



Router Teldat

Protocolo RIP

Doc. DM718 Rev. 10.10

Junio, 2003

ÍNDICE

Capítulo 1 Introducción.....	1
1. Introducción	2
2. El protocolo de routing RIP	3
3. Configuración del protocolo RIP	5
Capítulo 2 Configuración RIP	6
1. Comandos de Configuración del protocolo RIP	7
1.1. ? (AYUDA).....	7
1.2. ACCEPT-RIP-ROUTE.....	8
1.3. AGGREGATION-TYPE.....	8
1.4. ALLOW-DISCONNECTED-SUBNETTED-NETWORKS	9
1.5. AS-LABEL.....	10
1.6. AUTHENTICATION.....	10
1.7. COMPATIBILITY.....	11
1.8. COST-ADDITIONAL.....	11
1.9. DISABLE.....	12
1.10. DISTRIBUTE-LIST	12
a) DISTRIBUTE-LIST IN	13
b) DISTRIBUTE-LIST OUT	13
1.11. ENABLE.....	13
1.12. LIMIT-RIP.....	14
1.13. LIST	14
a) LIST ADDRESS-OPTIONS.....	14
b) LIST ALL	15
c) LIST AS-LABELS	16
d) LIST DISTRIBUTE-LISTS	16
e) LIST LIMIT-RIP.....	16
f) LIST TIMERS.....	16
1.14. NO.....	17
a) NO ACCEPT-RIP-ROUTE.....	17
b) NO ALLOW-DISCONNECTED-SUBNETTED-NETWORKS.....	17
c) NO AUTHENTICATION	17
d) NO DISTRIBUTE-LIST.....	18
e) NO LIMIT-RIP.....	18
f) NO OFFSET-LIST.....	18
g) NO ORIGINATE-RIP-DEFAULT	18
1.15. OFFSET-LIST	18
1.16. ORIGINATE-RIP-DEFAULT	20
1.17. RECEIVING.....	20
1.18. SENDING.....	21
1.19. TIMERS.....	22
1.20. EXIT.....	23
Capítulo 3 Monitorización RIP.....	24
1. Comandos de Monitorización del protocolo RIP	25
1.1. ? (AYUDA).....	25
1.2. LIST	25
1.3. EXIT.....	26
Apéndice A Filtrado mediante listas	27
1. Introducción	28
2. Uso de las listas para filtrar rutas	29

3.	Escenario de ejemplo	30
4.	Filtrado de rutas con máscara	32
5.	Filtrado de la ruta por defecto.....	33

Capítulo 1

Introducción



1. Introducción

Este capítulo describe la utilización del protocolo RIP (Routing Information Protocol), que es un protocolo de gateway interior (IGP). El **Router Teldat** soporta dos protocolos IGP distintos para la construcción de la tabla de routing IP. Estos protocolos son el OSPF, y el RIP.

RIP es un protocolo basado el algoritmo de vector de distancia o de Bellman-Ford que permite a los routers intercambiar su información sobre posibles destinos para calcular las rutas a lo largo de toda la red. Los destinos pueden ser redes o valores especiales que representan rutas por defecto. RIP no altera los datagramas IP y los encamina basándose únicamente en el campo de dirección destino.

El algoritmo de vector de distancia hace que los routers difundan periódicamente sus tablas de routing a todos sus routers vecinos. De esta forma, el router, al conocer las tablas de todos sus vecinos, puede decidir por donde debe enviar cada paquete.

La información está organizada en las siguientes secciones:

- El protocolo de routing RIP.
- Configuración del protocolo RIP.
- Comandos de configuración del protocolo RIP.
- Comandos de monitorización del protocolo RIP.

Los routers que utilizan el mismo protocolo de routing forman un Sistema Autónomo SA (Autonomous System -AS-). Este protocolo de routing común se denomina Protocolo de Gateway Interior (Interior Gateway Protocol). Los IGP detectan dinámicamente la accesibilidad de la red y la información de routing dentro de un Sistema Autónomo (SA), y utilizan esta información para confeccionar la tabla de routing IP. Los IGP también pueden importar a un Sistema Autónomo (SA) información de routing externa.

El **Router Teldat** puede ejecutar simultáneamente los protocolos OSPF y RIP. Cuando esto ocurre, se prefieren las rutas OSPF.

2. El protocolo de routing RIP

Con la aparición de OSPF se empezó a pensar que RIP estaba obsoleto. Aunque es cierto que los nuevos protocolos de routing son superiores en prestaciones al RIP, éste sigue teniendo algunas ventajas. La principal es que en redes pequeñas, RIP-2 añade muy poca sobrecarga “overhead” en términos de ancho de banda usado, y que es más fácil y rápido de configurar. Además, actualmente existen muchos más dispositivos ejecutando RIP que otros protocolos de routing.

RIP-1 no consideraba los sistemas autónomos, la interacción IGP/EGP, el “subnetting” (redes divididas en subredes) ni la autenticación. La falta de la máscara de subred en los paquetes RIP-1 planteaba un serio problema puesto que era necesaria para poder determinar la ruta de subredes. Actualmente los routers con RIP-1 suponen la máscara de subred igual a la del interfaz por la que ha entrado el paquete RIP-1 y de ahí que pongan como condición imprescindible que todas las subredes de una misma red tengan la misma longitud. Para solucionar esta problemática apareció el protocolo RIP-2.

Nota: Todos los interfaces de router que tengan RIP habilitado como RIP-1 deben tener la misma máscara de subred.

RIP-2 es una extensión de RIP-1. Utiliza el mismo formato de mensaje pero extiende el significado de alguno de los campos.

El **Router Teldat** soporta una implementación completa del protocolo de routing RIP-2, tal y como se especifica en las recomendaciones RFC 1723 y RFC 1388. Esta versión es compatible con los routers que ejecuten la Versión 1 de RIP. La información de RIP se intercambia entre routers que ejecuten las dos distintas versiones, aunque para ello hay que configurar el router con RIP-2 de una manera determinada.

RIP-2 está diseñado para proporcionar servicios no disponibles con el protocolo RIP-1. Sus características avanzadas incluyen:

- *Autenticación*, actualmente contraseña en claro. Proporciona seguridad adicional al routing.
- *Campo Rute Tag*, atributo asignado a cada ruta para poder separar las rutas internas con las externas y así tener un método para la interacción IGP/EGP.
- *Máscaras de subred de longitud variable*. Permiten fraccionar una dirección IP en subredes de tamaño variable, conservando el espacio de dirección IP.
- *Siguiente salto*, para eliminar paquetes encaminados con número de saltos extra.
- *Multicast* en vez de broadcast para eliminar cargas innecesarias en aquellos dispositivos que no están procesando paquetes RIP-2. La dirección multicast asociada a RIP-2 es 224.0.0.9. Para seguir manteniendo la compatibilidad con RIP-1 el uso de multicast será un parámetro configurable.

El protocolo RIP-2 soporta los siguientes tipos de redes físicas:

- *Punto a Punto*. Son las redes que usan una línea de comunicación para unir un único par de routers. Un ejemplo de red punto a punto puede ser una línea serie a 56 Kbps que conecte dos routers.
- *Broadcast*. Son redes que soportan más de dos routers conectados y que son capaces de direccionar un único mensaje físico a todos los routers conectados. Un ejemplo de red broadcast puede ser una red Token Ring.
- *No Broadcast*. Son redes que soportan más de dos routers conectados pero no tienen capacidad de broadcast. Una red de datos pública X.25 es un ejemplo de red no broadcast. Para que RIP-2 funcione correctamente esta red necesita información de configuración adicional sobre otros routers RIP-2 conectados a la red no broadcast.

