Teldat Router

TCP-IP Configuration

Doc. *DM702-I* Rev. *10.13*
October, 2003

INDEX

Chapter 1
Introduction

1. Introduction to IP Protocol

IP is a network layer protocol that provides a connectionless datagram service for the delivery of data. The fact that is connectionless makes IP an unreliable protocol: one that tries but does nothing to guarantee delivery of data. As used on the Internet, IP is the package used to carry data; actual delivery of the data is assured by transport layer protocols like TCP (Transmission Control Protocol).

TELDAT's IP implementation conforms the standards defined by the TCP/IP protocol suite.

1.1. The Meaning of IP Addresses

IP addresses identify where a host's interface attaches to the IP network or a particular network segment. If, for example, a host has more than one interface attached to the network, that host would have an IP address for each connection. This makes an IP address much like a postal street address, indicating where to send the data, not to whom to send the data.

An IP address is a 32 bit number in the header of an IP datagram that encodes network segment identification as well as identification of a unique host on that network.

Normally a special notation is used to indicate the IP addresses: the 32 bits are divided into four groups of 8. The values of the said groups are in decimal, separated by dots.

Thus an IP address in binary notation will be:

10000000 00101010 00001010 00010111

equivalent to:

128.42.10.23

Each IP address forms a pair of identifiers, one identifies the network, the **netid**; and another identifies a host on that network, the **hostid**.

1.2. IP Address Classes

IP addresses have three primary forms of designation: class A, class B and class C. A host determines the class of IP address by examining the high order bits of the address.

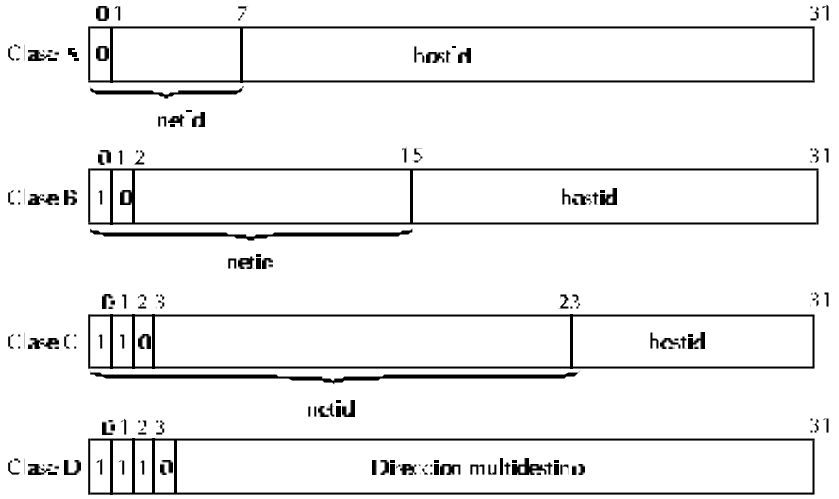
A Class A address is used for any network having more than 65,534 hosts. A host interprets a Class A address by reading bit 0 of the 32 bit address. If this bit is set to 0, the host interprets the **netid** field as the first 8 bits and **hostid** field as the last 24 bits. Only 127 Class A network numbers exist.

A Class B address is used for any intermediate size network having between 255 and 65,534 hosts. With this address the first 16 bits of the 32 bit address are devoted to the **netid** and last 16 bits are devoted to the **hostid**. A host interprets a Class B address by reading bits 0 and 1 of the 32 bit address. If these bits are set to 1 and 0 respectively, then the host interprets the **netid** field as the first 16 bits and the **hostid** field as the last 16 bits.

A Class C address is used for any network having less than 255 hosts. With this address the first 24 bits are devoted to the **netid** field and last 8 bits to the **hostid** field. A host interprets this address by reading bits 0, 1, y 2 of the 32 bit address. If these bits are set to 1, 1 and 0 respectively, then the host interprets the **netid** field as the first 24 bits and the **hostid** field as the last 8 bits.

In addition to these classes through which the addresses of the final systems are organized, there is also a fourth class, class D. A Class D address is used for IP multicasting. With this address the first

4 bits contain 1,1,1,0 and identify the address as a multicast. Bits 4 through 31 identify the specific multicast group.



This implementation of IP allows you to assign multiple IP addresses on the same interface. Multiple IP addresses allow flexibility when

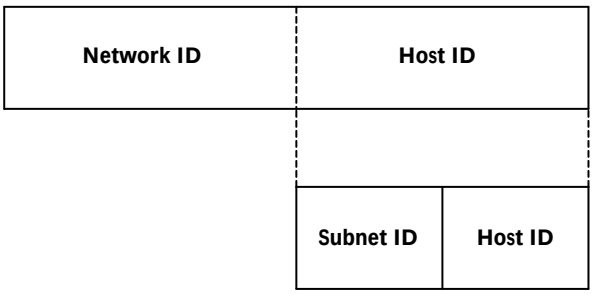
- Migrating from one IP address to another
- Using two subnets on the same physical network segment. For example, it is possible that the number of hosts on the physical network segment exceeds the current subnet's capacity. When this occurs, another subnet must be added to the physical network segment.

1.3. Subnet Addresses

The concept of subnet addressing or subnetting allows a site with multiple physical network segments to use a single IP network number. Subnetting adds another level of hierarchy to the Internet addressing structure. Instead of a 2 level (**netid**, **hostid**) hierarchy, there is now a 3 level (**netid**, **subnetid**, **hostid**) hierarchy. An organization is then assigned one, or at the very most, a few IP network numbers. An organization is then free to assign a distinct subnet number to each of its physical network segments (Local Area Networks and Wide Area Networks).

An organization's subnet structure is never visible outside the organization's network from a host (or router) located anywhere outside the limits of the said organization.

Conceptually, adding subnetting only changes the interpretation of IP address. Subnetting divides the address into a network ID, subnet ID, and host ID. The network segment is then identified by a combination of network ID and subnet ID.



There is no set standard for the width of the subnet part; it can be a few bits wide to most of the width of the **hostid** field.

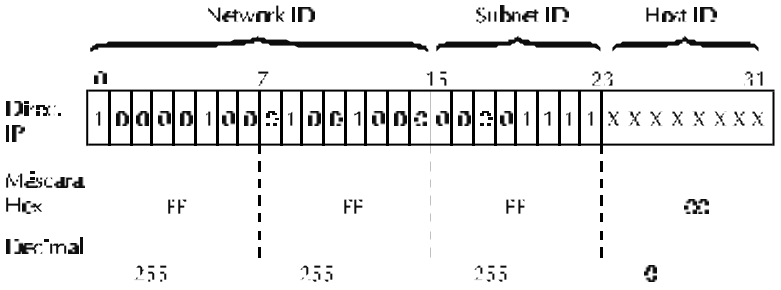
1.4. Subnet Mask

When you add an IP address to an interface, you must specify the subnet mask.

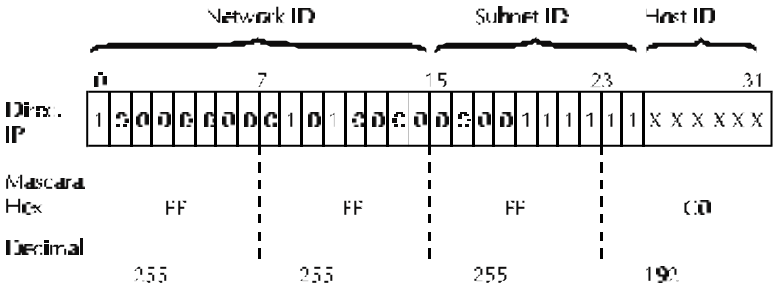
Subnet masks identify the portion of the address occupied by the **netid** field and the **subnetid** field. The mask is simply another 32 bits string written in dotted decimal notation with all ones in the **netid** and **subnetid** portion of the address and with all zeros in the **hostid** portion of the address.

For example, suppose you have a class B address. You want to assign the first 8 bits of the **hostid** as the **subnetid** leaving the new **hostid** with 8 bits only. Following the rule of placing all ones in the **netid** and **subnetid** fields and all zeros in the rest, you get the following mask:

255.255.255.0



The **subnetid** can consist of any number of host field bits that do not have to be multiples of eight as it was in the previous example. For example, you may want to assign the first ten bits of the **hostid** as the **subnetid**. This would create a mask of 255.255.255.192.



You should use three or more bits for a **subnetid**. A **subnetid** of two bits yields only four subnets, two of which (11 and 00) are reserved.

The **Teldat Router** IP implementation supports variable length subnets. This feature allows you to divide the **hostid** of a single IP network number into many variable sized subnets.

> ***Note: It is impossible to use different size subnetid when using RIP-1. In this case you must use OSPF or configure RIP-2.***

CAUTION: Assign variable length subnets with care. If you assign a subnet in an overlapping fashion, problems may occur.

1.5. IP Routing

IP uses routing tables to decide where to send each datagram. The routing table is a list of all the network segments that router knows how to reach. The routing table contains both dynamic and static routes.

A dynamic route is one that is learned through routing protocols such as OSPF and RIP. These protocols regularly update their routing tables as network conditions change. Dynamic routing allows the router to transmit datagrams around network failures.

