Teldat Router

TCP-IP Configuration

Doc. *DM502-I* Rev. *8.30*

February, 2000

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.

This 32 bit number is commonly represented in dotted decimal notation. In this notation, each decimal integer represents one octet of the 32 bit address.

Thus a 32 bit IP address, in base 2

10000000 00101010 00001010 00010111

is written as the following set of decimal numbers:

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.

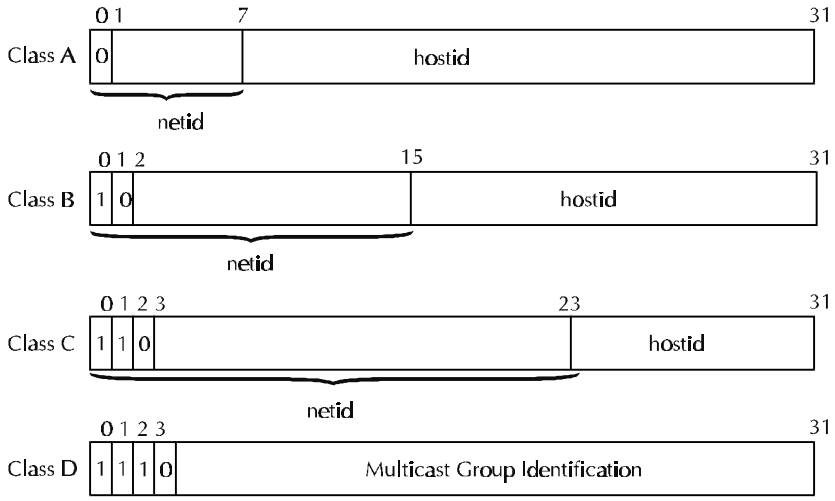
A Class A address is used for any network having more than 65,534 hosts. A host interprets a Class A address by reading bit 0 of the 32 bit address. If this bit is set to 0, the host interprets the **netid** field as the first 8 bits and **hostid** field as the last 24 bits. Only 127 Class A network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

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

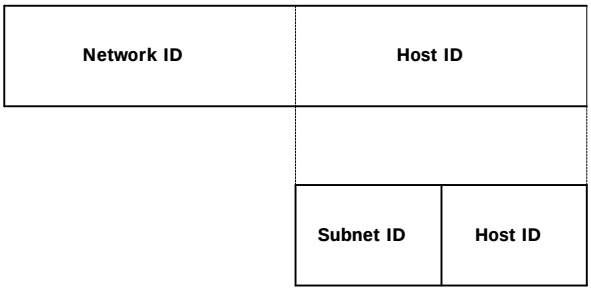
- Migrating from one IP address to another
- Using two subnets on the same physical network segment. For example, it is possible that the number of hosts on the physical network segment exceeds the current subnet's capacity. When this occurs, another subnet must be added to the physical network segment.

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.

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.

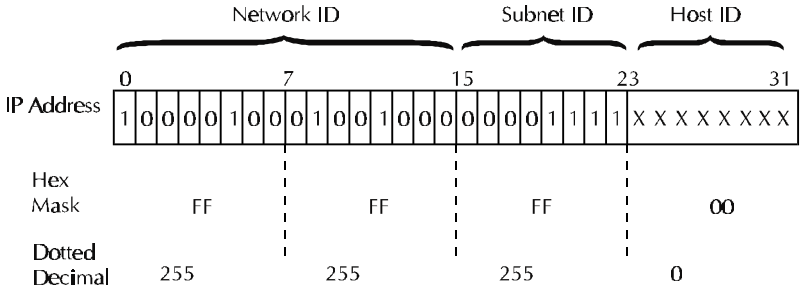
1.4. Subnet Mask

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

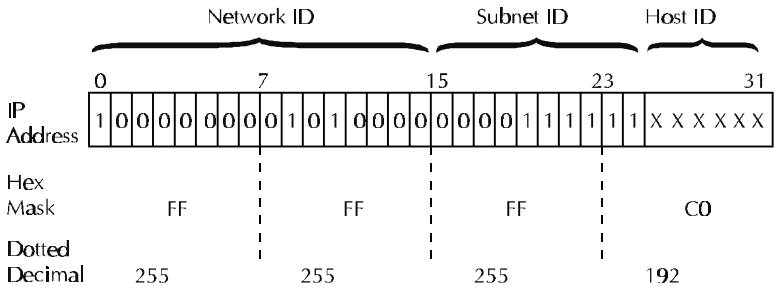
Subnet masks identify the portion of the address occupied by the **netid** field and the **subnetid** field. The mask is simply another 32 bits string written in dotted decimal notation with all ones in the **netid** and **subnetid** portion of the address and with all zeros in the **hostid** portion 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 size 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 a packet. The routing table is a list of all the network segments that IP knows how to reach. The routing table contains both dynamic and static routes.

A dynamic route is one that is learned through OSPF, RIP. These protocols regularly update their routing tables as network conditions change. Dynamic routing allows the router to transmit packets 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 on a directly connected network segment, IP matches the 32 bit destination address with the appropriate physical address in the ARP table. IP then hands the packet to the appropriate lower level protocol module for transmission directly to the destination node.
- If the packet is destined for a host on a remote network segment, IP uses the routing table to determine which router leads to that network segment. 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. Default routers are used to route packets 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.

