**ICMP Redirect Attack**

**Definitions:**

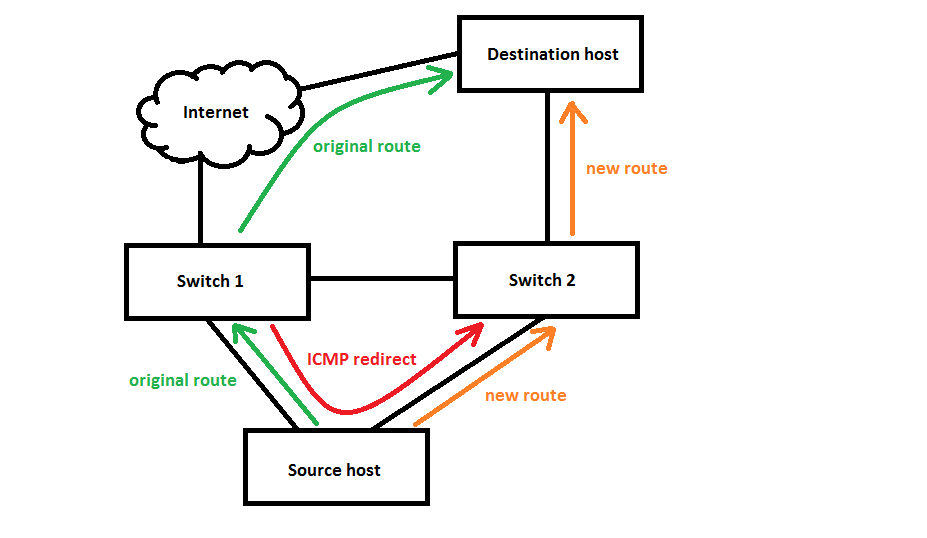
**ICMP**:

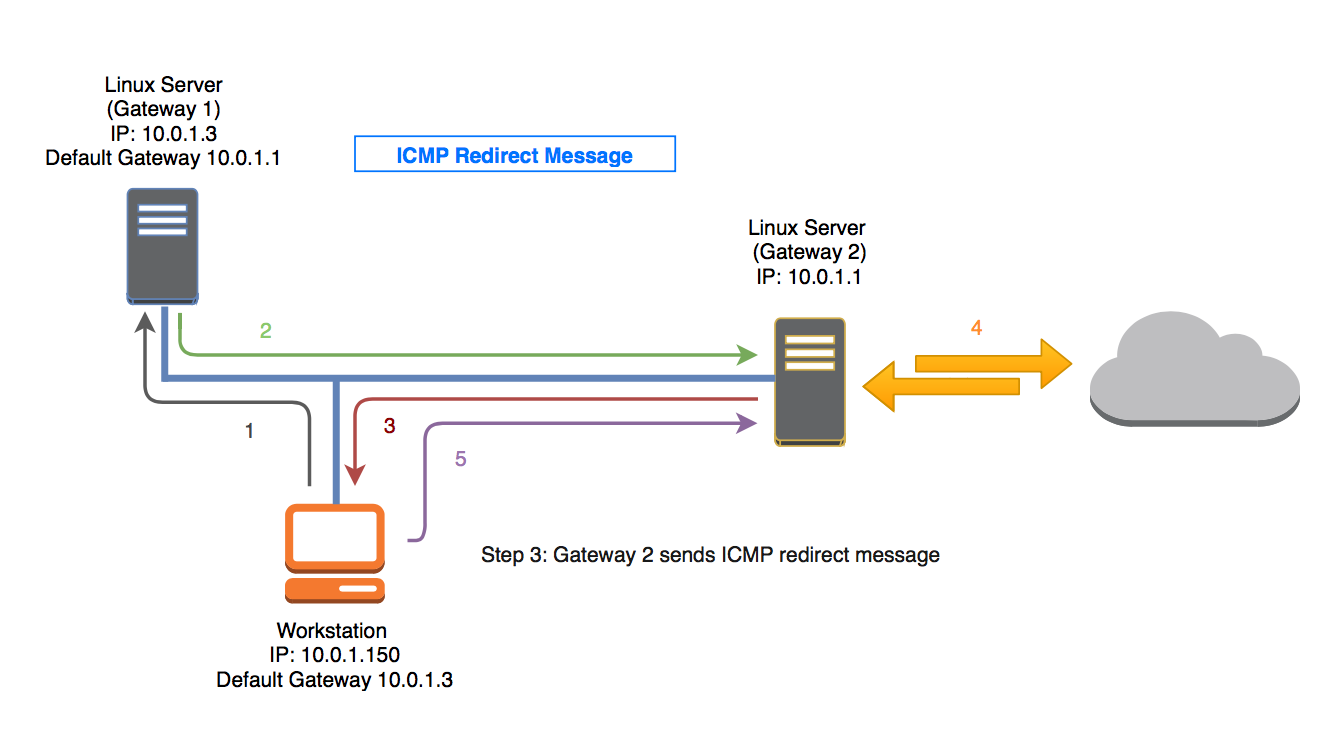
The **Internet Control Message Protocol** (**ICMP**) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached.

