

Professional Certificate of Competency in Advanced TCP/IP-Based Industrial Networking (CAV)

**Please note: Exercises 14, 15a & 17 are are purely for educational purpose and are not part of Assessment 1.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Module number** | Modules 1 to 6 | | |
| **Assessment type** | Exercises 14, 15 & 17 (not-assessed) | | |
| **Remote Lab Types:** | 1. EIT PC with hardware, 2. EIT PC with Simulation Software, 3. Cloud PC with software, 4. Student/Home PC | | |
| **Version** | 3 | | |
| **Created by** | D. Reynders | **Date** | 28 October 2013 |
| **Last Reviewed by** | D. Reynders | **Date** | 7 July 2021 |

|  |  |
| --- | --- |
| **Exercise 14:** | **Ethernet Basics** |
| **Remote Lab PC:** | **Labs 1 & 2** |
| **Remote Lab Type:** | **B, D** |

**Overview**

In these exercises we will focus on attributes of Ethernet, in particular the header structure and speed/duplex settings.

**Hardware**

You can perform these exercises on your own computer. Alternatively you can use Remote Labs 1 or 2 (or search for Wireshark on Electromeet). If, for any reason, you are unable to install the software on your computer, or encounter any other technical difficulties, then you must immediately contact your course coordinator.

**Lab & Software Information**

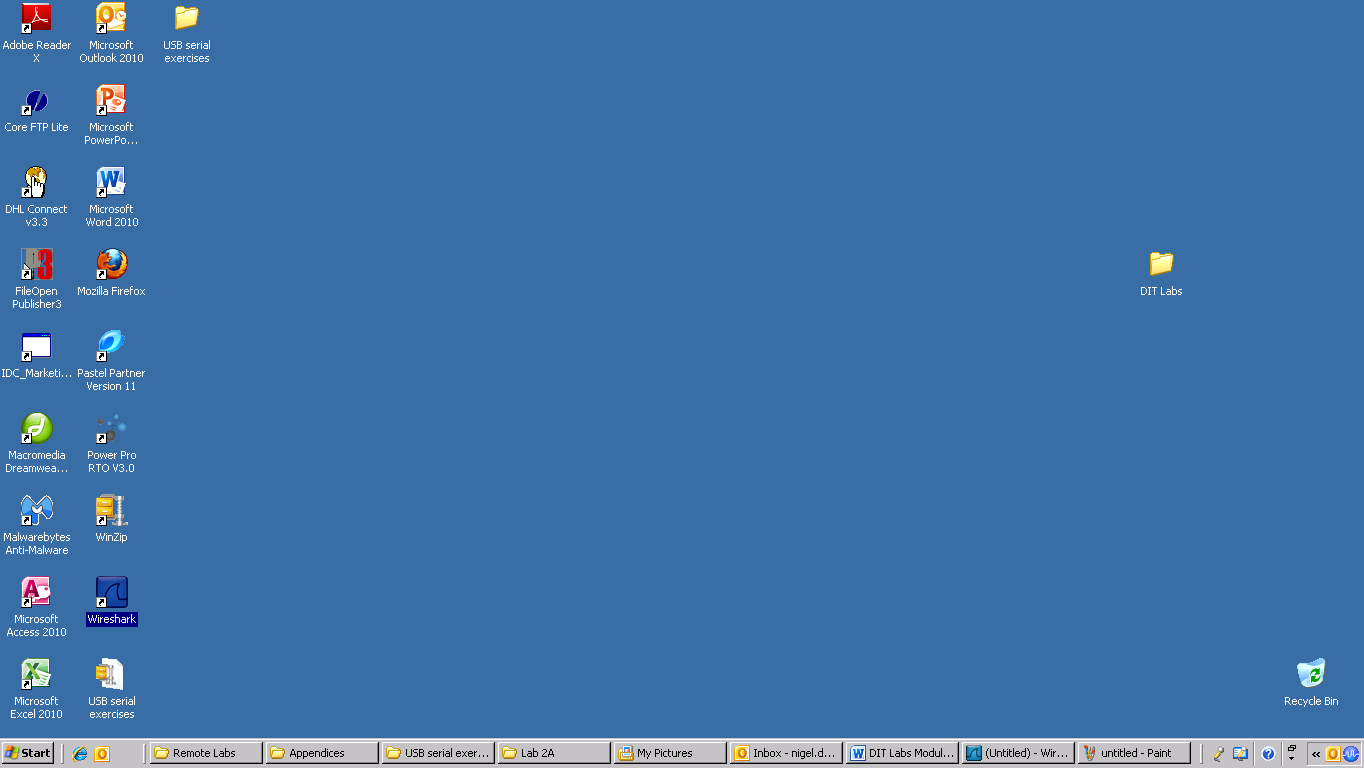
**Wireshark software:** Log into the Electromeet, open Lab 1 or 2. Alternatively download and install ot on your own computer [here](http://www.wireshark.org/download.html). *Note that there are different versions for 32- and 64-bit machines.*

**Screen capture software:** Jing and Screenhunter Free are examples of free screen capturing software. When downloading or installing such software, please be careful not to install any unnecessary add-ons eg. Toolbars. Select ‘advanced’ installation and decline all offers.

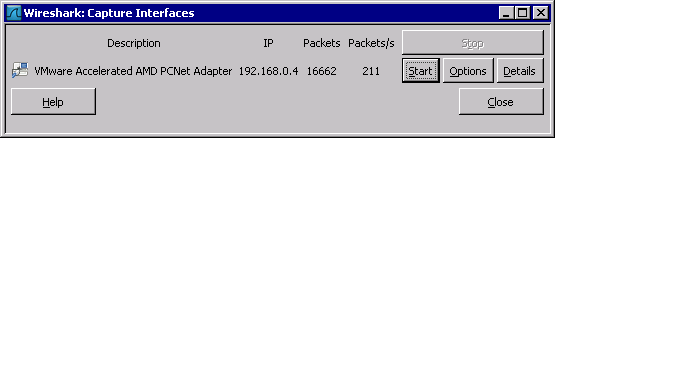
**Implementation**

**CAPTURING ETHERNET FRAME AND VERIFYING TYPE OF FRAME**

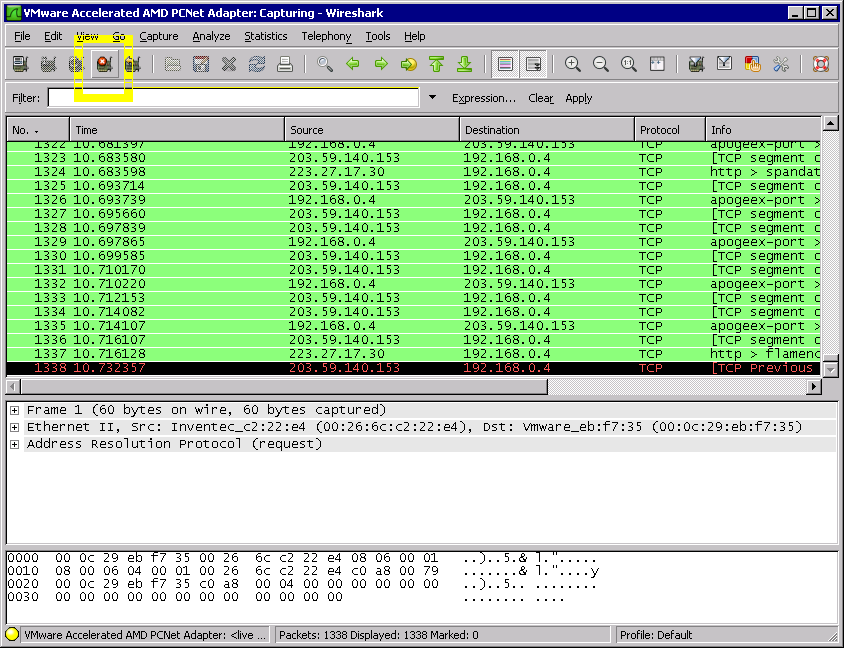
Click on Wireshark icon on the remote lab desktop.



