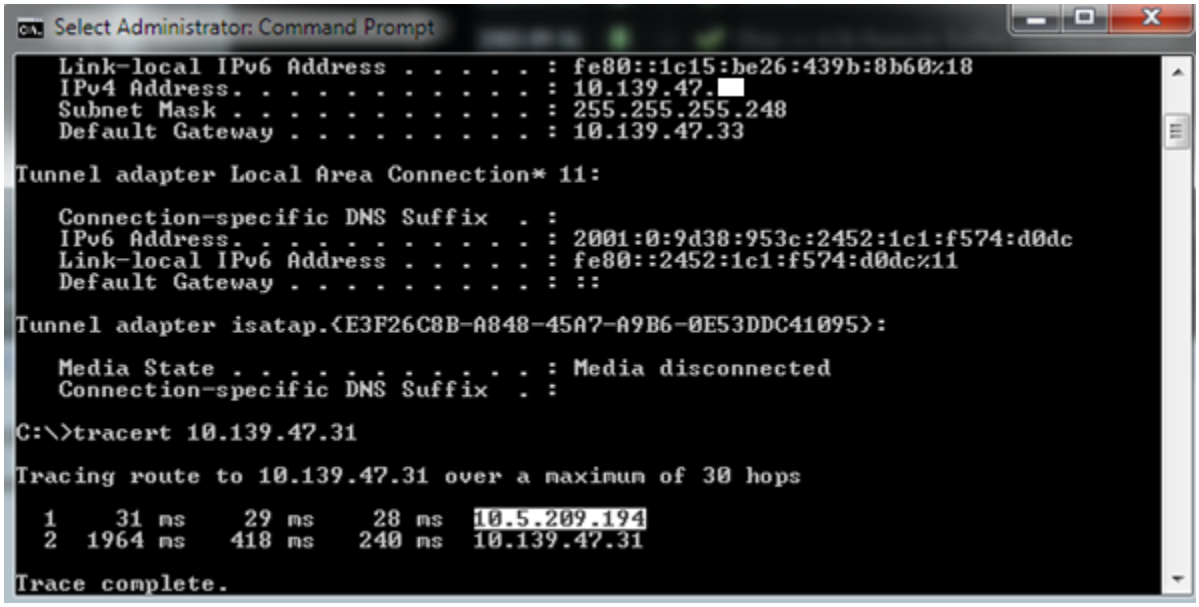
Why Telstra's 4G 'security' is non existent!

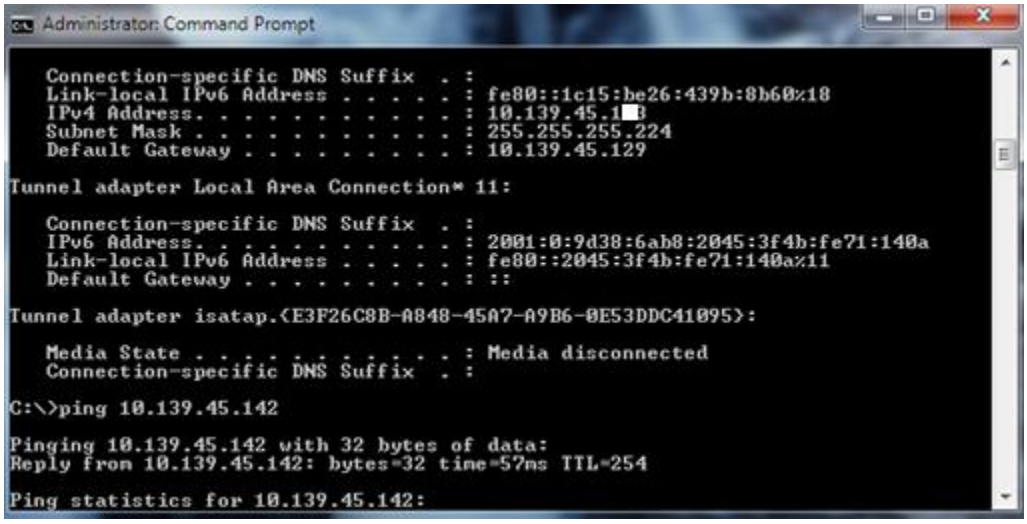
Always use a firewall protecting your 4G link.

