TCP-IP Configuration

bintec Dm702-I

Copyright© Version 11.0Q bintec elmeg

Legal Notice

Warranty

This publication is subject to change.

bintec offers no warranty whatsoever for information contained in this manual.

bintec is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

I Related Documents

bintec Dm704-I Configuration and Monitoring

bintec Dm720-I NAT Protocol

bintec Dm725-I TVRP Protocol

bintec Dm730-I DHCP Protocol

bintec Dm734-I ARP Proxy

bintec Dm735-I NAPT Facility

bintec Dm739-I IPSec

bintec Dm744-I Dial Routing

bintec Dm745-I Policy-based Routing

bintec Dm754-I NSLA

bintec Dm755-I Dynamic NAT Facility

bintec Dm759-I VRRP Protocol

bintec Dm762-I IGMP Protocol

bintec Dm772-I Common Configuration for Interfaces

bintec Dm775-I VRF

bintec Dm786-I AFS

bintec Dm804-I PIM Protocol

Chapter 1 Introduction

1.1 Introduction to IP Protocol

IP is a network layer protocol that provides a connectionless datagram service for data delivery. Being a connectionless protocol, it is often unreliable and only provides best effort delivery. IP packets over the Internet are used to carry data, whereas actual delivery is ensured by transport layer protocols such as TCP (Transmission Control Protocol).

bintec IP implementation complies with the standards defined by the TCP/IP protocol suite.

1.1.1 The Meaning of IP Addresses

IP addresses identify the IP network or particular segment the host interface is attached to. If, for example, a host has more than one interface attached to the network, said host has an IP address for each connection. Simply put, an IP address is similar to a postal address: it indicates where to send the data but not to whom.

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

A special notation is normally used to reference IP addresses: the 32 bits are divided into four groups of 8. Group values are given in decimal and separated with dots (periods).

Thus, an IP address in binary notation looks like this:

10000000 00101010 00001010 00010111

equivalent to:

128.42.10.23

Each IP address forms a pair of identifiers: one identifies the network (**netid**) and the other a host on said network (**hostid)**.

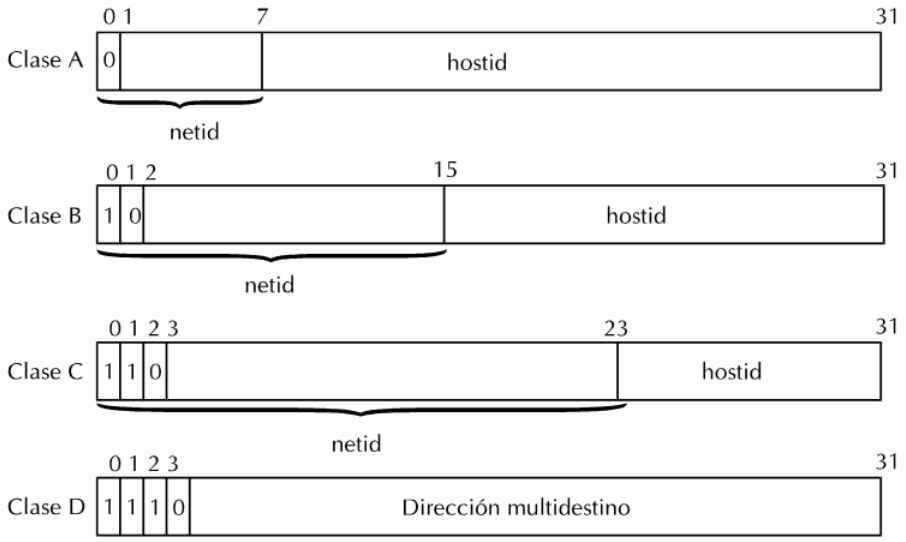
1.1.2 IP Address Classes

IP addresses are divided into classes, the three main ones being: A, B and C. A host identifies the class of an IP address by looking at the high order bits.

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

A Class B address is used for any medium-sized network with between 255 and 65,534 hosts. The first 16 bits of the address are devoted to the **netid** and the last 16 to the **hostid**. A host interprets Class B by reading bits 0 and 1 of the 32-bit address. If these bits are set to 1 and 0, respectively, then the host considers the **netid** field to be the first 16 bits and the **hostid** field to be the last 16.

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



In addition to these classes, which organize the final system addresses, there is also a fourth class, Class D. A class D address is used for IP multicasting. With this address, the first 4 bits are set to 1,1,1,0 and identify the address as a multicast. Bits 4 through to 31 identify the specific multicast group.

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

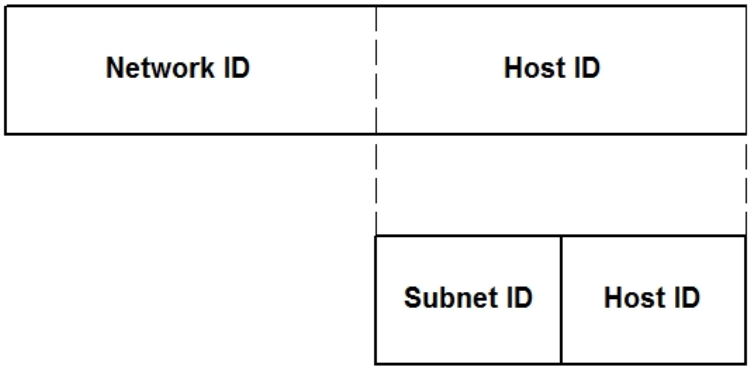
- Migrating from one IP address to another.
- Using two subnets on the same physical network segment. For example, the number of hosts on the physical network segment may exceed the current subnet capacity. When this occurs, another subnet must be added to the physical network segment.

1.1.3 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 two-level (**netid**, **hostid**) hierarchy, there is now a three-level (**netid**, **subnetid**, **hostid**) hierarchy. An organization is then assigned one or a few IP network numbers (at the very most). It can then 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 not visible to hosts (or routers) outside the organization.

Conceptually, adding subnetting only changes IP address interpretation. Subnetting divides the address into a network ID, a subnet ID and a 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; it can range from a few bits to occupying most of the width of the **hostid** field.

1.1.4 Subnet Mask

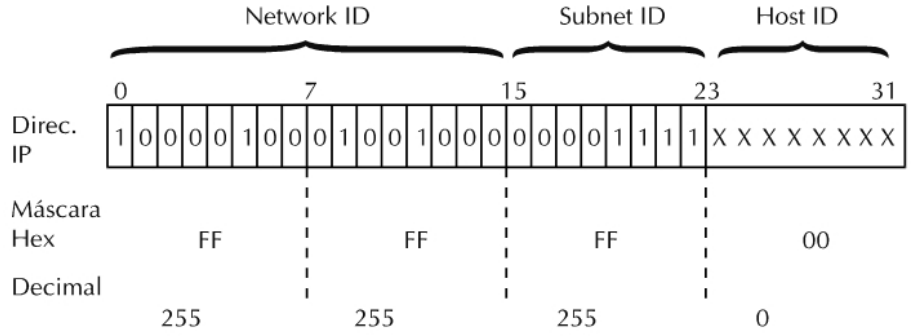
When adding an IP address to an interface, you must specify the subnet mask.

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

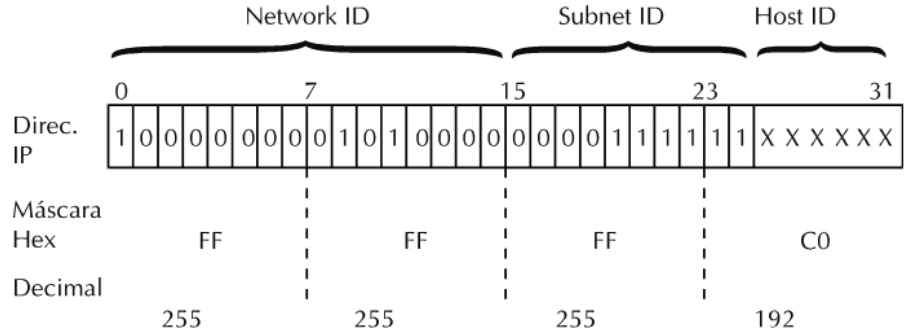
For example, suppose you have a Class B address. You want to assign the first 8 bits of the **hostid** as the **subnetid,**

leaving the new **hostid** with only 8 bits. 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 in the previous example). For example, you may want to assign the first ten bits of the **hostid** to the **subnetid**. This would create a mask of 255.255.255.192.



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

bintec IP implementation supports subnets of variable lengths. This feature allows you to divide a single IP network number **hostid** into many variable-sized subnets.

Note

Different sized subnetids can be used with RIP-1. You must either use OSPF or configure RIP-2.

Caution

Assign variable-length subnets with care. If you assign an overlapping subnet, problems may arise.

1.1.5 IP Routing

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

A dynamic route is learned through routing protocols such as RIP, OSPF and BGP. These protocols regularly update their routing tables as network conditions change. Dynamic routing allows the router to bypass 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 is unable to determine the correct route dynamically.

IP routing works as follows:

- IP receives a packet and reads the 32-bit destination address in the packet header.
- If the packet is destined for this router, further routing is unnecessary and IP hands the packet to the appropriate internal software module. Packets in this category include:

  - Control packets for the IP itself.

  - Routing update packets.

  - Packets used for diagnostic purposes.

- If a packet is addressed to a host connected to the same physical segment as one of the router ports, IP searches for the physical address associated with the datagram destination IP address, and then hands the packet to the appropriate lower-level protocol module so that it can be forwarded to the final destination. Associations between physical addresses and IP addresses are stored in an ARP table.
- If a packet is addressed to a host on a remote network segment, IP uses the routing table to determine the next hop address. 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 to be forwarded to the next hop.
- If a 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 in the routing table. This router is assumed to know the packet destination.

IP also performs several other major tasks: dropping erroneous packets or various types of filtering.

1.1.5.1 Default Router

A default router knows how to route packets other routers cannot route.

It performs routing for other devices that have traffic for an unknown-network destination.

The default network route can be manually configured as a static route or can be dynamically learned using a dynamic routing protocol. The default network route is given as destination 0.0.0.0.

1.1.5.2 Faulty Packets

The router drops packets that have not been correctly formatted or that have an erroneous destination address. The goal is to ensure said packets are not forwarded further into the network.

1.1.5.3 Router ID

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

1.1.5.4 Internal IP address

The internal IP address is an address that belongs to the router as a whole and doesn't have any particular interface. It is used only in situations where the router needs to ensure at least one address is always available.

If the internal IP address is configured 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.

1.1.5.5 Management IP address

Address used by the router to fill out the network address field in SNMP traps. If this is not configured, the router uses the internal IP address. If neither of these is configured, a packet output interface IP address is used.

1.1.5.6 Broadcast Packets

A broadcast message is destined for all hosts on the given network. IP occasionally sends broadcast messages on its own accord. These broadcast messages are used, among other things, to update the IP routing tables on other routers when running RIP-1 or RIP-2.

Note

The broadcast format programmed in the router's interface MUST match the format used by the systems connected to the same segment.

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

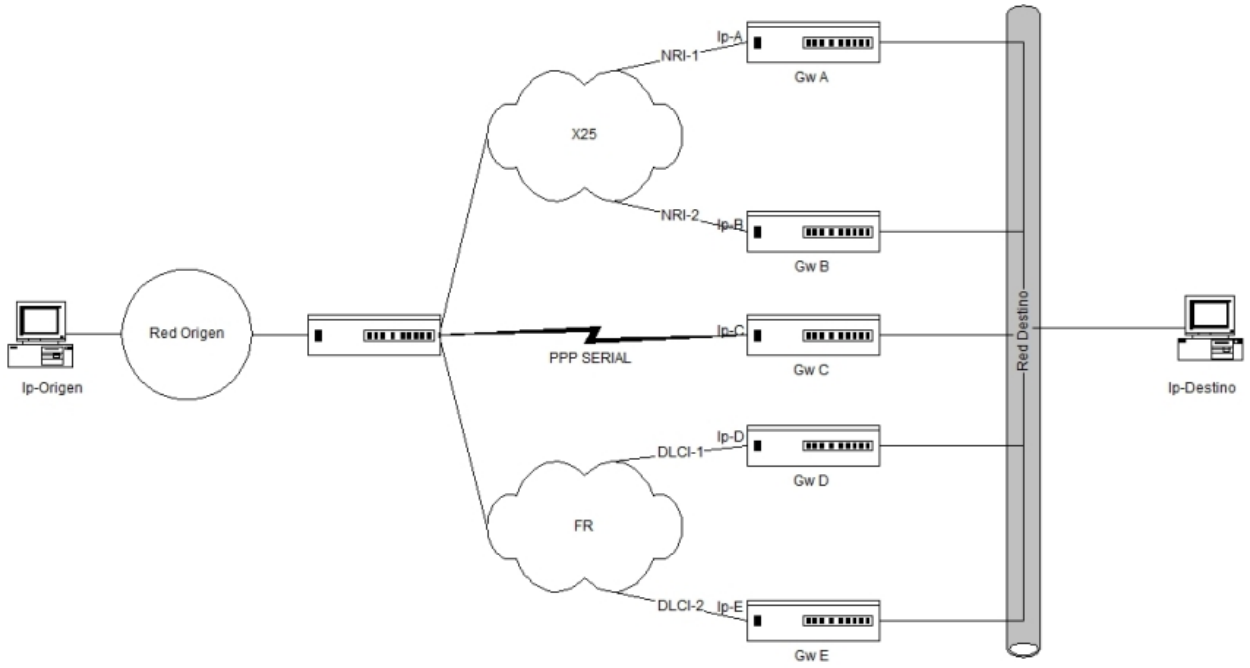
The IP recognizes all forms of broadcast messages and addressing. If the network portion of the broadcast address indicates either local wire or a directly connected IP network, IP treats the packet as if it were addressed to itself.

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

non-local broadcast address.

1.1.5.7 Multicast

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



In the above figure, you can see the possibility of forwarding to the IP destination address through different gateways (Gw).

The routes can be static or learned through a dynamic routing protocol that accepts the possibility of multipaths.

If two or more routes agree (i.e., they cost the same), the outbound interface is active and the **Multipath IP flag** is enabled, there is a balance of traffic (up to a maximum of 8 routes). If the flag is not enabled, then the traffic is not balanced.

1.1.5.8 IP classless

A router may receive packets destined for a network subnet that 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. In the example, the host forwards packets to 128.3.4.1. The router discards the packets it receives by default that are destined to a subnet not directly connected to it and with no subnet default route.