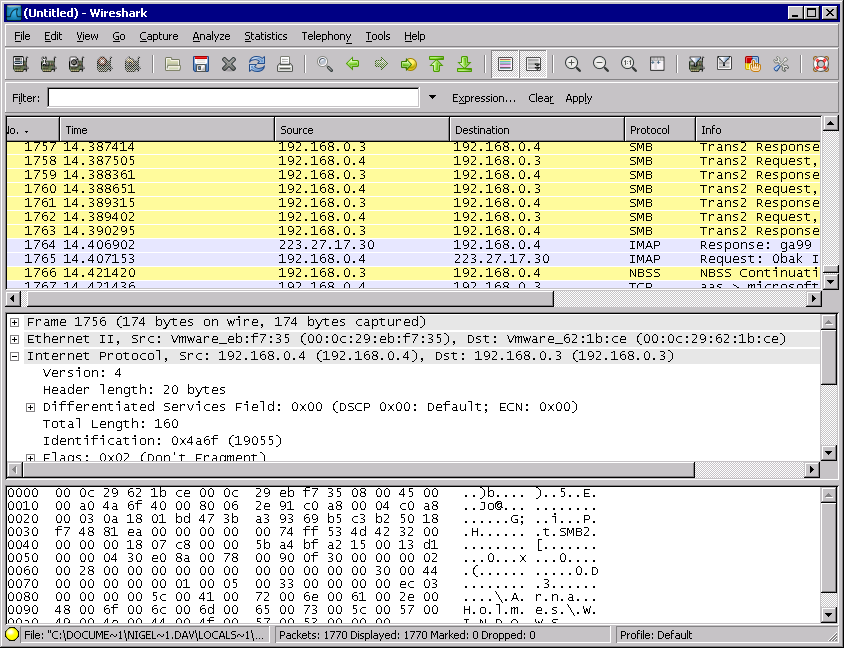
Capture several frames by clicking Start-> Interfaces and then clicking the ‘Start’ button against the interface currently in use (i.e. the one that shows an increasing number of packets). On newer versions of Wireshark you first need to check the box against the desired interface before hitting ‘Start’



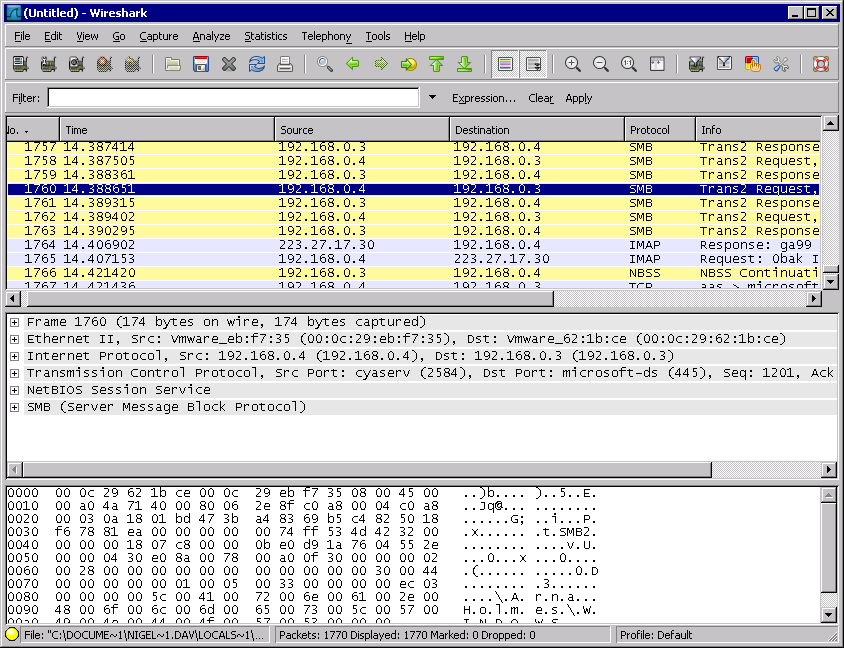
Capture a few packets, and then stop Wireshark



Divide the screen into three equal parts. The upper part shows a summary of the packets captured, the middle part shows the contents of the selected frame (packet) in terms of headers etc., and the lower part shows the contents of the selected frame in Hex and ASCII

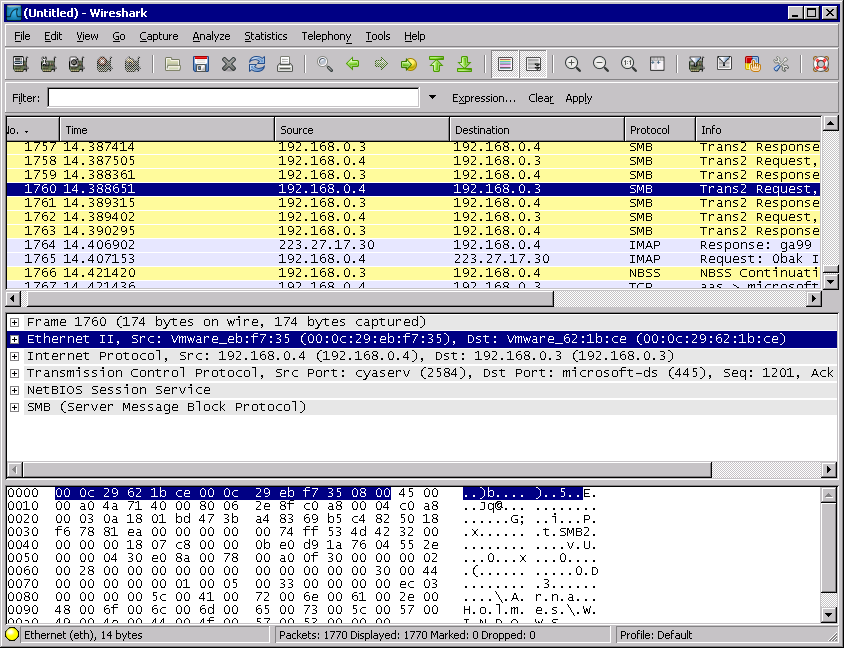


Select any packet (frame) in the top section of the screen



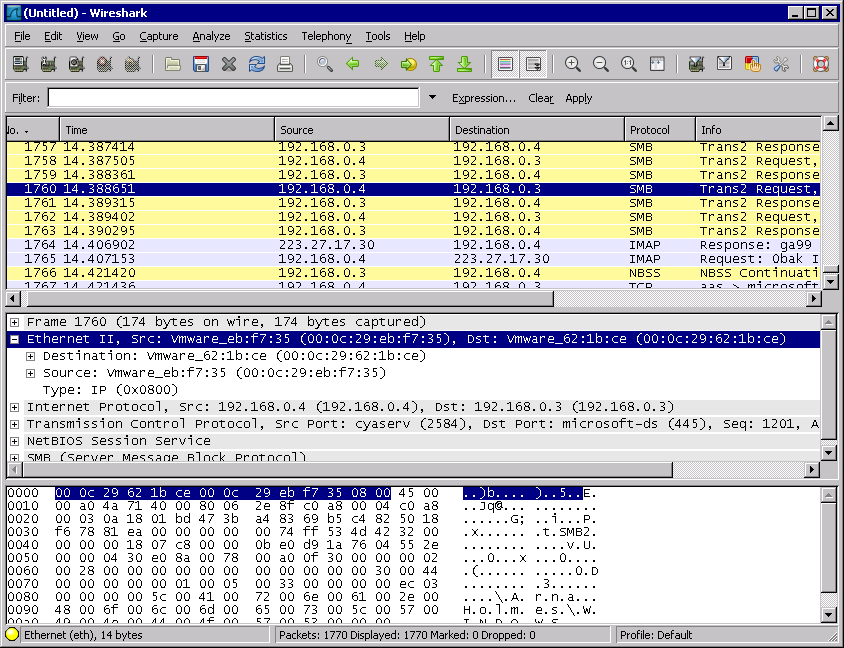
Go to the SECOND line in the centre section of the screen. This corresponds with Layer 2 (Data Link Layer) in the OSI model and hence, in our case, to Ethernet

*Note that it is likely to be an Ethernet II (also known as Ethernet V2 or ‘Bluebook) frame. Ethernet IEEE 802.3 frames will be labelled as such…but are fairly rare.*

