GTER 26
tudo o que você
(não)
quer saber sobre 802.11n

Luiz Eduardo Dos Santos
CISSP CWNE CEH GISP GCIH
Sr. Systems & Security Engineer
Americas

Wi-Fi Perfected

Ruckus™ WIRELESS

hello

Confidential

agenda

- evolution of wi-fi
- what makes lln
- what actually matters
- myths
- challenges
- security
- conclusion

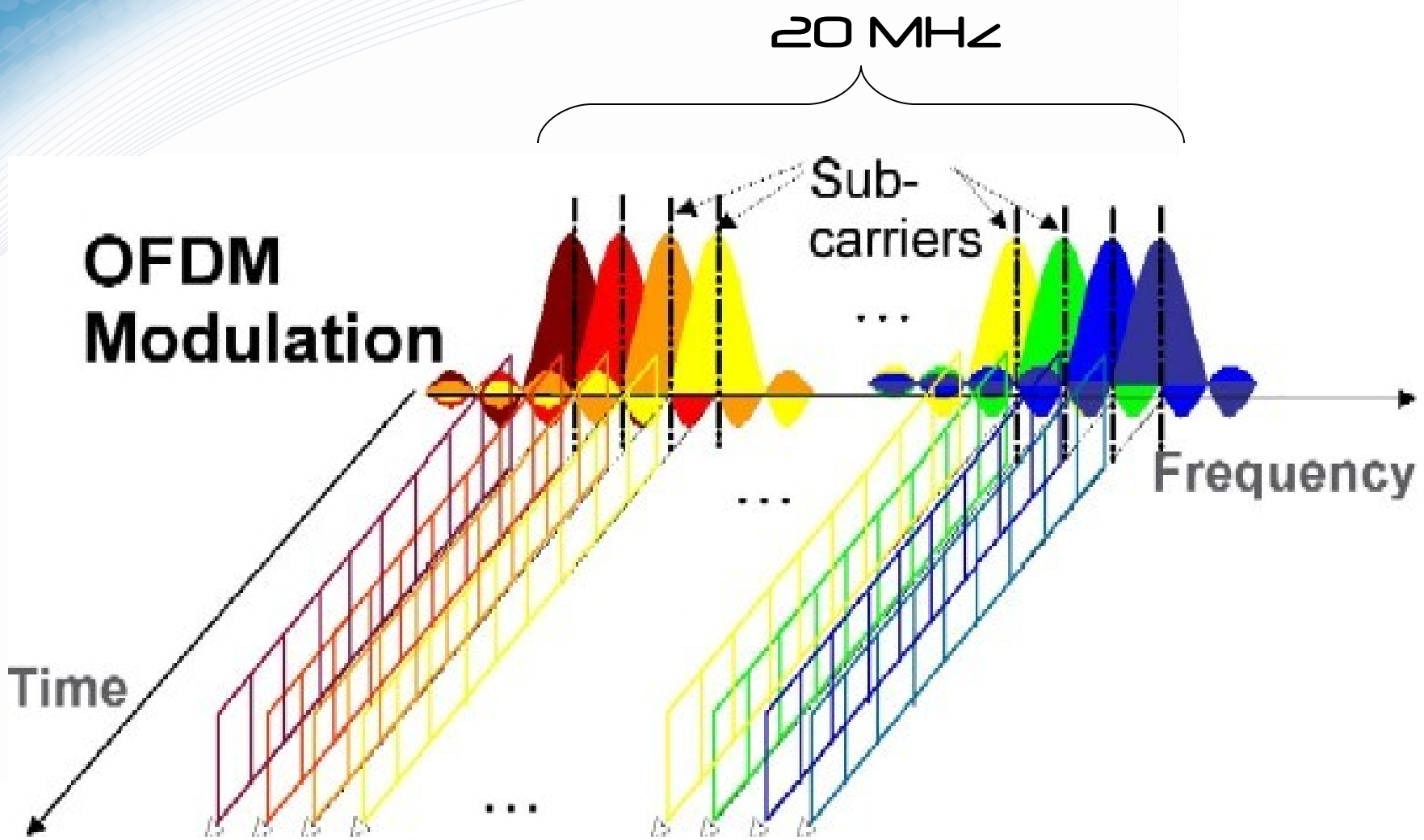
802.11b

- First widely deployed WiFi standard
- 2.4GHz band
- Single carrier (22MHz)
- CSMA/CA MAC
  - Random backoffs
  - MAC-layer acknowledgments
  - Retransmit failed packets
- 1, 2, 5.5, 11mbps PHY rates
- Maximum of ~7 mbps user throughput

802.11a

- 5GHz band – not compatible with 802.11b
- OFDM
  - 48 data + 4 pilot subcarriers in 20 MHz bandwidth
  - Increased robustness and spectral efficiency
- QAM modulation
- MAC essentially identical to 802.11b
- 6, 9, 12, 18, 24, 36, 48, 54 mbps PHY rates
- Maximum of ~36mbps user throughput