Let's begin…
connect to 4G. Command prompt. Ipconfig /all. Please note my own IPs are blotted out just in case.

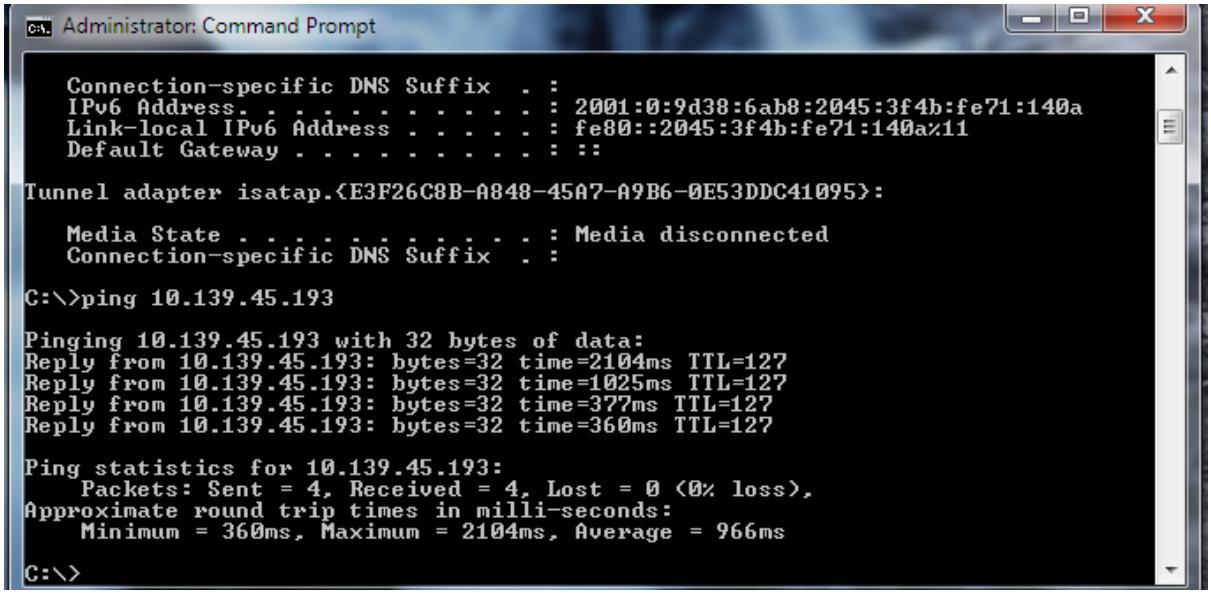


OK so I get an IP from my Telstra 4G USB stick of **10.139.47.xx.**

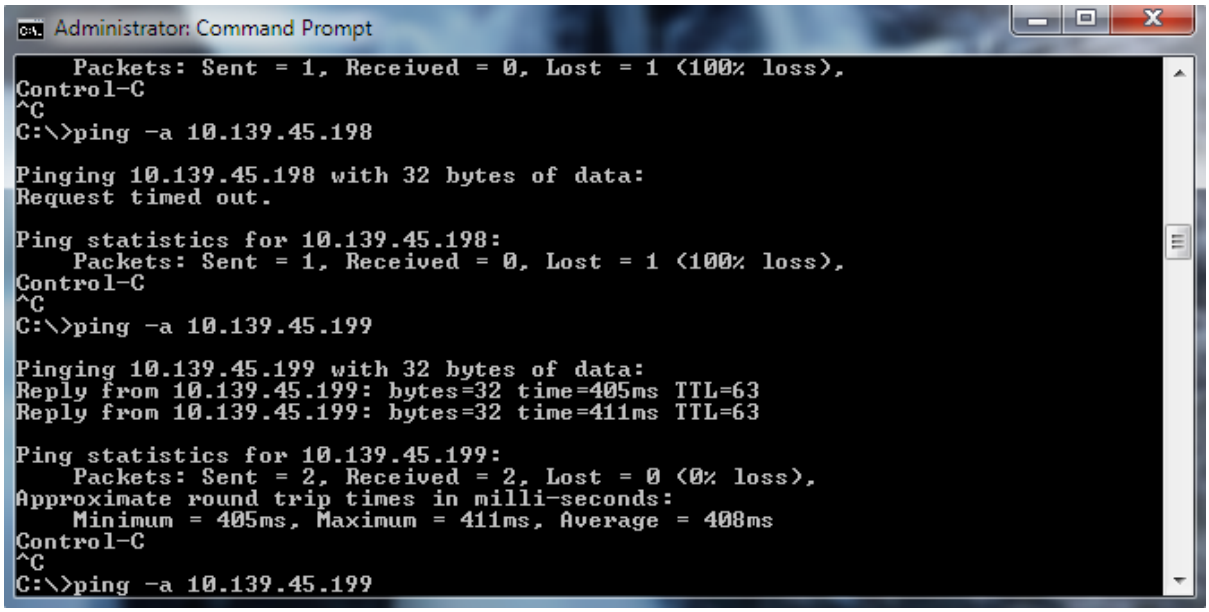
I pinged a random local IP on the same subnet. It was pingable. Then I did a ping –a on that IP. To my horror, I got a returned host name of RAYLENE-PC. I suspect another Telstra 4G customer with no firewall up. Yuck. I disconnected, and reconnected and got a new IP, and repeated the test. More pingable IPs on my subnet. I tried this a few times with different IPs and subnets, same results. On my 4th try or so I thought I better document this – I get the 10.139.45.xxx IP and 255.255.255.224 subnet giving me