Part B : Micro Project Report

Title: ICMP Protocol

1.0 Rational:

The ICMP protocol was designed to address the need for effective communication and troubleshooting in IP networks. It serves several important purposes that contribute to the overall functionality and reliability of network communication.

One of the main rationales for ICMP is error reporting. When a network device encounters an issue while processing an IP packet, it can generate an ICMP error message and send it back to the source host. This allows for the identification and resolution of network problems, such as unreachable destinations or packet fragmentation issues.

Another important rationale for ICMP is network diagnostics. ICMP provides various messages and functionalities that help in diagnosing network issues. For example, the Echo Request and Reply mechanism, commonly known as "ping," allows network devices to test the reachability of other devices. Additionally, ICMP messages like Time Exceeded and Destination Unreachable provide insights into network path problems and aid in troubleshooting.

ICMP also plays a crucial role in network reachability information. It allows hosts to determine network address mask information through messages like Address Mask Request and Reply. This helps in proper network configuration and routing decisions.

Overall, the rationale for the ICMP protocol is to ensure effective communication, efficient troubleshooting, and reliable network reachability in IP networks. It enhances the overall performance, stability, and management of networks, making it an essential component of modern networking protocols

.

2.0 Course Action Address:

1. Analyse the functioning of advance computer network.
2. Configure various networking devices.
3. Configure difference between IPV4 and IPV6 services.

3.0 Literature Review:

Books:

1) "Advance Computer Network" by Deepali A. Patil (Tech Neo Publications).
2) "Advance Computer Network" by J. S. Katre and Vaishali S. Joshi(TechKnowledge Publications).
3) "Computer Networks" by Andrew S. Tanenbaum and David J. Wetherall.

• Websites:

1) Oracle: https://www.oracle.com/database/what-is-database/
2) W3Schools: https://www.w3schools.com/
3) GeeksforGeeks: https://www.geeksforgeeks.org/

4.0 Actual Methodology:

Internet Control Messages Protocol

Internet Control Message Protocol (ICMP) is a network layer protocol used to diagnose communication errors by performing an error control mechanism. Since IP does not have an inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol (ICMP) to provide error control.

ICMP is used for reporting errors and management queries. It is a supporting protocol and is used by network devices like routers for sending error messages and operations information. For example, the requested service is not available or a host or router could not be reached.

Uses Of ICMP

ICMP is used for error reporting if two devices connect over the internet and some error occurs, So, the router sends an ICMP error message to the source informing about the error. For Example, whenever a device sends any message which is large enough for the receiver, in that case, the receiver will drop the message and reply back ICMP message to the source.
Another important use of ICMP protocol is used to perform network diagnosis by making use of traceroute and ping utility. We will discuss them one by one.

Traceroute: Traceroute utility is used to know the route between two devices connected over the internet. It routes the journey from one router to another, and a traceroute is performed to check network issues before data transfer.

Ping: Ping is a simple kind of traceroute known as the echo-request message, it is used to measure the time taken by data to reach the destination and return to the source, these replies are known as echo-replies messages.

How Does ICMP Works?

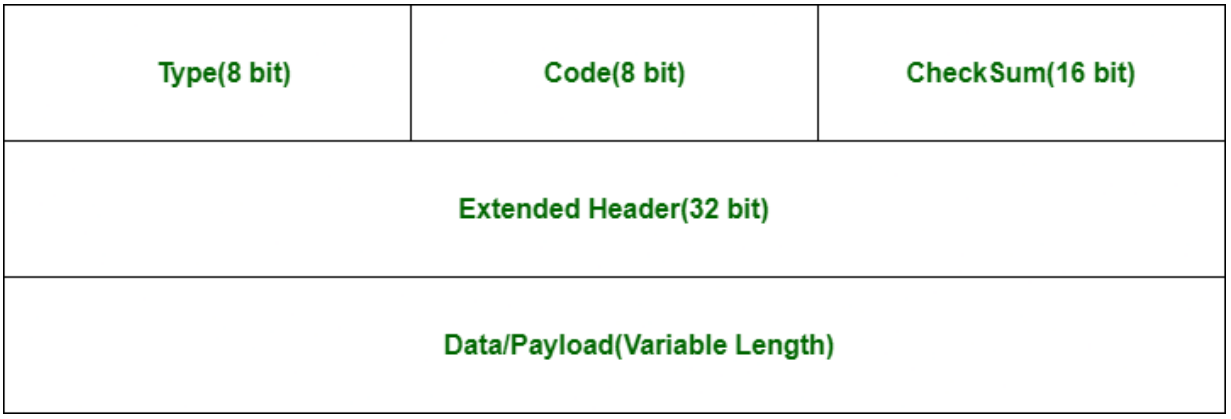
ICMP is the primary and important protocol of the IP suite, but ICMP isn't associated with any transport layer protocol (TCP or UDP) as it doesn't need to establish a connection with the destination device before sending any message as it is a connectionless protocol.
The working of ICMP is just contrasting with TCP, as TCP is a connection-oriented protocol whereas ICMP is a connectionless protocol. Whenever a connection is established before the message sending, both devices must be ready through a TCP Handshake.