ofdm



802.11g

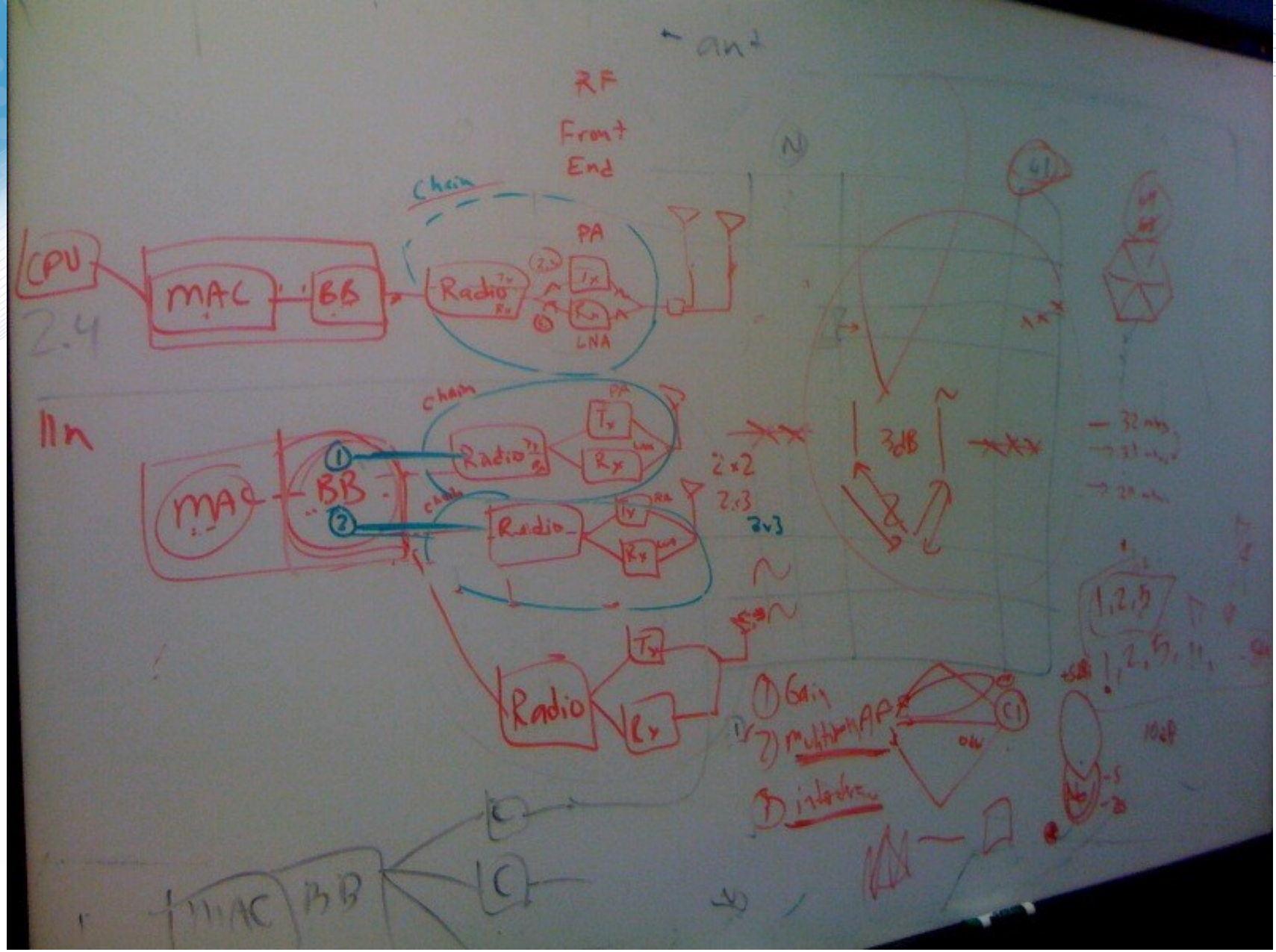
802.11a/g Rates		
Modulation	Coding	Mbps
BPSK	½	6
BPSK	¾	9
QPSK	½	12
QPSK	¾	18
16-QAM	½	24
16-QAM	¾	32
64-QAM	2/3	48
64-QAM	¾	54

