REMOTE LAB

Practical Exercise

Industrial Router Configuration

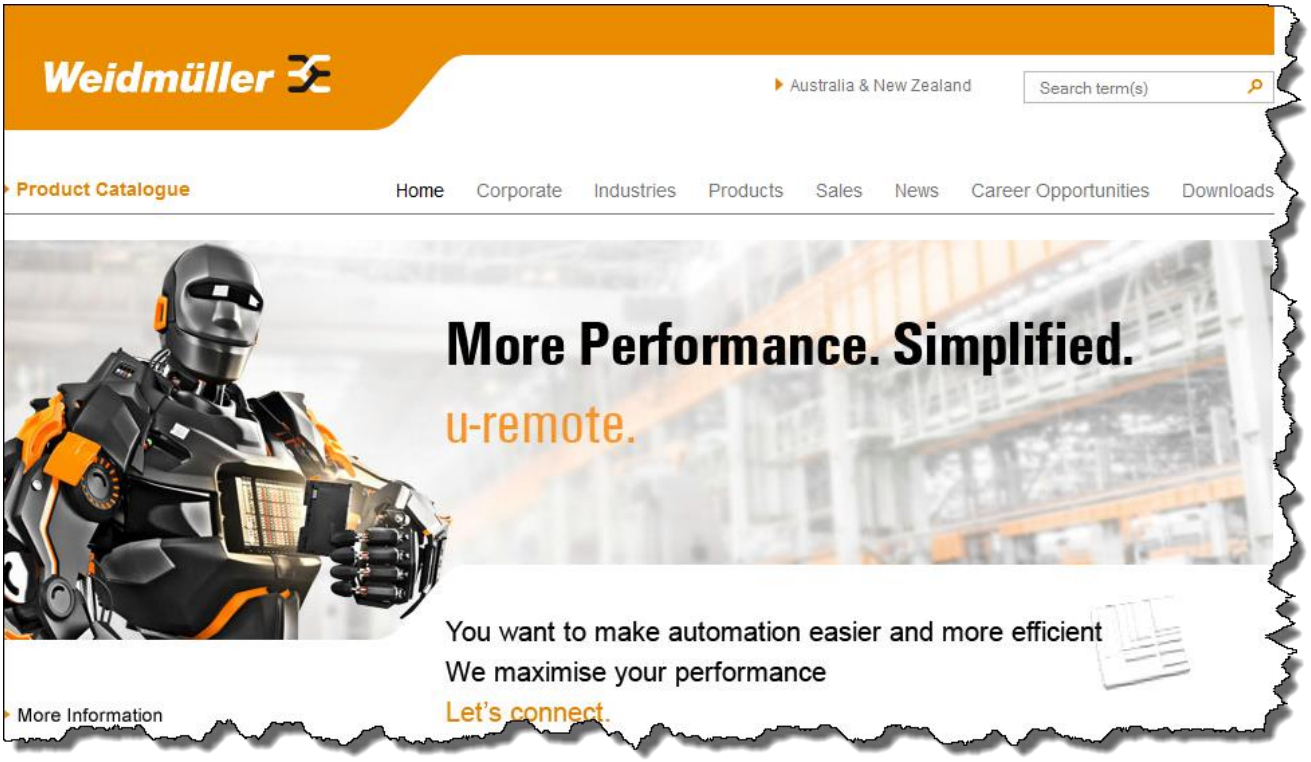
V1.0

Hardware List:			
Router	Weidmuller IE-ARM-E		
Software List:			
Protocol Analyzer	Wireshark	Version	Latest
Remote Lab PC:	RL1	Remote Lab Type:	A

R
Remote Lab Type: A-EIT PC with hardware, B-EIT PC with Simulation Software, C-Cloud PC with software, D-Student/Home PC

Created By:	DR	Date:	17/03/14
Checked By:	DS	Date:	14/11/2015
Released on:	14/11/2015	Next Review Date:	

EIT ENGINEERING INSTITUTE OF TECHNOLOGY



EIT wishes to acknowledge the contribution of Weidmuller Australia in donating the quipment for this exercise.

Weidmuller Pty Ltd

43 Huntingwood Drive

NSW, 2148 Huntingwood

PO Box 6944

Blacktown, NSW 2148

+ 61 (0)2 9671 9999 Tel

+ 61 (0)2 9671 9900 Fax

1. Objective

The objective of this exercise is to perform basic setup of a Weidmuller Industrial access router via a browser. We will do the following:

- Log into the router
- Check the IP addresses of the router ports
- Add a static route
- Confirm modem settings
- Perform basic firewall settings
- Ping/trace across the router
- Perform simple packet analysis to observe IP and MAC addresses for packets in transit

