WIRELESS & NETWORKING EXPERTS

How to get WiFi to my Shed?

How to Get WiFi to my Shed?

Run a Cable


UTP
NONE
LOW
TENSION
HIGH
CABLE REEL CONTROL
Cable Professional

Thank you for Listening

WIRELESS & NETWORKING EXPERTS

How to get WiFi to my Shed?

Jono Thompson

- Networking background started as a Cisco Engineer
- 24 years working in enterprise networking and data centres.
- MikroTik Consultant Since Dec 2014
- MikroTik Trainer since March 2017
- Ubiquiti Trainer since March 2019
- Certifications from other vendors.

Lin ITX
WIRELESS & NETWORKING EXPERTS

PRODUCTS | TRAINING | CONSULTANCY

ABOUT US:

- Technical sales team
- Professional support
- Extended warranties
- Trade accounts
- Credit accounts
- Live stock levels
- Trusted seller
- Training provider
- Next day delivery

WHAT WE OFFER:

- Wireless & networking products online
- MikroTik, Ubiquiti & TP-Link training
- Wireless & network consultancy

BRANDS WE STOCK

UBIQUITI · MIKROTIK · Hewlett Packard Enterprise · Omada by tp-link · Aginet · tp-link · ALTA LABS · TELTONIKA · Tachyon Networks · RF ELEMENTS

Linitx.com | 01449 888000 | shop@linitx.com

VIRAL VPS

REFURBISH. REPURPOSE.

HIGH QUALITY REFURBISHED EQUIPMENT

ABOUT US:

- High quality refurbishment
- Sustainability efforts
- Cost savings
- Knowledge base
- Prolong existing hardware
- Repair rather than replace
- Cheaper Alternatives
- Equipment upgrades

WHAT WE OFFER:

We specialise in providing IT hardware supply services, focusing on enterprise networking, storage solutions including disk arrays and tape libraries, as well as data wiping and drive testing. Our expertise spans across various industries, serving universities, councils, and large multinational organisations with worldwide sales.

viralvps.com | 01449 888003 | sales@viralvps.com

How to Get WiFi to my Shed?
&
Wireless Point to Point Links

Objectives

- Possible ways to extend Network to another building
- Common Mistakes people make
- Why wireless bridges don’t work
- Some design considerations for wireless point to point links

