Router Teldat

Configuración TCP-IP

Doc. *DM702* Rev. *10.13*
Octubre, 2003

ÍNDICE

Capítulo 1 Introducción....1

1. Introducción al Protocolo IP 2
   1.1. Significado de las direcciones IP....2
   1.2. Tipos de direcciones IP 2
   1.3. Direcciones de subred 3
   1.4. Máscara de subred....4
   1.5. Routing IP....5
   a) Routers por defecto....6
   b) Datagramas defectuosos....6
   c) Identificador de router (Router ID)....6
   d) Dirección IP interna....7
   e) Dirección IP de gestión 7
   f) Paquetes broadcast....7
   g) Recepción de paquetes broadcast IP 7
   h) Multicamino por paquete....7
   i) IP classless 8
   j) Controles de acceso 9
   k) Traslación de direcciones (NAT)....9
   1.6. Protocolos de routing interiores....10

Capítulo 2 Configuración....11

1. Configuración del Protocolo IP....12
   1.1. Acceso al entorno de Configuración IP 12
   1.2. Asignación de direcciones IP a interfaces de red....12
   1.3. Habilitación del routing dinámico 12
   1.4. Agregación de información estática de routing....13
   a) Routers por defecto....13
   b) Router subred por defecto....14
   c) Red Estática / rutas subred....14
   d) Rutas de agregación 14
   e) Multicamino....14
   f) IP Classless 16
   1.5. Configuración de Controles de acceso IP....16
   a) Controles de acceso IP globales....16
   b) Controles de acceso IP por interfaz....18
   1.6. Configuración de NAT....19
   1.7. Configuración de NAPT....19
   1.8. Configuración de IPSEC 19
   1.9. Configuración de Policy Routing....19

Capítulo 3 Comandos de Configuración....20

1. Comandos de Configuración del Protocolo IP 21
   1.1. ? (AYUDA)....22
   1.2. ACCESS-CONTROL....22
   a) ACCESS-CONTROL ENABLED 22
   b) ACCESS-CONTROL ENTRY....23
   c) ACCESS-CONTROL MOVE 24
   1.3. ACCESS-GROUP 24
   1.4. ADDRESS....24
   1.5. AGGREGATION-ROUTE....25
   1.6. BROADCAST-ADDRESS....25
   a) BROADCAST-ADDRESS LOCAL-WIRE....26
   b) BROADCAST-ADDRESS NETWORK....26

1.7. CLASSLESS 26
1.8. DIRECTED-BROADCAST 27
1.9. DNS-DOMAIN-NAME 27
1.10. FILTER 27
1.11. ICMP-REDIRECTS 28
1.12. ICMP-UNREACHABLES 28
1.13. INTERNAL-IP-ADDRESS 28
1.14. IP-PARAM 29
a) IP-PARAM CACHE-SIZE 29
b) IP-PARAM REASSEMBLY-SIZE 29
c) IP-PARAM ROUTING-TABLE-SIZE 29
1.15. IPSEC 30
1.16. LIST 30
a) LIST ACCESS-CONTROLS 30
b) LIST ACCESS-GROUP 30
c) LIST ADDRESSES 31
d) LIST ALL 31
e) LIST DNS-DOMAIN-NAME 32
f) LIST IP-PARAM 32
g) LIST IP-PROTOCOL 33
h) LIST POLICY 33
i) LIST POOL 33
j) LIST ROUTES 33
k) LIST RULE 33
1.17. LOCAL 34
a) LOCAL ACCESS-GROUP 34
b) LOCAL POLICY 34
1.18. MULTIPATH 34
1.19. NAT 35
a) NAT DYNAMIC 35
b) NAT PAT 35
c) NAT STATIC 35
1.20. NO 36
1.21. POLICY 36
1.22. POOL 36
1.23. PROXY-ARP 37
1.24. ROUTE 37
1.25. ROUTER-ID 37
1.26. RULE 38
1.27. TVRP 40
1.28. EXIT 40

Capítulo 4 Monitorización 41

1. Comandos de Monitorización del Protocolo IP 42
1.1. ? (AYUDA) 43
1.2. AGGREGATION-ROUTES 43
1.3. ACCESS control 43
1.4. BPING 44
1.5. CACHE 45
1.6. COUNTERS 45
a) COUNTERS DELETE 46
b) COUNTERS SHOW 46
1.7. DUMP routing tables 47
1.8. INTERFACE addresses 48
1.9. IPSEC 48
1.10. NAT 49
1.11. NAPT 49
1.12. PING [address] 49

1.13. POOL 50
1.14. ROUTE given address 51
1.15. SIZES 52
1.16. STATIC-ROUTES 52
1.17. TRACEROUTE address 53
1.18. TVRP 54
1.19. EXIT 54

Capítulo 1
Introducción

1. Introducción al Protocolo IP

El IP es un protocolo a nivel de red de tipo no orientado a conexión que proporciona a los datos que se desean transmitir un servicio de conexión datagramas. Así pues el protocolo IP no garantiza que los datos transmitidos lleguen a su destino. Cuando se utiliza en Internet, el protocolo IP es la envoltura para transportar los datos, en esta red es el protocolo TCP (Transmission Control Protocol) el que garantiza que los datos lleguen a su destino.

TELDAT ha implementado el protocolo IP de acuerdo con los estándares definidos para el protocolo TCP/IP.

1.1. Significado de las direcciones IP

Una dirección IP identifica el lugar donde un interfaz de un ordenador se conecta a la red IP o a un segmento de ésta. Por ejemplo, si un ordenador tiene más de un interfaz conectado a la red, se le debe asignar una dirección IP distinta para cada uno de estos. La dirección IP es, por tanto, como una dirección de correos donde se indica donde hay que enviar los datos y no a quien hay que entregarlos.

La dirección IP es un número de 32 bits situado en la cabecera del datagrama. En ella se indica el segmento de red así como la identificación de un único ordenador dentro de la red.

Normalmente se utiliza una notación especial para indicar las direcciones IP: los 32 bits se dividen en cuatro grupos de 8. Los valores de dichos grupos están en decimal, separados por puntos.

Una dirección IP que en notación binaria sea:

10000000 00101010 00001010 00010111

equivale a:

128.42.10.23

Cada dirección IP tiene una parte para identificación de la red que se denomina **netid**, y otra para identificar el terminal u ordenador que se denomina **hostid**.

1.2. Tipos de direcciones IP

Hay tres tipos de direcciones IP: clase A, clase B y clase C. Los tipos se identifican por los bits más significativos de la dirección.

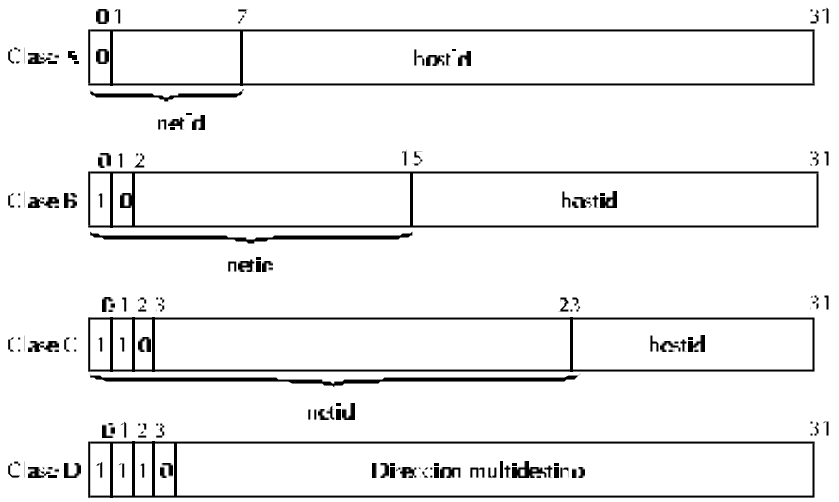
Las direcciones clase A se utilizan para las redes con más de 65.534 ordenadores. Se sabe que una dirección es clase A porque el bit más significativo vale 0. En clase A el campo **netid** ocupa los primeros 8 bits y el campo **hostid** los 24 restantes. Como se ve sólo hay 127 redes distintas de clase A.

La clase B se utiliza para redes de tamaño intermedio que tengan de 255 a 65.534 ordenadores. En estas direcciones los 16 primeros bits son el **netid** y los 16 restantes el **hostid**. Para reconocer una dirección como de clase B se tiene que cumplir que el primer y segundo bits sean 1 y 0 respectivamente.

Por último la clase C se utiliza para redes con menos de 255 ordenadores. Con estas direcciones los primeros 24 bits son el **netid** y los 8 restantes el **hostid**. Los tres bits más significativos de una dirección clase C son 1, 1 y 0.

Además de estas clases con las que se organizan las direcciones de los sistemas finales existe una cuarta clase, la clase D que identifica las direcciones multidestino o multicast en terminología

anglosajona. Para identificar una dirección multicast hay que comprobar que los cuatro bits más significativos sean 1, 1, 1 y 0. El resto de los bits de la dirección identifican el grupo multicast específico.



El router permite la asignación de múltiples direcciones IP en el mismo interfaz. Esto posibilita cierta flexibilidad cuando:

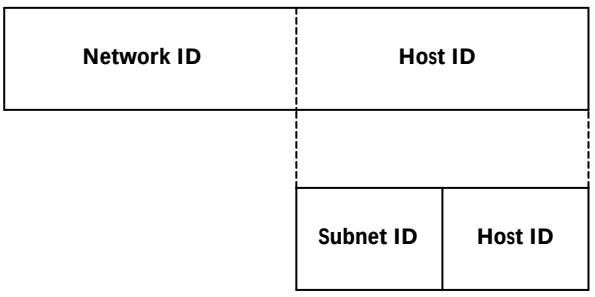
- Se esta en proceso de migrar de una dirección IP a otra.
- Se utilizan dos subredes en el mismo segmento de red físico. Por ejemplo, es posible que el número de ordenadores en un mismo segmento físico supere la capacidad de una subred. Cuando ocurre esto se puede añadir una nueva subred al segmento.

1.3. Direcciones de subred

El concepto de direccionamiento de subred (subnetting) permite que en una instalación con múltiples segmentos físicos utilice un único número de red IP. Las subredes añaden otro nivel de jerarquía en el esquema de direccionamiento de Internet. En lugar de la jerarquía de dos niveles (**netid**, **hostid**) se establece una de tres niveles (**netid**, **subnetid**, **hostid**). A una organización se le asigna de este modo uno o como mucho unos pocos números de red IP. La organización es libre de asignar distintos números de subred a sus distintos segmentos físicos, ya sean redes locales o redes de área extensa.

La estructura de subredes de una organización no es visible desde el punto de vista de cualquier ordenador o router situado fuera de los límites de dicha organización.

Conceptualmente, el añadir subredes sólo cambia la interpretación de la dirección IP. La dirección se divide en parte de red, parte de subred y parte de ordenador. Cada segmento físico se identifica entonces por la combinación de la parte de red y de subred.



No existe un tamaño normalizado para la parte de subred pudiendo ser unos pocos bits o la mayoría de los bits ocupados en principio por la parte de ordenador.

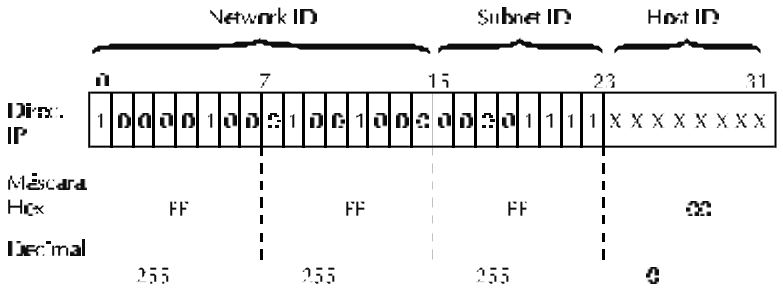
1.4. Máscara de subred

Cuando se añade una dirección IP a un interfaz hay que especificar la máscara de subred.

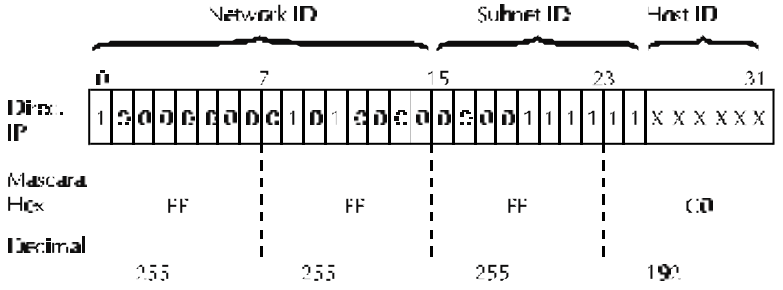
Dicha máscara identifica la porción de la dirección ocupada por los campos **netid** y **subnetid**. La máscara es simplemente otra cadena de 32 bits indicada en formato decimal separado por puntos en el que se indica con "1" la porción ocupada por los campos **netid** y **subnetid** y con "0" el espacio reservado a **hostid**.

Por ejemplo, supongamos que tenemos una dirección de clase B y que queremos asignar los 8 primeros bits del **hostid** como campo **subnetid**, dejando el nuevo **hostid** con sólo 8 bits. Siguiendo la regla de poner todo "1" los espacios ocupados por el **netid** y el **subnetid** y el resto a "0" tenemos la máscara:

255.255.255.0



El número de bits del campo que identifica a la subred no tiene porque ser múltiplo de ocho como es el caso del ejemplo anterior. Si se quiere, por ejemplo, que el campo de subred tenga diez bits queda una máscara, siguiendo el ejemplo anterior, igual a 255.255.255.192



Generalmente, cuando se utilizan subredes se reservan al menos tres bits para el **subnetid**. Dos bits dan para cuatro combinaciones de subred posibles, dos de las cuales: 11 y 00 son valores no permitidos.

El **Router Teldat** soporta subredes de distinta longitud en el identificador. Esto permite dividir el **hostid** de un único número de red IP en varias subredes con identificadores de subred de distinto tamaño.

Nota: No pueden utilizarse identificadores de subred de tamaño distinto cuando se utiliza RIP-1. En este caso deberá utilizarse OSPF o configurar RIP-2.

ATENCIÓN: Debe tenerse especial cuidado cuando se utilizan identificadores de subred de tamaño distinto, ya que se pueden producir solapamientos.

1.5. Routing IP

IP utiliza tablas de routing para decidir a donde debe enviarse cada datagrama. Una tabla de routing es una lista con las direcciones de todos los segmentos a los que el router sabe como llegar. Esta tabla contiene rutas estáticas y rutas dinámicas.

Una ruta dinámica es aquella que se aprende por medio de protocolos de routing, como son RIP y OSPF. Estos protocolos actualizan regularmente las tablas de routing reflejando los cambios que puedan darse en la topología de la red. De este modo el routing dinámico permite a los routers enviar los datagramas por caminos alternativos cuando se produce algún fallo en nodos o enlaces.

Una ruta estática es aquella que nunca cambia. Estas rutas se fijan manualmente en la configuración del IP. Las rutas estáticas se mantienen aunque se apague el equipo. Se utilizan cuando el router por alguna razón no puede determinar la ruta correcta dinámicamente.

