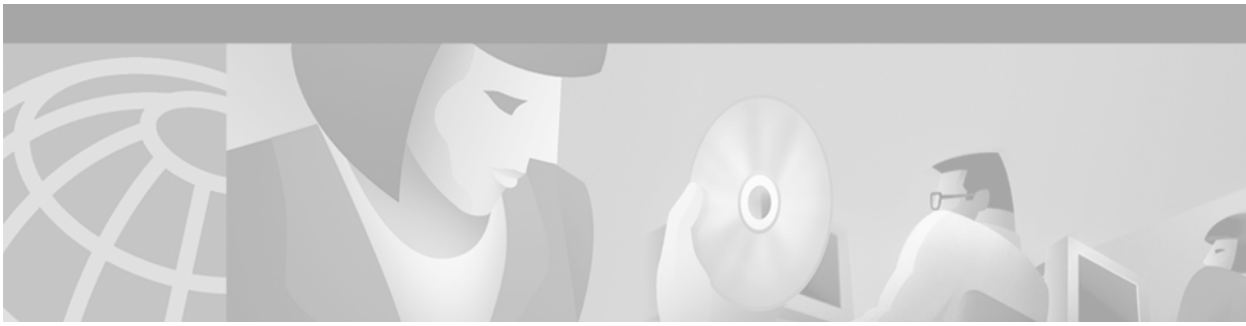


Configuring Routing Information Protocol

This chapter describes how to configure Routing Information Protocol (RIP). For a complete description of the RIP commands that appear in this chapter, refer to the "RIP Commands" chapter of the *Cisco IOS IP and IP Routing Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

RIP is a relatively old, but still commonly used, interior gateway protocol created for use in small, homogeneous networks. It is a classical distance-vector routing protocol. RIP is documented in RFC 1058.

RIP uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information. The Cisco IOS software sends routing information updates every 30 seconds, which is termed *advertising*. If a router does not receive an update from another router for 180 seconds or more, it marks the routes served by the nonupdating router as being unusable. If there is still no update after 240 seconds, the router removes all routing table entries for the nonupdating router.

The metric that RIP uses to rate the value of different routes is *hop count*. The hop count is the number of routers that can be traversed in a route. A directly connected network has a metric of zero; an unreachable network has a metric of 16. This small range of metrics makes RIP an unsuitable routing protocol for large networks.

A router that is running RIP can receive a default network via an update from another router that is running RIP, or the router can source (generate) the default network itself with RIP. In both cases, the default network is advertised through RIP to other RIP neighbors.

Cisco IOS software will source the default network with RIP if one of the following conditions is met:

- The **ip default-network** command is configured.
- The **default-information originate** command is configured.
- The default route is learned via another routing protocol or static route and then redistributed into RIP.

RIP sends updates to the interfaces in the specified networks. If the network of an interface network is not specified, it will not be advertised in any RIP update.

The Cisco implementation of RIP Version 2 supports plain text and MD5 authentication, route summarization, classless interdomain routing (CIDR), and variable-length subnet masks (VLSMs).

For protocol-independent features, which also apply to RIP, see the chapter "Configuring IP Routing Protocol-Independent Features" in this document.

RIP Configuration Task List

To configure RIP, perform the tasks in the following sections. You must enable RIP. The remaining tasks are optional.

- Enabling RIP (Required)
- Allowing Unicast Updates for RIP (Required)
- Applying Offsets to Routing Metrics (Optional)
- Adjusting Timers (Optional)
- Specifying a RIP Version (Optional)
- Enabling RIP Authentication (Optional)
- Configuring Route Summarization on an Interface (Optional)
- Verifying IP Route Summarization (Optional)
- Disabling Automatic Route Summarization (Optional)
- Running IGRP and RIP Concurrently (Optional)
- Disabling the Validation of Source IP Addresses (Optional)
- Enabling or Disabling Split Horizon (Optional)
- Configuring Interpacket Delay (Optional)
- Connecting RIP to a WAN (Optional)

For information about the following topics, see the "Configuring IP Routing Protocol-Independent Features" chapter:

- Filtering RIP information
- Key management (available in RIP Version 2)
- VLSM

Enabling RIP

To enable RIP, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# router rip`	Enable a RIP routing process, which places you in router configuration mode.
Step 2	`Router(config-router)# network` *network-number*	Associate a network with a RIP routing process.

