Teldat Router

RIP Protocol

Doc. *DM718-I* Rev. *10.10*
June, 2003

INDEX

Chapter 1
Introduction

1. Introduction

This chapter describes the use of the RIP protocol (Routing Information Protocol) which is an Interior Gateway Protocol (IGP). The **Teldat Router** supports two different IGP protocols to build the IP routing table. These protocols are OSPF and RIP.

RIP is a routing protocol based on the Bellman-Ford (or distance vector) algorithm that allows routers to exchange information on possible destinations in order to calculate routes throughout the network. Destinations may be networks or special values used to represent default routes. RIP does not alter IP datagrams and routes them based on destination address only.

Distance vector algorithm makes each router periodically broadcast its routing tables to all its router neighbors. Therefore the router knowing its neighbors' tables can decide how to transmit each packet.

This information is organized into the following sections:

- RIP routing protocol.
- RIP protocol configuration.
- RIP protocol configuration commands.
- RIP protocol monitoring commands.

Routers that use a common routing protocol form an Autonomous System (AS). This common routing protocol is known as Interior Gateway Protocol. IGPs dynamically detect network reachability and routing information within an AS and use this information to build the IP routing table. External routing information can also be imported to an AS by IGPs.

The **Teldat Router** can execute both the OSPF and RIP protocols simultaneously. When this happens, OSPF routes are chosen in preference.

2. RIP Routing Protocol

With the advent of OSPF, there are those who believe that RIP is obsolete. While it is true that the newer routing protocols are far superior to RIP, RIP does have some advantages. Primarily, in a small network, RIP-2 adds very little overhead in terms of bandwidth used, and it is far easier and quicker to configure. Furthermore, there are far more devices currently executing RIP than other routing protocols.

The RIP-1 protocol does not consider autonomous systems, the IGP/EGP interactions, subnetting (networks divided into subnets) or authentication. The lack of subnet masks in RIP-1 packets is a particularly serious problem for routers since they need a subnet mask to know how to determine subnet routes. Currently routers with RIP-1 assume that the subnet mask is the same as the interface mask where the RIP-1 packet entered. They also impose the condition that all the subnets of the same network have the same length. RIP-2 protocol was introduced to solve this problem.

Note: All the router interfaces having RIP enabled, as RIP-1 must have the same subnet mask.

RIP-2 is an extension of RIP-1. It uses the same message format but the meaning is extended in some of the fields.

The **Teldat Router** supports the complete implementation of the RIP-2 routing protocol in compliance with the RFC 1723 and RFC 1388 recommendations. This version is compatible with routers executing RIP Version 1. RIP information is exchanged between the routers which execute the different versions although the router must be specifically configured with RIP-2.

RIP-2 is designed to provide services which are not available from the RIP-1 protocol. Its advanced characteristics include:

- *Authentication*, currently this is a password in clear. This gives additional routing security.
- *Route Tag Field*, is an attribute assigned to a route which separates the internal routes from the external routes i.e. to achieve a method permitting IGP/EGP interaction.
- *Variable length Subnet Masks.* Permits fractioning of an IP address in variable length subnets, conserving the IP address space.
- *Next Hop*, to eliminate packets being routed with an extra number of hops.
- *Multicast* instead of broadcast in order to reduce unnecessary load on those hosts which are not processing RIP-2 packets. The multicast address associated to RIP-2 is 224.0.0.9. The use of multicast is a configurable parameter in order to maintain compatibility with RIP-1.

The RIP-2 supports the following types of physical networks:

- *Leased Lines*. These are networks that use a communication line to join a single pair of routers. An example of this is a serial line at 56 Kbps connecting two routers.
- *Broadcast*. These are networks that support more than two connected routers and are able to address a single physical message to all connected routers. An example of a broadcast network is Token Ring.
- *No Broadcast*. These are networks that support more than two connected routers but are incapable of broadcasting. An X.25 public data network is an example of a non-broadcast network. The network needs additional configuration information on the other RIP-2 routers connected to the non-broadcast network to ensure RIP-2 operates correctly.

The RIP protocol is primary intended for use in small homogeneous networks. For this reason the RIP protocol has the following specific limitations:

- The maximum number of hops is 15.
- RIP is slow to find new routes when the network changes.
- This protocol uses fixed "metrics" to compare alternative routes. It is not appropriate for situations where routes need to be chosen based on real-time parameters.

3. Configuring the RIP protocol

This section outlines the initial steps required to configure and run RIP protocol appropriately.