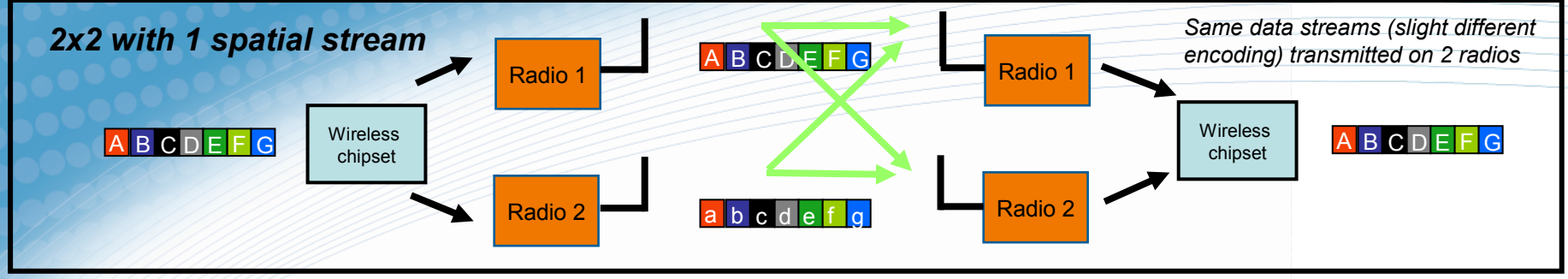

Wi Fi

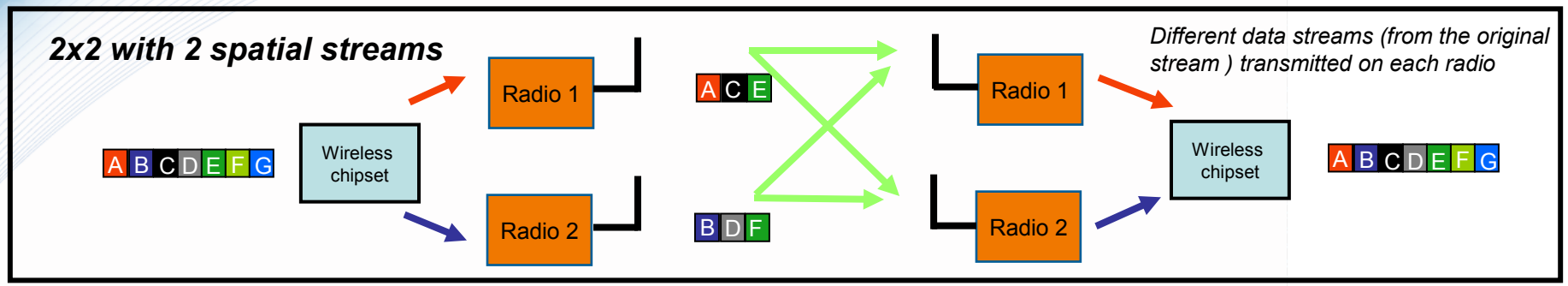
quick facts

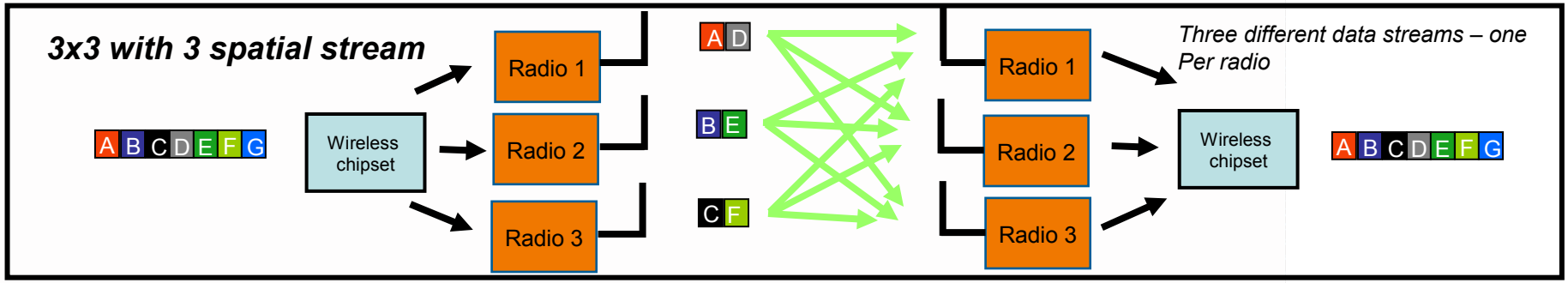
- 2.4 GHz and/or 5GHz
- Backward compatible with 11bg and/or 11a
- PHY Enhancements
  - 20MHz and 40MHz channels
  - Multiple radio chains
  - Spatial multiplexing (1, 2, 3, or 4 spatial streams)
  - Short guard interval
- MAC Enhancements
  - Aggregation & Block ACK
- Many optional extensions (e.g. beamforming)
- Maximum of 200+ mbps user throughput

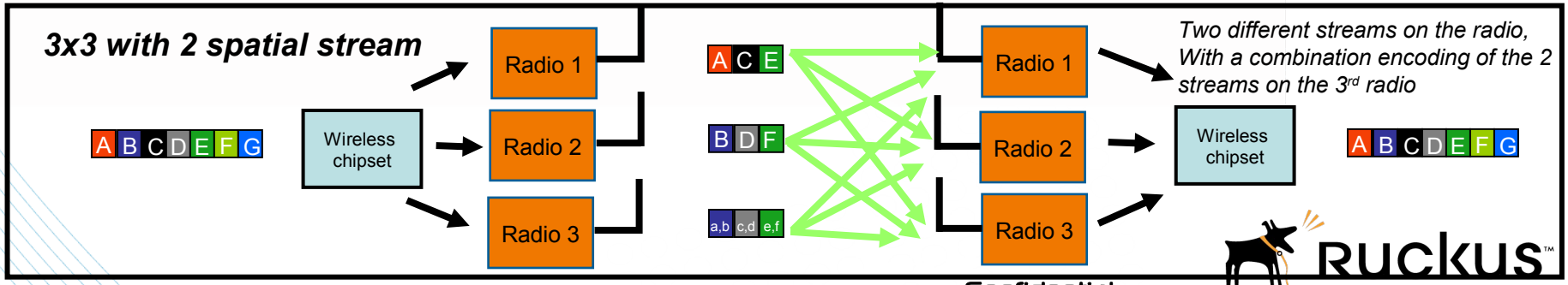
simo x mimo


RF
Front
End
Chain
PA
CPU
MAC
BB
Radio
LNA
2.4
11n
Chain
Radio
Radio
Radio
2x2
2x3
3x3
3dB
1,2,5
Gain
MultiAP
Diversity
MAC
BB









theoretical throughput of 802.11n

Expected 802.11n Data Rates

	One Spatial Stream			Two Spatial Streams		
802.11a 802.11g Rates	11n Mandatory Data Rates	With Channel Bonding (40MHz)	With Short Guard Interval	Two Spatial Streams	With Channel Bonding (40MHz)	With Short Guard Interval
6	6.5	13.5	15	13	27	30
9	13	27	30	26	54	60
12	19.5	40.5	45	39	81	90
18	26	54	60	52	108	120
24	39	81	90	78	162	180
36	52	108	120	104	216	240
48	58.5	121.5	135	117	243	270
54	65	135	150	130	270	300

Key benefits:
1. Second spatial stream doubles the rate
2. Channel bonding roughly doubles the rate
3. Short guard interval increases rate by roughly 10%

Note: the standard specifies up-to 600Mbps rates (4 spatial streams) – not supported by current generation chips

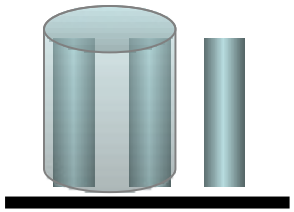
Other Takeaways

1. Higher Throughput with increase of PHY rate from 54 Mbps (.11g) to 300 Mbps (.11n)
2. Complexity of Selecting the Optimum Data Rate (8 rates for .11g vs. 12 rates for a two TX system and 24 rates for a three TX system)
3. Exponentially more difficult with additional modulation options (unequal modulation)

40 MHz channel (aka channel bonding)

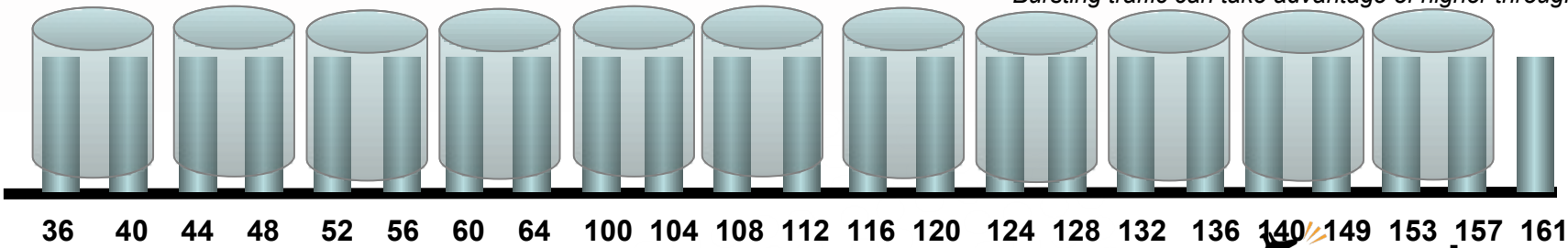
Wider bandwidth is analogous to wider highways

- Combines 2 x 20 MHz channels to increase spectral efficiency in periods of minimum interference
- regular implementations could be susceptible to interference
- usually results in higher and more consistent throughput



