logging features available on many routers, the administrator can characterize the nature of the traffic and determine the input link on which the attack is arriving. The administrator then moves on to the upstream router.

The administrator repeats the diagnostic procedure on this upstream router, and continues to trace backward, hop-by-hop, until the source of the attack is found inside the ISP’s administrative domain of control (such as the IP address of another customer of the ISP) or, more likely, until the entry point of the attack into the ISP’s network is identified. The entry point is typically an input link on a router that borders another provider’s network. Once the entry point into the ISP’s network is identified, the bordering provider carrying the attack traffic must be notified and asked to continue the hop-by-hop traceback. Unfortunately, there often is little or no economic incentive for such cooperation between ISPs.

**Limitations of Hop-by-Hop IP Traceback**

Hop-by-hop IP traceback has several limitations, such as the following:

- Traceback to the origin of an attack fails if cooperation is not provided at every hop or if a router along the way lacks sufficient diagnostic capabilities or resources.
- If the attack stops before the trace is completed, the trace fails.
- Hop-by-hop traceback is a labor-intensive, technical process, and since attack packets often cross administrative, jurisdictional, and national boundaries, cooperation can be difficult to obtain.
- Partial traceback can be useful, since packet filters can be put in place to limit the DoS flood.
- How anomalous the attack packets are and how well they can be characterized determines how restrictive the filters have to be.
- Overly restrictive filters can contribute to the negative effects of a DoS attack.

Hop-by-hop traceback can be considered to be the baseline from which all proposed improvements in tracking and tracing are judged. It is the most basic method for tracing large packet flows with spoofed source addresses, but it has many limitations and drawbacks. DDoS attacks are difficult, if not impossible, to trace via this process, since there are multiple sources of attack packets, multiple paths through the Internet, and a relatively small number of packets coming from each source.

**Backscatter Traceback**

Backscatter traceback is a technique for tracing a flood of packets that are targeting the victim of a DDoS attack. The backscatter traceback technique relies entirely on the standard characteristics of existing Internet routing protocols, and although some special router configurations are used, there is no custom modification of protocols or equipment that is outside of current Internet standards.

In a typical DDoS attack, a victim’s system is put out of service by a flood of malicious attack packets originating from a large number of zombie machines compromised by the attacker. The destination address field of each attack packet contains the IP address of the victim. The source IP address of each packet is typically spoofed. In contemporary DDoS attacks, the spoofed source address is typically chosen at random from the universe of all possible IP addresses.

**How the Backscatter Traceback Works**

1. *The attack is reported to an ISP:* The victim of a DDoS attack reports the problem to his or her ISP. The flood of attack packets has made the victim’s Internet connection unusable, putting the victim out of service.

2. *The ISP configures all of its routers to reject all packets destined for the victim:* The ISP uses a standard routing control protocol to quickly configure all of its routers to reject packets that are targeted to the victim. By rejecting all packets that have the source address of the victim, benign packets carrying legitimate traffic will also be lost; however, the overwhelming number of packets heading for the victim will be attack packets. If the technique is successful, the total blockade of packets destined for the victim will only be in place for a short period of time.

3. *Rejected packets are “returned to sender”:* When a router rejects a packet with the destination address of the victim, it sends an Internet Control Message Protocol (ICMP) “destination unreachable” error message packet back to the source IP address contained in the rejected packet. While some of the “return to sender” ICMP error messages will be sent to legitimate users whose benign packets have been rejected along with the malicious ones, most of the packets destined for the victim are malicious attack packets.