Wireless Network Design & Architecture

SANOG

Matt Peterson

Bay Area Wireless Users Group

Rajendra Poudel

Nepal Wireless/ENRD

This afternoon’s agenda

- Our backgrounds/CV
- An overview of WLAN/802.11 concepts
- Ecosystem / industry users
- Knowledge to apply to these models
- Install “lessons learned from the field”
- Resources
- More Q&A

Matt’s CV

- PlayaNET - Intranet in desert
- BAWUG - Founder of educational WLAN non-profit
- Independent Consultant
  - International hotspot firm
  - National WISP
  - Other small firms
- *Authority Figure*
  - USA Today, Wall St Journal, Wired, etc

Bay Area Wireless Users Group

BAWUG

- Est. September 2000
- Founded by IP and RF clued folks to educate the masses
- Bi-monthly meetings, active 2000+ subscriber mailing list
- Model as non-profit, currently in-formal
- Affiliated with FreeNetworks.org; an umbrella organization of CWN's (Community Wireless Networks)
- “We don't build networks” - supply the knowledge, roll your own

SPUTNIK

802.11 PLANET

The New York Times

USA TODAY

techtv

APRICOT Bangkok 2002

O'REILLY EMERGING TECHNOLOGY CONFERENCE.

Rajendra’s CV

- ENRD - Research organization
- Nepal Wireless - Team member (Voluenter based Project)
- Collage of Information & Technology - Lecturer
- CCNA, CCNP & MCSE

Afternoon modeled after BoF

- No sales pitch
  - PLEASE be interactive, interruptions are welcomed (and encouraged!)
  - We’re not experts, technology is constantly changing (not a day job’s); here to share experiences
- Not today
  - Bluetooth, HomeRF, HiperLAN, 802.16 “WiMAX” (will briefly touch base)
- What would you like to learn today?
  - Name, home country, goals
  - We’ll attempt to “tune” the workshop towards the audience

Industry Overview

- Starting to mature (vs VoIP); plenty of room for innovation (better routing protocols, antenna “magic”, etc)
- Extremely well adopted technology, some claim faster adoption rate then 100Mb switched Ethernet
- WiFi = trade org to certify equipment compatibility (enforce the IEEE standards); also a brand-name (a.k.a. WiFi Alliance)

Wi Fi® CERTIFIED

CISCO SYSTEMS

LINKSYS®

intel inside centrino™ MOBILE TECHNOLOGY

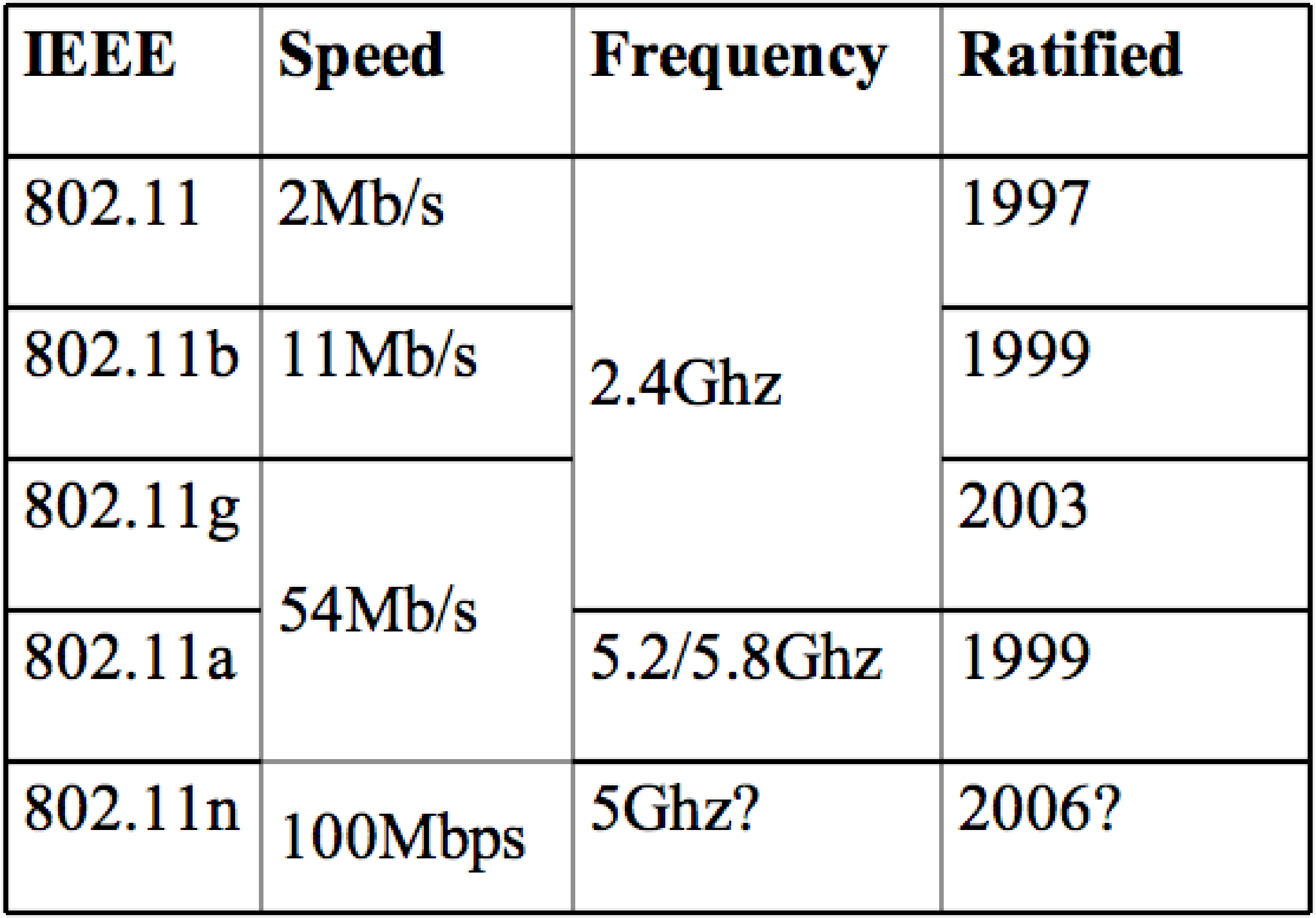
Why 802.11x Wireless?

