Open WLANs
the early results of WarDriving

Peter Shipley
shipley@dis.org

The Project

The purpose of my project is to raise the awareness of the security ramifications arising from the use of wireless Lans (WLAN) in the home and office community.

Network Security and Wireless Lans

- The convenience and low cost of WLANs has resulted in their deployment at a feverish rate.
- This is very similar to the Web race a several years ago.
- Sadly this deployment has brought security back ten years.

Hardware

- “low end” Laptop with FreeBSD –stable or Windows 98
- External Antenna (>5db)
- GPS (Garmin eMAP)
- Lucent /Aironet 802.11 (Wi-Fi) card

Software

- “wi-scan” – perl script for FreeBSD
- Netstumbler – a Windows App.
- dStumbler – A FreeBSD App. (beta)

The native drivers for cards can also be used although the operation will not be as automated.

Detection Methods

Currently the WLANs are being detected with a 802.11 feature called “broadcast SSID” or “Null SSID”.

The Lucent card supports this feature that when you to set your SSID to (null) or “ANY” the card will detects a AP’s beacon and automatically associate with it.

Detection Methods

Currently I run a script that resets then polls the card every three to five seconds.

When a new WLAN is detected the script notes the SSID, Mac address, signal strength, channel, location (via. GPS) and security configuration.

Detection Methods

Currently we can drive at speeds of up to fifty-five miles a hour and successfully locate and identify wireless networks.

Long Distance ?

Some security officers feel that if AP is distanced from the street or on a high floor of a building they will be safe from network trespassers.

Experiments show that we are able to successfully make a network connection twenty-five miles away from hilltops and high-rise buildings.

The view from a hilltop in Berkeley.

