Chapter 5

Network Layer

The network layer is responsible for the addressing and source-to-destination delivery of a packet. This layer is primarily responsible for logical addressing and path determination between logical address groupings. Important protocol of network layer is IP (Internet Protocol) which handles important issues like addressing and routing in networks. The internet error control mechanisms are provided by protocol such as ICMP (Internet Control Message Protocol). In this chapter, we take an overview of these core protocols and analyze their vulnerabilities and attacks with defense mechanisms.

5.1 Internet Protocol (IP)

IP is the backbone protocol of the entire TCP/IP suite. IP uses 32-bit packet headers to store address data, and is the busiest protocol included in the TCP/IP suite. One major security flaw within IP itself is that the IP protocol stack does not verify the "source address", and just assumes that the packets "source address" is the valid one. This is a major flaw as anyone can insert somebody else's IP address in the packet to hide his identity.

5.1.1 IP Packet Format

An IP packet consists of an IP header and payload data as shown in figure 5.1(a). IP datagram header is minimum 20 bytes long and contains several components. IP packets usually contain quite a few flags, and other important bits of data.

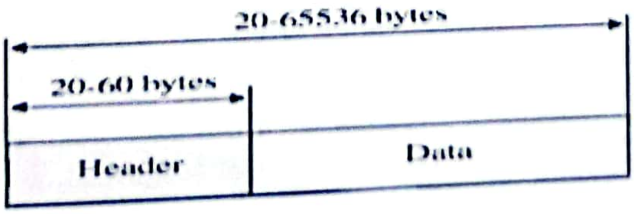

Figure 5.1 (a) IP Header and Payload Data

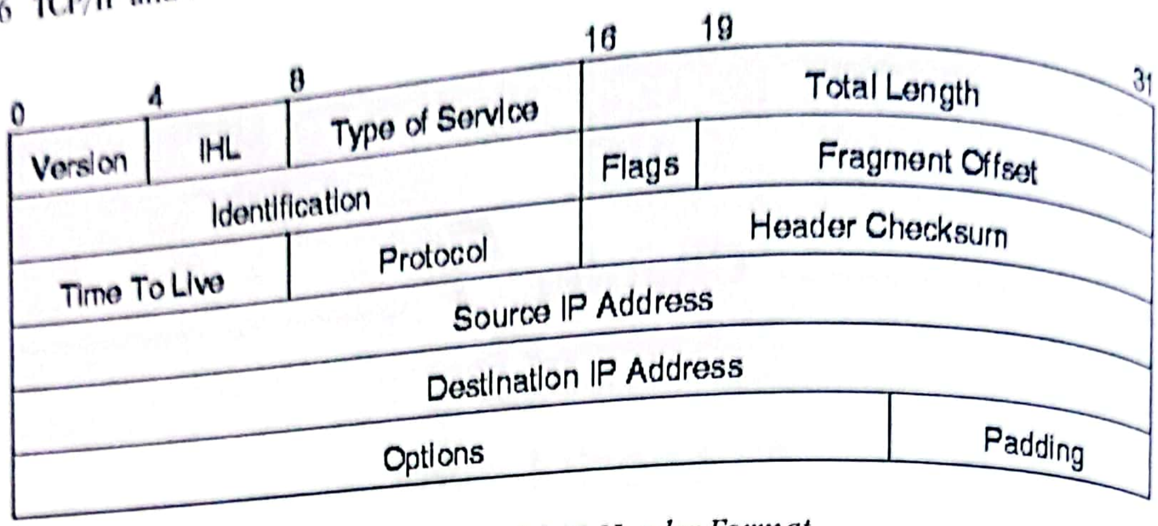

Figure 5.1 (b) IP Header Format

As shown in figure 5.1 (b) the various fields of the IP header are:

- The **version** field (4 bits wide) refers to the version of the IP protocol. The header shown is for IP v4.
- The **IHL (IP Header Length)** field (4 bits wide) is for Internet Header Length; it is the length of the IP header in 32-bit words. The minimum value for this field is 5 for five 32-bit words.
- **Type of Service** field (8 bits wide). They are both used to indicate the priority to be accorded to a packet. The routers may ignore these fields.
- The **Total Length** field (16 bits wide) is the size of the packet in bytes, including the header and the data. The minimum value for this field is 576.
- The **Identification** field (16 bits wide) is assigned by the sender to help the receiver with the assembly of fragments back into a datagram.
- The **Fragment offset** is used with fragmented datagrams which can be used in reassembly. The 8 bit protocol field identifies which higher-level TCP/ IP protocol is using the IP layer to encapsulate its data. When a packet arrives at the destination for which it is intended, IP extracts the encapsulated data and provides it to the designated higher-level protocol module.
- The control flags used by IP datagram are

Table 5.1 IP Header Flag Bits

0	Reserved
DF	Don't Fragment. 0 means allow fragmentation. 1 means do not allow fragmentation
MF	More Fragments. 0 means this is a last fragment. 1 means this is not last fragment.

