RIP Protocol

Teldat-Dm 718

Legal Notice

Warranty

This publication is subject to change.

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

Teldat 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

Teldat-Dm702-I TCP-IP

Teldat-Dm704-I Configuration and Monitoring

Teldat-Dm752-I Access Control

Teldat-Dm764-I Route Mapping

Teldat-Dm775-I VRF Lite Facility

Teldat-Dm780-I Prefix Lists

Chapter 1 Introduction

1.1 Introduction

This chapter focuses on the use of the RIP protocol (Routing Information Protocol), which is an Interior Gateway Protocol (IGP). The Teldat router supports three different IGP protocols to build the IP routing table. These protocols are OSPF, I-BGP 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 BGP, OSPF and RIP protocols simultaneously.

Preference between protocols is marked by the administrative distance. The closer the administrative, the greater the preference. Below you will see a table containing the administrative distance default values depending on the 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

1.2 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* . This attribute assigned to a route separates the internal routes from the external ones (i.e. it allows IGP/EGP interaction).
- *Variable length Subnet Masks*. Allows an IP address to be fractioned in variable length subnets, retaining the IP address space.
- *Next Hop*. Deletes packets being routed with an extra number of hops.
- *Multicast*. Unlike broadcast, this mode reduces unnecessary load on the hosts that 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 finding 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.

1.2.1 Route Redistribution

RIP, in its predefined behavior, handles directly connected networks for interfaces where the said protocol has been enabled and the routes learned by RIP for other devices. Through the SENDING command you can enable the sending of other routes using RIP such as those learned by OSPF or BGP.

You can also enable the sending of other routes with RIP through the REDISTRIBUTE command, thus offering better control (based on route maps allowing route filtering and defining metric assignment policies).

As RIP uses metrics to determine which networks are accessible and what the best path is, it’s important to define a suitable metric assignment policy for the redistribution of networks from other protocols. There are two strategies for this:

(1) Use the REDISTRIBUTE command with a route-map specifying the metric to be assigned in each case through the SET METRIC option. In cases where the metric isn’t specified, this takes the same metric value as the redistributed route.

(2) Use the standard metric assignation policy through the SENDING command.

The standard metric assignation policy operates in RIP depending on the protocol that originated each route, as described below.

1.2.1.1 Directly connected Routes

The same metric as the directly connected route, i.e. metric 1.

1.2.1.2 Static Routes

The same metric as the static route.

1.2.1.3 OSPF Routes

The metric is assigned depending on the OSPF COMPARISON command configuration.

COMPARISON 1 configuration: redistributes the type 2 external OSPF routes with the same metric and the rest of the OSPF routes with metric 1.

COMPARISON 2 configuration: doesn't redistributes the type 2 external OSPF routes and the rest of the OSPF routes are redistributed with the same metric.

1.2.1.4 BGP Routes

The same metric as the BGP route.

1.3 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 sending or reception filters for routes through a **distribute-list**.

(8) Configure the behavior for importing routes from other routing protocols through the **redistribute** command.

(9) 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

2.1 RIP Protocol Configuration commands

This section describes the commands to configure the RIP protocol. To access 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.
AGGREGATION-TYPE	Configures the RIP aggregation type.
ALLOW-DISCON-NECTED-SUBNET-TED-NETWORKS	Permits propagation of disconnected subnets.
AUTHENTICATION	Configures RIP authentication.
CLEAR	Deletes the entire RIP configuration.
COMPATIBILITY	Configures RIP compatibility in transmission and reception.
COST-ADDITIONAL	Associates a cost to an interface.
DISABLE	Disables the RIP protocol.
DISTANCE	Configures the administrative distance for the RIP routes.
DISTRIBUTE-LIST	Establishes filters for the distributed routes (incoming and outgoing).
ENABLE	Enables the RIP protocol.
FAST-UPDATES	Enables and configures the fast-update facility parameters.
LIMIT-RIP	Valid for WRS backup environments, where the principal is an FR interface and the secondary is a DIAL interface. Serves to disable the RIP protocol in the principal FR.
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.
REDISTRIBUTE	Configures redistribution (importing) of routes from other protocols towards RIP.
SENDING	Configures transmission parameters.
TIMERS	Configures the RIP timers.
VRF	Specifies parameters for a VPN (*Virtual Private Network*).

EXIT	Exits the RIP configuration process.

2.1.1 ? (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> ?
  aggregation-type                          RIP aggregation parameters
  allow-disconnected-subnetted-networks     Routes to subnets are always sent
  authentication                            Authentication is sent and checked
  clear                                     Clears current configuration
  compatibility                             Configure the compatibility
                                            selectors
  cost-additional                           Associates a cost to an interface
  disable                                   Disables the RIP protocol
  distance                                  Administrative distance for RIP
                                            protocol
  distribute-list                           Establish input/output filters
  enable                                    Enables the RIP protocol
  fast-updates                              Enable fast updates
  limit-rip                                 Deactivates the RIP protocol in FR
  list                                      Display RIP configuration
  no
  offset-list                               Establish input/output offset lists
  originate-rip-default                     Originate a default ip route
  receiving                                 RIP reception parameters
  redistribute                              Redistribute information from
                                            another routing protocol
  sending                                   RIP sending parameters
  timers                                    Timers which control the algorithm
  vrf                                       Specify parameters for a VPN
                                            Routing/Forwarding instance
  exit
RIP config>
```

2.1.2 AGGREGATION-TYPE

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

When introducing this command, you must indicate the logical interface where you are going to configure (existing IP address or the name of the interface in cases of unnumbered addresses) and subsequently select the required option.

Syntax:

