

# Mesh Networks | Hacking The T3lc0 Model



<http://arig.org.il>

# What's a Mesh Anyway ?

- ◆ Mesh = topology. anything not a star / bus / ring / tree
  - ◆ Nodes = routers, smart phones, cars – anything
  - ◆ Links = wireless connections
- ◆ Mesh Network Attributes:
  - ◆ Self-organizing
  - ◆ Self-healing
  - ◆ Scalable
  - ◆ Robust, hard to disconnect


# Mesh Node Recipe

- ◆ 1x 802.11 compatible radio device
- ◆ 1x radio driver, eg. atheros
- ◆ 1x Foss OS: eg. OpenWRT
- ◆ 1x Mesh Protocol
  - ◆ BGP, layer 7 ( uses TCP, port 179 ) & OSPF ( IP datagram encapsulated )
  - ◆ OLSR, layer 3 ( uses UDP packets )
  - ◆ B.A.T.M.A.N, layer 2 ( raw ethernet frames, kernel module)

```

- - - - -
|_| W I R E L E S S   F R E E D O M
- - - - -
KAMIKAZE (8.09, r13118) -----
* 10 oz Vodka           Shake well with ice and strain
* 10 oz Triple sec     mixture into 10 shot glasses.
* 10 oz lime juice     Salute!
-----
root@OpenWrt:/#
```

# Radio

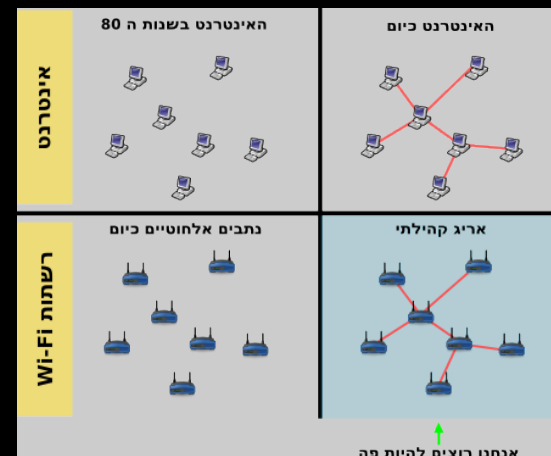
- ◆ Use of public 2.4GHz & 5GHz bands
- ◆ No special license to operation
- ◆ 3.7GHz also recently made available
- ◆ Open Spectrum: public radio frequency access
- ◆  **openspectrum.eu**
  - ◆ Open Source Cell Phone Network at \$2 per month

# Mesh Protocols

- ◆ Protocol Tasks:
  - ◆ Node announcement
  - ◆ Neighbor sensing
  - ◆ Routing table upkeep
  - ◆ Routing decisions
- ◆ Protocol Efficiency Metrics
  - maximize: raw data
  - minimize: control Data / ( control Data + raw Data )
- ◆ > 70 implementation, lots of academic Interest

# The Problem

- ◆ Present Routers, No Inter-Communication
- ◆ Low Service Improvement Incentive
- ◆ Centralized Power, Censorship
- ◆ No Service Improvement Incentive
- ◆ Infrastructure Vulnerability:
  - ◆ Crisis Scenarios
  - ◆ Cellular Service Failure (Cellcom, 2010)



# ~~The Solution~~

## part of a **Solution: Mesh Network**

- ◆ Open Mesh:
  - ◆ Open Source, Open Standards
  - ◆ Affordable
- ◆ Community Owned
- ◆ User Operated
- ◆ Induce ISP Service Improvement (mozilla effect)

# History, by Device: WRT54G

- ◆ Story of the Source Code:

- ◆ 1. Andrew Miklas posts on the Kernel Mailing List:

```
# dd if=WRT54G_1.02.1_US_code.bin of=test.dump skip=24577c bs=32c  
# mount -t cramfs test.dump /mnt
```

- ◆ 2. GPL requires Linksys to publish source code

- ◆ 3. pressure...

- ◆ 4. \$\$\$ profit! : Linksys open sourced the WRT54G firmware in July 2003

- ◆ A 60\$ turns into a 600\$ corporate router !

