ARP and ICMP Protocols

Prepared By
Dr. Islam Zakaria

References

- **ARP**

  https://info.support.huawei.com/info-finder/encyclopedia/en/ARP.html

- **ICMP**

  https://info.support.huawei.com/info-finder/encyclopedia/en/ICMP.html

Introduction

- **Address Resolution Protocol (ARP)** is used to discover the **Layer 2 (MAC)** address of a device on your **local network** when you only know its **Layer 3 (IP) address**.
- **Internet Control Message Protocol (ICMP)** is used for **sending error** and **control messages between network devices**. It's a fundamental support protocol that **helps routers and hosts communicate about** the **health** and **status** of the network, making it possible to **diagnose problems and ensure efficient operation**.

Comparison: ARP vs ICMP

Feature	ARP	ICMP
Layer	2 / 3	3
Purpose	Map IP → MAC	Control, errors, diagnostics
Works in LAN only?	Yes	No (Internet-wide)
Key message	Request / Reply	Echo, Time Exceeded, Unreachable
Security	Weak	Often blocked by firewalls

ARP

Why Do We Need ARP?

- **ARP is required to map IP addresses to MAC addresses.**
- For hosts or other **Layer 3 network devices** to communicate on a **LAN**, the **sender must** know the **destination IP address to which it will send IP packets**.
- **Sender must first** be **encapsulated** with **MAC addresses** before they can be transmitted over the physical network.
- It is therefore **necessary** for **hosts or Layer 3 network devices** to maintain an **ARP table** for **storing the mapping information of IP and MAC addresses**.

What Are the Types of ARP?

1. **Dynamic ARP**
   - It **entries** are **automatically** generated and maintained when **ARP packets** are **sent** and **received**.
   - **They can be aged, updated, or overwritten by Static ARP entries**.
   - **Dynamic ARP applies to complex networks that transmit delay-sensitive services.**

What Are the Types of ARP?

2. Static ARP

- It allows a network administrator to manually create the fixed mappings between **IP** and **MAC** addresses.
- **Static ARP entries cannot be aged or overwritten by dynamic ARP entries, ensuring system security.**
- **In most cases**, devices on a network can use **ARP** to **dynamically** learn **ARP entries** and **age** or **update** the **generated dynamic ARP entries**.
- **However**, when a network **encounters** an **ARP attack**, the **dynamic ARP entries** may be **incorrectly updated** or **aged**.
- **As a result**, the communication between authorized users becomes **abnormal**.

What Are the Types of ARP?