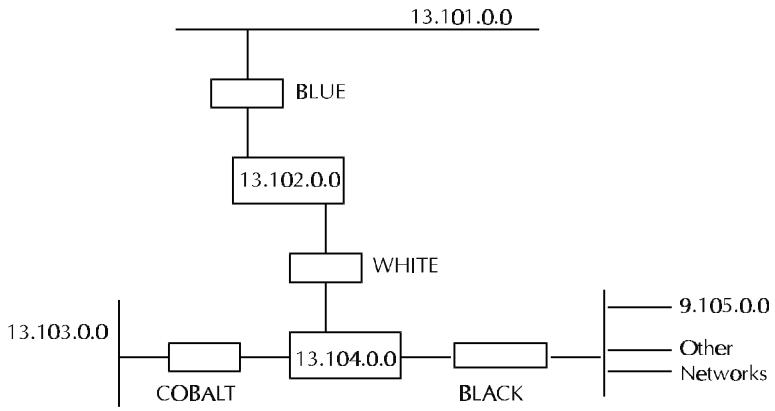
The default network route can be manually configured as a static route or can be dynamically learnt by using the RIP or OSPF protocols. Both protocols represent the default network route as destination 0.0.0.0.

- **Default subnet router**

Performs subnet routing in a network where the other routers do not know how to route traffic for specific subnets.

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, y BLACK. Where 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 toward the appropriate destination.

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 a particular 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) 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 address is filled with the pattern. During a NETWORK broadcast only the **hostid** is filled with the pattern.

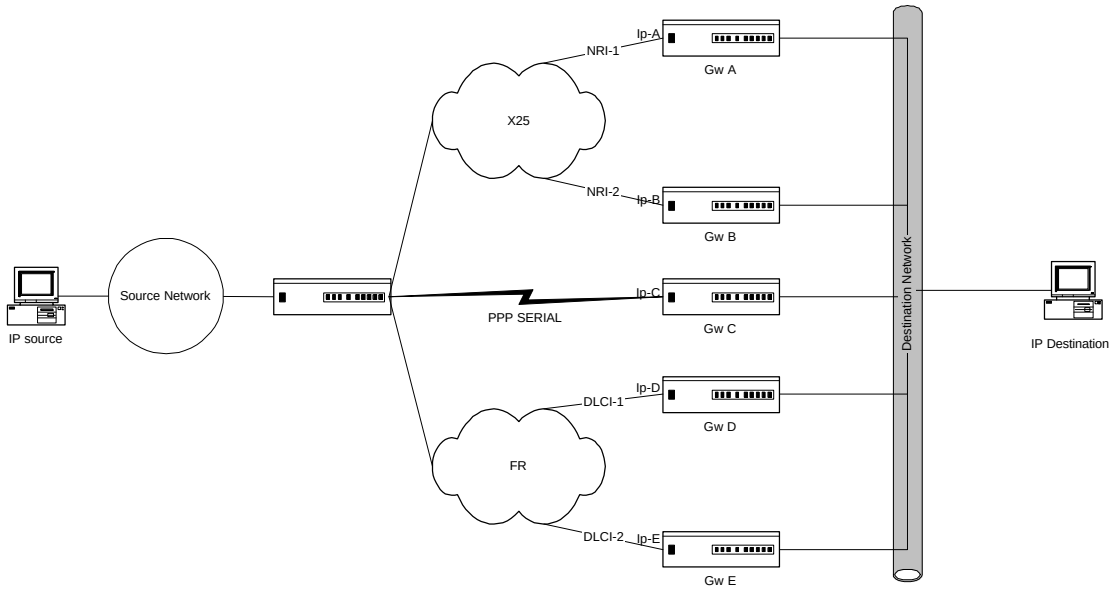
f) Receiving IP broadcasts

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.

g) Multicast Packets

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



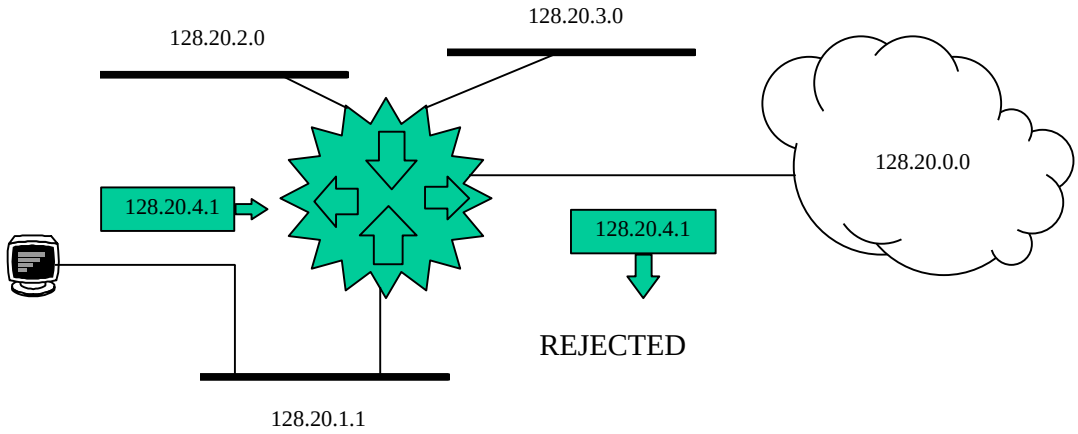
In the previous figure you can see the possibility of forwarding to the IP destination address through various distinct gateways (Gw).

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 outgoing 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.

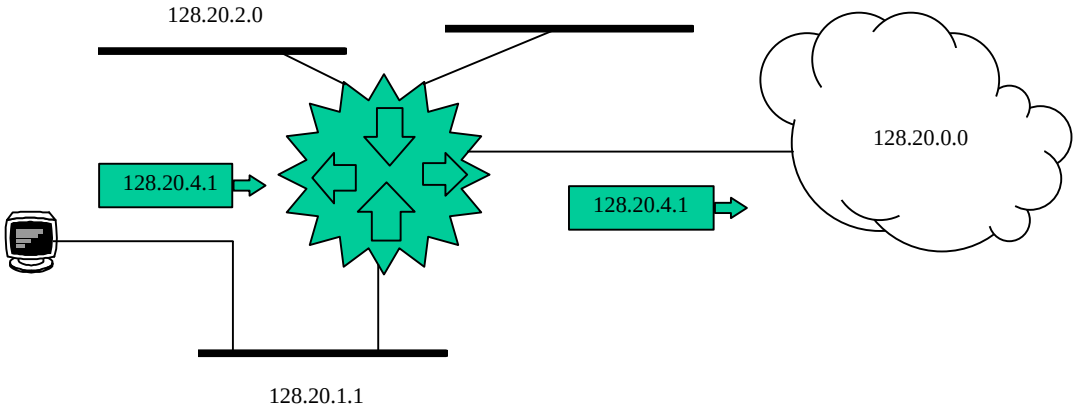
h) IP classless

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 case this is configured (network route 0.0.0.0 which is the supernet encompassing all networks).



