# Lab 04: Assignment: Ping Utility Analysis

Objective:

In this assignment, you will analyze the ping utility, a fundamental network diagnostic tool. You will explore its functionality, usage, and output, and demonstrate your understanding through a series of tasks.

Tasks:

1. Ping Basics

# Explain the purpose of the ping utility and its basic syntax.

**Ans :** The ping utility is used to test the connectivity between your computer and a network device (such as a server) by sending ICMP (Internet Control Message Protocol) Echo Request packets and waiting for a reply. It's commonly used to check if a network device is reachable and to measure the round-trip time of the packets.

Syntax : ping <website>

# Provide examples of how to use ping to test connectivity to a website and a local host. Ans :

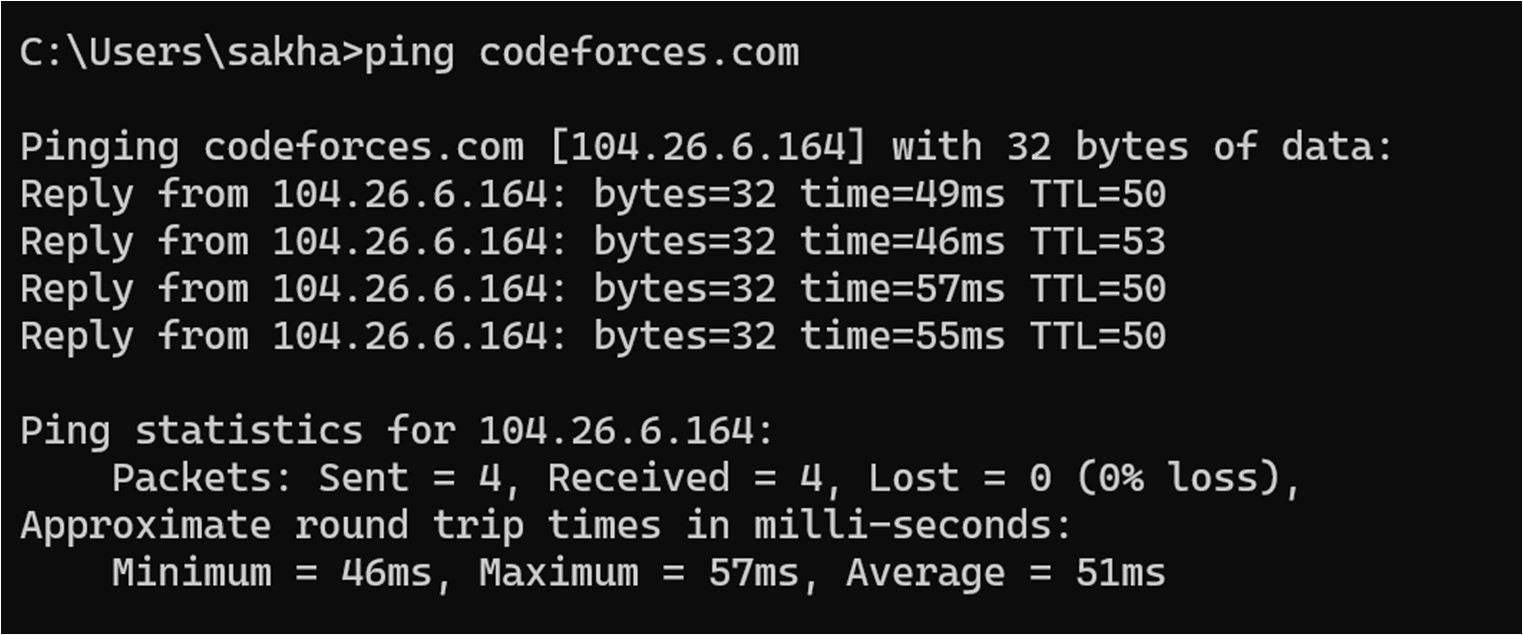
ping <website>

ping Amazon.com

ping 127.0.0.1

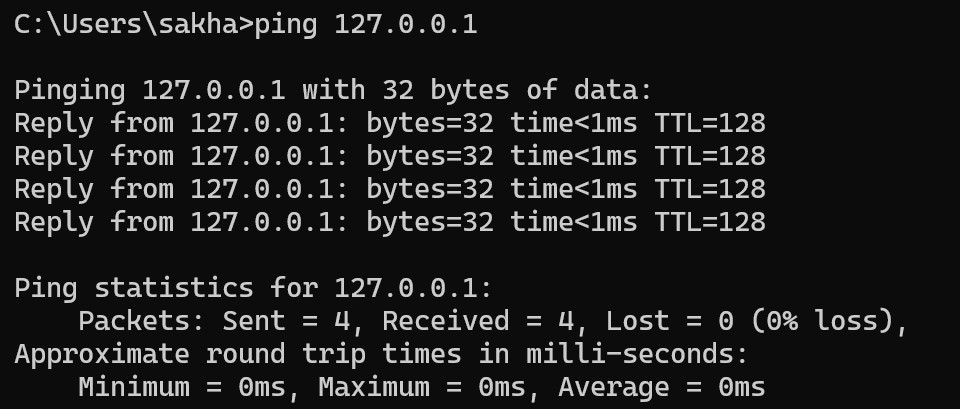
1. Ping Output Analysis

# Run the command ping (link unavailable) and capture the output.



* + **Analyze the output, explaining each line and its significance (e.g., packet loss, round-trip time, etc.).**
    - Here 32 bytes of data packet is being received and sent. (to 104.26.6.164 (codeforces.com)
    - Round trip time for first packet to go to the server and back is 49ms, then 46ms, then 57 ms, and 55 ms
    - As we can see here 4 packets were sent and 4 were received so 0 packets were lost and hence 0% loss.
    - TTL : time to live for every packet tells us how many hops is the packet allowed to make ( the number of routers in between)

