Chapter 23

Summary of RIP Configuration Statements

The following sections explain each of the individual statements in the [edit protocols rip] hierarchy. The statements are organized alphabetically.

authentication-key

Syntax authentication-key *password*;

Hierarchy Level [edit protocols rip],
[edit protocols rip group *group-name* neighbor *neighbor-name*]

Description Require authentication for RIP route queries received on an interface.

Options *password*—Authentication password. If the password does not match, the packet is rejected. The password can be 1 through 16 contiguous characters long and can include any ASCII strings.

Usage Guidelines See “Configure Authentication” on page 261.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

See Also authentication-type on page 268

authentication-type

Syntax authentication-type *type*;

Hierarchy Level [edit protocols rip],
[edit protocols rip group *group-name* neighbor *neighbor-name*]

Description Configure the type of authentication for RIP route queries received on an interface.

Default If you do not include this statement and the authentication-key statement, RIP authentication is disabled.

Options *type*—Authentication type:

md5—Use the MD5 algorithm to create an encoded checksum of the packet. The encoded checksum is included in the transmitted packet. The receiving router uses the authentication key to verify the packet, discarding it if the digest does not match. This algorithm provides a more secure authentication scheme.

none—Disable authentication. If none is configured, the configured authentication key is ignored.

simple—Use a simple password. The password is included in the transmitted packet, which makes this method of authentication relatively insecure. The password can be 1 to 16 contiguous letters or digits long.

Default—none (No authentication is performed.)

Usage Guidelines See "Configure Authentication" on page 261.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

See Also authentication-key on page 267

check-zero

Syntax (check-zero | no-check-zero);

Hierarchy Level [edit protocols rip],
[edit protocols rip group *group-name* neighbor *neighbor-name*]

Description Check whether the reserved fields in a RIP packet are zero:

check-zero—Discard Version 1 packets that have nonzero values in the reserved fields and Version 2 packets that have nonzero values in the fields that must be zero. This default behavior implements the RIP Version 1 and Version 2 specifications.

no-check-zero—Receive RIP Version 1 packets with nonzero values in the reserved fields or RIP Version 2 packets with nonzero values in the fields that must be zero in spite of the fact that they are being sent in violation of the specifications in RFC 1058 and RFC 2453.

Default: check-zero

Usage Guidelines See “Accept Packets Whose Reserved Fields Are Nonzero” on page 262.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

export

Syntax export [*policy-names*];

Hierarchy Level [edit protocols rip group *group-name*]

Description Apply a policy to routes being exported to the neighbors.

Options *policy-names*—Name of one or more policies.

Usage Guidelines See “Apply Export Policy” on page 264 and “Configure Routing Policy” on page 35.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

See Also import on page 270

group

Syntax

```
group group-name {
    preference number;
    metric-out metric;
    export policy;
    neighbor neighbor-name {
        authentication-key password;
        authentication-type type;
        (check-zero | no-check-zero);
        import policy-name;
        message-size number;
        metric-in metric;
        receive receive-options;
        send send-options;
    }
}
```

Hierarchy Level [edit protocols rip]

Description Configure a set of RIP neighbors that share an export policy and metric. The export policy and metric govern what routes to advertise to neighbors in a given group.

Options *group-name*—Name of the group.

The remaining statements are explained separately.

Usage Guidelines See “Configure Group-Specific Properties” on page 263.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

import

Syntax import [*policy-names*];

Hierarchy Level [edit protocols rip],
[edit protocols rip group *group-name* neighbor *neighbor-name*]

Description Apply one or more policies to routes being imported into the local router from the neighbors.

Options *policy-names*—Name of one or more policies.

Usage Guidelines See “Apply Import Policy” on page 263 and “Configure Routing Policy” on page 35.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

See Also export on page 269

message-size

Syntax message-size *number*;

Hierarchy Level [edit protocols rip],
[edit protocols rip group *group-name* neighbor *neighbor-name*]

Description Number of route entries to be included in every RIP update message. To ensure interoperability with other vendors' equipment, use the standard of 25 route entries per message.

Options *number*—Number of route entries per update message.
Range: 25 through 255
Default: 25 entries

Usage Guidelines See "Configure the Number of Route Entries in an Update Message" on page 262.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

metric-in

Syntax metric-in *metric*;

Hierarchy Level [edit protocols rip],
[edit protocols rip group *group-name* neighbor *neighbor-name*]

Description Metric to add to incoming routes when advertising into RIP routes that were learned from other protocols. Use this statement to configure the router to prefer RIP routes learned through a specific neighbor.

Options *metric*—Metric value.
Range: 1 through 16
Default: 1

Usage Guidelines See "Modify the Incoming Metric" on page 262.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

metric-out

Syntax metric-out *metric*;

Hierarchy Level [edit protocols rip group *group-name* neighbor *neighbor-name*]

Description Metric value to add to routes transmitted to the neighbor. Use this statement to control how other routers prefer RIP routes sent from this neighbor.

