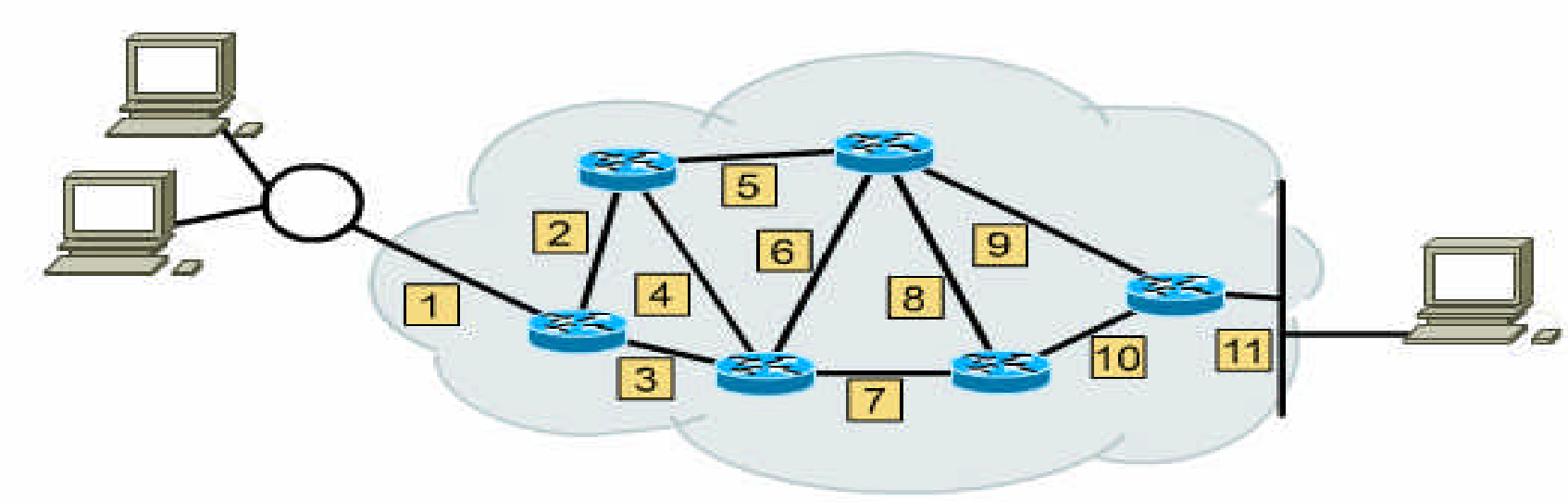
- **La determinación de ruta se produce en la capa de red (Capa 3).**
- **Consta de :**
  - **Evaluación de las rutas disponibles hacia un destino. Utilizando información de la topología de la red.**
  - **Establecer el mejor manejo de un paquete. Escoger la ruta.**
- **¿De donde se obtiene la información?**
  - **La puede configurar el administrador de red de forma estática.**
  - **Se puede recopilar a través de procesos dinámicos ejecutados en la red.**
- **La capa de red proporciona entrega de paquetes de máximo esfuerzo y de extremo a extremo a través de redes interconectadas.**
- **La capa de red utiliza la tabla de enrutamiento IP para enviar paquetes desde la red origen a la red destino.**

Red de destino	Interfaz (Salto siguiente)
172.16.0.0	S0
172.18.0.0	--
192.168.24.0	S0
Router por defecto	S1

Conceptos básicos sobre enrutamiento 2/5

Enrutamiento de paquetes del origen al destino por parte de los routers

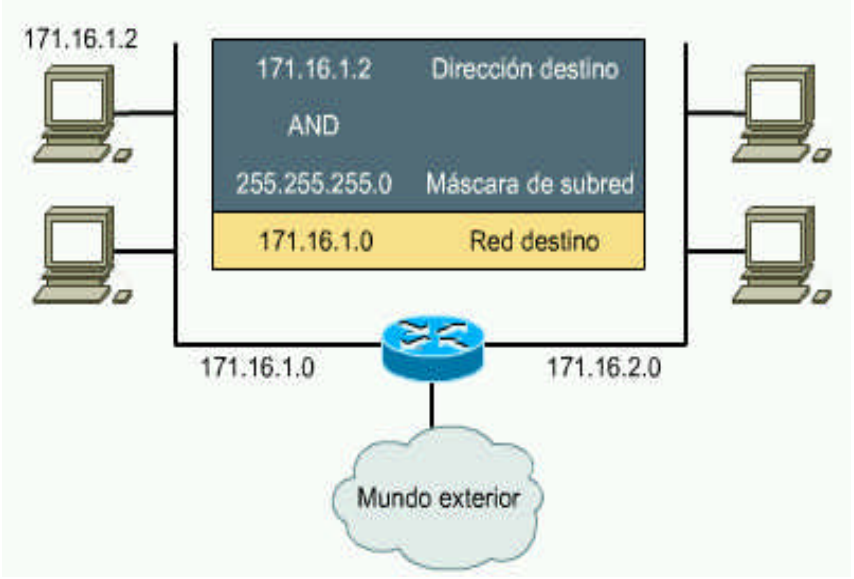
- **Una red debe representar de manera coherente las rutas disponibles entre los routers.**
- **Las direcciones de red deben proporcionar información que un proceso de enrutamiento puede utilizar para transportar paquetes desde un origen hacia un destino.**
- **La coherencia de las direcciones de Capa 3 en toda la internetwork mejora el uso del ancho de banda evitando los broadcasts innecesarios**

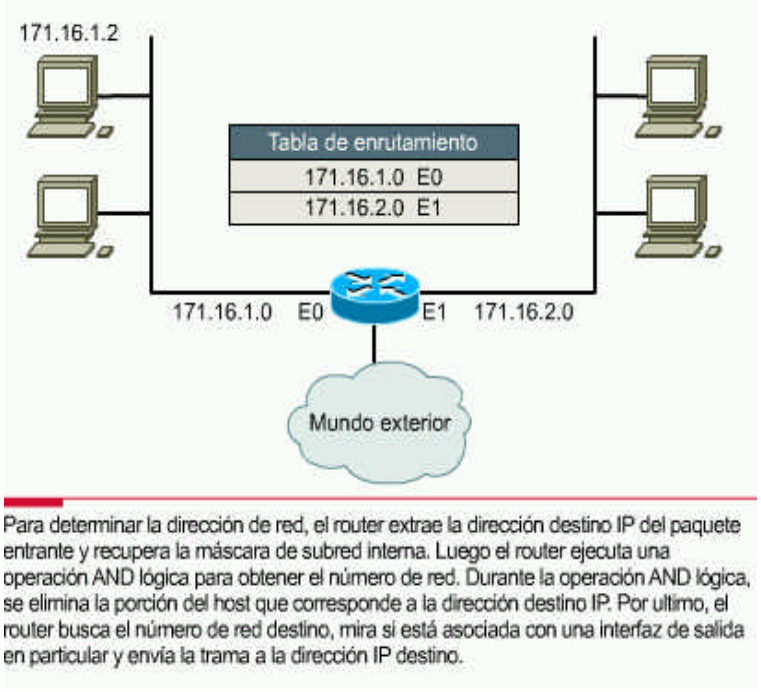


Conceptos básicos sobre enrutamiento 3/5

Direccionamiento de red y de host

- El router utiliza la dirección de red para identificar la red destino (LAN) de un paquete dentro de una internetwork.
- La asignación de direcciones de host dentro de una red puede ser:
  - Establecida por el administrador de red, que asigna direcciones de host de acuerdo con un plan predeterminado de direccionamiento de internetwork.
  - Parcial o totalmente dinámica.





Para determinar la dirección de red, el router extrae la dirección destino IP del paquete entrante y recupera la máscara de subred interna. Luego el router ejecuta una operación AND lógica para obtener el número de red. Durante la operación AND lógica, se elimina la porción del host que corresponde a la dirección destino IP. Por ultimo, el router busca el número de red destino, mira si está asociada con una interfaz de salida en particular y envía la trama a la dirección IP destino.

Conceptos básicos sobre enrutamiento 4/5

Protocolo enrutado versus protocolo de enrutamiento

Protocolo *enrutado* es cualquier protocolo de red que proporcione suficiente información en su dirección de capa de red para permitir que un paquete se envíe desde un host a otro tomando como base el esquema de direccionamiento.

- Los paquetes generalmente se transfieren de un sistema final a otro.
- Ejemplo : IP.

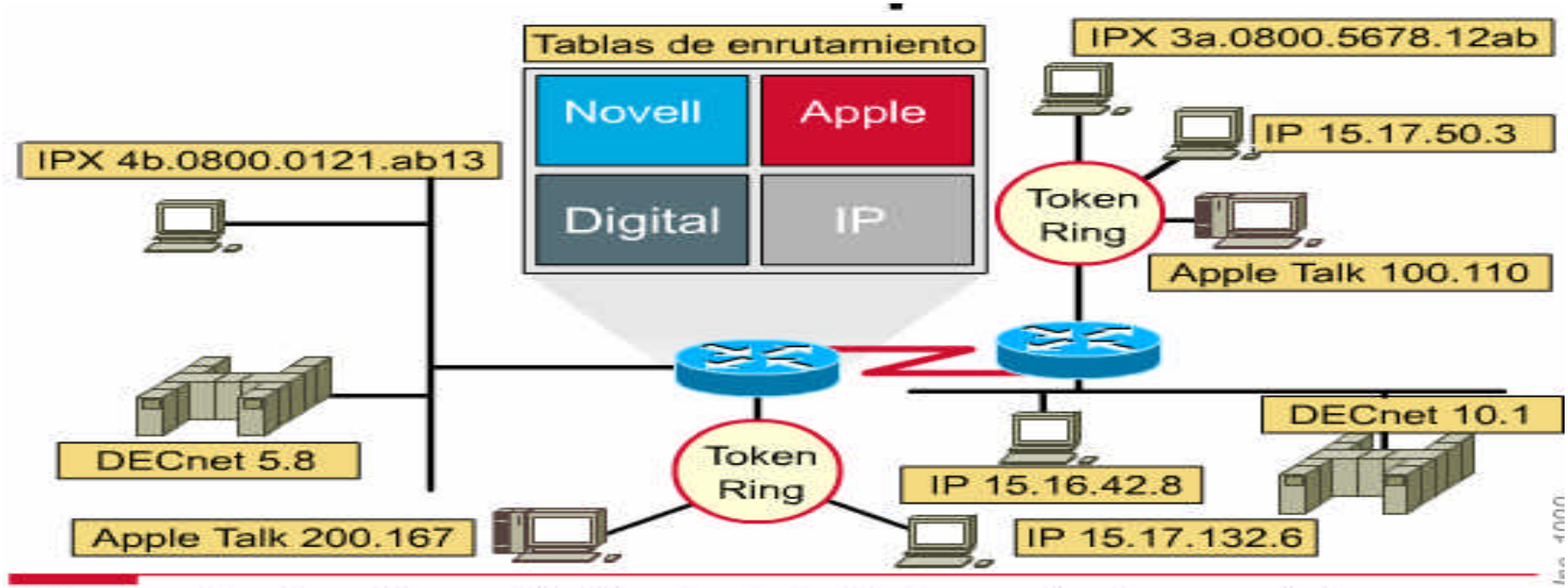
Los protocolos de *enrutamiento* soportan un protocolo enrutado proporcionando mecanismos para compartir la información de enrutamiento. Permite que los routers se comuniquen con otros routers para actualizar y mantener las tablas.

- Los mensajes se desplazan entre los routers.
- Ejemplos : RIP, IGRP, EIGRP, OSPF

Conceptos básicos sobre enrutamiento 5/5

Enrutamiento multiprotocolo

- Los routers pueden soportar varios protocolos de enrutamiento independientes y mantener tablas de enrutamiento para varios protocolos enrutados.
- Esta capacidad le permite al router entregar paquetes desde varios protocolos enrutados a través de los mismos enlaces de datos.



- Los routers transfieren el tráfico desde todos los protocolos enrutados a través de la internetwork

Necesidad de los protocolos de routing 1/3

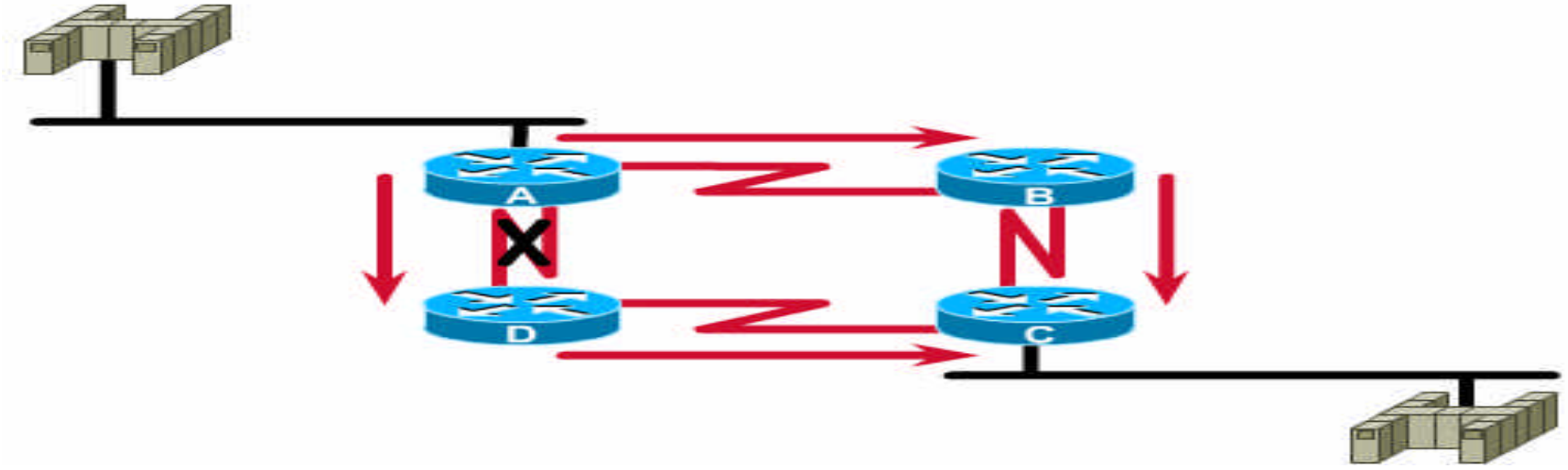
Necesidad del enrutamiento dinámico

- **Adaptación a los cambios en la topología**

  - Flexibilidad ante fallos, una ruta alternativa puede reemplazar una ruta defectuosa.

- **Carga compartida**

  - Los protocolos de enrutamiento dinámico también pueden dirigir el tráfico de una misma sesión a través de distintas rutas de una red para lograr un mejor rendimiento.



Necesidad de los protocolos de routing 2/3

Tres clases de protocolos de enrutamiento

Vector-distancia :determina la dirección (vector) y la distancia hacia cualquier enlace en la internetwork.

Estado-enlace : recrea la topología exacta de toda la internetwork (o por lo menos la porción en la que se ubica el router).

Híbridos : el enrutamiento híbrido balanceado combina aspectos de los algoritmos de estado-enlace y vector-distancia.

Necesidad de los protocolos de routing 3/3

Tiempo de convergencia

Siempre que la topología de una red cambia por razones de crecimiento, reconfiguración o falla, la base del conocimiento de la red también debe cambiar.

Cuando todos los routers de una internetwork se encuentran operando con el mismo conocimiento, se dice que la internetwork ha *convergido.*

La convergencia rápida es una función de red deseable, ya que reduce el período de tiempo durante el cual los routers continúan tomando decisiones de enrutamiento incorrectas.

El tiempo de convergencia es el tiempo que transcurre desde que se produce un cambio en la topología de una internetwork hasta que todos los routers actualizan su conocimiento de forma consistente con el resto y de forma que se vea reflejado el cambio.

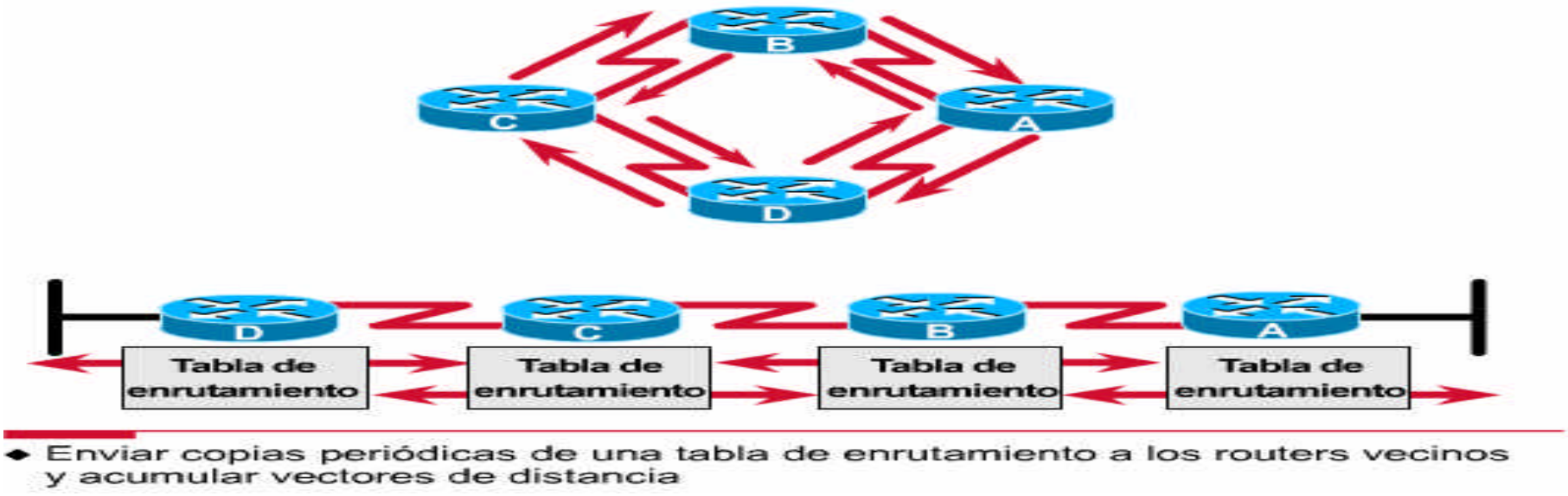
Enrutamiento vector-distancia 1/5

Principios básicos del enrutamiento de vector-distancia

• Envían copias periódicas de una tabla de enrutamiento de un router a otro. Estas actualizaciones regulares entre routers comunican los cambios de topología.

