**NETWORKING PRINCIPLES LAB MANUAL 3**

# Lab 3 – Part A – Trace Route

## Objectives

* Determine network connectivity to a destination host.
* Trace a route to a remote server using tracert.

## Background / Scenario

Data travels from a source end device to a destination device. Route tracing software lists the path traversed by this data.

This route tracing software is typically executed at the command line as:

**tracert** <destination network name or end device address>

(Microsoft Windows systems)

Or

**traceroute** <destination network name or end device address>

(UNIX, Linux systems, and Cisco devices, such as switches and routers)

Both **tracert** and **traceroute** determine the route taken by packets across an IP network. The **tracert** (or **traceroute**) tool is often used for network troubleshooting. By showing a list of routers traversed, the user can identify the path taken to reach a particular destination on the network or across internetworks. Each router represents a point where one network connects to another network and through which the data packet was forwarded. The number of routers traversed is known as the number of hops the data traveled from source to destination.

Command-line based route tracing tools are usually embedded with the operating system of the end device. This activity should be performed on a computer that has Internet access and access to a command line.

**Required Resources**

❖ PC with Internet access

**Instructions**

## Part A.1: Determine Network Connectivity to a Destination Host

To trace the route to a distant network, the PC must have a working connection to the Internet. Use the ping command to test whether a host is reachable. Packets of information are sent to the remote host with instructions to reply. The PC measures whether each packet receives a response, and how long it takes for those packets to cross the network.

1. Navigate to the Command Prompt, enter **ping www.cisco.com** to determine if it is reachable.
2. Now ping one of the Regional Internet Registry (RIR) websites located in different parts of the world to determine if it is reachable:

|  |  |
| --- | --- |
| Africa: | [www.afrinic.net](http://www.afrinic.net/) |
| Australia: | [www.apnic.net](http://www.apnic.net/) |
| South America: | [www.lacnic.net](http://www.lacnic.net/) |
| North America: | [www.arin.net](http://www.arin.net/) |

The website you selected will be used in the next part for use with the **tracert** command.

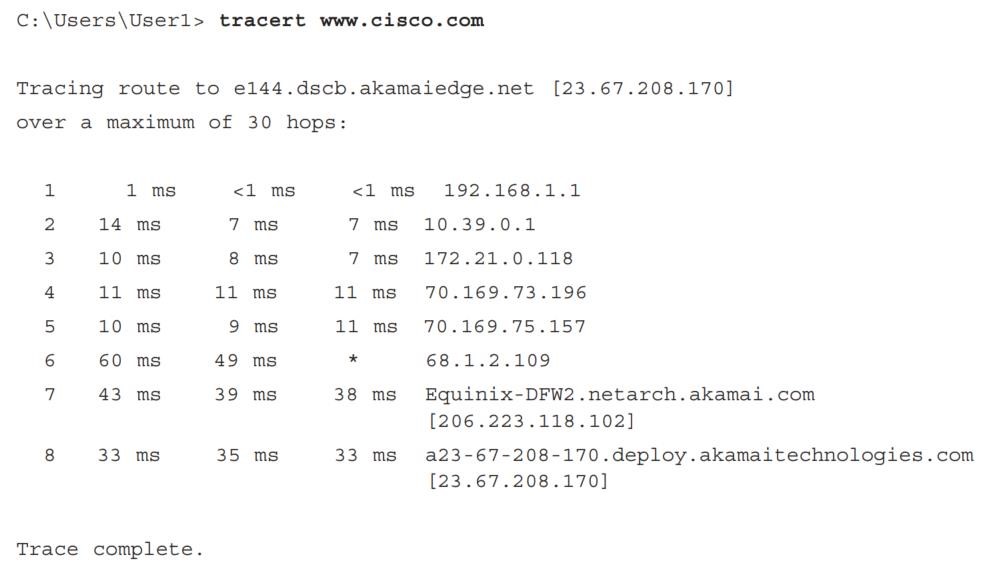
## Part A.2: Trace a Route to a Remote Server Using Tracert

After you use **ping** to determine if your chosen websites are reachable, you will use **tracert** to determine the path to reach the remote server. Look closely at each network segment that is crossed.