IP classless feature enabled

i) Access Control

This feature allows you to control the forwarding of packets by examining the masked source and masked destination addresses in the IP header, the protocol type in the IP header, or the port number in the TCP or UDP headers.

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.

j) 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 IP networks are minimum. NAT is described in the RFC 1631.

The router supports the NAT feature. For further information please see the manual Dm520.

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

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

OSPF 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 discuss each configuration task in more detail.

- Access the IP configuration environment.
- Assign IP addresses to the network hardware interfaces.
- Enable dynamic routing.
- Add static routing information.
- Set up IP access control.
- Exit the IP configuration process.
- Restart the router to activate the configuration changes.

1.1. Access the IP Configuration Environment

To access the IP configuration environment, enter the following command at the Config > prompt as shown:

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

1.2. Assign IP Addresses to Network hardware interfaces

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

In the following example, network interface number 2 has been assigned the address 128.185.123.22 with the associated address mask 255.255.255.0 (using the third byte for subnetting).

```
IP config> ADD ADDRESS 2  128.185.123.22  255.255.255.0
```

1.3. Enable Dynamic Routing

Use the following procedures to enable dynamic routing on the router. The routers support OSPF and RIP for Interior Router 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. Add 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 and distance to the 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 destinations (i.e., destinations not present in the routing table) toward the default router.

A default router is configured in the router 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> SET DEFAULT NETWORK-GATEWAY
Default gateway [130.1.1.191]?
gateway's cost [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, to create a default subnet router for the subnetted network 18.0.0.6, you could use the following command:

```
IP config> SET DEFAULT SUBNETWORK-GATEWAY
For which subnetted network ? [0.0.0.0] ? 18.0.0.0
Default gateway [0.0.0.0] ? 18.0.0.6
gateway's cost[0] ? 2
```

The above example specifies that the next hop to the subnet default router is 18.0.0.6 , and that the cost of routing a packet to the default subnet router is 2.

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 an IP network/subnet number (*IP-network/subnet/host*) and the destination's address mask (*IP-mask*). The route to the destination is described by the IP address of the first hop router to use (*next-hop*) and the cost of routing a packet to the destination (*cost*). 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, modify, delete a static route, use the commands:

```
IP config> ADD ROUTE <IP-network/subnet/host, IP-mask, next-hop, cost>
IP config> CHANGE ROUTE <destination-address, mask ,first-hop, new destination-
address, new-mask, new-first-hop, new-cost>
IP config> DELETE ROUTE <dest-addr mask, hop>
```

Routes dynamically learned through the RIP and 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> ADD AGGREGATION-ROUTE <net or subnet or host, mask >
IP config> DELETE AGGREGATION-ROUTE <destination-IP-address, mask >
```

e) Multipath

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

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

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

or

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

- Configure (or not) the TMP-RECOVER-BACKUP parameters of the X.25 Node's various global (See X.25 manual Dm507-I)

Case of generic outgoing interface

- The lower cost static route and active interface begin functioning.
- If two or more routes coincide in having minimum costs, an active outgoing interface and the 'per packet Multipath IP flag' is enabled, traffic balance is carried out (up to maximum of 4 paths). If it is not enabled, the flag does not carry out traffic balance.
- If the interface fails 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 outgoing interface

- Static routes that have an FR outgoing 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 outgoing interface

Static routes that have an X.25 outgoing 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, an 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 TMP-RECOVER-BACKUP.
    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 outgoing interface

Static routes that have a "Dial" outgoing interface always activate 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 a "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> ENABLE CLASSLESS
```

or

```
IP config> DISABLE CLASSLESS
```

1.5. IP Access Controls Configuration

The IP access control system allows the IP forwarder to control packet forwarding based on source and destination IP addresses, IP protocol number, and by port number for the TCP and UDP protocols. This can control access to particular classes of IP address and services.

The IP access control system is 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 optional port number for UDP and TCP protocols.

For each received packet, the headers are compared to all specified fields in each entry in the 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 result pair for both the source and destination IP address. 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, 89 for OSPF.

Each entry may also have an optional port number range. This applies only to TCP and UDP packets, since the port number is part of the TCP and UDP headers. Any TCP or UDP packet with a destination port number within the specified range will match. A range of 0 to 65535 disables port filtering. 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 on 192.67.67.20

```
IP config> ADD ACCESS-CONTROL INCLUSIVE 0.0.0.0  0.0.0.0  192.67.67.20
255.255.255.255  6  6  25  25
```

The next example prevents any host on subnet 1 of Class B network 150.150.0.0. from sending packets to hosts on subnet on subnet 2 of Class B network 150.150.0.0 (assuming a 1 byte subnet mask).

```
IP config> ADD ACCESS-CONTROL EXCLUSIVE 150.150.1.0  255.255.255.0  150.150.2.0
255.255.255.0  0  255  0  65535
```

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

```
IP config> ADD ACCESS-CONTROL INCLUSIVE 0.0.0.0  0.0.0.0  0.0.0.0  0.0.0.0  17  17
520  520
```

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

```
IP config> ADD ACCESS-CONTROL INCLUSIVE 0.0.0.0  0.0.0.0  0.0.0.0  0.0.0.0  89 89
```

If IP access control is enabled, you must be careful with packets that the router originates and receives. Be sure not to filter out the RIP or OSPF packets being sent or received by the router. The easiest way to do this is to add a wildcard inclusive entry as the last in the access control list. Alternately, you can add specific entries for RIP and/or OSPF, perhaps with restrictive addresses and masks. Note that some OSPF packets are sent to the Class D multicast addresses 224.0.0.5 and 224.0.0.6, which is important if address checking is being done for routing protocols. See the **ADD** command section in this chapter for more information on access control.