1. Enable the RIP protocol.
2. Define the router's RIP network interfaces.
3. Configure the transmission parameters by interface: Type of routes you wish to transmit and if you want to activate the *poisoned reverse* option in the said interface or not.
4. Configure the reception parameters by interface. Type of routes you require to process.
5. Configure the sending and reception compatibility by interface. These are the different types of layer compatibility defined by the RFC 1723 between RIP-1 and RIP-2 routers.
6. Configure authentication by interface. If you enable authentication, a password must be configured.
7. Configure IGP/EGP interaction. Configures the autonomous system label to which the router belongs, defines the default route-to-route traffic destined for non-RIP networks towards the router which carries out port functions.
8. Configure timers. This is to adjust the timers which intervene in RIP-2. We recommend that you do not adjust the default value, or this is carried out by qualified staff.

If you configure RIP to use broadcast messages to update its routes, you must specify the broadcast IP address format.

Chapter 2
RIP Configuration

1. RIP Protocol Configuration commands

This section describes the commands to configure the RIP protocol. To access to the RIP configuration environment, enter the following commands:

```
*PROCESS 4
Config> PROTOCOL RIP

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

Command	Function
? (HELP)	Lists the commands or their available options.
ACCEPT-RIP-ROUTE	Determines the networks that will always accept routes.
AGGREGATION-TYPE	Configures the RIP aggregation type.
ALLOW-DISCONNECTED-SUBNETTED-NETWORKS	Permits propagation of disconnected subnets.
AS-LABEL	Configures the Autonomous Systems for IGP/EGP interactions.
AUTHENTICATION	Configures RIP authentication.
COMPATIBILITY	Configures RIP compatibility in transmission and reception.
COST-ADDITIONAL	Associates a cost to an interface.
DISABLE	Disables the RIP protocol or determined characteristics.
DISTRIBUTE-LIST	Establishes filters for the distributed routes (incoming and outgoing).
ENABLE	Enables the RIP protocol or determined characteristics.
LIST	Lists the RIP configuration.
NO	Disables or eliminates functions.
OFFSET-LIST	Establish input/output offset lists.
ORIGINATE-RIP-DEFAULT	Establishes a default route for other routing protocols.
RECEIVING	Configures reception parameters.
SENDING	Configures transmission parameters.
TIMERS	Configures the RIP timers.
EXIT	Exits the RIP configuration process.

1.1. ? (HELP)

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

Syntax:

```
RIP config> ?
```

Example:

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

1.2. ACCEPT-RIP-ROUTE

With the **RECEIVING** command the router ignores the information received in the RIP packets referring to routes towards networks or subnets. These filters are individually established for each interface.

Through the **DISTRIBUTE-LIST IN** and **RECEIVING <address IP-NET/SUBNET> DISTRIBUTE-LIST** commands you can indicate that the router must only accept information received with reference to determined routes, filtering the said routes both globally for all the interfaces and well as individually for each interface.

However, even though you program these filters, it is possible to accept routes which have determined network or subnet destinations. This can be achieved through the **ACCEPT-RIP-ROUTE** command. The steps to be carried out are as follows: if you program **ACCEPT-RIP-ROUTE** 10.0.0.0, and the previously mentioned filters are programmed in a determined interface, the router analyzes the RIP packet. If the destination network referred to is 10.0.0.0, it will accept this information independently of the configured filters.

Syntax:

```
RIP config> ACCEPT-RIP-ROUTE <address IP-NET/SUBNET>
```

Example:

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

1.3. AGGREGATION-TYPE

The **AGGREGATION-TYPE** command is used to configure the type of RIP aggregation for the router network interfaces. The type of routes to transmit through a specified interface depends on the state of the sending flags and the type of aggregation configured. This will be described further on.

On executing the said command, a list of all the logical interfaces (IP addresses) will appear where you can configure the type of RIP aggregation. Introduce an existing address and subsequently select the required option.

Syntax:

```
RIP config> AGGREGATION-TYPE <address IP-NET/SUBNET>
none                    do not aggregate
aggregation-routes      use aggregation routes
subnetted-networks      aggregate subnets
all                     aggregate all
```

The meaning of the aggregation types is as follows:

none	No aggregation is carried out. I.e. aggregation routes and subnet aggregation routes are not sent. This is the default option.
aggregation-routes	Aggregation routes are not strictly speaking routes rather they are marks that appear in the active routes table indicating there is a series of routes being aggregated. On activating this type of aggregation, only aggregation routes and routes that do not pertain to any aggregation are sent. Therefore the aggregated routes are not sent. So that an aggregation route is announced, one of the routes composing this (aggregated route) must be of a certain type so that the sending flags permit its transmission.
subnetted-networks	In the routes table when a subnet route is learned or configured, a "Sbnt" route or subnets aggregation route with destination "subnet network" and next hop "none" automatically appears. On activating this type of aggregation the subnet aggregation routes are sent provided that one of the subnets providing this is of a certain type so that the sending flags permit the transmission.
all	Through this option, both of the above are enabled together. I.e. both the aggregation routes as well as the subnets aggregation routes are sent.

Example:

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

1.4. ALLOW-DISCONNECTED-SUBNETTED-NETWORKS

The **ALLOW-DISCONNECTED-SUBNETTED-NETWORKS** command is used to permit routes to subnets to be sent and received via the interface independently of the said interface network. By default disconnected networks are allowed.

On executing the said command, a list of all the logical interfaces (IP addresses) will appear where you can configure the said command. Introduce an existing address and the disconnected subnets transmission and reception will be enabled for the said address.

Syntax:

```
RIP config> ALLOW-DISCONNECTED-SUBNETTED-NETWORKS <address IP-NET/SUBNET>
```

1.5. AS-LABEL

For IGP/EGP interaction. This is configurable through the logical interface (IP address). On executing the **AS-LABEL** command, a list of all the logical interfaces appears where you can configure the said command. Introduce an existing address and subsequently introduce the Autonomous System (AS) number required.

Example:

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

1.6. AUTHENTICATION

Authentication is sent with each packet and checked in each received packet. Additionally this is configurable through the logical interface (IP address). On executing the **AUTHENTICATION**, a list of all the logical interfaces appears where you can configure the RIP authentication.

Example:

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

The following algorithm is used when authenticating:

- The router is not configured to authenticate. The unauthenticated RIP-1 and RIP-2 packets will be accepted. RIP-2 packets with authentication will be dropped.
- The router is configured to authenticate. All RIP-1 and those RIP-2 packets that do not pass authentication will be dropped. All sent packets will be authenticated.

1.7. COMPATIBILITY

The RFC 1058 recommendation specifies that all RIP messages version 0 must be dropped, those with version 1 must be dropped if any of the MBZ (must be zero) fields is not zero and those with versions subsequent to 1 must be accepted.

However, there does arise the need to implement a compatibility selector for two reasons. Firstly there are RIP-1 implementations that do not follow the above recommendation. Secondly, the use of multicast can prevent systems with RIP-1 from receiving RIP-2 packets. This compatibility selector is configurable in the interface.

Use the **COMPATIBILITY** command to configure the compatibility selectors.

On executing the said command, a list of all the logical interfaces (IP addresses) will appear where you can configure the RIP compatibility. Introduce an existing address and subsequently select the required option.

Syntax:

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

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

The send selector has four positions:

none: disables the transmission of RIP packets in this interface.

rip1: only RIP version 1 packets are sent.

rip2-broadcast: where RIP version 2 packets are sent by broadcast.

rip2-multicast: where RIP version 2 packets are sent by multicast.

We strongly recommend selecting values *RIP1* or *RIP2-multicast* and not *RIP2-broadcast* in order to avoid possible comprehension problems in *RIP1* devices. *RIP2-broadcast* should only be used when the administrator is fully aware of all the consequences.

The receive selector also has four positions:

rip1: only accepts RIP version 1 packets.

rip2: only accepts RIP version 2 packets.

both: accepts both versions.

none: disables RIP listening in this interface.

1.8. COST-ADDITIONAL

This command is used to associate a cost to an interface in such a way that all the RIP routes learned by the said interface will increase the cost in as many units as indicated by this parameter + 1 (if the cost is zero, the RIP protocol will only increase by 1 unit). The range of values is between 0 and 15 inclusive. The default value is zero.

Example:

```
RIP config> COST-ADDITIONAL
IP addresses for each interface:
 ethernet0/0     192.7.1.253     255.255.255.0   NETWORK broadcast,  fill 0
 serial0/0                                       IP disabled on this ifc
 serial0/1       10.0.0.1        255.255.255.0   NETWORK broadcast,  fill 0
 serial0/2                                       IP disabled on this ifc
 bri0/0                                          IP disabled on this ifc
 x25-node                                        IP disabled on this ifc
```

```
Which address (ifc name for unnumbered) [0.0.0.0]? 192.7.1.253
Per interface additional cost [0]? 5
RIP config>
```

If you introduce a value outside of the permitted range:

Example:

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

1.9. DISABLE

The **DISABLE** command disables the RIP protocol in the device.

Syntax:

