CompTIA Cybersecurity Analyst (CySA+)

Windows Command Line Tools

- **Introduction**
- **Exercise 1 - IPconfig**
- **Exercise 2 - Netstat**
- **Exercise 3 - Ping**
- **Exercise 4 - Tracert and Route**
- **Exercise 5 - ARP and Whoami**
- **Summary**

Introduction

The **Windows Command Line Tools** module provides you with the instructions and devices to develop your hands-on skills in the following topics.

- Ipconfig
- Netstat
- Ping
- Tracert and Route
- ARP and Whoami

From an internal perspective, we will use windows tools to investigate basic topology but also see in detail the services and processes happening within a windows system that are not directly visible without interrogation.

Lab time: It will take approximately 1 hour to complete this lab.

Exam Objectives

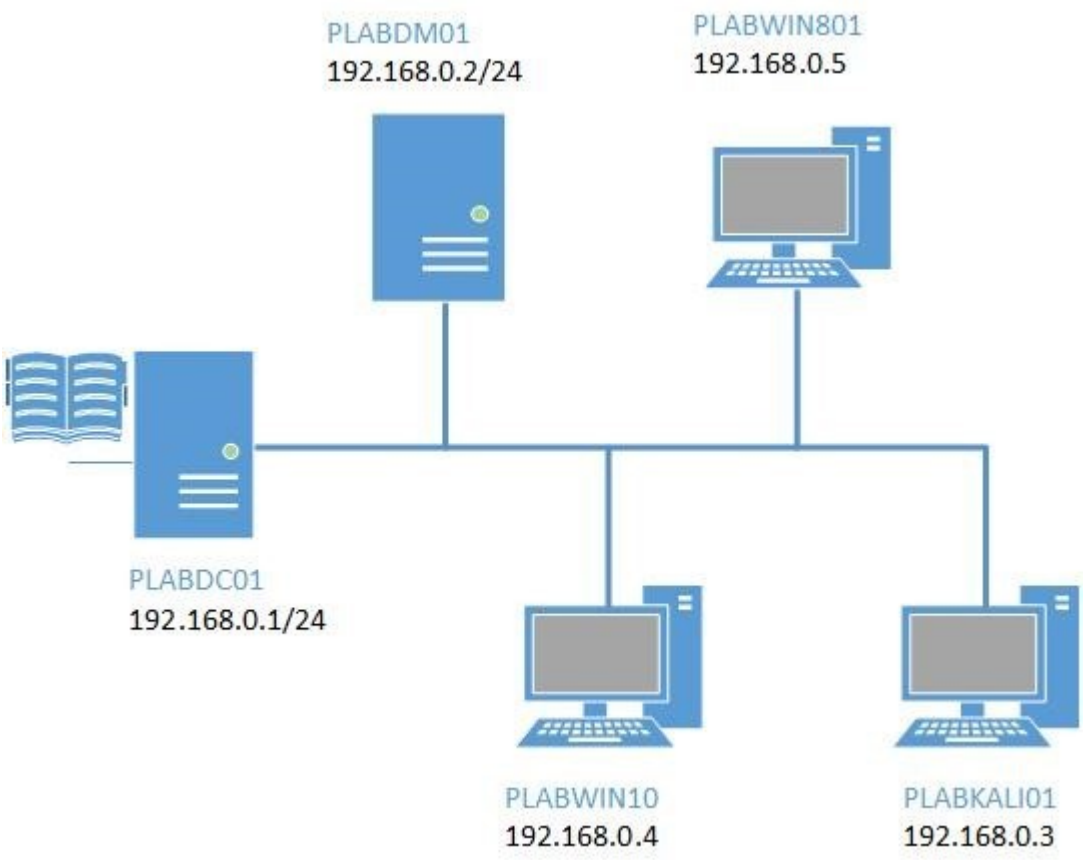
The following exam objectives are covered in this lab:

- **CS0-001 1.1:** Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes

- **CS0-001 1.2:** Given a scenario, analyze the results of a network reconnaissance

Lab Diagram

During your session, you will have access to the following lab configuration. Depending on the exercises you may or may not use all of the devices, but they are shown here in the layout to get an overall understanding of the topology of the lab.



Connecting to your lab

In this module, you will be working on the following equipment to carry out the steps defined in each exercise.

- **PLABDC01** (Windows Server 2012 R2 - Domain Controller)
- **PLABDM01** (Windows Server 2012 R2 - Member Server)
- **PLABWIN801** (Windows 8.1 - Domain Member)
- **PLABWIN10** (Windows 10 - Domain Member)
- **PLABKALI01** (Kali 2016.2)

To start, simply choose a device and click **Power on**. In some cases, the devices may power on automatically.

For further information and technical support, please see our Help and Support page.

Copyright Notice
This document and its content is copyright of Practice-IT - © Practice-IT 2017. All rights reserved. Any redistribution or reproduction of part or all of the contents in any form is prohibited other than the following:
1. You may print or download to a local hard disk extracts for your personal and non-commercial use only.
2. You may copy the content to individual third parties for their personal use, but only if you acknowledge the website as the source of the material. You may not, except with our express written permission, distribute or commercially exploit the content. Nor may you transmit it or store it in any other website or other form of electronic retrieval system.

Exercise 1 - IPconfig

IPconfig is a command-line tool that displays the current configuration of the installed IP stack on a networked computer.

When used with the **/all** switch, it displays a detailed configuration report for all interfaces, including any configured WAN miniports (typically used for remote access or VPN connections).

In this exercise you will complete the following tasks:

- Using the IPconfig command line tool

Please refer to your course material or use your favorite search engine to research for more information about this topic.

Task 1 - Using the IPconfig command line tool

In this task, you will be using the Ipconfig command-line tool to identify information such as the internet protocol configuration of the device you are using, together with TCP/IP network configurations variables.

Step 1

First, connect to the device **PLABDM01** and bring up the **command prompt** in administrator mode by right-clicking on the Windows Icon and clicking on the Command Prompt (Admin).

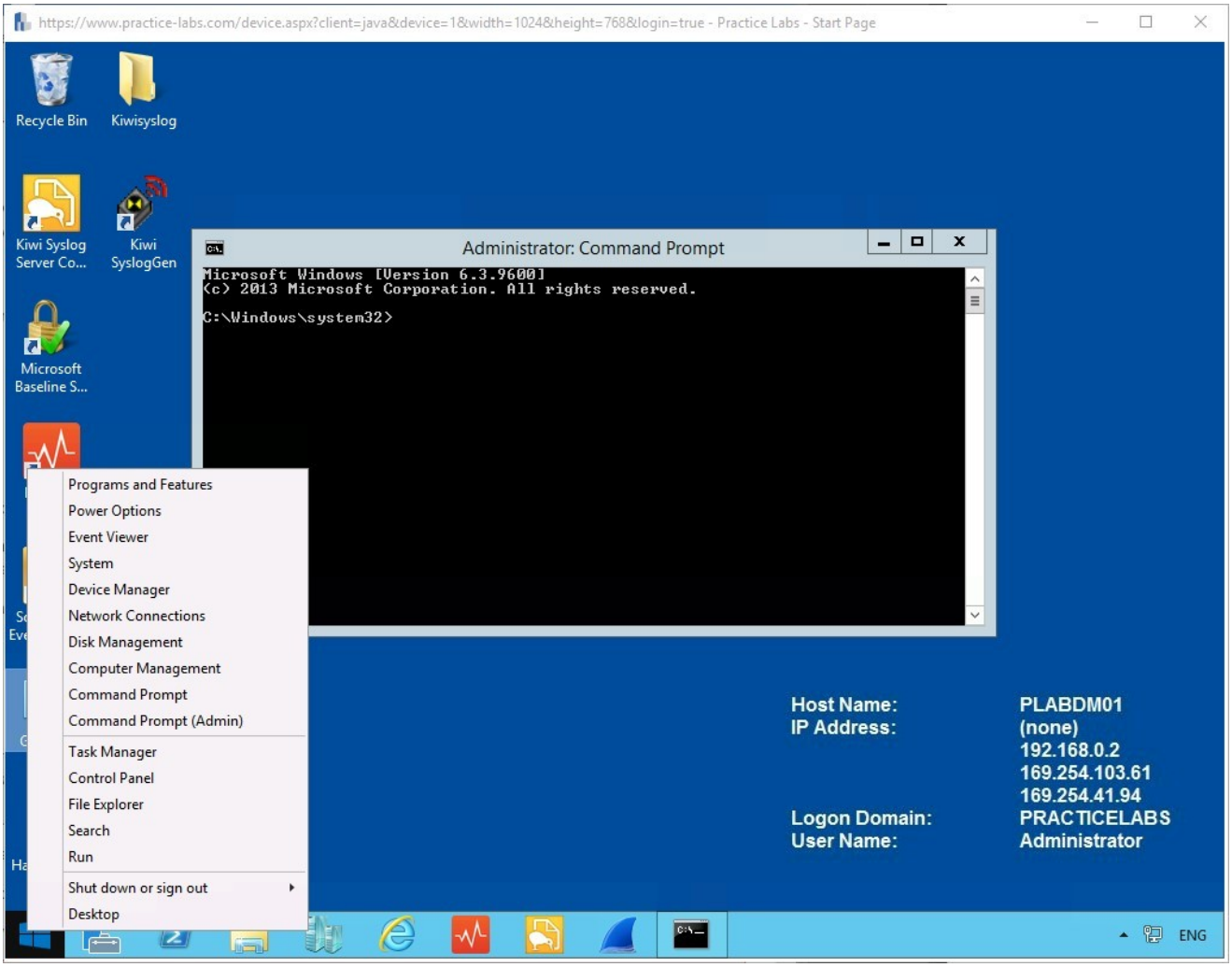


Figure 1.1 PLABDM01: Screenshot of the command prompt (Admin).

Step 2

Now we can begin exploring the environment of this machine to learn more about its processes and services.

We will begin by learning more about the Ethernet settings.

Type the following command into the console:

```
ipconfig
```

This will test us useful information about the computer is communicating with the network and what devices it is currently using to make that communication.

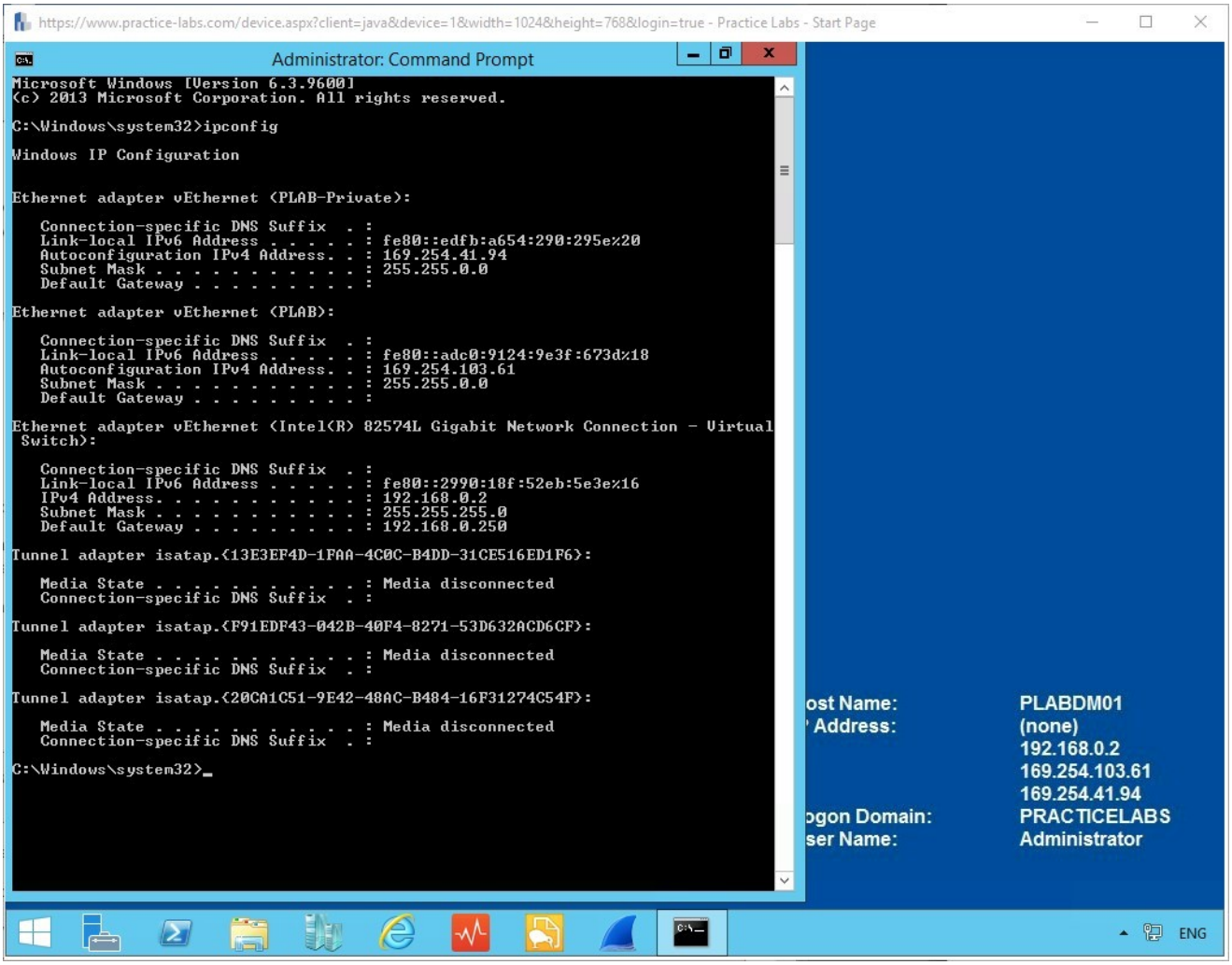


Figure 1.2 PLABDM01: Screenshot of Ipconfig output.

Here we view information about the Ethernet adapters attached to this device; these are displaying 3 different network addresses, from the diagram you will notice the IP 192.168.0.2 is the correctly assigned address.

Additionally, we are also provided with IPv6 addresses for the devices.

To clear the contents of the display, use the following command:

```
cls
```

Step 3

However, we might want to learn more detailed information about each device in the on this computer and how it is attached to the computer.