# Repeat the process for a local host (e.g., ping 127.0.0.1).



**Analysis :**

* + - Here 32 bytes of data packet is being received and sent. (to 127.0.0.1(localhost)
    - Round trip time for all the packages is <1ms (almost instantaneous because its localhost running on the same machine)
    - As we can see here 4 packets were sent and 4 were received so 0 packets were lost and hence 0% loss.
    - TTL : time to live for every packet tells us how many hops is the packet allowed to make ( the number of routers in between)

1. Ping Options

# Research and explain the following ping options:

The -c (count) option in the ping utility allows you to specify the number of ICMP Echo Request packets to send to the target. By default, ping continues to send packets until manually stopped, but using -c lets you define a specific number, making it useful for controlled testing. For example, ping -c 5 example.com will send exactly five packets and then terminate, providing a concise summary of the connection's performance.

The -s (size) option lets you define the size of the ICMP Echo Request packets in bytes. By default, the packet size is typically 56 bytes (resulting in 64 bytes of data including the ICMP header). Adjusting the size with -s can help in understanding how the network handles different amounts of data. For instance, ping -s 64 example.com sends packets of 64 bytes, which can be useful for testing the network's behavior under varying data loads.

The -t (ttl) option sets the Time to Live (TTL) for each packet. TTL is a value that determines the maximum number of hops (or routers) a packet can pass through before it is discarded. This option is useful for tracing the path packets take to reach their destination or for testing how far your packets can go in the network. For example, using ping -t 10 example.com limits the packet to 10 hops, helping diagnose issues related to routing or distance.

The -W (deadline) option specifies the maximum time, in seconds, that ping will wait for a response before it stops. Unlike -c, which limits the number of packets, -W sets a time limit on how long the command will run, regardless of the number of packets sent or received. For instance, ping -W 5 example.com will stop after 5 seconds, which is useful when you want to ensure that ping doesn't run indefinitely if the target is unreachable.

# - Provide examples of how to use each option.

Examples :

-c : ping -c 4 amazon.com , will only send 4 packets

-s : ping -s 100 amazon.com, will send packets of size 100 bytes

-t : ping -t 10 amazon.com, will send packets with ttl 10

-W : ping -W 10 amazon.com, will send packets with with a deadline of 10 second

1. Troubleshooting with Ping

# Describe a scenario where ping would be used for network troubleshooting (e.g., connectivity issues, slow network speeds).

* + **Explain how to use ping to diagnose the issue, including which options to use and why.**

### Scenario: Diagnosing Slow Network Speeds

Imagine you're experiencing slow network speeds when trying to access a website. You suspect that there might be a problem with your internet connection, a specific router along the path, or the destination server itself. To troubleshoot this issue, you can use the ping utility.

### Using Ping to Diagnose the Issue

1. **Basic Connectivity Check:** Start by using a simple ping command to the website (e.g., ping example.com). This will help you determine if your computer can reach the website at all. If the ping command returns responses, you know there's basic connectivity. If there are timeouts or packet loss, this indicates a problem with reaching the server.
2. **Check for Packet Loss:** Use the -c option to send a specific number of packets, such as ping -c 10 example.com. By sending a limited number of packets (e.g., 10), you can see if there are any lost packets, which might indicate issues like network congestion or a faulty connection.
3. **Measure Latency:** High latency (long round-trip times) can be a sign of slow network speeds. You can measure this by observing the time (in milliseconds) it takes for each ping response to return. If the latency is consistently high, it could indicate a problem with the network's speed or a congested route.
4. **Check for Routing Issues:** Use the -t option to set the Time to Live (TTL) value and track how far the packets travel before being dropped. For example, ping -t 10 example.com limits the hops to 10. If the packets are being dropped before reaching their destination, it could indicate a routing issue along the path.
5. **Test with Different Packet Sizes:** Sometimes, specific packet sizes can cause issues in the network. You can use the -s option to send different-sized packets (e.g., ping -s 128 example.com) and see if larger or smaller packets are causing delays. This can help identify issues like fragmentation problems or maximum transmission unit (MTU) mismatches.
6. **Set a Deadline:** If you're testing connectivity over a period and want to ensure ping doesn't run indefinitely, use the -W option (e.g., ping -W 5 example.com) to limit the test to a specific time frame. This is useful for getting a quick snapshot of network performance without committing to a long-running test.

By using these ping options strategically, you can diagnose whether the issue lies with your local connection, a specific router, or the destination server, helping you pinpoint the cause of the slow network speeds.

# Develop a ping type utility using Scapy. It should have the following points.

* + 1. Basic Functionality
  + Ensure the provided code works correctly.
  + Test with different destination IPs and counts.

1. Additional Features
   * Implement the following features:
     + Option to specify TTL (Time-To-Live)
     + Option to specify packet size
     + Option to specify timeout
   * Use Scapy's built-in functions to implement these features.
2. Error Handling
   * Add error handling for cases like:
     + Invalid destination IP
     + Invalid count or TTL values
     + Timeout errors
   * Use try-except blocks to catch and handle exceptions.
3. Output Formatting
   * Improve the output formatting to include:
   * Packet loss percentage
   * Average RTT (Round-Trip Time)
   * Maximum and minimum RTT values

- Use Python's built-in formatting options to create a clean output.