El protocolo RIP se desarrolló para utilizarse en redes homogéneas de tamaño pequeño. Por esta razón el RIP tiene las siguientes limitaciones:

- El número máximo de saltos es de 15.
- El RIP es un protocolo lento en encontrar nuevas rutas cuando se produce un cambio en la red.
- Este protocolo de routing utiliza métrica fija para comparar rutas alternativas, no es apropiado para routers que calculan el coste de la ruta con parámetros calculados en tiempo real.

3. Configuración del protocolo RIP

Los pasos siguientes esbozan las tareas necesarias para conseguir que RIP se ejecute correctamente.

1. Habilitar el protocolo RIP.
2. Definir los interfaces de red RIP del router.
3. Configurar parámetros de envío por interfaz. Tipo de rutas que se desean enviar y si se quiere o no activar la opción *poisoned reverse* en dicho interfaz.
4. Configurar parámetros de recepción por interfaz. Tipo de rutas que se desean procesar.
5. Configurar compatibilidad de envío y recepción por interfaz. Son los distintos tipos de nivel de compatibilidad que define la RFC 1723 entre routers RIP-1 y RIP-2.
6. Configurar autenticación por interfaz. Si se habilita autenticación hay que configurar la contraseña.
7. Configurar interacción IGP/EGP. Configurar la etiqueta del sistema autónomo al que pertenece el router, definir la ruta por defecto para encaminar tráfico para redes no RIP hacia el router que hará funciones de puerta.
8. Configurar temporizadores. Para ajustar los temporizadores que intervienen en RIP-2. Es aconsejable que se deje el valor por defecto y que únicamente lo cambie personal cualificado.

Si se configura que el RIP utilice mensajes de broadcast para la actualización de sus rutas, se debe especificar el formato de la dirección IP de broadcast.

Capítulo 2

Configuración RIP



1. Comandos de Configuración del protocolo RIP

En este capítulo se describen los comandos para configurar el protocolo RIP. Para acceder al entorno de configuración de RIP, se deben introducir los siguientes comandos:

```
*PROCESS 4
Config> PROTOCOL RIP

-- RIP protocol user configuration --
RIP config>
```

Comando	Función
? (AYUDA)	Lista los comandos u opciones disponibles.
ACCEPT-RIP-ROUTE	Determina las redes de las que siempre se aceptarán rutas.
AGGREGATION-TYPE	Configura el modo de agregación RIP.
ALLOW-DISCONNECTED-SUBNETTED-NETWORKS	Permite la propagación de subredes desconectadas.
AS-LABEL	Configura los Sistemas Autónomos para la interacción IGP/EGP.
AUTHENTICATION	Configura la autenticación RIP.
COMPATIBILITY	Configura la compatibilidad RIP en envío y en recepción.
COST-ADDITIONAL	Asocia un coste a un interfaz.
DISABLE	Deshabilita el protocolo RIP o determinadas características.
DISTRIBUTE-LIST	Establece filtros para las rutas distribuidas (entrantes y salientes).
ENABLE	Habilita el protocolo RIP o determinadas características.
LIST	Muestra la configuración RIP.
NO	Deshabilita o elimina funcionalidades.
OFFSET-LIST	Establece listas de offset de entrada/salida.
ORIGINATE-RIP-DEFAULT	Establece una ruta por defecto para otros protocolos de routing.
RECEIVING	Configura parámetros de recepción.
SENDING	Configura parámetros de transmisión.
TIMERS	Configura los temporizadores de RIP.
EXIT	Sale del proceso de configuración RIP.

1.1. ? (AYUDA)

Utilizar el comando ? (AYUDA) para listar los comandos disponibles en el prompt en el que se esté trabajando. También se puede usar este comando a continuación de un comando específico para listar las opciones disponibles.

Sintaxis:

```
RIP config> ?
```

Ejemplo:

```
RIP config> ?
ACCEPT-RIP-ROUTE           Acct rts with determined network dst
AGGREGATION-TYPE           RIP aggregation parameters
ALLOW-DISCONNECTED-SUBNETTED-NETWORKS  Routes to subnets are always sent
AS-LABEL                   For IGP/EGP interaction
AUTHENTICATION             Authentication is sent and checked
COMPATIBILITY              Configure the compatibility selectors
COST-ADDITIONAL           Associates a cost to an interface
DISABLE                    Disables the RIP protocol
DISTRIBUTE-LIST           Establish input/output filters
ENABLE                     Enables the RIP protocol
LIMIT-RIP                 Deactivates the RIP protocol in FR
LIST                       Display RIP configuration
NO
ORIGINATE-RIP-DEFAULT     Originate a default ip route
RECEIVING                 RIP reception parameters
SENDING                   RIP sending parameters
TIMERS                     Timers which control the algorithm
EXIT
RIP config>
```

1.2. ACCEPT-RIP-ROUTE

Con el comando **RECEIVING** se puede indicar al router que ignore la información recibida por paquetes RIP referida a rutas dirigidas a redes o subredes. Estos filtros se establecen de forma individual por cada interfaz.

Con los comandos **DISTRIBUTE-LIST IN** y **RECEIVING <dir IP-RED/SUBRED>** **DISTRIBUTE-LIST** se puede indicar al router que sólo acepte la información recibida referente a determinadas rutas, filtrando dichas rutas tanto de forma global para todos los interfaces como individual por cada interfaz.

Sin embargo, aunque se programen estos filtros, es posible aceptar las rutas que tengan como destino determinadas redes/subredes; esto es lo que se consigue con el comando **ACCEPT-RIP-ROUTE**. El proceso que se sigue es el siguiente: si se programa **ACCEPT-RIP-ROUTE 10.0.0.0**, y en un determinado interfaz están programados los filtros comentados anteriormente, el router analiza el paquete RIP y si la red destino a la que se refiere es la 10.0.0.0, acepta la información independientemente de los filtros configurados.

Sintaxis:

```
RIP config> ACCEPT-RIP-ROUTE <dir IP-RED/SUBRED>
```

Ejemplo:

```
RIP config> ACCEPT-RIP-ROUTE 10.0.0.0
RIP config>
```

1.3. AGGREGATION-TYPE

Se utiliza el comando **AGGREGATION-TYPE** para configurar el tipo de agregación RIP de los interfaces de red del router. El tipo de rutas a enviar por un determinado interfaz depende del estado de los flags de envío y del tipo de agregación configurado, que a continuación se pasará a describir.

Al ejecutar dicho comando aparece un listado de todos los interfaces lógicos (direcciones IP) donde se puede configurar el tipo de agregación RIP. Introducimos una dirección existente y a continuación seleccionamos la opción deseada.

Sintaxis:

```
RIP config> AGGREGATION-TYPE <dir IP-RED/SUBRED>
none                               do not aggregate
aggregation-routes                 use aggregation routes
subnetted-networks                 aggregate subnets
all                                 aggregate all
```

El significado de los tipos de agregación es el siguiente:

<i>none</i>	No se realiza ningún tipo de agregación, con lo que no se envían las rutas de agregación ni las rutas de agregación de subredes. Esta es la opción por defecto.
<i>aggregation-routes</i>	Las rutas de agregación no son rutas propiamente dichas sino marcas que aparecen en la tabla de rutas activas que indican que existen una serie de rutas que están siendo agregadas. Al activar este tipo de agregación se envían sólo las rutas de agregación y las rutas que no pertenecen a ninguna agregación. Por tanto quedan sin enviar las rutas agregadas. Para que una ruta de agregación sea anunciada es necesario que alguna de las rutas que la componen (ruta agregada) sea de una naturaleza tal que los flags de envío permitirían su envío.
<i>subnetted-networks</i>	Cuando en la tabla de rutas se aprende o configura una ruta de subred, automáticamente aparece una ruta de tipo “Sbnt” o ruta agregación de subredes con destino “la red de la subred” y siguiente salto “ninguno”. Al activar este tipo de agregación se envían las rutas de agregación de subred siempre y cuando alguna de las subredes que la provocó sea de una naturaleza tal que los flags de envío permitan su envío.
<i>all</i>	Mediante esta opción se habilitan las dos anteriores a la vez, es decir, se enviarán tanto rutas de agregación como rutas de agregación de subredes.