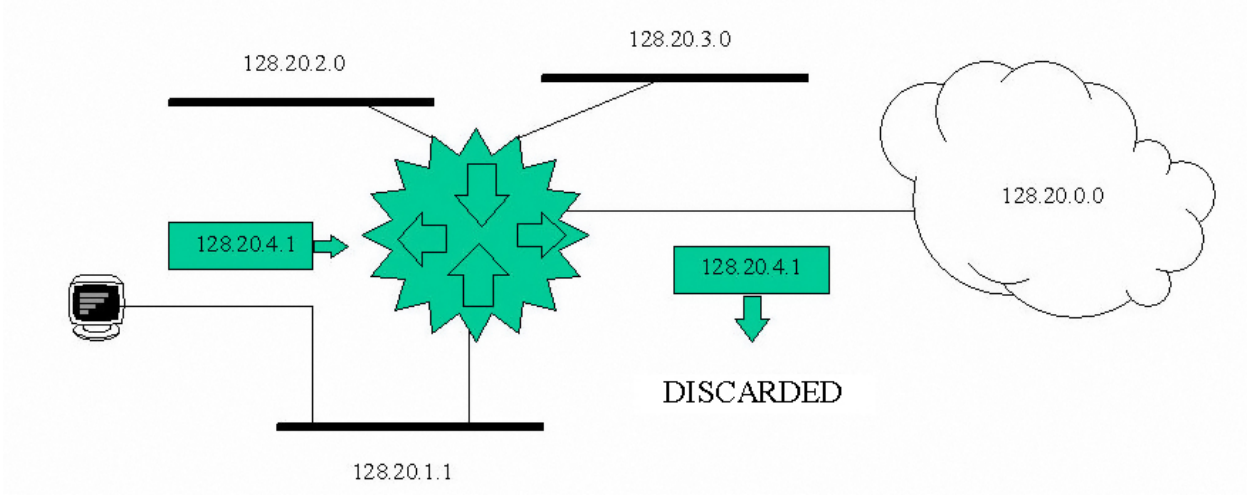


Fig. 1: **IP classless feature disabled**

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

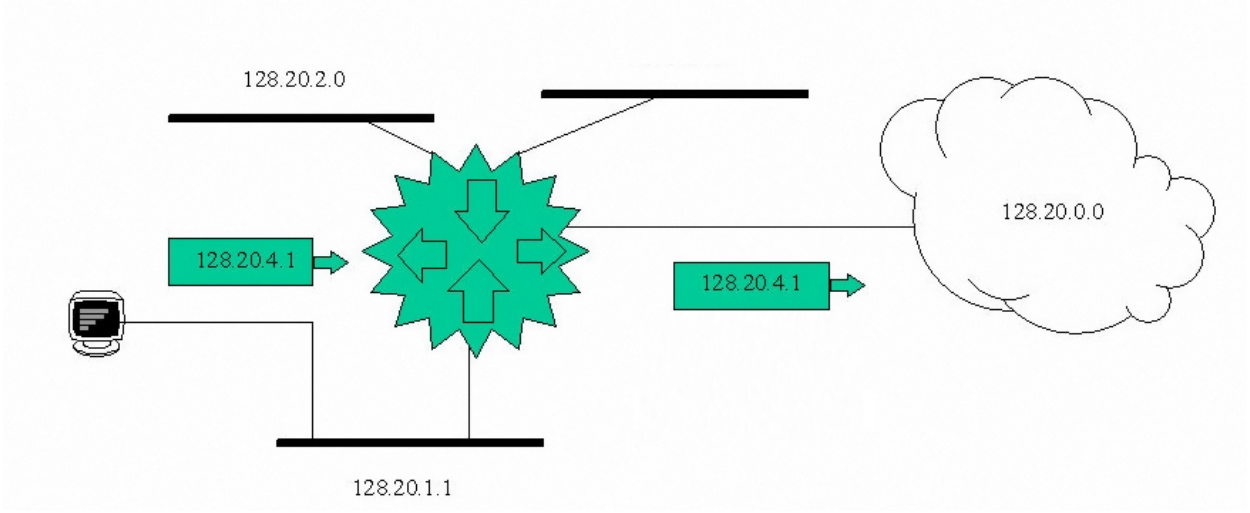


Fig. 2: **IP classless feature enabled**

1.1.5.9 Access Control

The access control options found in each interface help control packet routing by examining the access lists.

Prior to version 11.00.03, global access control configuration was allowed.

1.1.5.10 Address Translation (NAT)

The Network Address Translation (NAT) feature allows a company's IP network to appear to other IP networks as using an addressing space different to its internal one. For instance, NAT allows a company that uses private addresses (local addresses), which cannot be accessed by the Internet routing table, to connect to the Internet by converting said addresses into public ones (global addresses). NAT also allows companies to set up re-addressing strategies, where changes in the local IP networks are the lowest. NAT is described in RFC 1631.

This router supports NAT.

1.1.6 Interior Gateway Protocol

Routers that use a common routing protocol form an *autonomous system* (AS). This common routing protocol is known as 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, OSPF and I-BGP. Through these protocols, total compatibility is ensured with other routers available on the market.

1.1.7 Routing protocols between autonomous systems

Routing protocols are used to communicate routes between autonomous systems. Currently, E-BGP is the one most widely used.

1.1.8 Administrative distance

Preference between protocols marks the administrative distance. The lower the administrative distance, the greater the preference. The following table contains the administrative distance default values per type of route:

Type of Route	Administrative Distance
Directly Connected	0
OSPF (intra-area and inter-area)	10
Static	60
RIP	100
OSPF (external)	150
BGP	170
DHCP client	254

Chapter 2 Configuration

2.1 Configuration Commands

This section summarizes and describes the router configuration commands that can be found in the IP configuration menu. These commands allow you to configure the behavior of the router's IP protocols in order to meet your specific operation requirements.

Enter IP configuration commands at the **IP config>** prompt. To access this prompt, enter:

```
*p 4

Config>protocol ip
-- Internet protocol user configuration --
IP config>
```

Command	Function
? (HELP)	Lists all the commands or their options.
ACCESS-CONTROL	Configures entries in the global access control list (obsolete as of version 11.00.03).
ADMINISTRATIVE-DISTANCE	Activates the administrative distance concept.
AGGREGATION-ROUTE	Configures aggregation information.
CLASSLESS	Enables the IP Classless Routing Strategy.
DESCRIPTION	Adds a descriptive, or informative, text to make the configuration more legible.
DIRECTED-BROADCAST	Enables the forwarding of IP packets with destinations to a non-local network broadcast address.
DNS-DOMAIN-NAME	Configures the DNS domain name.
FILTER	Configures IP filters (obsolete as of version 11.00.03).
ICMP-REDIRECTS	Enables the forwarding of icmp redirect packets.
ICMP-UNREACHABLES	Enables the forwarding of icmp unreachable packets.
ID-ROUTE	Configures the route ID.
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 configuration of IP elements.
LOCAL	Configures functionalities associated with local traffic.
MANAGEMENT-IP-ADDRESS	Configures the router management IP address.
MULTIPATH	Enables multipath.
NAT	Enters the NAT facility configuration menus.
NO	Deletes a pre-added IP configuration parameter or re-establishes its default value.
POOL	Configures the range of addresses the router can assign through its PPP connections.
PROXY-ARP	Enters the ARP Proxy configuration menus (obsolete as of version 11.00.03).
PROXY-IGMP	Enters the IGMP Proxy configuration menus.
ROUTE	Configures IP routes.
ROUTER-ID	Configures the default IP address the router uses in locally originated packets. This will also become OSPF protocol 1 router-ID.
RULE	Configures IP connections.
TVRP	Enters the TVRP configuration menus.
VRF	Configures IP in a routing/forwarding domain in virtual private networks (VPN).
VRRP	Enters the VRRP configuration menus.
EXIT	Exits IP configuration.

Some of the interface-related IP parameters are set at the configuration menus of the interfaces themselves. As detailed in *Configuring IP per interface* on page 30, IP configuration commands are numbered and described for each interface.

As of version 10.7, commands from the IP main menu have been migrated to the IP submenu found in the interfaces menu. These commands still exist in the main IP menu. However, if you use them, a warning message appears stating they are old commands that may become obsolete in future versions.

Example:

```
IP config>address ethernet0/0 172.24.78.36 255.255.0.0
CLI Warning: This is a deprecated command.
CLI Warning: It may become obsolete in future versions.
CLI Warning: Please use per interface ip address config instead.
IP config>
```

We recommend configuring these IP parameters in the menu that corresponds to each interface. This warning was removed in version 11.00.03 and no longer appears since.

2.1.1 ? (HELP)

Lists the commands available at the level where the router is programmed, as well as their options.

Syntax:

```
IP config>?
```

2.1.2 ACCESS-CONTROL

Configures the IP access global control system.

Syntax:

```
IP config>access-control ?
  enabled      Enable access control system
  entry        Configure an access control entry
  move         Move an access control entry
```

2.1.2.1 ACCESS-CONTROL ENABLED

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

Syntax:

```
IP config>access-control enabled
```

Example:

```
IP config>access-control enabled
IP config>
```

To disable this, execute the same command preceded by **no**.

```
IP config>no access-control enabled
IP config>
```

Command history:

Release	Modification
11.00.03	This command is obsolete as of version 11.00.03. The access-control option menu is no longer supported.

2.1.2.2 ACCESS-CONTROL ENTRY

Configures an entry in the access control 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. You may also specify a range of IP protocols and reference a range of TCP and UDP ports, both at source and 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
```

Command	Function
Default	Creates an entry in the access control 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 identifier **<id>** .
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>
```

To delete an entry, execute the same command adding **no** at the beginning.

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

Command history:

Release	Modification
11.00.03	This command is obsolete as of version 11.00.03. The access-control option menu is no longer supported.

2.1.2.3 ACCESS-CONTROL MOVE

Changes the order of the access control list. This command removes the register *from#* immediately after *to#*, or takes it to the top of the list if you specify *top*.

Syntax:

```
IP config>access-control move <desde#> [top | <hasta#>]
```

Example:

```
IP config>access-control move 2 top
IP config>
```

Command history:

Release	Modification
11.00.03	This command is obsolete as of version 11.00.03. The access-control option menu is no longer supported.

2.1.3 ADMINISTRATIVE-DISTANCE

Enables the checking of the administrative distance value of routes before adding them to the active route table. The scope of this command is global, affecting all routing protocol comparisons. It is disabled by default.

Every routing protocol has an associated administrative distance. When several routes obtained from different protocols match, the ones with the shortest administrative distance values are meant to overwrite those learned through the rest of routing protocols. This check is carried out before comparing any route cost.

Distances can be modified through the configuration commands that appear in the menus for each protocol.

Syntax:

```
IP config>administrative-distance
```

Example:

```
IP config>administrative-distance
IP config>
```

Warning

We do not recommend operating this command in RUNNING-CONFIG mode because the distance of previously learned routes will not be updated with new values.

2.1.4 AGGREGATION-ROUTE

Adds IP aggregation information to the routing table.

The aggregation route is specified through an IP address (network, subnet, host) and a mask. The dynamic routing protocols (RIP and OSPF) are used to aggregate/summarize RIP and External OSPF networks.

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 aggregation routes, use the same command preceded by **no**.

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

2.1.5 CLASSLESS

Enables IP Classless Routing Strategy, also known as *Classless Inter-Domain Routing*.

Routing Strategy:

- *Class routing strategy*: suppose a router is directly connected to a subnet (10.1.1.0) pertaining to network 10.0.0.0. If the router receives packets destined to another subnet (10.2.1.0) within the same network, and does not have a specific route towards this (despite having a configured network default route (0.0.0.0/0)), the packet is dropped if there isn't a default route to this subnet (10.0.0.0/8). This is to prevent possible loops.
- *Classless routing strategy*: all packets received are forwarded to the next hop referenced by the route containing the destination, which is more restricted (more 1s in the mask) and has the lowest cost. This strategy is used by the Internet (since the introduction of *Classless Inter-Domain Routing* in 1993).

Syntax:

```
IP config>classless
```

Example:

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

To disable this, use the same command preceded by **no**.

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

Command history:

Release	Modification
11.00.05	The classless command has been removed as of version 11.00.05. The router always operates with CIDR (Classless Inter-Domain Routing).
11.01.00	The classless command has been removed as of version 11.01.00. The router always operates with CIDR (Classless Inter-Domain Routing).

2.1.6 DESCRIPTION

Configures an informative textual description to make the IP configuration easier to read.

Syntax:

```
IP config>description <text>
```

Example:

```
IP config>description "IP Protocol"
IP config>
```

To disable this, use the same command preceded by **no**.

```
IP config>no description
IP config>
```

2.1.7 DIRECTED-BROADCAST

Enables the forwarding of IP packets whose destination is a non-local (e.g., remote LAN) broadcast address. The source host creates the packet as a *unicast* and forwards it to a destination subnet as such, later transforming it 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 a Class D IP address. Default is enabled.

Syntax:

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

Example:

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

To disable this, use the same command preceded by **no**.

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

2.1.8 DNS-DOMAIN-NAME

Sets a domain name.

Syntax:

```
IP config>dns-domain-name <domain-name>
```

Example:

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

To delete this, use the same command preceded by **no**.

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

```
IP config>
```

2.1.9 FILTER

Designates a filter for an IP network/subnet. IP packets complying with the filter conditions are not forwarded but 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 a filter mechanism is more efficient than using 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 **no**.

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

Command history:

Release	Modification
11.00.03	The "*filter*" command is obsolete as of version 11.00.03.

2.1.10 ICMP-REDIRECTS

Enables ICMP redirected packet forwarding. Default is enabled.

Syntax:

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

Example:

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

To disable this, use the same command preceded by **no**.

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

2.1.11 ICMP-UNREACHABLES

Enables the forwarding of *ICMP Unreachable* packets. Default is enabled.

Syntax:

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

Example:

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

To disable this, use the same command preceded by **no**.

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

2.1.12 ID-ROUTE

Adds *Dial Routing* routes to the routing table. For further information, please see bintec manual *Dm744-I Dial Routing*.

2.1.13 INTERNAL-IP-ADDRESS

Configures the internal IP address that belongs to the router as a whole, and not to 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 configured 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 **no**.

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

2.1.14 IP-PARAM

Configures specific IP 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
```

2.1.14.1 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>
```

Default is 64. To return to the default value, execute the same command preceded by **no**.

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

2.1.14.2 IP-PARAM REASSEMBLY-SIZE

Configures the size of the buffers used to reassemble fragmented IP packets. Default 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 **no**.

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

2.1.14.3 IP-PARAM ROUTING-TABLE-SIZE

Configures the maximum size for the IP routing table. By default, there is no size limit for said table. If you configure a limit, you might lose routing information due to lack of space.

Syntax:

```
IP config>ip-param routing-table-size <#>
```

Example:

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

To delete the limit, execute the same command preceded by **no**.

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

2.1.15 IPSEC

Accesses the IPSEC configuration menus. For further information, please see bintec manual *Dm739-I IPSec*.

Syntax:

```
IP config>ipsec
```

Example:

```
IP config>ipsec

-- IPSec user configuration --
IPSec config>
```

2.1.16 LIST

Displays several IP configuration parameters, depending on the selected option.

2.1.16.1 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 through 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>
```

Command history:

Release	Modification
11.00.03	The "*list access-controls*" command is obsolete as of version 11.00.03.

2.1.16.2 LIST ACCESS-GROUP

Displays the *per interface* access controls. The access control lists assigned to inbound and outbound traffic are displayed for each interface (“” means there is *NO* associated access list).

Access controls defined for local traffic (traffic destined for the router itself) are also displayed.

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>
```

Command history:

Release	Modification
11.00.03, 11.01.00	The command output has changed as of versions 11.00.03 and 11.01.00. Information regarding *Per-interface access controls* is not shown, since the **access-group** command is obsolete.

2.1.16.3 LIST ADDRESSES

Displays 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>
```

2.1.16.4 LIST ALL

Displays 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

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

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

Local access-group: in 102

IP config>
```

2.1.16.5 LIST DNS-DOMAIN-NAME

Displays the domain name, configured through the IP configuration menu using **dns-domain-name**. This also displays the *FQDN*, which identifies the device through the domain name and the host name. The latter is configured through the router's general configuration menu (via **set hostname**).

Syntax:

```
IP config>list dns-domain-name
```

Example:

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

2.1.16.6 LIST IP-PARAM

Displays information on various IP parameters: maximum route table size, reassembly buffer size and route cache size.

Syntax:

```
IP config>list ip-param
```

Example:

```
IP config>list ip-param

Routing table max. size: unlimited
Reassembly buffer size: 12000 bytes
Routing cache size: 64 entries

IP config>
```

2.1.16.7 LIST IP-PROTOCOL

Shows whether the RIP and OSPF routing protocols are enabled, the use of multipath (in which routes exit towards the destination networks through several hops at the same cost), IP *classless routing strategy* and if ICMP Unreachable and ICMP Redirect packets can be transmitted.