A continuación se describe el proceso que sigue el router para encaminar un datagrama:

- El protocolo IP recibe el datagrama y lee los 32 bits de la dirección destino.
- Si el datagrama tiene como destino el propio router, este se manda al módulo interno correspondiente. Esto ocurre con los paquetes:
    - De control del propio protocolo IP
    - Paquetes de actualización de rutas
    - Paquetes usados para diagnósticos
- Si el datagrama está dirigido a un ordenador conectado al mismo segmento físico de alguna de las puertas del router, IP busca la dirección física asociada a la dirección IP destino del datagrama y manda el paquete al manejador de nivel inferior correspondiente para que envíe directamente el paquete al destino final. La dirección física asociada a la dirección IP se mantiene en una tabla mediante el protocolo ARP.
- Si el datagrama está dirigido a un ordenador situado en un segmento de red remoto, IP utiliza la tabla de routing para determinar la dirección del siguiente salto. Cada entrada en la tabla de routing contiene una dirección de red destino y la dirección IP del router del siguiente salto. Si el IP encuentra una coincidencia entre la dirección destino del datagrama y la dirección de red destino de una de las entradas de la tabla, el paquete es enviado al manejador de nivel inferior para que lo envíe al siguiente router.
- Si no hay ninguna entrada en la tabla de routing que coincida con la dirección destino del datagrama, éste se manda al router por defecto. El router por defecto es uno de los parámetros que se configuran en el protocolo IP y se utiliza para enviar los datagramas para los que no se encuentra ninguna ruta. Se supone que el router por defecto si tiene la información necesaria para encaminar adecuadamente el datagrama.

El protocolo IP realiza otra serie de tareas principales tales como la eliminación de paquetes defectuosos o diversos tipos de filtrado.

a) Routers por defecto

Un router por defecto es capaz de encaminar adecuadamente datagramas que otros routers no saben como. Hay dos tipos de routers por defecto:

- Router por defecto de red

Encamina el tráfico dirigido a una red destino para la que el resto de los routers no tienen información de routing.

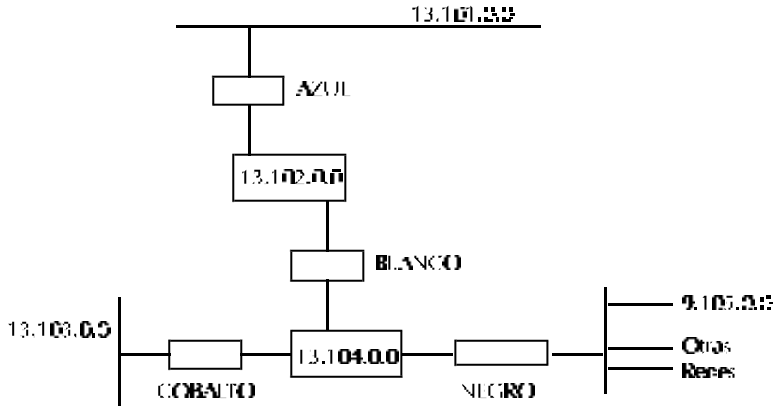
La ruta por defecto de red puede ser configurada manualmente como ruta estática o puede ser aprendida dinámicamente mediante RIP u OSPF. Ambos protocolos representan la ruta por defecto de red como la de destino 0.0.0.0.

- Router por defecto de subred

Encamina el tráfico dirigido a una subred destino para la que otros routers no tienen información de routing específica.

La ruta por defecto de subred puede ser configurada como ruta estática o puede ser aprendida dinámicamente. El destino de una ruta de este tipo es la red que ha sido dividida en subredes y la mascara es la específica de la clase a la que pertenece la red (A, B o C).

En la figura los segmentos de red son 13.101.0.0, 13.102.0.0, 13.103.0.0, 13.104.0.0 y 9.105.0.0. Los routers son AZUL, BLANCO, COBALTO, y NEGRO. En este caso el router por defecto es NEGRO por que es el que tiene datos sobre la red 13 y el resto de las redes. Los routers de la red 13 no tienen dato alguno del resto de redes.



En el segmento de red 13.104 el tráfico destinado a redes desconocidas es enviado al router NEGRO y a partir de este se dirige convenientemente al siguiente salto.

b) Datagramas defectuosos

El router detecta y elimina los datagramas formateados incorrectamente o que tengan una dirección de destino inadecuada evitando que progresen en la red causando cualquier tipo de problemas.

c) Identificador de router (Router ID)

Este parámetro es utilizado como dirección IP origen en distintos tipos de paquetes generados en el propio router. Por ejemplo el identificador de router es utilizado en el protocolo OSPF.

d) Dirección IP interna

Es la dirección del router general cuando no se considera un interfaz particular. Solo se utiliza en condiciones en las que es necesario asegurarse de que el router tiene al menos una dirección disponible.

Si se configura el identificador de router y la dirección IP interna, esta última tiene prioridad. Esto supone que la dirección IP interna pasa a ser el identificador de router en OSPF.

e) Dirección IP de gestión

Es la dirección que utiliza el router para rellenar el campo de dirección de red en las traps SNMP, si no está configurada el router utilizará la dirección IP interna y si esta no está configurada se rellenará a 0.0.0.0.

Los paquetes IP que transportan las traps, en el campo dirección IP origen utilizarán la dirección IP interna y si está configurada la dirección IP de gestión utiliza esta última. Si no estuvieran configuradas ninguna de las dos, se utilizaría la dirección IP de la interfaz de salida del paquete.

f) Paquetes broadcast

Un mensaje broadcast es aquel que tiene como destino a todos los ordenadores dentro de una determinada red. En ocasiones el protocolo IP envía mensajes broadcast por su cuenta. Estos mensajes son utilizados para tareas como actualizar las tablas de routing de otros routers cuando se utiliza RIP-1 o RIP-2 broadcast. El router nunca progresa los paquetes broadcast.

> ***NOTA: El formato de broadcast programado en el router DEBE coincidir con el formato utilizado por los sistemas que están conectados al mismo segmento.***

Para indicar que un paquete es de broadcast (dirigido a todos los sistemas conectados a la red), el router configura como dirección IP destino del datagrama la dirección de broadcast programada. El formato de broadcast puede ser tipo LOCAL-WIRE o tipo NETWORK utilizando como relleno "0" o "1". En un broadcast tipo LOCAL-WIRE todo el campo de dirección IP destino es rellenado con "1" o "0" según esté programado el relleno. Por el contrario en un broadcast tipo NETWORK sólo la parte de host de la dirección IP se inicializa con el patrón de relleno.

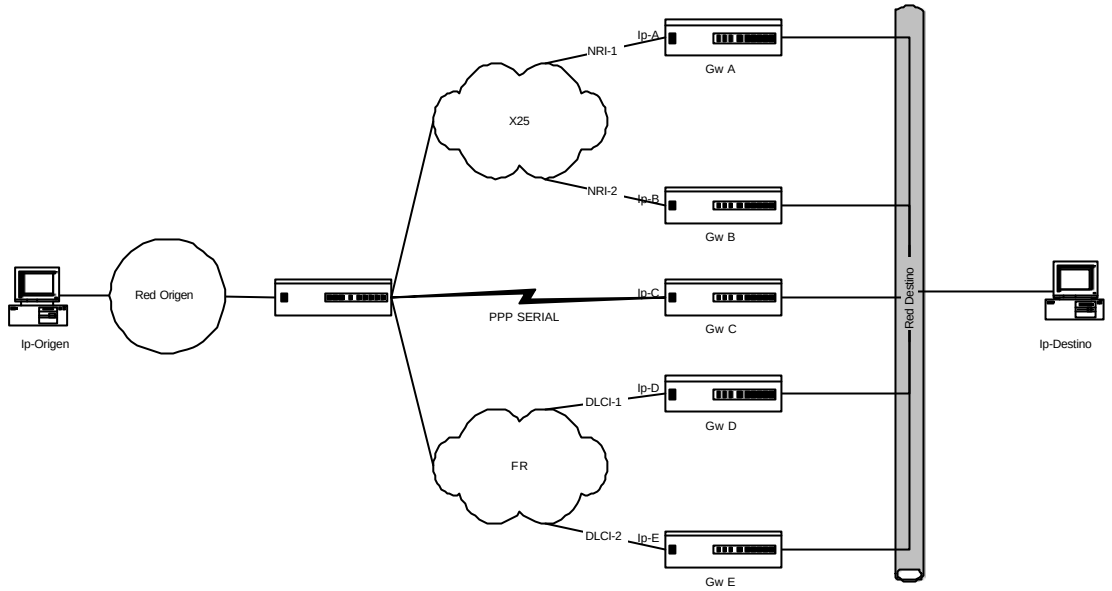
g) Recepción de paquetes broadcast IP

El protocolo IP reconoce todos los tipos de broadcast. Si la parte de red de la dirección indica broadcast segmento local o si dicha parte indica una red directamente conectada al router, el paquete se procesa como si fuera dirigido al propio router.

El protocolo IP progresa los broadcast directos. Un broadcast directo es un broadcast dirigido a una red diferente de la red donde se originó el paquete. Si se habilita la característica de broadcast directo en el router se progresan los paquetes cuya dirección IP destino es un broadcast no local.

h) Multicamino por paquete

En el protocolo IP existe la posibilidad de configurar dos o más rutas hacia una misma red destino a través de siguientes saltos distintos.



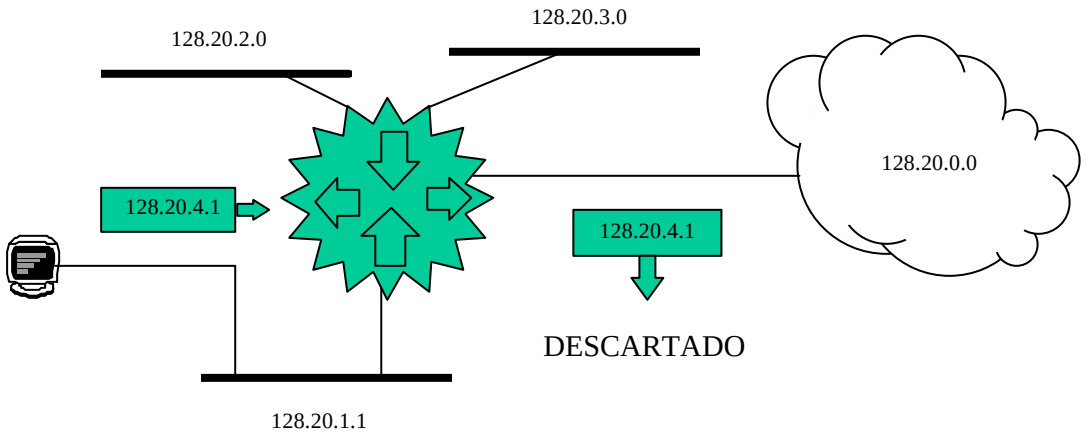
En la figura anterior se puede ver que existe la posibilidad de dirigirse al la dirección IP destino a través de distintos gateways (Gw).

Las rutas pueden ser estáticas o aprendidas mediante un protocolo de encaminamiento dinámico que acepte la posibilidad del multicamino (OSPF).

Si dos o más rutas cumplen que tienen el mismo coste e interfaz de salida activo y además está habilitado "el flag IP de Multicamino por paquete", entonces se realiza balanceo de tráfico (hasta un máximo de 4 caminos). Si no está habilitado el flag no se realiza balanceo.

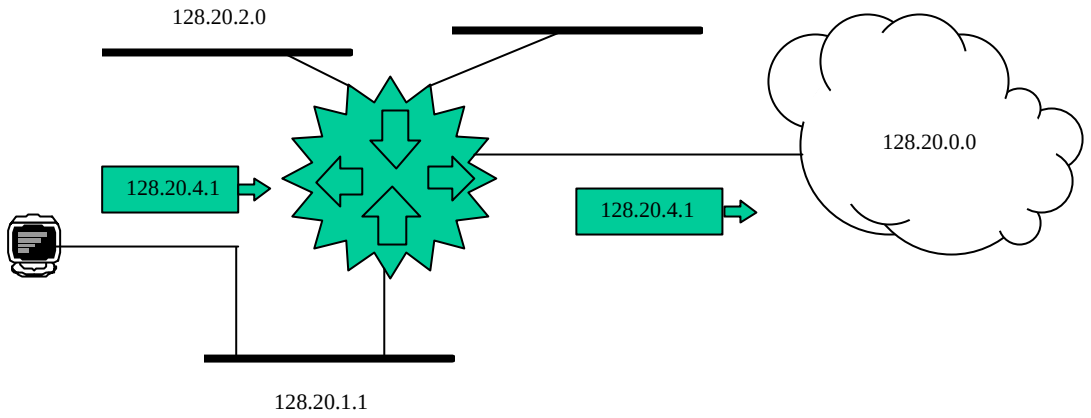
i) IP classless

Puede ocurrir que un router reciba paquetes destinados a una subred de una red de la que no tenga configurado un router por defecto de subred. La figura siguiente muestra un router que pertenece a la red 128.20.0.0 y que está conectado a las subredes 128.20.1.0, 128.20.2.0, y 128.20.3.0. Supóngase que el host envía paquetes hacia 128.20.4.1. Por defecto, si el router recibe paquetes destinados a una subred que no tiene directamente conectada, y además no posee un router por defecto de subred, el router descarta el paquete.



Funcionalidad IP classless deshabilitada

En la siguiente figura, la funcionalidad IP classless está habilitada en el router. Por tanto, cuando el host envía un paquete destinado a la subred 128.20.4.1, en lugar de descartar los paquetes, el router los encamina a la mejor ruta de superred (ruta con mascara menos restrictiva que englobe a la red destino), como última opción el paquete sería enviado a la ruta por defecto de red, en caso de que ésta estuviera configurada (ruta a red 0.0.0.0 que es la superred que engloba a todas las redes).



Funcionalidad IP classless habilitada

j) Controles de acceso

Estos permiten controlar el encaminamiento de paquetes mediante el examen de las direcciones de las máscaras origen y destino del datagrama IP que se encuentran en su cabecera, sobre el tipo de protocolo también indicado en la cabecera o sobre el número de puerto en el caso de que los protocolos utilizados sean TCP o UDP.

Cuando se habilitan los controles de acceso cada paquete que entra en el router se compara con la lista de accesos antes de compararse con la tabla de routing.

Hay dos tipos de entradas en la lista de controles de acceso, inclusiva y exclusiva. Si un paquete coincide con una entrada inclusiva se progresa. Si por el contrario coincide con una entrada exclusiva, se descarta el paquete. Por último, si no hay coincidencia con ninguna de las entradas de la lista de controles de acceso también se descarta el paquete.

Los controles de acceso deben ser utilizados con cautela. Los paquetes originados en el propio router también son sometidos a los controles de acceso. En concreto se debe evitar filtrar los paquetes RIP u OSPF enviados o recibidos. Para ello se puede utilizar una entrada que incluya todo como último elemento de la lista o bien poner una entrada inclusiva explícita.

k) Traslación de direcciones (NAT)

La facilidad NAT (Network Address Translation) permite a la red IP de una empresa aparentar, de cara al resto de redes IP, que está usando un espacio de direccionamiento distinto al que internamente está usando. Por tanto NAT permite a una empresa que usa direcciones privadas (direcciones locales) y que por tanto no son accesibles por tabla de rutas de Internet, conectarse a Internet al convertir dichas direcciones en públicas (direcciones globales) que si son accesibles desde Internet. NAT además permite a las empresas poner en marcha estrategias de redireccionamiento en las que los cambios en las redes IP locales son mínimos. NAT está descrito en la RFC 1631.