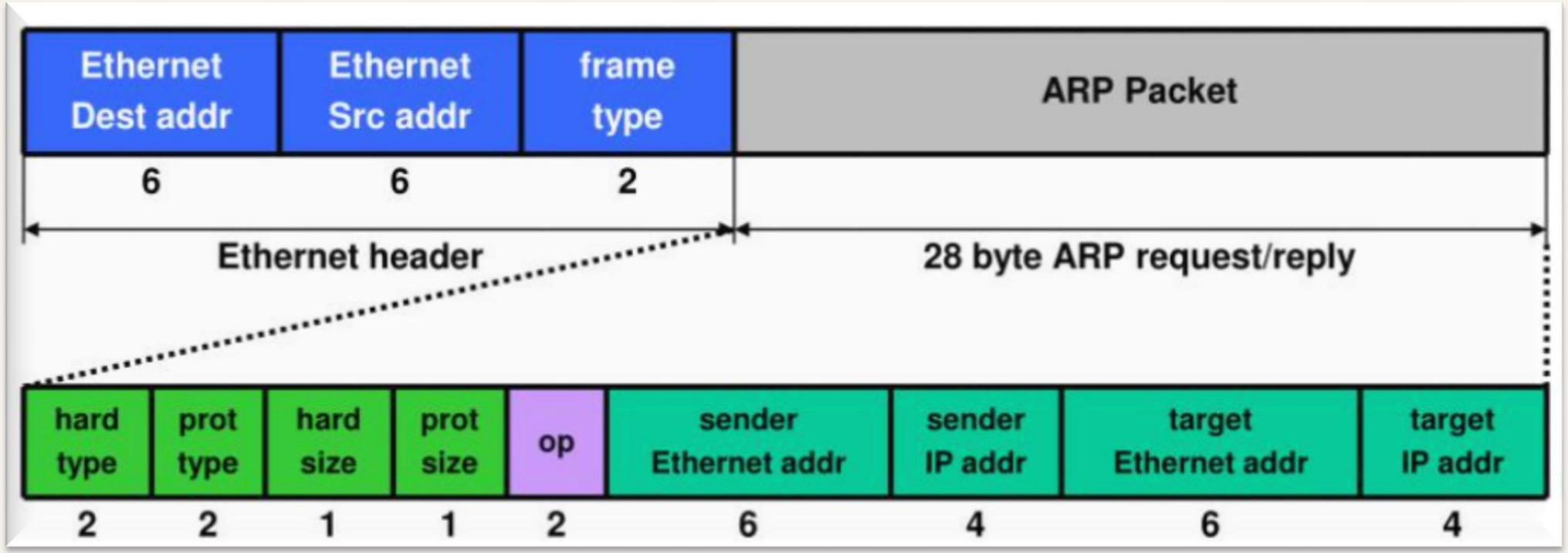
- If a **static ARP** entry is **configured** on a **device**, the **device** can communicate with the **peer device** using **only** the **specified MAC address**.
- **Network attackers** **cannot modify** the **mapping** between the **IP** and **MAC addresses** using **ARP packets**, **ensuring** communication between the two devices.
- **Static ARP entries are generally configured on gateways.**

What Are the Types of ARP?