direct IP access to 30 other customers machines (30 IPs.) Lets do some pings. **First IP I try returns the ping**. Some other 4G user without firewall preventing ping. My ipconfig is shown here and the first IP returning the Ping.



Lets try some more IPs. I renew IP again and this time I'm on 10.139.45.xxx (higher than last IP though). I'm on a .224 subnet again though…our host range on this subnet includes around 30 IPs.



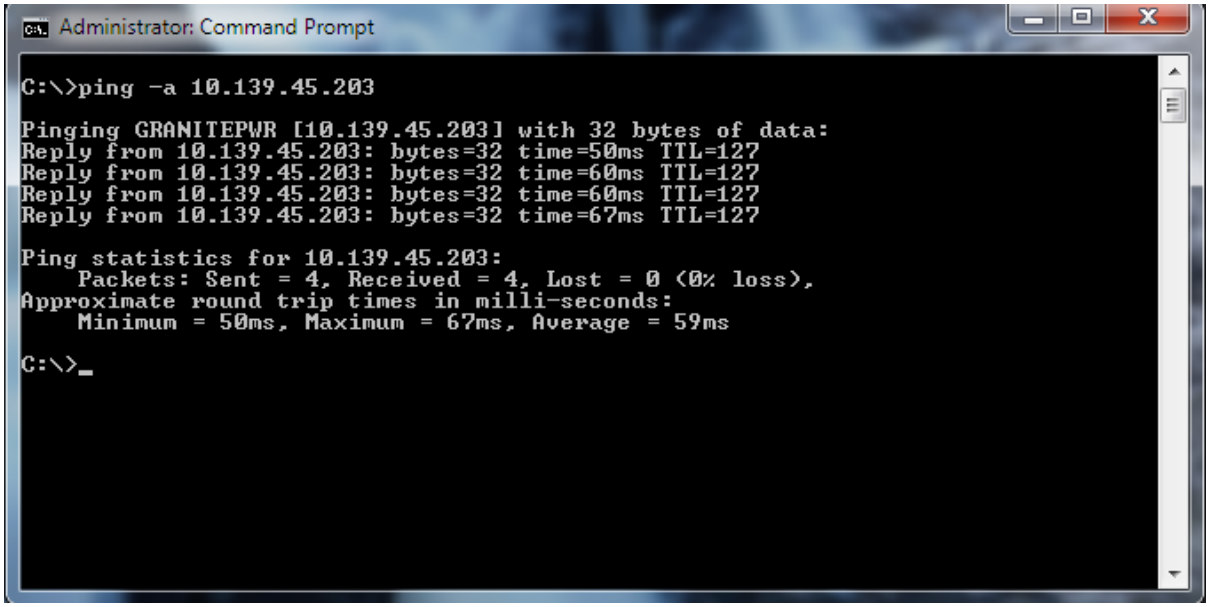
Uh oh they ping too. Even the first in the range (.193). Looks like we now have direct IP access to around 30 bigpond customer's PCs or servers etc. Lets do some investigating and see if we can ID one at least. Our host range here, due to Telstra's subnet configuration, is 10.138.7.193 – 10.138.7.222.