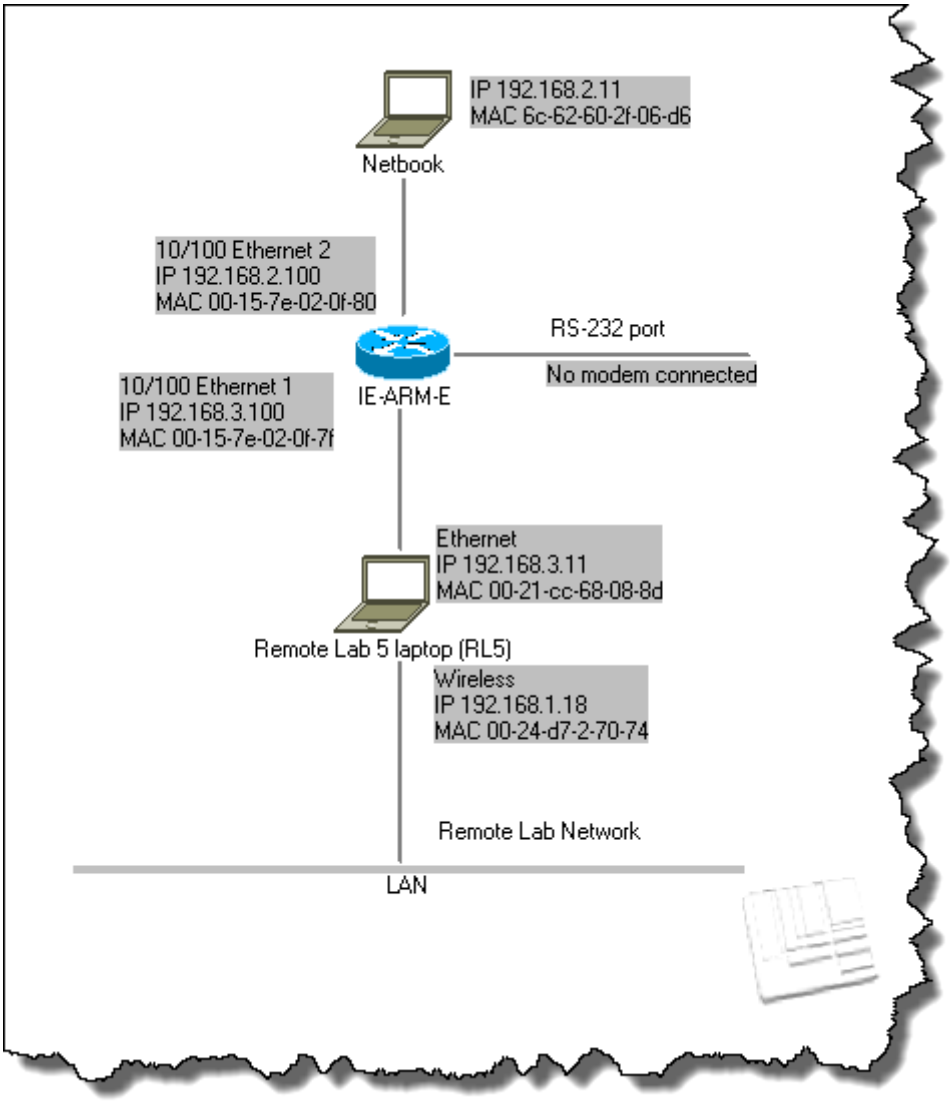
2. Background

The Weidmuller IE-ARM-E is a small-footprint Industrial access router that allows access to/from an Industrial network via Ethernet, or via a dialup link. The latter supports conventional modems, GSM, and ISDN, and allows dial-in, dial-out and callback. Because the purpose of this type of router is primarily to provide access to a network (e.g. for maintenance purposes) or to interconnect adjacent Industrial networks, it does not support routing protocols such as RIP, OSPF or EIGRP. Where necessary, manual routing table entries can be made.

For more technical detail on the router, please consult Annexure A.

The primary Eithernet port is named 10/100 Ethernet 1, and the secondary one is named 10/100 Ethernet 2. In the diagnostic menu theu are referred to as erh0 and eth1 respectively. The serial port is named RS-232 Console/Modem; ‘console’ for remote connection via a terminal emulator such as Hyperterminal, and ‘modem’ for connecting to a modem. This functionality is controlled via a small physical switch on the front panel.

The lab setup is as follows.



Note that the modem connection is shown for the sake of completeness, although it will not be used in this exercise. The 10/100 Ethernet 2 port IP address has been left at the default value of 192.168.2.100, but the 10/100 Ethernet 1 port has been changed from its default value of 192.168.1.100 to 192.168.3.100 in order to fit in with the lab network.

Also note that hardware in the lab may be replaced for maintenance purposes, hence MAC addresses can change. It is therefore in your own interest to verify these where applicable.