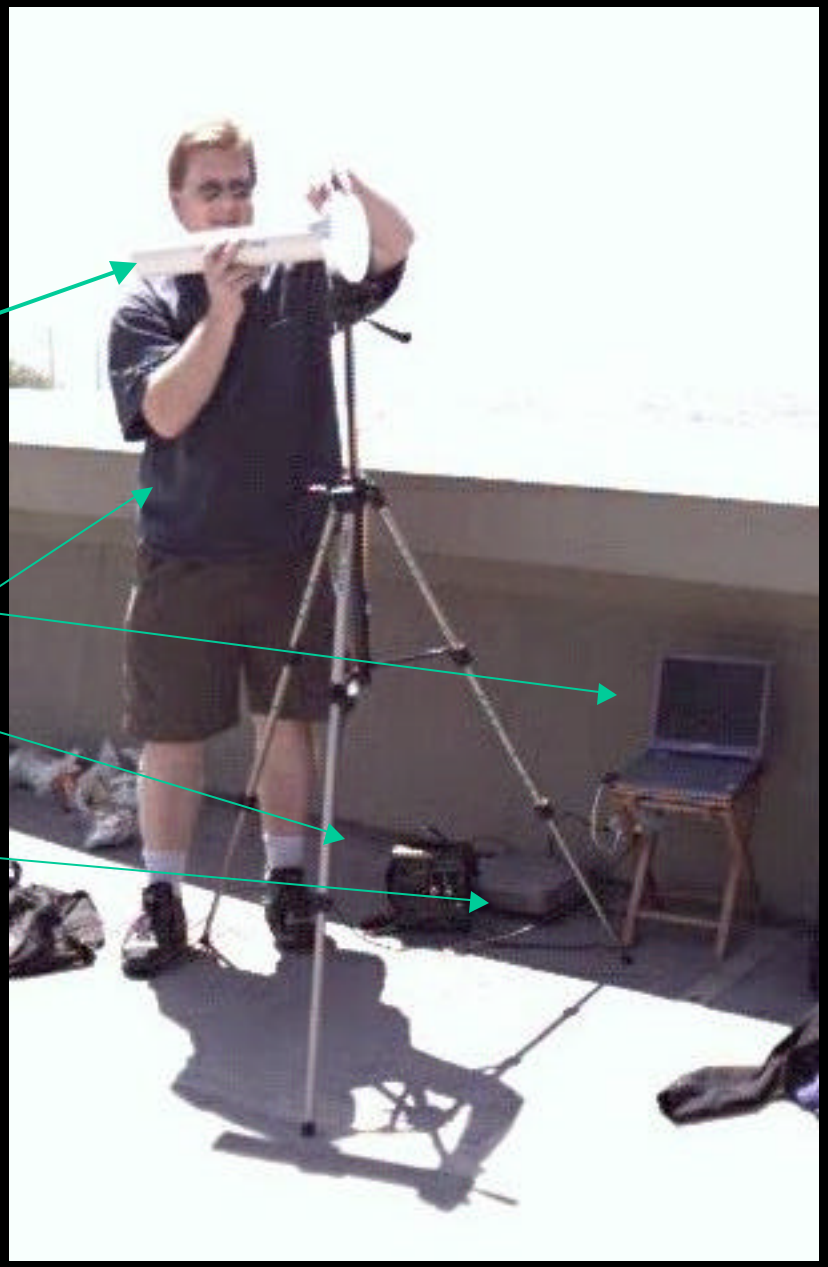
Hardware

Connecting to WLANs networks from across the bay.

24db dish connecting to a network on the horizon!

Hardware

- 15 db Yaggi
  - Laptop
- Portable power
- Amp
- Wyatt



Other Methods

Other methods include sniffing 802.11 frame this will all for more efferent and faster detection including more information about the Lan.

Sniffing can be done with most WLAN cards and the right software.