• Cada router recibe una tabla de enrutamiento de los routers vecinos directamente conectados.

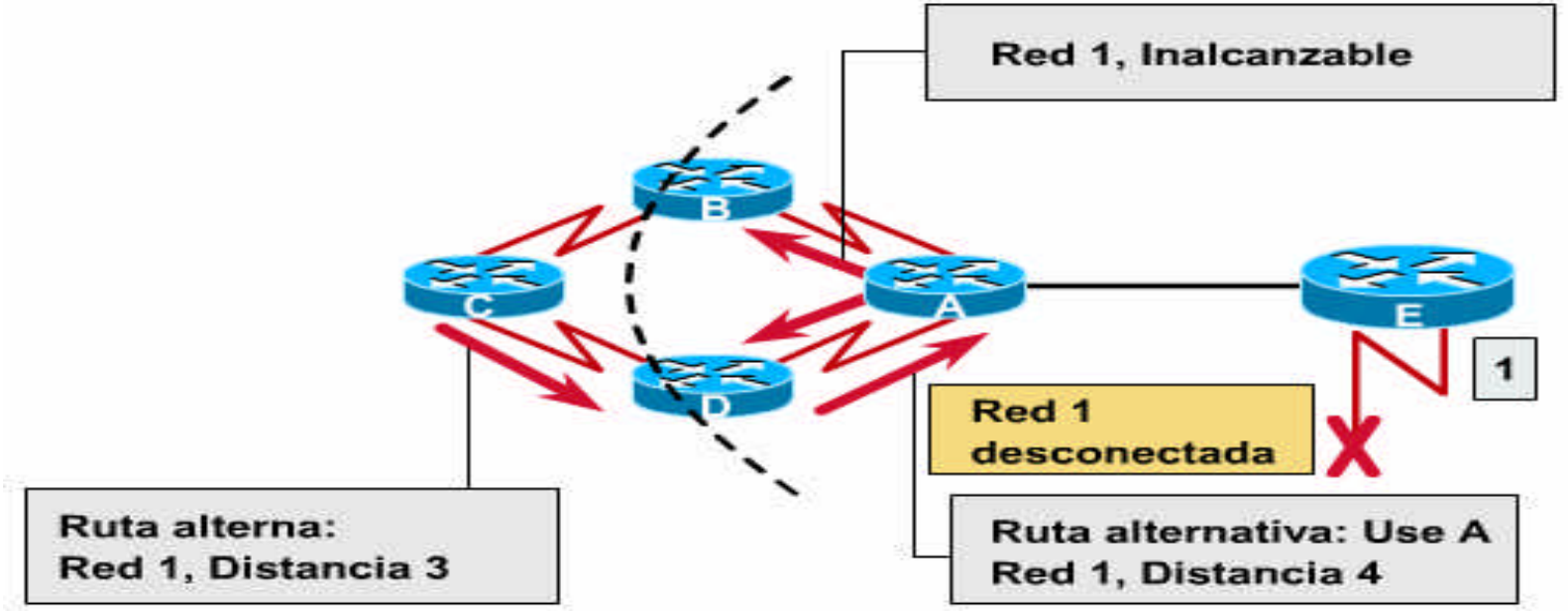
• Los algoritmos vector-distancia no permiten, sin embargo, que un router conozca la topología exacta de una internetwork.



Enrutamiento vector-distancia 2/5

El problema de los loops de enrutamiento

• Los loops de enrutamiento se pueden producir si la convergencia lenta de una red en una nueva configuración hace que las entradas de enrutamiento sean incorrectas.



1. La red ha convergido. La ruta preferida de C a 1 es a través de B.

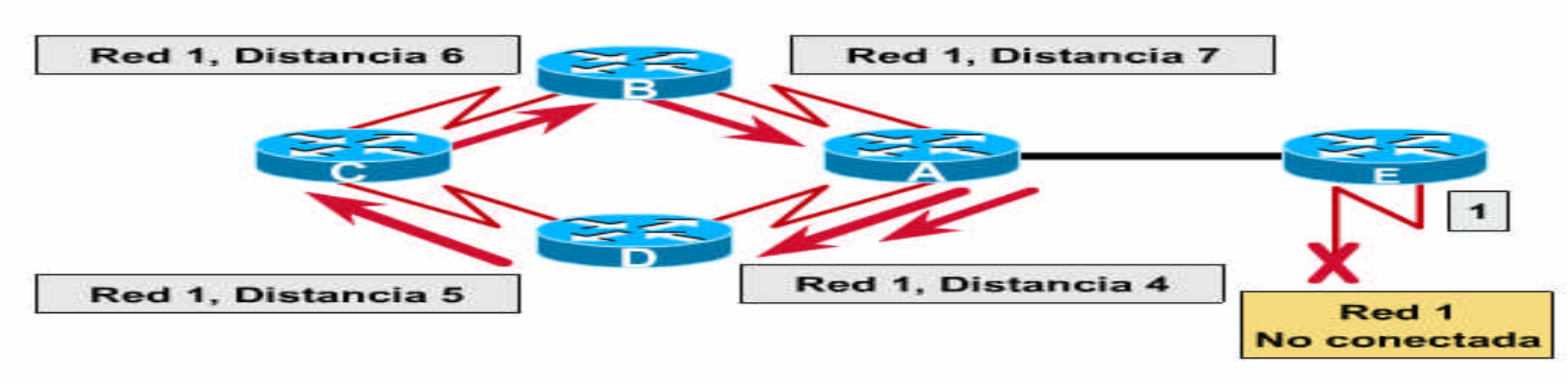
2. La red 1 falla, E manda actualización a A. A manda actualización a B y D, C no sabe nada.

3. C envía actualización a D, éste a A, y éste a B y E ✍ loop C, B, A, D …….

Enrutamiento vector-distancia 3/5

El problema de la cuenta al infinito

- **Las actualizaciones no válidas de la Red 1 (está caida) seguirán andando en círculos hasta que algún otro proceso detenga el recorrido del loop ✍ cuanta al infinito.**
- **Mientras los routers cuentan al infinito, la información no válida permite que se produzca un loop de enrutamiento.**
- **Si no se toman medidas para detener el proceso, el vector-distancia (métrica) de número de saltos se incrementa cada vez que el paquete atraviesa otro router.**
- **SOLUCION ✍ Definir un máximo: definir el infinito como un número máximo específico. Este número se refiere a la *métrica de enrutamiento* (por ej., un número de saltos simple). Superado el máximo, se descarta paquete, y se considera la red inalcanzable.**



Enrutamiento vector-distancia 4/5

Split horizon (horizonte dividido)

Otro origen posible de un loop de enrutamiento es cuando información incorrecta que se ha enviado a un router se contradice con la información correcta que éste envió.

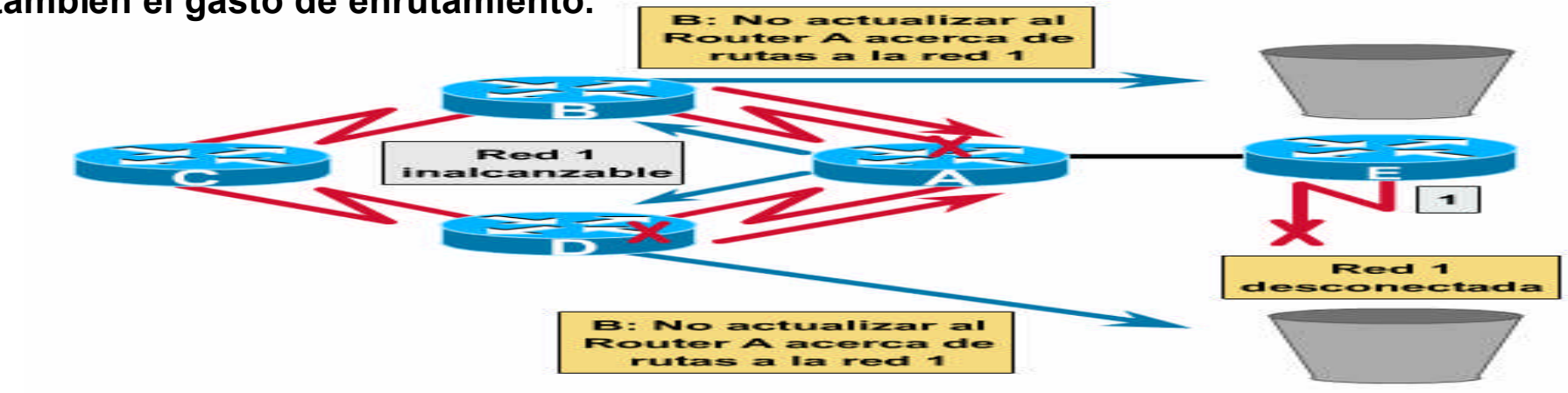
1. A ✍ B y D, red 1 fuera de servicio ; C ✍ B, red 1 distancia 4 a través de D.

2. B ✍ A, le comunica la nueva ruta……..

3. Loop de enrutamiento : A✍ B ✍ C ✍ D

<u>Lógica del Split Horizon</u> : Nunca es conveniente devolver una información sobre una ruta a la dirección desde la que ha llegado.

El split horizon reduce así la cantidad de información de enrutamiento incorrecta y reduce también el gasto de enrutamiento.



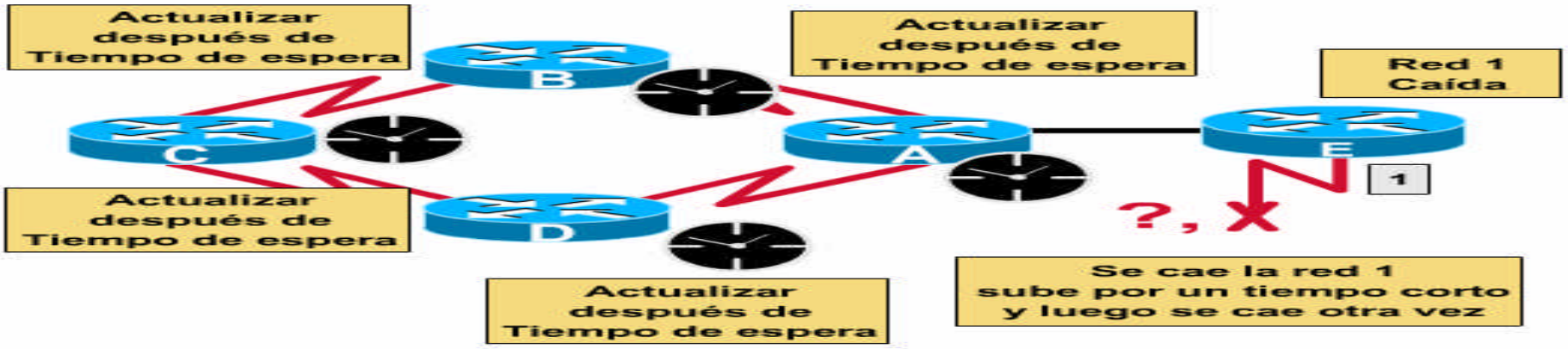
Enrutamiento vector-distancia 5/5

Temporizadores de espera

Se puede evitar el problema de cuenta al infinito mediante *temporizadores de espera*

Suponemos: red 1 inicialmente accesible, RouterA recibe de RouterE actualización : red 1 inaccesible, RouterA marca la ruta a la red 1 como inaccesible e inicia un temporizador de espera.

1. **Antes de que expire el temporizador, se recibe act. desde RouterE como accesible, se elimina el temporizador y se marca la red 1 como accesible.**
2. **Antes de que expire el temporizador, se recibe act. desde RouterX (cualquiera) como accesible con mejor métrica que la inicialmente registrada, se elimina el temporizador y se marca la red1 como accesible.**
3. **Antes de que expire el temporizador, se recibe act. desde RouterX (cualquiera) como accesible con peor métrica que la inicialmente registrada, se ignora la actualización.**



Enrutamiento estado de enlace 1/2

Aspectos básicos del enrutamiento estado de enlace

- **También conocidos como algoritmos *SPF (primero la ruta libre más corta).***
- **Mantienen una compleja base de datos de información de topología.**
- **Un algoritmo de enrutamiento estado de enlace conoce perfectamente los routers distantes y cómo se interconectan. Ej: OSPF.**

Enrutamiento estado de enlace 2/2

Propagación de los cambios de topología en estado-enlace

- **Siempre que una topología estado-enlace cambia, el router que primero se da cuenta del cambio envía la información a los demás routers o a un router designado que todos los demás routers pueden utilizar para realizar las actualizaciones.**

Para lograr la convergencia, cada router debe realizar lo siguiente:

1. **Mantener seguimiento de los routers vecinos: nombre, estado, costo del enlace.**
2. **Construcción de un paquete LSA que describa a los routers vecinos.**
3. **Envío de este paquete LSA para que todos los demás routers lo reciban**
4. **Registrar los paquetes LSA recibidos en la base de datos para que actualice el paquete LSA generado más recientemente por cada router.**
5. **Completar un mapa de la internetwork utilizando datos de los paquetes LSA acumulados y luego calcular rutas hacia todas las demás redes utilizando el algoritmo SPF.**

- **Cada vez que un paquete LSA provoca un cambio en la base de datos estado-enlace, el algoritmo de estado-enlace (SPF) vuelve a calcular cuáles son las mejores rutas y actualiza la tabla de enrutamiento.**

Entorno de los protocolos de enrutamiento 1/2

Comparación entre los protocolos de enrutamiento por vector-distancia y de estado-enlace

Vector -Distancia	Estado -Enlace
Visualizar la topología de red desde la perspectiva del vecino	Obtiene una visión común de toda la topología de red
Agrega vectores de distancia de router a router	Calcula la ruta más corta hacia los otros routers
Actualizaciones frecuentes, periódicas: Convergencia lenta	Actualizaciones activadas por eventos: Convergencia más rápida
Envía copias de las tablas de enrutamiento hacia los routers vecinos	Envía actualizaciones de enrutamiento de estado de enlace hacia los otros routers

Entorno de los protocolos de enrutamiento 2/2

Protocolos de enrutamiento híbrido

- **Combinan los aspectos del enrutamiento por vector-distancia y de estado de enlace ✍ e*nrutamiento híbrido balanceado*.**

- **Utilizan vectores de distancia con métricas más precisas para determinar las mejores rutas hacia las redes destino.**

- **Utilizan cambios de topología para provocar actualizaciones en las bases de datos de enrutamiento.**

- **Converge rápidamente, como los protocolos de estado de enlace.**

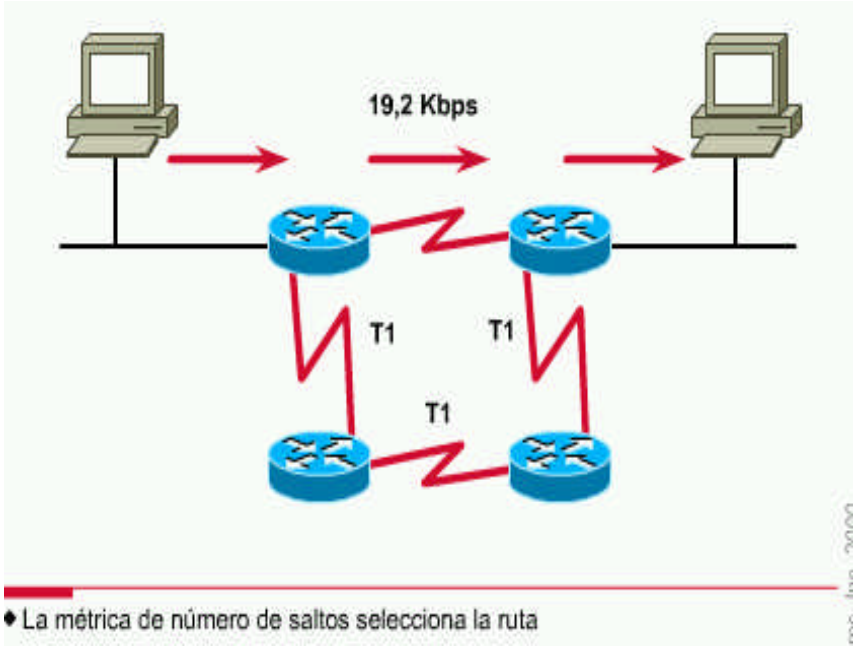
- **Utilizan menos recursos de ancho de banda, memoria y ciclos del procesador.**

- **Ejemplos : *IS-IS de OSI (Sistema intermedio a Sistema intermedio)* y *el protocolo EIGRP (Protocolo de enrutamiento de gateway interior mejorado) de Cisco*.**

Comandos de configuración: Protocolos de enrutamiento

- El comando `router` inicia el proceso de enrutamiento.
- El comando `network` es necesario porque permite que el proceso de enrutamiento pueda determinar cuáles son las interfaces que participarán en el envío y la recepción de actualizaciones de enrutamiento.
- Los números de red se deben basar en las direcciones de clase de red, no en direcciones de subred ni direcciones de host individuales. La direcciones de red principales se limitan a los números de red Clase A, B y C.

