Packet Tracer - Physical Layer Exploration - Physical Mode

Objectives

- Examine Local IP Addressing Information
- Trace the Path Between Source and Destination

Background / Scenario

In this Packet Tracer Physical Mode (PTPM) activity, you will trace the physical path of IP packets from a home in Monterey, California to a web server at the University of Hawaii on the island of Oahu, Hawaii. You will do this in Packet Tracer and on your computer.

In the Packet Tracer simulation, a student lives in Monterey, California (USA) and regularly uses a web browser to access the University of Hawaii's web site at www.hawaii.edu. As she views the information downloaded from the web server to her home computer, she becomes curious about how the IP packets traveled between Monterey and Hawaii. What is the path those packets actually take and how did they travel over the Pacific Ocean?

You are also interested in these questions and will investigate the path from your unique location to the server in Hawaii.

This activity follows the packets between two devices in two specific locations using their specific internet connections. Two other devices in both these same two locations, but using different internet connections (different ISPs), would most likely result in the IP packets taking a much different path.

This activity is only one example of how a variety of internet and network service providers interconnect to create a path between two devices that are communicating using the internet. There are many different possibilities of what path the packets may take depending on the following:

- The location of the client computer
- The client's ISP
- The location of the server computer
- The server's ISP
- How the various ISPs and other entities interconnect to form a path between the client and the server

In this activity, you will begin to get an understanding of some of the various entities and organizations involved in making sure IP packets travel successfully between two devices on the internet. You will see how packets between your home computer, known as a client computer, travel to a web server.

Note: This activity was created by following an actual connection between a home computer in Monterey, California, USA to a web server at the University of Hawaii, Honolulu, Hawaii, USA. The terms and devices referred to in this lab may differ from your connection depending on your location and the service providers involved. In addition, the information used in this activity is subject to change depending on the service providers. Some of the information has been simplified to make the information more understandable. Furthermore, all the information in this activity was discovered by the authors using common web research tools. None of the organizations mentioned in this activity were contacted to verify the accuracy. Finally, the IP addressing scheme has been altered to avoid using public IP addresses.

Requirements

- A PC with Packet Tracer installed and a connection to the internet. Using a mobile device for this activity is not recommended.

Instructions

Part 1: Examine Local IP Addressing Information

In this part, you will examine the IP addressing information in your home network.

Step 1: What is my IPv4 address?

Your IP address is used to identify your computer when sending and receiving packets, similar to how your home address is used to send and receive mail. You can use the **ipconfig** command on Windows and the **ifconfig** command on macOS and Linux.

Note: This activity opens inside the **Home Network**. If you explored other locations, navigate back to the **Home Network**.

a. Click the **Home PC** sitting on the desk, and then click **Desktop** tab > **Command Prompt**.

b. Enter the **ipconfig** command and examine the IPv4 addressing information for **Home PC**

```
C:\> ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::240:BFF:FEA6:4D5A
IPv6 Address.....: ::
   IPv4 Address.....: 192.168.0.75
   Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                                  192.168.0.1

<output omitted>

C:\>
```

The IPv4 address is 192.168.0.75, which is known as a **private IPv4 address**. Most client computers and other devices use a private IPv4 address. These are devices that do not require another device to access it from the internet. Private IPv4 addresses are used to conserve the limited number of globally routable **public IPv4 addresses**.

c. Repeat this step on your own device. What is the IPv4 address and default gateway for your device?

Step 2: What is the IPv4 address for my router?

This same Windows **ipconfig** command shows the IPv4 address of your local or home router, also known as the **default gateway**. Notice that our local router has the IPv4 address of 192.168.0.1.

This is the router that connects your local home network to your internet service provider's network and gives you access to the internet.

Note: You can use the **route -n get default** command to determine the default gateway on a computer using the MacOS or Linux operating system.

What is the IPv4 address for your router?

Step 3: What is my public IPv4 address?

Private IPv4 addresses are not routable on the internet. When IP packets leave your network, they need to have their private IPv4 address replaced with a public IPv4 address. The public IPv4 address is used by servers or any other destination to send packets back to your client computer.

Where does this translation between private and public IPv4 addresses occur? Your local router does this translation or you.