```
RIP config>DISABLE
```

Example:

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

1.10. DISTRIBUTE-LIST

The **DISTRIBUTE-LIST** command permits you to establish filters for the distributed routes, both for incoming (received) and outgoing (announced). All routes will be contrasted with the corresponding distribution lists and only in cases where these are not rejected by any of these lists will the said route be processed.

This lists used to filter the routes are the standard Access Control Lists. These are configurable through the FEATURE ACCESS menu found in the Configuration Process.

Please note that the access lists specified through this command are applied to the routes contained in the RIP packets and not to the source or destination address fields in the said packets.

The **DISTRIBUTE-LIST** command has two options. One to configure the list applicable to the received routes and the other to configure the list applicable to the announced routes.

Syntax:

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

a) DISTRIBUTE-LIST IN

Through this command, you can configure the global distribution list applicable to all routes received through any interface.

So that a route is accepted and processed, this must be permitted by the global distribution list and also by the interface distribution list through which it was received.

The access list going to be used must exist and cannot be assigned to any other protocol. Therefore before using this command you need to have created the said list from the FEATURE ACCESS configuration menu.

The valid values in the access control list are from 1 to 99 (standard IP lists).

Example:

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

b) DISTRIBUTE-LIST OUT

Through this command you can configure the global distribution list applicable to all routes to be sent via any interface.

So that a route is sent, it must be permitted by the global distribution list and also by the interface distribution list through which it is going to be sent.

The access list going to be used must exist and cannot be assigned to any other protocol. Therefore before using this command you need to have created the said list from the FEATURE ACCESS configuration menu.

The valid values in the access control list are from 1 to 99 (standard IP lists).

Example:

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

1.11. ENABLE

The **ENABLE** command enables the RIP protocol in the device.

Syntax:

```
RIP config> ENABLE
```

Example:

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

1.12. LIMIT-RIP

The **LIMIT-RIP** command deactivates the RIP protocol in Frame Relay interfaces. When LIMIT-RIP is enabled, the RIP packets are not sent via the Frame Relay interfaces unless they are in ISDN backup. The LIMIT-RIP option is disabled by default.

This command exists for when the **Teldat Router** operates with the **CENTRIX-P** backup device in certain Frame Relay virtual circuits backup scenarios over ISDN. This command affects all the device's Frame Relay interfaces.

Note: This command should not be enabled under other circumstances and must always be used by qualified staff.

Example:

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

1.13. LIST

Syntax:

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

a) LIST ADDRESS-OPTIONS

Use the **LIST ADDRESS-OPTIONS** command to see all the options for a determined interface.

Example:

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

b) LIST ALL

Use the **LIST ALL** command to obtain a list of all configured parameters.

Example:

```
RIP config> LIST ALL
RIP: enabled
RIP default origination: OSPF, cost = 1
Options per interface address:
Interface:  ethernet0/0
    Address: 192.7.1.253
        Output distribute list:.........No
        Send network routes:............Yes
        Send subnetwork routes:.........Yes
        Send static routes:.............No
        Send direct routes:.............Yes
```

```
        Send default routes:.............No
        Poison reverse enabled:..........Yes
        Autonomous system label:.........0
        Sending compatibility:...........RIP2 Multicast.
        Input distribute list:...........No
        Receive network routes:..........Yes
        Receive subnetwork routes:.......Yes
        Overwrite default routes:........No
        Overwrite static routes:.........No
        Receiving compatibility:.........RIP2.
        Authentication:..................Clear password.
        Aggregation type:................Do not aggregate.
        Allow disconnected networks:..Yes
        Per interface additional cost: 0
more ?
Interface:  serial0/1
    Address: 10.0.0.3
        Output distribute list:..........No
        Send network routes:.............Yes
        Send subnetwork routes:..........Yes
        Send static routes:..............No
        Send direct routes:..............Yes
        Send default routes:.............No
        Poison reverse enabled:..........Yes
        Autonomous system label:.........0
        Sending compatibility:...........RIP2 Broadcast.
        Input distribute list:...........No
        Receive network routes:..........Yes
        Receive subnetwork routes:.......Yes
        Overwrite default routes:........No
        Overwrite static routes:.........No
        Receiving compatibility:.........RIP1 or RIP2.
        Authentication:..................No.
        Aggregation type:................Do not aggregate.
        Allow disconnected subnetted networks:..Yes
        Per interface additional cost: 0
more ?
Address: 192.3.1.2
        Output distribute list:..........No
        Send network routes:.............Yes
        Send subnetwork routes:..........Yes
        Send static routes:..............No
        Send direct routes:..............Yes
        Send default routes:.............No
        Poison reverse enabled:..........Yes
        Autonomous system label:.........0
        Sending compatibility:...........RIP2 Broadcast.
        Input distribute list:...........No
        Receive network routes:..........Yes
        Receive subnetwork routes:.......Yes
        Overwrite default routes:........No
        Overwrite static routes:.........No
        Receiving compatibility:.........RIP1 or RIP2.
        Authentication:..................No.
        Aggregation type:................Do not aggregate.
        Allow disconnected subnetted networks:..Yes
        Per interface additional cost: 0
more ?
Accept RIP updates always for:
[NONE]

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

c) LIST AS-LABELS

Use the **LIST AS-LABELS** command to obtain a list of all the address labels identifying the Autonomous Systems (AS) configured in this address.

