Computer Network Reading Assignment

On

DHCP(Dynamic Host Configuration Protocol)

and

IMCP(Internet Control Message Protocol)

-submitted By

Mehul Patni BT17CSE089

Shrey Jasuja BT17CSE077

Q) what is the principle and working of DHCP?

DHCP definition

DHCP stands for dynamic host configuration protocol and is a network protocol used on IP networks where a DHCP server automatically assigns an IP address and other information to each host on the network so they can communicate efficiently with other endpoints.

In addition to the IP address, DHCP also assigns the subnet mask, default gateway address, domain name server (DNS) address and other pertinent configuration parameters. Request for comments (RFC) 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF)-defined standard based on the BOOTP protocol.

DHCP simplifies IP address management

The primary reason DHCP is needed is to simplify the management of IP addresses on networks. No two hosts can have the same IP address, and configuring them manually will likely lead to errors. Even on small networks manually assigning IP addresses can be confusing, particularly with mobile devices that require IP addresses on a non-permanent basis. Also, most users aren't technically proficient enough to locate the IP address information on a computer and assign it. Automating this process makes life easier for users and the network administrator.

Components of DHCP

When working with DHCP, it's important to understand all of the components. Below is a list of them and what they do:

- DHCP server
- DHCP client
- IP address pool
- Lease
- DHCP relay

Benefits of DHCP servers

In addition to simplified management, the use of a DHCP server provides other benefits. These include:

- Accurate IP configuration
- Reduced IP address conflicts
- Automation of IP address administration
- Efficient change management

What is the ICMP (Internet Control Message Protocol)?

In order to be able to exchange status information or fault messages, nodes in TCP/IP networks access the Internet Control Message Protocol (ICMP). In particular, application servers and gateways (routers) use the IP extension to display notifications of datagram problems to the packages' sender. The structure, mode of operation and classification in the internet protocol stack were specified in RFC 792 in 1981 RFC 792. For version 6 of the internet protocol RFC 4443 has been defined as the specific implementation of ICMPv6.

How does ICMP work?

To understand how the protocol works, you first need to look at the structure of the ICMP, or the header. This is directly linked to the IP header, which is marked by the protocol number 1 or 58 (ICMPv6) in the IP field "protocol." The header data area of the Internet Control Message Protocol itself is limited and has the following form:

	Bit 0–7	**Bit 8–15**	**Bit 16–23**	**Bit 24–31**
0	Type	Code	Checksum	
32	Header Information			

The first 8-bit "Type" field determines what type of notification the ICMP packet is. This information can be specified with the following "code" field, which is also 8 bits long. For example, an ICMP type 3 message specifies that the destination of the data packet is unavailable, while the code specifies this information to determine whether it was the destination network (0), the desired host (1) or the targeted port (3) that did not respond to the previous request. The ICMP checksum follows the information about the message type, and ensures the accuracy of the notification. This is done the same way as other standard protocols' checksums (IP, UDP, TCP).
Finally, the ICMP files are built and structured differently depending on the respective type and the triggering instance. The IP header often contains a listing of the first 64 bits of the data packet, which are responsible for the error message or the status query. When so-called ICMP tunneling takes place, this field is misused for sending useful data under firewalls' radars or for establishing an encrypted communication channel between two computers.

Now, there are many kinds of error messages generated, so we cover a subset of these, which are important and are the most frequent error messages sent.

1. **Destination Unreachable -** The ICMP destination unreachable message is generated by a router to inform the source host that the destination unicast address is unreachable. The IP header plus the first 8 bytes of the original datagram's data is returned to the sender. This data is used by the host to match the message to the appropriate process. If a higher level protocol uses port numbers, they are assumed to be in the first 64 data bits of the original datagram's data.

2. **Time Exceeded The ICMP -** Time exceeded message is one which is usually created by gateways or routers.The ICMP - Time exceeded message is generated when the gateway processing the datagram (or packet, depending on how you look at it) finds the Time To Live field (this field is in the IP header of all packets) is equal to zero and therefore must be discarded. The same gateway may also notify the source host via the time exceeded message.

3. **Redirect -** The ICMP Redirect message is used to notify a remote host to send data packets on an alternative route. A host SHOULD NOT send an ICMP Redirect message. Redirects SHOULD only be sent by gateways. The IP address of the gateway and the internet header plus the first 8 bytes of the original datagram's data is returned to the sender. This data is used by the host to match the message to the appropriate process. If a higher level protocol uses port numbers, they are assumed to be in the first 64 data bits of the original datagram's data. This message is not generated in response to a datagram destined for a multicast address.

4. **Echo -** The Identifier, sequence number and data fields should be returned to the sender unaltered. The data received in the echo request message must be returned in the echo reply message. The identifier and sequence number may be used by the echo sender to aid in matching the replies with the echo requests. For example, the identifier might be used like a port in TCP or UDP to identify a session, and the sequence number might be incremented on each echo request sent. The echoing node returns these same values in the echo reply. Code 0 may be received from a gateway or a host.

5. **Echo Reply -** This message is generated in response to an ICMP Echo request message. The Identifier, Sequence number and Data fields MUST be returned to the sender unaltered. The identifier and sequence number may be used by the echo sender to aid in matching the replies with the echo requests. For example, the identifier might be used like a port in TCP or UDP to identify a session, and the sequence number might be incremented on each echo request sent. The echoer returns these same values in the echo reply.