Wireless - What you see is not always what you get?

MikroTik User Meeting

Prague 2015

By Ron Touw

LinITX, England

Experience?

- RF Wireless Engineering for UK Government for 25 years.
- Training certifications from companies such as Marconi, Hewlett-Packard, Rohde & Schwarz, Microsoft, Ruckus, Meru.
- User of MikroTik since 2006
- Certified Consultant and Trainer since 2009.
- Member of RoutedWorld.com

Who are LinITX?

- Largest MikroTik Distributor in UK
- Largest number of MikroTik Certified Consultants in a single UK Distributor
- Certified MikroTik Training Centre
- Provide Consultancy and Third Line Support to ISPs and WISPs using MikroTik Routers

What's the Problem?

- Wireless is 'invisible'
- Needs other tools for it to be 'seen'
- Poor CCQ, Low or 'flapping' Data rates, even OFDM error stats only provide limited information - basically "there is a problem"
- We may change a card and the problem is solved
- But WHAT was the problem? We need to:
  - To get the complete picture
  - To fully understand what's "out there"

Solution to the Problem?

- Use a Spectrum Analyser? But which?
  - MikroTik ‘Built in’ - via The Dude?
  - MikroTik ‘Built in’ - via Simple CLI?
- Independent / Calibrated / High Cost? E.g.
  - HP Agilent
  - Rohde & Schwarz

Solution to the Problem?

- Or… Independent / Low Cost, e.g.
  - Metageeks Wi-Spy

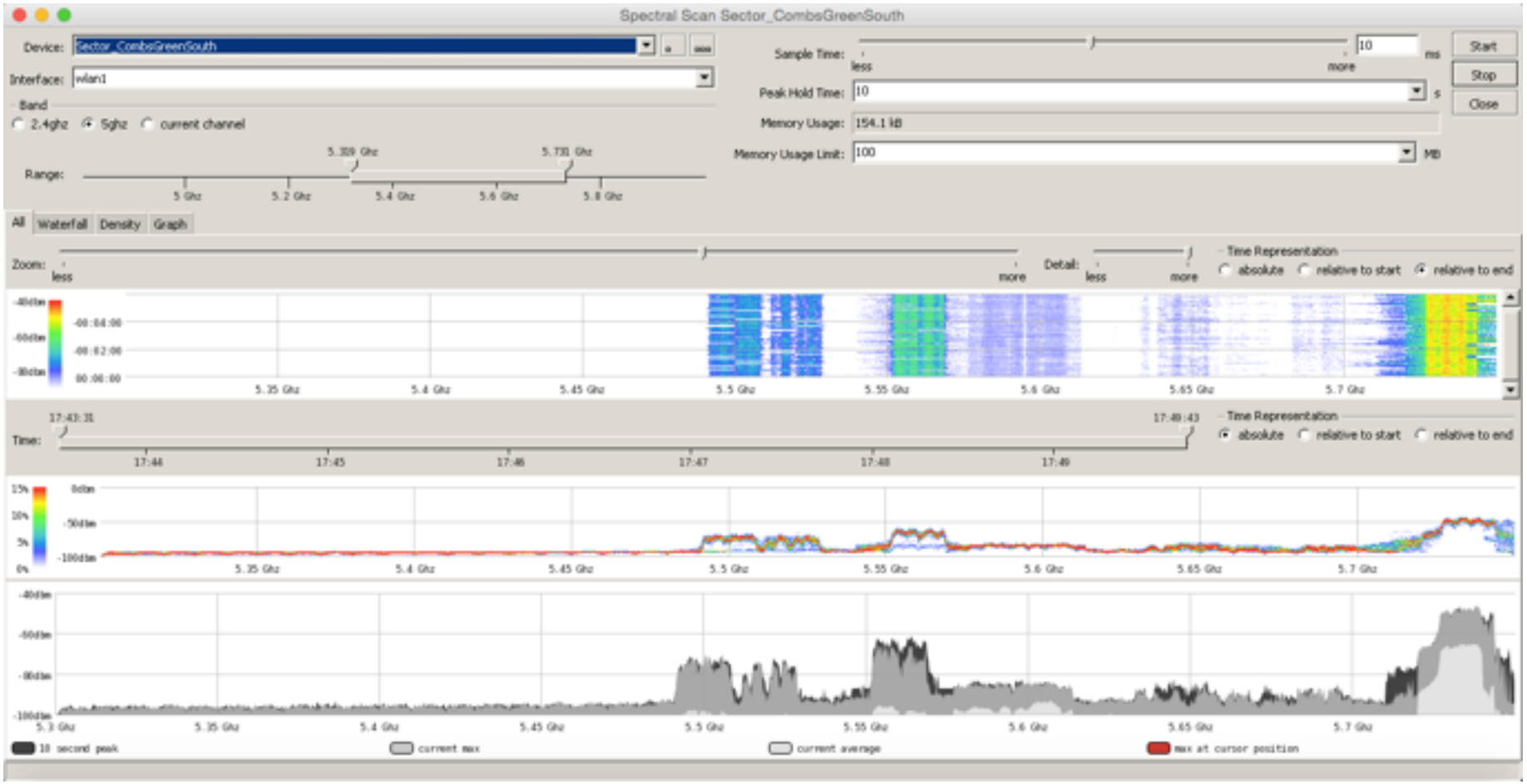
  - Signalhound

  - Aaronia Spectran

MikroTik Tools

- Benefit of using MikroTik ‘built in’ analysers:
  - Low cost - already paid for :)
  - Uses the actual link equipment itself
    - Any analysis will “see” the same as the link itself “sees”.
    - Same antenna, therefore
    - Same beam width / aperture
- Requires install of ‘TheDude’

Spectrum - via TheDude



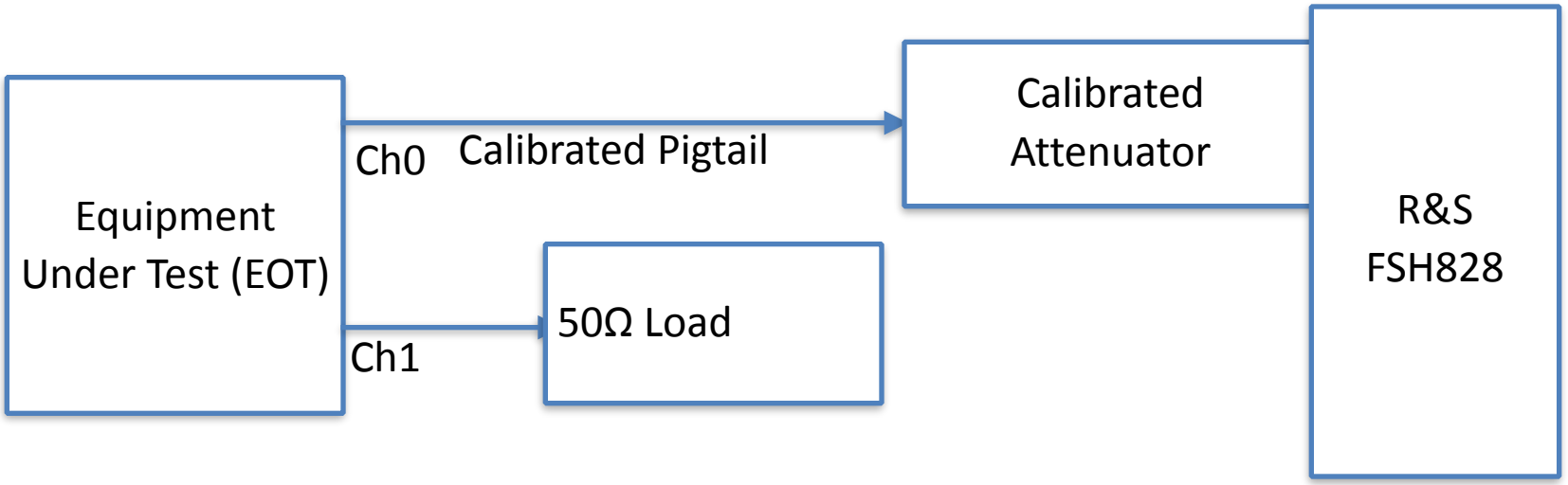
Spectrum Analysers

- Using a Spectrum Analyser is not just about seeing noise or interference on a link
- Also can be used to find what problems **we** are **generating** by using faulty equipment
- Can also be used to demonstrate the difference between “reality” and “theory”
  - Are we only operating on one frequency or are there spurious transmissions?
  - I.e. When we set a power level, is that the real power level we get?

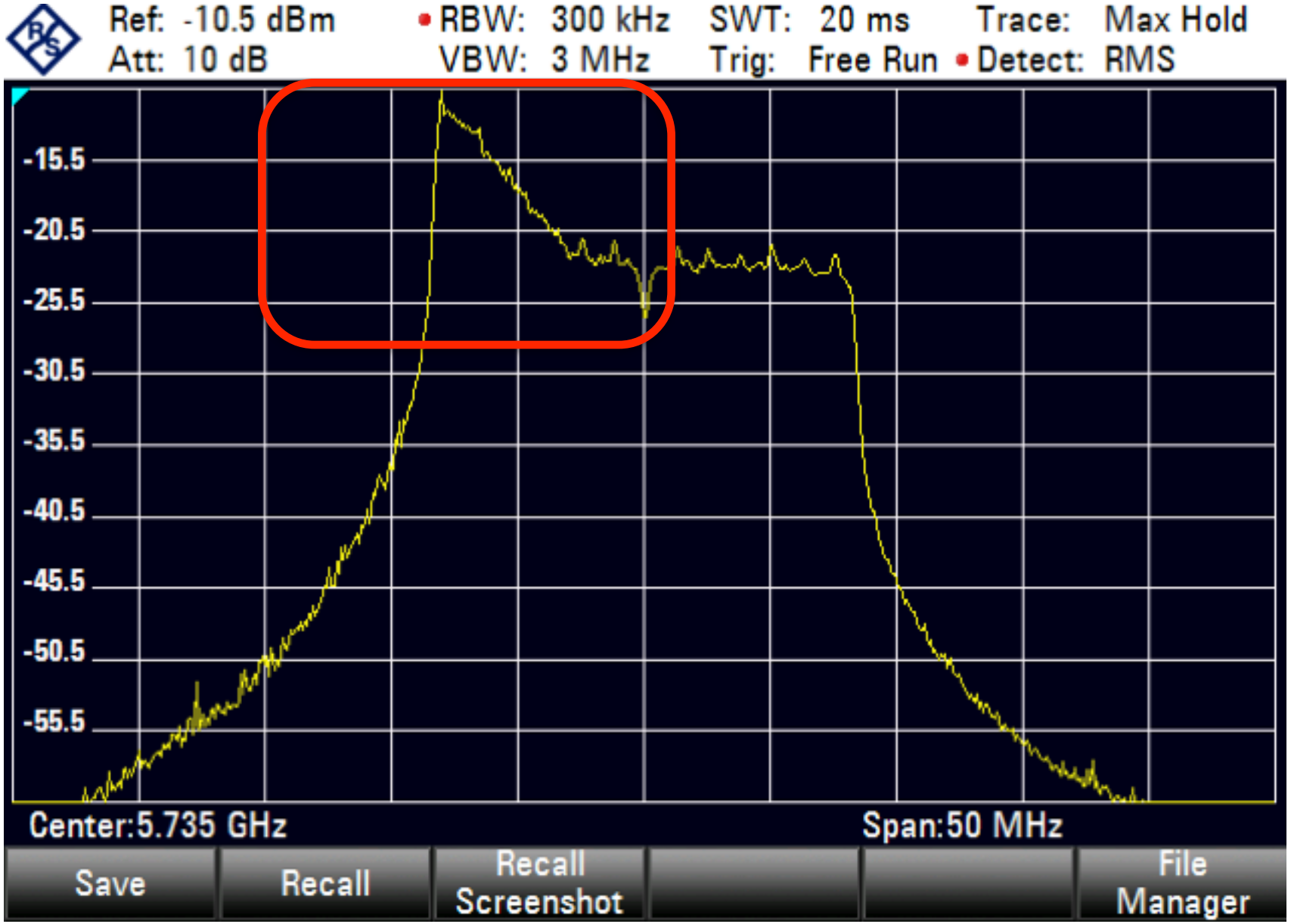
Self Generated problems?