El router soporta la facilidad NAT. Para más información ver el manual Dm 720.

1.6. Protocolos de routing interiores

Se llama sistema autónomo al conjunto de routers que utilizan el mismo protocolo de routing. A este protocolo de routing común se le llama protocolo de gateway interior (Interior Gateway Protocol o IGP). Los IGP´s detectan de manera dinámica la accesibilidad de las redes y la información de routing dentro de un sistema autónomo. Con esta información se construyen las tablas de routing.

Los protocolos de routing más extendidos en Internet son RIP y OSPF. Con estos protocolos se asegura la total compatibilidad con el resto de routers del mercado.

El primero (Routing Information Protocol) está basado en el algorítmo de vector de distancia. Su facilidad de manejo y robustez lo hacen idóneo para configuraciones de red sencillas.

El segundo (Open Shortest Path First) está basado en el algorítmo de modificaciones de estado (link state) y es la solución adecuada para redes complejas donde se hacen imprescindibles mayores prestaciones de tiempo de convergencia y aprovechamiento del ancho de banda de las líneas.

El router puede funcionar simultáneamente con RIP y OSPF.

Capítulo 2
Configuración

1. Configuración del Protocolo IP

En este apartado se describen los pasos requeridos para configurar el protocolo IP. Después de configurar las opciones deseadas, se debe guardar la configuración y reinicializar el router para que tenga efecto la nueva configuración. Las siguientes secciones describen el proceso de configuración con más detalle.

- Acceso al entorno de configuración de IP.
- Asignación de direcciones IP a interfaces de red.
- Habilitación del routing dinámico.
- Agregación de información estática de routing.
- Configuración de controles de acceso IP.
- Configuración de NAT.
- Configuración de NAPT.
- Configuración de IPSEC.
- Configuración de Policy Routing.

1.1. Acceso al entorno de Configuración IP

Para acceder al entorno de configuración IP, se deberá introducir el siguiente comando.

```
Config>PROTOCOL IP
IP config>
```

1.2. Asignación de direcciones IP a interfaces de red

El comando **ADDRESS** se debe utilizar para asignar direcciones IP a los interfaces hardware de la red. Los argumentos de este comando incluyen el nombre del interfaz (obtenido con el comando **LIST DEVICES**), la dirección IP así como su máscara asociada.

En el siguiente ejemplo al interfaz de red con nombre ethernet0/0 se le asigna la dirección 128.185.123.22 con la máscara 255.255.255.0 (utilizando el tercer byte para el direccionamiento de subred).

```
IP config>address ethernet0/0 128.185.123.22 255.255.255.0
```

1.3. Habilitación del routing dinámico

Se debe utilizar el siguiente procedimiento para permitir routing dinámico en el router. El router soporta como protocolos de routing interior OSPF y RIP.

Estos protocolos pueden ejecutarse simultáneamente. De cualquier forma, en la mayoría de los casos bastará con que solamente se ejecute uno de los protocolos. Se recomienda el protocolo OSPF por su robustez y las posibilidades que permite.

1.4. Agregación de información estática de routing

Este procedimiento es necesario solamente si no se puede obtener información de routing mediante cualquiera de los protocolos de routing dinámico.

El routing estático permanece aún habiendo fallos de alimentación y es utilizado en rutas que no cambian nunca o que no pueden aprender dinámicamente la información de routing. El routing estático se compone de:

Router por defecto: Los paquetes se encaminan al router por defecto cuando su dirección de destino no puede encontrarse en la tabla de routing.

Subred por defecto: Si se utilizan redes divididas en subredes (subnetted networks) se puede definir un router o router por defecto para cada una de ellas.

Rutas estáticas: Para cada destino que tiene una ruta fija se configura la dirección del siguiente salto y destino.

Rutas de agregación: Cuando existen muchas rutas con destinos que empiezan con la misma numeración puede ser conveniente definir una ruta de agregación: ruta que engloba a todas las anteriores. De esta manera, los protocolos de encaminamiento dinámico, configurados para solo anunciar las rutas de agregación, no inundan las tablas de rutas de los demás routers con información innecesaria. La ruta de agregación no es una ruta propiamente dicha sino una marca que aparece en la tabla de rutas activas que indica que existe una serie de rutas agregadas.

Multicamino: Se pueden configurar rutas a un mismo destino, a través de distintos siguientes saltos, con igual o distinto coste. En caso de que el multicamino esté habilitado además se balanceará tráfico si el coste es el mismo.

a) Routers por defecto

Los routers envían paquetes con direcciones IP desconocidas hacia el router por defecto (por ejemplo, cuando los destinos no figuran en la tabla de routing).

Se configura un router por defecto, indicando el siguiente salto para llegar al mismo y el coste de enviarle paquetes. Se pueden configurar tantos routers por defecto como se deseen, asignándole a cada uno un coste. Se activará aquel que tengan el coste menor y que esté accesible. En caso de que dos o más (hasta un límite de cuatro) estén activos al mismo tiempo, se realizará balanceo de tráfico si la facilidad multicamino está habilitada.

En el ejemplo siguiente el salto hacía el router es 130.1.1.191 y el coste de enviar un paquete al router por defecto es 1.

```
IP config>route 0.0.0.0 0.0.0.0 130.1.1.191 1
```

Tanto el protocolo OSPF, como el RIP, aprenden y anuncian los router por defecto. En el protocolo OSPF, un router puede ser configurado para anunciarse como el router por defecto.

En el protocolo RIP se puede configurar de forma tal que anuncia el router por defecto (si existiese) a sus vecinos.

El protocolo RIP también puede ser configurado de forma tal que si se entera de la existencia de un router por defecto, se suprimirá, si es que se ha realizado, la configuración estática del router por defecto.

b) Router subred por defecto

Puede configurarse un router subred por defecto para todas las subredes pertenecientes a una misma red. Se pueden configurar tantos routers por defecto como se deseen, asignándole a cada uno un coste. Se activará aquel que tengan el coste menor y que esté accesible. En caso de que dos o más (hasta un límite de cuatro) estén activos al mismo tiempo, se realizará balanceo de tráfico si la facilidad multicamino está habilitada. Cuando el router intenta enviar un paquete a una dirección destino correspondiente a una red dividida en subredes (subnetted network), si la dirección destino no puede ser encontrada en la tabla de routing, el paquete será enviado a la puerta del router de subred por defecto.

Configurar routers de subredes por defecto es lo mismo que configurar routers por defecto, la única diferencia es que se debe especificar el identificador de la red dividida en subredes (subnetted network). Por ejemplo, si tenemos configurado un interfaz con una dirección de subred 18.0.0.6 significaría que el router pertenece a la red dividida en subredes (subnetted network) de identificador 18.0.0.0, para configurar un router por defecto de esta red se utiliza el siguiente comando:

```
IP config>route 18.0.0.0 255.0.0.0 130.1.1.191 1
```

El ejemplo anterior especifica que el siguiente salto al router de la subred por defecto es 130.1.1.191 y que el coste del routing del paquete al router por defecto es 1.

c) Red Estática / rutas subred

Configure rutas estáticas para aquellos destinos que no puedan ser descubiertos por protocolos de routing dinámicos. El destino se describe por la dirección de red IP y la máscara de la dirección destino. La ruta destino se programa con la dirección IP de el primer salto a usar y el coste de routing del paquete destino. Se pueden configurar varias rutas estáticas a un mismo destino con distinto siguiente salto, y con igual o distinto coste. En caso de que dos o más rutas (hasta un límite de cuatro) estén activas al mismo tiempo, se realizará balanceo de tráfico si la facilidad multicamino está habilitada. Para crear, borrar rutas estáticas usar los comandos.

```
IP config>route <red o subred o host, mascara, salto, coste>
IP config>no route <direccion-IP-destino, mascara, siguiente salto>
```

Las rutas dinámicas aprendidas por protocolos RIP y/o OSPF pueden sobrescribir las rutas estáticas. Para el protocolo RIP, se puede deshabilitar este comportamiento de sobrescritura de las rutas estáticas.

d) Rutas de agregación

Para crear y borrar rutas de agregación usar los siguientes comandos.

```
IP config>aggregation-route <red o subred o host, mascara >
IP config>no aggregation-route <direccion-IP-destino, mascara >
```

e) Multicamino

Se puede configurar multicamino por paquete o por origen-destino.

Para conseguir configurar el multicamino por paquete realizar los siguientes pasos:

- Se añade una ruta estática por cada camino. Se le asigna un coste determinado.
- Habilitar o deshabilitar el flag IP de "Multicamino por paquete".

```
IP config>MULTIPATH PER-PACKET
```

ó

```
IP config>NO MULTIPATH
```

- Se configura o no el parámetro de BKUP-RCV-TIME de variables globales de Nodo X25. (Ver manual de X25 Dm 707)

Caso interfaz de salida genérico

- La ruta estática con menor coste e interfaz activo es la que entra en funcionamiento.
- Si dos o más rutas cumplen que tienen el mínimo coste e interfaz de salida activo y además está habilitado "el flag IP de Multicamino por paquete", entonces se realiza balanceo de tráfico (hasta un máximo de 4 caminos). Si no está habilitado el flag no se realiza balanceo.
- Si se cae un interfaz o se activa se vuelven a revisar las rutas estáticas para que entre en funcionamiento la de menor coste con interfaz activo.
- Ver casos particulares de FR (dlci), X25 (rutas por NRI) e interfaces Dial.

Caso interfaz de salida FR

- Las rutas estáticas que tengan como interfaz de salida uno de tipo FR se activan siempre que cumplan que son las de menor coste, que el interfaz está activo y que el dlci al que está asociado el siguiente salto está activo. La actividad o inactividad de dlci depende del LMI.
- Se desactivan si no se cumple alguna de las anteriores condiciones.

Caso interfaz de salida X25

Las rutas estáticas que tengan como interfaz de salida a X25 se activan siempre que cumplan que son las de menor coste, que el interfaz está activo y que el NRI al que está asociado el siguiente salto esté activo. La actividad o inactividad de un NRI depende de los siguientes puntos.

- Si el parámetro BKUP-RCV-TIME tiene el valor 0, los NRI siempre están activos con lo que las rutas estáticas asociadas al mismo si son las de menor coste siempre estarán activas.
- Si el parámetro BKUP-RCV-TIME tiene el valor distinto de 0:
    1. Al arrancar el router todos los NRI están activos.
    2. Si un paquete va dirigido al siguiente salto entonces provocará una llamada.
    3. Si la llamada se establece se activa el NRI. (ir a 2).
    4. Si la llamada no se establece se desactiva el NRI (con lo que la ruta o rutas estáticas asociadas al mismo se desactivan) y se inicia el proceso de reintento de llamada cada BKUP-RCV-TIME.
    5. Si la llamada se establece se reactiva el NRI y con él todas las rutas estáticas asociadas al mismo. (ir a 2).

IMPORTANTE: Si se configura el parámetro BKUP-RCV-TIME con un valor distinto de 0 es posible que en algún momento se realicen llamadas extras de X25 provocadas por el "Proceso de Reintento de Establecer Llamada". Esto puede ser un inconveniente para el caso de tener contratada una Tarifa no Plana. Si se configura a 0 se impide el reintento de llamada con lo que las rutas estáticas configuradas por X25 siempre estarían activas.

Caso interfaz de salida Dial-PPP y Dial-FR

Las rutas estáticas que tengan como interfaz de salida un "Dial" se activan siempre que se cumplan las dos condiciones siguientes: que sean las de menor coste y que el interfaz esté activo. Un interfaz de este tipo siempre está activo con lo que las rutas estáticas asociadas al mismo siempre se activarán si son las de menor coste configurado.

f) IP Classless

Estrategias de encaminamiento:

- Class routing strategy: supóngase un router directamente conectado a una subred (10.1.1.0) de la red 10.0.0.0. Si el router recibe paquetes destinados a otra subred (10.2.1.0) de la misma red, de la que no dispone información, aún teniendo ruta por defecto de red (0.0.0.0/0) configurada, si no tiene una ruta por defecto de subred configurada (10.0.0.0/8), el paquete no será progresado. Es un comportamiento preventivo para proteger posibles bucles.
- Classless routing strategy: todo paquete recibido es encaminado hacia el siguiente salto que indique la ruta que contenga el destino, que sea más restrictiva (más 1's en la máscara) y tenga menor coste.

Si no está habilitado "IP Classless routing", el router se basa en una estrategia de encaminamiento dependiente de la clase "class routing strategy".

Es una funcionalidad que debe evitarse siempre que sea viable, con el fin de proteger la red de bucles. Siempre se ha de intentar una solución alternativa que sería:

- No IP classless.
- Agregar tantas rutas por defecto de subred como redes divididas en subredes existan.

Por defecto es una funcionalidad que está deshabilitada, para poder habilitarla o deshabilitarla basta con ejecutar el siguiente comando:

```
IP config>CLASSLESS
```

ó

```
IP config>NO CLASSLESS
```

1.5. Configuración de Controles de acceso IP

Los controles de acceso IP permiten configurar filtros de paquetes basados en dirección IP origen y destino, número protocolo de IP y rangos de puertos origen y destino para los protocolos TCP y UDP. Esta funcionalidad puede controlar el acceso a determinadas clases de direcciones IP y servicios, así como restringir el tipo de tráfico permitido según el interfaz de entrada/salida.

Existen dos tipos de controles de acceso diferenciados:

- Controles de acceso GLOBALES.
- Controles de acceso POR INTERFAZ.

a) Controles de acceso IP globales

Los controles de acceso IP **globales** se basan en una lista ordenada global de controles de acceso exclusivos o inclusivos. Si el control de acceso es habilitado, cada paquete IP originado, traspasado o recibido es inspeccionado por la lista de control de acceso. Cada entrada de esta lista puede ser

inclusiva o exclusiva, permitiendo o denegando el paso. Cada entrada tiene campos de dirección IP origen y destino, el numero de protocolo IP opcional, y el rango de puertos origen y destino (opcional para protocolos UDP y TCP).

Para cada paquete recibido, se comparan todos los campos de la cabecera del paquete con todos los campos especificados de cada registro de la lista anterior. Si el registro coincide con el paquete y si además el registro de la lista es inclusivo, el paquete es traspasado. Si el campo de la lista es exclusivo el paquete no será traspasado. Finalmente si los registros no coinciden con la cabecera los paquetes son rechazados.

Cada registro tiene una dirección IP máscara, y el par resultante de una operación lógica entre las direcciones origen y destino. Para cada dirección se realiza una "Y-Lógica" (función AND) con la mascara y comparada con el resultado. Por ejemplo una máscara de 255.0.0.0 con un resultado de 26.0.0.0 coincidirá con cualquier dirección que tenga 26 en el primer byte. Una máscara de 255.255.255.255 con un resultado de 192.66.66.20 coincidirá solo con la dirección IP 192.66.66.20. Una máscara de 0.0.0.0 con un resultado de 0.0.0.0 es un comodín y por tanto coincide con cualquier dirección.

