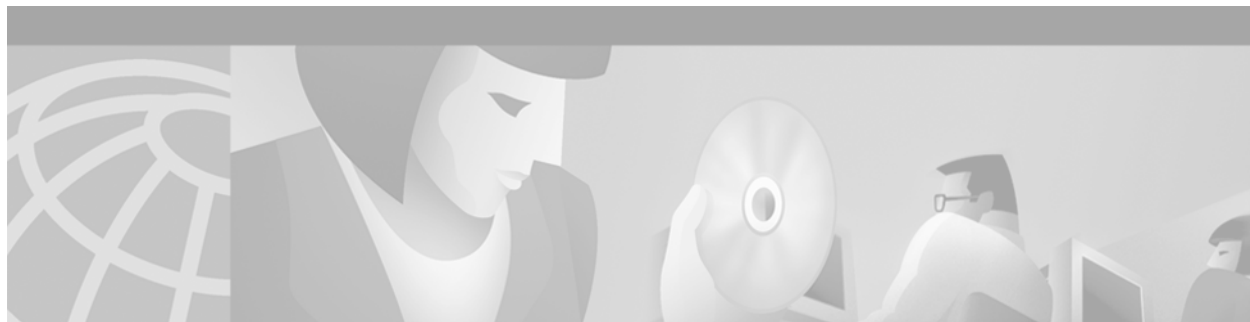




Neighbor Router Authentication: Overview and Guidelines

You can prevent your router from receiving fraudulent route updates by configuring neighbor router authentication.

This chapter describes neighbor router authentication as part of a total security plan. It describes what neighbor router authentication is, how it works, and why you should use it to increase your overall network security.

This chapter refers to neighbor router authentication as “neighbor authentication.” Neighbor router authentication is also sometimes called “route authentication.”

In This Chapter

This chapter describes the following topics:

- [About Neighbor Authentication](#)
- [How Neighbor Authentication Works](#)
- [Key Management \(Key Chains\)](#)
- [Finding Neighbor Authentication Configuration Information](#)

About Neighbor Authentication

This section contains the following sections:

- [Benefits of Neighbor Authentication](#)
- [Protocols That Use Neighbor Authentication](#)
- [When to Configure Neighbor Authentication](#)

Benefits of Neighbor Authentication

When configured, neighbor authentication occurs whenever routing updates are exchanged between neighbor routers. This authentication ensures that a router receives reliable routing information from a trusted source.

Without neighbor authentication, unauthorized or deliberately malicious routing updates could compromise the security of your network traffic. A security compromise could occur if an unfriendly party diverts or analyzes your network traffic. For example, an unauthorized router could send a fictitious routing update to convince your router to send traffic to an incorrect destination. This diverted traffic could be analyzed to learn confidential information of your organization, or merely used to disrupt your organization's ability to effectively communicate using the network.

Neighbor authentication prevents any such fraudulent route updates from being received by your router.

Protocols That Use Neighbor Authentication

Neighbor authentication can be configured for the following routing protocols:

- Border Gateway Protocol (BGP)
- DRP Server Agent
- Intermediate System-to-Intermediate System (IS-IS)
- IP Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)
- Routing Information Protocol (RIP) version 2

When to Configure Neighbor Authentication

You should configure any router for neighbor authentication if that router meets all of these conditions:

- The router uses any of the routing protocols previously mentioned.
- It is conceivable that the router might receive a false route update.
- If the router were to receive a false route update, your network might be compromised.
- If you configure a router for neighbor authentication, you also need to configure the neighbor router for neighbor authentication.

How Neighbor Authentication Works

When neighbor authentication has been configured on a router, the router authenticates the source of each routing update packet that it receives. This is accomplished by the exchange of an authenticating key (sometimes referred to as a password) that is known to both the sending and the receiving router.

There are two types of neighbor authentication used: plain text authentication and Message Digest Algorithm Version 5 (MD5) authentication. Both forms work in the same way, with the exception that MD5 sends a "message digest" instead of the authenticating key itself. The message digest is created using the key and a message, but the key itself is not sent, preventing it from being read while it is being transmitted. Plain text authentication sends the authenticating key itself over the wire.



