

Command Line Tools

Ramon Lopez Jr

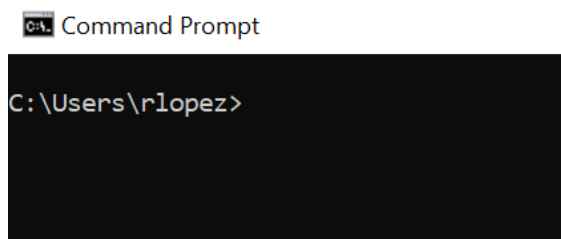
Department of Cyber Security, University of Advancing Technology

NTW102: Foundations of Network Engineering

Professor Jernery 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.

```
Ethernet adapter NIC1:

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

Ethernet adapter NIC2:

    Connection-specific DNS Suffix  . : seclab.local
    Link-local IPv6 Address . . . . . : fe80::9da1:1256:dbe7:1fe8%14
    IPv4 Address. . . . . : 192.168.5.39
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.5.1

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::24cb:ba23:2f07:abd%7
    IPv4 Address. . . . . : 192.168.80.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::c94f:ef1c:1bc5:a76d%8
    IPv4 Address. . . . . : 192.168.52.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

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.

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

Windows IP Configuration

Host Name . . . . . : RVMNTS-08
Primary Dns Suffix . . . . . : seclab.local
Node Type . . . . . : hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : seclab.local

Ethernet adapter NIC1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Broadcom NetXtreme Gigabit Ethernet #2
Physical Address. . . . . : 6C-2B-59-AC-DD-82
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Ethernet adapter NIC2:

Connection-specific DNS Suffix . : seclab.local
Description . . . . . : Broadcom NetXtreme Gigabit Ethernet
Physical Address. . . . . : 6C-2B-59-AC-DD-83
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::bd1:12d:d9f:1fd8%14(Preferred)
IPv4 Address. . . . . : 192.168.5.39(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, September 18, 2022 4:20:29 AM
Lease Expires . . . . . : Tuesday, October 4, 2022 4:20:39 AM
Default Gateway . . . . . : 192.168.5.1
DHCP Server . . . . . : 192.168.10.18
DHCPv6 IAID . . . . . : 241970009
DHCPv6 Client DUID. . . . . : 00-01-00-01-25-A4-05-FF-6C-2B-59-AC-DD-83
DNS Servers . . . . . : 192.168.10.11
                        192.168.10.18
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix . :
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet1
Physical Address. . . . . : 00-50-56-CB-00-01
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::34c:b23:2f07:ab25(Preferred)
IPv4 Address. . . . . : 192.168.80.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 83986646
DHCPv6 Client DUID. . . . . : 00-01-00-01-25-A4-05-FF-6C-2B-59-AC-DD-83
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . :
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet8
Physical Address. . . . . : 00-50-56-CB-00-08
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c94f:e1c:1bc5:a7ed%8(Preferred)
IPv4 Address. . . . . : 192.168.52.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 261347158
DHCPv6 Client DUID. . . . . : 00-01-00-01-25-A4-05-FF-6C-2B-59-AC-DD-83
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
NetBIOS over Tcpip. . . . . : Enabled
```

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.

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

Windows IP Configuration

    tremel.seclab.local
    -----
    Record Name . . . . . : tremel.seclab.local
    Record Type . . . . . : 1
    Time To Live . . . . . : 3439
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 192.168.10.71


    ad01.seclab.local
    -----
    Record Name . . . . . : AD01.seclab.local
    Record Type . . . . . : 1
    Time To Live . . . . . : 3420
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 192.168.10.11
```

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 ping
 - -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.

- 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.


```
C:\Users\rlopez>ping cisco.com

Pinging cisco.com [72.163.4.185] with 32 bytes of data:
Reply from 72.163.4.185: bytes=32 time=24ms TTL=238
Reply from 72.163.4.185: bytes=32 time=22ms TTL=238
Reply from 72.163.4.185: bytes=32 time=22ms TTL=238
Reply from 72.163.4.185: bytes=32 time=23ms TTL=238

Ping statistics for 72.163.4.185:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 24ms, Average = 22ms

C:\Users\rlopez>ping 72.163.4.185

Pinging 72.163.4.185 with 32 bytes of data:
Reply from 72.163.4.185: bytes=32 time=23ms TTL=238
Reply from 72.163.4.185: bytes=32 time=22ms TTL=238
Reply from 72.163.4.185: bytes=32 time=23ms TTL=238
Reply from 72.163.4.185: bytes=32 time=23ms TTL=238

Ping statistics for 72.163.4.185:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 23ms, Average = 22ms
```

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.

```

C:\Users\rlopez>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a      Displays all connections and listening ports.
-b      Displays the executable involved in creating each connection or
        listening port. In some cases well-known executables host
        multiple independent components, and in these cases the
        sequence of components involved in creating the connection
        or listening port is displayed. In this case the executable
        name is in [] at the bottom, on top is the component it called,
        and so forth until TCP/IP was reached. Note that this option
        can be time-consuming and will fail unless you have sufficient
        permissions.
-e      Displays Ethernet statistics. This may be combined with the -s
        option.
-f      Displays Fully Qualified Domain Names (FQDN) for foreign
        addresses.
-n      Displays addresses and port numbers in numerical form.
-o      Displays the owning process ID associated with each connection.
-p proto Shows connections for the protocol specified by proto; proto
        may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s
        option to display per-protocol statistics, proto may be any of:
        IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-q      Displays all connections, listening ports, and bound
        nonlistening TCP ports. Bound nonlistening ports may or may not
        be associated with an active connection.
-r      Displays the routing table.
-s      Displays per-protocol statistics. By default, statistics are
        shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
        the -p option may be used to specify a subset of the default.
-t      Displays the current connection offload state.
-x      Displays NetworkDirect connections, listeners, and shared
        endpoints.
-y      Displays the TCP connection template for all connections.
        Cannot be combined with the other options.
interval Redispays selected statistics, pausing interval seconds
        between each display. Press CTRL+C to stop redisplaying
        statistics. If omitted, netstat will print the current
        configuration information once.

```

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.