Each hop in the **tracert** results displays the routes that the packets take when traveling to the final destination. The PC sends three ICMP echo request packets to the remote host. Each router in the path decrements the time to live (TTL) value by 1 before passing it onto the next system. To decrement is to count down. When the decremented TTL value reaches 0, the router sends an ICMP Time Exceeded message back to the source with its IP address and the current time. When the final destination is reached, an ICMP echo reply is sent to the source host.

**Step 1:** Trace a route t[o www.cisco.com.](http://www.cisco.com/)

At the prompt, trace the route to **www.cisco.com**.



In this example, the source host sends three ICMP echo request packets to the first hop (192.168.1.1) with the TTL value of 1. When the router 192.168.1.1 receives the echo request packets, it decrements the TTL value to 0. The router sends an ICMP Time Exceeded message back to the source. This process continues until the source host sends the last three ICMP echo request packets with TTL values of 8 (hop number 8 in the output above), which is the final destination. After the ICMP echo request packets arrive at the final destination, the router responds to the source with ICMP echo replies.

For hops 2 and 3, these IP addresses are private addresses. These routers are the typical

setup for point-of-presence (POP) of the ISP. The POP devices connect users to an ISP network.

**Step 2:** Trace a route to a RIR web site.

1. Now perform a **tracert** to one of the RIR web sites from the previous part.

|  |  |
| --- | --- |
| Africa: | [www.afrinic.net](http://www.afrinic.net/) |
| Australia: | [www.apnic.net](http://www.apnic.net/) |
| South America: | [www.lacnic.net](http://www.lacnic.net/) |
| North America: | [www.arin.net](http://www.arin.net/) |

1. A web-based **whois** tool is found at http://whois.domaintools.com/. It can be used to determine the domains traveled from the source to destination.

**Question:** List the domains below from your **tracert** results using a web-based whois tool, such as [http://whois.domaintools.com/.](http://whois.domaintools.com/)

|  |
| --- |
| 172.20.0.1  172.16.16.1 |

# Lab 3 – Part B – My Protocol Rules

## Objectives

* Relate computer network protocols to the rules that you use every day for various forms of communication.
* Define the rules that govern how you send and interpret text messages.
* Explain what would happen if the sender and receiver did not agree on the details of the protocol.

## Background / Scenario

Before beginning to communicate with each other, we establish rules or agreements to govern the conversation. These rules, or protocols, must be followed for the message to be successfully delivered and understood. Among the protocol characteristics that govern successful human communication are:

* An identified sender and receiver
* Agreed upon method of communicating
* Common language and grammar
* Speed and timing of delivery
* Confirmation or acknowledgment requirements

The techniques that are used in network communications share these fundamentals with human conversations