- **End-to-end**
  - *eliminate telco/monopoly "partner"*
- **Bandwidth**
  - *own infrastructure, scale as needed*
- **Fast**
  - *anywhere from 0 to ~25Mb/s (real-world throughput)*
- **Unlicensed**
  - *no licensing/bidding, zero to limited recurring cost*
- **Standards**
  - *very economical, mass production, plug-n-play*

Why *not* 802.11x Wireless?

- Typically, we’re secondary band users, primary being government; also must accept interference (X10 “spy” cameras, cordless phones, baby monitors) or illegal entirely
  - Low power and above interference susceptible
- Line-of-sight required (tree’s are the enemy)
- Anyone can use it (just like walkie-talkies, ***requires*** some level of coordination for high congested areas)
- Doesn’t scale for large deployments (802.11 = **W**ireless **L**ocal **A**rea **N**etwork.. Not WAN)
- Insecure “out of the box” (factory direct)

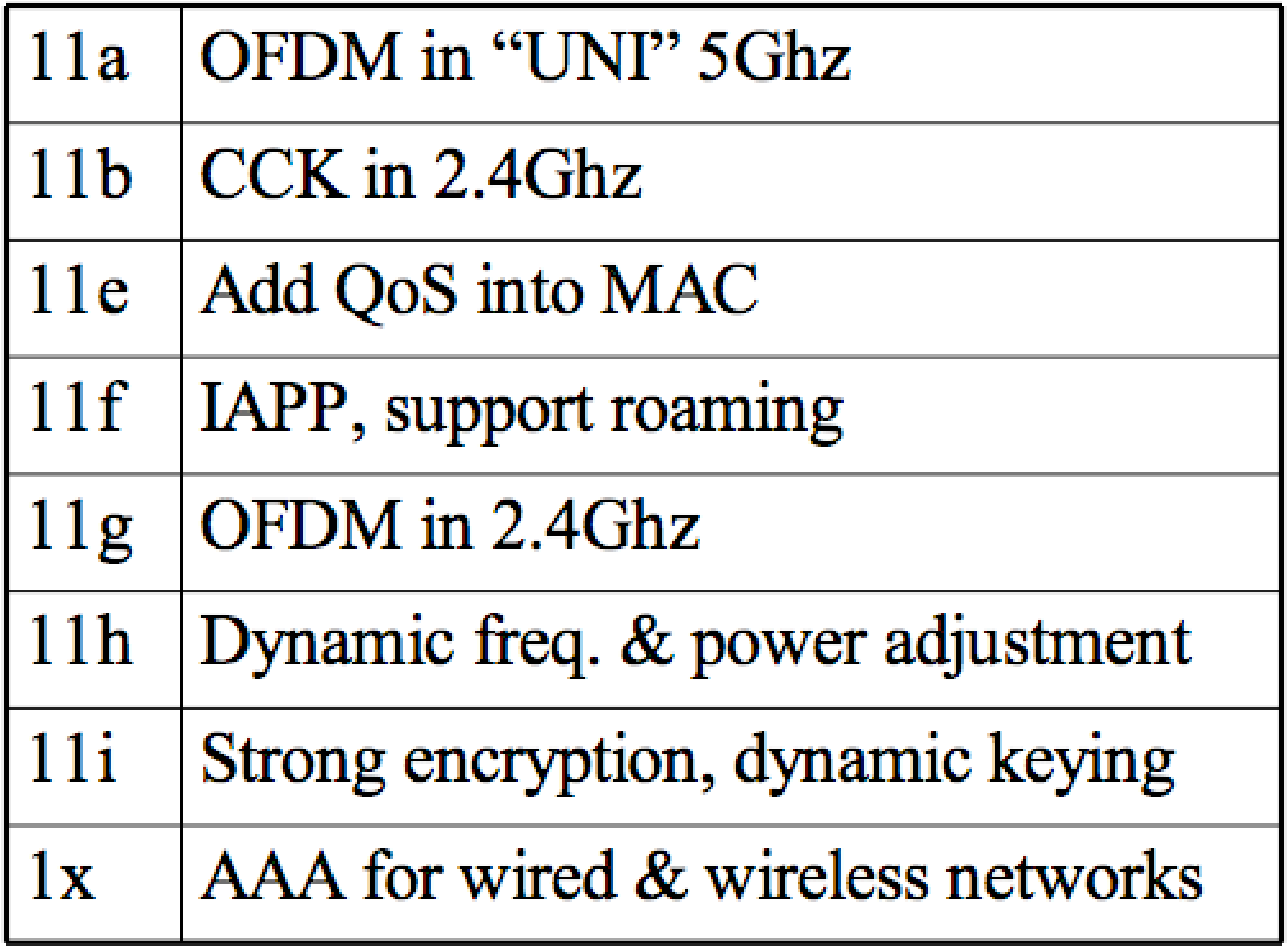
Standards



IEEE	Speed	Frequency	Ratified
802.11	2Mb/s	2.4Ghz	1997
802.11b	11Mb/s		1999
802.11g	54Mb/s		2003
802.11a		5.2/5.8Ghz	1999
802.11n	100Mbps	5Ghz?	2006?

Download IEEE 802 specs @ http://standards.ieee.org/getieee802/

Other 802.11 Standards



11a	OFDM in “UNI” 5Ghz
11b	CCK in 2.4Ghz
11e	Add QoS into MAC
11f	IAPP, support roaming
11g	OFDM in 2.4Ghz
11h	Dynamic freq. & power adjustment
11i	Strong encryption, dynamic keying
1x	AAA for wired & wireless networks

802.11 Users

- Home/SoHo - $80USD Linksys, limited security
- Enterprise/Edu - $1000 AP from Cisco, managed by IT dept., must be secure
- WISP (Wireless Internet Service Provider) – Entrepreneur ISP without broadband infrastructure
- CWN (Community Wireless Network) – Similar as above, different “biz model”
- HSO (Hotspot Operator) – Offer existing broadband wirelessly in public areas (cafes, airports)

Community Wireless Networks – Why?