How can you find out the public address that your local router substitutes for your private IPv4 address?

a. On your device, search the internet for "what is my ip". Some search engines will tell you your public IPv4 address without the need to visit another website. In addition, several web sites will be listed which will provide this and other information.

   Note: Many ISPs have begun to use IPv6 addresses. Private addresses are only necessary to conserve the limited number of public IPv4 addresses. Using two different addresses and translating between them, is not required for IPv6.

b. In Packet Tracer, close the **Command Window**, and then click **Web Browser**.

c. In the **URL** field, type **www.tellmemyip.com** and then click **Go**.

   Note: This website is fictious and currently only exists in Packet Tracer.

   In addition to the public IPv4 address, notice that the web site we used provided other information including the name of our ISP and geographical location. The ISP information is usually very reliable. However, the geographical information (city, state, and country) and geolocation (latitude and longitude) is not always completely accurate. Notice that the web site we used shows the city as Pacific Grove, about 5 miles from our home location in Monterey. This information is typically a region that the ISP has used for all customers in that area.

d. On your device, use one of the "what is my ip" websites you found in your search. List your public IPv4 address, location, and ISP.

Step 4: Examine the connections in your network.

a. What does the connection look like between your device and your router? Is it wired or wireless?

b. Where is the router that your device uses to access the internet?

c. What does the connection look like between your router and the internet? Does it use a cable from the cable company or the phone company? Is it wireless? Can you find the cable as it leaves your house or see the remote tower if it is a wireless connection?

d. Search YouTube for "Tour of Home Network 2020 8-bit guy". This is not your average home network but you may recognize many of the same devices found in your own home network.

Part 2: Trace the Path Between Source and Destination

In this part, you will use the **traceroute** command that is used for network diagnostics and for displaying the path packets take to a destination. It gathers information about every hop from your device to the destination. Each line in the output designates the IP address of a router, used to forward packets from one network to another network. These are known as "hops". In Windows, the command is **tracert**, whereas the macOS and

Linux operating systems use the **traceroute** command. In Packet Tracer, you use the Windows **tracert** command. The hops are simulated. However, they adhere closely to the actual path that the data would take between a device in Monterey, California, and the web server at the University of Hawaii in Honolulu.

Note: During this part, you will be investigating the output for two traceroutes. One will be from the Home PC inside Packet Tracer. The other will be from your own personal device.

Step 1: Use traceroute to display the path from Monterey to Hawaii.

a. In Packet Tracer, on the **Home PC**, close the **Web Browser** window if it is still open. From the **Desktop** tab, click **Command Prompt**.

b. Enter the **tracert www.hawaii.edu** command. Packet Tracer will take some time to resolve the domain name **hawaii.edu** to the IPv4 address. You can click **Fast Forward Time** (Alt+D) to speed up the process.

c. On your laptop or other computer, open a terminal window and enter the traceroute command for your operating system. Your output will be different from the output below and the output in Packet Tracer. Your output will most likely show the names of real routers and public IPv4 addresses. Unless you live close to Monterey, California, you will likely have very different router names, IPv4 addresses, and number of hops.

Note: In the output below, the real IPv4 addresses have been converted to private IPv4 addresses.

```
C:\> tracert www.hawaii.edu

Tracing route to web00.its.hawaii.edu [172.31.149.56] over
a maximum of 30 hops:

1     3 ms     4 ms     3 ms  10.0.0.1
2     13 ms    16 ms    11 ms  10.120.89.61
3     44 ms    18 ms    18 ms  po-302-1222-rur02.monterey.ca.sfba.comcast.net
      [10.110.178.133]
4     13 ms    14 ms    13 ms  po-2-rur01.monterey.ca.sfba.comcast.net
      [10.139.198.129]
5     21 ms    17 ms    15 ms  be-222-rar01.santaclara.ca.sfba.comcast.net
      [10.151.78.177]
6     16 ms    20 ms    19 ms  be-39931-cs03.sunnyvale.ca.ibone.comcast.net
      [10.110.41.121]
7     27 ms    14 ms    20 ms  be-1312-cr12.sunnyvale.ca.ibone.comcast.net
      [10.110.46.30]
8     24 ms    19 ms    23 ms  be-303-cr01.9greatoaks.ca.ibone.comcast.net
      [10.110.37.178]
9     19 ms    21 ms    17 ms  be-2211-pe11.9greatoaks.ca.ibone.comcast.net
      [10.110.32.246]
10    16 ms    23 ms    16 ms  ae-3.2011.rtsw.sunn.net.internet2.edu [172.16.69.141]
11    24 ms    24 ms    23 ms  et-2-3-0.3457.rtsw.losa.net.internet2.edu
      [172.16.20.255]
12    85 ms    87 ms    85 ms  172.16.47.134
13    87 ms    85 ms    85 ms  xe-1-1-0-54-kolanut-re0.uhnet.net [172.30.205.29]
14    87 ms    86 ms    87 ms  vl-669-10gigcolol3.uhnet.net [172.30.213.2]    15     *
      *        *     Request timed out.
 16     *        *        *     Request timed out.
^C

C:\>
```