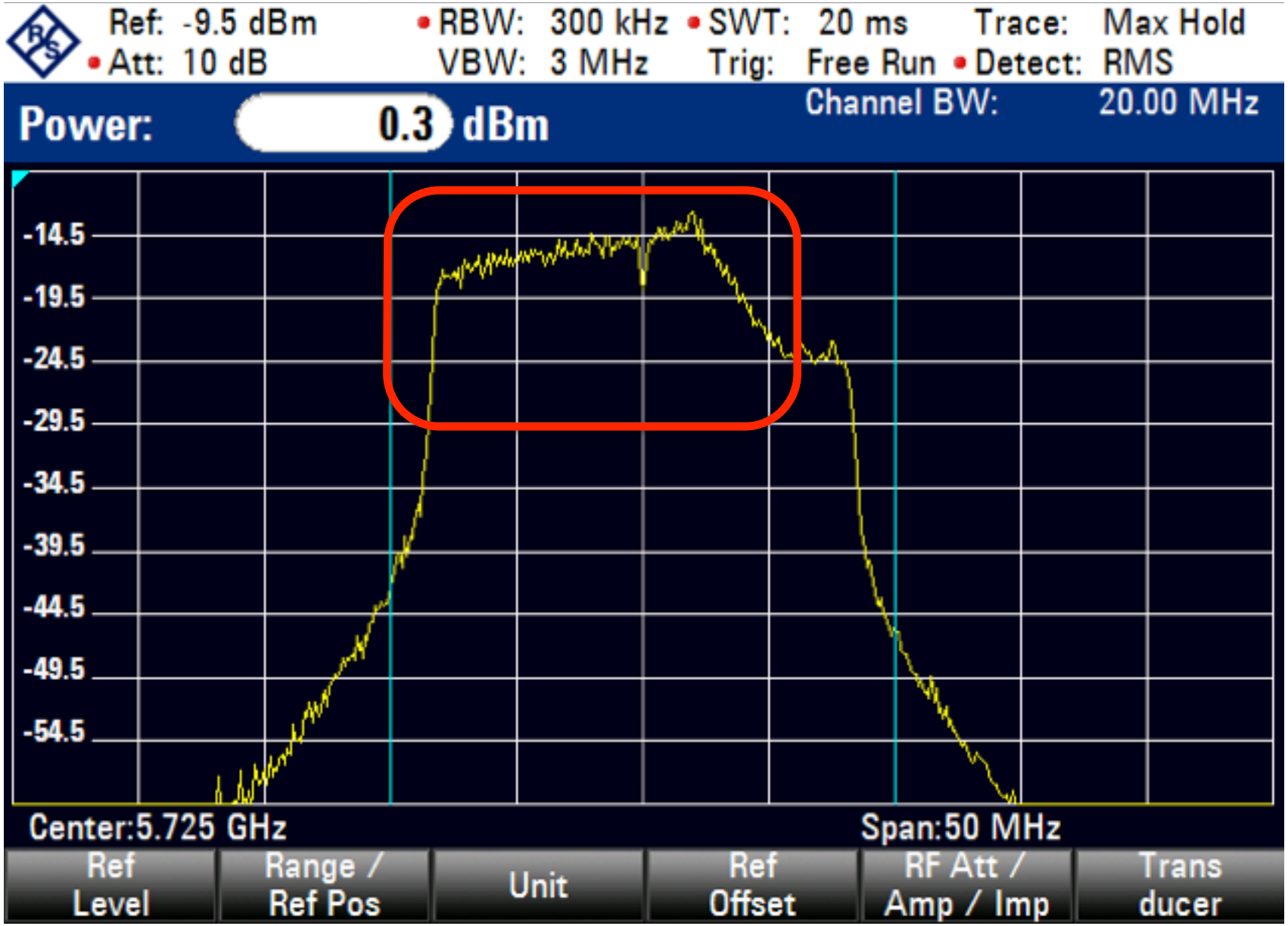
- Transmitter failure is predictable, sadly however what is not predictable is **when!**
- Nor do we know “how” it will fail
- Failure types:
  - No output at all - simple/visible/obvious
  - Lowered output - partially visible/ detectable?
  - Distorted output / spurious - ‘invisible’?
  - Interference or high noise floor?