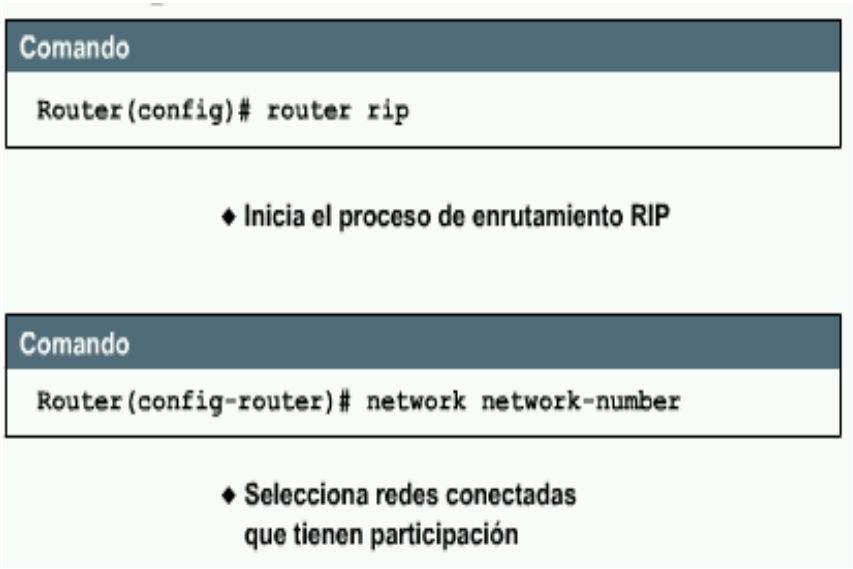
Funcionamiento RIP



♦ La métrica de número de saltos selecciona la ruta

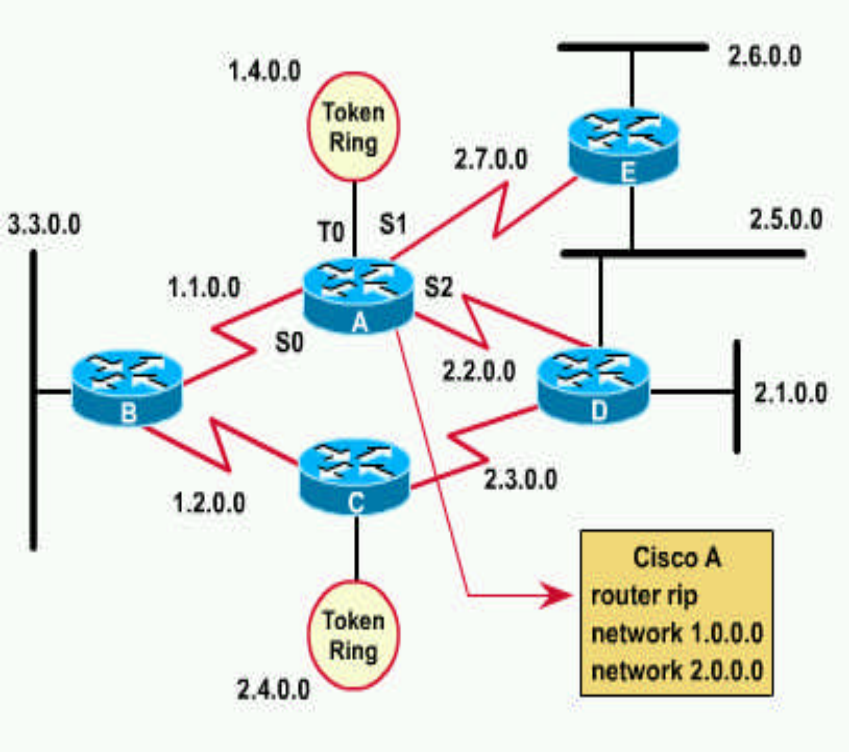
- RIP se especificó originalmente en RFC 1058. Sus principales características son las siguientes:
- Es un protocolo de enrutamiento por vector-distancia.
- Utiliza el número de saltos como métrica para la selección de rutas.
- Si el número de saltos es superior a 15, el paquete se descarta.
- Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 30 segundos.
- La distancia administrativa es de 120.

Comandos RIP



- El comando `router rip` selecciona a RIP como el protocolo de enrutamiento.
- El comando network asigna una dirección de `clase de red` a la cual un router se conectará directamente.
- El proceso de enrutamiento asocia interfaces con direcciones de red y empieza a utilizar RIP en las redes especificadas.
- Nota: En RIP todas las máscaras de subred deben ser las mismas. RIP no comparte la información de división en subredes en las actualizaciones de enrutamiento.

Ejemplo RIP

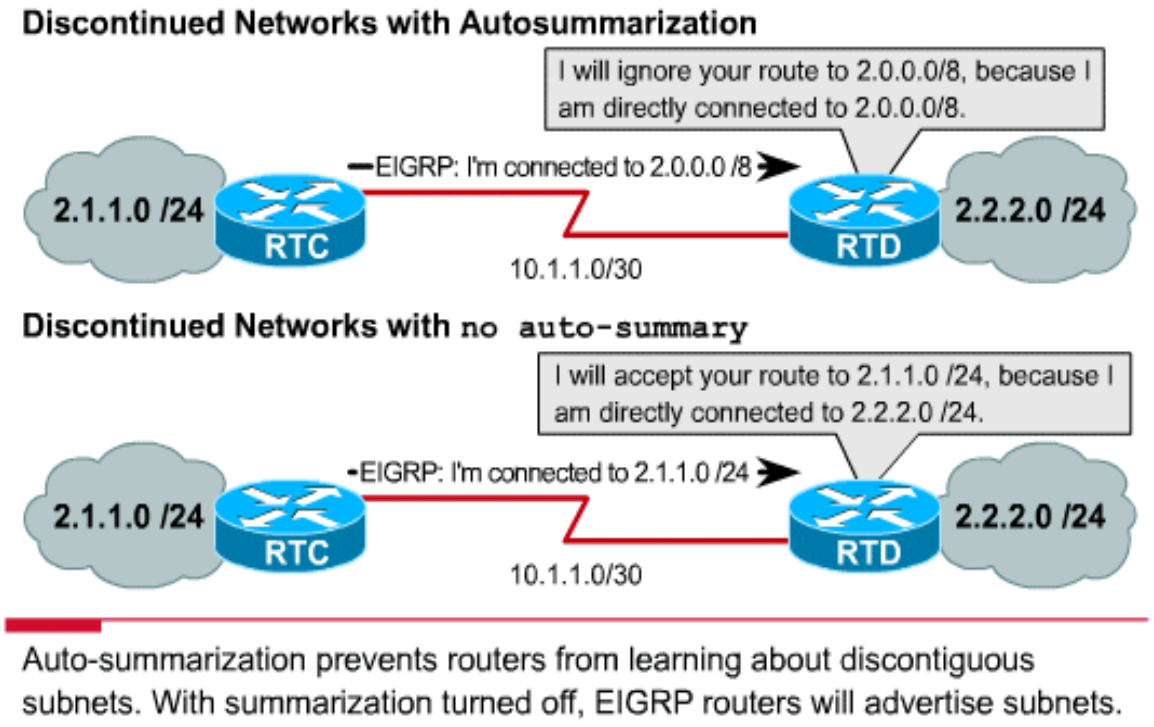


- `router rip` : selecciona a RIP como el protocolo de enrutamiento
- `network 1.0.0.0` : especifica una red directamente conectada
- `network 2.0.0.0` : especifica una red directamente conectada
- Las interfaces del router Cisco A que se encuentran conectadas a las redes 1.0.0.0 y 2.0.0.0 envían y reciben actualizaciones RIP. Estas actualizaciones de enrutamiento permiten que el router conozca la topología de red.

Otros conceptos y protocolos de enrutamiento

- **Auto-Sumarización**
- **RIPv2**
- **IGRP**
- **OSPF**
- **EIGRP**

Auto-sumarización



Auto-summarization prevents routers from learning about discontiguous subnets. With summarization turned off, EIGRP routers will advertise subnets.

- **La Sumarización es por defecto a clases principales**: máscaras /8, /16 o /24.
- *Pero RIP v2 o* ***EIGRP realizan un auto- summarization únicamente cada vez que se cruza una frontera entre dos clases principales difererentes****.*
- **En esta figura, debido a que RTC y RTD tienen ambos redes de clase general (1.0.0.0/8 y 2.0.0.0/8) y los paquetes son enviados a través de ellas , entonces se sumarizará por defecto.**

Características esenciales del RIP

Maduro (fue el primero)

Estable (depende ;-))

Ampliamente soportado (incluso en viejos servidores UNIX)

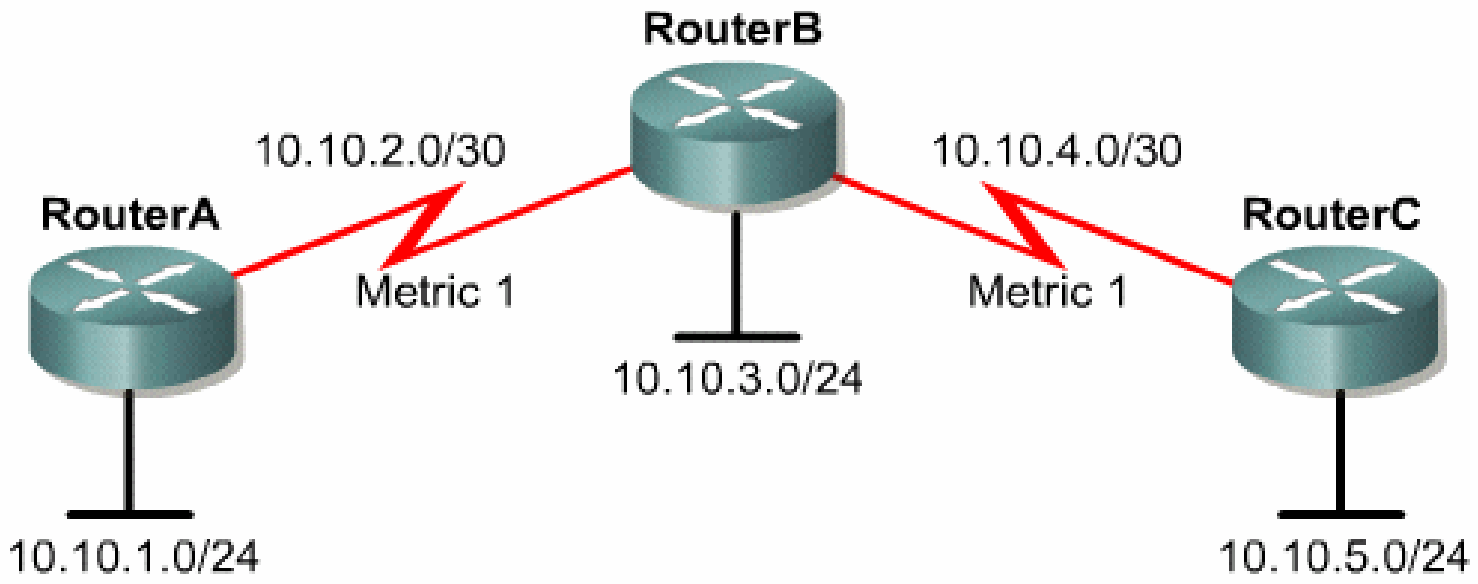
Fácil de configurar

Hay que tener en cuenta que, RIP v1 anuncia subredes sin la máscara (no sólo redes principales), únicamente si la subred anunciada tiene la misma submáscara que la interfaz a través de la cual son anunciados.

Esto es debido a que el router RIP v1 piensa que si se tiene la misma subred en el interfaz de recepción, asume que ya se es capaz de manejar estas subredes. Y las subredes con una máscara diferente, no serán anunciadas.

Algunas personas dicen que el RIP es un insulto para los protocolos de encaminamiento.

RIP v2

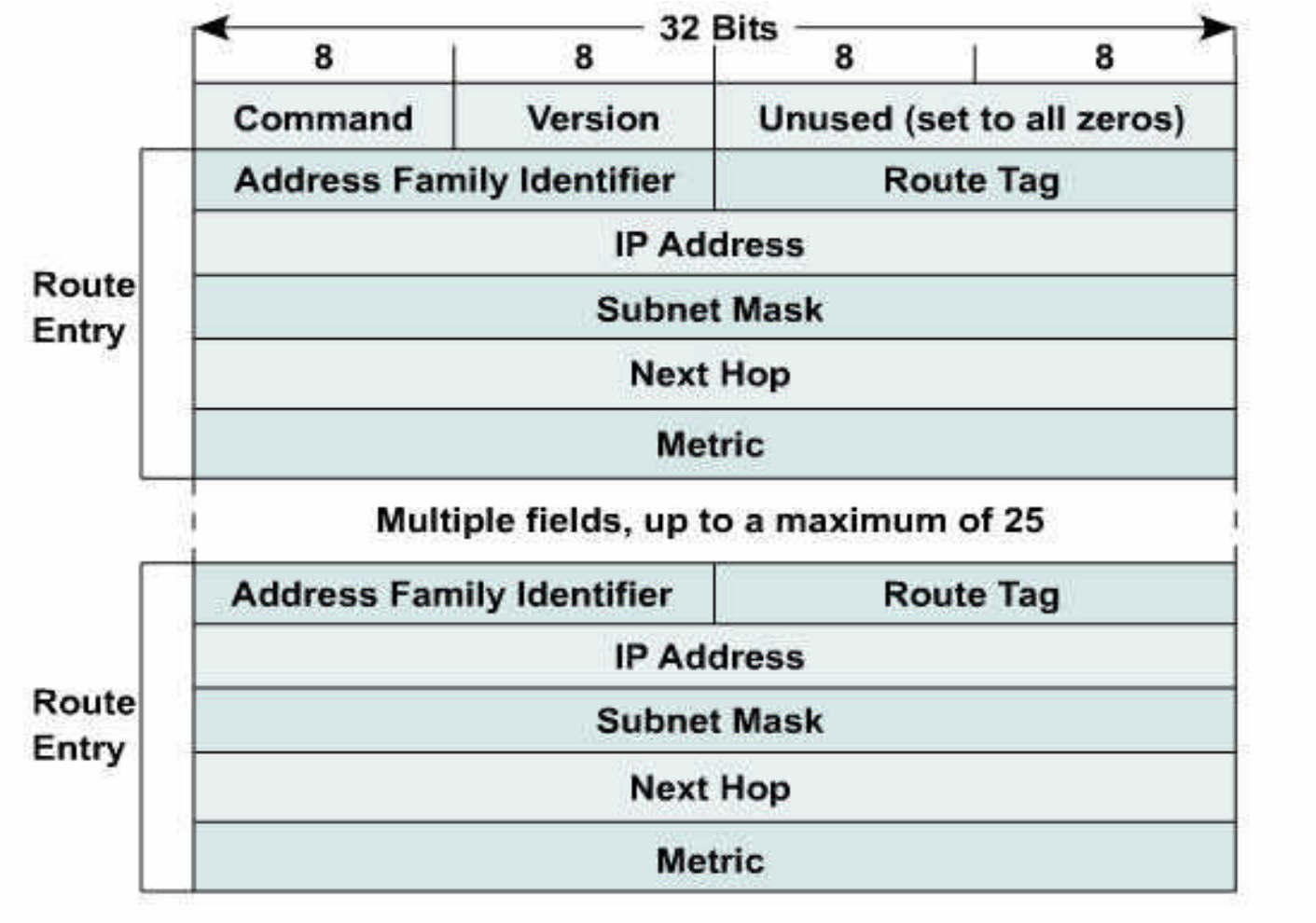


La clase principal 10.0.0.0/8 es particionada en subredes.

Rasgos de RIP v2

- Autenticación
- Adición of mascaras de red y VLSM
- Next hop IP addressed
- Multicasting RIP v2 en las actualizaciones de rutas

Formato del mensaje RIP v2



Compatibilidad con RIP v1

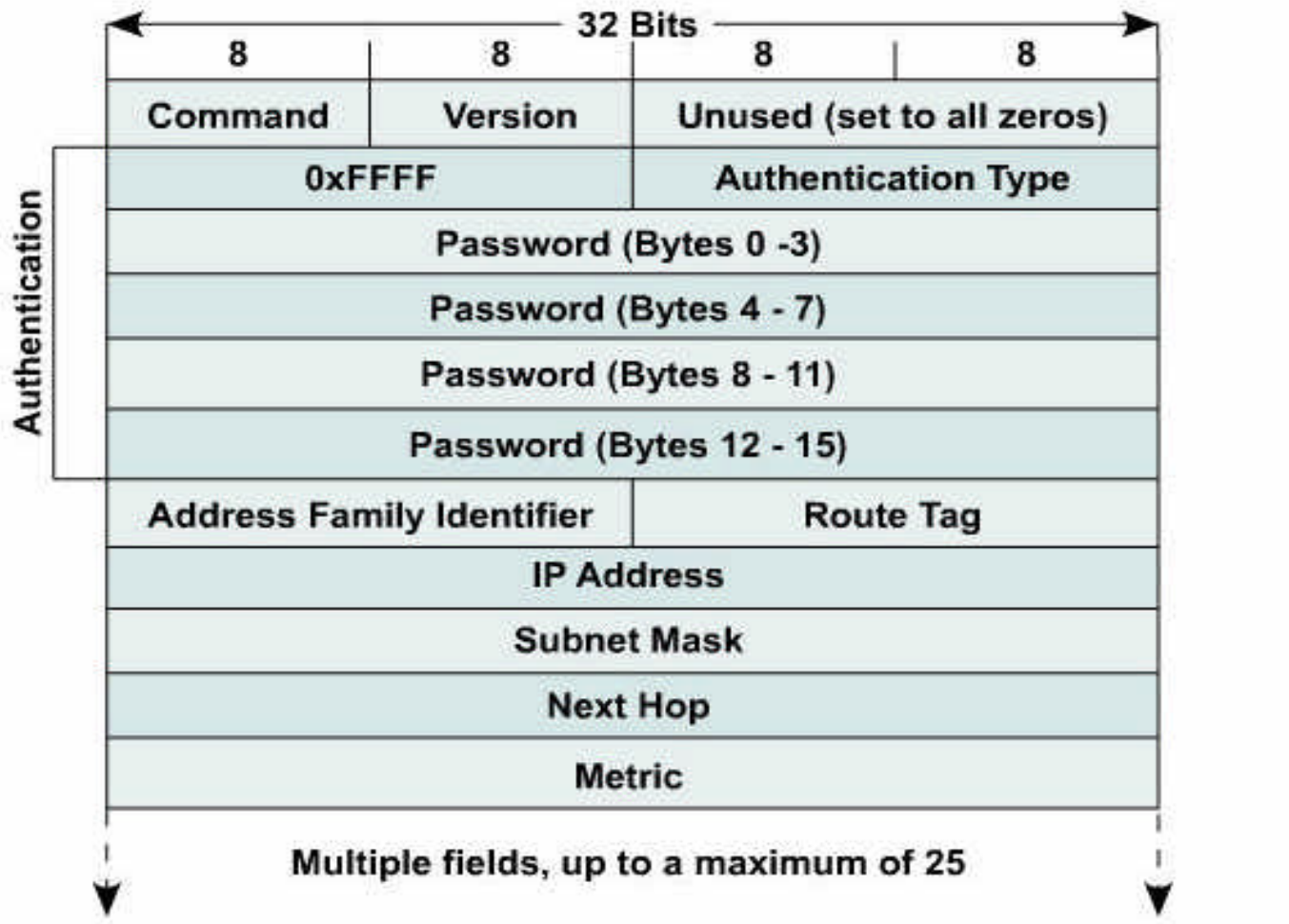
- **RFC 1723 define la compatibilidad, la cual permite que las versiones 1 y 2 interoperen:**

  RIP v1, en el cual únicamente mensajes RIP v1 son transmitidos.