- The **Time-To-Live** (TTL) control field is initialized to an arbitrary value by the sender. The value of the field is decremented by one by every network device that the packet passes through in transit to its destination. When the value reaches zero, the packet is considered unable to reach its destination. It is then discarded and the sending IP layer is sent a notification of the event using the Internet Control Message Protocol (ICMP).
- The **header checksum** field is a checksum only of IP header. It does not include data. The checksum is computed as 16 bit one's complement of the one's complement sum of all 16 bit words in the header.
- The 32 bit source **IP address** and 32 bit **destination IP address** represent the sender and receiver of the datagram.
- The **option** field is variable in length.

Sample Example 5.1

An IP datagram has arrived with the following information in header in Hex

45 00 00 34 01 7d 00 00 01 11 00 00 ac 10 0c 75 e0 00 00 fc

i) Are there any options?

ii) is the packet fragmented? Justify.

iii) What is the size of data?Is a checksum used?

iv) How many more routers can the packet travel to?

v) What is the identification number of the packet?

vi) What is the type of the service? Justify your answer with reason.

Solution: IP datagram have following format

(i) HLEN=$(5)_{16}$= 5*4 = 20bytes

Options are present after first 20 bytes which is not present in the given datagram. Thus the IP datagram does not have any options

(ii) According to the IP datagram format, the seventh and eighth bytes are required or refer to fragmentation. In our IP datagram the 7^{th} & 8^{th} bytes are 0000

$\therefore$ The IP packet is not fragmented

(iii) We know that Data size = Total length – header length

Total length =$(34)_{16}$

=52 bytes

Header length = 20bytes

$\therefore$ Data size = 52-20 = 32 bytes

(iv) According to the IP datagram format the checksum is provided in the 11^{th} & 12^{th} bytes of the packet. In given datagram the 11^{th} & 12^{th} bytes all 0's which is (0000)16

∴ The checksum is not used in the given packet

(v) In IP datagram format, the time to live is given in the 9^{th} byte of the IP packet.

In our packet the 9^{th} byte is (01)16

$\therefore TTL=(01)_{16}$

$=0000\ 0001$

$TTL=(1)_{10}$

∴The datagram can travel 1 more router.

(vi) Again we have the IP datagram which given its identification through the 5^{th} & 6^{th} bytes. In our packet the 5^{th} & 6^{th} bytes are 01 & 7d respectively

∴ Identification of the packet $=(017d)_{16}=381$

(vii) The type of service (TOS) is provided by the DS (differentiated service) field in the IP datagram which has the format

The DS is given in the 2^{nd} byte as (00)16 in our datagram

∴ TOS bits =0000=default

∴ The type of service provided by the packet is default.

5.1.2 IP Operation

IP Message Fragmentation Process: When an IP datagram is too large for the maximum transmission unit (MTU) of the underlying data link layer technology, it must be fragmented before it can be sent across the network. The higher-layer message to be transmitted is not sent in a single IP datagram but rather broken down into pieces called fragments that are sent separately. In some cases, the fragments themselves may need to be fragmented further.

Fragmentation Issues and Concerns: Fragmentation is necessary to implement a network-layer internet that is independent of lower layer details but introduces significant complexity to IP. Remember that IP is an unreliable, connectionless protocol. IP datagrams can take any of several routes on their way from the source to the destination, and some may not even make it to the destination at all. When we fragment a message we make a single datagram into many, which introduces several new issues to be concerned with:

Sequencing and Placement: The fragments will typically be sent in sequential order from the beginning of the message to the end, but they won't necessarily appear in

9.	ICMP Router Discovery is used to determine the IPv4 address of the best default gateway, and it is optional.	ICMPv6 Router Solicitation and Router Advertisement messages are used to determine the IP 'address of the best default gateway, and they are required For more information.
10.	Broadcast addresses are used to send traffic to all nodes on a subnet.	IPv6 uses a link-local scope all-nodes multicast address.
11.	Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP.
12.	Uses host address (A) resource records in Domain Name System (DNS) to map host names to IPv4 addresses.	Uses host address (AAAA) resource records in DNS to map host names to IPv6 addresses.
13.	Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.
14.	Must support a 576-byte packet size (possibly fragmented).	Must support a 1280-byte packet size (without fragmentation).

