Cisco Systems

Designing Network Security

Second Edition

A practical guide to creating a secure network infrastructure

ciscopress.com

Merike Kaeo, CCIE® No. 1287

Designing Network Security

Second Edition

Merike Kaeo

Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

each router uses this information to modify its routing tables. Routers use the following four primary mechanisms to create and modify their routing tables:

- **Direct connection**—Any network connection to which the router is directly connected is automatically added to the routing table. Of course, the link must be up.
- **Static routing**—Manual entries can be configured on routers to instruct the router to use a given route to get to a particular destination.
- **Dynamic routing**—Router messages are announced and received. These update messages are used to create routes in the routing table. The routing algorithm associated with a particular routing protocol determines the optimal path to a particular destination and updates the route table. It can automatically adapt to changes in the network.
- **Default routing**—A manually entered route is used as a last-resort method to reach a destination when the route is not known by any other routing mechanism.

NOTE If a routing table has routes from multiple sources, such as static routes and some dynamic routing protocol routes, there is always a hierarchy of preference defining which route is more preferable if there are two ways to reach a destination. The order of preference can vary depending on router manufacturer, and the order is user configurable. As a default, static routes typically always take precedence over any other routes.

Routing Protocol Classification

Routing protocols can be classified into two separate groups: interior and exterior routing protocols. An Interior Gateway Protocol (IGP) is used for exchanging routing information between gateways within an autonomous system. An Exterior Gateway Protocol (EGP) is used for exchanging routing information between different autonomous systems.

In large nationwide corporate networks such as financial institutions or government facilities, it is very unlikely that a single routing protocol will be used for the whole network. Rather, the network will be organized as a collection of autonomous systems. An *autonomous system* is a group of networking components that will in general be administered by a single entity, or at least will have some reasonable degree of technical and administrative control. Each autonomous system will have its own routing technology. This may well differ for different autonomous systems. The routing protocol used within an autonomous system is referred to as an IGP. A separate protocol is usually used to interface among the autonomous systems.

Interior Gateway Protocols

The four most common routing protocols used as IGPs are as follows:

- **Routing Information Protocol (RIP)**—RIP is a distance vector–based IGP. It maintains a list of distances to other networks measured in *hops*, the number of routers a packet must traverse to reach its destination. It has a maximum hop limitation of 15 hops, which only makes it suitable for smaller-scale networks. Routing updates are broadcast every 30 seconds to all neighboring RIP neighbors. In RIPv1, each update is a full routing table. RIPv2 added many enhancements, including triggered updates and authentication.
- **Enhanced Interior Gateway Routing Protocol (EIGRP)**—EIGRP is a proprietary Cisco IGP. It maintains a complex set of metrics to determine the distance to other networks. It integrates the capabilities of link-state protocols into distance vector protocols and saves not only the least-cost route but up to eight routes to a destination. EIGRP updates are sent only upon a network topology change; updates are not periodic.
- **Open Shortest Past First (OSPF)**—OSPF is a link-state IGP. It uses a link speed-based metric to determine paths to other networks. Each router maintains a simplified map of the entire network. Updates are sent via multicast and are sent only when the network configuration changes. Each update only includes changes to the network.
- **Intermediate System-to-Intermediate System (IS-IS)**—IS-IS is similar to OSPF and is also a link-state IGP. Instead of an area concept like OSPF, IS-IS has two levels: level 1 (areas) and level 2 (backbones). The IS-IS backbone is just a contiguous collection of level 2-capable routers linking level 1 areas together. Most networks use level 2 only because there is little benefit in the extra complexity that running both level 1 and level 2 offers. IS-IS does not use IP for transport; it uses Connectionless Network Service (CLNS). This could make IS-IS harder to attack because CLNS is rarely routed across the Internet.

The decision of which IGP to use depends significantly on both the customer's experience with and the technical capabilities of the routing protocols. Engineers with more experience with IS-IS will always choose IS-IS. Engineers with a strong background in OSPF will always choose OSPF. The rule of thumb seems to be that beginners to interior routing choose RIP or EIGRP because it is easier to get started. However, OSPF is a better choice because it forces good IGP design to ensure that the network will scale. Those who are very experienced tend to choose IS-IS because it allows for better scaling with more configuration options than the other IGPs.

Exterior Gateway Protocols

The Border Gateway Protocol version 4 (BGP-4) is a distance vector–based EGP. It employs a set of sophisticated rules to maintain paths to other networks. Updates are sent over TCP connections between specifically identified peers. BGP-4 supports route aggregation to support very large network. (Most of the Internet core deploys BGP-4.) A large enterprise network comprised of multiple autonomous systems should look at deploying BGP-4 in its backbones.

