a hop-count value. When a new network enters the topology, RIP sends a new, updated routing message to the router. When the router gets the updated destination network address, it changes its router table.

RIP is limited in that it allows only 15 hops in the path from source to destination. If a 16th hop is required, the network destination is then indicated as unreachable. The routing protocols OSPF (Open Shortest Path First) and IS-IS (Intermediate System to Intermediate System) can be used when RIP is not practical. OSPF is a link-state routing protocol used to manage router information based on the state (i.e., speed, bandwidth, congestion, and distance) of the various links between the source and destination. IS-IS is a link-state routing protocol that converges faster, supports much larger internetworks, and is less susceptible to routing loops than OSPF.

**Router Vulnerabilities**

The following common router vulnerabilities are likely avenues for attack:

- **HTTP authentication vulnerability**: With the aid of \[\text{http://router.address/level/$\text{NUMBER}$/exec/...}\], where $\text{NUMBER}$ is an integer between 16 and 99, it is possible for a remote user to gain full administrative access to a router.

- **NTP vulnerability**: By sending a crafted NTP control packet, it is possible to trigger a buffer overflow in the NTP daemon.

- **SNMP parsing vulnerability**: Malformed SNMP messages received by affected systems can cause various parsing and processing functions to fail, which results in a system crash and reloading. In some cases, access-list statements on the SNMP service do not protect the device.

**Router Attacks**

An intruder that takes control of a router can perform many different attacks on a network. They can gain knowledge of all possible vulnerabilities in a network once the router has been accessed.

An attacker who has gained access to a router can interrupt communication, disable the router, stop communication between compromised networks, as well as observe and record logs on both incoming and outgoing traffic. By compromising a router, attackers can avoid firewalls and intrusion detection systems (IDS), and can transmit any kind of traffic to a chosen network.

**Types of Router Attacks**

There are many types of router attacks. The following are the most common:

- Denial-of-service attacks
- Packet-mistreating attacks
- Routing table poisoning
- Hit-and-run attacks
- Persistent attacks

**Denial-Of-Service (DoS) Attacks**

A denial-of-service (DoS) attack renders a router unusable for network traffic by overloading the router’s resources so that no one can access it. An attacker that cannot gain access to a router can simply crash it by sending the router more packets than it can handle. A DoS attack is carried out with the following three goals:

- **Destruction**: These attacks damage the ability of the router to operate.
- **Resource utilization**: These attacks are achieved by overflowing the router with numerous requests to open connections at the same time.
- **Bandwidth consumption**: These attacks utilize the bandwidth capacity of a router’s network. An attacker who has successfully carried out a DoS attack can then modify configuration information and carry out an attack on any network the router is connected to.