- **US example**
  - **Q: VoIP between two geeks in same town, different ISP’s, packets go outside area**
  - **A: Route packets direct to each other (or atleast within same town)**
- **Nepal example**
  - **Q: Rural citizens make goods/handicrafts, need a way to export, limited capital and ISP availability**
  - **A: Provide free wireless internet service initially, tax business transactions and other online trades**
- **Technical reasons too:**
  - **(semi) Symmetrical bandwidth**
  - **Real IP space**
  - **limited AUPs/filtering & censoring, etc.**

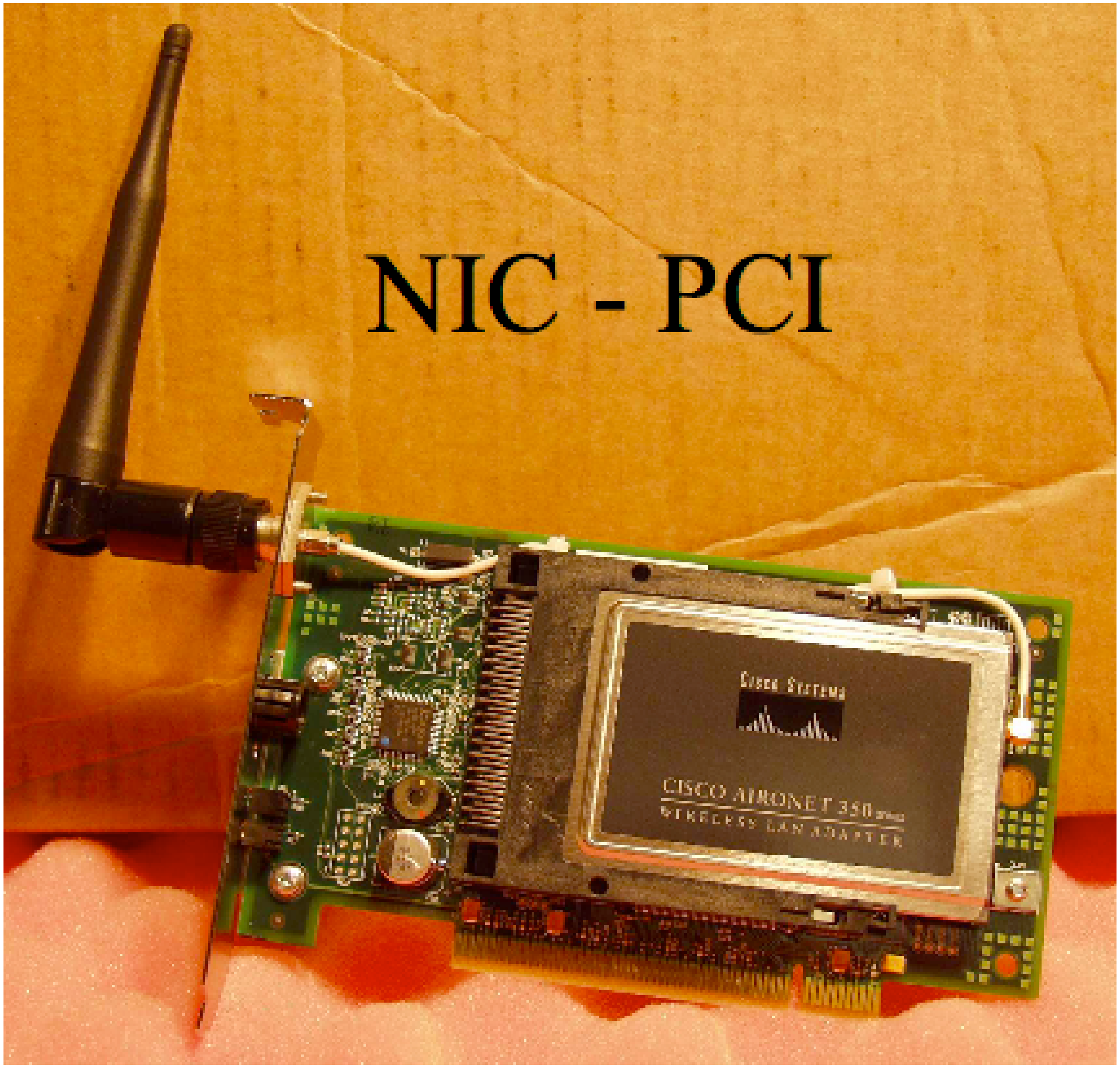
Concepts

- **AP = Access Point**
  - – L2 bridge (802.1d) between wired (802.3) & wireless (802.11)

- **STA = Station**
  - – 802.11 NIC (PHY in form of PC Card, USB, PCI, etc.)

WiFi PC Cards

NIC - PCI

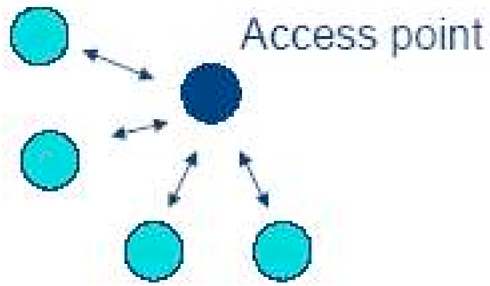

Cisco Systems
CISCO AIRONET 350 SERIES
WIRELESS LAN ADAPTER

MiniPCI

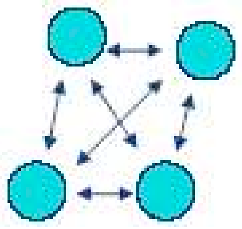
For
Laptops
& Embedded

802.11 Modes

- **BSS = Basic Service Set”** *Infrastructure*”
  - L2 bridge between wired (802.3) & wireless (802.11)

