Lab

1

Basic Network Administration and Troubleshooting Using Windows Command Line Utilities

Windows offers several powerful command line utilities that help administrators in troubleshooting their network connections.

ICON KEY

Valuable Information

Test Your Knowledge

Web Exercise

Workbook Review

Lab Scenario

Network troubleshooting is becoming the most common task that a network admin needs to perform in large or medium organizations. As a network administrator, you are often required to troubleshoot the network problems as a part of your role and responsibilities. Administrators should have basic knowledge of network troubleshooting required to diagnose, monitor, and repair network connections. There are various basic Windows commands available to diagnose a network problem that every network admin needs to know.

Lab Objectives

This lab demonstrates the use of basic Windows command-line utilities to perform troubleshooting in the network

Lab Environment

To carry out this lab, you need:

- Windows Server 2012 and Windows 10 VMs
- Administrator privileges to run the tools

Lab Duration

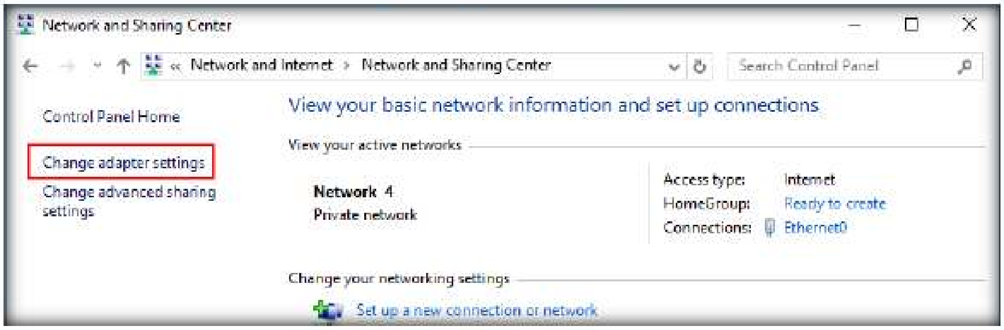
Time: 25 Minutes

Overview of the Lab

Windows Command utilities such as ipconfig, Ping, tracert, nslookup, netstat, arp, etc., allows you to administer, diagnose, monitor, and repair network connections.

Note: Before starting this lab, login to Windows 10 VM (User: Admin, Password: Pa$$w0rd) and disable the network adapter:

- Go to Control Panel → Network and Internet → Network and Sharing Center, and click Change adapter settings


Network and Sharing Center
Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
View your active networks
Change your networking settings
Set up a new connection or network

Network 4
Private network

Access type: Internet
HomeGroup: Ready to create
Connections: Ethernet0

FIGURE 1.1: Change Adapter Settings

- Select and right-click the Ethernet adapter, and click Disable from the context menu.

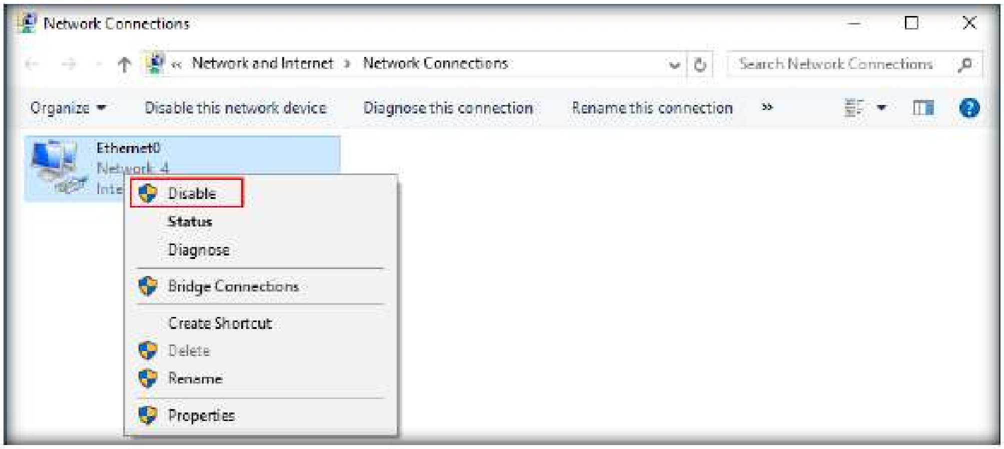
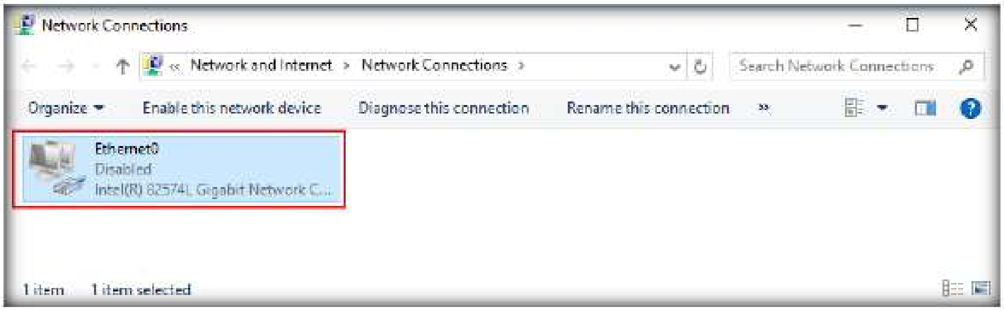


FIGURE 1.2: Disabling Network Adapter

- It will disable Ethernet adapter as shown below:


Network Connections
Network and Internet › Network Connections ›
Search Network Connections
Organize
Enable this network device
Diagnose this connection
Rename this connection
»
1 item
1 item selected

Ethernet0
Disabled
Intel(R) 82574L Gigabit Network C...

