IEEE 802.11 Wireless LAN Architecture

New Protocols and New Deployment Strategies

Matthew Gast

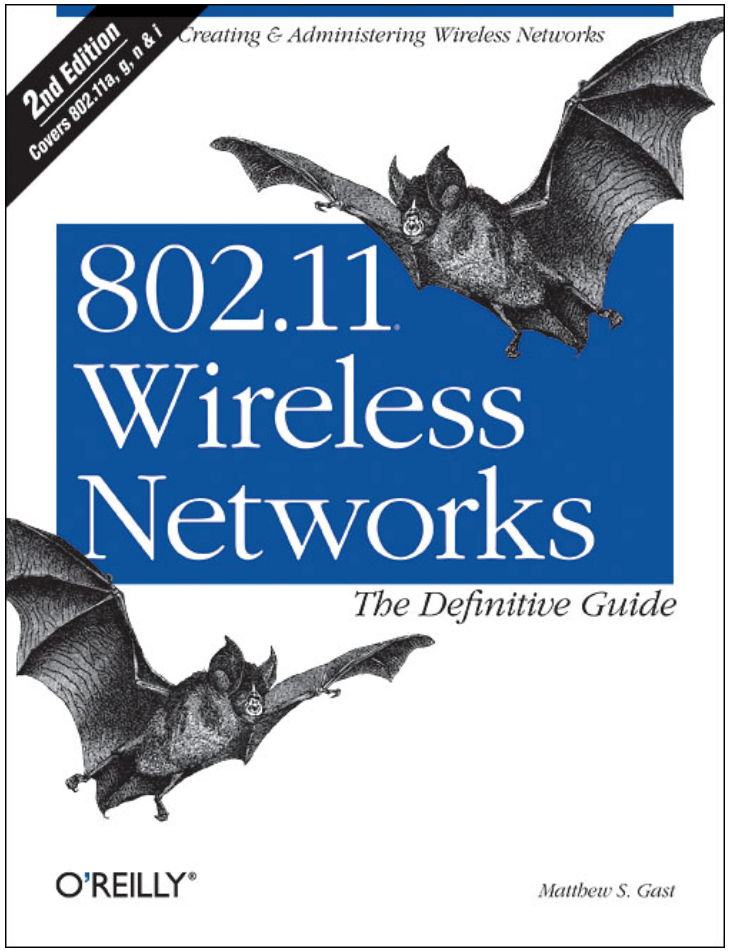
IEEE Communications Society – Oakland/East Bay

June 16, 2005

Who am I?

(And why should you listen anyway?)

- Author of this book
- Engineer with Interop Labs
- Day job
  - Director of Consulting Engineering at Trapeze
- Answer to Most FAQ: in bookstores now