ICMP packets are transmitted in the form of datagrams that contain an IP header with ICMP data. ICMP datagram is similar to a packet, which is an independent data entity.

ICMP Packet Format

ICMP Header comes after IPv4 & IPv6 packet header.
In the ICMP packet format, the first 32 bits of the packet contain three fields:
Type (8-bit): The initial 8-bit of the packet is for message type; it provides a brief description of the message so that receiving network would know what kind of message it is receiving and how to respond to it. Some common message types are as follows:

- Type 0 – Echo Reply
- Type 3 – Destination unreachable
- Type 5 – Redirect Message
- Type 8 – Echo request



- Type 11 – Time exceeded
- Type 12 – Parameter problem

Code (8-bit): Code is the next 8 bits of the ICMP packet format, this field carries some additional information about the error message and type
Checksum (16-bit): Last 16 bits are for the checksum field in the ICMP packet header. The checksum is used to check the number of bits of the complete message and enable the ICMP tool to ensure that complete data is delivered.
The next 32 bits of the ICMP Header are Extended Header which has the work of pointing out the problem in IP Message. Byte locations are identified by the pointer which causes the problem message and receiving device looks here for pointing to the problem.
The last part of the ICMP packet is Data or Payload of variable length. The bytes included in IPv4 are 576 bytes and in IPv6, 1280 bytes.

ICMP in DDoS Attacks

In Distributed DOS (DDoS) attacks, attackers provide so much extra traffic to the target, so that it cannot provide service to users. There are so many ways through which an attacker executes these attacks, which are described bw.

Ping of Death Attack

Whenever an attacker sends a ping, whose size is greater than the maximum allowable size, oversized packets are broken into smaller parts. When the sender re-assembles it, the size exceeds the limit which causes a buffer overflow and makes the machine freeze. This is simply called a Ping of Death Attack. Newer devices have protection from this attack, but older devices did not have protection from this attack.

ICMP Flood Attack

Whenever the sender sends so many pings that the device on whom the target is done is unable to handle the echo request. This type of attack is called an ICMP Flood Attack. This attack is

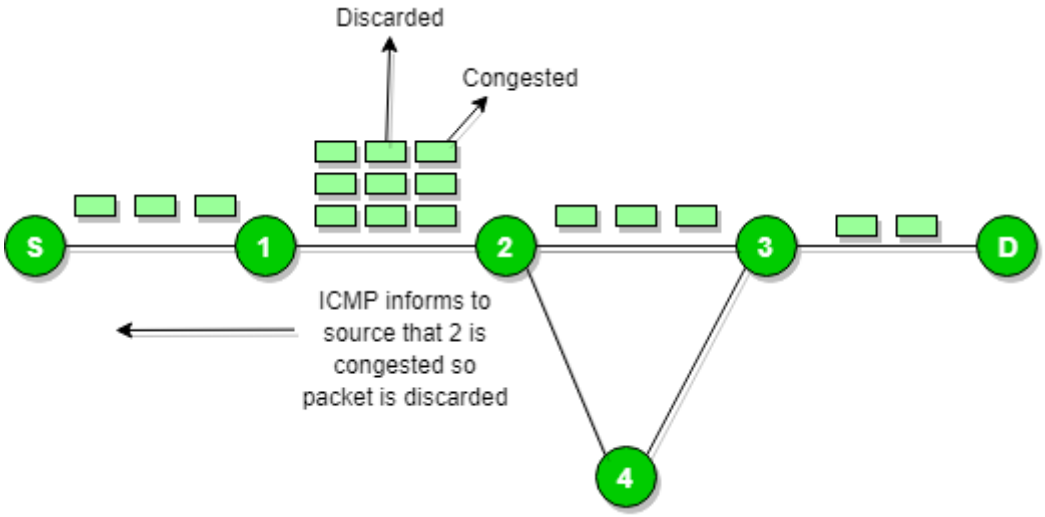
also called a ping flood attack. It stops the target computer's resources and causes a denial of service for the target computer.

