People's Democratic Republic of Algeria
Mustapha Stambouli University of Mascara
Faculty of Exact Sciences, Computer Science Department

Network Project: A Look Into The ICMP Protocol

The Concerned Students:
Meliani Mehdi

1st Year Master in Intelligent Systems Engineering

List of Figures

Contents

Chapter 1

Introduction to ICMP

Contents

1.1 What is ICMP?

ICMP (Internet Control Message Protocol) is a network layer protocol used for error reporting and diagnostic purposes in IP networks. It helps devices communicate issues like unreachable hosts or network congestion.

1.2 Why is ICMP Important?

ICMP is important because it enables network devices to report errors, diagnose issues, and manage communication. It supports tools like `ping` and `traceroute`, which are essential for troubleshooting and maintaining network health.

Here are some use cases for ICMP:

1.2.1 Error reporting

ICMP error messages report networking errors, such as unreachable destinations, timeouts, or fragmentation problems. The messages are especially important for User Datagram Protocol (UDP), which has a connectionless communications model.

UDP does not provide reliable, ordered delivery of packets. When a UDP packet is sent, it's possible that the packet may be lost, or it may be delivered with faults such as checksum errors. If this happens, the receiver sends ICMP error reporting messages back to the sender to notify it of the problem.

1.2.2 Diagnostics

You can use ICMP for network diagnostics. It's most commonly used for ping and traceroute commands.

The ping command tests the reachability of network devices by sending ICMP echo request packets to a target device. If the device is reachable, it returns an ICMP echo reply. It reliably checks network latency and ensures the device is available.

The traceroute command traces the path taken by packets from a source to a destination. To do this, the command sends echo request and echo reply messages to the intended destination.

Echo requests contain a time-to-live (TTL) value, which decreases by one each time the packet passes through a router. When a packet reaches a router with a TTL of zero, the router sends an ICMP message back to the source.

The message contains information about the route taken by the packet. Traceroute reveals the exact path of a packet, which can provide you with network performance insights.

1.2.3 Network security

You can use ICMP to detect unauthorized network traffic and permit only legitimate traffic over a network. Firewalls use ICMP to allow or block certain types of traffic. Network administrators also use ICMP monitoring tools to track the status and connectivity of network devices and detect unknown devices.

You can also use it to spot unusual traffic patterns that may indicate unauthorized activity.

1.3 How ICMP Fits into the TCP/IP and OSI Models

ICMP operates at the Network Layer (Layer 3) in the OSI models. In the TCP/IP model, it is part of the Internet Layer (Layer 2), ICMP works alongside IP to provide error reporting and diagnostic functions.
Figure 1.1 illustrates the position of ICMP in both the TCP/IP and OSI models.

