Off Grid Communications with Android:

Meshing the Mobile World

Josh Thomas | Research Consultant, R&D Team
Accuvant Labs | http://www.accuvant.com

/whoami

- ~ software engineer for the last 12 years
- Spent too much time working inside faraday cages
- Got bored writing my own bad code, figured it would be more fun to poke holes in other people's work
- I like to:
  - break / embed / repurpose things
  - solder things into other things
  - stare at asm
- jthomas@accuvant.com / m0nk.omg.pwnies@gmail.com
- @m0nk_dot

/team & project

- SPAN is an Open Source research project initially funded by the MITRE Corporation for use in Emergency Preparedness and Response situations
- Team:
  - Jeff Robble (mistr.stoker@gmail.com) - (MITRE) Lead Developer and currently running the MITRE effort
  - Nick Modly - (MITRE) Visualizations
  - Oliver Chong - (MITRE) Routing Algos and Security

MITRE

ACCUVANT LABS
Security Research and Assessment

Will he start already?

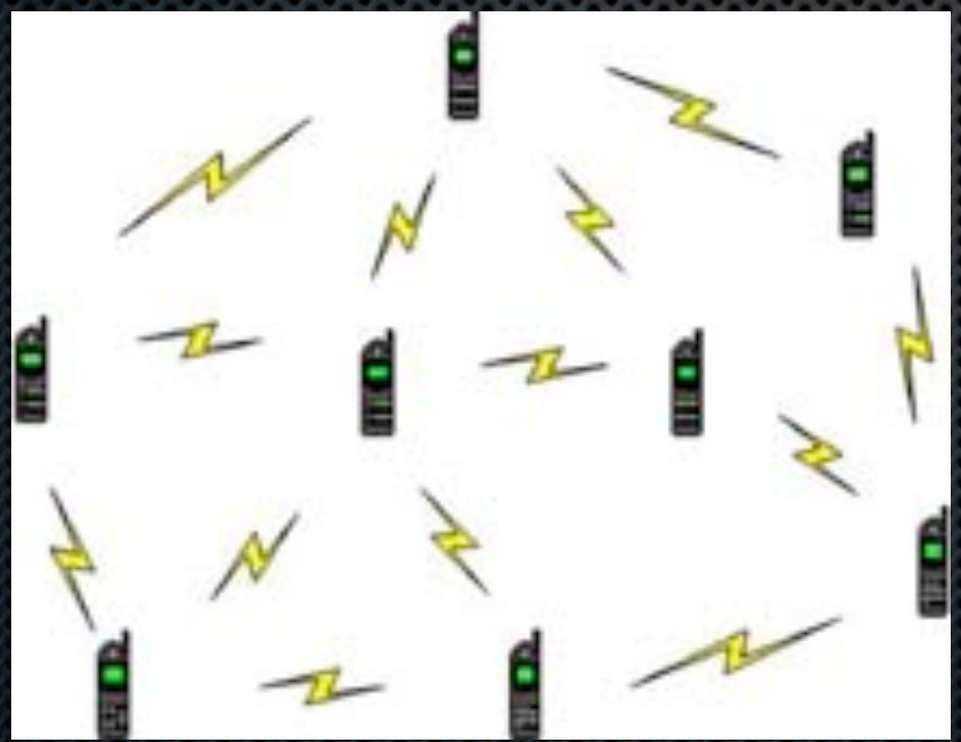
- What is a MANET?
- Why do I care about mesh networks?
- What is the SPAN project?
- Finally something technical - the guts of a mesh
- Baseball & Terrorism
- </end_session>

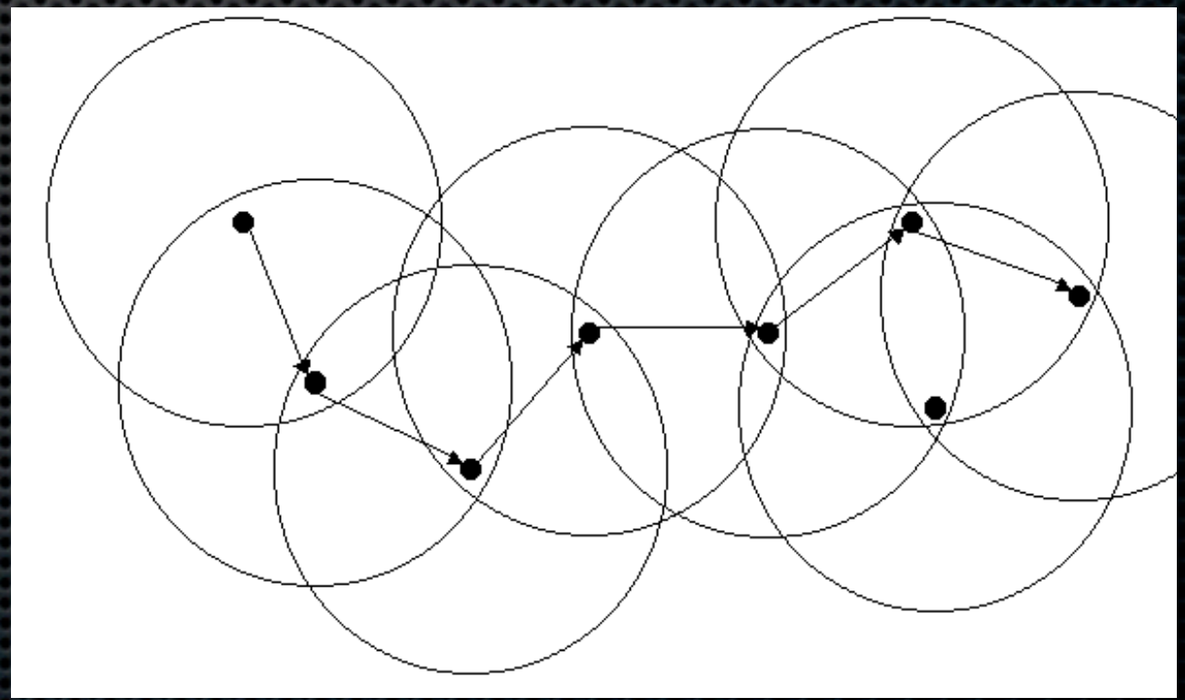
- TL;DR:
  - www.omg-pwnies.com
  - https://github.com/monk-dot