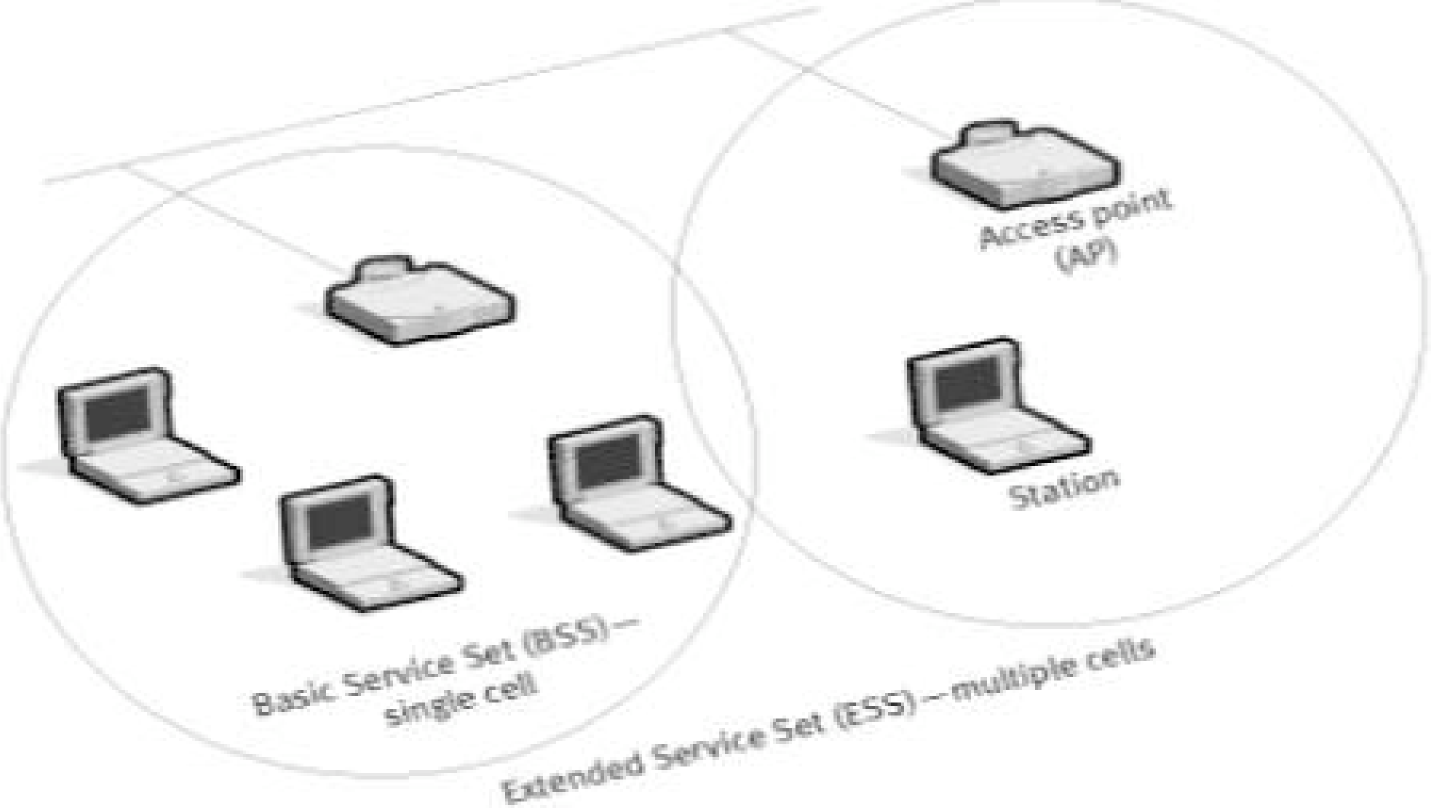


- **IBSS = Independent BSS** “*Ad-hoc*”
  - 802.11 NIC (PHY in form of PC Card, USB, PCI, etc.)



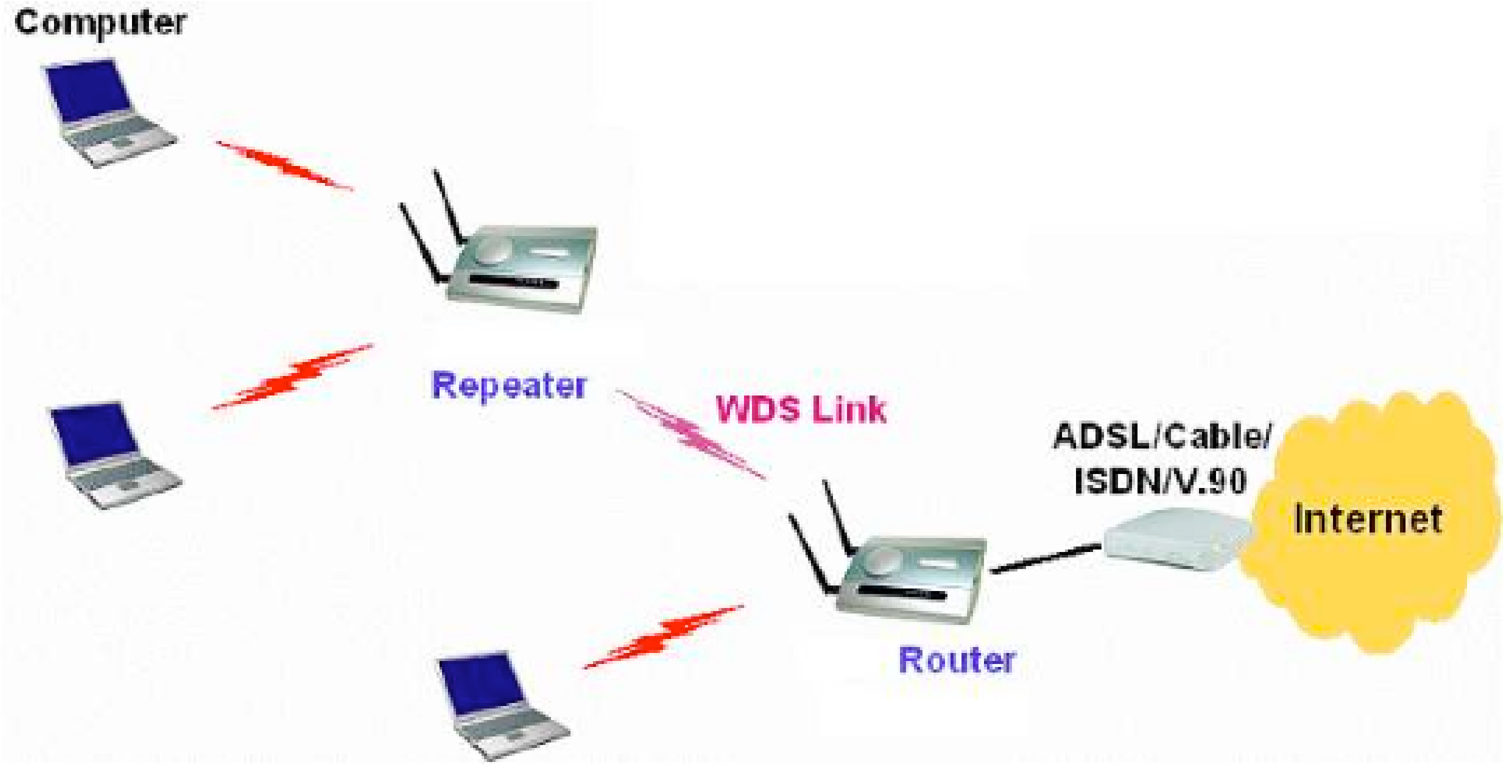
802.11 Modes (cont.)