**ICMP Redirect:**

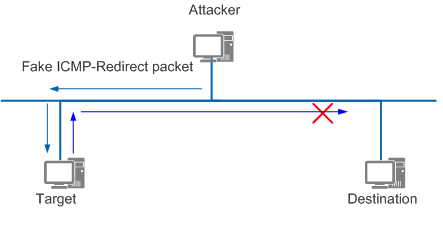
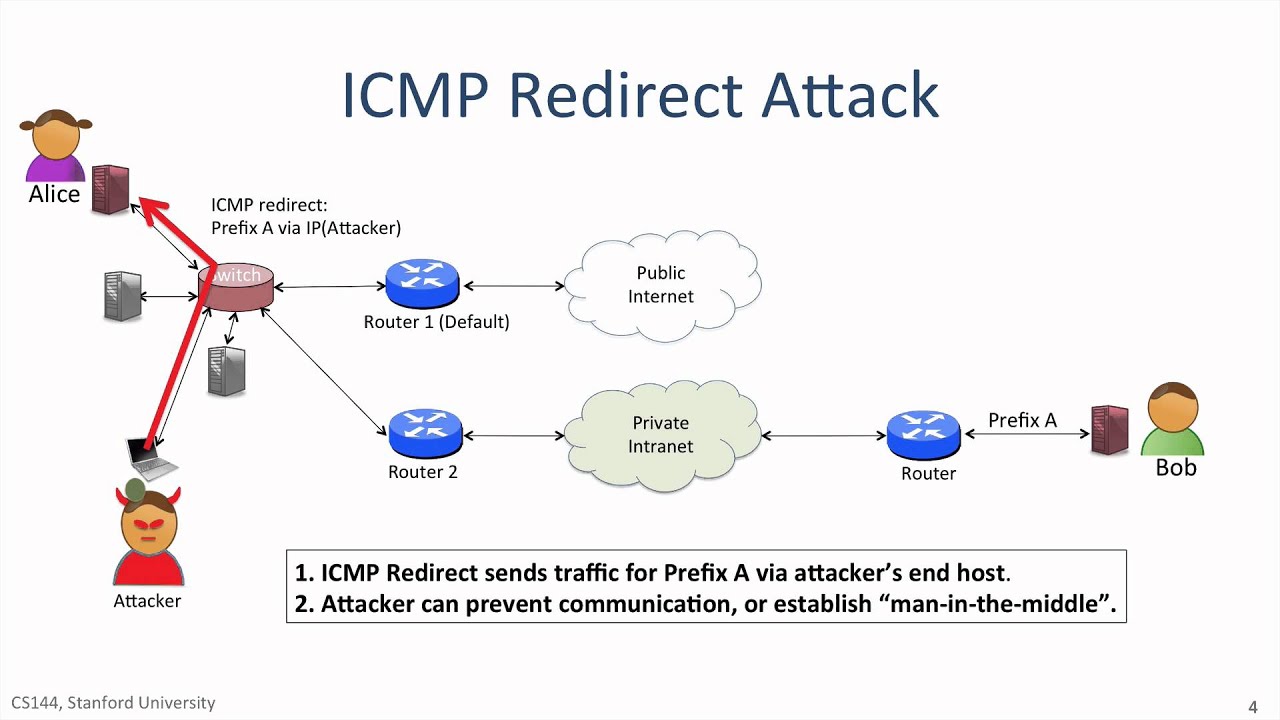
*Redirect* requests data packets be sent on an alternative route. ICMP Redirect is a mechanism for routers to convey routing information to hosts. The message informs a host to update its routing information (to send packets on an alternative route). If a host tries to send data through a router (R1) and R1 sends the data on another router (R2) and a direct path from the host to R2 is available (that is, the host and R2 are on the same Ethernet segment), then R1 will send a redirect message to inform the host that the best route for the destination is via R2. The host should then send packets for the destination directly to R2. The router will still send the original datagram to the intended destination. However, if the datagram contains routing information, this message will not be sent even if a better route is available. RFC 1122 states that redirects should only be sent by gateways and should not be sent by Internet hosts.