FIGURE 1.3: Network Adapter Disabled

Lab Tasks

TASK 1

Verifying IP Configuration Settings

1. Launch **Windows Server 2012** VM, and login to the local administrator account (username: **Administrator** and password: **Pa$$w0rd)**.

2. Open a command prompt in Admin mode by right-clicking on the **Start** icon and then click on **Command Prompt (Admin)** from the context menu.

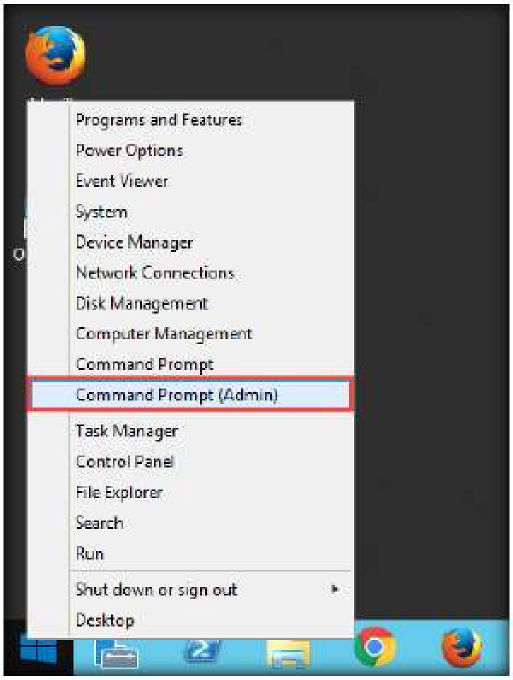
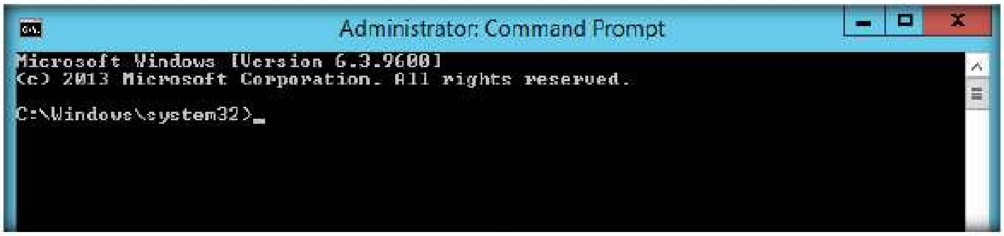