Smurf Attack

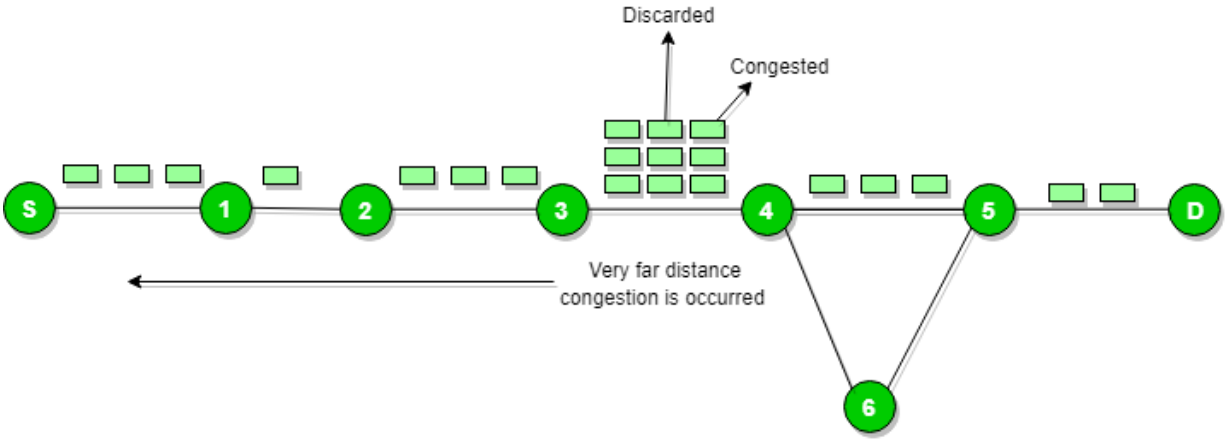
Smurf Attack is a type of attack in which the attacker sends an ICMP packet with a spoofed source IP address. This type of attacks generally works on older devices like the ping of death attack.

Source Quench Message

A



source quench message is a request to decrease the traffic rate for messages sent to the host destination) or we can say when receiving host detects that the rate of sending packets (traffic rate) to it is too fast it sends the source quench message to the source to slow the pace down so that no packet can be lost.

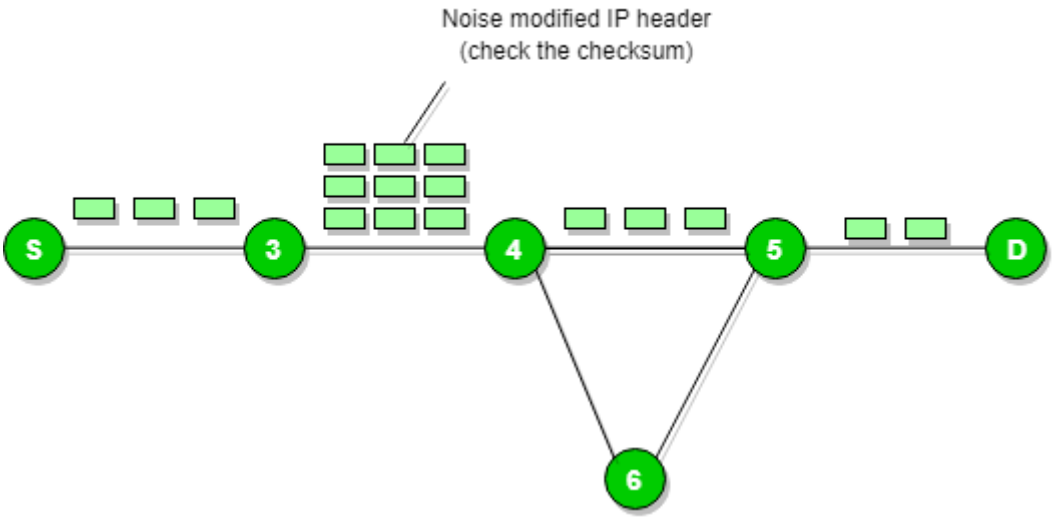


ICMP will take the source IP from the discarded packet and inform the source by sending a source quench message. The source will reduce the speed of transmission so that router will be free from congestion.

When the congestion router is far away from the source the ICMP will send a hop-by-hop source quench message so that every router will reduce the speed of transmission.