```
RIP config> aggregation-type { <IP_add> | <interface> }
  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, strictly speaking, not routes. They are marks that appear in the active routes table to indicate that several routes are 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 10.0.0.1 all
RIP config>
```

2.1.3 ALLOW-DISCONNECTED-SUBNETTED-NETWORKS

The **ALLOW-DISCONNECTED-SUBNETTED-NETWORKS** command is used to allow routes to subnets to be sent and received via the interface independently from said interface's network. Disconnected networks are allowed by default.

When entering this command, you must indicate the logical interface where you want to configure (existing IP address or the name of the interface in cases of unnumbered addresses) an existing address and the disconnected subnets transmission and reception will be enabled for said interface.

Syntax:

```
RIP config>allow-disconnected-subnetted-networks { <IP_add> | <interface> }
```

2.1.4 AUTHENTICATION

Authentication is sent with each packet and checked in each received packet. In addition, it is configurable through the logical interface (IP address or the interface name where there are unnumbered addresses). There are two types of authentication: password in clear and through MD5.

Syntax:

```
RIP config>authentication <authentication_type>{<IP_add> | <interface> }<password> |<key-chain>}
```

Example 1:

```
RIP config> authentication plain-text 1.1.1.1 <password>
RIP config>
```

If you use authentication with MD5, you must have previously configured the *key-chains* option in the features menu.

Example 2:

```
RIP config> authentication md5 1.1.1.1 <key_chain>
RIP config>
```

The following algorithm is used when authenticating:

- The router is not configured to authenticate. 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.

2.1.5 CLEAR

Deletes all the RIP configuration registers.

Syntax:

```
IP config>clear
```

Example:

```
IP config>clear
IP config>
```

2.1.6 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 over 1 must be accepted.

However, there is a 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 logical interface.

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

On executing this command, you need to enter an existing address or an interface name in cases of unnumbered addresses, and subsequently select the required option.

Syntax:

```
RIP config>compatibility
  <a.b.c.d>      Interface address
    receive        Receive selector
      both           Both versions are accepted
        <cr>
      rip1           Only accepts version 1 RIP packets
        <cr>
      rip2           Only accepts version 2 RIP packets
        <cr>
      none           RIP listening disabled in this interface
        <cr>
    send           Send selector
      rip1           Only RIP version 1 packets are sent
        <cr>
      rip2-broadcast Where the RIP version 2 packets are sent by broadcast
        <cr>
      rip2-multicast Where the RIP version 2 packets are sent by multicast
        <cr>      none           Disables the send RIP packets in this interface
        <cr>
  <interface>    Unnumbered interface
    receive        Receive selector
      both           Both versions are accepted
        <cr>
      rip1           Only accepts version 1 RIP packets
        <cr>
      rip2           Only accepts version 2 RIP packets
        <cr>
      none           RIP listening disabled in this interface
        <cr>
    send           Send selector
      rip1           Only RIP version 1 packets are sent
        <cr>
      rip2-broadcast Where the RIP version 2 packets are sent by broadcast
```

```
      <cr>
    rip2-multicast Where the RIP version 2 packets are sent by multicast
      <cr>
    none           Disables the send RIP packets in this interface
      <cr>
```

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.

2.1.7 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). Values range between 0 and 15 (both inclusive). The default value is zero.

Syntax:

```
RIP config>cost-additional ?
  <a.b.c.d>      Interface address
    <0..15>        Per interface additional cost
      <cr>
  <interface>    Unnumbered interface
    <0..15>        Per interface additional cost
      <cr>
```

Example:

```
RIP config> cost-additional 192.7.1.253 5
RIP config>
```

2.1.8 DISABLE

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

Syntax:

```
RIP config>disable
```

Example:

```
RIP config>disable
RIP config>
```

2.1.9 DISTANCE

The **DISTANCE** command sets the administrative distance for routes found through RIP. This administrative distance is used to determine if routes from other protocols should be overwritten when the administrative-distance command, explained in manual Teldat-Dm702-I "TCP-IP", is configured. If this command is enabled, the options for the RIP **RECEIVING** command, which affects the route overwriting, are ignored.

The default value is 100.

Syntax:

```
RIP config> distance ?
  <10..255>    Value in the specified range
```

Example:

```
RIP config>distance 30
RIP config>
```

2.1.10 DISTRIBUTE-LIST

The **DISTRIBUTE-LIST** command allows you to establish filters for the distributed routes, regardless of whether they are incoming (received) or outgoing (announced). All routes will be checked against the corresponding distribution lists. If the route is not rejected by any of these lists, it shall be processed.

The lists used to filter the routes are the standard Access Control Lists or the Prefix-Lists. These are configurable through the FEATURE ACCESS-LIST or FEATURE PREFIX-LIST menus. For further information on these Access Lists, please see manual Teldat-Dm 752-I "Access Control". Likewise, for more information on the configuration of Prefix Lists, see manual Teldat-Dm 780-I "Prefix Lists".

Note

Please note that only the routes contained in the RIP packets are checked against the access lists or prefix-lists specified through this command. The source or destination address fields in said packets are not.

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     Configures a list for input route filtering
  out    Configures a list for output route filtering
```

2.1.10.1 DISTRIBUTE-LIST IN ACCESS-LIST <id>

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

Note

For a route to be accepted and processed, it must be approved by the global distribution list and by the interface distribution list through which it was received.

There are two available options, depending on the type of list being assigned.

Syntax:

```
RIP config$distribute-list in ?
  access-list    Configures an access list
     <1..99>    Access List for routes filtering
  prefix-list    Configures a prefix list
     <1..199>    Prefix List for routes filtering
```

DISTRIBUTE-LIST IN ACCESS-LIST <ID>

This command assigns an *access* list for so all incoming routes can be filtered.

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 list from the FEATURE ACCESS configuration menu.

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

Example:

```
RIP config>distribute-list in access-list 1
RIP config>
```

DISTRIBUTE-LIST IN PREFIX-LIST <id>

This command assigns a *prefix* list so all incoming routes can be filtered.

