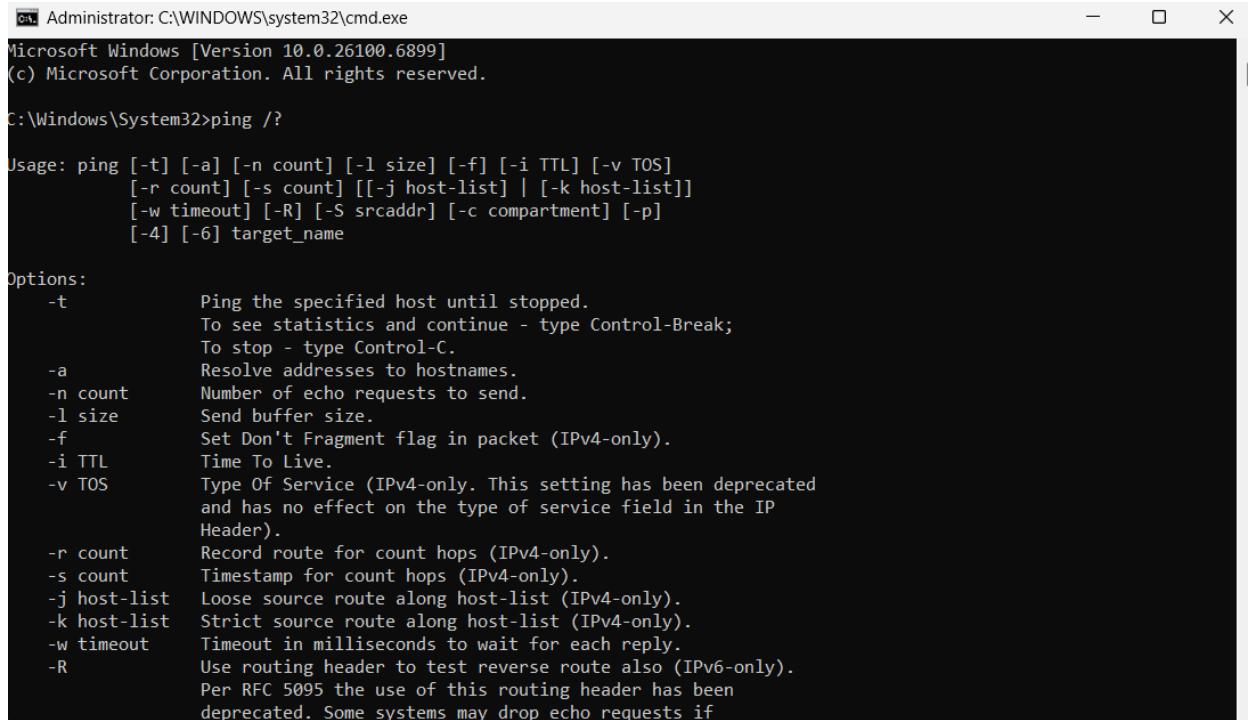
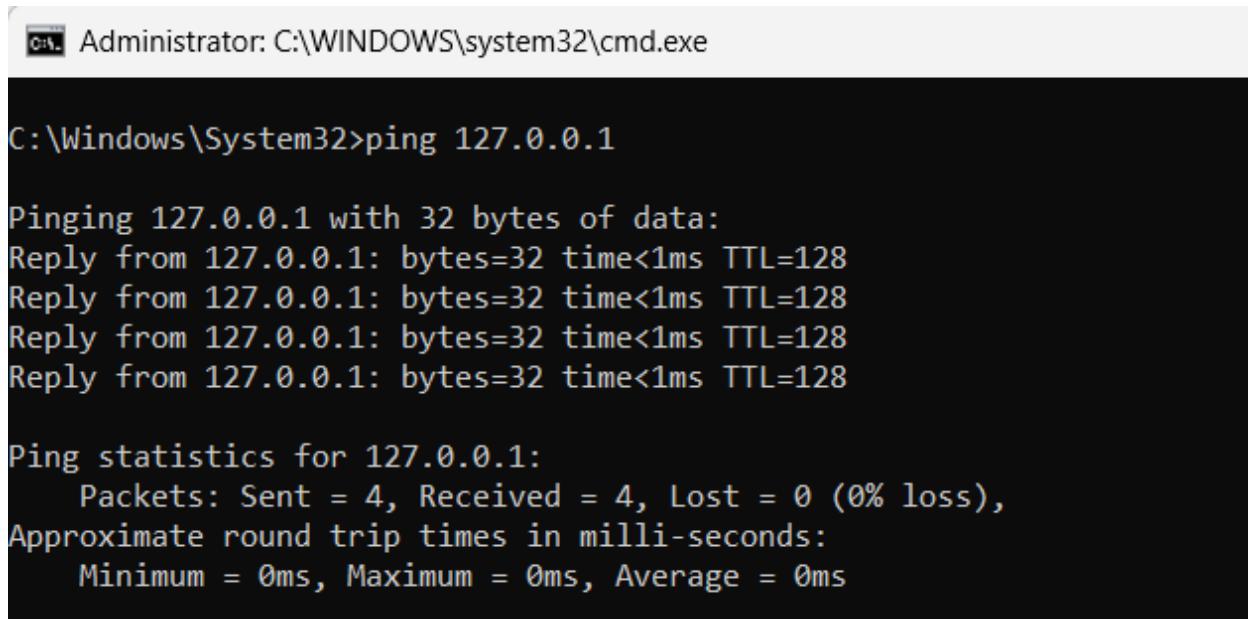