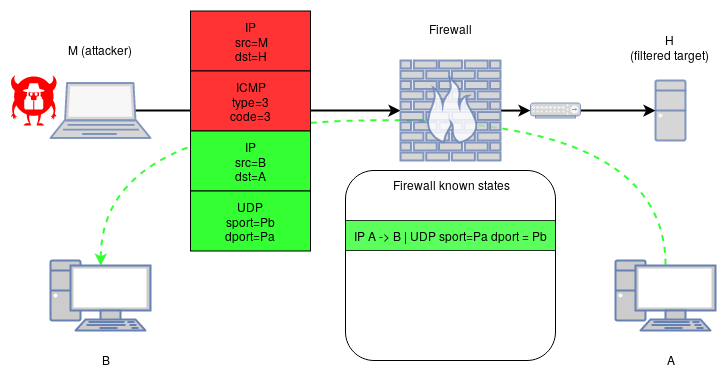
**Topology of ICMP Redirect :**

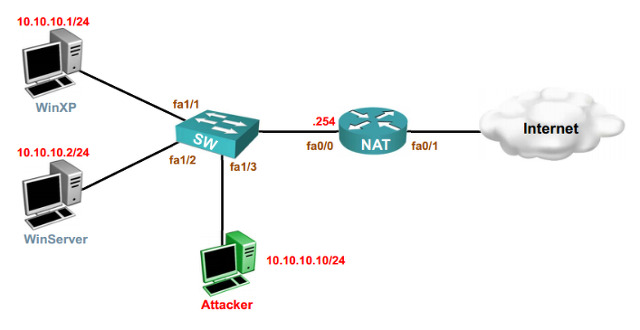




**Topology of ICMP Redirect Attack:**

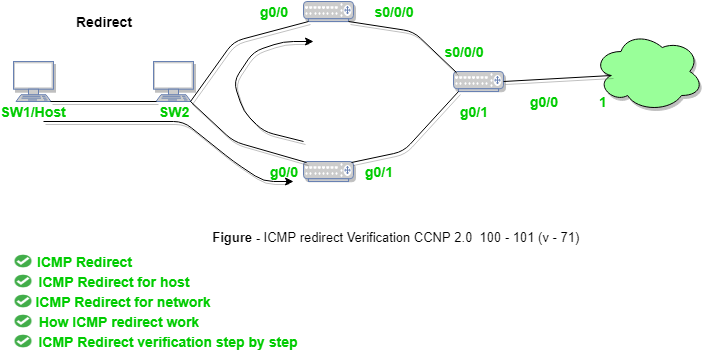


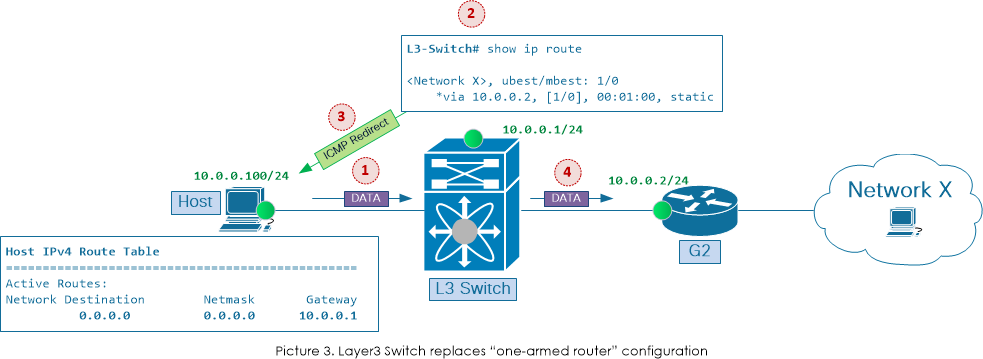




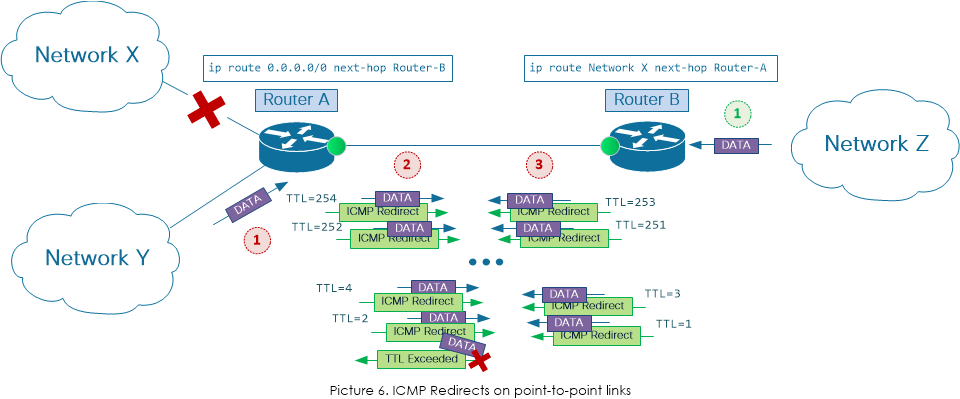
**Timing Diagram:**

**ICMP Redirect:**

****

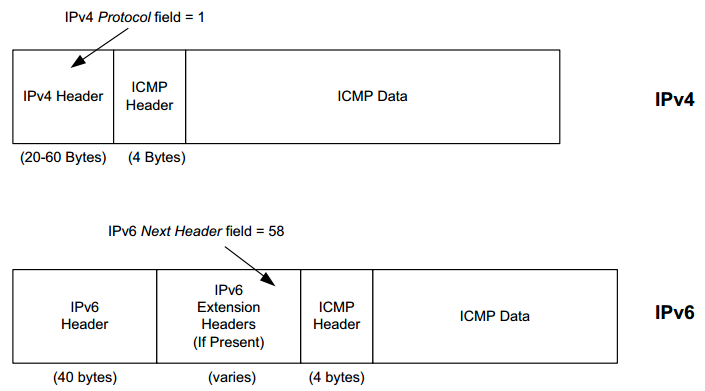


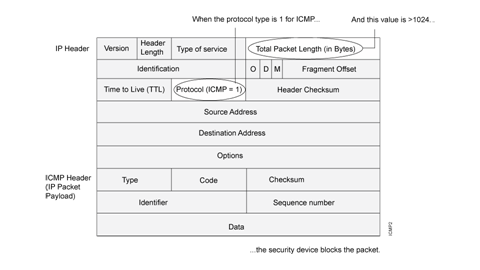
**ICMP Redirect Attack:**



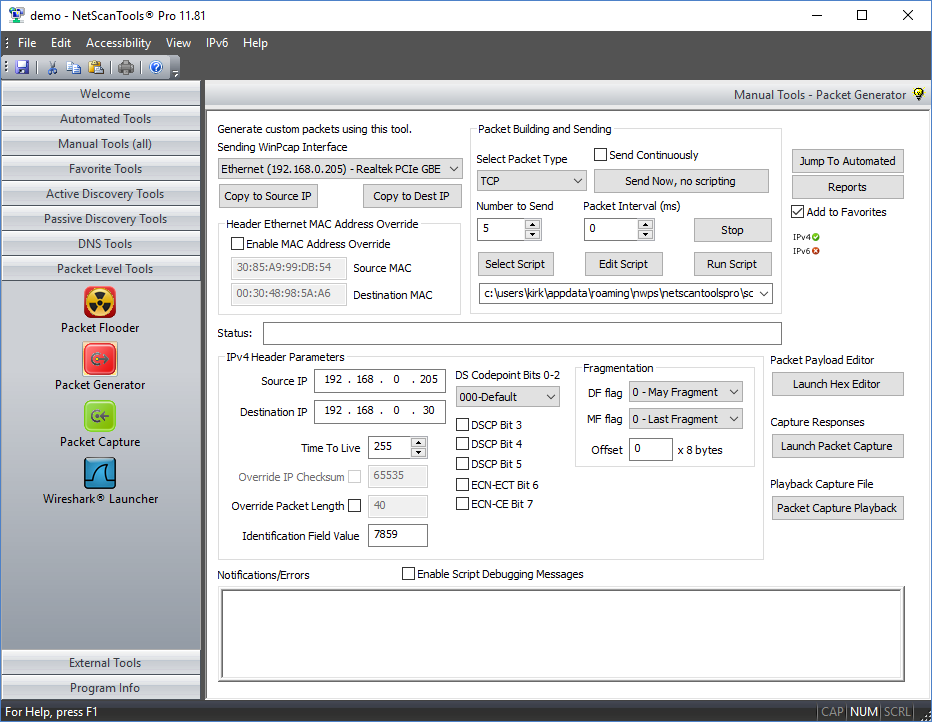
**Packet/Frame Details:**

**ICMP Header:**

****



**Packet Creation:**



**Strategy:**

The key idea is to write a raw socket that would allow making custom Headers. The existing sockets (tcp, udp) don’t allow this. In this custom header i(attacker) will put my ip and send them to the gateway router in a way so that for any Host to Target communication, the