3. Instructions

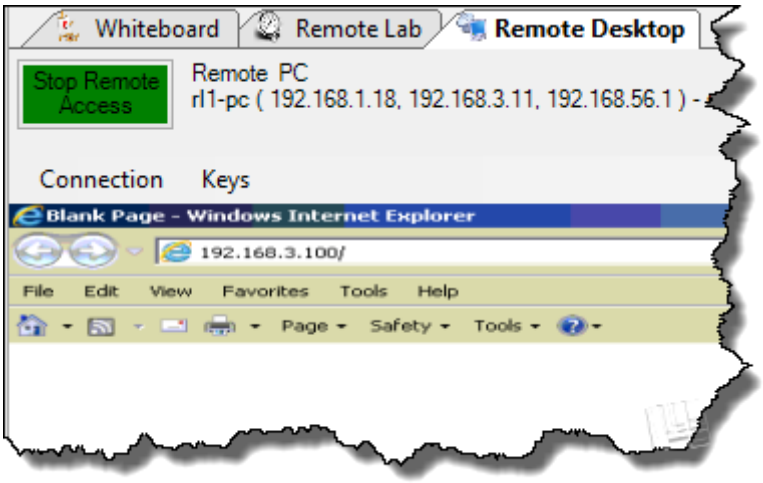
VERY IMPORTANT

THROUGHOUT THIS EXERCISE, PLEASE REFRAIN FROM SAVING ANY CHANGED SETTINGS

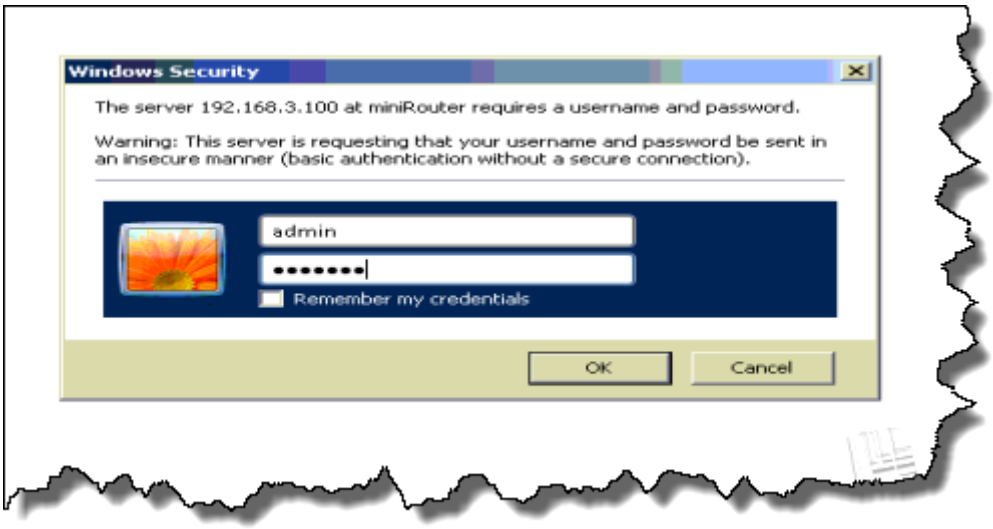
3.1 Logging into the router

Log into Electromeet, and open Remote Lab 1.

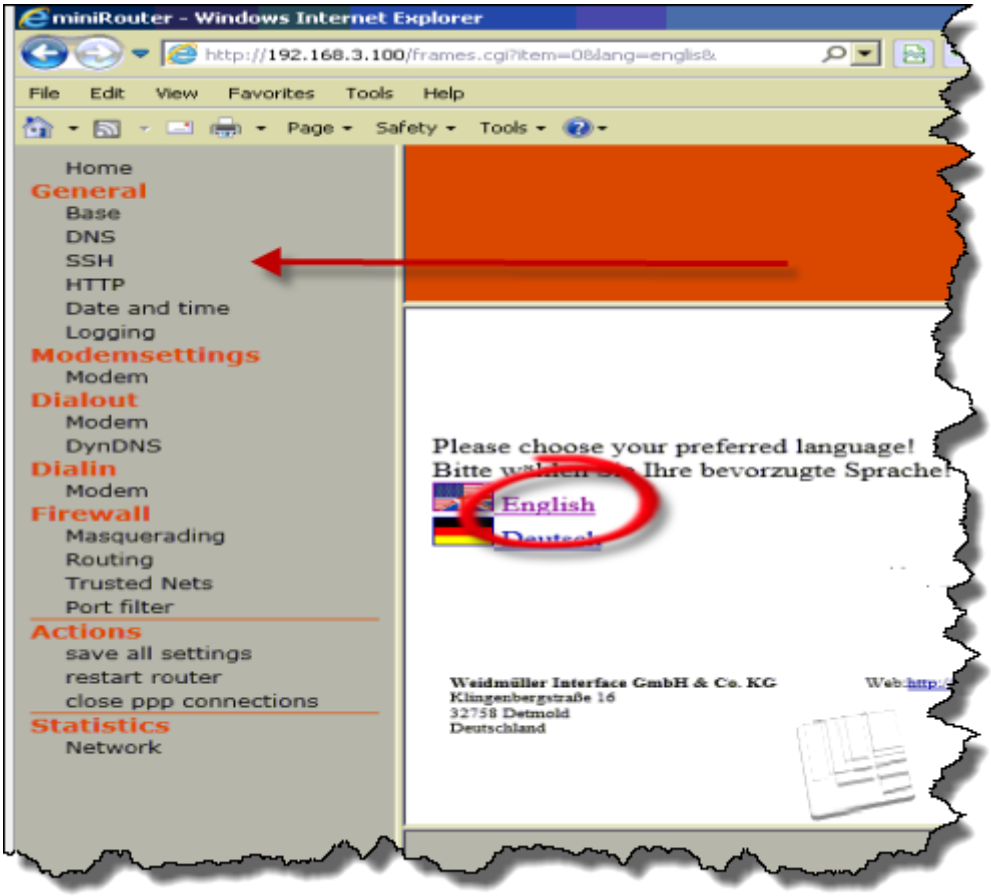
Open the browswer (IE) and type the router's IP address (192.168.3.100) in the search bar.