2.4 GHz *– Effective in certain situations*

- *Reduces the time exposed to interference*
- *Bursting traffic can take advantage of higher throughput*

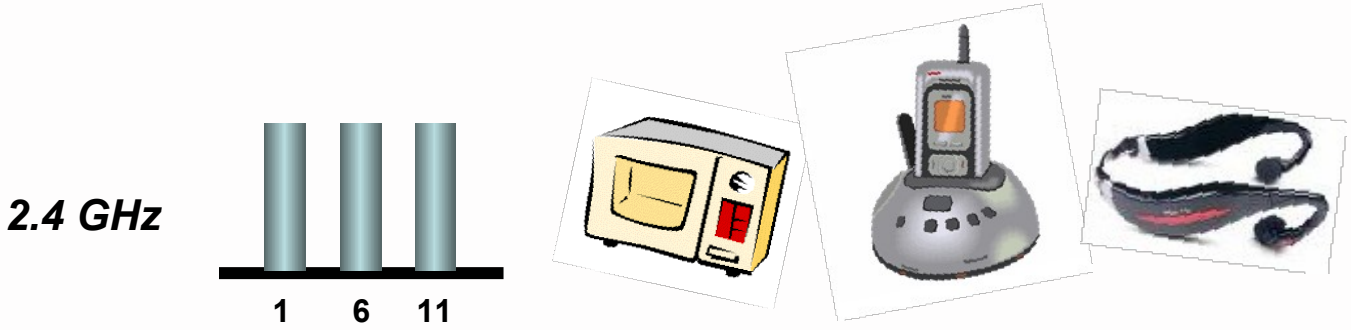


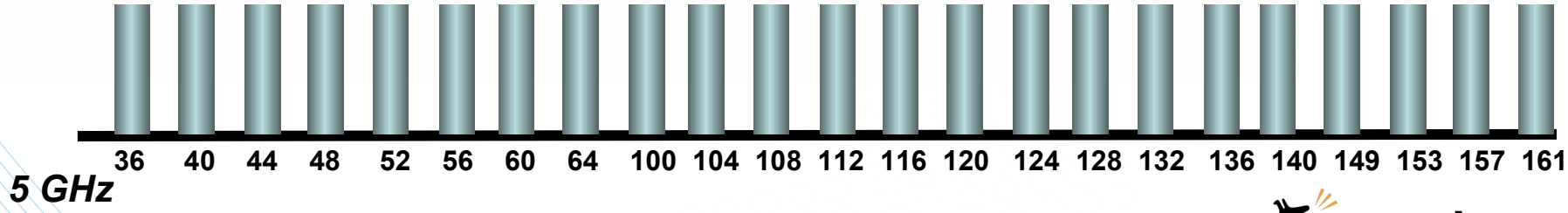
5 GHz *- Flexible for channel planning*

5 GHz operation

Operating in a cleaner frequency range, but more challenged attenuation

- Less crowded RF environment (most devices occupies 2.4 GHz range)
- More channels to operate (23 channels versus 3 channels)
- Higher attenuation of RF signals versus 2.4 GHz





PHY rates for current IIn chipsets

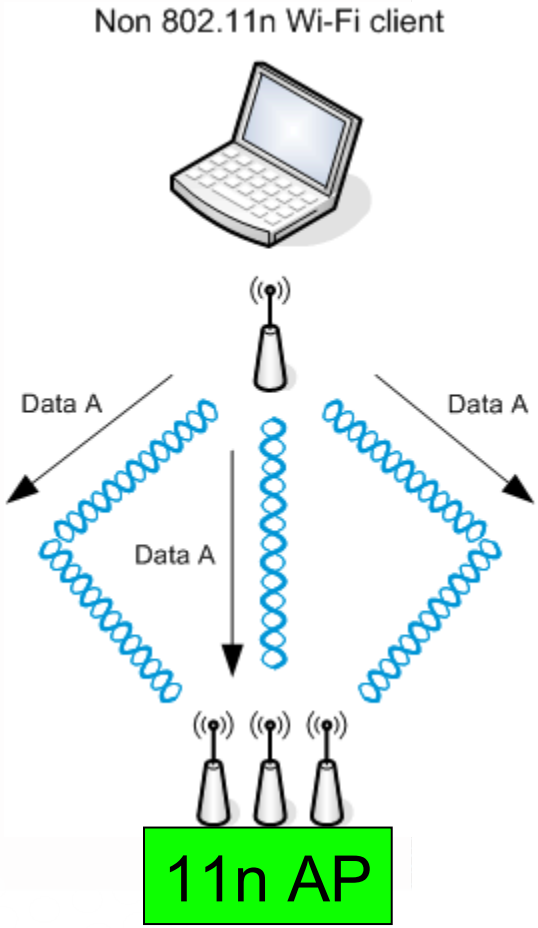
802.11n HT Rates				20 Mhz		40 Mhz	
				GI=800	GI=400	GI=800	GI=400
# Spatial Streams	Modulation	Coding	MCS	Mbps	Mbps	Mbps	Mbps
1	BPSK	½	0	6.5	7.2	13.5	15
1	QPSK	½	1	13	14.4	27	30
1	QPSK	¾	2	19.5	21.7	40.5	45
1	16-QAM	½	3	26	28.9	54	60
1	16-QAM	¾	4	39	43.3	81	90
1	64-QAM	2/3	5	52	57.8	108	120
1	64-QAM	¾	6	58.5	65	121.5	135
1	64-QAM	5/6	7	65	72.2	135	150
2	BPSK	½	8	13	14.4	27	30
2	QPSK	½	9	26	28.8	54	60
2	QPSK	¾	10	39	43.4	81	90
2	16-QAM	½	11	52	57.8	108	120
2	16-QAM	¾	12	78	86.6	162	180
2	64-QAM	2/3	13	104	115.6	216	240
2	64-QAM	¾	14	117	130	243	270
2	64-QAM	5/6	15	130	144.4	270	300

11n multi-radio techniques

- maximum ratio combining
- cyclic delay diversity
- spatial multiplexing
- transmit beamforming

