Foundstone
A division of McAfee

The Safety Dance: Wardriving the Public Safety Band

Robert Portvliet
Brad Antoniewicz

About Us

Rob

Brad

Robert.Portvliet@foundstone.com
Brad.Antoniewicz@foundstone.com

WHAT DOES IT ALL MEAN?

Code of Federal Regulations

47

Parts 0 to 19

Revised as of October 1, 2010

Telecommunication

Containing a codification of documents of general applicability and future effect

As of October 1, 2010

With ancillaries

Published by the Office of the Federal Register National Archives and Records Administration

A Special Edition of the Federal Register

Communications Act of 1934

COMMUNICATIONS ACT OF 1934

provide for the regulation of interstate and foreign communication by wire or radio and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

TITLE I--GENERAL PROVISIONS

SEC. [47 U.S.C. 151] PURPOSES OF AND CREATION OF FEDERAL COMMUNICATIONS COMMISSION.

The purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex, a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense, for the purpose of promoting safety of life and property through the use of wire and radio communication, and for the purpose of securing a more effective execution of this policy by centralizing authority heretofore granted by law to several agencies and by granting additional authority with respect to interstate and foreign commerce in wire and radio communication, there is hereby created a commission to be known as the "Federal Communications Commission," which shall be constituted as hereinafter provided, and which shall execute and enforce the provisions of this Act.

SEC. [47 U.S.C. 152] APPLICATION OF ACT.

(a) The provisions of this act shall apply to all interstate and foreign communication by wire or radio and all interstate and foreign transmission of energy by radio, which originates and/or is received within the United States, and to all persons engaged within the United States in such communication or such transmission of energy by radio, insofar as such jurisdiction and regulation shall be exercised by the Commission as hereinafter provided, but shall not apply to persons engaged in wire or radio communication or transmission in the Canal Zone, or to wire or radio communication or transmission wholly within the Canal Zone. The provisions of this Act shall apply with respect to cable service, to all persons engaged within the United States in providing such service, and to the facilities of cable operators which relate to such service, as provided in title VI.

(b) Except as provided in sections 223 through 227, inclusive, and section 332, and subject to the provisions of section 301 and title VI, nothing in this Act shall be construed to apply or to give

1

PROCEED WITH CAUTION!

Code of Federal Regulations

47

Parts 0 to 19

Revised as of October 1, 2010

Telecommunications

Containing a codification of documents of general applicability and future effect

As of October 1, 2010

With Ancillaries

Published by:
Office of the Federal Register
National Archives and Records Administration

A Special Edition of the Federal Register

COMMUNICATIONS ACT OF 1934

AN ACT To provide for the regulation of interstate and foreign communication by wire or radio, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

TITLE I--GENERAL PROVISIONS

SEC. 1. [47 U.S.C. 151] PURPOSES OF ACT, CREATION OF FEDERAL COMMUNICATIONS COMMISSION.

For the purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex, a rapid, efficient, Nationwide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of national defense, for the purpose of promoting safety of life and property through the use of wire and radio communication, and for the purpose of securing a more effective execution of this policy by centralizing authority heretofore granted by law to several agencies and by granting additional authority with respect to interstate and foreign commerce in wire and radio communication, there is hereby created a commission to be known as the "Federal Communications Commission," which shall be constituted as hereinafter provided, and which shall execute and enforce the provisions of this Act.

SEC. 2. [47 U.S.C. 152] APPLICATION OF ACT.

(a) The provisions of this act shall apply to all interstate and foreign communication by wire or radio and all interstate and foreign transmission of energy by radio, which originates and/or is received within the United States, and to all persons engaged within the United States in such communication or such transmission of energy by radio, and to the licensing and regulating of all radio stations as hereinafter provided; but it shall not apply to persons engaged in wire or radio communication or transmission wholly within the Canal Zone, or to persons engaged in such wire or radio communication or transmission wholly within the Canal Zone. The provisions of this act shall apply with respect to cable service, to all persons engaged within the United States in such service, and to the facilities of cable operators which relate to such service, as provided in title VI.

Except as provided in sections 223 through 227, inclusive, and section 332, and subject to the provisions of section 301 and title VI, nothing in this act shall be construed to apply or to give

Robert.Portvliet@foundstone.com
Brad.Antoniewicz@foundstone.com

Outline

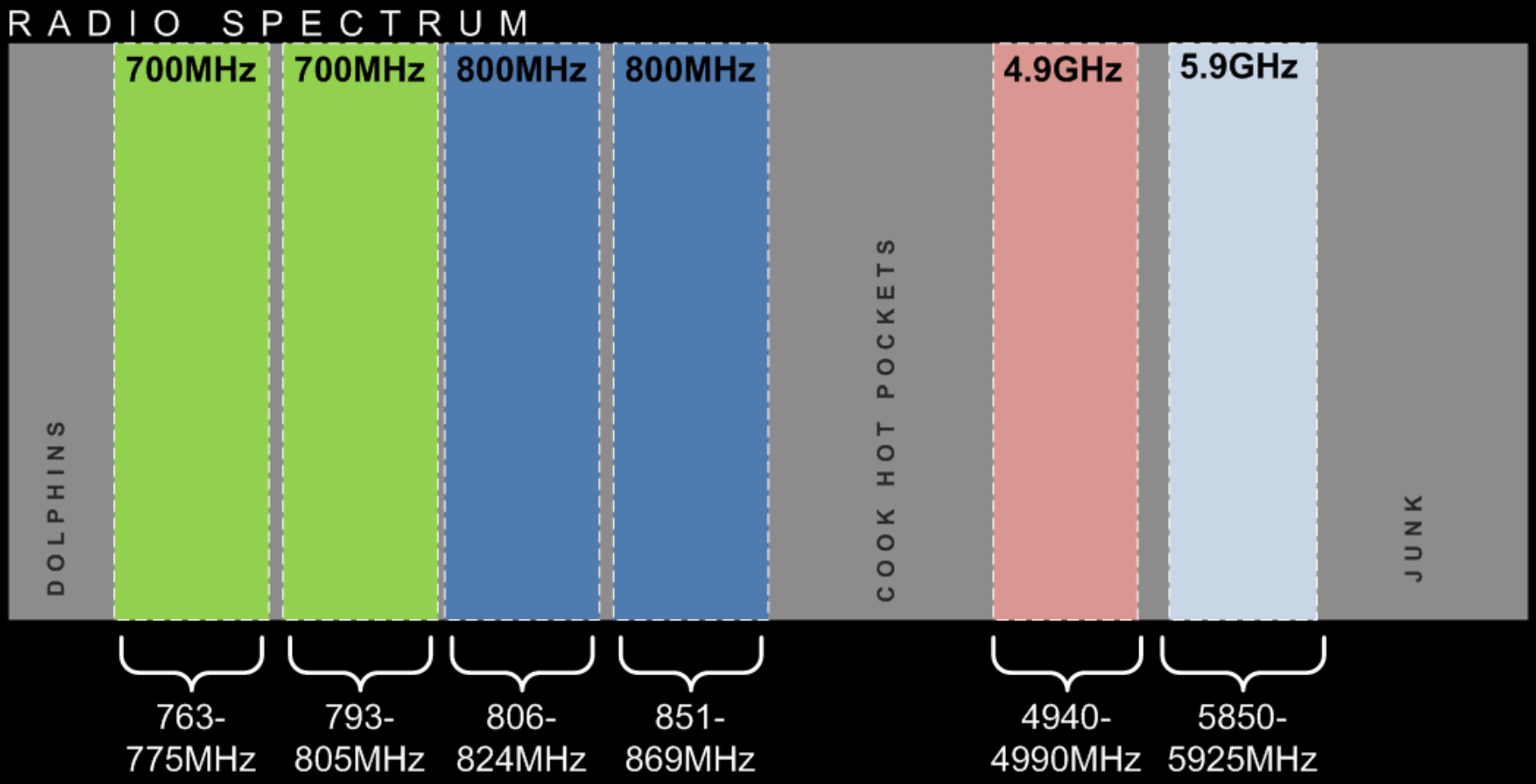
- Intro to Public Safety
- Spectrum Allocations
- Finding Public Safety Networks
- Protocols
- Interacting with Public Safety Networks

Focus on 4.9GHz

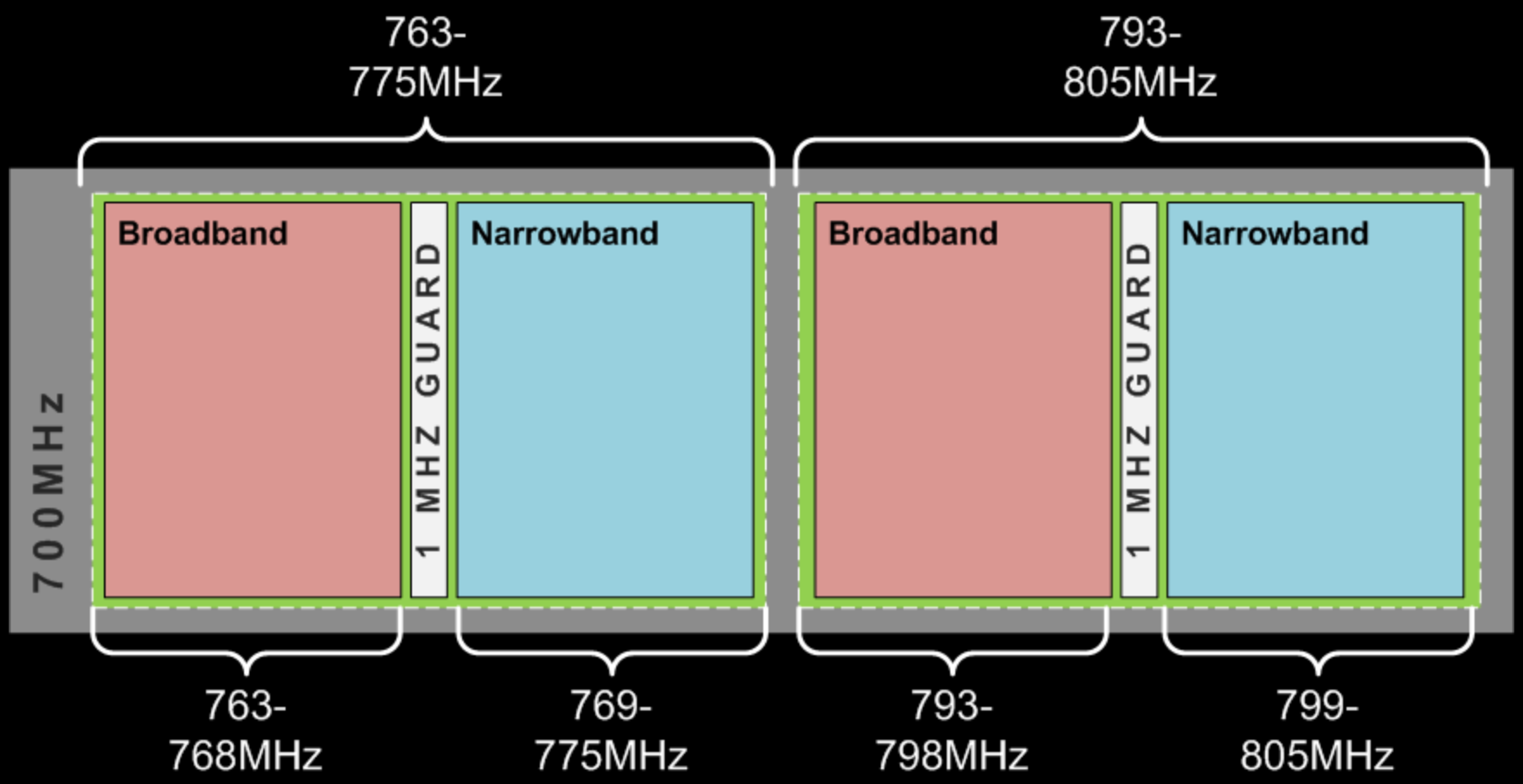
The Public Safety Spectrum

"The sole or principal purpose of which is to protect the safety of life, health, or property"