  RIP v1 Compatibilidad, la cual hace posible la difusion (broadcast) de mensajes RIP v2 en lugar de hacer uso de multicast para que de este modo RIP v1 pueda recibirlas.

  RIP v2, en el cual los mensajes RIP v2 son dirigidos mediante multicast a la dirección destino 224.0.0.9.

Autenticación RIP v2



Limitaciones de RIP v2

Las limitaciones más significantes que son heredadas por RIP v2 incluyen las siguientes:

- –Falta de rutas alaternativas: Únicamente la mejor
- –Cuenta al infinito
- –15-saltos máximos
- – Estáticas métricas de vector distancia: ninguna información adicional sobre la red, únicamente saltos.

RIP v2 y Cisco IOS

Por defecto, un proceso de RIP configurado sobre un router Cisco envía sólo mensajes RIPv1, pero escucha tanto RIP v1 como RIP v2.

Esto puede ser cambiado mediante el comando de versión. De esta forma, el router envía y recibe sólo mensajes RIPv2.

Configuración Basica RIP v2

Command
`Router(config)#router rip`

- Starts the RIP routing process

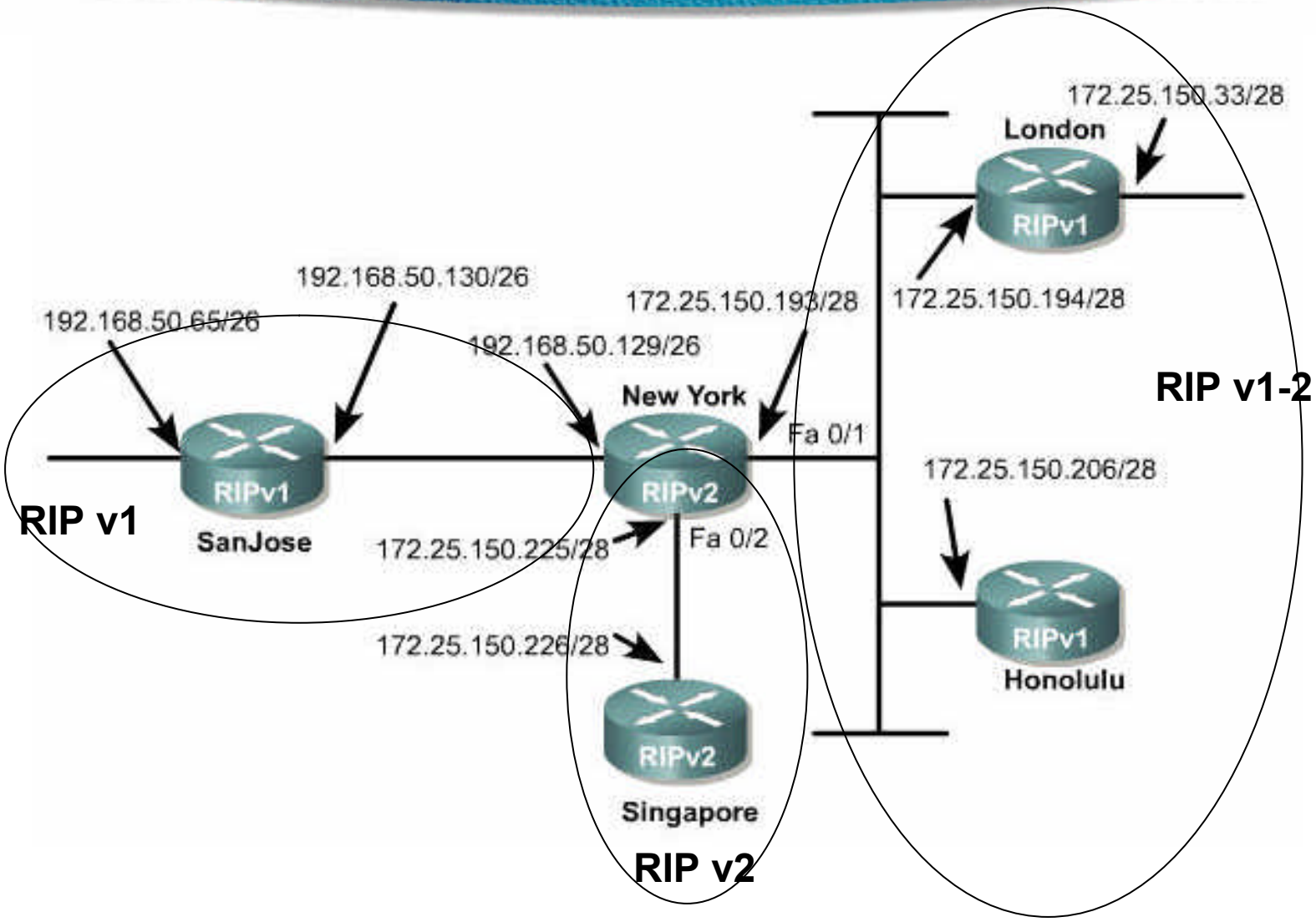
Command
`Router(config-router)#network network-number`

- Selects participating attached networks

Command
`Router(config-router)#version 2`

La mascara de subred es tomada de la configuración de interfaces

Ejemplo: RIP v2 Compatible con RIP v1



Ejemplo: Configuración New York

```
NewYork(config)#interface fastethernet0/0
  NewYork(config-if)#ip address 192.168.50.129 255.255.255.192
  NewYork(config-if)#ip rip send version 1
  NewYork(config-if)#ip rip receive version 1

NewYork(config)#interface fastethernet0/1
  NewYork(config-if)#ip address 172.25.150.193 255.255.255.240
  NewYork(config-if)#ip rip send version 1 2

NewYork(config)#interface fastethernet0/2
  NewYork(config-if)#ip address 172.25.150.225 225.255.255.240

NewYork(config)#router rip
  NewYork(config-router)#version 2
  NewYork(config-router)#network 172.25.0.0
  NewYork(config-router)#network 192.168.50.0
```

Redes discontinuas (separadas) y Classless Routing

RIP v1 siempre usa sumarización automática. Por defecto, el comportamiento de RIP v2 es sumarizar en direcciones de clase de red al igual que RIP v1.

Hay que usar el comando **`no auto-summary`** **con el RIP para desactivar la sumarización y permitir que las subredes sean anunciadas.**
Esto permitirá a RIP v2 realizar enrutamiento entre redes discontinuas mediante el anuncio de información de subredes

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
```

Configurando Autenticación en RIP v2

- **Pasos:**
  1. **Definir una "key chain" con un nombre.**
  2. **Definir las "key" o "keys" sobre la "key chain".**
  3. **Habilitar autenticación sobre una interfaz y especificar la "key chain" a usar.**
  4. **Especificar si la interfaz usará texto claro o autenticación MD5.**
  5. **Opcionalmente configurar la gestión de clave.**

Ejemplo de Autenticación

Ejemplo:

•Se configura una "key chain" denominada Romeo
•Key 1, la única clave sobre la cadena (chain), tiene el password Juliet
•FastEthernet0/0 then usa the clave, con autenticación MD5 para validar las actualizaciones desde los routers RIP v2 vecinos.

```
Router(config)#key chain Romeo
Router(config-keychain)#key 1
Router(config-keychain-key)#key-string Juliet

interface fastethernet 0/0
Router(config-if)#ip rip authentication key-chain Romeo
Router(config-if)#ip rip authentication mode md5
```

Verificando operación RIP v2 : comando `show ip protocols`

Cisco - Router

```
Router#show ip protocols
Routing Protocol is "rip"
 Sending updates every 30 seconds, next due in 8 seconds
 Invalid after 180 seconds, hold down 180, flushed after 240
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Redistributing: rip
 Default version control: send version 2, recieve version 2
   Interface    Send  Recv  Triggered RIP  Key-chain
   Ethernet2    2     2
   Ethernet3    2     2
   Ethernet4    2     2
   Ethernet5    2     2
 Automatic network summarization is not in effect
 Address Summarization:
  12.11.0.0/16 for Ethernet2
```

Comandos Debug

- Dos problemas de configuración comunes a RIP v2

  a) Entremezcladas versiones

  b) Inapropiada configuración de autenticación

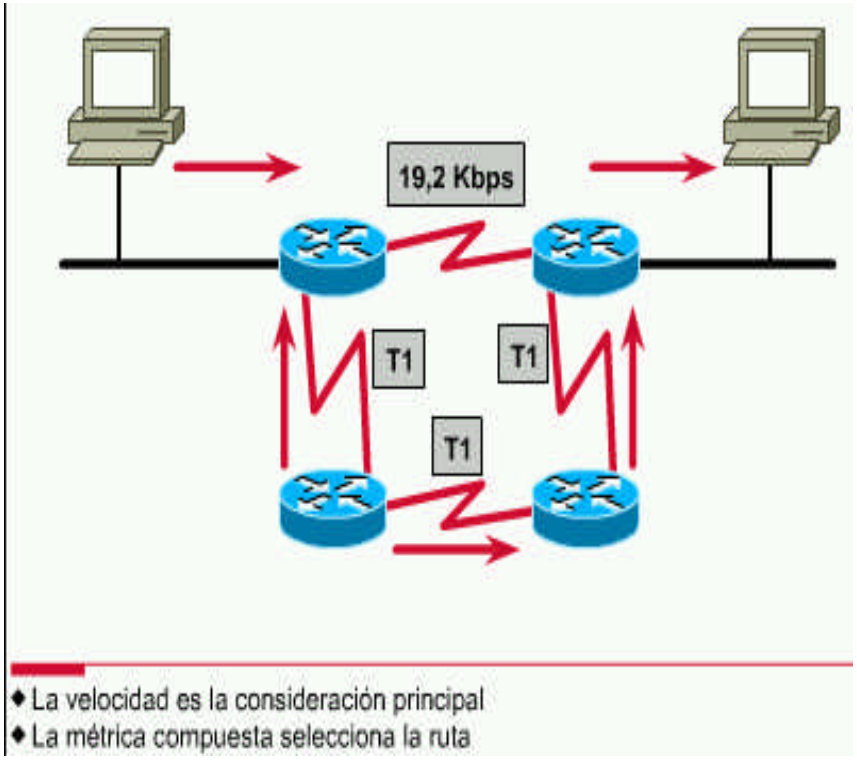
- Usar el EXEC comando `debug ip rip` para mostrar información sobre las transacciones del enrutamiento RIP.

```
Router#debug ip rip [events]
```

- Usar the `debug ip routing` EXEC para mostrar información sobre las tablas de enrutamiento RIP y actualizaciones de “route-cache”.

```
Router#debug ip routing
```

Funcionamiento IGRP



- **IGRP envía actualizaciones de enrutamiento a intervalos de 90 segundos, publicando las redes en un sistema autónomo en particular.**
- **La ruta elegida será la de menor métrica compuesta (Intervienen 5 factores: ancho de banda, retraso, carga, confiabilidad y Unidad Máxima de Transferencia o MTU).**
- **Utiliza por defecto dos métricas, ancho de banda y retardo. IGRP puede utilizar una combinación de variables para determinar una métrica compuesta.**
- **La distancia administrativa es de 100.**
- **La consideración principal es la velocidad.**

Comandos IGRP

Comando
`Router(config)# router igrp autonomous-system`

- Define IGRP como un proceso de enrutamiento IP

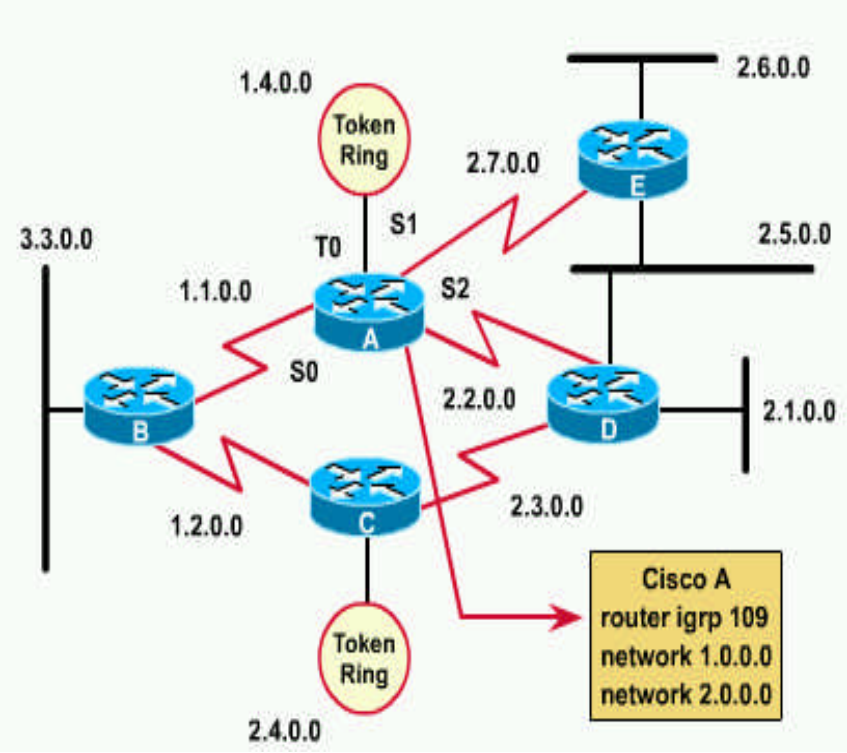
Comando
`Router(config-router)# network network-number`

- Selecciona las redes participantes directamente conectadas

comando `router igrp`	Descripción
`autonomous-system`	identifica los procesos del router IGRP que compartirán información de enrutamiento

Comando `network`	Descripción
`network-number`	especifica una red directamente conectada, una dirección de red que respeta las clases, describe una dirección de red Clase A, B o C.

Ejemplo IGRP



- **Se selecciona IGRP como el protocolo de enrutamiento para el sistema autónomo 109. Todas las interfaces conectadas a las redes 1.0.0.0 y 2.0.0.0 se utilizarán para enviar y recibir actualizaciones de enrutamiento IGRP. En el ejemplo:**
- ***router igrp 109*: selecciona IGRP como el protocolo de enrutamiento para el sistema autónomo 109**
- ***network 1.0.0.0*: especifica una red directamente conectada**
- ***network 2.0.0.0*: especifica una red directamente conectada**

Comando show ip interfaces

```
Router> show ip interfaces
Ethernet0 is up, line protocol is up
  Internet address is 183.8.128.2, subnet mask is 255.255.255.128
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is enabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching enabled
  IP fast switching on the same interface is disabled
  IP SSE switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  Probe proxy name replies are disabled
  -- More --
```

- El comando `show ip interfaces` muestra el estado y los parámetros globales asociados con todas las interfaces IP. El software IOS de Cisco introduce automáticamente una ruta directamente conectada en la tabla de enrutamiento si el software puede enviar y recibir paquetes a través de esa interfaz. Esa interfaz se marca como activada o `up`. Si la interfaz no se puede utilizar, se elimina de la tabla de enrutamiento. Al eliminar esa entrada se permite el uso de rutas de respaldo, en el caso de que existan.

Comando show ip protocols

```
Router> show ip protocol
Routing Protocol is igrp 300
  Sending updates every 90 seconds, next due in 55 seconds
  Invalid after 270 seconds, hold down 280, flushed after 360
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
  IGRP maximum metric variance 1
  Redistributing igrp 300
  Routing for Networks:
    183.8.0.0
    144.253.0.0
  Routing Information Sources
    Gateway              Distance       Last Update
    144.253.100.1        100             0:00:52
    183.8.128.12         100             0:00:43
    183.8.64.130         100             0:01:02
  Distance: (default is 100)
-- More --
```

- **El comando `show ip protocol` muestra parámetros, filtros e información de red acerca de todos los protocolos de enrutamiento (es decir, RIP, IGRP, etc.) en uso en el router. El algoritmo utilizado para calcular la métrica de enrutamiento para IGRP aparece en la pantalla. Define el valor de la métrica K1-K5 y el máximo número de saltos. La métrica K1 representa el ancho de banda y la métrica K3 representa el retardo. Por defecto, los valores de las métricas K1 y K3 se establecen en 1. Los valores métricos de K2, K4 y K5 se establecen en 0.**

Comando show ip route

```
Router> show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E-EGP
       i - IS-IS, L1 - IS-IS level 1, L2 - IS-IS level 2
       * - candidate default