When challenged, provide the login credentials for the router (admin/detmold). Note that we are only using the default values because it is a exercise. In real life this would constitute a serious security risk.

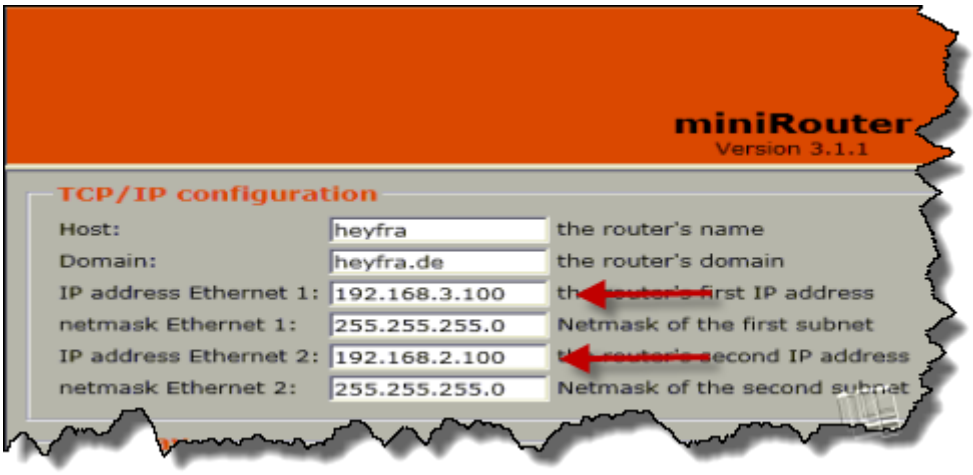


Click on 'English' and the menu will appear on the left-hand side.



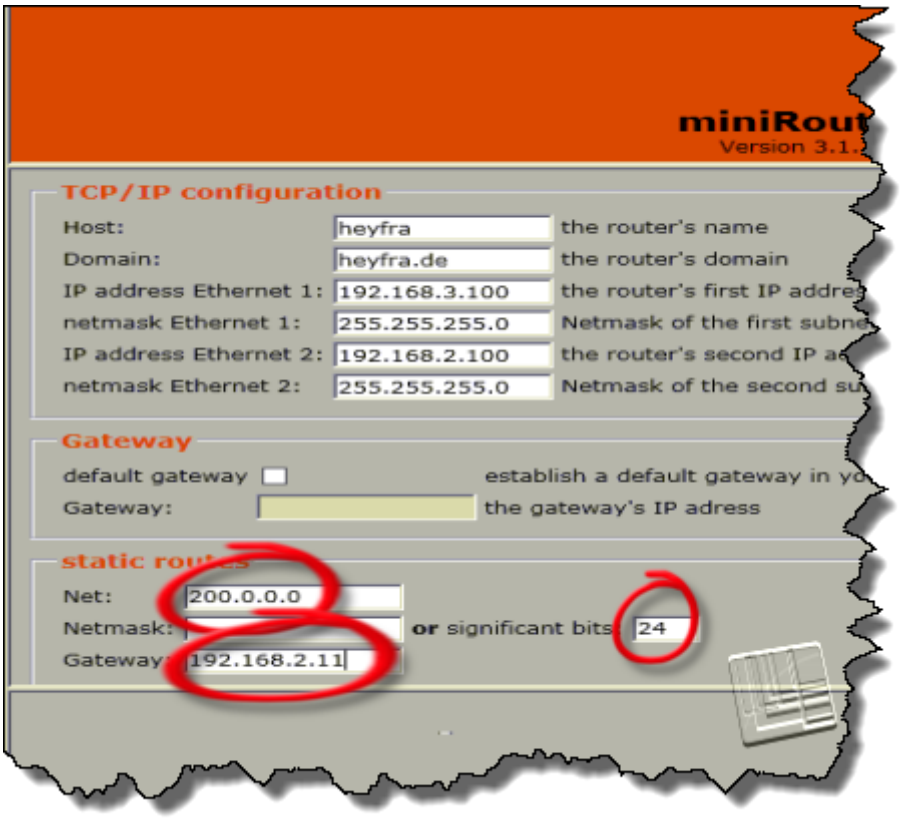
3.2 Checking IP Addresses

Select General-> Base on the menu and verify the two IP addresses. They should be as shown below. Do not change them.