The prefix list must have been previously created in the FEATURE PREFIX-LIST configuration menu and, unlike the access lists, can also be assigned to other protocols.

The valid values for the prefix lists range from 1 to 199.

Example:

```
RIP config>distribute-list in prefix-list 1
RIP config>
```

2.1.10.2 DISTRIBUTE-LIST OUT ACCESS-LIST <id>

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

Note

For a route to be sent, it must be approved by the global distribution list and by the interface distribution list through which it is going to be sent.

There are two available options, depending on the type of list being assigned.

Syntax:

```
RIP config>distribute-list out ?
  access-list    Configures an access list
     <1..99>    Access List for routes filtering
  prefix-list    Configures a prefix list
     <1..199>    Prefix List for routes filtering
```

DISTRIBUTE-LIST OUT ACCESS-LIST <id>

This command assigns an *access* list so all outgoing routes can be filtered.

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 list from the FEATURE ACCESS-LIST configuration menu.

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

Example:

```
RIP config>distribute-list out access-list 1
RIP config>
```

DISTRIBUTE-LIST OUT PREFIX-LIST <id>

This command assigns a *prefix* list so all outgoing routes can be filtered.

The prefix list must have been previously created in the FEATURE PREFIX-LIST configuration menu and, unlike the access lists, can also be assigned to other protocols.

The valid values for the prefix lists range from 1 to 199.

Example:

```
RIP config>distribute-list out prefix-list 1
RIP config>
```

2.1.11 ENABLE

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

Syntax:

```
RIP config>enable
```

Example:

```
RIP config>enable
RIP config>
```

2.1.12 FAST-UPDATES

The **FAST-UPDATES** command activates and configures the RIP "fast update facility parameters.

The RIP RFC establishes that when a determined interface which has RIP enabled activates, an "update" messages must be sent immediately (message containing all the configured RIP routes to be sent through the interface). There are situations where this message may be lost (due to network congestion, because it's a DIAL interface, configured so RIP does not trigger calls, etc). In cases where this first message is lost, it will not be resent until the period of time configured for the "Periodic sending timer" times out. This is usually set to 30 seconds, depending on the RIP convergence speed.

The "fast update" facility is a process through which the "update" message is sent, when an interface activates, a configurable number of times ("Fast update max iterations" parameter) with a period between retries also configurable ("Fast update rate" parameter). This allows you to ensure these are correctly sent and there is greater RIP convergence speed when interfaces activate.

Syntax:

```
RIP config>fast-updates ?
  <1..65535>    Fast update rate
    <1..65535>    Fast update max iterations
      <cr>
```

Example:

```
RIP config>fast-updates 1 10
```

2.1.13 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 circuit backup scenarios over ISDN. This command affects all the device's Frame Relay interfaces.

Note

This command should not be enabled in any other circumstances and must always be used by qualified staff.

Example:

```
RIP config>limit-rip
RIP config>
```

2.1.14 LIST

Displays the RIP protocol configuration.

Syntax:

```
RIP config> list ?
  address-options     See all the options for a determined interface
  all                 Obtain a list of all configured parameters
  distribute-lists    See all configured filter lists
  fast-update         List the fast-update's parameters
  limit-rip           See the LIMIT-RIP option
  timers              Obtain a list of the values configured in the timers
```

2.1.14.1 LIST ADDRESS-OPTIONS

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

Example:

```
RIP config>list address-options ?
  <a.b.c.d>      Interface address
  <interface>    Unnumbered interface
RIP config>list address-options 192.7.1.253
    Address: 192.7.1.253
        Output distribute list:.........No
        Send network routes:............Yes
        Send subnetwork routes:.........Yes
        Send bgp routes:................No
        Send ospf routes:...............Yes
        Send static routes:.............No
        Send direct routes:.............Yes
        Send default routes:............No
        Poison reverse enabled:.........Yes
        Spit horizon:...................Yes
        Sending compatibility:..........RIP2 Multicast.
        Input distribute list:..........Prefix List 1
        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>
```

Command history:

Release	Modification
11.01.00	Since version 11.01.00, the output of this command has changed and no longer shows info on the Autonomous System Label.

2.1.14.2 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: disabled
Options per interface address:
Interface: ethernet0/0
    Address: 172.24.78.115
```

```
        Output distribute list:.........No
        Send network routes:............Yes
        Send subnetwork routes:.........Yes
        Send bgp routes:................No
        Send ospf routes:...............Yes
        Send static routes:.............No
        Send direct routes:.............Yes
        Send default routes:............No
        Poison reverse enabled:.........Yes
        Spit horizon:...................Yes
        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
    Address: 192.6.1.251
        Output distribute list:.........No
        Send network routes:............Yes
        Send subnetwork routes:.........Yes
        Send bgp routes:................No
        Send ospf routes:...............Yes
        Send static routes:.............No
        Send direct routes:.............Yes
        Send default routes:............No
        Poison reverse enabled:.........Yes
        Spit horizon:...................Yes
        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

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 fast-update: enabled
    fast-update rate: 1
    fast-update maximum number of iterations: 10
RIP config>
```

Command history:

Release	Modification
11.01.00	Since version 11.01.00, the output of this command has changed and no longer shows info on the Autonomous System Label.

2.1.14.3 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>
```

Command history:

Release	Modification
11.01.00	Since version 11.01.00, this command has been obsoleted and is no longer available.

2.1.14.4 LIST DISTRIBUTE-LISTS

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

Example:

```
RIP config>list distribute-lists
Output distribute list: Access List 1
Input distribute list:  Prefix List 2
RIP config>
```

Note

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.

2.1.14.5 LIST FAST-UPDATE

Use the **LIST FAST-UPDATE** command to view the “fast update” facility configuration parameters.