## Instructions

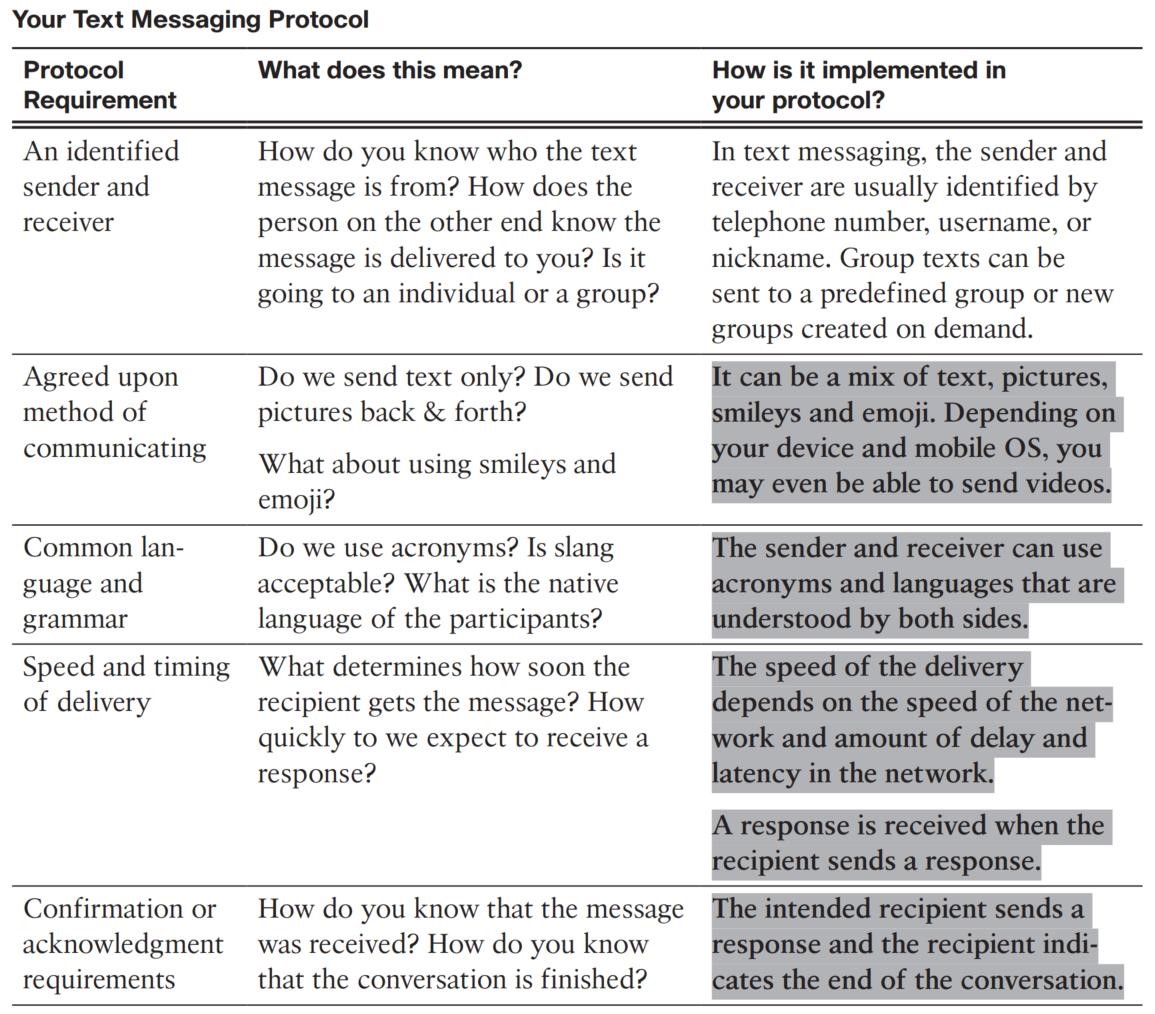
Think about the commonly accepted protocol standards for sending text messages to your friends. Fill out the chart on the next page with some of the rules that you follow when texting with friends and others. The first row has been filled in as an example.

The speed of the delivery depends on the data rate of the network and the latency of the network.

People can use acronyms and languages which are understandable by both sides.

A message status should be displayed to inform the user that the message was sent/received.

People communicate in various ways. Thus, it is important to support text, images and even emojis.



HCommunicassssssss

## Reflection

1. Now that you have documented the protocols that you use when sending and reading text messages, do you think that these protocols would be the same if you were texting with friends or with your parents and teachers? Explain your answer.

|  |
| --- |
| The protocol will be the same but the data will probably be different. |

1. What do you think that the consequences would be if there were no agreed-upon protocol standards for different methods of communications?

|  |
| --- |
| We would not be able to communicate as there would be many issues with communication such as misunderstandings |

1. Share your protocol rules with your classmates. Are there differences between your protocols and theirs? If so, could these differences result in misunderstanding of the messages?

|  |
| --- |
| If the protocols are not compatible, a misunderstanding of messages could result. |

# Lab 3 – Part C – Determine the MAC Address of a Host

## Objectives

* Determine the MAC address of a Windows computer on an Ethernet network using the **ipconfig /all** command.
* Analyze a MAC address to determine the manufacturer.

## Background / Scenario

Every computer on an Ethernet local network has a Media Access Control (MAC) address that is burned into the Network Interface Card (NIC). Computer MAC addresses are usually displayed as 6 sets of two hexadecimal numbers separated by dashes or colons (example: 15-EF-A3-45-9B-57). The **ipconfig /all** command displays the computer MAC address. You may work individually or in teams.

## Required Resources

* PC running Windows 10 with at least one Ethernet network interface card (NIC)
* Connectivity to the Internet

## Instructions Part C.1: Locating the MAC Address on a Computer

In this part of the lab, you will determine the MAC address of a computer using the Windows **ipconfig** command.