Type the following command into the console:

```
ipconfig /all
```

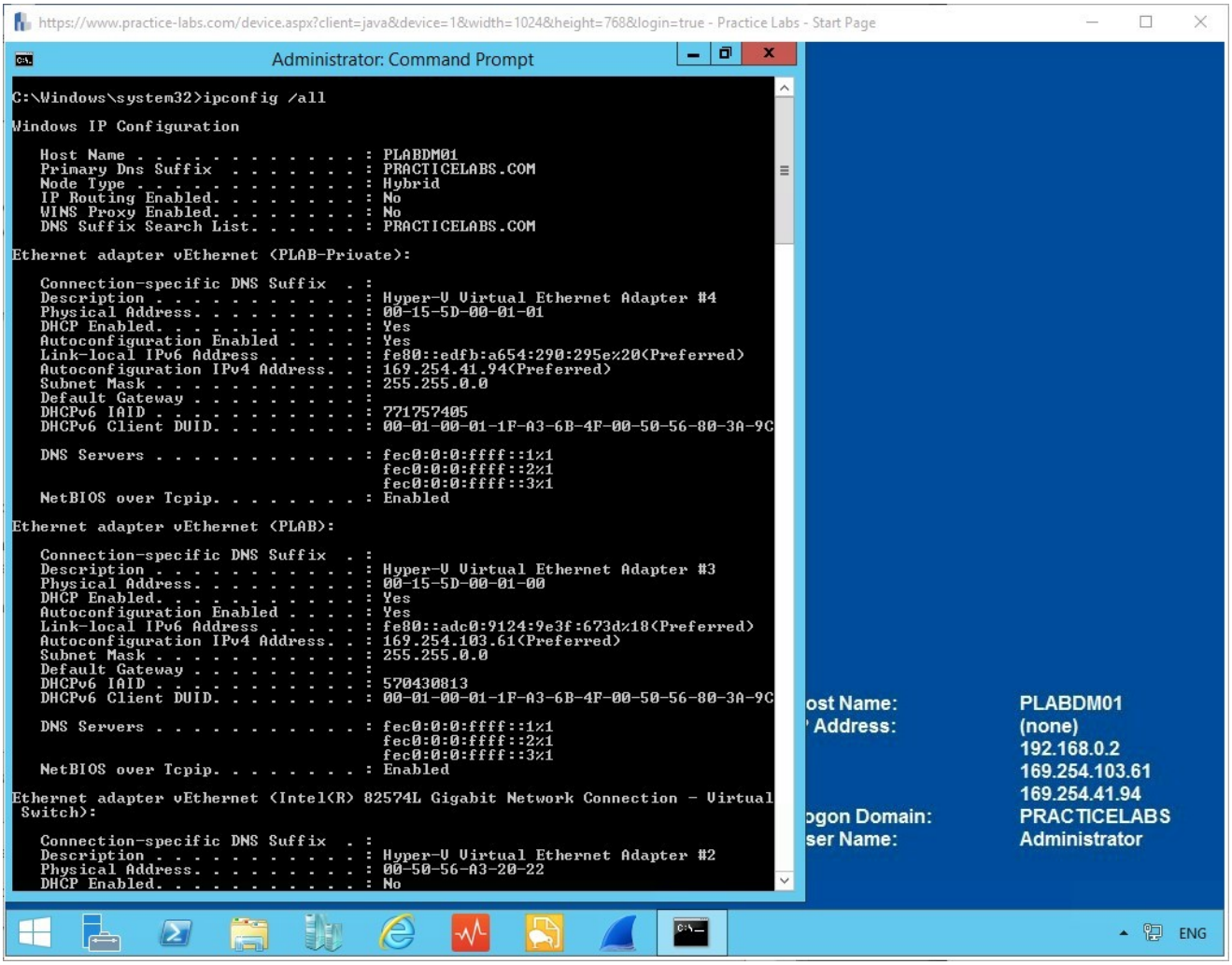


Figure 1.3 PLABDM01: Screenshot of ipconfig /all output.

A great deal more information is displayed so take your time absorbing the details about the information. We can see Host Names, that the Primary DNS is practicelabs.com.

The connections to each Ethernet adapter and the use of Hyper-V working from Adapter 2, 3, 4 providing information about the configuration of the IP's of those internal devices.

We also learn that NetBIOS over TCPIP has been enabled on those devices.

Step 4

We can use this command to identify the DNS values assigned to the device.

Type the following command into the console:

```
ipconfig /displaydns
```

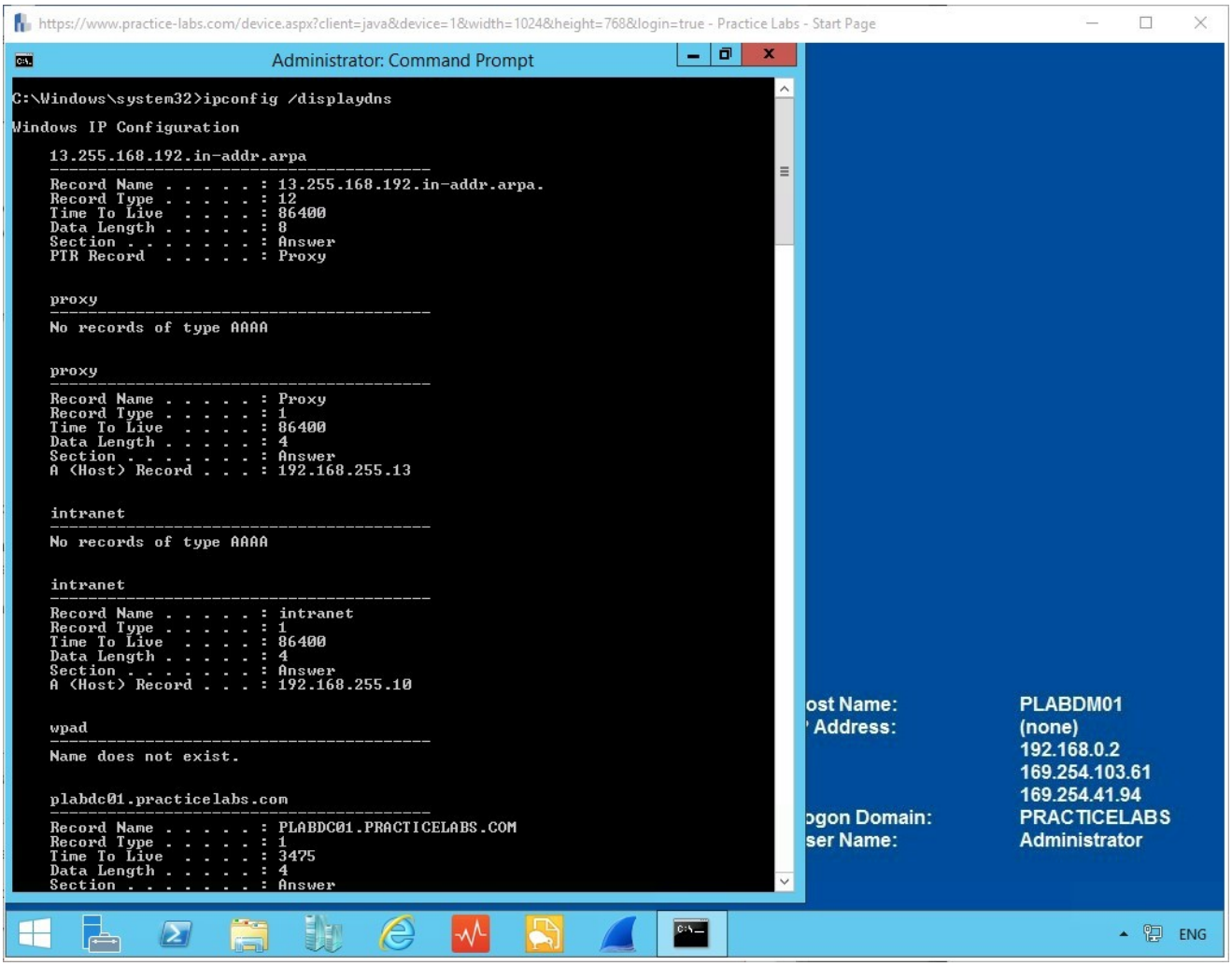


Figure 1.4 PLABDM01: Screenshot of ipconfig /displaydns.

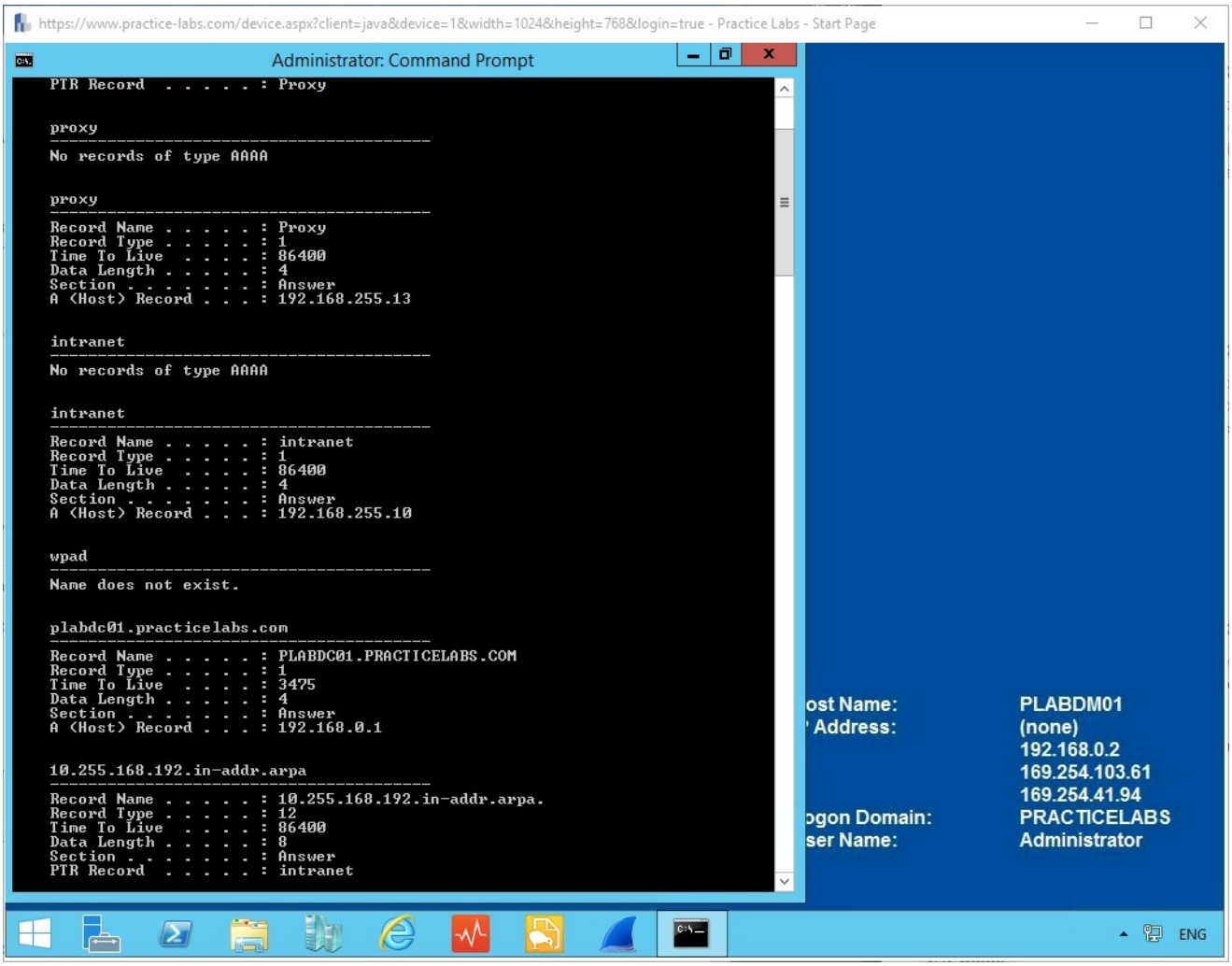


Figure 1.5 PLABDM01: Screenshot of ipconfig /displaydns continued.

DNS information is rendered to the screen and tells us about the nature of connections reaching out to external and an internal network, for example, we can clearly identify proxy data, alerting us to further topology information and further down the page we are greeted with the domain information of PRACTICELABS.COM.

Leave all devices powered on in their current state and proceed to the next exercise.

Exercise 2 - Netstat

Netstat 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).

In this exercise you will complete the following tasks:

- Using the Netstat command-line tool

Please refer to your course material or use your favorite search engine to research for more information about this topic.

Task 1 - Using the Netstat command-line tool

In this task, you will be using the Netstat command-line tool to display traffic flow data and device routing tables. Netstat will identify processes and the ports they are listening to or have already established themselves on. It can also be used to provide on the fly reports of traffic moving across interfaces.

Step 1

As a security engineer, you earlier used NMAP to see what services and ports were being broadcast, however, lets now look at the same functions running on **PLABDM01** but from the inside.

Enter the command:

```
netstat
```

We are given a heavy readout of information.

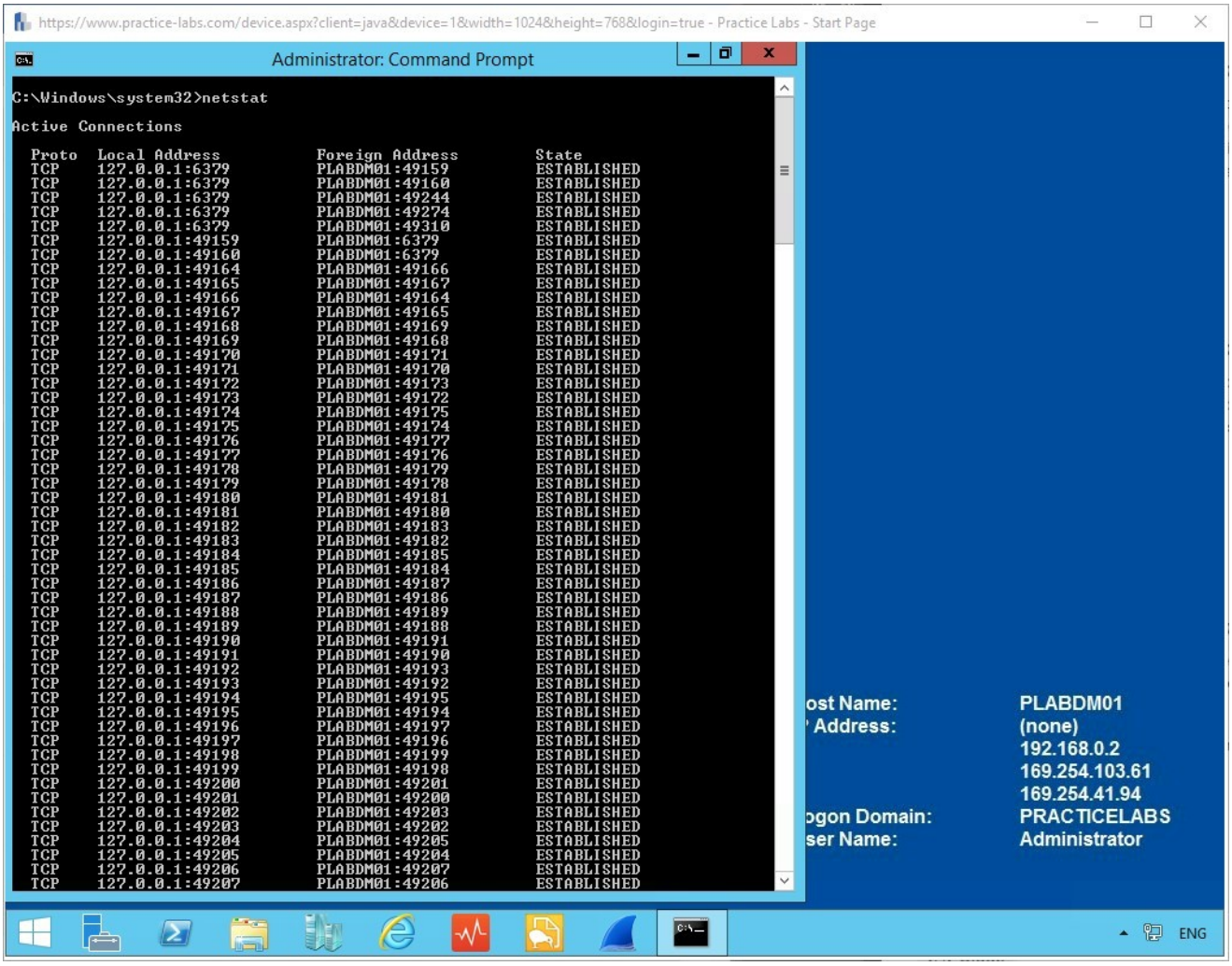


Figure 2.1 PLABDM01: Screenshot of netstat typical output.