5.2 Internet Message Control Protocol(ICMP)

The Internet Control Message Protocol (ICMP) is the basic network management tool of the TCP/IP protocol suite. ICMP is one protocol used by network devices for transmitting investigative messages. The Internet Control Message Protocol ("ICMP") is used by the IP layer to send one-way informational messages to a host. ICMPs are used by routers, intermediary devices, or hosts to communicate updates or error information to other routers, intermediary devices, or hosts.

5.2.1 ICMP Packet Format

Each ICMP message contains three fields that define its purpose and provide a checksum.

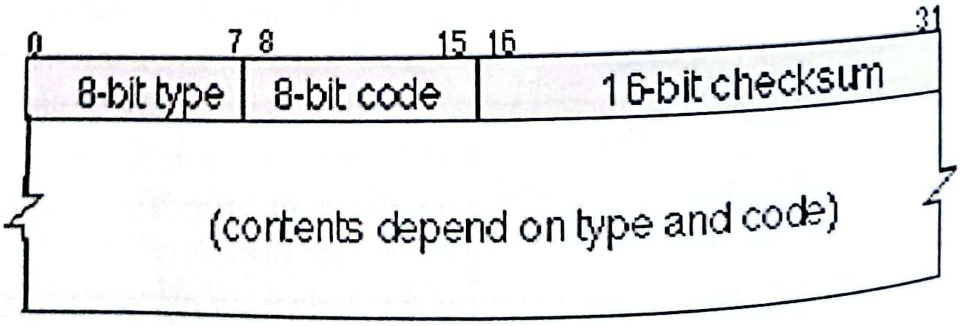

Figure 5.7 ICMP Message

The format of an ICMP message is shown in figure 5.7 above. The 8-bit type code identifies the types of message.

TYPE	Description
--------	----------------
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect Message
8	Echo Request
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request (No Longer Used)
16	Information Reply (No Longer Used)
17	Address Mask Request
18	Address Mask Reply

The CHECKSUM provides a method for determining the integrity of the message. This is followed by at least the first 28 bytes of the packet that resulted in generation of the error message. This payload is, for instance used by a sender that receives the ICMP message to perform Path MTU Discovery so that it may determine IP destination address of the packet that resulted in the error. One of the most common and popular use of ICMP is the "ping" utility. This utility sends an ICMP "Echo Request" to a host, and waits for that host to send back an ICMP "Echo Reply" message.

Example 5.7

An ICMP message has arrived wit the header in hex 0303102000000000. What is the type of message? What is the code? What is the purpose of the message?

(i) Given ICMP message is

08 00 10 20 00 00 00 00

The type of message is given by the first byte in the ICMP message

In our ICMP message, the first byte is$(08)_{16}$

$\therefore$ Type=(08)16

Now, which is of the form or 08 means echo request (ping) packet.

$\therefore$ The type of message is Destination unreachable.

(ii) The code is given by the 2nd byte in the ICMP message which then has different meanings.

In our ICMP message the code field =(00)16

$\therefore$ code =0

Now, code 0 means that the It is an Ping request.

The message is generated to test the connectivity to host by using ICMP ping packet.

Example 5.8

Consider the packet 03 03 00 00 10 20 00 00

Here type field is first byte which is 03. This indicates that packet is echo reply packet.

Code field is second byte which is 03. This indicates the error port unreachable.

The packet is sent to report error of destination port unreachable.

5.3 Vulnerabilities and Attacks in IP and ICMP

Here we describe some of the major vulnerabilities of Internet Protocol.

Vulnerabilities in IP

- **Connectionless:** IP is a connectionless protocol. Each unit of data transmitted, labeled as packet, is transmitted as an independent message and is not viewed as having a relationship with any other packets. Furthermore, IP does not ensure that a packet will reach its final destination or whether packets that do arrive will arrive in the original order that they were sent. There is no information in a packet to identify it as part of a sequence of related packets. Any mechanism for ensuring that transmitted data arrives at its destination, and in the correct order, is provided by a higher protocol in the suite.

- **Lack of Authentication:** The major vulnerability in most of the protocols of TCP/IP is lack of authentication mechanisms. This is the severe flaw which enables attacker to access the confidential information. The IP layer assumes that the source address on any IP packet it receives is the same IP address as the system that actually sent the packet. It does not provide any authentication mechanism. Many higher level protocols and applications also make this assumption so it seems that anyone able to forge the source address of an IP packet called "spoofing" an address could get unauthorized privileges.
- **Source Routing:** Source routing allows the originating host to specify the path route that the receiver should use to reply to it. An attacker may take advantage of this by specifying a route that by-passes the real host and instead directs replies to a path it can monitor e.g., to itself or a local subnet.

