**CPE464 Lab 7 – Traceroute, Internet Standards, UDP**

**What to turn in:**

Both the lab writeup and the programming (UDP code with sendtoErr()) are due by **Friday at 11:59 pm.**

Work as a group on this lab in the order given below. Do not work on the UDP code until the early parts of the lab are complete.

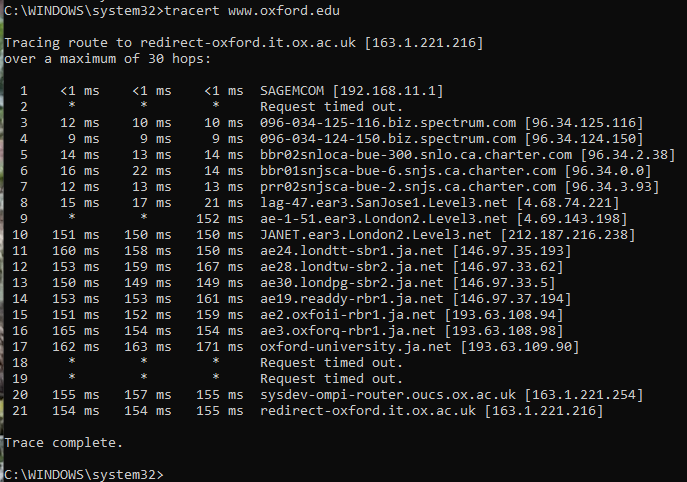
1. Turn in a PDF of the answers to this lab on Canvas
2. See udpClient/udpServer at the end of this lab for what is needed.

**Purpose of this lab:**

* Understand how traceroute works and how this is tied to the IP header
* Take a look at some of the standards bodies that make up the Internet
* Gain experience with UDP and integrating the sendtoErr() library into your code

1. **Introductions**
2. **Traceroute Packet analysis:**

First, you are going to look at a packet trace I captured in my office that shows a traceroute between my office computer and [www.oxford.com](http://www.oxford.com). The packet trace file is called TraceRT\_Oxford.pcapng.

1. Download this file and open the file in Wireshark.
2. The **output** from the traceroute to www.oxford.edu is shown here:
3. Going back to last week’s lab regarding subnets, in my office **what device has the IP address 192.168.11.1?** Note- if you look at the traceroute output, this is the first router in the path discovered by traceroute.
4. Looking at both the packet trace in the TraceRt\_Oxford file and the output from traceroute:

The pcap file contains the traceroute packets. Most other packets where removed from this file. Remember, traceroute is **probing** the network **hop by hop** to determine the routers between the source and destination computers.

* 1. Looking at the pcap file, what protocol is used by traceroute for sending packets?

ICMP

* 1. What would cause packet 1 to generate the error: Time-to-live exceeded that is shown in packet 2? Or packet 24 with TTL error in 25. Explain.

Packet 1 has a TTL of 1, so if it had just stopped at one extra router, the TTL would have expired and the error would have been generated. Packet 24 had a TTL of 5, so if it had stopped at 5 extra routers on its trip, it would have expired and generated an error as well.

* 1. Looking at the **output** from the traceroute (**above**), how many attempts does traceroute use to probe for each hop in the path (e.g. how many round trip times (RTT) in milliseconds are printed in each row, note - row 1 shows the name/IP of the router 1-hop away, row 2 show the name/IP of the router 2-hops away, row 3…)?

Traceroute attempts to probe each hop 3 times. (It’s the three columns in the traceroute printout.)

* 1. Looking at the pcap file, how many ICMP requests are sent with a time-to-live of 3? 4? 5?

TTL=3: 3

TTL=4: 3

TTL=5: 3

* 1. How does traceroute work - Explain how traceroute is probing the network for each router and getting an RTT for each hop.

Traceroute pings (in 3 ping bursts) to the desired destination starting with a TTL of 1 and incrementing it after each burst. Each router in the route should send back a TTL expired ICMP packet (unless it is configured not to). Traceroute times the response and gets the IP address of the each router from the TTL expired packet then looks up the owner of the IP to produce its output.

* 1. For most of the pcap packet trace you see an Echo Request and then Time-to-live exceeded pair. Packets 7, 8 and 9 do have any Time-to-live exceeded paired with them. Looking at the output from traceroute and these packets, can you explain what happened?

Note – the same thing happened to packets 46, 47 and 98 through 103.

There are no TTL exceeded pairs on packets intended for a router that is not configured return a ICMP when it receives a TTL exceeded or just does not respond. These non-paired packets correspond with requests that time out on the traceroute printout.

1. **Internet Standards**
2. **IP address questions:**
   1. Looking at the IANA site: <https://www.iana.org/numbers>:
      1. How many Regional Internet Registry’s (RIR) are there?

5

* + 1. What does ARIN stand for and what countries does it cover?

American Registry for Internet Numbers covers Canada, USA, and some Caribbean Islands.

1. Go to link: <https://whois.arin.net/ui/> - Enter the prefix number in the “SEARCH WhoisRWS” box on the upper right.
2. Regarding the IP address **4.182.3.4**
   * + - What organization is this addressed assigned to?

Microsoft Corporation

* + - * What address range do they have?

4.176.0.0 - 4.191.255.255

* + - * What year was this address registered?

1998

* + - * What is their CIDR address with netmask:

4.176.0.0/12

1. Regarding the IP address **129.65.3.4**?
   * + - What organization is this addressed assigned to?

Calpoly

* + - * What address range do they have?