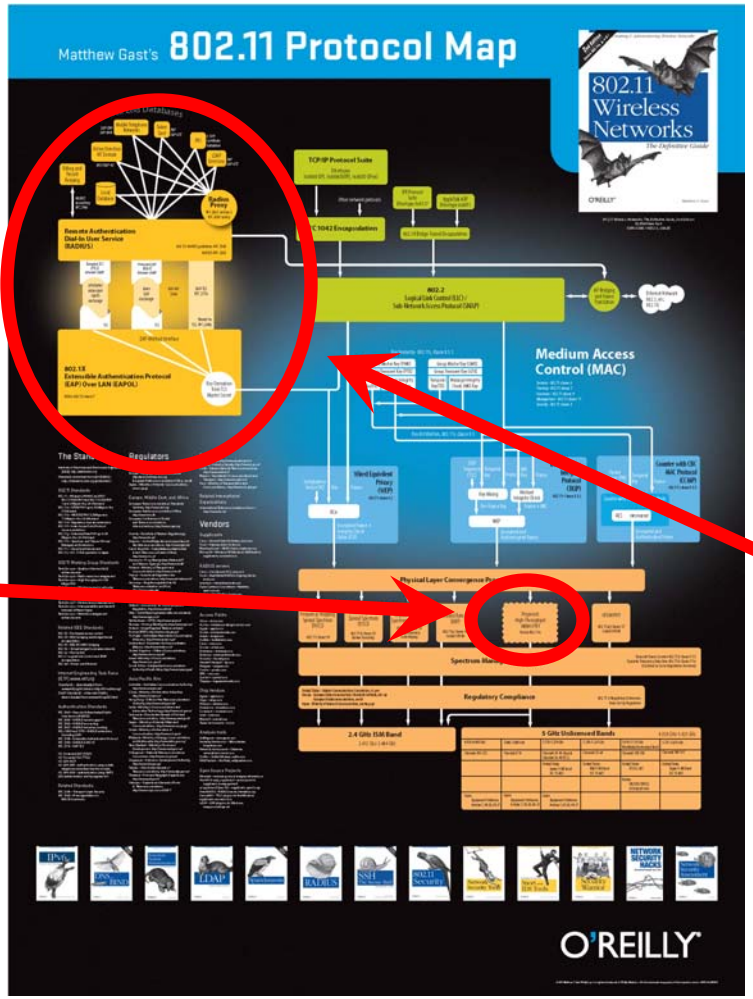


Agenda

- 802.11 TGn Goals & Motivations
- WWiSE Proposal
- TGnSync Proposal
- And something completely different: how to use fast networks everywhere with your home credentials

Visual Agenda

Most of the time will be down here in the weeds



With a bit up here at the end

802.11n Introduction

The last shot at a new PHY this decade?

TGn Goal

- Interesting goal: >100 Mbps net throughput
  - Previous proposals focused on peak data rates
  - “The scope of this project is to define an amendment that shall define standardized modifications to both the 802.11 physical layers (PHY) and the 802.11 Medium Access Control Layer (MAC) so that modes of operation can be enabled that are capable of much higher throughputs, with a maximum throughput of at least 100Mbps, as measured at the MAC data service access point (SAP).”
- Net throughput is measured at MAC layer

Getting to 100 Mbps

- Two choices
  - Make the data rate really fast:
    Lots-of-Mbps minus overhead > 100 Mbps
  - Make it work more efficiently:
    Slightly more than 100 Mbps minus lower overhead > 100 Mbps

Proposals

- World-Wide Spectrum Efficiency (WWiSE)
  - wwise.org
  - Chipmakers: Airgo, Broadcom, Conexant, TI
- TGnSync
  - tgnsync.org
  - Chipmakers: Agere, Atheros, Infineon, Intel, Marvell
  - Many more consumer electronics vendors: Sony, Panasonic, Sharp, Samsung, Philips, Mitsubishi
- Many similarities, also many differences

802.11n status: an outsider looks in

- Two major proposals under consideration
  - Plus a minor one from MIT & Motorola (though Motorola has joined WWiSE)
- IEEE rules: one must get 75% of the votes
  - Neither did last month in Australia, so all three are back on the table
  - Back to the elimination stage, then what???
- TGnSync has polled higher
  - But that support hasn't helped it get selected

Common points

- Multiple-input/multiple-output (MIMO)
- Open-loop operation
  - Just transmit the frame
- Channel widths: 20 MHz (same as a/g), 40 MHz
- Increase efficiency of MAC

MIMO

- A buzzword with the power to distract
- Uses multiple “RF chains” to increase speed and sensitivity
  - Components: error-correcting coder, modulator, amplifier, antenna
- Notation: ZxY (e.g. 2x2)
  - TX chains x RX chains
- Each chain adds cost, and eats power
  - 2 will be common client; high-end APs will probably have 3 or 4

Channel Bandwidth

- 20 MHz channels are used today
  - Likely to remain important in the ISM band, since there are only three of them
  - Identical channel mapping to 802.11a/g
  - Universal regulatory acceptance
- Both proposals support 40 MHz
  - Optional extension in WWiSE
  - Required by TGnSync
  - Not all regulators allow them