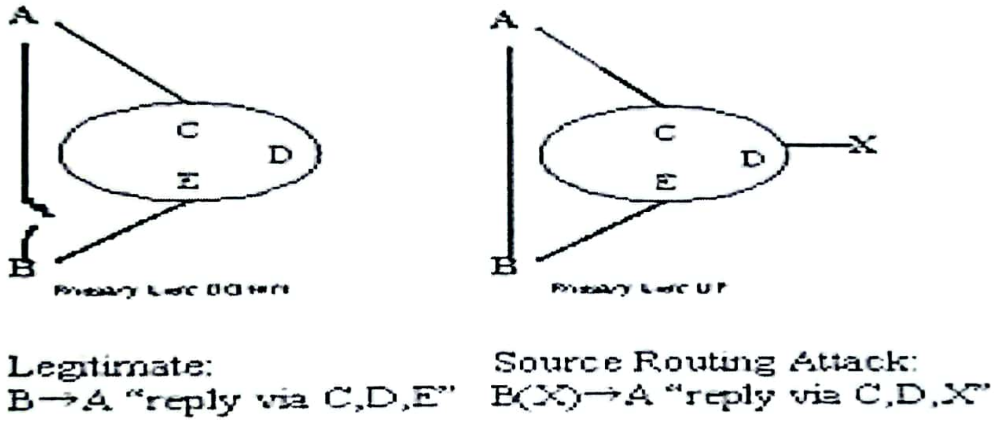

Figure 5.8 Source Routing Attack ((www.linuxsecurity.com))

Assume that the target host uses the reverse of the source route provided in a TCP open request for return traffic. If the originator of the connection wishes to specify a particular path for some reason, replies may not reach the originator if a different path is followed. The attacker can then pick any IP source address desired, including that of a trusted machine on the target's local network. Any facilities available to such machines become available to the attacker. Although simple, this attack may not be as successful now, as routers are commonly configured to drop packets with source routing enabled.

Attacks in IP

IP is the backbone protocol of the entire TCP/IP suite. However, it cannot do much on its own. IP uses 32-bit packet headers to store address data and is the busiest protocol included in the TCP/IP suite. One major security flaw within IP is the fact that the IP protocol stack does not verify the "source address", and just assumes that the packets "source address" is valid one.

- **IP Spoofing:** The term 'IP spoofing' can be used to describe any process in which a person fakes, or "forges" a packet to look like it came from elsewhere, often a "trusted" host. In client-side spoofing, a hacker impersonates himself as an authorized client and in turn gains service from an unintelligent server. There are various types, and various techniques attackers might use when attempting to spoof packets, or better, spoof a connection. IP spoofing can be used in two main ways: to cause DoS, or to gain access to a system as a"trusted" host.
- **Non-Blind Spoofing:** This type of attack takes place when the attacker is on the same subnet as the victim. The sequence and acknowledgment numbers can be sniffed, eliminating the potential difficulty of calculating them accurately. The biggest threat of spoofing in this instance would be session hijacking. This is accomplished by corrupting the data stream of an established connection, then re-establishing it based on correct sequence and acknowledgment numbers with the attack machine. Using this technique, an attacker could effectively bypass any authentication measures taken place to build the connection.
- **Blind Spoofing:** This is a more sophisticated attack, because the sequence and acknowledgment numbers are unreachable. Several packets are sent to the target machine in order to sample sequence numbers. It was relatively easy to discover the exact formula by studying packets and TCP sessions. Today, most OS's implement random sequence number generation, making it difficult to predict them accurately. If, however, the sequence number was compromised, data could be sent to the target. A properly crafted attack could add the requisite data to a system, blindly, enabling full access for the attacker who was impersonating a trusted host.
- **Denial of Service:** IP spoofing is almost always used in what is currently one of the most difficult attacks to defend against denial of service attacks, or DoS. Since attackers are concerned with consuming bandwidth and resources, they need not worry about properly completing handshakes and transactions. Rather, they wish to flood the victim with as many packets as possible in a short amount of time. In order to prolong the effectiveness of the attack, they spoof source IP addresses to make detection and prevention of DoS as difficult as possible.
- **IP fragmentation Attacks:** Described here are some of the attacks related to IP fragmentation
- **IP fragment overlapped:** The IP fragment overlapped exploit occurs when two fragments contained within the same IP datagram have offsets that indicate that they overlap each other in positioning within the datagram. This could mean that either fragment A is being completely overwritten by fragment B, or that fragment A is partially being overwritten by fragment B. Some operating systems do not

properly handle fragments that overlap in this manner and may throw exceptions or behave in other undesirable ways upon receipt of overlapping fragments.