FIGURE 1.4: Launching Command Prompt

3. The command prompt appears on the screen



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>_
```

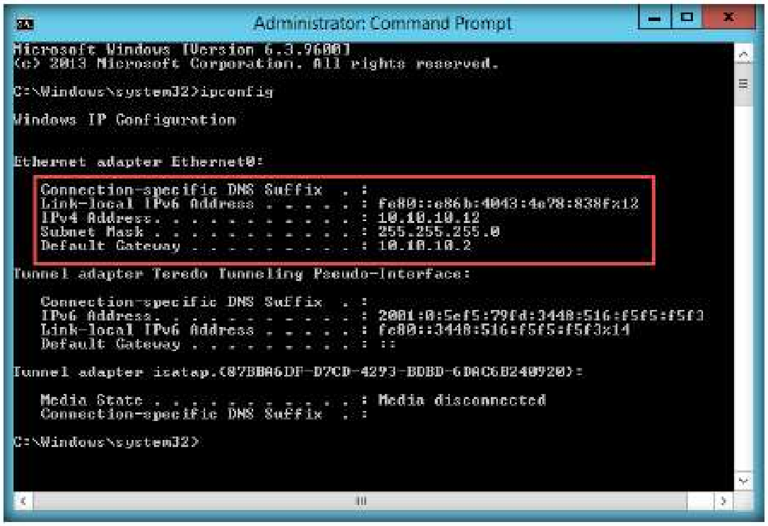
FIGURE 1.5: User Account Control

4. Type **ipconfig** in the command prompt and press **Enter** to verify the IP configuration settings of the machine.

5. The IP Configuration details of the system will be displayed. As a network admin you should know the IP configuration details of all the systems in the network.

ipconfig Syntax

ipconfig [/all] [/renew [Adapter]] [/release [Adapter]] [/flushdns] [/displaydns] [/registerdns] [/showclassid Adapter] [/setclassid Adapter [ClassID]].



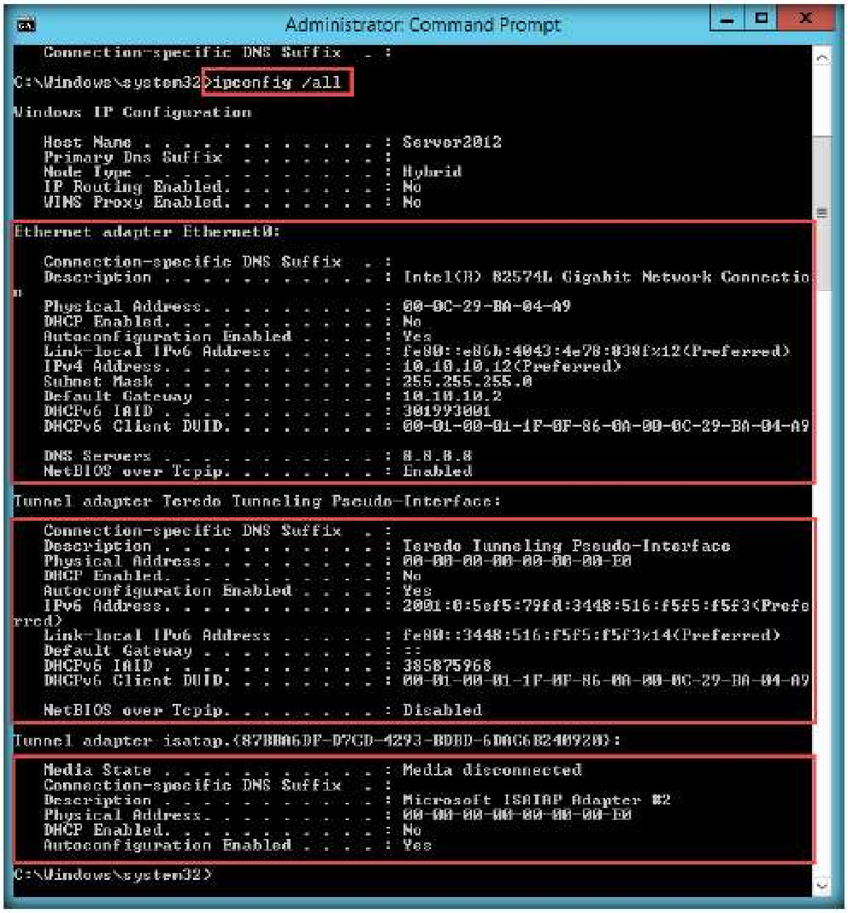
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e86b:4043:4e78:838f%12
   IPv4 Address. . . . . . . . . . . : 10.10.10.12
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:5ef5:79fd:3448:516:f5f5:f5f3
   Link-local IPv6 Address . . . . . : fe80::3448:516:f5f5:f5f3%14
   Default Gateway . . . . . . . . . : ::

Tunnel adapter isatap.{87BBA6DF-D7CD-4293-BDBD-6DAC6B240920}:

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

C:\Windows\system32>
```

FIGURE 1.6: Checking IP Configuration

6. You can use different ipconfig parameters to perform various network troubleshooting activities.

ipconfig Parameters	
/all	Displays the full TCP/IP configuration for all adapters.
/renew [Adapter]	Renews DHCP configuration for all adapters
/release [Adapter]	Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and discard the IP address configuration for either all adapters (if an adapter is not specified) or for a specific adapter
/flushdns	Flushes and resets the contents of the DNS client resolver cache.
/displaydns	Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer.
/registerdns	Initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer.
/showclassid Adapter	Displays the DHCP class ID for a specified adapter.
/setclassid Adapter [ClassID]	Configures the DHCP class ID for a specified adapter.
/?	Displays help at the command prompt.

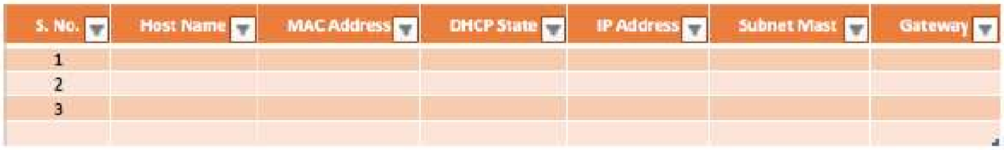
7. Now, type **ipconfig /all** and press **Enter**. This command will list out the System's IP configuration, host name, Ethernet Adapter installed and its MAC Address (Physical Address) and so on, as shown in the screenshot.



```
    Connection-specific DNS Suffix  . :

C:\Windows\system32>ipconfig /all

Windows IP Configuration

    Host Name . . . . . . . . . . . . : Server2012
    Primary Dns Suffix  . . . . . . . :
    Node Type . . . . . . . . . . . . : Hybrid
    IP Routing Enabled. . . . . . . . : No
    WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . :
    Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connectio
n
    Physical Address. . . . . . . . . : 00-0C-29-BA-04-A9
    DHCP Enabled. . . . . . . . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::e86b:4043:4e78:830f%12(Preferred)
    IPv4 Address. . . . . . . . . . . : 10.10.10.12(Preferred)
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . : 10.10.10.2
    DHCPv6 IAID . . . . . . . . . . . : 301993001
    DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1F-0F-86-0A-00-0C-29-BA-04-A9

    DNS Servers . . . . . . . . . . . : 8.8.8.8
    NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . :
    Description . . . . . . . . . . . : Teredo Tunneling Pseudo-Interface
    Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
    DHCP Enabled. . . . . . . . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    IPv6 Address. . . . . . . . . . . : 2001:0:5ef5:79fd:3448:516:f5f5:f5f3(Prefe
rred)
    Link-local IPv6 Address . . . . . : fe80::3448:516:f5f5:f5f3%14(Preferred)
    Default Gateway . . . . . . . . . : ::
    DHCPv6 IAID . . . . . . . . . . . : 385875968
    DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1F-0F-86-0A-00-0C-29-BA-04-A9

    NetBIOS over Tcpip. . . . . . . . : Disabled

Tunnel adapter isatap.{87BBA6DF-D7CD-4293-BDBD-6DAC6B240920}:

    Media State . . . . . . . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
    Description . . . . . . . . . . . : Microsoft ISATAP Adapter #2
    Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
    DHCP Enabled. . . . . . . . . . . : No
    Autoconfiguration Enabled . . . . : Yes

C:\Windows\system32>
```