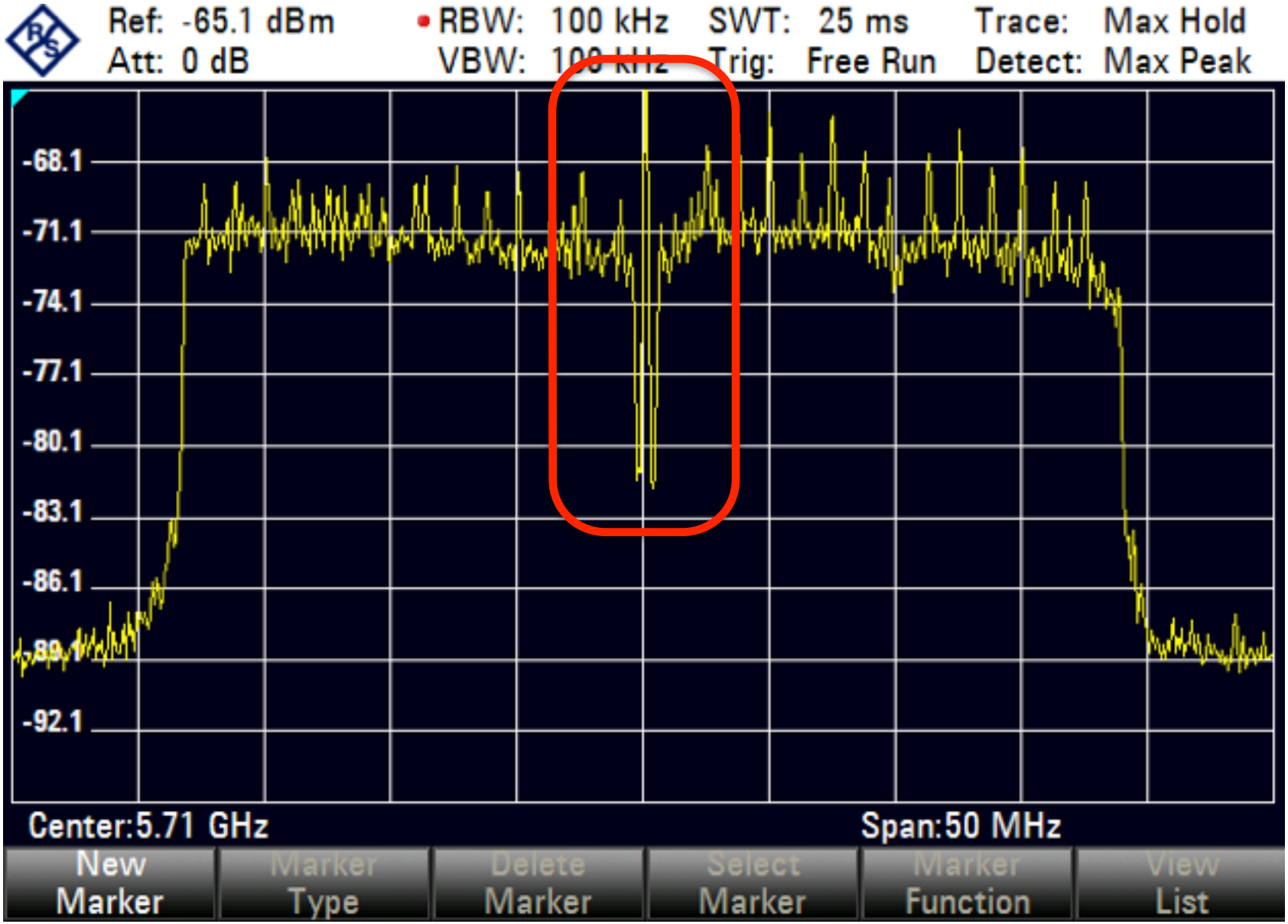
Let's see some Spectrum examples

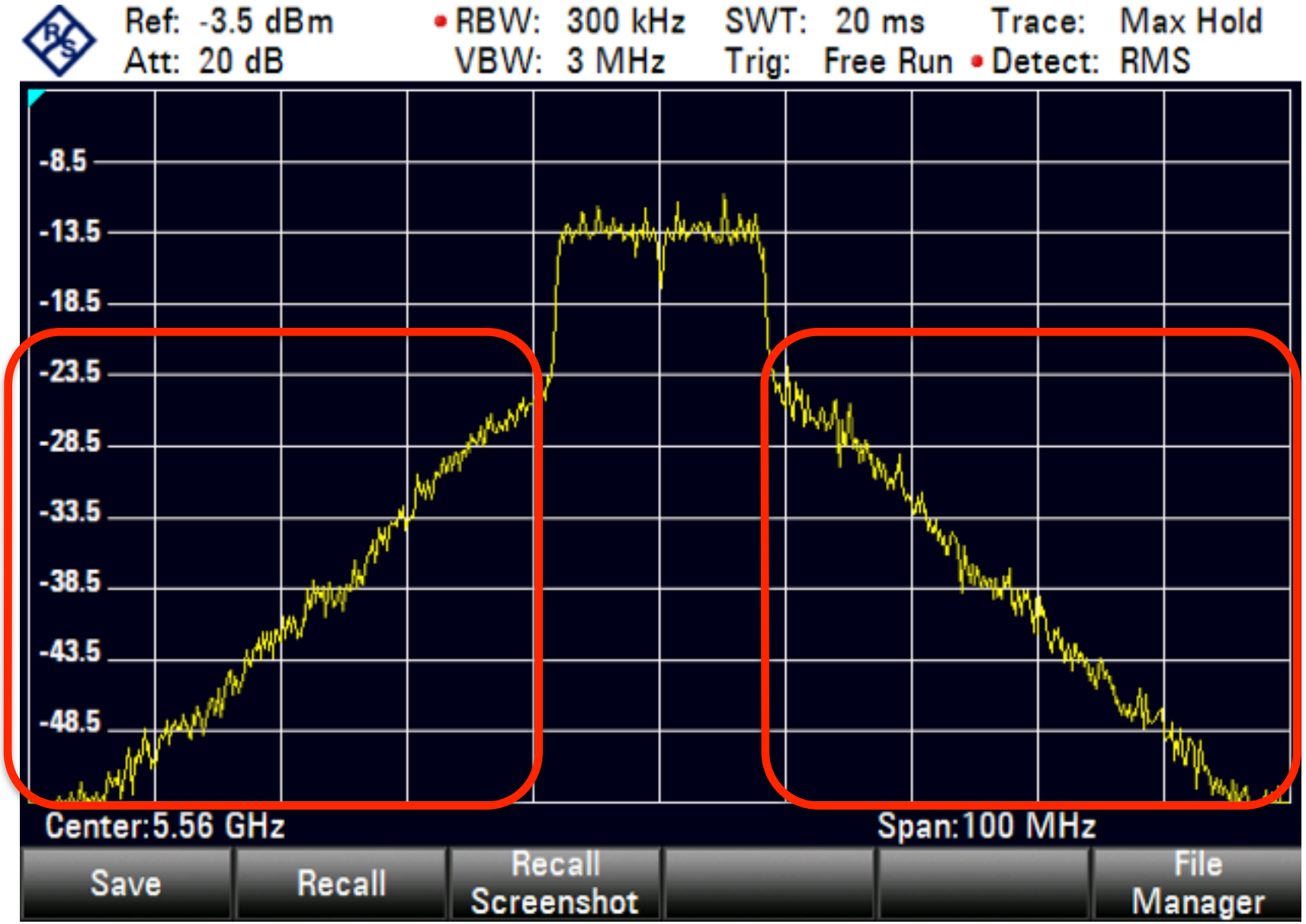


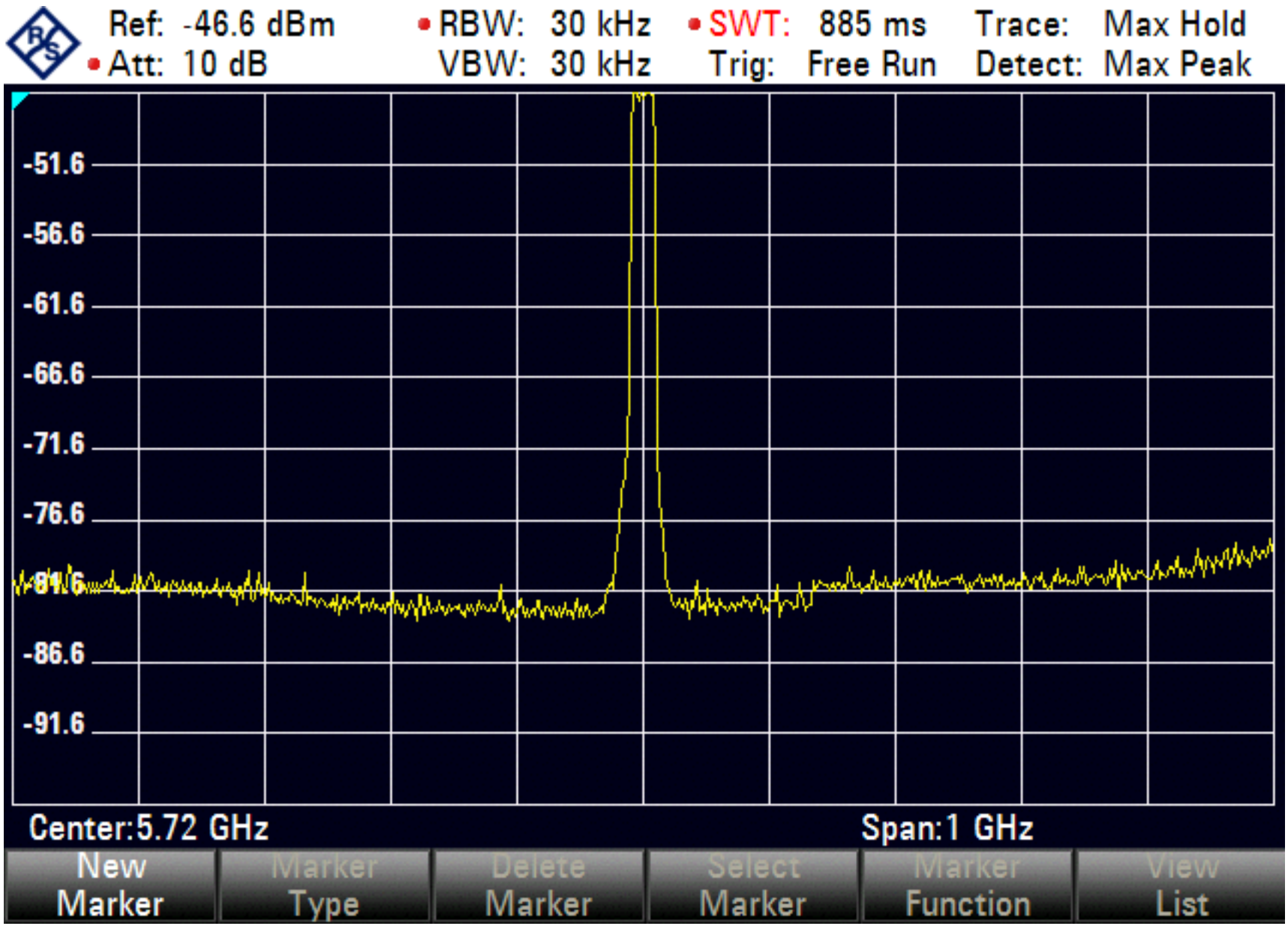
- Testing cards thought to be faulty or have caused suspicions in the past can be very illuminating…

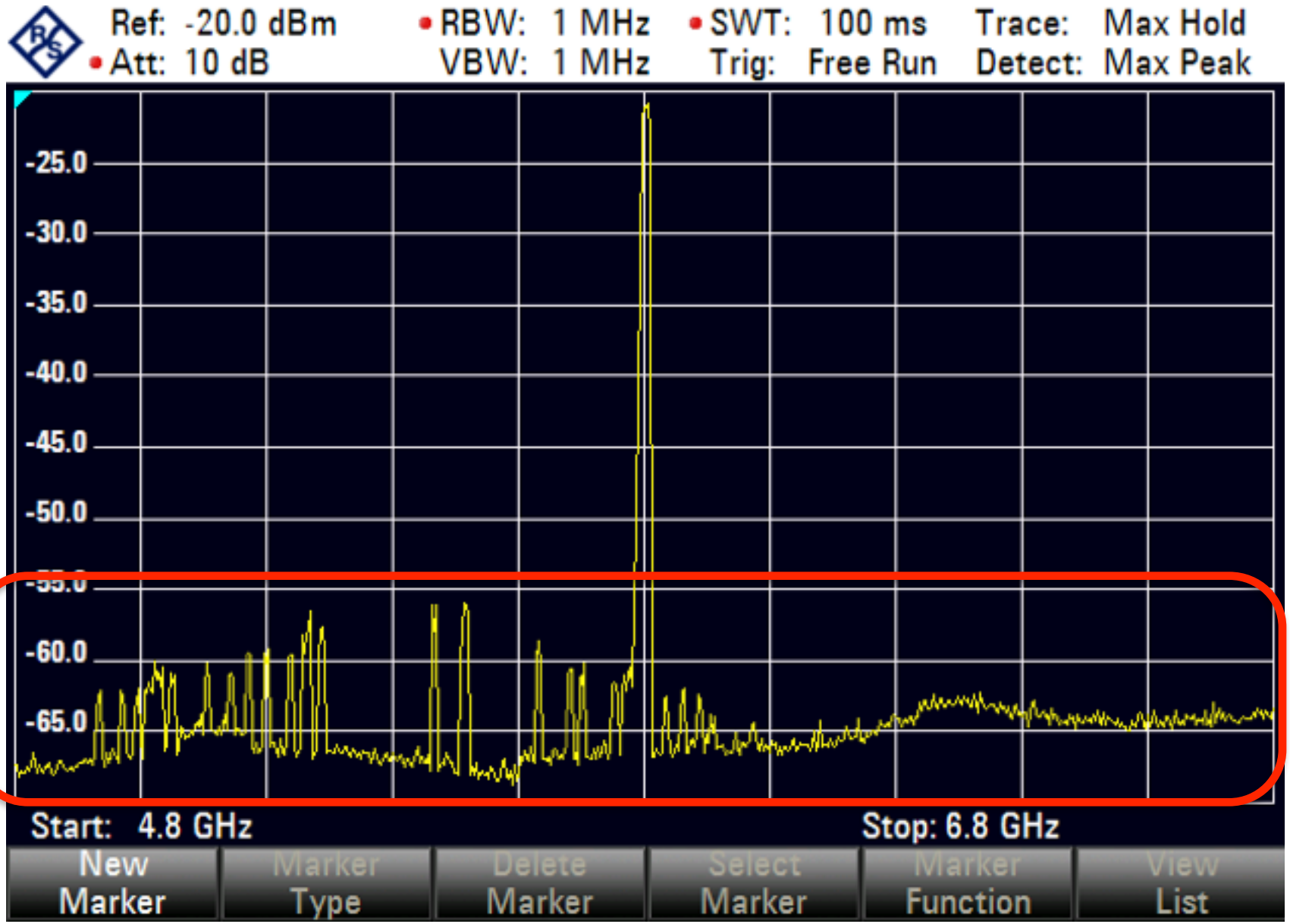

Ref: -10.5 dBm
Att: 10 dB
RBW: 300 kHz
VBW: 3 MHz
SWT: 20 ms
Trig: Free Run
Trace: Max Hold
Detect: RMS
-15.5
-20.5
-25.5
-30.5
-35.5
-40.5
-45.5
-50.5
-55.5
Center:5.735 GHz
Span:50 MHz
Save
Recall
Recall Screenshot
File Manager

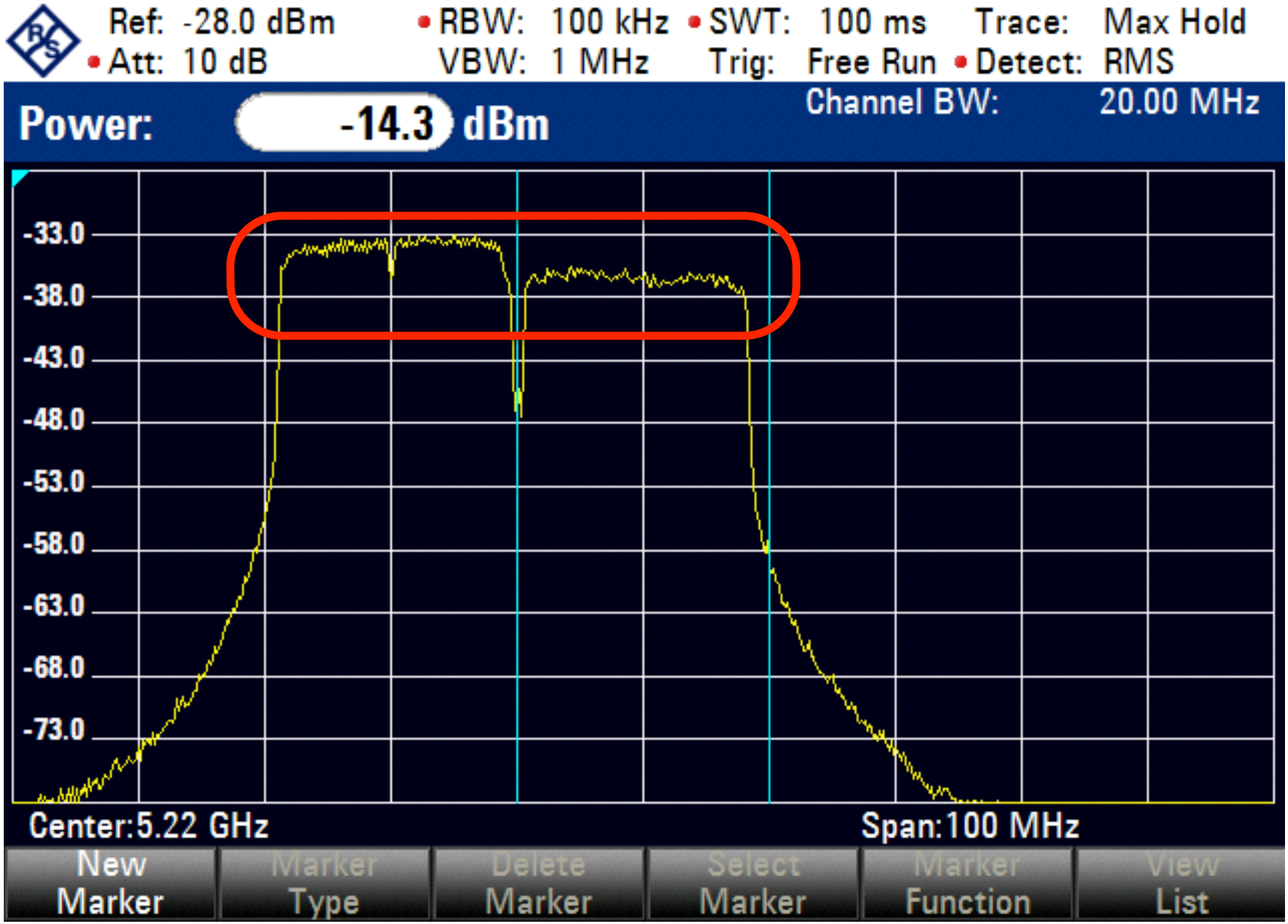

Ref: -9.5 dBm
RBW: 300 kHz
SWT: 20 ms
Trace: Max Hold
Att: 10 dB
VBW: 3 MHz
Trig: Free Run
Detect: RMS
Power: 0.3 dBm
Channel BW: 20.00 MHz
-14.5
-19.5
-24.5
-29.5
-34.5
-39.5
-44.5
-49.5
-54.5
Center:5.725 GHz
Span:50 MHz
Ref Level
Range / Ref Pos
Unit
Ref Offset
RF Att / Amp / Imp
Trans ducer