Allowing Unicast Updates for RIP

Because RIP is normally a broadcast protocol, in order for RIP routing updates to reach nonbroadcast networks, you must configure the Cisco IOS software to permit this exchange of routing information. To do so, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor ip-address`	Defines a neighboring router with which to exchange routing information.

To control the set of interfaces with which you want to exchange routing updates, you can disable the sending of routing updates on specified interfaces by configuring the **passive-interface** command. See the discussion on filtering in the "Filter Routing Information" section in the "Configuring IP Routing Protocol-Independent Features" chapter.

Applying Offsets to Routing Metrics

An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via RIP. Optionally, you can limit the offset list with either an access list or an interface. To increase the value of routing metrics, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# offset-list [access-list-number | name] {in | out} offset [type number]`	Apply an offset to routing metrics.

Adjusting Timers

Routing protocols use several timers that determine such variables as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters. You can adjust these timers to tune routing protocol performance to better suit your internetwork needs. You can make the following timer adjustments:

- The rate (time in seconds between updates) at which routing updates are sent
- The interval of time (in seconds) after which a route is declared invalid
- The interval (in seconds) during which routing information regarding better paths is suppressed
- The amount of time (in seconds) that must pass before a route is removed from the routing table
- The amount of time for which routing updates will be postponed

It also is possible to tune the IP routing support in the software to enable faster convergence of the various IP routing algorithms, and, hence, quicker fallback to redundant routers. The total effect is to minimize disruptions to end users of the network in situations where quick recovery is essential.

To adjust the timers, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# timers basic update invalid holddown flush [sleeptime]`	Adjusts routing protocol timers.

Specifying a RIP Version

The Cisco implementation of RIP Version 2 supports authentication, key management, route summarization, CIDR, and VLSMs. Key management and VLSM are described in the chapter "Configuring IP Routing Protocol-Independent Features."

By default, the software receives RIP Version 1 and Version 2 packets, but sends only Version 1 packets. You can configure the software to receive and send only Version 1 packets. Alternatively, you can configure the software to receive and send only Version 2 packets. To configure the software to send and receive packets from only one version, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# version {1 | 2}`	Configures the software to receive and send only RIP Version 1 or only RIP Version 2 packets.

The preceding task controls the default behavior of RIP. You can override that behavior by configuring a particular interface to behave differently. To control which RIP version an interface sends, use one of the following commands, beginning in interface configuration mode

:

Command	Purpose
`Router(config-if)# ip rip send version 1`	Configures an interface to send only RIP Version 1 packets.
`Router(config-if)# ip rip send version 2`	Configures an interface to send only RIP Version 2 packets.
`Router(config-if)# ip rip send version 1 2`	Configures an interface to send RIP Version 1 and Version 2 packets.

Similarly, to control how packets received from an interface are processed, use one of the following commands in interface configuration mode:

Command	Purpose
`Router(config-if)# ip rip receive version 1`	Configures an interface to accept only RIP Version 1 packets.
`Router(config-if)# ip rip receive version 2`	Configures an interface to accept only RIP Version 2 packets.
`Router(config-if)# ip rip receive version 1 2`	Configures an interface to accept either RIP Version 1 or 2 packets.

Enabling RIP Authentication

RIP Version 1 does not support authentication. If you are sending and receiving RIP Version 2 packets, you can enable RIP authentication on an interface.

The key chain determines the set of keys that can be used on the interface. If a key chain is not configured, no authentication is performed on that interface, not even the default authentication. Therefore, you must also perform the tasks in the section "Manage Authentication Keys" in the "Configuring IP Routing Protocol-Independent Features" chapter.

We support two modes of authentication on an interface for which RIP authentication is enabled: plain text authentication and MD5 authentication. The default authentication in every RIP Version 2 packet is plain text authentication.

Note Do not use plain text authentication in RIP packets for security purposes, because the unencrypted authentication key is sent in every RIP Version 2 packet. Use plain text authentication when security is not an issue, for example, to ensure that misconfigured hosts do not participate in routing.