Example:

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

d) LIST DISTRIBUTE-LISTS

Use the **LIST DISTRIBUTE-LISTS** command to view the global distribution lists. I.e. the lists configured to filter the routes to announce and the received routes at a global level.

Example:

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

This command only displays the global distribution lists; in order to view those specified for each interface, use the LIST ADDRESS-OPTONS or the LIST ALL commands.

e) LIST LIMIT-RIP

Use the **LIST LIMIT-RIP** command to view the LIMIT-RIP option.

Example:

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

f) LIST TIMERS

Use the **LIST TIMERS** command to obtain a list of the values configured in the timers.

Example:

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

1.14. NO

The **NO** command is used to eliminate or disable certain functionalities.

Syntax:

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

a) NO ACCEPT-RIP-ROUTE

Use the **NO ACCEPT-RIP-ROUTE** command to delete a route from the networks list that the RIP protocol always accepts.

Syntax:

```
RIP config> NO ACCEPT-RIP-ROUTE <address IP-NET/SUBNET>
```

Example:

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

b) NO ALLOW-DISCONNECTED-SUBNETTED-NETWORKS

Use the **NO ALLOW-DISCONNECTED-SUBNETTED-NETWORKS** command so that the routes to subnets are not broadcast outside of the network that the said subnets belong to. In the same way, a given interface will not accept routes to subnets that do not belong to the interface network.

On executing this command, a list of all the logical interfaces (IP addresses) appears where you can configure the said command. Introduce an existing address and the sent and receive of disconnected subnets outside of this network are disabled by the said address.

Syntax:

```
RIP config> NO ALLOW-DISCONNECTED-SUBNETTED-NETWORKS <address IP-NET/SUBNET>
```

c) NO AUTHENTICATION

Use the **NO AUTHENTICATION** command to disable authentication in a given interface.

Syntax:

```
RIP config> NO AUTHENTICATION <address IP-NET/SUBNET>
```

Example:

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

d) NO DISTRIBUTE-LIST

Use the **NO DISTRIBUTE-LIST** command to disable filtering of the receive or send routes. This command only affects the global filter configured through the **DISTRIBUTE-LIST** command not that configured in each interface.

The **NO DISTRIBUTE-LIST** command has two options, one to disable receive routes filtering and the other to disable filtering for the routes to announce.

Example:

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

e) NO LIMIT-RIP

The **NO LIMIT-RIP** command actives the RIP protocol in Frame Relay interfaces. Use this command if you do not wish to restrict the RIP protocol in the device.

Example:

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

f) NO OFFSET-LIST

The **NO OFFSET-LIST** command eliminates a previously configured offset-list.

Example:

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

g) NO ORIGINATE-RIP-DEFAULT

The **NO ORGINATE-RIP-DEFAULT** prevents the router from generating a default route.

Example:

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

1.15. OFFSET-LIST

An **OFFSET-LIST** permits the cost of certain routes to increase both in transmission and in reception. This cost increase is only carried out for routes that match the access list configured as an offset-list. Optionally you can specify a particular interface over which cost increase is carried out.

The lists used to vary the cost of the routes are standard Access Control Lists. These can be configured from the Configuration Process FEATURE ACCESS menu.

In order to compare the route IP addresses and mask with those in the access list, the same process is used as for the distribute-list with the RIP_LISTS_USE_MASK patch having the same effect (see appendix A, section 4).

Syntax:

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

ip-address	Specifies the IP address for a particular interface. If this parameter is not configured, the offset is applied to all the router interfaces which send/receive RIP routes.
in <offset>	Increases the cost of the incoming routes which coincide with the configured access list.
out <offset>	Increases the cost of the outgoing routes which coincide with the configured access list.

Example 1:

You wish to increase by 3, the cost of all the routes sent by any interface which are included in network 172.24.0.0.

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

Example 2:

You wish to increase by 1, the cost of all the network 172.1.0.0 routes which are sent by the interface with IP address 172.24.78.131 or by the interface with IP address 10.30.1.1, excepting those which exclusively refer to host 172.1.1.5.

```
Config> SHOW CONFIG
feature access-lists
; -- Access Lists user configuration --
   access-list 1
;
      entry 1 default
      entry 1 deny
      entry 1 source address 172.1.1.5 255.255.255.255
;
      entry 2 default
      entry 2 permit
      entry 2 source address 172.1.0.0 255.255.0.0
;
   exit
;
exit
;
protocol rip
; -- RIP protocol user configuration --
   enable
   offset-list 1 out 1 ip-address 172.24.78.131
;
   offset-list 1 out 1 ip-address 10.30.1.1
;
exit
;
```

1.16. ORIGINATE-RIP-DEFAULT

Use the **ORIGINATE-RIP-DEFAULT** command if the network is using RIP, and connects to a network using another routing protocol (such as OSPF) to establish (originate) a single default route to that network.