129.65.0.0 - 129.65.255.255

* + - * What year was this address registered?

1987

* + - * What is their CIDR address with netmask:

129.65.0.0/16

* + 1. Regarding Google. Enter google in the SEARCH box
       - Looking at the networks section (2nd section). How many different IPv4 networks does google have? (Note there would need to be one core routing table entry for each IPv4 network.)

34

* + - * How many external IPv6 addresses does Google have?

4

* + - * How many Autonomous Systems does Google manage?

5

1. **RFC Questions:**

Now that we are working at layer 3 and above we are going to look at some of the internet standards.

1. This questions concerns RFC’s: (See the web page: [www.rfc-editor.org](http://www.rfc-editor.org/))
   1. What are RFC’s? What are they used for?

RFC stands for request for comments. They propose standards for the internet and publish best practices and methods and other information.

* 1. Who can submit an RFC and what is the process?

Anyone can submit an RFC. You publish it as an internet draft then is reviewed by the RFC editor and IESG.

* 1. Give a brief summary of RFC 1541 (date, purpose, and author).

RFC 1541 describes Dynamic Host Configuration Protocol. It was published Oct. 1993 by R. Droms.

1. This question concerns the IETF: (see: [www.ietf.org](http://www.ietf.org/))
   1. What is the IETF? What is its mission?

IETF is a community of network people who make the internet better by building standards for the internet.

* 1. How do you become a member of the IETF?

Anyone can become a member by signing up for the mailing list and attending meetings (for a fee).

* 1. What is the IAB and what is its purpose?

The Internet Architecture Board ensures the internet is trustworthy, supports the technical direction, and promote technical evolution.

* 1. Regarding the *suit* Workgroup (go to How We Work menu item and then Working Groups)
     + What is its full name and what IETF area is it in?

The Software Updates for the Internet of Things is in the security area.

* + - What is its purpose (see charter of this group)?

Its purpose is to update the security of IoT to prevent vulnerabilities.

1. Concerning the IANA (see: [www.iana.org](http://www.iana.org/))
   1. What is IANA an acronym for?

Internet Assigned Numbers Authority

* 1. What role does the IANA perform?

It assigns IP addresses and other internet protocol resources.

* 1. Go to: Protocol Assignments. (Protocol Registries)
     + Describe the purpose of the **Port Numbers** entry**,** what are port numbers (decimal) 22, 23, 53 and 80?

These port numbers are used to distinguish between services that run over transport layer protocols.

22: ssh

53: domain name server

80: http

* + - Describe the purpose of the **Protocol Numbers** entry**,** what are protocol numbers 4, 6, and 17?

Protocol numbers are used in the IP header to indicate what protocol comes next.

4: IPv4

6: TCP

17: UDP

1. **Using Random numbers**

There tends to be a lot of confusion around using random numbers. This part of the lab looks at the random number library.

The sendtoErro() library, which you will use in program #3, uses random numbers to drop packets/flip bits. Some questions on the random library (e.g man rand):

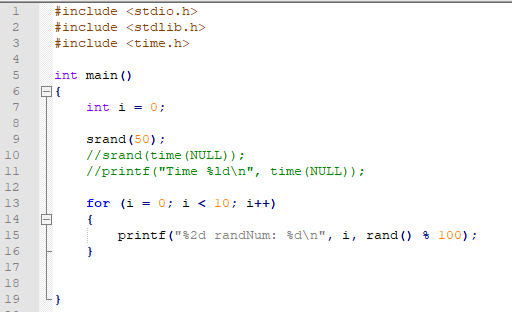
1. What is the purpose of the rand() function?

Rand provides a random integer.

1. What is the purpose of the srand() function?

Srand seeds a new sequence of random numbers for the rand function.

1. Create the following program:



* + - * 1. How does this program limit its range of random number? And what is this range? What would the printf() statement be if I wanted to limit the random number between 0 and 10?

Rand’s range is 0 to RAND\_MAX which is a machine defined constant. This program limits it from 0 to 100 by calling rand() % 100. To limit the random number between 0 to 10 you can call rand() % 10.

* + - * 1. Run the random code program 3 times and compare the output from each run. What does this output show regrading the generation of these random numbers based on the call to srand(50) in line 9.

Each time you run the program the output is the same because srand chooses the seed to be 50 each time. If you change 50 to another number, the output would change.

* + - * 1. Comment out line 9 and uncomment line 10 and 11. Now run the program 3 times. What difference do you see in the output of the program based on how you are calling srand() now versus how it was called before?

The output changes each time you run it now.

* + - * 1. The sendtoErr\_init() function allows you to turn on/off random dropping of packets (using the RSEED\_OFF vs. the RSEED\_ON macro). How do you think these macros are used in the library code? What effect do you think this has on the “random” packet loss pattern your program will experience?

If RSEED\_ON is chosen, the library probably seeds rand with time(null) to make it truly random.

* + - * 1. Side question: The time() function returns what? What is the start date this “epoch” is based on? (Note this date is used in MANY computer systems.)

Time returns the current time in seconds since the epoch (01-01-1970).

* + - 1. **See separate document for the UDP+sendtoErr coding part of this lab**

**Demo and what to turn in:**

1. You need to upload a PDF of the finished lab worksheet (this document) on Canvas by 11:59 pm this Friday.
2. handin (on the unix servers) your working UDP+sendtoErr() code by Friday at 11:59 pm (see UDP lab assignment document on canvas for details).
3. You will demo the UDP+sendtoErr() program in lab.