# Task 3: Basic Networking Commands

## 1 ping — Test Network Connectivity



Administrator: C:\WINDOWS\system32\cmd.exe  
Microsoft Windows [Version 10.0.26100.6899]  
(c) Microsoft Corporation. All rights reserved.  
C:\Windows\System32>ping /?  
  
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]  
 [-r count] [-s count] [[-j host-list] | [-k host-list]]  
 [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]  
 [-4] [-6] target\_name  
  
Options:  
 -t Ping the specified host until stopped.  
 To see statistics and continue - type Control-Break;  
 To stop - type Control-C.  
 -a Resolve addresses to hostnames.  
 -n count Number of echo requests to send.  
 -l size Send buffer size.  
 -f Set Don't Fragment flag in packet (IPv4-only).  
 -i TTL Time To Live.  
 -v TOS Type Of Service (IPv4-only. This setting has been deprecated  
 and has no effect on the type of service field in the IP  
 Header).  
 -r count Record route for count hops (IPv4-only).  
 -s count Timestamp for count hops (IPv4-only).  
 -j host-list Loose source route along host-list (IPv4-only).  
 -k host-list Strict source route along host-list (IPv4-only).  
 -w timeout Timeout in milliseconds to wait for each reply.  
 -R Use routing header to test reverse route also (IPv6-only).  
 -S srcaddr Per RFC 5095 the use of this routing header has been  
 deprecated. Some systems may drop echo requests if



Administrator: C:\WINDOWS\system32\cmd.exe  
C:\Windows\System32>ping 127.0.0.1  
  
Pinging 127.0.0.1 with 32 bytes of data:  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128  
  
Ping statistics for 127.0.0.1:  
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
 Approximate round trip times in milli-seconds:  
 Minimum = 0ms, Maximum = 0ms, Average = 0ms

Detail	Description
Purpose	Checks if a host is reachable on a network
Protocol Used	ICMP
Example Command	<code>ping google.com</code>

📌 It shows packet loss, latency, and whether target is alive or not.