d. When the output begins to time out, as for the 15th and 16th hop in the above output, enter **Ctrl+C** to end the traceroute. Otherwise, it will continue until the maximum of 30 hops is reached. The traceroute begins to timeout in this example because the router at the end of the path is most likely configured to not reply to traceroute requests.

The first highlighted entry in the example shows the first hop as 1.

e. Look closely at the first line of output. The three numbers preceding the IP address are timestamp values, such as 3ms, 4ms, 5ms, for the first hop. This is the roundtrip time between the source device and the router at that IPv4 address, in milliseconds. The traceroute also includes the IP address of the router interface that received the packet from the source of the traceroute, the client computer. The highlighted entry in the example shows that the first router has an IPv4 address of 10.0.0.1.

Some hops may also include domain name information used by the service provider to help document information about the router, such as **po-302-1222-rur02.monterey.ca.sfba.comcast.net** highlighted in the output.

Although the output timed out before reaching the server at hawaii.edu, the prior hops provide enough information to trace the path of our packets.

f. On your device, try tracing the route to other websites such as www.netacad.com or www.google.com. Some hops will probably timeout. Some web servers may not respond to traceroute.

Step 2: Investigate the second hop in the traceroute output.

The traceroute shows a second hop of:

```
2    13 ms    16 ms    11 ms  10.120.89.61
```

The IP packets now leave the home network and are sent to the ISP.

The 10.120.89.61 is the IPv4 address of the first router outside the local home network. This router belongs to the ISP. This router is known as the ISP's **point of presence** or **POP**. This is where the ISP provides its customers access to the internet.

The physical connection between the end user and the POP is known as the **local loop**, or is sometimes referred to as the "last mile".

Traditionally, the local loop was the telephone lines from a customer's premises to local telephone exchange, sometimes referred to as the Central Office (CO). The copper, twisted pair cables were used to carry analog voice and signaling information.

Today, the local loop may also include cables to carry digital information, which may be wired or wireless. In terms of internet connectivity, the local loop connects the customer's premises to the ISP POP.

The local loop may be one of several different types of connections, including:

- Cable connection, typically using the same coaxial cable used for TV and phone
- DSL (Digital Subscriber Line) using same telephone line for phone and TV
- Wireless signals or Wireless local loop (WLL), including cellular technologies
- Satellite connection, typically the same beamed signal as used for TV
- Fiber-optic cable
- Dial-up access telephone line using same twisted-pair copper cable used for phone

a. In Packet Tracer, notice that the **Home PC** on the desk is connected to the Home Router on the shelf behind the desk. However, the **Home Router** is not connected directly to the router at the next hop. Instead, it is connected to a cable modem. This cable modem is not a router. Therefore, it is not reported as a hop in the traceroute output.

b. Navigate to **Monterey**. Notice that the next hop is physically linked to the **Comcast POP** building. Click **Comcast POP**. A POP is physically located in a data center. A data center is a physical facility that

organizations use to house their critical equipment, applications, and data. The key components of a data center design include routers, switches, firewalls, storage systems, and servers. Although the **Comcast POP** would typically be a data center in the real world, in Packet Tracer it is only storing the equipment necessary for this activity. In the **Rack**, you will see several devices including a device simulating a cable modem termination system (CMTS), the Comcast-POP-Monterey router, a multilayer switch, and two servers.