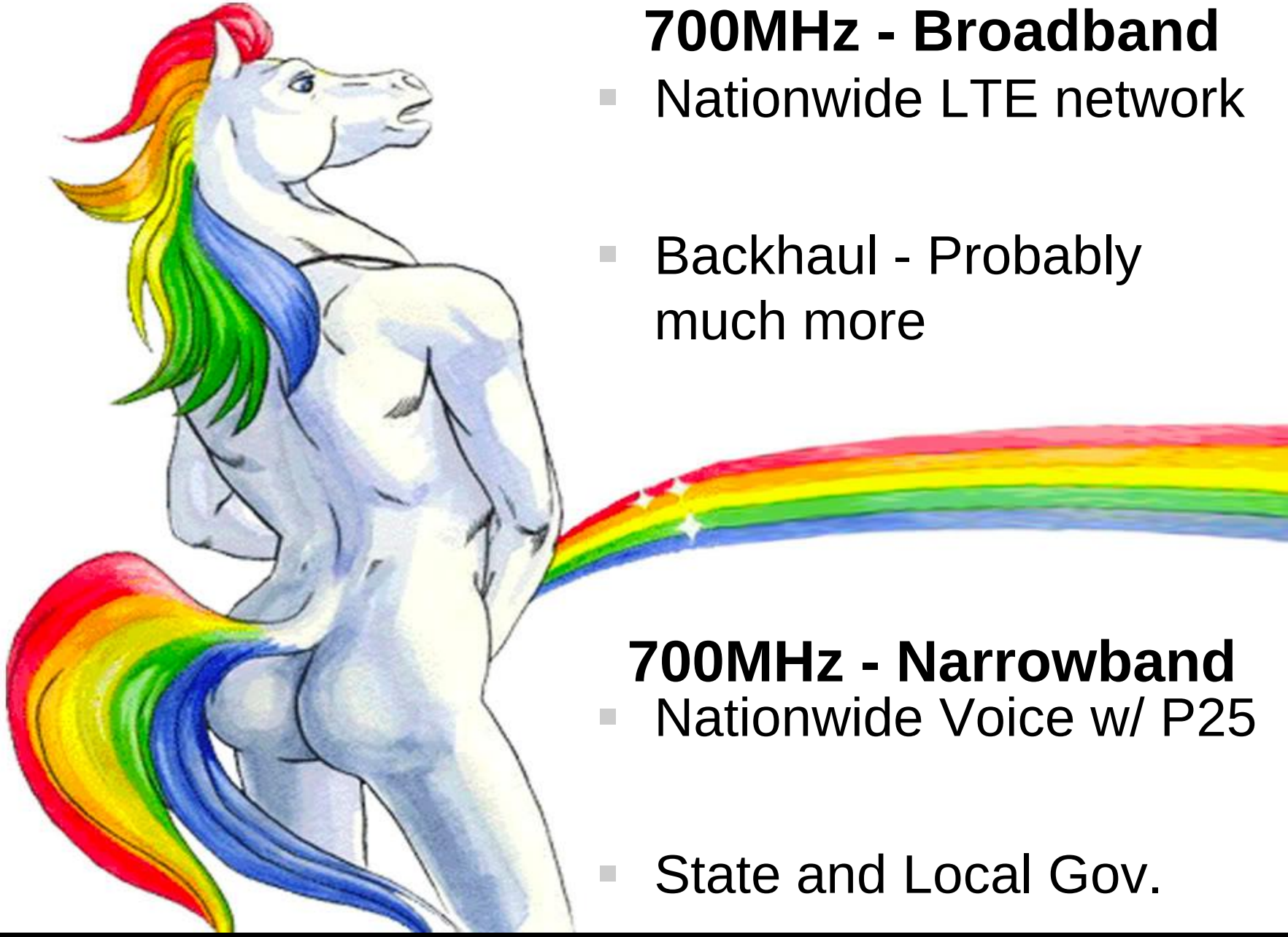
“New“ Frequencies



700MHz



- Reclaimed from Digital TV cutover
- Nationwide
- May Expand



700MHz - Broadband

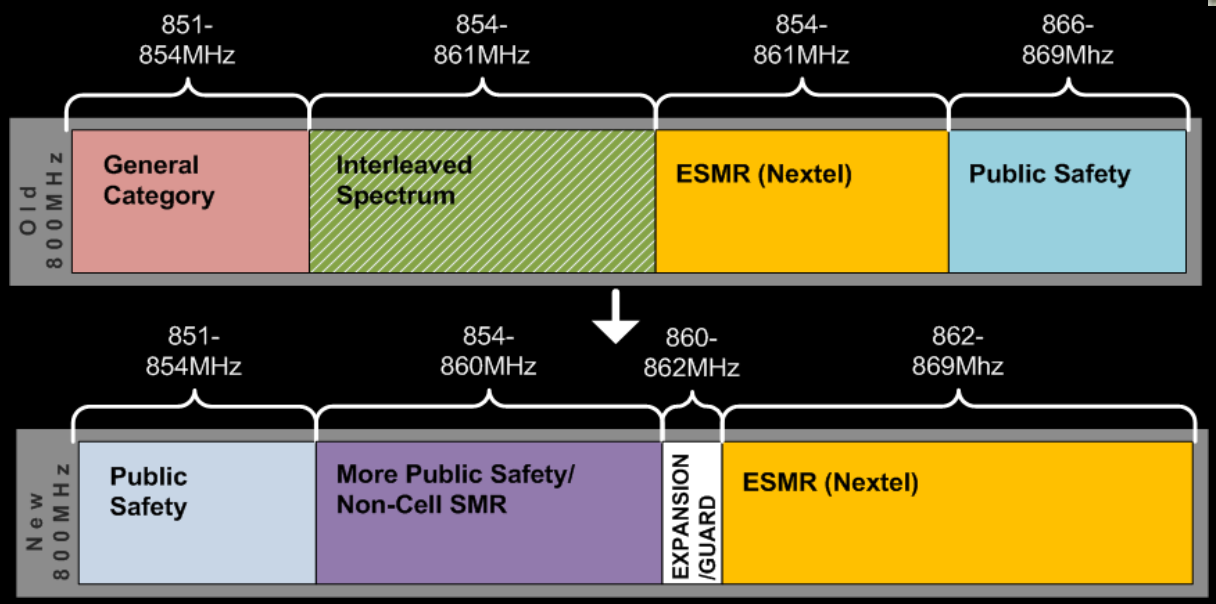
- Nationwide LTE network
- Backhaul - Probably much more

700MHz - Narrowband

- Nationwide Voice w/ P25
- State and Local Gov.

800MHz

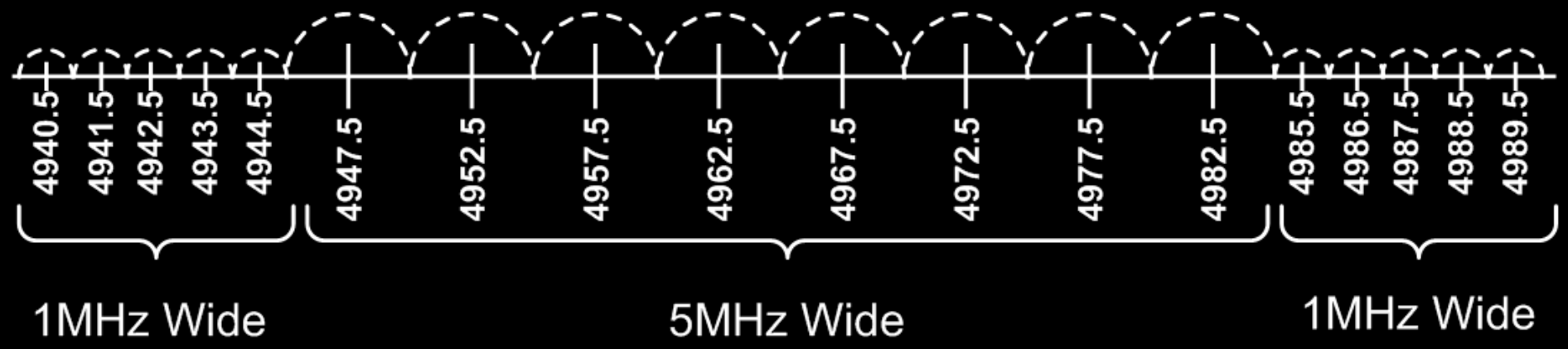
- “Reconfiguration” in progress
- PS Dedicated for voice (P25)