Gateway of last resort is not set

   144.253.0.0 is subnetted (mask is 255.255.255.0). 1 subnets
C  144.253.100.0 is directly connected, Ethernet1
I  133.3.0.0 [100/1200] via 144.253.100.200, 00:00:57, Ethernet1
I  153.50.0.0 [100/1200] via 183.8.128.12, 00:00:05, Ethernet0
   183.8.0.0 is subnetted (mask is 255.255.255.128), 4 subnets
I  183.8.0.128 [100/180671] via 183.8.64.130, 00:00:27, Serial1
   [100/180671] via 183.8.128.130, 00:00:27, Serial0
C  183.8.128.0 is directly connected, Ethernet0
C  183.8.64.128 is directly connected, Serial1
C  183.8.128.128 is directly connected, Serial0
I  172.16.0.0 [100/1200] via 144.253.100.1, 00:00:55, Ethernet1
I  192.3.63.0 [100/1300] via 144.253.100.200, 00:00:58, Ethernet1
```

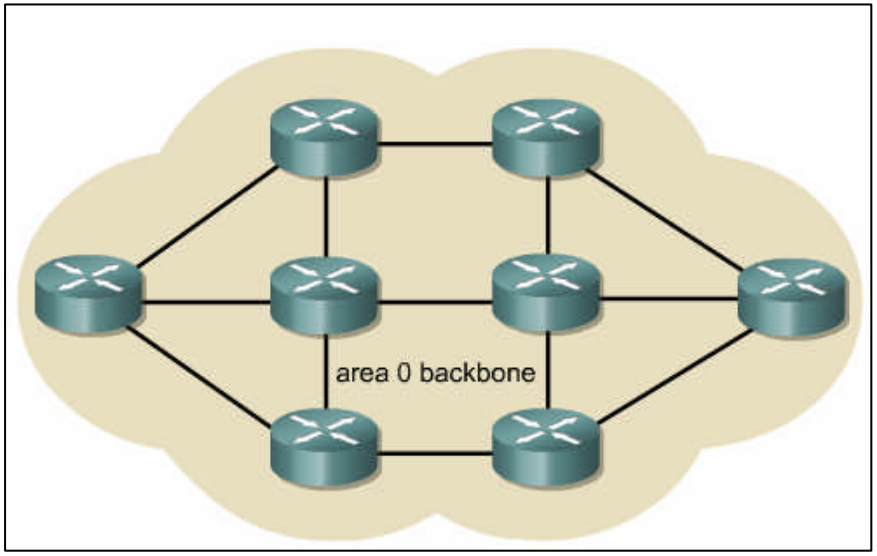
- **Muestra el contenido de la tabla de encaminamiento IP, que contiene todas las entradas para todas las redes y subredes conocidas, y los códigos que indican como se ha aprendido la información (I,C,R...).**

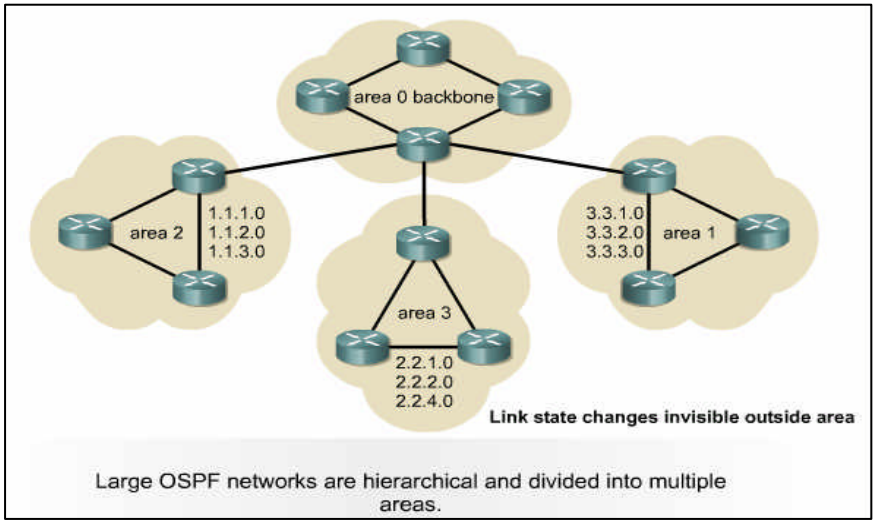
Comando debug ip *protocolo*

```
Router# debug ip rip
RIP Protocol debugging is on
Router#
RIP: received update from 183.8.128.130 on Serial0
     183.8.0.128 in 1 hops
     183.8.64.128 in 1 hops
     0.0.0.0 in 16 hops (inaccessible)
RIP: received update from 183.8.64.140 on Serial1
     183.8.0.128 in 1 hops
     183.9.128.128 in 1 hops
     0.0.0.0 in 16 hops (inaccessible)
RIP: received update from 183.8.128.130 on Serial0
     183.8.0.128 in 1 hops
     183.8.64.128 in 1 hops
     0.0.0.0 in 16 hops (inaccessible)
RIP: sending update to 255.255.255.255 via Ethernet0 (183.8.128.2)
     subnet 183.8.0.128, metric 2
     subnet 183.8.64.128, metric 1
     subnet 183.8.128.128, metric 1
     default 0.0.0.0, metric 16
     network 144.253.0.0, metric 1
RIP: sending update to 255.255.255.255 via Ethernet1 (144.253.100.202)
     default 0.0.0.0, metric 16
     network 153.50.0.0, metric 2
     network 183.8.0.0, metric 1
```

- **El comando `debug ip rip` o `debug ip igrp transactions` muestran las actualizaciones de enrutamiento RIP o IGRP respectivamente a medida que se envían y reciben.**
- **En este ejemplo, 183.8.128.130 envía la actualización. Informa sobre tres routers, uno de los cuales es inaccesible debido a que su número de saltos es mayor que 15.**
- **Los comandos debug son muy exigentes para el procesador y pueden empeorar el desempeño de la red o provocar pérdida de conectividad. Se debe utilizar únicamente en los horarios de uso menos intenso de la red. Hay que desactivar el comando una vez que se termina de usarlo (`no debug ip rip` o no debug ip transactions (en IOS versión 11 o superiores) y undebug (en IOS de versiones inferiores)**

Principios de OSPF

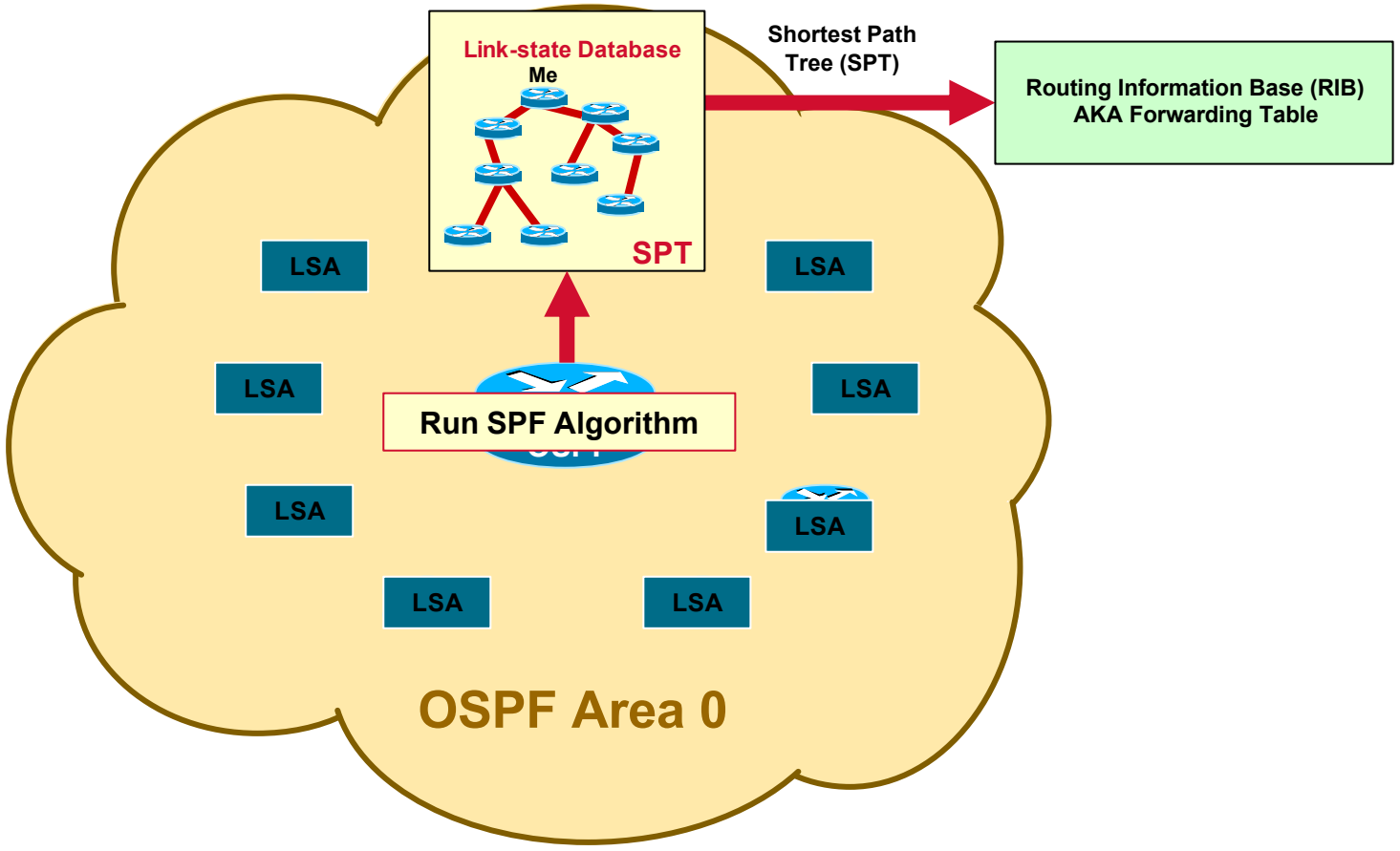




Large OSPF networks are hierarchical and divided into multiple areas.

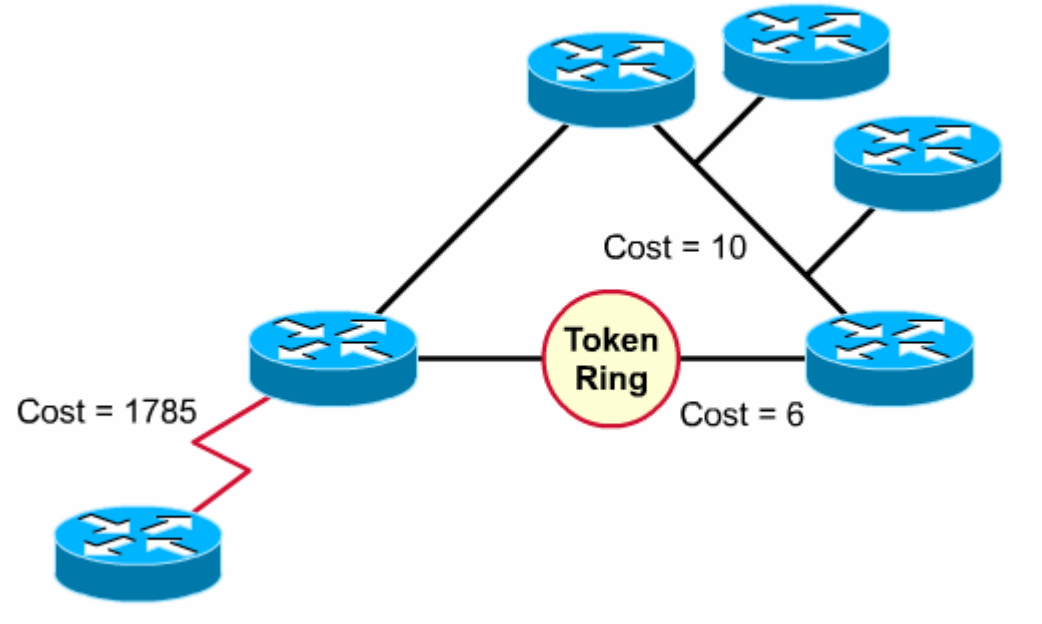
- OSPF puede ser usado y configurado como un área sola para pequeñas redes o puede ser usado para redes grandes.
- El Routing OSPF puede ser escalable a redes grandes si son usados principios de diseño de red jerárquicos.
- Múltiples áreas se conectan a un área de distribución, el área 0, también llamada backbone.
- Este diseño permite el control extenso de encaminamiento de actualizaciones.
- La definición las áreas reducen la sobrecarga, acelera la convergencia, y mejora el funcionamiento.

Elementos de OSPF



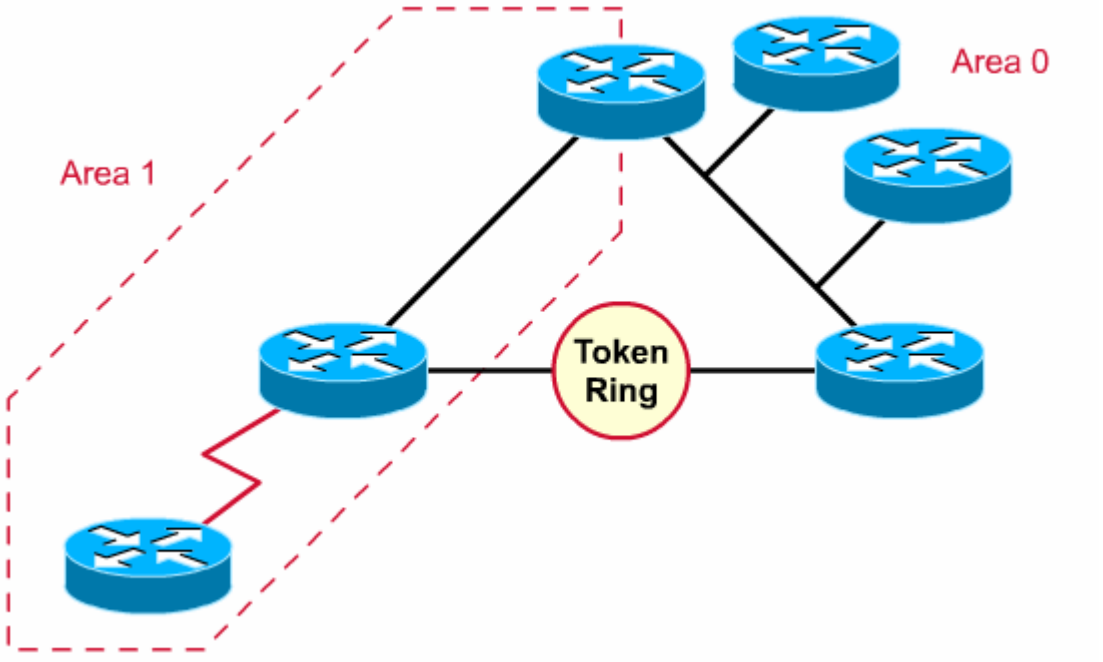
Métrica de OSPF basada en el Coste

- *Cost*: **Valor asignado a un enlace, basado en bandwidth (velocidad de transmisión).**



Áreas hacen OPSF escalable

- *Area*: colección de routers OSPF que tienen el mismo área de identificación.
- Area 0: Información de todad la red routers potentes (backbone).
- Otras Areas: Sólo información local y como llegar al Area 0.

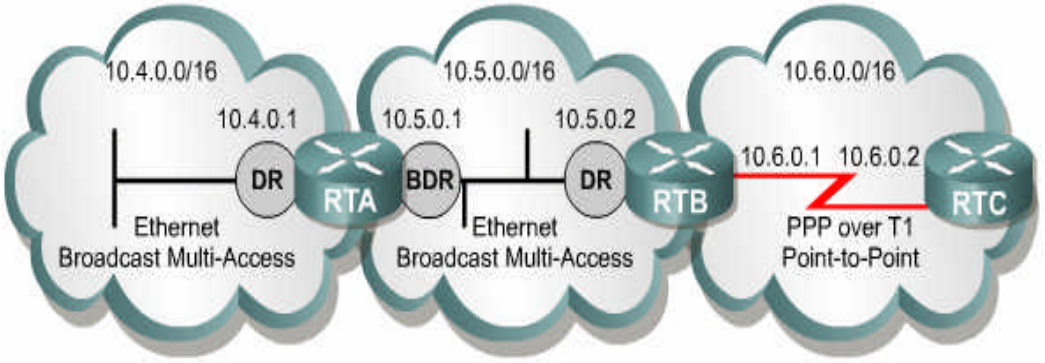


Areas OSPF

- Cada router OSPF debe pertenecer almenos a un área
- Cada red OSPF debe de tener un Area 0 (area backbone)
- El resto de Areas deberían estar conectadas al Area 0
- Los routers en el mismo área tienen la misma información.

DR/BDR

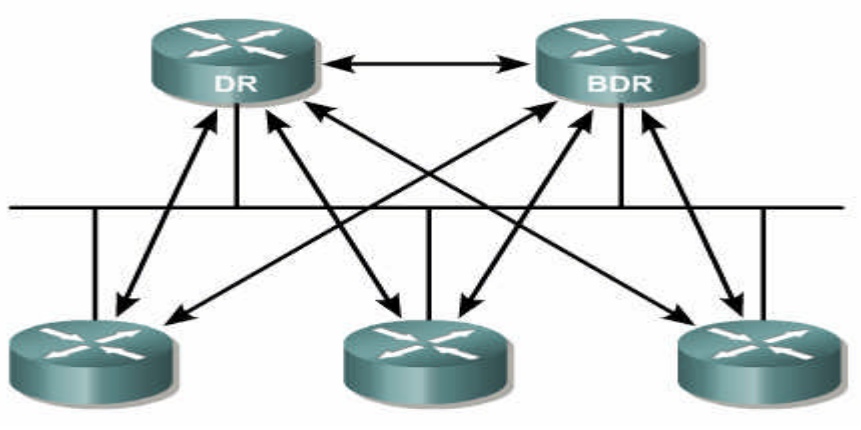
- ***Un DR/BDR se elige por medio en el caso de medios compartidos, en un enlace punto a punto no tiene sentido ya que no hay necesidad de centralizar la información de routing porque no es posible que cambie la topología de la red, de ahí la elección del DR/BDR; se hace en medios donde la topología es susceptible de cambiar (los compartidos).***
- ***DR*** **- Designated Router**
- ***BDR*** **– Backup DR.**



- **Para reducir el número de intercambios de la información de encaminamiento entre varios vecinos en la misma red, los routers OSPF eligen un router designado (DR) y otro de reserva (BDR) que sirvan como los puntos focales para el intercambio de información de encaminamiento.**

DR/BDR

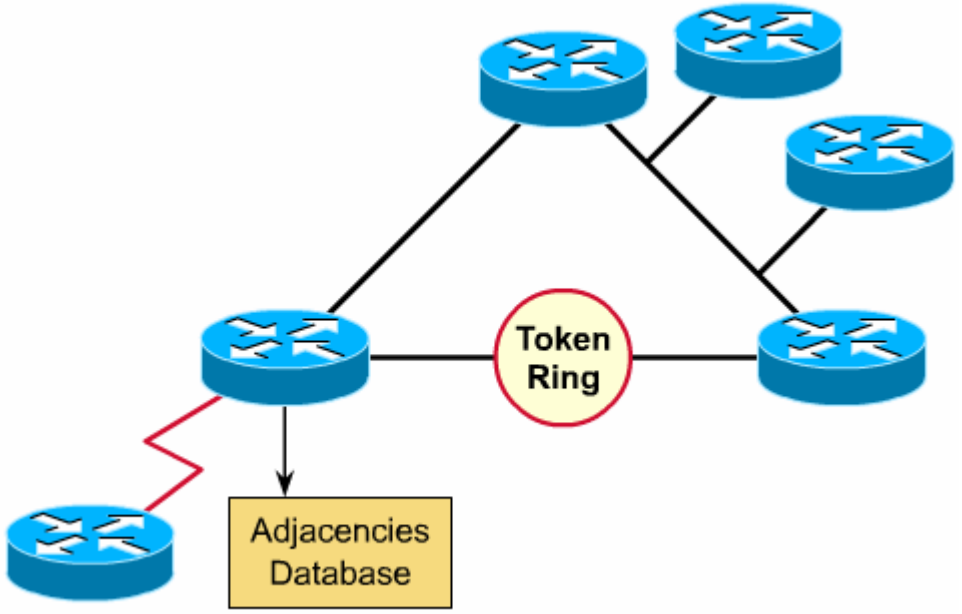
- **DR's sirve como puntos de colección para Link State Advertisements (LSAs), desde donde se difunden estos al resto de la red.**



- **Un BDR se usa como respaldo de DR.**
- **Si la red IP es *multi-aceso (ejemplo= ethernet)*, los routers OSPF elegirán 1 DR y 1 BDR (a menos que haya un sólo router en la red).**

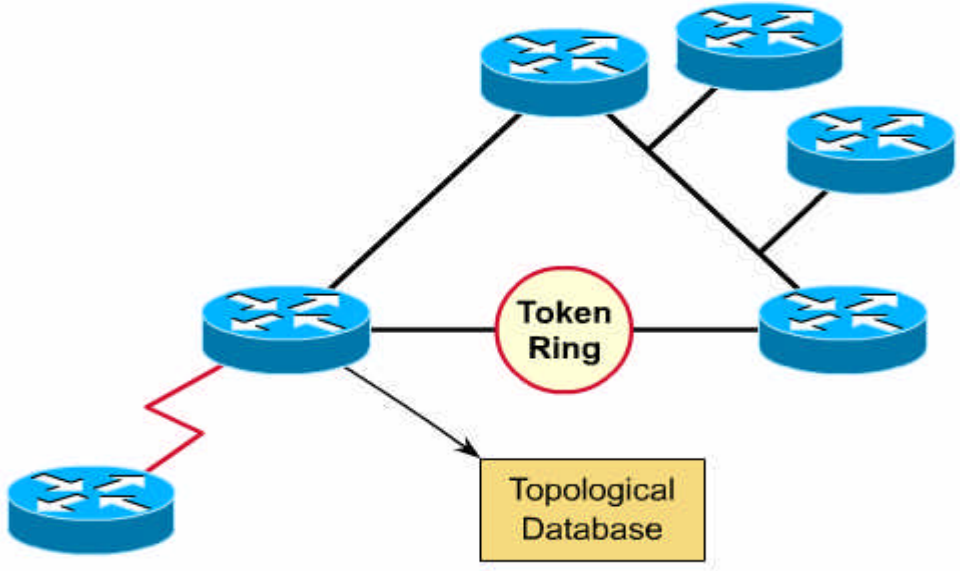
Base de Datos de Adyacencias

- **Los routers OSPF mantienen una lista de todos los vecinos con los cuales ellos han establecido comunicación bidireccional (uso de protocolo “Hello”).**



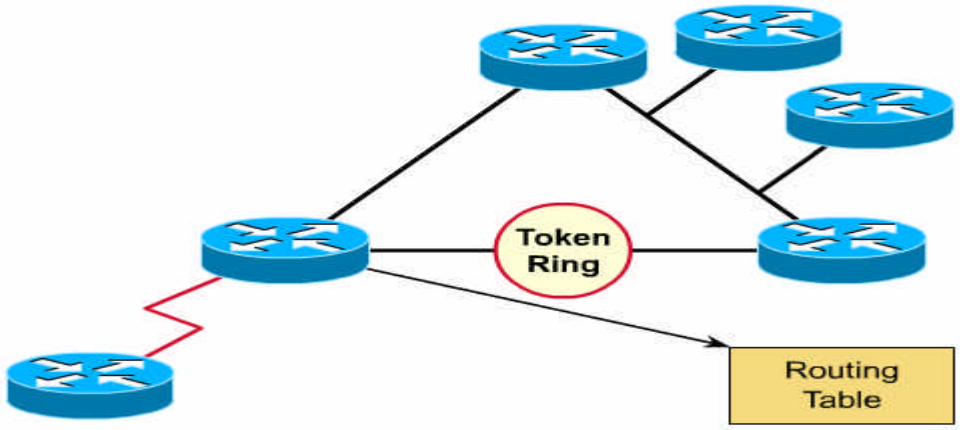
Link-state Database

- **Los Routers tratan la información sobre estados de enlace y construyen una base de datos, manteniendo la pista del resto de la internetwork.**



Forwarding Database

- Cada router OSPF usa su link-state database para generar una tabla de enrutamiento única.
- Cada router ejecuta el algoritmo del SPF en su propia copia de la base de datos. Este cálculo determina la mejor ruta a un destino. La trayectoria de coste más bajo se agrega a la tabla de encaminamiento (forwarding Database).



Relaciones con vecinos en OSPF

- **OSPF es capaz de establecer sofisticada comunicación entre vecinos.**
- **OSPF usa 5 tipos diferentes de paquetes para comunicar.**

Type	Description
1	Hello (establishes and maintains adjacency relationships with neighbors)
2	Database description packet (describes the contents of an OSPF router's link-state database)
3	Link-state request (requests specific pieces of a neighbor router's link-state database)
4	Link-state update (transports link-state advertisements (LSAs) to neighbor routers)
5	Link-state acknowledgement (Neighbor routers acknowledge receipt of the LSAs)

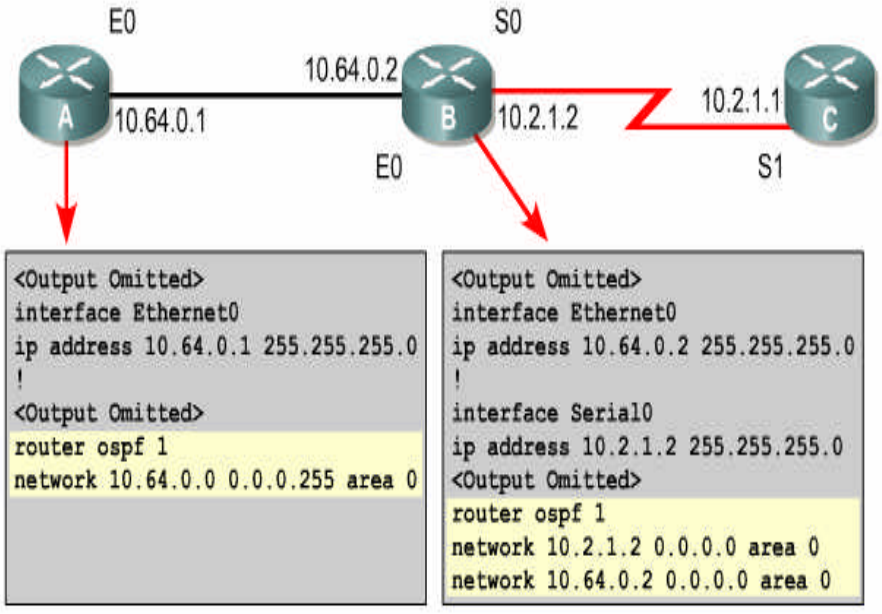
Operaciones en OSPF

1. Establecer adyacencias de router
2. Elegir DR y BDR
3. Descubrir Rutas
4. Seleccionar Rutas
5. Mantener Información de enrutamiento

Configuración OSPF básica

`Router(config)#router ospf process-id`

`Router(config-router)#network address wildcard-mask area area-id`



Network area Command	Description
address	Can be the network address, subnet, or the address of the interface. Instructs router to know which links to advertise, which links to listen to advertisements on, and what networks to advertise.
wildcard-mask	An inverse mask used to determine how to read the address. The mask has wildcard bits where 0 is a match and 1 is "do not care"; for example, 0.0.255.255 indicates a match in the first two bytes. (the equivalent REGULAR subnet mask would be a 16 bit mask of 255.255.0.0) If specifying the interface address, use mask 0.0.0.0.
area-id	Specifies the area to be associated with the address. Can be a number or can be similar to an IP address A.B.C.D. For a backbone area, the ID must equal 0.

Configurando direcciones OSPF loopback

