

# The Network Engineer's IPv4 Troubleshooting Toolkit

A visual reference guide to diagnostic commands, protocols, and end-to-end connectivity verification.



# The Troubleshooting Framework

Systematic network troubleshooting requires selecting the right tool to verify operation, analyze behavior, and isolate failures.

OSI Layer 3 | Network

Protocol: ICMP

**CCNA Pro-Tip:**

Always start with the physical layer and work your way up, but confirm local configuration first with ARP & IP Config.



## Monitoring

System Logging  
(The Network's Diary)



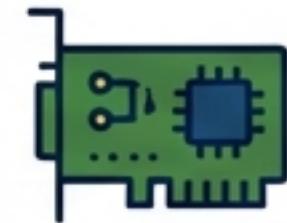
## Protocol Base

ICMP  
(The Language of Errors)



## Path Testing

Ping & Traceroute  
(Verifying Reachability)



## Endpoint Verification

ARP & IP Config  
(Local Mappings)

# System Logging: The Network's Diary

## Key Commands:

```
show logging
```

```
terminal monitor
```

### CCNA Pro-Tip:

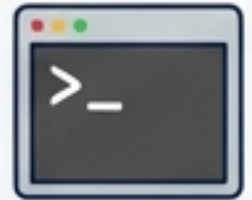
- Logs record events with Timestamps and Severity Levels (0-7).
- Level 0 is highest severity; Level 7 is lowest (debugging).