Syntax:

```
IP config>list ip-protocol
```

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>
```

2.1.16.8 LIST POLICY

Displays information on Policy Routing. For further information, please see bintec manual *Dm745-I Policy-based Routing*.

2.1.16.9 LIST POOL

Displays the range of addresses the router can assign through its PPP connections.

Syntax:

```
IP config>list pool
```

Example:

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

2.1.16.10 LIST ROUTES

Displays the list of static network/subnet routes configured and also lists any default router configured. It also displays the configured aggregation routes and any established filters.

Syntax:

```
IP config>list routes
```

Example:

```
IP config>list routes

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
route to 192.168.3.0,255.255.255.0 via DHCP default gateway on ethernet0/1.100, cost 1
IP config>
```

Command history:

Release	Modification
11.00.03	The command output has changed. As of version 11.00.03, *Filter* information is not shown as the **filter** command is obsolete.

2.1.16.11 LIST RULE

Displays defined IP connections.

Syntax:

```
IP config> list rule
```

Example:

```
IP config>list rule

Ip Connection Rules
  ID   Local Address    --> Remote Address    NAPT TOut AcLTOut FW  Adj-MSS Acc-List
       NAPT Address
 ------------------------------------------------------------------------------
 1     200.12.101.1     --> 200.12.101.2      YES  10    0        NO   OFF      0
       0.0.0.0
 2     ppp1             --> 0.0.0.0           YES  5     0        YES  OFF      0
       0.0.0.0

IP config>
```

2.1.17 LOCAL

Allows you to configure various functionalities related to local traffic (where the router itself is source or destination).

Syntax:

```
IP config>local ?
  access-group    Specify access control for local traffic
  policy          Enable policy routing for locally generated packets
```

2.1.17.1 LOCAL ACCESS-GROUP

Configures the access control system for local traffic. Access to several router services can be restricted (telnet, FTP, etc.) independently of the inbound interface.

Syntax:

```
IP config>local access-group <access list> in [silently-discard|tcp-reset|icmp-unreachable]
```

In:	Applies the generic access control list to local inbound traffic.
Silently-discard:	Instead of sending an icmp error packet, the packet is simply discarded. To enable this option, the AFS feature must be enabled. Please see bintec manual *Dm786-I AFS*. This option is automatically applied to configured access-groups when *AFS is enabled*.
Tcp-reset:	If the packet dropped is tcp, instead of sending an icmp error packet, a tcp reset packet is sent to each end. To enable this option, enable the AFS feature. Please see bintec manual *Dm786-I AFS*.
Icmp-unreachable	Sends an icmp error when the packet is discarded. This option is automatically applied to configured access-groups when *AFS is not enabled*.

Example:

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

To stop an access control list from being assigned to incoming traffic, execute the same command preceded by **no**.

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

Note

Default behavior when no option is configured for an access-group depends on whether or not the AFS feature is enabled. If AFS is not enabled, the access-group will behave according to the "icmp-unreachable" option. If AFS is enabled, the access-group will behave according to the "silently-discard" option.

Command history:

Release	Modification
11.01.11	The "*icmp-unreachable*" option has been added to the system. Default access-group behavior when no option is configured is described.

2.1.17.2 LOCAL POLICY

Enables policy routing for local traffic. For further information, please see bintec manual *Dm745-I Policy-based Routing*.

Example:

```
IP config>local policy route-map <name>
```

2.1.18 MULTIPATH

If this command is enabled and there are multiple equal-cost paths to a destination, the router will select a path (to route a packet) based on criteria like the relative weight or bandwidth configured in the output interfaces, a circular queue (Round-Robin mode), or depending on the AFS session. The command is disabled by default.

Syntax:

```
IP config>multipath {per-destination | per-packet {relative-weights | round-robin} | per-afs-session}
```

To disable this, use the same command preceded by **no**.

Example:

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

Command history:

Release	Modification
11.00.05	The **multipath per-afs-session** command was introduced as of version 11.00.05.
11.01.00	The **multipath per-afs-session** command was introduced as of version 11.01.00.

2.1.18.1 MULTIPATH PER-DESTINATION

Enables the use of various paths, or next hops, in routes with multipath and establishes session balance. That is, the router selects the next hop depending on the source-destination IP address pair.

Example:

```
IP config>multipath ?
  per-destination    Enable per source and destination multipath routing
  per-packet         Enable per packet multipath routing
  per-afs-session    Per AFS session multipath
IP config>multipath per-destination
IP config>
```

2.1.18.2 MULTIPATH PER-PACKET

Enables the use of various multipath paths. However, unlike what happens with the previous option, the next hop is selected when transmitting each packet (i.e., it's not configured for each source-destination IP address pair).

Syntax:

```
IP config>multipath per-packet {relative-weights | round-robin}
```

2.1.18.2.1 MULTIPATH PER-PACKET RELATIVE WEIGHTS

Allows you to apply a payload balance system, based on relative weights, configured in various output interfaces for paths included in the multipath. Next hop selection, to transmit a given packet, depends on the occupation factor of the interfaces involved (which directly depends on the relative weight or bandwidth configured in these).

Example:

```
IP config>multipath per-packet ?
  per-destination    Enable per source and destination multipath routing
```

```
  per-packet         Enable per packet multipath routing
  per-afs-session    Per AFS session multipath
IP config>multipath per-packet relative-weights
IP config>
```

This balance system aims to maximize the use of interfaces with different bandwidths. However, for good performance, you also need to configure relative weight in interfaces that distribute outgoing traffic.Unless it is specifically configured, this relative weight is considered to be 50 by default. Whenever this parameter is not specified in any of the interfaces in the balance group, behavior is equivalent to selecting multipath per packet with Round-Robin strategy (as the relative bandwidth or capacity for each one is not established with respect to the others).

Example:

```
network ethernet0/0
; -- Ethernet Interface User Configuration --
   ip relative-weight 75
exit
;
network ppp1
; -- Generic PPP User Configuration --
   ip relative-weight 25
   base-interface
; -- Base Interface Configuration --
      base-interface serial0/0 link
;
   exit
;
```

This indicates that if there is a multipath route whose next hops use, respectively, ethernet0/0 and ppp1 output interfaces, 75% of traffic sharing is done through the ethernet0/0 interface and 25% over the ppp1 output interface path. That is, the ethernet0/0 interface is considered to have 3 times more capacity than the ppp1 one.

2.1.18.2.2 MULTIPATH PER-PACKET ROUND-ROBIN

Selects a path where a packet is routed in Round-Robin mode.

Example:

```
IP config>multipath per-packet round-robin
IP config>
```

2.1.18.3 MULTIPATH PER-AFS-SESSION

Enables the use of various paths, or next hops, in multipath routes and establishes session balance. That is, the router selects the next hop depending on the AFS session associated with the incoming packet.

Example:

```
IP config>multipath ?
  per-destination    Enable per source and destination multipath routing
  per-packet         Enable per packet multipath routing
  per-afs-session    Per AFS session multipath
IP config>multipath per-afs-session
IP config>
```

As described in bintec manual *Dm786-I AFS*, when a packet is processed for the first time, AFS tries to find its corresponding session from out of the existing ones. If it can't, a new session is created and assigned to said packet. Furthermore, if *multipath per-AFS-session* is enabled and there are multiple equal-cost paths to a destination, the router assigns a next hop to each new AFS session in a circular queue (Round-Robin mode).

Activate *multipath per-afs-session* as follows.

```
IP config>multipath per-afs-session
```

If a static route configured with *multipath per-afs-session* is deleted during operation, and there were AFS sessions assigned to its next hop, the following occurs: when a packet for each session is rerouted, a new hop belonging to the remaining routes in the multipath is assigned (in Round Robin mode) for said sessions.

The multipath per-afs-session option offers recursive routing. When indirect routes are installed in the routing table, multipath per-afs-session is able to find the path across the routes until a next-hop that belongs to a directly connected network is found.

Command history:

Release	Modification
11.01.07	Recursive *multipath per-afs-session* has been implemented as of version 11.01.07.

2.1.18.3.1 REACTIVE MULTIPATH PER-AFS-SESSION

The current implementation of *multipath per-afs-session* behaves reactively when assigning a new hop to a new AFS session if the *mp-congestion* and/or *mp-disable* options are configured for IPv4 static routes in the multipath. This is described in bintec manual *Dm754-I NSLA*.

```
IP config>ROUTE <address> <mask> <gateway> [<cost>] [TRACK NSLA-ADVISOR <advisor-id>] \
[mp-congestion <advisor-id>] [mp-disable <advisor-id>]
```

The *mp-congestion* and *mp-disable* options both behave similarly. They are able to mark a route with congestion and disabling flags, depending on the result of the configured advisors. The flags are structured hierarchically and can be marked together.

Depending on the flags set, a route can be identified with unmarked, congested or disabled states. A route marked with both congestion and disabling flags is considered disabled. Disabled is a more restrictive state than congested.

The following figure shows a state diagram for routes configured with *multipath per-afs-session*, and the possible transitions between states.

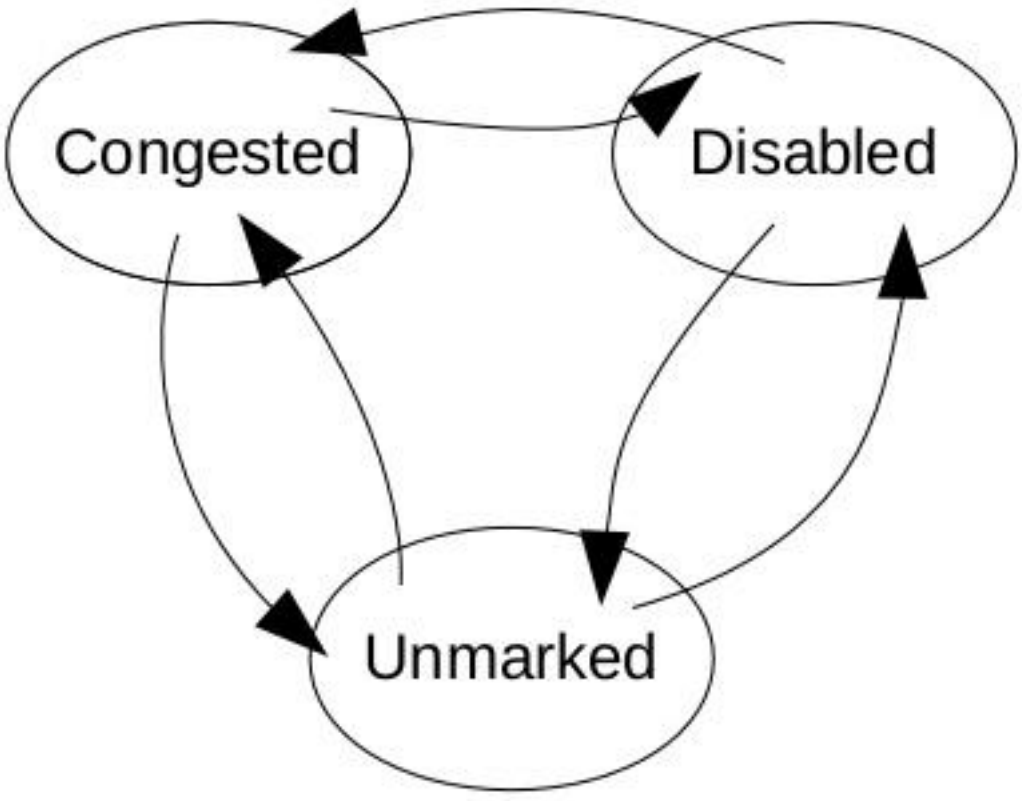


Fig. 3: State diagram

The *mp-congestion* option allows you to link a static route to an advisor. This way, when the advisor output is activated (TRUE), the route is marked as congested (allowing for unmarked routes to be selected in multipath routing instead).

If all routes in a multipath routing were marked as congested, one of them would still be selected.

The *mp-disable* option allows you to link a static route to an advisor. This way, when the advisor output is activated (TRUE), the route is marked as disabled (allowing for congested or unmarked routes to be selected in multipath routing instead).

If all routes in multipath routing were marked as disabled, one of them would still be selected.

If *mp-congestion* and *mp-disable* are configured together for a static route in multipath, each configured advisor de-

termines the state of each respective flag for said route and, as a result, the state of the route in the multipath.

There are no limitations when it comes to configuring the same advisor for several routes, or even for both *mp-congestion* and *mp-disable* at the same time.

In brief, the *multipath per-AFS-session* subsystem behaves as follows: firstly, it tries to select an unmarked route in the multipath; secondly, if no unmarked route is found, the subsystem searches for congested routes; and finally, if no unmarked nor congested routes are found, the system selects a disabled route.

A configuration example using reactive multipath per-afs-session can be found in bintec manual *Dm786-I AFS*.

Command history:

Release	Modification
11.00.05	The **mp-congestion** and **mp-disable** command options were introduced as of version 11.00.05.
11.01.00	The **mp-congestion** and **mp-disable** command options were introduced as of version 11.01.00.

2.1.19 NAT

Accesses different NAT configuration menus.

Syntax:

```
IP config>nat ?
  dynamic      Enter in the dynamic nat configuration menus
  pat          Enter in the pat configuration menus
  static       Enter in the static nat configuration menus
IP config>
```

2.1.19.1 NAT DYNAMIC

Accesses dynamic NAT configuration menus (DNAT). For further information, please see bintec manual *Dm755-I Dynamic NAT Facility* .

Syntax:

```
IP config>nat dynamic
```

Example:

```
IP config>nat dynamic

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

2.1.19.2 NAT PAT

Accesses the NAPT (*Network Address Port Translation*) configuration menus. All the information needed to configure and use this feature can be found in bintec *manual Dm735-I NAPT Facility*.

Syntax:

```
IP config>nat pat
```

Example:

```
IP config>nat pat

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

2.1.19.3 NAT STATIC

Accesses static NAT configuration menus. For further details, please see bintec manual *Dm720-I NAT facility*.

Syntax:

```
IP config>nat static
```

Example:

```
IP config>nat static

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

2.1.20 NO

Negates another command or restores a default configuration for a given parameter.

Syntax:

```
IP config>no <command>
```

To find out how **no** affects a command, please see the appropriate section on each command. An explanation on the impact **no** has on operations is provided, together with an example.

2.1.21 POOL

Configures a range of addresses the router can assign through its PPP connections. Default 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 **no**.

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

2.1.22 PROXY-ARP

Accesses the ARP Proxy configuration menus. For further information, please see bintec manual *Dm734-I Proxy ARP*.

Syntax:

```
IP config>proxy-arp
```

Example:

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

Proxy ARP cnfg>
```

Command history:

Release	Modification
11.00.03	This menu is obsolete as of version 11.00.03. **Proxy-arp** is no longer supported.

2.1.23 PROXY-IGMP

Accesses the IGMP Proxy configuration menus. For further information, please see bintec manual *Dm762-I IGMP Protocol*.

Syntax:

```
IP config>proxy-igmp
```

Example:

```
IP config>proxy-igmp

-- IGMP proxy user configuration --
```

```
IGMP proxy cnfg>
```

2.1.24 ROUTE

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

The destination is specified by an IP address (Network, Subnet, Host) and a mask, or by an FQDN. 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 a packet to the destination.

The next hop may be:

- An IP address pertaining to a network directly connected to a local interface.
- An interface. If an output interface is specified, you can also specify an IP address for the next hop through said interface.
- An IP address, which is accessible through another route from the routing table (indirect routes): recursive routing.
- An IP address a DHCP server assigns to an interface as default route in DHCP option 3. For this route to activate, the DHCP client must be enabled in the interface and must have received DHCP option 3 from the server. When the interface DHCP client is disabled, or the lease provided by the server times out, this route is no longer active.

In addition to the next hop, you can also specify the following parameters for each configured route.