```
! Create the loopback 0 interface
Sydney3(config)#interface loopback 0
Sydney3(config-if)#ip address 192.168.31.33
255.255.255.255
Sydney3(config-if)#exit
! Remove loopback 0 interface
Sydney3(config)#no interface loopback 0
Sydney3(config)#
01:47:27: %LINK-5-CHANGED: Interface Loopback0, changed
state to administratively down
```

Cuando el proceso del OSPF comienza, el IOS del Cisco utiliza el IP ADDRESS activo local más alto como identificación de router OSPF. Si no hay interfaz activo, el proceso del OSPF no comenzará. Si el interfaz esta caido, el proceso del OSPF no tiene ninguna identificación del router y por lo tanto deja de funcionar hasta que esté levantado.

Para asegurar estabilidad del OSPF se utiliza un interfaz del loopback (lógico),

Cuando se configura un interfaz del loopback, el OSPF utiliza esta dirección como la identificación, sin importar el valor. En un router que tenga más de un interfaz de loopback, el OSPF toma el IP ADDRESS más alto.

Establecer Prioridades

```
Sydney1(config)#interface fastethernet 0/0
Sydney1(config-if)#ip ospf priority 50
Sydney1(config-if)#end
Sydney1#
00:21:57: %SYS-5-CONFIG_I: Configured from console
by console
```

Las prioridades se pueden fijar a cualquier valor a partir de la 0 a 255.

Un valor de 0 previene que ese router sea el elegido. Un router con la prioridad más alta será seleccionado como el DR y el que tenga la segunda prioridad más alta será el BDR. Después del proceso de la elección, el DR y los BDR conservan su rol incluso si otros routers se agregan a la red con valores más altos de prioridad.

Métrica: Coste

```
Router(config)#interface serial 0/0
Router(config-if)#bandwidth 64

Router(config-if)#ip ospf cost number
```

Medium	Cost
56 kbps serial link	1785
T1 (1.544 Mbps serial link)	64
E1 (2.048 Mbps serial link)	48
4 Mbps Token Ring	25
Ethernet	10
16 Mbps Token Ring	6
100 Mbps Fast Ethernet, FDDI	1

OSPF utiliza como métrica el coste para determinar la mejor ruta. Se calcula el coste usando el fórmula 10^8/bandwidth, donde el ancho de banda se expresa en BPS.

Autenticación con MD5

Router(config-if)#ip ospf authentication-key *password*

Router(config-router)#area *area-number* authentication

Router(config-if)#ip ospf message-digest-key *key-id* md5 *encryption-type key*

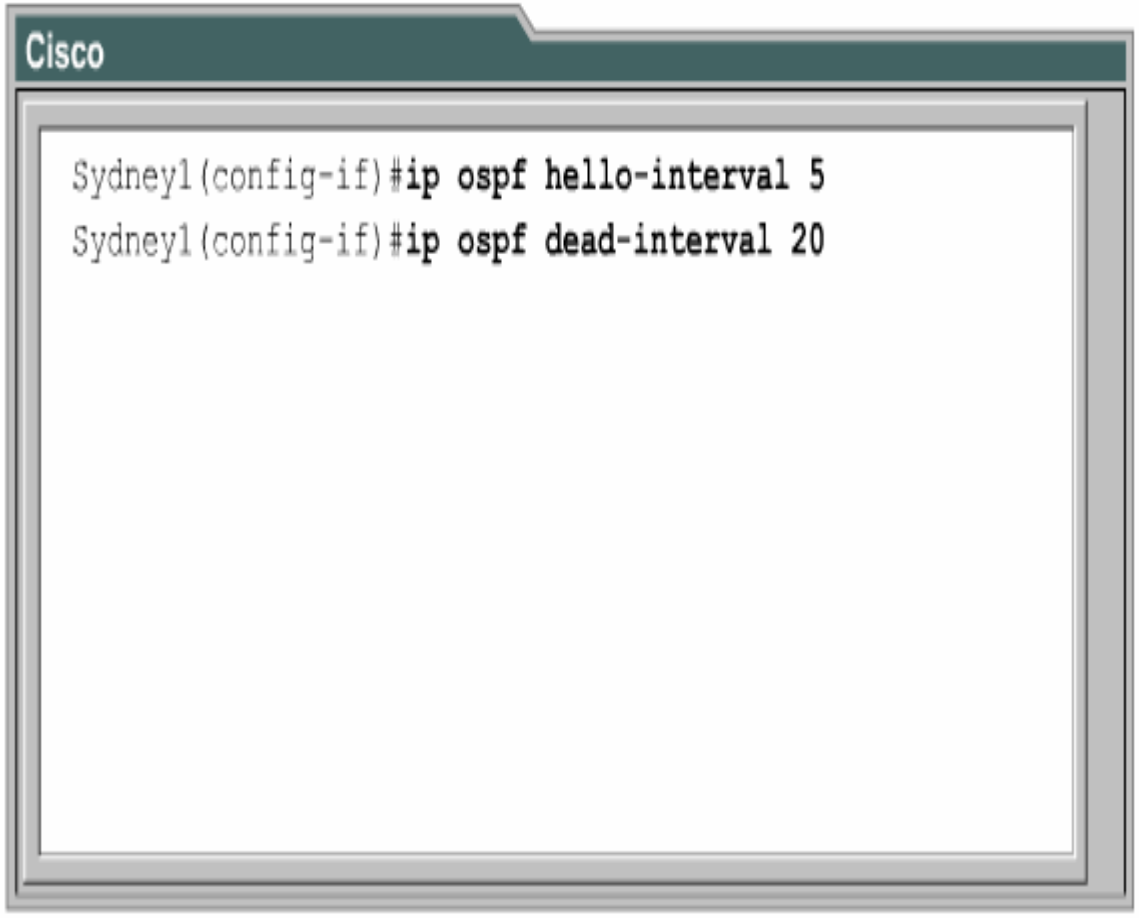
Router(config-router)#area area-id authentication message-digest

Cisco

```
Sydney1(config-if)#ip ospf message-digest-key 1 md5 7
asecret
Sydney1(config-if)#exit
Sydney1(config)#router ospf 1
Sydney1(config-router)#area 0 authentication message-
digest
Sydney1(config-router)#end
Sydney1#
```

Cada interfaz del OSPF puede presentar una clave de autenticación para que los routers puedan envíar la información del OSPF a otros routers en el segmento. La clave de la autenticación, conocida como contraseña, es secreta y compartida entre los routers. Esta clave se utiliza para generar los datos de la autenticación en la cabeza del paquete de OSPF. Se puede encriptar.

Intervalos hello y dead



Los routers deben tener los mismos hello intervalos y los mismos intervalos dead para intercambiar la información.

Por defecto, el intervalo dead es cuatro veces el valor del intervalo hello. Esto significa que un router tiene cuatro ocasiones de enviar un paquete hello antes de ser declarado dead.

Comandos de verificación

Command	Description
`show ip protocol`	Displays parameters about timers, filters, metrics, networks, and other information for the entire router.
`show ip route`	Displays the routes known to the router and how they were learned. This is one of the best ways to determine connectivity between the local router and the rest of the internetwork.
`show ip ospf interface`	Verifies that interfaces have been configured in the intended areas. If no loopback address is specified, the interface with the highest address is taken as the router ID. It also gives the timer intervals including the hello interval and shows the neighbor adjacencies
`show ip ospf`	Displays the number of times the shortest path first (SPF) algorithm has been executed. It also shows the link-state update interval, assuming no topological changes have occurred.
`show ip ospf neighbor detail`	Displays details list of neighbors, their priorities, and their state (for example: init, exstart, or full).

EIGRP

- **Cisco propietario, 1994**
- **Basado en IGRP**
- **EIGRP es un protocolo de routing de vector distancia avanzado que hace uso de rasgos comúnmente asociados con protocolos de estado de enlace. (algunas veces llamado *protocolo de routing híbrido*)**

EIGRP vs. OSPF

OSPF	EIGRP
rapid convergence, partial updates, neighbor discovery	rapid convergence, partial updates, neighbor discovery
Administrator can define route summarization	Automatic route-summarization and user-defined route summaries
Open standard; multivendor support	Proprietary; Cisco routers only
Scalable; administratively defined “areas” provide manageable hierarchy	Scalable
Difficult to implement	Easy to implement

EIGRP vs IGRP

- **IGRP y EIGRP son compatibles, aunque EIGRP ofrece soporte multiprotocolo e IGRP no.**

EIGRP soporta:

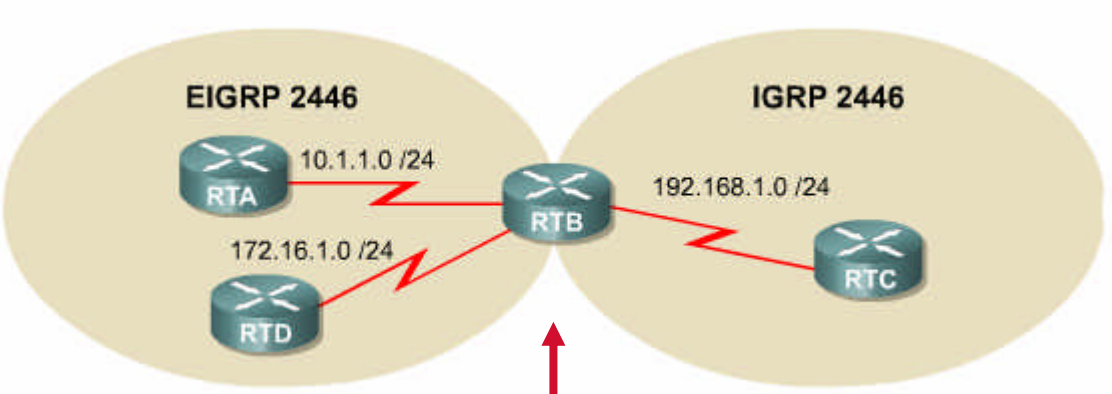
TCP/IP

IPX/SPX

AppleTalk

EIGRP e IGRP

- **Redistribuye automaticamente cuando se usa el mismo número de Sistema Autonomo.**