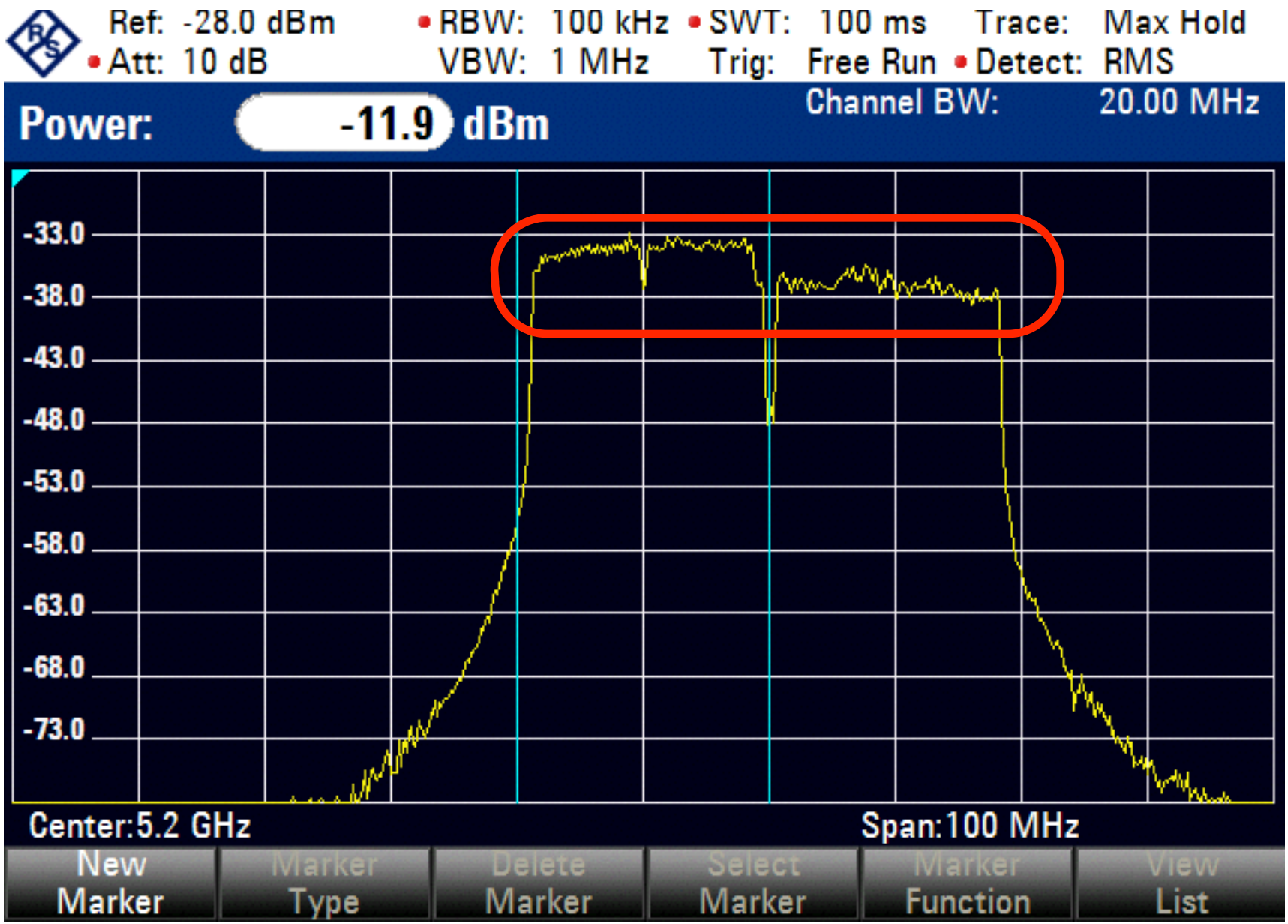

Ref: -65.1 dBm
Att: 0 dB
RBW: 100 kHz
VBW: 100 kHz
SWT: 25 ms
Trig: Free Run
Trace: Max Hold
Detect: Max Peak
-68.1
-71.1
-74.1
-77.1
-80.1
-83.1
-86.1
-89.1
-92.1
Center:5.71 GHz
Span:50 MHz
New Marker
Marker Type
Delete Marker
Select Marker
Marker Function
View List


Ref: -3.5 dBm
Att: 20 dB
RBW: 300 kHz
VBW: 3 MHz
SWT: 20 ms
Trig: Free Run
Trace: Max Hold
Detect: RMS
-8.5
-13.5
-18.5
-23.5
-28.5
-33.5
-38.5
-43.5
-48.5
Center:5.56 GHz
Span:100 MHz
Save
Recall
Recall Screenshot
File Manager


Ref: -46.6 dBm
Att: 10 dB
RBW: 30 kHz
VBW: 30 kHz
SWT: 885 ms
Trig: Free Run
Trace: Max Hold
Detect: Max Peak
-51.6
-56.6
-61.6
-66.6
-71.6
-76.6
-81.6
-86.6
-91.6
Center:5.72 GHz
Span:1 GHz
New Marker
Marker Type
Delete Marker
Select Marker
Marker Function
View List


Ref: -20.0 dBm
Att: 10 dB
RBW: 1 MHz
VBW: 1 MHz
SWT: 100 ms
Trig: Free Run
Trace: Max Hold
Detect: Max Peak
-25.0
-30.0
-35.0
-40.0
-45.0
-50.0
-60.0
-65.0
Start: 4.8 GHz
Stop: 6.8 GHz
New Marker
Marker Type
Delete Marker
Select Marker
Marker Function
View List


Ref: -28.0 dBm
RBW: 100 kHz
SWT: 100 ms
Trace: Max Hold
Att: 10 dB
VBW: 1 MHz
Trig: Free Run
Detect: RMS
Power: -14.3 dBm
Channel BW: 20.00 MHz
-33.0
-38.0
-43.0
-48.0
-53.0
-58.0
-63.0
-68.0
-73.0
Center:5.22 GHz
Span:100 MHz
New Marker
Marker Type
Delete Marker
Select Marker
Marker Function
View List


Ref: -28.0 dBm
RBW: 100 kHz
SWT: 100 ms
Trace: Max Hold
Att: 10 dB
VBW: 1 MHz
Trig: Free Run
Detect: RMS
Power: -11.9 dBm
Channel BW: 20.00 MHz
-33.0
-38.0
-43.0
-48.0
-53.0
-58.0
-63.0
-68.0
-73.0
Center:5.2 GHz
Span:100 MHz
New Marker
Marker Type
Delete Marker
Select Marker
Marker Function
View List

How about Tx Power?

- How can you know what Tx Power you are generating?
- Do you set the Tx-Power variable and blindly trust that is what you will get?
- What about card errors?
- What about fault conditions?
- Have you read the manufacturer's specifications regarding 'tolerance'?

802.11n/ac Differences

- For 802.11ac chipsets it reports Tx power of ALL chains combined
- For 802.11n chipsets it reports Tx power of each chain
- E.g.
  - 2 chain 802.11n, 27dBm is 27dBm PER Chain, therefore 30dBm total!
  - 2 chain 802.11ac, 27dBm is 27dBm

Datasheets & “Tolerance”

	Data Rate	TX Power		Tolerance
		1 chain	2 chains	
5G HT 20	MCS0/8	18dBm	21dBm	±2dB
	MCS1/9	18dBm	21dBm	±2dB
	MCS2/10	17dBm	20dBm	±2dB
	MCS3/11	17dBm	20dBm	±2dB
	MCS4/12	16dBm	19dBm	±2dB
	MCS5/13	16dBm	19dBm	±2dB
	MCS6/14	15dBm	18dBm	±2dB
	MCS7/15	12dBm	15dBm	±2dB
	Data Rate	TX Power		Tolerance
		1 chain	2 chains	
5G HT 40	MCS0/8	17dBm	20dBm	±2dB
	MCS1/9	17dBm	20dBm	±2dB
	MCS2/10	17dBm	20dBm	±2dB
	MCS3/11	17dBm	20dBm	±2dB
	MCS4/12	16dBm	19dBm	±2dB
	MCS5/13	14dBm	17dBm	±2dB
	MCS6/14	13dBm	16dBm	±2dB
	MCS7/15	9dBm	12dBm	±2dB

Datasheets & “Tolerance”

- Chipset manufacturers such as Intel or Qualcomm Atheros only provide a +/-2dB tolerance (or accuracy) in their data sheets
- Therefore any actual generated output power could be anywhere between +/-2dB from the value set in RouterOS. That’s 4dB of ‘uncertainty’.
- You set “20dBm” but what do you get?
- 18 - 22dBm!

Trusted?

- For testing the unknown or non-obvious problems we need equipment we can trust.
- Trustworthy equipment will be calibrated to a standard or is known to provide accurate trustworthy results.
- That requires the equipment to be calibrated against a ‘Standard’.

Trusted? (“Uncertainty”)

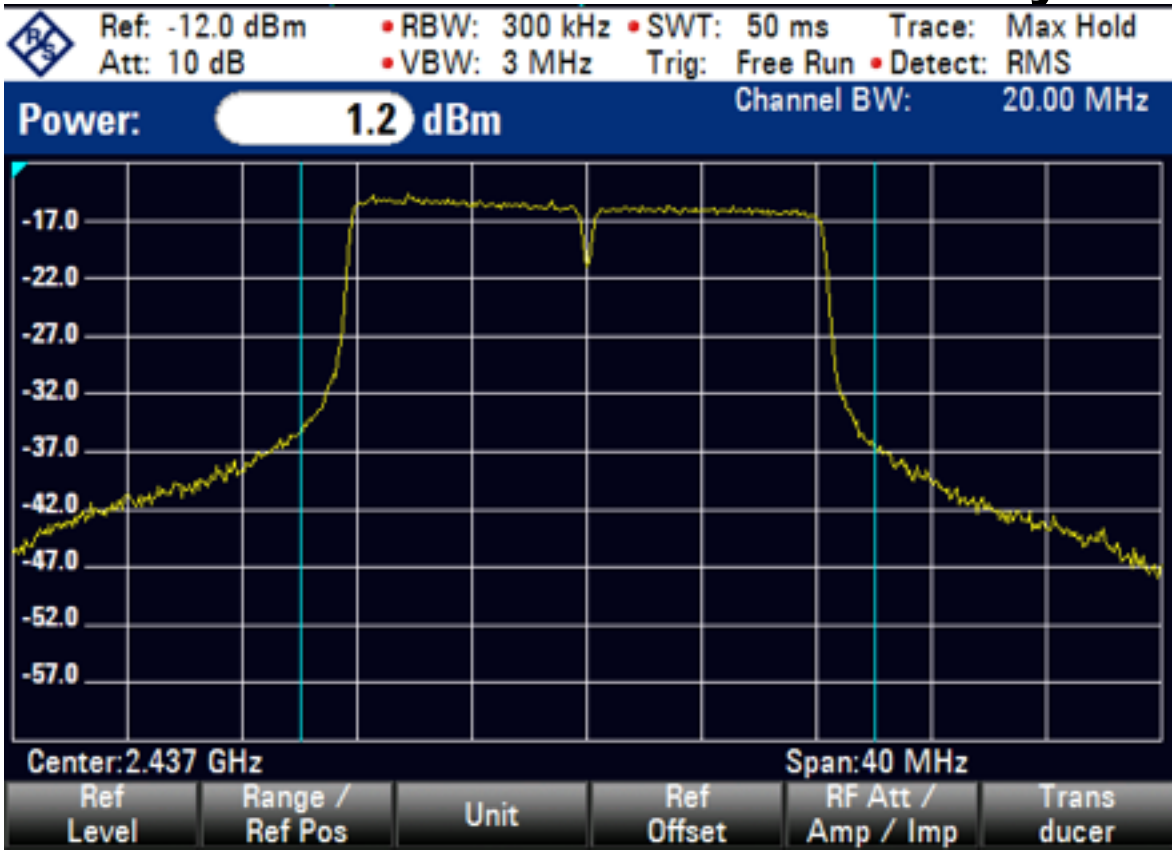
- But, first… A question - which is the more accurate measurement?
  - A - Tx Power = **23.4376** dBm or
  - B - Tx Power = **23.4** dBm?

Measuring Tx Power

- To ensure the measurement is trusted use calibrated equipment
- I use a Rohde and Schwarz FSH-828)

Measurement Method

- FSH828 has a special power measurement function for TDMA and CDMA systems



Accuracy?