!  
%LINK-3-UPDOWN: Interface  
Ethernet0/0 changed state to up



Console

✓ Default



Terminal  
Monitor



Memory  
Buffer



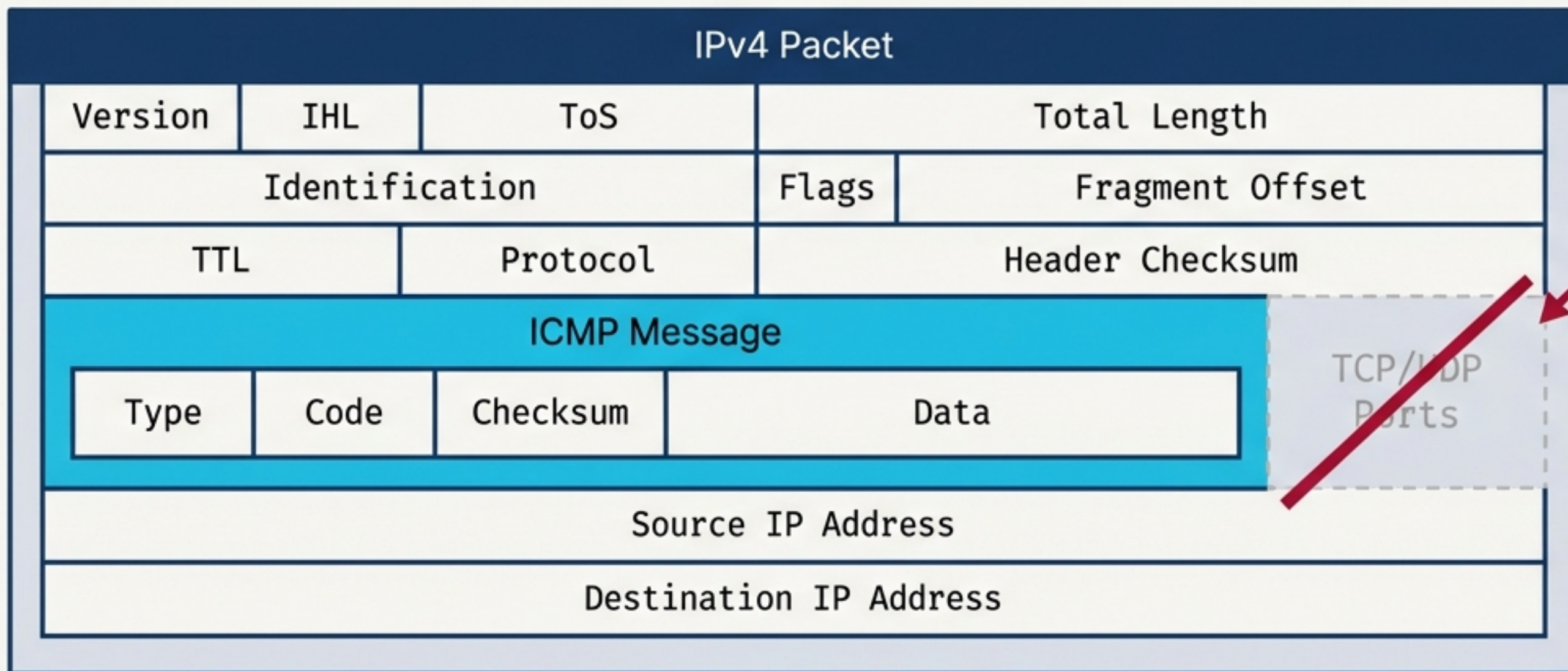
External  
Syslog Server



# ICMP: The Language of Network Errors

ICMP allows devices to report errors and diagnostic info about IP packet delivery. It is the underlying engine for tools like Ping and Traceroute.

## Anatomy of a Packet



ICMP does not use port numbers. It operates directly with IP at Layer 3.

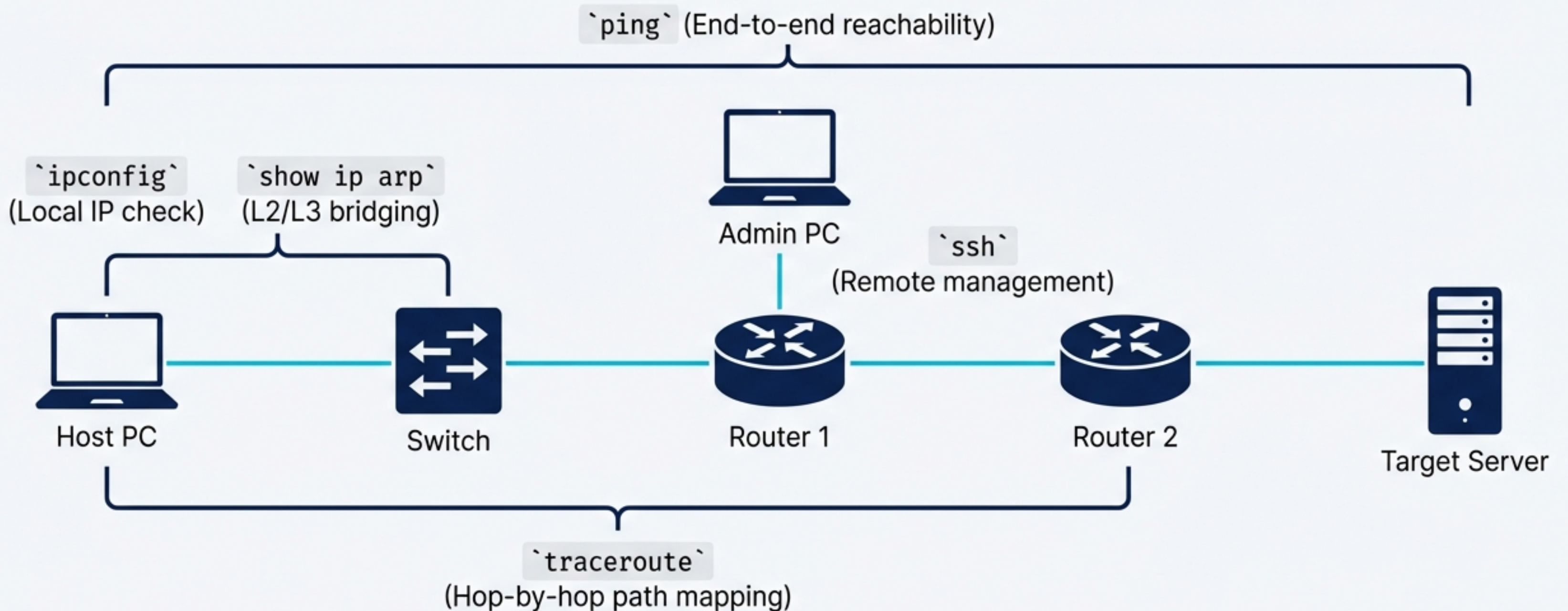
**CCNA Pro-Tip:** ICMP messages are encapsulated directly inside IP packets. No port numbers are used.