Options *metric*—Metric value.
Range: 1 through 16
Default: 1

Usage Guidelines See "Modify the Outgoing Metric" on page 265.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

neighbor

Syntax
```
neighbor neighbor-name {
    authentication-key password;
    authentication-type type;
    (check-zero | no-check-zero;
    import policy-name;
    message-size number;
    metric-in metric;
    receive receive-options;
    send send-options;
}
```

Hierarchy Level [edit protocols rip group *group-name*]

Description Configure neighbor-specific RIP parameters, thereby overriding the defaults set for the router.

Options *neighbor-name*—Name of an interface.

The remaining statements are explained separately.

Usage Guidelines See "Define RIP Neighbor Properties" on page 261.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

no-check-zero

See check-zero on page 269

preference

Syntax preference *preference*;

Hierarchy Level [edit protocols rip group *group-name*]

Description Preference of external routes learned by RIP as compared to those learned from other routing protocols.

Options *preference*—Preference value. A lower value indicates a more-preferred route.
Range: 0 through 255
Default: 100

Usage Guidelines See "Control Route Preference" on page 264.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

receive

Syntax receive *receive-options*;

Hierarchy Level [edit protocols rip],
[edit protocols rip group *group-name* neighbor *neighbor-name*]

Description Configure RIP receive options.

Options *receive-options*—One of the following:

both—Accept both RIP Version 1 and Version 2 packets.

none—Do not receive RIP packets.

version-1—Accept only RIP Version 1 packets.

version-2—Accept only RIP Version 2 packets.

Default: both

Usage Guidelines See "Configure Update Messages" on page 263.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

See Also send on page 274

rip

Syntax rip {...}

Hierarchy Level [edit protocols]

Description Enable RIP routing on the router.

Default RIP is disabled on the router.

Usage Guidelines See “Minimum RIP Configuration” on page 260.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

send

Syntax send *send-options*;

Hierarchy Level [edit protocols rip]
[edit protocols rip group *group-name* neighbor *neighbor-name*]

Description Configure RIP send options.

Options *send-options*—One of the following:

broadcast—Broadcast RIP Version 2 packets (RIP Version 1 compatible). This is the default.

multicast—Multicast RIP Version 2 packets

none—Do not send RIP updates

version-1—Broadcast RIP Version 1 packets

Default: multicast

Usage Guidelines See “Configure Update Messages” on page 263.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

See Also receive on page 273

traceoptions

Syntax

```
traceoptions {
    file name <replace> <size size> <files number> <no-stamp>
        <(world-readable | no-world-readable)>;
    flag flag <flag-modifier> <disable>;
}
```

Hierarchy Level [edit protocols rip]

Description RIP protocol-level tracing options.

Default The default RIP protocol-level trace options are those inherited from the global traceoptions statement.

Options disable—(Optional) Disable the tracing operation. One use of this option is to disable a single operation when you have defined a broad group of tracing operations, such as all.

file-name—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks. We recommend that you place RIP tracing output in the file /var/log/rip-log.

files *number*—(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed *trace-file*.0, then *trace-file*.1, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

If you specify a maximum number of files, you must also specify a maximum file size with the size option.

Range: 2 through 1000 files
Default: 1 trace file only

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. These are the RIP–specific tracing options:

auth—RIP authentication

error—RIP errors

expiration—RIP route expiration processing

holddown—RIP holddown processing

packets—All RIP packets

request—RIP information packets such as request, poll, and poll entry packets

trigger—RIP triggered updates

update—RIP update packets

The following are the global tracing options:

all—All tracing operations

general—A combination of the normal and route trace operations

normal—All normal operations.
Default: If you do not specify this option, only unusual or abnormal operations are traced.

policy—Policy operations and actions

route—Routing table changes

state—State transitions

task—Interface transactions and processing

timer—Timer usage

flag-modifier—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:

detail—Provide detailed trace information

receive—Packets being received

receive-detail—Provide detailed trace information for packets being received

send—Packets being transmitted

send-detail—Provide detailed trace information for packets being transmitted

no-stamp—(Optional) Do not place timestamp information at the beginning of each line in the trace file.
Default: If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

no-world-readable—(Optional) Disallow any user to read the log file.

replace—(Optional) Replace an existing trace file if there is one.
Default: If you do not include this option, tracing output is appended to an existing trace file.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB) or megabytes (MB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file*.0. When the *trace-file* again reaches its maximum size, *trace-file*.0 is renamed *trace-file*.1 and *trace-file* is renamed *trace-file*.0. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

If you specify a maximum file size, you must also specify a maximum number of trace files with the files option.

Syntax: *x*k to specify KB, *x*m to specify MB, or *x*g to specify GB
Range: 10 KB through the maximum file size supported on your system
Default: 1 MB

world-readable—(Optional) Allow any user to read the log file.

Usage Guidelines See "Trace RIP Protocol Traffic" on page 265.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.