40 MHz channels: the argument

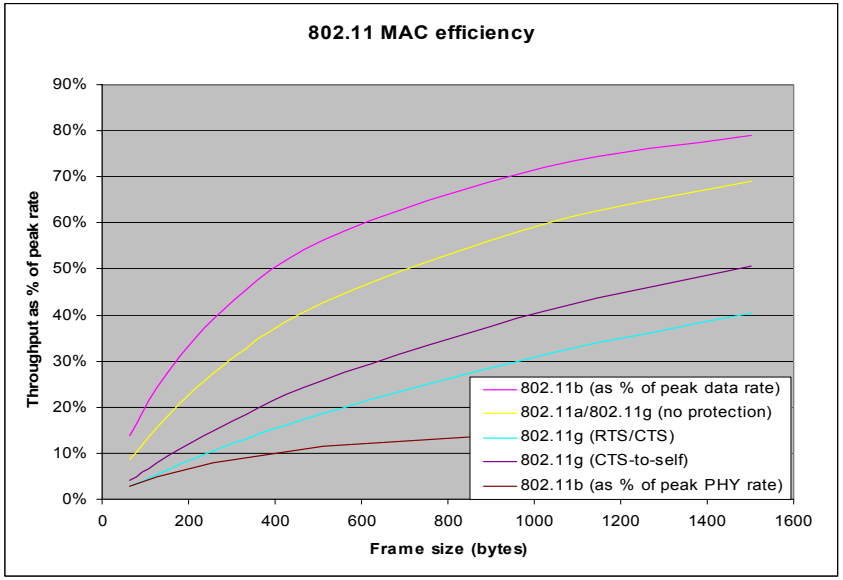
- This is a major point of contention
- For
  - It's faster! TGnSync bonding increase throughput by 2.25, not just 2
- Against
  - Many regulators have not approved 40 MHz operation (e.g. Japan)
- Regulations are often flexible – if users perceive a benefit, they press for regulatory changes

Open-loop Operation

- Just send frames without calibration
  - This is the way that 802.11 works now
  - Low complexity
- TGnSync adds a “closed-loop” mode
  - Frame exchanges calibrate channel before sending

MAC efficiency

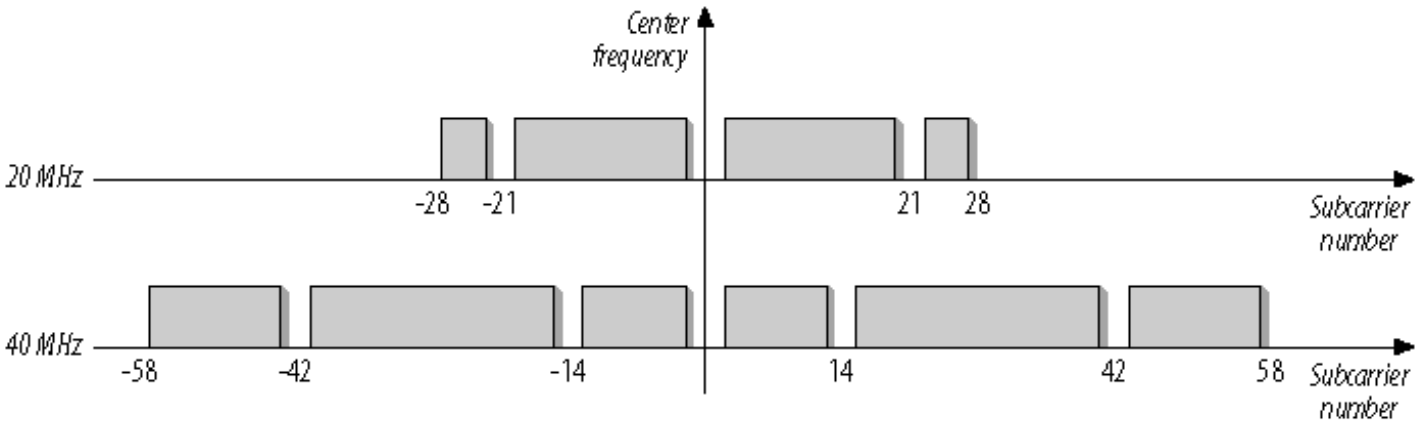
- Lots of overhead in 802.11 MAC
  - Data throughput of 50% of the “headline” rate is a good rule of thumb
- Improving data to control ratio increases net throughput
  - Block ACKs (bursting), aggregation, and header compression are used by both proposals