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. To add a network filter, use the following command:

```
IP config> ADD FILTER <dest-IP-address, address-mask>
```

It is recommended that you filter to local loopback network 127.0.0.0 so as not to propagate packets destined as a loopback. Use the following command:

```
IP config> ADD FILTER  127.0.0.0  255.0.0.0
```

1.6. NAT Configuration

For further information please consult the NAT manual Dm520-I.

Chapter 3
Configuration Commands

1. IP Configuration Commands

This section summarizes and then explains all IP configuration commands. These commands allow you to configure the router's IP protocol behavior to meet your specific 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 IP commands and associated options
ADD	Adds to the IP configuration information.
CHANGE	Modifies information that was originally entered with the ADD command.
DELETE	Deletes IP configuration information that had been entered with the ADD command.
DISABLE	Disable certain IP features that have been turned on by the ENABLE command.
ENABLE	Enables IP features.
LIST	Lists IP configuration items.
MOVE	Changes the order of access control records.
NAT	Enters in the NAT configuration menus.
SET	Establishes IP configuration modes such as the type of access control and the format of broadcast addresses.
TVRP	Enters the TVRP protocol configuration menus.
EXIT	Exits the IP configuration process.

The letters typed in **bold** are the minimum number of characters which need to be keyed in order to activate the command.

1.1. ? (HELP)

Use the **?** (HELP) command to list the commands that are available from the current prompt level. You can also enter a ? after a specific command name to list its options.

Syntax:

```
IP config> ?
```

Example:

```
IP config> ?
ADD
CHANGE
DELETE
DISABLE
ENABLE
LIST
MOVE
NAT
SET
TVRP
EXIT
IP config>
```

1.2. ADD

Use the **ADD** command to add IP information to your configuration. This command lets you add interface addresses, access controls, and filters.

Syntax:

```
IP config> ADD ?
ACCESS-CONTROL
ADDRESS
AGGREGATION-ROUTE
FILTER
ROUTE
```

a) ADD ACCESS-CONTROL

Adds an access control entry to the end of the access control list. This allows you to describe a class of packets to forward or drop, depending on the type of the entry. The length and order of the IP access control list can affect the performance of the IP forwarder.

This command adds an IP access control entry to the end of the list. Each entry must be assigned the following: type, IP source, source-mask, IP destination, and destination-mask fields. The type must either be inclusive or exclusive. The IP-source and IP-dest fields are in the form of IP addresses in dotted decimal notation. Optionally, you may specify an IP protocol number range with the *FIRST-*

PROTOCOL LAST-PROTOCOL fields. If a range of protocols has been specified, you may specify a TCP and UDP port number range with the *FIRST-PORT* and *LAST-PORT* fields.

Syntax:

```
IP config> ADD ACCESS-CONTROL <type, IP-source, source-mask, IP-dest, dest-mask
,first-protocol, last-protocol, first-port, last-port>
```

Example:

```
IP config> ADD ACCESS-CONTROL INCLUSIVE 0.0.0.0  0.0.0.0  192.6.1.250
255.255.255.255  6   6   23   23
IP config>
```

If you do not introduce all the necessary parameters in order to add an access control, the device will request them.

Example:

```
IP config> ADD ACCESS-CONTROL
Enter type[E]?I
Internet source [0.0.0.0]?
Source mask [255.255.255.255]? 0.0.0.0
Internet destination [0.0.0.0]? 192.6.1.250
Destination mask [255.255.255.255]?
Enter starting protocol number ([CR] for all)[-1]? 6
Enter ending protocol number[6]?
Enter starting port number ([CR] for all)[-1]? 23
Enter ending port number ([CR] for all)[-1]? 23
IP config>
```

b) ADD ADDRESS

Assigns an IP address to one of the router's hardware network interfaces. A hardware network 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 appropriate command interface-number.

Syntax:

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

Example:

```
IP config> ADD ADDRESS 0 128.185.123.22   255.255.255.0
IP config>
```

c) ADD AGGREGATION-ROUTE

This adds the IP aggregation information to the routing table.

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

Syntax:

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

Example:

```
IP config> ADD AGGREGATION-ROUTE 128.0.0.0  255.0.0.0
IP config>
```

d) ADD FILTER

Designates an IP network/subnet to be filtered. IP packets will not be forwarded to filtered networks/subnets, nor will routing information be disseminated concerning such destinations. Packets destined for filtered network/subnets are simply discarded.