Ejemplo:

```
RIP config> AGGREGATION-TYPE
IP addresses for each interface:
 ethernet0/0      192.7.1.253      255.255.255.0    NETWORK broadcast, fill 0
 serial0/0
 serial0/1        10.0.0.1          255.0.0.0        NETWORK broadcast, fill 0
 serial0/2
 bri0/0
 x25-node
Which address (ifc name for unnumbered) [0.0.0.0]? 10.0.0.1
none                               do not aggregate
aggregation-routes                 use aggregation routes
subnetted-networks                 aggregate subnets
all                                 aggregate all
Type an option [ ]? ALL
RIP config>
```

1.4. ALLOW-DISCONNECTED-SUBNETTED-NETWORKS

Se utiliza el comando **ALLOW-DISCONNECTED-SUBNETTED-NETWORKS** para permitir que las rutas a subredes se envíen y se reciban por el interfaz independientemente de la red de dicho interfaz. Se permiten subredes desconectadas por defecto.

Al ejecutar este comando aparece un listado de todos los interfaces lógicos (direcciones IP) donde se puede configurar. Introducimos una dirección existente y el envío y recepción de subredes desconectadas quedará habilitado para dicha dirección.

Sintaxis:

```
RIP config> ALLOW-DISCONNECTED-SUBNETTED-NETWORKS <dir IP-RED/SUBRED>
```

1.5. AS-LABEL

Para la interacción IGP/EGP. Es configurable por interfaz lógico (dirección IP). Al ejecutar el comando **AS-LABEL** aparece un listado de todos los interfaces lógicos donde se puede configurar dicho comando. Introducimos una dirección existente y a continuación procedemos a introducir el número de Sistema Autónomo (Autonomous System -AS-) deseado.

Ejemplo:

```
RIP config> AS-LABEL
IP addresses for each interface:
 ethernet0/0      192.7.1.253      255.255.255.0    NETWORK broadcast, fill 0
 serial0/0                IP disabled on this ifc
 serial0/1      10.0.0.1         255.0.0.0        NETWORK broadcast, fill 0
 serial0/2                IP disabled on this ifc
 bri0/0                IP disabled on this ifc
 x25-node                IP disabled on this ifc
Which address (ifc name for unnumbered) [0.0.0.0]? 10.0.0.1
Interface AS label[0]? 1
RIP config>
```

1.6. AUTHENTICATION

La autenticación se envía con cada paquete y se comprueba para cada paquete recibido. Además es configurable por interfaz lógico (dirección IP). Al ejecutar el comando **AUTHENTICATION** aparece un listado de todos los interfaces lógicos donde se puede configurar la autenticación RIP.

Ejemplo:

```
RIP config> AUTHENTICATION
IP addresses for each interface:
 ethernet0/0      192.7.1.253      255.255.255.0    NETWORK broadcast, fill 0
 serial0/0                IP disabled on this ifc
 serial0/1      10.0.0.1         255.255.255.0    NETWORK broadcast, fill 0
 serial0/2                IP disabled on this ifc
 bri0/0                IP disabled on this ifc
 x25-node                IP disabled on this ifc
Which address (ifc name for unnumbered) [0.0.0.0]? 10.0.0.1
Enter password: []? Cualquiera
RIP config>
```

El siguiente algoritmo es el que se usa a la hora de autenticar:

- El router está configurado para no autenticar. Los paquetes RIP-1 y RIP-2 sin autenticación serán aceptados. Los paquetes RIP-2 con autenticación serán descartados.
- El router está configurado para autenticar. Todos los RIP-1 y aquellos RIP-2 que no pasen la autenticación son descartados. Todos los paquetes enviados saldrán autenticados.

1.7. COMPATIBILITY

La recomendación RFC 1058 especifica que los mensajes RIP con versión 0 deben descartarse, los de versión 1 deben descartarse si alguno de los campos MBZ “must be zero” no son cero y los de versión superior a 1 deben aceptarse.

Sin embargo surge la necesidad de implementar un selector de compatibilidad por dos razones. Primero, hay implementaciones de RIP-1 que no siguen la recomendación descrita anteriormente. Segundo, el uso de multicast puede provocar que los sistemas con RIP-1 no reciban los paquete RIP-2. Dicho selector de compatibilidad es configurable por interfaz.

Para configurar los selectores de compatibilidad se utiliza el comando **COMPATIBILITY**.

Al ejecutar dicho comando aparece un listado de todos los interfaces lógicos (direcciones IP) donde se puede configurar la compatibilidad RIP. Introducimos una dirección existente y a continuación procedemos a elegir la opción deseada.

Sintaxis:

```
RIP config> COMPATIBILITY <direccion-ip>
receive      receive selector
              both          both versions are accepted
              rip1         only accepts version 1 RIP packets
              rip2         only accepts version 2 RIP packets
              none         RIP listening disabled in this interface

send         send selector
              rip1         only RIP version 1 packets are sent
              rip2-broadcast where the RIP version 2 packets are sent by broadcast
              rip2-multicast where the RIP version 2 packets are sent by multicast
              none         disables the send RIP packets in this interface
```

El selector de envío (send) posee 4 posiciones:

none: deshabilita el envío de paquetes RIP en este interfaz.

rip1: sólo paquetes RIP versión 1 son enviados.

rip2-broadcast: donde los paquetes RIP versión 2 son enviados por broadcast.

rip2-multicast: donde los paquetes RIP versión 2 son enviados por multicast.

Se recomienda que el valor escogido sea *RIP1* o *RIP2-multicast*, y no *RIP2-broadcast* para evitarnos posibles problemas de entendimiento con dispositivos *RIP1*. *RIP2-broadcast* sólo debe usarse cuando el administrador conozca y comprenda todas las consecuencias.

El selector de recepción (receive) posee 4 posiciones:

rip1: sólo se aceptan paquetes RIP con versión 1.

rip2: sólo se aceptan paquetes RIP con versión 2.

both: se aceptan ambas versiones.

none: deshabilitada escucha RIP en este interfaz.

1.8. COST-ADDITIONAL

Se utiliza este comando para asociar un coste a un interfaz, de tal manera que a todas las rutas RIP aprendidas por dicho interfaz se les incrementará el coste en tantas unidades como diga este parámetro + 1 (si coste a cero, el protocolo RIP sólo lo incrementará en 1 unidad). El rango de valores está comprendido entre 0 y 15. El valor por defecto es cero.