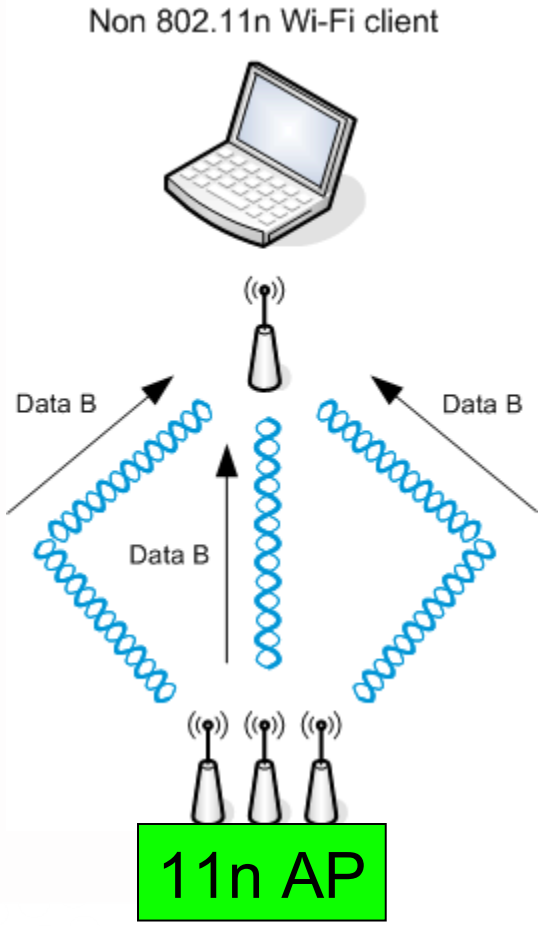
maximum ratio combining

- multiple receive radios
- mathematically combines signals
  - minimize errors
  - increase reliability
- backwards compatible with 802.11abg
- max theoretical gain
  - 2 rx chains: 3 dB
  - 3 rx chains: 5 dB
  - 4 rx chains: 6 dB
- works well in practice



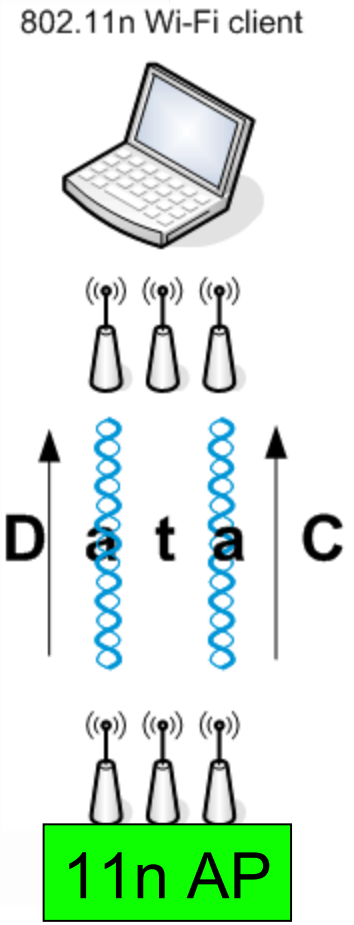
cyclic delay diversity

- multiple transmit radios
- backwards compatible with 802.11abg devices (legacy receiver)
- constantly vary the phase of 'extra' transmit signals to minimize self-interference
- does NOT always work well in practice
  - especially in line-of-sight conditions



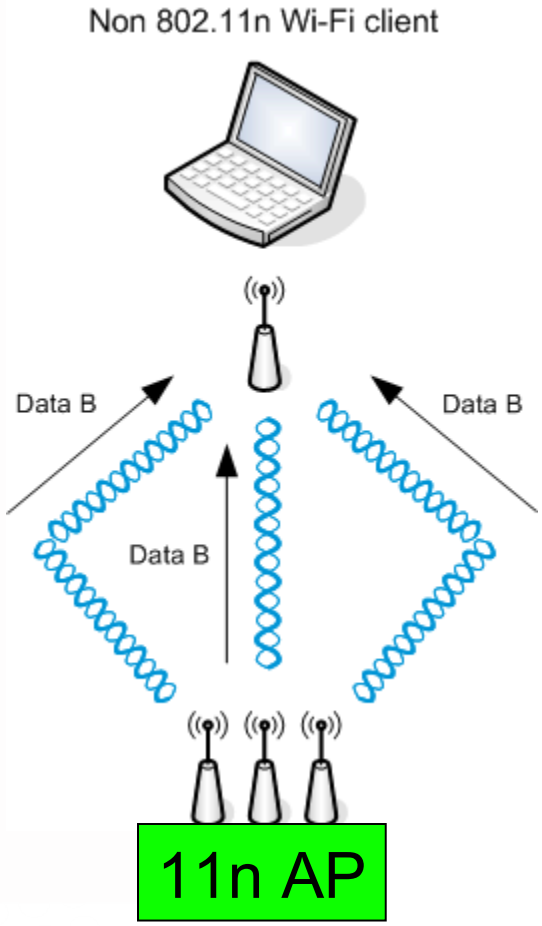
spatial multiplexing

- multiple Transmit radios
- multiple Receive radios
- requires support on both ends
- send data in parallel making use of multipath and DSP to decode
- 2, 3, or 4 Spatial Streams
  - Current chipsets implement 2 streams
- # radios must be >= # spatial streams
- sensitive to propagation environment



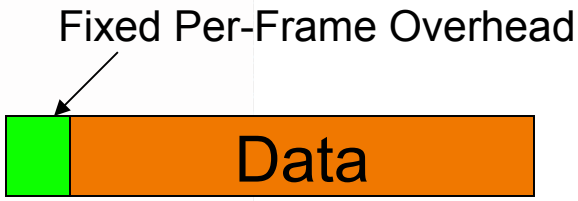
11n transmit beamforming

- multiple transmit radios
- use feedback and DSP to modify phase of each radio transmission
  - goal is to have them all arrive 'in-phase' at the receiver
- requires client support
- optional in 11n
  - not yet implemented in commercial chipsets
- theoretical gains similar to MRC but real-life gains are much lower due to implementation difficulties

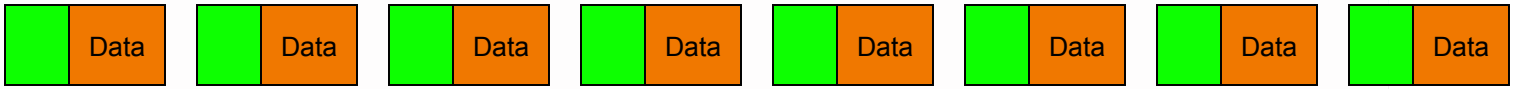


11n aggregation

- 802.11 has high per-frame overhead
  - minimum interframe spacing
  - channel access time (random backoff)
  - physical layer headers
  - MAC headers
  - 802.11 acknowledgement