**Step 1:** Display information for the command **ipconfig / all**.

1. Right-click on the **Start** button and select **Command Prompt**.

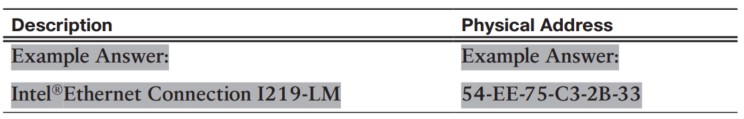
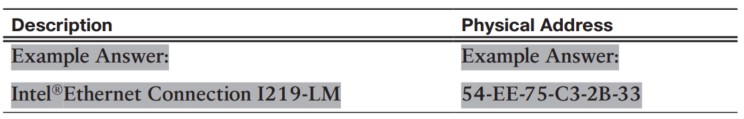
1. Enter the **ipconfig /all** command at the command prompt.

**Step 2:** Locate the MAC (physical) address(es) in the output from the **ipconfig /all** command.

Use the table below to fill in the description of the Ethernet adapter and the physical (MAC) Address:

Realtek Gaming GbE Family Controller

30-24-A9-86-F2-3E



**Question:** How many MAC addresses did you discover in your PC?

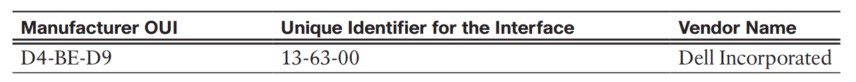
|  |
| --- |
| 5 |

## Part C.2: Analyzing the Parts of a MAC Address

Every Ethernet network interface has a physical address assigned to it when it is manufactured. These addresses are 48 bits (6 bytes) long and are written in hexadecimal notation. MAC addresses are made up of two parts. One part of the MAC address, the first 3 bytes, represents the vendor who manufactured the network interface. This part of the MAC is called the OUI (Organizationally Unique Identifier). Each vendor who wants to make and sell Ethernet network interfaces must register with the IEEE in order to be assigned an OUI.

The second part of the address, the remaining 3 bytes, are the unique ID for the interface. All MAC addresses that begin with the same OUI must have unique values in the last 3 bytes.

In this example, the physical MAC address for the Ethernet LAN interface is D4-BE-D9-13-63-00.



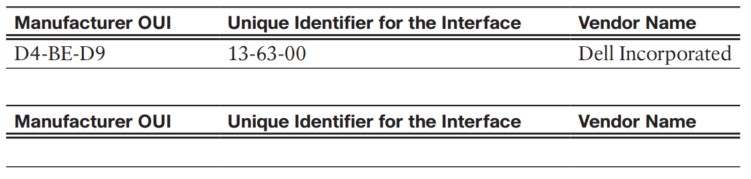
**Step 1:** List MAC addresses discovered by you and your classmates in the previous part.

List the 3-byte Manufacturer OUI and the 3-byte unique interface identifier. You will fill in the Vendor name in the table below.

4C-F4-C3

Intel Corporate

78-2B-46



**Step 2:** Look up the vendors who are the registered owners of the OUIs that you listed in the table.

1. Wireshark.org provides an easy-to-use lookup tool a[t https://www.wireshark.org/tools/ouilookup.html.](https://www.wireshark.org/tools/oui-lookup.html) Use this tool or use the Internet to search for other ways to identify an OUI.

1. Use the information that you found to update the vendor column in the chart in Step 1.

**Question:** How many different vendors did you discover?

|  |
| --- |
| 2 |

## Reflection

1. Why might a computer have more than one MAC address?

|  |
| --- |
| A computer can have multiple NIC which are for ethernet and wireless. |

1. The sample output from the **ipconfig /all** command shown previously had only one MAC address. Suppose the output was from a computer that also had wireless Ethernet capability. How might the output change?

|  |
| --- |
| The screen will show information of all NIC enabled on the computer |

1. Try connecting and disconnecting the network cable(s) to your network adapter(s) and use the **ipconfig /all** command again. What changes do you see? Does the MAC address still display? Will the MAC address ever change?

|  |
| --- |
| Although the IP address may change, the MAC address will not change. |

1. What are other names for the MAC address?

|  |
| --- |
| MAC address is also known as hardware address, ethernet address, or burned-in address (BIA) |