ACCUVANT LABS
Security Research and Assessment

Daddy, What's a Mesh Network?

- It's exactly like graph theory except:
  - Nodes are shiny electronic gadgets that run out of battery and move around a bunch
  - Vertices are unstable and based on arbitrary signal strength
  - The pics are uglier





ACCUVANT LABS
Security Research and Assessment

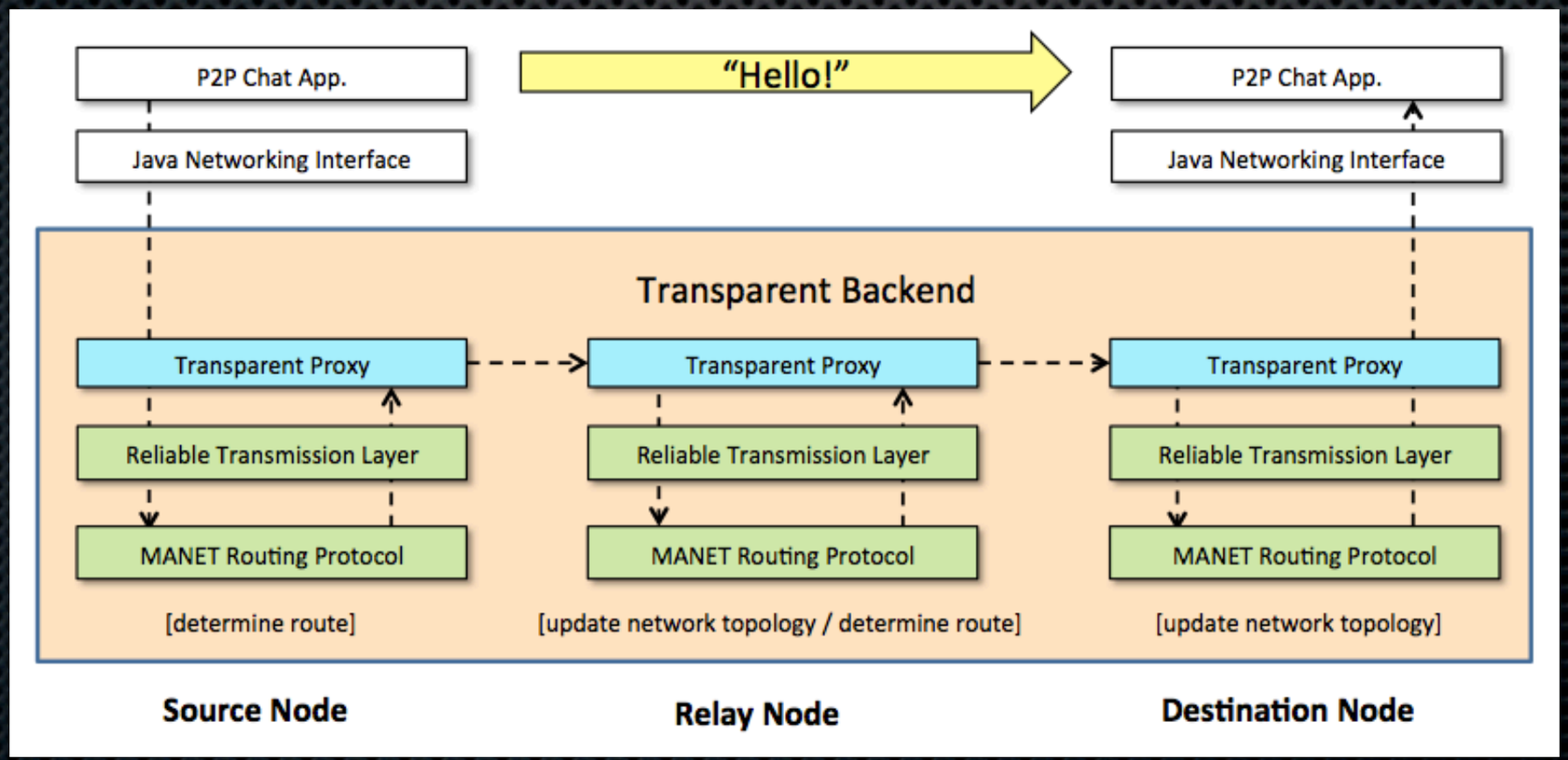
Ok, but why?