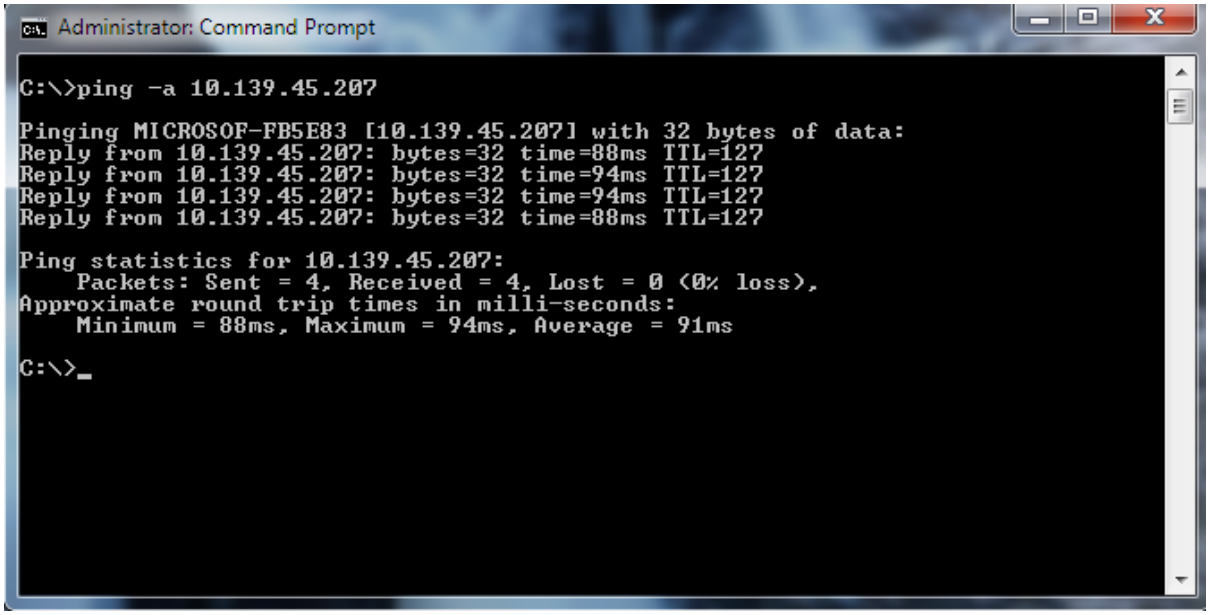
Well…I'm through the first 6 or so IPs. 5 have returned my pings. Ouch. A port scan on those IPs would have likely located a way in via multiple vulnerable services (in my experience). Anyway im still hunting for an unprotected windows box like the RAYLENE-PC I found earlier.