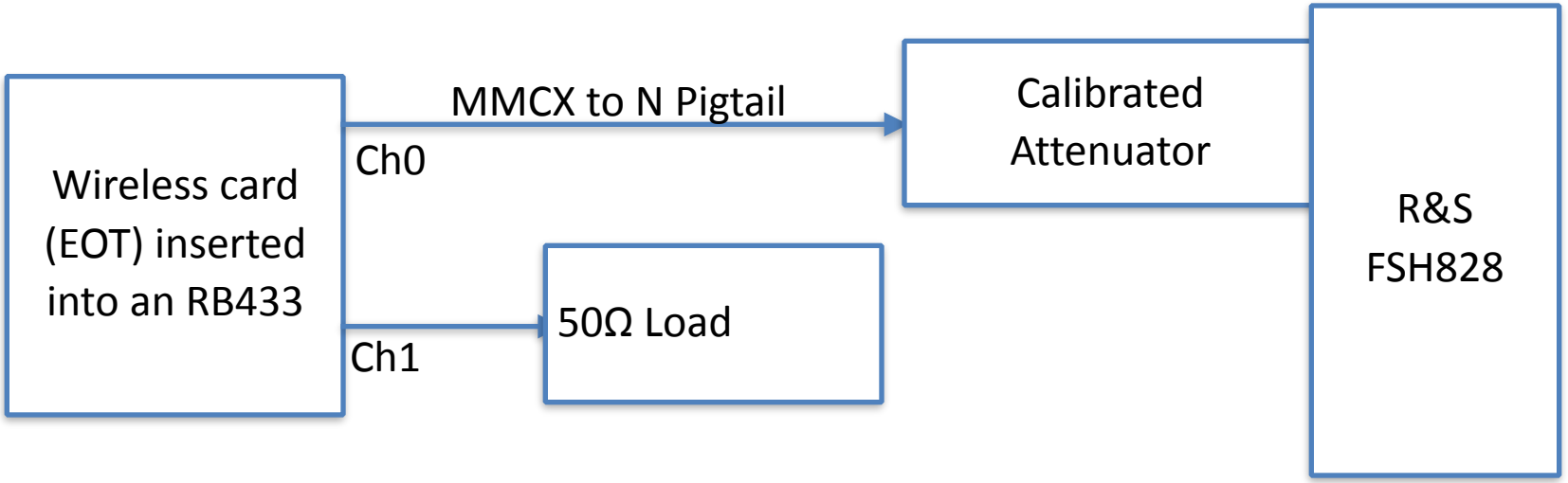
- FSH828 - R&S states in their technical data:

95 % confidence level, +20 °C to +30 °C, SNR > 16 dB, 0 dB to –50 dB below reference level, RF attenuation auto	
10 MHz ≤ f ≤ 3.6 GHz	< 1 dB, typ. 0.5 dB
3.6 GHz < f ≤ 20 GHz	< 1.5 dB, typ. 1 dB

- At 2.4GHz, it is <1 dB, typically 0.5 dB
- At 5GHz, it is <1.5 dB, typically 1 dB

- Therefore anything recorded with a greater accuracy than above, is not valid!

Measurement Method

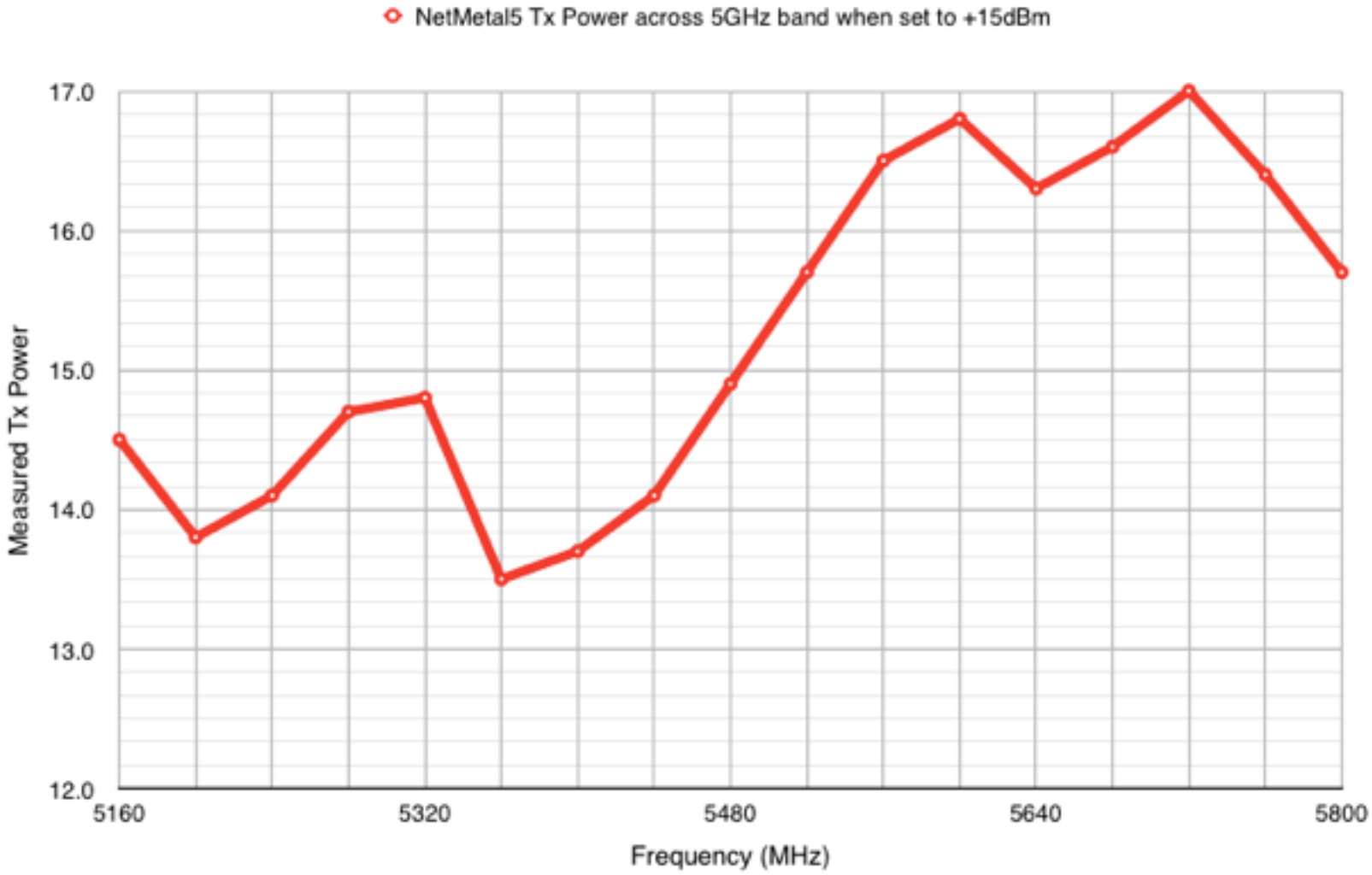


Typical Result across 2.4GHz band for +10dBm

Frequency	RouterOS Tx	Measured Tx	Error
2412 MHz	+10 dBm	+11 dBm	+1dB ✓
2437 MHz	+10 dBm	+11 dBm	+1dB ✓
2462 MHz	+10 dBm	+11 dBm	+1db ✓

- R52Hn running 802.11bg mode, beacons only, RouterOS v6.22, RouterBoot v3.18, wireless package (not wireless-fp)

+15dBm on 5GHz = +/-2dB



Various Tx-Power settings

Frequency	RouterOS Tx	Measured Tx	Error
2437 MHz	+5 dBm	+4.5 dBm	-0.5 dB ✓
2437 MHz	+10 dBm	+11 dBm	+1 dB ✓
2437 MHz	+15 dBm	+16 dBm	+1 db ✓
2437 MHz	+20 dBm	+21.5 dBm	+1.5 db ✓
2437 MHz	+23 dBm	+22.5 dBm	+1.5 dB ✓

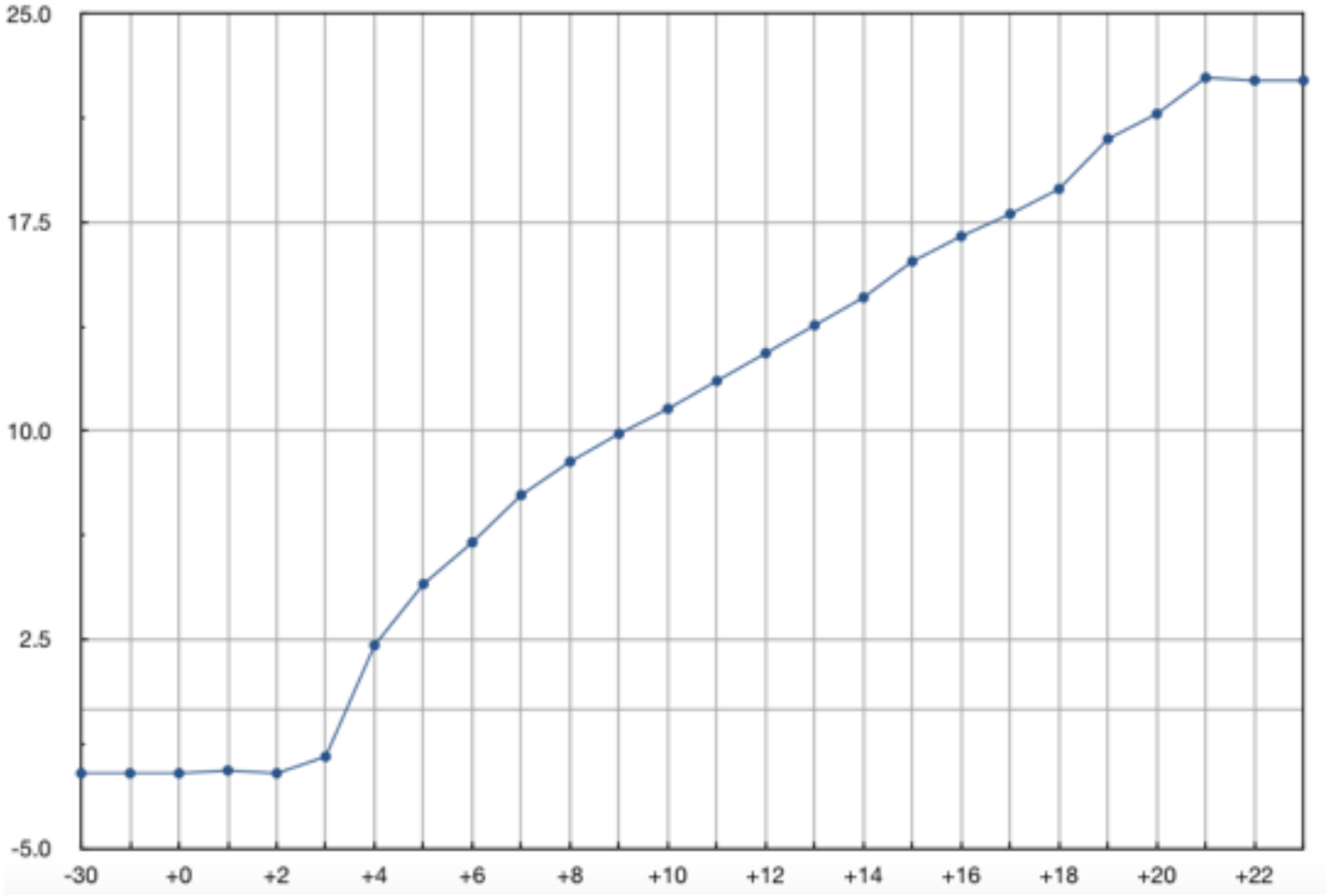
- R52Hn running 802.11bg mode, beacons only, RouterOS v6.22, RouterBoot v3.18, wireless package (not wireless-fp)

Low powers…

Frequency	RouterOS Tx	Measured Tx	Error
2437 MHz	-30 dBm	-2.0 dBm	+ 28.0 dB
2437 MHz	-20 dBm	-2.0 dBm	+ 18.0 dB
2437 MHz	-10 dBm	-2.0 dBm	+ 8.0 dB
2437 MHz	-1 dBm	-2.0 dBm	-1.0 dB
2437 MHz	0 dBm	-2.0 dBm	-2.0 dB
2437 MHz	+1 dBm	-2.0 dBm	-3.0 dB
2437 MHz	+2 dBm	-2.0 dBm	-4.0 dB
2437 MHz	+3 dBm	-1.5 dBm	-4.5 dB
2437 MHz	+4 dBm	+2.0 dBm	-2.0 dB

- R52Hn running 802.11bg mode, beacons only, RouterOS v6.22, RouterBoot v3.18, wireless package (not wireless-fp)

Is this “linear”?