# End-to-End Connectivity Testing

OSI Layers 3-4

Protocol: ICMP, TCP, UDP

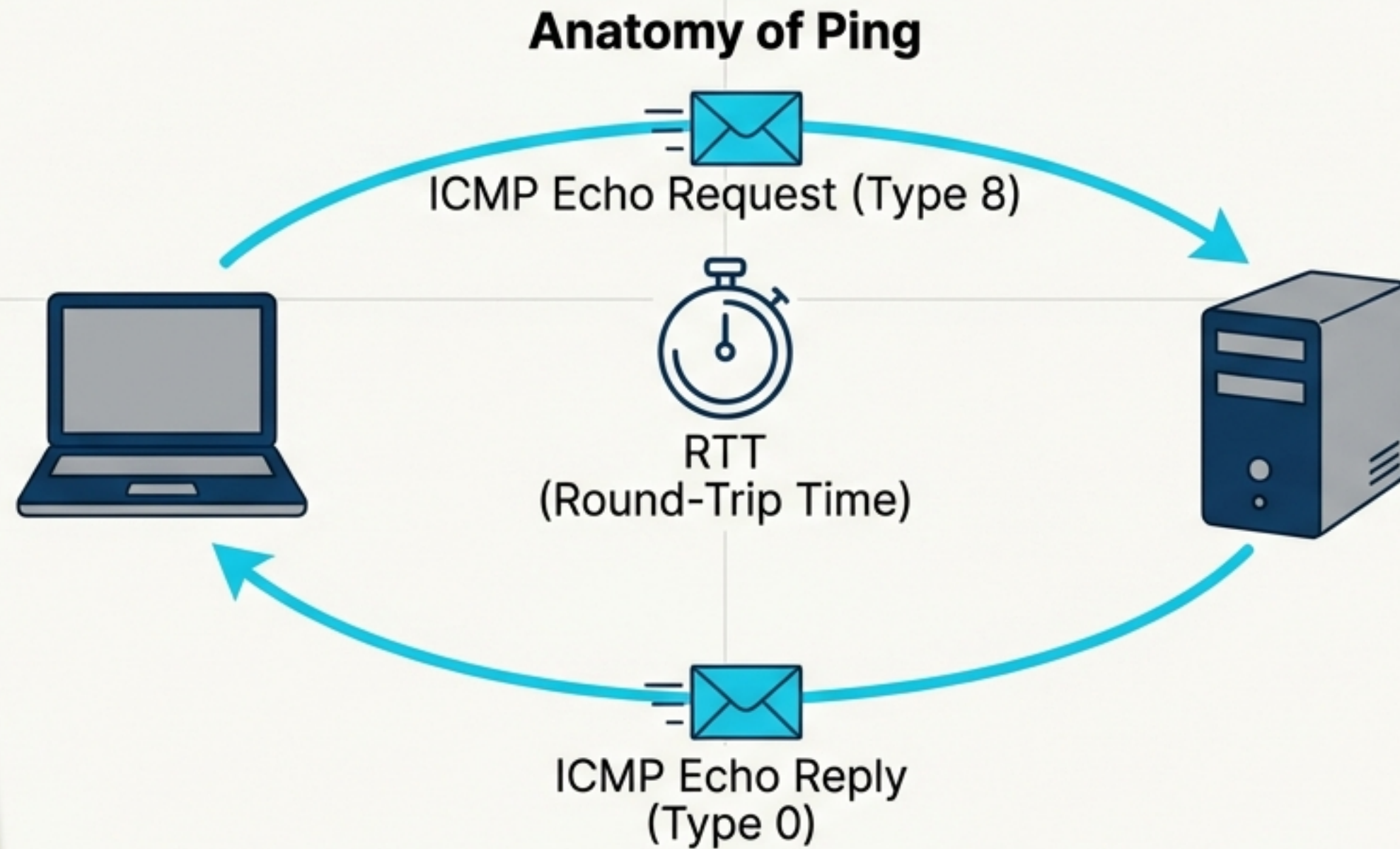
Connectivity tests verify communication across Layer 3 and Layer 4. Different tools test different segments of the network path.