c. Investigate the physical connections between the devices. One interface of the **Comcast-CMTS** is linked directly to the **Cable Modem** in the **Home Network**. The other interface is connected to the next hop router, **Comcast-POP-Monterey**, which is racked directly below it. The **Comcast-POP-Monterey** second interface links out to the next hop, which you will investigate in the next step. The third interface is connected to the switch, which is then connected to the two servers. The **DNS Server** is translating **www.hawaii.edu** and **www.tellmemyip.com** to their respective IPv4 address. The **Web Server** is serving the website **www.tellmemyip.com**.

d. In your own network, what is the technology for the local loop you are using? Cable? DSL? Satellite? Cellular? If it is a wired connection, see if you can find the cable leaving your home network. Where does it go? To a telephone pole? Underground?

e. The second hop in your traceroute command on your device is typically your ISP's POP. What is the IP address for your ISP's POP?

Step 3: Attempt to discover the physical location of the IP address for your ISP POP.

Who owns the POP for the second router in your traceroute output? You can search the internet for "ip lookup", which will result in a list of web sites that will give you information about an IP address.

Fill in the table below with the information you discovered from your IP lookup research. You may need to visit several different lookup websites to get all the information.

2nd Hop IPv4 address:	
ISP:	
City:	
Region:	
Country:	

The information regarding the name of the ISP is usually very reliable. However, the physical location information may not be accurate. In many cases, the physical location listed may be hundreds of miles from where the router and the datacenter are actually located. It could be the ISP's administrative office or even a random location.

Because the geolocation information (longitude and latitude) registered by the ISP is seldom accurate, you cannot rely on this information to find the actual location of the POP.

In this case, you would need to contact your ISP to see if they will tell you where this POP is located.

Step 4: Investigate why geolocation information is not always accurate.

Search the internet for "600 million IP addresses Kansas". You will find several articles about an ISP that chose to use a geolocation (latitude and longitude) at the center of the United States to register over 600

million of its IP addresses. Unfortunately, this particular latitude and longitude happened to be a private home in the middle of Kansas and not an ISP.

Anyone with complaints about the ISP, their internet connection, or receiving spam from one of these IP addresses would contact the homeowners. You can imagine the difficulties that ensued for both the people calling the home and especially the Kansas homeowners.

Be skeptical of any geolocation information that shows packets going from one location, to hundreds or thousands of miles away, then back again. For example, packets are not normally forwarded from California to Kansas and back to California.

Step 5: Investigate the local ISP network.

For the example of real traceroute output shown below, hops 2 through 9 all belong to Comcast. Recall that the real IPv4 addresses for these routers have been modified for this activity. Therefore, you cannot use them to do an IP lookup. However, you can look up the IP addresses for your own traceroute output to determine how many of hops belong to your ISP.

```
C:\> tracert www.hawaii.edu

Tracing route to web00.its.hawaii.edu [172.31.149.56] over
a maximum of 30 hops:

1     3 ms     4 ms     3 ms  10.0.0.1
2     13 ms    16 ms    11 ms  10.120.89.61
3     44 ms    18 ms    18 ms  po-302-1222-rur02.monterey.ca.sfba.comcast.net
      [10.110.178.133]
4     13 ms    14 ms    13 ms  po-2-rur01.monterey.ca.sfba.comcast.net
      [10.139.198.129]
5     21 ms    17 ms    15 ms  be-222-rar01.santaclara.ca.sfba.comcast.net
      [10.151.78.177]
6     16 ms    20 ms    19 ms  be-39931-cs03.sunnyvale.ca.ibone.comcast.net
      [10.110.41.121]
7     27 ms    14 ms    20 ms  be-1312-cr12.sunnyvale.ca.ibone.comcast.net
      [10.110.46.30]
8     24 ms    19 ms    23 ms  be-303-cr01.9greatoaks.ca.ibone.comcast.net
      [10.110.37.178]
9     19 ms    21 ms    17 ms  be-2211-pe11.9greatoaks.ca.ibone.comcast.net
      [10.110.32.246]
10    16 ms    23 ms    16 ms  ae-3.2011.rtsw.sunn.net.internet2.edu [172.16.69.141]
11    24 ms    24 ms    23 ms  et-2-3-0.3457.rtsw.losa.net.internet2.edu
      [172.16.20.255]
12    85 ms    87 ms    85 ms  172.16.47.134
13    87 ms    85 ms    85 ms  xe-1-1-0-54-kolanut-re0.uhnet.net [172.30.205.29]
14    87 ms    86 ms    87 ms  vl-669-10gigcolol3.uhnet.net [172.30.213.2]    15     *
      *        *     Request timed out.
 16     *        *        *     Request timed out.
^C

C:\>
```