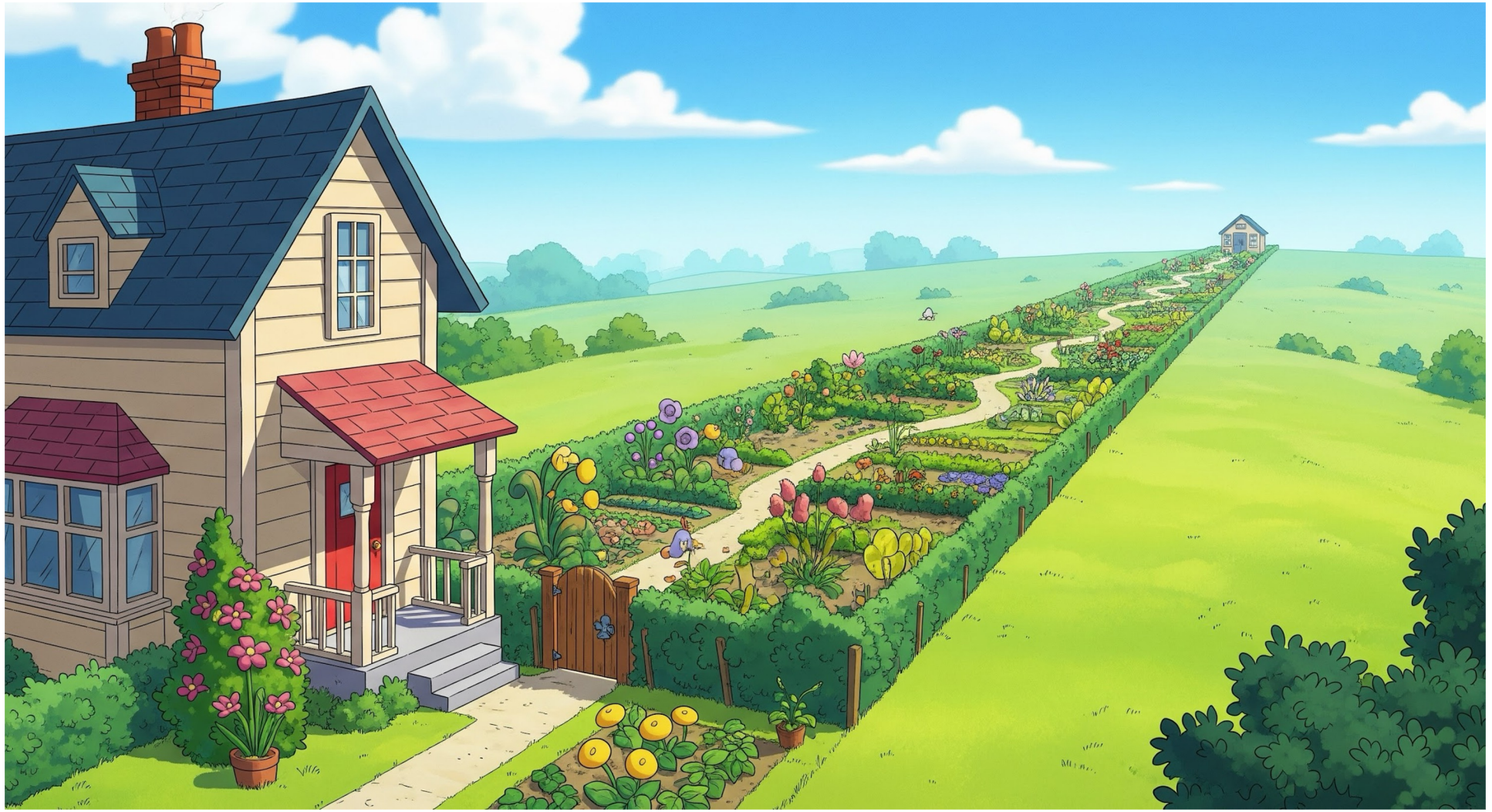
Run a Cable

It may not always be possible for lots of reasons….

Building gets up and moves about

Need to cross a road….

Long Distance



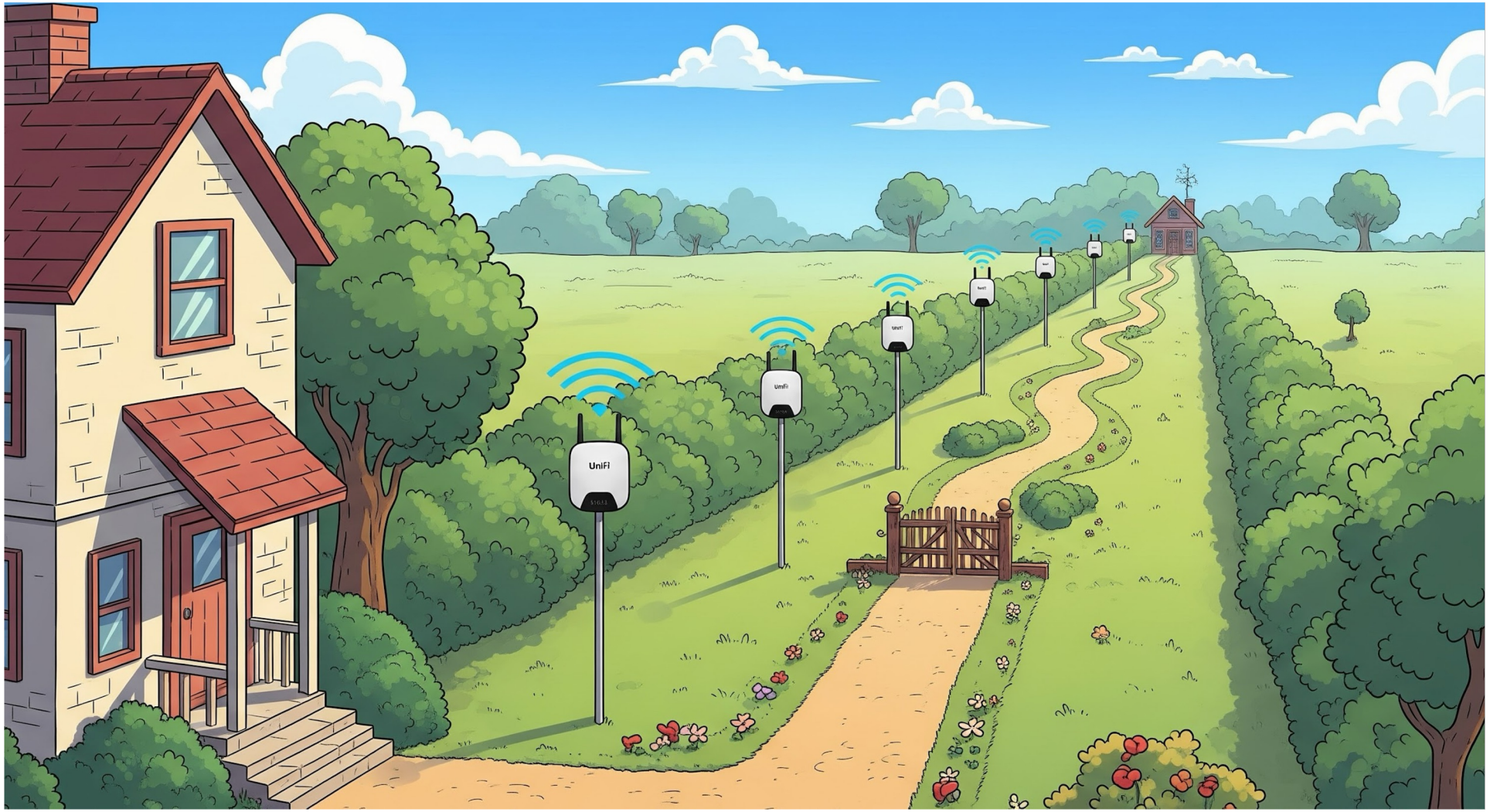
Wireless Options

- Mesh
- Outdoor AP
- Dedicated Wireless Point to Point Link (PtP)