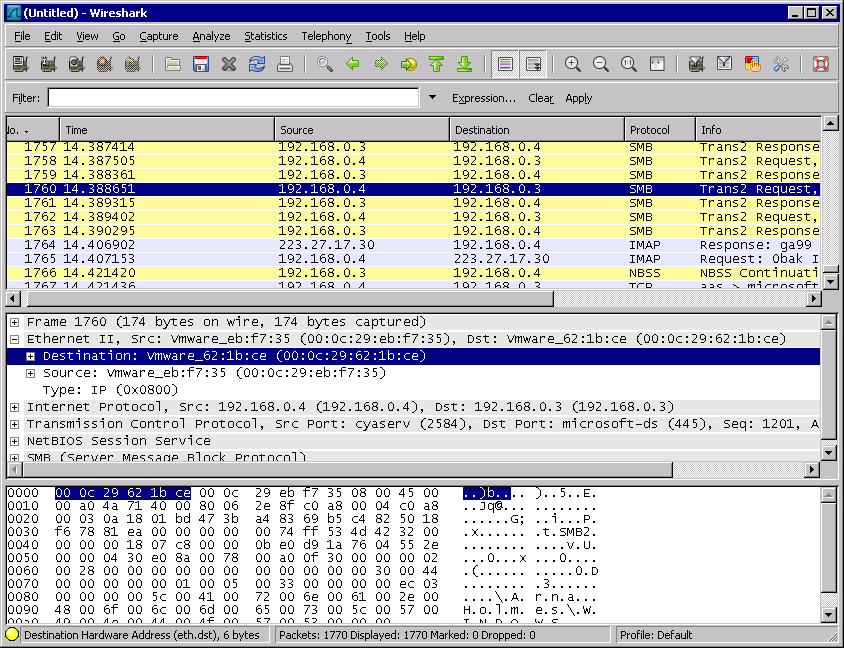


Click the [+] ONCE so that the Ethernet header opens up. You will see the source and destination hardware (‘MAC’) addresses. Click on them individually, and observe the actual MAC addresses (hexadecimal) in the bottom pane on the screen.

They should resemble the example below.



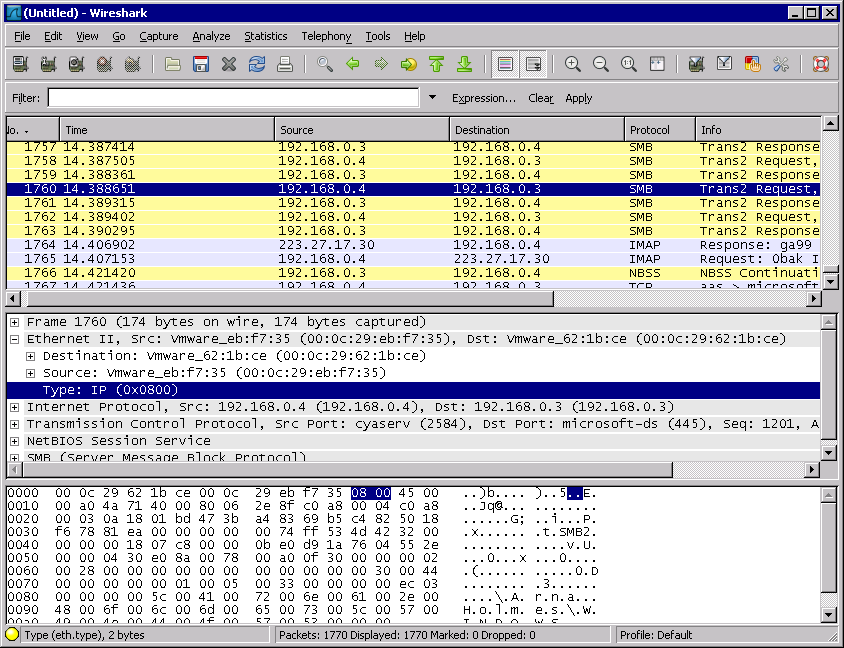
Note that, if you select a particular field within the header (in the centre section of the display), the corresponding bytes in the ‘raw’ data captured from the network is highlighted as well, in the bottom section of the screen as in the following example



**Snag the Ethernet header, but only the 4 lines related to the header i.e. the summary and the three fields within the header.**

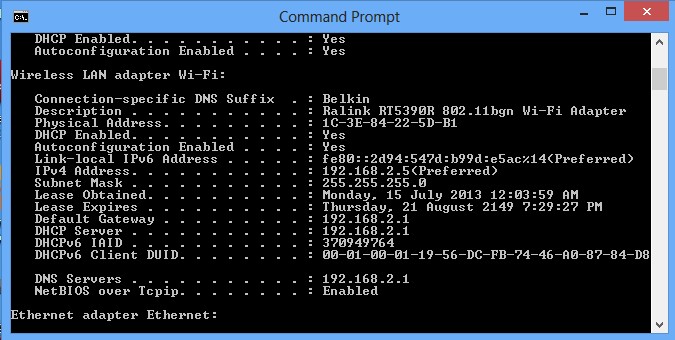
**Do not expand the individual MAC addresses, as that only clutters up the display. PLEASE do not capture the whole computer screen.**

Now observe the 3rd field. Since it contains a ‘Type’ number we know it is a V2 frame. For the IEEE 802.3 format this would be a ‘Length’ field.



Check the type number (0x0800 meaning 0800 Hex) here to confirm that the payload (that follows) is IP).

Go to the DOS(Command) prompt and type *ipconfig /all.* You will get something like this:



*Note your MAC address (a.k.a. Physical Address) for the connection you are currently using (Ethernet or Wi-Fi). In the example above it is 1C-3E-84-2-5D-B1.*

**Snag the IPCONFIG display**

1. What is the MAC address on your own computer?
2. Is the Ethernet packet you snagged earlier being sent to or from your machine? Justify your answer

**SPEED AND DUPLEX SETTINGS**

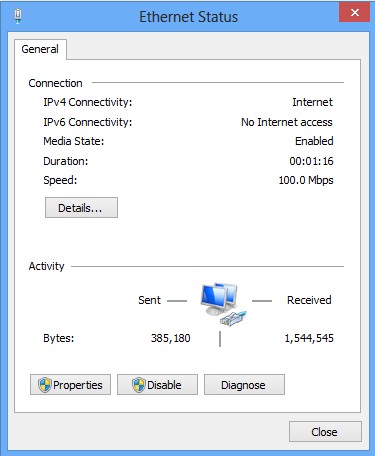
The initial steps may vary slightly between operating systems.

Go to your Control Panel. For Windows 7 and 8 you would select ‘Control Panel’ from the Start menu, in XP you would go Start->Settings->Control Panel.

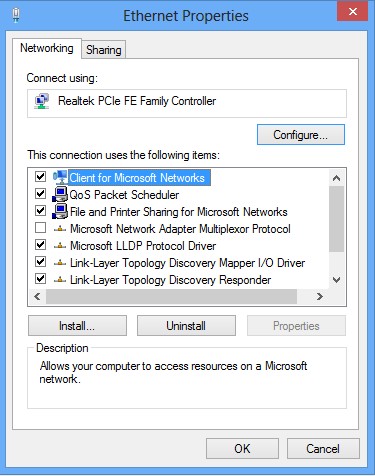
From here you can select View Network Status and tasks->Change Adapter Settings, or in XP you could select Networks directly from the Control Panel display



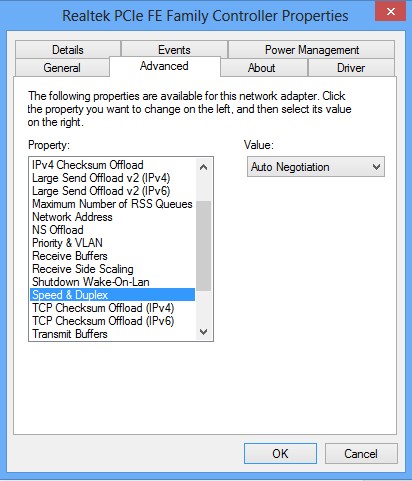
Click on the Ethernet connection to open up the Ethernet Status dialog box.