FIGURE 1.7: Complete IP Configuration

8. You can use the information obtained from the above steps to create an Inventory List of all the computing devices in the network. In later modules we will look at better and more sophisticated techniques to create a Network Inventory but this could be an ideal starting point.



S. No.	Host Name	MAC Address	DHCP State	IP Address	Subnet Mast	Gateway
1						
2						
3						

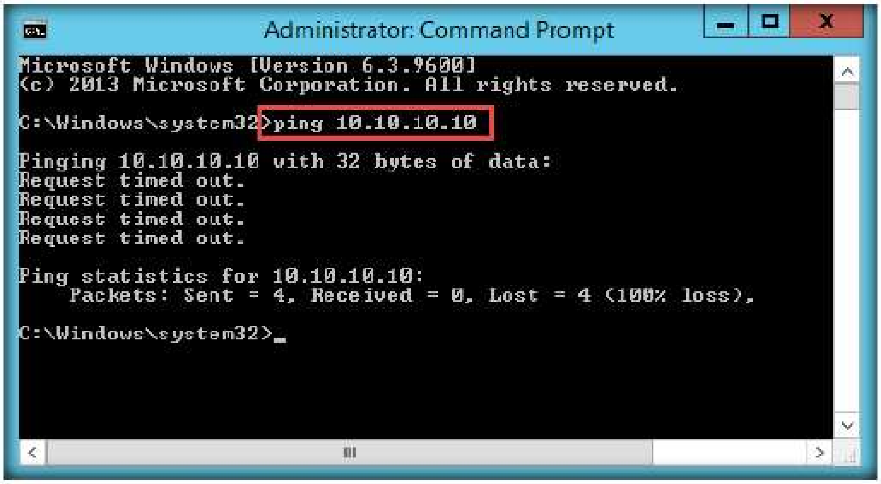
9. Close the command prompt after noting down all the information.

TASK 2

Checking IP level Connectivity Using Ping command

10. Now, we will explore the usage of the **Ping** command. Network administrators always encounter IP level Connectivity errors in the network such as **Request timed out**, **Destination host unreachable**, etc. With the help of the Ping command, they can ensure the reachability of a host to other hosts connected in the network

11. Open a command prompt in the Admin mode by right-clicking on the **Start** icon and then clicking on **Command Prompt (Admin)** from the context menu. Type **ping** followed by the IP address of the Windows 10 machine (it is 10.10.10.10 for this lab setup)