This default route will route traffic bound for non-RIP networks to a router carrying out port functions. The **Teldat Router** only accepts OSPF.

Example:

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

1.17. RECEIVING

Use the **RECEIVING** command to configure the RIP reception parameters for the router network interfaces. The set of routes which are processed by a logical interface (IP address), is the union of the selected routes activating some of the flags (described below). These flags control how the information received in the RIP frames is incorporated in the router's routing tables. By activating certain flags the router will not take static routing information into account in cases where the RIP finds a better route than that already set.

On executing this command, a list of all the local logical interfaces (IP addresses) appears where you can configure the RIP reception. Introduce an existing address and subsequently select the option required to enable it or respond no followed by the option to disable it:

Syntax:

```
RIP config> RECEIVING <address IP-NET/SUBNET>
default-routes          process default routes
distribute-list         access list for routes filtering
network-routes          process network routes
no
   default-routes          process default routes
   distribute-list         access list for routes filtering
   network-routes          process network routes
   subnetwork-routes       process subnetwork routes
   static-routes           process static routes
subnetwork-routes       process subnetwork routes
static-routes           process static routes
```

The meaning of each option is:

default-routes	Prevents a default RIP route, received by the IP Interface address, from being stored as the default route.
distribute-list	Determines the list to be used to filter the routes received by the IP Interface address. This option is disabled by default; therefore the routes will not be affected by this filter. In order to configure this option, you need to indicate a standard IP Access Control List (1 to 99) previously defined from the FEATURE ACCESS configuration menu.
network-routes	If this is activated, network routes are accepted. If this is deactivated, only those network routes introduced through the **ACCEPT-RIP-ROUTE** command will be accepted.
subnetwork-routes	If this is activated, subnet routes are accepted. If this is deactivated, only those subnet routes introduced through the **ACCEPT-RIP-ROUTE** command will be accepted
static-routes	This command prevents RIP routes received in the interface IP address overwrites the static routes.

If the "Allow disconnected subnetted networks" flag is disabled: for a given interface it will only accept those subnet routes which belong to the same IP network as the interface. E.g. destination subnet route: 192.6.1.144, mask: 255.255.255.248, if the incoming interface address is 192.6.1.x, the route is accepted. However, if the incoming interface belongs to a different IP network e.g. 193.5.1.x,

the route received is rejected. If contrariwise, the "Allow disconnected subnetted networks" is enabled, then reception of subnets via interfaces which do not belong to the subnet is permitted.

1.18. SENDING

Use the **SENDING** command to configure the RIP sending parameters for the router network interfaces. The type of routes to send through a determined interface depends on the status of the flags (described below).

On executing this command, a list of all the logical interfaces (IP addresses) appears where you can configure the RIP sending. Introduce an existing address and subsequently select the option required to enable it or respond no followed by the option to disable it:

Syntax:

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

The meaning of each option is:

default-routes — If this flag is activated, the router indicates the default route in the RIP responses to with the IP address, if a default router exists. The route for the default router is indicated as a route bound for destination 0.0.0.0.

direct-routes — If this flag is activated, the router will include all the routes for the directly connected networks in the RIP responses related to the IP address. If this is not activated, only directly connected networks which share RIP protocol (which have RIP enabled for send or reception) will be sent. By default this is activated.

distribute-list — Determines the list to be used to filter the routes to send related to the IP Interface address. This option is disabled by default; therefore the routes will not be affected by this filter. In order to configure this option, you need to indicate a standard IP Access Control List (1 to 99) previously defined from the FEATURE ACCESS configuration menu.

network-routes — If this flag is activated, the router indicates all the routes at the network layer in the RIP responses related to the IP address.

poisoned-reverse — This flag is activated by default. Enable or disable the poisoned reverse in the split-horizon process. When the routes learnt from a gateway are enabled, they are broadcast with infinite metrics (16). If this is disabled these routes are not broadcast. The protocol convergence is quicker when this is enabled

subnetwork-routes — If this flag is enabled, the router indicates the subnet routes in the RIP responses related to the IP address. Sending a subnet route depends on the

configuration of the aggregation type and the "Allow disconnected subnetted networks" flag. If the aggregation type is "Use aggregation routes" and the route is aggregated by the aggregation route (Aggr), only that route is sent (Aggr). If the aggregation is configured as "Aggregate subnets" then both are sent i.e. the subnet routes as well as the subnet aggregation (Sbnt). If the "Allow disconnected subnetted networks" flag is disabled: for a given interface only those subnet routes which belong to the same IP network as the interface are included. For the other interfaces the network route is included. E.g. destination subnet route: 192.6.1.144, mask: 255.255.255.248, if the outgoing interface address is 192.6.1.x, the route will send as is. But if the outgoing interface belongs to a different IP network e.g. 193.5.1.x, the route sent is the destination aggregation network: 192.6.1.0 mask: 255.255.255.0. If the "Allow disconnected subnetted networks" flag is enabled, then you can also send subnets via interfaces which do not pertain to the subnet.

static-routes If this flag is activated, the router will include all the network routes statically configured in the RIP responses related to the IP address.