To configure RIP authentication, use the following commands in interface configuration mode:

	Command	Purpose
Step 1	`Router(config-if)# ip rip authentication key-chain name-of-chain`	Enables RIP authentication.
Step 2	`Router(config-if)# ip rip authentication mode {text | md5}`	Configures the interface to use MD5 digest authentication (or let it default to plain text authentication).

See the "Key Management Examples" section of the "Configuring IP Routing Protocol-Independent Features" chapter for key management information and examples.

RIP Route Summarization

Summarizing routes in RIP Version 2 improves scalability and efficiency in large networks. Summarizing IP addresses means that there is no entry for child routes (routes that are created for any combination of the individual IP addresses contained within a summary address) in the RIP routing table, reducing the size of the table and allowing the router to handle more routes.

Summary IP address functions more efficiently than multiple individually advertised IP routes, because:

- The summarized routes in the RIP database are processed first.
- Any associated child routes that are included in a summarized route are skipped as RIP looks through the routing database, reducing the processing time required.

Cisco routers can summarize routes in two ways:

- Automatically, by summarizing subprefixes to the classful network boundary when crossing classful network boundaries (autosummary)

Note You need not configure anything for autosummary to be enabled. To disable autosummary, use the **Router(config-router)# no auto-summary** command.

- As specifically configured, advertising a summarized local IP address pool on the specified interface, (on a network access server) so that the address pool can be provided to dialup clients

Autosummary addressing always summarizes to the classful address boundary, while the **ip summary-address** command summarizes addresses on a specified interface. If autosummary addressing is enabled, autosummarization is the default behavior for interfaces on the router not associated with dial-in clients (the "backbone"), with *or* without the **ip summary-address rip** interface subcommand present.

For example, if a local IP address pool of 10.1.1.1 to 10.1.1.254 is configured on the network access server, you could configure the **ip summary-address rip 10.1.1.0 255.255.255.0** command on the network access server port that provides addresses to dialup clients to cause the router to advertise 10.1.1.0/24 routes to dialup clients. Because a summary route is advertised, advertisement of the /32 host routes (installed when the dialup client connects) is suppressed so that the router does not advertise these routes to the network access server interface.

- Autosummary will override the configured summary-address feature on a given interface except when *both* of the following conditions are true:
- The configured interface summary-address and the IP address of the configured interface share the same major network (the classful, nonsubnetted portion of the IP address).
- Split horizon is not enabled on the interface.

Note If split horizon is enabled, neither an autosummary address nor the interface summary-address is advertised.

In the following example configuration, the major network is 10.0.0.0. The 10 in the address defines a Class A address space, allowing space for 0.x.x.x unique hosts where x defines unique bit positions in the addresses for these hosts. The summary of the major net defines the prefix as implied by the class (A, B, or C) of the address, without any network mask. The summary address 10.2.0.0 overrides the autosummary address of 10.0.0.0, 10.2.0.0 is advertised out interface E1, and 10.0.0.0 is not advertised.

```
int E1
ip address 10.1.1.1 255.255.255.0
ip summary-address rip 10.2.0.0 255.255.0.0
no ip split-horizon

router rip
network 10.0.0.0
```

When RIP determines that a summary address is required in the RIP database, a summary entry is created in the RIP routing database. As long as there are child routes for a summary address, the address remains in the routing database. When the last child route is removed, the summary entry also is removed from the database. This method of handling database entries reduces the number of entries in the database because each child route is not listed in an entry, and the aggregate entry itself is removed when there are no longer any valid child routes for it.

RIP version 2 route summarization requires that the lowest metric of the “best route” of an aggregated entry, or the lowest metric of all current child routes, be advertised. The best metric for aggregated summarized routes is calculated at route initialization or when there are metric modifications of specific routes at advertisement time, and not at the time the aggregated routes are advertised.

Restrictions to RIP Route Summarization

Supernet advertisement (advertising any network prefix less than its classful major network) is not allowed in RIP route summarization, other than advertising a supernet learned in the routing tables. Supernets learned on any interface that is subject to configuration are still learned. For example, the following summarization is invalid:

```
interface E1
..
ip summary-address rip 10.0.0.0 252.0.0.0 (invalid supernet summarization)
```

Each route summarization on an interface must have a unique major net, even if the subnet mask is unique. For example, the following is not permitted:

```
int E1
...
ip summary-address rip 10.1.0.0 255.255.0.0
ip summary-address rip 10.2.0.0 255.255.0.0 (or different mask)
```

Note The **ip summary-address eigrp** command uses other options that are not applicable to RIP. Do not confuse EIGRP summary-address with the new RIP command, **ip summary-address rip**.