Cada registro puede también tener un rango numérico del protocolo IP. El byte de protocolo de la cabecera IP será inspeccionado para ver si está en este rango. Cualquier paquete IP con un valor de protocolo entre 0 y 255 dejará pasar cualquier paquete IP. Los números de protocolo más usados son:

1 para ICMP, 6 para TCP, 8 para EGP, 17 para UDP, y 89 para OSPF.

Cada registro puede también tener un rango de puertos tanto origen como destino. Esto sólo es válido para paquetes TCP y UDP, ya que los números de puerto son parte de las cabeceras de estos protocolos. Cualquier paquete TCP o UDP con un número de puerto, dentro de los rangos programados será traspasado. Un rango entre 0 y 65535 deshabilita el filtrado de número de puertos puesto que pasan todas. Algunos números de puertos usados frecuentemente son: 21 para FTP, 23 para TELNET, 25 para SMTP, 513 para rlogin, 520 para RIP, y 6000 para X. Ver la recomendación RFC 1060 "Números asignados", para los detalles de los números de puertos y de los protocolos IP.

El ejemplo siguiente permite a cualquier Host el envío de paquetes al SMTP TCP Socket a la dirección IP 192.67.67.20

```
IP config>access-control entry 1 default
IP config>access-control entry 1 inclusive
IP config>access-control entry 1 protocol-range 6 6
IP config>access-control entry 1 source network 0.0.0.0 0.0.0.0
IP config>access-control entry 1 destination network 192.67.67.20 255.255.255.255
IP config>access-control entry 1 destination port-range 25 25
```

El siguiente ejemplo evita que cualquier host de la subred 150.150.1.X envíe paquetes a ordenadores de la subred 150.150.2.X.

```
IP config>access-control entry 1 default
IP config>access-control entry 1 source network 150.150.1.0 255.255.255.0
IP config>access-control entry 1 destination network 150.150.2.0 255.255.255.0
```

Este comando permite el envío o recepción de todos los paquetes RIP.

```
IP config>access-control entry 1 default
IP config>access-control entry 1 inclusive
IP config>access-control entry 1 protocol-range 17 17
IP config>access-control entry 1 source network 0.0.0.0 0.0.0.0
IP config>access-control entry 1 destination network 0.0.0.0 0.0.0.0
```

El siguiente comando permite el envío o recepción de cualquier paquete OSPF.

```
IP config>access-control entry 1 default
IP config>access-control entry 1 inclusive
IP config>access-control entry 1 protocol-range 89 89
IP config>access-control entry 1 source network 0.0.0.0 0.0.0.0
IP config>access-control entry 1 destination network 0.0.0.0 0.0.0.0
```

No hay que olvidarse de agregar como última entrada la entrada comodín ya que cualquier paquete que no coincida con ninguna entrada será descartado/filtrado: si se habilita el control de acceso IP y sólo se quiere filtrar un determinado tipo de tráfico es necesario agregar el conjunto de entradas exclusivas necesarias para filtrar dicho tipo de tráfico y añadir una entrada inclusiva comodín como útlima entrada para permitir el resto de tráfico.

```
IP config>access-control entry 2 default
IP config>access-control entry 2 inclusive
IP config>access-control entry 2 source network 0.0.0.0 0.0.0.0
IP config>access-control entry 2 destination network 0.0.0.0 0.0.0.0
```

Si se tienen algunas redes o subredes IP por las que no se quiere que los paquetes progresen, o no distribuyan información de routing acerca de ellas; es mejor especificarlas como filtros (esto es más eficiente que el mecanismo de control de acceso). Para añadir un filtro de red hay que utilizar el siguiente comando:

```
IP config>filter <direccion-IP-destino, mascara-IP-destino>
```

Es recomendable filtrar el tráfico local de una red del tipo 127.0.0.0 para no propagar paquetes destinados sólo a esta red. Usar el siguiente comando:

```
IP config>filter  127.0.0.0  255.0.0.0
```

b) Controles de acceso IP por interfaz

Los controles de acceso IP **por interfaz** se basan en la utilización de listas de control de acceso genéricas. Para cada interfaz se pueden definir dos listas de acceso diferentes: una para filtrar el tráfico entrante y otra para filtrar el tráfico saliente, de modo que en cada interfaz se puede restringir el tráfico que envía y recibe. Si no se define ninguna lista de control de acceso entonces el interfaz dejará pasar todos los paquetes. Si la lista de acceso (entrante o saliente) permite el paquete, se continúa con su procesado (en tráfico entrante) o se envía por el interfaz (en tráfico saliente), mientras que si se rechaza el paquete, éste se descarta y además se envía un mensaje ICMP Host Unreachable.

Si se prevé que se va a producir una gran cantidad de paquetes descartados debido a los controles de acceso por interfaz, es recomendable deshabilitar el envío de mensajes ICMP Unreachables para evitar la carga que supone en el equipo.

Se pueden asociar a los interfaces listas de control de acceso "Estándar" o "Extendidas". En el caso de listas *Estándar* se comprueban exclusivamente las direcciones origen de los paquetes. En las listas *Extendidas* se comprueban direcciones origen y destino de los paquetes, protocolos, puertos, etc (permiten una especificación más detallada del tráfico que se permite o prohíbe).

El ejemplo siguiente muestra cómo aplicar la lista de control de acceso extendida 101 (suponiendo que previamente se encuentra definida) a los paquetes entrantes en el interfaz ethernet0/0:

```
IP config>access-group ethernet0/0 101 in
```

Para restringir el tráfico saliente del interfaz ppp1 según la lista de acceso estándar 10:

```
IP config>access-group ppp1 10 out
```

1.6. Configuración de NAT

Para más información acerca de este tema consultar el manual de NAT Dm 720.

1.7. Configuración de NAPT

Para más información acerca de este tema consultar el manual de NAPT Dm 735.

1.8. Configuración de IPSEC

Para más información acerca de este tema consultar el manual de IPSEC Dm 739.

1.9. Configuración de Policy Routing

Para más información acerca de este tema consultar el manual de Policy Routing Dm 745.

Capítulo 3
Comandos de Configuración

1. Comandos de Configuración del Protocolo IP

Esta sección resume y explica todos los comandos de configuración del router. Estos comandos le permitirán configurar el comportamiento de los protocolos IP del router, y poder de esta forma llegar a las especificaciones de funcionamiento deseadas.

Introducir los comandos de configuración IP cuando se tenga el prompt IP config>, para acceder a este prompt se debe teclear lo siguiente:

```
*P 4
User Configuration
Config>PROTOCOL IP
Internet protocol user configuration
IP config>
```

Comando	Función
? (AYUDA)	Lista comandos u opciones.
ACCESS-CONTROL	Configura entradas en la lista de controles de acceso GLOBALES.
ACCESS-GROUP	Configura los controles de acceso POR INTERFAZ.
ADDRESS	Configura direcciones IP en los interfaces.
AGGREGATION-ROUTE	Configura información de agregación.
BROADCAST-ADDRESS	Especifica el formato de las direcciones de broadcast que usa el router para un determinado interfaz.
CLASSLESS	Habilita la estrategia de enrutamiento IP "Classless Routing Strategy".
DIRECTED-BROADCAST	Habilita el progreso de paquetes IP con destino una dirección de broadcast de red no local.
DNS-DOMAIN-NAME	Configura el nombre del dominio DNS.
FILTER	Configura filtros IP.
ICMP-REDIRECTS	Habilita el envío de paquetes icmp redirects.
ICMP-UNREACHABLES	Habilita el envío de paquetes icmp unreachables.
INTERNAL-IP-ADDRESS	Configura la dirección IP interna del router.
IP-PARAM	Configura otros parámetros IP.
IPSEC	Entra en los menús de configuración de IPSEC.
LIST	Lista la configuración de los elementos IP.
LOCAL	Configura funcionalidades asociadas al tráfico local.
MANAGEMENT-IP-ADDRESS	Configura la dirección IP de gestión del router.
MULTIPATH	Habilita el multicamino.
NAT	Entra en los menús de configuración de la facilidad NAT.
NO	Borra un parámetro de la configuración IP previamente añadido o reestablece su valor por defecto.
POLICY	Habilita el Policy Routing en un interfaz.
POOL	Configura el rango de direcciones que el router puede asignar a través de sus conexiones PPP.
PROXY-ARP	Entra en los menús de configuración del Proxy ARP.
ROUTE	Configura rutas IP.

ROUTER-ID	Configura la dirección IP por defecto que el router utilizará en los paquetes localmente originados. Además pasará a ser l router-ID del protocolo OSPF.
RULE	Configura conexiones IP.
TVRP	Entra en los menús de configuración del protocolo TVRP.
EXIT	Sale de la configuración IP.

1.1. ? (AYUDA)

Utilizar el comando **?** (AYUDA) para listar los comandos válidos en el nivel donde se está programando el router. Se puede también utilizar este comando después de un comando específico para listar las opciones disponibles.

Sintaxis:

```
IP config>?
```

Ejemplo:

```
IP config>?
ACCESS-CONTROL              Configures global access control system
ACCESS-GROUP                Specifies per-interface access control system
ADDRESS                     Assigns an ip address to one network interfaces
AGGREGATION-ROUTE           Configures ip aggregation information
BROADCAST-ADDRESS           Sets the ip broadcast format for an interface
CLASSLESS                   Enables ip classless routing strategy
DIRECTED-BROADCAST          Enables directed broadcast
DNS-DOMAIN-NAME             Establishes the dns domain name
FILTER                      Designates an ip network/subnet to be filtered
ICMP-REDIRECTS              Enables sending icmp redirects
ICMP-UNREACHABLES           Enables sending icmp unreachables
INTERNAL-IP-ADDRESS         Sets the internal ip address
IP-PARAM                    Sets other ip parameters
IPSEC                       Enters in the ipsec configuration menus
LIST                        Lists ip configuration elements
LOCAL                       Local (not forwarded) traffic settings
MANAGEMENT-IP-ADDRESS       Sets the management ip address
MULTIPATH                   Enables multipath routing
NAT                         Enters in the nat configuration menus
NO                          Negates a command or sets its defaults
POLICY                      Enable policy routing on an interface
POOL                        Sets the range of addresses for ppp assignments
PROXY-ARP                   Enters in the proxy arp configuration menus
ROUTE                       Configures a static network/subnet ip route
ROUTER-ID                   Sets the router id
RULE                        Configures an ip connection rule
TVRP                        Enters in the tvrp configuration menus
EXIT
```

1.2. ACCESS-CONTROL

Mediante este comando se configura el sistema de control de acceso GLOBAL del protocolo IP.

Sintaxis:

```
IP config>ACCESS-CONTROL ?
ENABLED      Enables access control system
ENTRY        Configures an access control entry
MOVE         Moves an access control entry
```

a) ACCESS-CONTROL ENABLED

Habilita el sistema de control de acceso. Por defecto el sistema de control de acceso del protocolo IP está deshabilitado.

Sintaxis:

```
IP config>ACCESS-CONTROL ENABLED
```

Ejemplo:

```
IP config>ACCESS-CONTROL ENABLED
IP config>
```

Para deshabilitarlo hay que ejecutar el mismo comando precedido por "NO".

```
IP config>NO ACCESS-CONTROL ENABLED
IP config>
```

b) ACCESS-CONTROL ENTRY

Configura una entrada en la lista de controles de acceso. Permite especificar la clase de paquetes que hay que hacer progresar o descartar según el tipo de entrada. El tamaño y el orden de la lista de control de acceso IP puede afectar al rendimiento de la progresión IP.

Cada entrada contiene los siguientes campos: tipo, IP origen, Máscara IP origen, IP destino, Máscara IP destino. El tipo puede ser inclusivo o exclusivo. Las direcciones IP origen y destino se introducen con el formato decimal separado por puntos. Opcionalmente se puede especificar un rango de protocolos IP, y se puede indicar un rango de puertos TCP y UDP tanto en origen como en destino.

Sintaxis:

```
IP config>ACCESS-CONTROL ENTRY <id>
default              create a new access control
destination          destination ip network and port range
       network          destination ip network to match
       port-range       destination udp/tcp port range
exclusive            drop the packets that match this access control
inclusive            bypass the packets that match this access control
protocol-range       protocol range
source               source ip network and port range
       network          source ip network to match
       port-range       source udp/tcp port range
```

Default: Crea una entrada en la lista de controles de acceso con identificador <id> y los valores por defecto. Si ya existe pone por defecto sus valores.

Destination: Configura la red ip y el rango de puertos destino de la entrada con identificador <id>.

Exclusive: Cambia a modo exclusivo la entrada con identificador <id>.

Inclusive: Cambia a modo inclusivo la entrada con identificador <id>.

Protocol-range: Configura el rango de protocolos de la entrada con identificador <id>.

Source: Configura la red ip y el rango de puertos origen de la entrada con identificador <id>.

Ejemplo:

```
IP config>access-control entry 1 default
IP config>access-control entry 1 inclusive
IP config>access-control entry 1 protocol-range 6 6
IP config>access-control entry 1 source network 150.150.1.0 255.255.255.0
IP config>access-control entry 1 destination network 150.150.2.0 255.255.255.0
IP config>access-control entry 1 source port-range 1 100
IP config>access-control entry 1 destination port-range 200 300
IP config>
```

Para borrar una entrada ejecutar el mismo comando precedido por "NO".

```
IP config>no access-control entry 1
IP config>
```

c) ACCESS-CONTROL MOVE

Utilizar el comando **ACCESS-CONTROL MOVE** para cambiar el orden de la lista de control de acceso. Este comando desplaza el registro *desde#* inmediatamente después de *hasta#.* Después de mover el registro, estos se vuelven a numerar automáticamente.

Sintaxis:

```
IP config>ACCESS-CONTROL MOVE <desde# hasta#>
```

Ejemplo:

```
IP config>access-control move 2 0
About to move:
                                          Beg End  Beg   End   Beg  End
 Type             Source         Destination Pro Pro  SPrt  SPrt  DPrt DPrt
----- ------------------  ------------------ --- --- ----- ----- ----- -----
  2 E         2.2.2.2/32          0.0.0.0/32   0 255     0 65535     0 65535
to be the first element in the list
Are you sure this is what you want to do(Yes/No)? y
IP config>
```

1.3. ACCESS-GROUP

Mediante este comando se configura el sistema de control de acceso POR INTERFAZ del protocolo IP.

Sintaxis:

```
IP config>ACCESS-GROUP <interfaz> <lista de acceso>
in     inbound packets
out    outbound packets
```

In: Aplica la lista de control de acceso genérica al tráfico entrante del interfaz especificado.

Out: Aplica la lista de control de acceso genérica al tráfico saliente del interfaz especificado.

Ejemplo:

```
IP config>access-group ethernet0/0 101 in
IP config>access-group ethernet0/0 102 out
IP config>access-group ppp1 103 out
IP config>
```

Para eliminar un control de acceso por interfaz se emplea el mismo comando precedido por la partícula “NO”.

Ejemplo:

```
IP config>no access-group ethernet0/0 101 in
IP config>
```

1.4. ADDRESS

Asigna una dirección IP a uno de los interfaces del router. Un interfaz hardware no recibirá o transmitirá paquetes hasta tener al menos una dirección IP.

