Command Line Tools

Ramon Lopez Jr

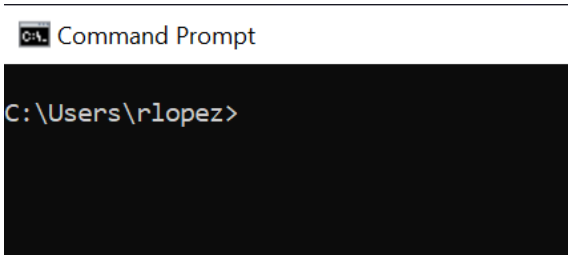
Department of Cyber Security, University of Advancing Technology

NTW102: Foundations of Network Engineering

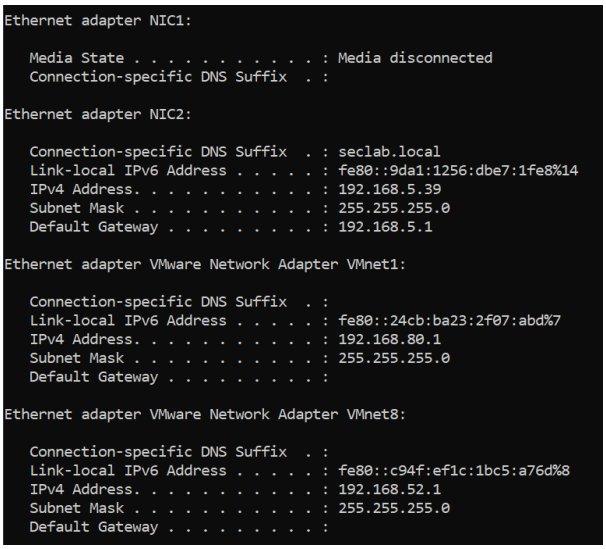
Professor Jermery Bunce

October 2nd, 2022

Command Line Tools

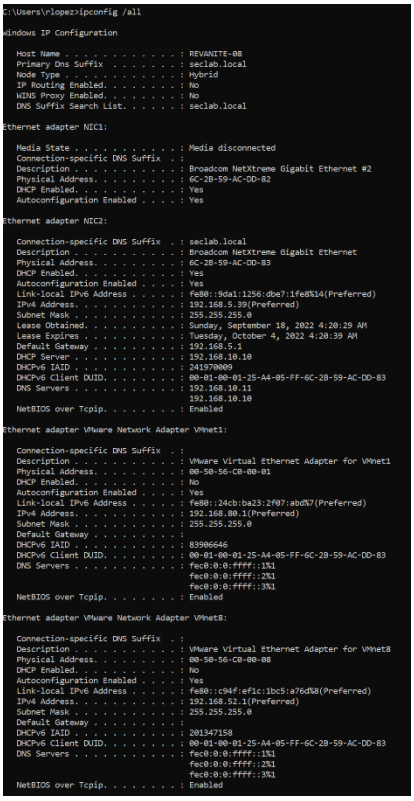


This assignment explored the use of Windows Command Line Interface (CLI) tools to gather essential network configuration information, perform connectivity tests, and understand how systems communicate over a network. The tasks included using key commands such as ipconfig, ping, and netstat—tools foundational to any network technician or cybersecurity analyst. To begin, I accessed the Command Prompt by pressing the Windows key and typing either “cmd” or “Command Prompt.” This utility opens a text-based interface that allows direct interaction with the operating system's network stack and diagnostic tools.



Using ipconfig

- The ipconfig command displays the current TCP/IP network configuration values. It revealed critical network information such as the Subnet Mask and Default Gateway.
- Additionally, the presence of a VMware Network Adapter in the output indicated that the system had a virtual machine environment installed.



Detailed Configuration: ipconfig /all

- Running ipconfig /all provided a more comprehensive view, including:
    - **Windows IP Configuration**
    - **Physical (MAC) Addresses**
    - **DHCP & DNS Server details**

