Each ICMP “return to sender” error message packet contains, in its source IP address field, the address of the router (controlled and configured by the ISP) that rejected the packet heading for the victim. The router is also the machine that is generating the ICMP message. In its destination IP address field, the ICMP “return to sender” error message packet contains the source IP address found in the rejected packet that had been heading for the victim. These ICMP error packets are the “backscatter” or “noise” that enables the ISP to trace the attack packets back to their ingress point into the ISP’s network.

4. **The ISP configures all of its routers to route for capture, or blackhole, many of the ICMP error packets (the backscatter) with illegitimate destination IP addresses:** The Internet Address Naming Authority (IANA) has yet to allocate several large blocks of IP addresses for global routing. No one should ever see a legitimate packet containing an IP source address from this unallocated address space entering a domain from an external network. The next step in backscatter traceback is for an ISP to select a large range of IP addresses unallocated by IANA and to configure all of the ISP’s routers to send packets destined for these invalid addresses to a specific blackhole machine for analysis. The centermost region in Figure 5-4 represents the fraction of the overall packets arriving at an ISP’s router that are blackholed for analysis. Since packets with these invalid destination addresses cannot have been routed into the ISP’s network from an external source, these packets can only be some of the ICMP “destination unreachable” error message packets generated internally by the ISP’s routers, which have been configured to reject all packets destined for the victim.

5. **Analysis by the blackhole machine quickly traces the attack to one or more routers at the outermost boundary of the ISP’s network:** A human or program at the blackhole machine looks at the source address of each ICMP error packet to determine the address of the router that sent it. Typically, only a single router, or a small number of routers, will be identified as the entry point of the attack into the ISP’s network.