Example:

```
RIP config>list fast-update
RIP fast-update: enabled
    fast-update rate: 1
    fast-update maximum number of iterations: 10
RIP config>
```

2.1.14.6 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>
```

2.1.14.7 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>
```

2.1.15 NO

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

Syntax:

```
RIP config>no ?
  allow-disconnected-subnetted-networks    Routes to subnets are always sent
  authentication                           Authentication is sent and checked
  distribute-list                          Establish input/output filters
  fast-updates                             Enable fast updates
  limit-rip                                Deactivates the RIP protocol in FR
  offset-list                              Establish input/output offset lists
  originate-rip-default                    Originate a default ip route
  redistribute                             Redistribute information from
                                           another routing protocol
  timers                                   Timers which control the algorithm
```

2.1.15.1 NO ALLOW-DISCONNECTED-SUBNETTED-NETWORKS

Use the **NO ALLOW-DISCONNECTED-SUBNETTED-NETWORKS** command to stop the routes to subnets from being broadcasted outside of their networks. In the same way, a given interface will not accept routes to subnets that do not belong to the interface network.

When entering this command, you must indicate which logical interface you want to configure (existing IP address or the name of the interface in cases of unnumbered addresses). The sending and receiving of subnets outside the scope of your network will be disabled for that address.

Syntax:

```
RIP config>no allow-disconnected-subnetted-networks
  <a.b.c.d>      Interface address
    <cr>
  <interface>    Unnumbered interface
    <cr>
```

2.1.15.2 NO AUTHENTICATION

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

Syntax:

```
RIP config>no authentication
  <a.b.c.d>      Interface address
    <cr>
  <interface>    Unnumbered interface
    <cr>
```

2.1.15.3 NO DISTANCE

Use the **NO DISTANCE** command to reset the default value for the administrative distance for routes learned through RIP. This value is 100.

Syntax:

```
RIP config>no distance
```

2.1.15.4 NO DISTRIBUTE-LIST

Use the **NO DISTRIBUTE-LIST** command to disable filtering for received or sent routes. This command only affects the global filter configured through the **DISTRIBUTE-LIST** command, and not the one configured in each interface.

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

Syntax:

```
RIP config>no distribute-list ?
  in     Configures a list for input route filtering
    <cr>
  out    Configures a list for output route filtering
    <cr>
```

2.1.15.5 NO FAST-UPDATES

The **NO FAST-UPDATES** command disables the RIP “fast update” facility in the device.

Syntax:

```
RIP config>no fast-updates
```

2.1.15.6 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.

Syntax:

```
RIP config>no limit-rip
```

2.1.15.7 NO OFFSET-LIST

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

Syntax:

```
RIP config>no offset-list <access_list>
  in     Applies the access list to incoming metrics
    <0..16>    Offset to be applied to metrics
      ip-address    Ip address to which the offset list is applied
        <a.b.c.d>      Interface address
          <cr>
        <interface>    Unnumbered interface
          <cr>
      <cr>
  out    Applies the access list to outgoing  metrics
    <0..16>    Offset to be applied to metrics
      ip-address    Ip address to which the offset list is applied
        <a.b.c.d>      Interface address
          <cr>
        <interface>    Unnumbered interface
          <cr>
      <cr>
```

2.1.15.8 NO ORIGINATE-RIP-DEFAULT

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

Syntax:

```
RIP config>no originate-rip-default
```

2.1.15.9 NO REDISTRIBUTE

The **NO REDISTRIBUTE** command deletes a redistribution clause.

Syntax:

```
RIP config>no redistribute
  bgp          Border Gateway Protocol (BGP)
    route-map    Route map reference
      <word>       Route map name
    <cr>
  connected    Connected
    route-map    Route map reference
      <word>       Route map name
    <cr>
  ospf         Open Shortest Path First (OSPF)
    route-map    Route map reference
      <word>       Route map name
    <cr>
  static       Static routes
    route-map    Route map reference
      <word>       Route map name
    <cr>
  <cr>
```

2.1.15.10 NO TIMERS

The **NO TIMERS** command sets the RIP timers default values.

Syntax:

```
RIP config>no timers
```

2.1.16 OFFSET-LIST

An **OFFSET-LIST** allows 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. You may also specify a particular (logical) 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. For further information on these Access Lists, please see manual Teldat-Dm 752-I "Access Control".

The same process used for the distribute-list with the RIP_LISTS_USE_MASK patch (see Appendix A, Section 4) is adopted to compare the route IP addresses and mask with those in the access list.

Syntax:

```
RIP config>offset-list <access_list>
  in     Applies the access list to incoming metrics
    <0..16>    Offset to be applied to metrics
      ip-address    Ip address to which the offset list is applied
        <a.b.c.d>      Interface address
          <cr>
        <interface>    Unnumbered interface
          <cr>
      <cr>
  out    Applies the access list to outgoing  metrics
    <0..16>    Offset to be applied to metrics
      ip-address    Ip address to which the offset list is applied
        <a.b.c.d>      Interface address
          <cr>
```

```
        <interface>    Unnumbered interface
          <cr>
      <cr>
```

ip-address	Specifies the IP address for a particular interface. This can be an existing IP address or an interface name in cases of unnumbered addresses. 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 that coincide with the configured access list.
out <offset>	Increases the cost of the outgoing routes that coincide with the configured access list.

Example 1:

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

```
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 network 172.1.0.0 routes sent by the interface with IP address 172.24.78.131 or by the interface with IP address 10.30.1.1 (except those exclusively referring 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
;
```

2.1.17 ORIGINATE-RIP-DEFAULT

The **ORIGINATE-RIP-DEFAULT** command should be used to create a default route using RIP. Through this command, you can also configure the cost of the default route and the moment you want to generate it.