WWiSE Proposal Details

Channelization

- 20 MHz channel structured identically to 802.11a
  - But uses fewer pilot carriers (2 instead of 4)
  - 2 pilot carriers through 2x2 MIMO has 4 carrier/antenna processing chains, and has similar performance to four pilot carriers through a single-antenna system
- 40 MHz channels are just twice as big: no efficiency

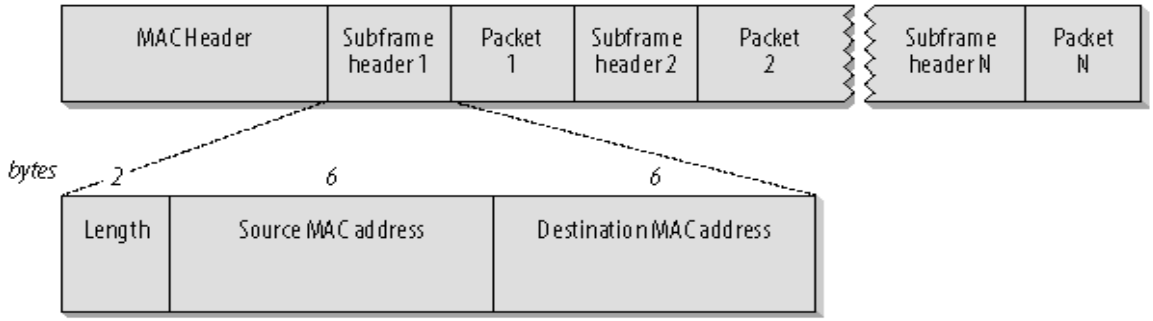


WWiSE Modulation Rates

- The proposal has a big table
  - Basic speed: 60.75 in a single 20 MHz channel
  - Top speed: 540 Mbps in four 40 MHz channels
  - Plus lots of speeds in between
- No new modulations: 64-QAM is still the top end (same as 802.11a)
- New higher code rate: 5/6 (as opposed to 3/4 in 802.11a)

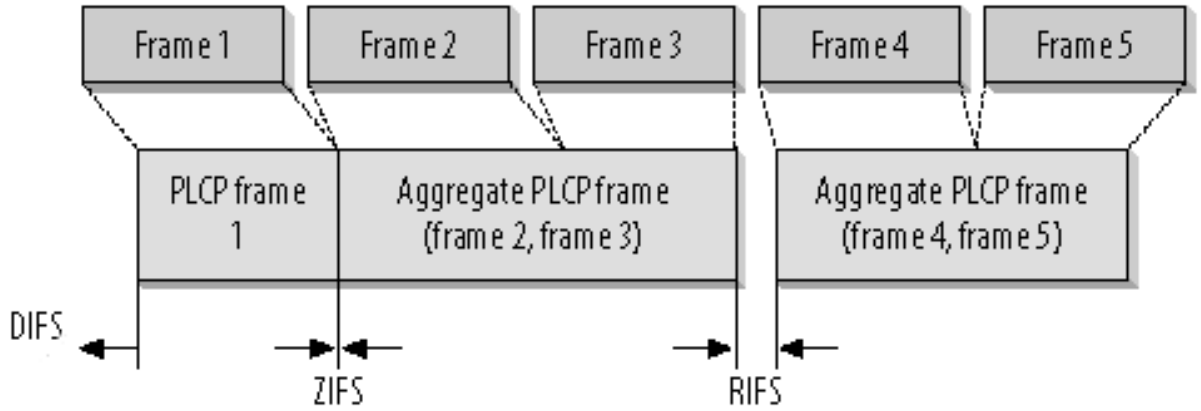
WWiSE Aggregation

- Max frame size increases from 2,304 bytes to 8,191 bytes
- Can only aggregate when Address1 field in MAC header is the same
  - Same receiver
  - Can aggregate multiple frames through an AP, since they have the same receiver (though maybe not destination)
- Cannot mix different frame types