A static route is a route that never changes. You must enter a static route when configuring IP. Static routes persist across power downs, restarts, and software reloads. They are used when the router for some reason cannot determine the correct dynamic route.

IP routing happens as follows:

- IP receives the packet and reads the 32 bit destination address found within the packet header.
- If the packet is destined for this router, further routing is not necessary and IP hands the packet to the appropriate internal software module. Packets in this category include the following:
    - Control packets for IP itself
    - Routing update packets
    - Packets used for diagnostics purposes
- If the packet is destined for a host connected to the same physical segment of one of the router ports, IP searches for the physical address associated to the datagram destination IP address and hands the packet to the appropriate lower level protocol module for transmission to the final destination. The physical address associated to the IP address is kept in a table through the ARP protocol.
- If the packet is destined for a host on a remote network segment, IP uses the routing table to determine the address of the next hop. Each entry in the routing table contains a destination address and the IP address of the next hop router. If IP matches the destination address in the table with the destination contained in the packet, the packet is handed to the appropriate lower level protocol module for transmission to that next hop.
- If the packet has no entry for its IP address in the routing table, the packet is routed to the default router. A default router is one of the parameters configured in the IP protocol and used to route datagrams whose destination address is not found in the routing table. This router is assumed to know the location of the packet's destination.

IP also performs several other major tasks: as faulty packets deletion or several filtering types.

a) Default Router

A default router knows how to route packets that other routers cannot route. There are two kinds of default routers:

- Default network router

Performs routing for other routers on an Internet that has packet traffic for an unknown-network destination.

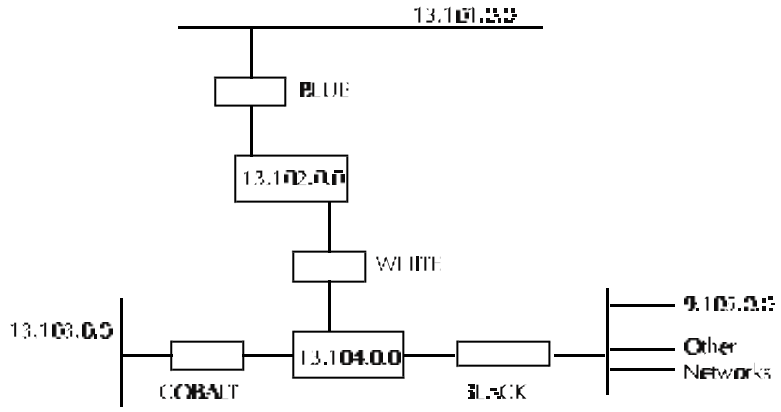
The default network route can be manually configured as a static route or can be dynamically learnt by using the RIP or OSPF protocols. Both protocols represent the default network route as destination 0.0.0.0.

- Default subnet router

Routes the traffic directed to a destination subnet so that other routers do not have specific routing information.

The default subnet route can be configured as a static route or can be dynamically learnt. The destination of this type of route is the network. This has been divided into subnets and the mask specifies which class the network belongs to (A, B or C).

In the next Figure the network segments are 13.101.0.0, 13.102.0.0, 13.103.0.0, 13.104.0.0 and 9.105.0.0. The routers are BLUE, WHITE, COBALT and BLACK. In this case BLACK is the default network router because it has knowledge of network 13 and any other networks. Network 13 routers do not have any knowledge of networks outside network 13.



On the network segment 13.104, unknown network traffic goes first to router BLACK then towards the appropriate destination (next hop).

b) Faulty Packets

The router will drop packets that are incorrectly formatted or have an improper destination address to ensure that these packets are not forwarded further into the network.

c) Router ID

The router ID becomes the source IP address in all locally originated IP packets that are sent over multicast lines. Also the router ID is used as the OSPF router ID.

d) Internal IP address

The internal IP address is an address that belongs to the router as a whole, and not any particular interface. It is used only in situations where the router needs to be assured of always having at least one address available.

If the internal IP address is set and the router ID is also set, the internal IP address takes precedence over the router ID. The internal IP address is used as the OSPF router ID.

e) Management IP address

Address used by the router to fill out the network address field in the SNMP traps. If this is not configured, the router uses the internal IP address. If this not configured either, the field is filled out to 0.0.0.0.

In the source IP address field, the IP packets transporting the traps use the internal IP address. If however the management IP address is configured this one will be used. If neither of these is configured, the packet output interface IP address is used.

f) Broadcast Packets

A broadcast message is one that is destined for all hosts on the given network. IP occasionally sends broadcast addresses on its own behalf. These broadcast messages are used, among other things, to update the IP routing tables on other routers when running RIP-1 or RIP-2. The router never forward broadcast packets.

NOTE: When configuring the router's broadcast address, all nodes or systems on the wire MUST use the same broadcast format.

To indicate that a packet is a broadcast packet (intended for all hosts), the senders sets the packet's IP destination address to the currently used broadcast address. The broadcast style that you configure is either a LOCAL WIRE broadcast or NETWORK broadcast that uses a fill pattern of all "0" or all "1". During a LOCAL WIRE broadcast the entire destination IP address field is filled with "0" or "1" depending on how the fill pattern has been programmed. During a NETWORK broadcast only the **hostid** is filled with the pattern.

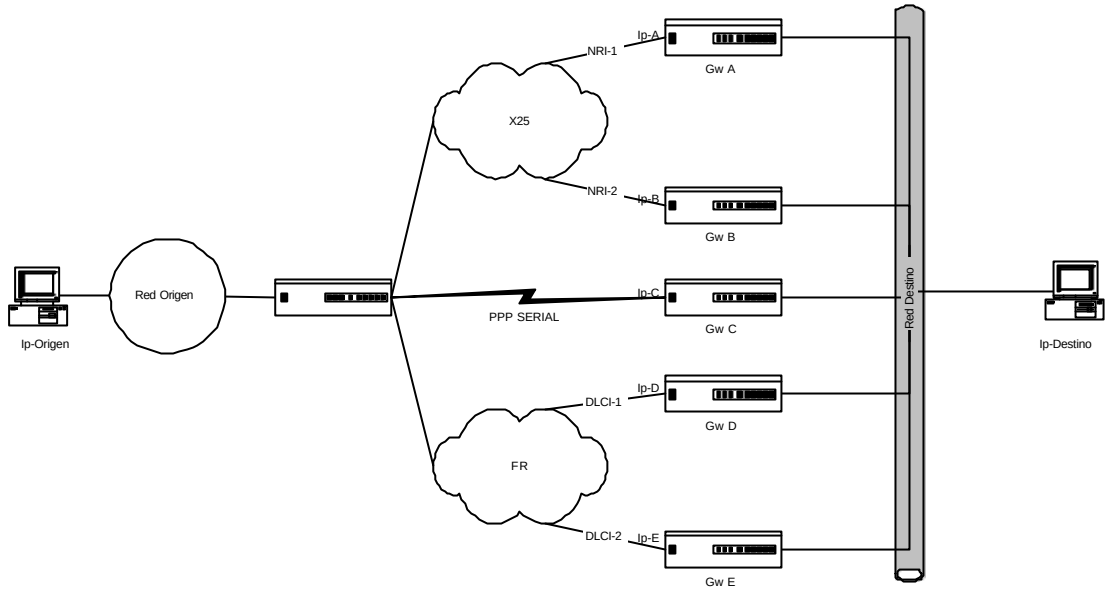
g) Receiving IP broadcasts

The IP recognizes all forms of broadcast messages and addressing. If the network portion of the broadcast address indicates either local wire or a directly connected IP network, IP treats the packet as if it is addressed to itself.

IP also forwards directed broadcasts. A directed broadcast is a broadcast destined for networks other than the networks on which it originated. By enabling IPs directed broadcast feature, you can forward IP packets whose destination is a non-local broadcast address.

h) Multicast Packets

You can configure 2 or more routes in IP protocol, towards the same destination network through the distinct sequential hops.



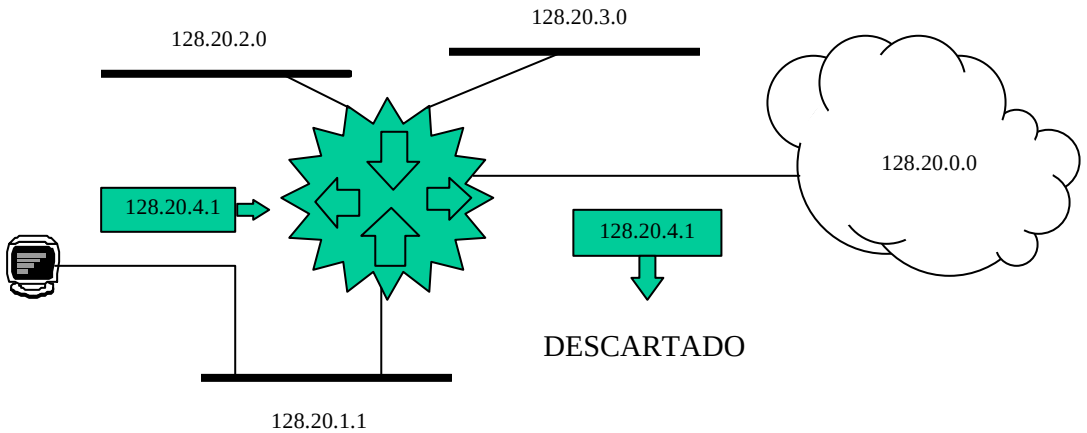
In the previous figure you can see the possibility of forwarding to the IP destination address through various distinct gateways (Gw).