4.9GHz

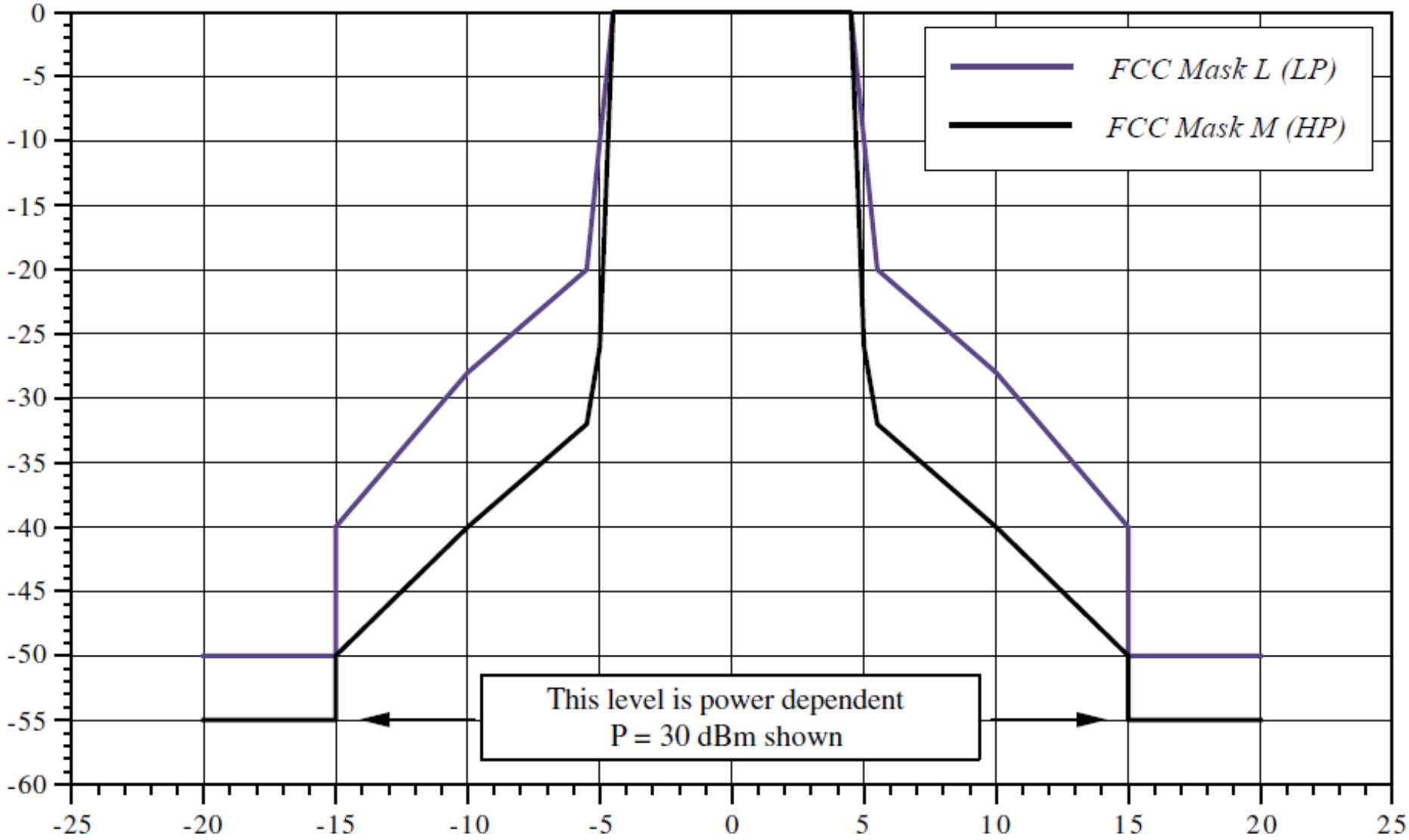
- General Use Spectrum
- Has been used for:
  - Video surveillance
  - RNC/DNC/G20
  - Access to Police cruisers
  - Emergency warning systems…
  - ..SCADA
  - Aircrafts
  - AMR

4.9GHz

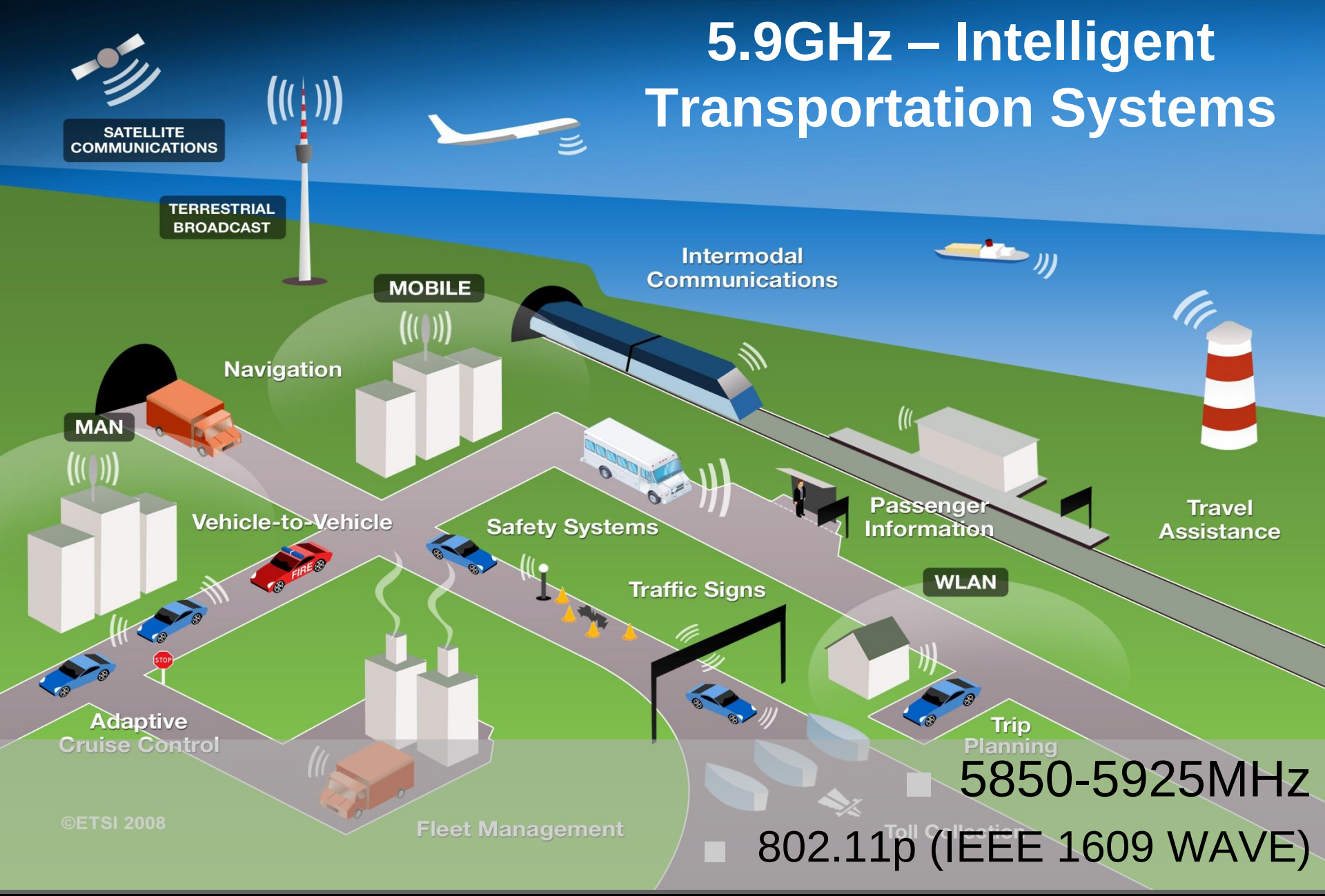


- Recommended for Low Power
- Required for High Power
- Can be grouped
  - NPSTC offers recommendations

4.9GHz – Emission Masks



5.9GHz – Intelligent Transportation Systems



- 5850-5925MHz
- 802.11p (IEEE 1609 WAVE)

Finding a Dance Partner

Radio Reference (700/800)

Firefox

Champaign County METCAD MDICE Tr...

www.radioreference.com/apps/db/?sid=4403

Google

Adobe Connect Centr...

Bookmarks

Talkgroups on this system can be patched to Starcom21 talkgroups (if needed) during emergencies.

System Frequencies

Red (c) are primary control channels | Blue (a) are alternate control channels | Site Map(s): FCC Callsigns RR Locations

RFSS	Site	Name	Freqs							
1 (1)	001 (1)	Simulcast	851.06250	851.55000	851.80000	852.10000	852.56250a	853.13750a	853.52500a	853.82500c

System Talkgroups

List All in one table Show New Talkgroups

METCAD Talkgroups

DEC	HEX	Mode	Alpha Tag	Description	Tag
21001	5209	E	METCAD 1	METCAD - Operations 1	Emergency Ops
21002	520a	E	METCAD 2	METCAD - Operations 2	Emergency Ops
21003	520b	E	METCAD 3	METCAD - Operations 3	Emergency Ops
21004	520c	E	METCAD 4	METCAD - Operations 4	Emergency Ops
21005	520d	E	METCAD EOC	METCAD - County EOC Net	Emergency Ops
21007	520f	D	RADIOSRV	METCAD - Radio Service Technicians	Public Works
21101	526d	D	MOTOROLA	Motorola System Technicians	Public Works

Interoperability Talkgroups

TG 22503 INC 4 is the primary police TG for sporting events, parades, concerts or other events

CAPRAD (700/800/4.9)

Firefox

CAPRAD 700MHz Plans

caprad.org/caprad/f_main.RegionalPlan700?p_cRegId=8&p_cOpt=1&p_cAreaId=999

Google

Adobe Connect Centr...

Bookmarks

Matthew Sobol | Log Out | FAQ | Help

CAPRAD COMPUTER ASSISTED PRE-COORDINATION RESOURCE AND DATABASE SYSTEM

NRPC

700 MHz Public Safety Spectrum

Home | 700 Mhz | 800 Mhz | 4.9 GHz | ICP

REGION 8 : New York - Metropolitan

SELECT AREA: -ENTIRE REGION- VIEW REGION

PLANNING | APPLICATIONS

NEW REGION

RESOURCES

Planning Data

- Channel Allotments
- Licenses
- Sites
- TV Stations
- Admin. Info

GO

Planning Information

- Status
- Comments
- Spectrum Summary
- Reports
- Plan Documents

Region 8 - New York - Metropolitan

FCC License Search (700/800/4.9/5.9)

Firefox

Connecting...

wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp

nudie pix

Adobe Connect Centr...

Bookmarks

Type ☐ Developmental ☐ Demonstration

Date Information

Date Type Select a date type

Select a fixed date range

Date From to 7/16/2012

(Date Format: MM/DD/YYYY)

Frequencies

Frequency

All Frequencies

Exact MHz

Range 4940 MHz to 4990 MHz

Customize Your Results

Results Display 10 matches per page sorted by Call Sign in ascending order

☐ Exact Matches Only

☐ Exclude Leases

RESET

GEOSEARCH SEARCH

*Please be aware that some combinations of search criteria may result in a longer wait.

Waiting for wireless2.fcc.gov...

FCC License Search (700/800/4.9/5.9)

Firefox

ULS License - Public Safety 4940-4990 M...

wireless2.fcc.gov/UlsApp/UlsSearch/licenseLocSum.jsp?licKey=2879527

how to hack optimus pri

Adobe Connect Centr...