You must specify a filtered network/subnet together with its subnet mask. 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> ADD FILTER <dest-IP-address, address- mask>
```

Example:

```
IP config> ADD FILTER 127.0.0.0   255.0.0.0
IP config>
```

e) ADD ROUTE

Adds a static network/subnet routes to the router's IP configuration. When dynamic routing information is not available for a particular destination, static routes are used.

The destination is specified by an IP address (IP network/subnet/host) together with an address mask (IP-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 directly connected interfaces.

Syntax:

```
IP config> ADD ROUTE <IP-network/subnet/host,  IP-mask,  next-hop, cost>
```

Example:

```
IP config> ADD ROUTE 128.1.2.0  255.255.255.0  128.185.123.22  6
```

1.3. CHANGE

Use the **CHANGE** command to change an IP configuration item previously installed by the **ADD** command. In general, you must specify the item you want to change, just as you specified the item with the **ADD** command.

Syntax:

```
IP config> CHANGE ?
ADDRESS
FILTER
ROUTE
```

a) CHANGE ADDRESS

Modifies one of the router's IP interface address. You must specify each new address together with the new address' subnet mask.

Syntax:

```
IP config> CHANGE ADDRESS <old-address, new-address, new-mask>
```

Example:

```
IP config> CHANGE ADDRESS 192.9.1.1 128.185.123.22 255.255.255.0
IP config>
```

b) CHANGE FILTER

Modifies the subnet mask associated with a filtered network/subnet. Networks that are filtered become black holes. No packets are forwarded to them; nor is routing information be distributed about them.

Syntax:

```
IP config> CHANGE FILTER <destination, new-mask>
```

Example:

```
IP config> CHANGE FILTER 127.0.0.0  255.0.0.0
IP config>
```

c) CHANGE ROUTE

Modifies either the subnet mask, next hop, or the cost associated with a configured static network/subnet route.

Syntax:

```
IP config> CHANGE ROUTE <destination-address, mask, first-hop, new-destination-
address, new-mask, new-first-hop, new-cost>
```

Example:

```
IP config> CHANGE ROUTE 10.0.0.0  255.0.0.0  128.185.123.18  10.1.0.0 255.255.0.0
128.185.123.19 6
```

1.4. DELETE

Use the **DELETE** command to delete an IP configuration IP item previously installed by the **ADD** command. In general, you must specify the item you want to delete, just as you specified the item with the **ADD** command.

Syntax:

```
IP config> DELETE ?
ACCESS-CONTROL
ADDRESS
AGGREGATION-ROUTE
DEFAULT
FILTER
ROUTE
```

a) DELETE ACCESS-CONTROL

Deletes one of the access control records.

Syntax:

```
IP config> DELETE ACCESS-CONTROL <record number>
```

Example:

```
IP config> DELETE ACCESS-CONTROL 2
IP config>
```

b) DELETE ADDRESS

Deletes one of the router's IP Interface addresses.

Syntax:

```
IP config> DELETE ADDRESS <IP-interface-address>
```

Example:

```
IP config> DELETE ADDRESS 128.185.123.22
IP config>
```

c) DELETE AGGREGATION-ROUTE

Deletes an IP aggregation route.

Syntax:

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

Example:

```
IP config> DELETE AGGREGATION-ROUTE 128.0.0.0  255.0.0.0
IP config>
```

d) DELETE DEFAULT

Deletes either the default gateway or the default subnet router for the specified subnetted network.

Syntax:

```
IP config> DELETE DEFAULT
NETWORK-GATEWAY <next-hop>
SUBNET-GATEWAY <subnetted network, next-hop>
```

Example:

```
IP config> DELETE DEFAULT NETWORK-GATEWAY 127.0.0.0
IP config>
```

Example:

```
IP config> DELETE DEFAULT SUBNET-GATEWAY 128.185.0.0 127.0.0.0
IP config>
```

e) DELETE FILTER

Deletes one of the router's filtered networks.

Syntax:

```
IP config> DELETE FILTER <dest-IP-address, address- mask>
```

Example:

```
IP config> DELETE FILTER 127.0.0.0 255.255.0.0
IP config>
```

f) DELETE ROUTE

Deletes one of the router's configured static routes.

Syntax:

```
IP config> DELETE ROUTE <dest-IP-address, mask,  next-hop>
```

Example:

```
IP config> DELETE ROUTE 10.0.0.0  255.255.0.0  128.185.123.22
IP config>
```

1.5. DISABLE

Use the **DISABLE** command to disable IP features previously enabled by the **ADD** command.

Syntax:

```
IP config> DISABLE ?
CLASSLESS
DIRECTED-BROADCAST
PER-PACKET-MULTIPATH
```

a) DISABLE CLASSLESS

Disables the IP routing strategy "Classless Routing Strategy" so the router continues with "IP Class Routing Strategy".

Syntax:

```
IP config> DISABLE CLASSLESS
```

Example:

```
IP config> DISABLE CLASSLESS
IP config>
```

b) DISABLE DIRECTED-BROADCAST

Disabled the forwarding of IP packet whose destination is a non-local (e.g., remote LAN) broadcast address. The source host originates the packet as a unicast where it is then forwarded as a unicast to a

destination subnet and “exploded” into a broadcast. You can use these packets to locate networks servers.

Syntax:

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

Example:

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

c) DISABLE PER-PACKET-MULTIPATH

If per-packet-multipath is disabled, the router will chose the first available path to a destination. The default for this feature is disabled.

Syntax:

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

Example:

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

1.6. ENABLE

Use the **ENABLE** command to activate IP features, capabilities, and information added to your IP configuration.

Syntax:

```
IP config> ENABLE ?
CLASSLESS
DIRECTED-BROADCAST
PER-PACKET-MULTIPATH
```

a) ENABLE CLASSLESS

Enables the IP routing strategy “Classless Routing Strategy”.

Syntax:

```
IP config> ENABLE CLASSLESS
```

Example:

```
IP config> ENABLE CLASSLESS
IP config>
```

b) ENABLE 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.

These packets can be used to locate network servers. 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> ENABLE DIRECT-BROADCAST
```

Example:

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

c) ENABLE PER-PACKET-MULTIPATH

If per-packet-multipath is enabled, and there are multiple equal-cost paths to a destination, the router chooses the path for forwarding each packet in a round robin fashion. The default for this feature is disable.

Syntax:

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

Example:

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

1.7. LIST

Use the **LIST** command to display various pieces of the IP configuration data, depending on the particular subcommand invoked.