The routes can be static or learnt through the dynamic routing protocol. This accepts the possibility of multipaths. (OSPF).

If two or more routes agree i.e. they cost the same, the outbound interface is active and the 'per packet Multipath IP flag' is enabled, there is a balance of traffic (up to a maximum of 4 routes). If the flag is not enabled then the traffic is not balanced.

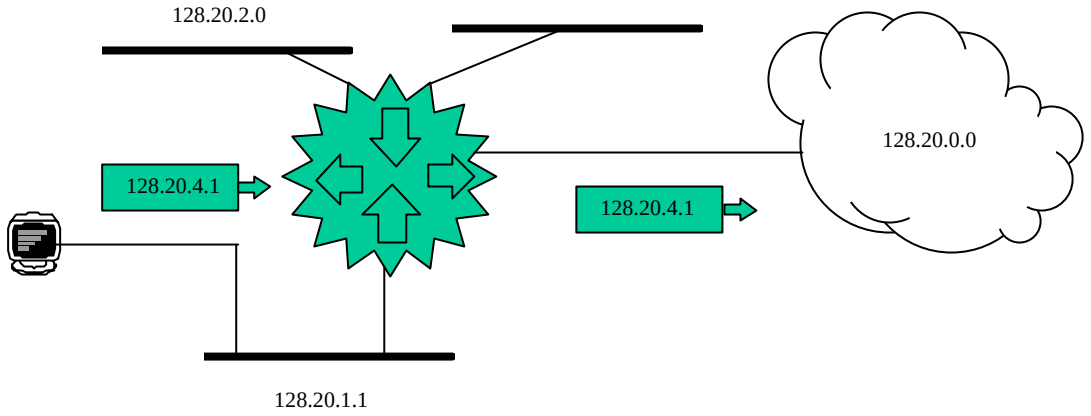
i) IP classless

A router may receive packets destined for a network subnet which does not have a subnet router configured by default. The following figure displays a router belonging to the 128.20.0.0 network and connected to the 128.20.1.0, 128.20.2.0, and 128.20.3.0 subnets. E.g. the host sends packets towards 128.3.4.1. If the router receives packets by default, destined to a subnet to which it is not directly connected and that doesn't possess a subnet default route, the router discards the packet.



IP classless feature disabled

In the following figure, the IP classless function is enabled in the router. So when the host forwards a packet destined to the 128.3.4.1 subnet, the router forwards it to the best supernet route (this is a route with a less restrictive mask which encompasses the destination network) instead of discarding it. As a last resort, the packet is sent to the network default route in cases where this is configured (network route 0.0.0.0 which is the supernet encompassing all networks).



IP classless feature enabled

j) Access Control

This feature allows you to control the forwarding of packets by examining the IP datagram masked source and masked destination addresses in the header, the protocol type in the IP header, or the port number in cases where the two protocols used are TCP or UDP.

After enabling access control, any packet that the router receives is matched to the control list before being matched to the routing table.

There are two types of entries in the access control list, inclusive and exclusive. If an address matches an inclusive entry, the packet is forwarded. If an address matches an exclusive entry, the packet is dropped. If no match exists, the packet is also dropped.

Beware when using access controls. Packets originated by the router are also subjected to access controls before being forwarded. Specifically do not filter out any RIP or OSPF packets being sent or received by the router. You can use the wild card inclusive entry as the last entry in the access control list, or explicitly include them.

k) Address Translation (NAT)

The NAT feature (Network Address Translation) allows an IP network of a company to appear to the other IP networks to be using an addressing space different to its internal one. I.e. NAT permits a company using private addresses (local addresses) which cannot be accessed by the Internet routing table, connect to Internet when these addresses are converted to public ones (global addresses) and are accessible from Internet. NAT also permits companies to set up re addressing strategies where the changes in the local IP networks are minimum. NAT is described in the RFC 1631.

The router supports the NAT feature. For further information please see the manual Dm 720-I.

1.6. Interior Gateway Protocol

Routers that use a common routing protocol form an *autonomous system* (AS). This common routing protocol is called an Interior Gateway Protocol (IGP). IGPs dynamically detect network reachability and routing information within an AS and use this information to build the IP routing table.

Internet's most extended routing protocols are RIP and OSPF. With these protocols total compatibility is assured with the rest of the routers available on the market.

RIP (Routing Information Protocol) is based on the distance vector algorithm. Its easy handling and robustness make it suitable for simple networks configurations.

OSPF (Open Shortest Path First) is based on link state technology and is the right solution for complex networks, where responsiveness and decreased bandwidth requirements are essential.

The router can simultaneously run RIP and OSPF.

Chapter 2
Configuration

1. IP Configuration

This section outlines the initial steps required to configure IP protocol. After completing these tasks, you must save the configuration and restart the router for the new configuration to take effect. The following sections describe each configuration task in more detail.

- Accessing the IP configuration environment.
- Assigning IP addresses to the network interfaces.
- Enabling dynamic routing.
- Adding static routing information.
- Configuring IP access control.
- Configuring NAT.
- Configuring NAPT.
- Configuring IPSEC.
- Configuring Policy Routing.

1.1. Accessing the IP Configuration Environment

To access the IP configuration environment, enter the following command:

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

1.2. Assigning IP Addresses to Network interfaces

Use the IP configuration **ADDRESS** command to assign IP addresses to the network hardware interfaces. The arguments for this command include the interface name (obtained from the **LIST DEVICES** command) and the IP address and its associated address mask.

In the following example, network interface ethernet0/0 is assigned address 128.185.123.22 with mask 255.255.255.0 (using the third byte for subnetting).

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

1.3. Enabling Dynamic Routing

Use the following procedure to enable dynamic routing on the router. The router supports OSPF and RIP for Interior Routing Protocols.

These two routing protocols can run simultaneously. However, most routers will probably run only one of them. The OSPF protocol is recommended because of its robustness and the additional IP features that it supports.

1.4. Adding Static Routing Information

This procedure is necessary only if you cannot gain routing information from any of the previous dynamic routing protocols.

Static routing persists over power failures and is used for routes that never change or are not able to be learned dynamically. Static routing information consists of any of the following items:

***Default Router**:* Packets are routed to default routers when the packet destination cannot be found in the routing table.

***Default Subnet Router**:* If you are using subnetted networks, you can define a separate default router for each subnetted network.

***Static Routes**:* For each destination that is to have a fixed route, configure the next hop address and destination.

***Aggregation routes**:* When you have a number of routes with the destination addresses beginning with the same numeration, defining an aggregation route can be convenient: i.e. a route that encompasses all the previous ones. In this way, the dynamic route protocols, configured only to announce the aggregated routes do not overload the routing tables of other routers with unnecessary information. The aggregation route is not really a route; it is a mark which appears in the active routes table indicating that a series of aggregated routes exist.

Multipath: Routes to the same destination can be configured through the distinct sequential hops at an equal or different cost. If the cost is equal, and the multipath is enabled, the traffic is balanced.

a) Default Routers

Routers send packets having unknown IP addresses (i.e., destinations not present in the routing table) toward the default router.

A default router is configured by specifying the next hop to use to get to the default router and the cost of sending packets to the default router. You can configure as many routers by default as you wish assigning each a cost. The cheapest accessible router is activated. If two or more routes (up to a maximum of four) are activated at the same time and providing the multipath feature is enabled, traffic balance is carried out.

In the following example, the next hop toward the default router is 130.1.1.191 and the cost of sending a packet to the default router is 1.

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

Default routers can be learned and advertised by both the OSPF and RIP protocol. For the OSPF protocol, a router can be configured to advertise itself as the default router.

The RIP protocol can be configured so that it will advertise knowledge of the default router (if it has any) to its neighbors.

RIP can also be configured so that a learned default router will (or will not) override a statically configured default router.

b) Default Subnet Routers

There can be a default subnet router configured for each subnetted network that the router knows about. You can configure as many routers by default as you wish, assigning each a cost. The cheapest accessible router is activated. If two or more routes (up to a maximum of four) are activated at the same time and provided the multipath feature is enabled, then traffic balance is carried out. When the router attempts to forward a packet to a destination belonging to the subnetted network, but that destination cannot be found in the routing table, the packet is forwarded instead to the default subnet router.