WWiSE Bursting

- When Address1 differs, frames must be sent in a burst
- Same TX power can use Zero IFS (ZIFS); different TX power uses Reduced IFS (RIFS) to maintain medium control
- Can be used in combination with aggregation

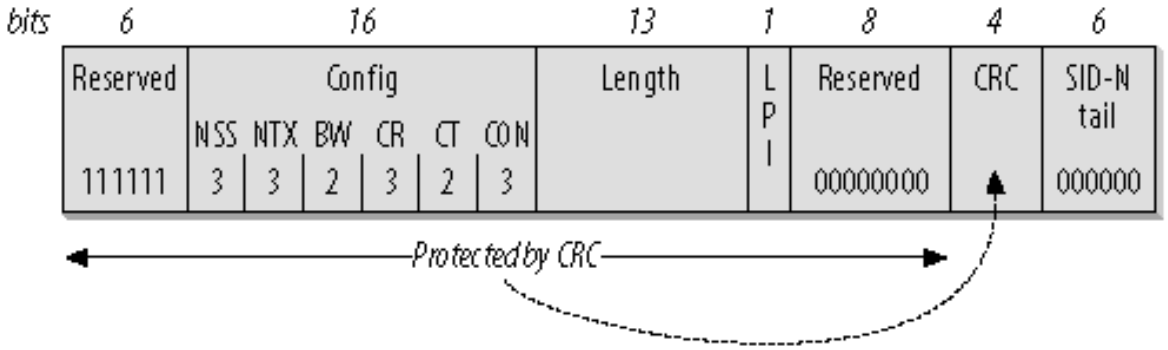


WWiSE: Meeting the throughput goal

- 12,000 bytes (960,000 bits) in 960 µs
- Basic 2x2 data rate = 135 Mbps
  - 711 µs for data
  - Preambles, framing, interframe spacing, and a single block ACK take 249 µs

WWiSE PLCP

- Two modes
  - Mixed mode coexists with 802.11a/g by using same PLCP header
  - “Greenfield” assumes there is no older network and goes straight to WWiSE header
- New SIGNAL-N header