The details shown relate to the Protocol being observed, the IP address which is a loopback address of 127.0.0.1 and finally at the bottom we can see the machine address of 192.168.0.2.

The third column displays the nature of the connection, it this case the connections have been established.

Step 2

Building on the netstat command, we have additional options which in turn present more and different forms of information.

Type into the console:

```
netstat -a
```

This now displays similar information but also displays all active connections and the TCP and UDP ports on which the computer is listening.

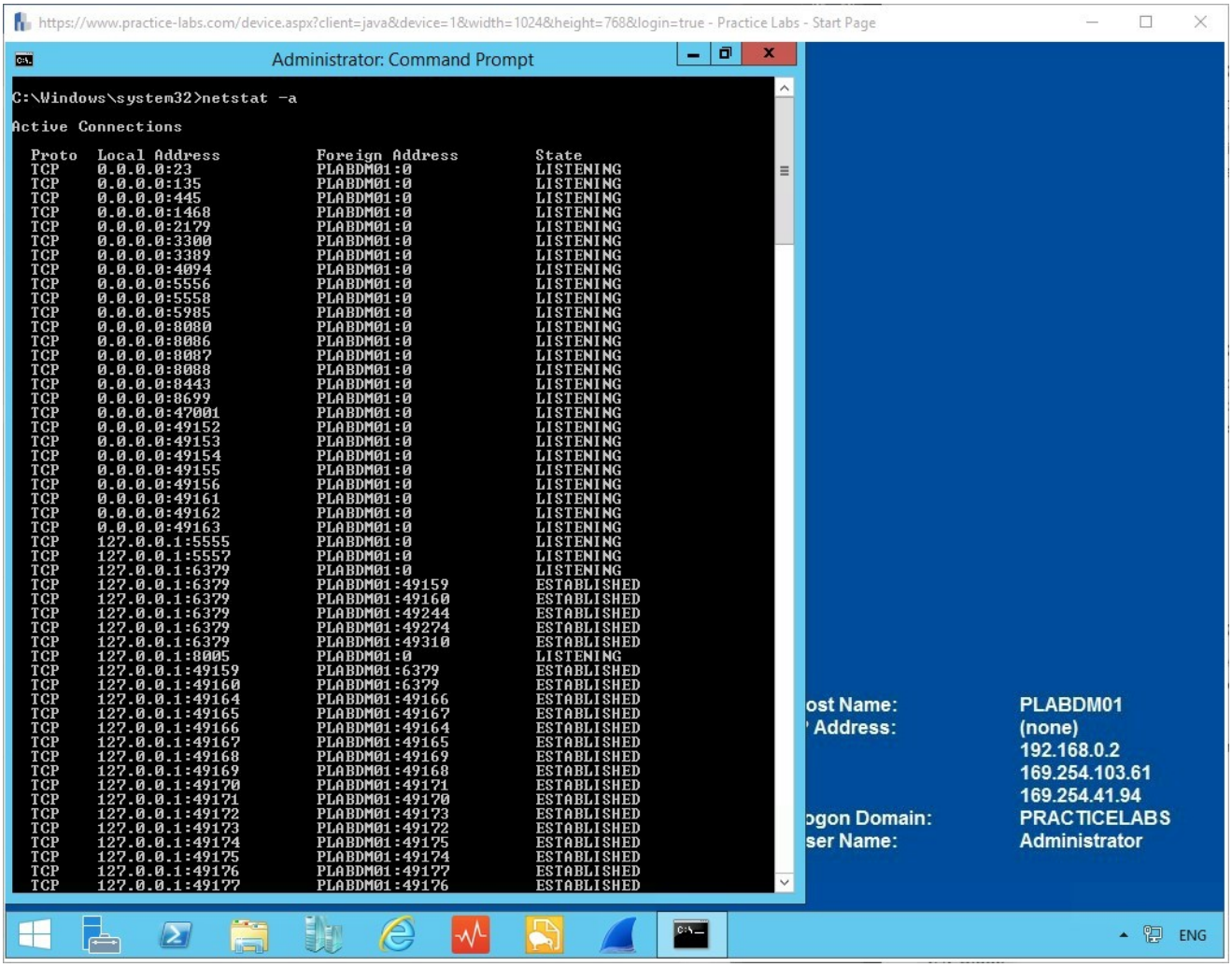


Figure 2.2 PLABDM01: Screenshot of netstat -a output.

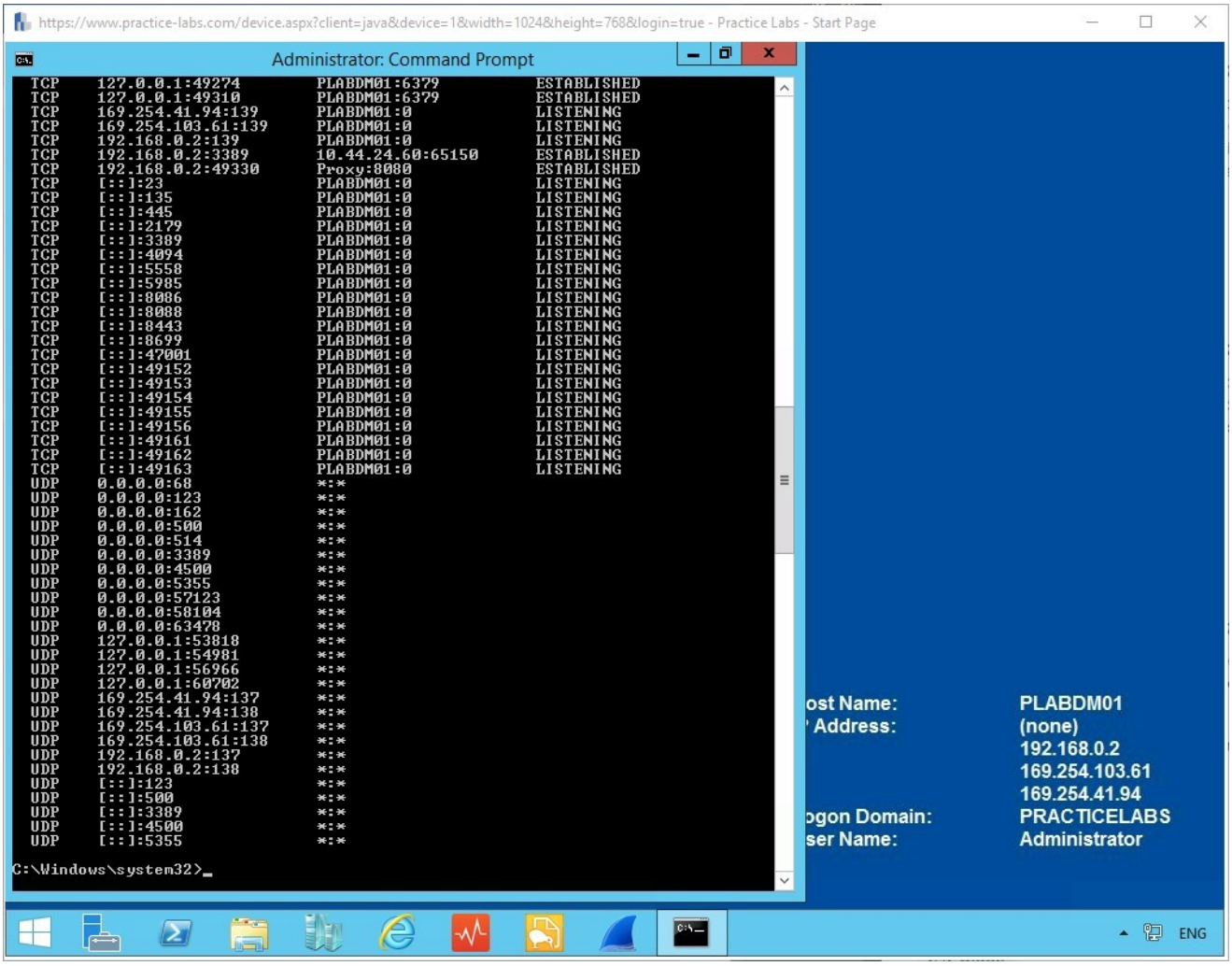


Figure 2.3 PLABDM01: Screenshot of netstat -a output continued.

A more verbose readout of ports and their condition is provided with this switch. It goes further to detail additional ports in a listening state and provides information on additional UDP as well as TCP protocols which are monitoring the network.

Step 3

To Display the top active connections to the device

Type into the console:

```
netstat -no
```

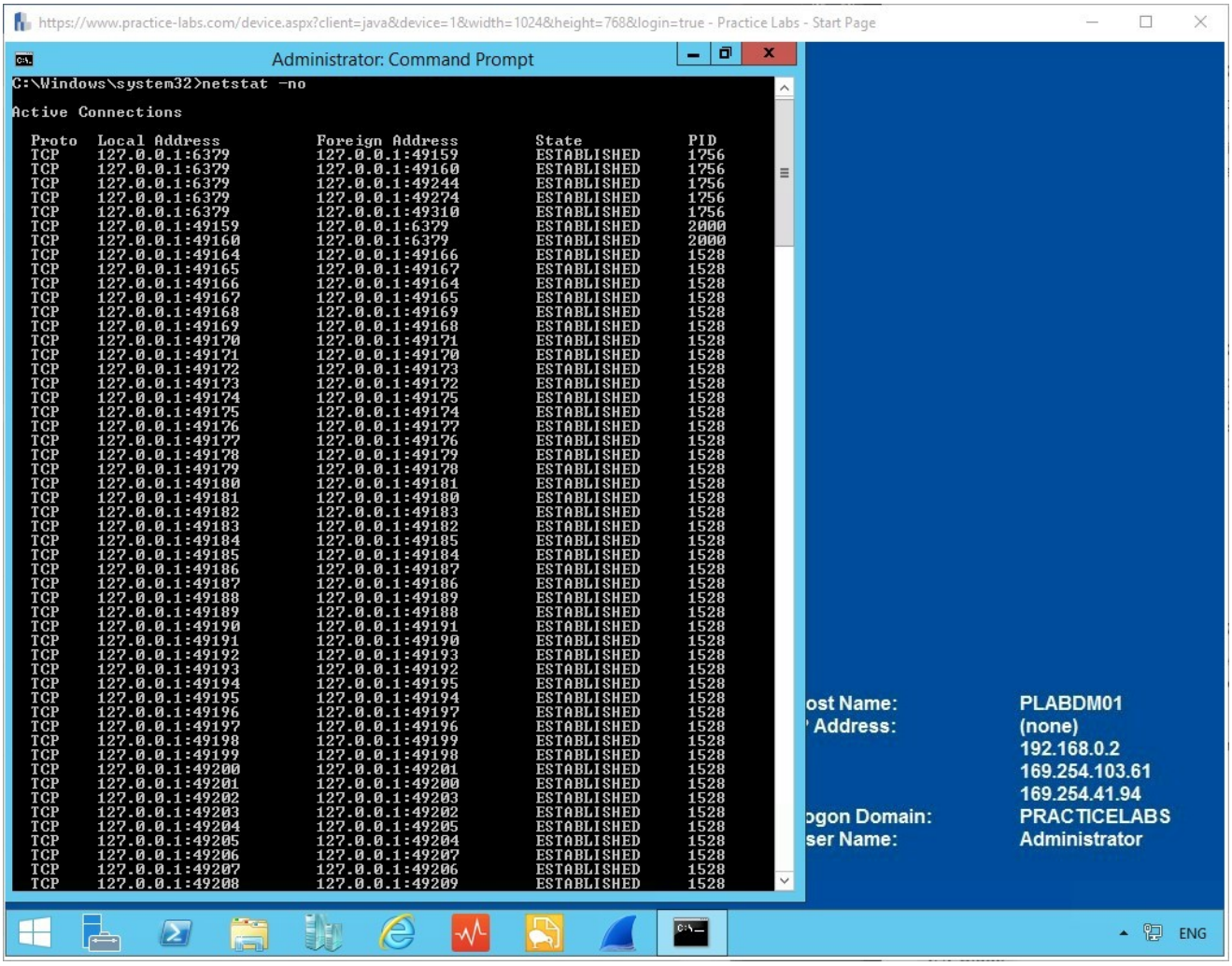


Figure 2.4 PLABDM01: Screenshot of netstat -no output.

This provides us with only the connections showing volumes of traffic and usefully it presents the PID or Process Identifier. Productively this is a useful method for quickly displaying those ports in use.

Now combine steps 2 and 3 together by typing the following command into the console:

```
netstat -ano
```

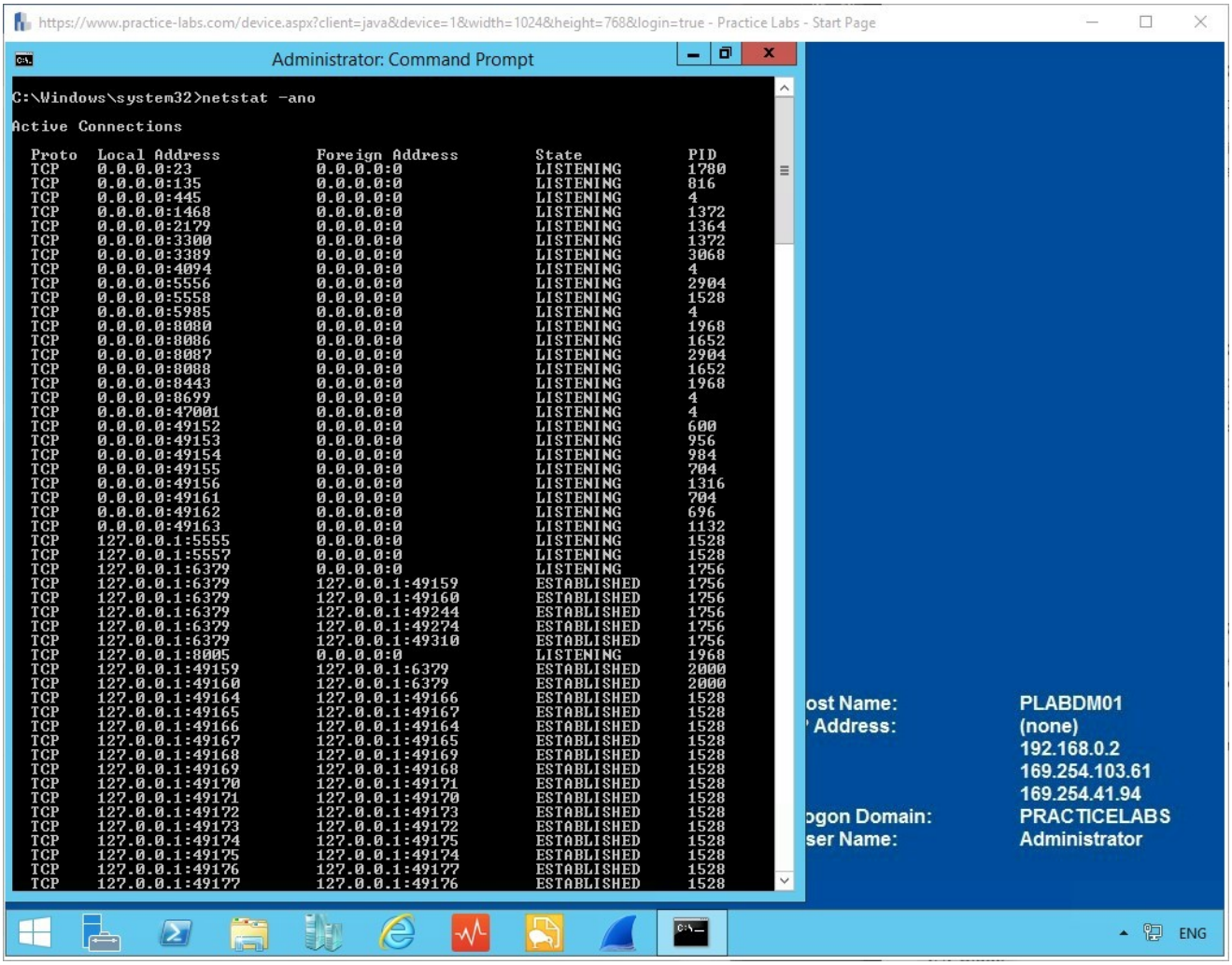


Figure 2.5 PLABDM01: Screenshot of netstat -ano output.