Configuring default subnet routers is the same as configuring the above default network routers. The only difference is that you must specify the subnetted network on the command line. For example, if you have an interface configured with a subnet address 18.0.0.6 this means that the router belongs to the subnetted network with identifier 18.0.0.0. To create a default subnet router for this subnetted network, you could use the following command:

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

The above example specifies that the next hop to the subnet default router is 130.1.1.191, and that the cost of routing a packet to the default subnet router is 1.

c) Static Network / Subnet Routes

Configure static routes for those destinations that cannot be discovered by the dynamic routing protocols. The destination is described by the IP network address and the destination's address mask. The route to the destination is described by the IP address of the first hop router to use and the cost of routing a packet to the destination. You can configure various static routes to the same destination with distinct sequential hops and at an equal or different cost. If two or more routes (up to a maximum of four) are activated at the same time and providing the multipath feature is enabled, traffic balance is carried out. To create or delete static routes, use the commands:

```
IP config>route <net or subnet or host, mask, hop, cost>
IP config>no route <IP-destination-address, mask, next hop>
```

Routes dynamically learned through the RIP and/or OSPF protocols can override static routes. For the RIP protocol, you can disable this override behavior.

d) Aggregation Routes

Use the following commands to create and delete aggregation routes.

```
IP config>aggregation-route < net or subnet or host, mask >
IP config>no aggregation-route <IP-destination-address, mask>
```

e) Multipath

You can configure multipath per packet or per source-destination.

In order to configure the multipath per packet, the following steps must be carried out:

- Add a static route to each path. A determined cost is assigned.
- Enable or disable the 'per packet Multipath' IP flag.

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

or

```
IP config>NO MULTIPATH
```

- Configure (or not) the BKUP-RCV-TIME parameters of the X.25 Node's global variables. (See X.25 manual Dm 707-I).

Case of generic outbound interface

- The lower cost static route and active interface begin functioning.
- If two or more routes coincide in having minimum costs, an active outbound interface and the 'per packet Multipath IP flag' is enabled, traffic balance is carried out (up to maximum of 4 paths). If the flag is not enabled, traffic balance is not carried out.
- If the interface drops or activates, the static routes are rechecked so the cheapest operates with the active interface.
- Check the specific cases of FR (dlci), X.25 (NN routes) and Dial interfaces.

FR outbound interface

- Static routes that have an FR outbound interface always activates the lowest cost route that has an active interface and the dlci, to which the next hop is associated, is active. The activity or inactivity of the dlci depends on the LMI.
- If one of the above conditions is not complied with, this is deactivated.

X25 outbound interface

Static routes that have an X.25 outbound interface always activate the lowest cost route that has an active interface and the NN, to which the next hop is associated, is active. The activity or inactivity of the NN depends on the following points.

- If the BKUP-RCV-TIME parameter has a 0 value, the NN are always active. This means that the static routes associated with it, provided they are low cost, are always active.
- If the BKUP-RCV-TIME parameter has a different value to 0:
    1. When you start the router, all the NN are active.
    2. If a packet is forwarded to the following hop, a call is provoked.
    3. If the call is established, the NN is activated. (go to 2).
    4. If the call is not established, the NN is deactivated (together with the associated static route or routes) and a recall procedure is initiated for each BKUP-RCV-TIME.
    5. If the call is established, the NN is reactivated with all the associated static routes. (go to 2).

IMPORTANT: If the BKUP-RCV-TIME parameter is configured with a value other than 0, extra X.25 calls may be carried out provoked by the "Retry to Establish Call Procedure". This could be inconvenient if you do not have a flat rate contract. By configuring 0, you prevent the call retries as the static routes configured for the X.25 remain active.

Dial-PPP and Dial-FR outbound interface

Static routes that have a "Dial" outbound interface always activate when the two following conditions are fulfilled: the lowest cost route that has an active interface. This type of interface is always active; consequently the associated static routes are always active when they are the lowest configured cost.

f) IP Classless

Routing strategies:

- IP Class routing strategy: Suppose a router directly connected to a subnet (10.1.1.0) of a major net 10.0.0.0. If the router receives packets destined for another subnet in the same major network (10.2.1.0) and the router does not have any explicit information on it, despite having a default network route (10.0.0.0/0) if there is no default subnet route configured (10.0.0.0/8) the packet is not forwarded. This is a protective behavior to prevent possible loops.
- Classless routing strategy: all received packets are forwarded to the following hop which indicates the destination route. It is the most restrictive (more 1's in the mask) and at the least cost.

If the "IP Classless routing" is not enabled, the router will route on an "IP class routing strategy" basis.

This operation should be avoided where possible to protect the network from loops. An alternative solution should be sought first e.g.

- No IP classless.
- Add as many subnet default routes as networks divided into subnets exist.

This feature is disabled by default. You can enable or disable by executing the following command:

```
IP config>CLASSLESS
```

or

```
IP config>NO CLASSLESS
```

1.5. IP Access Controls Configuration

The IP access controls allow you to configure packet filters based on source and destination IP addresses, IP protocol number, and source and destination port ranges for the TCP and UDP protocols. This can control access to particular classes of IP addresses and services, as well as restrict the type of permitted traffic depending on the input/output interface.

There are two types of differentiated access controls:

- GLOBAL access controls.
- PER INTERFACE access controls.

a) Global IP access controls

The **globals** IP access controls are based on one global ordered list of inclusive and exclusive access control entries. If access control is enabled, each IP packet being originated, forwarded, or received, is subject to the access control list. Each entry in the list may be inclusive or exclusive, permitting or denying forwarding. Each entry has fields for source and destination IP address, optional IP protocol number, and source and destination ports range (optional for UDP and TCP protocols).

For each received packet, the headers are compared to all specified fields in each entry in the previous list in turn. If the entry matches the packet and the entry is inclusive, the packet is forwarded. If the entry is exclusive, the packet is dropped. Finally if no entry matches after going through the entry list, the packet is dropped.

Each entry has an IP address mask, and the logical operation result pair between the source and destination IP addresses. An address is logically "AND-ed" with the mask, and compared to the result. For example, a mask of 255.0.0.0 with a result of 26.0.0.0 will match any address with 26 in the first byte. A mask of 255.255.255.255 with a result 192.66.66.20 matches only the IP host 192.66.66.20. A mask of 0.0.0.0 with a result of 0.0.0.0 is a wildcard, and matches any IP address.

Each entry may also have an optional IP protocol number range. This applies to the protocol byte in the IP header. Any IP packet with a protocol value within the specified range will match. A range of 0 to 255 matches all IP packets. The commonly used protocol numbers are: 1 for ICMP, 6 for TCP, 8 for EGP, 17 for UDP and 89 for OSPF.

Each entry may also have a range of both source and destination ports. This applies only to TCP and UDP packets, since the port numbers are part of the TCP and UDP headers. Any TCP or UDP packet with a port number within the specified ranges will match. A range of 0 to 65535 disables port filtering as all packets are forwarded. Some commonly used port numbers are: 21 for FTP, 23 for TELNET, 25 for SMTP, 513 for rlogin, 520 for RIP, and 6000 for X. See RCF 1060 "Assigned Numbers" for details on IP protocol and port numbers.

The following example allows any host to send packets to the SMTP TCP socket to IP address 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
```

The next example prevents any host on subnet 150.150.1.X from sending packets to hosts on subnet 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
```

This command allows the router to send or receive all RIP packets

```
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
```

This command allows the router to send or receive all OSPF packets.

```
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
```

Do not forget to add the wildcard entry as the last entry as any packet that does not coincide with any entry will be dropped/filtered: if you enable the IP access control and only wish to filter a determined type of traffic, you need to add the exclusive entry group required to filter this said traffic and add an inclusive wildcard entry as the last entry in order to permit the rest of the traffic.

```
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
```

If you have certain IP networks/subnets that you do not want to forward packets to, nor distribute routing information about, it is best to specify those networks as filters (this is more efficient than access control mechanisms). To add a network filter, use the following command:

```
IP config>filter <destination-IP-address, destination-IP-mask>
```

It is recommendable to filter the local traffic from a 127.0.0.0 network so as not to propagate packets only destined to this network. Use the following command:

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

b) IP per interface access controls

The IP **per interface** access controls are based on the use of generic access control lists. You can define two different access lists for each interface: one to filter inbound traffic and the other to filter outbound traffic. This means that you can restrict the traffic both being sent and received in each interface. If you do not define any access control list then the interface will pass all the packets. If the access list (input or output) allows the packet then this will be processed (inbound traffic) or will be sent by the interface (outbound traffic). If the packet is rejected, this will be dropped and an ICMP Host Unreachable message will be sent.

If you can foresee that a lot of packets are going to be dropped due to the per interface access controls, we recommend disabling the ICMP Unreachable message send to avoid overloading the device.

You can associate "*Standard*" or "*Extended*" access control lists to the interface. In cases of *Standard* lists, only the packets source address are checked. In *Extended* lists, the packets source and destination addresses, protocols, ports etc. are checked (permitting a more detailed specification of the traffic which is permitted or dropped.).

The following example shows how to apply the extended access control list 101 (assuming that this has been previously defined) to inbound packets in the ethernet0/0 interface:

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

In order to restrict traffic leaving the ppp1 interface in compliance with the standard access list 10:

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

1.6. Configuring NAT

For further information please consult the NAT manual Dm 720-I.

1.7. Configuring NAPT

For further information please consult the NAPT manual Dm 735-I.

1.8. Configuring IPSEC

For further information please consult the IPSEC manual Dm 739-I.

1.9. Configuring Policy Routing

For further information please consult the Policy Routing manual Dm 745-I.

Chapter 3
Configuration Commands

1. IP Protocol Configuration Commands

This section summarizes and then explains all router configuration commands. These commands allow you to configure the behavior of the router's IP protocols to meet your specific operation requirements.