Para ello se debe especificar una dirección IP conjuntamente con su máscara de subred. Por ejemplo si la dirección es una red de clase B, usando el tercer byte para la subred, la máscara podría ser 255.255.255.0. Se puede usar el comando **LIST DEVICES** para obtener los nombres de cada interfaz.

Sintaxis:

```
IP config>ADDRESS <interfaz, direccion-IP, mascara-IP>
```

Ejemplo:

```
IP config>address ethernet0/0  128.185.123.22  255.255.255.0
IP config>
```

Para borrar una dirección se usa el mismo comando precedido por la partícula “NO”.

```
IP config>no address ethernet0/0  128.185.123.22  255.255.255.0
IP config>
```

Un interfaz de tipo punto a punto puede ser configurado como no numerado utilizando este comando. Para ello se debe introducir “unnumbered” en vez de la dirección-IP y la mascara-IP

Sintaxis:

```
IP config>ADDRESS <interfaz> unnumbered
```

Ejemplo:

```
IP config>address atm1/0.1 unnumbered
IP config>
```

Para borrar una dirección se usa el mismo comando precedido por la partícula “NO”.

```
IP config>no address atm1/0.1 unnumbered
IP config>
```

1.5. AGGREGATION-ROUTE

Añade información de agregación IP a la tabla de encaminamiento.

La ruta de agregación se especifica mediante una dirección IP (Red, Subred, Host) y una máscara.

Sintaxis:

```
IP config>AGGREGATION-ROUTE <red o subred o host, mascara>
```

Ejemplo:

```
IP config>aggregation-route 128.0.0.0  255.0.0.0
IP config>
```

Para borrar una ruta de agregación se usa el mismo comando precedido por la partícula “NO”.

```
IP config>no aggregation-route 128.0.0.0  255.0.0.0
IP config>
```

1.6. BROADCAST-ADDRESS

Especifica el formato de las direcciones de broadcast que usa el router para un determinado interfaz. Los paquetes IP de broadcast se utilizan principalmente cuando el router envía paquetes RIP de actualización de tablas.

El *tipo de direccion (style address)* puede ser NETWORK o LOCAL-WIRE. Las direcciones de broadcast del tipo LOCAL-WIRE son o todo unos, (255.255.255.255) o todo ceros (0.0.0.0). Las direcciones del tipo NETWORK empiezan por el número de red y subred del interfaz.

El *patron para broadcast (Fill pattern for wildcard part)* puede ser 0 ó 1. Esto indica como se debe rellenar el resto de la dirección de broadcast (excepto red y subred) con unos o ceros.

Por defecto el tipo de dirección es NETWORK y el relleno es 0.

En recepción el router reconoce todos los formatos de direcciones de broadcast.

Sintaxis:

```
IP config>BROADCAST-ADDRESS ?
LOCAL-WIRE      Sets local-wire broadcast style address
NETWORK         Sets network broadcast style address
```

a) BROADCAST-ADDRESS LOCAL-WIRE

Mediante este comando se configura el *tipo de direccion (style address)* como LOCAL-WIRE. Las direcciones de broadcast del tipo LOCAL-WIRE son o todo unos, (255.255.255.255) o todo ceros (0.0.0.0). El patrón para broadcast puede ser 0 ó 1.

Sintaxis:

```
IP config>BROADCAST-ADDRESS local-wire <address, relleno>
```

El siguiente ejemplo configura una dirección de broadcast 255.255.255.255.

Ejemplo:

```
IP config>broadcast-adress local-wire 192.7.1.254 0
IP config>
```

Para volver a la configuración por defecto del comando se ejecuta el mismo comando precedido por "NO".

```
IP config>no broadcast-adress local-wire 192.7.1.254 0
IP config>
```

b) BROADCAST-ADDRESS NETWORK

Mediante este comando se configura el *tipo de direccion (style address)* como NETWORK. Las direcciones del tipo NETWORK empiezan por el número de red y subred del interfaz. El *patron para broadcast (Fill pattern for wildcard part)* puede ser 0 ó 1. Esto indica como se debe rellenar el resto de la dirección de broadcast (excepto red y subred) con unos o ceros.

Sintaxis:

```
IP config>BROADCAST-ADDRESS NETWORK <address, relleno>
```

El siguiente ejemplo configura una dirección de broadcast 192.7.1.255

Ejemplo:

```
IP config>broadcast-adress network 192.7.1.254 1
IP config>
```

Para volver a la configuración por defecto del comando se ejecuta el mismo comando precedido por "NO".

```
IP config>no broadcast-adress network 192.7.1.254 0
IP config>
```

1.7. CLASSLESS

Habilita la estrategia de enrutamiento IP "Classless Routing Strategy".

Sintaxis:

```
IP config>CLASSLESS
```

Ejemplo:

```
IP config>classless
IP config>
```

Para deshabilitarlo se usa el mismo comando precedido por la partícula "NO".

```
IP config>no classless
IP config>
```

1.8. DIRECTED-BROADCAST

Habilita el progreso de aquellos paquetes IP cuyo destino es una dirección broadcast de red no local (por ejemplo: una LAN remota). El paquete se origina en el host como "unicast", siendo enviado como "unicast" a la subred destino y convertido a broadcast.

Esta clase de paquetes se utiliza para localizar servidores en redes remotas. Los paquetes IP nunca se encaminan hacia niveles de enlace broadcast o multicast a no ser que correspondan a direcciones IP clase D. Este comando por defecto está habilitado.

Sintaxis:

```
IP config>DIRECTED-BROADCAST
```

Ejemplo:

```
IP config>directed-broadcast
IP config>
```

Para deshabilitarlo se usa el mismo comando precedido por la partícula "NO".

```
IP config>no directed-broadcast
IP config>
```

1.9. DNS-DOMAIN-NAME

Establece el nombre de dominio.

Sintaxis:

```
IP config>DNS-DOMAIN-NAME <nombre-dominio>
```

Ejemplo:

```
IP config>dns-domain-name teldat.es
Domain name : teldat.es
Domain Name configured.
IP config>
```

Para borrarlo se usa el mismo commando precedido por la partícula "NO".

```
IP config>no dns-domain-name
IP config>
```

1.10. FILTER

Designa un filtro para una red o subred IP. Un paquete IP que cumple las condiciones de filtrado no será encaminado y simplemente será rechazado.

Para filtrar un paquete IP se debe especificar el filtro de red conjuntamente con la máscara de subred. Por ejemplo para filtrar una subred de una red clase B, usando el tercer byte para la subred, la máscara podría ser 255.255.255.0.

Es importante saber que los mecanismos de filtrado son más eficientes que los mecanismos de control de acceso aunque no tan flexibles como éstos últimos.

Sintaxis:

```
IP config>FILTER <direccion-IP-destino, mascara-IP-destino>
```

Ejemplo:

```
IP config>filter 127.0.0.0  255.0.0.0
IP config>
```

Para borrar un filtro se usa el mismo comando precedido por la partícula "NO".

```
IP config>no filter 127.0.0.0  255.0.0.0
IP config>
```

1.11. ICMP-REDIRECTS

Habilita el envío de paquetes ICMP redirects. Por defecto está habilitado.

Sintaxis:

```
IP config>ICMP-REDIRECTS
```

Ejemplo:

```
IP config>icmp-redirects
IP config>
```

Para deshabilitarlo se usa el mismo comando precedido por la partícula "NO".

```
IP config>no icmp-redirects
IP config>
```

1.12. ICMP-UNREACHABLES

Habilita el envío de paquetes ICMP Unreachables. Por defecto se encuentra habilitado.

Sintaxis:

```
IP config>ICMP-UNREACHABLES
```

Ejemplo:

```
IP config>icmp-unreachables
IP config>
```

Para deshabilitarlo se usa el mismo comando precedido por la partícula "NO".

```
IP config>no icmp-unreachables
IP config>
```

1.13. INTERNAL-IP-ADDRESS

Establece la dirección IP interna del router como un solo equipo, no la asociada a un interfaz. Esta dirección siempre es accesible independientemente del estado del interfaz. Cuando se configura en un mismo router la dirección IP interna y el router-ID, la dirección IP interna tiene preferencia frente al router-ID.

Sintaxis:

```
IP config>INTERNAL-IP-ADDRESS <address>
```

Ejemplo:

```
IP config>internal-ip-address 192.7.1.254
IP config>
```

Para borrar la dirección ip interna se usa el mismo comando precedido por la partícula "NO".

```
IP config>no internal-ip-address
IP config>
```

1.14. IP-PARAM

Usar el comando **IP-PARAM** para configurar distintos parámetros del protocolo IP en función de la opción seleccionada.

Sintaxis:

```
IP config>IP-PARAM ?
CACHE-SIZE              Sets the maximum number entries for the IP routing cache
REASSEMBLY-SIZE         Sets the maximum size of reassembly buffers
ROUTING-TABLE-SIZE      Sets the maximum size of the IP routing table
IP config>
```

a) IP-PARAM CACHE-SIZE

Configura el número máximo de entradas en el cache de routing IP.

Sintaxis:

```
IP config>IP-PARAM CACHE-SIZE <#>
```

Ejemplo:

```
IP config>ip-param cache-size 120
IP config>
```

El valor por defecto es 64. Para volver al valor por defecto ejecutar el mismo comando precedido por la partícula "NO"

```
IP config>no ip-param cache-size
IP config>
```

b) IP-PARAM REASSEMBLY-SIZE

Configura el tamaño de los buffers que son utilizados para reensamblar los paquetes IP fragmentados. El valor por defecto es 12.000.

Sintaxis:

```
IP config>IP-PARAM REASSEMBLY-SIZE <#>
```

Ejemplo:

```
IP config>ip-param reassembly-size 13000
IP config>
```

Para volver al valor por defecto ejecutar el mismo comando precedido por la partícula "NO".

```
IP config>no ip-param reassembly-size
IP config>
```

c) IP-PARAM ROUTING-TABLE-SIZE

Establece el tamaño de la tabla de routing IP. El valor por defecto es 768 entradas. Si se configura menor se puede llegar a descartar la información dinámica de routing. Si se configura demasiado grande podemos estar desaprovechando la memoria del router.

Sintaxis:

```
IP config>IP-PARAM ROUTING-TABLE-SIZE <#>
```

Ejemplo:

```
IP config>ip-param routing-table-size 2000
IP config>
```

Para volver al valor por defecto ejecutar el mismo comando precedido por la partícula "NO"

```
IP config>no ip-param routing-table-size
IP config>
```

1.15. IPSEC

Mediante este comando se llega a los menús de configuración de IPSEC. Ver el manual de IPSEC Dm 739.

Sintaxis:

```
IP config>IPSEC
```

Ejemplo:

```
IP config>ipsec
IPsec user configuration
IPSec config>
```

1.16. LIST

Utilizar el comando **LIST** para visualizar distintos parámetros de la configuración IP en función de la opción seleccionada.

Sintaxis:

```
IP config>LIST ?
ACCESS-CONTROLS
ACCESS-GROUP
ADDRESSES
ALL
DNS-DOMAIN-NAME
IP-PARAM
IP-PROTOCOL
POLICY
POOL
ROUTES
RULE
```

a) LIST ACCESS-CONTROLS

Muestra el modo de control de acceso configurado (inclusivo, exclusivo, o deshabilitado), así como la lista de registros de control de acceso GLOBALES configurados. Cada registro lleva asociado un número de registro. Este número se utiliza para reordenar la lista con el comando **ACCESS-CONTROL MOVE**.

Sintaxis:

```
IP config>LIST ACCESS-CONTROLS
```

Ejemplo:

```
IP config>list access-controls
Access Control is: disabled
List of access control records:
                                          Beg End  Beg   End   Beg  End
 Type             Source         Destination Pro Pro  SPrt  SPrt  DPrt DPrt
----- ----------------- ----------------- --- --- ----- ----- ----- -----
  1 E         0.0.0.0/0       192.6.1.250/32   6   6    23    23    23    23
  2 I         0.0.0.0/0           0.0.0.0/0    0 255     0 65535     0 65535
IP config>
```

b) LIST ACCESS-GROUP

Muestra los controles de acceso POR INTERFAZ. Para cada interfaz se muestran las listas de control de acceso asignadas al tráfico entrante y saliente (**"0"** significa que NO hay lista de acceso asociada).

Sintaxis:

```
IP config>LIST ACCESS-GROUP
```

Ejemplo:

```
IP config>list access-group
Per-interface access controls (access-group)
 ethernet0/0     in 101, out 103
 ppp1            in   0, out 110

Local access-group: in 102
IP config>
```

c) LIST ADDRESSES

Muestra todas las direcciones IP para cada interfaz, así como el formato de las direcciones de broadcast.

Sintaxis:

```
IP config>LIST ADDRESSES
```

Ejemplo:

```
IP config>list addresses
IP addresses for each interface:
 ethernet0/0     172.24.78.115   255.255.0.0     NETWORK broadcast,  fill 0
                 192.7.1.14      255.255.255.0   NETWORK broadcast,  fill 0
 atm0/0                                          IP disabled on this ifc
 uart0/0                                         IP disabled on this ifc
 x25-node                                        IP disabled on this ifc
 atm0/0.1        200.12.101.1    255.255.255.0   NETWORK broadcast,  fill 0
 ppp1            unnumbered      0.0.0.0         NETWORK broadcast,  fill 0
 ppp2            unnumbered      0.0.0.0         NETWORK broadcast,  fill 0
 ppp3            200.12.103.123  255.255.255.255 NETWORK broadcast,  fill 0
 ppp4            unnumbered      0.0.0.0         NETWORK broadcast,  fill 0
 loopback1       10.10.10.1      255.255.255.255 NETWORK broadcast,  fill 0
Router-ID: 10.10.10.1
Internal IP address: 1.1.1.1
Management IP address  : 10.10.10.1
IP config>
```

d) LIST ALL

Muestra toda la configuración IP.