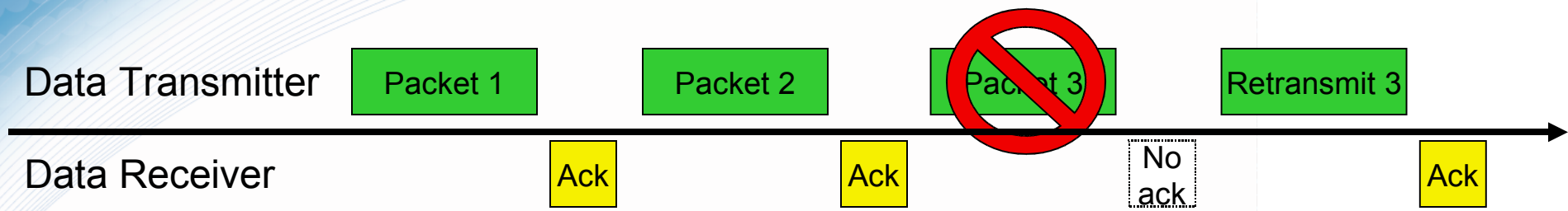
- increasing PHY rate reduces time spent transmitting data but does not reduce the fixed overhead!



- 802.11n would max out at around 50 mbps user throughput without aggregation

- with 11n aggregation, AP combines multiple frames and transmits them 'back-to-back' as one physical layer frame

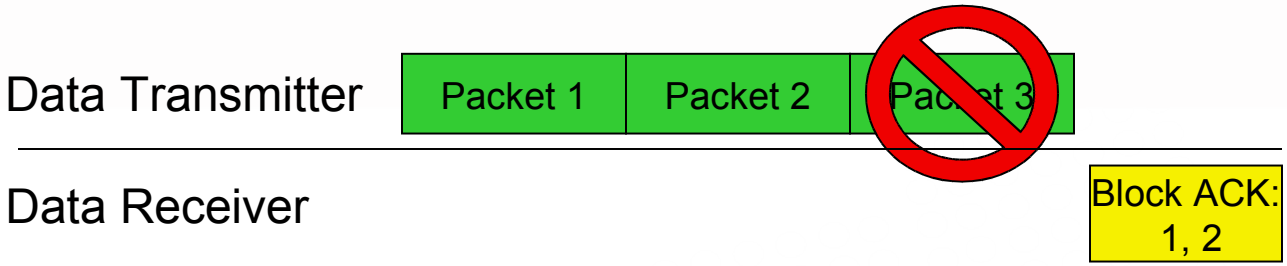
normal 802.11 acknowledgement



- very high Packet Error Rates at the physical layer
  - 2% - 20% are typical
  - 30% - 40% not uncommon
- retransmissions are necessary to provide the low Packet loss rates that most applications require
- 802.11 unicast packets are always acknowledged if successfully received
- 802.11 ACK is a very reliable mechanism
  - dedicated timeslot after data transmission
  - ACK is a very small frame (compared to data)
  - often sent at lower PHY rate than data frame

802.11n block ack

- used to make aggregation reliable
- extension of existing 802.11 ack mechanism
  - bitfield to individually acknowledge sub-frames
  - only the failed subframes need to be retransmitted
- enables user throughputs very close to the PHY data rate



pretty cool, huh?

- maybe not...

legacy-11n coexistence

- legacy clients and 11n clients can coexist on the same 11n AP
  - legacy clients use 11a/b/g rates
  - 11n clients use 11n phy rates
- but since clients 'share the air', legacy clients can consume a disproportionate share of the airtime
- smart AP scheduling algorithms can mitigate this effect

remember

- it's all about airtime
- and (self note) check YOUR TIME

11n operation modes

Mode 0: (called "Greenfield" Mode) – if all stations in a 20/40 MHz BSS are 20/40 MHz HT capable or if all stations in the BSS are 20 MHz HT stations in a 20 MHz BSS.

Mode 1: (called HT non-Member Protection Mode) – used if there are non-HT stations or APs using the primary and/or secondary channels

Mode 2: (called HT 20 MHz Protection Mode) – if only HT stations are associated in the 20/40 MHz BSS and at least one 20 MHz HT station is associated.

Mode 3: (called HT Mixed Mode) – used if one or more non-HT stations are associated in the BSS.

info from the cwmp.com folks

did you know?

- if you use wep or tkip, IIn will drop **automagically** to IIg speeds?

draft 2.0 says so, and IMHO it's a good thing

(some of the) lln challenges

- lln significantly improves best-case throughput
- but .lln has more performance variability
  - spatial Multiplexing requires de-correlated paths
  - use of 40MHz limited by interference
  - ,ore MAC+PHY parameters to optimize in real-time
    - selection of # of spatial streams
    - 40MHz versus 20MHz channels
    - long versus short Guard Interval
  - more sensitive to interference

spatial multiplexing problems

- SM requires each Spatial Stream to propagate differently through the environment
- If signal takes the same path from Tx antennas to RX antennas the spatial streams will interfere with each other
  - always a problem in Line-Of-Site environments
- furthermore, the signal quality of the **worse** of the two streams determines usable phy rate for both streams
- In many cases SM is not viable due to these issues
  - fallback to non-SM rates is common
  - IIn performance driven by % of time and locations the AP can use SM