- **IP fragmentation buffer full:** The IP fragmentation buffer full exploit occurs when there is an excessive amount of incomplete fragmented traffic detected on the protected network. This could be due to an excessive number of incomplete fragmented datagrams, a large number of fragments for individual datagrams or a combination of quantity of incomplete datagrams and number of fragments in each datagram. This type of traffic is most likely an attempt to bypass security measures or Intrusion Detection Systems by intentional fragmentation of attack activity.

- **IP fragment overrun:** The IP Fragment Overrun exploit is when a reassembled fragmented datagram exceeds the declared IP data length or the maximum datagram length. By definition, no IP datagram should be larger than 65,535 bytes. Systems that try to process these large datagrams can crash, and can be indicative of a denial of service attempt.

- **IP fragment overwrite:** Overlapping fragments may be used in an attempt to bypass Intrusion Detection Systems. In this exploit, part of an attack is sent in fragments along with additional random data; future fragments may overwrite the random data with the remainder of the attack. If the completed datagram is not properly reassembled at the IDS, the attack will go undetected.

- **IP fragment incomplete datagram:** This exploit occurs when a datagram can not be fully reassembled due to missing data. This can indicate a denial of service attack or an attempt to defeat packet filter security policies.

- **Fragment too small:** An IP Fragment Too Small exploit is when any fragment other than the final fragment is less than 400 bytes, indicating that the fragment is likely intentionally crafted. Small fragments may be used in denial of service attacks or in an attempt to bypass security measures or detection.

- **Man In the Middle Attack:** Both types of spoofing are forms of a common security violation known as a man in the middle (MITM) attack. In these attacks, a malicious party intercepts a legitimate communication between two friendly parties. The malicious host then controls the flow of communication and can eliminate or alter the information sent by one of the original participants without the knowledge of either the original sender or the recipient. In this way, an attacker can fool a victim into disclosing confidential information by "spoofing" the identity of the original sender, who is presumably trusted by the recipient. The attacker intercepts some or all traffic coming from the computer, collects the data, and then forwards it to the destination the user was originally intending to visit. The attack is described in figure 5.9