Mesh AP

- Mesh AP’s min 50% loss of throughput on each hop
- Mesh APs need to be on the same channel - CCI
- Mesh APs often placed at the extremity of the signal this giving 50% throughput of a very poor signal

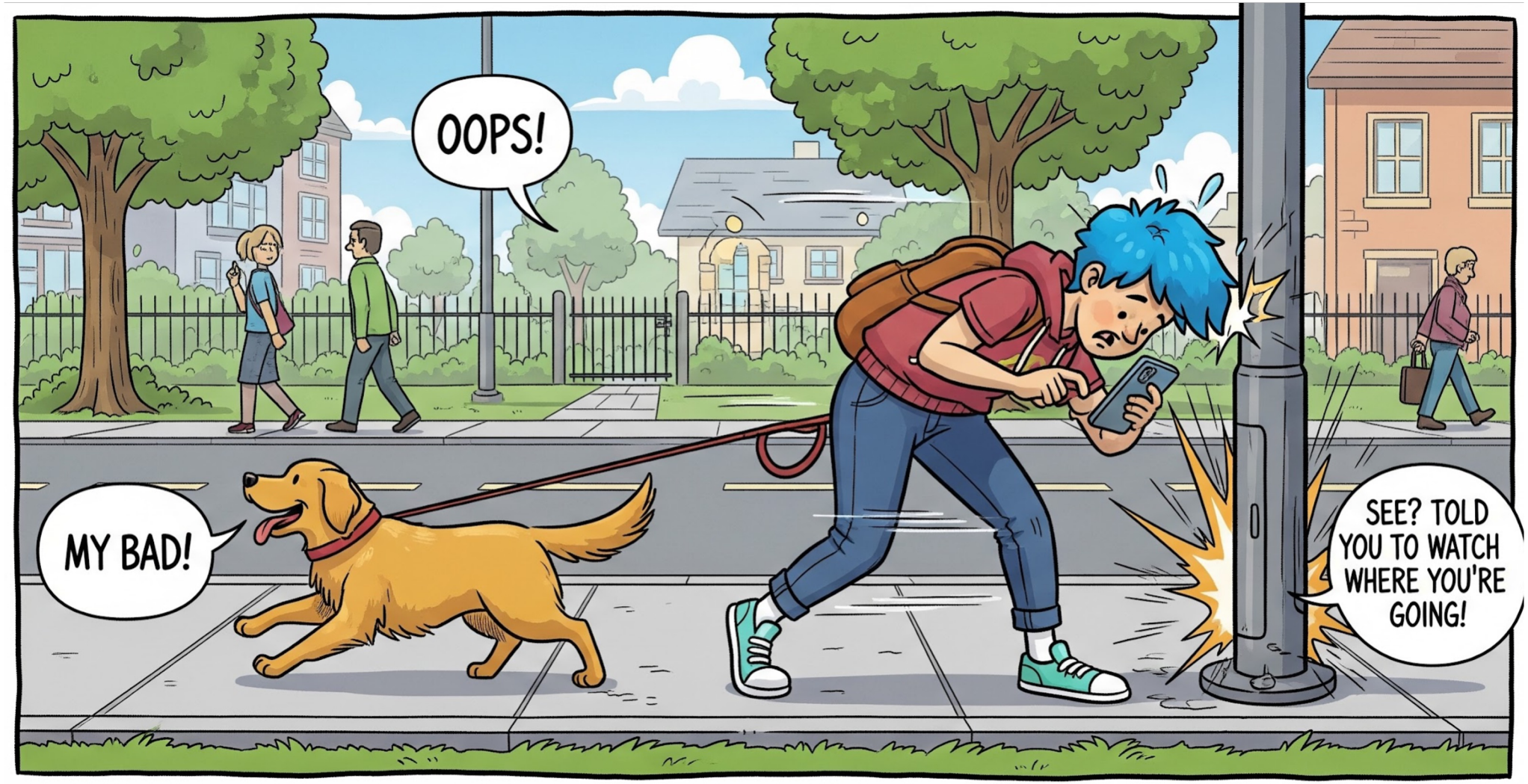
How are you going to power it?