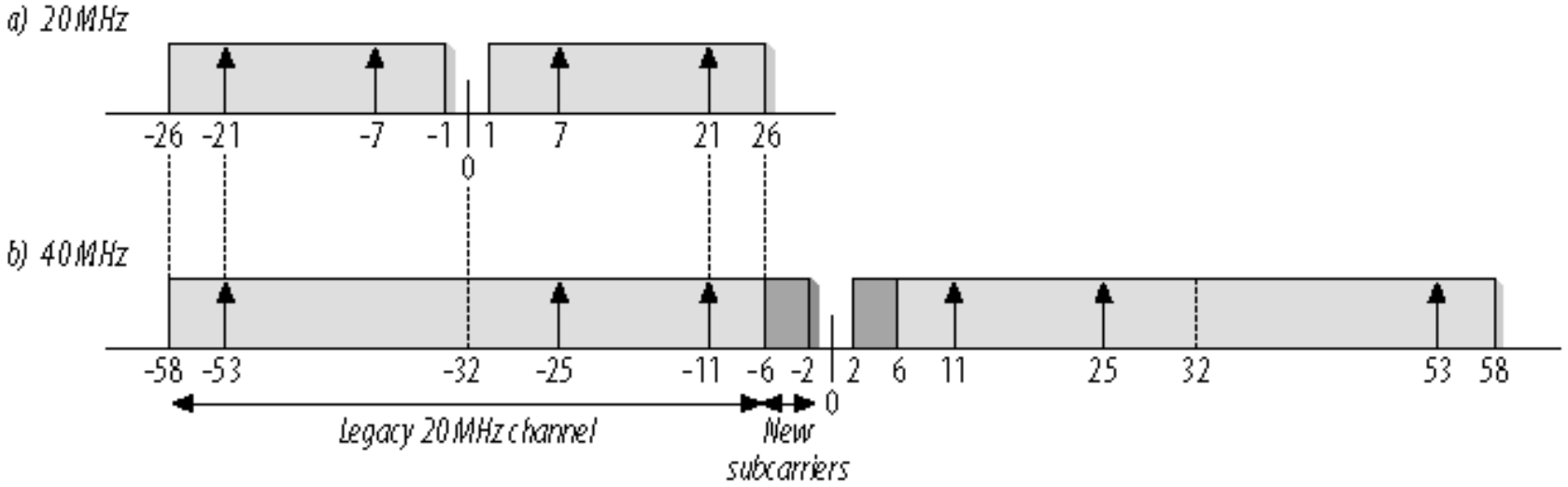
TGnSync Proposal Details

Components

- MAC
  - New aggregation
  - Power saving
- PHY
  - 40 MHz mandatory
  - Closed loop operation
    - Also enables 256 QAM
  - Short guard interval

TGnSync Channelization

- Same structure as 802.11a in 20 MHz
- 40 MHz structure “reclaims” carriers in the middle of the band
  - 2.25x the throughput, instead of just 2x
  - Support required by proposal



TGnSync Transmit Modes

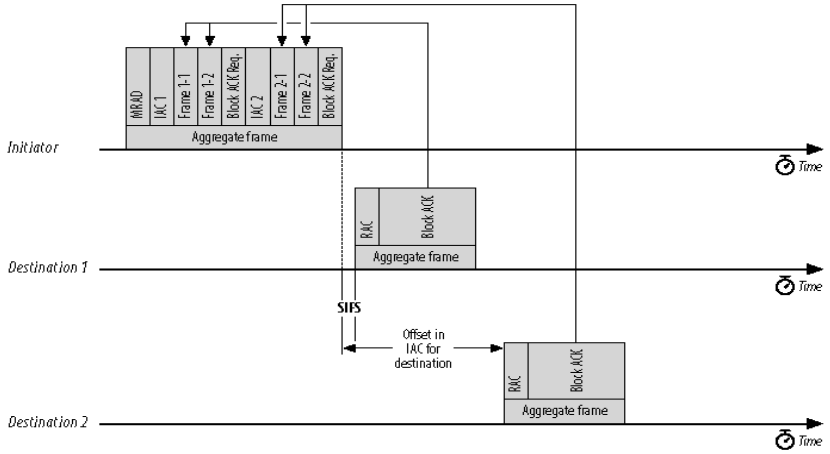
- Basic MIMO mode
  - Open loop operation
- Basic MIMO with beamforming
  - Closed loop
  - All spatial streams use identical power/modulation
- Advanced Beamforming (ABF) mode
  - Closed loop
  - Different power/modulation possible on each spatial stream
  - Required for highest data rates (256 QAM)

TGnSync Modulation Rates

- The proposal has a big table
  - Basic speed: up to 63 Mbps in a single 20 MHz channel
  - Top speed: 630 Mbps in four 40 MHz channels
- Plus lots of speeds in between
- New modulation: 256-QAM
- New higher code rate: 7/8
- Also has a short guard interval 400 ns (instead of 800 ns in 802.11a/g)