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>_
```

FIGURE 1.8: Demonstration of the Ping command

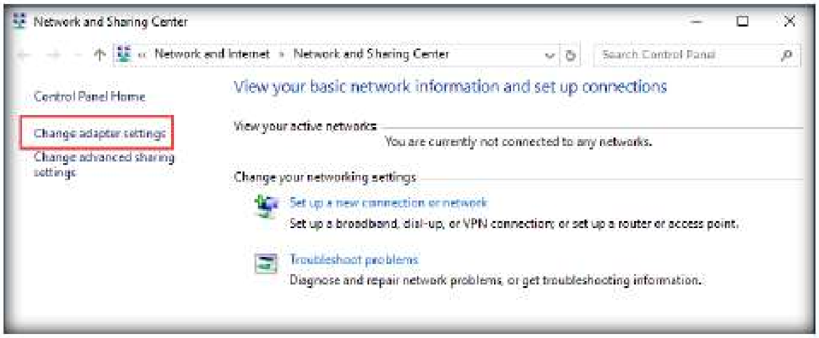
12. You can see that the "**Request timed out**" error. It means that the target system did not reply within the stipulated time frame. It implies that the target device is out of reach. The cause of this is either due to the target machine is turned off or the Network adapter is disabled on the target machine.

Option	Use
-n *Count*	Determines the number of echo requests to send. The default is 4 requests.
-w *Timeout*	Enables you to adjust the time-out (in milliseconds). The default is 1,000 (a 1-second time-out).
-l *Size*	Enables you to adjust the size of the ping packet. The default size is 32 bytes.
-f	Sets the Do Not Fragment bit on the ping packet. By default, the ping packet allows fragmentation.

13. Now, switch to the Windows 10 machine to troubleshoot the issue.

14. Go to **Control Panel -> Network and Internet -> Network and Sharing Center**. Check for the Network adapter status

15. Now you can see that Ethernet 2 adapter is showing up "No internet access". Click on **Change adapter settings** in the left pane


Network and Sharing Center
« Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
Set up a new connection or network
Troubleshoot problems

View your basic network information and set up connections

View your active networks

You are currently not connected to any networks.

Change your networking settings

Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Diagnose and repair network problems, or get troubleshooting information.

FIGURE 1.9: Ethernet 2 Network adapter error

16. Now you can see that the **Ethernet 2** adapter is disabled.

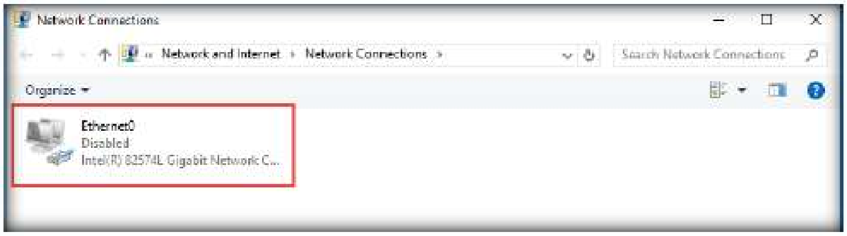

Network Connections
Network and Internet › Network Connections ›
Search Network Connections
Organize ▾
Ethernet0
Disabled
Intel(R) 82574L Gigabit Network C...

FIGURE 1.10: Disabled Ethernet adapter

17. Right click on it and select **Enable** from the context menu.

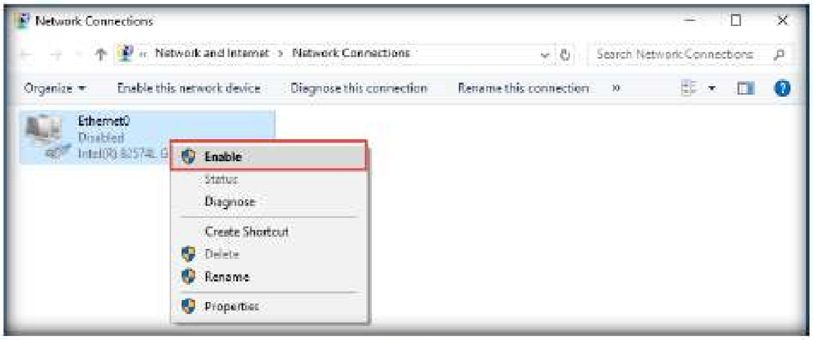
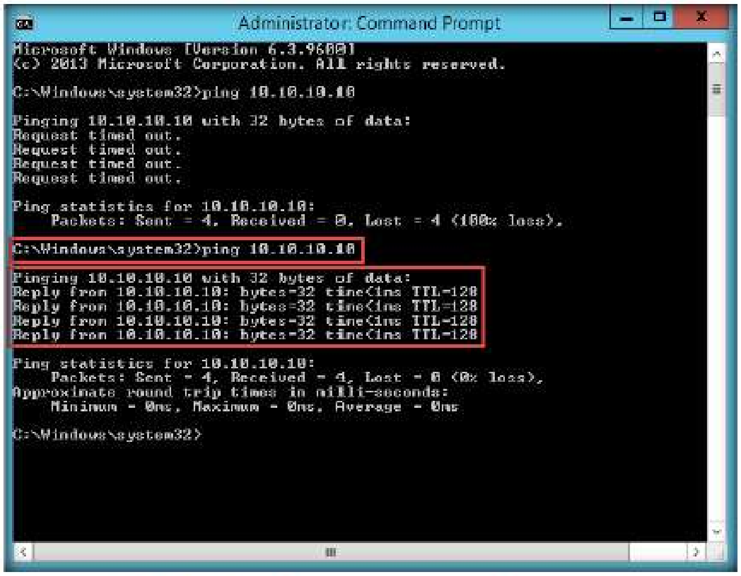


FIGURE 1.11: Enabling the disabled adapter

18. Now, switch back to **Windows Server 2012** machine and ping the target machine again



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>
```

FIGURE 1.12: Ping request successfully executed

19. This time, you will be able to ping Window 10 machine successfully.

Note: Sometimes even after enabling the adapter, the ping request might not be successful due to firewall restrictions. In such cases, you need to temporarily disable the firewall on the target machine to check its reachability

TASK 3

Tracing the route of packets using tracert command

20. Now, we will see the usage of the **tracert** command to know the number of hops between a source and a destination node in a network. **tracert** is useful for troubleshooting large networks where several paths can lead to the same point or where many intermediate components (routers or bridges) are involved.