Configuring Route Summarization on an Interface

The **ip summary-address rip** command causes the router to summarize a given set of routes learned via RIP version 2 or redistributed into RIP version 2. Host routes are especially applicable for summarization. To configure IP summary addressing, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface ethernet1`	Enters interface configuration mode.
Step 2	`Router(config-if)# ip summary-address rip` *ip_address ip_network_mask*	Specifies the IP address and network mask that identify the routes to be summarized.

See the "Route Summarization Examples" section at the end of this chapter for examples of using split horizon.

Verifying IP Route Summarization

You can verify which routes are summarized for an interface using the **show ip protocols** command. The following example shows potential summarizations and the associated interface summary-address/network mask for Ethernet interface 2:

```
router# show ip protocols
 Routing Protocol is "rip"
   Sending updates every 30 seconds, next due in 8 seconds
   Invalid after 180 seconds, hold down 180, flushed after 240
   Outgoing update filter list for all interfaces is
   Incoming update filter list for all interfaces is
   Redistributing: rip
   Default version control: send version 2, receive version 2
     Interface        Send  Recv  Triggered RIP  Key-chain
     Ethernet2        2     2
     Ethernet3        2     2
     Ethernet4        2     2
     Ethernet5        2     2
   Automatic network summarization is not in effect
   Address Summarization:
     12.11.0.0/16 for Ethernet2
```

You can check summary address entries in the RIP database. These entries will appear in the database only if there are relevant child routes being summarized. When the last child route for a summary address becomes invalid, the summary address is also removed from the routing table. The following example shows a summary address entry for route 12.11.0.0/16, with three child routes active:

```
router# show ip rip database
 11.0.0.0/8    auto-summary
 11.11.11.0/24    directly connected, Ethernet2
 12.0.0.0/8    auto-summary
 12.11.0.0/16    int-summary
 ^^^^^^^^^^^^^^^^^^^^^^^^^^^
 12.11.10.0/24    directly connected, Ethernet3
 12.11.11.0/24    directly connected, Ethernet4
12.11.12.0/24    directly connected, Ethernet5
```

Disabling Automatic Route Summarization

RIP Version 2 supports automatic route summarization by default. The software summarizes subprefixes to the classful network boundary when crossing classful network boundaries.

If you have disconnected subnets, disable automatic route summarization to advertise the subnets. When route summarization is disabled, the software sends subnet and host routing information across classful network boundaries. To disable automatic summarization, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# no auto-summary`	Disables automatic summarization.

Running IGRP and RIP Concurrently

It is possible to run IGRP and RIP concurrently. The IGRP information will override the RIP information by default because of the administrative distance of IGRP.

However, running IGRP and RIP concurrently does not work well when the network topology changes. Because IGRP and RIP have different update timers, and because they require different amounts of time to propagate routing updates, one part of the network will end up accepting and using IGRP routes and another part will end up accepting and using RIP routes. Running IGRP and RIP concurrently will result in routing loops. Even though these loops do not exist for very long, the time to live (TTL) value will quickly reach zero, and ICMP will send a “TTL exceeded” message. This message will cause most applications to stop attempting network connections.

Disabling the Validation of Source IP Addresses

By default, the software validates the source IP address of incoming RIP routing updates. If that source address is not valid, the software discards the routing update.

You might want to disable this feature if you have a router that is "off network" and you want to receive its updates. However, disabling this feature is not recommended under normal circumstances. To disable the default function that validates the source IP addresses of incoming routing updates, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# no validate-update-source`	Disables the validation of the source IP address of incoming RIP routing updates.

Enabling or Disabling Split Horizon

Normally, routers that are connected to broadcast-type IP networks and that use distance-vector routing protocols employ the *split horizon* mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router out of any interface from which that information originated. This behavior usually optimizes communications among multiple routers, particularly when links are broken. However, with nonbroadcast networks (such as Frame Relay and Switched Multimegabit Digital System (SMDS), situations can arise for which this behavior is less than ideal. For these situations, you might want to disable split horizon with IGRP and RIP.