- **ESS = Extended Service Set**
  - Collection of BSS AP’s on common backbone


Access point (AP)
Station
Basic Service Set (BSS)— single cell
Extended Service Set (ESS)—multiple cells

802.11 Modes (cont.)

- **WDS - Wireless Distribution System**
  - Bridge wired devices over wireless



802.11 Concepts (cont.)

- **SSID = Service Station Identifier**
  - Unique name for network
- **Brief on a the “association” process**
  - AP or IBSS master will “beacon” out an SSID, supported data rates, security requirements, etc. ~10 times a sec
  - STA’s send a broadcast probe to listen for beacons
  - AP/IBSS master & STA agree on AAA, then sync up
  - STA DHCP’s, etc.

Pre-install

Prerequisites before any deployment

Pre-install work

- Site Survey is **required**, don’t be lazy
  - Analog: mirror, binoculars
  - Digital: laptop w/ external antenna
- Discover the possible link paths
  - Tree (spring vs. fall season), building (new construction), mountains, etc.
  - Other development years in future
- This highly increases the likelihood of a successful link

Pre-install work (cont.)

- Bandwidth requirements
  - What services are you running, latency problems
- Access Point locations
- Coverage areas / proper antenna
- Frequency/channel allocation
  - Near other RF sources, TV/FM tower
- Logical network design *“keep local traffic local”*
  - Subnet’ing, segments
- Security
  - Physical & IP level

Designing WLAN in such area is challenge !!!

An example of data for calculating height.

Latitude/Longitude of the Villages and Relay Stations

S.N	Place	Latitude	Longitude	Elevation in Meter	Remark
1	Pokhara Station	28° 14.765'	83° 59.435'	980.00	Relays to Relay 1
2	Relay Station 1	28° 22.285'	83° 40.758'	3,320.00	
3	Relay Station 2	28° 28.336'	83° 42.487'	3,650.00	
4	Nangi	28° 22.300'	83° 38.306'	2,360.00	
5	Tikot (Relay 3)	28° 25.836'	83° 37.232'	2,250.00	Relays to Tatopani
6	Ghara (Relay 4)	28° 27.079'	83° 39.003'	1,965.00	Relays to Paudwar

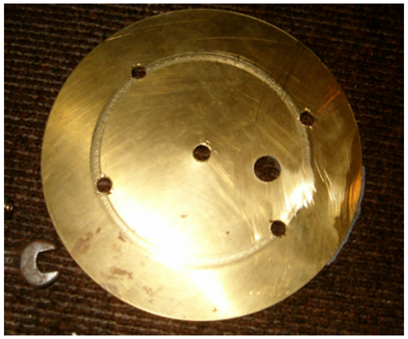
Antennas Characteristics

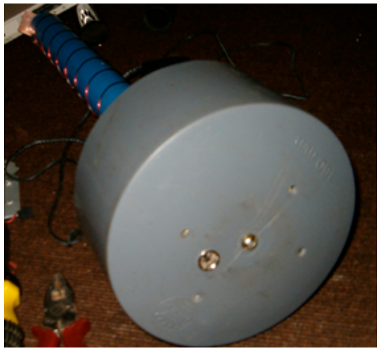
- **Polarization**
  - Orientation of element (horiz, vert, circle, etc)
- **Directivity**
  - Size of the beam
- **Bandwidth**
  - Frequencies tuned for
- **Gain**
  - Effective power increase

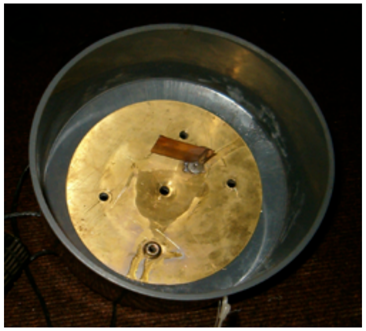
http://www.lns.com/papers/BAWUG-antenna101/

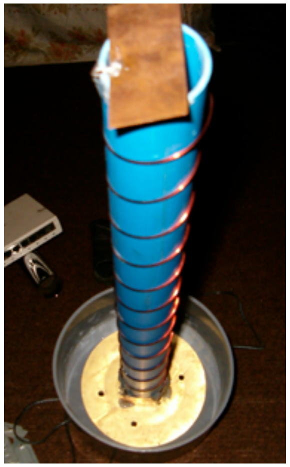
Homemade & Custom Nepal antennas

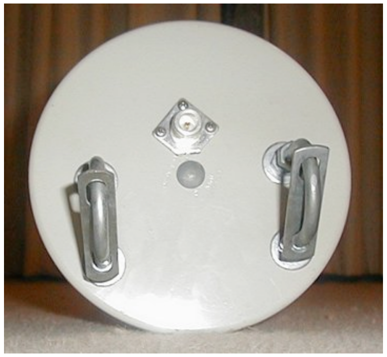
Parts of Helical antenna (homemade, your own risk, but good lesson