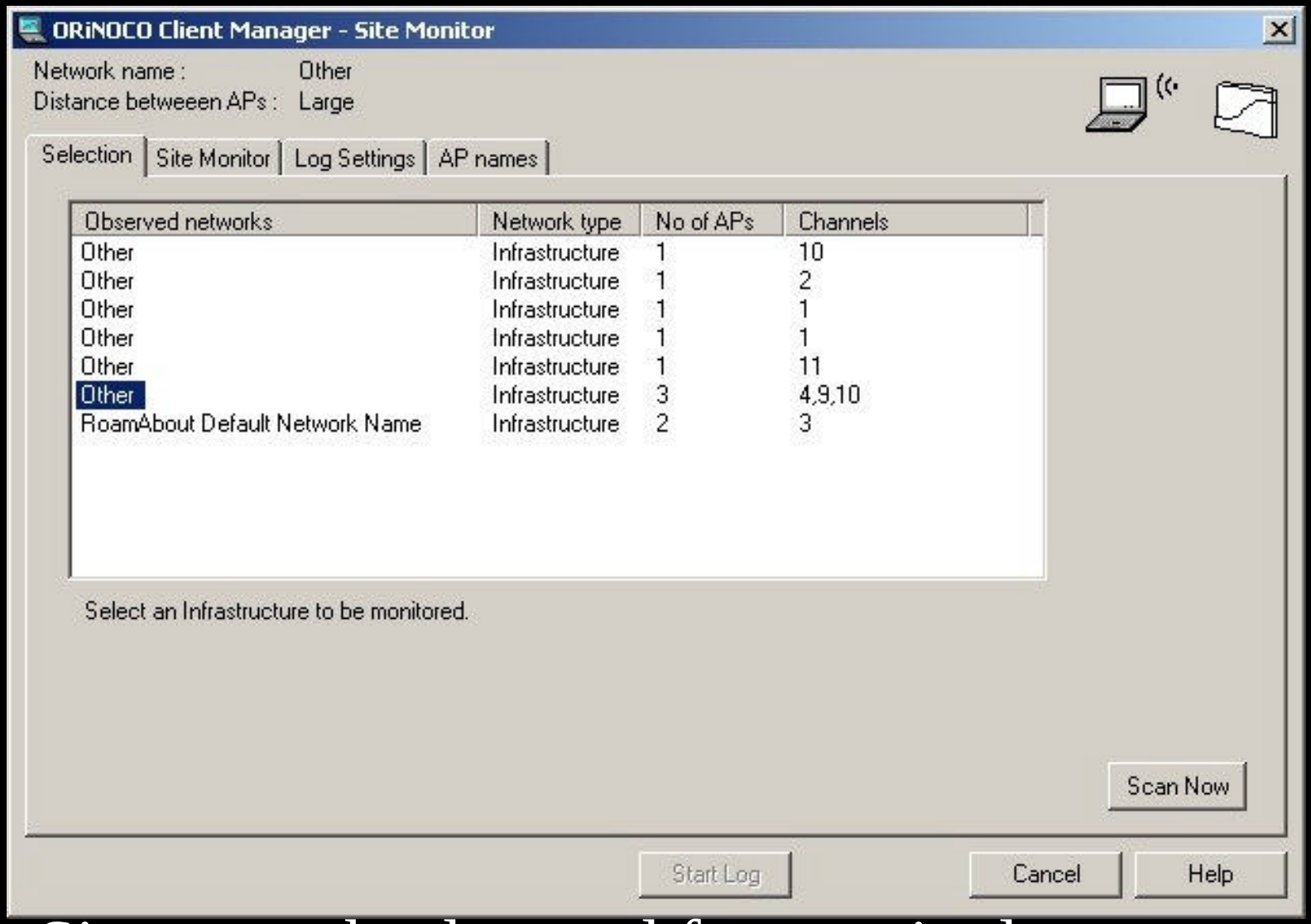
Detection Methods

Anyone can do this with a Windows based laptop and Wi-Fi card.

Detection Methods

Run the Client Manager software and set your SSID to “ANY” or (null).

Next from the “Advanced” menu of Client Manager and select “Site Monitor” a window should open listing all the local WLANs that are available from where you are standing.



Six networks detected from a single street corner in downtown San Francisco.

Detection Methods

The previous slide was taken from a street corner in downtown San Francisco.

Note that you have your choice of six networks open for access!

Statistics

We are still in the process in distilling the data

Currently we have located over 9000 APs.

- 60 % of APs are run in their default configuration.
- Majority are connected to a internal backbone network (not a DNZ).

Statistics

- A majority of these (85% or more) do not utilize WEP.
- Of those running WEP, near half utilize a default WEP/encryption key.

Statistics

Top SSIDs:

13%	tsunami
11%	AirWave
10%	WaveLAN Network
8%	WLAN
5%	linksys
2%	default
2%	TEKLOGIX

Statistics

Based on SSIDs and IP address it appears that over 60% of AP are running with a default configuration.

Risks

Not just personal and corporate LANs are going wireless:

- Banks
- Hospitals
- Legal firms
- Police Stations/Jails
- City hall/Municipal

Risks

This places people personal information at risk.

Home Networks

The risks to home users are greater then simple bandwidth theft.

Violations of Term of Use:

- SPAMing
- Hacking
- Anonymous threats

Violations can result in loss/disconnection of service

Corporate Networks

Failure to protect your network can result in costly headaches

- SPAMing
- Hacking
  - providing a starting point
  - Unrestricted internal access.
- Theft of corporate information
- Lawsuits
  - Failing to protect stockholders interests

What is “Free”

There are are growing number of free networks in parks, coffee shops and libraries.

How can you tell if a network is free?

Accidental Trespassing

If you are at a coffee shop that offers free wireless internet access it is possible for your client to “drift” and associate with a corporate LAN.

Making ***you*** unknowingly guilty of cyber trespassing.

Accidental Trespassing

There are already documented cases where to neighboring businesses with wireless had employees unknowingly using each others networks.

What is these companies were unfriendly competitors?

What can be done?

- Place APs in a DMZ
  - Place Access Points on a dedicated subnet.
  - Block unauthorized internal and external access.
- WEP
  - Stops “accidental trespassing”.
  - Some cards will not “associate” with out the correct key.

What can be done?

- IPSec
  - WEP will not protect your data.
  - Require clients to authenticate with the DMZ firewall/router.
- Arpwatch
  - Discovers new MAC addresses on your network.
- 802.1x
  - New protocol, not well supported / tested.

What can be done?

- Locking your AP to known MAC addresses
  - This only slows the attacker (a few seconds)
  - Stop accidental trespassing
  - Even with WEP the MAC address can still encrypted.
- Turn off “beacons”
  - This will stop you network from being discovered with simple probes.
  - Your network will still be visible to sniffers and protocol analyzers.