- WHY:
  - Fukushima, Haiti, Katrina, ...
  - Arab Spring
  - Normal <insert cellular company here> Service
- Physical infrastructure is prone to failure, networks shouldn't be
- Share information when networks are broken or untrustworthy
- Infrastructure is a single point for data sniffing and filtering
- Headless networks are cool!

ACCUVANT LABS
Security Research and Assessment

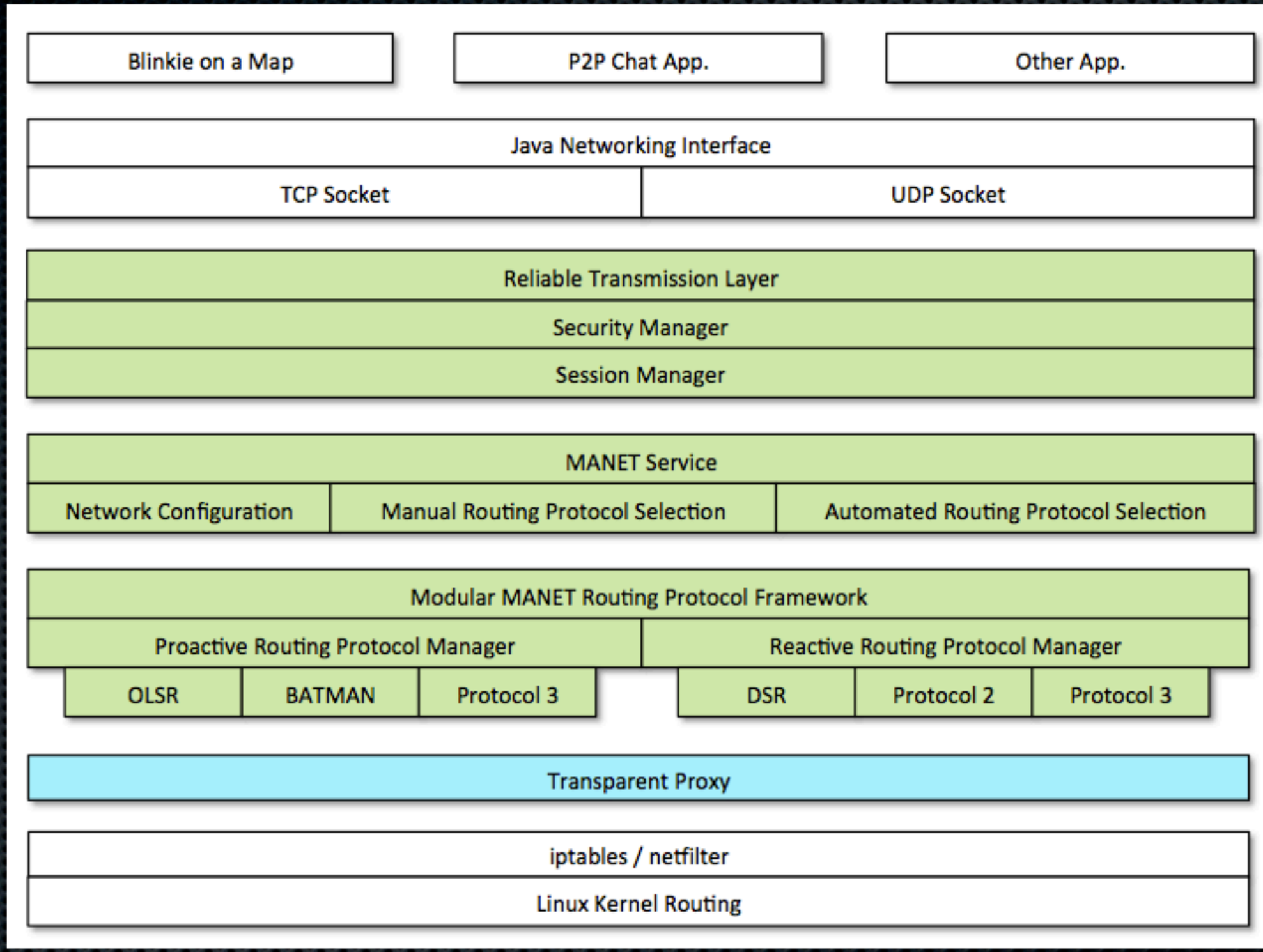
The SPAN Project

- There are too many headaches involved in starting MANET research before you actually get to the hard problems
- Simple framework implementation for MANET - Smart Phone AdHoc Networking
- A transparent proxy so normal applications just work
- Initially a MITRE funded research project, now open source