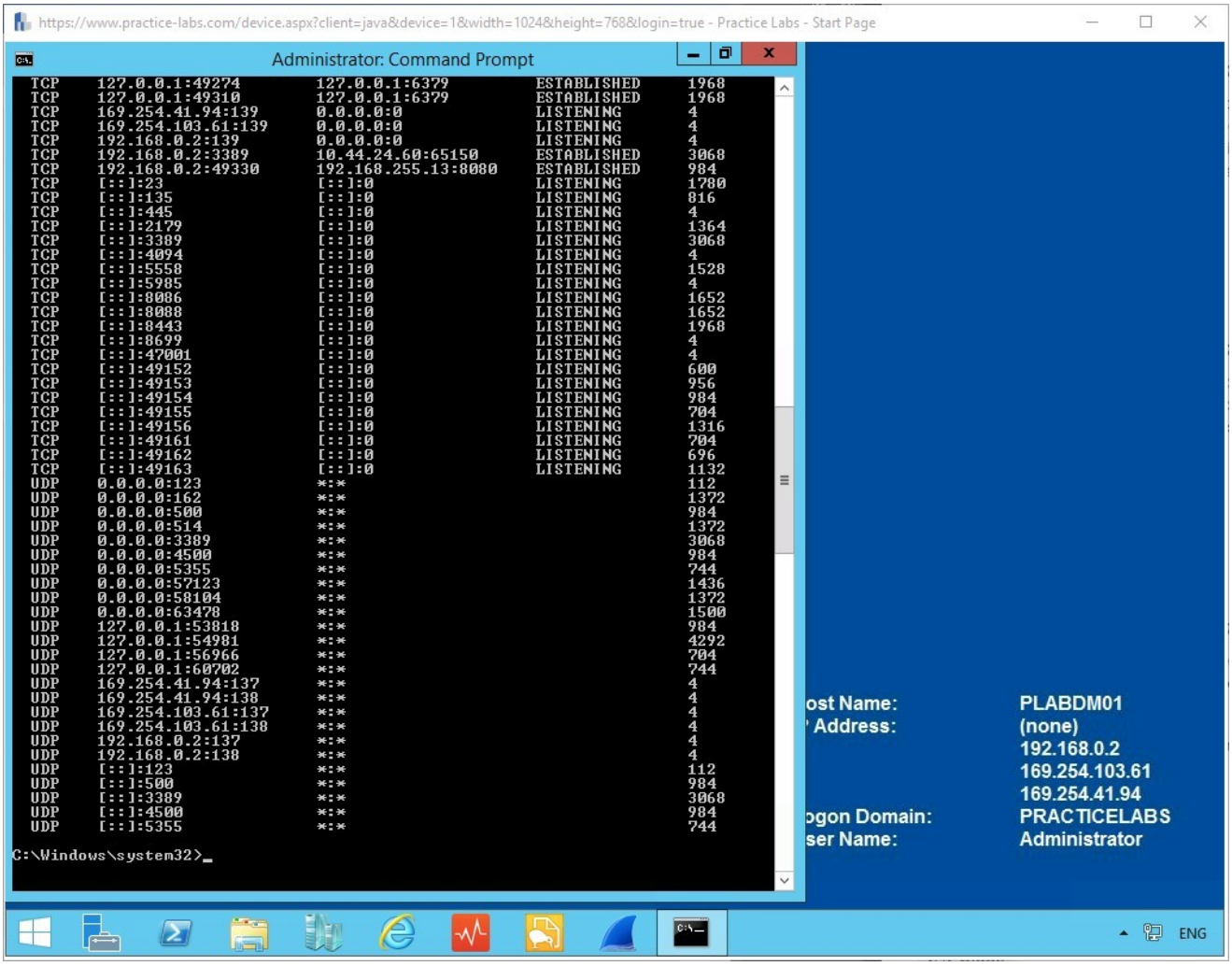


Figure 2.6 PLABDM01: Screenshot of netstat -ano output continued.

By applying the -a switch we display all the ports and their condition together with the PID that might be using or listening to the port for traffic to arrive or pass through.

Step 4

We can now track the PID information to see the process activity.

Right-click on the **Taskbar**.

Click on the **Task Manager** then navigate to the Tab at the top labeled **Details**.

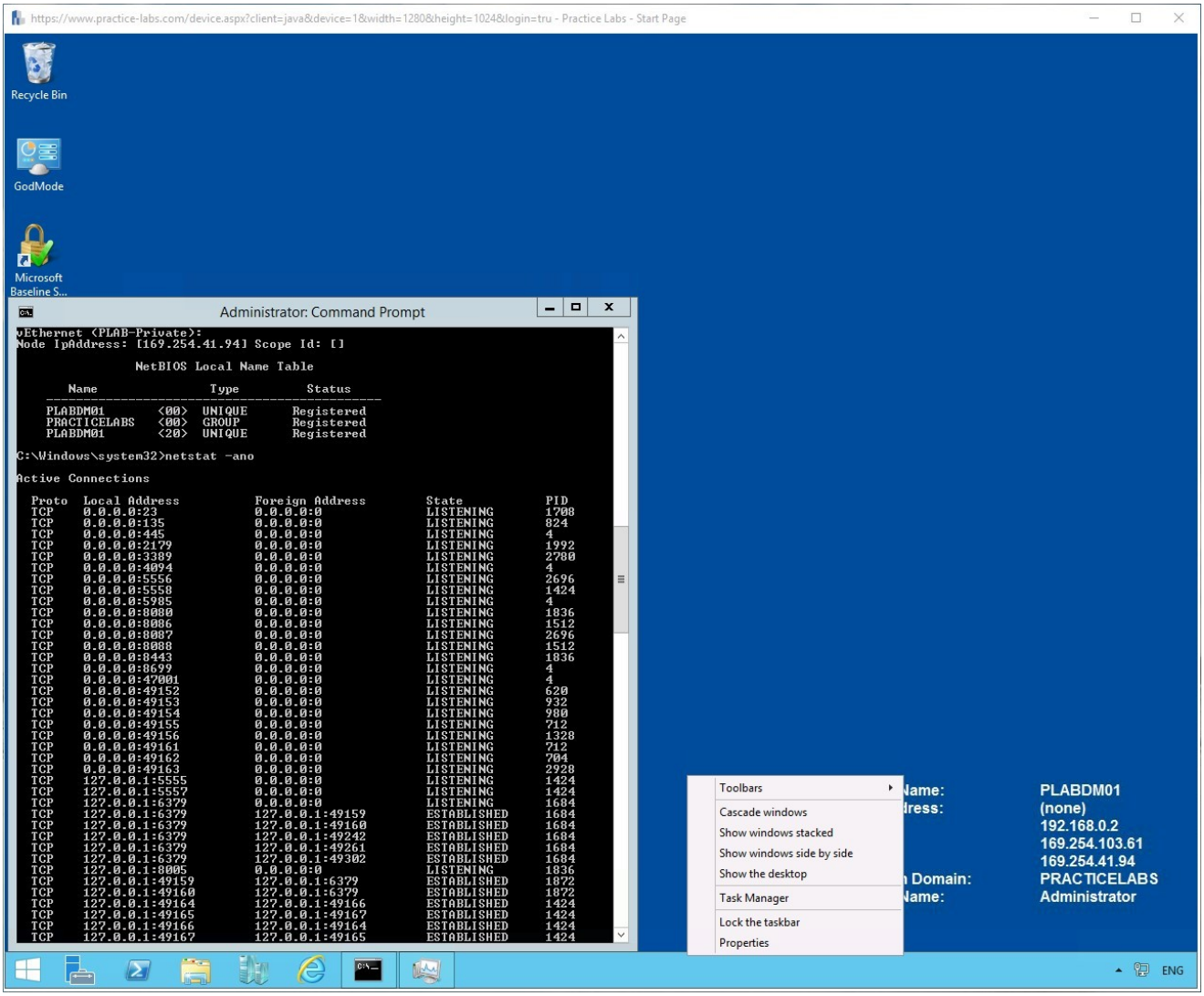


Figure 2.7 PLABDM01: Screenshot of Taskbar used to activate Task Manager.

You will see PID as one of the column headers.

Let's choose from the Netstat the PID of 4 from the Netstat output.

Organize the PID column by clicking on it to arrange by number.

Here we can see the PID process of 4 is being used by System.exe which is an NT Kernel and System process.

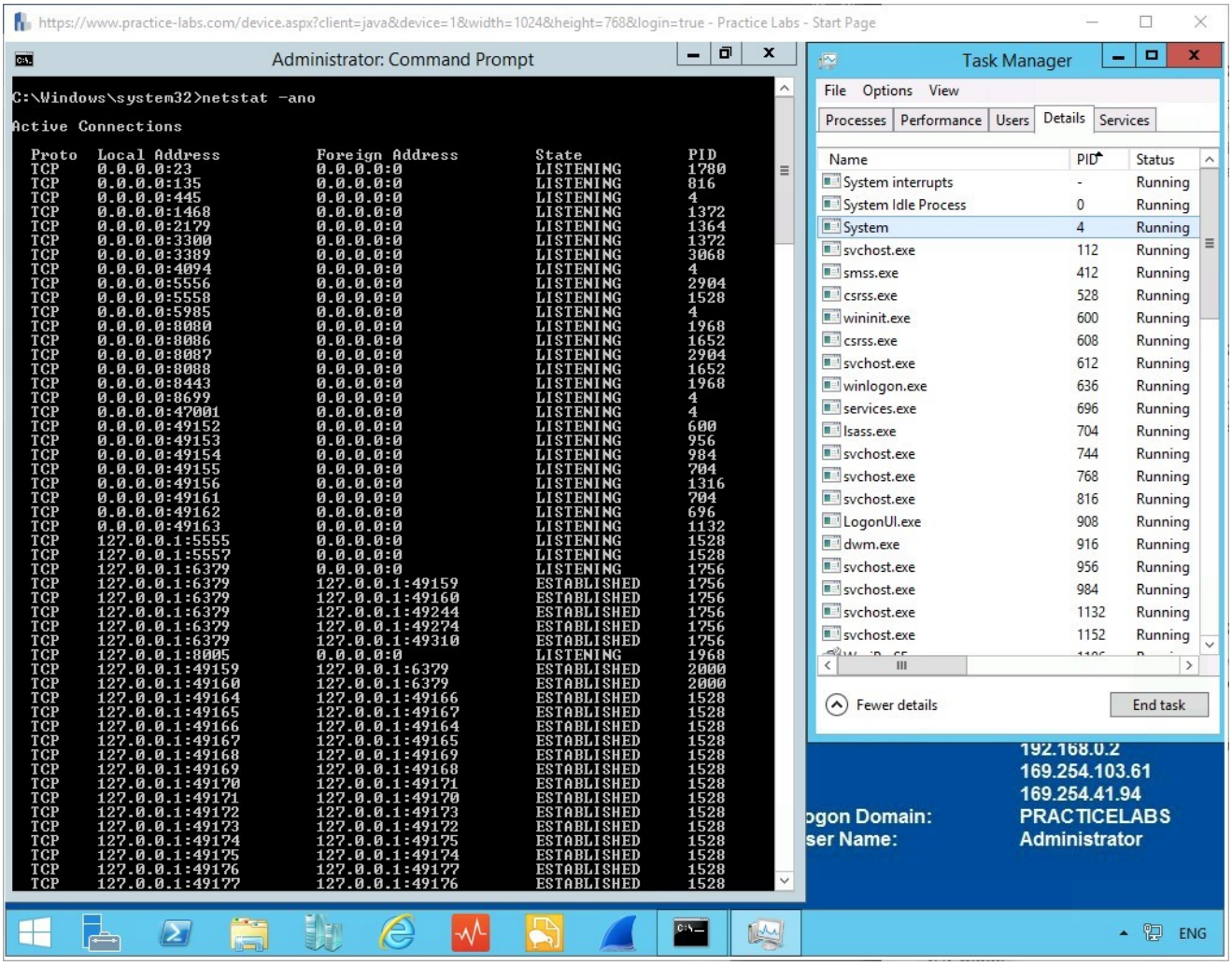


Figure 2.8 PLABDM01: Screenshot of Task Manager compared to netstat-ano with PID confirmation.

By using netstat we can investigate processes taking place on the network, so long as the process is visible directly in task manager it can be tracked down to provide a name. This, of course, can be further investigated to make sure it's nothing concerning.

We can use this method to track down the other netstat processes as well or eliminate activities which we are sure to be secure and normal.

Step 5

Display the Routing table.

Type the following command into the console:

```
netstat -r
```

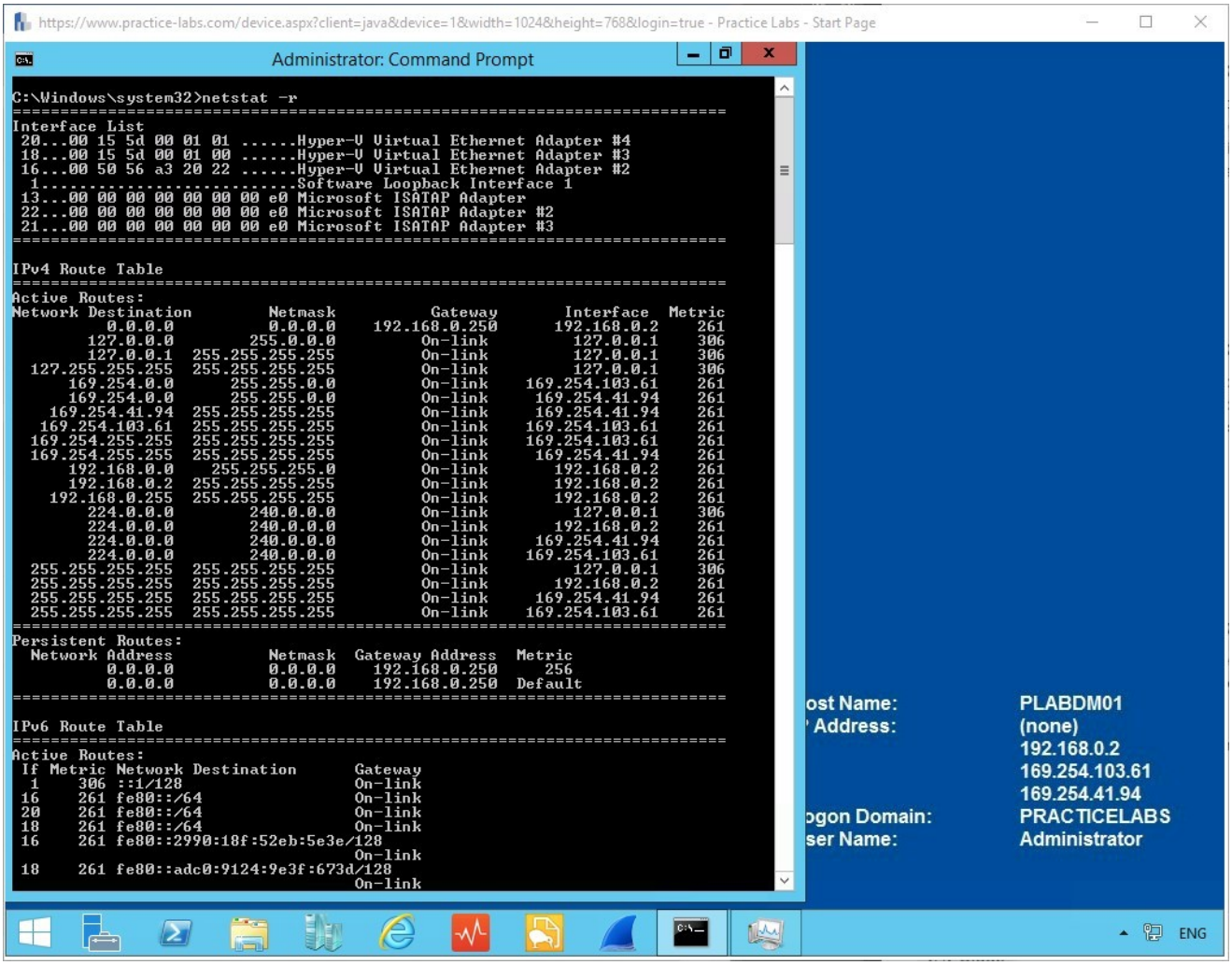


Figure 2.9 PLABDM01: Screenshot of netstat -r output.