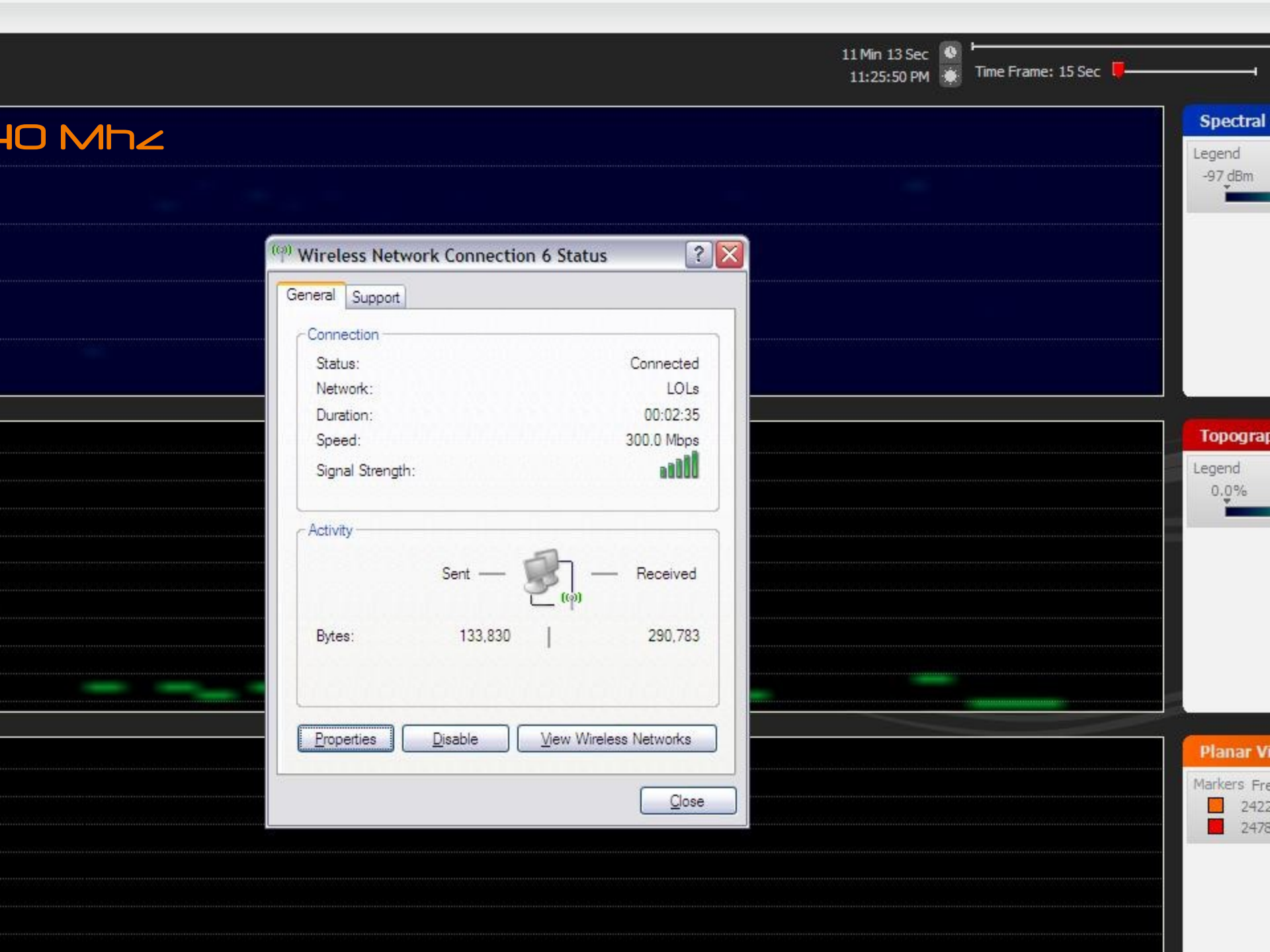
okay, it sucks then?