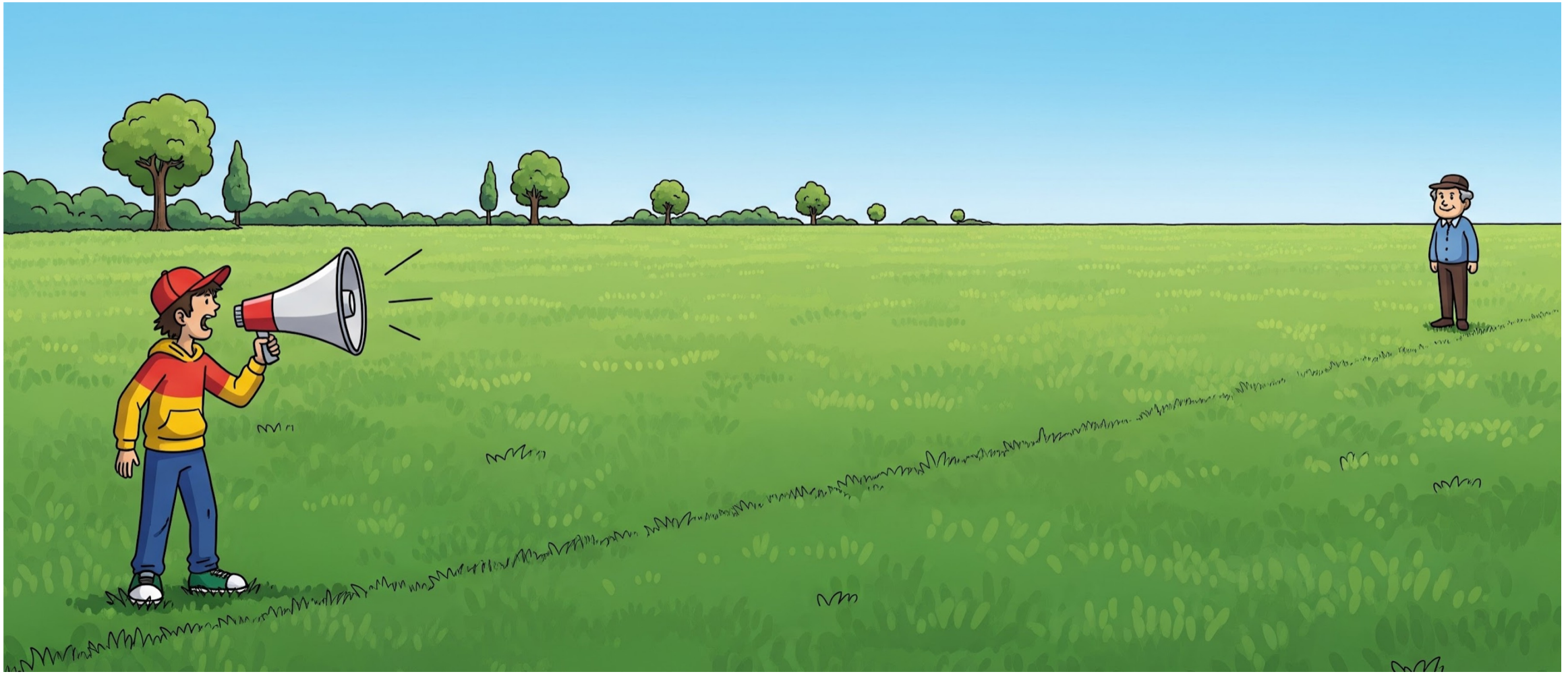
High Power Outdoor Access Point

- Outdoor access point running at full power
- 4W in band C is legal with a licence
- Client might have full signal strength on device but no access

Outdoor WiFi Coverage



AP / Client TX/RX power mismatch



High Power Outdoor Access Point

- Potentially full signal on client device
- WiFi doesn’t work!

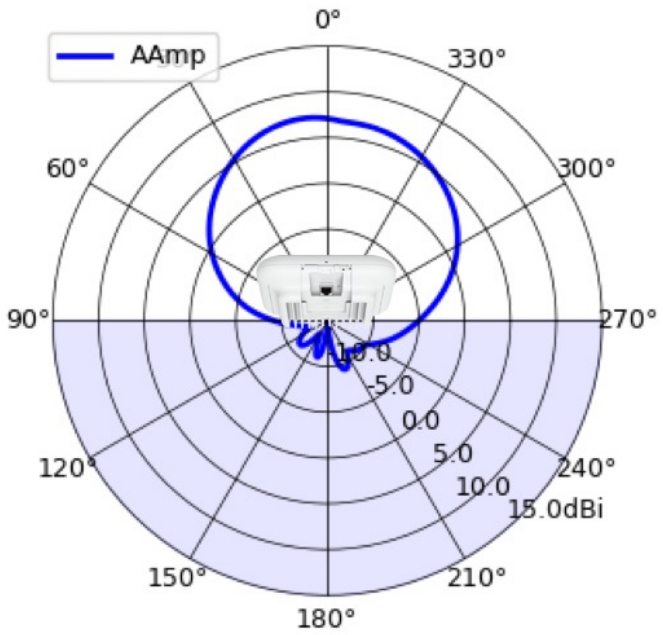
Outdoor Access Point

- Some vendor outdoor AP's have directional antennas which have increased gain which may increase performance
- Attenuation of building materials