Syntax:

```
IP config> LIST ?
ALL
ACCESS-CONTROLS
ADDRESSES
PROTOCOLS
ROUTES
SIZES
```

a) LIST ALL

Prints the entire IP configuration.

Syntax:

```
IP config> LIST ALL
```

Example:

```
IP config> LIST ALL
Interface addresses
IP addresses for each interface
intf  0   192.6.2.1        255.255.255.0    NET broadcast,    fill 0
intf  1   130.1.2.1        255.255.0.0        NET broadcast,    fill 0
Router-ID: 192.6.2.1
Internal IP address: 0.0.0.0

Routing

Protocols
Direct broadcast: enabled
OSPF: disabled
Per packet multipath: disabled
RIP: disabled
IP classless: disabled
IP config>
```

b) LIST ACCESS-CONTROL

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

Syntax:

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

Example:

```
IP config> LIST ACCESS-CONTROLS
Access Control is: disabled
List of access control records:
    Type                                          Beg  End   Beg  End
        Source   Mask      Destination  Mask       Pro  Pro   Prt  Prt
  1 E   0.0.0.0  00000000  192.6.1.250  FFFFFFFF   6    6     23   23
  2 I   0.0.0.0  00000000  0.0.0.0      00000000   0    255   0    65535
IP config>
```

c) LIST ADDRESSES

Prints the IP interface address that have been assigned to the router, along with their configured broadcast formats.

Syntax:

```
IP config> LIST ADDRESSES
```

Example:

```
IP config> LIST ADDRESSES
IP addresses for each interface
intf  0   192.6.2.1        255.255.255.0    NET broadcast,    fill 0
intf  1   130.1.2.1        255.255.0.0        NET broadcast,    fill 0
Router-ID: 192.6.2.1
Internal IP address: 0.0.0.0
IP config>
```

d) LIST PROTOCOLS

Prints the configured state of the IP routing protocols (RIP and OSPF).

Syntax:

```
IP config> LIST PROTOCOLS
```

Example:

```
IP config> LIST PROTOCOLS
Direct broadcast: enabled
OSPF: disabled
Per packet multipath: disabled
RIP: disabled
IP classless: disabled
IP config>
```

e) 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>
```

f) LIST SIZES

Displays the routing table size, reassembly buffer size, and the route cache size.

Syntax:

```
IP config> LIST SIZES
```

Example:

```
IP config> LIST SIZES
Routing table size: 768 nets (49152 bytes)
Reassembly buffer size: 12000 bytes
Routing cache size: 64 entries
IP config>
```

1.8. MOVE

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

Syntax:

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

Example:

```
IP config> MOVE ACCESS-CONTROL 5 2
IP config>
```

1.9. NAT

You can access the NAT configuration menus through this command. For further details please consult the NAT manual Dm520.

Syntax:

```
IP config> NAT
```

Example:

```
IP config> NAT
Conf NAT>
```

1.10. SET

Use the **SET** command to set certain values, routes, and formats within your IP configuration.

Syntax:

```
IP config> SET ?
ACCESS-CONTROL
BROADCAST-ADDRESS
CACHE-SIZE
DEFAULT
INTERNAL-IP-ADDRESS
REASSEMBLY-SIZE
ROUTING
ROUTER-ID
```

a) SET ACCESS-CONTROL

Allows you to configure the router to enable or disable IP access control.

Syntax:

```
IP config> SET ACCESS-CONTROL
ON
OFF
```

Example:

```
IP config> SET ACCESS-CONTROL ON
IP config>
```

b) SET BROADCAST-ADDRESS

Specifies the IP broadcast format that the router uses when broadcasting packets out a particular interface. IP broadcast are most commonly used by the router when sending RIP update packets.

The *style* parameter can take either the value LOCAL-WIRE or the value 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* 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.

When receiving the router recognizes all forms of the IP broadcast address. The following example configures a broadcast address 255.255.255.255.

Syntax:

```
IP config> SET BROADCAST-ADDRESS
```

Example:

```
IP config> SET BROADCAST-ADDRESS
Set for which interface address [0.0.0.0]?192.9.1.11
Use a NETWORK or LOCAL-WIRE style address [NETWORK]?LOCAL-WIRE
Fill pattern for wildcard part (0 or 1)[0]?
IP config>
```

c) SET CACHE-SIZE

Configures the maximum number entries for the IP routing cache.

Syntax:

```
IP config> SET CACHE-SIZE
```

Example:

```
IP config> SET CACHE-SIZE
number of cache entries [64]?
IP config>
```

d) SET DEFAULT

The *NETWORK-GATEWAY* option configures a route to the default gateway. You should assume that the default gateway has more complete routing information than the router itself. The route is specified by the IP address of the next hop and the distance (cost) to the default gateway.

The *SUBNET-GATEWAY* option configures a route to a default subnet gateway. You can configure a separate default subnet gateway for each subnetted network. The IP address of the next hop and the distance (cost) to the default subnet gateway specify the route. All packets destined for unknown subnets of a known subnetted network are forwarded to the subnetted network's default subnet gateway.

More than one default router can be configured.

Syntax:

```
IP config> SET DEFAULT
NETWORK-GATEWAY
SUBNETWORK-GATEWAY
```

Example:

```
IP config> SET DEFAULT NETWORK-GATEWAY
Default gateway [130.1.1.191]?
gateway's cost [0]?
IP config>
```

Example:

```
IP config> SET DEFAULT SUBNETWORK-GATEWAY
For which subnetted network? [0.0.0.0]?
Default gateway [130.1.1.191]?
gateway's cost [0]?
IP config>
```

e) SET INTERNAL-IP-ADDRESS

Set 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. To delete the internal IP address set the address to 0.0.0.0.

Syntax:

```
IP config> SET INTERNAL-IP-ADDRESS
```

Example:

```
IP config> SET INTERNAL-IP-ADDRESS
Internal IP address [0.0.0.0]?
IP config>
```

f) SET 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> SET REASSEMBLY-SIZE
```

Example:

```
IP config> SET REASSEMBLY-SIZE 12000
IP config>
```

g) SET ROUTING

Sets the size of the router's 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> SET ROUTING TABLE-SIZE
```

Example:

```
IP config> SET ROUTING TABLE-SIZE
number of nets [768]?
IP config>
```

h) SET ROUTER-ID

Sets the default IP address used by the router when sourcing 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 are set to the router-ID. In addition, the OSPF router ID are set to 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 just not configured, the default IP address of the router (and its OSPF router ID) is set to the first IP address in the router's configuration.

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

Syntax:

```
IP config> SET ROUTER-ID
```

Example:

```
IP config> SET ROUTER-ID
Router-ID [0.0.0.0]?
IP config>
```

1.11. 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 525-I.

Syntax:

```
IP config> TVRP
```

Example:

```
IP config> TVRP
TVRP Configuration

TVRP config>
```

1.12. 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 Monitoring Commands

This section summarizes and then explains all IP 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 IP commands and associated options.
AGGREGATION-ROUTE	Displays the aggregation routes that have been configured.
ACCESS controls	List the current 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 a table of all recent routed destinations.
COUNTERS	List various IP statistics, including counts of routing errors and packets dropped.
DUMP routing tables	List the contents of the IP routing table.
INTERFACE addresses	Lists the router's IP interface addresses.
PING [address]	Sends ICMP Echo Requests to another host once a second and watch for a response. This command can be used to isolate trouble in an internetwork environment. This admits parameters when no address is specified.
ROUTE given address	List whether a route exists for a specific IP destination, and if so, the routing table entry that corresponds to the route.
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.
NAT	Accesses the NAT monitoring menus.
EXIT	Exits the IP monitoring process.

The letters typed in **bold** are the minimum number of characters which need to be keyed in order to activate the command.

1.1. ? (HELP)

Use the **?** (HELP) command to list the commands that are available from the current prompt. You can also enter a **?** after a specific command name to list its options.

Syntax:

```
IP> ?
```

Example:

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

1.2. AGGREGATION-ROUTE

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-ROUTE
```

Example:

```
IP> AGGREGATION-ROUTE
Net          Mask
--------     ---------
200.0.0.0    255.0.0.0      aggregation
IP>
```

The meaning of each field is as follows:

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

1.3. ACCESS controls

Use the **ACCESS controls** command to print the access control mode in use together with a list of the configured access control records. The access control mode is one of the following:

Disabled: No access control is being done and the access control records are being ignored.

Enabled: Access control records is being done and the access control records are being recognized.

Exclusive: Packets matching the access control record are being discarded.

Inclusive: Packets matching the access control record are being 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 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 incoming or outgoing packet.

Syntax:

```
IP> ACCESS controls
```

Example:

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

List of access control records:
                                                          Beg  End  Beg  End
    Ty  Source       Mask     Destination     Mask        Pro  Pro  Prt  Prt    Invoc
1   E   0.0.0.0      00000000 192.6.1.250     FFFFFFFF    6    6    23   23     0
2   I   0.0.0.0      00000000 0.0.0.0         00000000    0    255  0    65535  0
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: outgoing packets. By default the device chooses the source interface address (logical) of the outgoing ping.

Destination mask: The subnet mask.

Time out: Time interval greater or equal to 10ms while waiting for an 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 [0.0.0.0]? 192.6.1.228
IP source [192.6.1.191]?
Destination mask [255.255.255.0]? 255.255.255.248
Time out(>=10ms)[1000]? 50
Avoid fragmentation[no](Yes/No)? Y
PING 192.6.1.225... not established contact
PING 192.6.1.226... not established contact
PING 192.6.1.227... time=8. ms
PING 192.6.1.228... not established contact
PING 192.6.1.229... not established contact
PING 192.6.1.230... not established contact
IP>
```

1.5. CACHE

Use the **CACHE** command to display the IP routing cache which contains recently routed destinations. If a destination is not in the cache, the router looks up the destination in the routing information table in order to make a forwarding 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->Node/0)
192.6.2.15      248     192.6.2.15     (EtherNet (10 MBit)/0)
192.6.1.157     206     130.1.1.191    (Router->Node/0)
192.6.2.3       4       192.6.2.3      (EtherNet (10 MBit)/0)
192.6.1.110     7       130.1.1.191    (Router->Node/0)
192.6.2.10      4       192.6.2.10     (EtherNet (10 MBit)/0)
192.6.1.34      1       130.1.1.191    (Router->Node/0)
192.6.1.250     1       130.1.1.191    (Router->Node/0)
IP>
```

The meaning of each field is:

Destination: IP destination host.

Usage: Number of packets recently sent to the destination host.

Next hop: IP address of the next router on the path toward the destination host. Also displayed is the network name of the interface used by the sending router to forward the packet.

1.6. COUNTERS

Use the **COUNTERS** command to display the statistics related to the IP forwarding process. This includes a count of routing errors, along with the number of packets that have been dropped due to congestion.

Syntax:

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

a) COUNTERS SHOW

Example:

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

Packets discarded through filter     0
IP multicast accepted:               0

IP input packet overflows
Net         Count
Eth/0       0
Router/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 the unknown destination.
Bad subnet number	Packets or routes that have been received for illegal subnets.
Bad net number	Packets or routes that have been received for illegal IP destinations.
Unhandled broadcast	Non-local IP broadcast received (these are not forwarded).
Unhandled multicast	IP multicast that have been received, but whose address was not recognized by the router (these are discarded).
Unhandled directed broadcast	Directed (non-local) IP broadcast received when forwarding of these packets is disabled.
Attempted forward of LL	Packets that are received having non-local IP addresses but were sent *broadcast* to a link level broadcast address. These are discarded.