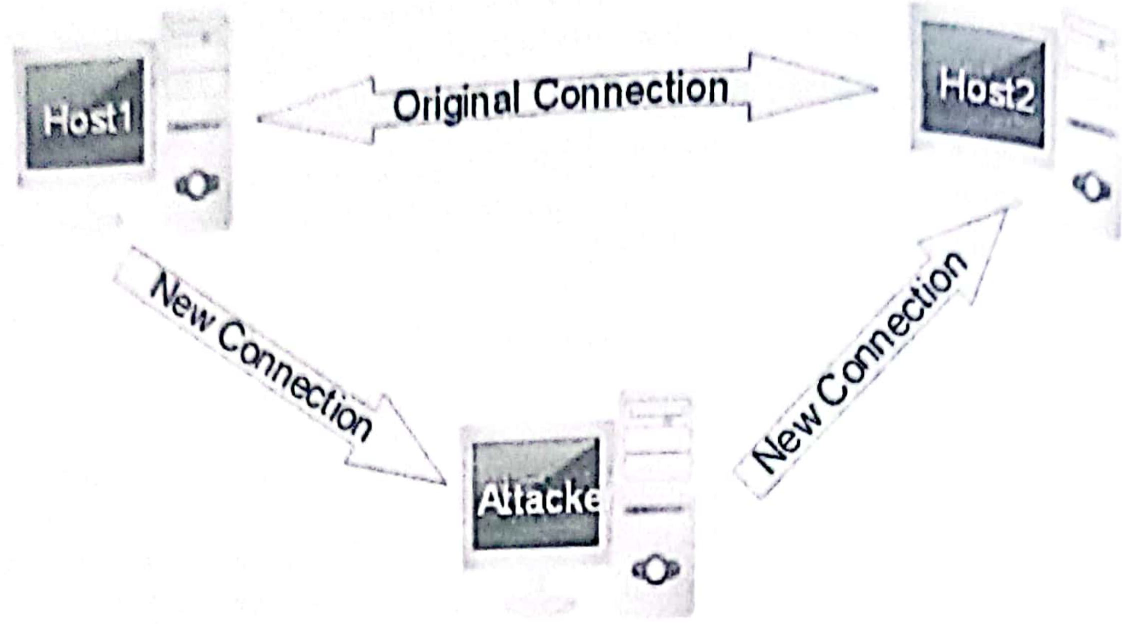

Figure 5.9 Man-in-the-Middle

- **SMURF Attack:** A smurf attack is an exploitation of the Internet Protocol (IP) broadcast addressing to create a denial of service. The attacker uses a program called Smurf to cause the attacked part of a network to become inoperable. Smurf takes advantage of certain known characteristics of the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP). The ICMP is used by network nodes and their administrators to exchange information about the state of the network. ICMP can be used to ping other nodes to see if they are operational. An operational node returns an echo message in response to a ping message. The smurf program builds a network packet that appears to originate from another address. The packet contains an ICMP ping message that is addressed to an IP broadcast address, meaning all IP addresses in a given network. The echo responses to the ping message are sent back to the "victim" address. Enough pings and resultant echoes can flood the network making it unusable for real traffic.
- **LAND Attack:** Land attacks work by sending a stream of TCP SYN packets that have the IP address and TCP port number set to the same value for both the sender and receiver. For some implementations of TCP/IP, this causes an infinite loop and eventual denial of service.

```
Structure Packet
{
Source IP Address= Destination IP Address
Source Port= Destination Port
}
```

The Land attack will affect different operating systems in different ways. For instance, this attack will cause a Windows NT 4.0 machine (with Service Pack 3 and all applicable hot fixes applied) to slow down for approximately sixty (60) seconds, after which it will resume normal operations without other effects. Windows 95 machines, on the other hand, will either crash or lock-up, requiring that they be rebooted. Most UNIX machines will either crash or hang, and not allow users to access services on the machine.

- **Manipulation of IP Identification Field:** IP packets can get fragmented along the route from the source to the destination because of different Maximum Transfer Units (MTUs) of different segments. All fragments that originally belonged to an IP packet are given the same IP id field number so that all the fragments can be identified and assembled back into a whole packet. As long as this purpose is served, the specific choice made for the value does not matter.

  The first encoding method simply replaces the IP identification field with the numerical ASCII representation of the character to be encoded. This allows for easy transmission to a remote host which simply reads the IP identification field and translates the encoded ASCII value to its printable counterpart.

  The lines below show a tcpdump representation of the packets on a network between two hosts "`computer.vjti.com`" and "Test`.vjti.com`." A coded message consisting of the letters "HELLO" was sent between the two hosts in packets appearing to be destined for the WWW server on Test`.vjti.com`.

  The actual packet data does not matter. The field in question is the IP portion of the packet called the "id" field located in the parenthesis.

  Note that the ID field is represented by an unsigned integer during the packet generation process of the included program. This program does not perform any type of byte ordering functions normally used in this process, therefore packet data is converted to the ASCII equivalent by dividing by 256.

Example 5.9

Packet One:

18:50:13.551117 computer.vjti.com.7180 > Test.vjti.com .www: S 537657344:537657344(0) win 512 (ttl 64, id 18432)

Decoding:...(ttl 64, id 18432/256) [ASCII: 72(H)]

Packet Two:

18:50:14.551117 computer.vjti.com.51727 > Test.vjti.com: S1393295360:1393295360(0) win 512 (ttl 64, id 17664)

Decoding:...(ttl 64, id 17664/256) [ASCII: 69(E)]

Packet Three:

18:50:15.551117 computer.vjti.com.9473 > Test.vjti.com:S 3994419200:3994419200(0) win 512 (ttl 64, id 19456)

Decoding:...(ttl 64, id 19456/256) [ASCII: 76(L)]

Packet Four:

18:50:16.551117 computer.vjti.com.56855 > Test.vjti.com.: S3676635136:3676635136(0) win 512 (ttl 64, id 19456)

Decoding:...(ttl 64, id 19456/256) [ASCII: 76(L)]

Packet Five:

18:50:17.551117 computer.vjti.com.1280 > Test.vjti.com.www: S 774242304:774242304(0) win 512 (ttl 64, id 20224)

Decoding:...(ttl 64, id 20224/256) [ASCII: 79(O)]

Packet Six:

18:50:18.551117 computer.vjti.com.21004 > Test.vjti.com. www: S3843751936:3843751936(0) win 512 (ttl 64, id 2560)

Decoding:...(ttl 64, id 2560/256) [ASCII: 10(Carriage Return)]

Internet Control Message Protocol

ICMP attacks are rather difficult; still, there are often holes that may be exploited. The first, and most obvious target, is the ICMP Redirect message; it is used by gateways to advise hosts of better routes. It's not surprising that there is no authentication in ICMP, which leads to attacks using ICMP that can result in a denial of service, or allowing the attacker to intercept packets [Bellovin89]. Lack of authentication in ICMP can result in a denial of service, or allowing the attacker to intercept packets.