Syntax:

```
RIP config>originate-rip-default
  cost       Configure default route cost
    <1..16>    Value in the specified range
      <cr>
  always     Always originate default route
    <cr>
  if-osfp    Originate default route if osfp
    <cr>
```

cost	Cost of the default route generated by RIP.
always RIP	Always originates the default route.
if-ospf	RIP originates the default route if an OSPF route has been found.

Example:

```
RIP config>originate-rip-default cost 5
RIP config>originate-rip-default always
RIP config>
```

2.1.18 RECEIVING

Use the **RECEIVING** command to configure the RIP reception parameters for the router network interfaces. The set of selected routes activating some of the flags is then processed by a logical interface (IP address or the name of the interface in cases of unnumbered addresses). These flags control how the information received in the RIP frames is added to the routing tables of the device. By activating certain flags, the router will not take static routing information into account in cases where the RIP finds a better route than the pre-set one.

It is important to bear in mind that both the **DISTRIBUTE-LIST IN** global command and the receiving command subject the route to some filtering. Therefore, for a route to be received and added to the table, it must pass the **DISTRIBUTE** and the **RECEIVING** command filters.

Syntax:

```
RIP config>receiving
  <a.b.c.d>      Interface address
    default-routes       Process default routes
      <cr>
    distribute-list      Establish filter list
      access-list          Configures an access list
        <1..99>              Access list for routes filtering
           <cr>
      prefix-list          Configures a prefix list
         <1..199>             Prefix list for routes filtering
           <cr>
    network-routes       Process network routes
```

```
    <cr>
  subnetwork-routes    Process subnetwork routes
    <cr>
  static-routes        Process static routes
    <cr>
  no
    default-routes       Process default routes
      <cr>
    distribute-list      Establish filter list
      <cr>
    network-routes       Process network routes
      <cr>
    subnetwork-routes    Process subnetwork routes
      <cr>
    static-routes        Process static routes
      <cr>
<interface>    Unnumbered interface
  default-routes       Process default routes
    <cr>
  distribute-list      Establish filter list
    access-list          Configures an access list
      <1..99>              Access list for routes filtering
        <cr>
    prefix-list          Configures a prefix list
       <1..199>             Prefix list for routes filtering
         <cr>
  network-routes       Process network routes
    <cr>
  subnetwork-routes    Process subnetwork routes
    <cr>
  static-routes        Process static routes
    <cr>
  no
    default-routes       Process default routes
      <cr>
    distribute-list      Establish filter list
      <cr>
    network-routes       Process network routes
      <cr>
    subnetwork-routes    Process subnetwork routes
      <cr>
    static-routes        Process static routes
      <cr>
```

The meaning of each option is:

default-routes	If this option is deactivated, it anticipates that a default RIP route (received by the IP Interface address) is going to be stored as the default route. If the administrative-distance command found in the IP general configuration is enabled, this option is ignored.
distribute-list	Determines the list to be used to filter the routes received by the IP Interface address. This option is disabled by default and the routes will not be affected by this filter. In order to configure this option, you need to select a standard IP Access Control List (1 to 99) from the FEATURE ACCESS configuration menu (please see manual Teldat-Dm752-I "Access Control") or a Prefix List from the FEATURE PREFIX-LIST configuration menu (please see manual Teldat-Dm 780-I "Prefix List").
network-routes	If this is activated, network routes are accepted. If this is deactivated, no network routes will be accepted.

subnetwork-routes	If this is activated, subnet routes are accepted. If this is deactivated, no subnet routes will be accepted
static-routes	If this option is deactivated, it anticipates that RIP routes received in the interface IP address overwrite the static routes. If the administrative-distance command found in the IP general configuration is enabled, this option is ignored.

If the "Allow disconnected subnetted networks" flag is disabled for a given interface, it will only accept the subnet routes that belong to the same IP network as the interface (e.g. with a destination subnet route of 192.6.1.144 and a mask of 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. Enabling the "Allow disconnected subnetted networks" option allows for the reception of subnets via interfaces that do not belong to the subnet.

2.1.19 REDISTRIBUTE

Use the **REDISTRIBUTE** command to redistribute routes from one routing domain to another. To disable redistribution, use the word **NO** before the command.

Syntax:

```
RIP config>redistribute <protocol>
    route-map    Route map reference
      <word>       Route map name
        <cr>
    <cr>
```

The meaning of each of the options is as follows:

protocol	Source protocol for the routes going to be redistributed. This can be any of the following: bgp, connected (routes to directly connected networks), ospf, static (static routes).
route-map	(Optional) Route map examined to filter source protocol routes importation to the current protocol. If none is specified, all the routes will be redistributed.

Redistribution is disabled by default.

The following example causes the redistribution of OSPF routes in RIP.

Example 1:

```
RIP config>redistribute ospf
RIP config>
```

The following example causes the redistribution of BGP routes in RIP after being filtered by the BGP2RIP route map. Please note how the RIP routes costs are set to 5 after being imported.

Example 2:

```
feature prefix-lists
; -- Prefix Lists user configuration --
   prefix-list 1
;
      entry 1 default
      entry 1 permit
      entry 1 prefix 10.0.0.0 255.0.0.0
      entry 1 prefix ge 8
;
   exit
;
exit
;
feature route-map
; -- Route maps user configuration --
   route-map BGP2RIP
```

```
;
      entry 1 default
      entry 1 permit
      entry 1 match ip prefix-list 1
      entry 1 set metric 5
;
   exit
;
exit
;
protocol rip
   redistribute bgp route-map BGP2RIP
exit
;
```