# Ping: Testing Reachability

Uses ICMP to verify reachability, measure Round-Trip Time (RTT), and detect packet loss.

```
ping 10.10.50.1
```



## CCNA Pro-Tip:

Always remember:  
Ping relies on ICMP  
Echo Request and  
Echo Reply messages.

# Decoding Cisco IOS Ping Responses



Reply received  
(Success)



Timeout  
(No reply)



Destination  
unreachable  
(ICMP  
unreachable  
received)



Source  
quench /  
too busy  
(rare/  
obsolete)



Can't fragment  
(MTU issue,  
often DF set)



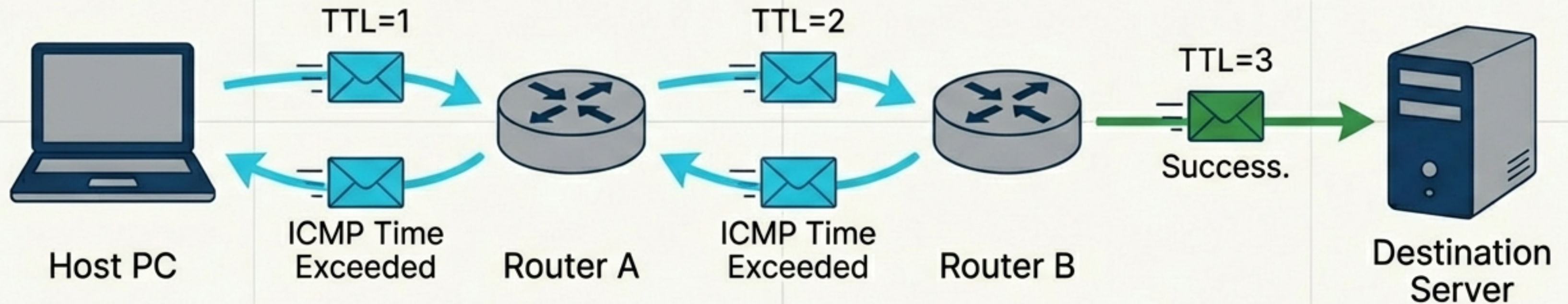
Unknown  
packet type



Packet lifetime  
exceeded  
(TTL expired)

# Traceroute: Mapping the Path

Sends packets with increasing TTL values. As TTL hits zero, routers discard the packet and return an ICMP Time Exceeded message, revealing their IP.