Packets discarded though 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 packet overflows	Packets that have been discarded due to congestion at the forwarder's input queue.

b) COUNTERS DELETE

Example:

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

1.7. DUMP routing tables

Use the **DUMP routing tables** command to display the IP routing table. A separate entry is printed for each reachable IP network/subnet. The IP default router in use (if any) is listed at the end of the display.

Syntax:

```
IP> DUMP routing tables
```

Example:

```
IP> DUMP routing tables
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	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— configured static 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 outgoing 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 outgoing 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.

A number in brackets at the end of the row indicates the number of active paths towards the destination at the same cost.

1.8. INTERFACE addresses

Use the **INTERFACE addresses** 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 addresses
```

Example:

```
IP> INTERFACE addresses
Interface   IP Address (es)  Mask (s)
Eth/0       192.6.1.191      255.255.255.0
PPP/0       10.2.38.22       255.0.0.0
PPP/1       194.179.62.89    255.255.255.0
IP>
```

The meaning of each field is:

Interface	Hardware type of the interface
IP address (es)	IP addresses of the interface
Mask (s)	Subnet mask of the interface

1.9. NAT

You can access the NAT configuration menus through this command. For further details please consult the NAT manual Dm520.

Syntax:

```
IP> NAT
```

Example:

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

1.10. PING [address]

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

Use the **PING** command to have the router send ICMP Echo requests to a given destination once a second and watch for a response. This command can be used to isolate trouble in an internetwork environment.

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 answers received.

IP source: outgoing packets. The device chooses the interface (logical) source address of the outgoing 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 an 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 router 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.

The **PING** command completes when a character is typed in the monitoring process. At the time, a summary of packet loss, round trip time and number of ICMP destination unreachables received is displayed.

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

Syntax:

```
IP> PING [address]
```

Example:

```
IP> PING 192.6.2.1
IP destination [0.0.0.0]? 192.6.1.231
IP source [192.6.1.191]?
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 192.6.2.1: 56 data bytes
64 bytes from 192.6.2.1: icmp_seq=0. time=2. ms
64 bytes from 192.6.2.1: icmp_seq=1. time=2. ms
64 bytes from 192.6.2.1: icmp_seq=2. time=2. ms
64 bytes from 192.6.2.1: icmp_seq=3. time=2. ms
```

```
---- 192.6.2.1 PING Statistics
6 packets transmitted, 4 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 be default.

Syntax:

```
IP> PING address
```

Example:

```
IP>PING 192.6.2.1

PING 192.6.2.1: 56 data bytes
64 bytes from 192.6.2.1: icmp_seq=0. time=2. ms
64 bytes from 192.6.2.1: icmp_seq=1. time=2. ms
64 bytes from 192.6.2.1: icmp_seq=2. time=2. ms
64 bytes from 192.6.2.1: icmp_seq=3. time=2. ms

---- 192.6.2.1 PING Statistics
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 2/2/2
IP>
```

1.11. 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 given address
```

Example:

```
IP> ROUTE 192.6.2.1
Destination:   130.1.0.0
Mask:          255.255.0.0
Route type:    Dir
Distance:      1
Age:           0
Tag:           0
Next hop (s):  130.1.1.191       (Router->Node/0)
IP>
```

1.12. SIZES

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

Syntax:

```
IP> SIZES
```

Example:

```
IP> SIZES
Routing table size:           768
Table entries used:           3
Reassembly buffer size:       12.000
Largest reassembled pkt:      0
Size of routing cache:        64
# cache entries in use:       2
IP>
```

The meaning of each field is:

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

1.13. STATIC ROUTES

Use the static routes command to display the list of configured static routes. Configured default routes and default subnet routers are also listed.

Each static route's destination is specified by an address-mask pair , the next hop address, its cost, the outgoing interface, the outgoing subinterface and the status. Default routers appear as static routes to destination 0.0.0.0 with mask 0.0.0.0. Default subnet routers also appear as static routes to the entire IP subnetted network.

The following example shows a configured default router, a configured default subnet router (assuming 128.185.0.0 is subnetted) and a static route to network 192.9.10.0.

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
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 Network address of the route.

Mask Subnet mask of the IP address.

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 outgoing interface identifier for the packets which select this route. If when the route is being monitored, the device is incapable of finding the outgoing interface (because it doesn't exist), UNK appears (unknown).

SubInt The outgoing subinterface identifier for the packets which select this route. FR indicates the outgoing DLCI, X.25 (R->N) indicates the outgoing NRI, 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 outgoing subinterface (because it doesn't exist), UNK appears (unknown).

State Indicate if the static route in question is active "UP" (active interface and subinterface) or not active "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 routing tables** 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.

1.14. 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 probes, and prints the IP address of the responder, together with the round trip time associated with the response. If a particular probe receives no response, an asterisk is printed. Each line in the display relates to this set of three probes, with the left most number 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 reaches 32 router hops.

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

"!N" indicates that an ICMP Destination Unreachable (net unreachable).

"!H" indicates that an ICMP Destination Unreachable (host unreachable) 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 strange port, a port unreachable is what we expect.

"!" Indicates that the destination has been reached, but the reply sent by the destination has been received with a TTL of 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
```

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 traced three times.
Destination Unreachable	Indicates that no route to destination is available .
1 * * *	Indicates that the router is expecting some form of response from the
2 * * *	destination, but the destination is not responding.

1.15. 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 525-I.

Syntax:

```
IP> EXIT
```

Example:

```
IP> TVRP
TVRP Monitoring

TVRP monit>
```

1.16. EXIT

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

Syntax:

```
IP> EXIT
```

Example:

```
IP> EXIT
+
```