2.1.20 SENDING

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

Syntax:

```
RIP config>sending
  <a.b.c.d>      Interface address
    bgp-routes           Process bgp routes
      <cr>
    default-routes       Process default routes
      <cr>
    direct-routes        Process direct routes
      <cr>
    distribute-list      Establish filter list
      access-list          Configures an access list
        <1..99>              Access list for routes filtering
           <cr>
      prefix-list          Configures a prefix list
         <1..199>             Prefix list for routes filtering
           <cr>    network-routes       Process network routes
      <cr>
    ospf-routes          Process ospf routes
      <cr>
    poisoned-reverse     Poisoned reverse enable/disable
      <cr>
    subnetwork-routes    Process subnetwork routes
      <cr>
    split-horizon        Split horizon enable/disable
      <cr>
    static-routes        Process static routes
      <cr>
    no
      bgp-routes           Process bgp routes
        <cr>
      default-routes       Process default routes
        <cr>
      direct-routes        Process direct routes
        <cr>
      distribute-list      Establish filter list
        <cr>
      network-routes       Process network routes
        <cr>
      ospf-routes          Process ospf routes
```

```
      <cr>
    poisoned-reverse     Poisoned reverse enable/disable
      <cr>
    subnetwork-routes    Process subnetwork routes
      <cr>
    split-horizon        Split horizon enable/disable
      <cr>
    static-routes        Process static routes
      <cr>
<interface>    Unnumbered interface
  bgp-routes           Process bgp routes
    <cr>
  default-routes       Process default routes
    <cr>
  direct-routes        Process direct routes
    <cr>
  distribute-list      Establish filter list
    access-list          Configures an access list
      <1..99>              Access list for routes filtering
        <cr>
    prefix-list          Configures a prefix list
       <1..199>             Prefix list for routes filtering
         <cr>
  network-routes       Process network routes
    <cr>
  ospf-routes          Process ospf routes
    <cr>
  poisoned-reverse     Poisoned reverse enable/disable
    <cr>
  subnetwork-routes    Process subnetwork routes
    <cr>
  split-horizon        Split horizon enable/disable
    <cr>
  static-routes        Process static routes
    <cr>
  no
    bgp-routes           Process bgp routes
      <cr>
    default-routes       Process default routes
      <cr>
    direct-routes        Process direct routes
      <cr>
    distribute-list      Establish filter list
      <cr>
    network-routes       Process network routes
      <cr>
    ospf-routes          Process ospf routes
      <cr>
    poisoned-reverse     Poisoned reverse enable/disable
      <cr>
    subnetwork-routes    Process subnetwork routes
      <cr>
    split-horizon        Split horizon enable/disable
      <cr>
    static-routes        Process static routes
      <cr>
```

The meaning of each option is:

default-routes	If this flag is activated and a default router exists, the router indicates the default route in the RIP responses to the IP address. 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 that share RIP protocol (and have RIP enabled for send or reception) will be sent. This is activated by default.
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 and the routes will not be affected by this filter. In order to configure this option, you need to select a standard IP Access Control List (1 to 99) from the FEATURE ACCESS configuration menu (please see manual Teldat-Dm752-I "Access Control") or a Prefix List from the FEATURE PREFIX-LIST configuration menu (please see manual Teldat-Dm 780-I "Prefix List").
network-routes	If this flag is activated, the router shows all the routes at the network layer in the RIP responses related to the IP address.
split-horizon	This flag is active by default. Enables or disables the *split-horizon* process: if this is enabled, it does not send notifications or updates on a route using RIP towards the network where this route was found.
poisoned-reverse	This flag is activated by default. Enable or disable the *poisoned reverse* in the *split-horizon* process. When the routes obtained from a gateway are enabled, they are broadcast with infinite metrics (16). If this mode is disabled, then these routes are not broadcast. The protocol convergence is quicker when this option 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 added 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 subnet routes belonging to the same IP network as the interface are included. For the other interfaces, the network route is included. For instance, with a destination subnet route of 192.6.1.144 and a mask of 255.255.255.248, if the outgoing interface address is 192.6.1.x, the route is send as it is. However, if the outgoing interface belongs to a different IP network (e.g. 193.5.1.x) then 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, you can also send subnets via interfaces that do not belong 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.
ospf-routes	If this flag is active, the router will include all the routes for networks learned by OSPF.
bgp-routes	If this flag is active, the router will include all the routes for networks learned by BGP.

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

Please note that, for a route to be sent through an interface, it must comply with the following requirements:

(1) It must be allowed by the filter defined through the **DISTRIBUTE-LIST OUT** global command.

(2) The **SENDING** command **network-routes** flag must not be disabled.

(3) In cases where this is a subnet route, the **SENDING** command **subnetwork-routes** flag must not be disabled.

(4) In cases where this is a default route, the **SENDING** command **default-routes** flag must not be disabled.

(5) If the route pertains to another routing protocol (directly connected, static, bgp, ospf, etc.) its redistribution must be enabled through the **REDISTRIBUTE** command or through the flag corresponding to the **SENDING** command **(direct-routes, static-routes, bgp-routes, ospf-routes)** . Please note that, for a route to be redistributed, the flag corresponding to the SENDING command must be enabled **or** the route must pass through a REDISTRIBUTE clause.

2.1.21 TIMERS

Three timers control the algorithm function (as defined in the RIP RFC). These values should only be changed under exceptional circumstances and the network manager should be fully aware of the possible consequences.

Syntax:

```
RIP config>timers ?
  <5..65535>    Periodic sending timer
    <5..65535>    Route expire timer
      <5..65535>    Route garbage timer
        <cr>
RIP config>
```

Example:

```
RIP config>timers 30 180 120
RIP config>
```

The meaning of the parameters is as follows:

Periodic sending timer	Time that elapses between the sending of periodic responses. The default value is 30 seconds.
Route expire timer	The default value is 180 seconds. If a response does not refresh the route before this time expires, it shall be deemed invalid.
Route garbage timer	The default value is 120 seconds. An invalid route is kept in the routing tables for 120 seconds, with metric value 16 (indefinite), to let all neighboring RIP routers know that it is going to be deleted.