```
distance <10-255>             Specifies the route's administrative distance

track nsla-advisor <1-65535>  Activates the route only when configured nsla poll is active

mp-congestion <1-65535>      Mark the route as congested, but keeping as existing

mp-disable <1-65535>         Mark the route as disabled, but keeping as existing
```

Depending on the output interface, we could find ourselves with the following situations:

Generic output interface

- Static route with the lowest cost and active interface begins to operate.
- If two or more routes fulfill the minimum cost and active output interface requirements and, additionally, have multipath enabled, traffic balance is executed (up to a maximum of 8 routes). If it is not enabled, traffic balance is not carried out.
- If an interface drops or activates, static routes are revised again to make sure that the route entering into operation is the one with the lowest cost and with an active interface.
- Please see below cases specific to FR (DLCI), X25 (routes through NRI) and Dial interfaces.

FR output interface

- Static routes with an FR output interface activate provided they are the lowest cost routes available, the interface is active and the DLCI assigned to the next hop is active. DLCI activity or inactivity depends on the LMI.
- Routes that do not comply with any of the above conditions deactivate.

X.25 output interface

Static routes with an X.25 output interface always activate (provided they are the lowest cost routes available, the interface is active and the NRI that the next hop is associated with is active). NRI activity or inactivity depends on the following points:

- If the BKUP-RCV-TIME parameter value is set to 0, NRIs are always active. Therefore, static routes associated with this are always active whenever they represent the lowest cost.
- If the BKUP-RCV-TIME parameter value is different to 0:
  - (1) On booting the router, all NRIs are active.
  - (2) If a packet is directed to the next hop, then a call is generated.
  - (3) If the call establishes, NRI activates (go to 2).
  - (4) If the call does not establish, then NRI deactivates (and so do the static route or routes associated with it) and the process to retry the call initiates each BKUP-RCV-TIME.
  - (5) If the call establishes, the NRI reactivates and so do all static routes associated with this (go to 2).

Important

If you configure BKUP-RCV-TIME with a value other than 0, at some point extra X.25 calls may be generated due to the “Call Establishment Retry Process”. This can be inconvenient where a Flat Rate has not been contracted. If said parameter is set to 0, call retry is disabled and static routes configured through X.25 are always active.

Dial-PPP and Dial-FR output interface

Static routes with a **Dial** output interface always activate when the following two conditions are met: they are the lowest-cost routes and the interface is active. An interface of this type is always active when it has outgoing calls and a release time without data enabled for values different to 0. Static routes associated with this always activate if they represent the routes with the lowest cost.

Syntax:

```
IP config>route <net, subset or host> <mask> <hop> [cost <cost>] [track nsla-advisor <id>] \
          [mp-congestion <id>] [mp-disable <id>]
```

Warning

When configuring routes with the same *hop*, please do not configure the same *mp-congestion id* and/or *mp-disable id*. Otherwise, the behavior in multipath routing could become unpredictable.

Example:

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

Example:

```
IP config>route 192.168.2.0 255.255.255.0 ethernet0/1 dhcp
IP config>
```

In this example, a route that is accessible through the ethernet0/1 outgoing interface has been configured using, as next hop, the IP address received from the default router in the DHCP client interface.

To delete a static route, use the same command preceded by **no**.

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

Command history:

Release	Modification
11.00.05, 11.01.00	The **mp-congestion** and **mp-disable** command options have been introduced.
11.00.05	The **cost** option has been changed as of version 11.00.05. From now on, it is configured as "cost <value>".
11.01.01	The **cost** option has been changed as of version 11.01.01. From now on, it is configured as "cost <value>".
11.01.04	Having FQDN as destination was introduced as of version 11.01.04.

2.1.25 ROUTER-ID

IP address used by the router as identifier in OSPF (OSPF router-id). This also participates in the selection carried out by the router for the default or global IP address. The router-ID must coincide with one of the interface IP addresses. If not, it is ignored. When ignored, or if the router's default IP address/OSPF router-ID are not configured, then the router-ID matches the first IP address configured in the router.

The default IP address is used by the router as a source IP address for packets originating locally and cannot be associated with a given output interface. This is either because it is multicast traffic or because the output interface does not have an IP address configured (unnumbered interfaces).

The process of selecting the default IP address follows this order:

(1) The internal IP address configured through the **internal-ip-address** command.

(2) The management IP address configured through the **management-ip-address** command.

(3) The IP address configured with the **router-id** command, as long as this address belongs to the active interface.

(4) The first address of the first active interface.

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 timeout, possibly as long as 30 minutes. This may increase the 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 **no**.

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

2.1.26 RULE

Creates IP connections to be used later in the NAPT facility and IPSec protocol.

An IP connection is an extension of the interface concept. It allows 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, a local IP address is enough to define the IP connection. For example, a PPP interface.

In point-to multipoint interfaces, you need to specify the remote IP address as well as the local IP address. For example, in an FR interface defined as point-to-multipoint, which has **Ia1** as source address (through DLCI 16 reaching **Ia2** and through 17 reaching **Ia3**), you can define 2 IP connections, the first being **Ia1-Ia2** and the second **Ia1-Ia3**.

As well as defining an IP connection, a rule can also have an associated NAPT configuration.

When 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 router that is 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, a packet and if NAPT is to be executed or not. This can be left as 0.0.0.0, meaning NAT will be applied over the the interface as a whole (e.g., over all DLCIs belonging to this interface).

If the link is Point-to-Point (e.g., PPP), this address must pertain to the same subnet as the local address. Defining it is unnecessary when the connection is Point-to Point.

Enable NAPT: Allows you to specify whether to enable NAPT for the added rule or not. If this is enabled, you must specify the following parameters relative to NAPT.

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

NAPT entry timer: This is the time, in minutes, the entry remains active in the translation ports table being used in this connection to execute port NAT on a received packet.

Rule <id> napt timeout access-list <list-id> {<value> | infinite}

This command configures a *timeout* value for the packets received that the access *list-id* deems **permitted**.

If you configure an **infinite** option, said entry will never timeout and can only be deleted through the **delete** command found in the monitoring menu of the port

NAT feature. For further information, please see bintec *manual Dm735-I NAPT Feature*.

You can configure up to 25 access lists. They are consulted in the order in which they are configured within a rule. Consequently, the *timeout* value is given by the first access list that matches the packet.

Rule <id> napt timeout all <value>

Use this command to specify the *timeout* value to apply to all the packets received that do not match an access list. If you configure said *timeout*, values configured using the following options are ignored.

Rule <id> napt timeout {tcp-syn | tcp-fin | tcp | tcp-rst | udp | icmp | pptp} <value>

Use this command to configure applicable time values, depending on the type of packet received. The following table contains the options available to identify different types of packets:

Option	Description
tcp-syn	Applied to TCP synchronous transmission packets. Default is 2 minutes.
tcp-fin	Applied to TCP finish packets. Default is 1 minute.
tcp-rst	Applied to TCP reset packets. Default is 1 minute.
tcp	Applied to packets in a TCP traffic flow. Default is 270 minutes.
udp	Applied to packets in a UDP traffic flow. Default is 5 minutes.
icmp	Applied to packets in an ICMP traffic flow. Default is 3 minutes.
pptp	Applied to packets in a PPTP traffic flow. Default is 150 minutes.

Rule <id> napt timeout <value>

The value configured using this command is applied to packets that do not match any of the previous criteria. Default is 3 minutes.

Firewalling capacity: This ensures the router is inaccessible for the connection defined in this rule, except through translation port table entries or through NAPT exceptions associated with this rule. Where this is enabled, the router won't be able to carry out outgoing connections using the NAPT source address or the interface address, i.e., connections where NAPT is not executed.

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

Access Control List: Through a generic access list, this allows you to select IP traffic that will have NAPT applied to it.

Syntax:

```
IP config>rule <id>
no
        napt
               access-list       Associated access list
               firewall          Firewall behavior
               timeout           Timeout of the napt translation
                  access-list    Timeout for packets permitted by the access list
                  tcp-fin        Timeout after a finish TCP packet
                  tcp            NAPT translation timeout for TCP flows
                  tcp-rst        Timeout after a reset TCP packet
                  tcp-syn        Timeout after a synchronous transmission TCP packet
                  udp            NAPT translation timeout for UDP flows
                  icmp           NAPT translation timeout for ICMP flows
                  pptp           NAPT translation timeout for PPTP flows
                  all            Forced timeout of NAPT translation for all flows
               translation       Apply napt translation
               tcp-adjust-mss    Adjust the mss of transit packets
local-ip       local ip of this rule
        remote-ip      remote 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
            access-list    Timeout for packets permitted by the access list
                  <1..1999>    Access list number
                        <1..2880>    Timeout value in minutes
                        infinite     Timeout never expires
            tcp-fin        Timeout after a finish TCP packet
            tcp            NAPT translation timeout for TCP flows
            tcp-rst        Timeout after a reset TCP packet
            tcp-syn        Timeout after a synchronous transmission TCP packet
            udp            NAPT translation timeout for UDP flows
            icmp           NAPT translation timeout for ICMP flows
            pptp           NAPT translation timeout for PPTP flows
            all            Forced timeout of NAPT translation for all flows
        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
```

No: Disables firewalling or NAPT in the rule with identifier **<id>**, >, eliminating access control list assignment to select IP traffic where NAPT is applied, or disabling MSS adjustment in the TCP SYN packets.

Example:

To create an 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 local-ip 213.4.21.187 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 **no**.

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

2.1.27 TVRP

Accesses the TVRP configuration menus. For further information, please see bintec manual *Dm725-I TVRP Protocol*.

Syntax:

```
IP config>tvrp
```

Example:

```
IP config>tvrp

-- TVRP Configuration --
TVRP config>
```

2.1.28 VRF

Configures IP in a routing/forwarding domain in virtual private networks (VPN). For further information, please see bintec manual *Dm775-I VRF.*

2.1.29 VRRP

Accesses the VRRP configuration menus. For further information, please see bintec manual *Dm759-I VRRP Protocol*.

Syntax:

```
IP config>vrrp
```

Example:

```
IP config>vrrp

-- Virtual Router Redundancy Protocol configuration --
```

```
VRRP config>
```

2.1.30 EXIT

Returns to the previous prompt level.

Syntax:

```
IP config>exit
```

Example:

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

2.2 Configuring IP per interface

IP-related configuration commands are specified here and are available in configuration menus for interfaces that support IP configuration. Configuring IP parameters is logical in interfaces that support the protocol and constitute the highest point in the base interface stack over which it is mounted.

The following IP configuration commands are available:

Command	Function
ACCESS-GROUP	Configures access control per interface.
ADDRESS	Configures IP addresses in interfaces.
AFS	Configures an AFS firewall in interfaces.
BROADCAST-ADDRESS	Specifies the broadcast address format used by the router in a given interface.
DHCP-RELAY	Specifically configures the DHCP-Relay agent per interface.
ICMP	Enables ICMP Redirect and/or ICMP Unreachable message sending through an interface.
IGMP	Configures IGMP-related parameters.
MTU	Configures the maximum size of IP packets transmitted through this interface.
PIM	Configures parameters related to the PIM protocol.
POLICY	Enables Policy Routing in an interface.
PROXY-ARP	Configures ARP Proxy parameters associated with one of the interface addresses.
RELATIVE-WEIGHT	Establishes relative weight for the interface, used where multipath per packet is enabled, with payload distribution proportional to the capacity of the interfaces involved.
SOURCE-ROUTING	Enables source routing processing.
TCP	Configures various TCP-related parameters.
TVRP	Configures a TVRP group.
UDP	Configures functions related to UDP.
VERIFY	Verifies IP options.
VRF	Configures parameters related to routing and forwarding in virtual private networks (VPN).
VRRP	Configures a VRRP virtual router.

Access these commands by entering **ip** and the required command from the configuration menu for the interface in question.

Example:

```
Config>network ethernet0/0

-- Ethernet Interface User Configuration --
ethernet0/0 config>ip ?
  access-group         Specify per-interface access control system
  address              Assign an ip address
  afs                  Configure AFS parameters
  broadcast-address    Set the ip broadcast format
  dhcp-relay           Enable the DHCP-Relay agent
  flow                 NetFlow related commands
```

```
  icmp                ICMP parameters
  igmp                IGMP protocol interface commands
  mtu                 Set ip maximum transmission unit
  pim                 PIM protocol related commands
  policy              Enable policy routing on an interface
  proxy-arp           Proxy ARP interface commands
  relative-weight     Set interface relative weight
  source-routing      Enables source routing processing
  tcp                 TCP parameters
  tvrp                TVRP configuration parameters
  udp                 UDP parameters
  verify              Verify IP options
  vrf                 VPN Routing/Forwarding parameters on the interface
  vrrp                VRRP configuration parameters
ethernet0/0 config>
```

To reverse the effect of these commands, simply put **no ip** in front of each one. This returns the default value to the corresponding IP parameter or deletes pre-added configuration elements.

Example:

```
ethernet0/0 config>no ip ?
  access-group        Specify per-interface access control system
  address             Assign an ip address
  afs                 Configure AFS parameters
  broadcast-address   Set the ip broadcast format
  dhcp-relay          Enable the DHCP-Relay agent
  flow                NetFlow related commands
  icmp                ICMP parameters
  igmp                IGMP protocol interface commands
  mtu                 Set ip maximum transmission unit
  pim                 PIM protocol related commands
  policy              Enable policy routing on an interface
  proxy-arp           Proxy ARP interface commands
  relative-weight     Set interface relative weight
  source-routing      Enable process source routing
  tcp                 TCP parameters
  tvrp                TVRP configuration parameters
  udp                 UDP parameters
  verify              Verify IP options
  vrf                 VPN Routing/Forwarding parameters on the interface
  vrrp                VRRP configuration parameters
ethernet0/0 config>
```

2.2.1 ACCESS-GROUP

Configures the IP access control system per interface.

Syntax:

```
<interface_name> config>ip access-group <access_list> {in | out}
                                        [silently-discard | tcp-reset | icmp-unreachable]
```

In	Applies the generic access control list to traffic entering the interface.
Out	Applies the generic access control list to traffic exiting the interface.
Silently-discard	Instead of sending an icmp error packet, the packet is simply discarded. To enable this option, the AFS feature must be enabled. Please see bintec manual *Dm786-I AFS*. This option is automatically applied to configured access-groups when *AFS is enabled*.
Tcp-reset	If the dropped packet is tcp, instead of sending an icmp error packet, a tcp reset packet is sent to each end. To enable this option, pre-enable the AFS feature. Please see bintec manual *Dm786-I AFS*.
Icmp-unreachable	Sends an icmp error when the packet is discarded. This option is automatically applied to configured access-groups when *AFS is not enabled*.

Example:

```
ethernet0/0 config>ip access-group 101 in
ethernet0/0 config>ip access-group 102 out
```

```
ethernet0/0 config>
```

To eliminate a per-interface access control, use the same command preceded by **no**.

Example:

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

Note

Default behavior when no option is configured for an access-group depends on whether or not the AFS feature is enabled. If AFS is not enabled, the access-group will behave according to the "icmp-unreachable" option. If AFS is enabled, the access-group will behave according to the "silently-discard" option.

Command history:

Release	Modification
11.01.11	The "*icmp-unreachable*" option has been added to the system. Default access-group behavior when no option is configured is described.

2.2.2 ADDRESS

Assigns an IP address to the interface. An interface does not receive or transmit packets until it has, at least, one IP address.

Three IP address types can be distinguished:

- **Numbered addresses:** the format for these is explained in *Introduction* on page 2, and varies according to their class (A, B, C or D). You configure this type of address by introducing the address itself, together with the subnet mask. For example, if the address is a Class B network, by using the third byte for the subnet the mask can be 255.255.255.0.

Syntax:

```
<interface_name> config>ip address <IP_address> <IP_mask> [secondary]
```

An interface can have one primary address and multiple secondary addresses (configured through the **secondary** option). Packets generated by the router always use the primary address. Therefore, all routers connected in the same segment must have primary addresses for the same network. Secondary addresses are treated like primaries, except the router never generates datagrams other than routing updates whose source addresses are secondary IP addresses.

Example:

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

Warning

No check is carried out to see whether the configured IP address overlaps the IP address of another interface. This is because, in certain cases such as interface backup (WRR), IP address overlapping is permitted.

- **Unnumbered addresses**: the value for these addresses is the interface number itself and they can only be used in point-to-point interfaces. In this case, you need to enter **unnumbered** instead of the IP address and subnet mask.

Syntax:

```
<point_to_point_interface_name> config>ip address unnumbered [<interface_name>]
```

When the router generates traffic, it needs to determine the source address for said traffic. The IP address of the output interface is normally used. However, if this is unnumbered, the IP address of a different interface must be used.

By using the **<interface_name>** parameter, you can specify which interface IP address should be used when necessary.

Unnumbered addresses must use a real address for packet source, transmitted through the corresponding interface.

Choosing the interface from which the address is taken is possible by specifically indicating this when configuring the unnumbered address.

Example:

```
ppp1 config>ip address unnumbered
```

Where you do not specify the **<interface_name>** parameter, the router generates traffic with the *global IP address* as source. The global IP address is the internal IP address, if configured, or, by default, the first configured IP address.

- **Addresses acquired through DHCP:** if you configure this type of **dhcp-negotiated** address in an Ethernet interface or subinterface, you enable the possibility of dynamically acquiring an address through DHCP in said interface (i.e., enable the DHCP client feature).

Syntax:

```
<name_int/subint_eth> config>ip address dhcp-negotiated
```

Example:

```
ethernet0/0 config>ip address dhcp-negotiated
ethernet0/0 config>
```

Please note that, when using a **dhcp-negotiated** address in an interface, you cannot use another numbered or unnumbered address simultaneously.

For further information on DHCP, please see bintec manual *Dm730-I DHCP Protocol*.

To delete an address, use the same command preceded by **no**.

```
ethernet0/0 config>no ip address ?
  <a.b.c.d>          New address
  dhcp-negotiated    dhcp-negotiated
  unnumbered         unnumbered
  <cr>
ethernet0/0 config>no ip address
ethernet0/0 config>
```

2.2.3 AFS

Configures a firewall using AFS. The firewall acts on the INPUT chain, meaning that all packets entering through the interface will be filtered. You can relax the filter to allow certain traffic to enter the system by setting exclusions. Two types of exclusions can be configured: one to allow packets containing IPsec information and the other to allow packets matching a specific access-list.

By default, the filter criteria to drop a packet is that the incoming packet does not belong to an established AFS session or match any static NAT rules. This criteria can be relaxed via the exclusion system, which is checked before verifying whether the packet matches any static NAT rules. The packet is accepted if it matches any of the exclusions configured.

A passive exclusion has been created to allow DHCP packets that provide an IP address to bypass the firewalled interface. This is only effective when the interface has been configured so that its IP address can be obtained via DHCP.

Syntax:

```
<interface_name> config>ip afs {firewall} {in} [exclude [ipsec | access-list <access-list number>]]
```

Command history:

Release	Modification
11.01.07	The "*afs*" command was introduced as of version 11.01.07.
11.01.07	The "*IPsec*" suboption became "*ipsec*" as of version 11.01.07.

2.2.3.1 Exclude

This option can be configured to exclude certain traffic from being filtered. It modifies the filter criteria to exclude traffic that contains IPsec information or packets that match a specific access-list. If the packet matches any of the configured exclusions, it will be accepted. The configuration is as follows:

Syntax:

```
<interface_name> config>ip afs {firewall} {in} exclude ?
  ipsec          Exclude IPsec traffic
  access-list    Exclude an access-list
  <cr>
<interface_name> config>
```

Command history:

Release	Modification
11.01.07	The "*exclude*" option under the "*ip afs firewall in*" command was introduced as of version 11.01.07.
11.01.07	The "*IPsec*" suboption became "*ipsec*" as of version 11.01.07.

2.2.3.1.1 IPsec

This exclusion checks whether packets contain IPsec information or belong to any of the protocols involved in the IPsec communication process.

Syntax:

```
<interface_name> config>ip afs firewall in exclude ipsec
```

Command history:

Release	Modification
11.01.07	The "*IPsec*" suboption under the "*exclude*" option was introduced as of version 11.01.07.
11.01.07	The "*IPsec*" suboption became "*ipsec*" as of version 11.01.07.

2.2.3.1.2 Access List

This exclusion checks whether the packet matches the access-list specified to be accepted. This option must be configured carefully because it can revert what the firewall intends to do.

Syntax:

```
<interface_name> config>ip afs firewall in exclude access-list <access-list number>
```

Command history:

Release	Modification
11.01.07	The "*access-list*" suboption under the "*exclude*" option was introduced as of version 11.01.07.

2.2.4 BROADCAST-ADDRESS

Specifies the IP broadcast format the router uses for a given 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 LOCAL-WIRE or NETWORK. LOCAL-WIRE value. Broadcast addresses are either all ones (255.255.255.255) or all zeros (0.0.0.0). The NETWORK style broadcast begins 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 references 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:

```
<interface_name> config>ip broadcast-address ?
  network-zero-filled    Zero filled network type broadcast
  network-one-filled     One filled network type broadcast
  0.0.0.0                Zero filled local wire broadcast
  255.255.255.255        One filled local wire broadcast
```

2.2.4.1 BROADSCAST-ADDRESS NETWORK-ZERO-FILLED

Configures *style address* as NETWORK. The NETWORK address begins with the number of the network and the interface subnet. The *fill pattern for wildcard part* in this case is 0: you need to fill out the rest of the broadcast address (except for the network and subnet) with zeros. This is the value the broadcast addresses take by default.

Syntax:

```
<interface_name> config>ip broadcast-address network-zero-filled ip-address
{<IP_addr> | dhcp-negotiated | unnumbered}
```

Example:

Broadcast address 172.24.0.0. has been used here.

2.2.4.2 BROADCAST-ADDRESS NETWORK-ONE-FILLED

Configures *style address* as NETWORK. The NETWORK address begins with the number of the network and the interface subnet. The *fill pattern for wildcard part* in this case is 1: you need to fill out the rest of the broadcast address (except for the network and subnet) with ones.

Syntax:

```
<interface_name> config>ip broadcast-address network-one-filled ip-address {<IP_address> |
dhcp-negotiated | unnumbered}
```

Example:

```
ethernet0/0 config>ip broadcast-address network-one-filled ip-address 172.24.78.36
ethernet0/0 config>
```

In the previous example, the broadcast address was configured as 172.24.255.255.

To return to the default configuration for the command (NETWORK broadcast address with 0 pattern), execute the same command preceded by **no**.

Example:

```
ethernet0/0 config>no ip broadcast-address network-one-filled ip-address 172.24.78.36
ethernet0/0 config>
```

2.2.4.3 BROADCAST-ADDRESS 0.0.0.0

Configures *style address* as **local-wire** and broadcast addresses with all zeros (0.0.0.0).

Syntax:

```
<interface_name> config>ip broadcast-address 0.0.0.0 ip-address {<IP_address> |
dhcp-negotiated | unnumbered}
```

The following example configures a 0.0.0.0 broadcast address.

Example:

```
ethernet0/0 config>ip broadcast-address 0.0.0.0 ip-address 172.24.78.36
ethernet0/0 config>
```

To return to the default configuration, execute the same command preceded by **no**.

Example:

```
ethernet0/0 config>no ip broadcast-address 0.0.0.0 ip-address 172.24.78.36
ethernet0/0 config>
```

2.2.4.4 BROADCAST-ADDRESS 255.255.255.255

Configures *style address* as **local-wire** and broadcast addresses with all ones (255.255.255.255).

Syntax:

```
<interface_name> config>ip broadcast-address 255.255.255.255 ip-address
{<IP_address> | dhcp-negotiated | unnumbered}
```

Example:

```
ethernet0/0 config>ip broadcast-address 255.255.255.255 ip-address 172.24.78.36
ethernet0/0 config>
```

This example configures a 255.255.255.255 broadcast address.

To return to the default configuration, execute the same command preceded by **no**.

Example:

```
ethernet0/0 config>no ip broadcast-address 255.255.255.255 ip-address 172.24.78.36
ethernet0/0 config>
```

2.2.5 DHCP-RELAY

Specifically enables a relay agent in the interface during configuration, using the parameters entered. There are two separate possibilities to enable DHCP-Relay in the interface.

Syntax:

```
<interface_name> config>ip dhcp-relay ?
  global              Enable the DHCP relay agent with global configuration
  server              Add a new DHCP server or change an existing one
  update              Update a level indicator
  monitor-options     Configure options for relay monitoring
  smart-relay         Configure DHCP Smart-Relay options
```

2.2.5.1 DHCP-RELAY GLOBAL

Enables a DHCP-Relay agent in the interface during configuration, using the parameters entered in the DHCP configuration menu (please see manual *Dm730-I DHCP Protocol*).

Syntax:

```
<interface_name> config>ip dhcp-relay global
```

Example:

```
ethernet0/0 config>ip dhcp-relay global
ethernet0/0 config>
```

To disable the DHCP-Relay agent in the interface, enter **no**.

Example:

```
ethernet0/0 config>no ip dhcp-relay global
ethernet0/0 config>
```

2.2.5.2 DHCP-RELAY SERVER

Enables a DHCP-Relay agent in the interface during configuration using specific parameters. In each command input, specify the DHCP server IP address where the DHCP packets are to be forwarded. You can define various DHCP servers.

Optionally, specify the VRF name used to access the DHCP server when the latter is not in the VRF associated with the interface being configured, and where there is a specified **token** to refer to the VRF global table: **global-vrf**.

Syntax:

```
<interface_name> config>ip dhcp-relay server [global-vrf | vrf <VRF_Name>] <IP_addr>
[giaddr <IP_addr> | source-address <IP_addr>]
```

Example:

```
ethernet0/0 config>ip dhcp-relay server 192.168.1.25 giaddr 192.168.1.40
ethernet0/0 config>ip dhcp-relay server vrf server-2 192.168.2.25
ethernet0/0 config>
```

In this example, we have enabled a relay agent in the **ethernet0/0** interface using address 192.168.1.25 as DHCP server. Optionally, we have configured the **giaddr** value (DHCP protocol field that uses relay agents to authenticate via a DHCP server). In the second line, we have configured a second server located in VRF **server-2**, only specifying the server IP address.

2.2.5.3 DHCP-RELAY UPDATE

Updates an NSLA level indicator to a certain value when a change in the state of the relay agent occurs. The indicator increases by said value when the agent detects that none of its DHCP servers is accessible (when the state changes to DOWN). The indicator decreases by the same value conversely (i.e., when the agent returns to an UP state). To configure an indicator through NSLA, please see bintec manual *Dm704-I NSLA*. For further information on relay agent monitoring, please see bintec manual *Dm730-I DHCP Protocol*.

Syntax:

```
<interface_name> config>ip dhcp-relay update level-indicator <1..255> value <1..255> when-down
```

Example:

```
ethernet0/0 config>ip dhcp-relay update level-indicator 1 value 10 when-down
ethernet0/0 config>
```

2.2.5.4 DHCP-RELAY MONITOR-OPTIONS

Configures parameters that regulate server monitoring in a relay agent. Said monitoring only activates if the relay agent has been configured to update an NSLA level indicator when a change in state occurs.

Syntax:

```
<interface_name> config>ip dhcp-relay monitor-options?
  packets-threshold    Number of sent packets without response
  interval             Time interval between servers monitoring
  always-on            Set servers monitoring always enable
```

2.2.5.4.1 packet-threshold

Establishes the threshold for DHCPDISCOVER packets transmitted in a relay agent server, without receiving a response from the latter. Once said threshold is reached, the agent considers the server is down.

Syntax:

```
<interface_name> config>ip dhcp-relay monitor-options packets-threshold <1..255>
```

Default is 10 packets.

2.2.5.4.2 interval

Configures the time interval between the consecutive sending of two DHCPDISCOVER packets internally generated by the relay agent due to the server's monitoring process.

Syntax:

```
<interface_name> config>ip dhcp-relay monitor-options interval <1s..1h>
```

2.2.5.4.3 always-on

Ensures periodic monitoring of the server is always active in the relay agent, instead of waiting until all its servers are down.

Syntax:

```
<interface_name> config>ip dhcp-relay monitor-options always-on
```

By default, this monitoring mode is deactivated.

Note

If this option is not configured, monitoring only initiates when all servers for a Relay agent are considered down.

2.2.5.5 DHCP-RELAY SMART-RELAY

Configures the parameters that regulate the "Smart-Relay" functionality in a Relay Agent. The "Smart-Relay" functionality allows the router to automatically modify the giaddr value. If the router sends requests (using the first IP address for the interface through which the client petition was received, or the router's global address if no other address is configured in the giaddr field of this interface) and doesn't get a response, it will move on and start using the second IP in the giaddr field instead.

Syntax:

```
<interface_name> config>ip dhcp-relay smart-relay ?
  enable               Enable the DHCP Smart-Relay
  packets-threshold    Number of packets sent without response
```

Command history:

Release	Modification
11.01.13	The "*smart-relay*" option has been introduced as of version 11.01.13.

2.2.5.5.1 enable

Enables the Smart-Relay functionality.

Syntax:

```
<interface_name> config>ip dhcp-relay smart-relay enable
```

2.2.5.5.2 packet-threshold

Establishes the threshold for DHCPDISCOVER packets transmitted in a Relay Agent server without receiving a response from the latter. Once this threshold is reached, the agent considers the server is down and the Relay Agent changes the Relay Agent's IP address.

Syntax:

```
<interface_name> config>ip dhcp-relay smart-relay packets-threshold <1..255>
```

The default value is 10 packets.

2.2.6 ICMP

Allows you to enable ICMP Redirect and/or ICMP Unreachable message sending through the configured interface.

Syntax:

```
<interface_name> config>ip icmp {redirects | unreachables}
```

To disable the sending of said messages, use the **no ip icmp redirects** or the **no ip icmp unreachables**commands, depending on the type of message you wish to disable.

Syntax:

```
<interface_name> config>no ip icmp {redirects | unreachables}
```

2.2.6.1 ICMP REDIRECTS

Enables ICMP Redirect message sending in this interface.

Example:

```
ethernet0/0 config>ip icmp ?
  redirects       Enable sending ICMP Redirect messages
  unreachables    Enable sending ICMP Unreachable messages
ethernet0/0 config>ip icmp redirects
ethernet0/0 config>
```

ICMP Redirect message sending is enabled by default.

To disable ICMP Redirect messages being sent out through this particular interface, use the same command preceded by **no**.

Example:

```
ethernet0/0 config>no ip icmp redirects
ethernet0/0 config>
```

2.2.6.2 ICMP UNREACHABLES

Enables ICMP Unreachable message sending in this interface.

Example:

```
ethernet0/0 config>ip icmp unreachables
ethernet0/0 config>
```

ICMP Unreachable message sending is enabled by default.

To disable ICMP Unreachable message sending through this interface, use the same command preceded by **no**.

Example:

```
ethernet0/0 config>no ip icmp unreachables
ethernet0/0 config>
```

2.2.7 IGMP

Configures various IGMP parameters in the interfaces. For further information, please see bintec manual *Dm762-I IGMP Protocol*.

2.2.8 MTU

Configures the maximum size of IP packets transmitted through this interface. The values allowed range between 68 and the mtu interface (or between 68 and 65535 if the interface doesn't have a configurable mtu).

Syntax:

```
ifcX config>ip mtu <mtu>
```

Example:

```
tnip1 config>ip mtu 1500
tnip1 config>
```

To delete a value established for the MTU interface, enter **no ip mtu**.

Example:

```
tnip1 config>no ip mtu
tnip1 config>
```

2.2.9 PIM

Configures various PIM parameters in the interfaces. For further information, please see bintec manual *Dm804-I PIM Protocol*.

2.2.10 POLICY

Enables Policy Routing in the interfaces. For further information, please see bintec manual *Dm745-I Policy-Based Routing*.

2.2.11 PROXY-ARP

Allows you to enable and configure several ARP Proxy parameters associated with an interface address.

For further information, please see bintec manual *Dm734-I ARP Proxy*.

2.2.12 RELATIVE-WEIGHT

Establishes the relative weight for an interface. This parameter is used when weighted traffic balance is enabled. Relative weight represents the relative bandwidth or capacity between interfaces participating in the balance group and in the payload distribution (proportionally carried out based on the configured value).

Values between 1 and 100 are allowed. If this parameter is not configured, default is 50.

Syntax:

```
<interface_name> config>ip relative-weight <weight>
```

Example:

```
ethernet0/0 config>ip relative-weight 25
ethernet0/0 config>
```

no ip relative-weight re-establishes the default value for the interface's relative weight (50).

Example:

```
ethernet0/0 config>no ip relative-weight
ethernet0/0 config>
```

2.2.13 SOURCE-ROUTING

Enables source routing processing. If this option is enabled, IP addresses that come up as options in packets are processed. This is disabled by default.

Syntax:

```
<interface_name> config>ip source-routing
```

Example:

```
ethernet0/0 config>ip source-routing
ethernet0/0 config>
```

no ip source-routing re-establishes the default value.

Example:

```
ethernet0/0 config>no ip source-routing
ethernet0/0 config>
```

Command history:

Release	Modification
11.01.07	The "*source-routing*" command was introduced as of version 11.01.07.

2.2.14 TCP

Configures various TCP-related parameters.

Syntax:

```
<interface_name> config>ip tcp ?
  adjust-mss    Adjust the mss of transit packets
```

To reestablish default values for TCP parameters, enter **no ip tcp**.

Syntax:

```
<interface_name> config>no ip tcp ?
  adjust-mss    Adjust the mss of transit packets
```

2.2.14.1 TCP ADJUST-MSS

Allows you to alter the TCP SYN packet MSS value to control the maximum size for this connection (normally limited to the MTU output interface, minus 40). Allowed values range from 500 to 1460.

Syntax:

```
<interface_name> config>ip tcp adjust-mss <mss>
```

Example:

```
ethernet0/0 config>ip tcp adjust-mss 1460
```

```
ethernet0/0 config>
```

The **no ip tcp adjust-mss** command ensures the TCP SYN packet MSS value is not altered when passing through the router.

Example:

```
ethernet0/0 config>no ip tcp adjust-mss
ethernet0/0 config>
```

2.2.15 TVRP

Configures a TVRP group. For further information, please see bintec manual *Dm725-I TVRP Protocol*.

2.2.16 UDP

Configures various UDP-related parameters.

Syntax:

```
<interface_name> config>ip udp ?
  broadcast-forward    Specify UDP broadcast forwarding
```

To re-establish default values for UDP parameters, enter **no ip udp**.

Syntax:

```
<interface_name> config>no ip udp ?
  broadcast-forward    Specify UDP broadcast forwarding
```

2.2.16.1 UDP BROADCAST-FORWARD

Allows you to configure the resending of UDP broadcast packets received in a specific port.

Resending is done by replacing the destination's IP address with the one configured, and routing it to said address.

Syntax:

```
<interface_name> config> ip udp broadcast-forward <destination_port> [global-vrf |
vrf <vrf_name>] <destination_address>
```

<destination_port>:	Resending applied to UDP packets with said port as destination.
global-vrf:	Packets resent to the global vrf.
<vrf_name>:	Name of the vrf where packets are going to be resent.
<destination_address>:	IP address where packets are going to be resent.

You can configure several resending addresses for the same UDP port. A copy of the packet is sent to each configured address.

Example:

We have a router with two configured interfaces:

(1) ethernet0/0: 172.24.78.116/16

(2) ethernet0/1: 192.168.222.116/24

We want routers in one network to see routers in the other network through NetBIOS. To do this, configure UDP packet resending in ports 137 and 138. The minimum configuration would be:

```
   log-command-errors
   no configuration
;
   network ethernet0/0
      ; Direccion y red directamente conectada
      ip address 172.24.78.116 255.255.0.0
      ; Reenvio de los paquetes NetBIOS broadcast
                     ip udp broadcast-forward 137 192.168.222.255
                     ip udp broadcast-forward 138 192.168.222.255
   exit
;
```

```
   network ethernet0/1
      ; Direccion y red directamente conectada
      ip address 192.168.222.116 255.255.255.0
      ; Reenvio de los paquetes NetBIOS broadcast
      ip udp broadcast-forward 137 172.24.255.255
      ip udp broadcast-forward 138 172.24.255.255
   exit
;
   dump-command-errors
   end
```

For this scenario to work, devices must also be correctly configured. For example, in Windows XP we had to change the Firewall configuration to allow *Share files and printers* in remote networks.

2.2.17 VERIFY

Displays IP verify options.

Syntax:

```
<interface_name> config> ip verify ?
  unicast    Verify unicast IP options
```

2.2.17.1 VERIFY UNICAST

Displays IP verify unicast options.

Syntax:

```
<interface_name> config> ip verify unicast ?
  reverse-path    Verify unicast reverse router
```

2.2.17.1.1 Verify unicast reverse-path

Provides a defense mechanism against IP spoofing.

As soon as this option is enabled, the router examines all packets received by the interface to ensure the source address is in the routing table. All traffic from an IP address *not* routed by the input interface is dropped.

Syntax:

```
<interface_name> config> ip verify unicast reverse-path
```

Example:

```
ethernet0/0 config>ip verify unicast reverse-path
ethernet0/0 config>
```

You can eliminate this option from the configuration using the **no ip unicast reverse path** command.

Example:

```
ethernet0/0 config>no ip verify unicast reverse-path
ethernet0/0 config>
```

2.2.18 VRF

Configures parameters related to *routing* and *forwarding* in virtual private networks (VPN).

Syntax:

```
<interface_name> config>ip vrf ?
  forwarding    Configure forwarding table
```

To delete a preconfiguration for parameters related to *routing* and *forwarding* in virtual private networks (VPN), use the **no ip vrf** command.

Syntax:

```
<interface_name> config>no ip vrf ?
  forwarding    Configure forwarding table
```

Command history:

Release	Modification
11.01.09	This command is obsolete as of version 11.01.09. The **VRF** command should be used instead of the obsolete **IP VRF** command. For further information, refer to bintec manual *Dm772-I Common Configuration for Interfaces*.

2.2.18.1 VRF FORWARDING

Associates the interface with a *routing* and *forwarding* table or instance (VRF, *Virtual Routing/Forwarding*), specified by name or identifier.

Syntax:

```
<interface_name> config>ip vrf forwarding <table_name>
```

Example:

```
ethernet0/0 config>ip vrf forwarding private
ethernet0/0 config>
```

To delete an association between the interface and a *routing* and *forwarding* table or instance (VRF, *Virtual Routing/Forwarding*), use **no ip vrf forwarding**.

Syntax:

```
<interface_name> config>no ip vrf forwarding <table_name>
```

Example:

```
ethernet0/0 config>no ip vrf forwarding private
ethernet0/0 config>
```

Command history:

Release	Modification
11.01.09	This command is obsolete as of version 11.01.09. The **VRF** command should be used instead of the obsolete **IP VRF** command. For further information, refer to bintec manual *Dm772-I Common Configuration for Interfaces*.

2.2.19 VRRP

Configures a VRRP virtual router. For further information, please see bintec manual *Dm759-I VRRP Protocol*.

2.3 Echo-responder Service

An echo service is a very useful measuring and debugging tool. It simply returns any data it receives to the original source from each VRF.

- *Echo service based on TCP*

The server waits for TCP connections in port TCP7. Once the connection is established, any data received is returned. This continues until the client terminates the connection.

- *Echo service based on UDP*

The server waits for UDP datagrams in port UDP 7. When a datagram is received, the data is returned in a response datagram.

The echo service implemented in bintec routers is *Echo service based on UDP*.

2.3.1 Configuring the echo-responder service

Configures the echo service in the *Echo-Responder* global configuration menu. You can activate the echo service based on UDP in said configuration menu.

Access the *Echo-Responder* configuration menu from the router configuration console. To access said menu, use the following sequence of commands:

```
*config
```

```
configuration environment
Config>feature echo-responder

-- ECHO user configuration --
ECHO config>
```

The commands available in the *Echo-Responder* configuration menu are:

```
ECHO config>?
  echo-responder    Configure Echo responder
  no                Negate a command or set its defaults
  vrf               VPN Routing/Forwarding parameters on the interface
  exit
```

2.3.2 Configuration commands

Describes the *Echo-Responder* configuration commands.

The configuration commands available in the *Echo-Responder* configuration menu are:

Command	Function
? (HELP)	Lists the available commands or their options.
ECHO-RESPONDER	Activates echo service.
NO	Deletes a command or sets its default value.
VRF	VPN Routing/Forwarding parameters on the interface.
EXIT	Returns to the configuration menu.

2.3.2.1 ECHO-RESPONDER

Allows you to configure the echo service and define which type you wish to initiate. Currently, the only echo service available is the one based on UDP.

Syntax:

```
ECHO config>echo-responder ?
  udp    Initiate the service udp-based echo
```

Example:

```
ECHO config>echo-responder udp
ECHO config>
```

2.3.2.2 VRF

Allows you to configure the echo service via VRF. Also, the only echo service available is the one based on UDP.

Syntax:

```
ECHO config>vrf ?
  <1..32 chars>    VPN Routing/Forwarding instance name
ECHO config>
```

Example:

```
ECHO config>vrf ?
  <1..32 chars>    VPN Routing/Forwarding instance name
ECHO config>vrf test ?
  <cr>
ECHO config>vrf test

-- VRF ECHO user configuration --
ECHO vrf config>?
  echo-responder    Configure Echo responder
  no                Negate a command or set its defaults
  exit
ECHO vrf config>echo-responder ?
  udp    Initiate the service udp-based echo
ECHO vrf config>echo-responder udp
```

```
ECHO vrf config>
```

Command history:

Release	Modification
11.01.08	The "*vrf*" command has been introduced as of version 11.01.08.

Chapter 3 Monitoring

3.1 IP Protocol Monitoring Commands

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

Check the IP monitoring commands at the IP prompt: *IP+*. To access said prompt, enter:

```
*p 3
Console Operator
+protocol ip
-- IP protocol monitor --
IP+
```

Command	Function
? (HELP)	Lists all commands and their options.
ACCESS-CONTROL	Monitors the IP access control mode, together with the configured access control records (obsolete as of version 11.00.03).
AGGREGATION-ROUTE	Displays configured aggregation routes.
BPING	Executes a ping to each host in a specified network (also known as ping broadcast).
CACHE	Displays the routing table in the cache memory.
COUNTERS	Lists various IP statistics, including routing error and packets dropped counters.
DUMP-ROUTING-TABLE	Lists the routing table.
INTERFACE-ADDRESSES	Lists the router IP interface addresses.
IPSEC	Accesses IPsec's monitoring menus.
NAT	Accesses the NAT feature monitoring menus.
PING	Sends queries to any other host (1 per second) and waits for a response. This command can be used to isolate trouble in a multiple network environment.
POOL	Displays both the address pool established in the router and the ranges of reserved addresses the router has.
PROXY-IGMP	Accesses proxy IGMP monitoring menus.
ROUTE-GIVEN-ADDRESS	Lists existing routes for a specific destination IP address.
SIZES	Displays the size of specific IP parameters.
STATIC-ROUTES	Displays configured static routes.
TCP-LIST	Lists active TCP connections.
TRACEROUTE	Displays the complete path (hop-by-hop) to a specific destination.
TVRP	Accesses TVRP monitoring menus.
UDP-LIST	Lists registered UDP ports.
VRF	Monitors IP for a specific VRF.
VRRP	Accesses VRRP monitoring menus.
EXIT	Exits IP monitoring.

3.1.1 ? (HELP)

Lists all valid commands, and their available options, at the router's monitoring level.

Syntax:

```
IP+?
```

3.1.2 ACCESS-CONTROLS

Shows the access control mode in use, together with a list of configured access control records. Access control modes can be:

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

Enabled:	Access control exists and access control records are inspected.
Exclusive:	Packets matching access control records are discarded.
Inclusive:	Packets matching access control records are forwarded.

When access control is enabled, packets that do not match any access control records are discarded. *Beg* and *End Pro* (protocol) reference the IP protocol number, *Beg* and *End Prt* (port) reference the port number (*SPrt*: source port, *DPrt*: destination port), *Invoc* specifies the number of times a specific entry in the IP access control system was invoked by the characteristics of an inbound or outbound 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   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+
```

Command history:

Release	Modification
11.00.03	The "*access-controls*" command is obsolete as of version 11.00.03.

3.1.3 AGGREGATION-ROUTE

Displays the list of aggregation routes configured.

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

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

Syntax:

```
IP+aggregation-route
```

Example:

```
IP+aggregation-route
Net             Mask
---             ----
1.1.0.0         255.255.0.0    aggregation
IP+
```

The meaning of each field is:

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

3.1.4 BPING

Sends an ICMP Echo request packet to every subnet address and waits for a response.

The following parameter is first requested via the console:

IP destination: Any address that belongs to the subnet.

This is the only parameter necessary in order to execute this command. A series of options that take default values (unless modified) will then appear. To accept default values for all other options, press the CR (carriage return) key. Said options are:

- *Destination mask* (mask): Subnet mask used to determine the group of addresses to which the Echo request is sent. By default, the destination mask is the one that corresponds to the IPv4 class the destination address pertains to.

- *IP source* (source): Outbound packets. By default, the router chooses the source interface address (logical) for the outbound ping.
- *Time out* (timeout): Time interval (expressed in milliseconds) greater than, or equal to, 10ms while waiting for a response to a sent packet. Time is marked from the moment the packet is sent. Default is one second.
- *Avoid fragmentation* (avoid-fragm): IP datagram. This is a command for the router, as the destination cannot reassemble the pieces. By default, the datagram can be fragmented.
- *Quiet* (quiet): Prevents the results for each ICMP packet sent via the screen from being printed. By default, results for each ICMP packet are presented on screen.

Packet size is 56 bytes excluding the ICMP header.

The address a packet is sent to increases after the first non-broadcast subnet address (i.e., the first and the last addresses are ignored). Packets are sent every 100ms. However, if timeout is longer than the time between pings and an answer has not been received yet, the router waits for the timeout period to expire before sending a new packet.

If you receive a valid response, the corresponding delay is displayed. Otherwise, a *contact not established* message appears.

The **bping** command can be disabled by clicking on any key, or when the subnet addresses finishes. At this point, a summary of packets sent and received is displayed.