Sintaxis:

```
IP config>LIST ALL
```

Ejemplo:

```
IP config>list all
Interface addresses
IP addresses for each interface:
 ethernet0/0     172.24.78.115   255.255.0.0     NETWORK broadcast,  fill 0
                 192.7.1.14      255.255.255.0   NETWORK broadcast,  fill 0
 atm0/0                                          IP disabled on this ifc
 uart0/0                                         IP disabled on this ifc
 x25-node                                        IP disabled on this ifc
 atm0/0.1        200.12.101.1    255.255.255.0   NETWORK broadcast,  fill 0
 ppp1            unnumbered      0.0.0.0         NETWORK broadcast,  fill 0
 ppp2            unnumbered      0.0.0.0         NETWORK broadcast,  fill 0
 ppp3            200.12.103.123  255.255.255.255 NETWORK broadcast,  fill 0
 ppp4            unnumbered      0.0.0.0         NETWORK broadcast,  fill 0
 loopback1       10.10.10.1      255.255.255.255 NETWORK broadcast,  fill 0
Router-ID: 10.10.10.1
Internal IP address: 1.1.1.1
```

```
Management IP address  : 10.10.10.1

Routing

route to 5.4.3.2,255.255.255.255 via 192.7.1.1, cost 1
route to 0.0.0.0,0.0.0.0 via ppp1, cost 1
route to 10.10.10.0,255.255.255.0 via 200.12.103.123, cost 1
Filter address 127.0.0.0, 255.0.0.0

Ip policy routing: disabled

Protocols
Directed broadcasts: enabled
RIP: disabled
OSPF: disabled
Multipath: disabled
Ip classless: enabled
Icmp redirects: enabled
Icmp unreachables: enabled

Pool
First address: 192.168.0.0
Last address: 192.168.255.255

Rules
  ID   Local Address   --> Remote Address   NAPT TOut FW  Adj-MSS Acc-List
       NAPT Address
 ------------------------------------------------------------------------
 1     200.12.101.1    --> 200.12.101.2     YES  5    NO   0        0
       0.0.0.0
 2     200.12.103.123  --> 0.0.0.0          YES  5    YES  0        0
       0.0.0.0
 3     ppp1            --> 0.0.0.0          YES  5    NO   0        0
       1.1.1.1

Per-interface access controls (access-group)
 ethernet0/0     in 101, out   0
 ppp1            in   0, out 110

Local access-group: in 102

IP config>
```

e) LIST DNS-DOMAIN-NAME

Muestra el nombre de dominio, configurado con el comando **DNS-DOMAIN-NAME** del menú de configuración de IP, y el FQDN, que identifica el equipo mediante el nombre de dominio y el nombre de host, configurado con el comando **SET HOSTNAME** del menú de configuración general del router.

Sintaxis:

```
IP config>LIST DNS-DOMAIN-NAME
```

Ejemplo:

```
IP config>list dns-domain-name
Domain name : dominio
FQDN : host1.dominio
IP config>
```

f) LIST IP-PARAM

Muestra la información de varios parámetros de IP: Tamaño de la tabla de rutas, tamaño del buffer de reensamblado y tamaño de la cache de rutas.

Sintaxis:

```
IP config>LIST IP-PARAM
```

Ejemplo:

```
IP config>list ip-param

Routing table size: 768 nets (52224 bytes)
Reassembly buffer size: 12000 bytes
Routing cache size: 64 entries

IP config>
```

g) LIST IP-PROTOCOL

Muestra la configuración de los protocolos de routing (RIP y OSPF), classless, multipath y otros parámetros de ICMP.

Sintaxis:

```
IP config>LIST PROTOCOLS
```

Ejemplo:

```
IP config>list ip-protocol
Directed broadcasts: enabled
RIP: disabled
OSPF: enabled
Multipath: disabled
Ip classless: disabled
Icmp redirects: enabled
Icmp unreachables: enabled
IP config>
```

h) LIST POLICY

Muestra información sobre Policy Routing (consultar el manual de Policy Based Routing, Dm 745).

i) LIST POOL

Muestra el rango que forma el pool de direcciones establecido en el router.

Sintaxis:

```
IP config>LIST POOL
```

Ejemplo:

```
IP config>list pool
First address: 192.168.0.0
Last address: 192.168.255.255
IP config>
```

j) LIST ROUTES

Muestra la lista de rutas de redes/subredes estáticas que hayan sido configuradas, así como cualquier router configurado por defecto. Muestra también las rutas de agregación que hayan sido configuradas.

Sintaxis:

```
IP config>LIST ROUTES
```

Ejemplo:

```
IP config>list routes
IP config>
```

k) LIST RULE

El comando **LIST RULE** muestra las conexiones IP definidas.

Sintaxis:

```
IP config>LIST RULE
```

Ejemplo:

```
IP config>list rule
  ID   Local Address   --> Remote Address   NAPT TOut FW  Adj-MSS Acc-List
       NAPT Address
 ------------------------------------------------------------------------
 1     200.12.101.1    --> 200.12.101.2     YES  10   NO   0        0
       0.0.0.0
 2     ppp1            --> 0.0.0.0          YES  5    YES  0        0
       0.0.0.0

IP config>
```

1.17. LOCAL

Permite configurar diversas funcionalidades relacionadas con el tráfico local (con origen o destino el propio router).

Sintaxis:

```
IP config>LOCAL ?
ACCESS-GROUP    Specify access control for local traffic
POLICY          Enable policy routing for locally generated packets
```

a) LOCAL ACCESS-GROUP

Mediante este comando se configura el sistema de control de acceso para el tráfico local. De este modo se puede restringir el acceso a los distintos servicios del router (telnet, ftp, etc.) con independencia del interfaz de entrada.

Sintaxis:

```
IP config>LOCAL ACCESS-GROUP <lista de acceso>
in     inbound packets
```

In: Aplica la lista de control de acceso genérica al tráfico local entrante.

Ejemplo:

```
IP config>local access-group 110 in
IP config>
```

Para volver a la configuración por defecto del comando se ejecuta el mismo comando precedido por "NO".

```
IP config>no local access-group 110 in
IP config>
```

b) LOCAL POLICY

Mediante este comando se habilita el Policy Routing para el tráfico local. Ver el manual de Policy Based Routing Dm 745.

Ejemplo:

```
IP config>LOCAL POLICY route-map <nombre>
```

1.18. MULTIPATH

Si este comando está habilitado, en el caso de que existan múltiples caminos para llegar a un destino de igual coste, el router escoge el camino para encaminar el paquete de acuerdo a los siguientes criterios: una cola circular (modo Round-Robin), o bien dependiendo del destino. Este comando por defecto está deshabilitado.

Sintaxis:

```
IP config>MULTIPATH ?
PER-DESTINATION    Enables per source and destination multipath routing
PER-PACKET         Enables per packet multipath routing
```

Ejemplo:

```
IP config>multipath
IP config>
```

Para deshabilitarlo se usa el mismo comando precedido por la partícula "NO".

```
IP config>no multipath
IP config>
```

1.19. NAT

Mediante este comando se llega a los menús de configuración de las facilidad NAT.

Sintaxis:

```
IP config>NAT ?
DYNAMIC      Enters in the dynamic nat configuration menus
PAT          Enters in the pat configuration menus
STATIC       Enters in the static nat configuration menus
IP config>
```

a) NAT DYNAMIC

Mediante este comando se llega a los menús de configuración de DNAT.

Sintaxis:

```
IP config>NAT DYNAMIC
```

Ejemplo:

```
IP config>nat dynamic

-- Dynamic NAT user configuration --
DNAT config>
```

b) NAT PAT

Mediante este comando se llega a los menús de configuración de la facilidad NAPT. Ver manual de la facilidad NAPT Dm 735.

Sintaxis:

```
IP config>NAT PAT
```

Ejemplo:

```
IP config>nat pat

-- NAPT configuration --
NAPT config>
```

c) NAT STATIC

Mediante este comando se llega a los menús de configuración de las facilidad NAT estático. Ver manual de la facilidad NAT estático Dm 720.

Sintaxis:

```
IP config>NAT STATIC
```

Ejemplo:

```
IP config>nat static

-- Static NAT configuration --
NAT config>
```

1.20. NO

Comando utilizado para negar otro comando o para restaurar la configuración por defecto de un determinado parámetro.

Sintaxis:

```
IP config>no ?
ACCESS-CONTROL              Configures global access control system
ACCESS-GROUP                Specifies per-interface access control system
ADDRESS                     Assigns an ip address to one network interfaces
AGGREGATION-ROUTE           Configures ip aggregation information
BROADCAST-ADDRESS           Sets the ip broadcast format for an interface
CLASSLESS                   Enables ip classless routing strategy
DIRECTED-BROADCAST          Enables directed broadcast
DNS-DOMAIN-NAME             Establishes the dns domain name
FILTER                      Designates an ip network/subnet to be filtered
ICMP-REDIRECTS              Enables sending icmp redirects
ICMP-UNREACHABLES           Enables sending icmp unreachables
INTERNAL-IP-ADDRESS         Sets the internal ip address
IP-PARAM                    Sets other ip parameters
LOCAL                       Disable local (not forwarded) traffic settings
MANAGEMENT-IP-ADDRESS       Sets the management ip address
MULTIPATH                   Enables multipath routing
POLICY                      Disable policy routing on an interface
POOL                        Sets the range of addresses for ppp assignments
ROUTE                       Configures a static network/subnet ip route
ROUTER-ID                   Sets the router id
RULE                        Configures an ip connection rule
IP config>
```

En el apartado de cada uno de los comandos que pueden ir precedidos por la partícula “NO” se ha explicado como afecta y se ha dado un ejemplo. Por tanto, para saber como afecta la partícula “NO” a cada uno de los comandos consultar el apartado explicatorio del comando en cuestión.

1.21. POLICY

Mediante este comando se habilita el Policy Routing en los interfaces. Ver el manual de Policy Based Routing Dm 745.

Sintaxis:

```
IP config>POLICY <interfaz> route-map <nombre>
```

1.22. POOL

Configura un rango de direcciones que el router puede asignar a través de sus conexiones PPP. El rango por defecto es el comprendido entre las direcciones IP 192.168.0.0 y 192.168.255.255.

Sintaxis:

```
IP config>POOL <first-address, last-address>
```

Ejemplo:

```
IP config>pool 192.168.0.0 192.168.255.255
IP config>
```

Para volver a restablecer la configuración de POOL por defecto ejecutar el mismo comando precedido por la partícula "NO".

```
IP config>no pool
IP config>
```

1.23. PROXY-ARP

Mediante este comando se accede a los menús de configuración del Proxy ARP. Para obtener más información sobre la configuración del Proxy ARP consultar el manual asociado Dm 734.

Sintaxis:

```
IP config>PROXY-ARP
```

Ejemplo:

```
IP config>proxy-arp
Proxy ARP Configuration

Proxy ARP cnfg>
```

1.24. ROUTE

Añade rutas estáticas IP de Red o Subred a la tabla de encaminamiento.

El destino se especifica por una dirección IP (Red, Subred, Host) junto con una máscara. Por ejemplo si el destino es una red clase B y el tercer byte de una dirección IP se usa como porción de una subred, la máscara podría ponerse a 255.255.255.0.

La ruta hacia el destino se especifica por la Dirección IP del siguiente salto, y el coste de routing del paquete hacia su destino. El siguiente salto debe estar en la misma red o subred que uno de los interfaces del router.

Sintaxis:

```
IP config>ROUTE <red o subred o host, mascara, salto, coste>
```

Ejemplo:

```
IP config>route 128.1.2.0  255.255.255.0  128.185.123.22   6
IP config>
```

Para borrar una ruta estática se usa el mismo comando precedido por la partícula "NO".

```
IP config>no route 128.1.2.0  255.255.255.0 128.185.123.22 6
IP config>
```

1.25. ROUTER-ID

Establece la dirección IP por defecto que el router utilizará cuando genere varios tipos de tráfico IP. Esta dirección es particularmente importante en multicasting. Por ejemplo, la dirección de origen de los pings (incluyendo multicast pings), traceroute y paquetes tftp enviados por el router llevan la dirección router-ID. Además el router-ID propio del protocolo OSPF coincide con con el router-ID configurado.

El router-ID debe coincidir con una de las direcciones IP de un interfaz, si no, se ignora. Cuando se ignora o simplemente no se configura la dirección IP por defecto del router, ni su OSPF router-ID, entonces el router-ID coincide con la primera dirección IP configurada en el router.

Nota: Al configurar el router-ID puede modificarse el router-id propio del protocolo OSPF. Si esto ocurre los mensajes de estado de los enlaces, originados por el router previos al cambio del router-ID persisten hasta que pase un tiempo aproximado de 30 minutos. Esto puede provocar un aumento de la base de datos de estados de enlaces.

Sintaxis:

```
IP config>ROUTER-ID <address>
```

Ejemplo:

```
IP config>router-id 192.7.1.254
IP config>
```

Para borrar el comando **ROUTER-ID** se usa el mismo comando precedido por la partícula "NO".

```
IP config>no router-id
IP config>
```

1.26. RULE

Mediante este comando se crean conexiones IP usadas posteriormente en la facilidad NAPT y en el protocolo IPSEC.

Una conexión IP es una extensión al concepto de interfaz, sirve para poder definir subinterfaces punto-punto sin tener la necesidad de crearlos. Un interfaz punto-multipunto puede tener más de una conexión IP. Un interfaz punto-punto sólo puede tener una conexión IP asociada.

En interfaces punto-punto la dirección IP local es suficiente para definir la conexión IP. Ejemplo, un interfaz PPP.

En interfaces punto-multipunto además de la dirección IP local es necesario especificar la dirección IP remota. Ejemplo, en un interfaz FR definido como punto-multipunto que tiene dirección origen "Ia1" y por el dlci 16 llega a la "Ia2" y por el 17 a la "Ia3" se pueden definir 2 conexiones IP, la primera "Ia1-Ia2" y la segunda "Ia1-Ia3".

Una regla además de definir una conexión IP le puede asociar una configuración de NAPT.

Al agregar una regla es necesario definir los siguientes parámetros:

Identificador: Es el identificador de la regla usado posteriormente en configuración de NAPT e IPSEC.

Dirección IP Local: Es la dirección del interfaz correspondiente del equipo que va a hacer NAPT. Esta será la dirección que se utilizará para hacer NAPT a no ser que se configure la dirección de NAPT (ver mas abajo).

Dirección IP Remota: En enlaces Punto a Multipunto (por ejemplo en Frame Relay) se puede definir este campo para identificar por cuál de los enlaces se ha recibido o se va a enviar el paquete y si hay que hacer o no NAPT. Otra posibilidad es dejarlo en 0.0.0.0 con lo que se aplicará NAT sobre todo el interfaz (por ejemplo sobre todos los dlcis de este interfaz).

Si el enlace es Punto a Punto (por ejemplo PPP), sabemos que esta dirección debe pertenecer a la misma subred que la dirección local por lo que no es necesario que esté definida siempre que la conexión sea de este tipo (Punto a Punto).

Habilitación de NAPT: Permite especificar si se habilita NAPT para la regla añadida. Si se habilita, también habrá que especificar los parámetros siguientes, relativos a NAPT.

Dirección NAPT: Si es configurada esta dirección se utilizará para hacer el NAPT en vez de la Dirección IP Local del interfaz. Si se mantiene en su valor por defecto (0.0.0.0) se utiliza la Dirección IP Local del interfaz para realizar el NAT.

Temporizador para la entrada NAPT: Es el tiempo en minutos que permanece ocupada la entrada en la tabla de puertos de traducción que se está utilizando en esta conexión. Es el tiempo en minutos que permanece activa la entrada NAPT durante la conexión.

Capacidad de firewalling: Es la forma de hacer que el equipo sea inaccesible por la conexión definida en esta regla, salvo a través de las entradas en la tabla de puertos de traducción o a través de las excepciones de NAPT referentes a esta regla.

Ajuste del MSS: Esta opción permite alterar el valor MSS de los paquetes TCP SYN, para controlar el tamaño máximo para esa conexión (normalmente limitandola al interfaz de salida MTU menos 40).

Lista de Control de Acceso: Permite seleccionar el tráfico IP al que se va ha hacer NAPT mediante una lista de acceso genérica.