2.1.22 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

3.1 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.
VRF	Monitoring the RIP protocol for a specific VRF.
EXIT	Exits the RIP monitoring process.

3.1.1 ? (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        Display RIP statistics
  vrf         RIP monitoring in a VPN Routing/Forwarding
  exit
RIP>
```

3.1.2 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    Routes rx    Triggered     Bad rx      Bad rx
                       errors       errors    updates tx    Authent.    SeqNum
Interface: ethernet0/0
192.7.1.253             0            0            0            0          0
Interface: serial0/0Interface: serial0/1
10.0.0.1                0            0            2            0          0
```

```
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.
Bad rx Authent.	Counts the number of packets dropped by MD5 authentication.
Bad rx SeqNum	Counts the number of packets dropped due to an erroneous sequence number.

3.1.3 VRF

Monitors the RIP protocol in a *routing/forwarding* domain in virtual private networks (VPN).

Please see the VRF manual for further details (Teldat-Dm775-I).

Syntax:

```
RIP+vrf <name_vrf>
```

Example:

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

The commands found in the following submenu, which apply to the VRF specified through <name_vrf>, are a sub-group of those found in the main RIP monitoring menu (listed in Section 1).

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

For further information on these commands, please see the help section on them under the RIP Protocol Monitoring Commands subsection.

3.1.4 EXIT

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

Syntax:

```
RIP+exit
```

Example:

```
RIP+exit
+
```

Appendix A Filtering through lists

A.1 Introduction

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

A.2 Using the lists to filter routes

To determine which routes are distributed and which ones are dropped, each route is checked against the assigned Lists, which can be Standard Access Control Lists or Prefix-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.

To determine if a list allows 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 allow said route or not.
- If none of the entries coincides with the route, then the route will not be permitted.

Matching criteria for a list depends on whether the list is Access or Prefix.

A.2.1 Matching with an Access Control List

To check the matching of a route with an entry in an access list, the announced network address is taken. This is compared with the list entry source address/mask. If the announced network address and the network address configured in the entry coincide (independently of the mask), then the route matches. If they don't coincide but the announcing network is a subnet of the one configured in the entry, then they also match.

Note

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

For example, supposing we have the following access list configured:

```
Standard Access List 1, assigned to RIP

1     DENY    SRC=192.168.128.0/24

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 192.168.128.0 (whatever the mask is), it is discarded as it coincides with the first entry on the list and this is Deny. This happens because the route address and the entry address coincide (without taking the mask into account).
- If we receive the route to network 192.168.128.128/25, it is discarded as it coincides with the first entry in the list and this is Deny. This occurs because, although the announcing network addresses and the entry are different, the first is a subnet of the second and therefore matches said entry.
- If we receive the route to network 192.168.2.0/24 it is processed. This route does not coincide with the first entry but does with the second one (it is a sub-

net of the configured network).This entry is Permit.

- If we receive the route to network 192.168.0.0 (whatever the mask), 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 (whatever the mask is), 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.

Note

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.

A.2.2 Matching with a Prefix-List

The prefix lists provide a simpler, more intuitive way of establishing filters for the routes. The matching criteria in a prefix list depend on the parameters configured in the entry:

- If only the prefix has been configured, a route will match the entry if the route address and mask *exactly match* the prefix address and mask configured in the entry.
- If the additional parameters **ge** (greater or equal) and/or **le** (less or equal) have also been configured, a route matches the entry if the *beginning of the route* matches the configured prefix (the route is a subset of the prefix) and the length of the route mask is *greater or equal* to the *ge* parameter and *less or equal* to the *le* parameter.

The following example, containing a list of prefixes, should help clarify matters:

```
Prefix List 1

 PREFIX LIST ENTRIES

1     DENY    PREFIX=192.168.128.0/24   Exact prefix match

2     PERMIT  PREFIX=192.168.0.0/16   Prefix length between 16 and 32
```

In the first entry we have only configured the *prefix* with 192.168.128.0/24. In the second entry, however, we have configured the *prefix* with 192.168.0.0/16 and the *ge* value with 16.

Similarly to the previous example, we are going to analyze the matching of certain routes with this list.

- If we receive the route to network 192.168.128.0/24, it is discarded because it *exactly* matches the prefix configured in the first entry on the list and this is Deny.
- If we receive the route to network 192.168.128.128/25, it is processed because it matches the second entry. The route is a subnet of the prefix configured in it and the mask length is within the permitted values. The second entry is Permit.
- If we receive the route to network 192.168.2.0 (with any valid mask), it is processed as it does not match the first entry but does match the second and this is Permit.
- If we receive the route to network 192.168.0.0 (with any valid mask), it is processed as it does not match the first entry but does match the second and this is Permit.
- If we receive the route to network 192.6.2.0 (with any mask), this is discarded because it doesn't match any entry on the list and the default action is Deny.
- If we receive the default route (network 0.0.0.0), it is discarded because it doesn't match any entry on the list and the default action is Deny.

Note

Similarly to what happens with Access Lists, in cases where you do not want a Prefix 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.

A.3 Example scenario

This section presents a basic user scenario for an entity accessing its branches via two Teldat routers.