Ejemplo:

```
RIP config> COST-ADDITIONAL
IP addresses for each interface:
 ethernet0/0      192.7.1.253      255.255.255.0   NETWORK broadcast, fill 0
 serial0/0
 serial0/1        10.0.0.1         255.255.255.0   NETWORK broadcast, fill 0
 serial0/2
 bri0/0
 x25-node
Which address (ifc name for unnumbered) [0.0.0.0]? 192.7.1.253
Per interface additional cost [0]? 5
RIP config>
```

Si introducimos un valor fuera del rango permitido:

Ejemplo:

```
RIP config> COST-ADDITIONAL
IP addresses for each interface:
 ethernet0/0      192.7.1.253      255.255.255.0   NETWORK broadcast, fill 0
 serial0/0
 serial0/1        10.0.0.1         255.255.255.0   NETWORK broadcast, fill 0
 serial0/2
 bri0/0
 x25-node
Which address (ifc name for unnumbered) [0.0.0.0]? 192.7.1.253
Per interface additional cost [5]? 16
Must be less than 16. Using default value.
RIP config>
```

1.9. DISABLE

El comando **DISABLE** deshabilita el protocolo RIP en el equipo.

Sintaxis:

```
RIP config> DISABLE
```

Ejemplo:

```
RIP config> DISABLE
RIP config>
```

1.10. DISTRIBUTE-LIST

El comando **DISTRIBUTE-LIST** permite establecer filtros para las rutas distribuidas, tanto las entrantes (recibidas) como las salientes (anunciadas). Toda ruta se contrastará con las correspondientes listas de distribución, y sólo en el caso de que no sea rechazada por ninguna de estas listas se seguirá procesando dicha ruta.

Las listas empleadas para filtrar las rutas serán Listas de Control de Acceso estándar, configurables desde el menú FEATURE ACCESS del Proceso de Configuración.

Es importante notar que las listas de acceso especificadas mediante este comando se aplicarán a las rutas contenidas en los paquetes RIP, y no a los campos de dirección origen ni destino de dichos paquetes.

El comando **DISTRIBUTE-LIST** tiene dos opciones, una para configurar la lista aplicable a las rutas recibidas, y otra para configurar la lista aplicable a las rutas a anunciar.

Sintaxis:

```
RIP config> DISTRIBUTE-LIST ?  
IN  
OUT
```

a) DISTRIBUTE-LIST IN

Mediante este comando podremos configurar la lista de distribución global, aplicable a todas las rutas recibidas por cualquier interfaz.

Para que una ruta sea aceptada y procesada debe ser permitida por la lista de distribución global, y también por la lista de distribución del interfaz por el que se recibió.

La lista de acceso a emplear debe existir y no estar asignada a ningún otro protocolo, por lo que antes de emplear este comando deberemos haber creado la lista en cuestión desde el menú de configuración FEATURE ACCESS.

Los valores válidos de lista de control de acceso son del 1 al 99 (listas IP estándar).

Ejemplo:

```
RIP config> DISTRIBUTE-LIST IN  
Access list for routes filtering [0]? 1  
RIP config>
```

b) DISTRIBUTE-LIST OUT

Mediante este comando podremos configurar la lista de distribución global, aplicable a todas las rutas a enviar por cualquier interfaz.

Para que una ruta se envíe debe ser permitida por la lista de distribución global, y también por la lista de distribución del interfaz por el que se va a enviar.

La lista de acceso a emplear debe existir y no estar asignada a ningún otro protocolo, por lo que antes de emplear este comando deberemos haber creado la lista en cuestión desde el menú de configuración FEATURE ACCESS.

Los valores válidos de lista de control de acceso son del 1 al 99 (listas IP estándar).

Ejemplo:

```
RIP config> DISTRIBUTE-LIST OUT  
Access list for routes filtering [0]? 1  
RIP config>
```

1.11. ENABLE

El comando **ENABLE** habilita el protocolo RIP en el equipo.

Sintaxis:

```
RIP config> ENABLE
```


Ejemplo:

```
RIP config> ENABLE
RIP config>
```

1.12. LIMIT-RIP

El comando **LIMIT-RIP** desactiva el protocolo RIP en interfaces Frame Relay. Cuando LIMIT-RIP está habilitado, los paquetes de RIP no se envían por los interfaces Frame Relay a no ser que éstos estén en backup por RDSI. La opción por defecto de LIMIT-RIP es deshabilitada.

Este comando está pensado para el funcionamiento del **Router Teldat** con la unidad de backup **CENTRIX-P** en ciertos escenarios de backup de circuitos virtuales de Frame Relay por RDSI. Este comando afecta a todos los interfaces Frame Relay del equipo.

NOTA: Este comando no debe habilitarse en otras situaciones y siempre debe ser utilizado por personal experto.

Ejemplo:

```
RIP config> LIMIT-RIP
Limit RIP: enabled.
RIP config>
```

1.13. LIST

Sintaxis:

```
RIP config> LIST ?
ADDRESS-OPTIONS      See all the options for a determined interface
ALL                  Obtain a list of all configured parameters
AS-LABELS           Obtain a list of all the address labels identifying the AS
DISTRIBUTE-LISTS    See all configured access lists
LIMIT-RIP          See the LIMIT-RIP option
TIMERS              Obtain a list of the values configured in the timers
```

a) LIST ADDRESS-OPTIONS

Utilizar el comando **LIST ADDRESS-OPTIONS** para ver todas las opciones de un determinado interfaz.

Ejemplo:

```
RIP config> LIST ADDRESS-OPTIONS
Enter address [0.0.0.0]? 192.7.1.253
Address: 192.7.1.253
Output distribute list:.....No
Send network routes:.....Yes
Send subnetwork routes:.....Yes
Send static routes:.....No
Send direct routes:.....Yes
Send default routes:.....No
Poison reverse enabled:.....Yes
Autonomous system label:.....0
Sending compatibility:.....RIP2 Multicast.
Input distribute list:.....No
Receive network routes:.....Yes
Receive subnetwork routes:.....Yes
Overwrite default routes:.....No
Overwrite static routes:.....No
Receiving compatibility:.....RIP2.
Authentication:.....Clear password.
Aggregation type:.....Do not aggregate.
```

```
Allow disconnected subnetted networks:..Yes
Per interface additional cost: 0
RIP config>
```

b) LIST ALL

Utilizar el comando **LIST ALL** para obtener un listado de todos los parámetros configurados.

Ejemplo:

```
RIP config> LIST ALL
RIP: enabled
RIP default origination: OSPF, cost = 1
Options per interface address:
Interface: ethernet0/0
Address: 192.7.1.253
Output distribute list:.....No
Send network routes:.....Yes
Send subnetwork routes:.....Yes
Send static routes:.....No
Send direct routes:.....Yes
Send default routes:.....No
Poison reverse enabled:.....Yes
Autonomous system label:.....0
Sending compatibility:.....RIP2 Multicast.
Input distribute list:.....No
Receive network routes:.....Yes
Receive subnetwork routes:.....Yes
Overwrite default routes:.....No
Overwrite static routes:.....No
Receiving compatibility:.....RIP2.
Authentication:.....Clear password.
Aggregation type:.....Do not aggregate.
Allow disconnected subnetted networks:..Yes
Per interface additional cost: 0
more ?
Interface: serial0/1
Address: 10.0.0.3
Output distribute list:.....No
Send network routes:.....Yes
Send subnetwork routes:.....Yes
Send static routes:.....No
Send direct routes:.....Yes
Send default routes:.....No
Poison reverse enabled:.....Yes
Autonomous system label:.....0
Sending compatibility:.....RIP2 Broadcast.
Input distribute list:.....No
Receive network routes:.....Yes
Receive subnetwork routes:.....Yes
Overwrite default routes:.....No
Overwrite static routes:.....No
Receiving compatibility:.....RIP1 or RIP2.
Authentication:.....No.
Aggregation type:.....Do not aggregate.
Allow disconnected subnetted networks:..Yes
Per interface additional cost: 0
more ?
Address: 192.3.1.2
Output distribute list:.....No
Send network routes:.....Yes
Send subnetwork routes:.....Yes
Send static routes:.....No
Send direct routes:.....Yes
Send default routes:.....No
Poison reverse enabled:.....Yes
Autonomous system label:.....0
Sending compatibility:.....RIP2 Broadcast.
Input distribute list:.....No
Receive network routes:.....Yes
Receive subnetwork routes:.....Yes
```

```
Overwrite default routes:.....No
Overwrite static routes:.....No
Receiving compatibility:.....RIP1 or RIP2.
Authentication:.....No.
Aggregation type:.....Do not aggregate.
Allow disconnected subnetted networks:..Yes
Per interface additional cost: 0

more ?
Accept RIP updates always for:
[NONE]

RIP timers:
Periodic sending timer: 30
Route expire timer: 180
Route garbage timer: 120
Limit RIP: disabled.
Output distribute list: No
Input distribute list: No
RIP config>
```

c) LIST AS-LABELS

Utilizar el comando **LIST AS-LABELS** para obtener un listado de todas las etiquetas de las direcciones que identifican los Sistemas Autónomos (Autonomous Systems -AS-) configurados en esa dirección.