ACCUVANT LABS
Security Research and Assessment

The Stack



Hard problems that shouldn't be hard

- WiFi chip manufactures:
  - Broadcom 4329 - Samsung Galaxy Nexus, Samsung Nexus S 4G, Nokia Lumia 900, older iPhones, Asus Transformer Prime, many more
  - Broadcom 4330 - Samsung Galaxy TAB 10.1, Samsung Galaxy S II / Epic Touch 4G, iPhone 4S, many many more
  - TI WL1285C - Motorola Razr / MAXX
  - Qualcomm - A ton of Android Phones
  - Murata - iPhone 5 (possibly a re-brand)
- Vendors that muck with open source projects and lock things down (for a reason normally)
  - Sprint / AT&T / Verizon / HTC / Motorola / Blah Blah Blah

ACCUVANT LABS
Security Research and Assessment

Ok, will my _X_ phone work?

- We need to be able to lock the WiFi Chip out of managed mode
  - You know how your phone sometimes scans for networks to join? We need to keep the chip in that mode

- Android kernel needs Wireless Extensions support enabled
  - Q: Why would you turn this off?
  - (A: To fight unpaid tethering)

- In short, if you can jailbreak / root your phone, run C & Java code and can somewhat control the WiFi hardware then yes, it will work (Android / iOS / Arduino / Linux / Windows /

Hard Problems that are in fact hard

- Routing
  - Proactive vs. Reactive
  - Sensor based routing
  - Other mesh & routing projects
    - OLSRd
    - SERVAL / BATMAN
    - Byzantium Mesh
    - FreiFunk
- Network Scale / Speed and Power consumption
- MANET configuration - PACMAN?
- Security

ACCUVANT LABS
Security Research and Assessment

I sleep in packets

- Mobile Devs want to save battery life so...
  - By default Android likes to filter and trash UDP packets when the screen is off.
  - First, we tried grabbing a wake lock and dimming the screen ourselves (this is what is commonly known as an ugly hack)
  - Then we found this:
    - dhd_pkt_filter_enabled=0 in the WiFi kernel module
    - Solved!

ACCUVANT LABS
Security Research and Assessment

??? Security ???

- Securing a mesh is awkward
- The SERVAL project has a fairly cool way of using the public key as the device address but devices still requires manual configuration
- We can use the MAC to auto-generate an IPv6 address, but it breaks the SERVAL paradigm
- We can use NFC / Bluetooth / Whatever to exchange keys when a device joins a network but that massively shortens the distance between nodes
- Enclaves across untrusted nodes
- Enclaves over internet bridges