a. In Packet Tracer, navigate to **Monterey**, and then click the **monterey.ca** building.

b. Notice that the two routers in the rack belong to **comcast.net**. You can hover your mouse over each router to see the IPv4 addresses. You can also click each router and investigate IPv4 addressing on the **Config** tab.

c. What is the IPv4 address of the 3rd hop in the Packet Tracer traceroute output?

10.110.178.133

d. Which router and interface in the **monterey.ca** building is configured with this IPv4 address?

rur02.monterey.ca.sfba.comcast.net; GigabitEthernet0/0

e. What is the IPv4 address of the 4th hop in the Packet Tracer traceroute output?

10.139.198.129

f. Which router and interface in the **monterey.ca** building is configured with this IPv4 address?

rur01.monterey.ca.sfba.comcast.net; GigabitEthernet0/0

g. Why do you think the IP addresses for the other interfaces are not shown in the traceroute output?

Those interfaces are the source for the packets that are sent to the next hop destination. Source IP addresses are not shown in traceroute output

h. List the hops in your own traceroute output that belong to your local ISP.

Step 6: Investigate the domain names in the output to discover more clues about the location of routers at each hop.

The domain name (if there is one) in the traceroute may provide additional information. There is no standard naming convention. If and how it is used is solely up to the discretion of the administrator of the device. In traceroute output above, Comcast has provided information in the domain name that gives you a clue about where the router may actually be located:

- po-302-1222-rur02.monterey.ca.sfba.comcast.net
- po-2-rur01.monterey.ca.sfba.comcast.net
- be-222-rar01.santaclara.ca.sfba.comcast.net
- be-39931-cs03.sunnyvale.ca.ibone.comcast.net
- be-1312-cr12.sunnyvale.ca.ibone.comcast.net
- be-303-cr01.9greatoaks.ca.ibone.comcast.net
- be-2211-pe11.9greatoaks.ca.ibone.comcast.net

All of these cities are located with the same geographical region known as the San Francisco Bay Area (sfba) and are controlled by Comcast.

- Monterey, California
- Santa Clara, California
- Sunnyvale, California
- San Jose, California (9greatoaks.ca)

We have made the assumption in Packet Tracer that all routers with the same city in the domain name are in the same data center. For example, as you have seen, these two routers are in the **monterey.ca** building:

- po-302-1222-rur02.monterey.ca.sfba.comcast.net
- po-2-rur01.monterey.ca.sfba.comcast.net

a. What information, if any, can you decipher from the domain names for your local ISP?

b. In Packet Tracer, navigate to **Monterey**. Notice the northbound link exiting **monterey.ca**.

c. Navigate up one level to **Intercity**. (Packet Tracer does not allow the renaming of **Intercity**.) You will see a representation of the physical links between the home in **Monterey** and Oahu island where the server for the University of Hawaii is located in **Honolulu**. Notice that the link first goes from **Monterey** to **San Jose**, and then **Los Angeles** before it crosses the Pacific Ocean to **Honolulu**.

d. Click **San Jose**. Notice there are three buildings, each labeled with a part of the domain name discovered in the traceroute output. Routers with the same domain name are located in the same building. Investigate each building, router, and interface to complete the following table.

