VYATTA, INC. | Vyatta System

RIP

Reference Guide

Vyatta
Suite 200
1301 Shoreway Road
Belmont, CA 94002
vyatta.com
650 413 7200
1 888 VYATTA 1 (US and Canada)

COPYRIGHT

Copyright © 2005–2009 Vyatta, Inc. All rights reserved.

Vyatta reserves the right to make changes to software, hardware, and documentation without notice. For the most recent version of documentation, visit the Vyatta web site at vyatta.com.

PROPRIETARY NOTICES

Vyatta is a registered trademark of Vyatta, Inc.

VMware, VMware ESX, and VMware server are trademarks of VMware, Inc.

All other trademarks are the property of their respective owners.

ISSUE DATE: February 2009

DOCUMENT REVISION. VC5 v03

RELEASED WITH: VC5.0.2

PART NO. A0-0118-10-0002

Table of Contents

Quick Reference to Commands

Use this section to help you quickly locate a command.

Quick List of Examples

Use this list to help you locate examples you'd like to try or look at.

Preface

This guide describes commands for the Routing Information Protocol (RIP) on the Vyatta system.

This preface provides information about using this guide. The following topics are covered:

- Intended Audience
- Organization of This Guide
- Document Conventions
- Vyatta Publications

Intended Audience

This guide is intended for experienced system and network administrators. Depending on the functionality to be used, readers should have specific knowledge in the following areas:

- Networking and data communications
- TCP/IP protocols
- General router configuration
- Routing protocols
- Network administration
- Network security

Organization of This Guide

This guide has the following aid to help you find the information you are looking for:

- **Quick Reference to Commands**

  Use this section to help you quickly locate a command.

- **Quick List of Examples**

  Use this list to help you locate examples you'd like to try or look at.

This guide has the following chapters:

Chapter	Description	Page
Chapter 1: Router-Level Configuration	This chapter describes commands for configuring RIP at the router level.	1
Chapter 2: Route Redistribution	This chapter describes commands for redistributing routes from other routing protocols into RIP.	24
Chapter 3: Route Filtering	This chapter describes commands for RIP route filtering.	36
Chapter 4: RIP on Ethernet Interfaces and Vifs	This chapter describes commands for deploying RIP on Ethernet interfaces and Ethernet vifs, including Ethernet interfaces with PPPoE encapsulation.	46
Chapter 5: RIP on the Loopback Interface	This chapter describes commands for deploying RIP on the loopback interface.	66

Document Conventions

This guide contains advisory paragraphs and uses typographic conventions.

Advisory Paragraphs

This guide uses the following advisory paragraphs:

Warnings alert you to situations that may pose a threat to personal safety, as in the following example:

WARNING *Risk of injury. Switch off power at the main breaker before attempting to connect the remote cable to the service power at the utility box.*

Cautions alert you to situations that might cause harm to your system or damage to equipment, or that may affect service, as in the following example:

CAUTION *Risk of loss of service. Restarting a running system will interrupt service.*

Notes provide information you might need to avoid problems or configuration errors:

NOTE *You must create and configure network interfaces before enabling them for routing protocols.*

Typographic Conventions

This document uses the following typographic conventions:

`Courier`	Examples, command-line output, and representations of configuration nodes.
`boldface Courier`	In an example, your input: something you type at a command line.
boldface	In-line commands, keywords, and file names .
italics	Arguments and variables, where you supply a value.
<key>	A key on your keyboard. Combinations of keys are joined by plus signs (“+”). An example is <Ctrl>+<Alt>+<Del>.
[*arg1* | *arg2*]	Enumerated options for completing a syntax. An example is [enable | disable].
num1–numN	A inclusive range of numbers. An example is 1–65535, which means 1 through 65535.
arg1..argN	A range of enumerated values. An example is eth0..eth3, which means eth0, eth1, eth2, and eth3.
arg [*arg* ...] *arg*,[*arg*,...]	A value that can optionally represent a list of elements (a space-separated list in the first case, and a comma-separated list in the second case).

Vyatta Publications

More information about the Vyatta system is available in the Vyatta technical library, and on www.vyatta.com and www.vyatta.org.

Full product documentation is provided in the Vyatta technical library. To see what documentation is available for your release, see the *Vyatta Documentation Map*. This guide is posted with every release of Vyatta software and provides a great starting point for finding what you need.

Chapter 1: Router-Level Configuration

This chapter describes commands for configuring RIP at the router level.

This chapter presents the following topics:

- Router-Level Configuration Commands

Router-Level Configuration Commands

This chapter contains the following commands.

Configuration Commands	
protocols rip default-distance <distance>	Sets the administrative distance for RIP.
protocols rip default-information originate	Generates a default route into a RIP routing domain.
protocols rip default-metric <metric>	Sets the default metric for external routes redistributed into RIP.
protocols rip interface <ethx>	Enables the Routing Information Protocol (RIP) for an interface.
protocols rip neighbor <ipv4>	Defines a RIP neighbor router.
protocols rip network <ipv4net>	Specifies a network for the Routing Information Protocol (RIP).
protocols rip network-distance <ipv4net>	Specifies the administrative distance for a RIP network.
protocols rip passive-interface <ethx>	Suppresses RIP routing updates on an interface.
protocols rip route <ipv4net>	Specifies a RIP static route.
protocols rip timers garbage-collection <seconds>	Allows you to set timers for RIP garbage collection.
protocols rip timers timeout <seconds>	Allows you to set the interval for RIP time-outs.
protocols rip timers update <seconds>	Allows you to set the timer for RIP routing table updates.
Operational Commands	
debug rip events	Enables or disables debug message generation related to RIP events.
debug rip packet	Enables or disables debug message generation related to all RIP packet types.
debug rip zebra	Enables or disables debug message generation for the Zebra RIP process.
show debugging rip	Displays RIP protocol debugging flags.
show ip route rip	Displays all IP RIP routes.
show ip rip	Displays information for the Routing Information Protocol (RIP).

debug rip events

Enables or disables debug message generation related to RIP events.

Syntax

debug rip events

no debug rip events

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to enable generation of trace-level messages related to Routing Information Protocol (RIP) events.

Use the **no** form of this command to disable debugging of RIP events.

debug rip packet

Enables or disables debug message generation related to all RIP packet types.

Syntax

debug rip packet [**recv** [**detail**] | **send** [**detail**]]

no debug rip packet [**recv** | **send**]

Command Mode

Operational mode.

Parameters

recv	Optional. Provides debugging on all received packets.
recv detail	Optional. Provides detailed debugging on all received packets.
send	Optional. Provides debugging on all sent packets.
send detail	Optional. Provides detailed debugging on all sent packets.

Default

None.

Usage Guidelines

Use this command to enable generation of trace-level messages related to all Routing Information Protocol (RIP) packet types.

Use the **no** form of this command to disable debugging of all RIP packet types.

debug rip zebra

Enables or disables debug message generation for the Zebra RIP process.

Syntax

debug rip zebra

no debug rip zebra

Command Mode

Operational mode.

Parameters

None.

Default

Debug messages are generated for actions related to the Zebra RIP process.

Usage Guidelines

Use this command to enable generation of trace-level messages related to the Zebra Routing Information Protocol (RIP) process.

Use the **no** form of this command to disable debugging for the Zebra RIP process.

protocols rip default-distance <distance>

Sets the administrative distance for RIP.

Syntax

set protocols rip default-distance *distance*

delete protocols rip default-distance

show protocols rip default-distance

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      default-distance 1-255
   }
}
```

Parameters

distance	Mandatory. Sets the default administrative distance for RIP. The range is 1-255. The default is 120.

Default

The default administrative distance for RIP is 120.

Usage Guidelines

Use the **set** form of this command to set the default administrative distance for RIP.

Use the **delete** form of this command to restore the default administrative distance for RIP.

Use the **show** form of this command to display the administrative distance for RIP.

protocols rip default-information originate

Generates a default route into a RIP routing domain.

Syntax

set protocols rip default-information originate

delete protocols rip default-information originate

show protocols rip default-information originate

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      default-information {
         originate
      }
   }
}
```

Parameters

None.

Default

By default, the system does not generate an external default route into the OSPF routing domain.

Usage Guidelines

Use the **set** form of this command to generate a default route into the RIP routing domain.

Use the **delete** form of this command to restore the default behavior for default route generation into RIP.

Use the **show** form of this command to display default route generation configuration.

protocols rip default-metric <metric>

Sets the default metric for external routes redistributed into RIP.

Syntax

set protocols rip default-metric *metric*

delete protocols rip default-metric

show protocols rip default-metric

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
    rip {
        default-metric 1-16
    }
}
```

Parameters

metric	Mandatory. The metric that will be assigned to external routes imported into RIP for redistribution. The range is 1-16. The default is 1.

Default

Routes being imported into RIP are assigned a metric of 1.

Usage Guidelines

Use the **set** form of this command to set the metric for routes being redistributed into RIP.

Use the **delete** form of this command to restore the default RIP metric to default values.

Use the **show** form of this command to display the default metric for routes being redistributed into RIP.

protocols rip interface <ethx>

Enables the Routing Information Protocol (RIP) for an interface.

Syntax

set protocols rip interface *ethx*

delete protocols rip interface *ethx*

show protocols rip interface *ethx*

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      interface: eth0..eth23
   }
}
```

Parameters

ethx	Mandatory. Multi-node. The name of a configured Ethernet interface. You can enable RIP on more than one interface by creating multiple **protocols rip interface** configuration nodes.

Default

None.

Usage Guidelines

Split-horizon is a stability feature that reduces the possibility of network loops, particularly in the case where links become disconnected and is enabled by default. Split-horizon stops an interface from including in its network updates any routes that it learned from that interface. Split horizon is effective at preventing loops between routers that are directly connected to one another, and speeds convergence when network conditions change.

Use the **set** form of this command to enable RIP on an interface. The interface must be enabled for RIP before you can use it for RIP routing.

Use the **delete** form of this command to disable RIP on an interface.

Use the **show** form of this command to display RIP interface configuration.

protocols rip neighbor <ipv4>

Defines a RIP neighbor router.

Syntax

set protocols rip neighbor *ipv4*

delete protocols rip neighbor *ipv4*

show protocols rip neighbor

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      neighbor: ipv4
   }
}
```

Parameters

ipv4	Mandatory. Multi-node. The IP address of the neighbor router. You can define more than one RIP neighbor router by creating multiple **protocols rip neighbor** configuration nodes.

Default

None.

Usage Guidelines

Use the **set** form of this command to define a RIP neighbor router.

Use the **delete** form of this command to remove a neighbor router.

Use the **show** form of this command to display RIP neighbor configuration.

protocols rip network <ipv4net>

Specifies a network for the Routing Information Protocol (RIP).

Syntax

set protocols rip network *ipv4net*

delete protocols rip network *ipv4net*

show protocols rip network

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      network: ipv4net
   }
}
```

Parameters

ipv4net	Mandatory. Multi-node. The IP network address of the RIP network. You can identify more than one RIP network by creating multiple **protocols rip network** configuration nodes.

Default

None.

Usage Guidelines

Use the **set** form of this command to specify a RIP network.

Use the **delete** form of this command to remove a RIP network.

Use the **show** form of this command to display RIP network configuration.

protocols rip network-distance <ipv4net>

Specifies the administrative distance for a RIP network.

Syntax

set protocols rip network-distance *ipv4net* {**access-list** *list-name* | **distance** *distance*}

delete protocols rip network-distance *ipv4net* [**access-list** *list-name* | **distance** *distance*]

show protocols rip network-distance *ipv4net* [**access-list** | **distance**]

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      network-distance ipv4net {
         access-list: text
         distance: 1-255
   }
}
```

Parameters

ipv4net	Mandatory. The IP network address identifying the network.
access-list	Applies a defined access to the specified network.
distance	Applies the specified administrative distance to the specified network. The range is 1 to 255. The default is 120.

Default

None.

Usage Guidelines

Use the **set** form of this command to set the default administrative distance for a RIP network or apply an access list to a RIP network.

The administrative distance indicates the trustworthiness of a router or group of routers as a source of routing information. In general, the higher the value, the less trusted the entity. An administrative distance of 1 usually represents a directly connected network, and and an administrative distance of 255 the routing source is unreliable or unknown. The administrative distance conventionally applied to RIP is 120.

Use the **delete** form of this command to restore the default administrative distance to a RIP network or remove an access list.

Use the **show** form of this command to display administrative distance of a RIP network or access list application.

protocols rip passive-interface <ethx>

Suppresses RIP routing updates on an interface.

Syntax

set protocols rip passive-interface *ethx*

delete protocols rip passive-interface *ethx*

show protocols rip passive-interface

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      passive-interface: eth0..eth23
   }
}
```

Parameters

eth0..eth23	Mandatory. Multi-node. The name of a configured Ethernet interface on which to suppress RIP routing updates. You can suppress routing updates on more than one RIP interface by creating multiple **protocols rip passive-interface** configuration nodes.

Default

RIP routing updates are not suppressed.