Bookmarks

FCC Federal Communications Commission

FCC Home | Search | Updates | E-Filing | Initiatives | For Consumers | Find People

Universal Licensing System

FCC > WTB > ULS > Online Systems > License Search

FCC Site Map

Public Safety 4940-4990 MHz Band License - WQGJ817 - City of Kerrville - SCADA

HELP

Locations Summary

New Search | Return to Results | Printable Page | Reference Copy | Map License

!?!?!

MAIN | ADMIN | LOCATIONS | FREQUENCIES

Call Sign	WQGJ817	Radio Service	PA - Public Safety 4940-4990 MHz Band
2 Total Locations 10 Locations per Summary Page		Locations Displayed: **All** | Fixed | Mobile | Itinerant | Temp Fixed | 6.1m	

SC = Special Condition TP = Termination Pending

Location	Transmitter Address / Area of Operation	Latitude, Longitude	Status
1 - Temporary Fixed SC	KERR County, TX		
2 - Mobile SC	KERR County, TX		

FCC License Search (700/800/4.9/5.9)

Firefox

ULS License - Public Safety 4940-4990 M...

wireless2.fcc.gov/UlsApp/UlsSearch/licenseFreqSum.jsp?licKey=3297237

blue waffle disease

Adobe Connect Centr... Bookmarks

FCC > WTB > ULS > Online Systems > License Search FCC Site Map

Public Safety 4940-4990 MHz Band License - WQNW346 - NEW YORK CITY TRANSIT AUTHORITY

Frequencies Summary

HELP

New Search | Refine Search | Return to Results | Printable Page | Reference Copy | Map License

MAIN | ADMIN | LOCATIONS | FREQUENCIES

Call Sign	WQNW346	Radio Service	PA - Public Safety 4940-4990 MHz Band

2 Frequencies for all locations
20 Frequencies per Summary Page

Filter Frequencies By Location: All Locations GO

SC = Special Condition TP = Termination Pending

Define View: **General** | Buildout | COSER | Emission | IRAC

Frequency	Loc#	Ant#	Freq ID	Station Class	Units	Paging Rec.	Output Power	Maximum ERP
004950.00000000	1	1	1	FXB	1		0.250	6.000
004970.00000000	1	1	2	FXB	1		0.250	6.000

2 Frequencies for all locations
20 Frequencies per Summary Page

Filter Frequencies By Location: All Locations GO

Using Google To Find Implementations

Firefox

4.9ghz nypd - Google Search

google.com https://www.google.com/search?q=4.9ghz+&ie=utf-8&oe=utf-8&aq=t&

meaning of life

42 Suggest...

Adobe Connect Centr...

+You Search Images Maps Play YouTube News Gmail Documents Calendar More

Google 4.9ghz nypd

Search About 2,090 results (0.16 seconds)

Web
Images
Maps
Videos
News
Shopping
More

Plano, TX
Change location

Show search tools

[PDF] **NYPD 4.9-GHz** Letter
www.dhses.ny.gov/oiec/committees/.../**NYPD-4.9GHz**-Letter.pdf
File Format: PDF/Adobe Acrobat - Quick View
0. 'New or. 'He _ a. POLICE DEPARTMENT. Electronics Section. 50-16 59'" Place. Woodside, NY 11377. November 6, 2006. FCC Region Eight Planning ...

[PDF] **NYPD 4.9-GHz** License
www.dhses.ny.gov/oiec/committees/.../**NYPD-4.9GHz**-License.pdf
File Format: PDF/Adobe Acrobat - Quick View
Licensee: NEW YORK,. _ _ Page 1 _of 2. Federal Communications Commission. Wireless Telecommunications Bureau. 203. RADIO STATION ...

[PDF] **4.9GHz** Applications and Technology Workgroup Presentation ...
www.publicsafetycommunications.org/.../_2a_2a_20Public_20Updat...
File Format: PDF/Adobe Acrobat - View as HTML
Customers worldwide, trial proven with FDNY and **NYPD**. •Performance ... Beta trials of **4.9Ghz** version, compliant with FCC and DSRC. Masks, begin 01/05 ...

[PDF] 700 MHz Broadband Public Safety Applications And Spectrum ...

4.9/5.9GHz Access Points

Firefox

Alvarion VL AU 5.4 / 4.9 Ghz variuos type...

www.ebay.com/itm/ws/eBayISAPI.dll?ViewItem&item=270738350575

Adobe Connect Centr...

Go | My eBay

Welcome! Sign in or register.

CATEGORIES | ELECTRONICS | FASHION | MOTORS | TICKETS | DEALS | CLASSIFIE

Back to search results | Computers/Tablets & Networking > Home Networking & Connectivity > Other

Alvarion VL AU 5.4 / 4.9 Ghz variuos types used + POE Used + SEC 4.9 and 5.4

See original listing

SOLD

Item condition: **Manufacturer refurbished**
Ended: Jul 05, 2012 00:33:45 PDT
Price: **US $250.00** [5 sold]
Shipping: FREE Economy Shipping
Item location: Ca
Seller: w

See suggestions | Sell one like this

Firefox

BELAIR NETWORKS BELAIR100 100 4.9 5....

www.ebay.com/itm/ws/eBayISAPI.dll?ViewItem&item=160823991791&ssPageName=ADME

Adobe Connect Centr...

Go | My eBay | Sell

Welcome! Sign in or register.

CATEGORIES | ELECTRONICS | FASHION | MOTORS | TICKETS | DEALS | CLASSIFIEDS

Back to search results | Computers/Tablets & Networking > Enterprise Networking, Servers > Other

This listing was ended by the seller because the item is no longer available.

BELAIR NETWORKS BELAIR100 100 4.9 5.9 GHZ PTP PMP Wi-Fi WARRANTY FREE SHIPPING

See original listing

Item condition: **Used**
Ended: Jun 21, 2012 08:33:59 PDT
Price: **US $229.95** [1 sold]
Shipping: FREE Standard Shipping
ul, Minnesota, United States
tworks (1042) me | Seller's other items

Share:

Firefox

Belair 100 dual radio high end wireless a...

cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&item=170861471234

Adobe Connect Centr...

Go | My eBay | Sell | Community | Cust

Welcome! Sign in or register.

CATEGORIES | ELECTRONICS | FASHION | MOTORS | TICKETS | DEALS | CLASSIFIEDS

Back to My eBay | Computers/Tablets & Networking > Home Networking & Connectivity > Boosters, Extenders & Antennas

This listing was ended by the seller because the item is no longer available.

Belair 100 dual radio high end wireless access point

See original listing

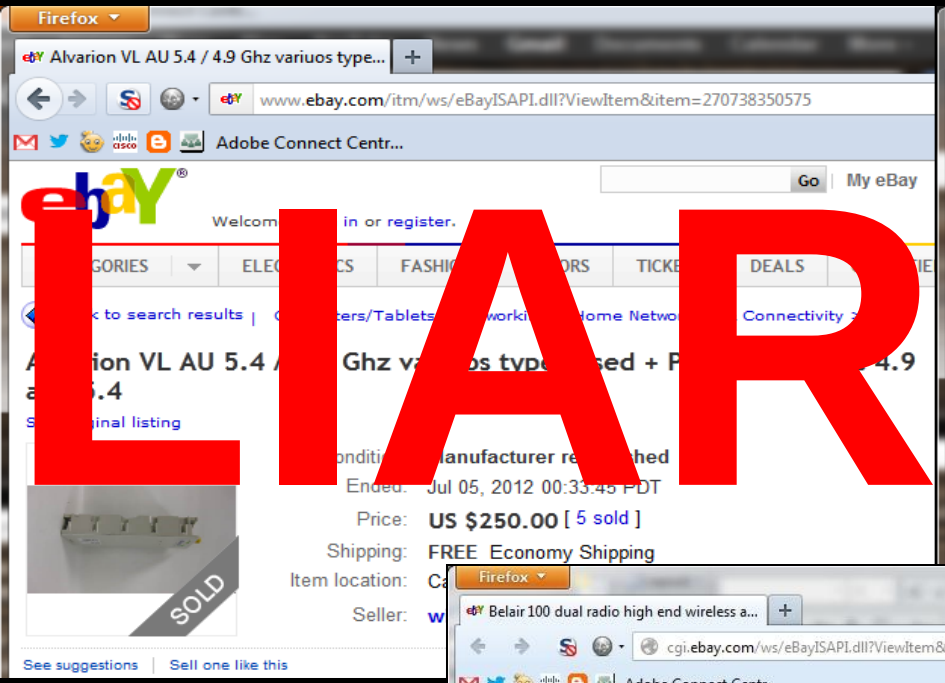
ENDED

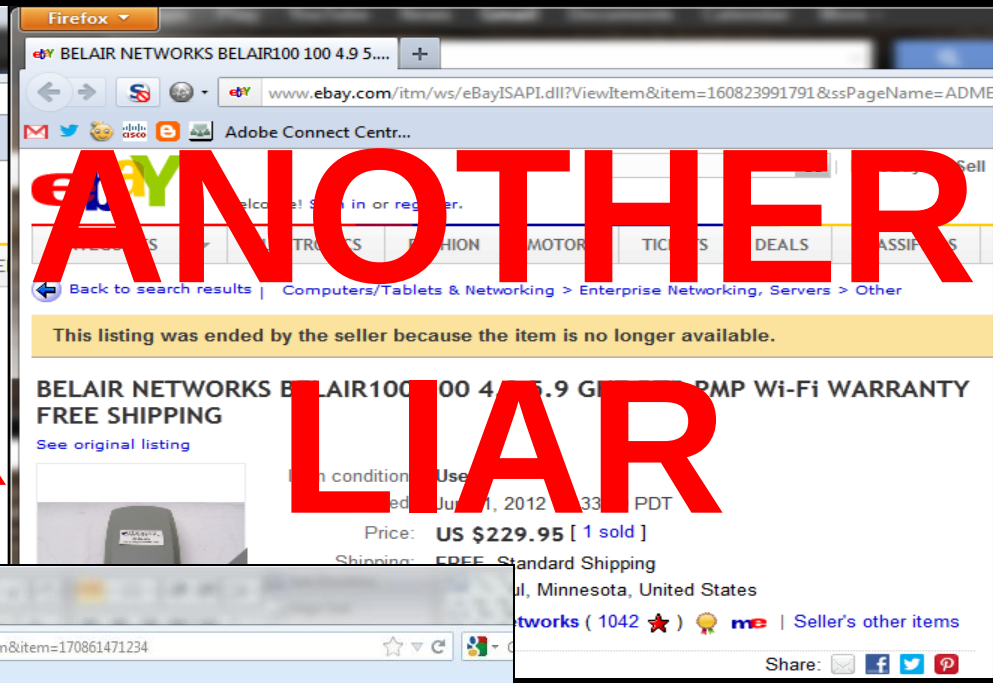
Item condition: **Used**
Ended: Jun 19, 2012 22:52:47 PDT
Price: **GBP 80.00**
Approximately US $125.06
Shipping: Read item description or contact seller for details.
Item location: bognor regis West Sussex, GB, United Kingdom
Seller: **dazzaebyer** (488) | Seller's other items