## Cisco IOS

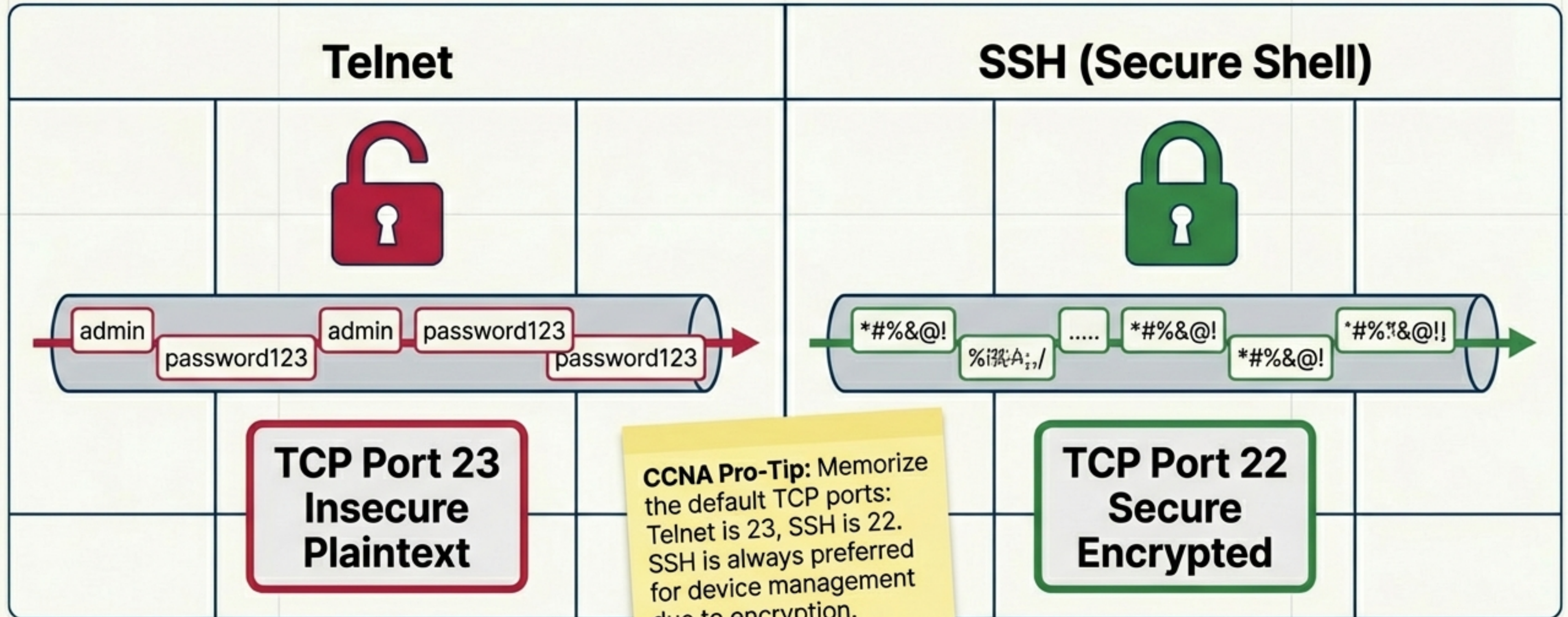
```
traceroute 10.10.50.2
```

## Microsoft Windows

```
tracert 10.10.50.2
```

# Remote Access: Telnet vs. SSH

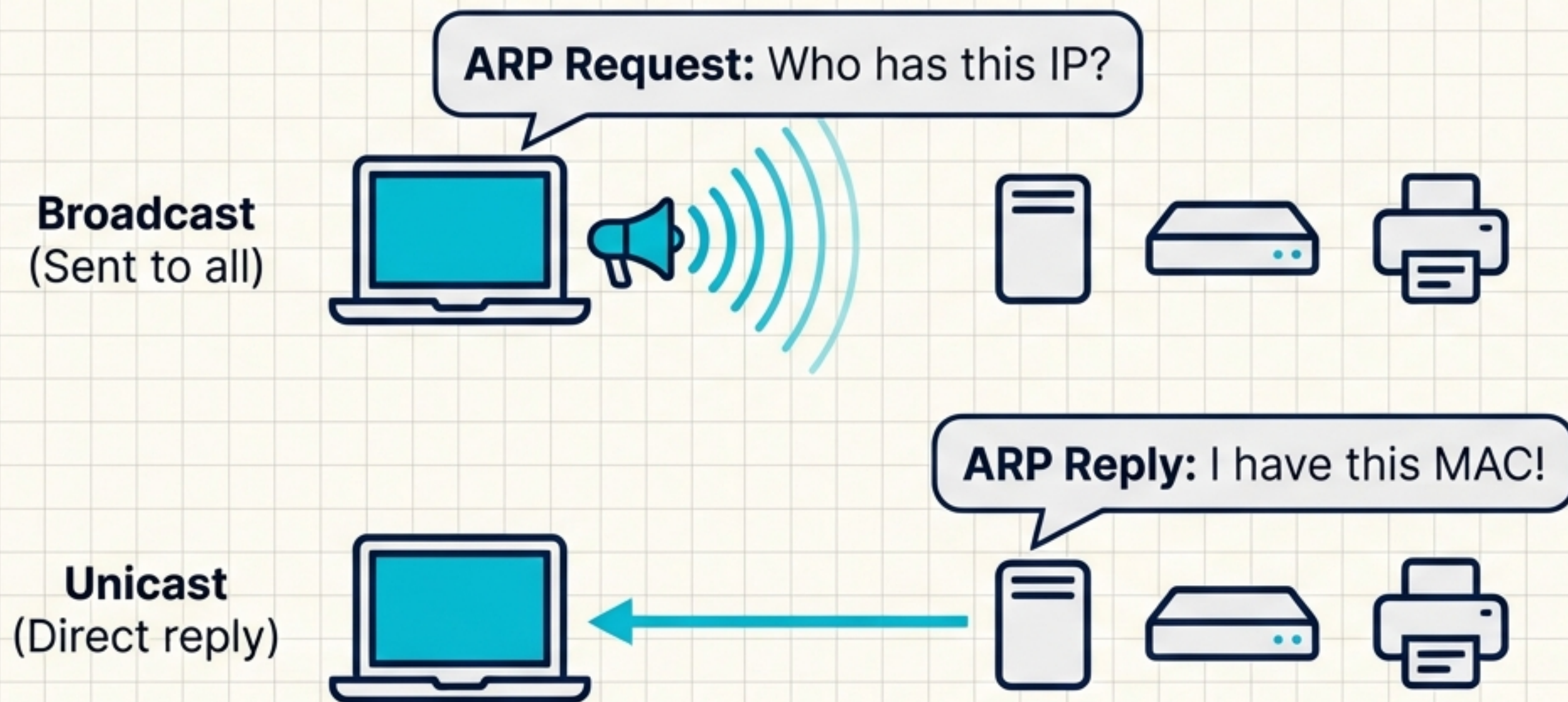
Can test specific TCP port connectivity (e.g., `telnet 10.10.50.2 80` tests if HTTP port 80 is open).