    About tracert:

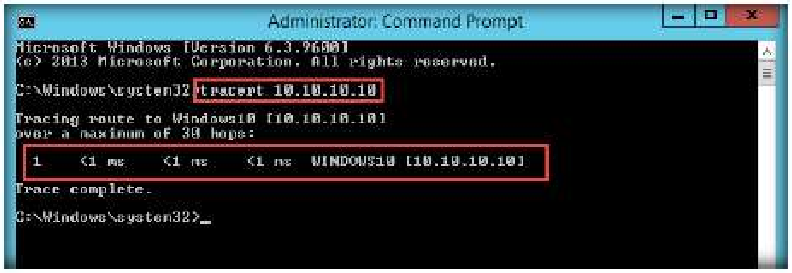
    Source: *https://support.microsoft.com*

    The **tracert** diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. In these packets, **tracert** uses varying IP Time-To-Live (TTL) values. Because each router along the path is required to decrement the packet's TTL by at least 1 before forwarding the packet, the TTL is effectively a hop counter. When the TTL on a packet reaches zero (0), the router sends an ICMP "Time Exceeded" message back to the source computer.

    tracert sends the first echo packet with a TTL of 1 and increments the TTL by 1 on each subsequent transmission, until the destination responds or until the maximum TTL is reached. The ICMP "Time Exceeded" messages that intermediate routers send back show the route. Note however that some routers silently drop packets that have expired TTLs, and these packets are invisible to **tracert**.

    tracert prints out an ordered list of the intermediate routers that return ICMP "Time Exceeded" messages. Using the **-d** option with the tracert command instructs **tracert** not to perform a DNS lookup on each IP address, so that tracert reports the IP address of the near-side interface of the routers.

21. On the Windows Server 2012 machine. Open a command prompt in the Admin mode by right-clicking on **Start** icon and then clicking **Command Prompt (Admin)** from the context menu. Type **tracert** followed by the target system IP address the command prompt and press Enter.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>tracert 10.10.10.10

Tracing route to Windows10 [10.10.10.10]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  WINDOWS10 [10.10.10.10]

Trace complete.

C:\Windows\system32>_
```

FIGURE 1.13: Demonstration of Tracert command

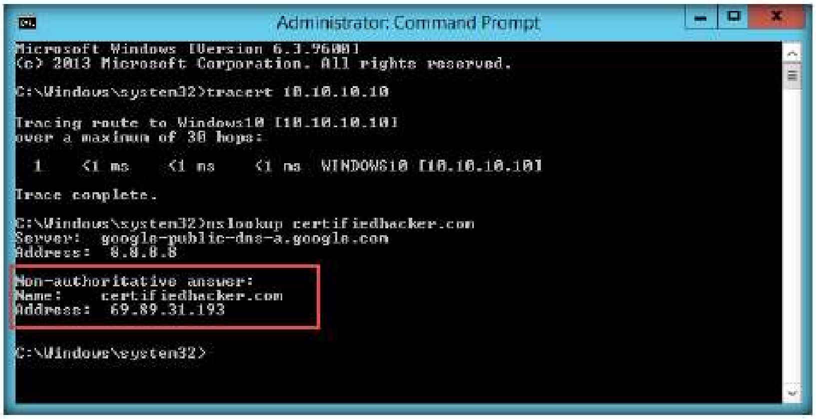
22. From the above screenshot, we can see that the destination was reached in the first hop itself.

TASK 4

Resolving Domain names with Using nslookup command

23. Now we will demonstrate the use of **nslookup** command. Nslookup stands for name server lookup. It is used to query a DNS server to obtain its domain name and associated IP address. It can be used with the domain name as an argument or independently

24. On the Windows Server 2012 machine, type **nslookup** followed by the domain name which you want to resolve (here, certifiedhacker.com) in the command prompt and press Enter.

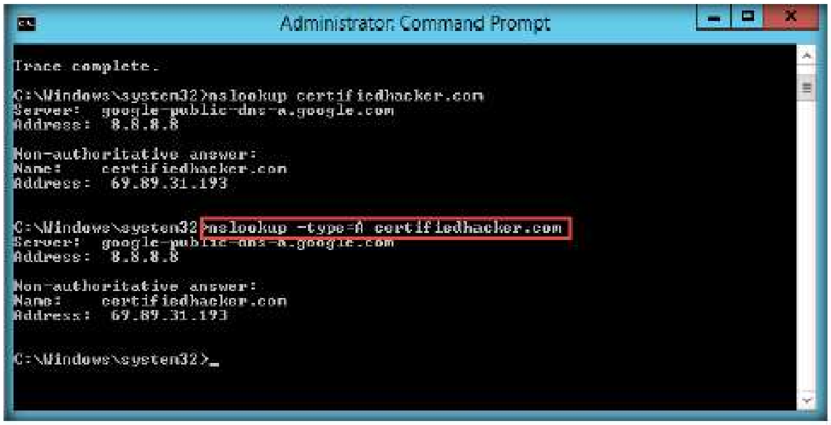


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>tracert 10.10.10.10

Tracing route to Windows10 [10.10.10.10]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  WINDOWS10 [10.10.10.10]

Trace complete.

C:\Windows\system32>nslookup certifiedhacker.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    certifiedhacker.com
Address:  69.89.31.193

C:\Windows\system32>
```