Parameter Problem

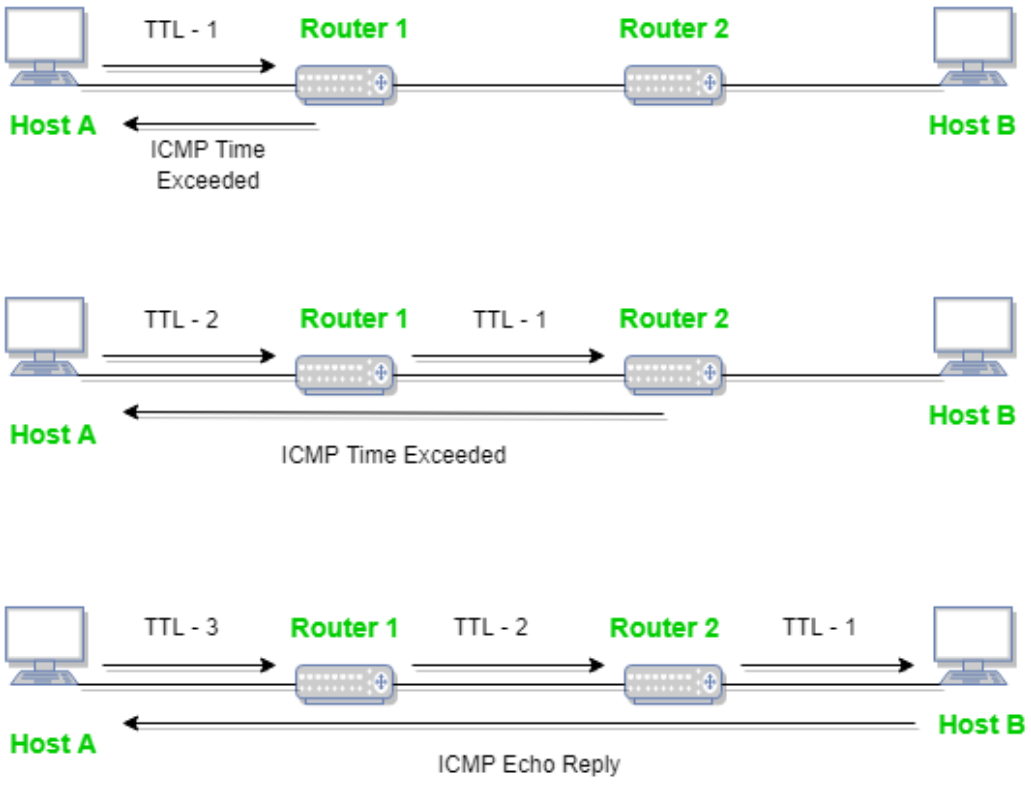
Whenever packets come to the router then the calculated header checksum should be equal to the received header checksum then only the packet is accepted by the router.



If there is a mismatch packet will be dropped by the router.

ICMP will take the source IP from the discarded packet and inform the source by sending a parameter problem message.

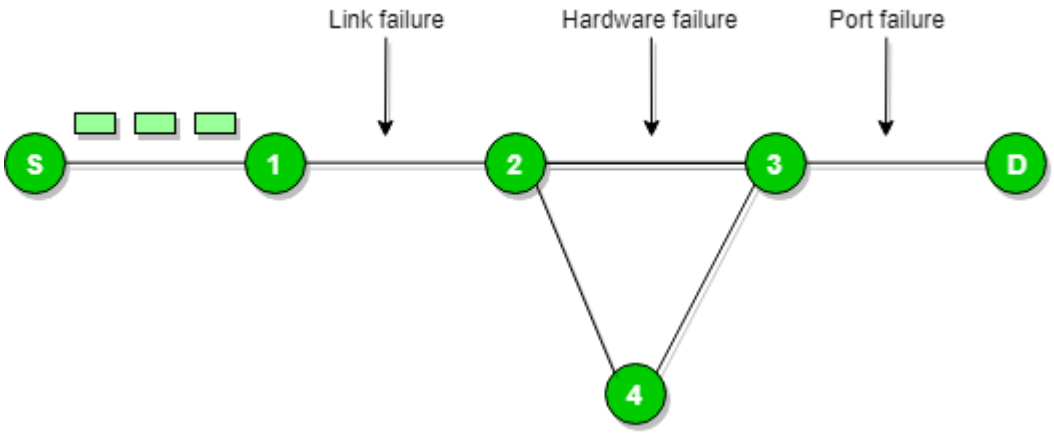
Time Exceeded Message



When some fragments are lost in a network then the holding fragment by the router will be dropped then ICMP will take the source IP from the discarded packet and informs the source, of discarded datagram due to the time to live field reaching zero, by sending the time exceeded message.

Destination Un-reachable

The destination is unreachable and is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason.



There is no necessary condition that only the router gives the ICMP error message time the destination host sends an ICMP error message when any type of failure (link failure, hardware failure, port failure, etc) happens in the network.

Redirection Message

Redirect requests data packets are sent on an alternate route. The message informs a host to update its routing information (to send packets on an alternate route).

