

Concepts

This appendix contains information on the following topics:

- IP routing protocols
- Point-to-Point Protocol (PPP) authentication protocols
- Dialer profiles

Selecting IP Routing Protocols

The Cisco 805 router supports the following IP routing protocols:

- Routing Information Protocol (RIP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)

Table C-1 summarizes the characteristics of RIP and EIGRP. The following sections contain more details on RIP and EIGRP.

Selecting IP Routing Protocols

Table C-1 RIP and EIGRP Comparison

IP Routing Protocol	Ideal Topology	Metric	Routing Updates
RIP	Suited for topologies with 15 or fewer hops to reach a destination.	Hop count; maximum hop count is 15. Best route is one with lowest hop count.	By default, every 30 seconds. You can reconfigure this value and also use triggered extensions to RIP.
EIGRP	Suited for large topologies with 16 or more hops to reach a destination.	Distance information. Based on a successor, which is a neighboring router that has a least-cost path to a destination that is guaranteed not to be part of a routing loop.	Hello packets sent every 5 seconds plus incremental updates sent when the state of a destination changes.

Routing Information Protocol

RFC 1058 is the specification for RIP.

RIP is a distance-vector routing protocol, which means that it uses distance (hop count) as its metric for route selection. *Hop count* is the number of routers that a packet must traverse to reach its destination. For example, if a particular route has a hop count of 2, then a packet must traverse two routers to reach its destination. RIP selects routes based on the lowest hop count. For example, if two routes to the same destination exist and one route has 3 hops associated with it and the other has 2 hops, RIP selects the route with 2 hops. If multiple routes have the same hop count, RIP selects routes alternately. According to RIP, the maximum allowable hop count is 15.

By default, RIP routing updates are broadcast every 30 seconds. You can reconfigure the interval at which the routing updates are broadcast.

You can also configure triggered extensions to RIP so that routing updates are sent only when the routing data base is updated. For more information on triggered extensions to RIP, refer to the Cisco IOS documentation set. For information on accessing the documentation, see the “References to Cisco IOS Documentation Set” in “About this Guide.”

RIP supports load balancing. You can evenly distribute traffic among multiple routes to the same destination and that have the same metric. By default, the RIP routing table includes up to four equal routes.

Enhanced Interior Gateway Routing Protocol

EIGRP is an advanced Cisco-proprietary distance-vector routing protocol, which means it uses a metric more sophisticated than distance (hop count) for route selection. EIGRP uses a metric based on a successor, which is a neighboring router that has a least-cost path to a destination that is guaranteed to not be part of a routing loop. If a successor for a particular destination does not exist but neighbors advertise the destination, the router must recompute a route.

Each router running EIGRP sends hello packets every 5 seconds to notify neighboring routers that it is functioning. If a particular router does not send a hello packet within a prescribed period, EIGRP assumes that the state of a destination has changed and sends an incremental update.

Selecting PPP Authentication Protocol

The Cisco 805 router supports two PPP authentication protocols:

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

Table C-2 summarizes the characteristics of PAP and CHAP so that you can decide which protocol you want to use. The following sections contain more details on PAP and CHAP.

Note Cisco recommends using CHAP because it is the more secure of the two protocols.

PAP

Table C-2 PAP and CHAP Comparison

Authentication Protocol	Controls Authentication Attempt(s)	Handshake Method	Password	Protection from Playback or Repeated Attacks?
PAP	Remote office router (remote node)	Two-way. Remote office router sends username/password pair until corporate office router accepts.	Uses clear text password.	No.
CHAP	Corporate office router (local node)	Three-way. Corporate office router sends challenge to remote office router. Remote office router responds. Corporate office router accepts or rejects authentication.	Uses variable, unique, and unpredictable challenge value.	Yes, through the challenge variable and repeated challenges after the link has been established.

PAP

To understand how PAP works, imagine a network topology where a remote office router (Cisco 805 router) is connected to a corporate office router (such as a Cisco 3600 router). After the PPP link is established, the remote office router repeatedly sends a configured username and password until the corporate office router accepts the authentication.

PAP has the following characteristics:

- The password portion of the authentication is sent across the link in clear text (not scrambled or encrypted).
- PAP provides no protection from playback or repeated trial-and-error attacks.
- The remote office router controls the frequency and timing of the authentication attempts.

CHAP

To understand how CHAP works, imagine a network topology where a remote office router (Cisco 805 router) is connected to a corporate office router (such as a Cisco 3600 router). After the PPP link is established, the corporate office router sends a challenge message to the remote office router. The remote office router responds with a variable value. The corporate office router checks the response against its own calculation of the value. If the values match, the corporate office router accepts the authentication. The authentication process can be repeated any time after the link is established.

CHAP has the following characteristics:

- The authentication process uses a variable challenge value rather than a password.
- CHAP provides protection against playback attack through the use of the variable challenge value, which is unique and unpredictable. Repeated challenges limit the time of exposure to any single attack.

The corporate office router controls the frequency and timing of the authentication attempts.

Dialer Profiles

You can use *dialer profiles* to configure the router physical (serial) interface separately from the logical configuration required for a call. You can also configure the router to allow the logical and physical configurations to be dynamically bound together on a per-call basis. All calls going to or from a destination subnetwork use the same dialer profile.

A dialer profile consists of the following elements:

- A *dialer interface* (a logical entity) configuration with one or more dial strings, each used to reach a specific destination subnetwork.
- A *dialer map class* defining all the characteristics for any call to the specified dial string (telephone number). This element is optional; it is typically used to specify ISDN speeds. Because the Cisco 805 router has only a serial interface, the sample networks specify the call characteristics with the dialer interface configuration rather than defining a dialer map class.
- A *dialer pool* of physical interfaces to be used by the dialer interface. The physical interfaces in a dialer pool are ordered according to priority.

Dialer Interface

A *dialer interface* is a WAN interface on the router that is not connected to a remote device all the time but which dials the remote device whenever a connection is required.

Configuring an interface on a Cisco router to dial a specific remote device at specific times requires configuring dialer profiles.

A dialer interface configuration is a group of settings the router uses to connect to a remote network. One dialer interface can use multiple dial strings (telephone numbers). Each dial string is associated with its own dialer map class. The dialer map class defines all the characteristics for any call to the specified dial string. For example, the dialer map class for one destination might specify the amount of idle time as 3 seconds before calls are disconnected, and the map class for a different destination might specify 10 seconds.

Dialer Pool

Each dialer interface uses one group of physical interfaces called a *dialer pool*. One physical interface can belong to multiple dialer pools.

When you use dialer profiles to configure dial-on-demand routing (DDR), the physical interface is configured only for encapsulation and the dialer pools to which the interface belongs. All other characteristics used for making calls are defined in the dialer map.