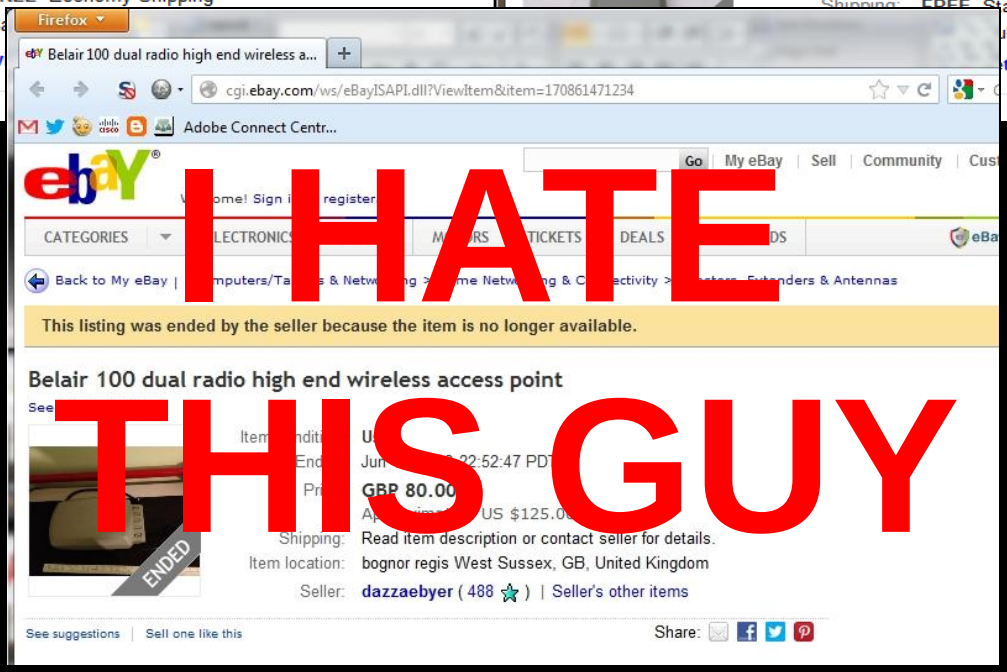
See suggestions | Sell one like this

Share:

4.9/5.9GHz Access Points







LIAR ANOTHER LIAR I HATE THIS GUY

4.9/5.9GHz Access Points

Firefox

PROXIM / TSUNAMI 4954-SUR-US, 4.9 G...

www.ebay.com/itm/180793241135?ssPageName=STRK:MEWNX:IT&_trksid=p3984.m1439.l2649

Google

Adobe Connect Centr...

Book

Click to view larger image and other views

PROXIM / TSUNAMI 4954-SUR-US, 4.9 Ghz, SUBSCRIBER UNIT, w/ mount and Power supp

POINT TO POINT, WIRELESS RADIO, ANTENNA, BRIDGE

Item condition: **New other (see details)**

Sold For: **US $100.00**

Add to list

BillMeLater **$10 back on first Bill Me Later purchase**
Subject to credit approval. See terms

Shipping: **$25.00** - Standard Shipping | See all details
Item location: **AZ, United States**
Ships to: **United States**

Delivery: Estimated within 4-8 business days

Payments: PayPal, Bill Me Later | See details

Returns: 7 days money back, buyer pays return

Seller information

splatvonzipper (169)

100% Positive feedback

Save this seller

See other items

4.9/5.9GHz Access Points

Firefox

PROXIM / TSUNAMI 4954-SUR-US, 4.9 G...

www.ebay.com/itm/180793241135?ssPageName=STRK:MEWNX:IT&_trksid=p3984.m1439.l2649

Google

Adobe Connect Centr...

Book

PROXIM / TSUNAMI 4954-SUR-US, 4.9 Ghz, SUBSCRIBER UNIT, w/ mount an

Tsunami® MP.11 Series

Our Most Popular Outdoor and Indoor Wireless Access System for License Free Frequency Bands World-Wide

Click to view larger image and other views

4.9/5.9GHz Access Points

Firefox

PROXIM / TSUNAMI 4954-SUR-US, 4.9 G...

www.ebay.com/itm/180793241135?ssPageName=STRK:MEWNX:IT&_trksid=p3984.m1439.l2649

Google

Adobe Connect Centr...

Book

PROXIM / TSUNAMI 4954-SUR-US, 4.9 Ghz, SUBSCRIBER UNIT, w/ mount and

Tsunami® MP.11 Series

Click to view larger image and other views

4.9/5.9GHz Access Points

UBIQUITI NETWORKS forum

Register | UBNT Home | Community | Translations | Forum Rules

Ubiquiti Networks Forum > Ubiquiti Product Forum > airMAX > 5GHz Based M Series Products
4.9ghz from Nanostation M5

User Name | Remember Me?
Password | Log in

reply

Thread Tools | Display Modes

12-14-2010, 10:44 AM #1

farang
New User

Join Date: Jan 2010
Posts: 18
Likes: 0

4.9ghz from Nanostation M5

The spec sheet shows that the NSM5 can do 4.9-5.9GHz but I cant seem to access anything in 4.9ghz. Do I need to do something special? Change the firmware?

quote

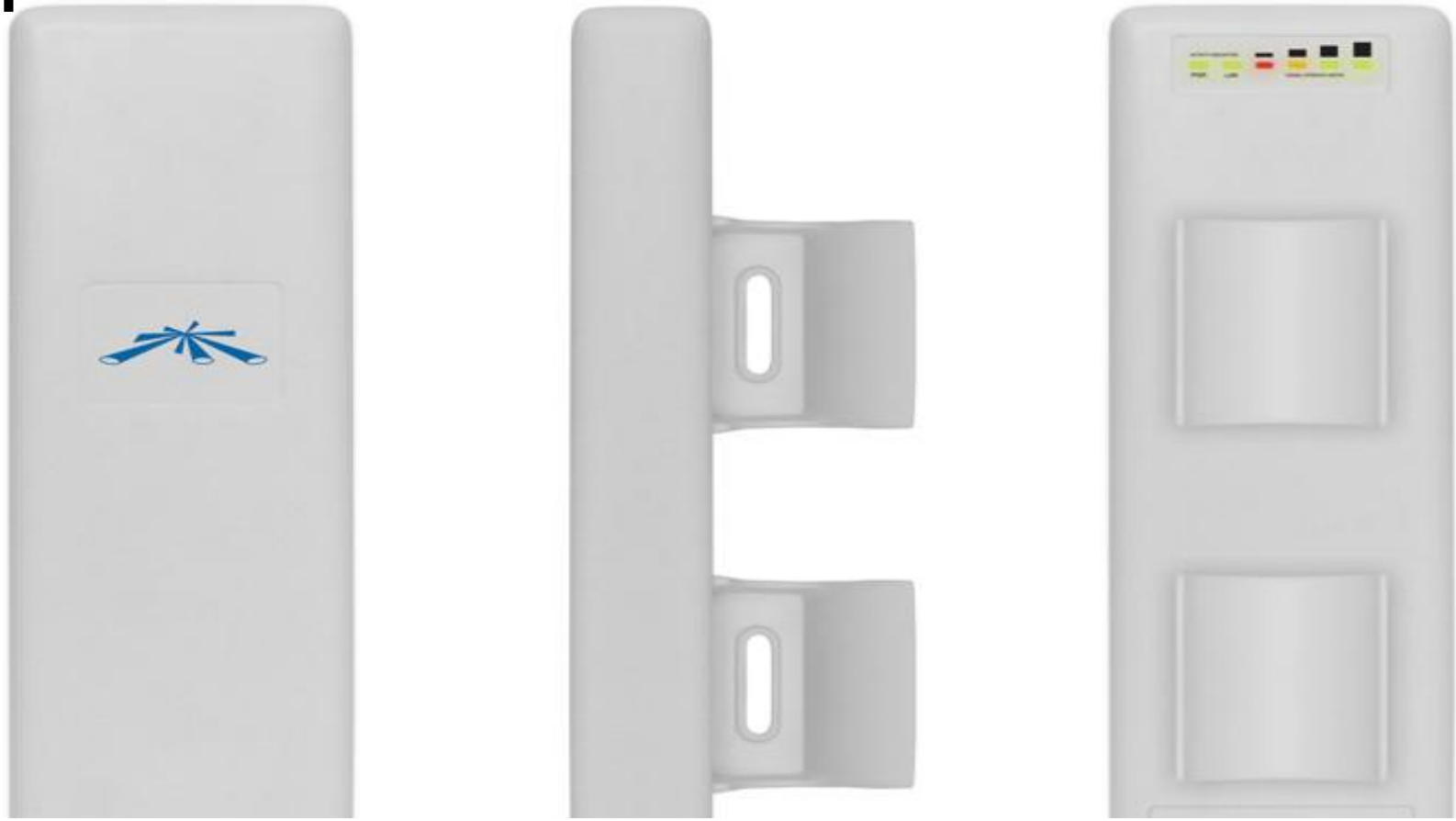
12-14-2010, 11:12 AM #2

Migptm
New User

Join Date: Oct 2010
Location: Portimão

On menu WIRELESS change the country code to " Compilance Test "

Ubiquiti NSM5-WORLD



Ubiquiti 5GHz equipment (M5 / AirMax): Starting in May 2011, Ubiquiti is designating two versions, each with different firmware US and World. The part# ends with either "US" or "World." The US version firmware will have restrictions to use only in the legal frequency bands/channels.

4.9/5.9GHz Access Points

UBIQUITI NETWORKS

Important F.C.C. Sales, Shipping & Use Restrictions: For F.C.C. Licensed Users

Ubiquiti Networks only authorizes for shipment to the United States and for use in the United States, versions of its products that are locked to United States country frequency channels. These are regulated by the F.C.C. as to its use and sale. All non-U.S. models must be for EXPORT only. If non-U.S. product is sold for use within the United States, the buyer and end-user must certify by signing this statement that they:

a) Hold a valid, current and appropriate F.C.C. license to operate that equipment in the frequency range of the equipment to be purchased and used;
b) Agree to utilize such equipment fully in continual compliance with all U.S. regulatory regulations regarding the use of such equipment and selected frequencies in any situation;
c) Agree not to transfer, sell or lend in any fashion the equipment to any other party for use for other purposes contrary to those mentioned herein.