- ◆ Unlocked features:

- ◆ shell access,

- ◆ run VPN / VoIP servers,

- ◆ use as a repeater or a bridge → mesh possible





# History, by Device - XO-1

- ◆ 100\$ laptop per child Project
- ◆ Mesh to Provide Classroom & Village connectivity
- ◆ Partial 802.11s implementation ( no security for example )
- ◆ Plug-n-Play, at least in theory:
  - # iwconfig msh0 mode ad-hoc channel 13 essid hello-mesh-world
  - # ifconfig msh0 <IP address>
- ◆ Disappointing real-world performance
  - ◆ Low powered radio → short range



# History, by Network: Consume.net

- ◆ England, 2001,
- ◆ Context: dialup, 512Kbps = \$60,000
- ◆ Clink Street Building Internet Sharing:  
Artists, Photographers, Filmmakers, etc.
- ◆ Expand to 2<sup>nd</sup> building → cross a 5m wide street:  
running cables across the street is illegal !
- ◆ Buy a \$4000 Breezecom AP10 ( 2Mbps, 100 users, 4 years uptime! )
- ◆ Low cost, 802.11b PCMCIA cards
- ◆ motto: Consume the net !



# Pico-Peering Agreement



- ♦ Written by the Consume.net founders. Key points:
  - ♦ Free Transit:
    - ♦ Owner agrees to provide free transit across their free network.
    - ♦ Owner agrees not to modify/interfere with data as it passes through their free network.
  - ♦ Open Communication:
    - ♦ The owner agrees to publish the information necessary for peering to take place
    - ♦ This information shall be published under a free license
    - ♦ The owner agrees to be contactable and will provide at least an email adress
  - ♦ No Warranty
  - ♦ Terms of Use:
    - ♦ The owner is entitled to formulate an 'acceptable use policy'
    - ♦ This may or may not contain information about additional services provided

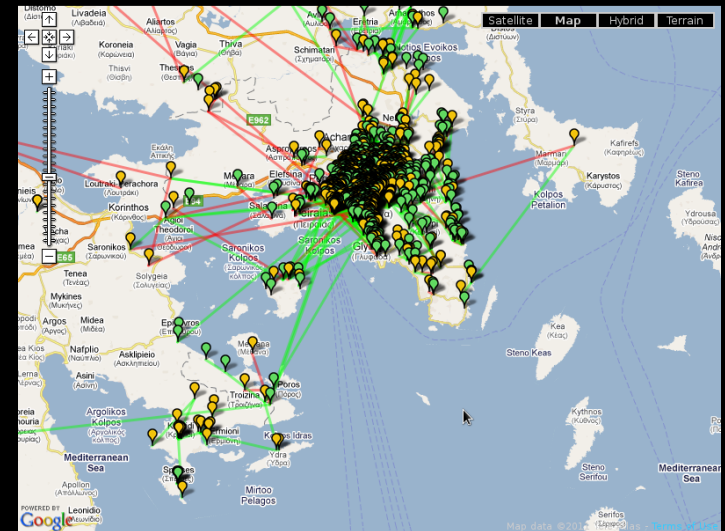
# History, by Network: Freifunk

- ♦ Germany, 2002
- ♦ Context: Post Unification, East-Germany:
  - ♦ Fiber Internet project:
    1. rip out all PSTN copper
    2. install fiber lines
  - ♦ Project budget overrun → end users left with nothing !
- ♦ Early Start: PCs on rooftops
- ♦ Very fast adoption
- ♦ Active today, strong hacking culture



# History, by Network: **AWMN**

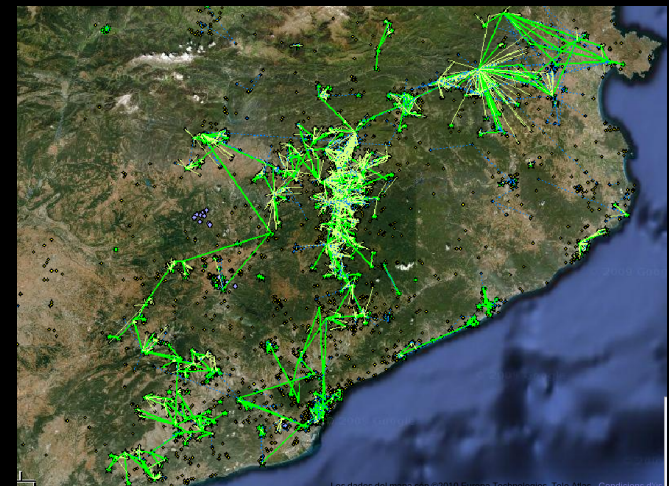
- ◆ Greece, 2002
- ◆ Small group of dissatisfied tech'ies
- ◆ ~1120 backbone nodes, > 2500 ap clients
- ◆ DIY mentality