Click on Properties to open up the Ethernet Properties dialog box



Your Ethernet interface shows up under ‘Connect using:’. Now click on Configure and select the Advanced tab. From the Property box select Speed and Duplex, and then open the drop-down menu under Value. The current setting should be Auto-negotiation, but there are several other possibilities. DO NOT CHANGE THE SETTING at the present moment. You may need to do so if, for example, you attach your laptop to switch that fails to auto-negotiate a setting, at which point you might need to alter the setting



**Take a screenshot of the speed and duplex settings, with the Value dialog box open if possible. However, Screenhunter might insist on closing it, as in the snag above.**

|  |  |
| --- | --- |
| **Exercise 15a:** | **Protocols viz. IP (IPv4), ICMP and ARP.** |
| **Remote Lab PC:** | **Labs 1 & 2** |
| **Protocol Analyser:** | **Wireshark** |
| **Utility:** | **IPConfig Manager** |
| **Remote Lab Type:** | **B, D** |

**Objective**

In this exercise we will observe three of the Internet layer (OSI ‘Network’ layer) protocols viz. IP (IPv4), ICMP and ARP.

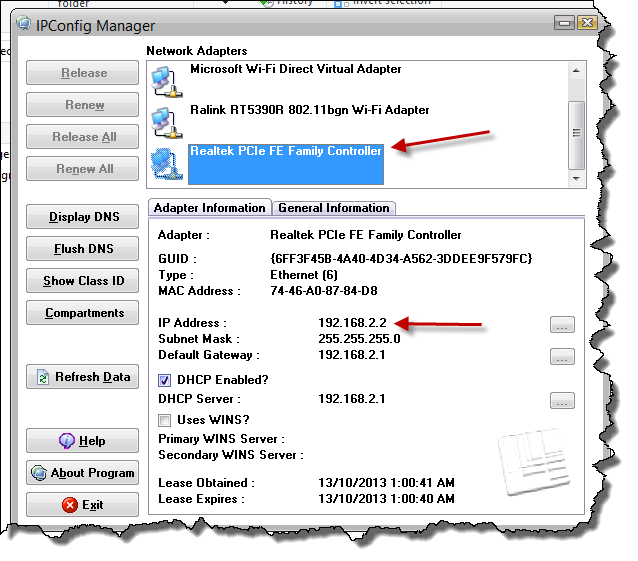
**Software Instructions**

Download IPConfigMgr from Moodle. In addition you will need Wireshark. If you have not downloaded it yet, get it from Wireshark.org and make sure you install WinPCap as well.

**Exercise**

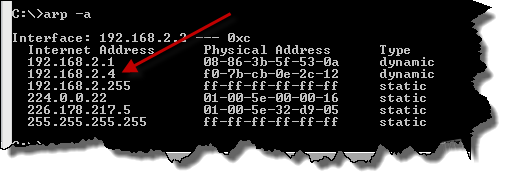
First of all, let’s check our own configuration. Run IPConfig Manager and select the currently used interface. Then check the IP address.

**Snag Your Results**

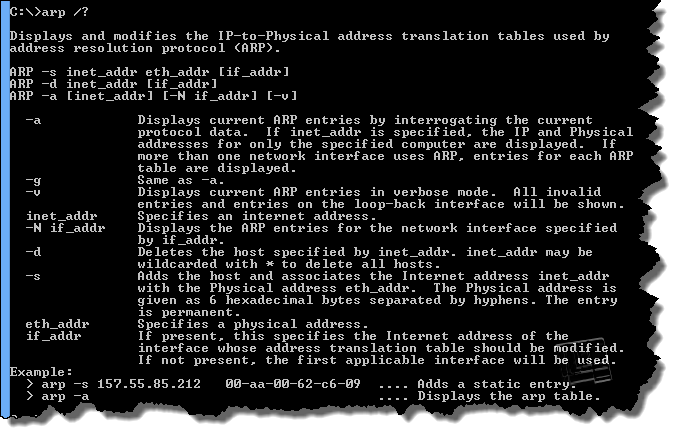


We are going to ping another machine on the local network, in this case 192.168.2.4.

However, we want to invoke an ARP request, so we need to check if 192.168.2.4 is already showing up in the ARP cache or not.



Because of this, there is no need for an ARP, so we need to delete it first. If you are unsure of the options (‘switches’) you can type arp /?

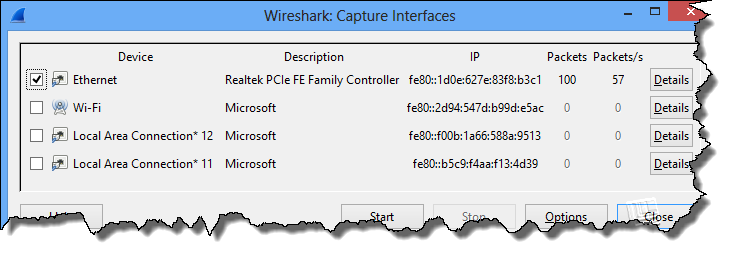


Good, we will type arp –d \* (space after the ‘d’) and get rid of the dynamic entries.

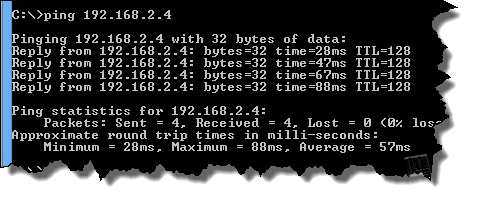


*If you do not have another device on your network (except your ADSL router), you have a monor problem. You cannot delete the static entry for your router (default gateway; 192.168.2.1 in the screenshot above), as your computer will re-populate that entry immediately. However, this is done via an ARP Request/Reply, so if you run Wireshark and then delete that entry, e.g. arp –d 192.168.2.1, then you will be able to capture associated the ARP frames.*

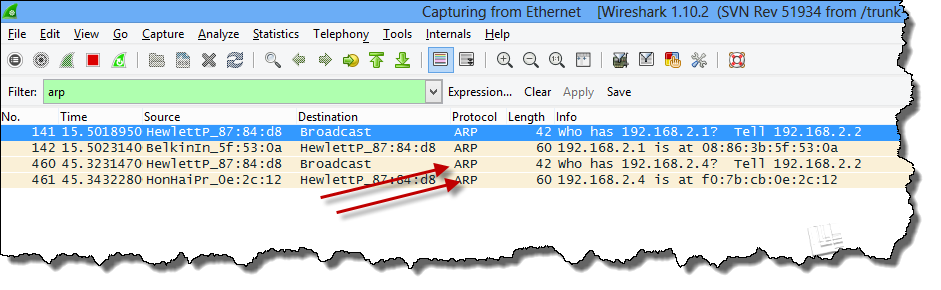
*For the sake of this exercise we will assume there is another computer viz. 192.168.2.4.* So let us ping 192.168.2.4. But first get Wireshark up and running. Click *Capture->Interfaces*, select your active network connection, and click start.



Ok, go ahead and ping.

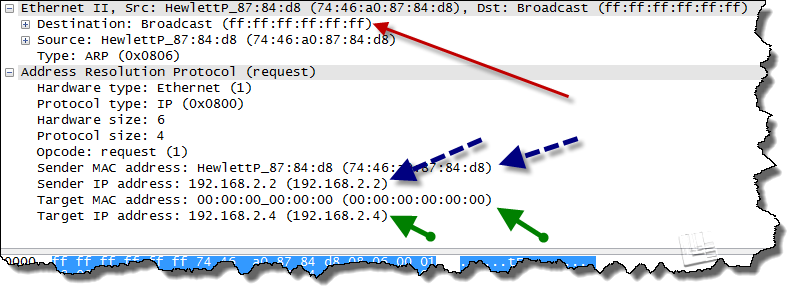


Now stop Wireshark (red square or *Capture->Stop*) and type *6arp* in the filter box (and apply) to hide the rest of the traffic. We already know what our IP address is, and we know that we are pinging 192.168.2.4, so it is easy to locate the ARP Request and Reply.