Usage Guidelines

Use the **set** form of this command to suppress RIP routing updates on an interface

Use the **delete** form of this command to disable RIP routing update suppression on an interface.

Use the **show** form of this command to display RIP route suppression configuration for an interface.

protocols rip route <ipv4net>

Specifies a RIP static route.

Syntax

set protocols rip route *ipv4net*

delete protocols rip route *ipv4net*

show protocols rip route

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      route ipv4net
   }
}
```

Parameters

ipv4net	Mandatory. The network address defining the RIP static route.

Default

None.

Usage Guidelines

Use the **set** form of this command to define a RIP static route.

Use the **delete** form of this command to remove a RIP static route.

Use the **show** form of this command to display RIP static route configuration.

protocols rip timers garbage-collection <seconds>

Allows you to set timers for RIP garbage collection.

Syntax

set protocols rip timers garbage-collection *seconds*

delete protocols rip timers garbage-collection [*seconds*]

show protocols rip timers garbage-collection

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
    rip {
        timers {
            garbage-collection: 5-2147483647
        }
    }
}
```

Parameters

seconds	Mandatory. The timer interval period in seconds. The range is 5 to 2147483647.

Default

The default is 120.

Usage Guidelines

Use the **set** form of this command to set the garbage collection timer. When the timer expires, the system will scan for stale RIP resources and release them for use.

Use the **delete** form of this command to restore the default value for the RIP garbage collection timer.

Use the **show** form of this command to display RIP garbage collection timer configuration.

protocols rip timers timeout <seconds>

Allows you to set the interval for RIP time-outs.

Syntax

set protocols rip timers timeout *seconds*

delete protocols rip timers timeout [*seconds*]

show protocols rip timers timeout

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      timers {
         timeout: 5-2147483647
      }
   }
}
```

Parameters

seconds	Mandatory. The RIP timeout interval, in seconds. The range is 5 to 2147483647. The default is 180.

Default

RIP time-outs occur at 180 second.

Usage Guidelines

Use the **set** form of this command to set the value for RIP time-outs.

Use the **delete** form of this command to restore the RIP timeout interval to the default value.

Use the **show** form of this command to display RIP timeout configuration.

protocols rip timers update <seconds>

Allows you to set the timer for RIP routing table updates.

Syntax

set protocols rip timers update *seconds*

delete protocols rip timers update [*seconds*]

show protocols rip timers update

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      timers {
         update: 5-2147483647
      }
   }
}
```

Parameters

seconds	Mandatory. The interval at which RIP routing table updates will occur. The range is 5 is 2147483647. The default is 30.

Default

The RIP routing table is updated every 30 seconds.

Usage Guidelines

Use the **set** form of this command to set the interval between RIP routing table updates. The shorter this interval, the more accurate the routing information in the tables; however, the more protocol network traffic occurs.

Use the **delete** form of this command to restore the RIP update timer to the default value.

Use the **show** form of this command to display the RIP update time configuration.

show debugging rip

Displays RIP protocol debugging flags.

Syntax

show debug rip

Command Mode

Operational mode.

Parameters

None

Default

None.

Usage Guidelines

Use this command to see how debugging is set for RIP.

show ip route rip

Displays all IP RIP routes.

Syntax

show ip route rip

Command Mode

Operational mode.

Parameters

None.

Default

None.

Usage Guidelines

Use this command to display RIP routes contained in the Routing Information Base (RIB).

Examples

Example 1-1 shows all RIP routes from the RIB.

Example 1-1 "show ip route rip": Displaying routes

```
vyatta@vyatta:~$  show ip route rip
Codes: K - kernel route, C - connected, S - static, R - RIP, O -
OSPF,
       I - ISIS, B - BGP, > - selected route, * - FIB route
vyatta@vyatta:~$
```

show ip rip

Displays information for the Routing Information Protocol (RIP).

Syntax

show ip rip [**status**]

Command Mode

Operational mode.

Parameters

status	Optional. Displays only RIP protocol status information.

Default

Displays all RIP protocol information.

Usage Guidelines

Use this command to see information about the Routing Information Protocol.

Examples

Example 1-2 lists RIP information.

Example 1-2 “show ip rip”: Displaying RIP information

```
vyatta@vyatta:~$  show ip rip
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) -
redistribute,
      (i) - interface

    Network         Next Hop       Metric From          Tag Time
C(i) 192.168.1.0/24    0.0.0.0             1 self            0
vyatta@vyatta:~$
```

Chapter 2: Route Redistribution

This chapter describes commands for redistributing routes from other routing protocols into RIP.

This chapter presents the following topics:

- Route Redistribution Commands

Route Redistribution Commands

This chapter contains the following commands.

Configuration Commands	
protocols rip redistribute bgp	Allows you to redistribute BGP routes into RIP routing tables.
protocols rip redistribute connected	Allows you to redistribute directly connected routes into RIP routing tables.
protocols rip redistribute kernel	Allows you to redistribute kernel routes into RIP routing tables.
protocols rip redistribute ospf	Allows you to redistribute OSPF routes into RIP routing tables.
protocols rip redistribute static	Allows you to redistribute static routes into RIP routing tables.
Operational Commands	
None	

protocols rip redistribute bgp

Allows you to redistribute BGP routes into RIP routing tables.

Syntax

set protocols rip redistribute bgp [**metric** *metric* | **route-map** *map-name*]

delete protocols rip redistribute bgp [**metric** | **route-map**]

show protocols rip redistribute bgp [**metric** | **route-map**]

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      redistribute {
         bgp {
            metric: 1-16
            route-map: text
         }
      }
   }
}
```

Parameters

metric metric	The routing metric to be applied to BGP routes being imported into RIP routing tables. The range is 1-16. The default is 1.
map-name	Optional. Applies the specified route map to BGP routes being imported into RIP routing tables.

Default

BGP routes being redistributed into RIP are assigned a routing metric of 1. By default, no route map is applied to redistributed BGP routes.

Usage Guidelines

Use the **set** form of this command to set the routing metric for BGP routes being redistributed into RIP, or to specify a route map to be applied to redistributed BGP routes.

Use the **delete** form of this command to remove BGP route redistribution configuration.

Use the **show** form of this command to display BGP route redistribution configuration.

protocols rip redistribute connected

Allows you to redistribute directly connected routes into RIP routing tables.

Syntax

set protocols rip redistribute connected [**metric** *metric* | **route-map** *map-name*]

delete protocols rip redistribute connected [**metric | route-map**]

show protocols rip redistribute connected [**metric | route-map**]

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
    rip {
        redistribute {
            connected {
                metric: 1-16
                route-map: text
            }
        }
    }
}
```

Parameters

metric	Optional. The routing metric to be applied to connected routes being imported into RIP routing tables. The range is 1-16. The default is 1.
map-name	Optional. Applies the specified route map to connected routes being imported into RIP routing tables.

Default

Connected routes being redistributed into RIP are assigned a routing metric of 1. By default, no route map is applied to redistributed connected routes.

Usage Guidelines

Use the **set** form of this command to set the routing metric for connected routes being redistributed into RIP, or to specify a route map to be applied to redistributed connected routes.

Use the **delete** form of this command to remove connected route redistribution configuration.

Use the **show** form of this command to display connected route redistribution configuration.

protocols rip redistribute kernel

Allows you to redistribute kernel routes into RIP routing tables.

Syntax

set protocols rip redistribute kernel [**metric** *metric* | **route-map** *map-name*]

delete protocols rip redistribute kernel [**metric** | **route-map**]

show protocols rip redistribute kernel [**metric** | **route-map**]

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
    rip {
        redistribute {
            kernel {
                metric: 1-16
                route-map: text
            }
        }
    }
}
```

Parameters

metric	Optional. The routing metric to be applied to kernel routes being imported into RIP routing tables. The range is 1-16. The default is 1.
map-name	Optional. Applies the specified route map to kernel routes being imported into RIP routing tables.

Default

Kernel routes being redistributed into RIP are assigned a routing metric of 1. By default, no route map is applied to redistributed kernel routes.

Usage Guidelines

Use the **set** form of this command to set the routing metric for kernel routes being redistributed into RIP, or to specify a route map to be applied to redistributed kernel routes.

Use the **delete** form of this command to remove kernel route redistribution configuration.

Use the **show** form of this command to display kernel route redistribution configuration.

protocols rip redistribute ospf

Allows you to redistribute OSPF routes into RIP routing tables.

Syntax

set protocols rip redistribute ospf [**metric** *metric* | **route-map** *map-name*]

delete protocols rip redistribute ospf [**metric | route-map**]

show protocols rip redistribute ospf [**metric | route-map**]

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      redistribute {
         ospf {
            metric: 1-16
            route-map: text
         }
      }
   }
}
```

Parameters

metric	Optional. The routing metric to be applied to OSPF routes being imported into RIP routing tables. The range is 1-16. The default is 1.
map-name	Optional. Applies the specified route map to OSPF routes being imported into RIP routing tables.

Default

OSPF routes being redistributed into RIP are assigned a routing metric of 1. By default, no route map is applied to redistributed OSPF routes.

Usage Guidelines

Use the **set** form of this command to set the routing metric for OSPF routes being redistributed into RIP, or to specify a route map to be applied to redistributed OSPF routes.

Use the **delete** form of this command to remove OSPF route redistribution configuration.

Use the **show** form of this command to display OSPF route redistribution configuration.

protocols rip redistribute static

Allows you to redistribute static routes into RIP routing tables.

Syntax

set protocols rip redistribute static [**metric** *metric* | **route-map** *map-name*]

delete protocols rip redistribute static [**metric | route-map**]

show protocols rip redistribute static [**metric | route-map**]

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      redistribute {
         static {
            metric: 1-16
            route-map: text
         }
      }
   }
}
```

Parameters

metric	Optional. The routing metric to be applied to static routes being imported into RIP routing tables. The range is 1-16. The default is 1.
map-name	Optional. Applies the specified route map to static routes being imported into RIP routing tables.

Default

Static routes being redistributed into RIP are assigned a routing metric of 1. By default, no route map is applied to redistributed static routes.

Usage Guidelines

Use the **set** form of this command to set the routing metric for static routes being redistributed into RIP, or to specify a route map to be applied to redistributed static routes.

Use the **delete** form of this command to remove static route redistribution configuration.

Use the **show** form of this command to display static route redistribution configuration.

Chapter 3: Route Filtering

This chapter describes commands for RIP route filtering.

This chapter presents the following topics:

- RIP Route Filtering Commands

RIP Route Filtering Commands

This chapter contains the following commands.

Configuration Commands	
protocols rip distribute-list access-list	Applies an access list for filtering inbound or outbound RIP packets.
protocols rip distribute-list interface <ethx> access-list	Applies an access list to a specific interface for filtering inbound or outbound RIP packets.
protocols rip distribute-list interface <ethx> prefix-list	Applies a prefix list to a specific interface for filtering inbound or outbound RIP packets.
protocols rip distribute-list prefix-list	Applies a prefix list for filtering inbound or outbound RIP packets.
Operational Commands	
None.	

protocols rip distribute-list access-list

Applies an access list for filtering inbound or outbound RIP packets.

Syntax

set protocols rip distribute-list access-list {**in** *in-list* | **out** *out-list*}

delete protocols rip distribute-list access-list {**in** | **out**}

show protocols rip distribute-list access-list {**in** | **out**}

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      distribute-list {
         access-list {
            in: u32
            out: u32
         }
      }
   }
}
```

Parameters

in-list	The identifier of a defined access list. The access list will be applied to filter inbound RIP packets.
out-list	The identifier of a defined access list. The access list will be applied to filter outbound RIP packets.

Default

None.

Usage Guidelines

Use the **set** form of this command to apply an access list for filtering inbound or outbound RIP packets.

Use the **delete** form of this command to remove access list packet filtering from RIP packets.

Use the **show** form of this command to display RIP access list filtering configuration.

protocols rip distribute-list interface <ethx> access-list

Applies an access list to a specific interface for filtering inbound or outbound RIP packets.

Syntax

set protocols rip distribute-list interface *eth0..eth23* **access-list** {**in** *in-list* | **out** *out-list*]

delete protocols rip distribute-list interface *eth0..eth23* **access-list** {**in | out**}

show protocols rip distribute-list interface *eth0..eth23* **access-list** {**in | out**}

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      distribute-list {
         interface eth0..eth23
            access-list {
               in: u32
               out: u32
            }
         }
      }
   }
}
```

Parameters

eth0..eth23	Mandatory. Interface on which to filter packets.
in-list	The identifier of a defined access list. The access list will be applied to the specified interface to filter inbound RIP packets.
out-list	The identifier of a defined access list. The access list will be applied to the specified interface to filter outbound RIP packets.

Default

None.

Usage Guidelines

Use the **set** form of this command to apply an access list to a specific interface for filtering inbound or outbound RIP packets.

Use the **delete** form of this command to remove RIP access list packet filtering from an interface.

Use the **show** form of this command to display RIP access list filtering configuration for an interface.

protocols rip distribute-list interface <ethx> prefix-list

Applies a prefix list to a specific interface for filtering inbound or outbound RIP packets.

Syntax

set protocols rip distribute-list interface *eth0..eth23* **prefix-list** {**in** *in-list* | **out** *out-list*}

delete protocols rip distribute-list interface *eth0..eth23* **prefix-list** {**in** | **out**}

show protocols rip distribute-list interface *eth0..eth23* **prefix-list** {**in** | **out**}

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      distribute-list {
         interface eth0..eth23
            prefix-list {
               in: text
               out: text
            }
         }
      }
   }
}
```

Parameters

eth0..eth23	Mandatory. Interface on which to apply the access list filter.
in-list	The identifier of a defined prefix list. The prefix list will be applied to the specified interface to filter inbound RIP packets.
out-list	The identifier of a defined prefix list. The prefix list will be applied to the specified interface to filter outbound RIP packets.