gateway router sends a redirect message to the Host telling it to send it’s packets to me(updating routing table of the router so that the router thinks that the shortest path to the Target(receiver) is through me).For this I’ll have to send a routing update message to the gateway router setting the cost to target through me lower than the existing path.

**Sample Code:**

static void create\_socket(socket\_st \*sock, int family, int socktype, int protocol, int requisite)

{

int do\_fallback = 0;

errno = 0;

assert(sock->fd == -1);

assert(socktype == SOCK\_DGRAM || socktype == SOCK\_RAW);

if (socktype == SOCK\_DGRAM)

sock->fd = socket(family, socktype, protocol);

if (sock->fd == -1 && errno == EAFNOSUPPORT && family == AF\_INET)

do\_fallback = 1;

if (sock->fd == -1 && errno == EPROTONOSUPPORT)

do\_fallback = 1;

if (sock->fd == -1 && errno == EACCES)

do\_fallback = 1;

if (socktype == SOCK\_RAW || do\_fallback) {

socktype = SOCK\_RAW;

sock->fd = socket(family, SOCK\_RAW, protocol);

}

if (sock->fd == -1) {

if ((errno == EAFNOSUPPORT && socktype == AF\_INET6) ||

options & F\_VERBOSE || requisite)

error(0, errno, "socket");

if (requisite)

exit(2);

} else

sock->socktype = socktype;

}

**Justification:**

**Why my design should work:**

If a gateway router sends a ICMP redirect message to the Host, there’s no way a host can verify it. It redirects its messages in the new route. So if i can confuse the gateway router that the shortest path from Host to receiver is through me, gateway router will send ICMP redirect message to me and I’ll receive the message, blocking their communication or worse, getting valuable information from the communication.