Suppose we have two devices installed in the same segment, both providing access to the entity branch offices as shown in the following figure:

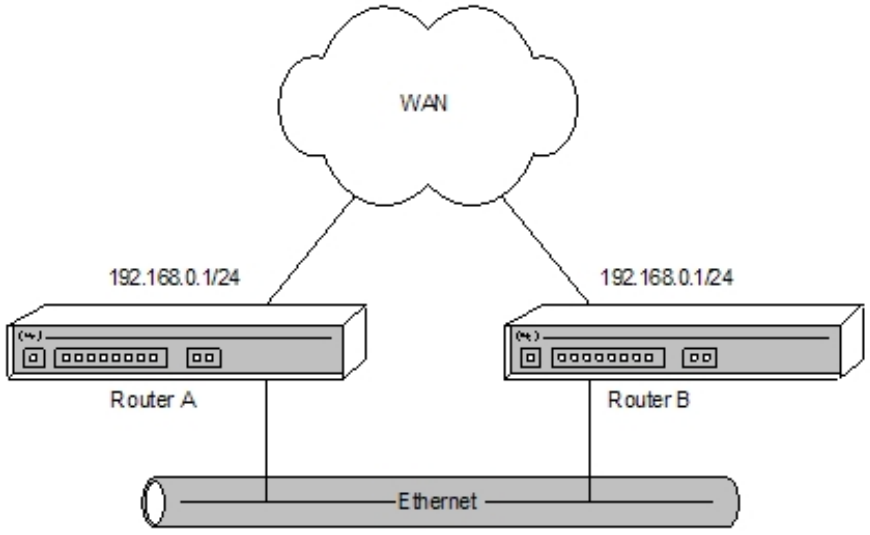

Fig. 1: **Basic user scenario**

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

Below we are going to analyze the alternatives we have to solve the problem.

A.3.1 Filtering with Prefix-List

The use of Prefix Lists in RIP **is limited to global route filtering** (through the **DISTRIBUTE-LIST** command), *and is not available* for specific filtering in interfaces. You can use prefix lists with the **REDISTRIBUTE** command through Route Maps (please see manual Teldat-Dm764-I “Route Mapping”).

To achieve our aim, we have to define the following prefix list:

```
Config>feature prefix-lists

-- Prefix Lists user configuration --
Prefix Lists config>prefix-list 1


Prefix List 1>entry 1 deny
Prefix List 1>entry 1 prefix 192.168.0.0 255.255.255.0
Prefix List 1>entry 2 permit
Prefix List 1>exit
Prefix Lists config>exit
```

And assign the prefix list to the RIP protocol to filter the routes that are going to be sent:

```
Config>protocol rip

-- RIP protocol user configuration --
RIP config>distribute-list out prefix-list 1
```

```
RIP config>exit
Config>
```

By doing this, all the routes except the one corresponding to network 192.168.0.0/24 are broadcast. If you also wish to filter all the possible subnets contained in the previous network, configure the *ge* parameter in the corresponding entry on the Prefix List:

```
Config>feature prefix-lists

-- Prefix Lists user configuration --
Prefix Lists config>prefix-list 1


Prefix List 1>entry 1 deny
Prefix List 1>entry 1 prefix ge 24
Prefix List 1>exit
Prefix Lists config>exit
Config>
```

This way, all subnets corresponding to 192.168.0.x with mask length between 24 and 32 bits are denied.

There are, however, several points worth mentioning:

- We have had to add the second entry on the list (Permit without further parameters) because the default action for this list (when there is no match with any entry) is Deny. In this way all routes that do not match the first entry are Permitted.
- In short, thanks to the second entry, all default routes are broadcast.

A.3.2 Filtering with Access Control List

The use of Access Control Lists in RIP is possible for all types of filtering, both global and specific, in interfaces.

In order to do this, simply define the following access list:

```
Config>feature access-list

-- 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 access-list 1
RIP config>exit
Config>
```

This way, all routes except those belonging to network 192.168.0.0 (whatever the mask is, provided it's valid) 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 allowed.
- The list therefore allows for the distribution of the default routes thanks to the second entry.
- The first entry, unlike the example where we used prefix lists, **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, and the entry checking does not take the masks into account. This effect is dealt with and resolved in the next chapter.

A.4 Filtering of routes with mask using Access Control Lists

Sometimes, it may be necessary to use both the IP address and the route mask propagated by RIP when filtering through access lists.

Let's go back to the example scenario where we created a list to prevent network 192.168.0.0/24 from 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 to network 192.168.0.0/24 will be discarded
- Routes to network 192.168.0.0/16 will not be discarded
- Routes to network 192.168.0.0/32 will be discarded

Activating the *patch* produces similar results to using a *prefix list*, as seen in an example in the previous chapter.

To enable the *patch*, use the **ENABLE PATCH** configuration command and assign value **1** to option **RIP_LISTS_USE_MASK**.

Example:

```
Config>enable patch rip_lists_use_mask 1
Config>
```

To disable the *patch*, use the **DISABLE PATCH** configuration command with option **RIP_LISTS_USE_MASK**.

Example:

```
Config>disable patch rip_lists_use_mask
Config>
```

This patch only affects the behavior of the Access Lists and does not have any affect whatsoever on the Prefix Lists.

A.5 Filtering the default route using Access Control Lists

It's possible to filter the default route through access lists, both to permit it and to deny it. However, the configuration varies depending on whether 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
```

Appendix B Personalized Parameters

B.1 Supported personalized parameters

The Teldat devices have personalized parameters that modify the behavior of the device *under certain special circumstances* (personalized versions). For further information on the activation, deactivation and listing of these parameters, please see the help command in the **enable, patch, disable patch** and **list patch** commands respectively. These can be found in manual Teldat-Dm704-I Configuration and Monitoring, Chapter 2.

The RIP protocol in the Teldat router has the following personalized parameters:

RIP_NO_TTL_1

This patch allows RIP packets originating in the device to have a TTL different to 1. This functionality is useful when the RIP packet is destined for a device that is reached using more than one hop and there are intermediate nodes that decrease the TTL.

Value: 0	Normal operation (the RIP sends the broadcast/multicast packets with TTL set to 1).
Value: x	The RIP sends the broadcast/multicast packets with TTL set to default (60).

RIP_LISTS_USE_MASK

Further details on this patch are given in Appendix A.