Note

Note that plain text authentication is not recommended for use as part of your security strategy. Its primary use is to avoid accidental changes to the routing infrastructure. Using MD5 authentication, however, is a recommended security practice.

**Caution**

As with all keys, passwords, and other security secrets, it is imperative that you closely guard authenticating keys used in neighbor authentication. The security benefits of this feature are reliant upon your keeping all authenticating keys confidential. Also, when performing router management tasks via Simple Network Management Protocol (SNMP), do not ignore the risk associated with sending keys using non-encrypted SNMP.

This section includes the following sections:

- [Plain Text Authentication](#)
- [MD5 Authentication](#)

Plain Text Authentication

Each participating neighbor router must share an authenticating key. This key is specified at each router during configuration. Multiple keys can be specified with some protocols; each key must then be identified by a key number.

In general, when a routing update is sent, the following authentication sequence occurs:

-
- Step 1** A router sends a routing update with a key and the corresponding key number to the neighbor router. In protocols that can have only one key, the key number is always zero.
 - Step 2** The receiving (neighbor) router checks the received key against the same key stored in its own memory.
 - Step 3** If the two keys match, the receiving router accepts the routing update packet. If the two keys do not match, the routing update packet is rejected.

These protocols use plain text authentication:

- DRP Server Agent
 - IS-IS
 - OSPF
 - RIP version 2
-

MD5 Authentication

MD5 authentication works similarly to plain text authentication, except that the key is never sent over the wire. Instead, the router uses the MD5 algorithm to produce a “message digest” of the key (also called a “hash”). The message digest is then sent instead of the key itself. This ensures that nobody can eavesdrop on the line and learn keys during transmission.

These protocols use MD5 authentication:

- OSPF
- RIP version 2
- BGP
- IP Enhanced IGRP

Key Management (Key Chains)

You can configure key chains for these IP routing protocols:

- RIP version 2
- IP Enhanced IGRP
- DRP Server Agent

These routing protocols offer the additional function of managing keys by using key chains. When you configure a key chain, you specify a series of keys with lifetimes, and the Cisco IOS software rotates through each of these keys. This decreases the likelihood that keys will be compromised.

Each key definition within the key chain must specify a time interval for which that key will be activated (its “lifetime”). Then, during a given key’s lifetime, routing update packets are sent with this activated key. Keys cannot be used during time periods for which they are not activated. Therefore, it is recommended that for a given key chain, key activation times overlap to avoid any period of time for which no key is activated. If a time period occurs during which no key is activated, neighbor authentication cannot occur, and therefore routing updates will fail.

Multiple key chains can be specified.

Note that the router needs to know the time to be able to rotate through keys in synchronization with the other participating routers, so that all routers are using the same key at the same moment. Refer to the Network Time Protocol (NTP) and calendar commands in the “Performing Basic System Management” chapter of the *Cisco IOS Configuration Fundamentals Configuration Guide* for information about configuring time at your router.

Finding Neighbor Authentication Configuration Information

To find complete configuration information for neighbor authentication, refer to the appropriate section and chapter in the *Cisco IOS IP Configuration Guide* as listed in [Table 29](#).

Table 29 Location of Neighbor Authentication Information for Each Supported Protocol

Protocol	Chapter	Section
BGP	“Configuring BGP”	“Configuring Neighbor Options”
DRP Server Agent	“Configuring IP Services”	“Configuring a DRP Server Agent”
IP Enhanced IGRP	“Configuring IP Enhanced IGRP”	“Configuring Enhanced IGRP Route Authentication”
IS-IS	“Configuring Integrated IS-IS”	“Assigning a Password for an Interface” and “Configuring IS-IS Authentication Passwords”
OSPF	“Configuring OSPF”	“Configuring OSPF Interface Parameters” and “Configuring OSPF Area Parameters” and “Creating Virtual Links”
RIP version 2	“Configuring RIP”	“Enabling RIP Authentication”

To find complete configuration information for key chains, refer to the “Managing Authentication Keys” section in the chapter “Configuring IP Routing Protocol-Independent Features” of the *Cisco IOS IP Configuration Guide*.