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

Syntax:

```
IP+bping <destination_IP_address> [mask <destination_mask>] [source
<source_IP_address>]          [timeout <timeout_ms>] [avoid-fragm] [quiet]
```

Example:

```
IP+bping 192.6.1.228 mask 255.255.255.248 source 192.7.1.253

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

---- BPING Statistics----
6 packets transmitted, 2 packets received
IP+
```

Command history:

Release	Modification
10.08.34.05.07, 10.08.36.01.04, 10.08.42, 10.09.08.01.15, 10.09.20, 11.00.00.02.06, 11.00.02	A summary of the packets sent and received is displayed.

3.1.5 CACHE

Lists recently used destination routes stored in the routing cache memory. If a destination is not in the cache memory, the router looks it up in the general routing table before making a decision.

Syntax:

```
IP+cache
```

Example:

```
IP+cache
Destination      Usage        Next hop
192.6.2.12       6            192.6.2.12      (ethernet0/0)
192.6.2.15       248          192.6.2.15      (ethernet0/0)
```

```
192.6.2.3        4            192.6.2.3       (ethernet0/0)
192.6.2.10       4            192.6.2.10      (ethernet0/0)
IP+
```

The meaning of each field is:

Destination:	Host destination address.
Usage:	Number of packets sent to host.
Next hop:	IP address of next router on the path towards the destination host. The interface used by this packet is also displayed.

3.1.6 COUNTERS

Lists statistics related to forwarded IP packets. These statistics include a routing error counter that displays the number of packets dropped due to congestion.

Syntax:

```
IP+counters ?
  delete    Delete counters
  show      Display counters
```

3.1.6.1 COUNTERS DELETE

Example:

```
IP+counters delete
IP+
```

3.1.6.2 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   Attempted forward of LL broadcast

Packets discarded through filter  0
IP multicasts accepted:           212

IP input packet overflows
    Net          Count
ethernet0/0      0
serial0/0        0
serial0/1        0
serial0/2        0
bri0/0           0
x25-node         0
IP+
```

The meaning of each field is:

Routing table overflow	Routes discarded: routing table is full.
Net unreachable	Packets not forwarded due to unknown destination.
Bad subnet or net number	Illegal net/subnet routes or packets.
Unhandled broadcast	Non-local IP broadcast received (not forwarded).
Unhandled multicast	IP multicast packets received with an address not recognized by the router.
Unhandled directed broadcast	Directed (non-local) IP broadcast received when forwarding for said packets is disabled.

Attempted forward off LL broadcast	Packets received with non-local IP addresses, but sent to a link level broadcast address. These are discarded.
Packets discarded through filter	Received packets addressed to filtered networks /subnets.
IP multicast accepted	IP multicasts received and successfully processed by the router.
IP input packet overflows	Packets discarded due to congestion at the packet input queue.

3.1.7 DUMP-ROUTING-TABLE

Lists the IP active route table or any of its subgroups. A line is printed for each IP network route. The default router (if there is one) is printed at the end.

The active route table contains a set of routes used at a given moment in IP traffic routing. This feeds on routes provided by each dynamic routing protocol (RIP, OSPF, BGP), static routes and directly connected routes.

A route must meet the following requirements to be included in the active route table:

(1) An output interface for the next hop must exist and must be active.

(2) If there are two or more routes heading towards the same destination network and each comes from a different routing protocol, the route belonging to the protocol with the shortest administrative distance is installed.

(3) If there are two or more routes heading towards the same destination network and each comes from the same routing protocol, the route with the least cost (weight) is installed.

If a route's next hop is left without an active exit, the route becomes incomplete and is eliminated from the active route table. There is a periodic refresh process for the active route table. This process checks the next hops for the routes and eliminates all incomplete routes.

According to the nature of the next hop, routes can be classified as *direct* or *indirect*.

(1) Direct routes: those whose next hop is directly connected to an interface.

(2) Indirect routes: those whose next hop is accessible via another route.

Furthermore, next-hops can be marked with congestion and disabling flags if *multipath per-afs-session* is activated and some static route has configured advisors. The active route table feeds on static routes to keep every next-hop flag updated.

Syntax:

```
IP+dump-routing-table [<IP_addr> [<mask>]] ?
  all          Print routes at once
  dir          Directly connected net or subnet
  stat         Statically configured route
  rip          Route learnt by RIP protocol
  dflt         Default
  del          Deleted route
  sbnt         Subnet route
  spf          Intra-area OSPF route
  spia         Inter-area OSPF route
  spe1         External OSPF route (type 1)
  spe2         External OSPF route (type 2)
  rnge         Range of active OSPF addresses
  bgp          BGP route
  aggr         Aggregation of nets
  nh-flags     Include next-hop flags column
  summary      Print only the summary of routes
  <cr>
```

To execute this command, you may: 1) limit listed routes to those included in a range determined by **<ip_address>** and **<mask>**; 2) specify the type of route that can be displayed so unselected types are not listed; 3) select several types simultaneously. Once a type is selected, it disappears from the options list, which remains available for further selections; 4) if the *nh-flags* option is selected, an extra column that shows the current flag status for each next-hop is printed; 5) by default, this command displays requested active routes in blocks of 15 lines, and asks for a carriage return in order to keep printing. Select *all* to print all selected routes at once.

Example:

```
IP+dump-routing-table
Type                 Dest net/Mask   Cost Age  Next hop(s)

Stat(2)[0]            0.0.0.0/0    [ 60/1 ] 0   172.24.78.130 (ethernet0/0)  (C)
                                            0   192.6.1.3 (ethernet0/0)
```

```
Sbnt(0)[0]            1.0.0.0/8   [240/1 ] 0   None
Stat(3)[0]            1.1.1.1/32  [ 60/1 ] 0   ethernet0/0  (C)
                                           0   2.2.2.2
                                           0   3.3.3.3
Sbnt(0)[0]            2.0.0.0/8   [240/1 ] 0   None
 RIP(0)[0]            2.2.2.2/32  [ 60/1 ] 0   172.24.0.98 (ethernet0/0)
Sbnt(0)[0]            3.0.0.0/8   [240/1 ] 0   None
 BGP(1)[0]            3.3.3.3/32  [ 60/1 ] 0   172.24.51.38 (ethernet0/0)
 SPF(0)[1]         172.24.0.0/16  [  0/1 ] 1   ethernet0/0
 Dir(0)[1]          192.6.1.0/24  [  0/1 ] 0   ethernet0/0
 SPF(0)[1]        192.6.1.251/32  [  0/0 ] 0   SNK/0

Default gateway in use.
Type Cost Age  Next hop
Stat 1    0   172.24.78.130 (ethernet0/0)  (C)
          0   192.6.1.3 (ethernet0/0)

Routing table size: 768 nets (64512 bytes), 10 nets known, 10 shown
IP+
```

The meaning of each field is:

Type (type of route)	References relating to the route provider. dflt— default 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 RIP. del— deleted route. stat— statically configured route. fltr— filter (obsolete as of versions 11.00.03 and 11.01.00.). spf— route is an intra-area OSPF route. spia— route is an inter-area OSPF route. spe1, spe2 — the route is an external OSPF route (types 1 and 2 respectively). rnge— range of active OSPF addresses. Not used to route packets. bgpr— BGP route that IGP can renounce (Interior Gateway Protocol). cnd— route is an EGP route. egpc— information on the EGP nucleus. egpr— EGP route that IGP can renounce. rdr— route redirected by ICMP. gwd— ICMP gateway discovery route. dii1, dii2— Dual ISIS route (levels 1 and 2 respectively). tlx— Sockets tellinux routes.
Dest net	IP destination net or subnet.
Mask	Destination IP network mask.
Cost	Cost of route summary. Format: [administrative-distance/cost]
Age	For RIP routes, refers to the time lapsed since the routing table was last re-freshed.
Flags	Markable flags for a next hop. Each flag can be displayed through an uppercase or lower case letter. An uppercase letter indicates that a flag is marked, whilst lower case indicates that this flag is not marked.

	C/c — Congestion flag is marked / not marked. D/d — Disabling flag is marked / not marked.
Next hop(s)	IP address of next router on the path towards the destination or outbound interface the router uses to forward a packet.

The number in parentheses *(num)* after *Type* references the number of static routes configured with the same destination as the printed route.

The number between square brackets *[num]* after *type of route* references the number of existing direct routes with the same destination as the printed route.

A percentage sign *%* after *Type* means RIP *updates* are always accepted for said destination.

Letter *A* after *Type* means the route matches an aggregation route.

Letter *a* after *Type* means the route is being added by an aggregation route.

When a route has more than one active path of equal cost towards a destination, each path is displayed on a separate line in the *Next hop(s)* column where *(C)* references the current path. For further information on how the current path is selected, please refer to the relevant section on multipath configuration found in this manual. Moreover, if the *per packet multipath* option is enabled with load sharing (according to the relative weights of the interfaces involved), the percentage of traffic transmitted against the total traffic using this route will appear in brackets.

If the next-hop belongs to a network directly connected to the router, the next-hop followed by the output interface is displayed in brackets. If the next-hop is accessible via another network (indirect route), the output interface is not displayed.

If you only want to see a summary of the routing table, rather than displaying all the routes, you can select the **summary** option.

Example:

```
IP+dump-routing-table bgp summary

Routing table size: 768 nets (64512 bytes), 10 nets known, 1 filtered
IP+
```

Release	Modification
11.00.05	The *nh-flags* command option was introduced as of version 11.00.05.
11.01.01	The *nh-flags* command option was introduced as of version 11.01.01.
11.01.12	The *summary* command option was introduced as of version 11.01.12.
11.02.01	The *summary* command option was introduced as of version 11.02.01.

3.1.8 INTERFACE-ADDRESSES

Displays the IP addresses of router interfaces. Each address is listed together with the corresponding hardware interface and IP address mask.

Use this command to display special IP addresses active in the router: internal IP address, management IP address, router-ID and global IP address.

The global IP address is the internal IP (where configured), router-id (where this matches one configured in an interface), or the first IP address configured in an interface in the router.

Syntax:

```
IP+interface-addresses
```

Example:

```
IP+interface-addresses
Interface IP Addresses:
-----------------------
ethernet0/0     172.24.78.36/16
serial0/0       192.3.1.2/24
                10.0.0.3/8
x25-node        192.168.252.1/24

Special IP Addresses:
```

```
---------------------
internal-address    0.0.0.0
management-address  0.0.0.0
router-id           0.0.0.0
global-address      172.24.78.36
IP+
```

3.1.9 IPSEC

Accesses the IPsec monitoring menus. For further information, please see bintec manual *Dm739-I IPSec*.

Syntax:

```
IP+ipsec
```

Example:

```
IP+ipsec
-- IPSec protocol monitor --
IPSec+
```

3.1.10 NAT

Accesses the NAT monitoring menus: *static*, *dynamic* and *ports*.

Syntax:

```
IP+nat ?
  dynamic    Dynamic NAT monitoring
  pat        Port address translation monitoring
  static     Static NAT monitoring
```

3.1.10.1 NAT DYNAMIC

Accesses the Dynamic NAT monitoring menus. For further information, please see bintec manual *Dm755-I Dynamic NAT protocol*.

Example:

```
IP+nat dynamic
-- Dynamic NAT monitoring --
DNAT+
```

3.1.10.2 NAT PAT

Accesses the NAPT monitoring menus. For further information, please see bintec manual *Dm735-I NAPT Facility*.

Example:

```
IP+nat pat
-- Port Address Translation monitoring --
NAPT+
```

3.1.10.3 NAT STATIC

Accesses the static NAT monitoring menus. For further information, please see bintec manual *Dm720-I NAT Protocol*.

Example:

```
IP+nat static
-- Static NAT monitoring --
SNAT monit>
```

3.1.11 PING

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 for each transmitted packet. This command can be used to isolate trouble in the network.

Syntax:

```
IP+*ping
      <destination_IP_addr>|<destination_URL>
         [source <source_IP_addr>] [data-bytes <num_bytes>]
         [interval-pings <t_entre_pings_ms>] [num-pings <num_pings>]
         [timeout <timeout_ms>] [avoid-fragm] [quiet] [ttl <num_nodes>]
      vrf <vrf>
      <cr>
```

Through the **vrf** option, you can specify the VRF you want to ping. If you do not specify any, the main VRF is used.

The first ping parameter, once the VRT is (implicitly or explicitly) specified, is:

IP destination: destination packets are sent to and from the place where responses are expected. This is specified through the IP address or a URL. For the second option, a DNS query is performed, so DNS must be configured.

This parameter is the only one needed to execute said command. A series of options that take default values (unless modified) will then appear. To accept default values for the remaining options, simply press the CR (carriage return) key. These options are:

- *IP source* (source): Source IP address, outbound packets. The router chooses the interface's (logical) source address for outbound ping by default.
- *Number of data bytes* (data-bytes): ICMP message size, excluding the ICMP header. Default is 56 bytes.
- *Time between pings* (interval-pings): Time interval between pings. This should be greater than, or equal to, 10ms. Default is one second.
- *Number of pings* (num-pings): Number of packets to send. Default is zero (i.e., packets are sent indefinitely).
- *Time out* (timeout): Time interval (expressed in milliseconds) greater than, or equal to, 10ms while waiting for a response to a sent packet. This time is marked from the moment a packet is sent. Default is zero (i.e., the router will wait indefinitely for a response).
- *Avoid fragmentation* (avoid-fragm): Avoid IP datagram fragmentation. This command is for routers, since a destination cannot reassemble the pieces. By default, the datagram can be fragmented.
- *Quiet* (quiet): Prevents the results for each ICMP packet, sent via the screen, from being printed. By default, results for each ICMP packet are presented on screen.
- Time to live (TTL): Indicates how many nodes a packet can pass before being dropped by the network or returned to its origin. By default, its value is 60.

If timeout is longer than the time between pings and an answer has not been received yet, the router waits for the timeout period to expire before sending a new packet.

This process is executed continuously, incrementing the ICMP sequence number with each additional packet. Matching ICMP Echo responses received are reported with their sequence number and round trip time. Time resolution of the round trip time calculation is usually (depending on the platform) around 20 milliseconds. If this response is not received during timeout, a message appears indicating that the time has been exceeded.

The **ping** command ends when the user presses any key, or when all packets to be sent with their corresponding responses have been dealt with. At this point, a summary is displayed. This includes the packets sent, received, lost and those whose responses have surpassed timeout, as well as the minimum, mean and maximum round trip time.

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

Example:

```
IP+ ping 192.7.1.1 data-bytes 1472 interval-pings 150 num-pings 4 timeout 30 avoid-fragm

PING: 1472 data bytes
1480 bytes from 192.7.1.1: icmp_seq=0. time=2. ms
1480 bytes from 192.7.1.1: icmp_seq=1. time=2. ms
1480 bytes from 192.7.1.1: icmp_seq=2. time=2. ms
1480 bytes from 192.7.1.1: icmp_seq=3. time=2. ms

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

This example focuses on the use of the **ping** command when only the destination is introduced (through its IP address or URL). Here, all configurable parameters take said value by default.

Example:

```
IP+ping 192.7.1.1

PING: 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

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

Sends a ping to address 192.71.1 using the **VRF client**.

Example:

```
IP+ping vrf cliente 192.7.1.1

PING: 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

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

3.1.12 POOL

Allows the user to view the address pool set in the router, as well as the ranges of addresses used and the reason for reserving them.

Reserved pool address ranges are expressed in the form of an address and a mask. The following table gives details on why they are reserved:

SET	Ranges of addresses configured in the router.
RADIUS	Ranges of addresses 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 X.25 preconfiguration.