Hop	Domain Name	Interface	IPv4 Address
5	santaclara.ca.sfba.comcast.net	GigabitEthenet0/0	10.151.78.177
6	sunnyvale.ca.ibone.comcast.net	GigabitEthenet0/0	10.110.41.121
7	sunnyvale.ca.ibone.comcast.net	GigabitEthenet0/0	10.110.46.30
8	9greatoaks.ca.ibone.comcast.net	GigabitEthenet0/0	10.110.37.178
9	9greatoaks.ca.ibone.comcast.net	GigabitEthenet0/0	10.110.32.246

e. What is the building, router, interface, and IPv4 address for the outbound link to Los Angeles?

greatoaks.calibone; pe11.9greatoaks.ca.ibone.comcast.net; GigabitEthernet1/0; and 172.16.69.142

IXP Data Center

An IXP (Internet Exchange Point) is typically a colocation center that houses ISPs and other customers, with the purpose of connecting with one another.

At some point an ISP like Comcast will need to forward the packets to another ISP. This usually occurs in an IXP. The locations are often thought of as being at the "edge" of an ISP's network, meaning a place where packets leave the ISP's internal network and are forwarded to another ISP.

This is a place where ISPs and others can exchange internet traffic between their networks.

IXPs are typically owned and operated by a neutral party, meaning they are not an ISP or "customer" of their own data center.

Note: The term Network Access Point (NAP) is an older term for IXP that has now been deprecated.

Step 7: Investigate the link between Comcast and Internet2.

This last hop within the Comcast ISP network before packets are forwarded to another ISP occurs at hop 9.

```
  9    19 ms    21 ms    17 ms  be-2211-pe11.9greatoaks.ca.ibone.comcast.net
[10.110.32.246]
```

Again, Comcast gives us a clue where the router is located. However, the domain name is not indicating a city, but an address.

a. Search the internet for "9 great oaks California" and you will find that an Equinix data center is located at 9 Great Oaks Boulevard in San Jose, California. If you then use Google Maps and search for that address, you can use the satellite view or street view to see the actual building.

Equinix is an Internet Exchange Point (IXP) known as Equinix SV5. It provides connections between different ISPs and is hosting the connection between Comcast and the next ISP, which is Internet2.

b. There are many web sites that provide information about large IXP data centers including the ISPs they host. Search the internet for "Inflect data center". Use the website to explore and see if you can find where they list Comcast as one of the organizations hosted at Equinix SV5.

c. In Packet Tracer, navigate to **San Jose**, if necessary, and then click the **9greatoaks.ca** building. Notice the name of the third router in the rack indicates that it belongs to Internet2. This router is the 10th hop in the traceroute output.

```
10    16 ms    23 ms    16 ms  ae-3.2011.rtsw.sunn.net.internet2.edu [172.16.69.141]
```

d. What is the interface for the 10th hop?

GigabitEthernet0/0

Step 8: Investigate Internet2.

Internet2? Is this a new version of the internet? No. Internet2 is a non-for-profit ISP. It is a consortium of research, education, industry, and government communities that provide high-speed network services, cloud services, and other services tailored for research and education.

Search for the Wikipedia information and other web sites to get more information about Internet2. What speed is the Internet backbone that provides connections between its members?

As of the writing of this lab, this answer can be found on Wikipedia under the Objectives section: Internet2 provides…a 100 Gbit/s network backbone to more than 210 U.S. educational institutions, 70 corporations and 45 non-profit and government agencies.

For fun, search for "This Man Launched a New Internet Service Provider from His Garage". It is the story about Brandt Kuykendall, a resident of the small town of Dillon Beach, California. The internet service in his town was too slow and expensive, so he started his own ISP from his garage.

Step 9: Investigate the link to Los Angeles.

Our traceroute reveals that the next hop is another Internet2 router. Luckily, the domain name provides us with this information.

```
11    24 ms    24 ms    23 ms  et-2-3-0.3457.rtsw.losa.net.internet2.edu
[172.16.20.255]
```

A search of "internet2 router proxy" may help you verify that the "losa" in the domain name indicates that this Internet2 router is in **Los A**ngeles, California. IP packets have left the San Francisco Bay Area ("sfba") are traveling south approximately 350 miles to Los Angeles, California.

a. In Packet Tracer, navigate to the **Intercity** level, and then click **Los Angles**.

b. The **losa.net.internet2.edu** building is located somewhere in Los Angeles County. Click the building to enter it.

c. The rack has one router, which is connect to the San Francisco Bay Area and a submarine cable that crosses the Pacific Ocean. What is the interface used for this 11th hop in the traceroute output?