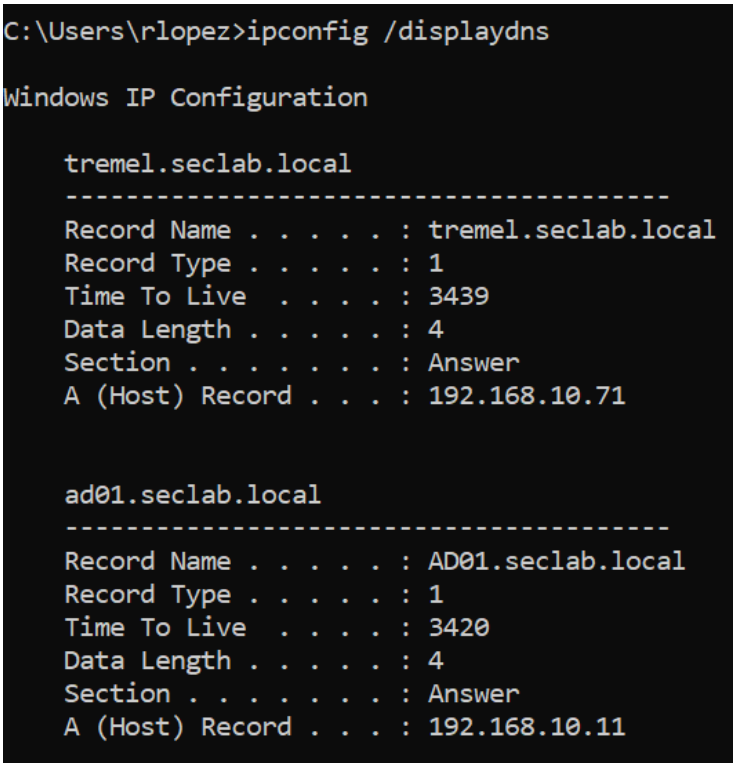
- Multiple network adapters and their statuses

This information is crucial when troubleshooting IP conflicts, DNS issues, or identifying devices on a network.

```
C:\Users\rlopez>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.


The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:
    > ipconfig                      ... Show information
    > ipconfig /all                 ... Show detailed information
    > ipconfig /renew               ... renew all adapters
    > ipconfig /renew EL*           ... renew any connection that has its
                                        name starting with EL
    > ipconfig /release *Con*       ... release all matching connections,
                                        eg. "Wired Ethernet Connection 1" or
                                            "Wired Ethernet Connection 2"
    > ipconfig /allcompartments     ... Show information about all
                                        compartments
    > ipconfig /allcompartments /all ... Show detailed information about all
                                        compartments
```

Understanding Commands: ipconfig /?

- This command outputs help documentation and available flags for the ipconfig utility.
- It explains each switch and provides usage examples, including:
  - /release, /renew, /flushdns, and more.
- Such documentation is essential for adapting commands to various networking scenarios.



Displaying DNS Cache: ipconfig /displaydns

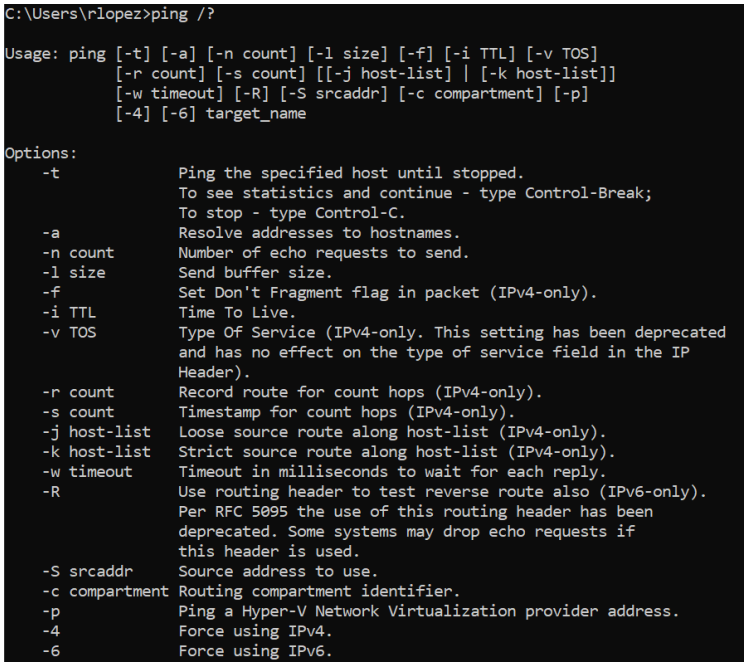
- This command reveals a list of cached DNS entries.
- For instance, the record tremel.seclab.local was shown with attributes:
  - **Record Type**: 1 (Host Record)
  - **TTL (Time to Live)**: 3439 seconds
  - **Data Length**: 4
  - **A Record IP Address**: 192.168.10.71