Default

None.

Usage Guidelines

Use the **set** form of this command to apply a prefix list to a specific interface for filtering inbound or outbound RIP packets.

Use the **delete** form of this command to remove RIP prefix list packet filtering from an interface.

Use the **show** form of this command to display RIP prefix list filtering configuration for an interface.

protocols rip distribute-list prefix-list

Applies a prefix list for filtering inbound or outbound RIP packets.

Syntax

set protocols rip distribute-list prefix-list {**in** *in-list* | **out** *out-list*}

delete protocols rip distribute-list prefix-list {**in** | **out**}

show protocols rip distribute-list prefix-list {**in** | **out**}

Command Mode

Configuration mode.

Configuration Statement

```
protocols {
   rip {
      distribute-list {
         prefix-list {
            in: text
            out: text
         }
      }
   }
}
```

Parameters

in-list	The identifier of a defined prefix list. The prefix list will be applied to filter inbound RIP packets.
out-list	The identifier of a defined prefix list. The prefix list will be applied to filter outbound RIP packets.

Default

None.

Usage Guidelines

Use the **set** form of this command to apply a prefix list for filtering inbound or outbound RIP packets.

Use the **delete** form of this command to remove RIP prefix list packet filtering.

Use the **show** form of this command to display RIP prefix list filtering configuration.

Chapter 4: RIP on Ethernet Interfaces and Vifs

This chapter describes commands for deploying RIP on Ethernet interfaces and Ethernet vifs, including Ethernet interfaces with PPPoE encapsulation.

This chapter presents the following topics:

- Ethernet Interface and Vif RIP Commands

Ethernet Interface and Vif RIP Commands

This chapter contains the following commands.

Configuration Commands	
Ethernet Interfaces	
interfaces ethernet <ethx> ip rip	Enables RIP on an Ethernet interface.
interfaces ethernet <ethx> ip rip authentication	Specify RIP authentication for the Ethernet interface.
interfaces ethernet <ethx> ip rip split-horizon poison-reverse	Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.
Ethernet with PPPoE	
interfaces ethernet <ethx> pppoe <num> ip rip	Enables RIP on a PPPoE interface.
interfaces ethernet <ethx> pppoe <num> ip rip authentication	Specifies authentication for RIP on a PPPoE interface.
interfaces ethernet <ethx> pppoe <num> ip rip split-horizon poison-reverse	Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.
Ethernet Vifs	
interfaces ethernet <ethx> vif <vlan-id> ip rip	Enables RIP on a virtual interface.
interfaces ethernet <ethx> vif <vlan-id> ip rip authentication	Specify RIP authentication for the virtual interface.
interfaces ethernet <ethx> vif <vlan-id> ip rip split-horizon poison-reverse	Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.
Operational Commands	
None.	

interfaces ethernet <ethx> ip rip

Enables RIP on an Ethernet interface.

Syntax

set interfaces ethernet *ethx* **ip rip**

delete interfaces ethernet *ethx* **ip rip**

show interfaces ethernet *ethx* **ip rip**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   ethernet eth0..eth23 {
      ip {
         rip
      }
   }
}
```

Parameters

ethx	Mandatory. Multi-node. The identifier for the ADSL interface you are defining. This may be **adsl0** to **adsl***x*, depending on what physical ADSL ports are actually available on the system.

Default

None.

Usage Guidelines

Use this command to enable Routing Information Protocol (RIP) on an Ethernet interface.

Use the **set** form of this command to enable RIP on an interface.

Use the **delete** form of this command to remove all RIP configuration and disable RIP on the interface.

Use the **show** form of this command to display RIP configuration.

interfaces ethernet <ethx> ip rip authentication

Specify RIP authentication for the Ethernet interface.

Syntax

set interfaces ethernet *ethx* **ip rip authentication** [**md5** *md5-key* **password** *md5-password* | **plaintext-password** *password*]

delete interfaces ethernet *ethx* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

show interfaces ethernet *ethx* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   ethernet eth0..eth23 {
      ip {
         rip {
            authentication {
               md5 u32 {
                  password: text
               }
               plaintext-password: text
            }
         }
      }
   }
}
```

Parameters

ethx	Mandatory. Multi-node. An identifier for the Ethernet interface you are defining. This may be **eth0** to **eth23**, depending on what Ethernet interfaces that are actually available on the system. To see the interfaces available to the system kernel, use the **system** option of the **show interfaces** command (see page 76).

md5-key	Optional. The authentication key ID. This must be the same on both the sending and receiving systems. The range is 1 to 255.
md5-password	Optional. The password to use in MD5 authentication. This must be the same on both the sending and receiving systems.
password	Optional. The password to use in simple (plain-text) authentication. This must be the same on both the sending and receiving systems.

Default

None.

Usage Guidelines

Use this command to specify the authentication method to be used for RIP on an Ethernet interface. This authentication is independent of the authentication configured for the RIP area.

In plain text authentication, passwords are sent through the network in plain text. In MD5 authentication, the system uses the Message Digest 5 (MD5) algorithm to compute a hash value from the contents of the RIP packet and the password. The hash value and the MD5 key are included in the transmitted packet, and the receiving system (configured with the same password) calculates its own hash function, which must match.

The authentication parameters must be the same for all routers that are to establish two-way communication within a network. If two routers do not agree on these parameters, they will not consider establish adjacencies, and will disregard one another’s communications.

Use the **set** form of this command to set RIP authentication for an Ethernet interface.

Use the **delete** form of this command to remove RIP Ethernet interface authentication configuration information.

Use the **show** form of this command to display RIP Ethernet interface authentication configuration information.

interfaces ethernet <ethx> ip rip split-horizon poison-reverse

Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.

Syntax

set interfaces ethernet *ethx* **ip rip split-horizon poison-reverse**

delete interfaces ethernet *ethx* **ip rip split-horizon**

show interfaces ethernet *ethx* **ip rip split-horizon**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   ethernet eth0..eth23 {
      ip {
         rip {
            split-horizon {
               poison-reverse
            }
         }
      }
   }
}
```

Parameters

ethx	Mandatory. Multi-node. An identifier for the Ethernet interface you are defining. This may be **eth0** to **eth23**, depending on what Ethernet interfaces that are actually available on the system. To see the interfaces available to the system kernel, use the **system** option of the **show interfaces** command (see page 76).

Default

None.

Usage Guidelines

Use this command to enable or disable split-horizon poison-reverse on a ADSL interface with Point-to-Point Protocol over Ethernet (PPPoE) encapsulation running RIP.

Split-horizon is a stability feature that reduces the possibility of network loops, particularly in the case where links become disconnected. Enabling split-horizon stops an interface from including in its network updates any routes that it learned from that interface. Split horizon is effective at preventing loops between routers that are directly connected to one another, and speeds convergence when network conditions change.

Poison reverse is a variation of split horizon. When an interface with poison reverse enabled detects that a link is down, it increases the metric for that route to 16, and propagates that information in its next update. Since 15 is the largest number of hops considered reachable on a RIP network, increasing the metric to 16 renders the route unreachable as far as downstream RIP routers are concerned. This is called “poisoning” the route. Poison reverse can be useful for propagating information about bad routes to routers that are downstream but not immediate neighbors, where split horizon is ineffective.

When this option is enabled, the router includes the route in announcements to the neighbor from which it was learned. When this option is disabled, the router omits the route in announcements to the neighbor from which it was learned.

Use the **set** form of this command to enable split-horizon poison-reverse on a RIP interface.

Use the **delete** form of this command to disable split-horizon poison-reverse on a RIP interface.

Use the **show** form of this command to display split-horizon poison-reverse configuration.

interfaces ethernet <ethx> pppoe <num> ip rip

Enables RIP on a PPPoE interface.

Syntax

set interfaces ethernet *ethx* **pppoe** *num* **ip rip**

delete interfaces ethernet *ethx* **pppoe** *num* **ip rip**

show interfaces ethernet *ethx* **pppoe** *num* **ip rip**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   ethernet eth0..eth23 {
      pppoe 0-15 {
         ip {
            rip
         }
      }
   }
}
```

Parameters

ethx	Mandatory. Multi-node. An identifier for the Ethernet interface you are defining. This may be **eth0** to **eth23**, depending on what Ethernet interfaces that are actually available on the system. To see the interfaces available to the system kernel, use the **system** option of the **show interfaces** command (see page 76).
num	Mandatory. The name of a defined PPPoE unit. The range is 0 to 15.

Default

None.

Usage Guidelines

Use this command to enable Routing Information Protocol (RIP) on a Point-to-Point over Ethernet (PPPoE) interface.

Use the **set** form of this command to enable RIP on an interface.

Use the **delete** form of this command to remove all RIP configuration and disable RIP on the interface.

Use the **show** form of this command to display RIP configuration.

interfaces ethernet <ethx> pppoe <num> ip rip authentication

Specifies authentication for RIP on a PPPoE interface.

Syntax

set interfaces ethernet *ethx* **pppoe** *num* **ip rip authentication** [**md5** *md5-key* **password** *md5-password* | **plaintext-password** *password*]

delete interfaces ethernet *ethx* **pppoe** *num* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

show interfaces ethernet *ethx* **pppoe** *num* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   ethernet eth0..eth23 {
      ip {
      pppoe 0-15 {
            rip {
               authentication {
                  md5 u32 {
                     password: text
                  }
                  plaintext-password: text
               }
            }
         }
      }
   }
}
```

Parameters

ethx	Mandatory. Multi-node. An identifier for the Ethernet interface you are defining. This may be **eth0** to **eth23**, depending on what Ethernet interfaces that are actually available on the system. To see the interfaces available to the system kernel, use the **system** option of the **show interfaces** command (see page 76).
num	Mandatory. The name of a defined PPPoE unit. The range is 0 to 15.
md5-key	Optional. The authentication key ID. This must be the same on both the sending and receiving systems. The range is 1 to 255.
md5-password	Optional. The password to use in MD5 authentication. This must be the same on both the sending and receiving systems.
password	Optional. The password to use in plain-text authentication. This must be eight characters or less and the same on both the sending and receiving systems.

Default

None.

Usage Guidelines

Use this command to specify the authentication method to be used for RIP on a Point-to-Point over Ethernet (PPPoE) interface. This authentication is independent of the authentication configured for the RIP area.

In plain text authentication, passwords are sent through the network in plain text. In MD5 authentication, the system uses the Message Digest 5 (MD5) algorithm to compute a hash value from the contents of the RIP packet and the password. The hash value and the MD5 key are included in the transmitted packet, and the receiving system (configured with the same password) calculates its own hash function, which must match.

The authentication parameters must be the same for all routers that are to establish two-way communication within a network. If two routers do not agree on these parameters, they will not consider establish adjacencies, and will disregard one another’s communications.

Use the **set** form of this command to set RIP authentication for a PPPoE interface.

Use the **delete** form of this command to remove RIP PPPoE interface authentication configuration information.

Use the **show** form of this command to display RIP PPPoE interface authentication configuration information.

interfaces ethernet <ethx> pppoe <num> ip rip split-horizon poison-reverse

Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.

Syntax

set interfaces ethernet *ethx* **pppoe** *num* **ip rip split-horizon poison-reverse**

delete interfaces ethernet *ethx* **pppoe** *num* **ip rip split-horizon**

show interfaces ethernet *ethx* **pppoe** *num* **ip rip split-horizon**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   ethernet eth0..eth23 {
      pppoe 0-15 {
         ip {
            rip {
               split-horizon {
                  poison-reverse
               }
            }
         }
      }
   }
}
```

Parameters

ethx	Mandatory. Multi-node. An identifier for the Ethernet interface you are defining. This may be **eth0** to **eth23**, depending on what Ethernet interfaces that are actually available on the system. To see the interfaces available to the system kernel, use the **system** option of the **show interfaces** command (see page 76).
num	Mandatory. The name of a defined PPPoE unit. The range is 0 to 15.

Default

None.

Usage Guidelines

Use this command to enable or disable split-horizon poison-reverse on a RIP interface.

Split-horizon is a stability feature that reduces the possibility of network loops, particularly in the case where links become disconnected. Enabling split-horizon stops an interface from including in its network updates any routes that it learned from that interface. Split horizon is effective at preventing loops between routers that are directly connected to one another, and speeds convergence when network conditions change.