Enter IP configuration commands at the prompt: IP config>, to access this prompt you must enter:

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

Command	Function
? (HELP)	List all the commands or their options.
ACCESS-CONTROL	Configures entries in the GLOBAL access controls list.
ACCESS-GROUP	Configures the PER INTERFACE access controls.
ADDRESS	Configures IP addresses in the interfaces.
AGGREGATION-ROUTE	Configures aggregation information.
BROADCAST-ADDRESS	Specifies the broadcast addresses format used by the router for a determined interface.
CLASSLESS	Enables IP "Classless Routing Strategy".
DIRECTED-BROADCAST	Enables forwarding of IP packets with destination to a non-local network broadcast address.
DNS-DOMAIN-NAME	Configures the DNS domain name.
FILTER	Configures IP filters.
ICMP-REDIRECTS	Enables forwarding of icmp redirects packets.
ICMP-UNREACHABLES	Enables the sending of icmp unreachables packets.
INTERNAL-IP-ADDRESS	Configures the router's internal IP address.
IP-PARAM	Configures other IP parameters.
IPSEC	Enters the IPSEC configuration menus.
LIST	Lists the IP elements configuration.
LOCAL	Configures functionalities associated to the local traffic.
MANAGEMENT-IP-ADDRESS	Configures the router's management IP address.
MULTIPATH	Enables the multipath.
NAT	Enters the NAT facility configuration menus.
NO	Deletes a previously added IP configuration parameter or re-establishes its default value.
POLICY	Enables Policy Routing in an interface.
POOL	Configures the range of addresses that the router can assign through its PPP connections.
PROXY-ARP	Enters the Proxy ARP configuration menus.
ROUTE	Configures IP routes.
ROUTER-ID	Configures the default IP address that the router will use in locally originated packets. This will also become OSPF protocol 1 router-ID.

RULE	Configures IP connections.
TVRP	Enters the TVRP protocol configuration menus.
EXIT	Exits the IP configuration.

1.1. ? (HELP)

Use the **?** (HELP) command to list the commands that are available from the level where the router is programmed. You can also enter this command after a specific command to list its available options.

Syntax:

```
IP config>?
```

Example:

```
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

Through this command you can configure the IP protocol access GLOBAL control system.

Syntax:

```
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

Enables the access control system. By default the IP protocol access control system is disabled.

Syntax:

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

Example:

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

In order to disable this, execute the same command preceded with the word "NO".

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

b) ACCESS-CONTROL ENTRY

Configures an entry in the access controls list. This allows you to specify the packet class that requires forwarding or dropping, depending on the type of entry. The length and order of the IP access control list can affect the performance of the IP forwarder.

Each entry contains the following fields: type, source IP, source IP Mask, destination IP, destination IP mask. The type can be inclusive or exclusive. The source and destination IP addresses are introduced in dotted decimal format. Optionally you can specify a range of IP protocols and you can indicate a range of TCP and UDP ports both at source as well as destination.

Syntax:

```
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: Creates an entry in the access controls list with identifier <id> and the default values. If this already exists the values are given by default.

Destination: Configures the IP network and the range of entry destination ports with <id> identifier.

Exclusive: Changes the entry with identifier <id> to exclusive mode.

Inclusive: Changes the entry with identifier <id> to inclusive mode.

Protocol-range: Configures the entry protocols range with identifier <id>.

Source: Configures the IP network and the entry range of source ports with identifier <id>.

Example:

```
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>
```

In order to delete an entry, execute the same command putting "NO" before the said command.

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

c) ACCESS-CONTROL MOVE

Use the **ACCESS-CONTROL MOVE** command to change the order of the access control list. This command places the register *from#* immediately after *to#*. After you move the register, they are immediately renumbered to reflect the new order.

Syntax:

```
IP config>ACCESS-CONTROL MOVE <from# to#>
```

Example:

```
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

Through this command you configure the IP protocol access control system PER INTERFACE.

Syntax:

```
IP config>ACCESS-GROUP <interface> <access list>
in     inbound packets
out    outbound packets
```

In: Applies the generic access control list to traffic coming in through a specified interface.

Out: Applies the generic access control list to traffic leaving through a specified interface.

Example:

```
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>
```

To eliminate a per interface access control, use the same command preceded by the word "NO".

Example:

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

1.4. ADDRESS

Assigns an IP address to one of the router interfaces. A hardware interface will not receive or transmit IP packets until it has at least one IP address.

You must specify an IP address together with its subnet mask. For example, if the address is on a class B network, using the third byte for subnetting, the mask would be 255.255.255.0. Use the **LIST DEVICES** command to obtain the names of each interface.

Syntax:

```
IP config>ADDRESS <interface, IP-address, IP-mask>
```

Example:

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

To delete an address, use the same command preceded by the word "NO".

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

A point-to-point type interface can be configured as unnumbered through this command. Introduce "unnumbered" instead of the IP-address and IP-mask for this.

Syntax:

```
IP config>ADDRESS <interface> unnumbered
```

Example:

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

To delete an address, use the same command preceded by the word "NO".

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

1.5. AGGREGATION-ROUTE

This adds IP aggregation information to the routing table.

The aggregation route is specified through an IP address (Network, Subnet, Host) and a mask.

Syntax:

```
IP config>AGGREGATION-ROUTE <net or subnet or host, mask>
```

Example:

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

To delete an aggregation routes, use the same command preceded by the word "NO".

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

1.6. BROADCAST-ADDRESS

Specifies the IP broadcast format that the router uses for a determined interface. IP broadcast packets are most commonly used by the router when sending RIP update table packets.

The *style address* parameter can take either the value LOCAL-WIRE or NETWORK. LOCAL-WIRE broadcast addresses are either all ones (255.255.255.255) or all zeros (0.0.0.0). NETWORK style broadcast begin with the network and subnet portion of the IP-interface-address.

You can set the *fill-pattern for wildcard part* parameter to either 1 or 0. This indicates whether the rest of the broadcast address (i.e., other than the network and subnet portions, if any) should be set to all ones or zeros.

By default the address type is NETWORK and the fill pattern is 0.

When receiving the router recognizes all forms of the IP broadcast address.

Syntax:

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

a) BROADCAST-ADDRESS LOCAL-WIRE

Through this command you can configure the *style address* as LOCAL-WIRE. The LOCAL-WIRE broadcast addresses are all ones (255.255.255.255) or all zeros (0.0.0.0). The fill pattern for broadcast can be 0 or 1.

Syntax:

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

The following example configures a broadcast address 255.255.255.255.

Example:

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

To return to the command default configuration, execute the same command preceded with the word "NO".

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

b) BROADCAST-ADDRESS NETWORK

Through this command you can configure the *style address* as NETWORK. The NETWORK type addresses begin with the network number subnet number of the interface. The *fill-pattern for wildcards* can be 0 or 1. This indicates how to fill out the rest of the broadcast address (except network and subnet) with either ones or zeros.

Syntax:

```
IP config>BROADCAST-ADDRESS NETWORK <address, fill-pattern>
```

The following example configures a broadcast address 192.7.1.255.

Example:

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

To return to the command default configuration, execute the same command preceded with the word "NO".

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

1.7. CLASSLESS

Enables the IP routing strategy "Classless Routing Strategy".

Syntax:

```
IP config>CLASSLESS
```

Example:

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

To disable this, use the same command preceded by the word "NO".

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

1.8. DIRECTED-BROADCAST

Enables the forwarding of IP packets whose destination is non-local (e.g., remote LAN) broadcast address. The packet is originated by the source host as a unicast where it is then forwarded as a unicast to a destination subnet and "exploded" into a broadcast.

This class of packets can be used to locate network servers in remote networks. The IP packet forwarder never forwards link level broadcast/multicast, unless they correspond to Class D IP address. The default setting for this feature is enabled.

Syntax:

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

Example:

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

To disable this, use the same command preceded by the word "NO".

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

1.9. DNS-DOMAIN-NAME

Establishes the domain name.

Syntax:

```
IP config>DNS-DOMAIN-NAME <domain-name>
```

Example:

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

To delete this, use the same command preceded by the word "NO".

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

1.10. FILTER

Designates a filter for an IP network/subnet. IP packets that comply with the filter conditions will not be forwarded and are simply discarded.

You must specify the network filter together with the subnet mask to filter an IP packet. For example, to filter a subnet of a class B network, using the third byte for subnetting, the mask would be 255.255.255.0.

Using the filter mechanism is more efficient than IP access controls, although not as flexible.

Syntax:

```
IP config>FILTER <destination-IP-address, destination-IP-mask>
```

Example:

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

To delete a filter, use the same command preceded by the word "NO".

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

1.11. ICMP-REDIRECTS

Enables the sending of ICMP redirects packets. By default this is enabled.

Syntax:

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

Example:

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

To disable this, use the same command preceded by the word "NO".

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

1.12. ICMP-UNREACHABLESS

Enables the sending of ICMP Unreachables packets. This is enabled by default.

Syntax:

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

Example:

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

To disable this, use the same command preceded by the word "NO".