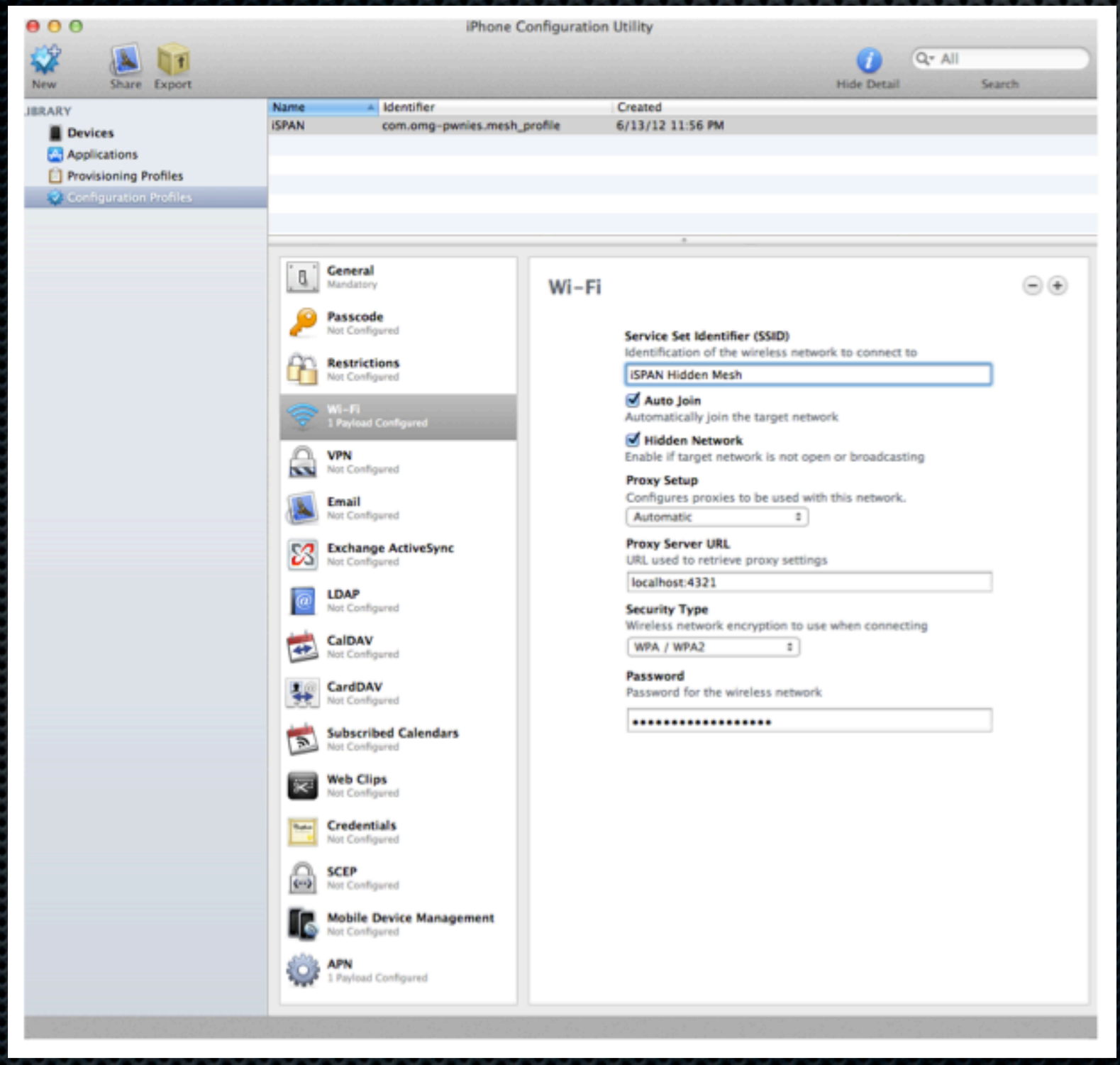
<Odd_Problem>

- Both the Samsung Galaxy Nexus and the Epic Touch 4G devices we were testing with contained the BCM4330 chipset
- They could join the same network but once ~10 ET4G devices joined, the SGN phones just disappeared
- After many headaches, we found the devices were broadcasting at different wavelengths / waveforms and at different signal strengths
- The ET4G devices were actually creating a sort of white noise that cancelled the lower power transmission out
- These are the odd problems from software controlled power / signal strengths

</Odd_Problem>

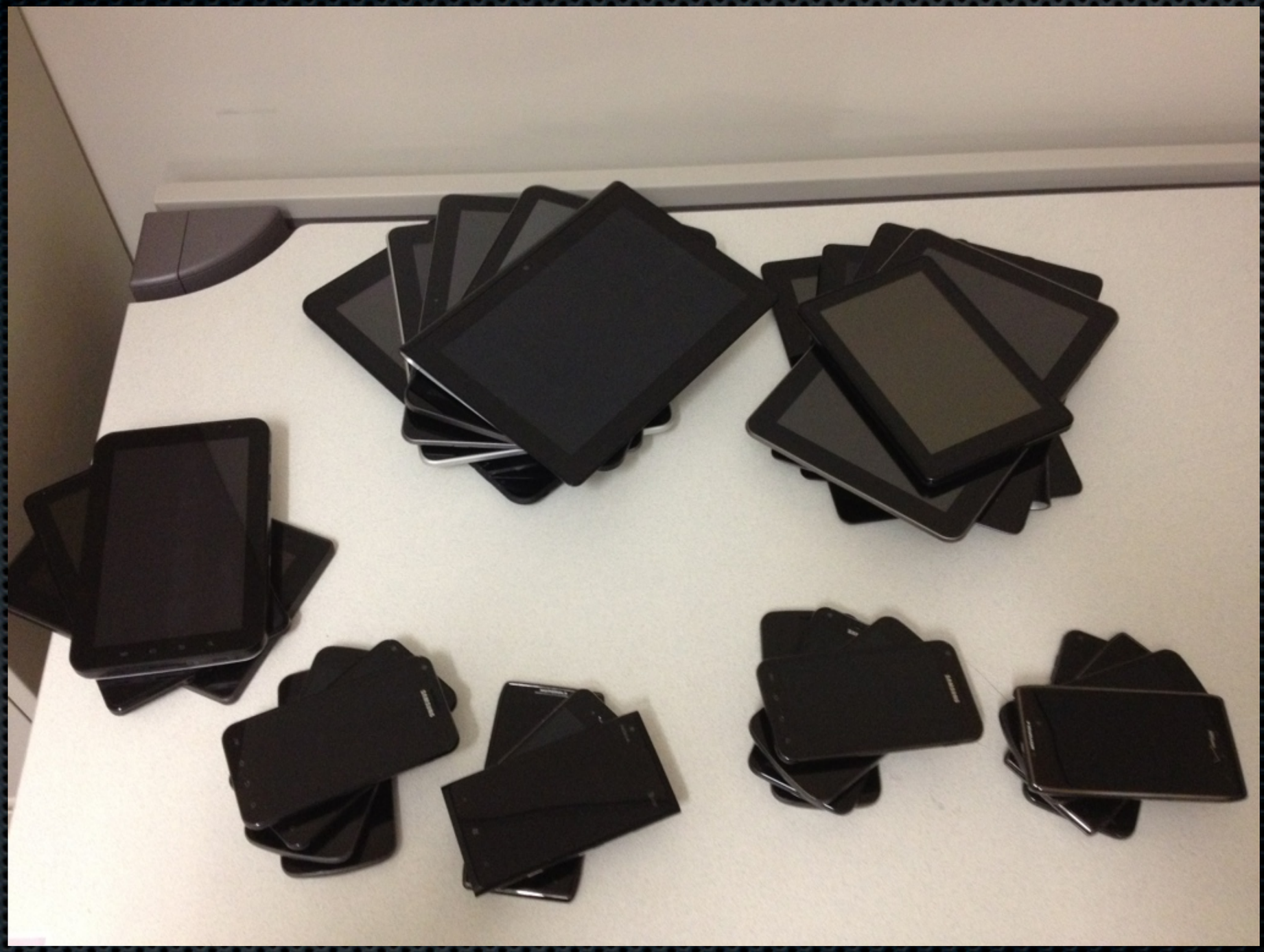
ACCUVANT LABS
Security Research and Assessment