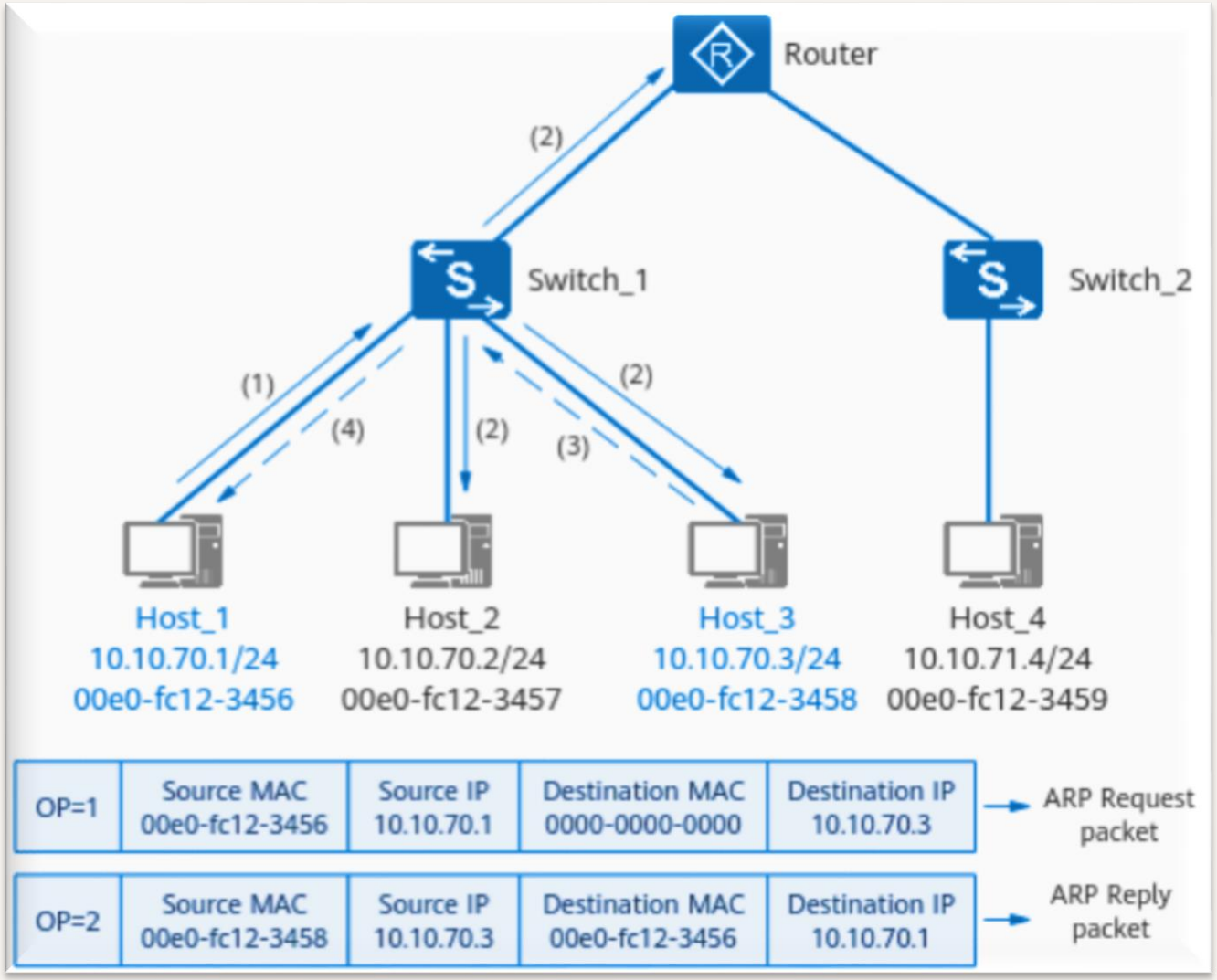
3. Gratuitous ARP

- It allows a device to send an **ARP Request** packet that **carries** its **own IP address** as the **destination IP address**.
- **Gratuitous ARP has the following functions:**
  - **Checks for IP address conflicts.**
  - **Advertises a new MAC address**.

ARP Format


Ethernet Dest addr
Ethernet Src addr
frame type
ARP Packet
6
6
2
Ethernet header
28 byte ARP request/reply
hard type
prot type
hard size
prot size
op
sender Ethernet addr
sender IP addr
target Ethernet addr
target IP addr
2
2
1
1
2
6
4
6
4

How Does ARP Work?



ARP Operation (Example)

- **Assume:**
  - **Host A: 192.168.1.10**
  - **Host B: 192.168.1.20**
  - **Host A** wants to send packet to **Host B**.
- **Step 1: ARP Request (Broadcast)**
  - **Host A** doesn't know **B's MAC**, so it sends **broadcast frame**:
  - **Destination MAC: FF:FF:FF:FF:FF:FF**
  - **Contents:** "Who has **192.168.1.20**?"
- **Step 2: ARP Reply (Unicast)**
  - **Host B** responds directly to **A: 192.168.1.20** is at **MAC: AA:BB:CC:DD:EE:FF**.

ARP Operation (Cont.)

- **Step 3: ARP Cache Update**
  - **Host A** saves **mapping:**

IP	MAC	Timer
192.168.1.20	AA:BB:CC:DD:EE:FF	~2–20 mins

  - **This Timer Handling MAC Address Changes (The device using a specific IP address can change, and thus its MAC address will be different)**

- **Step 4: Communication Begins**
  - Now **Host A** sends actual data to **Host B** using **Layer 2 MAC + Layer 3 IP.**

Problems with ARP

1. **Security Problems**
   - **ARP Spoofing/Poisoning:** Attackers send **fake ARP replies to associate their MAC address with a legitimate IP,** enabling:
     - **Man-in-the-Middle (MitM) attacks for data interception.**
     - **Denial-of-Service (DoS) by redirecting traffic to a non-existent MAC.**
   - **MAC Flooding:** Attackers flood a switch with **fake MAC addresses**, causing the switch to **broadcast traffic to all ports (like a hub)**.
   - **No Authentication:** ARP has no mechanism to verify that an **ARP reply** is from the **legitimate owner** of an **IP address**. **It is a trusting, stateless protocol**.