Select the first ARP packet (Request),and expand the Ethernet and ARP headers (just on once). Notice the following:

**SNAG YOUR RESULT**

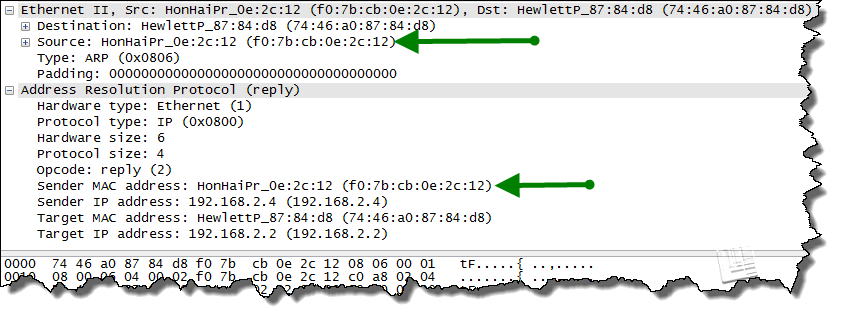


Ethernet is broadcasting the message to all nodes (red arrow).

Both our IP and MAC addresses appear (blue arrows).

The MAC address of the target is left blank (green arrows), because that is what we are trying to ascertain.

Select the next message (ARP Reply) in the upper frame and look at the Ethernet/ARP headers.

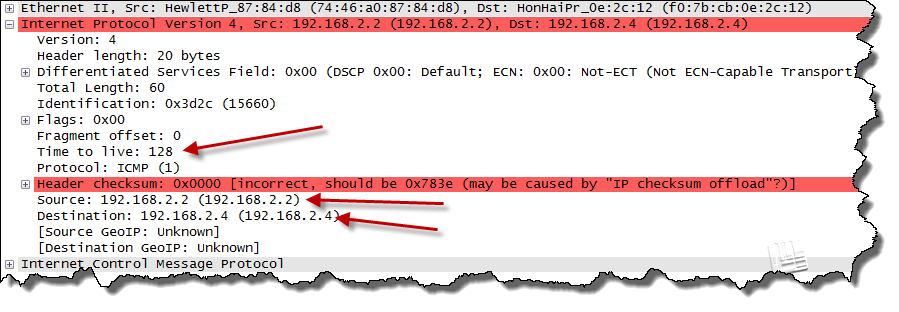


192.168.2.4 changes from the target to the sender, and supplies its MAC adress both in the Ethernet header and in the ARP header (green arrows).

Now change the Wireshark filter to *icmp* and click apply. Select an Echo Request packet (directed at 192.168.2.4).

Expand ONLY the IP header, not the TTL and source/destnation IP addresses.

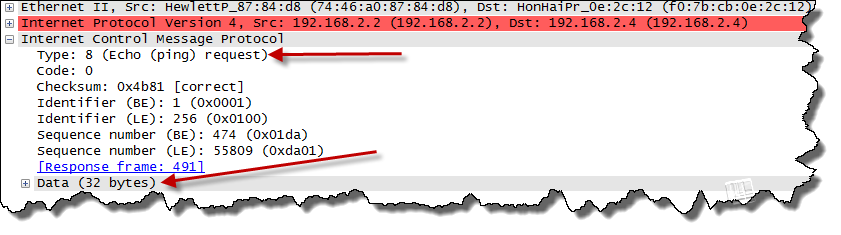
**SNAG YOUR RESULT**



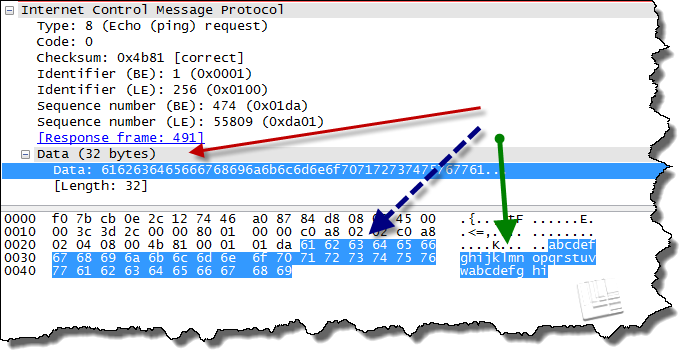
Note that the text in [brackets] is not part of the actual header.

No collapse the IP header, and expand the ICMP header. Note the Type (8) and the 32 bits of data.

**SNAG YOUR RESULT**



Now expand the ICMP data field (red). See the actual ‘raw’ ASCII data in this field, as well as its alhabetical representation.



You may want to select the next packet in the upper frame (Echo Reply) and see what changes in the display above.

|  |  |
| --- | --- |
| **Exercise 17a:** | **TCP/IP Command Line Utilities** |
| **Remote Lab PC:** | **N/A** |
| **Remote Lab Type:** | **D** |

**Objective**

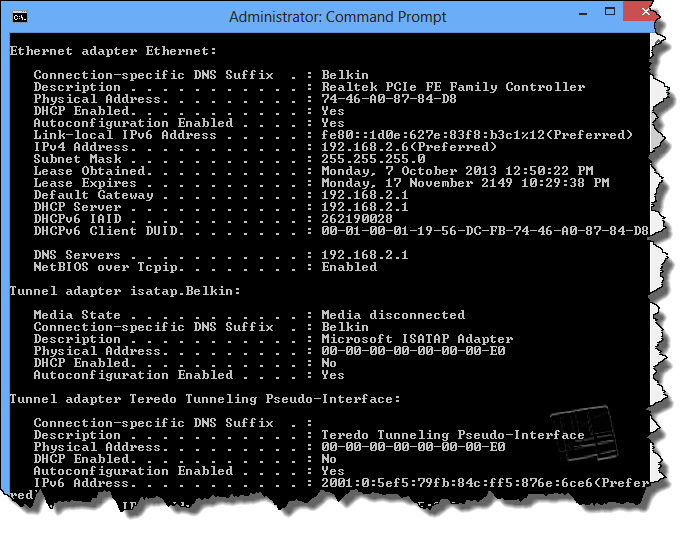
The purpose of this exercise is to demonstrate a few of the built-in TCP/IP utilies viz. ‘ipconfig’, ‘ping’, ‘arp’, ‘tracert’, and to demonstrate the use of the ‘hosts’ file.

**Determining your own IP address**

At the command prompt, type ipconfig /a (with a space after the ‘g’) in order to determine your own IP address as well as the IP address of your default gateway (typically the ‘inside’ IP address of your ADSL router).

If necessary, scroll down to locate your interface currently in use. In this case it was Ethernet. Note the host IP address of 192.68.2.6 and the Default Gateway address of 192.168.2.1.

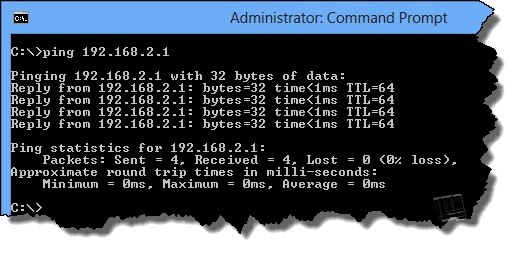
**Snag Your Results**



**Pinging your Router**

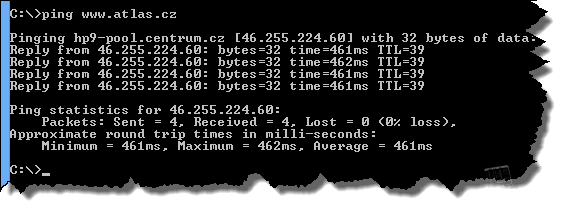
Ping your default gateway, e.g. *ping 192.168.2.1* in this case.

**SNAG YOUR RESULT**



Next, ping a website in the Czech Republic, viz. *atlas.cz*.

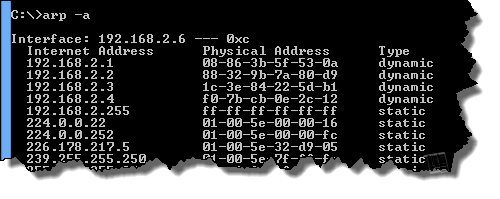
**SNAG YOUR RESULT**



**Reading your ARP cache**

Observe the content of your Arp cache by typing arp –a. If there are no entries, just ping someone.