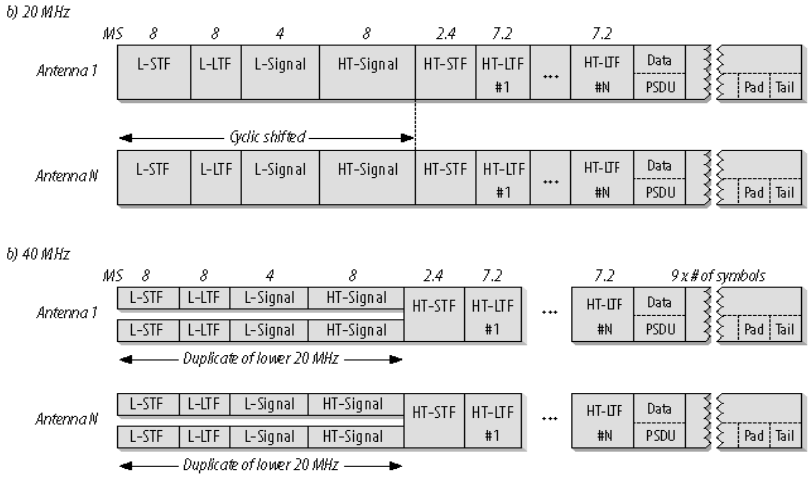
TGnSync Aggregation

- Aggregated frames can use block acknowledgements
  - Aggregate must have one receiver
- Optional “multi-receiver aggregate” MRA
  - Multiple receivers must each acknowledge



TGnSync PLCP

- Retains legacy headers
  - Used to “spoof” duration times used by the MAC



TGnSync Power Saving

- No comparable feature in WWiSE!
- Can shut down all but one RF chain
  - “MIMO enabled” and “MIMO disabled” states
- AP is responsible for keeping track of which stations are in MIMO disabled

Comparison

Speed

- TGnSync has a slight edge on speed, if you assume aggressive channel coding
- TGnSync numbers reflect short GI. With long GI, it's actually slower.
- Call this one a draw, especially with the disagreement over closed vs open loop operation

	20 MHz	40 MHz
WWiSE	135 Mbps	270 Mbps
TGnSync		
Basic	140	315
ABF	160	360

Operation mode

- Closed loop is hard
  - Not often done because it is so hard, and it is going in silicon
  - Bad if it does not work
- WWiSE spreads signals across multiple chains without closed-loop operation

Other comparisons

- Spectral usage
  - Regulations are malleable, so 40 MHz is probably OK
- Aggregation
  - Both proposals need lots of aggregation to meet the throughput goal
  - TGnSync MRA is a neat option because it allows one PHY header to hold lots of different MAC frames
- Intellectual property
  - RAND vs RAND-Z; but the RAND-Z proposal from WWiSE is only triggered if the 802.11n specification is “substantially similar” to WWiSE

Federated Authentication

And now, for something completely different

Motivation

- Visiting other organizations
- 802.11 is on nearly every laptop now
- Wouldn’t it be great to just use your laptop when you visit
  - No pesky IT staff to worry about

Examples

- Higher education
  - Faculty with joint appointments or on joint projects
    - Stanford professor on the Berkeley campus
    - Or even within a university
- The corporate world
  - Visiting vendors
  - Long-term contractors
  - Joint ventures
  - Large companies trying to revive feudalism

Common attributes of the problem

- Boundaries of administrative network control
  - Politics, politics, politics…
  - Security policies
- “Roaming” takes on a new meaning
  - Not seamless handoff, but configuration portability
  - Like GSM

Definition: network federation

- Independent member networks
  - Each network retains administrative control
  - Users are provisioned in a “home” network
- Some level of shared trust
  - Authentication proxy; perhaps authorization as well
    - Authorization is often restricted in the “visited” network
  - Users in one member network expect service in other members, though generally not seamless handoff
- Non-technical example: the United States

Building a Federation

- Need some trust mechanism between member networks
- Right now, all we have is RADIUS proxy
  - It's limited because it has a fixed topology for routing, and you need to be careful not to overload the user namespace
  - Every network must share a RADIUS secret with the core
  - RADIUS shared secrets have bad security properties
- Security Assertion Markup Language (SAML) is a promising future technology

RADIUS Star Architecture

- Multiple networks under separate administrative control
- Each network has a server
  - Some requests are handled locally
  - Unknown users are passed to other servers
  - Core server is an “identity router” for authentication requests
- We built a mini-version of this in the Interop Labs earlier this month