Problems with ARP

2. **Management & Troubleshooting Problems**
   - **Lack of Scalability:** In **large Layer 2 networks**, the **volume of ARP broadcast traffic can become a significant overhead**.
   - **No Built-in Loop Prevention: ARP frames** are **bridged** like any other traffic, so **network loops can cause ARP frames to circulate endlessly, exacerbating storms**.
3. **Reliability & Network Problems**
   - **IP Address Conflicts:** If two devices have the **same IP**, **ARP caches** on other hosts become **unstable**, **flipping between two MAC addresses and causing broken connectivity**.

ICMP

What Is ICMP?

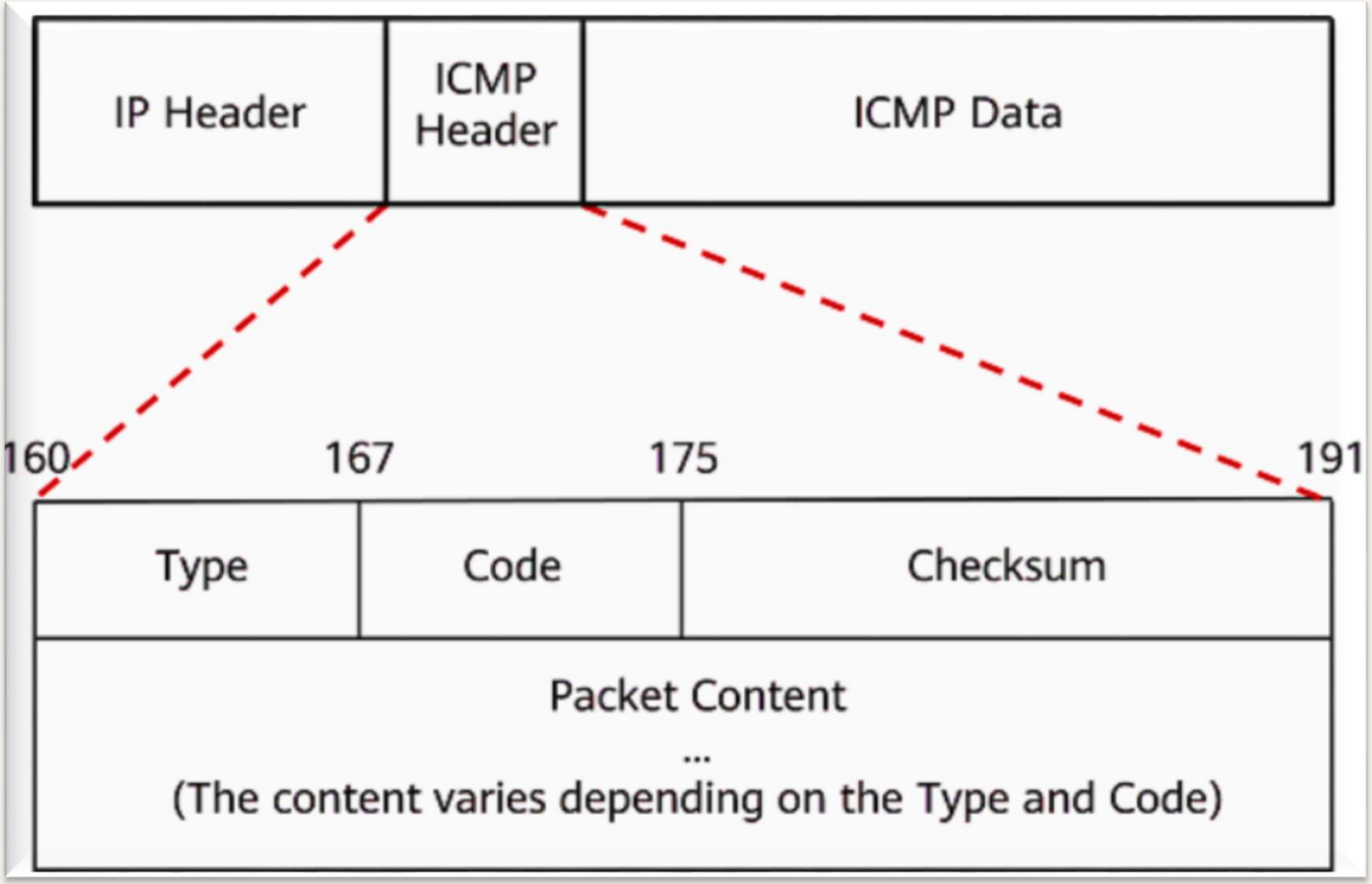
- **ICMP** is a **network layer protocol** used to **transmit control messages** between **hosts** and **routers** to **report whether hosts are reachable and routes are available**.
- It plays an important role in the TCP/IP protocol suite and is typically **used by** the **IP** or **higher layer protocols** (TCP or UDP).
- Although these **control messages do not transmit user data**.