The set of routes to send through a specific interface also depends on the type of aggregation configured.

1.19. TIMERS

There exist three timers which control the algorithm function (as defined in the RIP RFC). These values should only be changed in certain exceptional cases and the network manager should be fully aware of the possible consequences.

Example:

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

The meaning of the parameters is as follows:

Periodic sending timer The default value is 30 seconds this being the time between sending the periodic responses.

Route expire timer The default value is 180 seconds. If this time should expire without a response refreshing the route, this route is considered invalid.

Route garbage timer The default value is 120 seconds. Once the route is considered invalid, it is maintained in the routing tables for 120 seconds with metric value 16 (indefinite) so the neighboring RIP routers realize that it is going to be deleted.

1.20. EXIT

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

Syntax:

```
RIP config> EXIT
```

Example:

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

Chapter 3
RIP Monitoring

1. RIP Protocol Monitoring commands

This chapter describes all the RIP protocol monitoring commands. In order to access the RIP protocol monitoring environment, enter the following commands:

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

Command	Function
? (HELP)	Lists the available commands or options.
LIST	Displays the RIP statistics.
EXIT	Exits the RIP monitoring process.

1.1. ? (HELP)

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

Syntax:

```
RIP> ?
```

Example:

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

1.2. LIST

Use the **LIST** command to display RIP statistics. This also shows the detailed statistics for each interface.

Syntax:

```
RIP> LIST
```

Example:

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

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

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

The meaning of the parameters is as follows:

Pack. rx errors	Counts the number of packets received with errors.
Routes rx errors	Counts the number of routes received with errors.
Triggered updates tx	Counts the updating for sent route changes.

1.3. EXIT

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

Syntax:

```
RIP> EXIT
```

Example:

```
RIP> EXIT
```

Appendix A
Filtering through lists

1. Introduction

Through the **DISTRIBUTE-LIST**, **RECEIVING DISTRIBUTE-LIST** and **SENDING DISTRIBUTE-LIST** commands you can configure a powerful routes filtering tool depending on your destination network. This tool is based on the Access Control Standard IP Lists in order to determine which routes are distributed and which ones are dropped.

2. Using the lists to filter routes

In order to determine which routes are distributed and which ones are dropped, each route is compared with the assigned Access Control Lists which must be Standard IP lists.

- At reception: the route is only processed if it is permitted by both the list configured through the **DISTRIBUTE-LIST IN** command and by the list configured through the **RECEIVING <IP net address through which the route is received> DISTRIBUTE-LIST** command.
- In transmission: the route is only sent if it is permitted by both the list configured through the **DISTRIBUTE-LIST OUT** command and by the list configured through the **SENDING <IP net address through which the route is sent> DISTRIBUTE-LIST** command.

In order to determine if a list will permit a route, the route is checked against each entry in the list. This is always carried out in the order defined when the list was created.

- The first entry that coincides with the route is the one that will determine if the list will permit the said route or not.
- If none of the entries coincides with the route, then the route will not be permitted.

To compare a route with an entry in the list, the announced network address is taken. This is compared with the list entry source address/mask.

The RIP protocol can only use Standard IP lists and only the list entries Source field is used.

For example, supposing we have the following list configured:

```
Standard Access List 1, assigned to RIP

1     DENY    SRC=192.168.1.0/24

2     PERMIT  SRC=192.168.0.0/16
```

If this list is applied at reception, the following occurs:

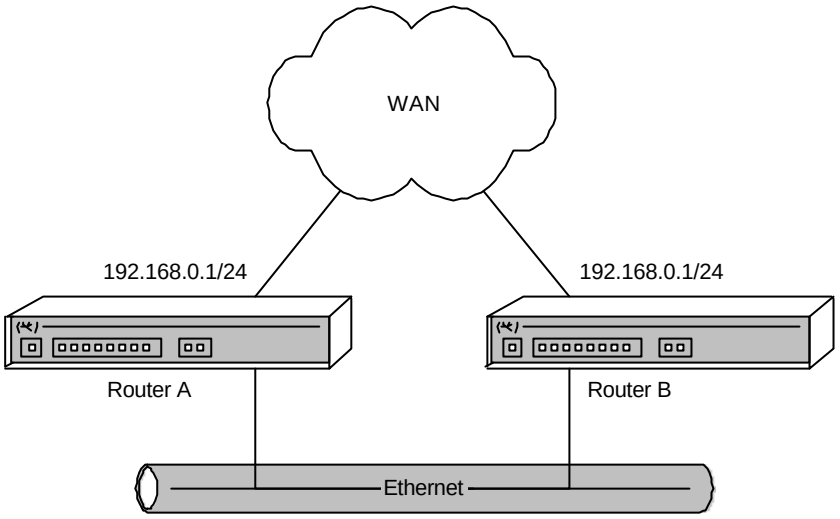
- If we receive the route to network 192.168.1.0 it is discarded as it coincides with the first entry in the list and this is Deny.
- If we receive the route to network 192.168.2.0 it is processed. This route does not coincide with the first entry but does with the second one. This entry is Permit.
- If we receive the route to network 192.168.0.0 it is processed. This route does not coincide with the first entry but does with the second one. This entry is Permit.
- If we receive the route to network 192.6.2.0 it is discarded as it does not coincide with any entry in the list and the default action is Deny.
- If we receive a default route (network 0.0.0.0) this is discarded as it does not coincide with any entry in the list and the default action is Deny.

In cases where you do not want a list to discard default routes, you must add an entry to that effect. This is because the default routes are propagated by RIP as network 0.0.0.0/0.

3. Example scenario

In this section, a basic user scenario for an entity accessing its branches via two **Teldat Routers** is presented.

Supposing we have two devices installed in the same segment, which provide access to the entity branch offices as shown in the following figure:



In this case, both Router A and Router B access the WAN with the same IP address (192.168.0.1) and we do not want the said network to be broadcast by RIP to the segment.

In order to do this, simply define an access list:

```
Config> FEATURE ACCESS

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


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

and assign the access list to the RIP protocol to filter the routes to be sent:

```
Config> PROTOCOL RIP

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

In this way, all the routes except those from network 192.168.0.0 are distributed. There are a few points that should be noted:

- You need to have added the second entry in the list (Permit 0.0.0.0/0) as the default action of a list (when no entry coincides) is to Deny. In this way all routes that do not coincide with the first entry are Permitted.
- The first entry will deny the aggregation network 192.168.0.0/16, as its IP address (192.168.0.0) is contained in 192.168.0.0/24.
- The list therefore permits distributing of the default routes thanks to the second entry.

4. Filtering of routes with mask

On occasions it may be necessary to not only use the IP address but also to use the route mask propagated by RIP when filtering through lists.

Let's go back to the example scenario where we created a list to prevent network 192.168.0.0/24 being propagated by RIP.

```
Standard Access List 1, assigned to RIP

1     DENY    SRC=192.168.0.0/24

2     PERMIT  SRC=0.0.0.0/0
```

In this case, as you can see, it is impossible for the aggregation network 192.168.0.0/16 to be propagated by RIP as both networks share the same 192.168.0.0 address which is Denied through the first list entry.

In order to avoid this, you can enable a *patch* which ensures that the mask is also compared. When this *patch* is enabled, the route network will only agree with a list entry if:

- The route network is identical to the entry source network or
- The route network is a subnet of the entry source network.

For example, with the scenario list:

- Routes towards network 192.168.0.0/24 will be discarded
- Routes towards network 192.168.0.0/16 will not be discarded
- Routes towards network 192.168.0.0/32 will be discarded

In order to enable the *patch*, use the **ENABLE PATCH** configuration command and assign value **1** with the name **RIP_LISTS_USE_MASK**.

Example:

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

In order to disable the *patch*, use the **DISABLE PATCH** configuration command with the name **RIP_LISTS_USE_MASK**.

Example:

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

5. Filtering the default route

It's possible to filter the default route through access lists, both to permit this and to deny it. However, the configuration varies depending if the **RIP_LISTS_USE_MASK** patch is enabled or not. The access list configurations for each case are shown below.

Permit default route, without enabling RIP_LISTS_USE_MASK

The following entry in the access list explicitly permits the default route:

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

Permits default route, with RIP_LISTS_USE_MASK enabled

In this case, in order to only permit the default route, you must deny all other routes (subnets) which you do not wish to distribute. This is shown in the following example where only the default route is permitted, all others being denied.

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

Deny default route, without enabling RIP_LISTS_USE_MASK

To only deny the default route, you can create an access list in the following way:

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

Deny default route, with RIP_LISTS_USE_MASK enabled

In this case, in order to only deny the default route, you must permit all the other routes (subnets) as shown in the following example:

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