GigabitEthernet0/0

Step 10: Investigate the link across the Pacific Ocean.

The next hop in our traceroute is:

```
12    85 ms    87 ms    85 ms  172.16.47.134
```

Although there is no domain name information provided, there are two pieces of interesting information here.

Although you can't use the IP address for this example as it has been converted to a private IP address, you can use an "IP lookup" web site to determine who owns the IP address for your result. In the example here, the authors were able to determine that the IP address for hop 12 also belongs to Internet2.

Even more interesting is when we look at the roundtrip times of 85 ms, 87 ms, and 85 ms. Notice that there is a large increase in the time compared to the previous hop from San Jose to Los Angeles (24 ms, 24 ms, 23 ms respectively).

Why do we see smaller incremental increases from hops 1 to 11, and then a such a big jump to in the roundtrip time at hop 12?

We can deduce that this router at hop 12 must be much further away than the previous router at hop 11 in Los Angeles, California. We also notice that there are no other places in our traceroute that show such a large difference in times as there is between hop 11 in California and hop 12.

Therefore, these packets must have traveled a much longer distance than any other two points in along the path from Monterey to Hawaii. The router at hop 12 must be in Hawaii where packets traveled almost 2,500 miles from California.

This router is at the Internet2 Peer Exchange (IP2X) in Hawaii and is the last hop within the Internet2 network. IP2X forwards packets to the next hop router belonging to the University of Hawaii.

Note: Students should be able to find answers for these questions at submarinecable.com.

a. Search the internet for "submarine cable map" and see if you can locate any submarine cables that have a landing point both in Hermosa Beach and Hawaii. How many submarine cables terminate at Hermosa Beach?

At the time this activity was written, 3 submarine cables terminated at Hermosa Beach: Hong Kong-Americas (HKA), JUPITER, and SEA-US

b. What is the name of the submarine cable that runs from Hermosa Beach to Hawaii?

SEA-US

c. What is the name of the landing point in Hawaii?

Makaha

d. How many submarine cables terminate at this landing point in Hawaii?

At the time this activity was written, 4 submarine cables terminated at Makaha: HIFN (Hawaii Island Fibre Network), Japan-U.S. Cable Network (JUS), Paniolo Cable Network, and SEA-US.

e. The SEA-US cable was done through partnership between the University of Hawaii and RAM Telecom International, Inc. (RTI). This partnership allows the University of Hawaii System to connect Hawaii to the continental United States, Guam, and beyond.

Search for "Underwater cable speeds UH connections across Pacific" to find an article and video about this cable being laid across the Pacific Ocean.

f. For more information, search YouTube or other video sites for "submarine cable." You will find many videos showing how these cables are constructed and laid across the sea-bed.

g. In Packet Tracer, navigate to the **Intercity** level. Follow the cable across the Pacific Ocean. Two repeaters are shown here although there would be more dozens more. Search the internet to find how many kilometers separate each repeater on a submarine cable.

Answer will vary. But students should be able to find a reasonable answer between 70 and 100 km by searching for "how many signal repeaters on a submarine cable."

h. Click **Honolulu**. You are now on the island of Oahu. Notice that the submarine cable terminates at Makaha.

i. Click the **i2px-Hawaii** building. In the rack are two routers. The first one belongs to I2PX and represents the 12th hop in the traceroute output. What interface is assigned to the 12th hop?

GigabitEthernet0/0

Step 11: Investigate the link between Internet2 and the University of Hawaii network.

The next hop in our traceroute is:

```
13     87 ms     85 ms     85 ms  xe-1-1-0-54-kolanut-re0.uhnet.net [205.166.205.29]
```

The domain name for this router indicates that it is part of the University of Hawaii network (uhnet.net). This router is located at the Honolulu Internet Exchange (HIX) in Honolulu, Hawaii, most likely located within the same IXP as the i2px.hawaii router.

In Packet Tracer, notice that the second router in **i2px-Hawaii** rack is **kolanut-re0.uhnet.net** router. What interface is assigned to the 13th hop?