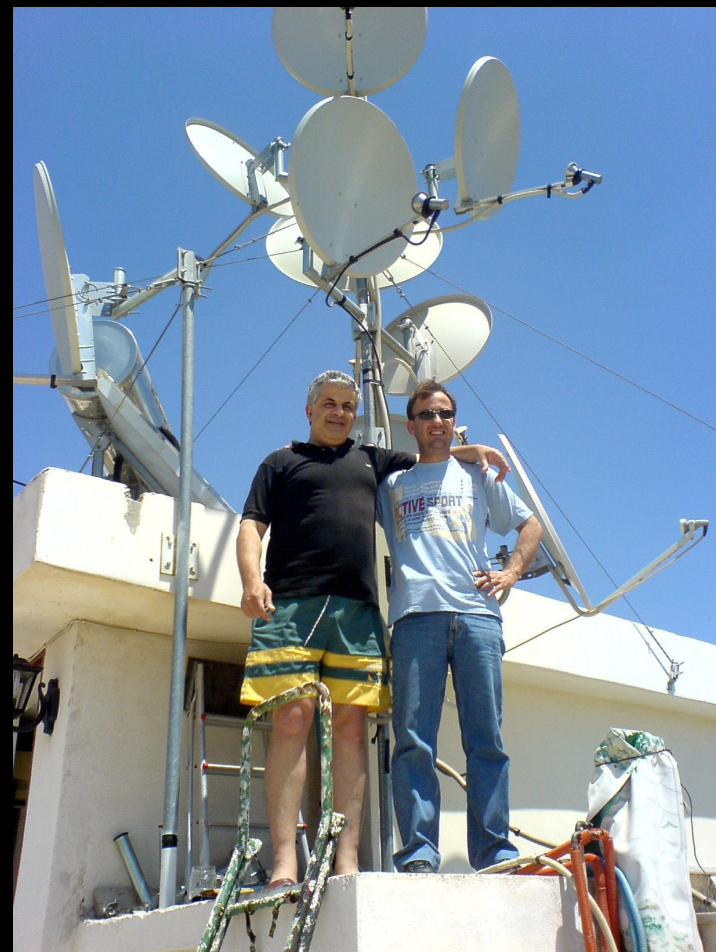


# History, by Network: Guifi.net



- ◆ Catalonia, 2004
- ◆ Context: poor Internet access in rural areas
- ◆ ~13.500 nodes - likely the biggest in the world
- ◆ Lots of accumulated experience
- ◆ Strong community back





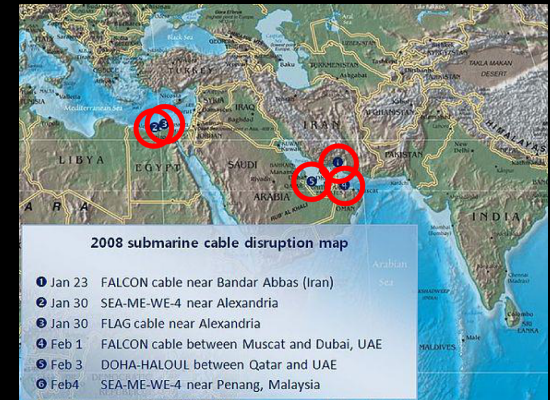
# Mesh Network Services

- ◆ Network wide: IP assignment, DNS
- ◆ Mass Communication:
  - ◆ VoIP
  - ◆ Municipal Notification Service, e.g. Shderot
  - ◆ Broadcast, Multicast: local radio, podcasts, etc.
- ◆ P2P services: file sharing, social networks
- ◆ Distributed Services: cache, backup, DNS
- ◆ Sensor Networks



# In the News...

- ♦ Mediterranean, 2008: Submarine Cable Disruption
  - ♦ 5 ! cables cut
  - ♦ Israel only connected with two
- ♦ Israel, Dec. 2010:
  - ♦ Cellcom Service Downtime
- ♦ Egypt, Jan. 28 2011 ( see also: Yeman, Lybia, Syria ):
  - ♦ Internet shutdown. nothing fancy, simply power off !
- ♦ Disruptions third world exclusive? no:
  - ♦ Aug. 2011, San Francisco: BART cut cell service to avert protest
- ♦ US, 2011, State Department:
  - ♦ spending > \$70 million on “shadow networks”




# Israel, 2011: Internet = 'קוטג' ?

- ◆ Users forced into dual subscription: ספק, תשתית, the only country !
- ◆ Slower speed = more money
- ◆ Private, al la 'NGN' style user separation