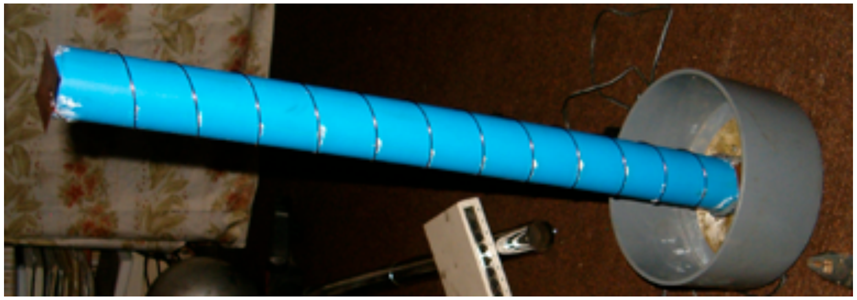






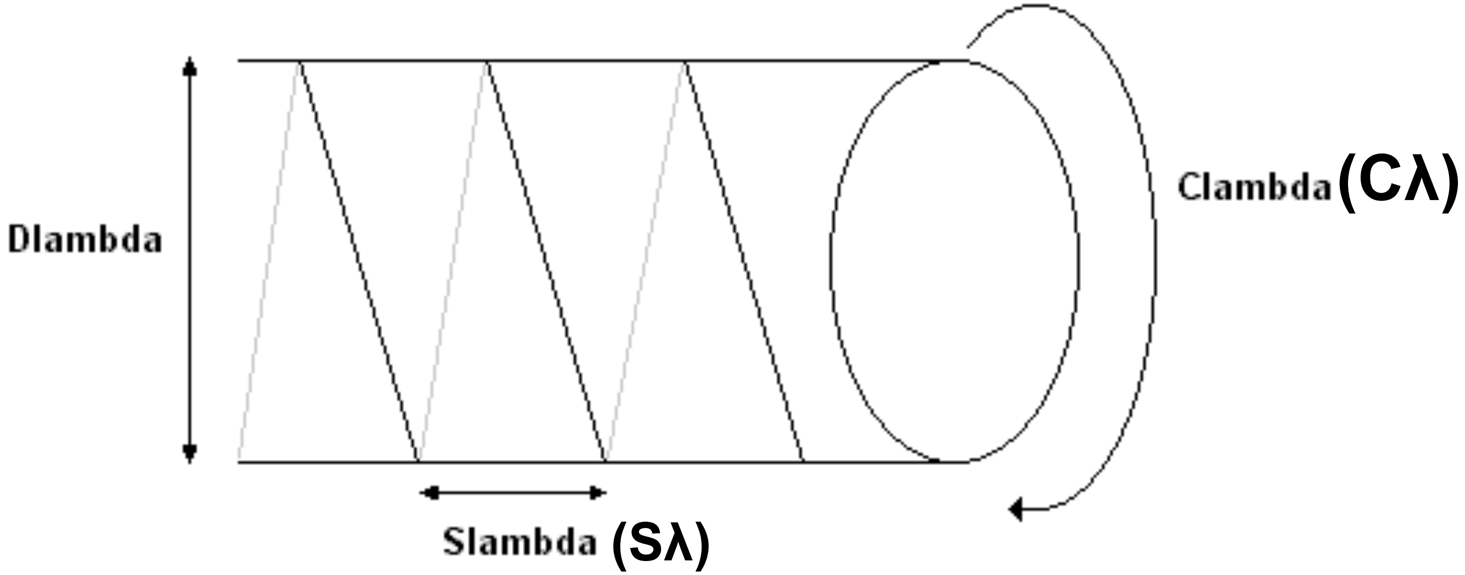






Theory

The design for this antenna was derived from the good ol' ARRL Antenna Handbook. It has got some fixed mathematical parameters



Defined mathematical parameters

$C_\lambda = 0.75$ to 1.33_λ : Circumference of winding

$S_\lambda = 0.2126\ C_\lambda$ to $0.2867\ C_\lambda$: Axial length of one turn

$G = 0.8$ to $1.1\ \lambda$: Diameter of ground plane / reflector

$D\lambda = 0.75$ to 1.33λ: Diameter of the helical pipe

$C_\lambda = \pi D_\lambda$: Circumference is π (pi) times the diameter of helical pipe

(Measurement is given in mm)

***** Since the diameter of the winding is fixed, with the PVC tubing Here, the value of λ determines the wavelength of centre frequency.**

For the 2.4 GHz frequency the the value of λ becomes around 0.123711 meters (12371.1mm)

****** Minimum 13 round required- also Buddhist stupa has got 13 round. !!!!!!!!**

***** (Value of λ is derived by C/F where, C= speed of electromagnetic wave & F= Frequency of signal)**

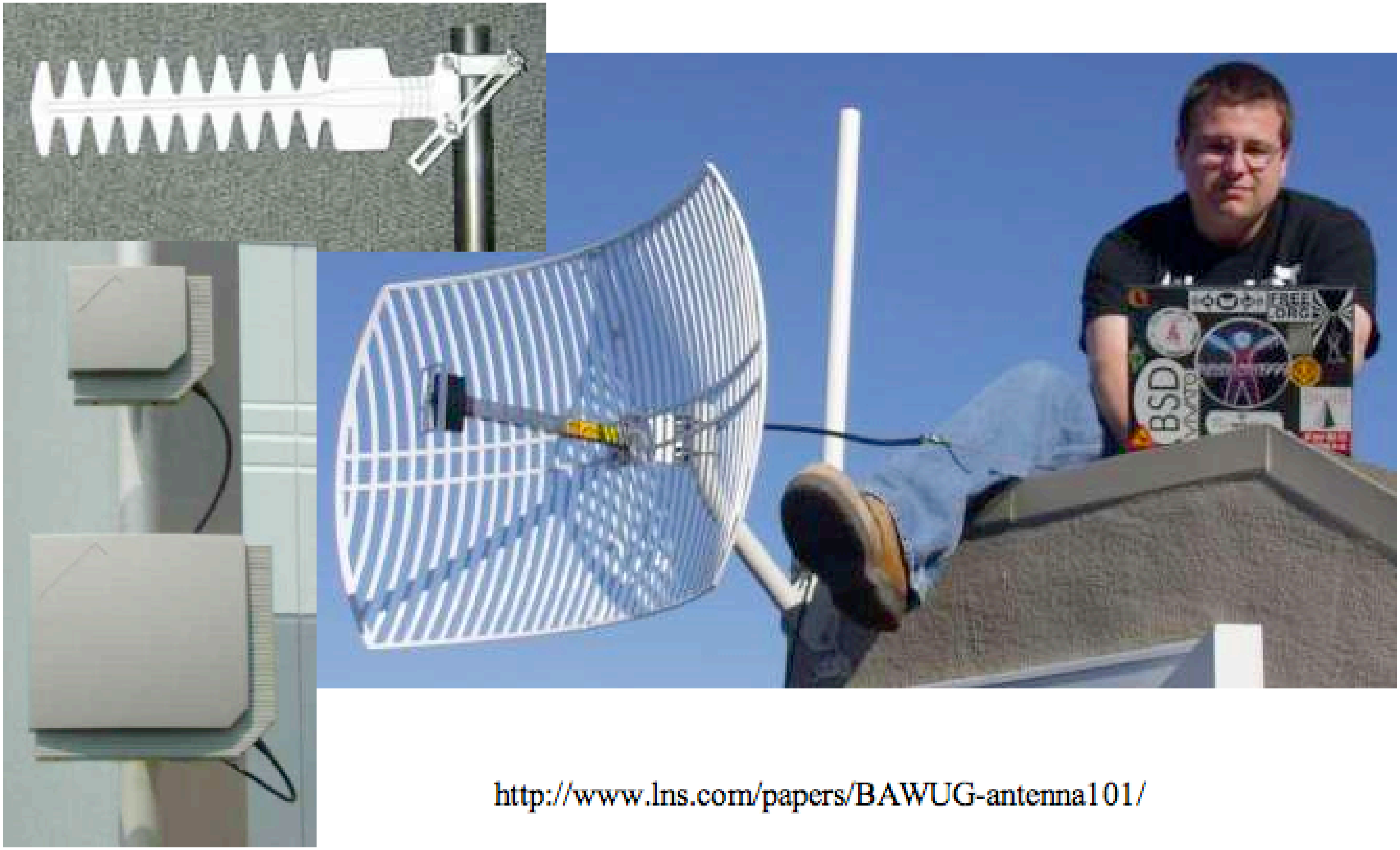
*****(it is an around value, more calculation needs for finding exact frequency wavelength)**