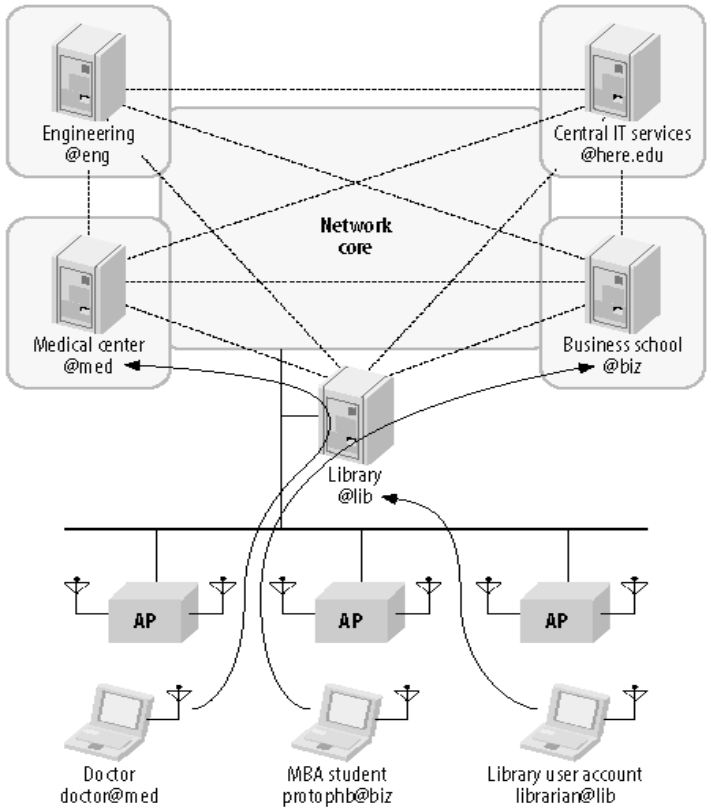


Figure used with permission from *802.11:TDG*, 2nd Ed

Using a RADIUS Star

- Also handy for working with balkanized political environments
  - Everybody gets to do their own thing
- Provides RADIUS server configuration help
  - Most APs only need to be configured on one or two RADIUS servers
- Early example: University of Utah
  http://utahgeeks.sourceforge.net/projects/WirelessWhitepaper-v1.03.pdf
  http://wireless.utah.edu/global/support/radius_mesh/RADIUS_Mesh_Long.pdf

Authentication Routing

- RADIUS realms
  - Structured user names (msg@eng, phb@mkt) can be used to send authentication to the right place
- This is like simple static routing
  - There's a great opportunity to fix

RADIUS Proxy Between Organizations

- Good for guest authentication
  - Ask visitor's employer to establish identity
  - Requires trust between organizations
- This is sometimes called "federated" authentication
  - Separately built & run networks
  - Users can use any member network
  - Generally no seamless roaming between two member networks

Yes, You Can Actually Do This

- Eduroam (http://www.eduroam.org/)
  - European-wide RADIUS star
  - Also hooked into Australia R&E network
  - United States core built at University of Utah
- Internet2 project for U.S. network
  - http://security.internet2.edu/fwna/
- General description of the technical issues:
  - http://www.oreillynet.com/pub/a/wireless/2005/01/01/authentication.html

Eduroam at Interop LV 2005

- Path of authentication for Norwegian test account
  - Interop Labs RADIUS server (Las Vegas)- > United States core server (Utah)- >Eduroam core server (Netherlands)- > Norwegian core server- > University of Oslo
- Authentication took about seven seconds
  - But it worked!
  - Faster handoff between APs is obviously necessary for usability

Open Questions for Federations

- Policy
  - What types of guests do you accept?
  - What access should they get?
- Legal stuff
  - Who is liable if a guest launches an attack from your network? You? The guest's employer?

Questions?

Matthew Gast

msg@trapezenetworks.com

matthew.gast@gmail.com