# ARP: Bridging L2 and L3

Maps IPv4 addresses to MAC addresses within a local network.

```
show ip arp
```



**CCNA Pro-Tip:**  
ARP only operates on local networks. The Request is a Broadcast; the Reply is a Unicast.



# ICMP Deep Dive: Types & Codes

Inter OSI Layer 3

Inter Protocol: ICMP

Type 8



Echo Request  
("Are you there?")

Type 0



Echo Reply  
("Yes, I'm here")

Type 11



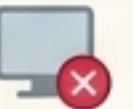
Time Exceeded  
("TTL hit 0")

## Type 3: Destination Unreachable ("I can't reach it")

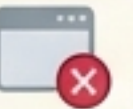
Code 0: Net Unreachable



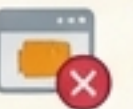
Code 1: Host Unreachable



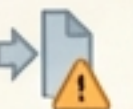
Code 2: Protocol Unreachable



Code 3: Port Unreachable



Code 4: Fragmentation Needed (DF Set)



Minor Types: Type 5 (Redirect), Type 9/10 (Router Adv/Sol)

# The CCNA Quick Reference Matrix

Essential ICMP mappings for exam and diagnostic recall.

Inter OSI Layer 3

Inter Protocol: IP, ICMP

**Tool:  
Ping**

**Requires:  
ICMP Type 8 &  
Type 0**

**CCNA  
Study  
Material**

**Problem:  
"Can't reach  
destination"**

**Look for:  
ICMP Type 3**

**Tool:  
Traceroute**

**Relies on:  
ICMP Type 11**

# The Command Cheat Sheet

Inter OSI Layer 3

Inter Protocol: IP, ICMP

Network Task	Cisco Command	Windows Command
Test Basic Connectivity	<code>ping</code>	<code>ping</code>
Map Network Path	<code>tracert</code>	<code>tracert</code>
Verify Local Interface	<code>show ip int brief</code>	<code>ipconfig /all</code>
View MAC/IP Mappings	<code>show ip arp</code>	<code>arp -a</code>
Check System Events	<code>show logging</code>	N/A (Event Viewer implied)
Test TCP Port Open	<code>telnet [ip] [port]</code>	<code>telnet [ip] [port]</code>

**CCNA Pro-Tip:** Master these core commands for rapid diagnostics. Practice using both Cisco and Windows variations!

# The Troubleshooting Process

Mastering these commands is only the beginning. True network mastery comes from combining them into a structured diagnostic methodology.