```
RTB(config)#router igrp 2446
RTB(config-router)#network 192.168.1.0
RTB(config)#router eigrp 2446
RTB(config-router)#network 10.1.1.0
RTB(config-router)#network 172.16.1.0
```

RTB corre EIGRP e IGRP

Cálculo de métricas: IGRP/EIGRP

$$metric = [K1 * bandwidth + (K2 * bandwidth) / (256 * load) + (K3 * delay)] * [K5/(reliability + K4)]$$

(con los siguientes valores por defecto):

Constante	Valor
K1	1
K2	0
K3	1
K4	0
K5	0

EIGRP escala la métrica de IGRP por un factor de 256. Esto es porque EIGRP utiliza una métrica de 32 bits de longitud, e IGRP utiliza una métrica de 24-bit. Multiplicando o dividiendo por 256, EIGRP puede intercambiar fácilmente la información por IGRP.

- bandwidth for IGRP = (10000000/bandwidth)
- bandwidth for EIGRP = (10000000/bandwidth) * 256
- delay for IGRP = delay/10
- delay for EIGRP = delay/10 * 256

Nota: Cuando K2, K4 y K5 son cero la formula se reduce a *metric = bandwidth + delay*

•IGRP tiene un número máximo del saltos de 255. EIGRP tiene un límite máximo de de 224. Esto es más que adecuado para redes más grandes, correctamente diseñadas.

Cálculo de métrica

Nosotros fijamos el *bandwidth* y *delay*, y el router dinámicamente calcula *load* y *reliability*.

Los cuatro valores pueden ser examinados usando `show interface`

Cálculo de métricas

```
NAT_Boundary>show interfaces s1/0
Serial1/0 is up, line protocol is up
  Hardware is QUICC Serial
  Description: Out to VERIO
  Internet address is 207.21.113.186/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 33/255, rxload 246/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
<output omitted>
```

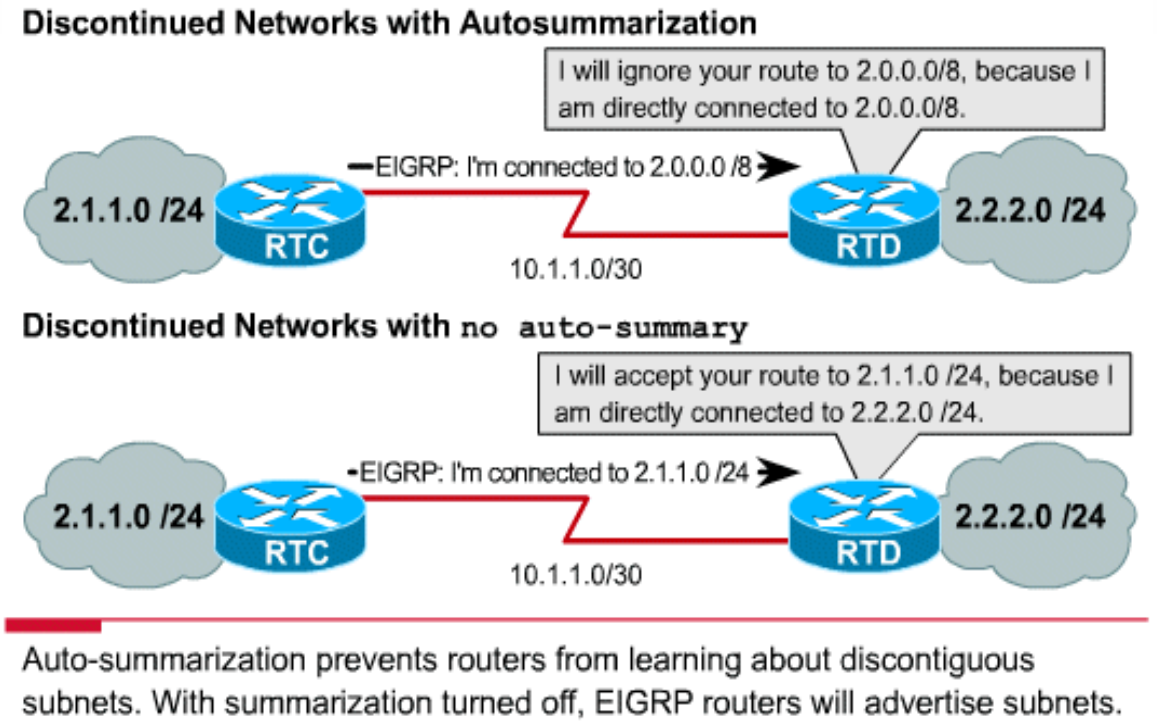
bandwidth

delay

reliability

load

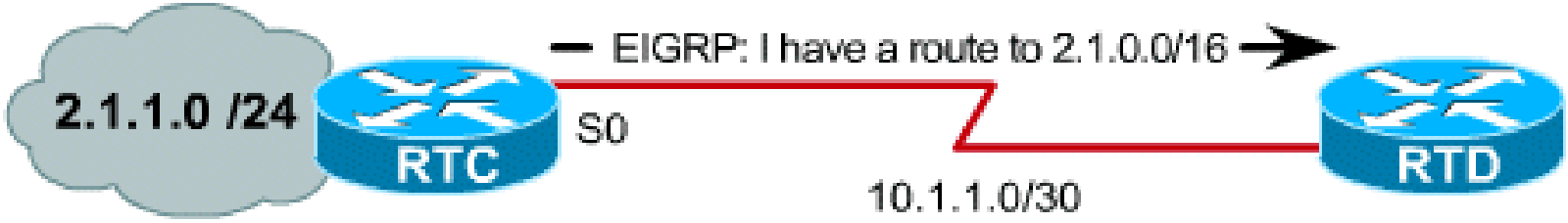
Recordemos la Auto-sumarización



Auto-summarization prevents routers from learning about discontiguous subnets. With summarization turned off, EIGRP routers will advertise subnets.

- **La Sumarización es por defecto a direcciones de clases de red**: máscaras /8, /16 o /24.
- *Pero RIP v2 o **EIGRP realizan un auto- summarization únicamente cada vez que se cruza una frontera entre dos clases principales difererentes**.*
- **En esta figura, debido a que RTC y RTD tienen ambos redes de clase general (1.0.0.0/8 y 2.0.0.0/8) y los paquetes son enviados a través de ellas , entonces se sumarizará por defecto.**

Sumarización Manual




```
RTC(config)#router eigrp 2446
RTC(config-router)#no auto-summary
RTC(config-router)#exit
RTC(config)#interface serial0
RTC(config-if)#ip summary-address eigrp 2446 2.1.0.0 255.255.0.0
```

EIGRP summary addresses can be manually configured on a per-interface basis.

Tecnologías EIGRP

Tecnologías que forman EIGRP a parte de IGRP

- Neighbor discovery and recovery
- Reliable Transport Protocol (RTP)
- DUAL finite-state machine (FSM)
- PDM (Protocol-dependent Module)

Neighbor Discovery/Recovery

- Routers EIGRP establecen adyacencias con routers vecinos usando paquetes hello pequeños.
- Un router EIGRP asume que, mientras recibe paquetes ¡hello! de vecinos conocidos, aquellos vecinos (y sus rutas) permanecen accesibles.

RTP (Reliable Transport Protocol)

- EIGRP es independiente de protocolos; es decir esto no se basa en TCP/IP para intercambiar la información de encaminamiento de la manera en que el RIP, IGRP, y OSPF lo hacen.
- Para conseguir ser independente de IP, usa su propio protocolo de transporte, para garantizar la entrega de info. de routing: RTP.
- Soporta entrega fiable y no fiable.
- Soporta unicasting y multicasting

DUAL FSM

- **La pieza central de EIGRP es DUAL, mecanismo de cálculo de ruta EIGRP**
- **El nombre completo de esta tecnología es DUAL** finite state machine (**FSM**)**. Este mecanismo contiene toda la lógica usada para calcular y comparar rutas en una red EIGRP.**

¿Qué es un FSM?

- Un FSM es una máquina abstracta, no un dispositivo mecánico
- FSMs definen un juego de estados posibles que se puede examinar, que acontecimientos causan aquellos estados, y que acontecimientos son resultado de aquellos estados.
- Los diseñadores usan FSMS para describir como un dispositivo, programa de ordenador, o el algoritmo de encaminamiento reaccionarán a unos determinados eventos de entrada.

DUAL FSM

- DUAL selecciona rutas alternativas rápidamente usando la información de las tablas EIGRP.
- Si un link cae, DUAL busca un sucesor factible en su vecino y tablas de topología.
- Un sucesor es una ruta que actualmente es usada para envios de paquetes
- Es la ruta de menor coste al destino, y no forma parte de un bucle.
- Sucesores factibles (Feasible successors) son rutas que representan los siguientes caminos de coste más bajo a un destino sin introducir bucles de encaminamiento.
- Rutas de sucesor factibles pueden ser usadas en caso de fallo en la ruta existente ; los paquetes a la red de destino inmediatamente son enviados usando al sucesor factible, que en este punto, alcanza el estado de sucesor.

PDMs

- PDM (Protocol-dependent module)
- EIGRP es modular
- Diferentes PDMs pueden ser añadidos a EIGRP con la mejora o desarrollo de nuevos protocolos enrutados IPv4, IPv6, IPX, and AppleTalk

Terminología EIGRP

Routers EIGRP guardan la ruta y la información de topología en la RAM, permitiendo reaccionar rápidamente a cambios. Como OSPF, EIGRP salva esta información en varias tablas y bases de datos.

EIGRP mantiene tres tablas:

1. Tabla de vecinos (Neighbor table)
2. Tabla de topología (Topology table)
3. Tabla de routing (Routing Table)

Otros términos ya mencionados: Successor y Feasible Successor

Terminología EIGRP

- ***Tabla Neighbor***

  Cada router EIGRP mantiene una tabla de vecinos que lista los routers adyacentes

  Es comparable a la BD de adyacencias usada por OSPF

  Hay una tabla por cada protocolo que EIGRP soporta

Show IP EIGRP Neighbors

```
RTX#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   10.2.0.2                Se1              12 00:27:39  333  1998  0  10
0   10.1.0.1                Se0              14 01:17:14   40   240  0  27
```

- ***Smooth Round Trip Timer (SRTT)*** *Tiempo medio que se necesita para enviar un recibir paquetes desde un vecino*
- ***Hold Time*** *Intervalo de tiempo de espera sin recibir nada des un vecino antes de considerar el enlace como no accesible*
- ***Neighbor address*** *Dirección de red del router vecino*
- ***Queue count*** *Número de paquetes esperando en la cola para ser enviados. Un número alto indica congestión*

Terminología EIGRP

Topology table (tabla topológica)

- ***Cada router EIGRP mantiene una tabla de la topología para cada protocolo de red configurado.***
- ***Esta tabla incluye las entradas de la ruta para todos los destinos que el router ha aprendido.***
- ***Todas las rutas aprendidas a un destino se mantienen en la tabla de la topología.***

Tabla Topologica

- **EIGRP usa su tabla** topologica para almacenar toda la información que necesita par calcular un conjunto de distancias y direcciones a todos los destinos alcanzables.

Show ip eigrp topology all

```
RTX#show ip eigrp topolgy all
IP-EIGRP Topology Table for process 1

_
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

_
P 10.2.0.0/16, 1 successors, FD is 2169856, serno 24
         via Connected, Serial1
P 10.3.0.0/16, 1 successors, FD is 2681856, serno 33
         via 10.2.0.2 (2681856/2169856), Serial1
P 10.0.0.0/8, 1 successors, FD is 2169856, serno 5
         via Summary (2169856/0), Null0
P 10.1.0.0/16, 1 successors, FD is 2169856, serno 1
         via Connected, Serial0
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

_
P 192.168.5.0/24, 1 successors, FD is 3219456, serno 37
         via 10.2.0.2 (3219456/2707456), Serial1
```

Tabla Topológica

- EIGRP clasifica las rutas como internas o externas.
- EIGRP utiliza un proceso llamado *route tagging* con etiqueta para agregar etiquetas especiales a cada ruta.
- Estas etiquetas identifican una ruta como interna o externa, y pueden incluir otras informaciones también.

Tabla Topológica

- Todas las rutas externas se incluyen en la tabla de la topología, y se marcan con etiqueta con la información siguiente:
- El número de identificación (Router ID) del router EIGRP que redistribuyó la ruta en la red de EIGRP
- número S. A. del destino
- el protocolo usado en la red externa
- el coste o métrica recibida de ese protocolo externo
- la etiqueta configurable del administrador

Show ip eigrp top

```
RTX#sh ip eigrp top 204.100.50.0
IP-EIGRP topology entry for 204.100.50.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2297856
  Routing Descriptor Blocks:
  10.1.0.1 (Serial0), from 10.1.0.1, Send flag is 0x0
      Composite metric is (2297856/128256), Route is External
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 192.168.1.1
        AS number of route is 0
        External protocol is Connected, external metric is 0
        Administrator tag is 0 (0x00000000)
```

Tabla de enrutamiento EIGRP

- EIGRP elige las mejores (es decir, sucesor) a un destino desde la tabla topologica y coloca la ubicación de estas rutas en la tabla de encaminamiento.
- Cada router de EIGRP mantiene una tabla de encaminamiento para cada protocolo de red.
- La tabla de encaminamiento contiene las rutas instaladas por DUAL como las mejores trayectorias libres de bucles a un destino dado.
- EIGRP mantendrá hasta cuatro rutas por destino.

Conceptos

- **Distancia factible (FD): Ésta es la métrica calculada más baja hacia cada destino. Por ejemplo, la distancia factible a 32.0.0.0 es 2195456. La distancia de la ruta que está en la tabla de encaminamiento.**
- **Origen de la ruta: Número de identificación del router que publicó esa ruta en primer lugar. Este campo se llena sólo para las rutas que se aprenden de una fuente externa a la red EIGRP. El rotulado de rutas puede resultar particularmente útil con el enrutamiento basado en políticas. Por ejemplo, el origen de la ruta a 32.0.0.0 es 200.10.10.10.**
- **Distancia informada (RD): La distancia informada (RD) de la ruta es la distancia informada por un vecino adyacente hacia un destino específico. Por ejemplo, la distancia informada a 32.0.0.0 por el vecino 200.10.10.10 es 2195456 tal como lo indica (90/2195456).**
- **Información de interfaz: La interfaz a través de la cual se puede alcanzar el destino.**
- **Estado de ruta: El estado de una ruta. Una ruta se puede identificar como pasiva, lo que significa que la ruta es estable y está lista para usar, o activa, lo que significa que la ruta se encuentra en el proceso de recálculo por parte de DUAL.**

Rutas Externas e Internas