Ejemplo:

```
RIP config> LIST AS-LABELS
AS labels per interface
10.0.0.3      0
192.3.1.2    0
192.7.1.253  0
RIP config>
```

d) LIST DISTRIBUTE-LISTS

Utilizar el comando **LIST DISTRIBUTE-LISTS** para ver las listas de distribución globales, es decir, las listas configuradas para filtrar a nivel global las rutas a anunciar y las rutas recibidas.

Ejemplo:

```
RIP config> LIST DISTRIBUTE-LISTS
Output distribute list: No
Input distribute list: No
RIP config>
```

*Este comando sólo muestra las listas de distribución globales; para ver las específicas de cada interfaz se debe emplear el comando **LIST ADDRESS-OPTIONS** o el comando **LIST ALL**.*

e) LIST LIMIT-RIP

Utilizar el comando **LIST LIMIT-RIP** para ver la opción de LIMIT-RIP.

Ejemplo:

```
RIP config> LIST LIMIT-RIP
Limit RIP: disabled.
RIP config>
```

f) LIST TIMERS

Utilizar el comando **LIST TIMERS** para obtener un listado de los valores configurados en los temporizadores.

Ejemplo:

```
RIP config> LIST TIMERS
RIP timers:
Periodic sending timer: 30
Route expire timer: 180
Route garbage timer: 120
RIP config>
```

1.14. NO

El comando **NO** se emplea para eliminar o deshabilitar ciertas funcionalidades.

Sintaxis:

RIP config> NO ?	
ACCEPT-RIP-ROUTE	Accept rts with determined network dst
ALLOW-DISCONNECTED-SUBNETTED-NETWORKS	Routes to subnets are always sent
AUTHENTICATION	Authentication is sent and checked
DISTRIBUTE-LIST	Establish input/output filters
LIMIT-RIP	Deactivates the RIP protocol in FR
ORIGINATE-RIP-DEFAULT	Originate a default ip route

a) NO ACCEPT-RIP-ROUTE

Utilizar el comando **NO ACCEPT-RIP-ROUTE** para borrar una ruta de la lista de redes que el protocolo RIP siempre acepta.

Sintaxis:

```
RIP config> NO ACCEPT-RIP-ROUTE <dir IP-RED/SUBRED>
```

Ejemplo:

```
RIP config> NO ACCEPT-RIP-ROUTE 10.0.0.0
RIP config>
```

b) NO ALLOW-DISCONNECTED-SUBNETTED-NETWORKS

Se utiliza el comando **NO ALLOW-DISCONNECTED-SUBNETTED-NETWORKS** para que las rutas a subredes no se propaguen fuera del ámbito de la red a la que dichas subredes pertenecen. Del mismo modo, un interfaz dado no aceptará rutas a subredes que no sean de la red de ese interfaz.

Al ejecutar este comando aparece un listado de todos los interfaces lógicos (direcciones IP) donde se puede configurar. Introducimos una dirección existente y el envío y recepción de subredes desconectadas fuera del ámbito de su red quedará deshabilitado para dicha dirección.

Sintaxis:

```
RIP config> NO ALLOW-DISCONNECTED-SUBNETTED-NETWORKS <dir IP-RED/SUBRED>
```

c) NO AUTHENTICATION

Utilizar el comando **NO AUTHENTICATION** para deshabilitar la autenticación en un interfaz dado.

Sintaxis:

```
RIP config> NO AUTHENTICATION <dir IP-RED/SUBRED>
```

Ejemplo:

```
RIP config> NO AUTHENTICATION 10.0.0.0
RIP config>
```

d) NO DISTRIBUTE-LIST

Utilizar el comando **NO DISTRIBUTE-LIST** para deshabilitar el filtrado de las rutas entrantes o de las rutas a enviar. Este comando sólo afecta al filtro global configurado mediante el comando **DISTRIBUTE-LIST**, no al configurado en cada interfaz.

El comando **NO DISTRIBUTE-LIST** tiene dos opciones, una para deshabilitar el filtrado de las rutas recibidas, y otra para deshabilitar el de las rutas a anunciar.

Ejemplo:

```
RIP config> NO DISTRIBUTE-LIST ?
IN
OUT
```

e) NO LIMIT-RIP

El comando **NO LIMIT-RIP** activa el protocolo RIP en interfaces Frame Relay. Debe utilizarse este comando si ya no se quiere restringir el protocolo RIP en el equipo.

Ejemplo:

```
RIP config> NO LIMIT-RIP
Limit RIP: disabled.
RIP config>
```

f) NO OFFSET-LIST

El comando **NO OFFSET-LIST** elimina una offset-list previamente configurada.

Ejemplo:

```
RIP config> NO OFFSET-LIST 1 in 3
RIP config>
```

g) NO ORIGINATE-RIP-DEFAULT

El comando **NO ORIGINATE-RIP-DEFAULT** evita que el router genere una ruta por defecto.

Ejemplo:

```
RIP config> NO ORIGINATE-RIP-DEFAULT
RIP config>
```

1.15. OFFSET-LIST

Una **OFFSET-LIST** permite incrementar el coste de ciertas rutas tanto en transmisión como en recepción. Este incremento de coste se realiza únicamente para las rutas que encajan dentro de la lista de acceso configurada como una offset-list. Opcionalmente se permite especificar un interfaz en concreto sobre el cuál realizar el incremento de coste.

Las listas empleadas para variar el coste de las rutas serán Listas de Control de Acceso estándar, configurables desde el menú FEATURE ACCESS del Proceso de Configuración.

Para comparar las direcciones IP y máscara de la ruta con las de la lista de acceso se utiliza el mismo procedimiento que para las distribute-list teniendo aquí el mismo efecto el parche RIP_LISTS_USE_MASK (ver apéndice A apartado 4).

Sintaxis:

```
RIP config> OFFSET-LIST <access-list>
ip-address      ip address to which the offset list is applied
in              applies the access list to incoming metrics
no
out             applies the access list to outgoing metrics
```

- ip-address** Especifica la dirección IP de un interfaz concreto. Si no se configura este parámetro el offset se aplica a todos los interfaces del router que envíen/reciban rutas RIP.
- in <offset>** Incrementa el coste de las rutas entrantes que encajan con la lista de acceso configurada.
- out <offset>** Incrementa el coste de las rutas salientes que encajan con la lista de acceso configurada.