Why ICMP is Needed

- ICMP is essential because IP (Internet Protocol) itself is "unreliable" and lacks built-in mechanisms for diagnostics and error reporting. ICMP fills this critical gap.

1. **For Error Reporting and Signaling.**
   - **Informs Senders of Delivery Failures.**
   - **Prevents Packet Loops:** Sends **"Time Exceeded"** messages when a packet's TTL (Time to Live) reaches zero.
2. **For Network Diagnostics and Troubleshooting**
   - **Connectivity Testing:** The **ping** command uses **ICMP Echo Request** and **Reply** to **verify** if a **remote host** is **online** and **reachable**, and to measure **round-trip latency**.
   - **Path Discovery:** The **traceroute** (or **tracert**) **command** uses **ICMP Time Exceeded** and **Destination Unreachable** messages to **map** the **entire network path between source and destination**.

ICMP Message Format



ICMP Message Format (Cont.)

Field	Size (Bytes)	Description
Type	1	**Identifies the general category of the ICMP message.** ➢ **0** = **Echo Reply** ➢ **8** = **Echo Request** ➢ **3** = **Destination Unreachable** ➢ **11** = **Time Exceeded**
Code	1	**Provides more specific detail within the given Type.** **e.g., For Type 3 (Destination Unreachable):** ➢ **0** = **Network unreachable** ➢ **1** = **Host unreachable** ➢ **3** = **Port unreachable**
Checksum	2	**Error-checking value for the entire ICMP message.** **Used to detect corruption during transmission.**

Common ICMP Messages

1. **Echo Request / Echo Reply (ping)**
   - **Used to test**: **Host reachability**, **Round-trip time**, and **Packet loss**.
   - **Ping** = **ICMP Type 8** (**request**) and **Type 0** (**reply**).
   - **Example:**

```
C:\Users\Islam Zakaria>ping www.youtube.com

Pinging youtube-ui.l.google.com [142.250.180.174] with 32 bytes of data:
Reply from 142.250.180.174: bytes=32 time=66ms TTL=111
Reply from 142.250.180.174: bytes=32 time=98ms TTL=111
Reply from 142.250.180.174: bytes=32 time=66ms TTL=111
Reply from 142.250.180.174: bytes=32 time=67ms TTL=111

Ping statistics for 142.250.180.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 66ms, Maximum = 98ms, Average = 74ms
```

Fields explained:

bytes → **packet payload**

time → **RTT**

TTL → **remaining hops**

Common ICMP Messages (Cont.)

2. Destination Unreachable (Type 3)

- Generated when a router or host cannot deliver a packet.
- Common codes:

Code	Meaning
0	Network unreachable
1	Host unreachable
3	Port unreachable
4	Fragmentation needed (MTU issue)

Common ICMP Messages (Cont.)

