ITS332 – Quiz 1

Information Technology Lab II, Semester 2, 2010

Prepared by Steven Gordon on 10 December 2010
ITS332Y10S2Q01, Steve/Courses/CSS322/Assessment/Quiz1.tex, r1525

Question 1 [0 marks]

What is the number of your computer (it is on the monitor)?

Question 2 [1 marks]

Consider your Ethernet interface that has Internet connectivity. What is the IPv6 address of the interface? Give both the address and the command you used to find the address.

Answer. *The command to be used is* `ifconfig`*. The* inet6 addr *field gives the IPv6 address.*

Consider your Ethernet interface that has Internet connectivity. What is the hardware address of the interface? Give both the address and the command you used to find the address.

Answer. *The command to be used is* `ifconfig`*. The* HWaddr *field gives the hardware address.*

Question 3 [2 marks]

(a) How many interfaces does your computer have? Describe each of them (e.g. what are the devices that each interface corresponds to, what are they used for).

Answer. *The computers have 4 interfaces (as seen using* `ifconfig`*). Three interfaces are Ethernet cards, and there is one loopback interface for sending to oneself.*

(b) What is the IPv6 address of the interface that has Internet connectivity? What command did you use to find it?

Answer. *The command to be used is* `ifconfig`*. The* inet6 addr *field gives the IPv6 address.*

Question 4 [3 marks]

Use `tcpdump` and Wireshark to capture a DNS protocol exchange. Then answer the following questions:

(a) Draw a captured DNS query packet, labelling the headers with the appropriate protocol, and indicating the size of each header in Bytes.

Answer. *Ethernet (14B) – IP (20B) – UDP (8B) – DNS (32B)*

(b) What is the value, in binary, of the reply code flag in the DNS query response packet?

Answer. *0000*

Use `tcpdump` and Wireshark to capture an ICMP (ping) protocol exchange. Then answer the following questions:

(a) Draw a captured ping request packet, labelling the headers with the appropriate protocol, and indicating the size of each header in Bytes.

Answer. *Ethernet (14B) – IP (20) – ICMP (56 or 64B)*

(b) What is the maximum value, in decimal, of the sequence number field an a ICMP packet?

Answer. $2^{16} - 1$ *(since the field is 2 Bytes or 16 bits in length)*

While using `tcpdump` and Wireshark to capture a DNS protocol exchange, find the IP address for `www.bing.com`. Then answer the following questions:

(a) What is an IP address of the `www.bing.com` server?

Answer. *The output of* `nslookup` *may give multiple addresses, including for example* `58.97.45.42`*.*

(b) Is `www.bing.com` the "real" name of the server? If yes, then how do you know? If no, then what is the "real" name?

Answer. *No. The canonical name is:* `a134.g.akamai.net`

(c) What is the value, in hexadecimal or binary, of the type of answer?

Answer. *In the answer, the type is CNAME. In hexadecimal that is 0005.*

While using `tcpdump` and Wireshark to capture a DNS protocol exchange, find the IP address for `www.yahoo.com`. Then answer the following questions:

(a) What is an IP address of the `www.yahoo.com` server?

Answer. *The output of* `nslookup` *may give multiple addresses, including for example* `72.30.2.43`*.*

(b) What is the port number used by the DNS server?

Answer. *53*

(c) The output of `nslookup` tells you that the answer is non-authoritative. How does you DNS client software know the answer is non-authoritative?

Answer. *In the DNS query response, the Authoritative flag is 0.*

Question 5 [3 marks]

(a) Write a command that will send exactly 3 ICMP echo request messages to the computer `192.168.10.1`.

Answer. `ping -c 3 192.168.10.1`

(b) How many routers between your computer and 192.168.10.1? Explain how you obtained your answer.

Answer. *The output of the* `ping` *command shows a TTL of 61. That means three routers have decreased the TTL, hence 3 routers between the source and destination.*

(a) Write a command that will send exactly 4 ICMP echo request messages, each containing 100 Bytes of data, to 10.10.6.1, with the time between sending the 1st and sending the 4th is 1 second.

Answer. `ping -c 4 -i 0.333 -s 100 10.10.6.1`

(b) What command or program would you use to find the set of routers between your computer and any destination on the Internet?

Answer. *tracepath or traceroute*

Question 6 [2 marks]

(a) What is an IP address of the IBM (`www.ibm.com`) web server?

(b) What is the address of the server that your computer obtained the above answer from?

Answer. *The answers can be obtained from using* ***nslookup****. The results show first the DNS server that returned the answer, such as* `10.10.10.9`*, and then (most likely under* Non-authoritative answer*) the domain name and IP address, e.g.* `129.42.56.216`*.*

(a) What is an IP address of the DynDNS (`www.dyndns.org`) web server?

(b) What is the port number of the server that your computer obtained the above answer from?

Answer. *The answers can be obtained from using* ***nslookup****. The results show first the DNS server that returned the answer, such as* `10.10.10.9`*, and then (most likely under* Non-authoritative answer*) the domain name and IP address, e.g.* `204.13.248.116`*.*

Question 7 [1 marks]

What command/program would you use to find the set of routers between a source and destination in the Internet?

Answer. *`tracepath` or `traceroute`*

What is the exact command you would use to send exactly 5 ICMP packets to computer `10.10.6.11` over a total period of 16 seconds?

Answer. *`ping -c 5 -i 4 10.10.6.11`*