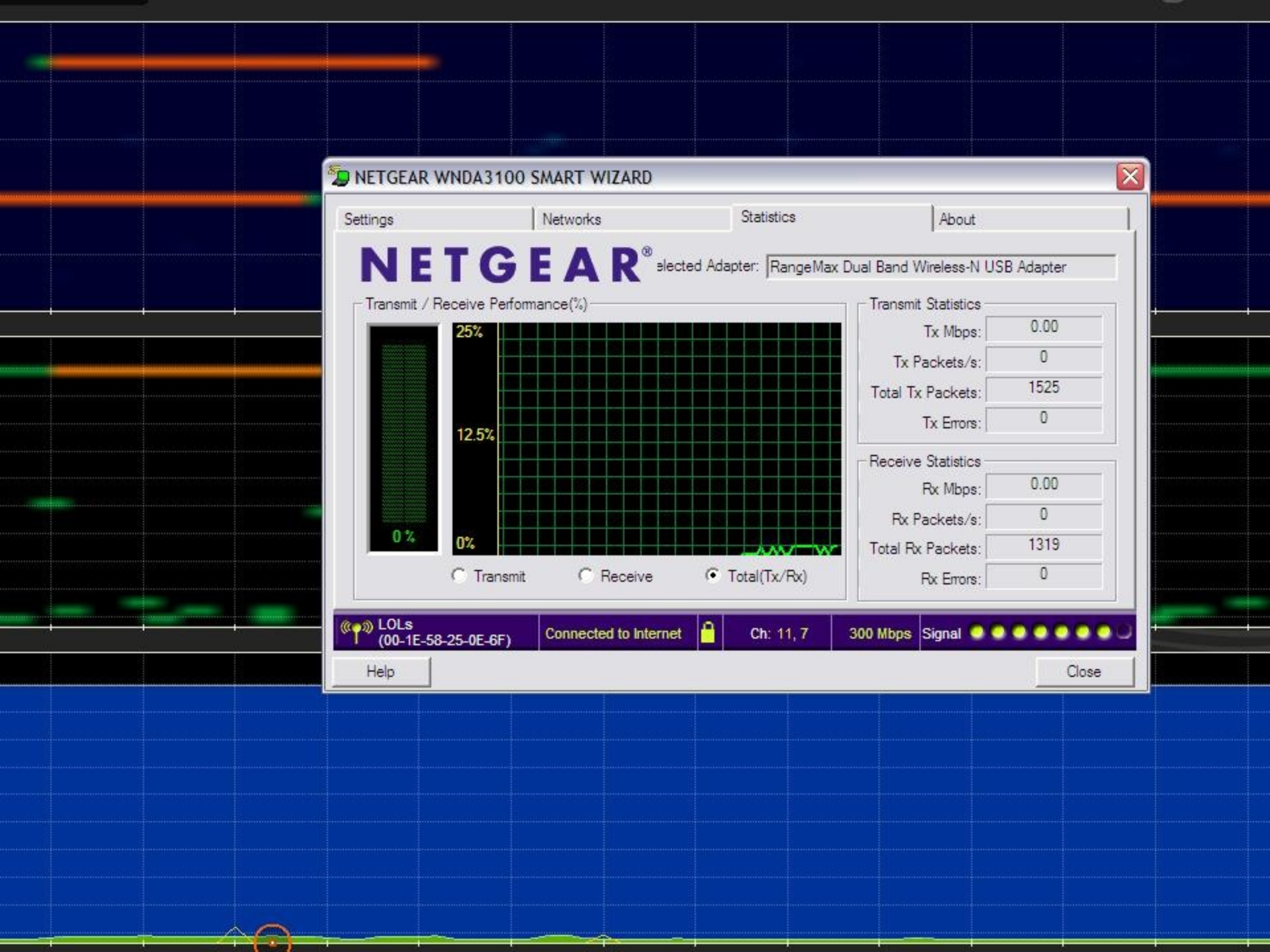
- absolutely not


REALITY
CHECK
AHEAD

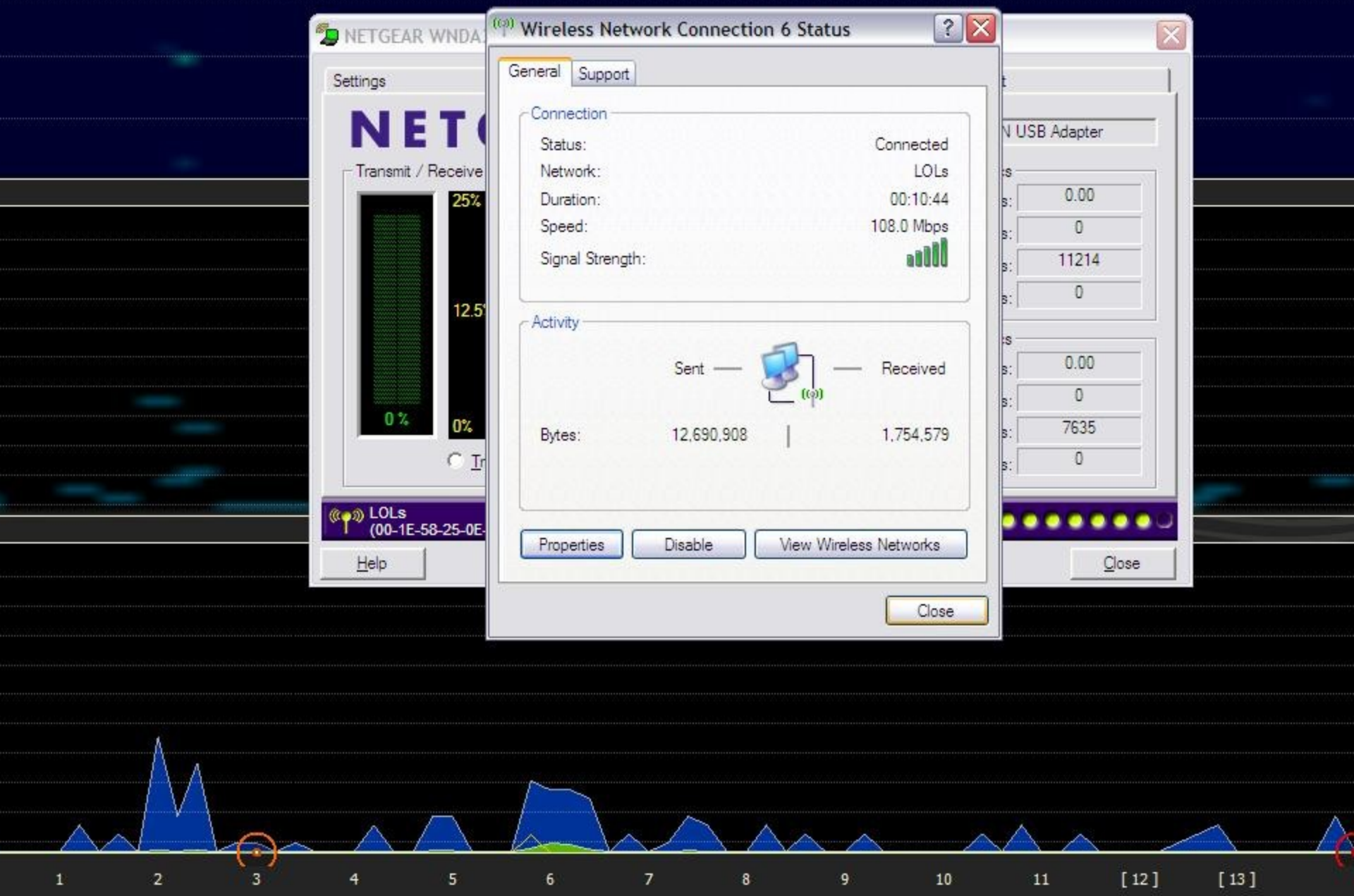
considerations

- site surveys
- existing infrastructure (speed/ poe)
- wlan technologies, models and possible changes
- client support


11 Min 13 Sec
11:25:50 PM
Time Frame: 15 Sec
40 Mhz
Spectral
Legend
-97 dBm
Topograp
Legend
0.0%
Planar V
Markers Fre
2422
2478
Wireless Network Connection 6 Status
General
Support
Connection
Status: Connected
Network: LOLs
Duration: 00:02:35
Speed: 300.0 Mbps
Signal Strength:
Activity
Sent
Received
Bytes: 133,830 290,783
Properties
Disable
View Wireless Networks
Close


NETGEAR WNDA3100 SMART WIZARD
Settings
Networks
Statistics
About
NETGEAR®
elected Adapter:
RangeMax Dual Band Wireless-N USB Adapter
Transmit / Receive Performance(%)
25%
12.5%
0%
0 %
Transmit
Receive
Total(Tx/Rx)
Transmit Statistics
Tx Mbps: 0.00
Tx Packets/s: 0
Total Tx Packets: 1525
Tx Errors: 0
Receive Statistics
Rx Mbps: 0.00
Rx Packets/s: 0
Total Rx Packets: 1319
Rx Errors: 0
LOLs
(00-1E-58-25-0E-6F)
Connected to Internet
Ch: 11, 7
300 Mbps
Signal
Help
Close

mix mode/ n and g



security considerations?

- on top of what was mentioned...
- pre-N greenfield aps/ bridges
- does not address mgmt frames crypto

conclusion

questions?

obrigado!

le@ruckuswireless.com

Ruckus WIRELESS