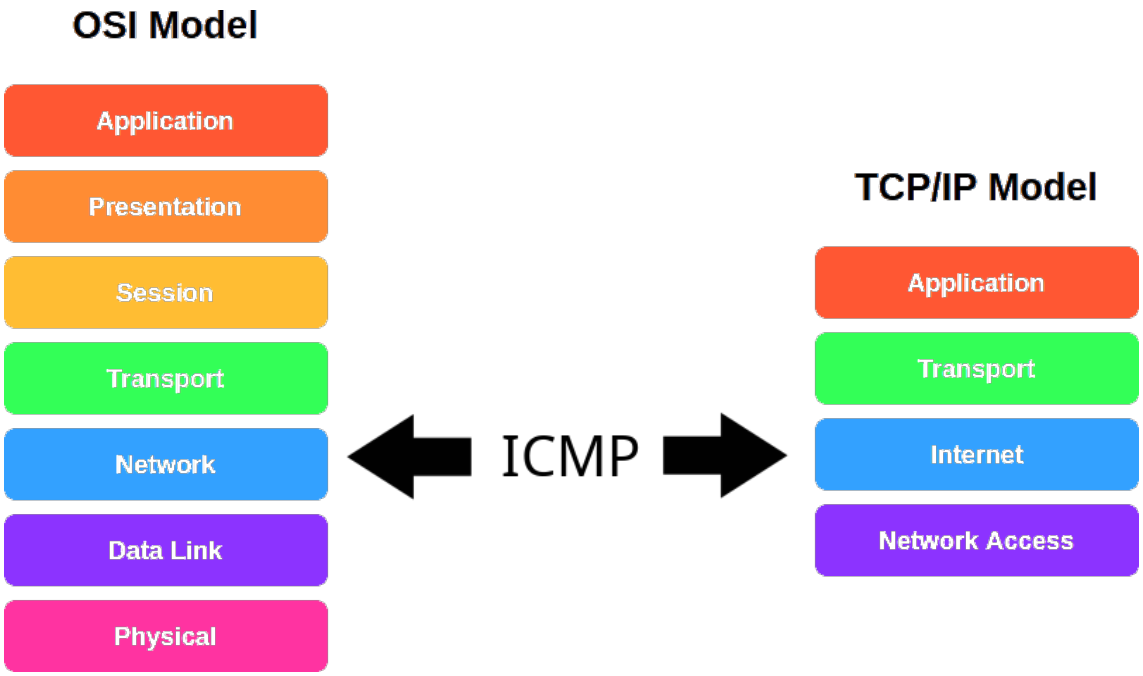

Figure 1.1: Position of ICMP in the TCP/IP and OSI Models

Chapter 2

ICMP Structure

Contents

2.1 ICMP Packet

2.1.1 What is an ICMP packet?

An ICMP packet is a packet that uses the ICMP protocol. ICMP packets include an ICMP header after a normal IP header. When a router or server needs to send an error message, the ICMP packet body or data section always contains a copy of the IP header of the packet that caused the error.

2.1.2 ICMP Packet Format

The ICMP packet structure starts with the first 32 bits, which consist of three primary fields:

- **Type (8-bit):** This field defines the message type and provides a brief description, helping the receiving network identify the message and determine how to respond. Common ICMP message types include:
  - 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):** The next 8-bit field provides additional information about the specific error type or condition, refining the details given by the Type field.
- **Checksum (16-bit):** The final 16 bits of the first 32-bit segment form the checksum, which ensures the integrity of the entire ICMP message by verifying that no data corruption has occurred during transmission.

Following these fields, the **next 32 bits** of the ICMP header act as an **Extended Header**, which identifies errors within an IP message. Specific byte locations of errors are marked using a pointer, allowing the receiving device to pinpoint and analyze the issue.

The **final section** of the ICMP packet is the **Data or Payload**, which has a variable length. For IPv4, this payload typically contains up to **576 bytes**, whereas in IPv6, it extends up to **1280 bytes**.

Type (8 bits)	**Code (8 bits)**	**Checksum (16 bits)**
Rest of Header (32 bits)		
Data (Variable length)		

Table 2.1: ICMP Packet Format

2.2 Understanding ICMP Messages

ICMP messages are identified by their **Type** and **Code** fields. Below are some of the most well-known and widely used ICMP message types and their codes:

- **Echo Request (Type 8, Code 0)**: Sent by tools like `ping` to check if a host is reachable.
- **Echo Reply (Type 0, Code 0)**: Sent in response to an Echo Request to confirm reachability.
- **Destination Unreachable (Type 3)**:
  - **Code 0**: Network Unreachable.
  - **Code 1**: Host Unreachable.
  - **Code 3**: Port Unreachable.
  - **Code 4**: Fragmentation Needed but DF (Don't Fragment) flag set.
- **Time Exceeded (Type 11)**:
  - **Code 0**: TTL (Time to Live) expired in transit.
  - **Code 1**: Fragment reassembly time exceeded.
- **Redirect (Type 5)**:
  - **Code 0**: Redirect for the Network.
  - **Code 1**: Redirect for the Host.
- **Parameter Problem (Type 12, Code 0)**: Indicates an issue with the IP header or options.

These message types and codes are essential for diagnosing and troubleshooting network issues, for more ICMP message type you can refure to the table bellow (table:2.2).

Type	**Code**	**Description**
0 – Echo Reply	0	Echo reply
3 – Destination Unreachable	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation is needed and the DF flag set
	5	Source route failed
5 – Redirect Message	0	Redirect the datagram for the network
	1	Redirect datagram for the host
	2	Redirect the datagram for the Type of Service and Network
	3	Redirect datagram for the Service and Host
8 – Echo Request	0	Echo request
9 – Router Advertisement	0	Used to discover the addresses of operational routers
10 – Router Solicitation	0	
11 – Time Exceeded	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12 – Parameter Problem	0	The pointer indicates an error
	1	Missing required option
	2	Bad length
13 – Timestamp	0	Used for time synchronization
14 – Timestamp Reply	0	Reply to Timestamp message

Table 2.2: ICMP Types and Codes

Chapter 3

CH3 Title

Contents

3.1 Sec 1