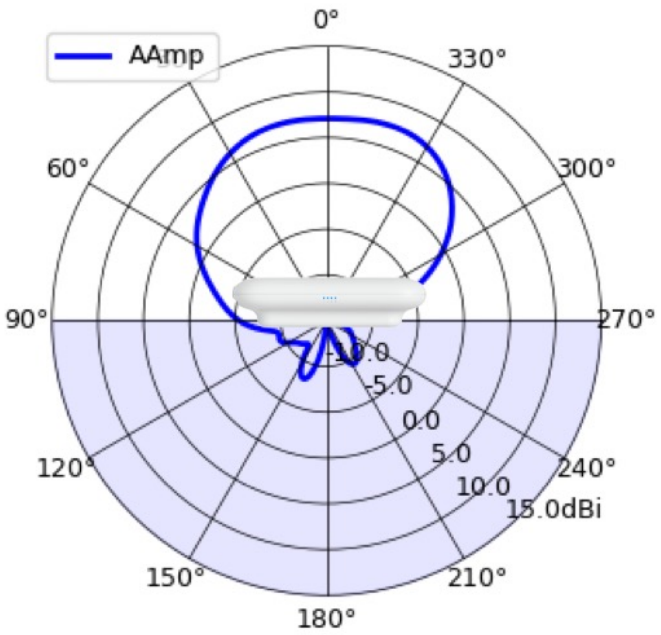
Outdoor Directional AP - UniFi U7 Outdoor