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+
```

3.1.13 PROXY-IGMP

Accesses the **proxy-igmp** monitoring menus. For further information, please see bintec manual *Dm762-I IGMP Protocol*.

Syntax:

```
IP+proxy-igmp
```

Example:

```
IP+proxy-igmp
-- IGMP proxy monitor --
IGMP proxy+
```

3.1.14 ROUTE-GIVEN-ADDRESS

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

Syntax:

```
IP+route-given-address <address>
```

Example:

```
IP+route-given-address 1.1.1.1
Destination:    1.1.1.1
Mask:           255.255.255.255
Route type:     Stat
Distance:       1
Tag:            0
Next hop(s):    1.1.1.1          (ethernet0/0    ) Age: 0
                2.2.2.2                            Age: 0
                3.3.3.3                            Age: 0
```

3.1.15 SIZES

Displays the configured sizes of specific IP parameters that belong to the IP protocol.

Syntax:

```
IP+sizes
```

Example:

```
IP+sizes
        Routing table max. size:        unlimited
        Table entries used:             1242 (128 kb)
        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:

Max. routing table size	Limits the number of entries in the routing table. This also displays the amount of memory the routing table will use if it reaches said limit.
Table entries used	Number of entries used from the IP routing table. This also displays the amount of memory the routing table uses.
Reassembly buffer size	Reassembly buffer size used to reassemble fragmented IP packets.
Largest reassembly pkt	Largest IP packet this router has had to reassemble.
Size of routing cache	Size of the IP routing table.
# cache entries in use	Number of cache entries currently being used.

3.1.16 STATIC-ROUTES

Displays the list of configured static routes. It also displays the default network and subnet routers.

Each static route destination is specified by an address, its corresponding mask, the next hop address, its cost, the outbound interface, 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 network destinations.

Syntax:

```
IP+static-routes
```

Example:

```
IP+static-routes
Flags: A added to routing table, R refresh, T track up, D DHCP default gateway
Type  Net               Cost  Next_hop        Int               Circuit State
----  ---               ----  --------        ---               ------- -----
CNFG  0.0.0.0/0         1     172.24.78.130   ethernet0/0       N/A     Ar
CNFG  0.0.0.0/0         1     192.6.1.3       ethernet0/0       N/A     Ar
CNFG  1.1.1.1/32        1     0.0.0.0         ethernet0/0       N/A     Ar
CNFG  1.1.1.1/32        1     2.2.2.2         UNK               UNK     Ar
CNFG  1.1.1.1/32        1     3.3.3.3         UNK               UNK     Ar
CNFG  1.1.1.1/32        1     4.4.4.4         UNK               UNK     AR
CNFG  2.2.2.2/32        1     172.24.0.98     ethernet0/0       N/A     Ar
CNFG  3.3.3.3/32        1     172.24.51.38    ethernet0/0       N/A     ArD
IP+
```

The meaning of each field is:

Type	Type of route. Indicates if this route is: configured by the user with IP as destination (CNFG), configured by the user with FQDN as destination (FQDN), installed through DHCP, a management route (MNG), a dynamic route generated through route-id (IDLNK), a route learned by IPCP, by RADIUS (RAD), or a route generated by IPSec based on the Reverse Route Injection (RRI) algorithm.
Net	Route destination network or subnet.
Cost	Cost of using this route.
Next hop	IP address for the subsequent router where packets are sent so that they reach the referenced destination.
Int	Outbound interface identifier for packets that select this route. If, while being monitored, the router cannot find the outbound interface (because it doesn't exist), or the next hop is accessible via a different route (indirect routes), UNK (unknown) appears.
Circuit	Outbound subinterface identifier for packets selecting this route. FR references the outbound DLCI, X.25 (R->N) the outbound NRI, and N/A (not applicable) a generic interface that can't be divided into subinterfaces. If, while being monitored, the router cannot find the outbound interface (because it doesn't exist), or the next hop is accessible via a different route (indirect routes), UNK (unknown) appears.
State	The first letter shows if the static route in question has been registered in the active route table (**A** or, if not, **a**). This registration is always carried out unless there has been a serious error. The second letter shows whether the route needs to be refreshed, **R** (if not, **r**). A route needs to be refreshed (**R**) if it is incomplete (next hop is inaccessible) and the active route itself has less preference (either due to the administrative distance between the routing protocols or to metrics with routes from the same routing protocol). Refresh checks if the next hop for the route has an active output interface and, if it does, adds said route to the active route table. If we have a route linked to advisors (*track*, *mp-congestion* and/or *mp-disable*), a **T** appears when said advisor is active (**t** when it isn't - inhibited route); a **C** when the route is congested (**c** not congested) and **O** when the route is disabled (**o** when enabled). **D** means the next hop was configured on receiving DHCP option 3 from the output interface DHCP client.

Command history:

Release	Modification
11.01.04	Routes of a FQDN type have been introduced as of version 11.01.04.

3.1.17 TCP-LIST

Lists the TCP connections in the router that provide information on the socket: local IP address, local TCP port, remote IP address, remote TCP port. It also provides information on the connection status (one of the possible states in the TCP states diagram).

Syntax:

```
IP+tcp-list
```

Example:

```
IP+tcp-list
LOCAL ADDR      LOCAL PORT  REMOTE ADDR     REMOTE PORT  STATE
--------------  ----------  --------------  -----------  --------
0.0.0.0         18888       0.0.0.0         0            LISTEN
0.0.0.0         21          0.0.0.0         0            LISTEN
0.0.0.0         23          0.0.0.0         0            LISTEN
0.0.0.0         53          0.0.0.0         0            LISTEN
172.24.121.21   23          172.24.51.155   2957         ESTAB
172.24.121.21   23          172.24.121.3    1024         ESTAB
172.24.121.1    1024        172.24.121.3    23           ESTAB
IP+
```

There are various ports open; the listening port where a remote client initiated a connection, two established connections corresponding to Telnet sessions on the router itself (local port is 23), together with another Telnet session executed from the local router (port 23 here is located at the remote end).

3.1.18 TRACEROUTE

Displays the entire path to a given destination, hop by hop. For each successive hop, **traceroute** sends out various 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 appears.

This command is executed whenever the destination is reached, an ICMP Destination Unreachable is received, or path length surpasses the maximum number of hops specified by the user.

The following parameter is requested:

IP destination: Address of the router whose path you want to see. This is specified through the IP address or through a URL; for the latter, a pre-configured DNS query is executed.

This parameter is the only one needed to execute this command. A series of options that take default values (unless modified) will then appear. To accept default values for the remaining options, simply press the CR (carriage return) key. Said options are:

- *Protocol* (protocol): Probe packets protocol: UDP or ICMP. Default is UDP.
- *Beginning destination UDP port* (udp-port): This parameter is only available if the user selected UDP. It provides the destination port in the UDP packet sent, which increases for each probe. Default is 33434.
- *IP source* (source): Packet output. By default, the router selects the output interface (logical) source address.
- *Seconds to wait for response* (timeout): Time, in seconds, to wait for a response to the probe packet sent. Default is 3.
- *Probes at each TTL* (probes): Number of probes to be sent by each TTL. Default is 3.
- *Minimum Time To Live* (min-ttl): Number of hops from where you wish to view the path. If you have pre-configured a max-ttl value, this is the maximum value the min-ttl takes. Default is 1.
- *Maximum Time To Live* (max-ttl): Maximum number of hops. If you have pre-configured the min-ttl value, this is the minimum value the max-ttl takes. Default is 30.
- *Verbose* (verbose)*:* Type of trace view. If you select verbose, you can see on the left the distance (in hops) to the router. The consecutive lines show the results for each probe for this number of hops. It also shows the IP address of the responding router. Traditional viewing shows a single line with the results of all polls, executed with the same TTL, with just one IP address from one of the responding routers. Default is deactivated.

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

!N references an ICMP Destination Unreachable (net unreachable) packet has been received.

!H references an ICMP Destination Unreachable (host unreachable) packet has been received.

!P references an ICMP Destination Unreachable (protocol unreachable) packet has been received.

If the probe packets are ICMP, the expected response is an ICMP Echo Reply packet. When sending UDP packets to a remote port, the expected response is *port out of reach*. If an **!** is displayed on the screen (together with the response time), the destination has been reached, but the reply sent by the destination contains a TTL equal to 1. This usually indicates an error at destination, prevalent in some versions of UNIX, as the destination has included probe packet TTLs in its replies. This leads to a number of lines consisting solely of asterisks before destination is finally reached.

Syntax:

```
IP+traceroute <destination_IP_addr>|<destination_URL> [protocol udp|icmp]
[udp-port <port_num>] [source <source_IP_addr>] [timeout <timeout_s>]
[probes <num_probes>] [min-ttl <minimum_ttl>] [max-ttl <maximum_ttl>] [verbose]
```

Example:

```
IP+traceroute 213.140.36.226 protocol icmp timeout 2 max-ttl 15 verbose

Press any key to abort

 Tracing the route to: 213.140.36.226 [],
 Protocol: ICMP, 15 hops max, 56 byte packets

 1
   Probe:  1, Time     2 ms, IP:      172.24.0.98
   Probe:  2, Time     5 ms, IP:      172.24.0.98
   Probe:  3, Time     2 ms, IP:      172.24.0.98
 2
   Probe:  1, Time    41 ms, IP:       213.4.10.1
   Probe:  2, Time    41 ms, IP:       213.4.10.1
   Probe:  3, Time    42 ms, IP:       213.4.10.1
 3
   Probe:  1, Time    46 ms, IP:     80.58.121.82
   Probe:  2, Time    42 ms, IP:     80.58.121.82
   Probe:  3, Time    43 ms, IP:     80.58.121.82
 4
   Probe:  1,     *
   Probe:  2,     *
   Probe:  3,     *
 5
   Probe:  1, Time   125 ms, IP:      84.16.8.113
   Probe:  2, Time   105 ms, IP:      84.16.8.113
   Probe:  3,     *
 6
   Probe:  1, Time    42 ms, IP:   213.140.38.250
   Probe:  2, Time    45 ms, IP:   213.140.38.250
   Probe:  3, Time    42 ms, IP:   213.140.38.250
 7
   Probe:  1, Time    59 ms, IP:   213.140.36.190
   Probe:  2, Time    44 ms, IP:   213.140.36.190
   Probe:  3, Time    42 ms, IP:   213.140.36.190
 8
   Probe:  1, Time    69 ms, IP:   213.140.36.226
   Probe:  2, Time    72 ms, IP:   213.140.36.226
   Probe:  3, Time    68 ms, IP:   213.140.36.226
 Trace complete.
```

The meaning of each field is:

Press any key to abort:	If the user presses a key while the **traceroute** command is being executed, said process is aborted.
Tracing the route to:	Displays the destination address, the protocol used to send packets, the maximum number of hops and the size of the packet sent. If the destination address is specified as a domain name, the IP address that results from consulting the DNS is displayed between square brackets.
1:	First trace from the destination.
Probe:	Probe for a given TTL. This displays the response time and the IP address of the responding device. In this case, three probe packets are sent for each hop.

Trace complete: The trace has been completed.

In this case, the **traceroute** command is used when only the destination is entered (through its IP address or URL). Here, all configurable parameters take their default values.

Example:

```
IP+traceroute 213.155.151.120

Press any key to abort.

Tracing the route to: 213.4.10.1 [],
Protocol: UDP, 30 hops max, 56 byte packets

 1     1 ms    1 ms    1 ms     172.24.0.98
 2     *       *     616 ms      213.4.10.1
 3   158 ms  167 ms  168 ms    80.58.121.65
 4     *       *       *       Time exceeded in transit
 5     *     651 ms    *        84.16.8.121
 6   212 ms  167 ms  172 ms  213.140.43.146
 7   157 ms  177 ms  165 ms  213.248.75.117
 8     *      76 ms    *     213.248.65.237
 9     *       *       *       Time exceeded in transit
10  2968 ms  152 ms  175 ms    80.91.250.98
11   160 ms    *      81 ms  195.12.255.166
12   172 ms  162 ms    *    213.155.151.120

     Trace complete
```

The meaning of each field is:

1: First trace to display the destination NSAP, as well as the time necessary to reach this. Three probes are sent (packet is sent 3 times).

** * * Time exceeded in transit:* Indicates the router is waiting for a response from the destination (still waiting).

3.1.19 TVRP

Accesses the TVRP monitoring menus. For further information, please see bintec manual *Dm725-I TVRP*.

Syntax:

```
IP+tvrp
```

Example:

```
IP+tvrp
-- TVRP Console --
TVRP+
```

3.1.20 UDP-LIST

Lists all active UDP ports in the router. A description for each reserved UDP port is also provided.

Syntax:

```
IP+udp-list
```

Example:

```
IP+udp-list
Total active UDP Ports: 15

Active UDP Ports:
port  1025 (DNS miniresolver)
port    67 (DHCP-SERVER)
port    68 (DHCP-CLIENT)
port   500 (IKE-SERVER)
port  4500 (IKE-SERVER NATT)
port   848 (IKE-SERVER GDOI)
port   161 (Socket)
port   162 (SNMP TRAP)
```

```
port   123 (Socket)
port  1026 (DNS-CLIENT main)
port  1027 (Socket)
port    53 (Socket)
port  1028 (Socket)
port  1029 (Socket)
port  1030 (Socket)
IP+
```

Command history:

Release	Modification
11.01.14	Statistics for total active UDP ports and UDP port descriptions have been introduced as of version 11.01.14.
11.02.02	Statistics for total active UDP ports and UDP port descriptions have been introduced as of version 11.02.02.

3.1.21 VRF

Monitors IP in a *routing/forwarding* domain in virtual private networks (VPNs). For further information, please see bintec manual *Dm775-I VRF*.

Syntax:

```
IP+vrf <vrf_name>
```

Example:

```
IP+vrf vrf1
-- IP protocol monitor for a VRF --
IP vrf+
```

The following commands are available in this submenu. They are a subset of commands belonging to the main IP monitoring menu (listed in section 1) that, in this case, apply to the VRF and are specified through **<name_vrf>**.

Command	Function
? (HELP)	Lists the available commands or their options.
AGGREGATION-ROUTE	Displays configured aggregation routes.
BPING	Executes a broadcast ping.
DUMP-ROUTING-TABLE	Lists the routing table.
INTERFACE-ADDRESSES	Lists IP addresses for router interfaces (only those that belong to the VRF).
ROUTE-GIVEN-ADDRESS	Lists existing routes for a certain IP destination address.
SIZES	Displays the size of the IP parameters.
STATIC-ROUTES	Displays configured static routes.
TCP-LIST	Lists active TCP connections.
TRACEROUTE	Shows the complete path, hop by hop, to a specific destination address.
UDP-LIST	Lists registered UDP ports.
EXIT	Exits the VRF IP monitoring console.

For further information on these commands, please see the **HELP** command for each of the above in the subsection corresponding to IP Protocol Monitoring Commands.

3.1.22 VRRP

Accesses the VRRP monitoring menus. For further information, please see bintec manual *Dm759-I VRRP Protocol*.

Syntax:

```
IP+vrrp
```

Example:

```
IP+vrrp
-- VRRP console --
VRRP+
```

3.1.23 EXIT

Returns to the previous prompt level.

Syntax:

```
IP+exit
```

Example:

```
IP+exit
+
```

Appendix A Personalized Parameters

A.1 Supported personalized parameters

bintec routers have customized parameters that modify the behavior of the router *under certain special circumstances* (personalized versions). For further information on the activation, deactivation, and listing of these parameters, please see the **help** command under the **enable patch, disable patch** and **list patch** options. Please see bintec manual *Dm704-I Configuration and Monitoring* (*Chapter 2*).

TCP-IP in bintec has the following customized parameter:

TCP_MAXTIME

This patch allows you to define a timeout when non-responding TCP connections are considered lost, instead of relying on the number of retransmissions.

Value: 0 Normal operation (9 retransmissions).

Value: x Number of timeout seconds where a non-responding TCP connection is considered lost.