What about iOS?



ACCUVANT LABS
Security Research and Assessment

A Short story in 7 Pictures & 9 Words



ACCUVANT LABS
Security Research and Assessment

Terrorists love Baseball

ACCUVANT LABS
Security Research and Assessment

Hotels hate me

ACCUVANT LABS
Security Research and Assessment

Snipers hate Engineers

ACCUVANT LABS
Security Research and Assessment

Questions? Comments?

https://github.com/monk-dot

http://www.omg-pwnies.com

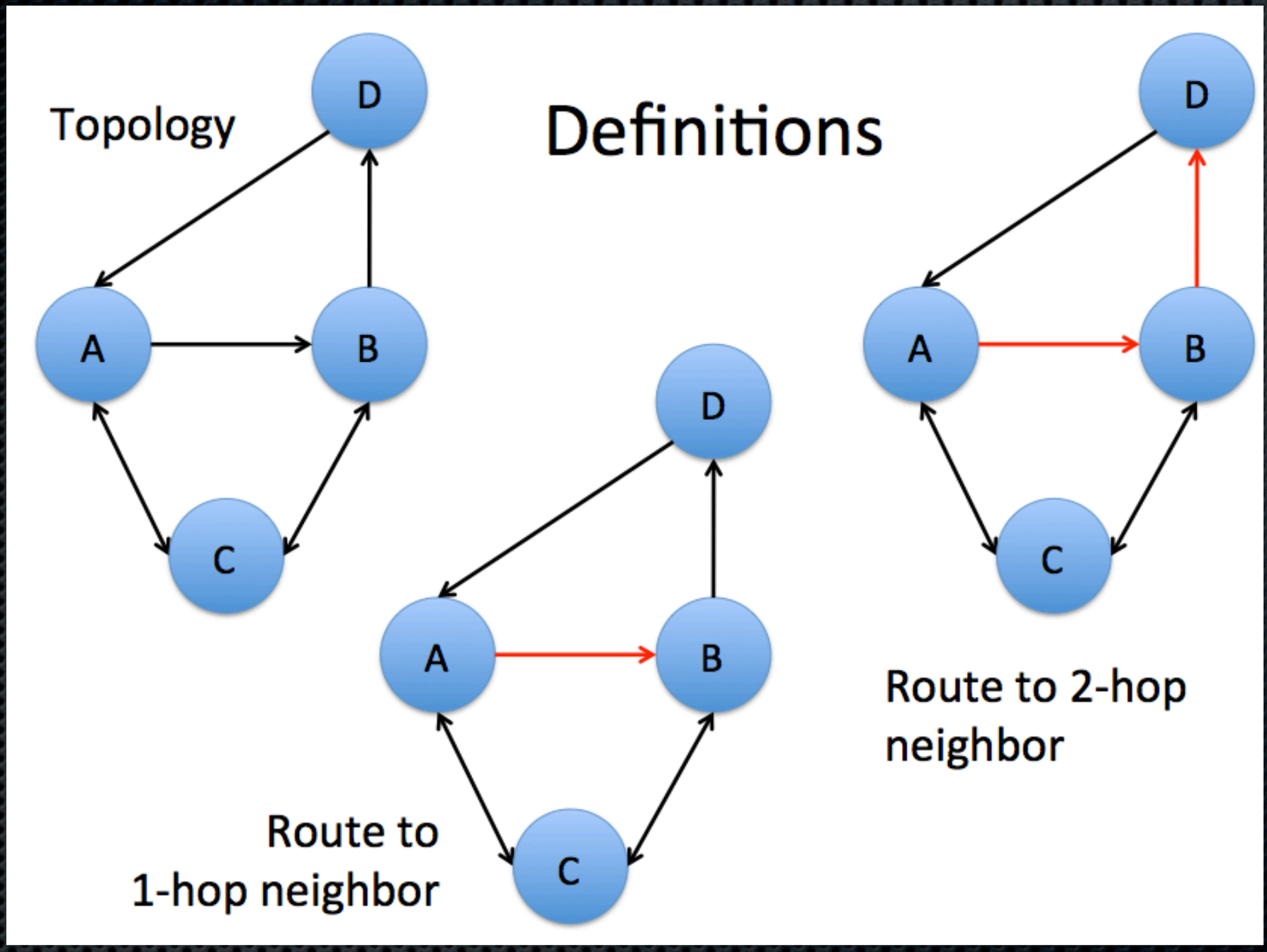
- </talk>

The Links

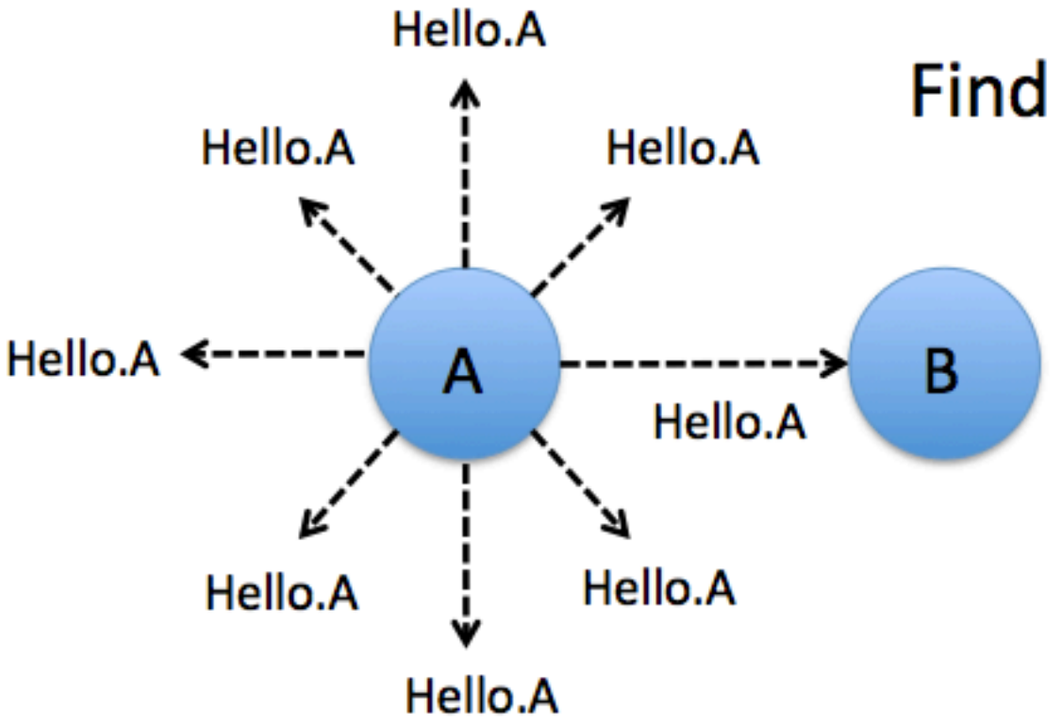
- http://code.google.com/p/android-wifi-tether/
- http://www.olsrd.org
- http://www.servalproject.org
- http://berlin.freifunk.net
- http://project-byzatium.org

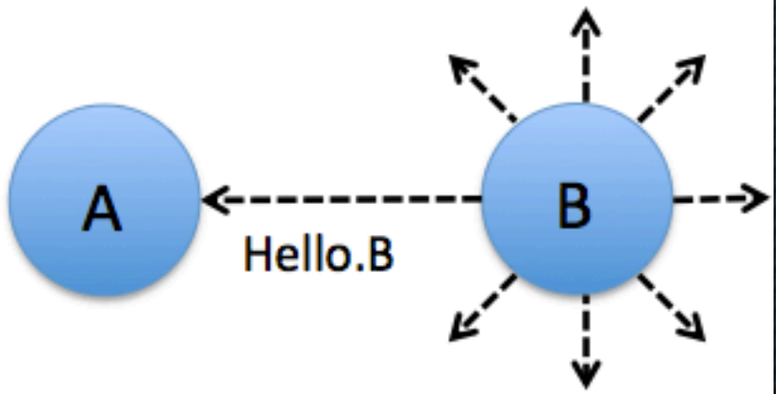
Backup Slides

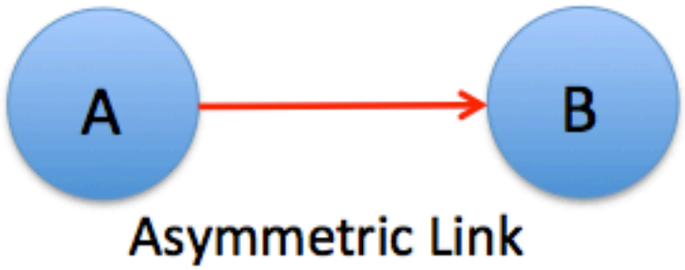
Routing Protocol Pics (or it didn't happen)