Credit due

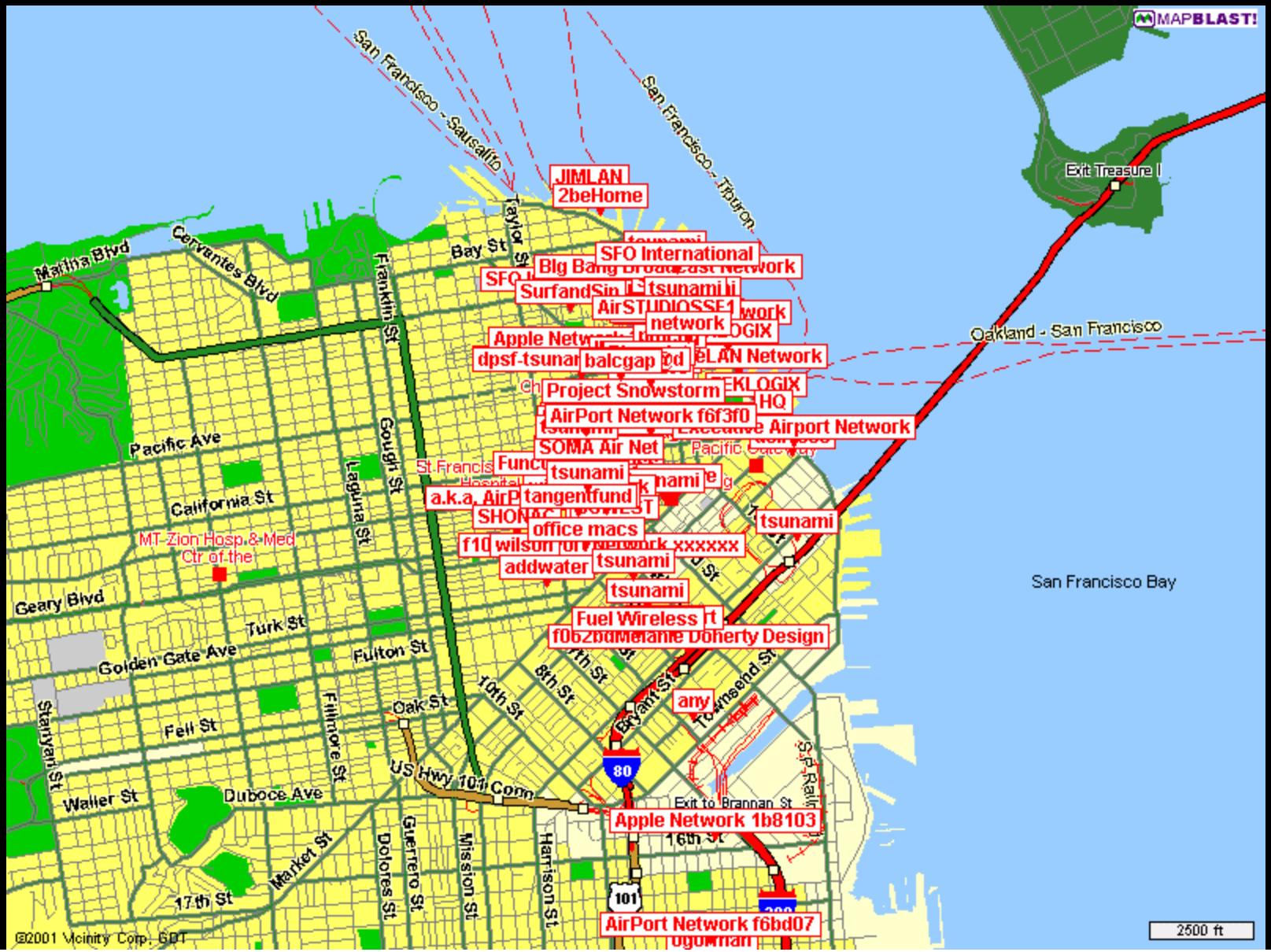
- Matt Peterson -Hardware questions
- Aaron Peterson (no relation) - Data processing scripts
- Cal -Linux support
- Wyatt -Misc. hardware fabrication
- Bay Area Wireless Users Group
- DoC: Dis Org Crew