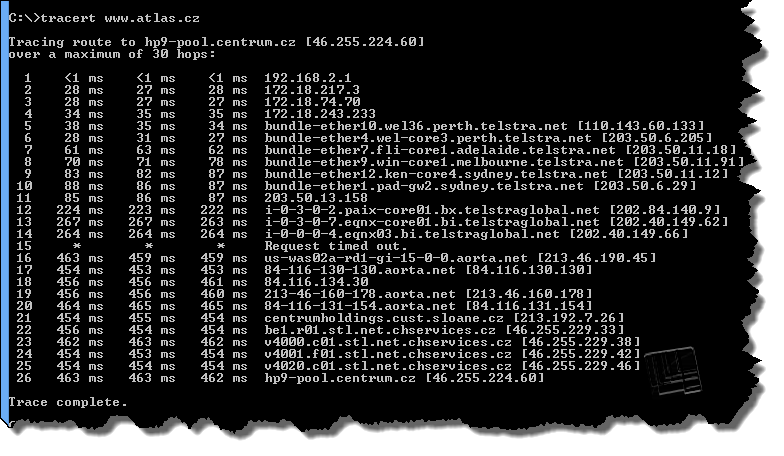
**SNAG YOUR RESULT**



**Tracing a route**

Type tracert [www.atlas.cz](http://www.atlas.cz) in order to trace the route from you to atlas.cz.

**SNAG YOUR RESULT**



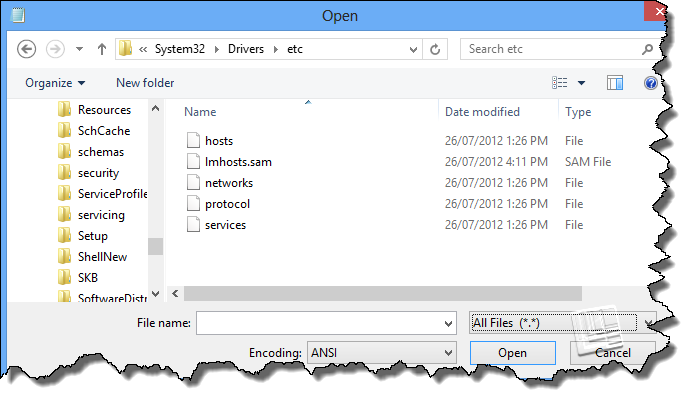
**Modifying the Hosts file**

The Hosts file (note: no extension) is located in C:\Windows\System32\Drivers\etc. Once you have located it, you can edit it with Notepad. In Vista, 7 and 8 you will need Administrator priveleges to modify its contents.

**Windows 8**

1. Move your cursor to the top right-hand side of the screen
2. Click on the ‘search’ charm when it appears, and type the first few letters of *notepad*
3. When the system finds it, right-click on it and select the ‘run as administrator’ icon at the bottom of the screen

When browsing for it, remember to select ‘all files’ as the file type, because Norepad defaults to .txt hence the hosts file will not show up.



Open ‘hosts’ (without an extension, i.e. not hosts.sam)

**Windows Vista and Windows 7**

1. Click *Start -> All Programs -> Accessories*

2. Right click Notepad and select *Run as administrator*

3. Click Continue on the "Windows needs your permission" UAC window.

4. When Notepad opens Click *File -> Open*

5. In the filename field type *C:\Windows\System32\Drivers\etc\hosts* (or navigate there) Click *Open*

**Windows NT/2000/XP**

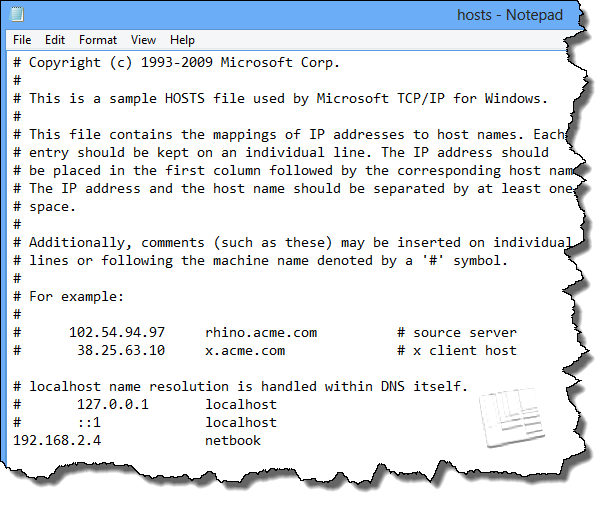
1. Click *Start -> All Programs -> Accessories -> Notepad*

2. Click *File -> Open*

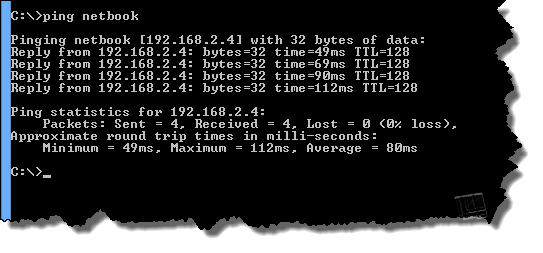
3. In the filename field type *C:\Windows\System32\Drivers\etc\hosts* (or just navigate there)

4. Click Open

The ‘hosts’ file opens. The entries with the ‘#’ sign are seen as comments. In the case below we entered the name of another device (any one) an added a ‘nickname’. This name is not the Computer Name (i.e. NetBIOS name), but one that we allocated *ad lib*.



Save the modified hosts file, and then attempt to ping the name you added, like ‘netbook’ in this case.



Keep in mind that ‘netbook’ as an alias for 192.168.2.4 will only exist on this machine.

|  |  |
| --- | --- |
| **Exercise 17b:** | **TCP/IP Windows-Based Ping/Trace Utilities** |
| **Remote Lab PC:** | **N/A** |
| **Trace Utility:** | **Visual Route 2010** |
| **IP Scanner:** | **SoftPerfect Network Scanner** |
| **Remote Lab Type:** | **D** |

**Objective**

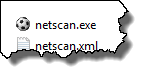
The purpose of this exercise is to demonstrate Windows utilities that can be used for pinging and route tracing. There are several alternatives when it comes to these ptograms.

**Instructions**

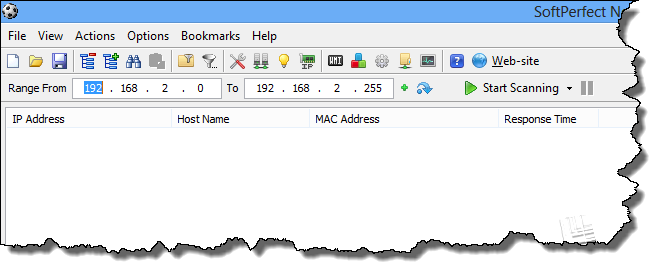
Download VisualRoute 2010 Lite from [here](http://www.visualroute.com/download.html). Download the SoftPerfect Network Scanner (.zip) from Moodle.

**IP address Scan**

Run SoftPerfect Network Scanner (netscan.exe).



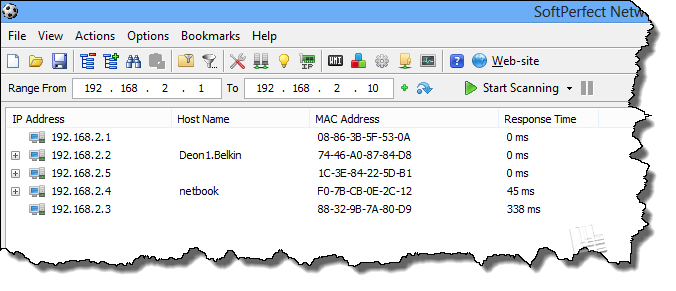
It will open up like this:



The manual is included, so take some time to investigate all the options. We will, however, just do a quick scan now. Type in a range of IP addresses to scan. To save time, we will scan from 192.168.2.1 to 192.168.2.10. Click *Start Scanning* when done.

Notice the MAC adresses in addition to the IP addresses. The Host names have to be treated with some care, they are not necessarily the assigned Computer Names (NetBIOS Names); they could also be the associated entries in your own Hosts file.

**SNAG YOUR RESULTS**



Done!