3.3 Adding a static route

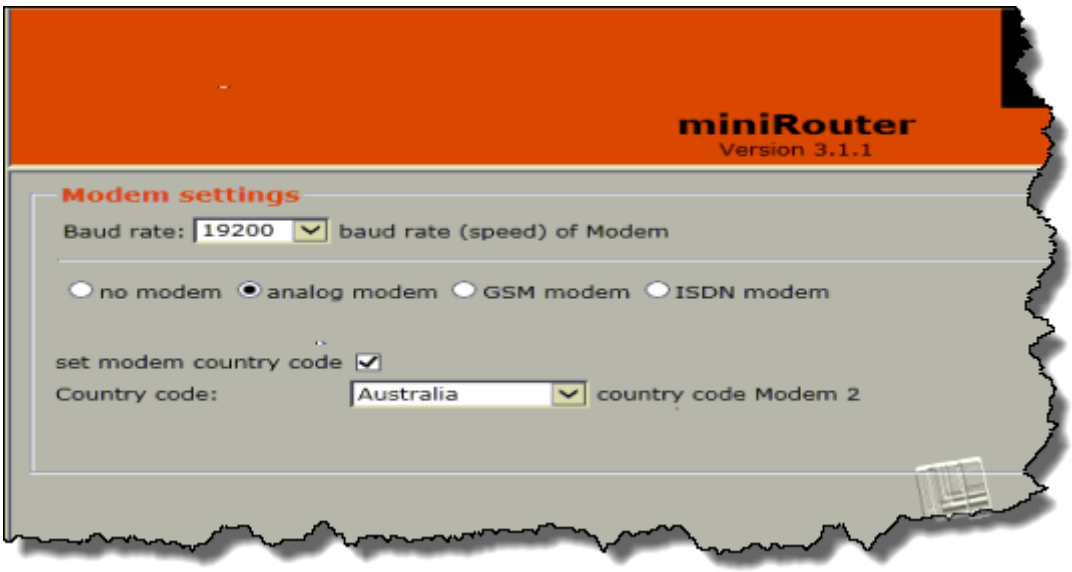
Let's imagine that the netbook (192.168.2.11) is actually a router, and that its other port is attached to network 200.0.0.0 mask 255.255.255.0. We now need to tell the IE-ARM that, if it ever has a packet destined for 200.0.0.0/24, it needs to forward it to 192.168.2.11. This is done on the same menu (General->Base) as shown below.



Do not save!

3.4 Modem Settings

Go to Modemsettings->Modem. Here we are assuming a simple analog modem, running at 19200 baud.



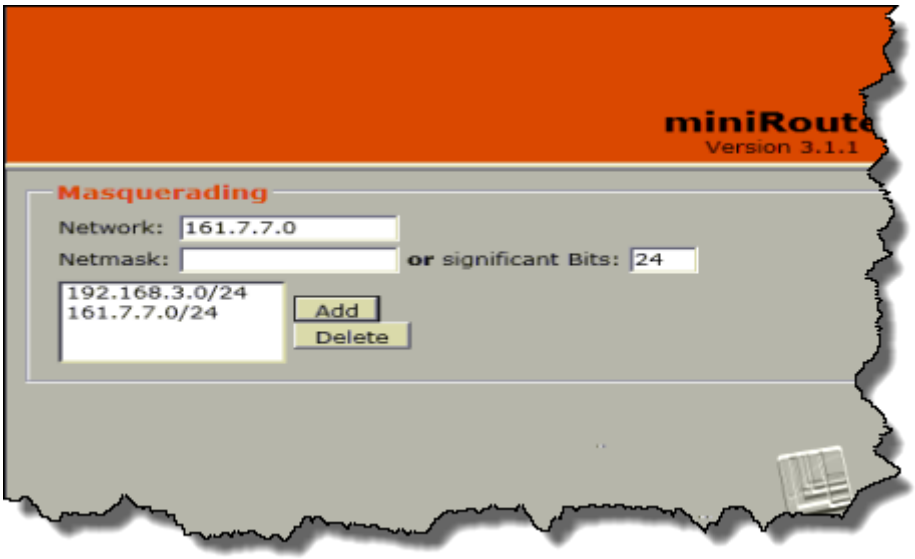
3.5 Basic firewall settings

There are four menus under 'Firewall', viz. Masquerading, Routing Without Masquerading, Trusted Nets, and Port Filter.

(a) Masquerading

This is only a fictitious example as we have set up our IP addresses differently.
Assume that Network 1 is Private (192.168.3.0/24) and Network 2 is not (e.g. 161.7.7.0/24). By masquerading the router will accept packets from Network 1 and replace the IP addresses with 161.7.7.100, where 161.7.7.100 is the router's IP address on Network 2.