Routing Protocol Security

The kind of damage that can be done in an unsecured routing infrastructure is discussed in more detail in Chapter 5, "Threats in an Enterprise Network." This chapter focuses on what security mechanisms are available to secure routing updates. Of course, it goes hand-in-hand in protecting the physical routers themselves.

A major concern is to avoid false routing update packets that falsely modify routing tables. Often, this is due more to misconfiguration rather than malicious intent. Two basic approaches for protecting routing table integrity are as follows:

- **Use only static routes**—This works for very small networks but will become an administrative nightmare for networks with more than 5 to 10 entries.
- **Authenticate routing updates**—All dynamic routing protocols have mechanisms to provide some sort of route authentication (that is, ensuring that router updates came from legitimate sources).

NOTE Currently, there is not a good way to ensure that the routing updates included from the legitimate source were updates the source was authorized to send. This is a difficult problem and still under research in the routing community.

Authenticating Routing Protocol Updates

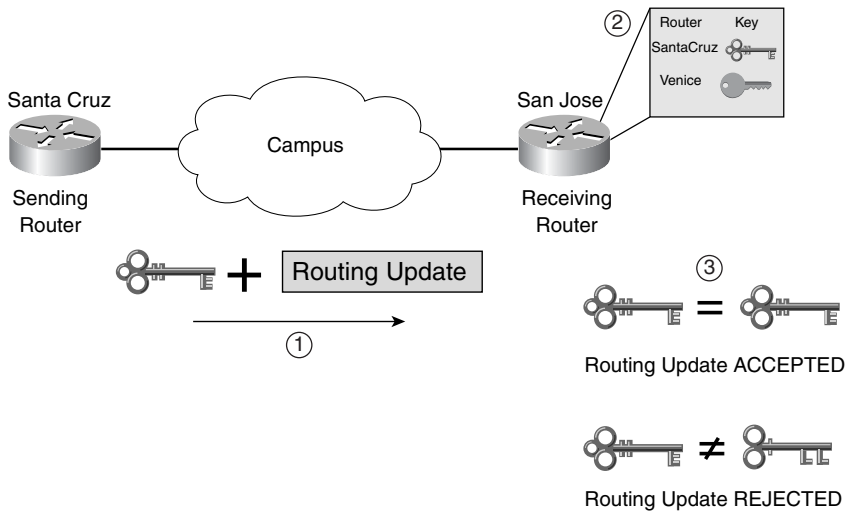
Most routing protocols incorporate neighbor authentication to protect the integrity of the routing domain. Authentication occurs when two neighboring routers exchange routing information and ensures that the receiving router incorporates into its tables only the route information that the trusted sending neighbor really intends to send. Authentication prevents a legitimate router from accepting and then using unauthorized, malicious, or corrupted routing updates that may compromise the security or availability of the network (for example, having an unauthorized device send a routing update that makes the legitimate router believe that the best route for certain traffic is via an alternative path that may or may not exist). Such a compromise would lead to rerouting of traffic, a denial of service, or just giving access to certain packets of data to an unauthorized person.

When neighbor authentication is configured, the router authenticates the source of each routing update packet it receives. This is accomplished by the exchange of an authentication key (sometimes referred to as a *shared secret*) that is known to both the sending and the receiving routers. Two types of neighbor authentication are typically used: plaintext authentication and cryptographic authentication (typically using the keyed Message Digest 5 [MD5] checksum that was discussed in Chapter 2, "Security Technologies").

Plaintext Authentication

Each participating router must share an authentication key. This key must be specified in each router's configuration. Multiple keys can be specified with some protocols; each key must be identified with a key number. Figure 4-1 illustrates how plaintext authentication is used for routing updates.

Figure 4-1 *Plaintext Neighbor Authentication*



The following steps are carried out:

Step 1 A router sends a routing update with a key and the corresponding key number to the neighbor router. For protocols that can have only one key, the key number is always zero.

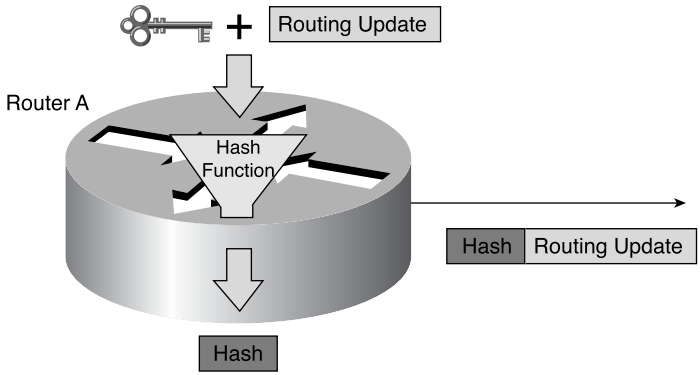
Step 2 The receiving (neighbor) router checks the received key against the same key stored in its own memory.