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

1.13. INTERNAL-IP-ADDRESS

Sets the internal IP address that belongs to the router as a whole, and not any particular interface. This address is always reachable regardless of the state of the interface. When the internal IP address and the router ID are set in the same router, the internal IP address has precedence over the router ID.

Syntax:

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

Example:

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

To delete the internal IP address, use the same command preceded by the word "NO".

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

1.14. IP-PARAM

Use the **IP-PARAM** command to set certain IP protocol parameters depending on the option selected.

Syntax:

```
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

Configures the maximum number of entries for the IP routing cache.

Syntax:

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

Example:

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

The default value is 64. To return to the default value, execute the same command preceded by the word "NO".

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

b) IP-PARAM REASSEMBLY-SIZE

Configures the size of the buffers that are used for the reassembly of fragmented IP packets. The default value is 12,000.

Syntax:

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

Example:

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

To return to the default value, execute the same command preceded by the word "NO".

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

c) IP-PARAM ROUTING-TABLE-SIZE

Sets the size of the IP routing table. The default size is 768 entries. Setting the routing table size to small causes dynamic routing information to be discarded. Setting the routing table size too large wastes router memory resources.

Syntax:

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

Example:

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

To return to the default value, execute the same command preceded by the word "NO".

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

1.15. IPSEC

Access the IPSEC configuration menus through this command. See the IPSEC manual Dm 739-I.

Syntax:

```
IP config>IPSEC
```

Example:

```
IP config>IPSec
IPSec user configuration
IPSec config>
```

1.16. LIST

The LIST command is used to view the various IP configuration parameters depending on the selected option.

Syntax:

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

a) LIST ACCESS-CONTROLS

Displays the configured access control mode (inclusive, exclusive, or disabled), and the list of configured GLOBAL access control records. Each record is listed with its record number. This record number can be used to reorder the list with the **ACCESS-CONTROL MOVE** command.

Syntax:

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

Example:

```
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

Displays the PER INTERFACE access controls. The access control lists assigned to inbound and outbound traffic are displayed for each interface ("**0**" means that there is NO associated access list.)

Syntax:

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

Example:

```
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

Displays all the IP interface addresses for each interface as well as the broadcast address format.

Syntax:

```
IP config>LIST ADDRESSES
```

Example:

```
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

Displays all the IP configuration.

Syntax:

```
IP config>LIST ALL
```

Example:

```
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

Displays the domain name, configured through the IP configuration menu with the **DNS-DOMAIN-NAME** command. This also displays the FQDN which identifies the device through the domain name and the host name configured through the router's general configuration menu with the **SET HOSTNAME** command.

Syntax:

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

Example:

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

f) LIST IP-PARAM

Displays information on various IP parameters: routing table size, reassembly buffer size and the routes cache size.

Syntax:

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

Example:

```
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

Displays the configuration for the routing protocols (RIP and OSPF), classless, multipath and other ICMP parameters.

Syntax:

```
IP config>LIST PROTOCOLS
```

Example:

```
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

Displays information on Policy Routing (please see the Policy Based Routing manual, Dm 745-I.

i) LIST POOL

Displays the range making up the address pool established in the router.

Syntax:

```
IP config>LIST POOL
```

Example:

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

j) LIST ROUTES

Displays the list of static network/subnet routes that have been configured and also lists any configured default router. This also displays the configured aggregation routes.

Syntax:

```
IP config>LIST ROUTES
```

Example:

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

k) LIST RULE

The **LIST RULE** command displays the defined IP connections.

Syntax:

```
IP config>LIST RULE
```

Example:

```
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

Permits you to configure various functionalities related to the local traffic (with the router itself being source or destination).

Syntax:

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

a) LOCAL ACCESS-GROUP

Through this command you can configure the access control system for local traffic. Access to the distinct router services can be restricted (telnet, ftp, etc) independently of the inbound interface.

Syntax:

```
IP config>LOCAL ACCESS-GROUP <access list>
in     inbound packets
```

In: Applies the generic access control list to the local inbound traffic.

Example:

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

In order to return to the default configuration for this command, execute the same command preceded by the word "NO".

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

b) LOCAL POLICY

Through this command you can enable the Policy Routing for the local traffic. For further information please see the Policy Based Routing manual Dm 745-I.

Example:

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

1.18. MULTIPATH

If this command is enabled, in cases where multiple paths exist in order to reach an equal cost destination, the router will choose the path to route the packet complying with the following criteria: a circular queue (Round-Robin mode), or depending on the destination. This command is disabled by default.

Syntax:

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

Example:

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

To disable this, use the same command preceded by the word "NO".

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

1.19. NAT

Through this command you can access the NAT facility configuration menus.

Syntax:

```
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

Through this command you can access the DNAT configuration menus.

Syntax:

```
IP config>NAT DYNAMIC
```

Example:

```
IP config>nat dynamic

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

b) NAT PAT

Access the NAPT feature configuration menus through this command. For further details, please see the NAPT facility manual Dm 735-I.

Syntax:

```
IP config>NAT PAT
```

Example:

```
IP config>nat pat

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

c) NAT STATIC

You can access the static NAT facility configuration menus through this command. For further details please consult the static NAT facility manual Dm 720-I.

Syntax:

```
IP config>NAT STATIC
```

Example:

```
IP config>nat static

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

1.20. NO

Command used to negate another command or to restore the default configuration for a determined parameter.

Syntax:

```
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>
```

In the section for each of the commands that can be preceded by the word "NO", an explanation on how this affects operations has been given together with an example. Therefore in order to know how "NO" affects the said command, please see the appropriate section on this for each command.

1.21. POLICY

You can enable Policy Routing in the interfaces through this command. Please see the Policy Based Routing manual, Dm 745-I.

Syntax:

```
IP config>POLICY <interface> route-map <name>
```

1.22. POOL

Sets a range of addresses that the router can assign through its PPP connections. The default range consists of IP addresses between 192.168.0.0 and 192.168.255.255.

Syntax:

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

Example:

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

To re-establish the default POOL configuration, execute the same command preceded by the word "NO".

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

1.23. PROXY-ARP

You can access the ARP Proxy configuration menus through this command. For further information relative to the ARP Proxy configuration, consult the associated manual Dm 734-I.

Syntax:

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

Example:

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

Proxy ARP cnfg>
```

1.24. ROUTE

Adds a static network/subnet IP routes to the routing table.

The destination is specified by an IP address (Network, Subnet, Host) together with a mask. For example, if the destination is a subnet of a class B network, and the third byte of the IP address is used as the subnet portion, the address mask would be set to 255.255.255.0.

The route to the destination is specified by the IP address of the next-hop, and the cost of routing the packet to the destination. The next hop must be on the same (sub)net as one of the router's interfaces.

Syntax:

```
IP config>ROUTE <net or subnet or host, mask, hop, cost>
```

Example:

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

To delete a static route, use the same command preceded by the word "NO".

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

1.25. ROUTER-ID

Sets the default IP address used by the router when generating various kinds of IP traffic. This address is of particular importance in multicasting. For example the source address in pings (including multicast pings), traceroute, and tftp packets sent by the router take the router-ID address. In addition, the OSPF protocol router ID coincides with the configured router ID.

The router ID must match one of the configured IP interface addresses of the router. If not, it is ignored. When ignored, or the router's default IP address is simply not configured nor its OSPF router-ID, then the router-ID coincides with the first IP address configured in the router.

Note: Configuring a router-ID may cause the router's OSPF protocol router ID to change. If this happens, link state messages originated by the router before the router ID change persist until they time-out, possibly as long as 30 minutes. This may cause an increase in link state database size.

Syntax:

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

Example:

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

To delete the **ROUTER-ID** command, use the same command preceded by the word "NO".

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

1.26. RULE

Through this command IP connections subsequently used in the NAPT facility and in the IPSEC protocol are created.

An IP connection is an extension to the interface concept; this enables you to define point-to-point subinterfaces without having to create them. A point-to-multipoint interface can have more than one IP connection. A point-to-point interface can only have one associated IP connection.

In point-to-point interfaces the local IP address is sufficient to define the IP connection. E.g. a PPP interface.

In point-to multipoint interfaces, you need to specify the remote IP address as well as the local IP address. E.g. in an FR interface defined as point-to-multipoint which has "Ia1" as source address and through the dlci 16 reaches the "Ia2" and through 17 reaches "Ia3" you can define 2 IP connections, the first "Ia1-Ia2" and the second "Ia1-Ia3".

A rule as well as defining an IP connection, an NAPT configuration can also be associated.

On aggregating a rule you must define the following interfaces:

Identifier: This is the rule identifier subsequently used in NAPT and IPSEC configuration.

Local IP Address: Interface address corresponding to the device going to execute NAPT. This is the address used to execute NAPT if the NAPT address is not configured (see below).

Remote IP Address: In Point to Multipoint links (e.g. Frame Relay) you can define this field to identify which link has received or is going to send the packet and if NAPT is to be executed or not. This can be left as 0.0.0.0 i.e. NAT will be applied over the whole of the interface (e.g. over all the dlcis of this interface).

If the link is Point-to-Point (e.g. PPP) you know that this address must pertain to the same subnet as the local address, therefore it is unnecessary to define this provided that the connection is Point-to Point.

Enable NAPT: Permits you to specify whether to enable NAPT for the added rule. If this is enabled, you must specify the following parameters relative to NAPT.

NAPT Address: If this address is configured it will be used to execute NAPT instead of the interface Local IP address. If you maintain the default value (0.0.0.0), the interface Local IP address will be used to carry out NAT.

NAPT entry timer: This is the time in minutes that the entry in the translation ports table being used in this connection will remain occupied. I.e. the time in minutes that the NAPT entry will remain active during the connection.

Firewalling capacity: This ensures that the device will be inaccessible for the connection defined in this rule except through the translation ports table entries or through the NAPT exceptions referent to this rule.

Ajust MSS: This option allows you to alter the MSS value of TCP SYN packets, to control the maximum size for that connection (usually limiting it to your outgoing interface's MTU minus 40).

Access Control List: Through a generic access list, this permits you to select the IP traffic where NAPT is going to be carried out.

Syntax:

```
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: Creates a rule with identifier <id> and the default values. If this already exists then the default values are established.