Poison reverse is a variation of split horizon. When an interface with poison reverse enabled detects that a link is down, it increases the metric for that route to 16, and propagates that information in its next update. Since 15 is the largest number of hops considered reachable on a RIP network, increasing the metric to 16 renders the route unreachable as far as downstream RIP routers are concerned. This is called “poisoning” the route. Poison reverse can be useful for propagating information about bad routes to routers that are downstream but not immediate neighbors, where split horizon is ineffective.

When this option is enabled, the router includes the route in announcements to the neighbor from which it was learned. When this option is disabled, the router omits the route in announcements to the neighbor from which it was learned.

Use the **set** form of this command to enable split-horizon poison-reverse on a RIP interface.

Use the **delete** form of this command to disable split-horizon poison-reverse on a RIP interface.

Use the **show** form of this command to display split-horizon poison-reverse configuration.

interfaces ethernet <ethx> vif <vlan-id> ip rip

Enables RIP on a virtual interface.

Syntax

set interfaces ethernet *ethx* **vif** *vlan-id* **ip rip**

delete interfaces ethernet *ethx* **vif** *vlan-id* **ip rip**

show interfaces ethernet *ethx* **vif** *vlan-id* **ip rip**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   ethernet eth0..eth23 {
      vif 0-4095 {
         ip {
            rip
         }
      }
   }
}
```

Parameters

ethx	Mandatory. Multi-node. An identifier for the Ethernet interface you are defining. This may be **eth0** to **eth23**, depending on what Ethernet interfaces that are actually available on the system. To see the interfaces available to the system kernel, use the **system** option of the **show interfaces** command (see page 76).
vlan-id	Mandatory. Multi-node. The VLAN ID for the vif, for use with 802.1q VLAN tagging. Only tagged packets are received on vifs configured on Ethernet interfaces. The range is 0 to 4095. You can define more than one vif for a single interface by creating multiple **vif** configuration nodes.

Default

None.

Usage Guidelines

Use this command to enable Routing Information Protocol (RIP) on a virtual interface.

Use the **set** form of this command to enable RIP on an interface.

Use the **delete** form of this command to remove all RIP configuration and disable RIP on the interface.

Use the **show** form of this command to display RIP configuration.

interfaces ethernet <ethx> vif <vlan-id> ip rip authentication

Specify RIP authentication for the virtual interface.

Syntax

set interfaces ethernet *ethx* **vif** *vlan-id* **ip rip authentication** [**md5** *md5-key* **password** *md5-password* | **plaintext-password** *password*]

delete interfaces ethernet *ethx* **vif** *vlan-id* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

show interfaces ethernet *ethx* **vif** *vlan-id* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   ethernet eth0..eth23 {
      ip {
      vif 0-4095 {
            rip {
               authentication {
                  md5 u32 {
                     password: text
                  }
                  plaintext-password: text
               }
            }
         }
      }
   }
}
```

Parameters

ethx	Mandatory. Multi-node. An identifier for the Ethernet interface you are defining. This may be **eth0** to **eth23**, depending on what Ethernet interfaces that are actually available on the system. To see the interfaces available to the system kernel, use the **system** option of the **show interfaces** command (see page 76).
vlan-id	Mandatory. Multi-node. The VLAN ID for the vif, for use with 802.1q VLAN tagging. Only tagged packets are received on vifs configured on Ethernet interfaces. The range is 0 to 4095. You can define more than one vif for a single interface by creating multiple **vif** configuration nodes.
md5-key	Optional. The authentication key ID. This must be the same on both the sending and receiving systems. The range is 1 to 255.
md5-password	Optional. The password to use in MD5 authentication. This must be the same on both the sending and receiving systems.
password	Optional. The password to use in simple (plain-text) authentication. This must be the same on both the sending and receiving systems.

Default

None.

Usage Guidelines

Use this command to specify the authentication method to be used for RIP on a virtual interface. This authentication is independent of the authentication configured for the RIP area.

In plain text authentication, passwords are sent through the network in plain text. In MD5 authentication, the system uses the Message Digest 5 (MD5) algorithm to compute a hash value from the contents of the RIP packet and the password. The hash value and the MD5 key are included in the transmitted packet, and the receiving system (configured with the same password) calculates its own hash function, which must match.

The authentication parameters must be the same for all routers that are to establish two-way communication within a network. If two routers do not agree on these parameters, they will not consider establish adjacencies, and will disregard one another’s communications.

Use the **set** form of this command to set RIP authentication for a virtual interface.

Use the **delete** form of this command to remove RIP virtual interface authentication configuration information.

Use the **show** form of this command to display RIP virtual interface authentication configuration information.

interfaces ethernet <ethx> vif <vlan-id> ip rip split-horizon poison-reverse

Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.

Syntax

set interfaces ethernet *ethx* **vif** *vlan-id* **ip rip split-horizon poison-reverse**

delete interfaces ethernet *ethx* **vif** *vlan-id* **ip rip split-horizon**

show interfaces ethernet *ethx* **vif** *vlan-id* **ip rip split-horizon**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   ethernet eth0..eth23 {
      vif 0-4095 {
         ip {
            rip {
               split-horizon {
                  poison-reverse
               }
            }
         }
      }
   }
}
```

Parameters

ethx	Mandatory. Multi-node. An identifier for the Ethernet interface you are defining. This may be **eth0** to **eth23**, depending on what Ethernet interfaces that are actually available on the system. To see the interfaces available to the system kernel, use the **system** option of the **show interfaces** command (see page 76).

vlan-id	Mandatory. Multi-node. The VLAN ID for the vif, for use with 802.1q VLAN tagging. Only tagged packets are received on vifs configured on Ethernet interfaces. The range is 0 to 4095. You can define more than one vif for a single interface by creating multiple **vif** configuration nodes.

Default

None.

Usage Guidelines

Use this command to enable or disable split-horizon poison-reverse on a RIP interface.

Split-horizon is a stability feature that reduces the possibility of network loops, particularly in the case where links become disconnected. Enabling split-horizon stops an interface from including in its network updates any routes that it learned from that interface. Split horizon is effective at preventing loops between routers that are directly connected to one another, and speeds convergence when network conditions change.

Poison reverse is a variation of split horizon. When an interface with poison reverse enabled detects that a link is down, it increases the metric for that route to 16, and propagates that information in its next update. Since 15 is the largest number of hops considered reachable on a RIP network, increasing the metric to 16 renders the route unreachable as far as downstream RIP routers are concerned. This is called “poisoning” the route. Poison reverse can be useful for propagating information about bad routes to routers that are downstream but not immediate neighbors, where split horizon is ineffective.

When this option is enabled, the router includes the route in announcements to the neighbor from which it was learned. When this option is disabled, the router omits the route in announcements to the neighbor from which it was learned.

Use the **set** form of this command to enable split-horizon poison-reverse on a RIP interface.

Use the **delete** form of this command to disable split-horizon poison-reverse on a RIP interface.

Use the **show** form of this command to display split-horizon poison-reverse configuration.

Chapter 5: RIP on the Loopback Interface

This chapter describes commands for deploying RIP on the loopback interface.

This chapter presents the following topics:

- Loopback Interface RIP Commands

Loopback Interface RIP Commands

This chapter contains the following commands.

Configuration Commands	
interfaces loopback lo ip rip	Enables RIP on the loopback interface.
interfaces loopback lo ip rip authentication	Specify RIP authentication for the loopback interface.
interfaces loopback lo ip rip split-horizon poison-reverse	Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.
Operational Commands	
None.	

interfaces loopback lo ip rip

Enables RIP on the loopback interface.

Syntax

set interfaces loopback lo ip rip

delete interfaces loopback lo ip rip

show interfaces loopback lo ip rip

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   loopback lo {
      ip {
         rip
      }
   }
}
```

Parameters

None.

Default

None.

Usage Guidelines

Use this command to enable Routing Information Protocol (RIP) on an Ethernet interface.

Use the **set** form of this command to enable RIP on an interface.

Use the **delete** form of this command to remove all RIP configuration and disable RIP on the interface.

Use the **show** form of this command to display RIP configuration.

interfaces loopback lo ip rip authentication

Specify RIP authentication for the loopback interface.

Syntax

set interfaces loopback lo ip rip authentication [**md5** *md5-key* **password** *md5-password* | **plaintext-password** *password*]

delete interfaces loopback lo ip ospf authentication [**md5** *md5-key* **password** | **plaintext-password**]

show interfaces loopback lo ip ospf authentication [**md5** *md5-key* **password** | **plaintext-password**]

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
    loopback lo {
        ip {
            rip {
                authentication {
                    md5 u32 {
                        password: text
                    }
                    plaintext-password: text
                }
            }
        }
    }
}
```

Parameters

md5-key	Optional. The authentication key ID. This must be the same on both the sending and receiving systems. The range is 1 to 255.
md5-password	Optional. The password to use in MD5 authentication. This must be the same on both the sending and receiving systems.
password	Optional. The password to use in simple (plain-text) authentication. This must be the same on both the sending and receiving systems.

Default

None.

Usage Guidelines

Use this command to specify the authentication method to be used for RIP on the loopback interface. This authentication is independent of the authentication configured for the OSPF area.

In plain text authentication, passwords are sent through the network in plain text. In MD5 authentication, the system uses the Message Digest 5 (MD5) algorithm to compute a hash value from the contents of the RIP packet and the password. The hash value and the MD5 key are included in the transmitted packet, and the receiving system (configured with the same password) calculates its own hash function, which must match.

The authentication parameters must be the same for all routers that are to establish two-way communication within a network. If two routers do not agree on these parameters, they will not consider establish adjacencies, and will disregard one another's communications.

Use the **set** form of this command to set RIP authentication for the loopback interface.

Use the **delete** form of this command to remove RIP loopback interface authentication configuration information.

Use the **show** form of this command to display RIP loopback interface authentication configuration information.

interfaces loopback lo ip rip split-horizon poison-reverse

Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.

Syntax

set interfaces loopback lo ip rip split-horizon poison-reverse

delete interfaces loopback lo ip rip split-horizon

show interfaces loopback lo ip rip split-horizon

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   loopback lo {
      ip {
         rip {
            split-horizon {
               poison-reverse
            }
         }
      }
   }
}
```

Parameters

None.

Default

None.

Usage Guidelines

Use this command to enable or disable split-horizon poison-reverse on the loopback interface.

Split-horizon is a stability feature that reduces the possibility of network loops, particularly in the case where links become disconnected. Enabling split-horizon stops an interface from including in its network updates any routes that it learned from that interface. Split horizon is effective at preventing loops between routers that are directly connected to one another, and speeds convergence when network conditions change.

Poison reverse is a variation of split horizon. When an interface with poison reverse enabled detects that a link is down, it increases the metric for that route to 16, and propagates that information in its next update. Since 15 is the largest number of hops considered reachable on a RIP network, increasing the metric to 16 renders the route unreachable as far as downstream RIP routers are concerned. This is called “poisoning” the route. Poison reverse can be useful for propagating information about bad routes to routers that are downstream but not immediate neighbors, where split horizon is ineffective.

When this option is enabled, the router includes the route in announcements to the neighbor from which it was learned. When this option is disabled, the router omits the route in announcements to the neighbor from which it was learned.

Use the **set** form of this command to enable split-horizon poison-reverse on the loopback interface.

Use the **delete** form of this command to disable split-horizon poison-reverse on the loopback interface.

Use the **show** form of this command to display split-horizon poison-reverse configuration.

Chapter 6: RIP on Serial Interfaces

This chapter describes commands for deploying RIP on serial interfaces.

This chapter presents the following topics:

- Serial Interface RIP Commands

Serial Interface RIP Commands

This chapter contains the following commands.

Configuration Commands	
Cisco HDLC	
interfaces serial <wanx> cisco-hdlc vif 1 ip rip	Enables RIP on the virtual interface of a Cisco HDLC serial interface.
interfaces serial <wanx> cisco-hdlc vif 1 ip rip authentication	Specifies authentication for RIP on a Cisco HDLC serial interface.
interfaces serial <wanx> cisco-hdlc vif 1 ip rip split-horizon poison-reverse	Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.
Frame Relay	
interfaces serial <wanx> frame-relay vif <dlci> ip rip	Enables RIP on the virtual interface of a Frame Relay serial interface.
interfaces serial <wanx> frame-relay vif <dlci> ip rip authentication	Specifies authentication for RIP on a Frame Relay serial interface.
interfaces serial <wanx> frame-relay vif <dlci> ip rip split-horizon poison-reverse	Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.
Point-to-Point Protocol	
interfaces serial <wanx> ppp vif 1 ip rip	Enables RIP on the virtual interface of a PPP serial interface.
interfaces serial <wanx> ppp vif 1 ip rip authentication	Specifies authentication for RIP on a virtual interface of a PPP serial interface.
interfaces serial <wanx> ppp vif 1 ip rip split-horizon poison-reverse	Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.
Operational Commands	
None.	

interfaces serial <wanx> cisco-hdlc vif 1 ip rip

Enables RIP on the virtual interface of a Cisco HDLC serial interface.