Analyzing the DNS cache allows users to verify name resolution and inspect previously visited domains.

```
C:\Users\rlopez>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time<1ms TTL=127
Reply from 192.168.10.10: bytes=32 time<1ms TTL=127
Reply from 192.168.10.10: bytes=32 time<1ms TTL=127
Reply from 192.168.10.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\rlopez>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time<1ms TTL=127
Reply from 192.168.10.11: bytes=32 time<1ms TTL=127
Reply from 192.168.10.11: bytes=32 time<1ms TTL=127
Reply from 192.168.10.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Testing DNS Servers with ping

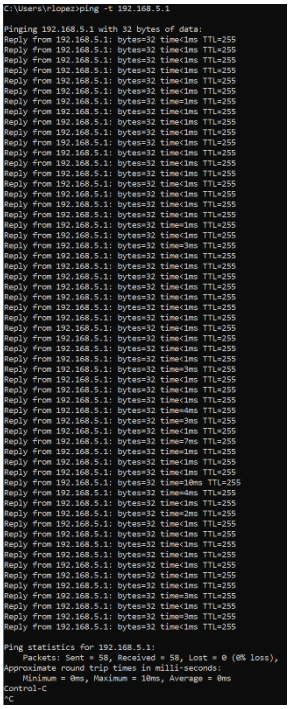
- Using DNS addresses (e.g., 192.168.10.10 and 192.168.10.11), I performed ping tests.
- Each test sent 4 packets, all of which were received successfully—indicating stable connectivity with the DNS servers.



```
C:\Users\rlopez>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).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

Exploring ping /? Options

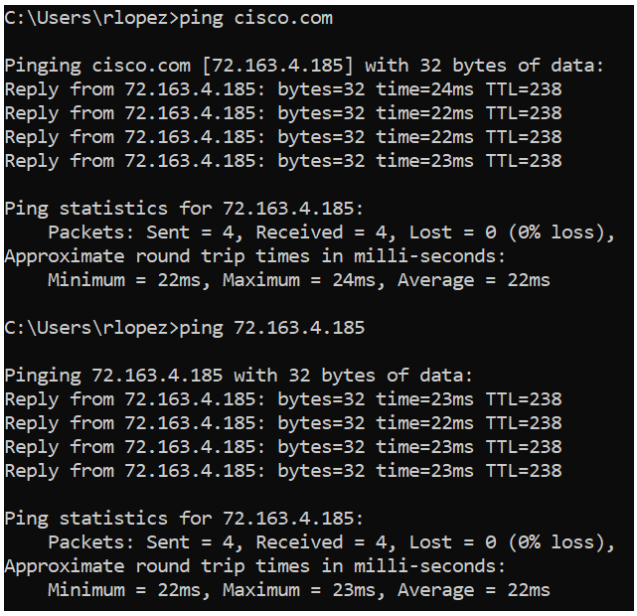
- This command displayed available options for ping, such as:
    - -t for continuous pinging
    - -l for changing packet size
    - -n for specifying the number of echo requests
- Knowing these parameters is valuable for customizing tests depending on network performance or stress testing needs.



Pinging the Default Gateway Continuously

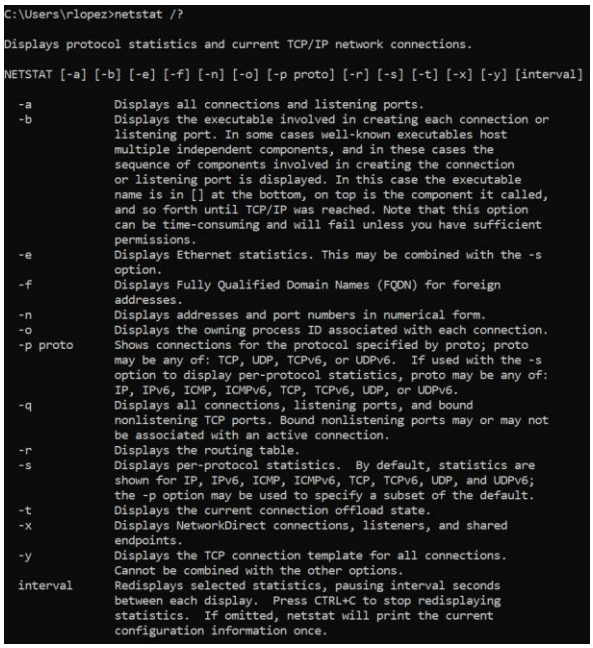
- I executed ping -t 192.168.5.1 to send a continuous stream of ping requests.
- The process was stopped using Ctrl + C, which summarized:
    - **Total Pings Sent**: 58
    - **Minimum/Maximum/Average RTT**: 0 to 10 ms

This test helps validate consistent communication with the gateway/router over time.



Pinging a Website and Its IP

- I first pinged cisco.com, receiving 4 successful replies with an average round-trip time of 22 ms.
- Then, I pinged the resolved IP address 72.163.4.185, which returned identical results.
- The exercise emphasized that pinging DNS names gives more context than IPs alone—particularly when the IP’s origin isn't known.



Using netstat /? for Network Statistics

- The command netstat /? provided a list of switches for viewing real-time network connections.
- Notable options included:
  - -a: Displays all active connections and listening ports
  - -n: Shows numerical IP addresses and port numbers
- This tool is crucial for identifying open ports, active sessions, and potential unauthorized connections.