No: Disables firewalling or NAPT in the rule whose identifier is <id>.

Local-ip: Configures the rule's local IP address whose identifier is <id>.

Napt : Configures the rule's NAPT parameters whose identifier is <id>.

Remote-ip: Configures the rule's remote IP address whose identifier is <id>.

Example:

To create the IP address with local address 213.4.21.187 and remote address 213.4.21.188 and to also enable NAPT and 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>
```

To delete a rule, execute the same command preceded by the word "NO".

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

1.27. TVRP

You can access the TVRP protocol configuration menus through this command. For further information on this protocol please consult the TVRP Protocol manual Dm 725-I.

Syntax:

```
IP config>TVRP
```

Example:

```
IP config>tvrp
TVRP Configuration

TVRP config>
```

1.28. EXIT

Use the **EXIT** command to return to the previous prompt level.

Syntax:

```
IP config>EXIT
```

Example:

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

Chapter 4
Monitoring

1. IP Protocol Monitoring Commands

This section summarizes and then explains all router monitoring commands. These commands allow you to monitor the router's IP protocol behavior to meet your specific requirements.

Enter IP monitoring commands at the IP prompt: IP>, to access this prompt you must enter:

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

Command	Function
? (HELP)	Lists all the commands and associated options.
AGGREGATION-ROUTE	Displays the aggregation routes that have been configured.
ACCESS controls	List the IP access control mode, together with the configured access control records.
BPING	Carries out ping to each host in a specified network. This is also known as ping broadcast.
CACHE	Displays the routing table.
COUNTERS	List various IP statistics, including the routing errors and packets dropped counters.
DUMP routing tables	Lists the routing table.
INTERFACE addresses	Lists the router's IP interface addresses.
IPSEC	Accesses the IPSEC monitoring menus.
NAT	Accesses the NAT feature monitoring menus.
NAPT	Accesses the NAPT feature monitoring menus.
PING [address]	Sends queries to any other host once a second and waits for a response. This command can be used to isolate trouble in a multiple network environment. This admits parameters when no address is specified.
POOL	Displays the address pool established in the router as well as the ranges of addresses reserved for this.
ROUTE given address	Lists the existing routes for a specific destination IP address.
SIZES	Displays the size of specific IP parameters.
STATIC-ROUTES	Displays the static routes that have been configured.
TRACEROUTE address	Displays the complete path (hop-by-hop) to a particular destination.
TVRP	Accesses the TVRP protocol monitoring menus.
EXIT	Exits the IP monitoring.

1.1. ? (HELP)

Use the **?** (HELP) command to list the valid commands at the level where the router is programmed. You can also enter a **?** after a specific command to list its options.

Syntax:

```
IP>?
```

Example:

```
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

Use the **AGGREGATION-ROUTE** command to view the list of configured aggregation routes.

Each route is already specified by an address and its corresponding mask.

The following example shows an aggregation route (aggregating all the networks which begin with 200).

Syntax:

```
IP>AGGREGATION-ROUTES
```

Example:

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

The meaning of each of the fields is as follows:

Net	Route destination network or subnet.
Mask	Route destination network or subnet mask.

1.3. ACCESS control

Use this command to view the access control mode in use together with a list of the configured access control records. The access control modes can be:

Disabled: No access control is being carried out therefore the access control records are ignored.

Enabled: Access control exists and the access control records are inspected.

Exclusive: Packets matching the access control records are discarded.

Inclusive: Packets matching the access control record are forwarded.

When access control is enabled, packets failing to match any access control record are discarded. *Beg* and *End Pro* (protocol) indicates the IP protocol number and *Beg* and *End Prt* (port) indicates the port number. *Invoc* specifies the number of times that a particular entry in the IP access control system was invoked by the characteristics of an inbound or outbound packet.

Syntax:

```
IP>ACCESS
```

Example:

```
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 the **BPING** (Broadcast PING) command so that the router can send an ICMP Echo request packet to every subnet address and await a response.

A series of parameters are requested via the console:

IP destination: Any address pertaining to the subnet.

IP source: outbound packets. By default the device chooses the source interface address (logical) of the outbound ping.

Destination mask: The subnet mask.

Time out: Time interval greater or equal to 10ms while waiting for a response to the packet sent. This time is marked from the moment the packet is sent. The default value is one second.

Avoid fragmentation: IP datagram. This is an order for the router, as the destination cannot reassemble the pieces. The datagram can be fragmented by default.

The packet size is 56 bytes excluding the ICMP header.

The address the packet is sent to increases, beginning with the first subnet address which is not broadcast i.e. the first and the last address are ignored. The packets are sent every 100ms, however if the time out is longer that the time between pings and an answer has not been received, the device waits until the time out period has elapsed before sending a new packet.

If you receive a valid response, the corresponding delay is displayed. If not a 'contact not established' message is printed.

The **BPING** command is ended by clicking on any key or when the subnet addresses finish.

In the following example the destination address is 192.6.1.228 and the mask 255.255.255.248. After executing the corresponding logical AND operation, the broadcast addresses are 192.6.1.224 and 192.6.1.231. This means that the BPING command is executed between addresses 192.6.1.225 and 192.6.1.230.

Syntax:

```
IP>BPING
```

Example:

```
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

This command is useful to list the recently used destination routes. These are found in the routing cache memory. If a destination is not in the cache memory, the router looks up the said destination in the general routing table in order to make a decision.

Syntax:

```
IP>CACHE
```

Example:

```
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>
```

The meaning of each field is as follows:

Destination: Host destination address.

Usage: Number of packets sent to the Host.

Next hop: IP address of the next router on the path toward the destination host. The interface used by this packet is also displayed.

1.6. COUNTERS

This command is used to list the statistics relative to the IP packets that have been forwarded. These statistics include a routing error counter with the amount associated to the packets which have been dropped due to congestion.

Syntax:

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

a) COUNTERS DELETE

Example:

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

b) COUNTERS SHOW

Example:

```
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>
```

The meaning of each field is:

Routing table overflow	Routes that have been discarded due to the routing table being full.
Net unreachable	Packets that could not be forwarded due to unknown destination.
Bad subnet or net number	Illegal net/subnet routes or packets.
Unhandled broadcast	Non-local IP broadcast received (these are not forwarded).
Unhandled multicast	IP multicast packets that have been received, but whose address was not recognized by the router.
Unhandled directed broadcast	Directed (non-local) IP broadcast received when forwarding of these packets is disabled.
Attempted forward off LL broadcast	Packets that are received having non-local IP addresses but were sent to a link level broadcast address. These are discarded.
Packets discarded through filter	Received packets that have been addressed to filtered networks /subnets.
IP multicast accepted	IP multicasts that have been received and successfully processed by the router.
IP input packet overflows	Packets that have been discarded due to congestion at the packet input queue.

1.7. DUMP routing tables

This command is used to list the IP routing table. A line is printed for each IP network route. The default router (if there is one) is printed at the end.

Syntax:

```
IP>DUMP
```

Example:

```
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>
```

The meaning of each field is:

Type (type of route)	Indicates how to create the route. Sbnt— the network is divided into subnets: the entry type is a mark. Aggr— aggregation of nets; the entry type is a mark. Dir— directly connected net or subnet. RIP— route learnt by the RIP protocol. Del— route has been deleted. Stat— statically configured route. Fltr— filter. SPF— the route is an intra-area OSPF route. SPIA—the route is an intra-area OSPF route. SPE1, SPE2— the route is an external OSPF route (type 1 and 2 respectively). Rang—range of active OSPF addresses. This is not used to route packets.
Dest net	IP destination net or subnet.
Mask	Destination IP network mask.
Cost	Cost of route.
Age	For RIP routes, refers to the time elapsed since the routing table was last refreshed.
Next hop(s)	IP address of the subsequent router towards the destination or outbound interface that the router uses to forward the packet.

The number in brackets *(num)* after *Type* indicates the number of static or directly configured routes with the outbound interface and subinterface activated and have the route as the destination.

A percentage sign *"%"* after the *Type* indicates the RIP "updates" are always accepted for this destination.

A letter "*A*" after the *Type* indicates that the route coincides with an aggregation route.

A letter "*a*" after the *Type* indicates that the route is being added by an aggregation route.