Maps

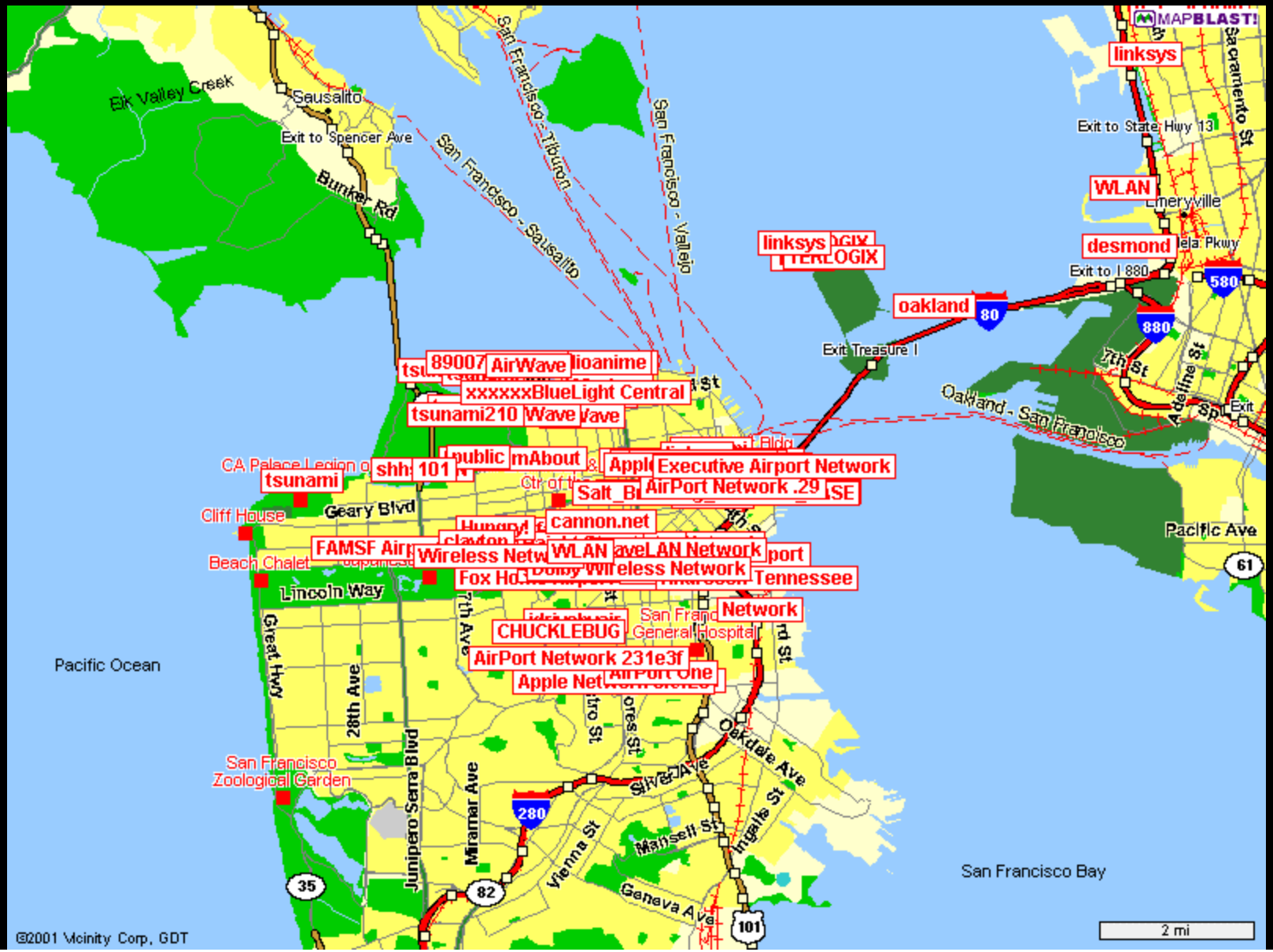
Here are some maps of the data we have collected on the open networks.