ICMP may also be used for targeted denial of service attacks. Several of its messages, such as Destination Unreachable and Time to Live Exceeded, may be used to reset existing connections. If the intruder knows the local and remote port numbers of a TCP connection, an ICMP packet aimed at that connection may be forged. Such information is sometimes available through the netstat service. A more powerful denial of service attack can be launched by sending a fraudulent Subnet Mask Reply message. Some hosts will accept any such message, whether they have sent a query or not; a false one could effectively block all communications with the target host.

Attacks in ICMP

ICMP attacks are rather difficult still, there are often holes that may be exploited.

- **Flooding:** Ping flooding is arguably one of the most popular DoS attacks on the Internet. Ping flooding involves sending continuous stream of ICMP_ECHO requests. Suppose the attacker sends a continuous stream of ICMP_ECHO packets to Host S as fast as they can. Since the attacker continuously sends ICMP packets without waiting for a reply from a spoofed address, host S is severely bogged down with the process of responding to the spoofed ping requests. Eventually sometimes Host S is forced to devote 100% CPU utilization to the responding of the ICMP packets. The reason the attacker spoofs the source address of the packets is because if they didn't, they would be flodded with ICMP_ECHO reply packets.
- **SMURF Attack:** A smurf attack is an exploitation of the Internet Protocol (IP) broadcast addressing to create a denial of service. The attacker uses a program called Smurf to cause the attacked part of a network to become inoperable. The smurf program builds a network packet that appears to originate from another address. The packet contains an ICMP ping message that is addressed to an IP broadcast address, meaning all IP addresses in a given network. The echo responses to the ping message are sent back to the "victim" address. Enough pings and resultant echoes can flood the network making it unusable for real traffic.
- **ICMP Redirect message:** It is used by gateways to advise hosts of better routes. The complication is that a Redirect message must be tied to a particular, existing connection; it cannot be used to make an unsolicited change to the host's routing

tables. Furthermore, Redirects are only applicable within a limited topology; they may be sent only from the first gateway along the path to the originating host. A later gateway may not advise that host, nor may it use ICMP Redirect to control other gateways.

5.4 Defense Mechanisms

Following are the defense mechanisms for protection from IP exploits.

- **Source /routing:** The best idea for defense against source routing attacks would be for the gateways into the local network to reject external packets. A simpler method for defense against source routing attacks might be to reject pre-authorized connections if source routing information was present.
- **IPSec:** An international working group organized under the IETF has developed a method of doing exactly that. They call it the IP security (IPSec) protocol suite. The IPSec protocol suite is based in powerful new encryption technologies, and adds security services to the IP layer in a fashion that is compatible with the existing IP standard (IPv.4), and which is mandatory in the upcoming one (IPv.6 1). IPSec provides secure gateway-to-gateway connections across outsourced private wide area network (WAN). Designed by the Internet Engineering Task Force (IETF) as the security architecture for the Internet Protocol (IP), IPSec defines IP packet formats and related infrastructure to provide end-to-end strong authentication, integrity, anti-replay, and (optionally) confidentiality for network traffic.

  The IPSec protocols are designed to be independent of the actual lower-level cryptographic algorithms.
- **Network Intrusion Prevention System(NIPS):** A network intrusion detection system is mostly place at strategic points in a network, so that it can monitor the traffic travelling to or from different devices on that network. A network-based IPS monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity. Network-based IPS components are shown in figure 5.10. A network-based IPS sensor monitors and analyzes network activity on one or more network segments. Sensors are available in two formats: appliance-based sensors, which are comprised of specialized hardware and software optimized for IPS sensor use, and software-only sensors, which can be installed onto hosts that meet certain specifications.