Doesn't take me long….

We're only 5 more hosts in! … Here's an unprotected Windows box, probably a server or home workstation, on a nice fast link. With a little playing right now I could take full control of this machine whether its running almost any windows version. Bigpond customers would probably not like this situation.



gulp. Didn't take me long to find another one either…..



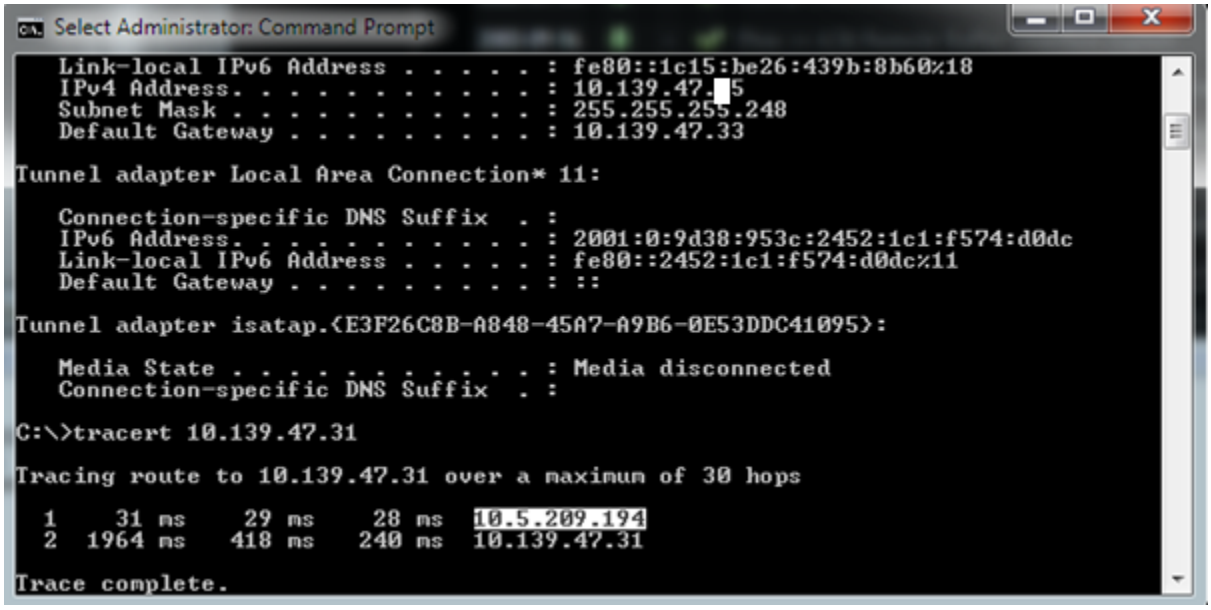
Im only 14 hosts in and ive found two already. Im going to stop now.

The reason this is happening? Telstra's subnet configurations. Some of the time, when you connect your 4G, you get a nice tight restricted .252 subnet. You can't get to anyone else's computer. That's great. Except for the other times (over 50%) you get a .224 or other subnet, giving you direct IP access to a wide range of other customer's computers. This would be OK if the routing between them, via the Telstra FreeBSD we examine in the next few pages, had firewalling or at least port restrictions, but it doesn't. Anyway lets check out what's doing this dodgy routing.