Formula for calculating dBi

Gain= 11.8+10log10(C λ *C λ *n*S λ) Where n is the number of turn
= 11.8+10log10(1.066* 1.066*13*0.31830)
=18.5dBi

Formula for Calculating beam

Beam width= 52/(C λ *sqrt(n*s λ)) degrees
= 52/(1.066*sqrt(13*0.31830)
= 23.98 degrees



http://www.lns.com/papers/BAWUG-antenna101/

Logical network design

- Remember RFC1918
  - 192.168, 10.0, 172.16
  - Private networks will use these (home routers @ NGOs, etc); your network can’t conflict, you want SNMP/HTTP management

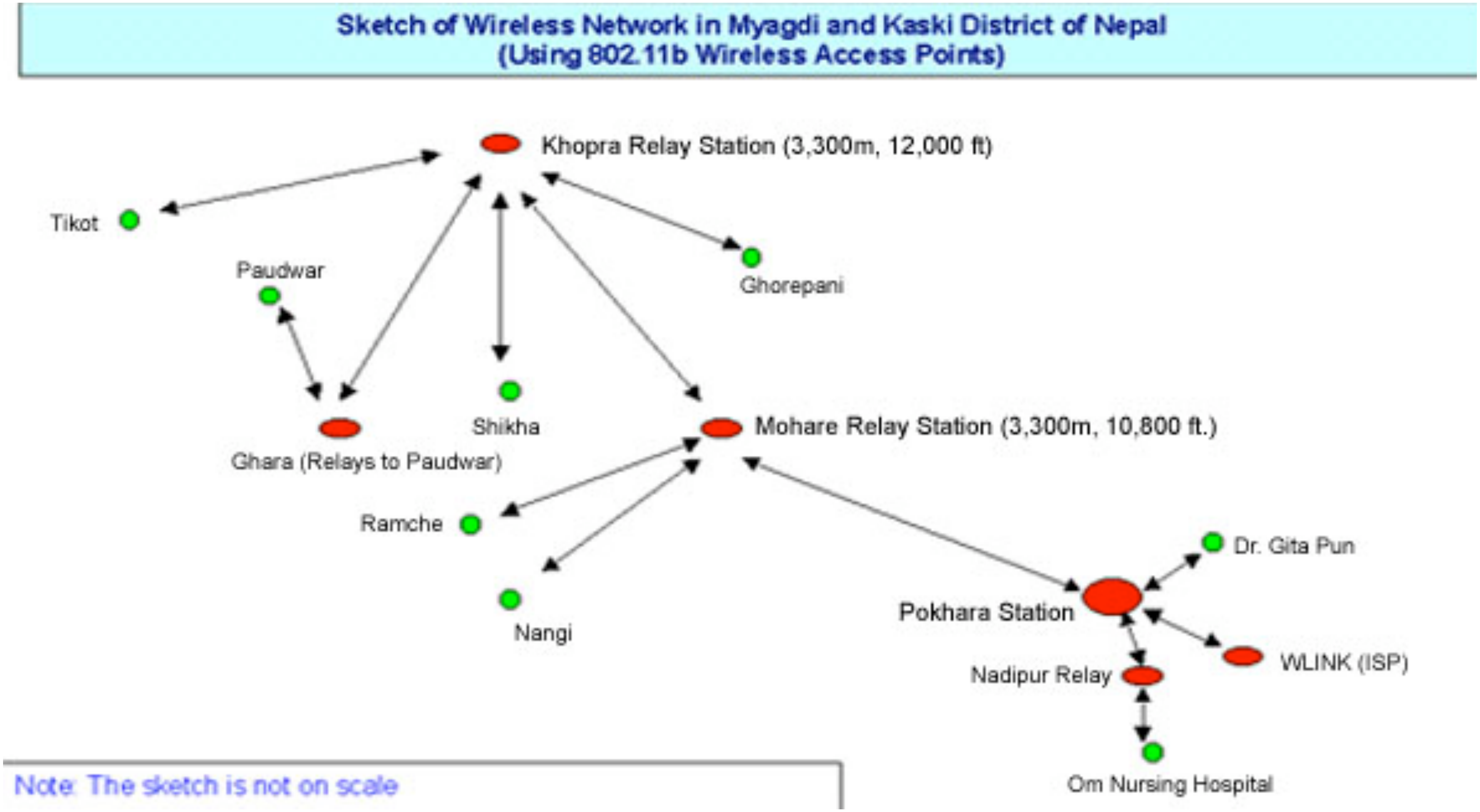
Physical network design

- Point to Point
  - Backbone to Backbone
  - Don’t use Private IP’s (if possible)
- Point to Multipoint
  - Backbone to Client
  - Private IP’s Ok, using NAT (ick)

Deployment

Lessons learned from the field

WiFI in Nepal



Sketch of Wireless Network in Myagdi and Kaski District of Nepal
(Using 802.11b Wireless Access Points)

Note: The sketch is not on scale

Buy professional made towers!

