RIP-2 FOR NOS

INTRODUCTION

This document covers the implementation of RIP-2 (RFC 1388) in NOS. Specifically the WG7J version of NOS. RIP-2 is an enhanced version of the RIP protocol (RFC 1058). RIP and RIP-2 are an interior gateway protocol (IGP). RIP-2 for NOS was implemented by Jeff White, N0POY.

This documentation is for the beta release V0.9

FEATURES

The NOS implementation implements all features of the normal RIP protocol (RFC 1058) and all features of the RIP-2 protocol (RFC 1388) except multicasting (which NOS does not currently implement) and Route Tags (NOS does not implement any EGPs). Features include:

- Routing Domains
- Authentication
- Proxy routing
- Filtering of naughty nodes
- Optional refusal of a default route
- Enhanced logging and tracing
- Route subnet masks correctly maintained
- Optional refusal to accept older RIP version broadcasts
- Mixing of RIP-1 and RIP-2 support

NOS RIP COMMANDS

RIP ACCEPT <GATEWAY>

The RIP ACCEPT command resumes the acceptance of RIP broadcasts from a specific node given in the <GATEWAY> field. Ex: RIP ACCEPT 192.55.248.1 or RIP ACCEPT skeggi.tcman.ampr.org

RIP ADD <DEST> <INTERVAL> [<FLAGS>] [<RIPVER>] [AUTH <PASSWORD>] [RD <ROUTING DOMAIN>]

The RIP ADD command adds a node to the list of stations that are to be broadcast to with the local nodes routing table. <DEST> is the destination node, usually a broadcast address. <INTERVAL> is the number of seconds between broadcasts. <FLAGS> are the RIP flags used (see below for the flags), it is a hexadecimal number. <RIPVER> is the version of the RIP broadcasts. This may be a 1 or 2. The AUTH identifier preceeds the authentication password to be included with the RIP broadcasts to this destination. The RD identifier preceeds the routing domain number. This number must range from 0 to 65535. The authentication fields and routing domain fields are only valid with RIP-2 broadcasts. The password must be 16 characters or less. Printable ASCII characters are recommended, but not required.

RIP FLAGS

- 0x01 Do split horizon processing
- 0x02 Include ourselves in the routing broadcast
- 0x04 Broadcast RIP packets (default type)
- 0x08 Multicast RIP packets (not implemented) (RIP-2)
- 0x10 Poisoned Reverse on
- 0x20 Authentication data to be included in broadcast (RIP-2)

Recommend flags are Split Horizon, and Poisoned Reverse or 0x11. Authentication and routing domain data entered here only applies to the outgoing RIP broadcasts. See RIP AUTHADD and RIP AUTHDROP for entering acceptable passwords and routing domains.

Example: RIP ADD SKEGGI.TCMAN.AMPR.ORG 30 0x31 2 AUTH frodo RD 2

RIP ADD BIGGUS.TCMAN.AMPR.ORG 300 0x11 1

RIP PROXY <SRC> <DEST> <INTERVAL> [<FLAGS>] [AUTH <PASSWORD>] [RD <ROUTING DOMAIN>]

The RIP PROXY command adds a node to the list of stations that are to be broadcast to with the local nodes routing table. <SRC> is the node that the broadcast will "point" to. <DEST> is the destination node, usually a broadcast address. <INTERVAL> is the number of seconds between broadcasts. <FLAGS> are the RIP flags used (see below for the flags), it is a hexadecimal number. The AUTH identifier preceeds the authentication password to be included with the RIP broadcasts to this destination. The RD identifier preceeds the routing domain number. This number must range from 0 to 65535. The authentication fields and routing domain fields are only valid with RIP-2 broadcasts. The password must be 16 characters or less. Printable ASCII characters are recommended, but not required.

RIP FLAGS

- 0x01 Do split horizon processing
- 0x02 Include ourselves in the routing broadcast
- 0x04 Broadcast RIP packets (default type)
- 0x08 Multicast RIP packets (not implemented) (RIP-2)
- 0x10 Poisoned Reverse on
- 0x20 Authentication data to be included in broadcast (RIP-2)

Recommend flags are Split Horizon, and Poisoned Reverse or 0x11. Authentication and routing domain data entered here only applies to the outgoing RIP broadcasts. See RIP AUTHADD and RIP AUTHDROP for entering acceptable passwords and routing domains.

Proxy RIP is tricky, complex and not needed for normal use. Do NOT use proxy rip unless you understand what you are doing. Proxy RIP's primary use would be to advertise routes to another machine that is aquiring routing information via another routing protocol. See RFC 1388 for further details.

RIP DROP <DEST> [<DOMAIN>]

RIP DROP removes a routing broadcast entry. If a RIP-2 broadcast was entered, the correct routing domain needs to be entered, since it is possible to broadcast multiple routing domains to the same address.

Example: RIP DROP SKEGGI.TCMAN.AMPR.ORG 2

RIP AUTHADD <INTERFACE> <ROUTING DOMAIN> [<PASSWORD>]

RIP AUTHADD adds an acceptable routing domain and optionally a password to a specific interface.

Example: RIP AUTHADD ax0 2 frodo

RIP AUTHADD en0 3

RIP AUTHDROP <INTERFACE> <ROUTING DOMAIN>

RIP AUTHDROP removes an acceptable routing domain (and password if any) from a specific interface.

Example: RIP AUTHDROP ax0 2

RIP REJECT <VERSION>

RIP REJECT is used to ignore older RIP broadcasts, as they may cause undesirable routing table alterations. The version number is the version number and below that are ignored. RIP version 0 (XNS RIP) is always ignored. The default is 0. To ignore RIP-1 broadcasts: RIP REJECT 1 would do the job.

RIP FILTER <ON|OFF>

RIP FILTER will cause advertisements to the default route (0.0.0.0) to be tossed and ignored. By default this is off. This can serve as a LID filter. Default routes should NOT be advertised, unless there is a specific reason (ie this machine is a gateway to the rest of the Internet).

RIP MERGE <ON|OFF>

RIP MERGE will cause overlapping routing entries to be merged into one routing entry. For example N0BEL.TCMAN.AMPR.ORG is a route to 192.133.30.0/28, and 192.133.30.16/28, with merging on this would become a single entry of 192.133.30.0/27.

RIP REFUSE <GATEWAY>

RIP REFUSE will reject all RIP broadcasts from the GATEWAY station. RIP ACCEPT is the opposite. By default all stations are accepted.

RIP REQUEST <GATEWAY>

RIP REQUEST asks the gateway station to send a routing table now, rather than waiting for periodic updates.

RIP STATUS

RIP STATUS will display various statistics for RIP-1 and RIP-2, RIP broadcasts, RIP refusals, and acceptable Interface, Domain and Password combinations. It also displays the refusing version level. The DEFAULT interface is for every interface. Thus unless removed, and RIP-2 broadcast with a domain of 0 does not require a password and will be accepted.

RIP TRACE <LEVEL> [<FILE>]

RIP TRACE will begin tracing RIP operations. The higher the level, the more detailed the logging. Level 9 is the useful maximum, with level 0 (the default) being no logging. If a file is specified, logging will go to that file, else logging appears on the console.

RIP TTL <TIME-TO-LIVE>

RIP TTL sets the time-to-live before RIP entries expire from the routing tables. The default should work for almost all cases.