The routing table is a key piece of information to display topologies directly related to the device and its surrounding environment. It details types of adapters used to make connections, the gateways that traffic is flowing through, and primarily its used as a troubleshooting tool when investigating where traffic bottlenecks might be occurring.

Step 6

The options -t, -u, -w, and -x show active TCP, UDP, RAW, or Unix socket connections. If you provide the -a flag, in addition, sockets that are waiting for a connection (i.e., listening) are displayed as well. This display will give you a list of all services that are currently running on your system.

Displaying connections on TCP which are awaiting a connection.

Type the following command into the console:

```
netstat -ta
```

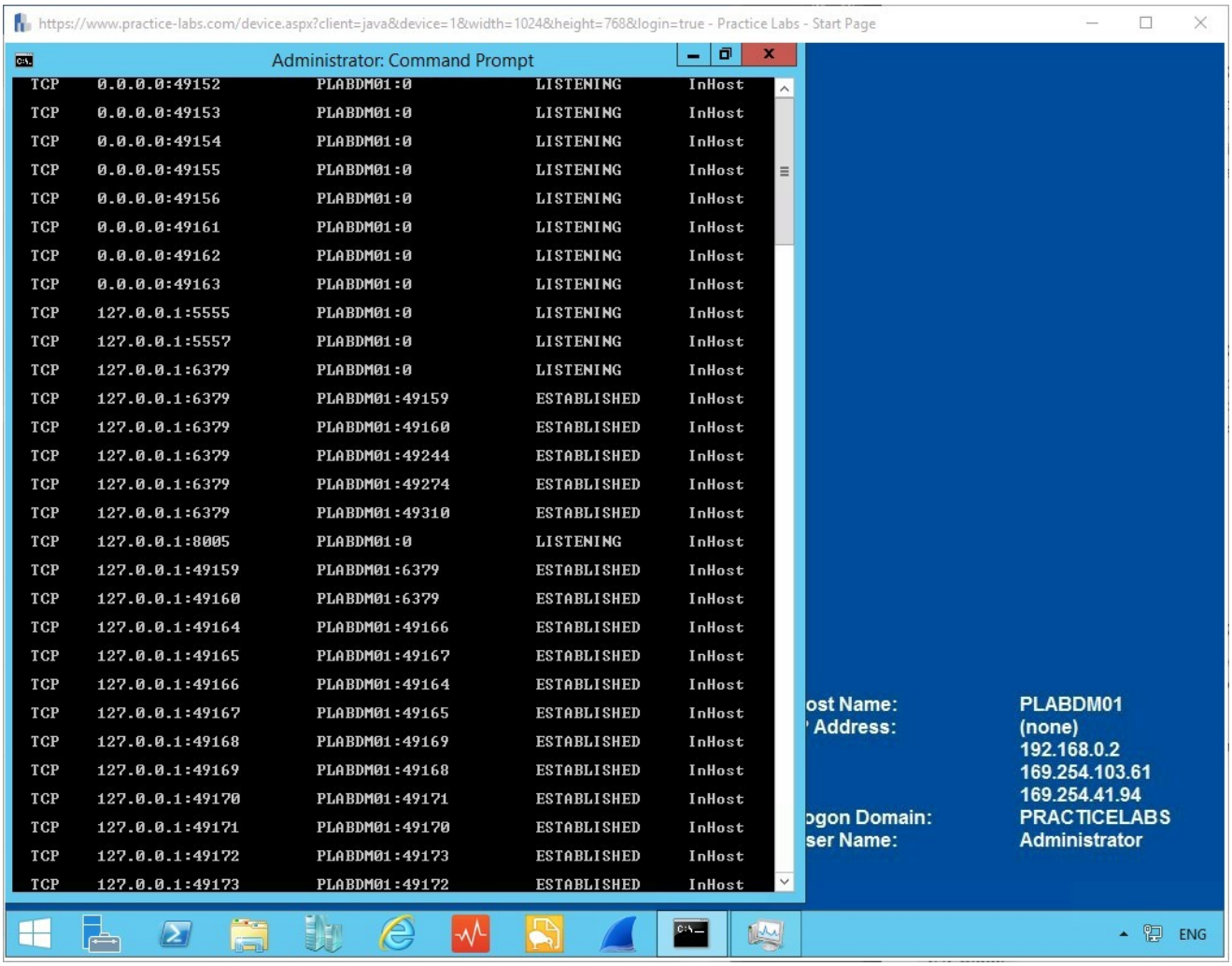


Figure 2.10 PLABDM01: Screenshot of netstat -ta output.

The output demonstrates with the switch -ta.

Step 7

To have netstat display statistics (-s) about TCP traffic (-p), and also force the addresses to be displayed in FQDN format (-f).

Type the following command into the console:

```
netstat -s -p tcp -f
```

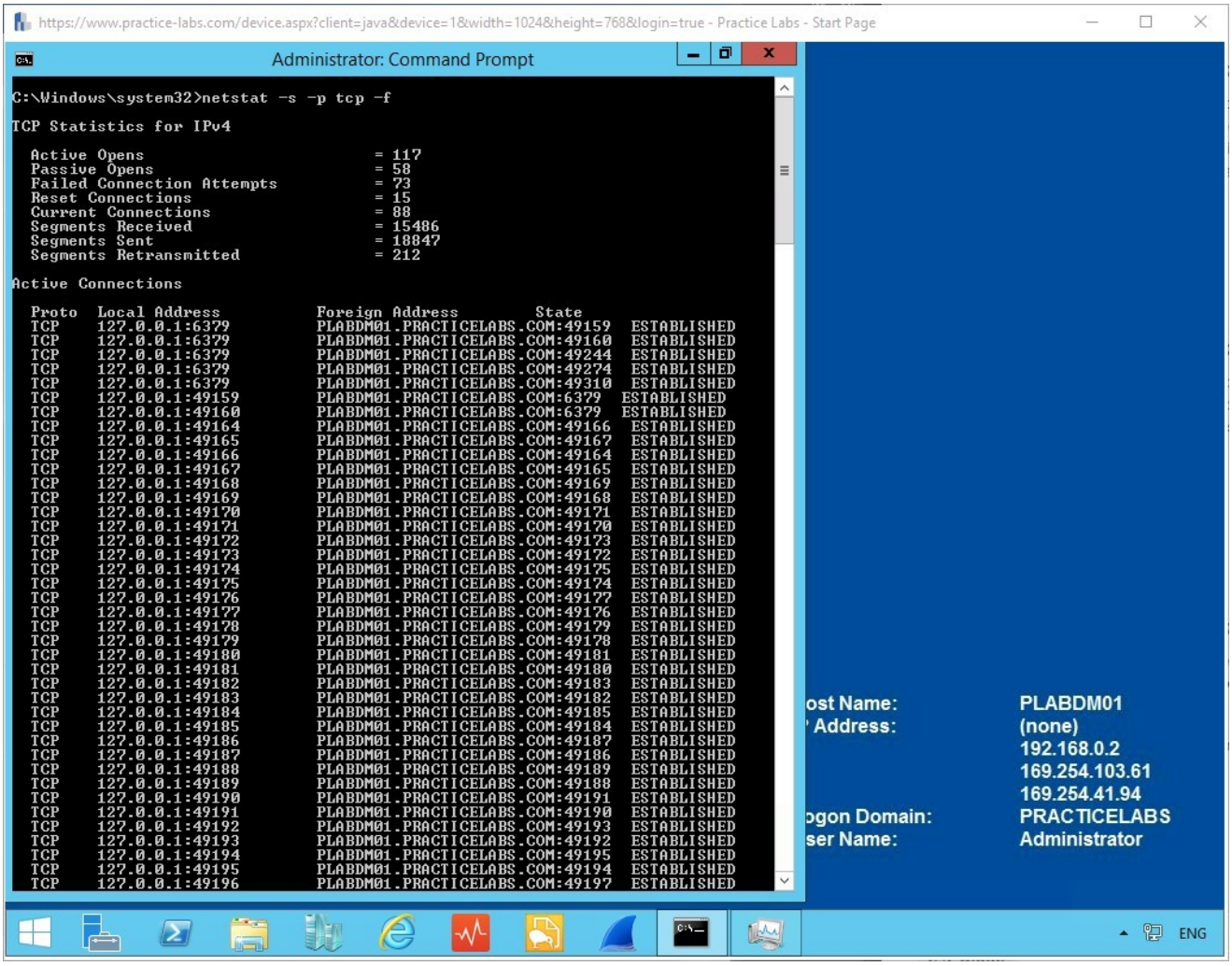


Figure 2.11 PLABDM01: Screenshot of netstat -s -p tcp -f output.

Step 8

To have a repeating function taking place in netstat displaying the network interface statistics (-e) and have them updated every 5 seconds we will use (-t 5).

Type the following command into the console:

```
netstat -e -t 5
```

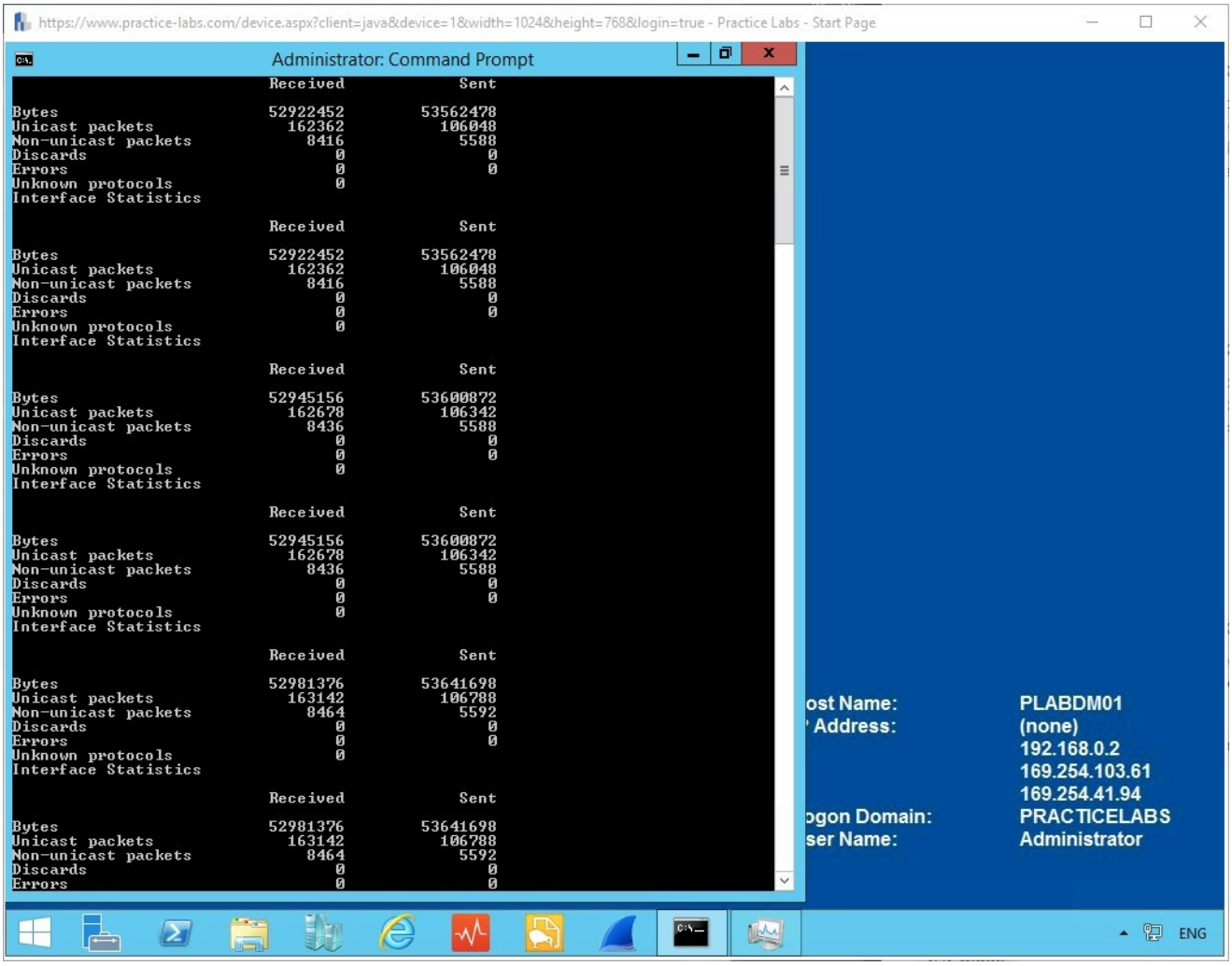


Figure 2.12 PLABDM01: Screenshot of netstat -e -t 5 output.

If we were expecting to see large traffic changes across the network, then manually monitoring the information as such is helpful as the figures displayed assist with network configuration confirmation.

When finished, stop the command by typing the following into the console:

```
Ctrl C
```

This will return you to the C:> prompt

Step 9

This command will check every second and print the results if a process starts listening on TCP port 80.