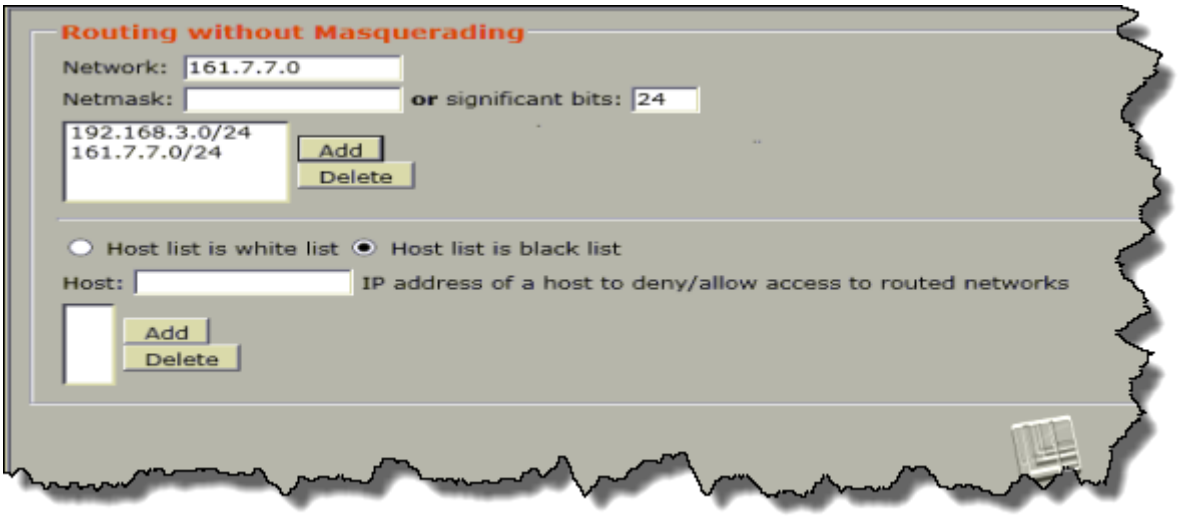
To allow this, select Firewall->Masquerading, select the default networks one-by-one, and delete. Then enter the two network addresses (Note: not IP addresses). The mask can be entered as 255.255.255.0 or 'significant bits' i.e. 24 (as in /24).



Do not save ('apply').

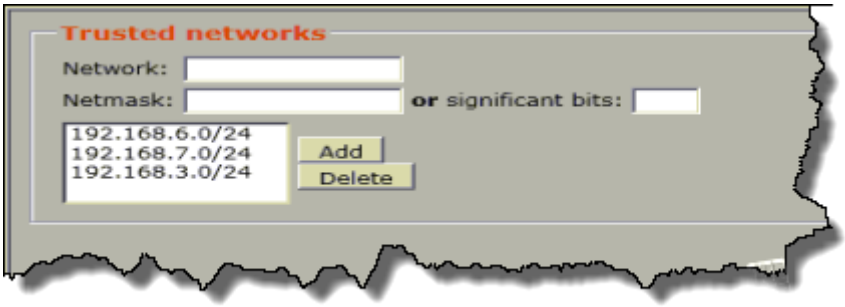
(b) Routing Without Masquerading

This is the same as (a), but as the name implies there is no masquerading. It is also possible ro enter a whitelist (IP addresses allowed access through the router) or a blacklist (IP addresses blocked). A blacklist with no entries means all IP addresses are allowed.



(c) Trusted networks

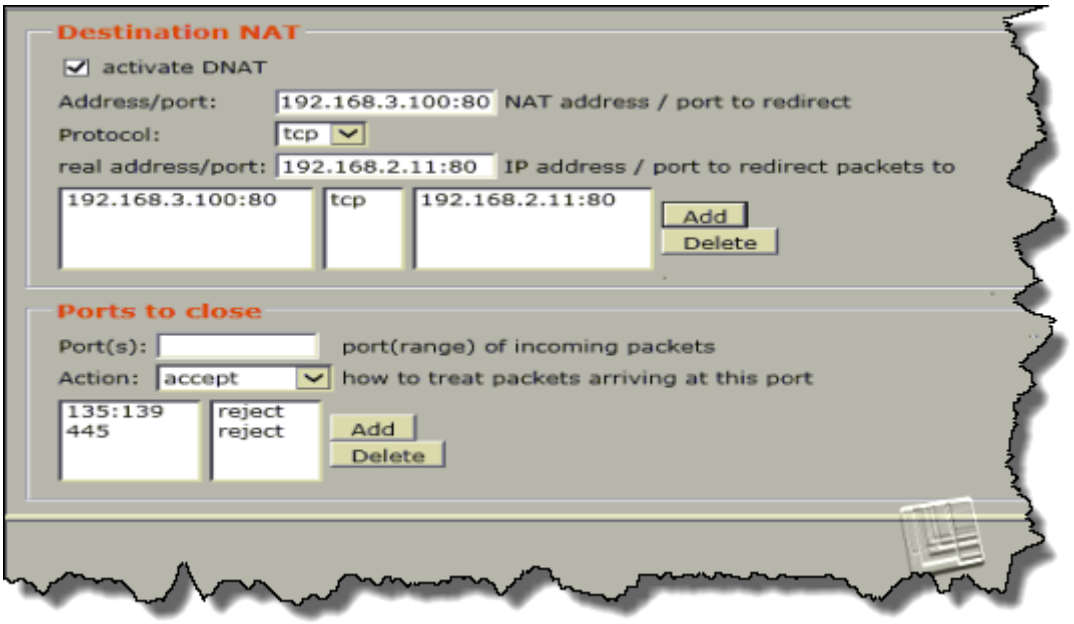
As the name implies this is simply a list of tristed networks. Delete/add as required.