Ejemplo 1:

Se desea aumentar en 3 el coste de todas las rutas enviadas por cualquier interfaz que estén incluidas en la red 172.24.0.0.

```
Config> SHOW CONFIG
feature access-lists
; -- Access Lists user configuration --
  access-list 1
;
  entry 1 default
  entry 1 permit
  entry 1 source address 172.24.0.0 255.255.0.0
;
  exit
;
exit
;
protocol rip
; -- RIP protocol user configuration --
  enable
  offset-list 1 out 3
;
exit
;
```

Ejemplo 2:

Se desea aumentar en 1 el coste de todas las rutas de la red 172.1.0.0 que sean enviadas por el interfaz con dirección IP 172.24.78.131 o por el interfaz con dirección IP 10.30.1.1, excepto las referidas exclusivamente al host 172.1.1.5.

```
Config> SHOW CONFIG
feature access-lists
; -- Access Lists user configuration --
  access-list 1
;
  entry 1 default
  entry 1 deny
  entry 1 source address 172.1.1.5 255.255.255.255
;
  entry 2 default
  entry 2 permit
```

```

    entry 2 source address 172.1.0.0 255.255.0.0
;
    exit
;
exit
;
protocol rip
; -- RIP protocol user configuration --
    enable
    offset-list 1 out 1 ip-address 172.24.78.131
;
    offset-list 1 out 1 ip-address 10.30.1.1
;
exit

```

1.16. ORIGINATE-RIP-DEFAULT

El comando **ORIGINATE-RIP-DEFAULT** se debe utilizar si la red utiliza RIP, y se conecta a una red que usa otro protocolo de routing (como OSPF) para establecer (originar) una ruta por defecto hacia esa red.

Esta ruta por defecto encaminará tráfico para redes no RIP hacia un router que hará funciones de puerta. El **Router Teldat** sólo acepta OSPF.

Ejemplo:

```

RIP config> ORIGINATE-RIP-DEFAULT
Originate default of cost[1]? 1
RIP config>

```

1.17. RECEIVING

Se utiliza el comando **RECEIVING** para configurar los parámetros de recepción RIP de los interfaces de red del router. El conjunto de rutas que se procesan por un interfaz lógico (dirección IP) es la unión de las rutas seleccionadas activando alguno de los flags que a continuación se describen. Dichos flags controlan como la información recibida en las tramas RIP se incorpora en las tablas de routing del router. La activación de ciertos flags permiten al router no tomar en cuenta la información de routing estática, en el caso de que el RIP encuentre una ruta mejor que la prefija da.

Al ejecutar dicho comando aparece un listado de todos los interfaces lógicos (direcciones IP) locales donde se puede configurar la recepción RIP. Introducimos una dirección existente y a continuación seleccionamos la opción deseada para habilitarla, o la palabra “no” seguida de la opción para deshabilitarla:

Sintaxis:

```

RIP config> RECEIVING <dir IP-RED/SUBRED>
default-routes      process default routes
distribute-list     access list for routes filtering
network-routes      process network routes
no
    default-routes      process default routes
    distribute-list     access list for routes filtering
    network-routes      process network routes
    subnetwork-routes   process subnetwork routes
    static-routes       process static routes
subnetwork-routes   process subnetwork routes
static-routes       process static routes

```

El significado de las opciones es:

<i>default-routes</i>	Previene que una ruta RIP por defecto, la cual es recibida por la dirección del Interfaz IP, sea almacenada como ruta por defecto.
<i>distribute-list</i>	Determina la lista a emplear para filtrar las rutas recibidas por la dirección del Interfaz IP. Esta opción está deshabilitada por defecto, con lo que las rutas no se ven afectadas por este filtrado. Para configurar esta opción se deberá indicar una Lista de Control de Acceso IP estándar (1 a 99) previamente definida desde el menú de configuración FEATURE ACCESS.
<i>network-routes</i>	Si está activado se aceptan rutas de red, si está desactivado se aceptan sólo aquellas rutas de red introducidas con el comando ACCEPT-RIP-ROUTE .
<i>subnetwork-routes</i>	Si está activado se aceptan rutas de subred, si está desactivado se aceptan sólo aquellas rutas de subred introducidas con el comando ACCEPT-RIP-ROUTE .
<i>static-routes</i>	Este comando previene que rutas RIP recibidas en la dirección IP del interfaz sobrescriban las rutas estáticas.

Si el flag “Allow disconnected subnetted networks” está deshabilitado: por un interfaz dado sólo se aceptan aquellas rutas de subred que pertenecen a la misma red IP que el interfaz. Por ejemplo, sea la ruta subred destino : 192.6.1.144 máscara : 255.255.255.248, si el interfaz de entrada tiene dirección 192.6.1.x, la ruta se acepta. Pero si el interfaz de entrada pertenece a otra red IP, por ejemplo 193.5.1.x, la ruta que se recibe se rechaza. Si, por el contrario, el flag “Allow disconnected subnetted networks” está habilitado, entonces se permite la recepción de subredes también por interfaces que no pertenecen a la subred.

1.18. SENDING

Se utiliza el comando **SENDING** para configurar los parámetros de envío RIP de los interfaces de red del router. El tipo de rutas a enviar por un determinado interfaz depende del estado de los flags que a continuación se describen.

Al ejecutar dicho comando aparece un listado de todos los interfaces lógicos (direcciones IP) donde se puede configurar el envío RIP. Introducimos una dirección existente y a continuación seleccionamos la opción deseada para habilitarla, o la palabra “no” seguida de la opción para deshabilitarla:

Sintaxis:

```
RIP config> SENDING <dir IP-RED/SUBRED>
default-routes      process default routes
direct-routes      process direct routes
distribute-list     access list for routes filtering
network-routes     process network routes
no
  default-routes    process default routes
  direct-routes     process direct routes
  distribute-list   access list for routes filtering
  network-routes   process network routes
  poisoned-reverse  poisoned reverse enable/disable
  subnetwork-routes process subnetwork routes
  static-routes     process static routes
poisoned-reverse   poisoned reverse enable/disable
subnetwork-routes  process subnetwork routes
static-routes      process static routes
```

El significado de las opciones es:

<i>default-routes</i>	Si este flag está activado, el router indica la ruta por defecto en las respuestas RIP relacionadas con la dirección IP, si es que existe un router por defecto. La ruta para el router por defecto se señala como una ruta al destino 0.0.0.0.
-----------------------	---

<i>direct-routes</i>	Si este flag está activado, el router incluirá todas las rutas de las redes conectadas directamente en las respuestas RIP relacionadas con la dirección IP. Si no está activado, sólo se enviarán las redes directamente conectadas que participen del protocolo RIP (que tengan habilitado RIP para envío o para recepción). Por defecto está activado.
<i>distribute-list</i>	Determina la lista a emplear para filtrar las rutas a enviar relacionadas con la dirección del Interfaz IP. Esta opción está deshabilitada por defecto, con lo que las rutas no se ven afectadas por este filtrado. Para configurar esta opción se deberá indicar una Lista de Control de Acceso IP estándar (1 a 99) previamente definida desde el menú de configuración FEATURE ACCESS.
<i>network-routes</i>	Si este flag está activado, el router indica todas las rutas a nivel de red en las respuestas RIP relacionadas con la dirección IP.
<i>poisoned-reverse</i>	Este flag está activo por defecto. Habilita o deshabilita el poisoned reverse en el proceso del split-horizon. Cuando está habilitado las rutas que se han aprendido de un gateway dado se anuncian con métrica infinito (16). Si está deshabilitado dichas rutas simplemente no se anuncian. Lo mejor es que esté habilitado porque así la convergencia del protocolo es más rápida.
<i>subnetwork-routes</i>	Si este flag está activado, el router indica las rutas de subred en las respuestas RIP relacionadas con la dirección IP. El envío de una ruta de subred depende de la configuración del tipo de agregación y del flag "Allow disconnected subnetted networks". Si el tipo de agregación es "Use aggregation routes" y la ruta esta agregada por una ruta de agregación (Aggr), sólo se envía la ruta de agregación (Aggr). Si está configurada la agregación como "Aggregate subnets", entonces se envían ambas, tanto la subred como la agregación de subred (Sbnt). Si el flag "Allow disconnected subnetted networks" está deshabilitado: por un interfaz dado sólo se incluyen aquellas rutas de subred que pertenecen a la misma red IP que el interfaz. Para el resto de interfaces se incluye la ruta de red. Por ejemplo, sea la ruta subred destino : 192.6.1.144 máscara : 255.255.255.248, si el interfaz de salida tiene dirección 192.6.1.x, la ruta se envía tal cual. Pero si el interfaz de salida pertenece a otra red IP, por ejemplo 193.5.1.x, la ruta que se envía es la agregación red destino: 192.6.1.0 máscara: 255.255.255.0. Si el flag "Allow disconnected subnetted networks" está habilitado entonces se permite el envío de subredes también por interfaces que no pertenecen a la subred.
<i>static-routes</i>	Si este flag está activado, el router incluirá todas las rutas de las redes configuradas estáticamente en las respuestas RIP relacionadas con la dirección IP.