Type the following command into the console:

```
netstat -an 1 | find “80”
```

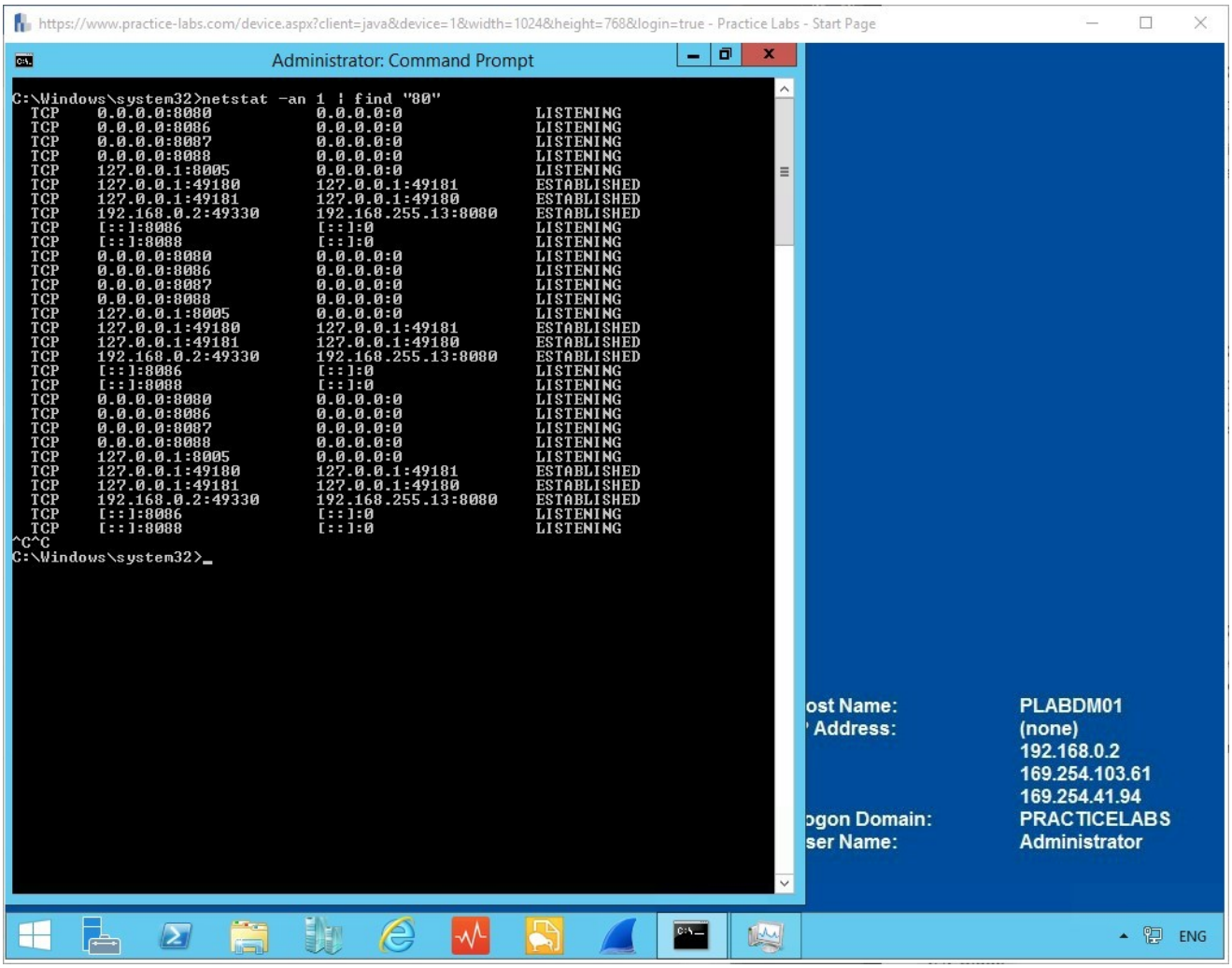


Figure 2.13 PLABDM01: Screenshot of netstat -an 1 | find “80” output.

Often we are interested in specific ports, especially if the port is being abused in some manner, as given in the output, port 80 has been specified, and we can watch the traffic changes occurring each second to see if anything unusual is taking place.

Remember to stop the query by typing:

```
Ctrl C
```

Leave all devices powered on in their current state and proceed to the next exercise.

Exercise 3 - Ping

Ping verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.

In this exercise you will complete the following tasks:

- Using the Ping command-line tool

Please refer to your course material or use your favorite search engine to research for more information about this topic.

Task 1 - Using the Ping command-line tool

In this task, you will be using the Ping command-line tool which is used to check connectivity to devices and establish is they are “up” or “down”.

Step 1

Ping uses the ICMP echo; here we are working with the IPv4 address, but the same concept is applied to IPv6 as well. We will ping PLABDC01.

Type the following command into the console:

```
ping 192.168.0.1
```

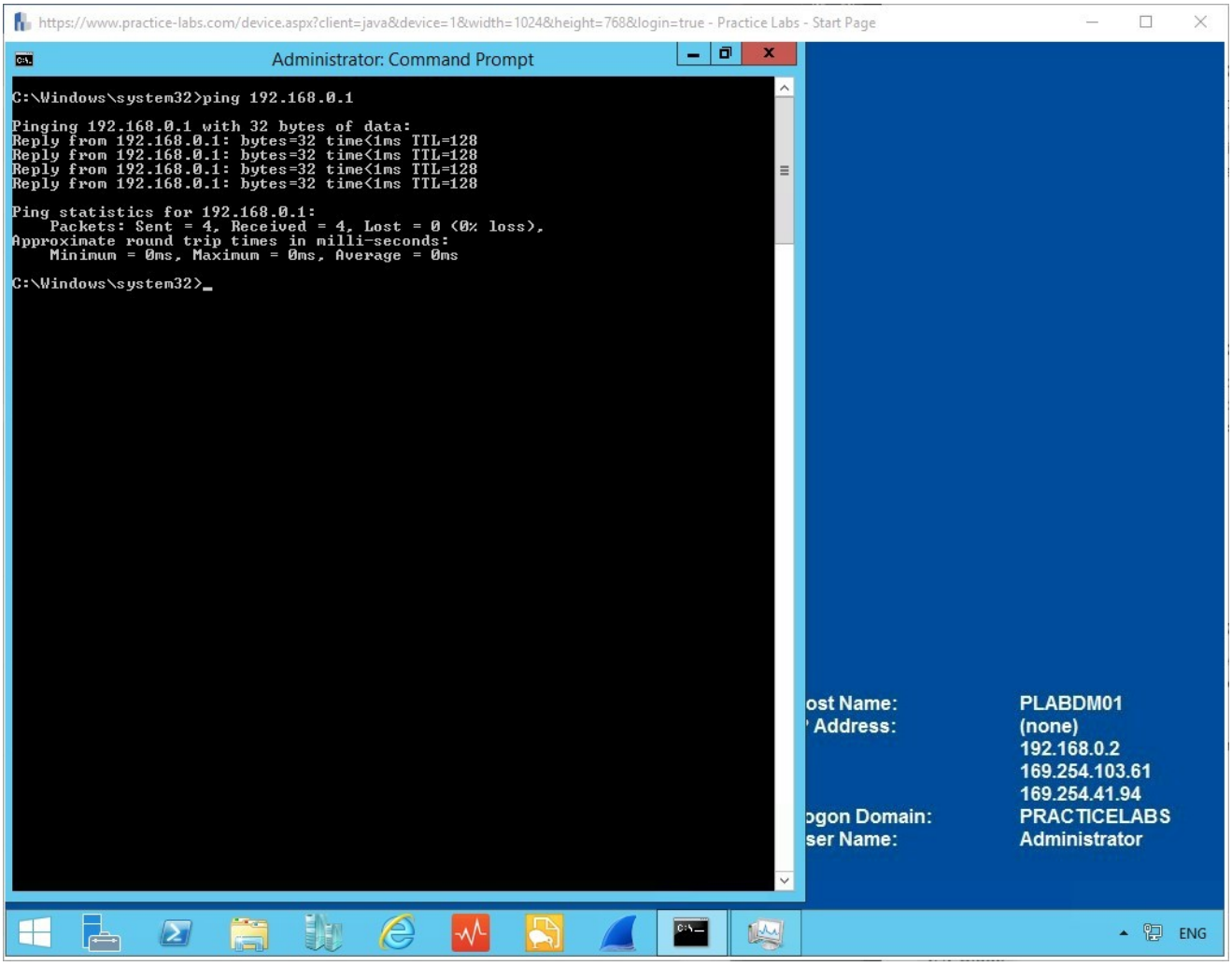


Figure 3.1 PLABDM01: Screenshot of ping command output.

This command helps us to check for any lost of packets returning the device; it establishes the concept of network errors or device connectivity.

Step 2

Let's now continuously send packets until the command to terminate is entered.

We might perform this check if we need to constantly monitor an interface which is under a maintenance check.

Type the following command into the console:

```
ping -t 192.168.0.1
```

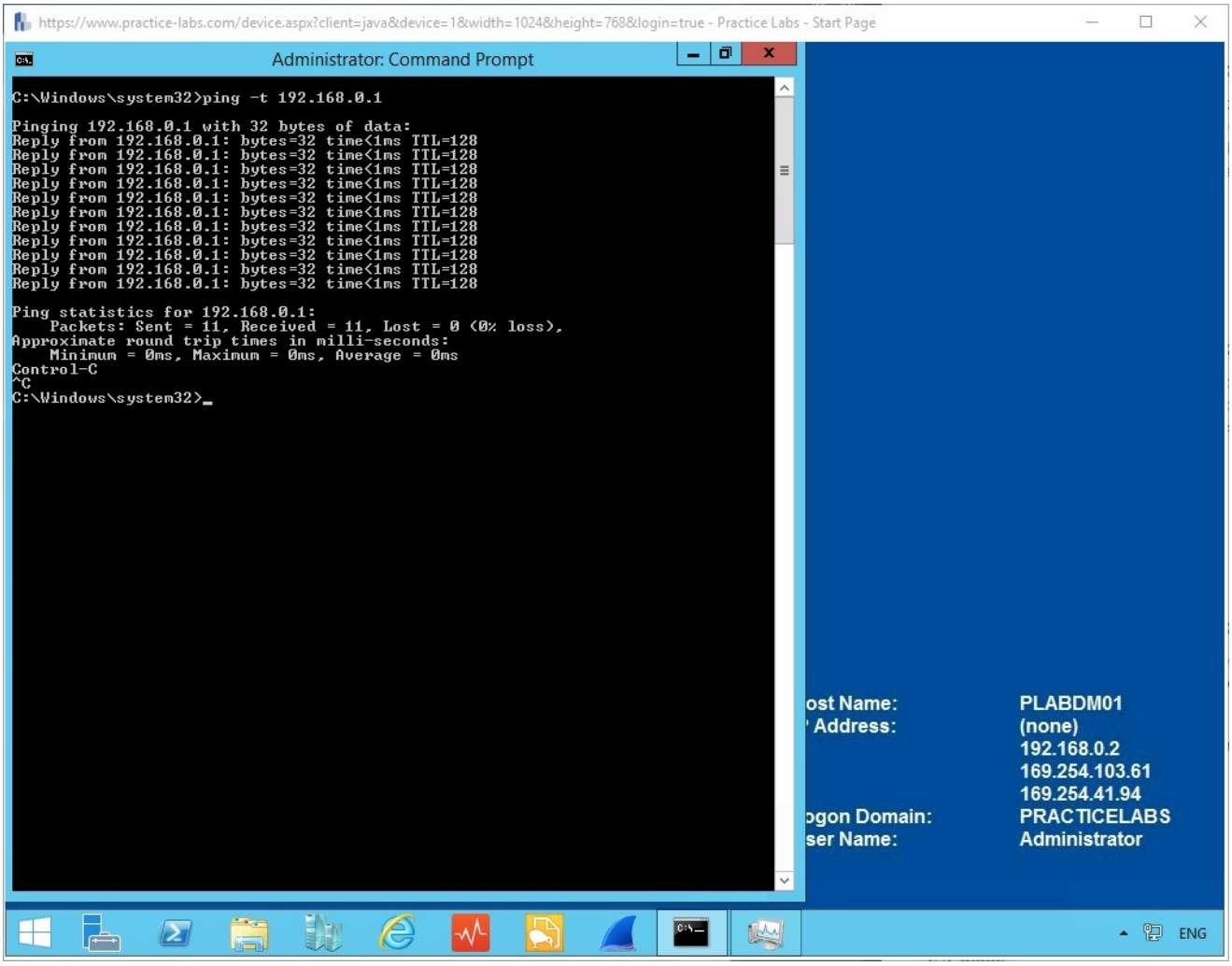


Figure 3.2 PLABDM01: Screenshot of ping -t command output.

This method is manipulating a number of times a ping should take place is useful when investigating devices which are having problems connecting to the network. However, it's the beginning method where we can flood a device by requesting it acknowledge out requests.

Type the following command into the console:

```
Ctrl -C
```

Step 3

Finally let's modify the ping command to edit the number of echo counts to 30, each having a size of 1000 bytes.

Type the following command into the console:

```
ping -n 30 -l 1000 192.168.0.1
```

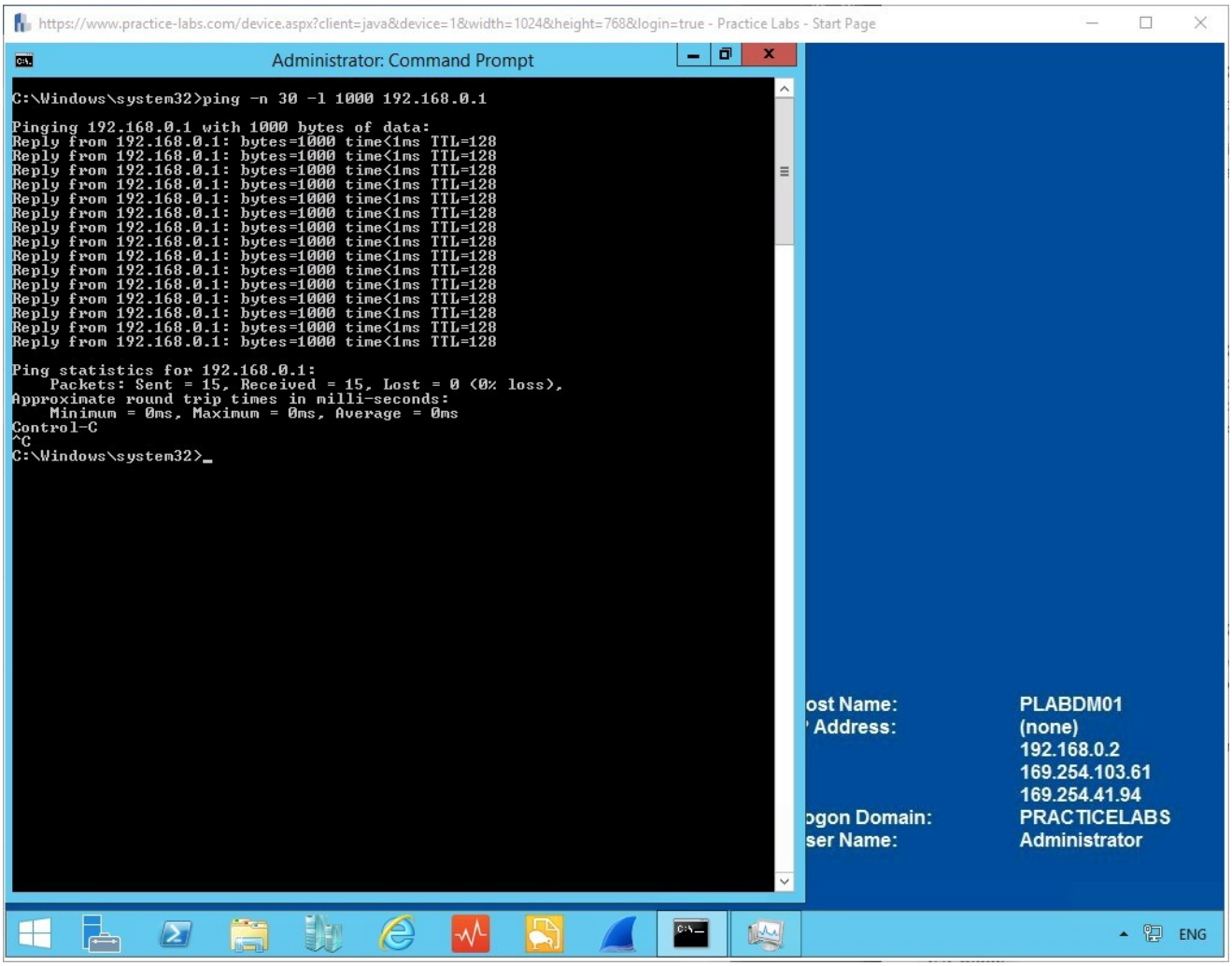


Figure 3.3 PLABDM01: Screenshot of ping -n 30 -l (ip) output.