2.450GHz

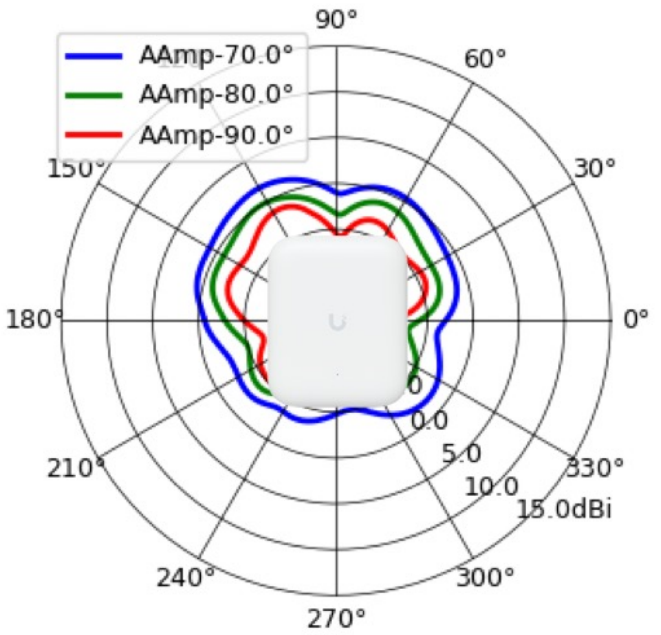
Elevation - 0.0°



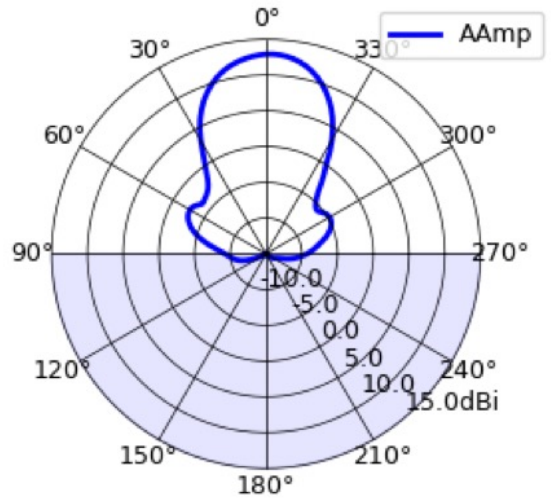
Elevation - 90.0°

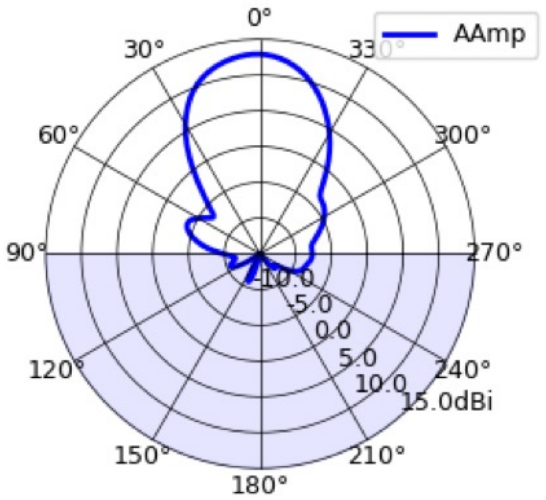


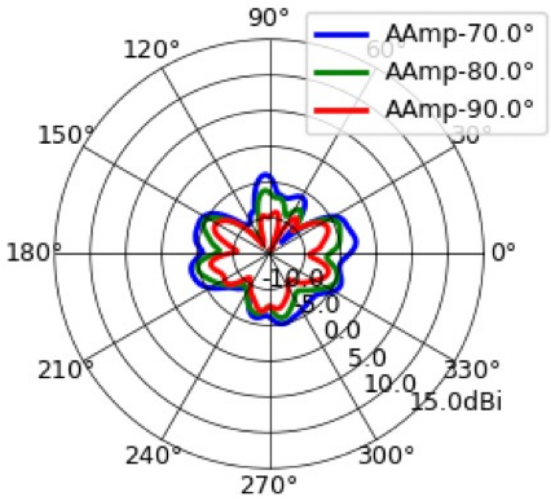
Azimuth



5.150GHz







Antenna’s improve both TX and rX

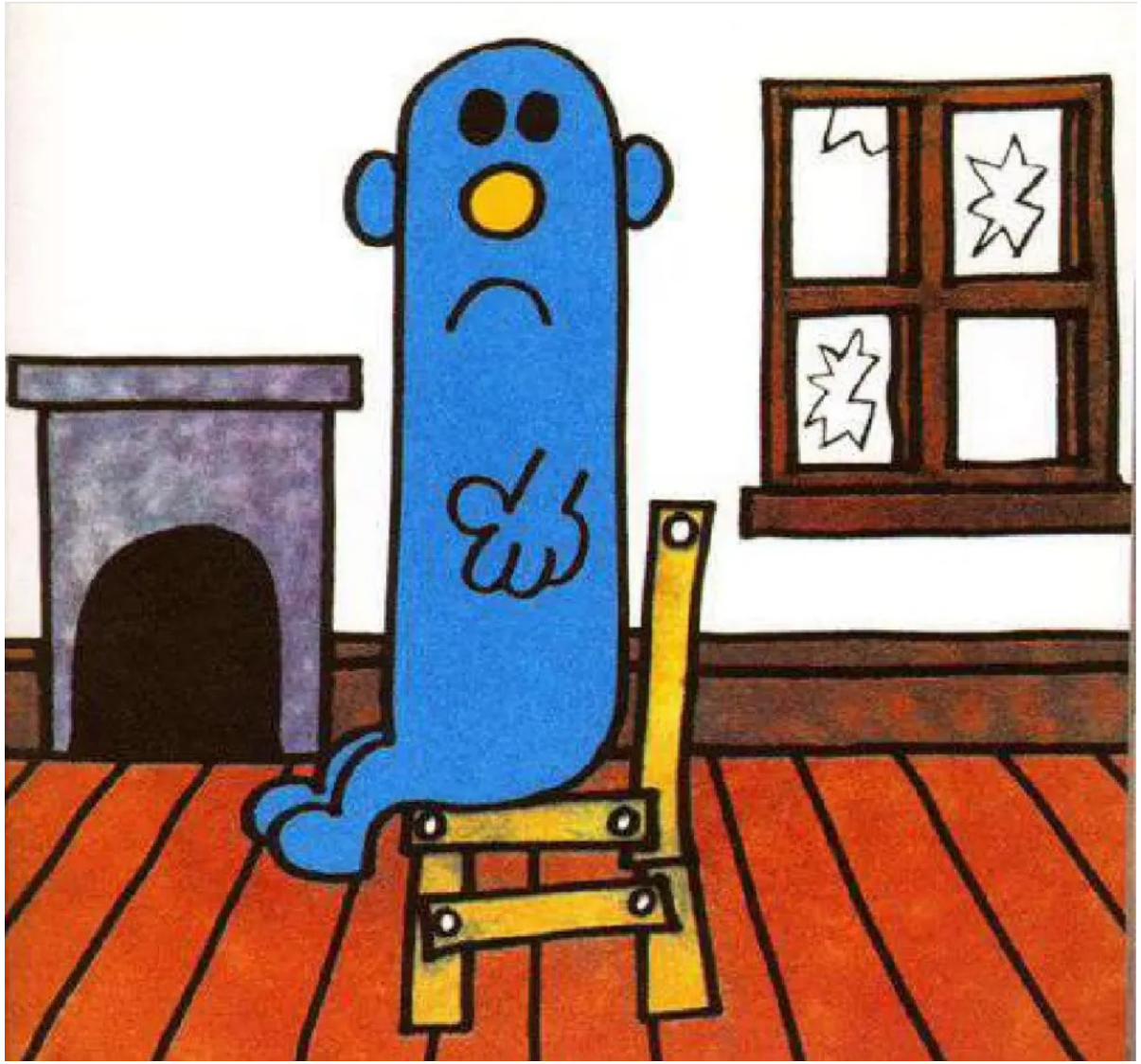
Point to Point Links

- Dedicated Radio for the link, not shared with clients
- Doesn’t need to be on same channel as clients
- Range of antennas reduces interference
- High gain options