Moreover, the signer below understand and agrees that any purchase and/or subsequent shipment of any non-U.S. devices within the United States for other than lawful use and/or authorized export could subject you to FCC or other regulatory agency fines and other enforcement action by the United States government, including possible criminal sanctions. All products must be used in full compliance with F.C.C. and other regulatory rules.

4.9GHz Adapters

Ubiquiti SR4C

4.9GHz/5.9GHz Adapters

Ubiquiti SRC300

SuperRange Cardbus
Technical Specifications

UBIQUITI NETWORKS

495-499 Montague Expwy.
Milpitas, CA 95035
T (408)-942-3085
F (408)-351-4973
sales@ubnt.com
http://www.ubnt.com

CARD INFORMATION	
Wireless Chipset	Atheros 5004
Radio Operation	IEEE 802.11a/b/g with CCK/OFDM at BPSK/QPSK/16QAM/64QAM
Interface	32-bit Cardbus Type II
Operation Voltage	3.3VDC
Antenna Ports	Dual MMCX (Primary only required; secondary optional for diversity)
Temperature Range	-40C to +80C (extended temp version up to +95C)
Security	WPA, WPA2, AES-CCM & TKIP Encryption, 802.1x, 64/128/152bit WEP
Data Rates	6Mbps, 9Mbps, 12Mbps, 24Mbps, 36Mbps, 48Mbps. 54Mbps
RoHS Compliance	YES

REGULATORY INFORMATION	
Wireless Modular Approvals	FCC , Industry Canada, CE (100mW limited)

OPERATING FREQUENCY 5745MHz-5825MHz

2.4GHz TX SPECIFICATIONS	DataRate	TX Power	Tolerance
802.11b	1Mbps	24 dBm	+/-1dB
	2Mbps	24 dBm	+/-1dB
	5.5Mbps	24 dBm	+/-1dB
	11Mbps	24 dBm	+/-1dB
802.11g OFDM	6Mbps	24 dBm	+/-1dB
	9Mbps	24 dBm	+/-1dB
	12Mbps	24 dBm	+/-1dB
	18Mbps	24 dBm	+/-1dB
	24Mbps	24 dBm	+/-1dB
	36Mbps	23 dBm	+/-1dB
	48Mbps	22 dBm	+/-1dB
	54Mbps	20 dBm	+/-1dB

2.4GHz RX SPECIFICATIONS	DataRate	Sensitivity	Tolerance
802.11b	1Mbps	-96 dBm	+/-1dB
	2Mbps	-95 dBm	+/-1dB
	5.5Mbps	-94 dBm	+/-1dB
	11Mbps	-91 dBm	+/-1dB
802.11g OFDM	6Mbps	-94 dBm	+/-1dB
	9Mbps	-93 dBm	+/-1dB
	12Mbps	-91 dBm	+/-1dB
	18Mbps	-90 dBm	+/-1dB
	24Mbps	-86 dBm	+/-1dB
	36Mbps	-83 dBm	+/-1dB
	48Mbps	-77 dBm	+/-1dB
	54Mbps	-74 dBm	+/-1dB

OPERATING FREQUENCY 2412MHz-2462MHz

5GHz TX SPECIFICATIONS	DataRate	TX Power	Tolerance
802.11a OFDM	6Mbps	20 dBm	+/-1dB
	9Mbps	20 dBm	+/-1dB
	12Mbps	20 dBm	+/-1dB
	18Mbps	20 dBm	+/-1dB
	24Mbps	20 dBm	+/-1dB
	36Mbps	19 dBm	+/-1dB
	48Mbps	18 dBm	+/-1dB
	54Mbps	16 dBm	+/-1dB

RADIO 2 5GHz RX SPECIFICATIONS	DataRate	Sensitivity	Tolerance
802.11a OFDM	6Mbps	-94 dBm	+/-1dB
	9Mbps	-93 dBm	+/-1dB
	12Mbps	-91 dBm	+/-1dB
	18Mbps	-90 dBm	+/-1dB
	24Mbps	-86 dBm	+/-1dB
	36Mbps	-83 dBm	+/-1dB
	48Mbps	-77 dBm	+/-1dB
	54Mbps	-74 dBm	+/-1dB

CURRENT CONSUMPTION INFORMATION

TX CURRENT CONSUMPTION	DataRate	TX Power	Tolerance
802.11b	1Mbps	0.80 A	+/-100 mA
	2Mbps	0.80 A	+/-100 mA
	5.5Mbps	0.80 A	+/-100 mA
	11Mbps	0.80 A	+/-100 mA
11g/a	6-24Mbps	0.80 A	+/-100 mA
	36Mbps	0.75 A	+/-100 mA
	48Mbps	0.70 A	+/-100 mA
	54Mbps	0.60 A	+/-100 mA

RX CURRENT CONSUMPTION	DataRate	Sensitivity	Tolerance
802.11b	1Mbps	350 mA	+/-100 mA
	2Mbps	350 mA	+/-100 mA
	5.5Mbps	350 mA	+/-100 mA
	11Mbps	350 mA	+/-100 mA
11g/a	6-24Mbps	350 mA	+/-100 mA
	36Mbps	350 mA	+/-100 mA
	48Mbps	350 mA	+/-100 mA
	54Mbps	350 mA	+/-100 mA

RANGE PERFORMANCE	
Indoor (Antenna Dependent):	Up to 150meters
Outdoor (Antenna Dependent):	Over 1km

DRIVER INFORMATION	
Operating System Support	Linux, WindowsXP, Windows2000
Advanced Mobility / QuickHandoff	WindowsXP/2000 Utility with Enhanced Mobility Driver from Ubiquiti
Cisco Support	CCX 4.0 Supported Driver/Utility also available from Ubiquiti
For help with special driver support, please e-mail support@ubnt.com	

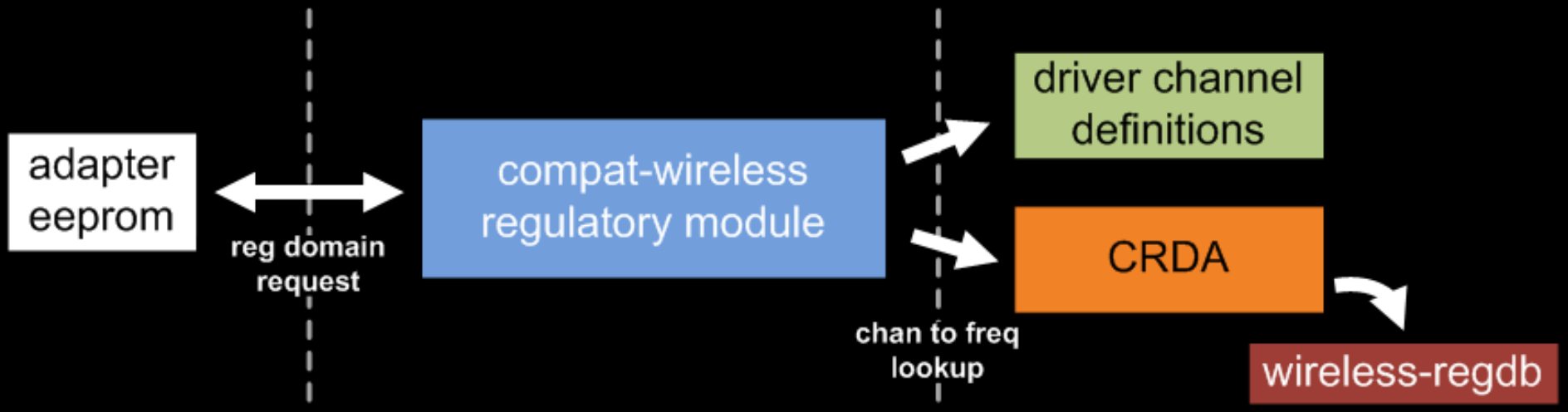
LAPTOP ANTENNA INFORMATION	
Antenna Dimensions	5.1 in x 0.83 in
Cable	18 in with MMCX plug
Antenna Type / Polarization	Omni-directional / Vertical Polarized
Antenna Gain	5dBi
Mounting Type	Adjustable Laptop Clip Mount and Sticker Mount Included

Kugutsumen: “DEBUG” reg domain - the SRC has the abilities to support 4910 – 6100MHz

Extending Drivers

- Previous patches [that no longer work]
  - Zero Chaos
    - Awesome – but no channel width support
  - Spench <- this guy is fucking awesome
    - Meant for RADAR stuff so its overly complex for our purpose

compat-wireless



Manual regulatory domain override?

`iw reg set`

(never seems to work)

Extending ath5k for 4.9GHz

drivers/net/wireless/ath/ath5k/caps.c:

```
if(ath_is_49ghz_allowed(regdom))
  range_5ghz_min = 4920
else
  range_5ghz_min = 5005
range_5ghz_max = 6100
```

drivers/net/wireless/ath/regd.c:

```
bool ath_is_49ghz_allowed() {
…
}
```

Extending ath5k for 4.9GHz

drivers/net/wireless/ath/ath5k/caps.c:

```
if(ath_is_49ghz_allowed(regdom))
  range_5ghz_min = 4920
else
  range_5ghz_min = 5005
range_5ghz_max = 6100
```

drivers/net/wireless/ath/regd.c:

```
bool ath_is_49ghz_allowed() {
  return true;
}
```

Supporting Different Channel Widths

```
drivers/net/wireless/reg.c:
/*
 * Note that right now we assume the desired
 * channel bandwidth is always 20MHz...
 * To support  smaller custom bandwidths such as 5 MHz or
 * 10 MHz we'll need a new ieee80211_channel.target_bw…
 */
```

…Required a little more work.. But not that much

Supporting Different Channel Widths

```
# modprobe ath5k default_bwmode=2
```

default_bwmode option name from RADAR patch

0=20MHz (default)

1= 5MHz

2=10Mhz

3=40Mhz

Setup

```
# ./49ghz_install.sh
```

Manual

```
# modprobe ath5k default_bwmode=2
# iw dev wlan0 interface add mon0 type mode monitor
# ifconfig mon0 up
# iwconfig mon0 freq 4.950G
# tcpdump -i mon0 -X
```

github.com/opensecurityresearch

db-ReturnTrue.conf

```
country US:
        (4910 - 5170 @ 10), (N/A, 23)
        (5715 - 6100 @ 10), (N/A, 23)
```

kismet-ReturnTrue.conf

```
ncsource=mon0:type=ath5k:forcevap=false
channeldwell=2
channellist=ps5mhz:4920-4990-5-.5
channellist=ps10mhz:4920-4990-10-.5
channellist=ps20mhz:4920-4990-20-.5
```