(d) Port filter

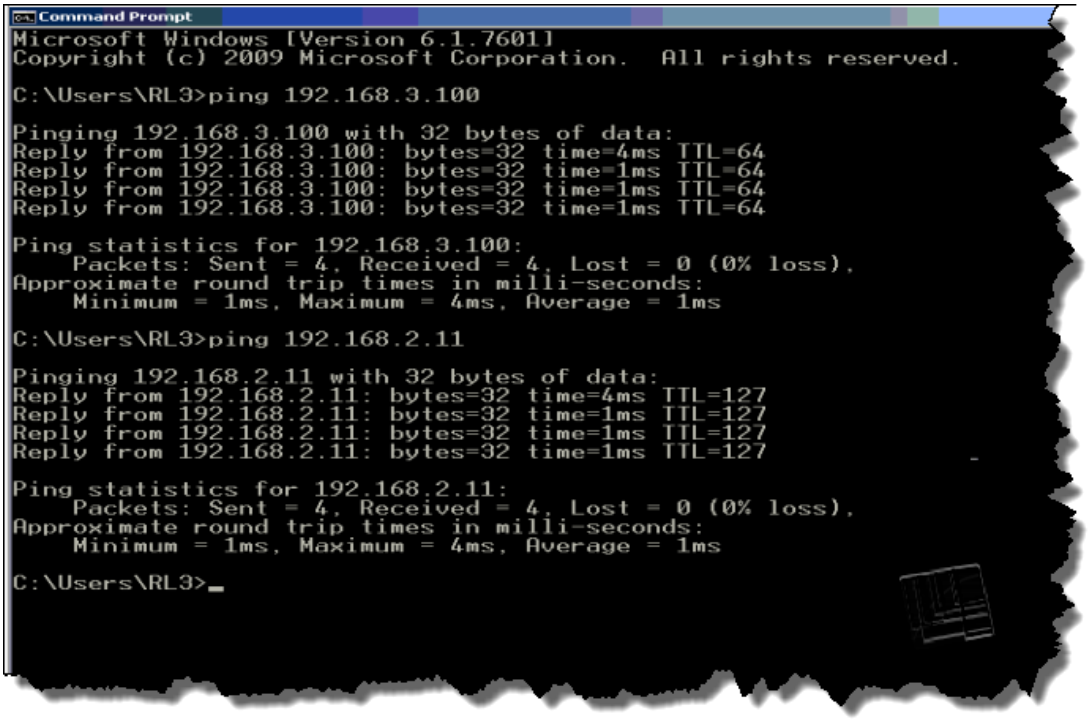
In this example DNAT (port forwarding) is enabled and attempted TCP connections to 192.168.3.100 port 80 will be forwarded to 192.168.2.11 port 80.

In addition ports 135, 139 and 445 will be blocked.



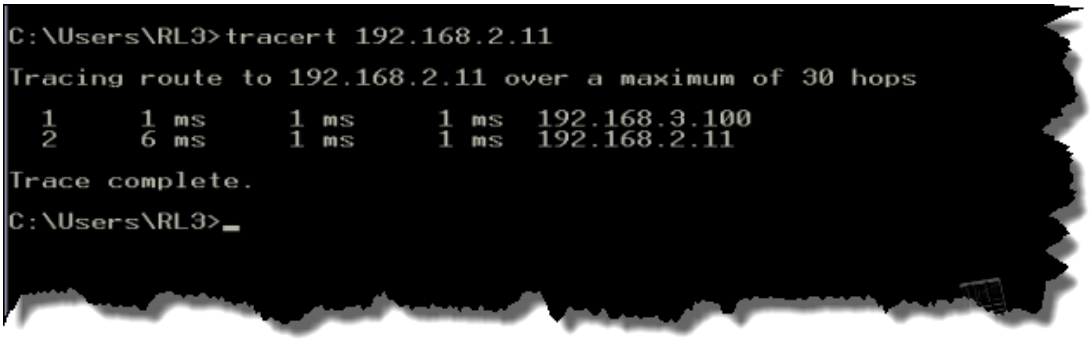
3.6 Pinging and tracing

First ping the port of the router closest to us, and then ping the netbook.