Point to Point Links

- Some vendors offer property TDMA protocols which make more efficient use of airtime over CSMA/CA so 802.11 devices are unable to connect
- Some vendors offer proprietary chipsets for improved performance
- These can not be used as an 802.11 access point

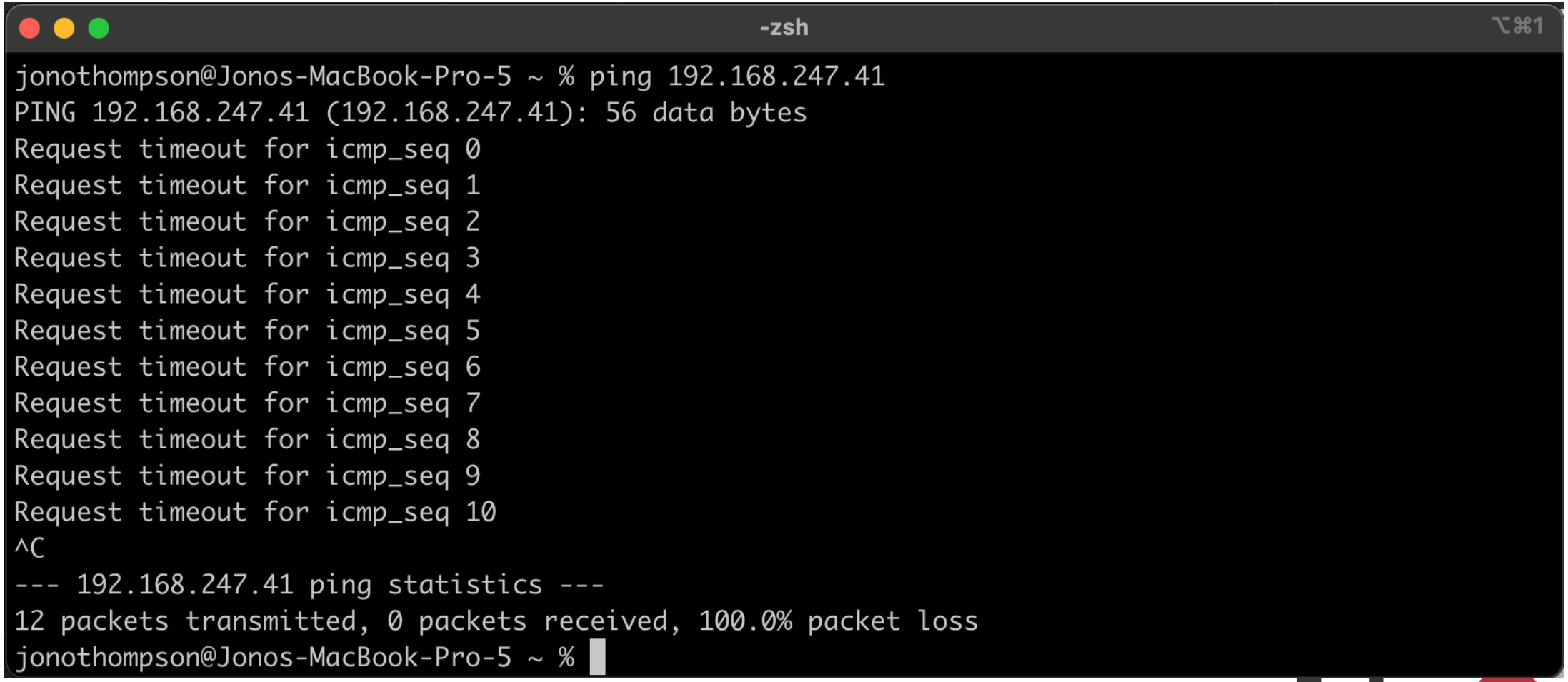
The Cheep Option



The DIY Option

The DIY Option

- Does not work.



Wireless Bridges

- 802.3 standard simply specifies that frames have two mac address
  - Source mac address
  - Destination mac address

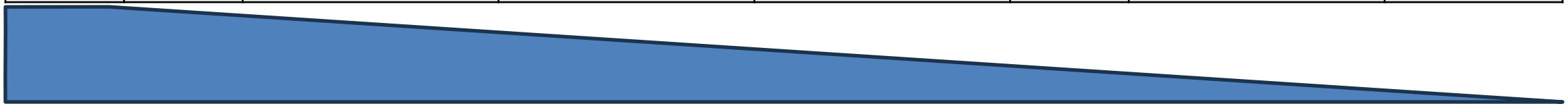
Wireless Bridges

- 802.11 standard specifies that frames between station and AP device must be transmitted in so called *3 address* frame format, meaning that header of frame contains 3 MAC addresses.