**Route Trace**

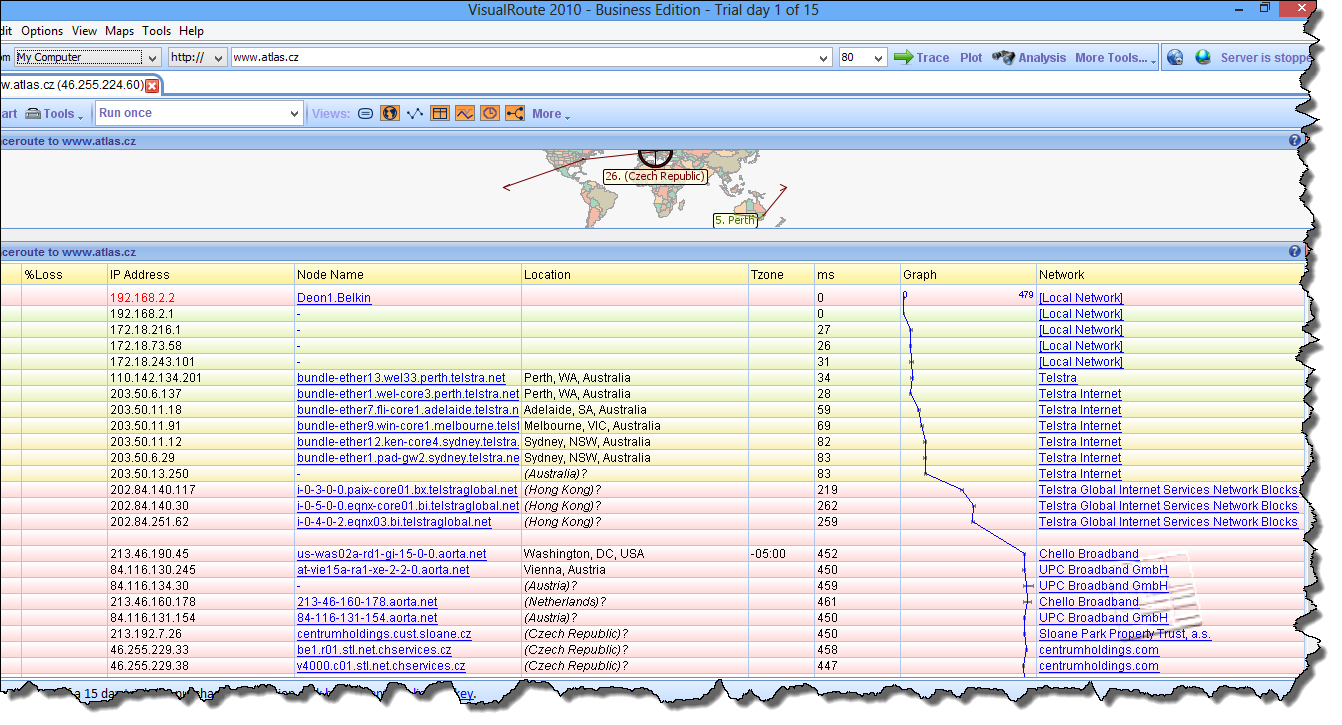
Run VisualTrace.



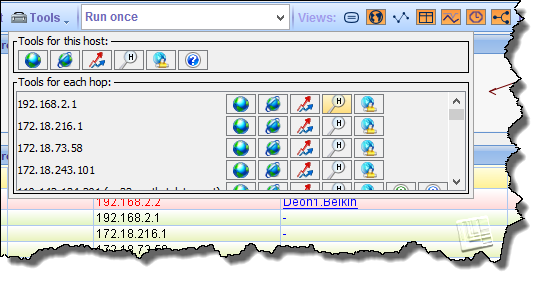
Close the welcome message.

We are going to trace the route to *atlas.cz*, just like we did with the DOS utility (tracert). Enter the URL and click Start.

When the trace is complete, it wil look like this:

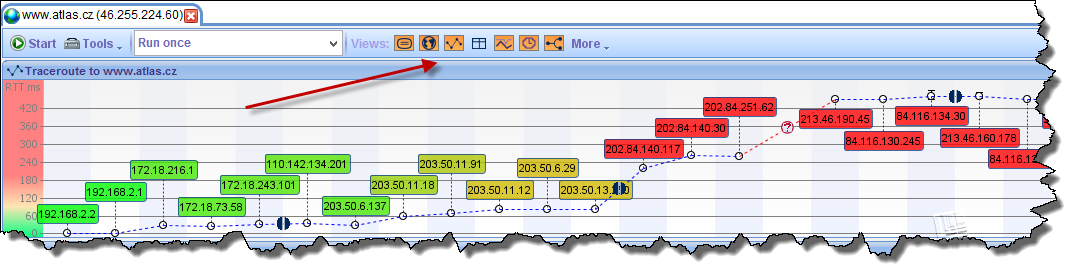


You can click the down arrow for ‘Tools’ and explore a few options there.

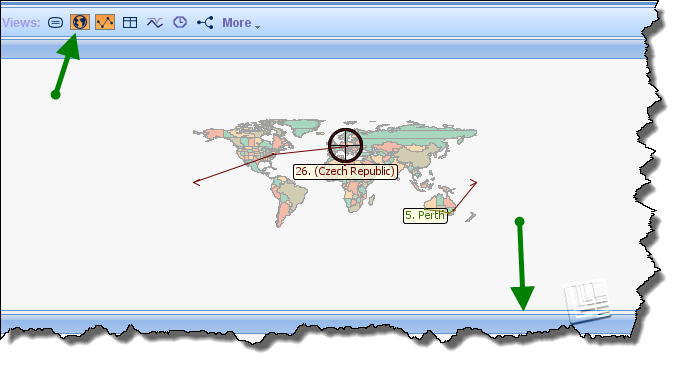


You can also explore the ‘Views’ options (see red arrow below). This not only shows the progression of the packet through all the routers on its way; it also indicates the ‘round trip time’ to each router.

**SNAG YOUR RESULT**

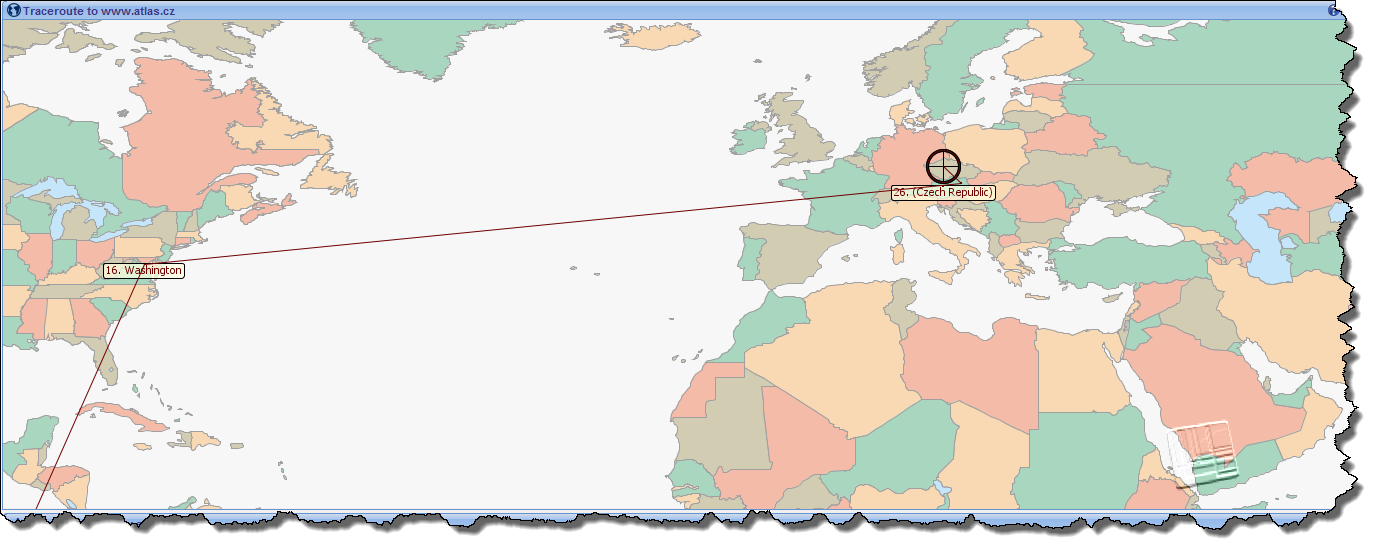


Select the ‘Map’ option (red arrow).