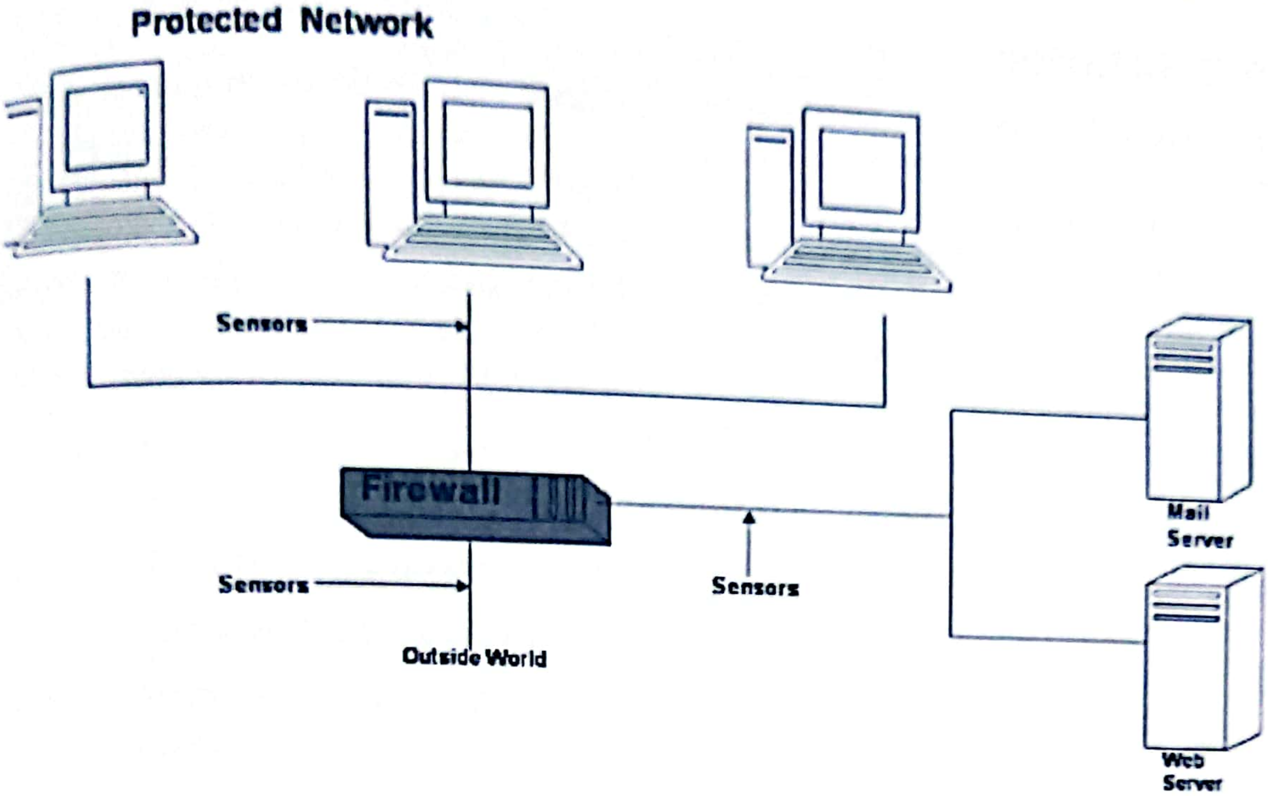

Figure 5.10 Network Intrusion Prevention System(NIPS)

- **Defense against smurf**

  One way to defeat smurfing is to disable IP broadcast addressing at each network router since it is seldom used.

- **Defense against LAND attack**

  A workaround for the **Land** attack is to block IP-spoofed packets. Attacks such as **Land** rely on the use of forged packets, that is, packets where the attacker deliberately falsifies the origin address. With the current IP protocol technology, it is impossible to eliminate IP-spoofed packets. However, a site administrator can reduce the likelihood of having his or her network being used to initiate forged packets by filtering outgoing packets that have a source address different from that of the internal network.

Defense Mechanisms for ICMP

- A defense against Redirect attacks is to restrict route changes to the specified connection; the global routing table should not be modified in response to ICMP Redirect messages6.
- Denying ICMP broadcasting is one of the possible solution for avoiding Ping flooding or Smurf attacks. The some of the other solutions which can be implemented are
  1. Performing active and passive monitoring of TCP Sessions. This will provide security for sessions in communications.
  2. Implement stateful firewalling to monitor packets and states of sessions.

5.5 Conclusion

This chapter describes security analysis of IP and ICMP in detail. In current Internet scenario it is important to protect data in transit. The resources on Internet are prone to Denial-of-service, spoofing, poisoning and many more types of attacks. The attackers are exploring vulnerabilities of existing protocols and targeting raw and unprotected information. The analysis given in this chapter helps new entrants in security research area to understand the different attacks, their underlying vulnerabilities and countermeasures. We hope that our insights will influence the design of future networks to be robust to any type of attacks.