If an interface is configured with secondary IP addresses and split horizon is enabled, updates might not be sourced by every secondary address. One routing update is sourced per network number unless split horizon is disabled.

To enable or disable split horizon, use one of the following commands beginning in interface configuration mode:

Command	Purposes
`Router(config-if)# ip split-horizon`	Enables split horizon.
`Router(config-if)# no ip split-horizon`	Disables split horizon.

Split horizon for Frame Relay and SMDS encapsulation is disabled by default. Split horizon is not disabled by default for interfaces using any of the X.25 encapsulations. For all other encapsulations, split horizon is enabled by default.

See the "Route Summarization Examples" section at the end of this chapter for examples of using split horizon.

Note In general, changing the state of the default is not recommended unless you are certain that your application requires making a change in order to advertise routes properly. Remember: If split horizon is disabled on a serial interface (and that interface is attached to a packet-switched network), you *must* disable split horizon for all routers in any relevant multicast groups on that network.

Configuring Interpacket Delay

By default, the software adds no delay between packets in a multiple-packet RIP update being sent. If you have a high-end router sending to a low-speed router, you might want to add such interpacket delay to RIP updates, in the range of 8 to 50 milliseconds. To do so, use the following command, beginning in router configuration mode:

Command	Purpose
`Router(config-router)# output-delay delay`	Add interpacket delay for RIP updates sent.

Connecting RIP to a WAN

Routers are used on connection-oriented networks to allow potential connectivity to many remote destinations. Circuits on the WAN are established on demand and are relinquished when the traffic subsides. Depending on the application, the connection between any two sites for user data could be short and relatively infrequent.

There are two problems using RIP to connect to a WAN:

- Periodic broadcasting by RIP generally prevented WAN circuits from being closed.
- Even on fixed, point-to-point links, the overhead of periodic RIP transmissions could seriously interrupt normal data transfer because of the quantity of information that hits the line every 30 seconds.

To overcome these limitations, triggered extensions to RIP cause RIP to send information on the WAN only when there has been an update to the routing database. Periodic update packets are suppressed over the interface on which this feature is enabled. RIP routing traffic is reduced on point-to-point, serial interfaces. Therefore, you can save money on an on-demand circuit for which you are charged for usage. Triggered extensions to RIP partially support RFC 2091, Triggered Extensions to RIP to Support Demand Circuits.

To enable triggered extensions to RIP, use the following commands in global configuration mode:

Command	Purpose
interface serial *number*	Configures a serial interface.
ip rip triggered	Enables triggered extensions to RIP.

To display the contents of the RIP private database, use the following command in EXEC mode:

Command	Purpose
show ip rip database [*prefix mask*]	Displays the contents of the RIP private database.

RIP Configuration Examples

This section provides the following RIP configuration examples:

- IP route summarization examples
- RIP split horizon configuration examples.

Route Summarization Examples

A correct (Example 1: Correct Configuration) and an incorrect (Example 2: Incorrect Configuration) configuration example of route summarization are provided.

Example 1: Correct Configuration

The following example shows how the **ip summary-address rip** command works with autosummary addressing in RIP, starting in global configuration mode. In the example, the major network is 10.0.0.0. The summary address 10.2.0.0 overrides the autosummary address of 10.0.0.0, so that 10.2.0.0 is advertised out interface e1 and 10.0.0.0 is not advertised.

Note If split horizon is enabled, neither autosummary nor interface summary addresses (those configured with the **ip summary-address rip** command) are advertised.

```
router rip
 network 10.0.0.0
 exit
interface ethernet1
 ip address 10.1.1.1 255.255.255.0
 ip summary-address rip 10.2.0.0 255.255.0.0
 no ip split-horizon
 exit
```

Example 2: Incorrect Configuration

The following example shows an illegal use of the **ip summary-address rip** command, because both addresses to be summarized have the same major network. Each route summarization on an interface must have a unique major network, whether or not the addresses have unique address masks.

```
interface ethernet1
...
ip summary-address rip 10.1.0.0 255.255.0.0
ip summary-address rip 10.2.0.0 255.255.255.0
```

Split Horizon Examples

Two examples of configuring split horizon are provided.