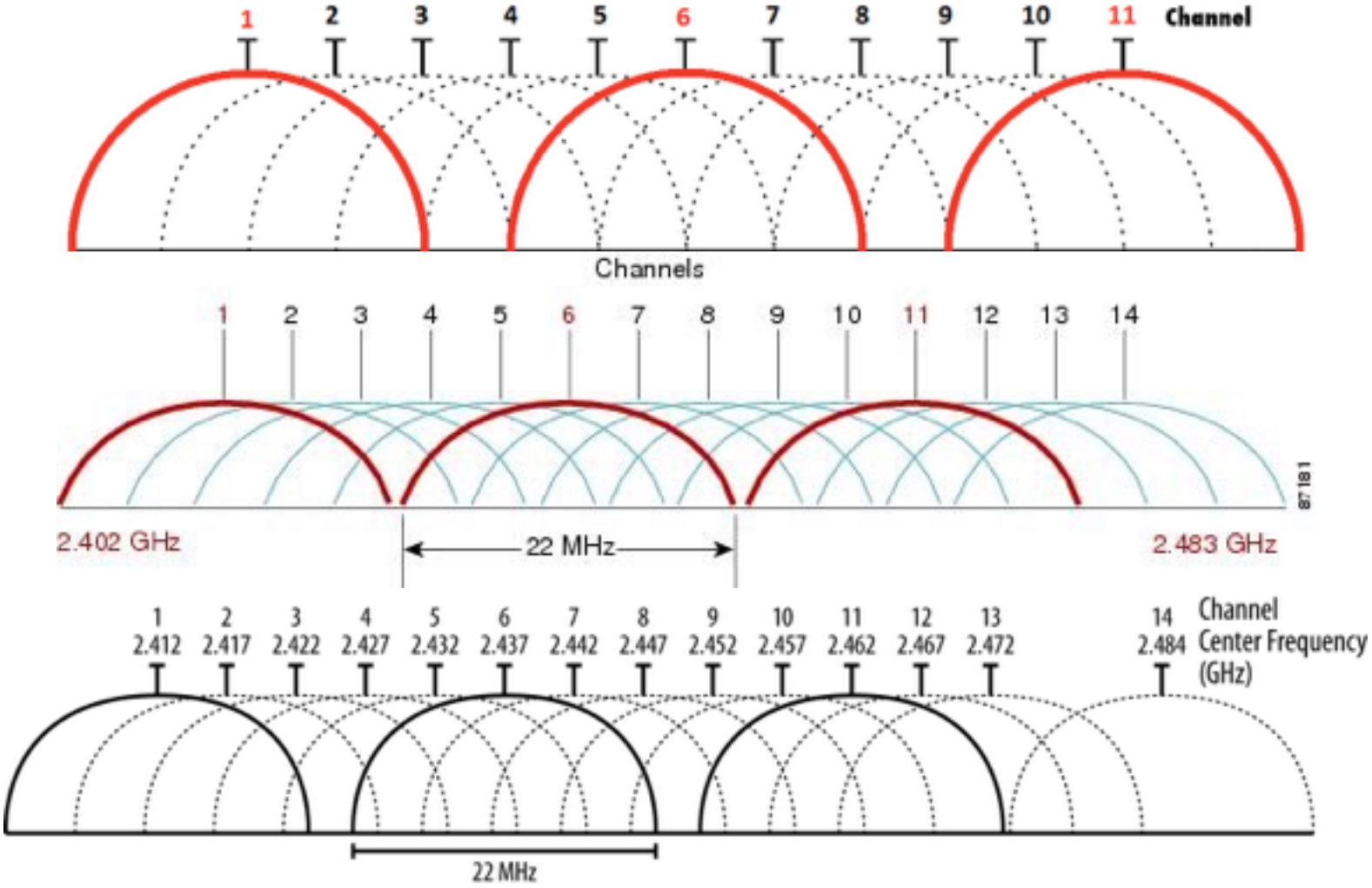
Spectrum Occupancy

- We have seen that although they do not appear to be truly linear, the devices are within the manufacturer's tolerance levels (+/-2dB)
- But - what did you expect for $40-$60?!
- So, if Tx powers are not always what you thought you would get…
- How about the spectrum occupied?

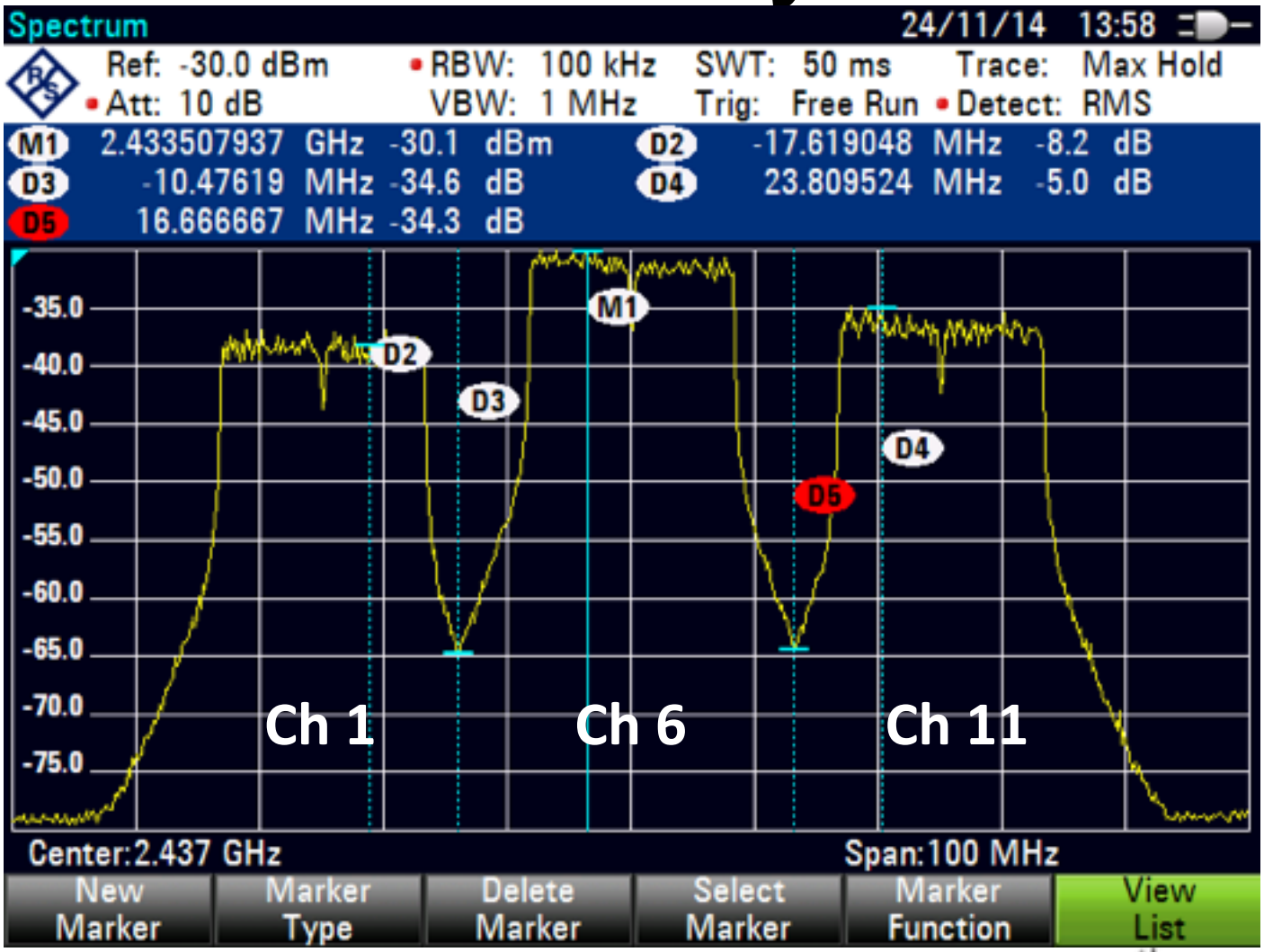
True or False?

- On 2.4GHz, there are three non-overlapping 20MHz channels, 1, 6 and 11.
- When deploying Access Points in a building, one should always use a channel layout using only 1, 6 and 11.
- Co-locating APs on Channels 1,6 and 11 do not interfere with each other

Seen these diagrams?



Reality


Spectrum
24/11/14 13:58
Ref: -30.0 dBm
RBW: 100 kHz
SWT: 50 ms
Trace: Max Hold
Att: 10 dB
VBW: 1 MHz
Trig: Free Run
Detect: RMS
M1 2.433507937 GHz -30.1 dBm
D2 -17.619048 MHz -8.2 dB
D3 -10.47619 MHz -34.6 dB
D4 23.809524 MHz -5.0 dB
D5 16.666667 MHz -34.3 dB
-35.0
-40.0
-45.0
-50.0
-55.0
-60.0
-65.0
-70.0
-75.0
M1
D2
D3
D4
D5
Ch 1
Ch 6
Ch 11
Center:2.437 GHz
Span:100 MHz
New Marker
Marker Type
Delete Marker
Select Marker
Marker Function
View List

Non-overlapping?

- Reality is that energy of WiFi signals actually extends further away from centre frequency than you may think
- Co-locating adjacent 20/40M channels on 5GHz also have the same problem
- Separate by at least 20MHz of free spectrum
- E.g. 5500 Upper = 5490-5530, therefore next channel should be on 5560 Upper, not 5540 Upper

How about Pigtail losses?

- Short high quality pigtails between a radio and antenna have minimal loss but it is not the **same** loss across the whole 5GHz band due to resonances in the cable (E.g. +/-1dB)

Need for Accuracy?

- When calculating EiRP for regulatory authorities - how accurate should you be?
- As we have seen, the card maybe +/-2 dB and the pigtail may be +/-1dB and then there is the antenna gain - this may be different at different frequencies too!
- So .. try not to work too hard to calculate the exact dBm power level. It will only be a calculated “guess” :)

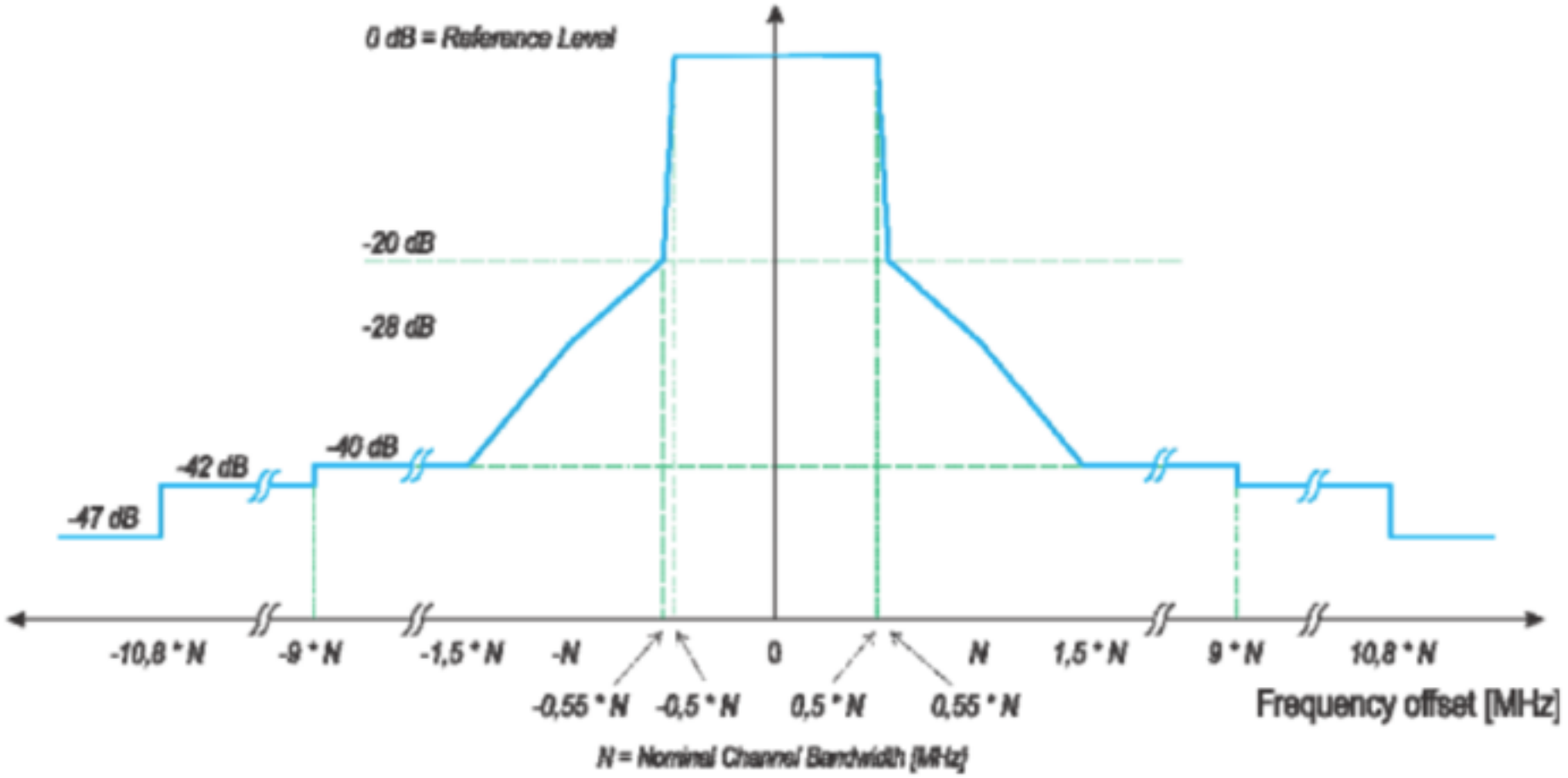
“I need more power!”