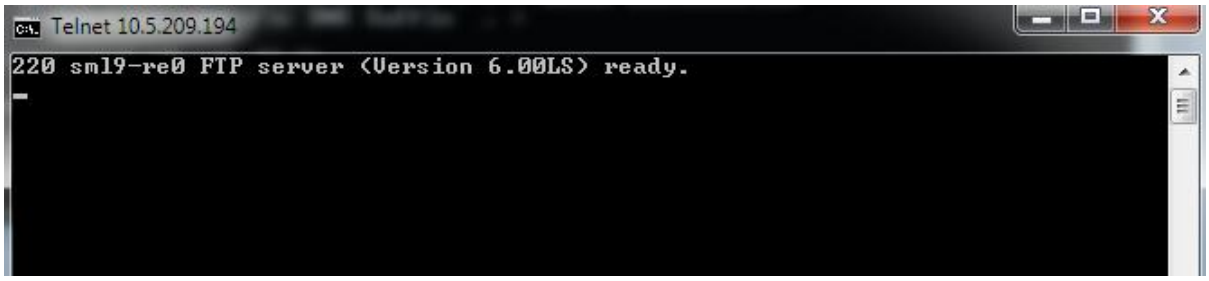
OK. So their client security sucks. No firewalling between nodes. No VLAN separation. Let's investigate the actual security of the service! Bad news….

OK, so when I tracert my path to these 'local' subnet IPs I've been pinging above, I'm actually being routed through what I assume is a Telstra machine. More digging is required. What is my traffic going through? And why isn't it restricting me…

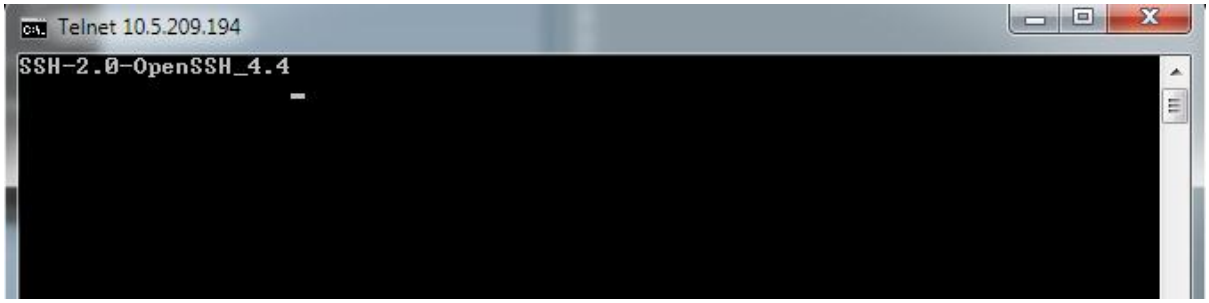
Let's see. I tracert to any other IP to see what server I go through. I then repeat this same test more than 10 times – its ALWAYS this exact IP/machine doing your routing. Interesting.



I do some probing.
Port 21 is open -



I'm suspecting FreeBSD linux at this point. (Version 6.00LS seems to be ftpd or ProFTPd from FreeBSD).
SSH is open (port 22)



Worse yet, it's a version of openSSH (4.4) that is both old , and quite vulnerable,

with numerous information disclosure vulnerabilities in the public domain, as well as published exploit code including a remote exploit to retrieve kernel memory complete with (one would assume, given a few attempts) password hashes and other very useful information.

At this point I decide to stop and report this to Telstra. This is terrible security for a wireless network. I won't list in here the actual CVEs or ways you could sit there and try and take advantage of that. It's pretty obvious. The important thing here is to ensure you follow these…

I consider blotting out the IP addresses in this release. However anyone with a 4G link and about 10 minutes of online learning about IP networking can easily figure absolutely all of this out! It is already clearly common knowledge totally unprotected by Telstra and this should be fixed and people should at least be aware of this.

Resulting Recommendations:

a. Run a personal firewall and ensure your Telstra 4G wireless connection's actual IP is being actively protected.

b. Disable services on your local PC like remote desktop, VNC, file sharing, if you are only using your 4G connection to access the internet and are not on a network performing sharing. If you are on a network, ensure your shared services are made available only on your wired LAN or wireless LAN card's IP addresses. The configuration required for this differs widely between operating system and software so either engage an expert or take the securest / safest option and disable it.

c. Consider your PC part of a shared connection to the internet and take steps to secure aspects of your computer e.g. passwords, what is stored on it, etc.

Anonymous