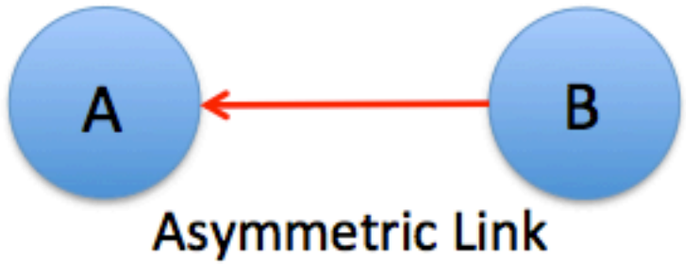
Find 1-hop neighbors







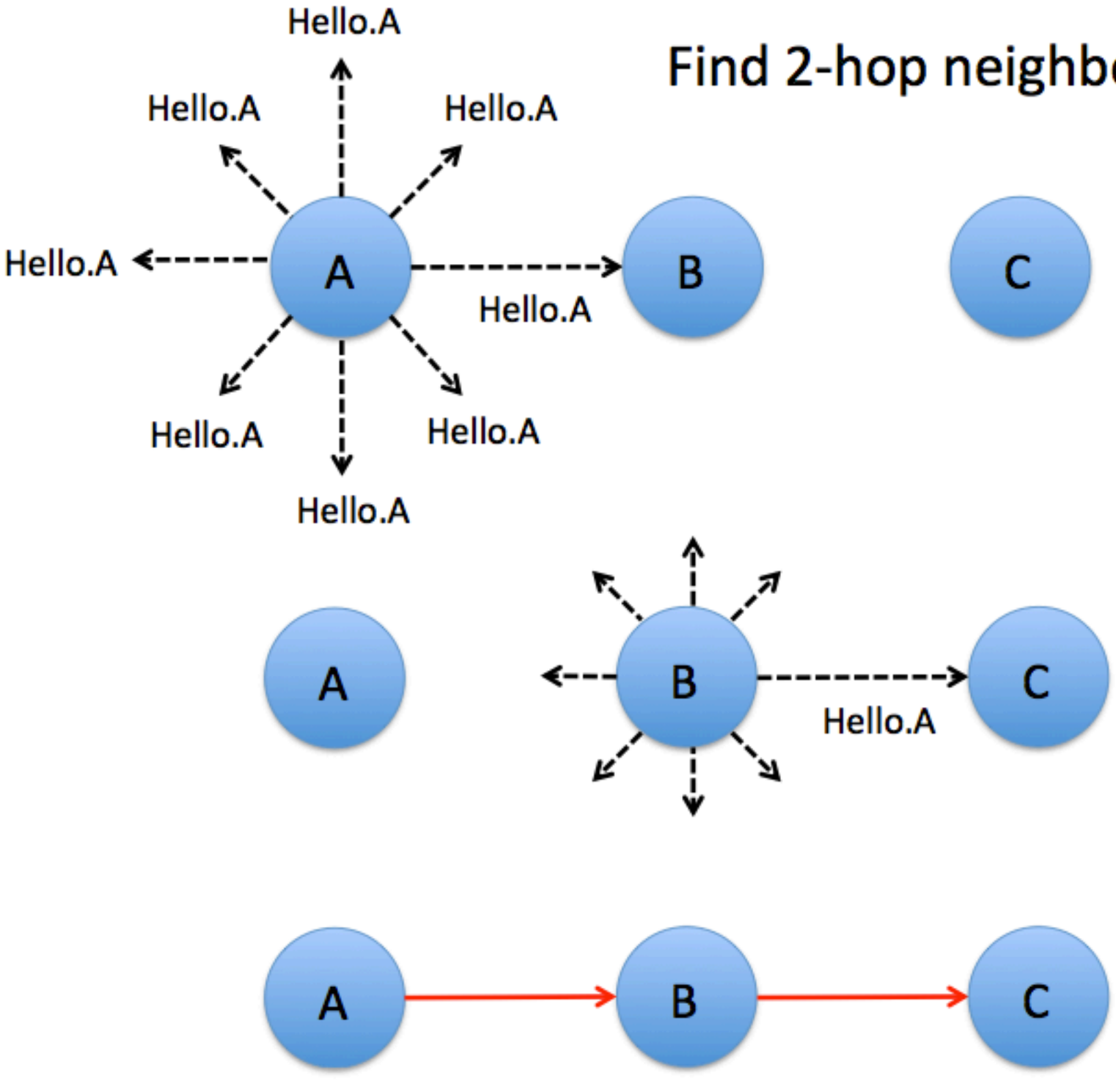
Asymmetric Link



Asymmetric Link

Symmetric Link

Find 2-hop neighbors



Multi-Point Relay