3. Time Exceeded (Type 11)

- **Used by traceroute.**
- **Occurs when:**
  - **TTL** becomes **zero**, so **packet is dropped**.
  - **Router** sends **ICMP Time Exceeded** back to sender
- **Routers decrement TTL by 1 each hop**.

```
C:\Users\Islam Zakaria>tracert www.youtube.com

Tracing route to youtube-ui.l.google.com [142.251.209.46]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  DESKTOP-1LD9KH9 [192.168.1.1]
  2    29 ms    29 ms    30 ms  197.161.132.1
  3    31 ms    28 ms    28 ms  172.24.144.73
  4    28 ms    28 ms    28 ms  172.24.144.53
  5    28 ms    30 ms    28 ms  172.19.1.241
  6    29 ms    29 ms    29 ms  81.10.87.222
  7    70 ms    67 ms    71 ms  93.186.129.182
  8    66 ms    66 ms    65 ms  93.186.129.45
  9    66 ms    66 ms    67 ms  72.14.221.64
 10    66 ms    67 ms    66 ms  192.178.96.161
 11    99 ms    66 ms    66 ms  142.251.235.177
 12    66 ms    66 ms    66 ms  mil04s51-in-f14.1e100.net [142.251.209.46]

Trace complete.
```

ICMP in Real-World Tools

1. **ping (Connectivity Test)**
   - Sends **ICMP Echo Request** (**Type 8**) to target.
   - Target replies with **ICMP Echo Reply** (**Type 0**).
   - **Measures: Reachability**, **Round-trip Time (Latency)**, **Packet Loss.**
2. **traceroute/tracert (Path Discovery)**
   - Uses **ICMP Time Exceeded messages** (**Type 11**)
   - Sends packets with increasing **TTL** values
   - Each router along path sends **ICMP Time Exceeded** when **TTL=0**
   - **Maps entire network path to destination**
3. **Path MTU Discovery**
   - Uses **ICMP Fragmentation Needed messages** (**Type 3**, **Code 4**)
   - **Discovers maximum packet size without fragmentation**
   - **Automatically adjusts packet size for optimal performance**

ICMP in Real-World Tools (Cont.)

4. **Destination Unreachable Diagnostics**
   - Helps identify why connections fail
5. **Network Monitoring Systems**
   - Use ICMP Echo for continuous availability monitoring
   - Alert when hosts become unreachable
   - Track latency and jitter over time
6. **Router Redirect Function**
   - Routers inform hosts of better network paths
   - Optimizes local network routing
7. **Error Reporting in Applications**
   - Operating systems use ICMP messages to report connection failures
   - e.g., "Connection refused" from Port Unreachable messages
   - "No route to host" from Host/Network Unreachable messages

ICMP Attacks

1. **Reconnaissance Attacks**
   - **Host Discovery**: Attackers use ping to identify live hosts on a network
   - **Network Mapping**: traceroute reveals network topology and firewall locations
   - **OS Fingerprinting**: Analyzing ICMP response behavior to identify operating systems.
2. **Denial of Service (DoS) Attacks**
   - **ICMP Flood**: Overwhelm target with massive amounts of ICMP Echo Requests
   - **Ping of Death**: Oversized ICMP packets cause buffer overflow and system crashes
3. **Redirect Attacks**
   - **ICMP Redirect**: Attackers send fake redirect messages to poison routing tables

ICMP Security Measures

1. **Filtering & Blocking**
   - Block unnecessary ICMP types at network perimeter
   - Use stateful inspection to only allow replies to outbound requests
   - Implement rate limiting to prevent flood attacks
2. **ICMP Type Management**
   - **Allow:** Echo Reply (0), Destination Unreachable (3), Time Exceeded (11)
   - **Block:** Redirect (5), external Echo Requests (8), Address Mask Requests (17)
3. **Monitoring & Detection**
   - Detect unusual ICMP patterns and volumes
   - Inspect payloads for hidden data
   - Log suspicious ICMP messages

ICMP Security Measures (Cont.)

4. **Host Hardening**
   - Disable ICMP on critical servers when possible
   - Harden OS ICMP stack settings
   - Use host-based firewalls for granular control

Any Questions