The modification of packet sizes is also a helpful tool when diagnosing networking problems, but again this technique is known to flood old server and routing devices by having them handle packets which are beyond their firmware capabilities.

Leave all devices powered on in their current state and proceed to the next exercise.

Exercise 4 - Tracert and Route

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.

Route displays and modifies the entries in the local IP routing table which helps to understand the topology of a network.

In this exercise you will complete the following tasks:

- Using the Tracert command line tool
- Using the Route command line tool

Please refer to your course material or use your favorite search engine to research for more information about this topic.

Task 1 - Using the Tracert command line tool

In this task, you will be using the Tracert command line tool to read information about packet paths taken. This can identify blocks on the network or show where information is not being routed correctly.

Step 1

The -h in this command specify a max hop of 5 steps. Given we are working on a small topology all hops will effectively be only 1 step large.

Type the following command into the console:

```
tracert -h 5 192.168.0.1
```

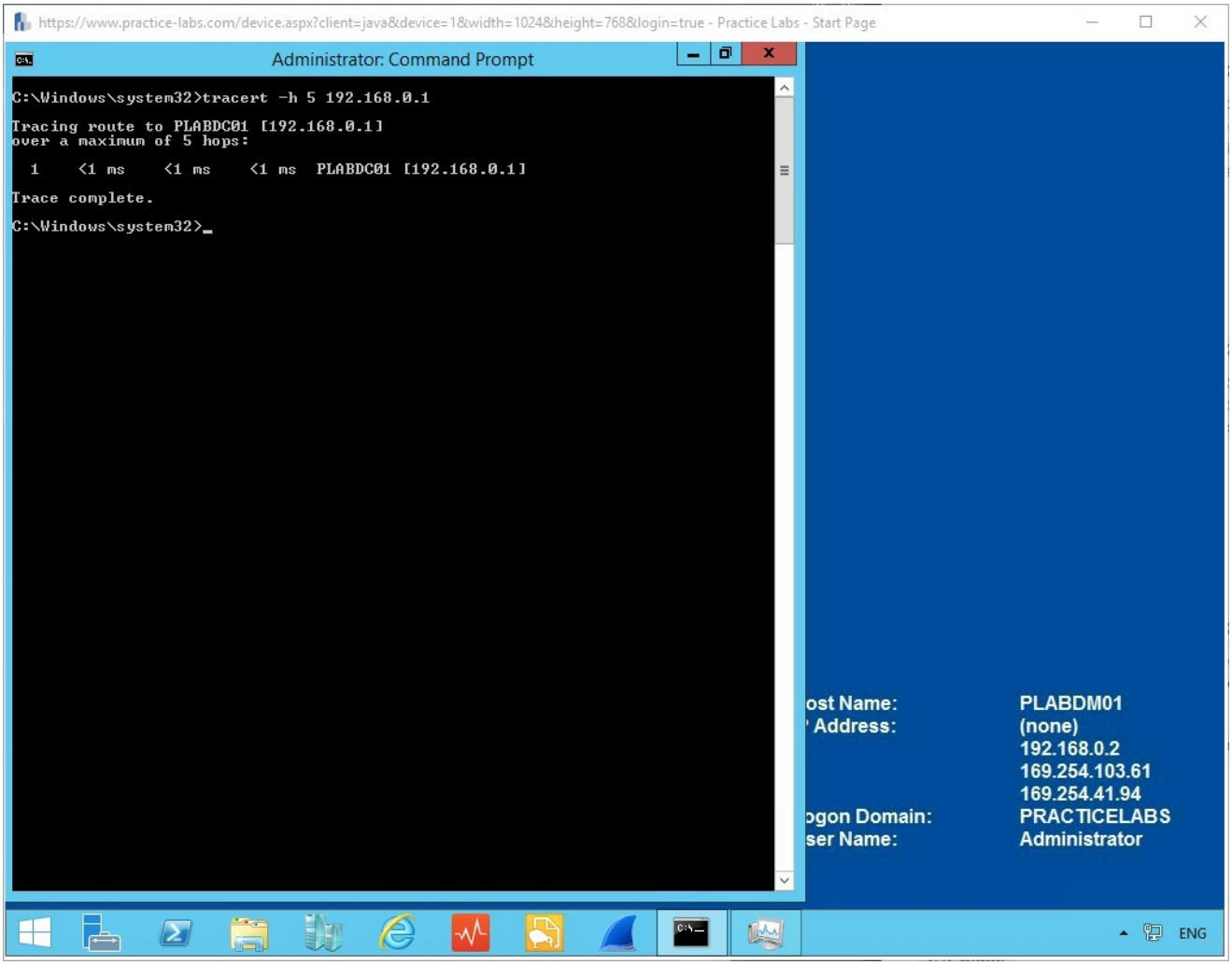


Figure 4.1 PLABDM01: Screenshot of tracert -h 5 (ip) output.

Task 2 - Using the Route command line tool

Another method for calling the routing table like netstat -r is the route command. In this task, you will be using the route command to display the same route information but it's useful to know a variety of commands which have similar functions.

Step 1

Type the following command into the console:

```
route PRINT
```

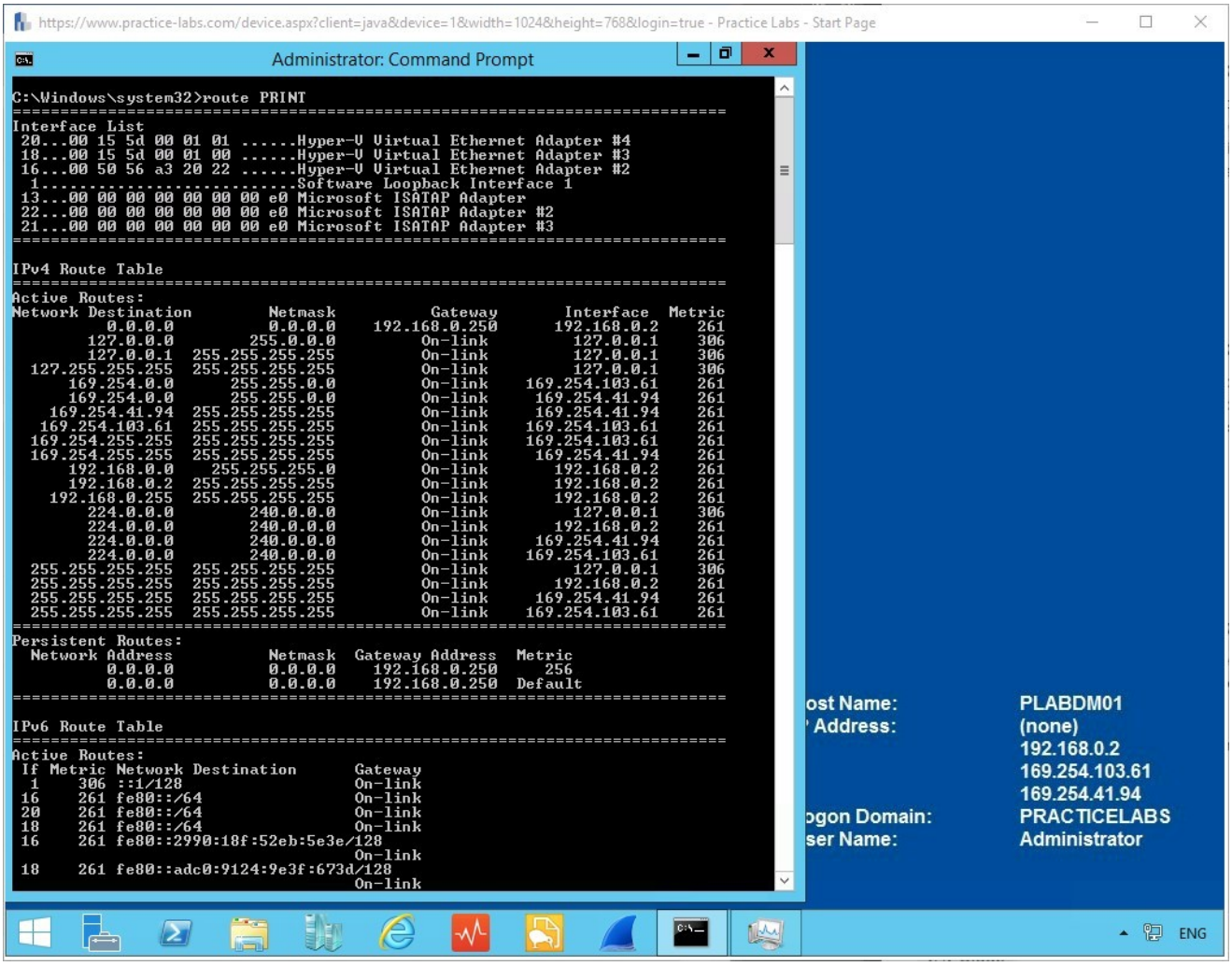


Figure 4.2 PLABDM01: Screenshot of route PRINT output.

We are presented with an Interface List attached to the device which can be key to learning more about the network configurations.

Importantly we are then presented with an IPv4 Route Table which shows us the Active Routes being applied to the network adapters, we are given the Network Destinations, any masking taking effect on the IP's, the Gateway the communications are traveling through, the interface IP and metrics of data flowing.

Finally, we are told if there are any persistent routes on the devices.

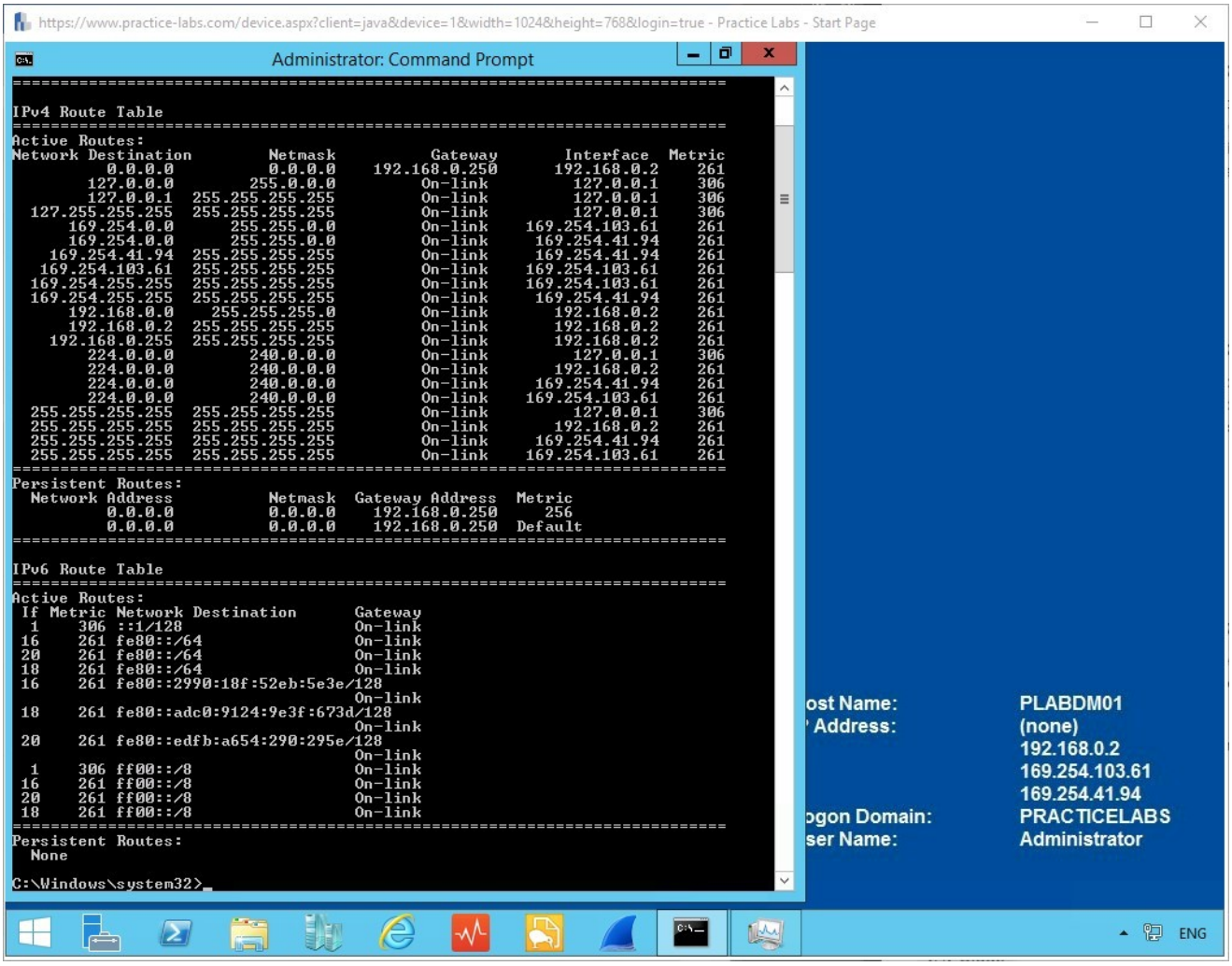


Figure 4.3 PLABDM01: Screenshot of route PRINT output continued.

The route command also tells us that there are no persistent routing paths being used with this device on IPv6.

Leave all devices powered on in their current state and proceed to the next exercise.

Exercise 5 - ARP and Whoami

Address Resolution Protocol (ARP) performs IP address-to-media access control address resolution for outgoing packets. As each outgoing addressed IP datagram is encapsulated in a frame, source and destination MAC addresses must be added. Determining the destination MAC address for each frame is the responsibility of ARP.

Whoami Displays user, group and privileges information for the user who is currently logged on to the local system. If used without parameters, it displays the current domain and user name.

In this exercise you will complete the following tasks:

- Using the ARP command line tool
- Using the “Whoami” command line tool

Please refer to your course material or use your favorite search engine to research for more information about this topic.

Task 1 - Using the ARP command line tool

In this task, you will be using the ARP command line tool to displays entries in the Address Resolution Protocol cache, which contains one or more tables that are used to store IP addresses and their resolved Ethernet addresses.