Coax Hints

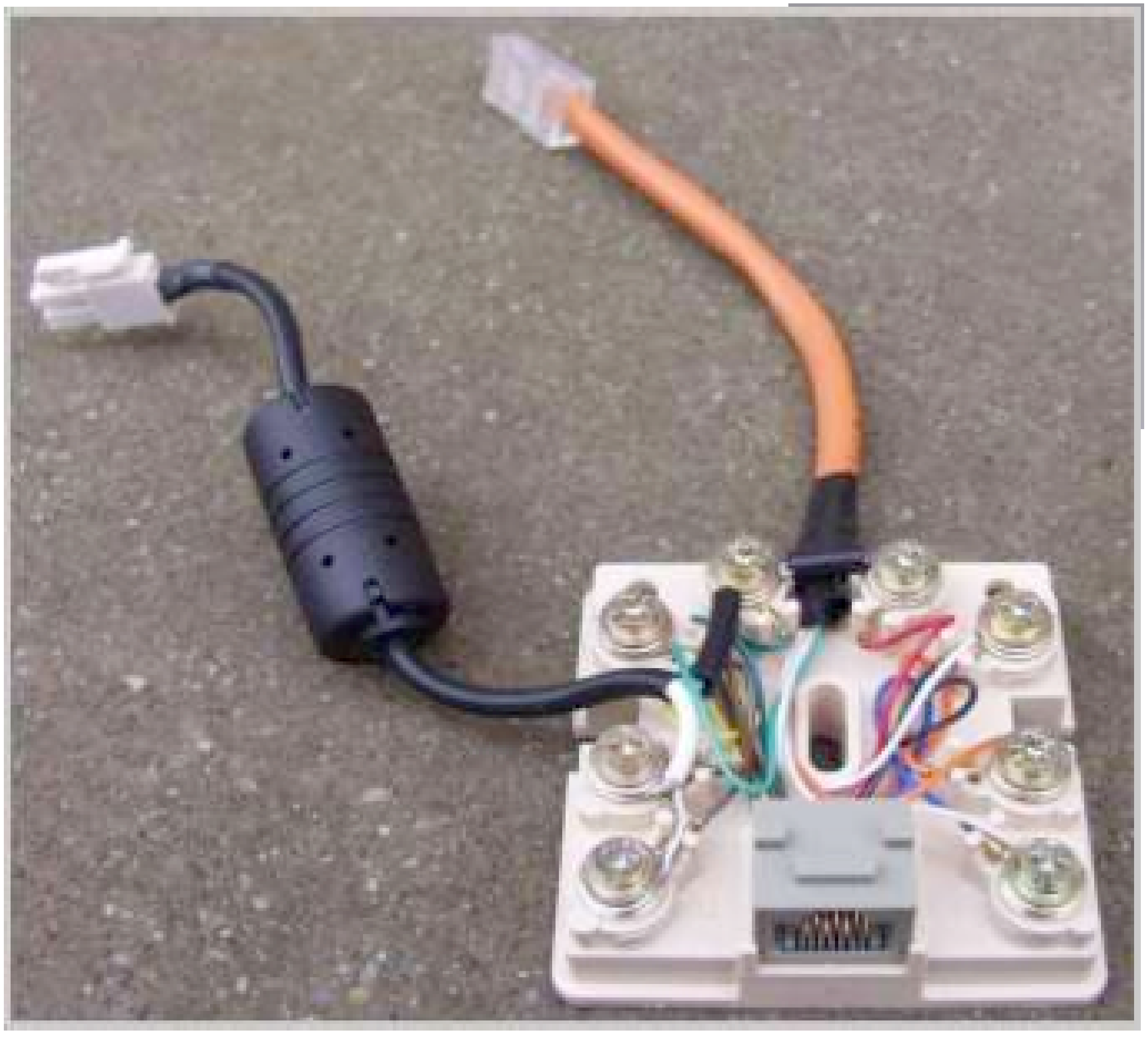
- Don’t use RG-8 (television) cable
  - LMR400 is very popular (low loss/high price)
- Use correct tools
  - Crimper, soldering iron, heatshrink, glue, etc.
- Cheaper (in headache time) to buy pre-made

Power over Ethernet

- Push DC voltage on unused pairs of Cat5 cable
  - Cost tradeoff
    - No new AC outlets needed on tower/shack
    - PoE injectors required ($20USD single port)
  - Emergency mode
    - Just un-plug, no tower climbing to reboot
- Homemade works fine, IEEE has 802.3af standard to sense PoE support

http://www.nycwireless.net/poe/

Homemade PoE



Security

- Bad things happen
  - – Not on purpose, “ANY” STA “stumbles” on your network
  - – On purpose, “drive-by spamming” (spam police knock on your door!)
- Out of the box (all can be defeated)
  - – Disable SSID name in beacon
  - – MAC address “whitelist” filtering
  - – Static WEP keys

Security (cont.)

- Keep AP firmware updated
- Disable/filter SNMP/CLI/HTTP management
- Note the BSSID (MAC address of AP)
  - Rogue AP might have same SSID, channel and MAC anyways (everything can be spoofed)
- Swap out omni antennas to directional
  - Not much security help, but atleast helps RF
- Difficult to shield from both 802.11 protocol & RF DoS attacks

Security (cont.)

- 802.1x (AAA) + Dynamic WEP keys
  - Who is the user “matt”
  - Is he still employed “yes” (in RADIUS)
  - What is he allowed access to “IT vlan”
  - Thumps up “here’s a personalized WEP key for him”
- In general, this rarely works
  - OS drivers, configuration
  - Need AAA (RADIUS, Kerberos, etc) servers
  - Someone to maintain
- Use IPsec or some form of end-to-end (SSH w/ keys)

Equipment

- Commerical products
  - Designed for indoor
  - No antenna connector
- Homemade is good

Thank you