Step 3 If the two keys match, the receiving router accepts the routing update and incorporates the route information into its routing tables. If the two keys do not match, the routing update is rejected.

MD5 Authentication

MD5 authentication works similarly to plaintext authentication, except that the key is never sent over the wire. Instead, the router uses the combination of a shared secret key and the routing update as input to the MD5 algorithm to produce a message digest (also called a *hash*). The shared secret between the sending and receiving routers must typically be manually preconfigured. Figure 4-2 illustrates the sequence of events involved for routing protocol authentication for the originating router.

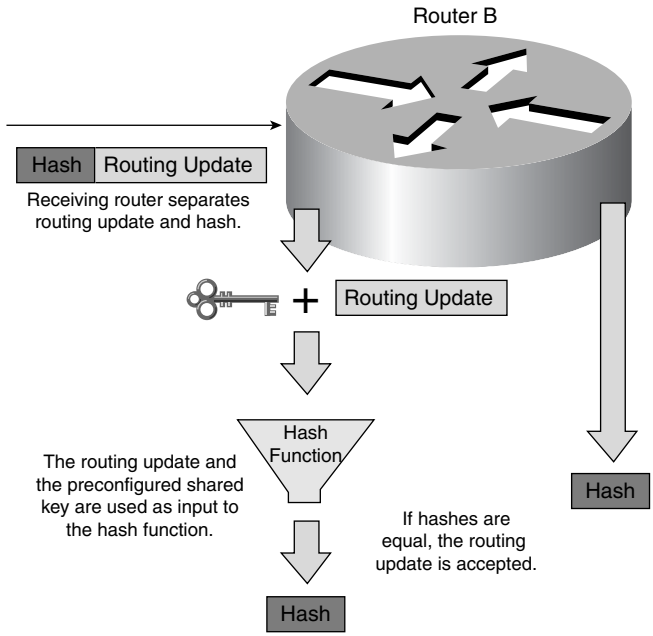
Figure 4-2 *MD5 Neighbor Authentication: Originating Router*



The preconfigured shared secret and the routing update are the input to the MD5 algorithm, which results in a message digest (hash). This message digest is appended to the routing update packet and sent out the appropriate interface.

Figure 4-3 illustrates the sequence of events for routing protocol authentication at the destination router.

Figure 4-3 *MD5 Neighbor Authentication: Destination Router*



The receiving router takes the routing update and, along with its preconfigured shared secret, uses this as input to the MD5 algorithm to produce a message digest. If this new digest matches the one that was received, the neighbor is authenticated and the routing update is incorporated into the router's routing table.

NOTE Plaintext authentication is not recommended for use as part of your security strategy. Its primary use is to avoid accidental changes to the routing infrastructure. Keyed MD5 is a more robust authentication mechanism and should be used wherever possible.

IPsec and Routing Protocols

It is possible to use IPsec to protect your routing protocol infrastructure. This would give the added benefits of confidentiality and replay protection. In most cases, the overhead involved in configuring IPsec for routing protocols far outweighs any practical benefits. It is more important that no one sends or spoofs routing updates. Therefore, IPsec is not commonly used to further protect routing updates because all routing protocols have extensions built in to address the authentication piece.

It is widely thought that in current routing infrastructures, confidentiality is not a major issue; and in all routing protocols themselves, there have been no extensions provided for confidentiality. As noted later in this chapter, however, some routing protocols that have working documents for IPv6 specify using IPsec as their inherent security mechanism.

Routing Protocol Security Details

Although all routing protocols generally implement neighbor authentication in a similar manner, there are some differences in each. This section provides more detail on each routing protocol, first describing an overview of the protocol and then detailing how the neighbor authentication is incorporated into each protocol. In addition, it describes the current work in progress for any additional security functionality for the various routing protocols, if it exists. The reader is encouraged to track these ongoing efforts in the particular working groups in the routing area of the Internet Engineering Task Force (IETF), which is located at http://ietf.org/html.charters/wg-dir.html.

RIP

Some people think that RIP is obsolete, given that other IGPs are more robust and flexible. However, RIP does have some advantages over newer IGP routing protocols such as OSPF, IS-IS, and EIGRP. Primarily, in a small network, RIP has very little overhead in terms of bandwidth used and configuration and management time. RIP is also very easy to