Step 1

Type the following command into the console:

```
arp -a
```

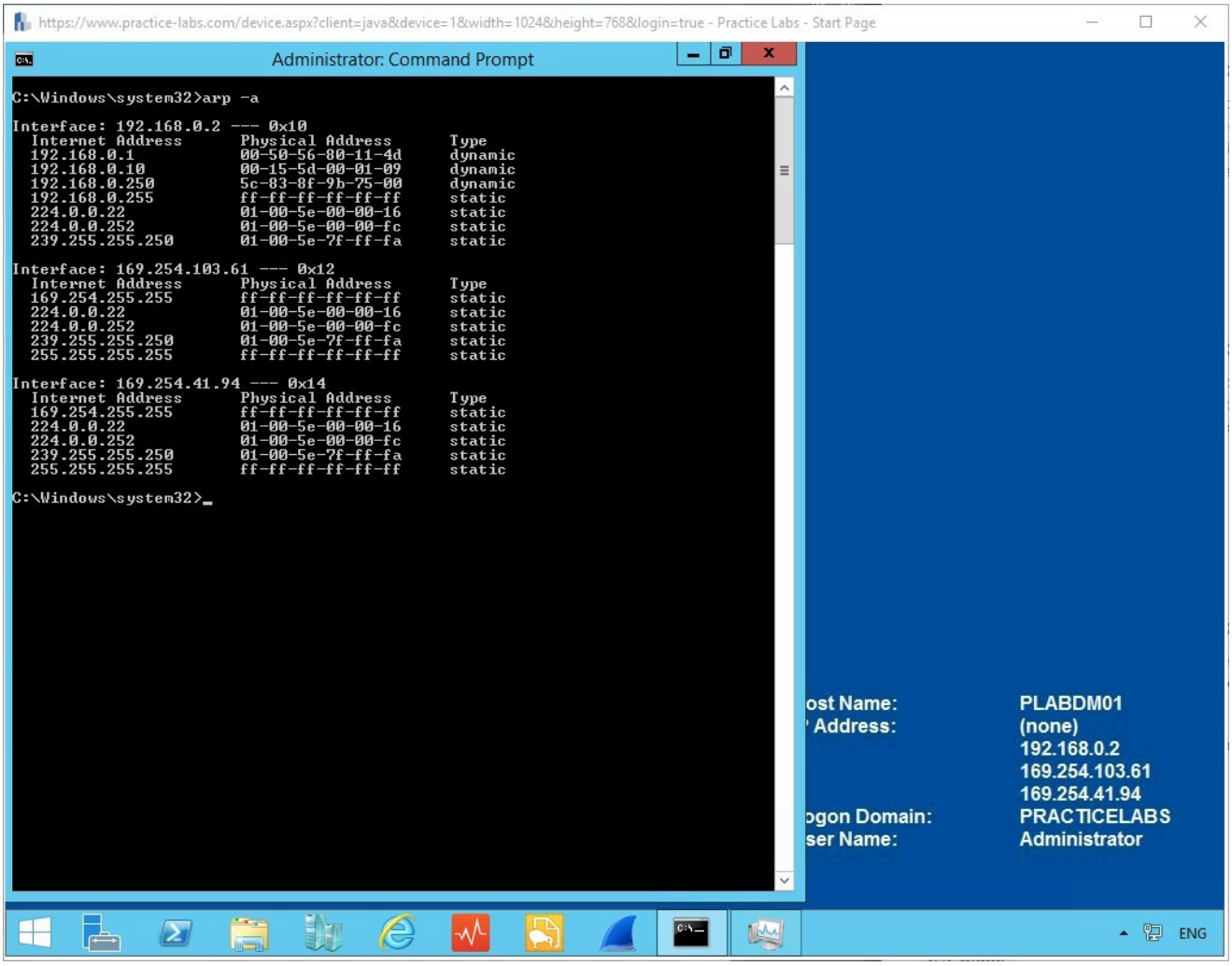


Figure 5.1 PLABDM01: Screenshot of arp -a output.

The command arp -a is used to display static and dynamic entries to the ARP cache table, above we can see that IP of the PLABDM01 device against its physical address location or MAC address and the type of relationship described as dynamic.

Step 2

Type the following command into the console:

```
arp -av
```

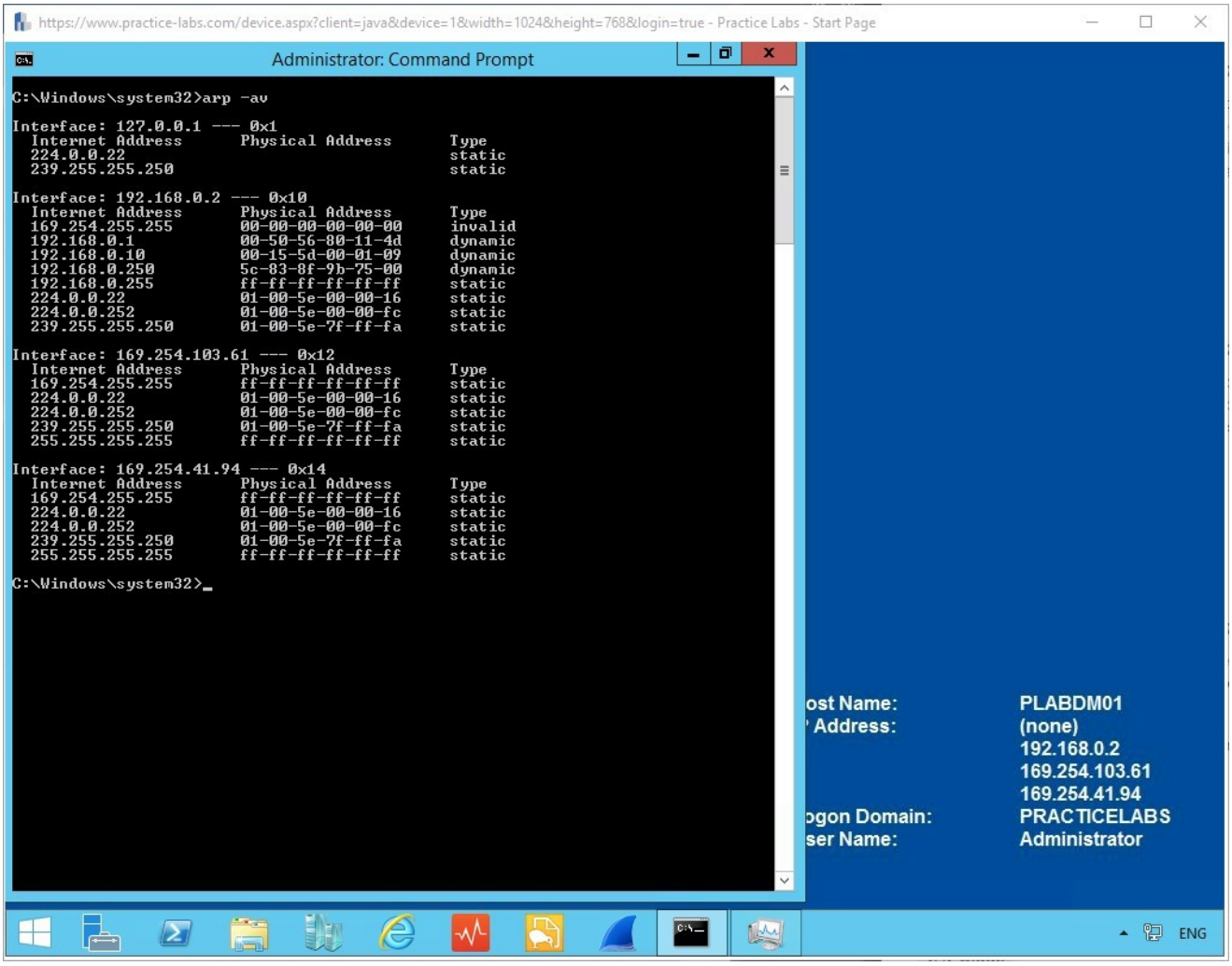


Figure 5.2 PLABDM01: Screenshot of arp-av output.

Attaching the -av switch displays information in a verbose mode and brings into view the additional interface of the loopback address.

Step 3

Type the following command into the console:

```
arp -a -N 192.168.0.2
```

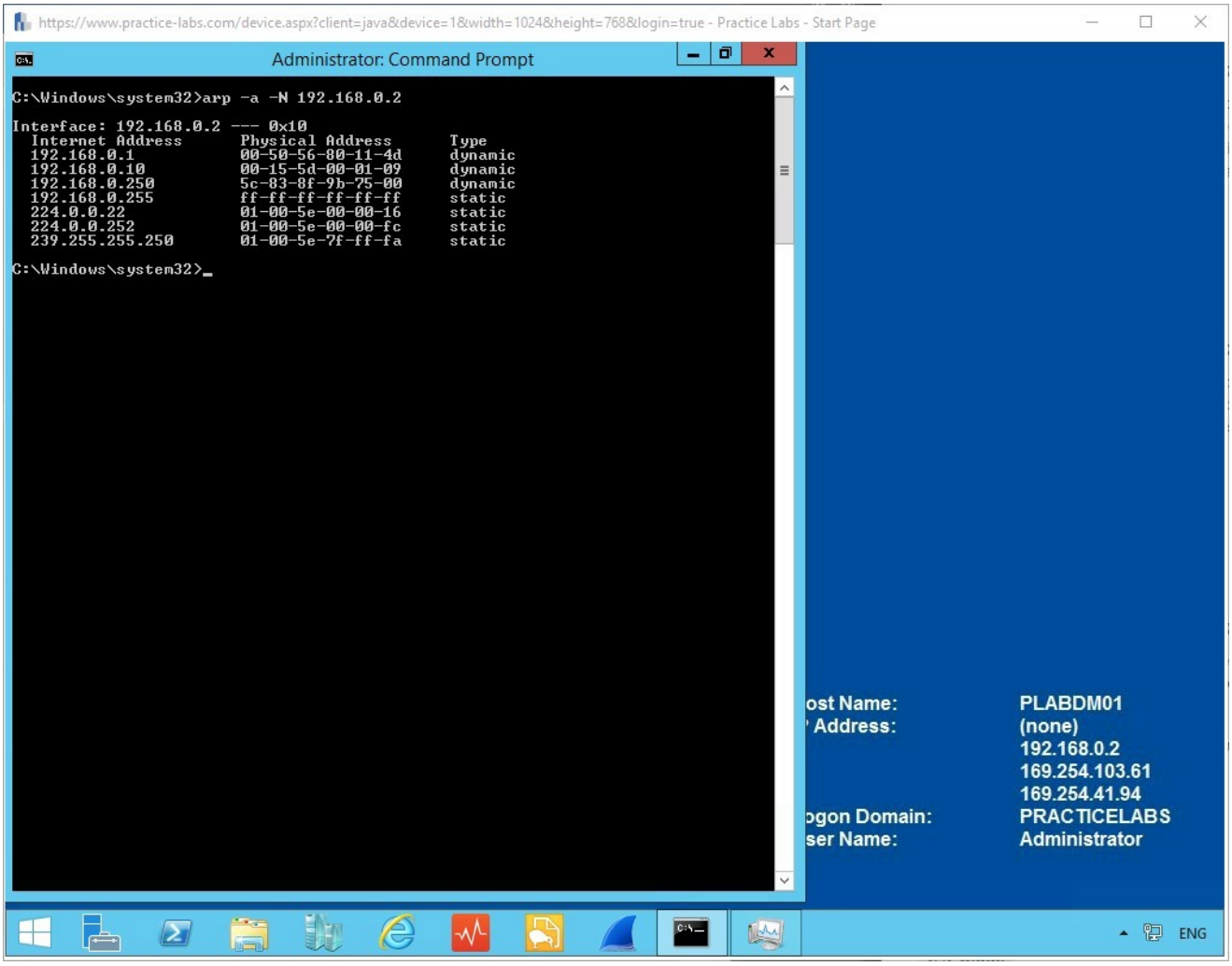


Figure 5.3 PLABDM01: Screenshot of arp -a -N (ip) output.

By applying the switch of -N we learn more about the interfaces by listing the entries for the specified interface.

Task 2 - Using the "Whoami" command line tool

In this task you will be using the Whoami command line tool, to discover which user account is currently logged into the device.

Step 1

Type the following into the console:

```
whoami
```

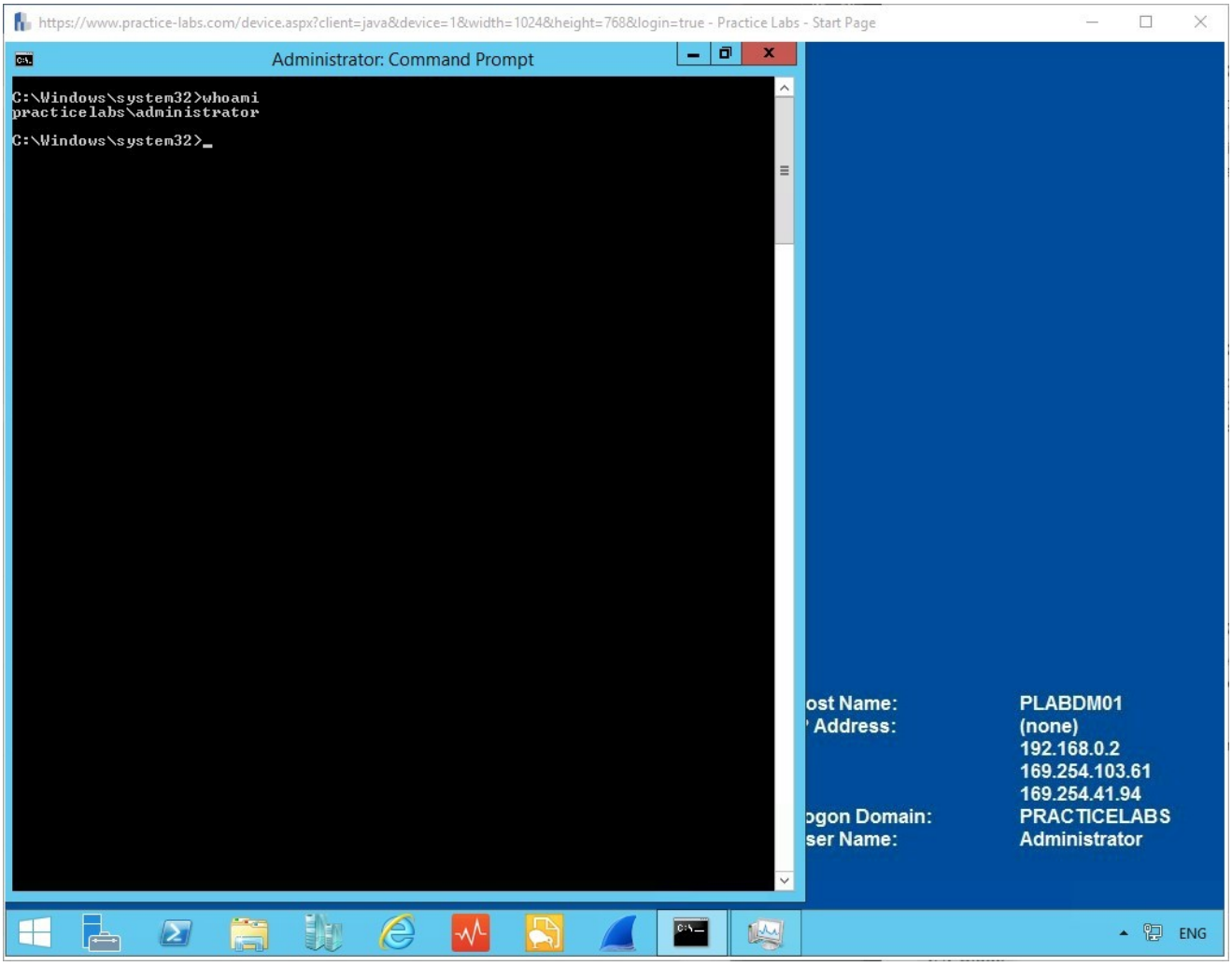


Figure 5.4 PLABDM01: Screenshot of Whoami output.

The output is a call to the windows device to clarify exactly what level of authority is currently using the console interface. This is a simple but effective.

> Shut down all virtual machines used in this exercise using Practice Labs power button function to revert these devices to their default settings. Alternatively, you may sign out of the lab portal to power down all devices.

Summary

You covered the following activities in this module:

- Ipconfig
- Netstat

- Ping
- Tracert and Route
- ARP and Whoami