```
RTA#show ip route
<output omitted>
C    10.1.1.0 is directly connected, Serial0
D    172.16.0.0 [90/2681856] via 10.1.1.0, Serial0
D EX 192.168.1.0 [170/2681856] via 10.1.1.1, 00:00:04,
   Serial0
```

Tipos de paquetes EIGRP

Son 5:

- **Hello**
- **Acknowledgement**
- **Update**
- **Query**
- **Reply**

Tipos de paquetes EIGRP

- ***hello packets*** **descubren, verifican, y redescubren los routers vecinos.**
- **Los routers EIGRP envían hellos en un intervalo fijo (y configurable), llamado intervalo hello.**
- **El intervalo por defecto depende del ancho de banda del interfaz. 5 segundos si esta por encima de T1, 60 segundos si está por debajo.**
- **hello paquetes son multicast.**
- **Sobre redes IP , routers EIGRP envían *hellos* a la IP multicast 224.0.0.10.**

Paquetes de Reconocimiento

- Son paquetes hello sin datos
- Se utilizan para asegurar una comunicación fiable.
- Son unicast.

Paquetes Update

Se utilizan cuando un router descubre un nuevo vecino.

Un EIGRP envía los paquetes de actualización unicast a ese nuevo vecino de modo que pueda agregar a su tabla de la topología.

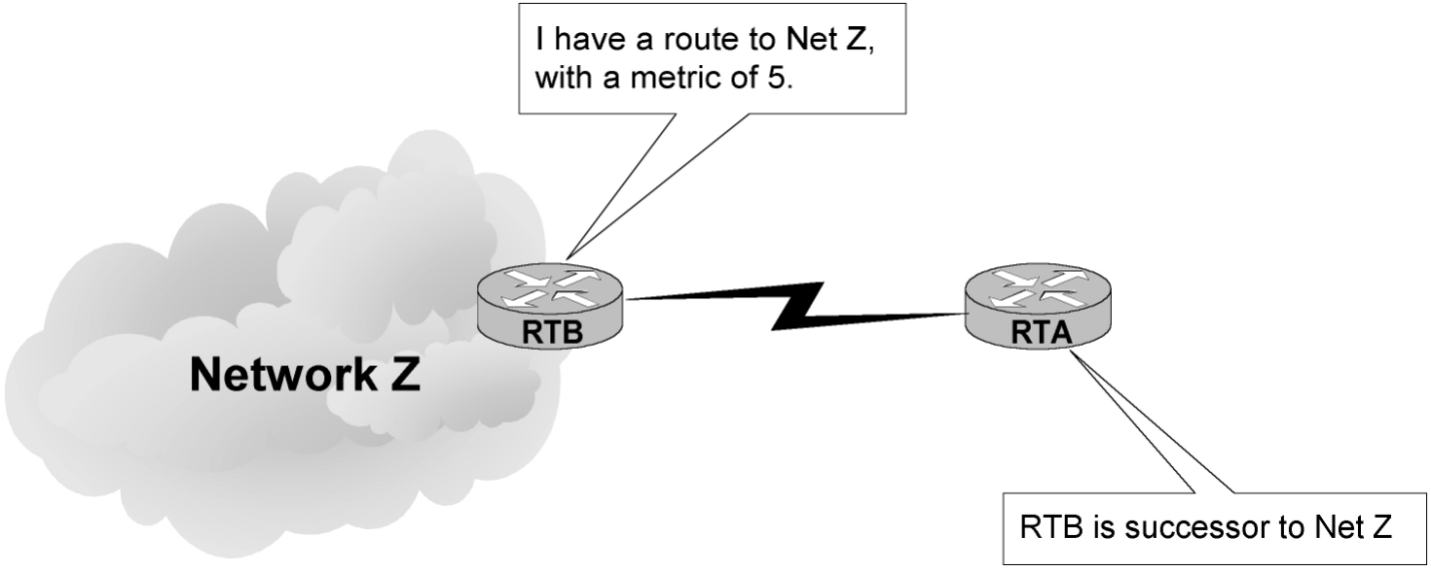
Puede ser necesario más de un paquete de actualización para transportar toda la información de la topología al vecino nuevamente descubierto.

Son también usados cuando un router detecta un cambio en la topologia . En este caso se envía paquetes multicast de alerta a todos los vecinos.

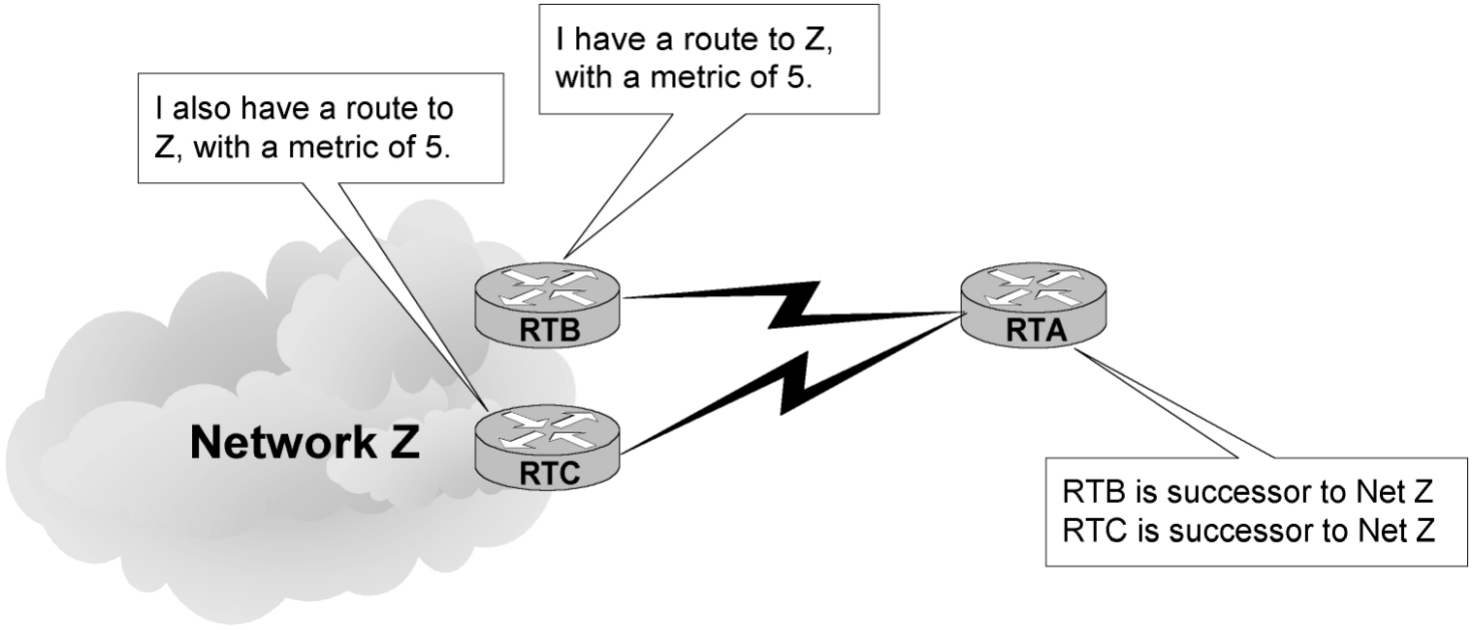
Paquetes Query y Reply

- Los Query se usan siempre que se necesite la información específica de uno o todos sus vecinos.
- Un paquete Reply se utiliza para responder a una pregunta.
- Si un router pierde su sucesor y no puede encontrar un sucesor factible para una ruta, DUAL pone la ruta en estado activo.
- los routers mandan una query multicast a todos los vecinos, buscando un sucesor para la red destino
- . Los vecinos deben enviar las contestaciones que proporcione la información de sucesores, o indicar que no hay información de sucesor disponible.
- Las preguntas pueden ser multicast o unicast, mientras que las contestaciones son siempre unicast. Ambos tipos del paquetes se envían de forma segura o fiable.

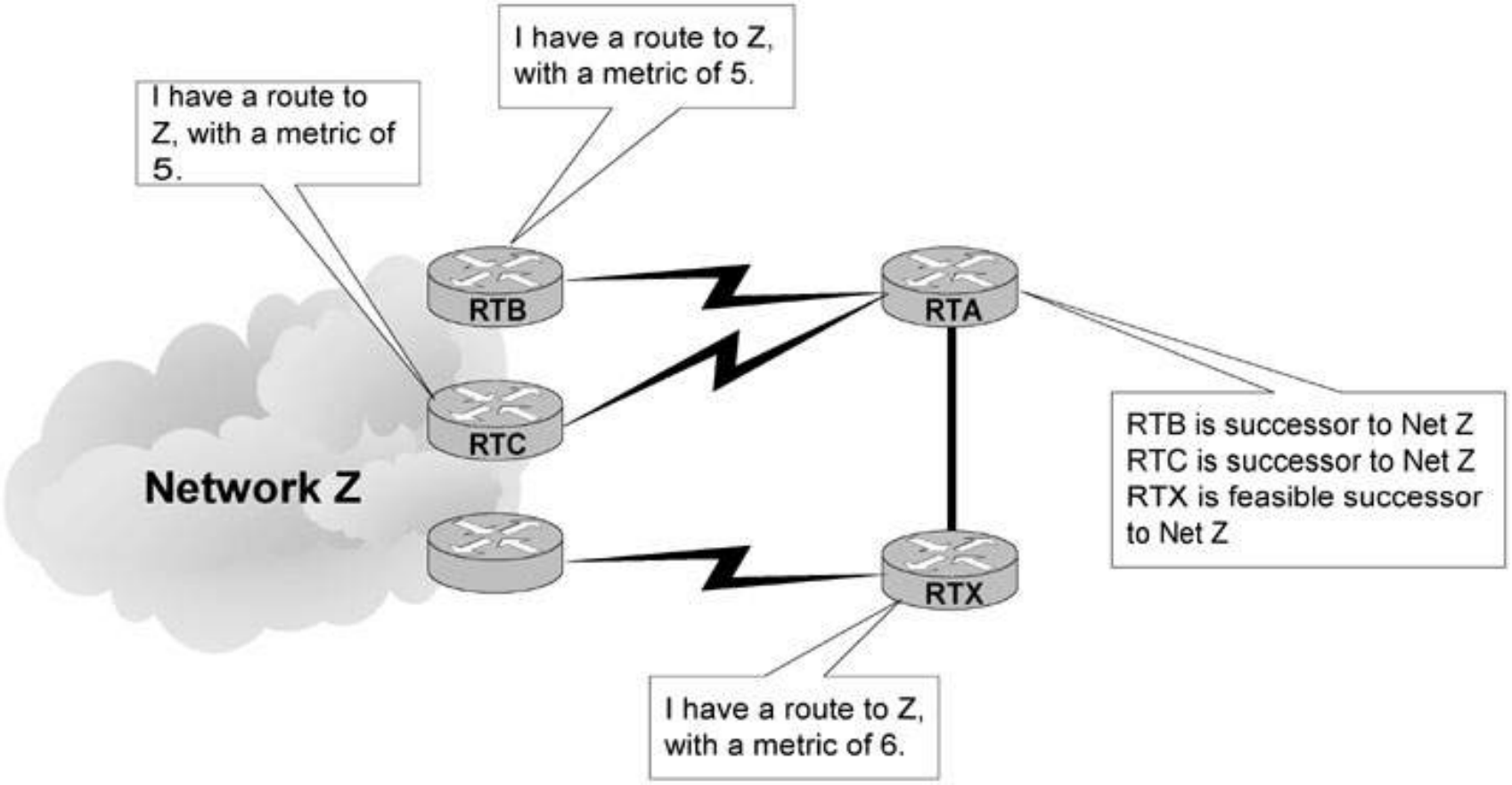
Sucesores y Sucesores Factibles



Sucesores y Sucesores Factibles



Sucesores y Sucesores Factibles



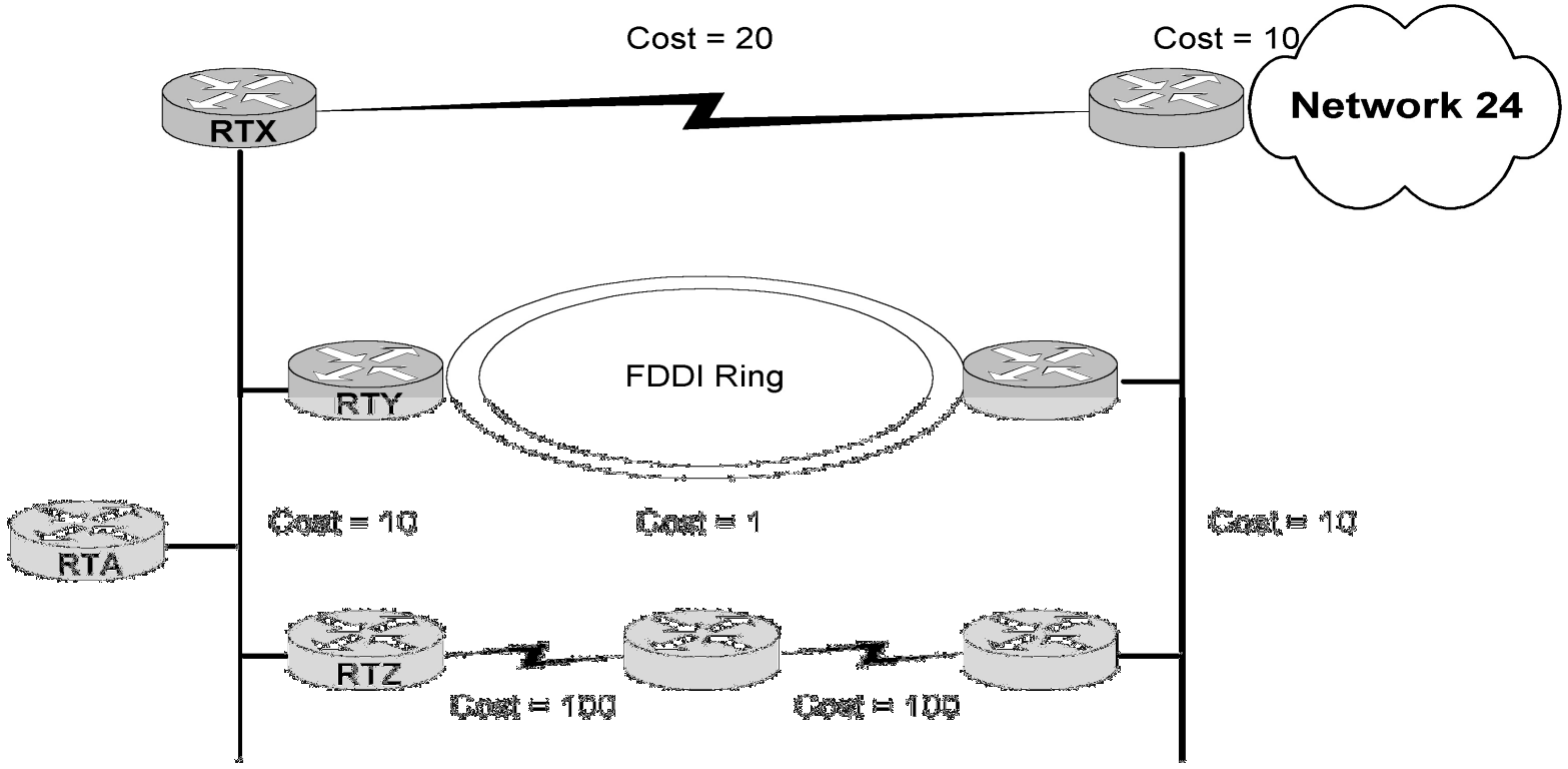
Sucesores y Sucesores Factibles

- Un router ve a sus sucesores factibles como vecinos que están flujo abajo, o más cercanos, al destino que el mismo. Si algo va mal con el sucesor, DUAL identifica rápidamente un sucesor factible de la tabla topologíca, e instala una nueva ruta al destino.
- Si no existe ningún sucesor factible al destino, DUAL coloca la ruta en el estado activo. Las entradas en la tabla de la topología pueden estar en uno de dos estados: activo o pasivo. Una ruta pasiva es una que está estable y disponible para el uso. Una ruta activa es una ruta en el proceso de ser reprocesada por DUAL. El reprocesamiento sucede si una ruta se convierte en inalcanzable y DUAL no puede encontrar sucesores factibles.

Sucesores y Sucesores Factibles

- **El router debe pedir a sus vecinos ayuda para encontrar una trayectoria nueva, libre de bucles, al destino. Se obliga a los routers vecinos que contesten a esta pregunta. Si un vecino tiene una ruta, contestará con la información sobre el sucesor(es). Si no, el vecino notifica el remitente que no tiene una ruta al destino dado.**

Convergencía usando EIGRP (1)



Convergencía usando EIGRP (2)

Neighbor	Computed Cost to Net 24	Reported Distance to Net 24
RTY	**31**	**21**
RTZ	**230**	**220**
RTX	**40**	**30**

RTY es sucesor con un coste calculado de 31.

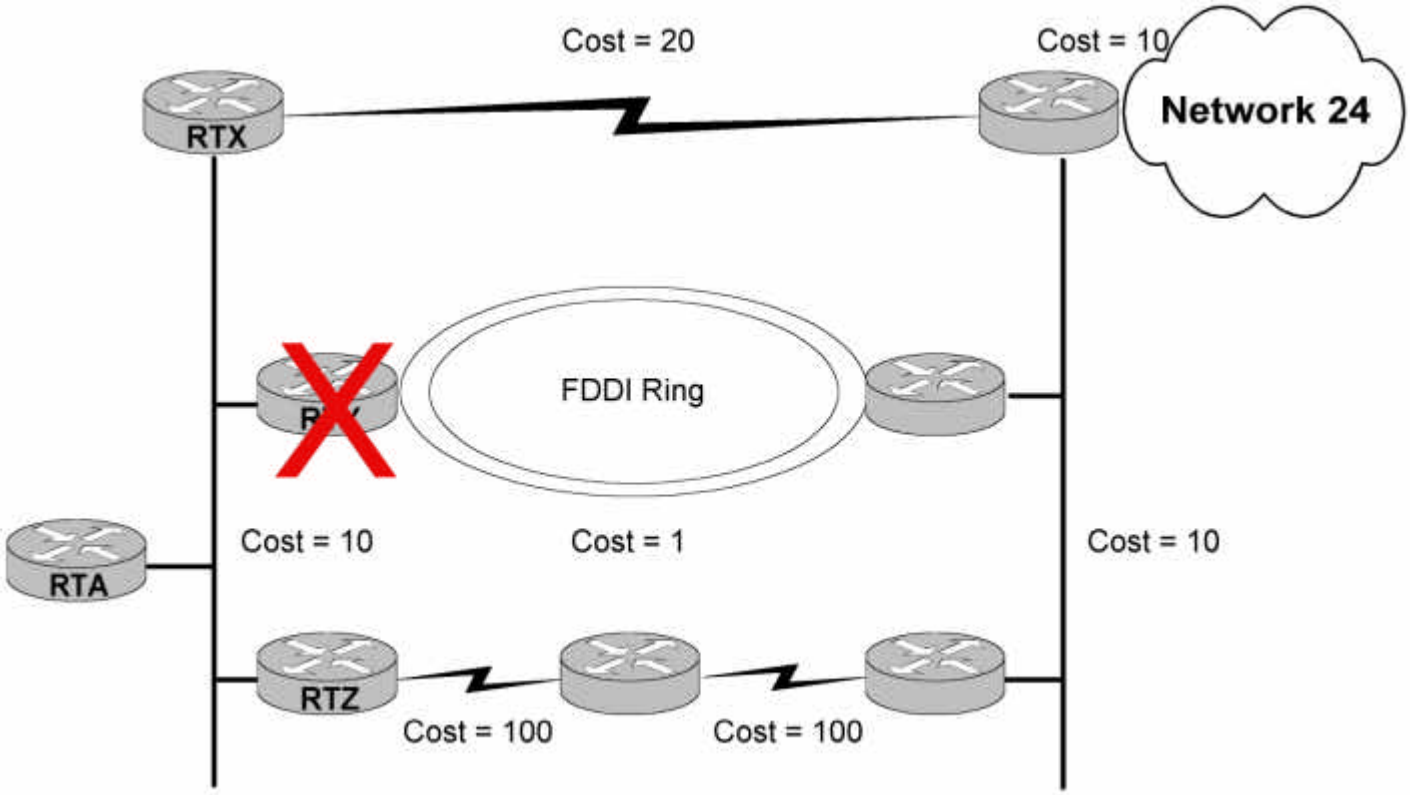
“31” es la Feasible Distance (FD).

1) RTX RD (30) es menor que FD (31).

2) RTX CC (40) es menor que RTZ CC (230)

3) Resultado de 1) y 2) coincide ✍ RTX Sucesor Factible

Convergencía usando EIGRP (3)



Convergencía usando EIGRP (4)

Neighbor	Computed Cost to Net 24	Reported Distance to Net 24
RTY	**31**	**21**
RTZ	**230**	**220**
RTX	**40**	**30**

Desde que RTX es un “feasible successor”, es introducido en la tabla de enrutamiento inmediatamente (ningún cálculo de procesamiento).

Convergencía usando EIGRP (5)

Neighbor	Computed Cost to Net 24	Reported Distance to Net 24
RTY	**31**	**21**
RTZ	**230**	**220**
RTX	**40**	**30**

RTZ no es un sucesor factible todavía. Su RD (220) es más grande que el FD (31) para Net 24. Antes de que esta ruta pueda ser introducida, la ruta a net 24 debe ser puesta previamente a ***active state*** y reprocesada, ya que la FD solo puede cambiar durante una transicción activa a pasiva.

Convergencía usando EIGRP (6)

- RTA no puede encontrar sucesores factibles ✍ transicción de Pasiva a Activa (red 24), y consulta a vecinos sobre esa red.
- Cuando la red 24 se encuentra en estado Activa, se reinicia la FD, lo que permite aceptar a RTZ.

Configuración EIGRP

```
RTA(config)#        router eigrp 123
RTA(config-router)# eigrp log-neighbor-changes
RTA(config-router)#  network 1.0.0.0
```

El comando, *router eigrp 123* configura EIGRP con un número de S.A. 123.

comando *network* para establecer las redes directamente conectadas

`eigrp log-neighbor-changes` cuando se trate de la primera configuración EIGRP . Sin este comando, la información vecina crítica no será registrada (consola,, syslog, etc). Se necesitará esta información vecina para localizar fallos.

Configuración EIGRP opcional

Comando Opcional de Interface:

```
RTA(config-if)#ip bandwidth-percent eigrp 123 40
```

Por defecto, EIGRP no utiliza más del 50% de ancho de de banda de los links para los *hellos*, las actualizaciones, las preguntas, y los reconocimientos. Este comando del ejemplo configura EIGRP para que en el S.A 123 no se utilice más del 40% (por ejemplo para casos con enlaces de baja velocidad).