FIGURE 1.14: Demonstration of nslookup command

25. From the above screenshot, you will see that the domain name (certifiedhacker.com) resolves to its corresponding IP address (69.89.31.193)

26. You can also use the nslookup command with type parameters to get non-authoritative name server (NS) information as shown in the screenshot below:

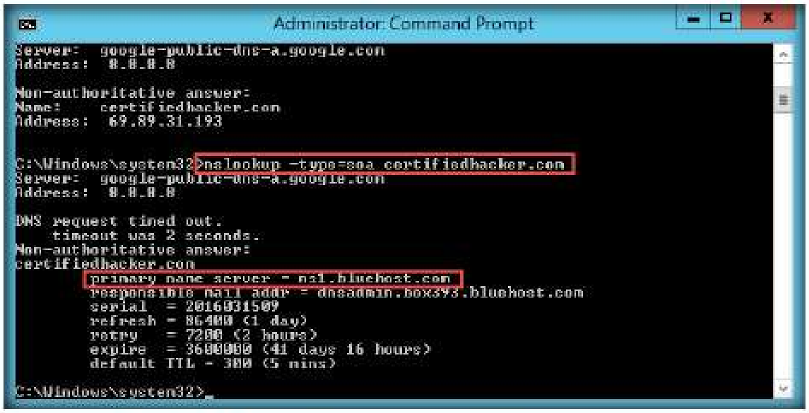


```
Trace complete.

C:\Windows\system32>nslookup certifiedhacker.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    certifiedhacker.com
Address:  69.89.31.193

C:\Windows\system32>nslookup -type=A certifiedhacker.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    certifiedhacker.com
Address:  69.89.31.193

C:\Windows\system32>_
```

FIGURE 1.15: nslookup command with type parameter

27. To get an authoritative NS information, you can use –type=soa parameter with nslookup.

An Authoritative or Primary Nameserver is a nameserver (DNS Server) that holds the actual DNS records (A, CNAME, PTR, etc) for a particular domain/ address.



```
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    certifiedhacker.com
Address:  69.89.31.193

C:\Windows\system32>nslookup -type=soa certifiedhacker.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
certifiedhacker.com
        primary name server = ns1.bluehost.com
        responsible mail addr = dnsadmin.box393.bluehost.com
        serial  = 2016031509
        refresh = 86400 (1 day)
        retry   = 7200 (2 hours)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 300 (5 mins)

C:\Windows\system32>_
```

FIGURE 1.16: nslookup command with type parameter

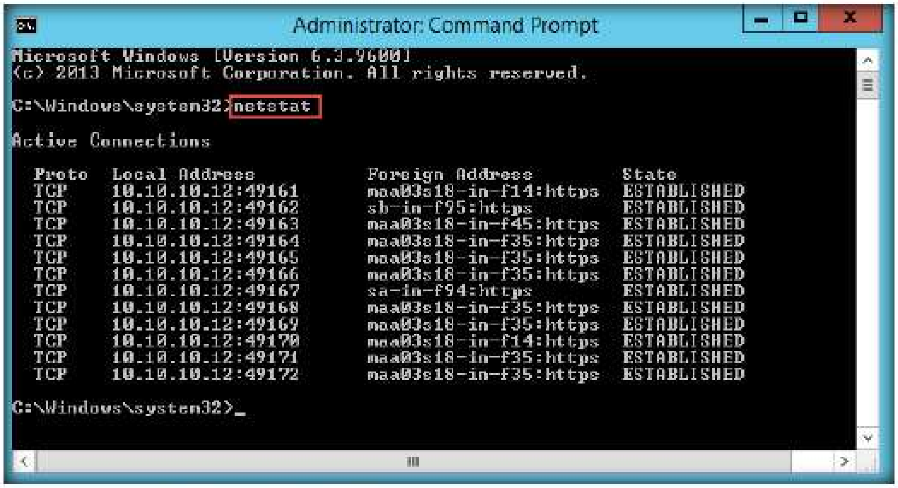
28. The address labelled as primary name server in the above screenshot is the DNS authority for the domain.

TASK 5

Checking your network configuration and statistics netstat command

29. Now we will see the use of the **netstat** command. Netstat stands for Network statistics. Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, netstat displays active TCP connections.