Example 1

The following configuration shows a simple example of disabling split horizon on a serial link. In this example, the serial link is connected to an X.25 network.

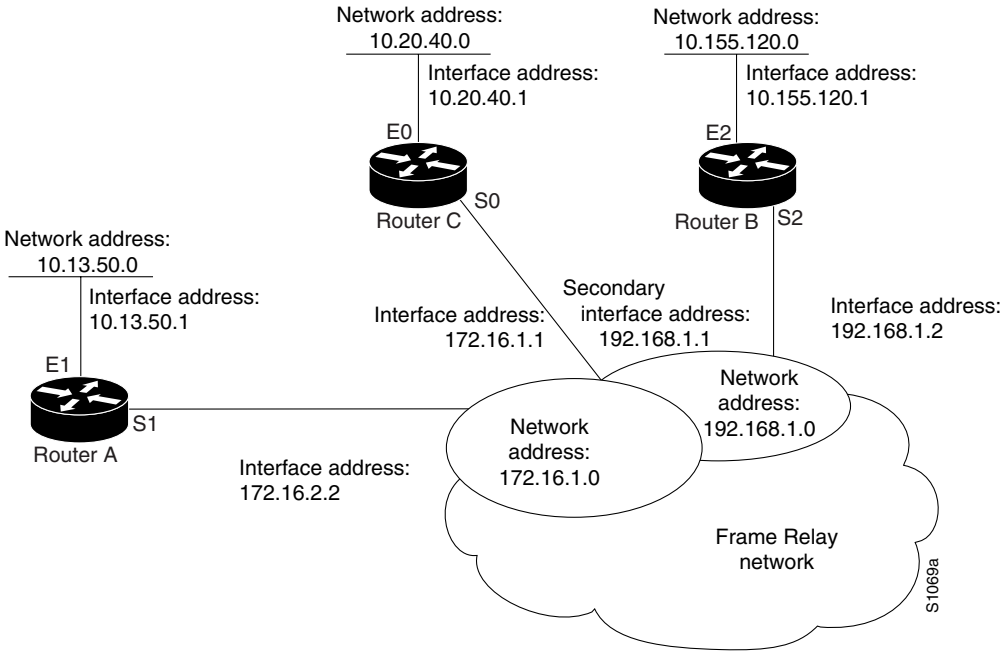
```
interface serial 0
encapsulation x25
no ip split-horizon
```

Example 2

In the next example, Figure 25 illustrates a typical situation in which the **no ip split-horizon** interface configuration command would be useful. This figure depicts two IP subnets that are both accessible via a serial interface on Router C (connected to Frame Relay network). In this example, the serial interface on Router C accommodates one of the subnets via the assignment of a secondary IP address.

The Ethernet interfaces for Router A, Router B, and Router C (connected to IP networks 10.13.50.0, 10.20.40.0, and 10.155.120.0, respectively, all have split horizon *enabled* by default, while the serial interfaces connected to networks 172.16.1.0 and 192.168.1.0 all have split horizon *disabled* with the **no ip split-horizon** command. Figure 25 shows the topology and interfaces.

Figure 25 Disabled Split Horizon Example for Frame Relay Network



In this example, split horizon is disabled on all serial interfaces. The split horizon must be disabled on Router C in order for network 172.16.0.0 to be advertised into network 192.168.0.0 and vice versa. These subnets overlap at Router C, interface S0. If split horizon were enabled on serial interface S0, it would not advertise a route back into the Frame Relay network for either of these networks.

Configuration for Router A

```
interface ethernet 1
 ip address 10.13.50.1
!
interface serial 1
 ip address 172.16.2.2
 encapsulation frame-relay
 no ip split-horizon
```

Configuration for Router B

```
interface ethernet 2
 ip address 10.155.120.1
!
interface serial 2
 ip address 192.168.1.2
 encapsulation frame-relay
 no ip split-horizon
```

Configuration for Router C

```
interface ethernet 0
 ip address 10.20.40.1
!
interface serial 0
 ip address 172.16.1.1
 ip address 192.168.1.1 secondary
 encapsulation frame-relay
 no ip split-horizon
```