Example: If the host tries to send data through a router R1 and R1 sends data on a router R2 and there is a direct way from the host to R2. Then R1 will send a redirect message to inform the host that there is the best way to the destination directly through R2 available. The host then sends data packets for the destination directly to R2.
The router R2 will send the original datagram to the intended destination.
But if the datagram contains routing information, then this message will not be sent even if a better route is available as redirects should only be sent by gateways and should not be sent by Internet hosts.

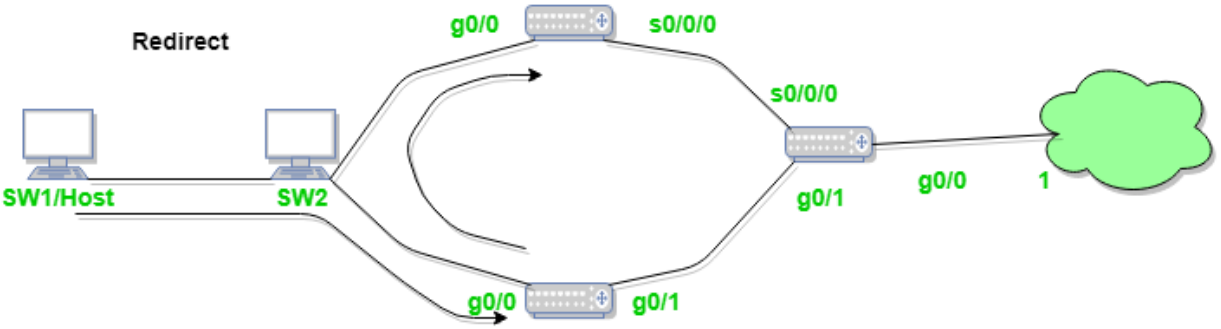


Figure - ICMP redirect Verification CCNP 2.0 100 - 101 (v - 71)

- ICMP Redirect
- ICMP Redirect for host
- ICMP Redirect for network
- How ICMP redirect work
- ICMP Redirect verification step by step

Whenever a packet is forwarded in the wrong direction later it is re-directed in a current direction then ICMP will send a re-directed message.

5.0 Actual resources used:

Sr. No	Name of Resource / Material	Specification	Qty
1	Computer System	16 GB Ram, Windows 11 OS	1
2	Websites	Geeks of Geeks, W3Schools	-
3	Textbook/Manual	Computer Networks "By Andrew S. Tanenbaum and David J. Wetherall"	-

6.0 Skills developed:

1. Teamwork
2. Communication skills
3. Able to get all information about ICMP Protocol

7.0 Application of Micro project:

1) **Network Diagnostics:** ICMP is often used for network troubleshooting and diagnostics. Tools like ping and traceroute use ICMP messages to check if a remote host is reachable and measure round-trip times to it. This helps network administrators identify connectivity issues and measure network latency.

2) **Error Reporting:** ICMP is used to report errors in network operations. For example, if a router encounters a problem while forwarding a packet, it can send an ICMP error message to the source, indicating the issue (e.g., "Destination Unreachable" or "Time Exceeded"). This allows for better error handling and debugging.

3) **Path MTU Discovery:** ICMP is used to perform Path Maximum Transmission Unit (PMTU) discovery. This helps determine the maximum packet size that can traverse a network path without fragmentation, improving the efficiency of data transmission.

4) **Network Redundancy:** In some cases, ICMP can be used to check the availability of redundant network paths. If one path becomes unavailable, ICMP can be used to detect the failure and switch to an alternate route.

5) **Router and Network Device Management:** Network administrators can use ICMP to manage network devices remotely. For example, they can configure routers to respond to ICMP Echo Requests, allowing them to monitor the device's availability and latency.

6) **Firewall and Security:** ICMP can be used to test and assess the security of a network. For example, some security systems and firewalls can be configured to filter or block certain types of ICMP messages to protect against specific types of attacks.

8.0 Conclusion:

The Internet Control Message Protocol (ICMP) plays a critical role in the functioning and maintenance of the Internet. It is a fundamental part of the TCP/IP protocol suite and is primarily used for diagnostics, error reporting, and network management. ICMP enables devices to communicate with each other, report errors, and ensure the reliable delivery of data across networks.

9.0 References:

Books:

- "Advance Computer Network" by Deepali A. Patil (Tech Neo Publications).
- "Computer Networks" by Andrew S. Tanenbaum and David J. Wetherall.

• Websites:

- Oracle: https://www.oracle.com/database/what-is-database/
- W3Schools: https://www.w3schools.com/
- GeeksforGeeks: https://www.geeksforgeeks.org/