- It is not wise to set everything to the maximum power possible for the card.
- Use ‘default’ Tx Power mode, Regulatory settings and input antenna gain figure or set to ‘all-rates-fixed’ and input a reduced power value.

“all-rates-fixed”

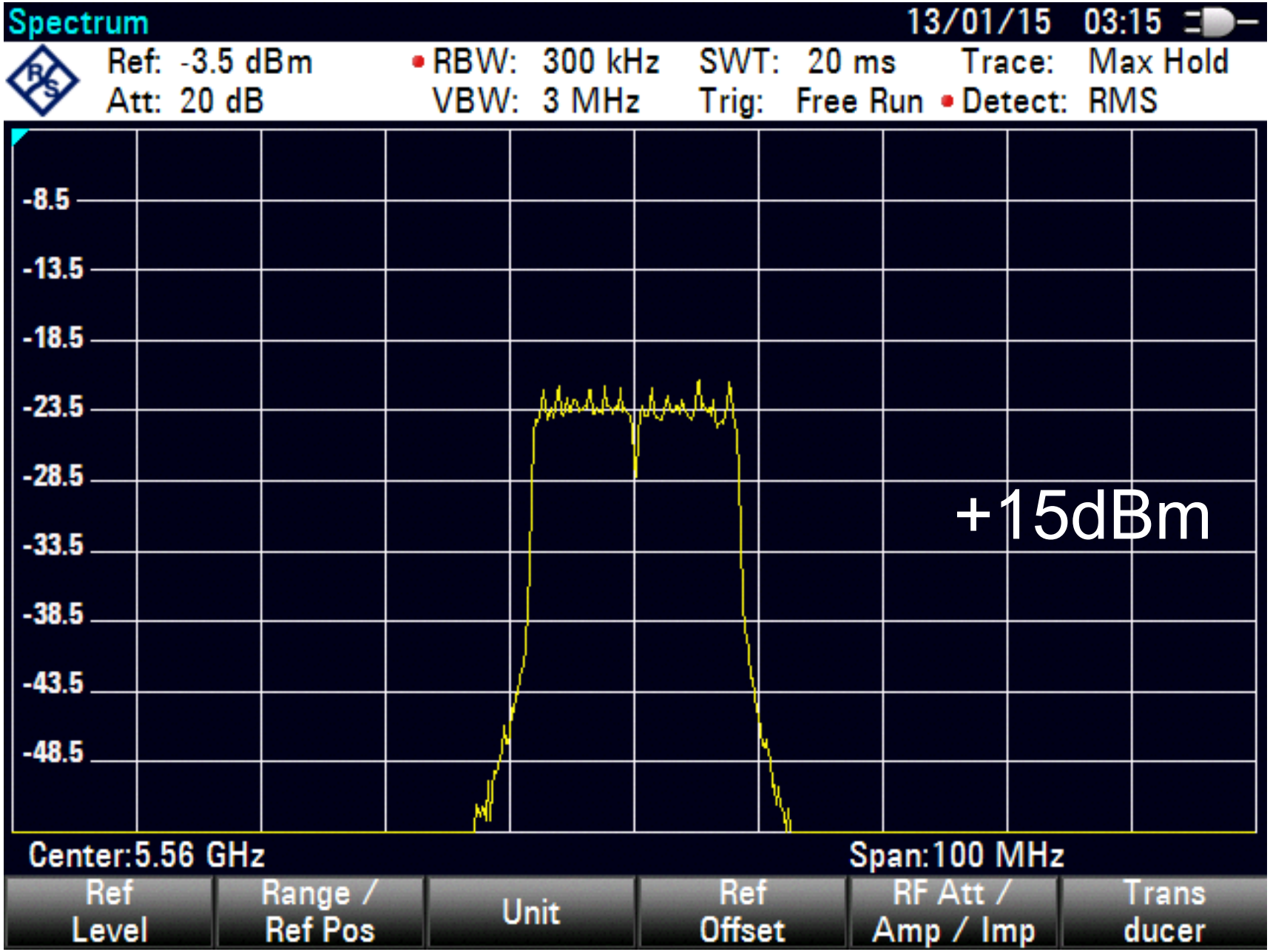
- From Wiki:
  - *“Note that it is not recommended to use 'all-rates-fixed' mode as the wireless card tx-power for the higher data rates is lower…”*
- Meaning = To ensure ETSI Compliance by keeping the spectrum within the regulatory spectral mask, the higher data rates usually have the Tx-Power automatically lowered, but by using ‘all-rates-fixed’ you are overriding this!