Note the difference in TTL. Apart from the difference in magnitude, the one value equals a power of two while the other equals a power of two minus one. Why is this?

Now do a trace route to the netbook. Does this explain anyting?

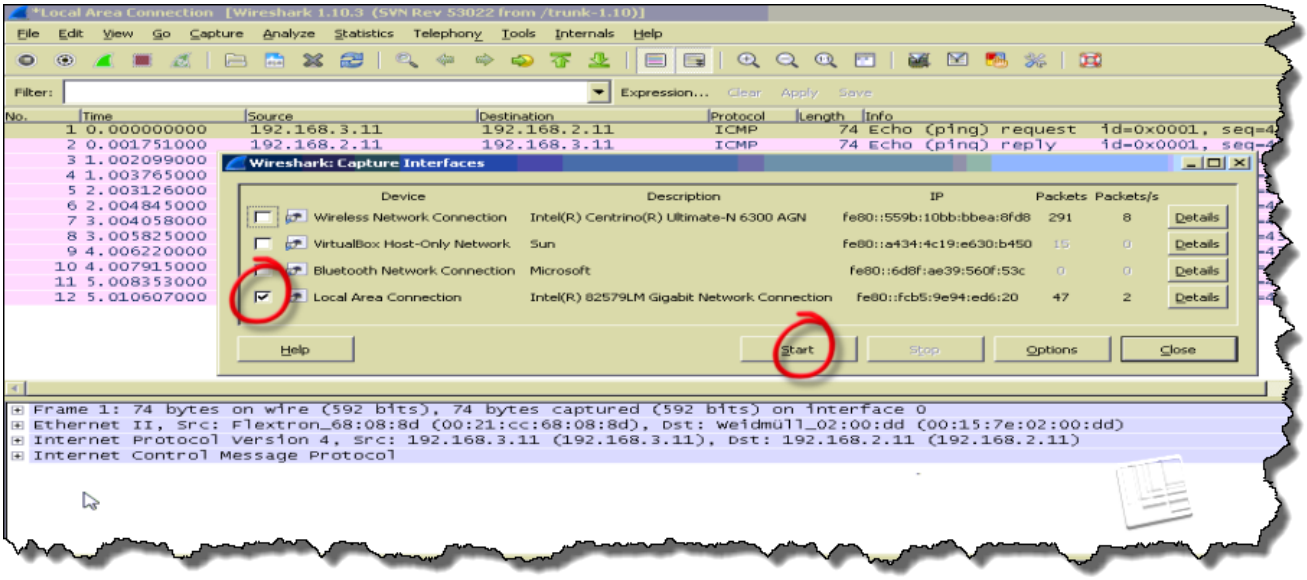


3.7 Packet analysis

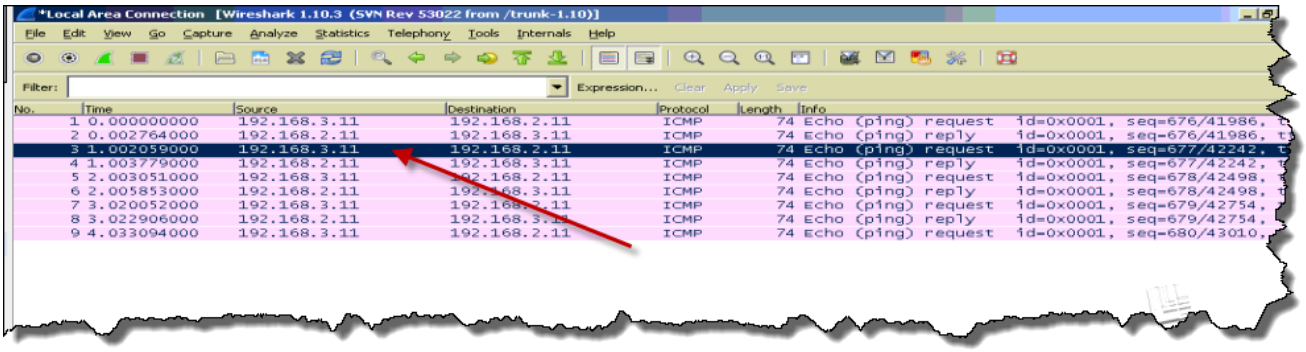
Ping the Netbook repetitively (*ping 192.168.2.11 –t*).

Now run Wireshark.

Click *Capture->Interfaces*, select the Ethernet interface, and click start.



Capture a few packets and then stop. Select one of the Echo Request packets.



Now expand the Ethernet (Ethernet II) and IP (Internet Protocol Version 4) headers, compare the IP/MAC addresses with those shown in section 2, and verify that they match. They do not.

So what is going on here?

END OF EXERCISE