Syntax

set interfaces serial *wanx* **cisco-hdlc vif 1 ip rip**

delete interfaces serial *wanx* **cisco-hdlc vif 1 ip rip**

show interfaces serial *wanx* **cisco-hdlc vif 1**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   serial wan0..wan23 {
      cisco-hdlc {
         vif 1 {
            ip rip
         }
      }
   }
}
```

Parameters

wanx	Mandatory. Multi-node. The identifier for the serial interface you are defining. This may be **wan0** to **wan23**, depending on what serial interfaces that are actually available on the system.
1	The identifier of the virtual interface. Currently, only one vif is supported for Cisco HDLC interfaces, and the identifier must be 1.

Default

RIP is not enabled on Cisco HDLC interfaces.

Usage Guidelines

Use this command to enable the Routing Information Protocol (RIP) routing protocol on the virtual interface of a Cisco HDLC serial interface.

Use the **set** form of this command to enable RIP on a Cisco HDLC virtual interface.

Use the **delete** form of this command to disable RIP on a Cisco HDLC virtual interface.

Use the **show** form of this command to display Cisco HDLC virtual interface configuration.

interfaces serial <wanx> cisco-hdlc vif 1 ip rip authentication

Specifies authentication for RIP on a Cisco HDLC serial interface.

Syntax

set interfaces serial *wanx* **cisco-hdlc vif 1 ip rip authentication** [**md5** *md5-key* **password** *md5-password* | **plaintext-password** *password*]

delete interfaces serial *wanx* **cisco-hdlc vif 1 ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

show interfaces serial *wanx* **cisco-hdlc vif 1 ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   serial wan0..wan23 {
      cisco-hdlc {
         vif 1 {
            ip {
               rip {
                  authentication {
                     md5 u32 {
                        password: text
                     }
                     plaintext-password: text
                  }
               }
            }
         }
      }
   }
}
```

Parameters

wanx	Mandatory. Multi-node. The identifier for the serial interface you are defining. This may be **wan0** to **wan23**, depending on what serial interfaces that are actually available on the system.
1	The identifier of the virtual interface. Currently, only one vif is supported for Cisco HDLC interfaces, and the identifier must be 1.
md5-key	Optional. The authentication key ID. This must be the same on both the sending and receiving systems. The range is 1 to 255.
md5-password	Optional. The password to use in MD5 authentication. This must be the same on both the sending and receiving systems.
password	Optional. The password to use in plain-text authentication. This must be eight characters or less and the same on both the sending and receiving systems.

Default

None.

Usage Guidelines

Use this command to specify the authentication method to be used for RIP on a Cisco HDLC serial interface. This authentication is independent of the authentication configured for the RIP area.

In plain text authentication, passwords are sent through the network in plain text. In MD5 authentication, the system uses the Message Digest 5 (MD5) algorithm to compute a hash value from the contents of the RIP packet and the password. The hash value and the MD5 key are included in the transmitted packet, and the receiving system (configured with the same password) calculates its own hash function, which must match.

The authentication parameters must be the same for all routers that are to establish two-way communication within a network. If two routers do not agree on these parameters, they will not consider establish adjacencies, and will disregard one another's communications.

Use the **set** form of this command to set RIP authentication for a Cisco HDLC serial interface.

Use the **delete** form of this command to remove RIP Cisco HDLC serial interface authentication configuration information.

Use the **show** form of this command to display RIP Cisco HDLC serial interface authentication configuration information.

interfaces serial <wanx> cisco-hdlc vif 1 ip rip split-horizon poison-reverse

Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.

Syntax

set interfaces serial *wanx* **cisco-hdlc vif 1 ip rip split-horizon poison-reverse**

delete interfaces serial *wanx* **cisco-hdlc vif 1 ip rip split-horizon**

show interfaces serial *wanx* **cisco-hdlc vif 1 ip rip split-horizon**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   serial wan0..wan23 {
      cisco-hdlc {
         vif 1 {
            ip {
               rip {
                  split-horizon {
                     poison-reverse
                  }
               }
            }
         }
      }
   }
}
```

Parameters

wanx	Mandatory. Multi-node. The identifier for the serial interface you are defining. This may be **wan0** to **wan23**, depending on what serial interfaces that are actually available on the system.
1	The identifier of the virtual interface. Currently, only one vif is supported for Cisco HDLC interfaces, and the identifier must be 1.

Default

None.

Usage Guidelines

Use this command to enable or disable split-horizon poison-reverse on a RIP interface.

Split-horizon is a stability feature that reduces the possibility of network loops, particularly in the case where links become disconnected. Enabling split-horizon stops an interface from including in its network updates any routes that it learned from that interface. Split horizon is effective at preventing loops between routers that are directly connected to one another, and speeds convergence when network conditions change.

Poison reverse is a variation of split horizon. When an interface with poison reverse enabled detects that a link is down, it increases the metric for that route to 16, and propagates that information in its next update. Since 15 is the largest number of hops considered reachable on a RIP network, increasing the metric to 16 renders the route unreachable as far as downstream RIP routers are concerned. This is called “poisoning” the route. Poison reverse can be useful for propagating information about bad routes to routers that are downstream but not immediate neighbors, where split horizon is ineffective.

When this option is enabled, the router includes the route in announcements to the neighbor from which it was learned. When this option is disabled, the router omits the route in announcements to the neighbor from which it was learned.

Use the **set** form of this command to enable split-horizon poison-reverse on a RIP interface.

Use the **delete** form of this command to disable split-horizon poison-reverse on a RIP interface.

Use the **show** form of this command to display split-horizon poison-reverse configuration.

interfaces serial <wanx> frame-relay vif <dlci> ip rip

Enables RIP on the virtual interface of a Frame Relay serial interface.

Syntax

set interfaces serial *wanx* **frame-relay vif** *dlci* **ip rip**

delete interfaces serial *wanx* **frame-relay vif** *dlci* **ip rip**

show interfaces serial *wanx* **frame-relay vif** *dlci*

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   serial wan0..wan23 {
      frame-relay {
         vif 16-991 {
            ip rip
         }
      }
   }
}
```

Parameters

wanx	Mandatory. Multi-node. The identifier for the serial interface you are defining. This may be **wan0** to **wan23**, depending on what serial interfaces that are actually available on the system.
dlci	The identifier of the virtual interface. For Frame Relay interfaces, this is the DLCI number for the interface. The range is 16 to 991.

Default

RIP is not enabled on Frame Relay interfaces.

Usage Guidelines

Use this command to enable the Routing Information Protocol (RIP) routing protocol on a virtual interface of a Frame Relay serial interface.

Use the **set** form of this command to enable RIP on a Frame Relay virtual interface.

Use the **delete** form of this command to disable RIP on a Frame Relay virtual interface.

Use the **show** form of this command to display Frame Relay virtual interface configuration.

interfaces serial <wanx> frame-relay vif <dlci> ip rip authentication

Specifies authentication for RIP on a Frame Relay serial interface.

Syntax

set interfaces serial *wanx* **frame-relay vif** *dlci* **ip rip authentication** [**md5** *md5-key* **password** *md5-password* | **plaintext-password** *password*]

delete interfaces serial *wanx* **frame-relay vif** *dlci* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

show interfaces serial *wanx* **frame-relay vif** *dlci* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   serial wan0..wan23 {
      frame-relay {
         vif 16-991 {
            ip {
               rip {
                  authentication {
                     md5 u32 {
                        password: text
                     }
                     plaintext-password: text
                  }
               }
            }
         }
      }
   }
}
```

Parameters

wanx	Mandatory. Multi-node. The identifier for the serial interface you are defining. This may be **wan0** to **wan23**, depending on what serial interfaces that are actually available on the system.
dlci	The identifier of the virtual interface. For Frame Relay interfaces, this is the DLCI number for the interface. The range is 16 to 991.
md5-key	Optional. The authentication key ID. This must be the same on both the sending and receiving systems. The range is 1 to 255.
md5-password	Optional. The password to use in MD5 authentication. This must be the same on both the sending and receiving systems.
password	Optional. The password to use in plain-text authentication. This must be eight characters or less and the same on both the sending and receiving systems.

Default

None.

Usage Guidelines

Use this command to specify the authentication method to be used for RIP on a virtual interface of a Frame Relay serial interface. This authentication is independent of the authentication configured for the RIP area.

In plain text authentication, passwords are sent through the network in plain text. In MD5 authentication, the system uses the Message Digest 5 (MD5) algorithm to compute a hash value from the contents of the RIP packet and the password. The hash value and the MD5 key are included in the transmitted packet, and the receiving system (configured with the same password) calculates its own hash function, which must match.

The authentication parameters must be the same for all routers that are to establish two-way communication within a network. If two routers do not agree on these parameters, they will not consider establish adjacencies, and will disregard one another’s communications.

Use the **set** form of this command to set RIP authentication for a virtual interface of a Frame Relay serial interface.

Use the **delete** form of this command to remove RIP authentication configuration information from the virtual interface of a Frame Relay serial interface.

Use the **show** form of this command to display RIP authentication configuration information for the virtual interface of a Frame Relay serial interface.

interfaces serial <wanx> frame-relay vif <dlci> ip rip split-horizon poison-reverse

Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.

Syntax

set interfaces serial *wanx* **frame-relay vif** *dlci* **ip rip split-horizon poison-reverse**

delete interfaces serial *wanx* **frame-relay vif** *dlci* **ip rip split-horizon**

show interfaces serial *wanx* **frame-relay vif** *dlci* **ip rip split-horizon**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   serial wan0..wan23 {
      frame-relay {
         vif 16-991 {
            ip {
               rip {
                  split-horizon {
                     poison-reverse
                  }
               }
            }
         }
      }
   }
}
```

Parameters

wanx	Mandatory. Multi-node. The identifier for the serial interface you are defining. This may be **wan0** to **wan23**, depending on what serial interfaces that are actually available on the system.
dlci	The identifier of the virtual interface. For Frame Relay interfaces, this is the DLCI number for the interface. The range is 16 to 991.

Default

None.

Usage Guidelines

Use this command to enable or disable split-horizon poison-reverse on a RIP interface.

Split-horizon is a stability feature that reduces the possibility of network loops, particularly in the case where links become disconnected. Enabling split-horizon stops an interface from including in its network updates any routes that it learned from that interface. Split horizon is effective at preventing loops between routers that are directly connected to one another, and speeds convergence when network conditions change.

Poison reverse is a variation of split horizon. When an interface with poison reverse enabled detects that a link is down, it increases the metric for that route to 16, and propagates that information in its next update. Since 15 is the largest number of hops considered reachable on a RIP network, increasing the metric to 16 renders the route unreachable as far as downstream RIP routers are concerned. This is called “poisoning” the route. Poison reverse can be useful for propagating information about bad routes to routers that are downstream but not immediate neighbors, where split horizon is ineffective.

When this option is enabled, the router includes the route in announcements to the neighbor from which it was learned. When this option is disabled, the router omits the route in announcements to the neighbor from which it was learned.

Use the **set** form of this command to enable split-horizon poison-reverse on a RIP interface.

Use the **delete** form of this command to disable split-horizon poison-reverse on a RIP interface.

Use the **show** form of this command to display split-horizon poison-reverse configuration.

interfaces serial <wanx> ppp vif 1 ip rip

Enables RIP on the virtual interface of a PPP serial interface.

Syntax

set interfaces serial *wanx* **ppp vif 1 ip rip**

delete interfaces serial *wanx* **ppp vif 1 ip rip**

show interfaces serial *wanx* **ppp vif 1**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   serial wan0..wan23 {
      ppp {
         vif 1 {
            ip rip
         }
      }
   }
}
```

Parameters

wanx	Mandatory. Multi-node. The identifier for the serial interface you are defining. This may be **wan0** to **wan23**, depending on what serial interfaces that are actually available on the system.
1	The identifier of the virtual interface. Currently, only one vif is supported for PPP interfaces, and the identifier must be 1.

Default

RIP is not enabled on PPP interfaces.

Usage Guidelines

Use this command to enable the Routing Information Protocol (RIP) routing protocol on the virtual interface of a Point-to-Point Protocol (PPP) serial interface.

Use the **set** form of this command to enable RIP on a PPP virtual interface.

Use the **delete** form of this command to disable RIP on a PPP virtual interface.

Use the **show** form of this command to display PPP virtual interface configuration.

interfaces serial <wanx> ppp vif 1 ip rip authentication

Specifies authentication for RIP on a virtual interface of a PPP serial interface.

Syntax

set interfaces serial *wanx* **ppp vif 1 ip rip authentication** [**md5** *md5-key* **password** *md5-password* | **plaintext-password** *password*]

delete interfaces serial *wanx* **ppp vif 1 ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

show interfaces serial *wanx* **ppp vif 1 ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   serial wan0..wan23 {
      ppp {
         vif 1 {
            ip {
               rip {
                  authentication {
                     md5 u32 {
                        password: text
                     }
                     plaintext-password: text
                  }
               }
            }
         }
      }
   }
}
```

Parameters

wanx	Mandatory. Multi-node. The identifier for the serial interface you are defining. This may be **wan0** to **wan23**, depending on what serial interfaces that are actually available on the system.

