EL4012 Lab 3: Network Layer

Learning Outcomes

1. Explore the Local Network
2. Set up and configure Wireshark
3. Use Wireshark to explore Network layer protocols
4. Use Wireshark filters
5. Capture Ping and ARP packets

## Task 1: Exploring the network

We continue on from last week:

1. Use the ifconfig command to confirm your own IP address
2. Enter the following nmap command to list out all the ‘hosts’ connected to the network:  
     
   nmap -sP X.Y.Z.0/24 //see last week for values of X, Y, Z  
     
   Wait until it completes. It takes a while because it tries every address in the range you have given, and waits for the reply to see if there is anyone home. You should be able to spot and identify your own IP address.
3. Choose one of the IP addresses shown in (2) above. You can use the ‘ping’ command to confirm if the device is still on-line:  
     
   ping [IP address]  
     
   ping continues until you stop it by pressing ctrl-c. Check that the BBC website is on-line using:  
     
   ping bbc.co.uk  
     
   Note that you get the IP address of the BBC web server as a bonus; ping does a ‘DNS lookup’ for you. If you cannot get a link to the BBC website it may be because you are not on the correct network (no gateway).
4. Now that you have contacted a number of machines on your LAN, you can find their MAC addresses with the ‘arp’ command:  
     
   arp -a  
     
   Give it time to run. What you have is a list of all the machines’ MAC addresses that your machine has contacted on the LAN. Note that the BBC’s MAC address is not there – why?
5. Note that the form of ‘arp’ command that we used gave symbolic names to the computers on the network. To get the IP addresses use:  
     
   arp -n //n = numeric

## Task 2: Install Wireshark

So far we have used Ubuntu’s ‘Advanced Package Tool’ (APT) to install software. Today we will look at using the Software Catalog.

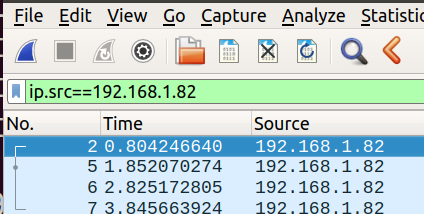
1. As always, before installing any new software, check that the current setup is up to date using the following terminal sudo apt upcommand:  
     
   sudo apt update //you will need your password

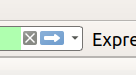
Then, follow the advice to see a list of upgradable packages, and update them using:  
  
sudo apt upgrade //upgrade, not update

This is good advice, and should always be followed when adding/upgrading software, so you will not be advised again - - don’t forget

1. Go to software catalogue (orange paper bag icon on the left) and search for ‘Wireshark’. Select to install

Tick the ‘Should non-superusers be able to capture packets?’ box, then Next in order to complete the installation.

1. When complete, click ‘Launch’. You will be limited as to what you can do (basically, you cannot capture any real packets).
2. BEFORE you close it down, note the ‘blue shark fin’ icon on the left (it shows Wireshark is running). Right click on it and select add to favourites – this will mean that the icon will remain even when you close Wireshark.
3. The reason you cannot capture packets is that you are not a member of the ‘wireshark’ group. Make yourself a member of the wireshark group (see earlier lab work on groups, remembering to log out/in for the setting to take effect).
4. Check you are a member of the wireshark group and run Wireshark by clicking on the shark fin icon you created earlier. This time you should see a range of adaptors that you can capture from. Find out which adaptor is the one in use (it will have an IP address on the your network, and will probably be labelled ‘ens33’) and select it by double clicking on it.
5. This should start the capture process – there may be lots of packets being captured. Clicking the red square icon (top left) should stop the process (clicking the blue fin next to it will restart). The packets are numbered down the left hand side of the screen. Double click on one of the packets you see and note down the destination:  
     
   Destination = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(should be a valid IP address)  
     
   To see packets we are interested in we need to apply some filters. At the top of Wireshark window, enter the following text

ip.src == *your ip address*  
  
and click on the white/blue arrow button to the right Restart the capture using the shark fin, and note that there are fewer packets being displayed, although the capture count at the bottom of the screen is still increasing.

1. Whilst Wireshark is in this state, change the filter to ‘icmp’ (valid entries cause it to go green); don’t forget to press the blue/white arrow to implement the change. Open a terminal and ping the BBC website. Consider what is happening (stop the ping after 4 ping messages). Look at the packets that have been captured (they show up in pink on my screen). In particular, use Wireshark to note down the IP address of the BBC as ‘looked up’ by the DNS enquiry, and the address of the DNS server used to do the lookup. Describe the ‘test message’ sent by the ping command (double click on the packet to open it).  
     
   BBC: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
     
   Local DNS server: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
     
   PING test message: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Use the Internet to find out how to filter packets so that you can see the ping replies (your address is now the destination) coming from the BBC – if any.
3. The number of ping packets sent by the ping command can be configured by adding ‘ –c x’ (-c means ‘count’) to the ping command, where x is the number of pings you want. If the BBC is not responding, try pinging the local gateway – the address of the gateway can be found with the command line ‘route –n’
4. Now capture some ARP packets, and check that they are as we discussed in the lecture. The filter is just ‘arp’. Open the packets up and examine them.

**Notes:**

1. It is worth reading about Wireshark filters because they are very useful.
2. You need to be able to use Wireshark to diagnose network/comms error – practise!