El conjunto de rutas a enviar por un determinado interfaz depende también del tipo de agregación configurado.

1.19. TIMERS

Tal como queda definido RIP en su RFC existen 3 temporizadores que controlan el funcionamiento de su algoritmo. Únicamente en casos excepcionales podría ser deseable cambiar sus valores, para ello el administrador debe estar seguro y entender las posibles consecuencias.

Ejemplo:

```
RIP config> TIMERS
Enter periodic sending timer [30]? 30
Enter route expire timer [180]? 180
Enter route garbage timer [120]? 120
RIP config>
```

El significado de los parámetros es:

Periodic sending timer

Su valor por defecto es de 30 segundos y es el tiempo que transcurre entre envío de respuestas periódicas.

Route expire timer

Su valor por defecto es de 180 segundos. Si transcurre dicho tiempo sin haber sido refrescada una ruta por una respuesta, dicha ruta pasará a ser inválida.

Route garbage timer

Su valor por defecto es de 120 segundos. Una vez dada como inválida una ruta se mantiene en la tabla de rutas durante 120 segundos con métrica 16 (infinito) para que los routers RIP vecinos se den cuenta que va a ser borrada.

1.20. EXIT

Utilizar el comando **EXIT** para volver al nivel de prompt en el que se estaba anteriormente.

Sintaxis:

```
RIP config> EXIT
```

Ejemplo:

```
RIP config> EXIT
Config>
```

Capítulo 3

Monitorización RIP



1. Comandos de Monitorización del protocolo RIP

En este capítulo se describen los comandos para monitorizar el protocolo RIP. Para acceder al entorno de monitorización del protocolo RIP, se deben introducir los siguientes comandos:

```
*PROCESS 3
Console Operator
+PROTOCOL RIP
RIP protocol monitor
RIP>
```

Comando	Función
? (AYUDA)	Lista los comandos u opciones disponibles.
LIST	Muestra los estadísticos RIP.
EXIT	Sale del proceso de monitorización RIP.

1.1. ? (AYUDA)

Utilizar el comando ?(AYUDA) para listar los comandos disponibles en el prompt en el que se esté trabajando. También se puede usar este comando a continuación de un comando específico para listar las opciones disponibles.

Sintaxis:

```
RIP> ?
```

Ejemplo:

```
RIP> ?
LIST
EXIT
RIP>
```

1.2. LIST

Utilizar el comando LIST para mostrar estadísticas RIP. Además se muestran estadísticas detalladas para cada interfaz.

Sintaxis:

```
RIP> LIST
```

Ejemplo:

```
RIP> LIST
RIP globals:
Route changes due to RIP:.....0
Responses sent due to received requests:.....0

RIP per interface:
      Pack. rx errors      Ruotes rx errors      Triggered updates tx
Interface: ethernet0/0
192.7.1.253                0                    0                    0
Interface: serial0/0
Interface: serial0/1
10.0.0.1                   0                    0                    2
```

```
Interface: serial0/2
Interface: bri0/0
Interface: x25-node
RIP>
```

El significado de los parámetros es:

Pack. rx errors	Contabiliza el número de paquetes con error recibidos.
Ruotes rx errors	Contabiliza el número de rutas erróneas recibidas.
Triggered updates tx	Contabiliza las actualizaciones por cambio de ruta enviados.

1.3. EXIT

Utilizar el comando **EXIT** para volver al nivel de prompt en el que se estaba anteriormente.

Sintaxis:

```
RIP> EXIT
```

Ejemplo:

```
RIP> EXIT
```

Apéndice A

Filtrado mediante listas



1. Introducción

Mediante los comandos **DISTRIBUTE-LIST**, **RECEIVING DISTRIBUTE-LIST** y **SENDING DISTRIBUTE-LIST** se puede configurar una potente herramienta de filtrado de rutas en función de su red de destino. Esta herramienta se basa en Listas IP Estándar de Control de Acceso para determinar qué rutas se distribuyen y cuáles se descartan.

2. Uso de las listas para filtrar rutas

Para determinar qué rutas se distribuyen y cuáles se descartan se compara cada ruta con las Listas de Control de Acceso asignadas, que deben ser listas IP Estándar.

- En recepción: sólo se procesa la ruta si es permitida por la lista configurada mediante el comando **DISTRIBUTE-LIST IN** y también por la lista configurada mediante el comando **RECEIVING <dirección red IP por la que llega la ruta> DISTRIBUTE-LIST**.
- En transmisión: sólo se envía la ruta si es permitida por la lista configurada mediante el comando **DISTRIBUTE-LIST OUT** y también por la lista configurada mediante el comando **SENDING <dirección red IP por la que se envía la ruta> DISTRIBUTE-LIST**.

Para determinar si una lista permite una ruta, se comprueba la ruta con cada entrada de la lista, siempre en el orden definido al crear la lista.

- La primera entrada que concuerda con la ruta es la que determina si la lista permite o no dicha ruta.
- Si ninguna entrada concuerda con la ruta, la lista no permite dicha ruta.

Para comparar una ruta con una entrada de la lista se toma la dirección de la red anunciada, y se compara con la dirección/máscara de origen de la entrada de la lista.

El protocolo RIP sólo puede utilizar listas IP Estándar, y sólo se emplea el campo Origen de las entradas de la lista.