1	The identifier of the virtual interface. Currently, only one vif is supported for PPP interfaces, and the identifier must be 1.
md5-key	Optional. The authentication key ID. This must be the same on both the sending and receiving systems. The range is 1 to 255.
md5-password	Optional. The password to use in MD5 authentication. This must be the same on both the sending and receiving systems.
password	Optional. The password to use in plain-text authentication. This must be eight characters or less and the same on both the sending and receiving systems.

Default

None.

Usage Guidelines

Use this command to specify the authentication method to be used for RIP on the virtual interface of a Point-to-Point Protocol (PPP) serial interface. This authentication is independent of the authentication configured for the RIP area.

In plain text authentication, passwords are sent through the network in plain text. In MD5 authentication, the system uses the Message Digest 5 (MD5) algorithm to compute a hash value from the contents of the RIP packet and the password. The hash value and the MD5 key are included in the transmitted packet, and the receiving system (configured with the same password) calculates its own hash function, which must match.

The authentication parameters must be the same for all routers that are to establish two-way communication within a network. If two routers do not agree on these parameters, they will not consider establish adjacencies, and will disregard one another’s communications.

Use the **set** form of this command to set RIP authentication for the virtual interface of a Point-to-Point Protocol (PPP) serial interface.

Use the **delete** form of this command to remove RIP authentication configuration information from the virtual interface of a Point-to-Point Protocol (PPP) serial interface.

Use the **show** form of this command to display RIP authentication configuration information for the virtual interface of a Point-to-Point Protocol (PPP) serial interface.

interfaces serial <wanx> ppp vif 1 ip rip split-horizon poison-reverse

Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.

Syntax

set interfaces serial *wanx* **ppp vif 1 ip rip split-horizon poison-reverse**

delete interfaces serial *wanx* **ppp vif 1 ip rip split-horizon**

show interfaces serial *wanx* **ppp vif 1 ip rip split-horizon**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   serial wan0..wan23 {
      ppp {
         vif 1 {
            ip {
               rip {
                  split-horizon {
                     poison-reverse
                  }
               }
            }
         }
      }
   }
}
```

Parameters

wanx	Mandatory. Multi-node. The identifier for the serial interface you are defining. This may be **wan0** to **wan23**, depending on what serial interfaces that are actually available on the system.
1	The identifier of the virtual interface. Currently, only one vif is supported for PPP interfaces, and the identifier must be 1.

Default

None.

Usage Guidelines

Use this command to enable or disable split-horizon poison-reverse on a RIP interface.

Split-horizon is a stability feature that reduces the possibility of network loops, particularly in the case where links become disconnected. Enabling split-horizon stops an interface from including in its network updates any routes that it learned from that interface. Split horizon is effective at preventing loops between routers that are directly connected to one another, and speeds convergence when network conditions change.

Poison reverse is a variation of split horizon. When an interface with poison reverse enabled detects that a link is down, it increases the metric for that route to 16, and propagates that information in its next update. Since 15 is the largest number of hops considered reachable on a RIP network, increasing the metric to 16 renders the route unreachable as far as downstream RIP routers are concerned. This is called “poisoning” the route. Poison reverse can be useful for propagating information about bad routes to routers that are downstream but not immediate neighbors, where split horizon is ineffective.

When this option is enabled, the router includes the route in announcements to the neighbor from which it was learned. When this option is disabled, the router omits the route in announcements to the neighbor from which it was learned.

Use the **set** form of this command to enable split-horizon poison-reverse on a RIP interface.

Use the **delete** form of this command to disable split-horizon poison-reverse on a RIP interface.

Use the **show** form of this command to display split-horizon poison-reverse configuration.

Chapter 7: ADSL Interfaces

This chapter describes commands for deploying RIP on ADSL interfaces.

This chapter presents the following topics:

- ADSL Interface RIP Commands

ADSL Interface RIP Commands

This chapter contains the following commands.

Configuration Commands	
ADSL with Classical IPOA Encapsulation	
interfaces adsl <adslx> pvc <pvc-id> classical-ipoa ip rip	Enables RIP on an ADSL PVC with Classical IPOA encapsulation.
interfaces adsl <adslx> pvc <pvc-id> classical-ipoa ip rip authentication	Specify RIP authentication for an ADSL PVC with Classical IPOA encapsulation.
interfaces adsl <adslx> pvc <pvc-id> classical-ipoa ip rip split-horizon <param>	Enables or disables split-horizon in RIP updates coming from an ADSL PVC with Classical IPOA encapsulation.
ADSL with PPPoA Encapsulation	
interfaces adsl <adslx> pvc <pvc-id> pppoa <num> ip rip	Enables RIP on an ADSL PVC with PPPoA encapsulation.
interfaces adsl <adslx> pvc <pvc-id> pppoa <num> ip rip authentication	Specify RIP authentication for an ADSL PVC with PPPoA encapsulation.
interfaces adsl <adslx> pvc <pvc-id> pppoa <num> ip rip split-horizon poison-reverse	Enables or disables split-horizon poison-reverse in RIP updates coming from an ADSL PVC with PPPoA encapsulation.
ADSL with PPPoE Encapsulation	
interfaces adsl <adslx> pvc <pvc-id> pppoe <num> ip rip	Enables RIP on an ADSL PVC with PPPoE encapsulation.
interfaces adsl <adslx> pvc <pvc-id> pppoe <num> ip rip authentication	Specify RIP authentication for an ADSL PVC with PPPoE encapsulation.
interfaces adsl <adslx> pvc <pvc-id> pppoe <num> ip rip split-horizon poison-reverse	Enables or disables split-horizon poison-reverse in RIP updates coming from an ADSL PVC with PPPoE encapsulation.
Operational Commands	
None.	

interfaces adsl <adslx> pvc <pvc-id> classical-ipoa ip rip

Enables RIP on an ADSL PVC with Classical IPOA encapsulation.

Syntax

set interfaces adsl *adslx* **pvc** *pvc-id* **classical-ipoa ip rip**

delete interfaces adsl *adslx* **pvc** *pvc-id* **classical-ipoa ip rip**

show interfaces adsl *adslx* **pvc** *pvc-id* **classical-ipoa ip rip**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   adsl adslx {
      pvc [0-255/0-65535|auto] {
         classical-ipoa {
            ip {
               rip
            }
         }
      }
   }
}
```

Parameters

adslx	Mandatory. Multi-node. The identifier for the ADSL interface you are defining. This may be **adsl0** to **adsl***x*, depending on what physical ADSL ports are actually available on the system.
pvc-id	Mandatory. The identifier for the PVC. It can either be the *vpi*/*vci* pair or the keyword **auto**, where *vpi* is a Virtual Path Index from 0 to 255, *vci* is a Virtual Circuit Index from from 0 to 65535, and **auto** directs the system to detect the Virtual Path Index and Virtual Circuit Index automatically.

Default

None.

Usage Guidelines

Use this command to enable Routing Information Protocol (RIP) on a PVC with Classical IP over Asynchronous Transfer Mode (IPOA) encapsulation on an ADSL interface.

Use the **set** form of this command to enable RIP on an interface.

Use the **delete** form of this command to remove all RIP configuration and disable RIP on the interface.

Use the **show** form of this command to display RIP configuration.

interfaces adsl <adslx> pvc <pvc-id> classical-ipoa ip rip authentication

Specify RIP authentication for an ADSL PVC with Classical IPOA encapsulation.

Syntax

set interfaces adsl *adslx* **pvc** *pvc-id* **classical-ipoa ip rip authentication** [**md5** *md5-key* **password** *md5-password* | **plaintext-password** *password*]

delete interfaces adsl *adslx* **pvc** *pvc-id* **classical-ipoa ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

show interfaces adsl *adslx* **pvc** *pvc-id* **classical-ipoa ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   adsl adslx {
      pvc [0-255/0-65535|auto] {
         classical-ipoa {
            ip {
               rip {
                  authentication {
                     md5 u32 {
                        password: text
                     }
                     plaintext-password: text
                  }
               }
            }
         }
      }
   }
}
```

Parameters

adslx	Mandatory. Multi-node. The identifier for the ADSL interface you are defining. This may be **adsl0** to **adsl***x*, depending on what physical ADSL ports are actually available on the system.
pvc-id	Mandatory. The identifier for the PVC. It can either be the *vpi*/*vci* pair or the keyword **auto**, where *vpi* is a Virtual Path Index from 0 to 255, *vci* is a Virtual Circuit Index from from 0 to 65535, and **auto** directs the system to detect the Virtual Path Index and Virtual Circuit Index automatically.
md5-key	Optional. The authentication key ID. This must be the same on both the sending and receiving systems. The range is 1 to 255.
md5-password	Optional. The password to use in MD5 authentication. This must be the same on both the sending and receiving systems.
password	Optional. The password to use in simple (plain-text) authentication. This must be the same on both the sending and receiving systems.

Default

None.

Usage Guidelines

Use this command to specify the authentication method to be used for RIP on a PVC with Classical IP over Asynchronous Transfer Mode (IPOA) encapsulation on an ADSL interface. This authentication is independent of the authentication configured for the RIP area.

In plain text authentication, passwords are sent through the network in plain text. In MD5 authentication, the system uses the Message Digest 5 (MD5) algorithm to compute a hash value from the contents of the RIP packet and the password. The hash value and the MD5 key are included in the transmitted packet, and the receiving system (configured with the same password) calculates its own hash function, which must match.

The authentication parameters must be the same for all routers that are to establish two-way communication within a network. If two routers do not agree on these parameters, they will not consider establish adjacencies, and will disregard one another’s communications.

Use the **set** form of this command to set RIP authentication for a PVC with Classical IPOA encapsulation on an ADSL interface.

Use the **delete** form of this command to remove RIP authentication configuration information.

Use the **show** form of this command to display RIP authentication configuration information.

interfaces adsl <adslx> pvc <pvc-id> classical-ipoa ip rip split-horizon <param>

Enables or disables split-horizon in RIP updates coming from an ADSL PVC with Classical IPOA encapsulation.

Syntax

set interfaces adsl *adslx* **pvc** *pvc-id* **classical-ipoa ip rip split-horizon poison-reverse**

delete interfaces adsl *adslx* **pvc** *pvc-id* **classical-ipoa ip rip split-horizon**

show interfaces adsl *adslx* **pvc** *pvc-id* **classical-ipoa ip rip split-horizon**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   adsl adslx {
      pvc [0-255/0-65535|auto] {
         classical-ipoa {
            ip {
               rip {
                  split-horizon {
                     poison-reverse
                  }
               }
            }
         }
      }
   }
}
```

Parameters

adslx	Mandatory. Multi-node. The identifier for the ADSL interface you are defining. This may be **adsl0** to **adsl***x*, depending on what physical ADSL ports are actually available on the system.

pvc-id	Mandatory. The identifier for the PVC. It can either be the *vpi*/*vci* pair or the keyword **auto**, where *vpi* is a Virtual Path Index from 0 to 255, *vci* is a Virtual Circuit Index from from 0 to 65535, and **auto** directs the system to detect the Virtual Path Index and Virtual Circuit Index automatically.

Default

None.

Usage Guidelines

Use this command to enable or disable split-horizon poison-reverse on a RIP interface.

Split-horizon is a stability feature that reduces the possibility of network loops, particularly in the case where links become disconnected. Enabling split-horizon stops an interface from including in its network updates any routes that it learned from that interface. Split horizon is effective at preventing loops between routers that are directly connected to one another, and speeds convergence when network conditions change.

Poison reverse is a variation of split horizon. When an interface with poison reverse enabled detects that a link is down, it increases the metric for that route to 16, and propagates that information in its next update. Since 15 is the largest number of hops considered reachable on a RIP network, increasing the metric to 16 renders the route unreachable as far as downstream RIP routers are concerned. This is called “poisoning” the route. Poison reverse can be useful for propagating information about bad routes to routers that are downstream but not immediate neighbors, where split horizon is ineffective.

When this option is enabled, the router includes the route in announcements to the neighbor from which it was learned. When this option is disabled, the router omits the route in announcements to the neighbor from which it was learned.

Use the **set** form of this command to enable split-horizon poison-reverse on a RIP interface.

Use the **delete** form of this command to disable split-horizon poison-reverse on a RIP interface.

Use the **show** form of this command to display split-horizon poison-reverse configuration.

interfaces adsl <adslx> pvc <pvc-id> pppoa <num> ip rip

Enables RIP on an ADSL PVC with PPPoA encapsulation.