30. Type the **netstat** command to check your network statistics as shown in following screenshot



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.10.10.12:49161      maa03s18-in-f14:https  ESTABLISHED
  TCP    10.10.10.12:49162      sb-in-f95:https        ESTABLISHED
  TCP    10.10.10.12:49163      maa03s18-in-f45:https  ESTABLISHED
  TCP    10.10.10.12:49164      maa03s18-in-f35:https  ESTABLISHED
  TCP    10.10.10.12:49165      maa03s18-in-f35:https  ESTABLISHED
  TCP    10.10.10.12:49166      maa03s18-in-f35:https  ESTABLISHED
  TCP    10.10.10.12:49167      sa-in-f94:https        ESTABLISHED
  TCP    10.10.10.12:49168      maa03s18-in-f35:https  ESTABLISHED
  TCP    10.10.10.12:49169      maa03s18-in-f35:https  ESTABLISHED
  TCP    10.10.10.12:49170      maa03s18-in-f14:https  ESTABLISHED
  TCP    10.10.10.12:49171      maa03s18-in-f35:https  ESTABLISHED
  TCP    10.10.10.12:49172      maa03s18-in-f35:https  ESTABLISHED

C:\Windows\system32>_
```

FIGURE 1.17: Demonstration of netstat command

31. You can use different **nestat** parameters to obtain important connection information

Parameters	Use
-a	Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
-e	Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with –s

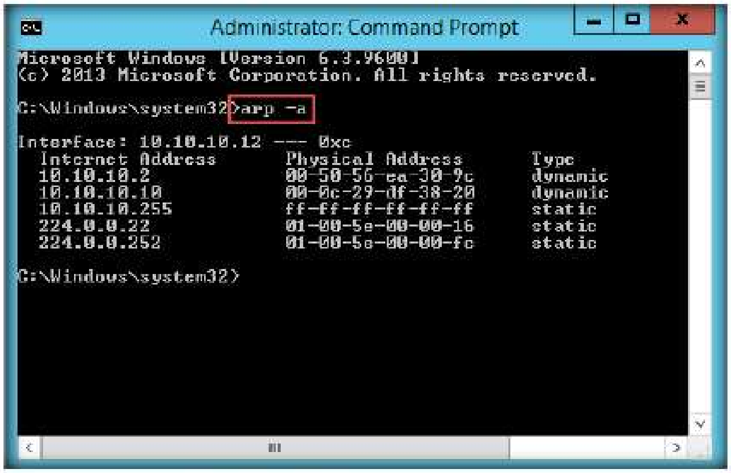
-n	Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.
-o	Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the **Processes** tab in Windows Task Manager. This parameter can be combined with **-a**, **-n**, and **-p**.
-p *Protocol*	Shows connections for the protocol specified by *Protocol*. In this case, the *Protocol* can be **tcp**, **udp**, **tcpv6**, or **udpv6**. If this parameter is used with **-s** to display statistics by protocol, *Protocol* can be **tcp**, **udp**, **icmp**, **ip**, **tcpv6**, **udpv6**, **icmpv6**, or **ipv6**.
-s	Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The **-p** parameter can be used to specify a set of protocols.
-r	Displays the contents of the IP routing table. This is equivalent to the **route print** command.
Interval	Redisplays the selected information every *Interval* seconds. Press CTRL+C to stop the redisplay. If this parameter is omitted, **netstat** prints the selected information only once.
/?	Displays help at the command prompt.

TASK 6

Displaying Address Resolution Protocol (ARP) cache using arp command

32. The **arp –a** command displays ARP cache. The cache has a mapping of IP addresses with their respective MAC addresses. It has many options and if you use ARP without any option it displays the available options

33. Type **arp –a** command and press Enter to display the ARP cache entries.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>arp -a

Interface: 10.10.10.12 --- 0xc
  Internet Address      Physical Address      Type
  10.10.10.2            00-50-56-ea-30-9c     dynamic
  10.10.10.10           00-0c-29-df-38-20     dynamic
  10.10.10.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static

C:\Windows\system32>
```

FIGURE 1.18: Using arp –a command

Note: If you want to view the MAC address of only a particular IP address, type the IP address after **arp –a** command and press Enter.

Similarly, you can use the following useful commands for network administration and troubleshooting

Commands	Objectives
Gpresult	Starts the Operating System Group Policy Result tool
ipconfig /flushdns	Flushes the DNS resolver cache. Helpful when troubleshooting DNS name resolution problems
nbtstat -a <MachineName>	Obtains info from WINS or LMHOST (discovers who is logged on)
nbtstst -A <IP>	Gets info from WINS or LMHOST (discovers who is logged on)
nbtstat –R	Purges and reloads the remote cache name table
nbtstat –n	Lists local NetBIOS names.
nbtstat –r	Useful for detecting errors when browsing WINS or NetBIOS
netstat –ab	The b switch links each used port with its application
netstat –an	Shows open ports
netstat -an 1 | find "15868"	Locates only lines with the number 15868 and redisplays every one second
netstat -an | find "LISTENING"	Shows open ports with LISTENING status
net use	Retrieves a list of network connections
net user	Shows user account for the computer
net user /domain	Displays user accounts for the domain
net user /domain <UserName>	Shows account details for specific user
net group /domain	Shows group accounts for the domain
net view	Displays domains in the network
net view /domain	Specifies computers available in a specific domain
net view /domain: <DomainName> | more	Shows user accounts from specific domain
net view /cache	Shows workstation names
ping -a <IP>	Resolves IP to Hostname
ping -t <IP>	Pings host until stopped
Pathping	Displays the route and ping information when performing queries such as –n and –h options representing hostnames and maximum hops respectively.
set U	Shows which user is logged on
set L	Shows the logon server
telnet <IP> <port>	Confirms whether the port is open

Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	□ No
Platform Supported	
☑ Classroom	☑ iLabs