4.9GHz

NYC 4.9GHZ MESH!

```
channellist=nyc:4950-4950-10-10
```

NYC 4.9GHz – Video Surveillance

Source	Destination	Protocol	Info
Cisco_	Broadcast	IEEE	Probe Request, SN=2332, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=2951, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=2960, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=3983, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=3023, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=176, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=302, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=320, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=329, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=347, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=356, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=365, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=374, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=383, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=392, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=401, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=410, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=419, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=428, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=437, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=455, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=464, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=473, FN=0, Flags=.....C, SSID=
Cisco_	Broadcast	IEEE	Probe Request, SN=500, FN=0, Flags=.....C, SSID=

sorry bro not tellin'

..but there are default SSIDs :)

NYC 4.9GHz – At the Station

Source	Destination	Protocol	Info
Cisco_	Cisco_	IEEE	Probe Response, SN=3164, FN=0, Flags=.....C, BI=100, SSID=REMOVED,
	Cisco_	IEEE	Acknowledgement, Flags=.....C
Cisco_	Broadc	IEEE	Beacon frame, SN=3165, FN=0, Flags=.....C, BI=100, SSID="\000", Name="
Cisco_	Cisco_	IEEE	Authentication, SN=992, FN=0, Flags=.....C
	Cisco_	IEEE	Acknowledgement, Flags=.....C
Cisco_	Cisco_	IEEE	Reassociation Request, SN=993, FN=0, Flags=.....C, SSID REMOVED, N
	Cisco_	IEEE	Acknowledgement, Flags=.....C
	Cisco_	IEEE	Acknowledgement, Flags=.....C
Cisco_	Cisco_	EAPOL	Start
Cisco_	Cisco_	EAPOL	Start
	Cisco_	IEEE	Acknowledgement, Flags=.....C
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
	Cisco_	IEEE	Acknowledgement, Flags=.....C
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
	Cisco_	IEEE	Acknowledgement, Flags=.....C
Cisco_	Cisco_	EAP	Response, EAP-Cisco Wireless (LEAP) [Norman]
Cisco_	Cisco_	EAP	Response, EAP-Cisco Wireless (LEAP) [Norman]
Cisco_	Cisco_	EAP	Response, EAP-Cisco Wireless (LEAP) [Norman]
Cisco_	Cisco_	EAP	Response, EAP-Cisco Wireless (LEAP) [Norman]
Cisco_	Cisco_	EAP	Response, EAP-Cisco Wireless (LEAP) [Norman]
Cisco_	Cisco_	EAP	Response, EAP-Cisco Wireless (LEAP) [Norman]

NYC 4.9GHz – At the Station

Source	Destination	Protocol	Info
Cisco_	Cisco_	IEEE	Probe Response, SN=3164, FN=0, Flags=.....C, BI=100, SSID=REMOVED,
	Cisco_	IEEE	Acknowledgement, Flags=.....C
Cisco_	Broadc	IEEE	Beacon frame, SN=3165, FN=0, Flags=.....C, BI=100, SSID="\000", Name="
Cisco_	Cisco_	IEEE	Authentication, SN=992, FN=0, Flags=.....C
	Cisco_	IEEE	Acknowledgement, Flags=.....C
Cisco_	Cisco_	IEEE	Reassociation Request, SN=993, FN=0, Flags=.....C, SSID REMOVED, N
	Cisco_	IEEE	Acknowledgement, Flags=.....C
	Cisco_	IEEE	Acknowledgement, Flags=.....C
Cisco_	Cisco_	EAPOL	Start
Cisco_	Cisco_	EAPOL	Start
	Cisco_	IEEE	Acknowledgement, Flags=.....C
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
	Cisco_	IEEE	Acknowledgement, Flags=.....C
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
Cisco_	Cisco_	EAP	Response, Identity [RFC3748]
	Cisco_	IEEE	Acknowledgement, Flags=.....C
Cisco_	Cisco_	EAP	Response, EAP-Cisco Wireless (LEAP) [Norman]
Cisco_	Cisco_	EAP	Response, EAP-Cisco Wireless (LEAP) [Norman]
Cisco_	Cisco_	EAP	Response, EAP-Cisco Wireless (LEAP) [Norman]
Cisco_	Cisco_	EAP	Response, EAP-Cisco Wireless (LEAP) [Norman]
Cisco_	Cisco_	EAP	Response, EAP-Cisco Wireless (LEAP) [Norman]
Cisco_	Cisco_	EAP	Response, EAP-Cisco Wireless (LEAP) [Norman]

.. ((record scratch))

LEAP?! RLY?

NYC 4.9GHz

- Crack LEAP = Own NYPD?
  - See Moxie and h1kari's talk today
- Proxim WORP(Wireless Outdoor Routing Protocol)?
  - Older versions – remove driver FCS check
  - New versions – DFU Mode APs?

VEGAS BABY!!!


```
channellist=vegas:4980-4980-10-10
```

VEGAS 4.9GHz

Source	Destination	Protocol	Info
Motoro	Broadcast	IEEE	Beacon frame, SN=3018, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3019, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3020, FN=0, Flags=.....C, BI=100, SSID=
Meshne	Broadcast	LLC	U, func=UI; SNAP, OUI 0x000000 (Encapsulated Ethernet), PID 0x88A9
Motoro	Broadcast	IEEE	Beacon frame, SN=3022, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3023, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3024, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3025, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3027, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3029, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3030, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3031, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3032, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3033, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3037, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3039, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3040, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3042, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3043, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3044, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3045, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3048, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3052, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3053, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3054, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3055, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3056, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3060, FN=0, Flags=.....C, BI=100, SSID=
	Broadcast	(RA) IEEE	Acknowledgement, Flags=.....C
	Broadcast	(RA) IEEE	Acknowledgement, Flags=.....C
	Broadcast	(RA) IEEE	Acknowledgement, Flags=.....C
	Broadcast	(RA) IEEE	Acknowledgement, Flags=.....C
	Broadcast	(RA) IEEE	Acknowledgement, Flags=.....C
Motoro	Broadcast	IEEE	Beacon frame, SN=3061, FN=0, Flags=.....C, BI=100, SSID=
	Broadcast	(RA) IEEE	Acknowledgement, Flags=.....C

REMOVED

EXTREMELY OBVIOUS!

..but not tellin

REMOVED

VEGAS 4.9GHz

Source	Destination	Protocol	Info
Motoro	Broadcast	IEEE	Beacon frame, SN=3018, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3019, FN=0, Flags=.....C, BI=100, SSID=
Meshne	Broadcast	LLC	U, func=UI; SNAP, OUI 0x000000 (Encapsulated Ethernet), PID 0x88A9
Motoro	Broadcast	IEEE	Beacon frame, SN=3023, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3024, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3025, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3027, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3029, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3030, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3031, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3032, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3033, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3037, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3039, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3040, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3042, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3043, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3044, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3045, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3048, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3052, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3053, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3054, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3055, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3056, FN=0, Flags=.....C, BI=100, SSID=
Motoro	Broadcast	IEEE	Beacon frame, SN=3060, FN=0, Flags=.....C, BI=100, SSID=
	Broadcast	(RA) IEEE	Acknowledgement, Flags=.....C
	Broadcast	(RA) IEEE	Acknowledgement, Flags=.....C
	Broadcast	(RA) IEEE	Acknowledgement, Flags=.....C
	Broadcast	(RA) IEEE	Acknowledgement, Flags=.....C
	Broadcast	(RA) IEEE	Acknowledgement, Flags=.....C
Motoro	Broadcast	IEEE	Beacon frame, SN=3061, FN=0, Flags=.....C, BI=100, SSID=
	Broadcast	(RA) IEEE	Acknowledgement, Flags=.....C

REMOVED

EXTREMELY OBVIOUS!

..but not tellin

REMOVED

VEGAS 4.9GHz

```
    Header Length: 32
    DLT: 105
  ⊞ 802.11-Common
⊞ IEEE 802.11 Data, Flags: ......FTC
⊟ Logical-Link Control
    DSAP: SNAP (0xaa)
    IG Bit: Individual
    SSAP: SNAP (0xaa)
    CR Bit: Command
  ⊟ Control field: U, func=UI (0x03)
      000. 00.. = Command: Unnumbered Information (0x00)
      .... ..11 = Frame type: Unnumbered frame (0x03)
    Organization Code: Encapsulated Ethernet (0x000000)
    Type: Unknown (0x88a9)
⊟ Data (356 bytes)
    Data: 0301020200000e04f400ffffca63ffffffffffff[redacted]..
    [Length: 356]

0040  03 00 00 00 88 a9 03 01  02 02 00 00 0e 04 f4 00  ........ ........
0050  ff ff ca 63 ff ff ff ff  ff ff [redacted]  ...c.... ........
0060  [redacted]  ..E..H.. ....9...
0070                                                    .......D .C.4....
0080  06 00 7e 66 d0 f8 00 1c  00 00 00 00 00 00 00 00  ..~f.... ........
0090  00 00 00 00 00 00 00 00  00 00 00 05 12 0a 12 ab  ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
0110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
0130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
0140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
0150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
0160  00 00 00 00 00 00 00 00  00 00 63 82 53 63 35 01  ........ ..c.Sc5.
0170  01 33 04 ff ff ff ff 0c  0f 44 45 56 30 30 30 [redacted]  .3...... .DEV000[redacted]
0180  [redacted]  07 01 1c 02 03 0f 06 [redacted]7.......
0190  0c ff 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
01a0  00 00 00 00 00 00 00 00  00 00 a1 4b 61 82         ........ ...Ka.
```

VEGAS 4.9GHz

- Motorola MOTOMESH
  - 4 Radios – 2 for 802.11, 2 for MEA
  - If 4.9ghz is not there try 2.4GHz!
  - Saw ARP for public routable IP addresses
    - Not immediately accessible
- Mobility Enhanced Access (MEA)
  - Proprietary crapola – needs more investigating