Syntax

set interfaces adsl *adslx* **pvc** *pvc-id* **pppoa** *num* **ip rip**

delete interfaces adsl *adslx* **pvc** *pvc-id* **pppoa** *num* **ip rip**

show interfaces adsl *adslx* **pvc** *pvc-id* **pppoa** *num* **ip rip**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   adsl adslx {
      pvc [0-255/0-65535|auto] {
         pppoa 0-15 {
            ip {
               rip
            }
         }
      }
   }
}
```

Parameters

adslx	Mandatory. Multi-node. The identifier for the ADSL interface you are defining. This may be **adsl0** to **adsl***x*, depending on what physical ADSL ports are actually available on the system.
pvc-id	Mandatory. The identifier for the PVC. It can either be the *vpi*/*vci* pair or the keyword **auto**, where *vpi* is a Virtual Path Index from 0 to 255, *vci* is a Virtual Circuit Index from from 0 to 65535, and **auto** directs the system to detect the Virtual Path Index and Virtual Circuit Index automatically.
num	Mandatory. The PPPoA unit number. This number must be unique across all PPPoA interfaces. In addition, only one PPPoA instance can be configured on a PVC. PPPoA units range from 0 to 15 and the resulting interfaces are named **pppoa0** to **pppoa15**.

Default

None.

Usage Guidelines

Use this command to enable Routing Information Protocol (RIP) on a PVC with Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA) encapsulation on an ADSL interface.

Use the **set** form of this command to enable RIP on an interface.

Use the **delete** form of this command to remove all RIP configuration and disable RIP on the interface.

Use the **show** form of this command to display RIP configuration.

interfaces adsl <adslx> pvc <pvc-id> pppoa <num> ip rip authentication

Specify RIP authentication for an ADSL PVC with PPPoA encapsulation.

Syntax

set interfaces adsl *adslx* **pvc** *pvc-id* **pppoa** *num* **ip rip authentication** [**md5** *md5-key* **password** *md5-password* | **plaintext-password** *password*]

delete interfaces adsl *adslx* **pvc** *pvc-id* **pppoa** *num* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

show interfaces adsl *adslx* **pvc** *pvc-id* **pppoa** *num* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   adsl adslx {
      pvc [0-255/0-65535|auto] {
         pppoa 0-15 {
            ip {
               rip {
                  authentication {
                     md5 u32 {
                        password: text
                     }
                     plaintext-password: text
                  }
               }
            }
         }
      }
   }
}
```

Parameters

adslx	Mandatory. Multi-node. The identifier for the ADSL interface you are defining. This may be **adsl0** to **adsl***x*, depending on what physical ADSL ports are actually available on the system.
pvc-id	Mandatory. The identifier for the PVC. It can either be the *vpi*/*vci* pair or the keyword **auto**, where *vpi* is a Virtual Path Index from 0 to 255, *vci* is a Virtual Circuit Index from from 0 to 65535, and **auto** directs the system to detect the Virtual Path Index and Virtual Circuit Index automatically.
num	Mandatory. The PPPoA unit number. This number must be unique across all PPPoA interfaces. In addition, only one PPPoA instance can be configured on a PVC. PPPoA units range from 0 to 15 and the resulting interfaces are named **pppoa0** to **pppoa15**.
md5-key	Optional. The authentication key ID. This must be the same on both the sending and receiving systems. The range is 1 to 255.
md5-password	Optional. The password to use in MD5 authentication. This must be the same on both the sending and receiving systems.
password	Optional. The password to use in simple (plain-text) authentication. This must be the same on both the sending and receiving systems.

Default

None.

Usage Guidelines

Use this command to specify the authentication method to be used for RIP on a PVC with Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA) encapsulation on an ADSL interface. This authentication is independent of the authentication configured for the RIP area.

In plain text authentication, passwords are sent through the network in plain text. In MD5 authentication, the system uses the Message Digest 5 (MD5) algorithm to compute a hash value from the contents of the RIP packet and the password. The hash value and the MD5 key are included in the transmitted packet, and the receiving system (configured with the same password) calculates its own hash function, which must match.

The authentication parameters must be the same for all routers that are to establish two-way communication within a network. If two routers do not agree on these parameters, they will not consider establish adjacencies, and will disregard one another’s communications.

Use the **set** form of this command to set RIP authentication for a PVC with PPPoA encapsulation on an ADSL interface.

Use the **delete** form of this command to remove RIP authentication configuration information.

Use the **show** form of this command to display RIP authentication configuration information.

interfaces adsl <adslx> pvc <pvc-id> pppoa <num> ip rip split-horizon poison-reverse

Enables or disables split-horizon poison-reverse in RIP updates coming from an ADSL PVC with PPPoA encapsulation.

Syntax

set interfaces adsl *adslx* **pvc** *pvc-id* **pppoa** *num* **ip rip split-horizon poison-reverse**

delete interfaces adsl *adslx* **pvc** *pvc-id* **pppoa** *num* **ip rip split-horizon**

show interfaces adsl *adslx* **pvc** *pvc-id* **pppoa** *num* **ip rip split-horizon**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   adsl adslx {
      pvc [0-255/0-65535|auto] {
         pppoa 0-15 {
            ip {
               rip {
                  split-horizon {
                     poison-reverse
                  }
               }
            }
         }
      }
   }
}
```

Parameters

adslx	Mandatory. Multi-node. The identifier for the ADSL interface you are defining. This may be **adsl0** to **adsl***x*, depending on what physical ADSL ports are actually available on the system.

pvc-id	Mandatory. The identifier for the PVC. It can either be the *vpi*/*vci* pair or the keyword **auto**, where *vpi* is a Virtual Path Index from 0 to 255, *vci* is a Virtual Circuit Index from from 0 to 65535, and **auto** directs the system to detect the Virtual Path Index and Virtual Circuit Index automatically.
num	Mandatory. The PPPoA unit number. This number must be unique across all PPPoA interfaces. In addition, only one PPPoA instance can be configured on a PVC. PPPoA units range from 0 to 15 and the resulting interfaces are named **pppoa0** to **pppoa15**.

Default

None.

Usage Guidelines

Use this command to enable or disable split-horizon poison-reverse on an ADSL interface with Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA) encapsulation running RIP.

Split-horizon is a stability feature that reduces the possibility of network loops, particularly in the case where links become disconnected. Enabling split-horizon stops an interface from including in its network updates any routes that it learned from that interface. Split horizon is effective at preventing loops between routers that are directly connected to one another, and speeds convergence when network conditions change.

Poison reverse is a variation of split horizon. When an interface with poison reverse enabled detects that a link is down, it increases the metric for that route to 16, and propagates that information in its next update. Since 15 is the largest number of hops considered reachable on a RIP network, increasing the metric to 16 renders the route unreachable as far as downstream RIP routers are concerned. This is called “poisoning” the route. Poison reverse can be useful for propagating information about bad routes to routers that are downstream but not immediate neighbors, where split horizon is ineffective.

When this option is enabled, the router includes the route in announcements to the neighbor from which it was learned. When this option is disabled, the router omits the route in announcements to the neighbor from which it was learned.

Use the **set** form of this command to enable split-horizon poison-reverse on a RIP interface.

Use the **delete** form of this command to disable split-horizon poison-reverse on a RIP interface.

Use the **show** form of this command to display split-horizon poison-reverse configuration.

interfaces adsl <adslx> pvc <pvc-id> pppoe <num> ip rip

Enables RIP on an ADSL PVC with PPPoE encapsulation.

Syntax

set interfaces adsl *adslx* **pvc** *pvc-id* **pppoe** *num* **ip rip**

delete interfaces adsl *adslx* **pvc** *pvc-id* **pppoe** *num* **ip rip**

show interfaces adsl *adslx* **pvc** *pvc-id* **pppoe** *num* **ip rip**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   adsl adslx {
      pvc [0-255/0-65535|auto] {
         pppoe 0-15 {
            ip {
               rip
            }
         }
      }
   }
}
```

Parameters

adslx	Mandatory. Multi-node. The identifier for the ADSL interface you are defining. This may be **adsl0** to **adsl***x*, depending on what physical ADSL ports are actually available on the system.
pvc-id	Mandatory. The identifier for the PVC. It can either be the *vpi*/*vci* pair or the keyword **auto**, where *vpi* is a Virtual Path Index from 0 to 255, *vci* is a Virtual Circuit Index from from 0 to 65535, and **auto** directs the system to detect the Virtual Path Index and Virtual Circuit Index automatically.
num	Mandatory. The name of a defined PPPoE unit. The range of values is 0 to 15.

Default

None.

Usage Guidelines

Use this command to enable Routing Information Protocol (RIP) on a PVC with Point-to-Point Protocol over Ethernet (PPPoE) encapsulation on an ADSL interface.

Use the **set** form of this command to enable RIP on an interface.

Use the **delete** form of this command to remove all RIP configuration and disable RIP on the interface.

Use the **show** form of this command to display RIP configuration.

interfaces adsl <adslx> pvc <pvc-id> pppoe <num> ip rip authentication

Specify RIP authentication for an ADSL PVC with PPPoE encapsulation.

Syntax

set interfaces adsl *adslx* **pvc** *pvc-id* **pppoe** *num* **ip rip authentication** [**md5** *md5-key* **password** *md5-password* | **plaintext-password** *password*]

delete interfaces adsl *adslx* **pvc** *pvc-id* **pppoe** *num* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

show interfaces adsl *adslx* **pvc** *pvc-id* **pppoe** *num* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   adsl adslx {
      pvc [0-255/0-65535|auto] {
         pppoe 0-15 {
            ip {
               rip {
                  authentication {
                     md5 u32 {
                        password: text
                     }
                     plaintext-password: text
                  }
               }
            }
         }
      }
   }
}
```

Parameters

adslx	Mandatory. Multi-node. The identifier for the ADSL interface you are defining. This may be **adsl0** to **adsl***x*, depending on what physical ADSL ports are actually available on the system.
pvc-id	Mandatory. The identifier for the PVC. It can either be the *vpi*/*vci* pair or the keyword **auto**, where *vpi* is a Virtual Path Index from 0 to 255, *vci* is a Virtual Circuit Index from from 0 to 65535, and **auto** directs the system to detect the Virtual Path Index and Virtual Circuit Index automatically.
num	Mandatory. The name of a defined PPPoE unit. The range of values is 0 to 15.
md5-key	Optional. The authentication key ID. This must be the same on both the sending and receiving systems. The range is 1 to 255.
md5-password	Optional. The password to use in MD5 authentication. This must be the same on both the sending and receiving systems.
password	Optional. The password to use in simple (plain-text) authentication. This must be the same on both the sending and receiving systems.

Default

None.

Usage Guidelines

Use this command to specify the authentication method to be used for RIP on a PVC with Point-to-Point Protocol over Ethernet (PPPoE) encapsulation on an ADSL interface. This authentication is independent of the authentication configured for the RIP area.

In plain text authentication, passwords are sent through the network in plain text. In MD5 authentication, the system uses the Message Digest 5 (MD5) algorithm to compute a hash value from the contents of the RIP packet and the password. The hash value and the MD5 key are included in the transmitted packet, and the receiving system (configured with the same password) calculates its own hash function, which must match.

The authentication parameters must be the same for all routers that are to establish two-way communication within a network. If two routers do not agree on these parameters, they will not consider establish adjacencies, and will disregard one another’s communications.

Use the **set** form of this command to set RIP authentication for a PVC with PPPoE encapsulation on an ADSL interface.

Use the **delete** form of this command to remove RIP authentication configuration information.

Use the **show** form of this command to display RIP authentication configuration information.

interfaces adsl <adslx> pvc <pvc-id> pppoe <num> ip rip split-horizon poison-reverse

Enables or disables split-horizon poison-reverse in RIP updates coming from an ADSL PVC with PPPoE encapsulation.

Syntax

set interfaces adsl *adslx* **pvc** *pvc-id* **pppoe** *num* **ip rip split-horizon poison-reverse**

delete interfaces adsl *adslx* **pvc** *pvc-id* **pppoe** *num* **ip rip split-horizon**

show interfaces adsl *adslx* **pvc** *pvc-id* **pppoe** *num* **ip rip split-horizon**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   adsl adslx {
      pvc [0-255/0-65535|auto] {
         pppoe 0-15 {
            ip {
               rip {
                  split-horizon {
                     poison-reverse
                  }
               }
            }
         }
      }
   }
}
```

Parameters

adslx	Mandatory. Multi-node. The identifier for the ADSL interface you are defining. This may be **adsl0** to **adsl***x*, depending on what physical ADSL ports are actually available on the system.

pvc-id	Mandatory. The identifier for the PVC. It can either be the *vpi*/*vci* pair or the keyword **auto**, where *vpi* is a Virtual Path Index from 0 to 255, *vci* is a Virtual Circuit Index from from 0 to 65535, and **auto** directs the system to detect the Virtual Path Index and Virtual Circuit Index automatically.
num	Mandatory. The name of a defined PPPoE unit. The range of values is 0 to 15.

Default

None.

Usage Guidelines

Use this command to enable or disable split-horizon poison-reverse on a RIP interface.

Split-horizon is a stability feature that reduces the possibility of network loops, particularly in the case where links become disconnected. Enabling split-horizon stops an interface from including in its network updates any routes that it learned from that interface. Split horizon is effective at preventing loops between routers that are directly connected to one another, and speeds convergence when network conditions change.