Por ejemplo, supongamos que tenemos la siguiente lista configurada:

```
Standard Access List 1, assigned to RIP
1 DENY SRC=192.168.1.0/24
2 PERMIT SRC=192.168.0.0/16
```

Si aplicamos esta lista en recepción tendremos que:

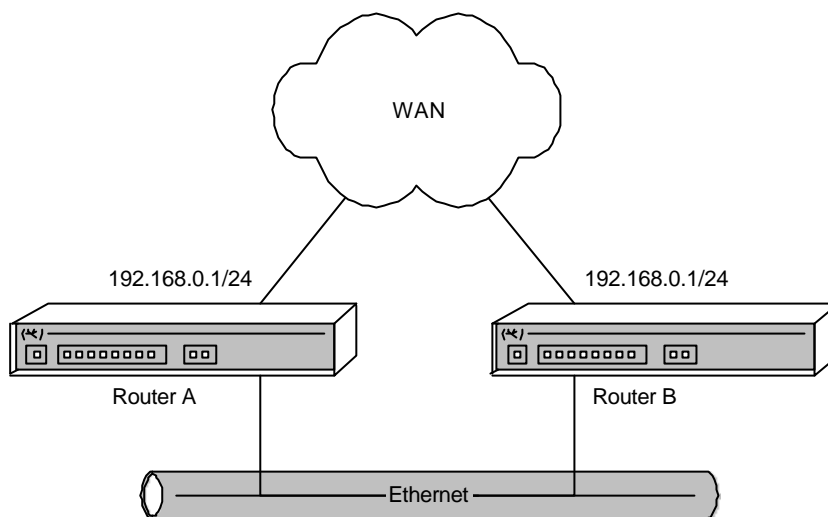
- Si recibimos la ruta a la red 192.168.1.0 la descartaremos, porque concuerda con la primera entrada de la lista, y ésta la Deniega.
- Si recibimos la ruta a la red 192.168.2.0 la procesaremos, porque no concuerda con la primera entrada, pero sí con la segunda, y esta entrada la Permite.
- Si recibimos la ruta a la red 192.168.0.0 la procesaremos, porque no concuerda con la primera entrada, pero sí con la segunda, que la Permite.
- Si recibimos la ruta a la red 192.6.2.0 la descartaremos, porque no concuerda con ninguna entrada de la lista, y la acción por defecto es Denegar.
- Si recibimos una ruta por defecto (red 0.0.0.0) la descartaremos, porque no concuerda con ninguna entrada de la lista, y la acción por defecto es Denegar.

Siempre que se quiera que una lista no descarte rutas por defecto, se deberá añadir una entrada a tal efecto, ya que las rutas por defecto se propagan por RIP como la red 0.0.0.0/0.

3. Escenario de ejemplo

En este apartado se presenta un escenario básico de una entidad que accede a sus oficinas a través de dos **Routers Teldat**.

Supongamos que tenemos dos equipos instalados en un mismo segmento, que dan acceso a las oficinas de la entidad, tal como se muestra en la siguiente figura:



En este caso tanto Router A como Router B acceden a la WAN con la misma dirección IP (192.168.0.1), y no queremos que dicha red se propague por RIP al segmento.

Para ello basta con definir una lista de acceso:

```
Config> FEATURE ACCESS

-- Access Lists user configuration --
Access Lists config> ACCESS-LIST 1

Standard Access List 1> ENTRY 1 DENY
Standard Access List 1> ENTRY 1 SOURCE ADDRESS 192.168.0.0 255.255.255.0
Standard Access List 1> ENTRY 2 PERMIT
Standard Access List 1> EXIT
Access Lists config> EXIT
```

y asignar la lista de acceso al protocolo RIP para filtrar las rutas a enviar:

```
Config> PROTOCOL RIP

-- RIP protocol user configuration --
RIP config> DISTRIBUTE-LIST OUT 1
RIP config> EXIT
Config>
```

De este modo conseguiremos que se propaguen todas las rutas menos las de la red 192.168.0.0. Hay algunos puntos que conviene destacar:

- Se ha tenido que añadir la segunda entrada de la lista (Permitir 0.0.0.0/0) porque la acción por defecto de una lista (cuando no concuerda ninguna entrada) es Denegar. De este modo se Permitirán todas las rutas que no concuerden con la primera entrada.
- La primera entrada denegaría la red de agregación 192.168.0.0/16, ya que su dirección IP (192.168.0.0) está contenida en 192.168.0.0/24.
- La lista permite la propagación de rutas por defecto gracias a la segunda entrada.

4. Filtrado de rutas con máscara

En ocasiones puede ser necesario emplear no sólo la dirección IP, sino también la máscara de la ruta propagada por RIP a la hora de filtrar mediante listas.

Retomemos el escenario de ejemplo, en el que creábamos una lista para impedir que la red 192.168.0.0/24 se propagase por RIP:

```
Standard Access List 1, assigned to RIP
1      DENY    SRC=192.168.0.0/24
2      PERMIT  SRC=0.0.0.0/0
```

En este caso nos encontramos con la imposibilidad de hacer que la red de agregación 192.168.0.0/16 se propague por RIP, ya que ambas redes comparten la misma dirección 192.168.0.0, que es Denegada por la primera entrada de la lista.

Para evitar esto, se puede habilitar un *patch* que obliga a comparar también la máscara. Cuando se habilita este *patch*, la red de la ruta sólo concuerda con una entrada de la lista si:

- la red de la ruta es idéntica a la red de origen de la entrada o
- la red de la ruta es una subred de la red de origen de la entrada.

Por ejemplo, con la lista del escenario:

- Las rutas a la red 192.168.0.0/24 se descartan
- Las rutas a la red 192.168.0.0/16 no se descartan
- Las rutas a la red 192.168.0.0/32 se descartan

Para habilitar el *patch* emplearemos el comando de configuración **ENABLE PATCH** y asignaremos el valor **1** con nombre **RIP_LISTS_USE_MASK**.

Ejemplo:

```
Config> ENABLE PATCH
Patch Name:  [ ]? RIP_LISTS_USE_MASK
Patch Value: [0]? 1
Config>
```

Para deshabilitar el *patch* emplearemos el comando de configuración **DISABLE PATCH** con el nombre **RIP_LISTS_USE_MASK**.

Ejemplo:

```
Config> DISABLE PATCH
Patch Name:  [ ]? RIP_LISTS_USE_MASK
Config>
```

5. Filtrado de la ruta por defecto

Es posible filtrar la ruta por defecto mediante listas de acceso, tanto para permitirla como para descartarla, pero la configuración varía según tengamos o no habilitado el parche **RIP_LISTS_USE_MASK**. A continuación se muestran las configuraciones de lista de acceso para cada caso.

Permitir la ruta por defecto, sin habilitar RIP_LISTS_USE_MASK

La siguiente entrada de la lista de acceso permite explícitamente la ruta por defecto:

```
Standard Access List 1> ENTRY 1 SOURCE ADDRESS 0.0.0.0 255.255.255.255
```

Permitir la ruta por defecto, con RIP_LISTS_USE_MASK habilitado

En este caso, para permitir sólo la ruta por defecto, deberemos denegar todas las rutas (subredes) que no queramos distribuir, tal como se muestra en el siguiente ejemplo, en el que sólo se permite la ruta por defecto, descartando todas las demás:

```
Standard Access List 1> ENTRY 1 DENY
Standard Access List 1> ENTRY 1 SOURCE ADDRESS 128.0.0.0 128.0.0.0
Standard Access List 1> ENTRY 2 DENY
Standard Access List 1> ENTRY 2 SOURCE ADDRESS 0.0.0.0 128.0.0.0
Standard Access List 1> ENTRY 3 PERMIT
```

Descartar la ruta por defecto, sin habilitar RIP_LISTS_USE_MASK

Para descartar solamente la ruta por defecto podemos crear una lista de acceso del siguiente modo:

```
Standard Access List 1> ENTRY 1 DENY
Standard Access List 1> ENTRY 1 SOURCE ADDRESS 0.0.0.0 255.255.255.255
Standard Access List 1> ENTRY 2 PERMIT
```

Descartar la ruta por defecto, con RIP_LISTS_USE_MASK habilitado

En este caso, para descartar solamente la ruta por defecto, deberemos permitir todas las demás rutas (subredes), tal como se muestra en el siguiente ejemplo:

```
Standard Access List 1> ENTRY 1 SOURCE ADDRESS 128.0.0.0 128.0.0.0
Standard Access List 1> ENTRY 2 SOURCE ADDRESS 0.0.0.0 128.0.0.0
```