Sintaxis:

```
IP config>RULE <id>
default        restore default values
no
       napt
              firewall         firewall behaviour
              translation      apply napt translation
              tcp-adjust-mss   adjust the mss of transit packets
local-ip       local ip of this rule
napt           napt parameters configuration
        access-list      associated access list
       firewall         firewall behaviour
       ip               local ip address to make napt
       timeout          timeout of the napt translation
       translation      apply napt translation
       tcp-adjust-mss   adjust the mss of transit packets
              mss_clamping    mss clamping
              <1..65534>      truncate the mss to this value

remote-ip      remote ip of this rule
Type an option [default]?
IP config>
```

Default: Crea una regla con identificador <id> y los valores por decto. Si ya existe pone por defecto sus valores.

No: Deshabilita el firewalling o el NAPT en la regla cuyo identificador es <id>.

Local-ip: Configura la dirección ip local de la regla cuyo identificador es <id>.

Napt : Configura los parámetros NAPT de la regla cuyo identificador es <id>.

Remote-ip: Configura la dirección ip remota de la regla cuyo identificador es <id>.

Ejemplo:

Para crear la conexión IP con direcció local 213.4.21.187 y remota 213.4.21.188, y además habilitar NAPT y firewalling

```
IP config>rule 1 default
IP config>rule 1 local-ip 213.4.21.187
IP config>rule 1 remote-ip 213.4.21.188
IP config>rule 1 napt translation
IP config>rule 1 napt timeout 6
IP config>
```

Para borrar una regla ejecutar el mismo comando precedido por “NO”.

```
IP config>no rule 1
IP config>
```

1.27. TVRP

Mediante este comando se llega a los menús de configuración del protocolo TVRP. Para más información sobre este protocolo consultar el manual Protocolo TVRP Dm 725.

Sintaxis:

```
IP config>TVRP
```

Ejemplo:

```
IP config>tvrp
TVRP Configuration

TVRP config>
```

1.28. EXIT

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

Sintaxis:

```
IP config>EXIT
```

Ejemplo:

```
IP config>exit
Config>
```

Capítulo 4
Monitorización

1. Comandos de Monitorización del Protocolo IP

Esta sección resume y explica todos los comandos de monitorización del router. Estos comandos le permitirán monitorizar el comportamiento de los protocolos IP del router, y poder de esta forma llegar a las especificaciones de funcionamiento deseadas.

Introducir los comandos de monitorización IP cuando se tenga el prompt IP>, para acceder a este prompt se debe teclear lo siguiente:

```
*P 3
Console Operator
+PROTOCOL IP
IP>
```

Comando	**Función**
? (AYUDA)	Lista comandos u opciones.
AGGREGATION-ROUTE	Enseña las rutas de agregación que han sido configuradas.
ACCESS controls	Lista el modo de control de acceso de IP conjuntamente con los registros del control de acceso.
BPING	Realiza un ping a cada host de una red determinada. También llamado ping broadcast.
CACHE	Muestra la tabla encaminamiento.
COUNTERS	Lista estadísticos IP, incluye contadores de errores de routing y paquetes perdidos.
DUMP routing tables	Lista la tabla de encaminamiento.
INTERFACE addresses	Lista las direcciones IP del interfaz del router.
IPSEC	Para acceder a los menús de monitorización de IPSEC.
NAT	Para acceder a los menús de monitorización de la facilidad NAT.
NAPT	Para acceder a los menús de monitorización de la facilidad NAPT.
PING [address]	Envía una pregunta a cualquier otro host cada segundo y espera la respuesta. Este comando se utiliza para aislar problemas en un entorno de múltiples redes. Admite parámetros cuando no se especifica dirección.
POOL	Muestra el pool de direcciones establecido en el router, así como los rangos de direcciones reservados del mismo.
ROUTE given address	Lista encaminamientos existentes para dirección IP destino específico.
SIZES	Enseña el tamaño de parámetros IP específicos.
STATIC-ROUTES	Enseña los rutas estáticas que han sido configuradas.
TRACEROUTE address	Enseña el camino completo salto a salto a una dirección destino concreta.
TVRP	Para acceder a los menús de monitorización del protocolo TVRP.
EXIT	Sale de la monitorización IP.

1.1. ? (AYUDA)

Utilizar el comando **?** (AYUDA) para listar los comandos válidos en el nivel donde se está programando el router. También se puede utilizar este comando después de un comando específico para listar sus opciones.

Sintaxis:

```
IP>?
```

Ejemplo:

```
IP>?
AGGREGATION-ROUTE
ACCESS controls
BPING
CACHE
COUNTERS
DUMP routing tables
INTERFACE addresses
IPSEC
NAT
NAPT
PING [address]
POOL
ROUTE given address
SIZES
STATIC-ROUTES
TRACEROUTE address
TVRP
EXIT
IP>
```

1.2. AGGREGATION-ROUTES

Utilizar el comando **AGGREGATION-ROUTES** para visualizar la lista de rutas de agregación configuradas.

Cada ruta viene especificada por una dirección y su correspondiente máscara.

El siguiente ejemplo muestra una ruta de agregación (agregar todas las redes que comienzan por 200).

Sintaxis:

```
IP>AGGREGATION-ROUTES
```

Ejemplo:

```
IP>AGGREGATION-ROUTES
Net             Mask
---             ----
1.1.0.0        255.255.0.0    aggregation
IP>
```

El significado de cada uno de los campos es el siguiente:

Net	Red o subred destino de la ruta.
Mask	Máscara de la red o subred destino de la ruta.

1.3. ACCESS control

Utilizar este comando para visualizar el modo de control de acceso en uso conjuntamente con la lista de los registros de control de acceso. Los modos de control de acceso pueden ser:

Disabled: No existe control de acceso y por tanto todos los registros de control de acceso son ignorados.

Enabled: Existe control de acceso y los registros de control de acceso son inspeccionados.

Exclusive: Los paquetes coincidentes con los registros de control de acceso son rechazados.

Inclusive: Los paquetes coincidentes con los registros de la lista de control de acceso son encaminados.

Cuando se habilita el control de acceso, los paquetes que no coincidan con cualquiera de los registros del control de acceso son rechazados. *Beg* y *End Pro* indican el número de protocolo IP y *Beg* y *End Prt* indican el número de puerto. *Invoc* especifica el número de veces que una particular entrada del sistema de control de acceso ha sido invocada por las características de un paquete entrante o saliente.

Sintaxis:

```
IP>ACCESS
```

Ejemplo:

```
IP>ACCESS
Access Control currently enabled
Access Control run 0 times, 0 cache hits

List of access control records:
                                          Beg End  Beg   End   Beg  End
Type        Source           Destination  Pro Pro  SPrt  SPrt  DPrt DPrt Invoc
1 E         0.0.0.0/0       192.6.1.250/32   6   6    23    23    23    23    0
2 I         0.0.0.0/0          0.0.0.0/0    0 255     0 65535     0 65535   14
IP>
```

1.4. BPING

Use el comando **BPING** (Broadcast PING) para que el router mande un paquete del tipo ICMP Echo request a cada dirección de una subred, y espere una respuesta.

Por consola se piden una serie de parámetros:

IP destination: (Dirección IP destino) Una dirección cualquiera perteneciente a la subred.

IP source: (Dirección IP origen) de salida de los paquetes. Por defecto el equipo elige la dirección origen del interfaz (lógico) de salida del ping.

Destination mask: (máscara de red) La de la subred.

Time out: Intervalo de tiempo mayor o igual que 10ms dentro del cual se espera la respuesta de un paquete enviado. El origen del time out lo marca el lanzamiento del paquete. Por defecto su valor es de un segundo.

Avoid fragmentation: (impedir fragmentación) del datagrama IP. Es una orden para los routers porque el destino es incapaz de juntar las piezas de nuevo. Por defecto el datagrama puede fragmentarse.

El tamaño de los paquetes es de 56 bytes excluyendo la cabecera ICMP.

La dirección a la que se envía el paquete se va incrementando comenzando por la primera dirección de la subred que no sea de broadcast, es decir, habría que saltarse la primera dirección y la última. Los paquetes se mandan cada 100ms, pero en el caso de que time out sea mayor que este tiempo, si no se recibe respuesta se espera a consumir el time out antes de enviar un nuevo paquete.

Si se recibe respuesta válida se visualiza el retardo correspondiente, si no, se imprime un mensaje de contacto no establecido.

El comando **BPING** finaliza cuando se pulsa cualquier tecla o se terminan las direcciones de la subred.

En el ejemplo siguiente siendo la dirección de destino 192.6.1.228 y su mascara 255.255.255.248, después de efectuar la operación AND lógica correspondiente, las direcciones de broadcast serían 192.6.1.224 y 192.6.1.231. Por lo que el comando **BPING** se ejecuta entre las direcciones 192.6.1.225 y 192.6.1.230.

Sintaxis:

```
IP>BPING
```

Ejemplo:

```
IP>BPING
IP destination [192.6.1.0]? 192.6.1.228
Destination mask [255.255.255.0]? 255.255.255.248
IP source [192.7.1.253]?
Time out(>=10ms)[1000]?
Avoid fragmentation[no](Yes/No)?
PING 192.6.1.225...  time=16. ms
PING 192.6.1.226...  not established contact
PING 192.6.1.227...  not established contact
PING 192.6.1.228...  time=30. ms
PING 192.6.1.229...  not established contact
PING 192.6.1.230...  not established contact
IP>
```

1.5. CACHE

Este comando es útil para listar las rutas de destino usadas recientemente y que se encuentran en la memoria cache de routing. Si un destino no se encuentra en la memoria cache, el router busca dicho destino en la tabla general de routing para tomar una decisión al respecto.

Sintaxis:

```
IP>CACHE
```

Ejemplo:

```
IP>CACHE
Destination            Usage   Next hop
192.6.2.12             6       192.6.2.12    (EtherNet (10 MBit)/0)
194.179.1.100          520     130.1.1.191   (Router->Nodo/0)
192.6.2.15             248     192.6.2.15    (EtherNet (10 MBit)/0)
192.6.1.157            206     130.1.1.191   (Router->Nodo/0)
192.6.2.3              4       192.6.2.3     (EtherNet (10 MBit)/0)
192.6.1.110            7       130.1.1.191   (Router->Nodo/0)
192.6.2.10             4       192.6.2.10    (EtherNet (10 MBit)/0)
192.6.1.34             1       130.1.1.191   (Router->Nodo/0)
192.6.1.250            1       130.1.1.191   (Router->Nodo/0)
IP>
```

El significado de cada uno de los campos es el siguiente:

Destination: Dirección destino de Host.

Usage: Número de paquetes enviados a Host.

Next hop: Dirección IP en el siguiente router para llegar a la dirección Host. También enseña el interfaz usado por este paquete.

1.6. COUNTERS

Utilizar este comando para listar estadísticos relativos a paquetes IP que han progresado. Estos estadísticos incluyen un contador de errores de routing con la cantidad asociada de paquetes que han sido desechados, debido a congestión.

Sintaxis:

```
IP>COUNTERS ?
DELETE
SHOW
```

a) COUNTERS DELETE

Ejemplo:

```
IP>COUNTERS DELETE
IP>
```

b) COUNTERS SHOW

Ejemplo:

```
IP>COUNTERS SHOW
Routing errors
Count  Type
   0   Routing table overflow
2371   Net unreachable
   0   Bad subnet number
   0   Bad net number
  27   Unhandled broadcast
   0   Unhandled multicast
   0   Unhandled directed broadcast
5537   Attemped forward of LL broadcast

Packets discarded through filter  0
IP multicasts accepted:           212

IP input packet overflows
    Net   Count
   Eth/0  0
    FR/0  0
   X25/0  0
   X25/1  0
   BRI/0  0
  R->N/0  0
   PPP/0  0
IP>
```

El significado de cada uno de los campos es el siguiente:

Routing table overflow	Rutas que han sido desechadas debido a que la tabla de routing estaba llena.
Net unreachable	Paquetes que no se han podido traspasar debido a desconocerse su destino.
Bad subnet or net number	Paquetes o rutas de red/subred ilegales.
Unhandled broadcast	Paquetes IP recibidos de tipo broadcast no locales (por lo tanto no progresados).
Unhandled multicast	Paquetes IP multicast recibidos cuyas direcciones no han sido reconocidas por el router.
Unhandled directed broadcast	Broadcast recibidos directos (no locales) cuando el traspaso de estos paquetes está deshabilitado.
Attempted forward off LL broadcast	Paquetes recibidos teniendo dirección IP no local pero que fueron enviados a una dirección broadcast de nivel de enlace. Estos se descartan.
Packets discarded through filter	Los paquetes recibidos que habían sido direccionados a redes/subredes filtradas.
IP multicast accepted	Multicast IP que han sido recibidos y procesados satisfactoriamente por el router.

IP input packet overflows	Paquetes que han sido descartados debido a congestión en la cola de entrada de paquetes.

1.7. DUMP routing tables

Utilizar este comando para listar la tabla de routing IP. Se imprime una línea por cada ruta de red IP. El router por defecto, si existe, se imprime al final.

Sintaxis:

```
IP>DUMP
```

Ejemplo:

```
IP>DUMP
Type           Dest net       Mask       Cost  Age   Next hop(s)
Stat(1)        0.0.0.0        00000000   0     0     192.6.1.3
Sbrd(0)        3.0.0.0        FF000000   1     0     None
 SPF(1)        3.7.8.0        FFFFFF00   1     1     Eth/0
 SPF(0)        3.7.8.250      FFFFFFFF   1     1     3.7.8.250
 Dir(1)        192.6.1.0      FFFFFF00   1     0     Eth/0
 SPF(0)        192.6.1.251    FFFFFFFF   0     0     SNK/0
Stat(1)        192.6.2.0      FFFFFF00   1     0     192.168.1.2
 RIP(0)        192.6.3.0      FFFFFF00   2     20    192.6.1.14
Aggr(0)A       200.0.0.0      FF000000   1     0     None
Stat(1)a       200.1.1.0      FFFFFF00   2     0     98.61.1.2
Stat(1)a       200.1.2.0      FFFFFF00   1     0     98.61.1.2

Default gateway in use.
Type Cost Age Next hop
Est  0    0    192.6.1.3
Routing table size: 768 nets (52224 bytes), 8 nets known
IP>
```

El significado de cada uno de los campos es el siguiente:

Type (tipo de ruta)	Indica como se creo la ruta. Sbnt— la red está dividida en subredes; este tipo de entrada es una marca. Aggr—agregación de redes; este tipo de entrada es una marca. Dir— red o subred conectada diréctamente. RIP— ruta aprendida por el protocolo RIP. Del— la ruta fue borrada. Stat— ruta estáticamente configurada. Fltr— filtro. SPF— la ruta es una ruta OSPF intra-área. SPIA—la ruta es una ruta OSPF inter-área. SPE1**,** SPE2— la ruta es una ruta OSPF externa (tipo 1 y 2 respectivamente). Rang—rango de direcciones activo de OSPF. No se usa para encaminar paquetes.
Dest net	Red o subred IP destino.
Mask	Máscara de la red IP destino.
Cost	Coste de la ruta.
Age	Para las rutas de tipo RIP, tiempo que ha trancurrido desde que se ha refrescado la tabla de routing.
Next hop(s)	Dirección IP del siguiente router en el camino hacia el destino o interfaz de salida que el router usará para encaminar el paquete.

Un número entre paréntesis *(num)* después del *tipo de ruta* indica el número de rutas estáticas o directas configuradas, con interfaz y subinterfaz de salida activo y que poseen como destino el de la ruta.