Poison reverse is a variation of split horizon. When an interface with poison reverse enabled detects that a link is down, it increases the metric for that route to 16, and propagates that information in its next update. Since 15 is the largest number of hops considered reachable on a RIP network, increasing the metric to 16 renders the route unreachable as far as downstream RIP routers are concerned. This is called “poisoning” the route. Poison reverse can be useful for propagating information about bad routes to routers that are downstream but not immediate neighbors, where split horizon is ineffective.

When this option is enabled, the router includes the route in announcements to the neighbor from which it was learned. When this option is disabled, the router omits the route in announcements to the neighbor from which it was learned.

Use the **set** form of this command to enable split-horizon poison-reverse on a RIP interface.

Use the **delete** form of this command to disable split-horizon poison-reverse on a RIP interface.

Use the **show** form of this command to display split-horizon poison-reverse configuration.

Chapter 8: Multilink Interfaces

This chapter describes commands for deploying RIP on multilink interfaces.

This chapter presents the following topics:

- Multilink Interface RIP Commands

Multilink Interface RIP Commands

This chapter contains the following commands.

Configuration Commands	
interfaces multilink <mlx> ip rip	Enables RIP on a multilink interface.
interfaces multilink <mlx> ip rip authentication	Specifies authentication for RIP on a multilink interface.
interfaces multilink <mlx> ip rip split-horizon poison-reverse	Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.
Operational Commands	
None.	

interfaces multilink <mlx> ip rip

Enables RIP on a multilink interface.

Syntax

set interfaces multilink *mlx* **ip rip**

delete interfaces multilink *mlx* **ip rip**

show interfaces multilink *mlx* **ip rip**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   multilink ml0..ml23 {
      ip {
         rip {
      }
   }
}
```

Parameters

mlx	Mandatory. The identifier of the multilink bundle. You can create up to two multilink bundles. Supported values are **ml0** (“em ell zero”) through **ml23** (“em ell twenty-three”).

Default

None.

Usage Guidelines

Use this command to enable Routing Information Protocol (RIP) on a multilink interface.

Use the **set** form of this command to enable RIP on an interface.

Use the **delete** form of this command to remove all RIP configuration and disable RIP on the interface.

Use the **show** form of this command to display RIP configuration.

interfaces multilink <mlx> ip rip authentication

Specifies authentication for RIP on a multilink interface.

Syntax

set interfaces multilink *mlx* **ip rip authentication** [**md5** *md5-key* **password** *md5-password* | **plaintext-password** *password*]

delete interfaces multilink *mlx* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

show interfaces multilink *mlx* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   multilink ml0..ml23 {
      ip {
         rip {
            authentication {
               md5 u32 {
                  password: text
               }
               plaintext-password: text
            }
         }
      }
   }
}
```

Parameters

mlx	Mandatory. The identifier of the multilink bundle. You can create up to two multilink bundles. Supported values are **ml0** (“em ell zero”) through **ml23** (“em ell twenty-three”).
md5-key	Optional. The authentication key ID. This must be the same on both the sending and receiving systems. The range is 1 to 255.

md5-password	Optional. The password to use in MD5 authentication. This must be the same on both the sending and receiving systems.
password	Optional. The password to use in plain-text authentication. This must be eight characters or less and the same on both the sending and receiving systems.

Default

None.

Usage Guidelines

Use this command to specify the authentication method to be used for RIP on a multilink interface. This authentication is independent of the authentication configured for the RIP area.

In plain text authentication, passwords are sent through the network in plain text. In MD5 authentication, the system uses the Message Digest 5 (MD5) algorithm to compute a hash value from the contents of the RIP packet and the password. The hash value and the MD5 key are included in the transmitted packet, and the receiving system (configured with the same password) calculates its own hash function, which must match.

The authentication parameters must be the same for all routers that are to establish two-way communication within a network. If two routers do not agree on these parameters, they will not consider establish adjacencies, and will disregard one another's communications.

Use the **set** form of this command to set RIP authentication for a multilink interface.

Use the **delete** form of this command to remove RIP multilink interface authentication configuration information.

Use the **show** form of this command to display RIP multilink interface authentication configuration information.

interfaces multilink <mlx> ip rip split-horizon poison-reverse

Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.

Syntax

set interfaces multilink *mlx* **ip rip split-horizon poison-reverse**

delete interfaces multilink *mlx* **ip rip split-horizon**

show interfaces multilink *mlx* **ip rip split-horizon**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   multilink ml0..ml23 {
      ip {
         rip {
            split-horizon {
               poison-reverse
            }
         }
      }
   }
}
```

Parameters

mlx	Mandatory. The identifier of the multilink bundle. You can create up to two multilink bundles. Supported values are **ml0** (“em ell zero”) through **ml23** (“em ell twenty-three”).

Default

None.

Usage Guidelines

Use this command to enable or disable split-horizon poison-reverse on a RIP interface.

Split-horizon is a stability feature that reduces the possibility of network loops, particularly in the case where links become disconnected. Enabling split-horizon stops an interface from including in its network updates any routes that it learned from that interface. Split horizon is effective at preventing loops between routers that are directly connected to one another, and speeds convergence when network conditions change.

Poison reverse is a variation of split horizon. When an interface with poison reverse enabled detects that a link is down, it increases the metric for that route to 16, and propagates that information in its next update. Since 15 is the largest number of hops considered reachable on a RIP network, increasing the metric to 16 renders the route unreachable as far as downstream RIP routers are concerned. This is called “poisoning” the route. Poison reverse can be useful for propagating information about bad routes to routers that are downstream but not immediate neighbors, where split horizon is ineffective.

When this option is enabled, the router includes the route in announcements to the neighbor from which it was learned. When this option is disabled, the router omits the route in announcements to the neighbor from which it was learned.

Use the **set** form of this command to enable split-horizon poison-reverse on a RIP interface.

Use the **delete** form of this command to disable split-horizon poison-reverse on a RIP interface.

Use the **show** form of this command to display split-horizon poison-reverse configuration.

Chapter 9: Tunnel Interfaces

This chapter describes commands for deploying RIP on tunnel interfaces.

This chapter presents the following topics:

- Tunnel Interface RIP Commands

Tunnel Interface RIP Commands

This chapter contains the following commands.

Configuration Commands	
interfaces tunnel <tunx> ip rip	Enables RIP on a tunnel interface.
interfaces tunnel <tunx> ip rip authentication	Specifies authentication for RIP on a tunnel interface.
interfaces tunnel <tunx> ip rip split-horizon poison-reverse	Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.
Operational Commands	
None.	

interfaces tunnel <tunx> ip rip

Enables RIP on a tunnel interface.

Syntax

set interfaces tunnel *tunx* **ip rip**

delete interfaces tunnel *tunx* **ip rip**

show interfaces tunnel *tunx* **ip rip**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   tunnel tun0..tun9 {
      ip {
         rip {
      }
   }
}
```

Parameters

tunx	Mandatory. The name of the tunnel interface you are configuring. The range is **tun0** to **tun9**.

Default

None.

Usage Guidelines

Use this command to enable Routing Information Protocol (RIP) on a tunnel interface.

Use the **set** form of this command to enable RIP on an interface.

Use the **delete** form of this command to remove all RIP configuration and disable RIP on the interface.

Use the **show** form of this command to display RIP configuration.

interfaces tunnel <tunx> ip rip authentication

Specifies authentication for RIP on a tunnel interface.

Syntax

set interfaces tunnel *tunx* **ip rip authentication** [**md5** *md5-key* **password** *md5-password* | **plaintext-password** *password*]

delete interfaces tunnel *tunx* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

show interfaces tunnel *tunx* **ip rip authentication** [**md5** *md5-key* **password** | **plaintext-password**]

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   tunnel tun0..tun9 {
      ip {
         rip {
            authentication {
               md5 u32 {
                  password: text
               }
               plaintext-password: text
            }
         }
      }
   }
}
```

Parameters

tunx	Mandatory. The name of the tunnel interface you are configuring. The range is **tun0** to **tun9**.
md5-key	Optional. The authentication key ID. This must be the same on both the sending and receiving systems. The range is 1 to 255.

md5-password	Optional. The password to use in MD5 authentication. This must be the same on both the sending and receiving systems.
password	Optional. The password to use in plain-text authentication. This must be eight characters or less and the same on both the sending and receiving systems.

Default

None.

Usage Guidelines

Use this command to specify the authentication method to be used for RIP on a tunnel interface. This authentication is independent of the authentication configured for the RIP area.

In plain text authentication, passwords are sent through the network in plain text. In MD5 authentication, the system uses the Message Digest 5 (MD5) algorithm to compute a hash value from the contents of the RIP packet and the password. The hash value and the MD5 key are included in the transmitted packet, and the receiving system (configured with the same password) calculates its own hash function, which must match.

The authentication parameters must be the same for all routers that are to establish two-way communication within a network. If two routers do not agree on these parameters, they will not consider establish adjacencies, and will disregard one another's communications.

Use the **set** form of this command to set RIP authentication for a tunnel interface.

Use the **delete** form of this command to remove RIP tunnel interface authentication configuration information.

Use the **show** form of this command to display RIP tunnel interface authentication configuration information.

interfaces tunnel <tunx> ip rip split-horizon poison-reverse

Enables or disables split-horizon poison-reverse in RIP updates coming from this interface.

Syntax

set interfaces tunnel *tunx* **ip rip split-horizon poison-reverse**

delete interfaces tunnel *tunx* **ip rip split-horizon**

show interfaces tunnel *tunx* **ip rip split-horizon**

Command Mode

Configuration mode.

Configuration Statement

```
interfaces {
   tunnel tun0..tun9 {
      ip {
         rip {
            split-horizon {
               poison-reverse
            }
         }
      }
   }
}
```

Parameters

tunx	Mandatory. The name of the tunnel interface you are configuring. The range is **tun0** to **tun9**.

Default

None.

Usage Guidelines

Use this command to enable or disable split-horizon poison-reverse on a tunnel interface.

Split-horizon is a stability feature that reduces the possibility of network loops, particularly in the case where links become disconnected. Enabling split-horizon stops an interface from including in its network updates any routes that it learned from that interface. Split horizon is effective at preventing loops between routers that are directly connected to one another, and speeds convergence when network conditions change.

Poison reverse is a variation of split horizon. When an interface with poison reverse enabled detects that a link is down, it increases the metric for that route to 16, and propagates that information in its next update. Since 15 is the largest number of hops considered reachable on a RIP network, increasing the metric to 16 renders the route unreachable as far as downstream RIP routers are concerned. This is called “poisoning” the route. Poison reverse can be useful for propagating information about bad routes to routers that are downstream but not immediate neighbors, where split horizon is ineffective.

When this option is enabled, the router includes the route in announcements to the neighbor from which it was learned. When this option is disabled, the router omits the route in announcements to the neighbor from which it was learned.

Use the **set** form of this command to enable split-horizon poison-reverse on a RIP interface.

Use the **delete** form of this command to disable split-horizon poison-reverse on a RIP interface.

Use the **show** form of this command to display split-horizon poison-reverse configuration.

Glossary of Acronyms

ACL	access control list
ADSL	Asymmetric Digital Subscriber Line
AS	autonomous system
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BPDU	Bridge Protocol Data Unit
CA	certificate authority
CHAP	Challenge Handshake Authentication Protocol
CLI	command-line interface
DDNS	dynamic DNS
DHCP	Dynamic Host Configuration Protocol
DLCI	data-link connection identifier
DMI	desktop management interface
DMZ	demilitarized zone
DNS	Domain Name System
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
eBGP	external BGP
EGP	Exterior Gateway Protocol

ECMP	equal-cost multipath
ESP	Encapsulating Security Payload
FIB	Forwarding Information Base
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HDLC	High-Level Data Link Control
I/O	Input/Ouput
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGP	Interior Gateway Protocol
IPS	Intrusion Protection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPOA	IP over ATM
IPsec	IP security
IPv4	IP Version 4
IPv6	IP Version 6
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LACP	Link Aggregation Control Protocol
LAN	local area network
MAC	medium access control
MIB	Management Information Base
MLPPP	multilink PPP
MRRU	maximum received reconstructed unit
MTU	maximum transmission unit

NAT	Network Address Translation
ND	Neighbor Discovery
NIC	network interface card
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OSPFv2	OSPF Version 2
OSPFv3	OSPF Version 3
PAM	Pluggable Authentication Module
PAP	Password Authentication Protocol
PCI	peripheral component interconnect
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPPoA	PPP over ATM
PPPoE	PPP over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PVC	permanent virtual circuit
QoS	quality of service
RADIUS	Remote Authentication Dial-In User Service
RIB	Routing Information Base
RIP	Routing Information Protocol
RIPng	RIP next generation
Rx	receive
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SSH	Secure Shell
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus

TCP	Transmission Control Protocol
ToS	Type of Service
Tx	transmit
UDP	User Datagram Protocol
vif	virtual interface
VLAN	virtual LAN
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	wide area network