When a route has more than one active path towards a destination at equal costs, each path is displayed on a line in the *Next hop(s)* column where a *"(C)*" indicates the current path. Depending on the configured multipath policy, the actual path will consecutively pass through all the paths (Round robin) or according to the routed packets source/destination (please see the MULTIPATH configuration command).

1.8. INTERFACE addresses

Use this command to display the router's IP interface addresses. Each address is listed together with its corresponding hardware interface and IP address mask.

Syntax:

```
IP>INTERFACE
```

Example:

```
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>
```

The meaning of each field is:

Interface:	Interface hardware type
IP Address(es):	Interface IP address
Mask(s):	Interface subnet mask.

1.9. IPSEC

Through this command you can access the IPSEC monitoring menus. For further details please consult the IPSEC manual Dm 739-I.

Syntax:

```
IP>IPSEC
```

Example:

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

1.10. NAT

Through this command you can access the NAT facility monitoring menus. For further details please consult the NAT manual Dm 720-I.

Syntax:

```
IP>NAT
```

Example:

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

1.11. NAPT

Through this command you can access the NAPT facility monitoring menus. For further details please consult the NAPT manual Dm 735-I.

Syntax:

```
IP>NAPT
```

Example:

```
IP>NAPT
NAPT>
```

1.12. PING [address]

"Packet Internet Grouper": Test program associated with TCP/IP and used to test the communications channel between INTERNET stations.

Through the **PING** command, the router sends ICMP Echo request packets to a given address and waits for a response to each transmitted packet. This command can be used to isolate trouble in the network.

If you specify an address immediately after a **PING** command, the router does not carry out a parameter petition, it takes the default values. If there is no specified address, the device requests a series of parameters:

IP destination: This is where the packets are sent and responses are received from.

IP source: outbound packets. The device chooses the interface (logical) source address of the outbound ping by default.

Number of data bytes: ICMP message size, excluding the ICMP header. The value is 56 bytes by default.

Time between pings: Time interval between pings. This should be greater or equal to 100ms. The value is one second by default.

Number of pings: Number of packets to send. This value is zero by default i.e. packets are sent indefinitely.

Time out: Time interval greater or equal to 10ms while waiting for a response to the packet sent. This time is marked from the moment the packet is sent. The value is zero by default i.e. the router will wait indefinitely for a response.

Avoid fragmentation: IP datagram. This is an order for the routers, as the destination cannot reassemble the pieces. The datagram can be fragmented by default.

If the time out is longer that the time between pings and an answer has not been received, the device waits until the time out period has elapsed before sending a new packet.

This process is done continuously, incrementing the ICMP sequence number with each additional packet. Matching received ICMP Echo responses are reported with their sequence number and the

round trip time. The time resolution of the round trip time calculation is usually (depending on platform) on the order of 20 milliseconds. If this response is not received during timeout a message is printed indicated that this time has been surpassed.

The **PING** command completes on pressing any character or when all the packets to be sent with their corresponding responses have been dealt with. At this point, a summary of packets sent, received, lost and those whose responses have surpassed time out as well as the minimum, mean and maximum round trip time is displayed.

When a multicast address is given as destination, there may be multiple responses printed for each ICMP packet sent, one for each group member. Each returned response is displayed with the source address of the responder.

Syntax:

```
IP>PING
```

Example:

```
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>
```

A special case is the use of the **PING address** command where all the configurable parameters take its value by default.

Syntax:

```
IP>PING address
```

Example:

```
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

Use the **POOL** command to view the addresses pool established in the router as well as the ranges of address used by this and the reason why they are reserved.

The reserved pool address ranges are expressed in the format of an address and a mask. The following shows the reasons why they are reserved:

SET	Ranges of addresses configured in the router.
RADIUS	Ranges of address received from a RADIUS Server. The router assigns these addresses to the remote ends of its PPP connections.
POOL	Ranges of addresses taken from the pool. The router assigns these addresses to the remote ends of its PPP connections.
LOCAL	Ranges of addresses received from the router's remote PPP connections. These are assigned to the local ends.
ASSIGN	Ranges of addresses configured in the router's PPP interfaces. The router assigns these addresses to the remote ends of its PPP connections.
REMOTE	Addresses configured in the router's remote PPP connections and sent by them.
INTERNAL	Internal IP address configured in the router.
ROUTER ID	Router-ID address configured in the router.
MNGMENT	Management IP address configured in the router.
SNMP	Range of addresses reserved for the X.25 pre-configuration.

Syntax:

```
IP>POOL
```

Example:

```
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

Use the **ROUTE** command to display the route (if one exists) to a given IP destination. If a route exists, the IP address(es) of the next hop(s) is displayed, along with the detailed information concerning the matching routing table entry.

Syntax:

```
IP>ROUTE address
```

Example:

```
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

Use the **SIZES** command to display the configured sizes of specific IP parameters pertaining to the IP protocol.

Syntax:

```
IP>SIZES
```

Example:

```
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>
```

The meaning of each field is:

Routing table size	Number of entries in the routing table that the router is capable of maintaining.
Table entries used	Number of entries used from the IP routing table.
Reassembly buffer size	Reassembly buffer size used to reassemble fragmented IP packets.
Largest reassembly pkt	Largest IP packet that this router has had to reassemble.
Size of routing cache	Size of the IP routing table.
# cache entries in use	Number of entries currently being used from cache.

1.16. STATIC-ROUTES

Use the **STATIC-ROUTES** command to display the list of configured static routes. This also displays the default network routers and subnet.

Each static route's destination is specified by an address, its corresponding mask, the next hop address, its cost, the outbound interface, the outbound subinterface and the status. Default routers appear as static routes to destination address 0.0.0.0 with mask 0.0.0.0. Default subnet routers also appear as static routes with subnetted networks destinations.

The following example shows a default network router, a default subnet router (assuming 128.185.0.0 is subnetted), a route to host 172.16.2.3 and static routes to networks 192.6.2.0 and 192.168.67.0.

Syntax:

```
IP>STATIC-ROUTES
```

Example:

```
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>
```

The meaning of each field is:

Net	Route destination network or subnet.
Mask	Network mask or destination subnet of the route.

Cost	Cost of using this route.
Next hop	IP address of the subsequent router where the packets are sent in order to reach the destination indicated on the route.
Int	The outbound interface identifier for the packets which select this route. If when the route is being monitored, the device is incapable of finding the outbound interface (because it doesn't exist), UNK appears (unknown).
Subint	The outbound subinterface identifier for the packets which select this route. Cases of FR indicates the outbound DLCI; X.25 (R->N) indicates the outbound NRI and generic interface which is not divisible in subinterfaces indicates N/A (Not Applicable). If when the route is being monitored, the device is incapable of finding the outbound subinterface (because it doesn't exist), UNK appears (unknown).
State	Indicates if the static route in question is active "UP" (active interface and subinterface) or inactive "DWN" (interface and subinterface are not active or unknown). Even if the status indicates activity, this does not mean that the route is active within the active routing tables (monitored by the **DUMP** command). This simply means that this static route has been chosen as the best route as no other route exists (static or dynamic) at a better cost.

1.17. TRACEROUTE address

Use the **TRACEROUTE** command to display the entire path to a given destination, hop by hop. For each successive hop, **TRACEROUTE** sends out three packets, and displays the IP address of the responding router, together with the round trip time associated with the response. If a particular packet receives no response, an asterisk is seen. Each line shown is related to this set of three packets, with the figure furthest to the left indicating the distance from the router executing the command (in router hops).

This command is done whenever the destination is reached, an ICMP Destination Unreachable is received, or the path length surpasses 32 router hops.

When a probe receives an unexpected result, several indications can be viewed:

"!N" indicates that an ICMP Destination Unreachable (net unreachable) packet has been received.

"!H" indicates that an ICMP Destination Unreachable (host unreachable) packet has been received.

"!P" indicates that an ICMP Destination Unreachable (protocol unreachable) has been received.

Since the probe is a UDP packet sent to a remote port, a port unreachable response is expected. "!" indicates that the destination has been reached, but the reply sent by the destination has been received with a TTL equal to 1. This usually indicates an error in the destination, prevalent in some versions of UNIX, whereby the destination is inserting the probe's TTL in its replies. This leads to a number of lines consisting solely of asterisks before the destination is finally reached.

Syntax:

```
IP>TRACEROUTE address
```

Example:

```
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>
```

The meaning of each field is:

TRACEROUTE	Displays the destination area address and the size of the packet being sent to that address.
1	The first trace showing the destination's NSAP and the amount of time it took the packet to arrive at the destination. The packet is sent three times.
Net unreachable	Indicates that no route is available towards the destination indicated in the command.
*1 * * * 2 * * *	Indicates that the router is waiting for a response from the destination but the destination is not responding.

1.18. TVRP

You can access the TVRP protocol monitoring menus through this command. For further information on this protocol please consult the TVRP Protocol manual Dm 725-I.

Syntax:

```
IP>TVRP
```

Example:

```
IP>TVRP
TVRP Monitoring

TVRP monit>
```

1.19. EXIT

Use the **EXIT** command to return to the previous prompt level.

Syntax:

```
IP>EXIT
```

Example:

```
IP>EXIT
+
```