Downtown San Francisco

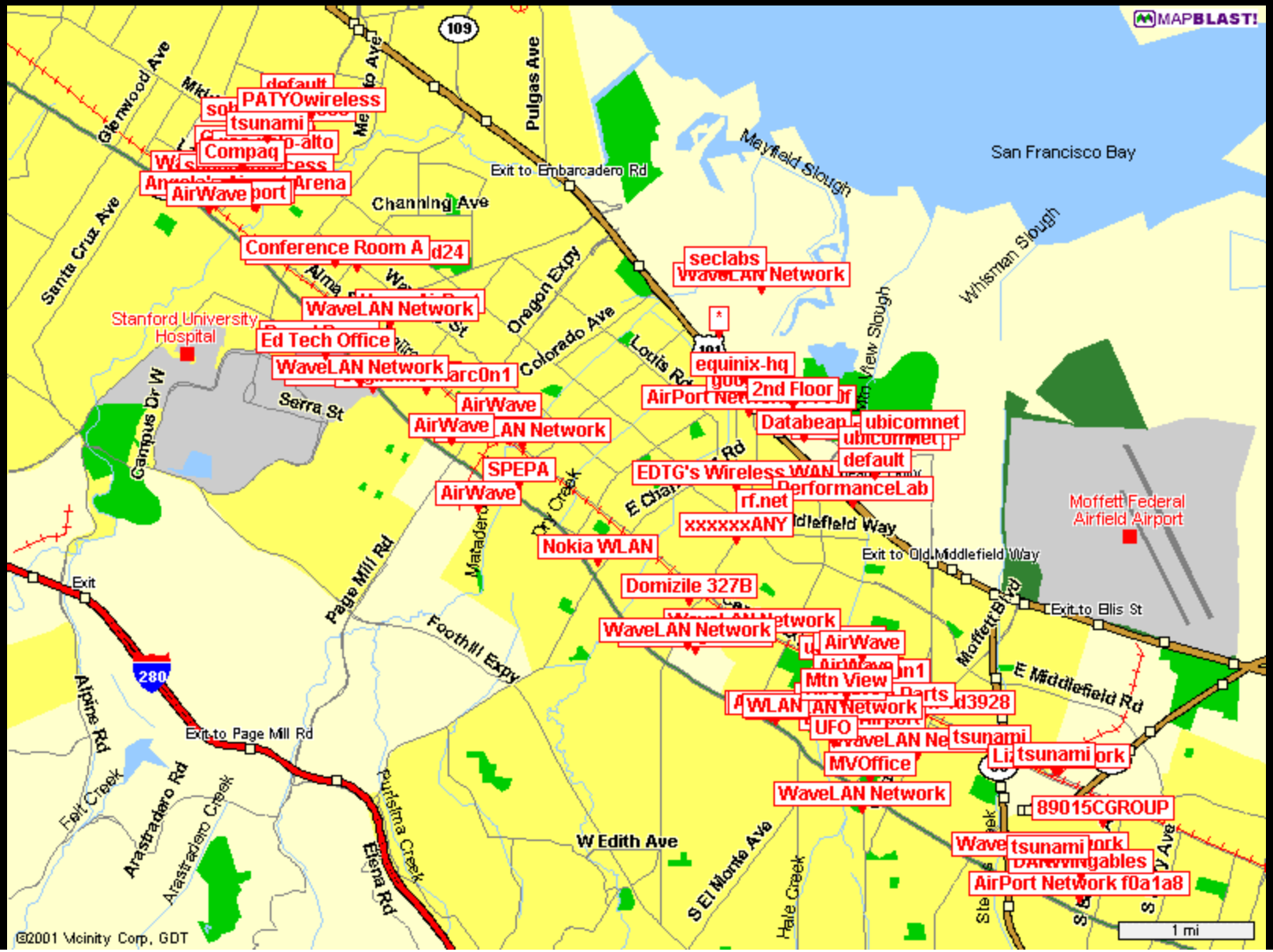
Downtown San Francisco



San Francisco & East Bay



Sunnyvale & Mnt. View



References

- Bay Area Wireless Users Group
  www.BAWUG.org
- Dis.Org Crew info files www.dis.org/filez
- NetStumbler.com: www.netstumbler.com wireless news and references
- IEEE : www.ieee.org 802.11 standards
- Arrl: www.arrl.org antenna design info.

Peter Shipley
+1 510 849 2203
Shipley@dis.org