

Durban Wireless Community War drive – 24th February 2007

Results prepared by Donald Jolley

We did a short drive for about 45 minutes in opposite directions from Umbilo. One team when south via Montclair and along to the Bluff while the other went via Cato Manor (don't ask) brickfield road to Springfield park and then back along ridge road.

Team one picked up 150 Networks while team two picked up 250 networks and failed to save their results. Idiots!

Big Drive

We then charged up the laptop a bit more and then headed for the big drive. We used Kismet running on a HP Intel P4 laptop with a live linux distro. The radio was a Senao 100mw PCMCIA 802.11b with a 12db patch antenna.

It took us along Umbilo road right into Berea road along West street and right into Stanger (or there about) and right into Smith street back into Berea Road and right in botanical gardens / cowey road. Straight through to Argyle. Right into argyle left in Florida, all the way up and right into Innes, left into Windermere, right in Goble. Left into NMR right toward Blue Lagoon, left on the M4 freeway.

Took the La Lucia Mall off ramp. Right into Armstrong up to the top traffic circle right into Umhlanga rocks drive and over the M41 bridge around the back of gateway, across the Millennium bridge a bit of a drive around in that area and then back onto the M41 and on the N2 southbound freeway. Left onto N3 east bound tollgate bridge turn off right over the bride up south ridge, left into Moore, right into clever/bulwer road along into Nicholson homeward bound. It took about 1 hour and 20 minutes.

DISCLAIMER!!

As this was just a fun exercise, the results have not been double checked and will not be unless someone wants to point out something. Percentages may not add up to 100%... tough! The idea of the drive was purely for information purposes and the notes are just opinion. You are welcome to use these findings as you please however it would be nice if DWC was mentioned (any quoted information should have the source linked to it anyway) DWC (Durban Wireless Community) is certainly not the definitive source of wireless information in Durban so these results should be used with caution. Now that that is out the way!

Result of the big drive:

293 – No Encryption of which 5 showed up as default (eg they didn't even change the passwords)

308 – WEP Encryption

156 – WPA Encryption

757 – Total networks

Percent ages

Not encrypted – 38.70% (Default – 0.66 % included)

WEP – 40.69%

WPA – 20.61%

Channel usage

0 – 56 7.4% (could not determine, eg probe or channel hopping networks) -

1 – 126 16.65%

2 – 14 1.85%

3 – 16 2.11%

4 – 25 3.30%

5 – 5 0.66%

6 – 234 30.91%

7 – 38 5.02%

8 – 21 2.77%

9 – 7 0.92%

10 – 20 2.64%

11 – 187 24.70%

12 – 1 0.13%

13 – 6 0.79%

Notes about this drive

There is a ton of networks in Durban's CBD. It would make sense then that as the number of wireless 2.4Ghz networks grows so does the noise levels making link quality worse. As a community we have noticed this over the last year that there has been a huge decline in our 2.4Ghz link quality.

119 of the networks found had the ESSID of Marconi (default ESSID for Telkom wireless ADSL router) all had at least WEP enabled. This is fairly promising as at least there is some out the box protection.

Many of what looks like Wireless ISPs do not have encryption on their networks or parts of their networks. This is a little disturbing as there is business information running across those links. Eg emails with usernames, passwords and IP addresses of the mail servers making it easy for undesirables to gather information on companies.

Many of what can be assumed to be hotspots don't offer any sort of encryption. While this is a general practice as it makes it difficult to manage, I believe that it should be noted and people that choose to use these hotspots should take other security precautions such as using secure protocols eg SSH and HTTPS or a secure VPN.

We captured enough packets** for 34 networks to determine the IP addresses therefore would be able to guess the IP range they use. We travelled way to fast to capture any meaningful data however even with a driveby we were able to pick up a POP3 account username password and public IP address.

Best ESSID name – Sliced Cheese 😊

Summary

There has been a definite increase in 2.4Ghz in the past year. This really goes without saying.

It is pleasing to see that there are many more encrypted networks then our previous drive about a year ago. There is definitely a tendency that there is encryption on in the business areas. Saying that there are still unprotected Business networks out there. I do believe that sometimes this is intentional as those wireless Access Points do not connect to the corporate network.

Combined results from team one and main drive

Note the duplicates have been taken out. Duplicates were based on BSSID (Mac address)

341 – No Encryption of which about 10 showed up as default (eg they didn't even change the passwords)

362 – WEP Encryption

185 – WPA Encryption

888 – total networks

Percentages

Not encrypted – 38.40% (Default – 0.66 % included)

WEP – 40.77%

WPA – 20.83%

Sorry don't feel like doing the channel stats

Interesting to note that the encryption percentages are almost the same.

Any comment, suggestions, flames, well dones. please post on the DWC forum at <http://www.dwc.za.net/phpBB2/index.php>. If you don't want the comment to be public please feel free to email me at donald@dwc.za.net . A thanks to all the people that helped and had fun on the day.

**If in the same place for long enough and there is a large number of data packets it is possible to identify the IP address.