## 2 traceroute / tracert — Trace Route Packets

### Travel

```
Administrator: C:\WINDOWS\system32\cmd.exe
C:\Windows\System32>
C:\Windows\System32>
C:\Windows\System32>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

 1      9 ms      2 ms      2 ms  172.29.57.212
 2      *          *          *      Request timed out.
 3    131 ms     98 ms     99 ms  192.168.203.1
 4    192 ms     50 ms     45 ms  192.168.203.2
 5    134 ms     98 ms     96 ms  123.63.86.122
 6     76 ms    101 ms     98 ms  182.19.106.113
 7    107 ms     97 ms     99 ms  72.14.205.216
 8    174 ms     99 ms    203 ms  142.251.49.177
 9     86 ms    142 ms     99 ms  142.250.227.73
10   199 ms     99 ms     98 ms  dns.google [8.8.8.8]

Trace complete.
```

OS	Command
Windows	<code>tracert google.com</code>
Linux / macOS	<code>traceroute google.com</code>
👉 Shows router hops & path taken by packets to reach destination.	

### 3 netstat — Show Network Connections & Ports

```

Administrator: C:\WINDOWS\system32\cmd.exe
C:\Windows\System32>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State      PID
  TCP    0.0.0.0:135            0.0.0.0:0            LISTENING  1644
  TCP    0.0.0.0:445            0.0.0.0:0            LISTENING  4
  TCP    0.0.0.0:1521           0.0.0.0:0            LISTENING  6660
  TCP    0.0.0.0:2179           0.0.0.0:0            LISTENING  3364
  TCP    0.0.0.0:3306           0.0.0.0:0            LISTENING  7232
  TCP    0.0.0.0:5040           0.0.0.0:0            LISTENING  10932
  TCP    0.0.0.0:5500           0.0.0.0:0            LISTENING  6660
  TCP    0.0.0.0:7070           0.0.0.0:0            LISTENING  5964
  TCP    0.0.0.0:9999           0.0.0.0:0            LISTENING  6744
  TCP    0.0.0.0:33060          0.0.0.0:0            LISTENING  7232
  TCP    0.0.0.0:49667          0.0.0.0:0            LISTENING  1316
  TCP    0.0.0.0:49668          0.0.0.0:0            LISTENING  1148
  TCP    0.0.0.0:49669          0.0.0.0:0            LISTENING  2120
  TCP    0.0.0.0:49670          0.0.0.0:0            LISTENING  3580
  TCP    0.0.0.0:49671          0.0.0.0:0            LISTENING  5884
  TCP    0.0.0.0:49688          0.0.0.0:0            LISTENING  7780
  TCP    0.0.0.0:49696          0.0.0.0:0            LISTENING  1268
  TCP    10.0.0.13:139          0.0.0.0:0            LISTENING  4
  TCP    10.0.0.13:2030         0.0.0.0:0            LISTENING  6700
  TCP    127.0.0.1:49675         127.0.0.1:49676       ESTABLISHED 7232
  TCP    127.0.0.1:49676         127.0.0.1:49675       ESTABLISHED 7232
  TCP    127.0.0.1:49677         127.0.0.1:49678       ESTABLISHED 7232
  TCP    127.0.0.1:49678         127.0.0.1:49677       ESTABLISHED 7232
  TCP    127.0.0.1:49693         0.0.0.0:0            LISTENING  7780
  TCP    127.0.0.1:49694         0.0.0.0:0            LISTENING  7780

```

Detail	Description
Purpose	Lists active connections, listening ports & routing table
Useful Options	<b>netstat -a (all), -n (numeric), -tulnp (Linux services)</b>



## 4 ipconfig / ifconfig — Interface Configuration

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . :
IPv6 Address . . . . . : 2001::1
Link-local IPv6 Address . . . . . : fe80::5810:74f2:1545:e105%3
IPv4 Address . . . . . : 192.168.20.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Tunnel adapter isatap.{A93807F0-65BF-47D1-8782-44D114DE82D8}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

```

OS	Command	Purpose
Windows	<code>ipconfig</code>	Shows IP, subnet mask, gateway
Linux	<code>ifconfig</code>	Displays network interface details