Now pull down the border (green arrow above) and then zoom in/out of the map with left/right mouse clicks, or dragging the picture by holding down the left mouse button.

**SNAG YOUR RESULT**



|  |  |
| --- | --- |
| **Exercise 17c:** | **TCP/IP Port Scanners** |
| **Remote Lab PC:** | **N/A** |
| **Port Scanner:** | **Advanced Port Scanner - NMap** |
| **Remote Lab Type:** | **D** |

**Objective**

The purpose of this exercise is to demonstrate the use of Windows-based port scanners for detecting TCP ports.

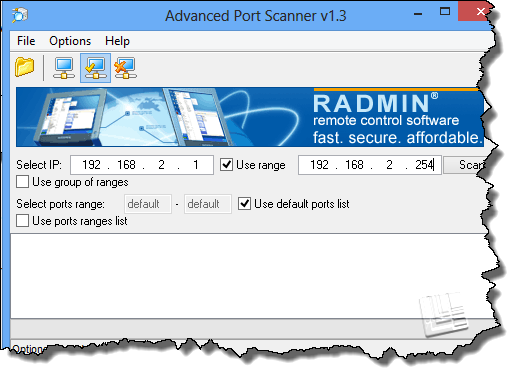
**Instructions**

Download NMAP from [here](http://nmap.org/download.html). Download Advanced Port Scanner from Moodle and install by running pscan12.



Scanning ports with Advanced Port Scanner

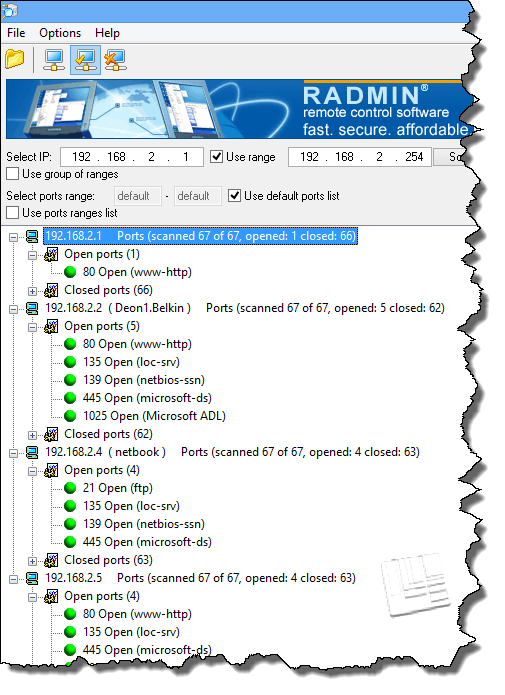
Run the program. It will open up like this:



Enter a range to be scanned. If you are doing this at home, set the range to include your ADSL router (Default Gateway) or wireless Access Point as well.

Once the scan is complete, click on the [+] to expand and keep ‘drilling down’ until you can see all the open ports.

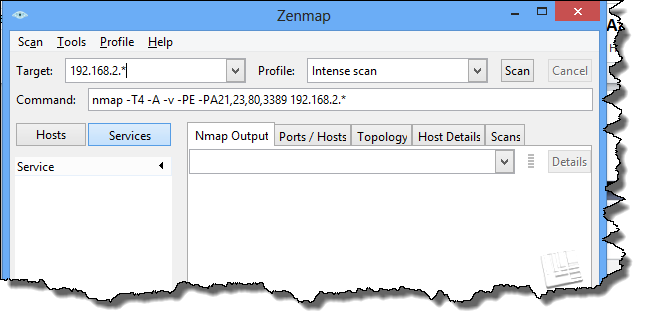
**SNAG YOUR RESULT**



What is the significance of the 21s and 80s showing up? You may also want to look up the 135, 139, 445 etc. [here](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers).

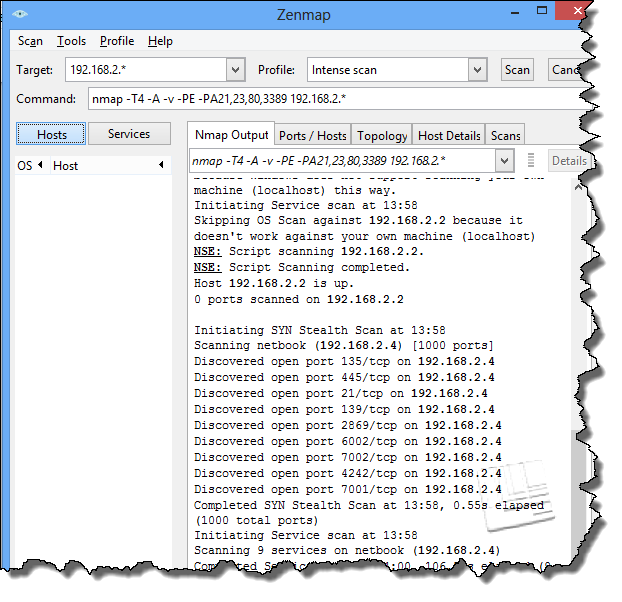
Scanning ports on hosts with NMap (Zenmap)

Run Nmap



You can type in the IP address of a specific host, or scan the whole subnet with the wilcard character (\*). The result will look like this:

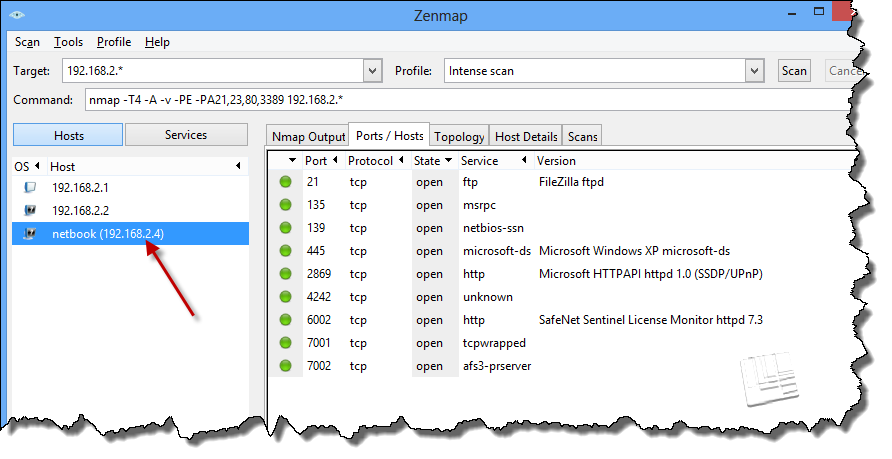
**SNAG YOUR RESULT, SHOWING THE RESULTS FOR AT LEAST ONE HOST**



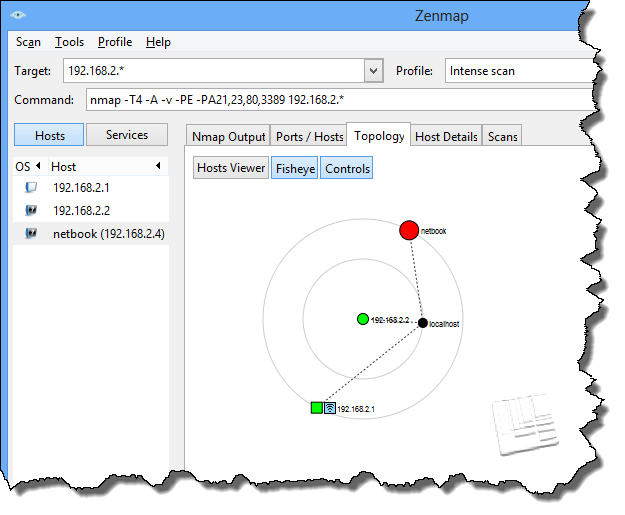
Different aspects of the scan results are displayed under the five tabs (Nmap Output, Ports /Hosts, Topology, Host Details, and Scans) of the Zenmap window.

‘Nmap Output’ shows the familiar Nmap output, displaying all the open and closed ports of the hosts on the network. See above.

‘Ports/Hosts’ shows all the ports on the selected host (see red arrow on the next page), along with version information when available.



‘Topology’ (below) gives an interactive view of the connections between hosts in a network.



‘Host Details’ displays all the information regarding a selected host into a hierarchical display.