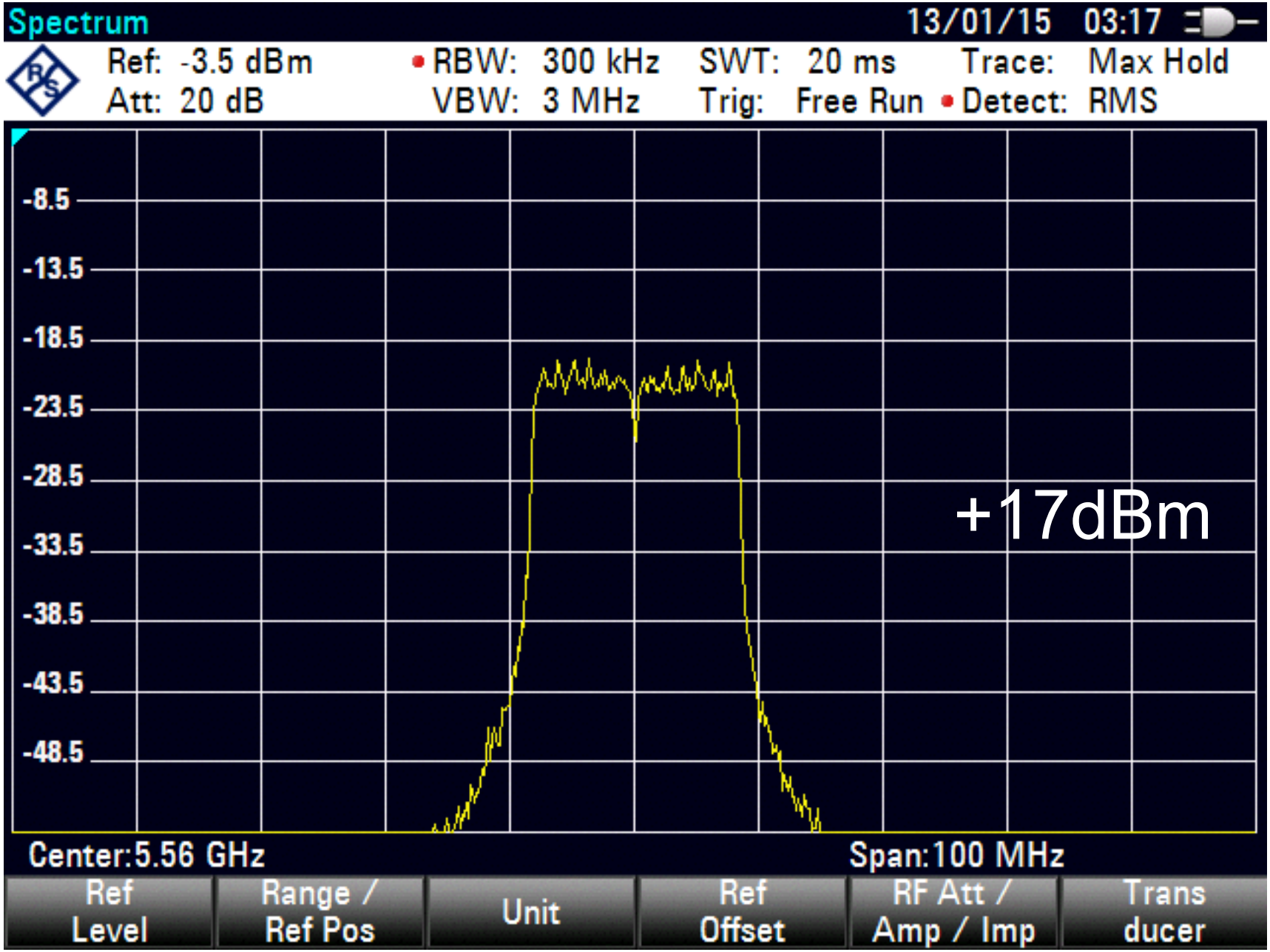
ETSI Spectral Mask

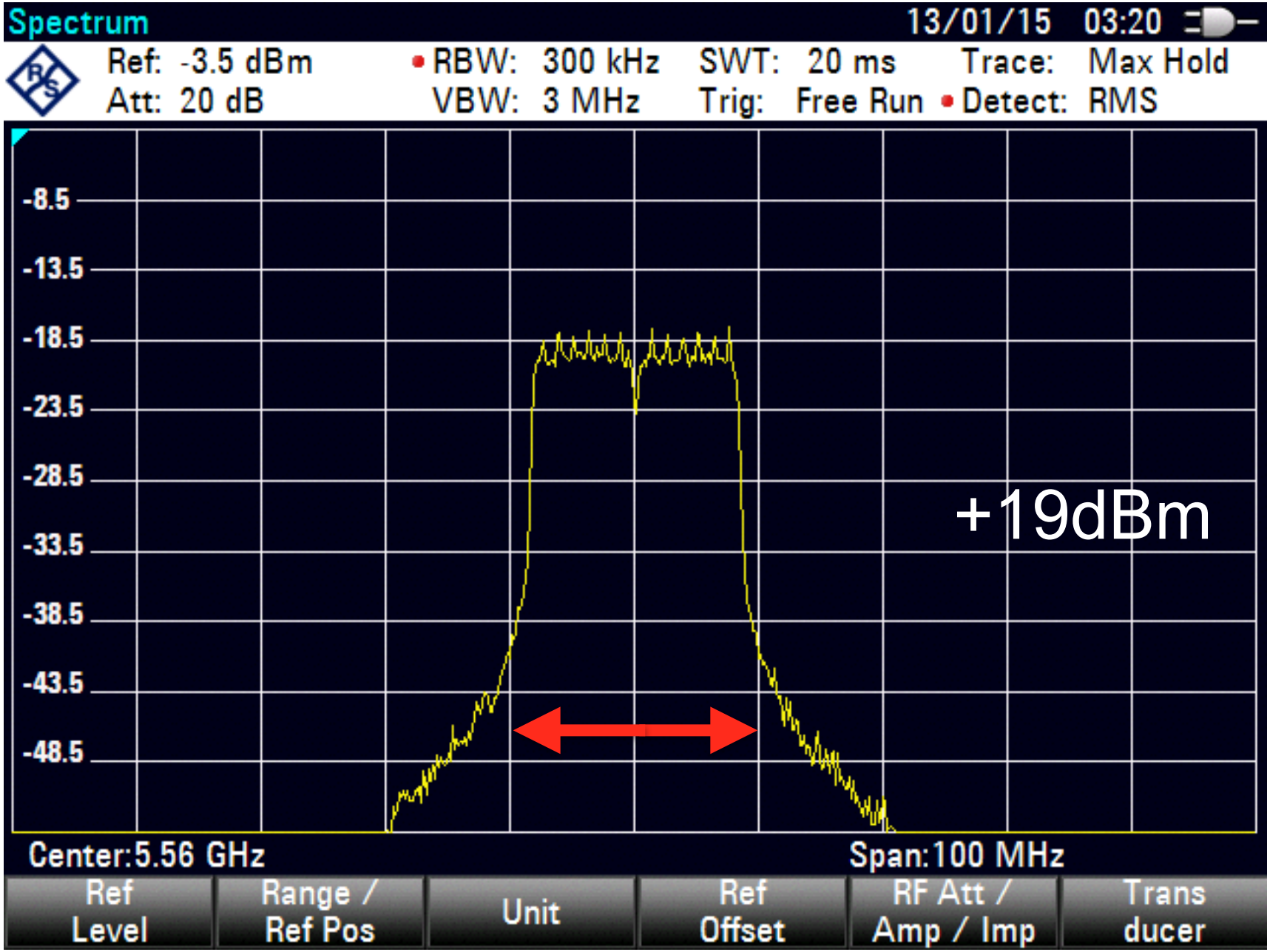


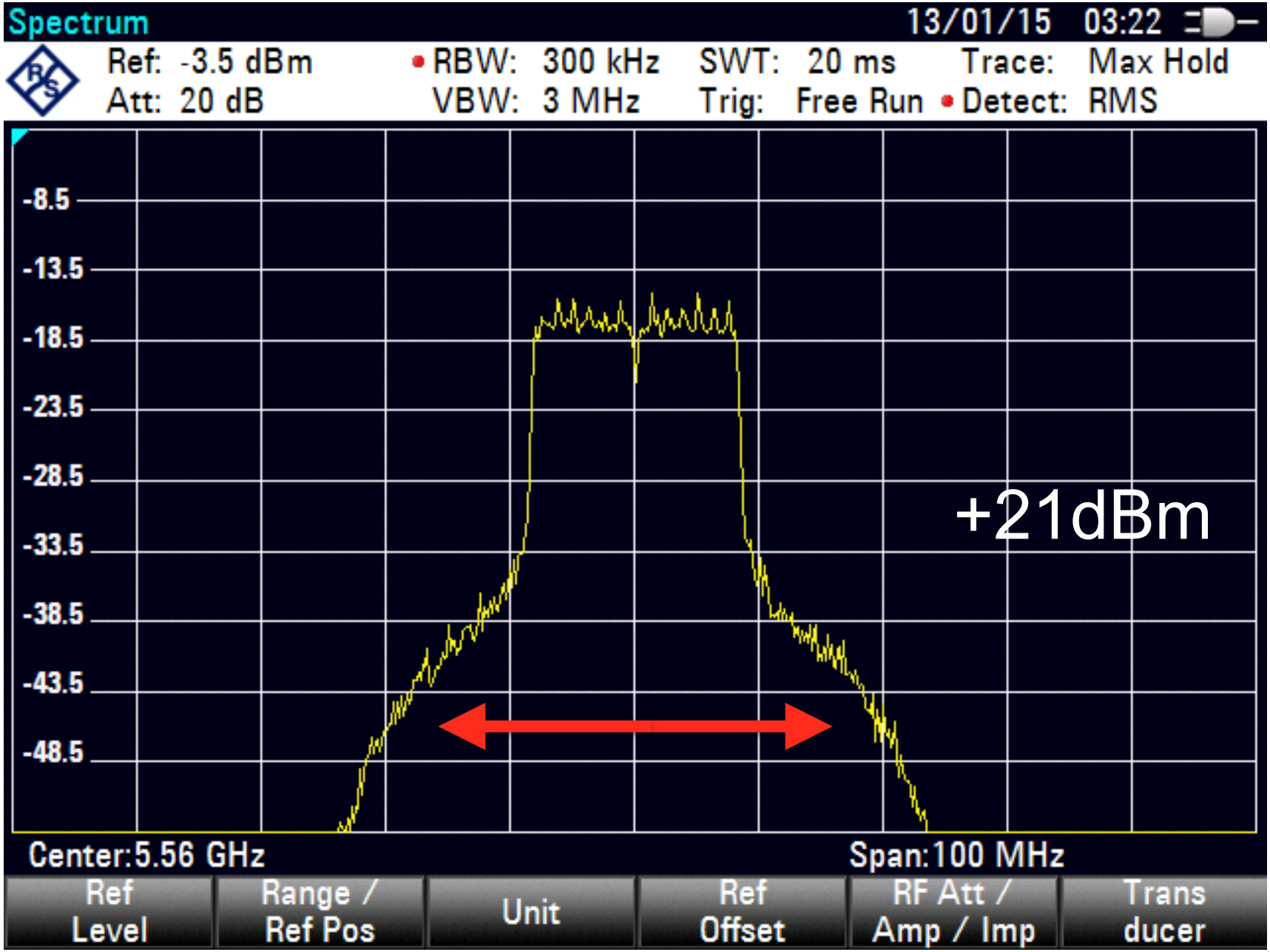
So - what happens?

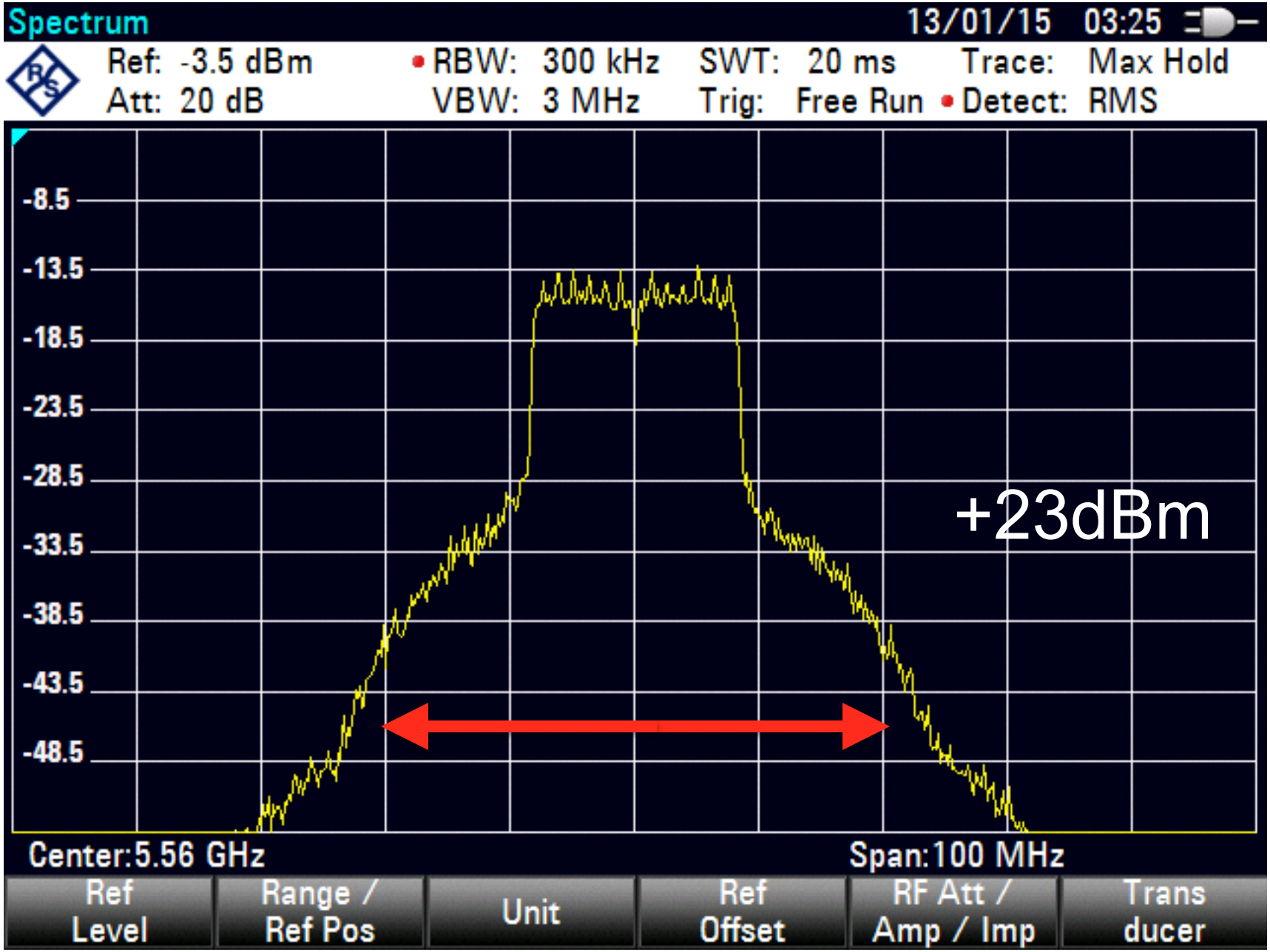
- E.g. Increasing the Tx-Power setting on a R52nM Card by 2dB steps, while leaving the Tx-Power Mode on “all-rates-fixed” instead of ‘default’ (and using ‘antenna gain’ value to reduce power if necessary)


Spectrum
13/01/15 03:15
Ref: -3.5 dBm
Att: 20 dB
RBW: 300 kHz
VBW: 3 MHz
SWT: 20 ms
Trig: Free Run
Trace: Max Hold
Detect: RMS
-8.5
-13.5
-18.5
-23.5
-28.5
-33.5
-38.5
-43.5
-48.5
+15dBm
Center:5.56 GHz
Span:100 MHz
Ref Level
Range / Ref Pos
Unit
Ref Offset
RF Att / Amp / Imp
Trans ducer


Spectrum
13/01/15 03:17
Ref: -3.5 dBm
Att: 20 dB
RBW: 300 kHz
VBW: 3 MHz
SWT: 20 ms
Trig: Free Run
Trace: Max Hold
Detect: RMS
-8.5
-13.5
-18.5
-23.5
-28.5
-33.5
-38.5
-43.5
-48.5
+17dBm
Center:5.56 GHz
Span:100 MHz
Ref Level
Range / Ref Pos
Unit
Ref Offset
RF Att / Amp / Imp
Trans ducer


Spectrum
13/01/15 03:20
Ref: -3.5 dBm
Att: 20 dB
RBW: 300 kHz
VBW: 3 MHz
SWT: 20 ms
Trig: Free Run
Trace: Max Hold
Detect: RMS
-8.5
-13.5
-18.5
-23.5
-28.5
-33.5
-38.5
-43.5
-48.5
+19dBm
Center:5.56 GHz
Span:100 MHz
Ref Level
Range / Ref Pos
Unit
Ref Offset
RF Att / Amp / Imp
Trans ducer


Spectrum
13/01/15 03:22
Ref: -3.5 dBm
RBW: 300 kHz
SWT: 20 ms
Trace: Max Hold
Att: 20 dB
VBW: 3 MHz
Trig: Free Run
Detect: RMS
-8.5
-13.5
-18.5
-23.5
-28.5
-33.5
-38.5
-43.5
-48.5
+21dBm
Center:5.56 GHz
Span:100 MHz
Ref Level
Range / Ref Pos
Unit
Ref Offset
RF Att / Amp / Imp
Trans ducer


Spectrum
13/01/15 03:25
Ref: -3.5 dBm
Att: 20 dB
RBW: 300 kHz
VBW: 3 MHz
SWT: 20 ms
Trig: Free Run
Trace: Max Hold
Detect: RMS
-8.5
-13.5
-18.5
-23.5
-28.5
-33.5
-38.5
-43.5
-48.5
+23dBm
Center:5.56 GHz
Span:100 MHz
Ref Level
Range / Ref Pos
Unit
Ref Offset
RF Att / Amp / Imp
Trans ducer

MTCWE?

- Why not join us for MTCWE training and learn more about MikroTik and Wireless configuration?
- Special discount if you speak with me today :)
- See www.mikrotik.com/training …

- March 30-April 01, Czech Republic, MUM Prague, LinITX (MTCWE), English

Now you see that you do not always get what you wanted!

Thank You.

By Ron Touw
LinITX, England

Contact Details

Ron Touw – MikroTik Trainer & Consultant
LinITX
Tel: +44 1449 724250
VOIP: sip:contact@linitx.com
IRC: irc.z.je #routerboard
Email: shop@linitx.com
WWW: http://linitx.com

Materials Copyright

- Ron Touw of LinITX hereby acknowledges that some of the material contained within this presentation contains copyrighted images and descriptive text belonging to Mikrotīkls SIA and others.