The screenshot shows the Globes website interface. At the top, there are navigation links for 'English', 'תוכן', 'חדש', 'הסדרה', 'מחירים', 'ניוזליים', 'ערוץ דיגיטלי', 'הפוך לעמוד הבית', and 'אמייל ארום'. Below this is a 'BUYBACK' banner with the LANIA logo and the slogan 'The Power to be Different'. A navigation bar contains buttons for 'חדשות', 'פורטל פיננסי', 'תיק אישי', 'מלולר', 'גלובס TV', 'Tools', 'נייץ', and 'חיפוש'. A secondary navigation bar includes 'ראשי', 'שוק הון', 'חול סמריט', 'נוונפמ', 'היי טק', 'גדל"ן', 'נתח שוק וצרכנות', 'דין וחשבון', 'קריירה', 'רכב', 'ספורט', 'פנאי', and 'דסק'. The main content area features a red banner with the headline 'לקוחות ה-NGN בבזק בינלאומי ייהנו מרשת נפרדת' (NGN customers in Bezeq International will benefit from a separate network). The article text below the headline reads: 'המשמעות היא שכל לקוח שישדרג את מהירותו ל-10 מגה ינותב לרשת תקשורת ייעודית שנבנתה במטרה לקדם את הגלישה המהירה ברשתות החדשות ויעבור לשירות לקוחות ייעודי שיטפל ב...'. To the left of the article is a sidebar with a 'דפדף' (scroll) button, 'פריטיות' (favorites) with a plus sign, and 'מוקבים' (bookmarks) with a plus sign. An image of a computer monitor displaying financial data is visible on the left side of the article.

# Israel, 2011: The 'Law'

## ♦ תיקון חוק לשון הרע :

  
**בתי המשפט**

הפ 000250/08

**בבית המשפט המחוזי בתל-אביב-יפו**

לפני: כבוד השופטת ד"ר דרורה פלפל / ס. נשיא

**בעניין:**

1. חברת ברוקר טוב בע"מ
2. סמואל עידו

ע"י ב"כ עו"ד א' אילון

**המבקשים**

נ ג ד

1. חברת גוגל ישראל בע"מ
2. הוט טלקום שותפות מוגבלת
3. חברת ביזנס נט מידע מקוון בע"מ
4. חברת טלנירי בסט אינווסט ניהול השקעות ומינסיס בע"מ
5. מכללת מגמות המרכז ללימודים פיננסיים ושוק ההון
6. חברת Be Trader בע"מ
7. חברת Level 2 בע"מ

**המשיבים**

**פסק-דין**

**מהות התובענה**

א.

זו בקשה בה עותרים המבקשים מבית המשפט להורות למשיבה מס. 1 להמציא לידיהם בתצהיר את כל המידע והפרטים בעבר ובהווה המוחזקים בידה או בשליטתה הקשורים במישרין ובעקיפין לכתובות הדוא"ל rokerate@gmail.com ו- lior@brokertov.com, לרבות שמם המלא של בעלי כתובות הדוא"ל וכתובתם הפיזית.

**הכנסת השמונה-עשרה**

הצעת חוק של חבר הכנסת

זבולון אורלב

---

2476/18/פ

**הצעת חוק איסור לשון הרע (תיקון – חשיפת פרטי מעוול), התש"ע-2010**

1. החספת סעיף 9א 1. בחוק איסור לשון הרע, התשכ"ה-1965<sup>1</sup>, אחרי סעיף 9 יבוא:

"חשיפת פרטי מעוול

9א. (א) אדם הסבור כי מידע שהופץ ברשת האינטרנט הכיל לשון הרע עליו, רשאי להגיש המרצת פתיחה נגד ספק שירותי האינטרנט המחזיק בפרטי המפץ בבקשה שיחשוף את זהותו של מפץ המידע; לענין סעיף זה, "מפץ" – משתמש אתר האינטרנט המעלה תוכן מכל סוג שהוא לאתר, למעט מנהל אתר האינטרנט או אדם אחר מטעמו.

## ♦ חשיפת פרטי גולשים:

Are we happy with this  
design ?

# פרוייקט אריג

- ◆ Israel is way behind - about ~10 years !
- ◆ Vision:
  - ◆ Open, Community dedicated mesh
  - ◆ אריג != ISP
  - ◆ ISP, אריג co-existence
  - ◆ Community owned, operated
- ◆ Learn from past attempts
- ◆ Israeli housing protest: inter camp connection effort
- ◆ Global Cooperation - Funkfeuer.at:
  - ◆ CNDB ( common node DB schema ) development
  - ◆ Borrowed public IPv6 block



# Technical Challenges

- ◆ Spectrum Congestion
- ◆ Limited Wi-Fi Range
- ◆ Central Network Services:
  - ◆ Node ID Assignment: IP / MAC
  - ◆ DNS Servers
- ◆ Layer 8: User Resource Sharing

# Sustainability is Key

++node operators, **not** nodes.

++mesh communities, **not** mesh networks.

# Security

- ◆ OpenWRT Dual-Mode:
  - ◆ WPA enabled private network
  - ◆ Ad-hoc public network
- ◆ Is an open AP really a security risk ?
- ◆ Preventing, dealing with abuse
- ◆ Security at the protocol level: GNUnet





The End,  
Thank You

<http://arig.org.il>