VEGAS 4.9GHz SkyPilot

```
Skypilot_Broadcast LLC   S F, func=RNR, N(R)=72; DSAP 0xc2 Individual, SSAP 0x4a Response
Skypilot_Broadcast LLC   S P, func=RNR, N(R)=72; DSAP 0xda Group, SSAP 0x52 Command
Skypilot_Broadcast LLC   U F, func=Unknown; DSAP HP JetDirect Printer Individual, SSAP 0x60 Response
Skypilot_Broadcast LLC   U P, func=Unknown; DSAP 0xa2 Group, SSAP 0xec Command
Skypilot_Broadcast LLC   I P, N(R)=72, N(S)=119; DSAP 0xb8 Individual, SSAP ARP Command
Skypilot_Broadcast LLC   S F, func=RNR, N(R)=72; DSAP 0x56 Individual, SSAP 0x64 Response
Skypilot_Broadcast LLC   S, func=SREJ, N(R)=73; DSAP 0x64 Group, SSAP 0x2a Response
Skypilot_Broadcast LLC   U F, func=UP; DSAP 0x22 Individual, SSAP 0x32 Response
Skypilot_Broadcast LLC   U F, func=RD; DSAP 0x58 Group, SSAP 0x40 Response
Skypilot_Broadcast LLC   I P, N(R)=73, N(S)=69; DSAP 0xf2 Individual, SSAP 0x94 Command
Skypilot_Broadcast LLC   U, func=SNRM; DSAP 0xa0 Group, SSAP 0x36 Command
Skypilot_Broadcast LLC   I, N(R)=74, N(S)=81; DSAP 0xf6 Individual, SSAP ISO 8208 (X.25 over 802.2) Response
Skypilot_Broadcast LLC   I P, N(R)=74, N(S)=14; DSAP 0xce Individual, SSAP 0x90 Response
Skypilot_Broadcast LLC   U, func=UA; DSAP 0x16 Group, SSAP 0x9a Command
Skypilot_Broadcast LLC   I P, N(R)=74, N(S)=61; DSAP 0xce Individual, SSAP 0x6c Response
Skypilot_Broadcast LLC   S P, func=RNR, N(R)=74; DSAP 0xc6 Group, SSAP 0xde Command
Skypilot_Broadcast LLC   S P, func=REJ, N(R)=74; DSAP 0x40 Individual, SSAP 0xbe Command
Skypilot_Broadcast LLC   S F, func=RR, N(R)=74; DSAP 0x32 Individual, SSAP 0x7c Response
Skypilot_Broadcast LLC   I P, N(R)=74, N(S)=115; DSAP 0x4c Individual, SSAP LLC Sub-Layer Management Command
Skypilot_Broadcast LLC   U F, func=Unknown; DSAP Banyan Vines Group, SSAP 0x78 Response
Skypilot_Broadcast LLC   S, func=REJ, N(R)=75; DSAP 0x16 Individual, SSAP 0xf6 Response
Skypilot_Broadcast LLC   I, N(R)=75, N(S)=38; DSAP 0xec Individual, SSAP 0x52 Response
Skypilot_Broadcast LLC   S, func=SREJ, N(R)=75; DSAP 0xd8 Group, SSAP PROWAY (IEC955) Network Management and Initiali
Skypilot_Broadcast LLC   U F, func=Unknown; DSAP 0x50 Group, SSAP 0x92 Response
Skypilot_Broadcast LLC   I, N(R)=75, N(S)=91; DSAP 0xa6 Group, SSAP 0x5e Command
Skypilot_Broadcast LLC   U, func=Unknown; DSAP Spanning Tree BPDU Group, SSAP 0x52 Command
Skypilot_Broadcast LLC   I, N(R)=75, N(S)=113; DSAP 0x9a Individual, SSAP 0x9a Response
Skypilot_Broadcast LLC   S P, func=REJ, N(R)=75; DSAP 0x6c Individual, SSAP 0x76 Command
Skypilot_Broadcast LLC   I P, N(R)=75, N(S)=16; DSAP 0x64 Individual, SSAP 0x68 Response
Skypilot_Broadcast LLC   I P, N(R)=75, N(S)=39; DSAP ISO Network Layer (OSLAN 1) Group, SSAP 0x30 Command
Skypilot_Broadcast LLC   I P, N(R)=75, N(S)=55; DSAP 0xea Group, SSAP 0xe2 Response
Skypilot_Broadcast LLC   S F, func=REJ, N(R)=75; DSAP 0x78 Group, SSAP Banyan Vines Response
```

WarDriving Summary

- Make sure you have channels right
- Not all networks have data on 802.11 compatible 4.9GHz
- Lots of proprietary protocols

Is 4.9GHz Being Targeted?

Front Page | **News** | Sports | Business | Entertainment | Opinion | Lifestyle

Home > Featured Articles > **Evanston**

Police: Hacker may have targeted Lemont's tornado sirens

July 03, 2012 | By Ryan Haggerty | Tribune reporter

Lemont police suspect that someone hacked into the village's tornado siren system, causing all seven sirens to sound for about 30 minutes, Police Chief Kevin Shaughnessy said today.

Three sirens were activated inexplicably in Evanston at 7:30 p.m. Saturday night, including two at fire stations, officials said.

A tornado siren on a Downers Grove water tower in 2008. (T...

Is 4.9GHz Being Targeted?

Front Page | News | Sports | Business | Entertainment | Opinion | Lifestyle

Home > Featured Articles > Evanston

Polic
torna

July 03,

Lemont p
into the v
all seven
Police Ch

Three sir
Evanstor
including

Home » Products » Technology » Telecommunications » Illinois village deploys unified broadband and video for safety

Illinois village deploys unified broadband and video for safety

Apr 23, 2008 12:00 AM

To enhance public safety, the village of Lemont, Ill., recently installed a municipal networked security system. The system integrates wireless video surveillance with broadband communications, allowing first responders to send high-speed data and streaming video over a licensed 4.9-GHz frequency. "Keeping Lemont's community, citizens and visitors safe and secure is our top priority," said Lemont Chief of Police Kevin Shaughnessy. Municipal broadband networks can integrate public-warning devices (such as sirens or tone-alert radios), first-responder notification (ranging from text alerts to telephone messages) and communications infrastructure (4.9- or 2.4-GHz frequencies and 900-MHz data networks). Federal Signal Corp., University Park, Ill.

Article Tools

Bookmark

Most Popular News

How's Your Pay?; NIGP 2012 Salary Survey

Tools to prevent inappropriate government spending

Movement to telework gaining a foothold in federal agencies

Want to use this article? Click here for options!

THE TRUCK BLUE BOOK

Is 4.9GHz Being Targeted?

Front Page | News | Sports | Business | Entertainment | Opinion | Lifestyle

Home > Featured A

Polic
torna

July 03,

Lemont
into the
all seven
Police Ch

Three sir
Evanstor
including

Home

Illin

Apr 23

Artic

Most

How's
Salary
Tools
gover
Move
a foot

THE TRUCK BLUE BOOK

New User? Register | Sign In | Help

Preview Mail w/ Y! Toolbar

YAHOO! ANSWERS

Search

HOME | BROWSE CATEGORIES | ABOUT

Ask What would you like to ask? Continue

Ans

What are you looking for? Search Y! Answers

Timmy

How do you hack into a tornado siren warning system and trigger the sirens from your home computer?

I'm totally just curious - I'm not planning on doing this

2 years ago

Report Abuse

github.com/opensecurityresearch

?

Robert.Portvliet@foundstone.com
Brad.Antoniewicz@foundstone.com

*many of the pics in this presentation were found on the internet – credit goes to images.google.com

References and Linkz

Previous ath5k Driver Patches: http://wiki.spench.net/wiki/RADAR

Supported Atheros chipset list http://wireless.kernel.org/en/users/Drivers/ath5k#Supported_Devices

RTL-SDR compatibility list - http://www.reddit.com/r/RTLSDR/comments/s6ddo/rtlsdr_compatibility_list_v2_work_in_progress/

"DVB-T TV Receiver Realtek RTL2832U Elonics E4000 Radio P335", and "Ezcap EZTV668" used for testing

Ettus Research https://www.ettus.com/product/details/VERT2450

Pasadena Networks http://www.wlanparts.com/product/SF-D49NSR/49GHz-53dBi-Black-Fiber-N-male.html

Business Systems Connection http://shop.bizsyscon.com/proxim-orinoco-a4908-4-9ghz-4-99ghz-8dbi-omni-antenna/ - Didn't steal Brad's credit card, should be ok..

Discone antennas do 25-1300MHz http://www.rfparts.com/diamond/d130j.html

Build your own http://helix.air.net.au/index.php/d-i-y-discone-for-rtlsdr/

http://www.ve3sqb.com/s

Kind of hard to find. Expensive in most cases..

Horizon 12dBi Omni, 5750-6150MHz http://interline.pl/modules/content/index.php?id=1&s=showcard&code=INT-HOR-12/57-V&lang=english

MTI 17/19dBi, 4.9-6.1GHz

- http://www.wlanparts.com/product/MT-465019NVD/MTI-Wireless-Edge-MT-465019NVD-Triple-Polarity-1719dBi.html
  - $192

Weirdness..

MN:

```
Frame 14: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits)
PPI version 0, 60 bytes
IEEE 802.11 Deauthentication, Flags: ........C
    Type/Subtype: Deauthentication (0x0c)
    Frame Control: 0x00C1 (Normal)
    Duration: 1
    Destination address: 49:00:49:c9:30:07 (49:00:49:c9:30:07)
    Source address: 28:00:de:4d:84:0f (28:00:de:4d:84:0f)
    BSS Id: de:4d:84:0f:de:4d (de:4d:84:0f:de:4d)
    Fragment number: 3
    Sequence number: 3960
    Frame check sequence: 0x6a2eb0ab [correct]
IEEE 802.11 wireless LAN management frame
    Fixed parameters (2 bytes)
    Tagged parameters (42 bytes)
[Malformed Packet: IEEE 802.11]
```

NJ:

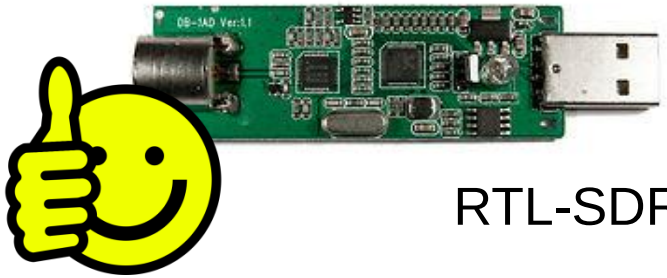
```
Frame 19: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)
PPI version 0, 32 bytes
IEEE 802.11 Deauthentication, Flags: ........C
    Type/Subtype: Deauthentication (0x0c)
    Frame Control: 0x00C1 (Normal)
    Duration: 1
    Destination address: HarrisCo_b1:2a:87 (01:00:c3:b1:2a:87)
    Source address: 28:00:00:00:00:00 (28:00:00:00:00:00)
    BSS Id: de:4d:84:1d:de:4d (de:4d:84:1d:de:4d)
    Fragment number: 3
    Sequence number: 3640
    Frame check sequence: 0x6dfceac6 [correct]
IEEE 802.11 wireless LAN management frame
    Fixed parameters (2 bytes)
    Tagged parameters (42 bytes)
[Malformed Packet: IEEE 802.11]
```

Interacting with APCO P25

GNU Radio

osmocomOP25

- Attacks:
  - http://www.crypto.com/papers/p25sec.pdf
  - http://www.nicta.com.au/pub?doc=5076



RTL-SDR