Un signo de porcentaje *"%"* después del *tipo de ruta* indica que los "updates" de RIP siempre son aceptados para este destino.

Una letra *"A"* después del *tipo de ruta* indica que la ruta coincide con una ruta de agregación.

Una letra *"a"* después del *tipo de ruta* indica que la ruta está siendo agregada por una ruta de agregación.

Cuando una ruta hacia un destino tiene más de un camino activo con igual coste, en la columna *Next hop(s)* se muestra cada camino en una línea, y se marca con "*(C)*" el camino actual. Dependiendo de la política multicamino configurada, el camino actual pasará por todos los caminos consecutivamente (Round robin) o bien según el origen/destino de los paquetes encaminados (ver comando de configuración MULTIPATH).

1.8. INTERFACE addresses

Utilizar este comando para visualizar las direcciones IP del interfaz del router. Cada dirección aparece con su correspondiente interfaz hardware y con su mascara de dirección IP.

Sintaxis:

```
IP>INTERFACE
```

Ejemplo:

```
IP>INTERFACE
Interface  IP Address(es)   Mask(s)
   Eth/0   192.7.1.253      255.255.255.0
    FR/0   192.3.1.2        255.255.255.0
           10.0.0.3         255.0.0.0
  R->N/0   192.168.252.1    255.255.255.0
IP>
```

El significado de cada uno de los campos es el siguiente:

Interface:	Tipo de hardware del interfaz
IP Address(es):	Dirección IP del interfaz
Mask(s):	Máscara de la subred del interfaz

1.9. IPSEC

Mediante este comando se llega a los menús de monitorización de IPSEC. Ver el manual de IPSEC Dm 739.

Sintaxis:

```
IP>IPSEC
```

Ejemplo:

```
IP>IPSEC
IPSEC protocol monitor
IPSEC>
```

1.10. NAT

Mediante este comando se llega a los menús de monitorización de la facilidad NAT. Ver manual de la facilidad NAT Dm 720.

Sintaxis:

```
IP>NAT
```

Ejemplo:

```
IP>NAT
NAT monitoring
NAT monit >
```

1.11. NAPT

Mediante este comando se llega a los menús de monitorización de la facilidad NAPT. Ver manual de la facilidad NAPT Dm 735.

Sintaxis:

```
IP>NAPT
```

Ejemplo:

```
IP>NAPT
NAPT>
```

1.12. PING [address]

"Packet Internet Grouper": Programa de prueba asociado con TCP/IP utilizado para probar el canal de comunicaciones entre estaciones en INTERNET.

Con el comando **PING,** el router manda paquetes del tipo ICMP Echo request a una dirección dada y espera una respuesta para cada paquete enviado. Este comando es útil para localizar problemas en la red.

Si se especifica una dirección inmediatamente después del comando **PING**, no se realiza petición de parámetros, escogiendo valores por defecto. Si no se especifica ninguna dirección, el equipo pide una serie de parámetros:

IP destination: a la que se envían los paquetes y de la que se esperan las respuestas.

IP source: de salida de los paquetes. Por defecto el equipo elige la dirección origen del interfaz (lógico) de salida del ping.

Number of data bytes: Tamaño del mensaje ICMP, excluyendo la cabecera ICMP. Por defecto su valor es de 56 bytes.

Time between pings: Intervalo entre envíos que tiene que ser mayor o igual que 100ms. Por defecto su valor es de un segundo.

Number of pings: Número de paquetes a enviar. Por defecto su valor es cero con lo que se mandan paquetes indefinidamente.

Time out: Intervalo de tiempo mayor o igual que 10ms, dentro del cual se espera la respuesta a un paquete enviado. El origen de time out lo marca el lanzamiento del paquete. Por defecto su valor es cero con lo que se espera indefinidamente la llegada de la respuesta.

Avoid fragmentation: del datagrama IP. Es una orden para los routers porque el destino es incapaz de juntar las piezas de nuevo. Por defecto el datagrama puede fragmentarse.

En el caso de que el time out sea mayor que el tiempo entre pings, si no se recibe respuesta se espera a consumir el time out antes de enviar un nuevo paquete.

Por cada paquete que se manda se incrementa el número de secuencia ICMP. La respuesta que se corresponde con el paquete enviado se visualiza junto con el número de secuencia y el retardo correspondiente. La precisión del tiempo de medida es del orden de 20 ms (dependiendo de las plataformas). Si no se recibe esa respuesta durante time out se imprime un mensaje de superación de dicho tiempo.

El comando **PING** finaliza cuando se pulsa cualquier tecla, o ya se han tratado todos los paquetes a enviar con sus correspondientes respuestas. En este momento se muestra un resumen de los paquetes transmitidos, recibidos, perdidos, y cuya respuesta ha superado time out, así como los retardos mínimos, medios y máximos.

Cuando la dirección de destino es una dirección multicast, pueden recibirse múltiples repuestas por cada paquete ICMP enviado. Una para cada miembro del grupo. En este caso se muestra cada respuesta recibida con la dirección IP del host que responde.

Sintaxis:

```
IP>PING
```

Ejemplo:

```
IP>PING
IP destination [192.7.1.0]? 192.7.1.1
IP source [192.7.1.253]?
Number of data bytes[56]? 1500
Time between pings(>=100ms)[1000]? 150
Number of pings[0]? 4
Time out(>=10ms)[0]? 30
Avoid fragmentation[no](Yes/No)? Y

PING 192.7.1.1: 56 data bytes
64 bytes from 192.7.1.1: icmp_seq=0. time=2. ms
64 bytes from 192.7.1.1: icmp_seq=1. time=2. ms
64 bytes from 192.7.1.1: icmp_seq=2. time=2. ms
64 bytes from 192.7.1.1: icmp_seq=3. time=2. ms

----192.7.1.1 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 2/2/2
IP>
```

Un caso especial es el uso del comando **PING address** en el que todos los parámetros configurables toman su valor por defecto.

Sintaxis:

```
IP>PING address
```

Ejemplo:

```
IP>PING 192.7.1.1
PING 192.7.1.1: 56 data bytes
64 bytes from 192.7.1.1: icmp_seq=0. time=2. ms
64 bytes from 192.7.1.1: icmp_seq=1. time=2. ms

----192.7.1.1 PING Statistics----
2 packets transmitted, 2 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 2/2/2
IP>
```

1.13. POOL

Utilizar el comando **POOL** para visualizar el pool de direcciones establecido en el router, así como los rangos de direcciones ocupados del mismo y la causa por la que están reservados.

Los rangos de direcciones ocupados del pool se expresan en formato de una dirección y una máscara, siendo sus causas de reserva las siguientes:

SET	Rangos de direcciones configurados en el router.
RADIUS	Rangos de direcciones recibidos de un Servidor RADIUS, para que el router asigne direcciones a los extremos remotos de sus conexiones PPP.
POOL	Rangos de direcciones tomados del pool, para que el router asigne direcciones a los extremos remotos de sus conexiones PPP.
LOCAL	Rangos de direcciones recibidos de los extremos remotos de las conexiones PPP del router, para que se asignen a los extremos locales.
ASSIGN	Rangos de direcciones configurados en los interfaces PPP del router, para que éste asigne direcciones a los extremos remotos de sus conexiones PPP.
REMOTE	Direcciones configuradas en los extremos remotos de las conexiones PPP del router, y enviadas por ellos.
INTERNAL	Dirección IP interna configurada en el router.
ROUTER ID	Dirección router-ID configurada en el router.
MNGMENT	Dirección IP de gestión configurada en el router.
SNMP	Rango de direcciones reservado por la preconfiguración de X.25.

Sintaxis:

```
IP>POOL
```

Ejemplo:

```
IP>POOL
First address: 192.168.0.0
Last address: 192.168.255.255

TAKEN ADDRESS RANGES
IP Address(es)   Mask(s)
192.168.0.0      255.255.255.252 (POOL)
192.168.0.4      255.255.255.252 (POOL)
IP>
```

1.14. ROUTE given address

Utilizar el comando **ROUTE** para visualizar la ruta (si existe) a una dirección IP dada. Si la ruta existe, se muestran las direcciones, los saltos así como información detallada de la tabla de routing.

Sintaxis:

```
IP>ROUTE address
```

Ejemplo:

```
IP>ROUTE 192.6.1.169
Destination:    192.6.1.0
Mask:           255.255.255.0
Route type:     RIP
Distance:       2
Age:            10
Tag:            0
Next hop(s):     192.3.1.1        (FR/0)
IP>
```

1.15. SIZES

Utilizar el comando **SIZES** para visualizar el tamaño configurado de ciertos parámetros propios del protocolo IP.

Sintaxis:

```
IP>SIZES
```

Ejemplo:

```
IP>SIZES
Routing table size:             768
Table entries used:             6
Reassembly buffer size:         12000
Largest reassembled pkt:        0
Size of routing cache:          64
# cache entries in use:         2
IP>
```

El significado de cada uno de los campos es el siguiente:

Routing table size	Número de entradas de la tabla de routing que el router es capaz de mantener.
Table entries used	Número de entradas de la tabla de routing IP utilizadas.
Reassembly buffer size	Longitud buffer de reensamblado que se usa para reensamblar paquetes IP fragmentados.
Largest reassembly pkt	Mayor paquete IP que el router ha tenido que reensamblar.
Size of routing cache	Longitud de la tabla de routing IP.
# cache entries in use	Número de entradas de la tabla en uso.

1.16. STATIC-ROUTES

Utilizar el comando **STATIC-ROUTES** para visualizar la lista de rutas estáticas configuradas. También se muestran los routers de red y subred por defecto.

Cada ruta viene especificada por una dirección, su correspondiente máscara, la dirección del siguiente salto, su coste, el interfaz de salida, el subinterfaz de salida y el estado. Los routers por defecto aparecen como rutas estáticas con la dirección de destino 0.0.0.0 y máscara 0.0.0.0. Los routers de subred por defecto también aparecen como rutas estáticas con destinos las redes divididas en subredes.

El siguiente ejemplo muestra un router de red por defecto, un router de subred por defecto (suponiendo que hay subredes en 128.185.0.0), una ruta al host 172.16.2.3 y rutas estáticas a las redes 192.6.2.0 y 192.168.67.0.

Sintaxis:

```
IP>STATIC-ROUTES
```

Ejemplo:

```
IP>STATIC-ROUTES
Net            Mask              Cost  Next_hop        Int      SubInt       State
---            ----              ----  --------        ---      ------       -----
0.0.0.0        0.0.0.0           0     3.7.8.100       Eth/0    N/A          UP
128.185.0.0    255.255.0.0       1     192.168.3.18    Eth/0    N/A          UP
172.16.2.3     255.255.255.255   1     172.16.1.9      FR/0     118          DWN
192.6.2.0      255.255.255.0     1     192.168.1.2     FR/1     16           UP
192.168.67.0   255.255.255.0     1     192.168.2.18    R->N/0   3456782123   UP
IP>
```

El significado de cada uno de los campos es el siguiente:

Net	Red o subred destino de la ruta.
Mask	Máscara de la red o subred destino de la ruta.
Cost	Coste del uso de esta ruta.
Next hop	Dirección IP del siguiente router donde serán enviados los paquetes para llegar al destino indicado en la ruta.
Int	Identificador del interfaz de salida de los paquetes que escojan esta ruta. Si en el momento en el que se monitoriza la ruta, el equipo no es capaz de averiguar el interfaz de salida (porque no exista), aparecerá UNK (desconocido).
Subint	Identificador del subinterfaz de salida de los paquetes que escojan esta ruta. En caso de FR indica el DLCI de salida, en el caso de X25 (R->N) indica el NRI de salida, en caso de un interfaz genérico que no sea divisible en subinterfaces aparece N/A (No Aplicable). Si en el momento en el que se monitoriza la ruta, el equipo no es capaz de averiguar el subinterfaz de salida (porque no exista), aparecerá UNK (desconocido).
State	Indica si la ruta estática en cuestión está activa "UP" (interfaz y subinterfaz activos) o inactiva "DWN" (interfaz o subinterfaz inactivos, o desconocidos). Que el estado indique actividad no quiere decir que la ruta esté activa dentro de la tabla de rutas activas (monitorizable con el comando **DUMP**). Únicamente indica que la ruta estática sería elegida como mejor ruta en caso de que no exista otra ruta (estática o dinámica) con mejor coste.

1.17. TRACEROUTE address

Utilizar el comando **TRACEROUTE** para visualizar el camino completo a un destino. Para cada salto, **TRACEROUTE** lanza tres paquetes y visualiza la dirección IP del router que responde así como el retardo asociado a la respuesta. Si una paquete no recibe respuesta, se visualiza un asterisco. Cada línea que se muestra está relacionada con los tres paquetes, siendo la cifra más a la izquierda la distancia al router en saltos sobre el que se hace la prueba.

El comando finaliza cuando se ha llegado al destino, se recibe un paquete del tipo ICMP Destino Inalcanzable o se han superado 32 saltos.

Cuando una prueba recibe una respuesta no esperada, se visualizan distintas indicaciones. "!N" indica que se ha recibido un paquete del tipo ICMP Destino Inalcanzable (red inalcanzable). "!H" indica que se ha recibido un paquete del tipo ICMP Destino Inalcanzable (host inalcanzable). "!P" indica que se ha recibido un paquete del tipo ICMP Destino Inalcanzable (protocolo inalcanzable). Dado que la prueba lanzada es un paquete UDP enviado a un puerto remoto, la respuesta esperada es puerto no alcanzable. "!" indica que se ha alcanzado el destino, pero la respuesta enviada por el destinatario ha sido recibida con TTL igual a 1. Esto suele significar un error en destino que prevalece en algunas versiones de UNIX, ya que el destinatario está incluyendo el TTL del paquete de prueba en su respuesta. Esto provoca varias líneas con asteriscos hasta que finalmente se alcanza al destino.

Sintaxis:

```
IP>TRACEROUTE address
```

Ejemplo:

```
IP>TRACEROUTE 128.185.142.239
TRACEROUTE 128.185.124.110: 56 data bytes
1 128.185.142.7    16 ms 0 ms   0 ms
1 128.185.123.22   16 ms 0 ms  16 ms
3 * * *
4 * * *
5 128.185.124.110  16 ms ! 0 ms ! 0 ms !
IP>
```

El significado de cada uno de los campos es el siguiente:

TRACEROUTE	Muestra la dirección de área de destino así como el tamaño del paquete enviado.
1	La primera traza que muestra NSAP del destino así como el tiempo necesario para llegar al mismo. El paquete es enviado 3 veces.
Net unreachable	Indica que no hay ninguna ruta disponible hacia el destino indicado en el comando.
1 * * *	Indica que el router está esperando una respuesta del destinatario que no se
2 * * *	recibe.

1.18. TVRP

Mediante este comando se llega a los menús de monitorización del protocolo TVRP. Ver manual del protocolo TVRP Dm 725.

Sintaxis:

```
IP>TVRP
```

Ejemplo:

```
IP>TVRP
TVRP Monitoring

TVRP monit>
```

1.19. EXIT

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

Sintaxis:

```
IP>EXIT
```

Ejemplo:

```
IP>EXIT
+
```