GigabitEthernet0/0

Step 12: Investigate the last known IP address in the traceroute output.

In Packet Tracer, all the hops are simulated. Navigate back to **Honolulu** and investigate the **uhnet.net** building and the **hawaii.edu** campus. In each building, you will find the devices that simulate the rest of the traceroute path in Packet Tracer.

In real world traceroute output, the hops begin to timeout. For the example in this activity, it times out at hop 15. It most likely times out for you at a different hop.

```
C:\> tracert www.hawaii.edu

Tracing route to web00.its.hawaii.edu [172.31.149.56] over
a maximum of 30 hops:

<output omitted>

 14    87 ms     86 ms     87 ms  vl-669-10gigcolol3.uhnet.net [172.30.213.2]
15     *         *         *      Request timed out.
 16     *         *         *      Request timed out. ^C
```

For hop 14, the name implies that this is another router that is part of the University of Hawaii network. At this point, the traceroute begins to timeout.

It is common for routers and other devices such as a web server not to respond to traceroute messages. A router may even be configured to deny any traceroute messages being forwarded on to the next hop router. Most likely a University of Hawaii router or firewall, prior to the web server, is blocking any further traceroutes messages from entering the network.

However, you have tracked the path of these packets from Monterey, California all the way to the University of Hawaii in Honolulu.

Conclusion and Some Things to Consider

We saw that from tracking the hops in our traceroute that our packets went through three different groups of networks:

- Comcast ISP
- Internet2 ISP
- University of Hawaii Network

```
Comcast ISP
1      3 ms      4 ms      3 ms  10.0.0.1
2      13 ms     16 ms     11 ms  10.120.89.61
3      44 ms     18 ms     18 ms  po-302-1222-rur02.monterey.ca.sfba.comcast.net
       [10.110.178.133]
4      13 ms     14 ms     13 ms  po-2-rur01.monterey.ca.sfba.comcast.net
       [10.139.198.129]
```

```
5     21 ms    17 ms    15 ms  be-222-rar01.santaclara.ca.sfba.comcast.net
      [10.151.78.177]
6     16 ms    20 ms    19 ms  be-39931-cs03.sunnyvale.ca.ibone.comcast.net
      [10.110.41.121]
7     27 ms    14 ms    20 ms  be-1312-cr12.sunnyvale.ca.ibone.comcast.net
      [10.110.46.30]
8     24 ms    19 ms    23 ms  be-303-cr01.9greatoaks.ca.ibone.comcast.net
      [10.110.37.178]
9     19 ms    21 ms    17 ms  be-2211-pe11.9greatoaks.ca.ibone.comcast.net
[10.110.32.246]
Internet2 ISP
10    16 ms    23 ms    16 ms  ae-3.2011.rtsw.sunn.net.internet2.edu [172.16.69.141]
11    24 ms    24 ms    23 ms  et-2-3-0.3457.rtsw.losa.net.internet2.edu
      [172.16.20.255]
12    85 ms    87 ms    85 ms  172.16.47.134
University of Hawaii
13    87 ms    85 ms    85 ms  xe-1-1-0-54-kolanut-re0.uhnet.net [172.30.205.29]
14    87 ms    86 ms    87 ms  vl-669-10gigcolol3.uhnet.net [172.30.213.2]    15
      *        *        *     Request timed out.
 16     *        *        *     Request timed out.
^C

C:\>
```

Comcast, Internet2, and the University of Hawaii are each known as an **autonomous system (AS)**. The internet is an interconnection of hundreds of ASs throughout the world. On the internet, packets are forwarded between ASs.

An AS is typically an ISP such as Comcast, a telecommunications provider such as Internet2, a content provider such as NetFlix, a company such as Cisco Systems, or educational institution such as the University of Hawaii.

The packets from the Home Network in Monterey, California to the University of Hawaii were forwarded from Comcast ISP to Internet2 ISP and eventually the University of Hawaii. Within each of these ASs, the packets were forwarded by multiple routers belonging to each AS.

Bonus: Did you try switching to Logical mode? This mode was left unlocked so that the curious student might find delight in discovering what the physical representation of the traceroute in this activity might look like as a logical topology. Enjoy!