Frame Control	Duration ID	Address 1 (Receiver)	Address 2 (Sender)	Address 3 (Filtering)	seq-ctl	Address 4 (Optional)	Frame body

Wireless Bridges

Frame Control	Duration ID	Address 1 (Receiver)	Address 2 (Sender)	Address 3 (Filtering)	seq-ctl	Address 4 (Optional)	Frame body



Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Man	More Data	Protocol Frame	HTC Other

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Dst Address	Src Address	AP Address	N / A
0	1	Dst Address	Transmitter Address	Src Address	N / A
1	0	Receiver Address	Src Address	Dst Address	N / A
1	1	Receiver Address	Transmitter Address	Dst Address	Src Address

To the DS

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	1	Dst Address	Transmitter Address	Src Address	N/A
1	0	Receiver Address	Src Address	Dst Address	N/A

Address 2 Src MAC Address

74:D8:3E:EA:22:07
192.168.247.35

Address 1 Receiver MAC Address

48:A9:8A:64:EB:7F
192.168.247.34

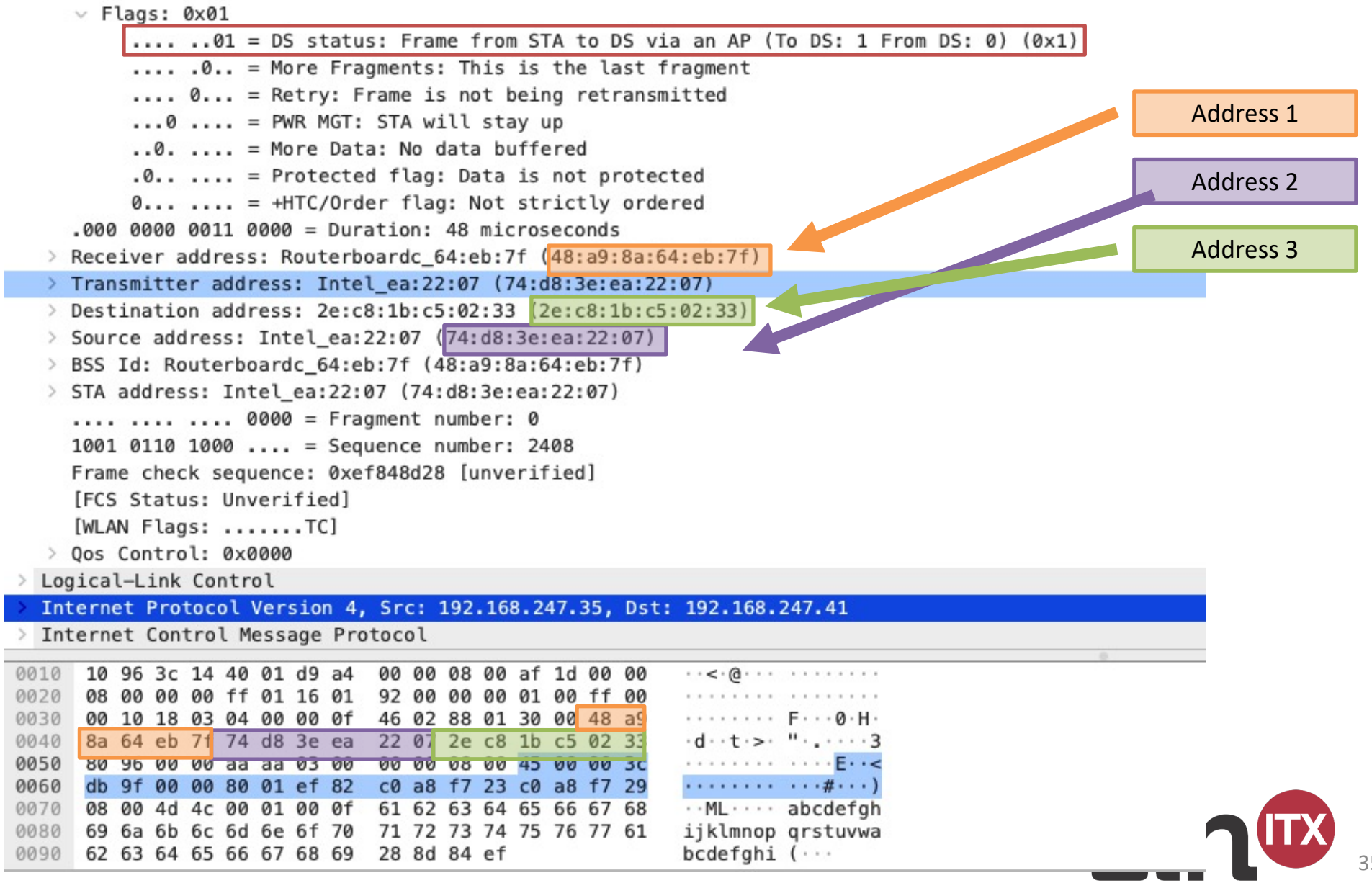
Address 3 Dst MAC Address

2E:C8:1B:C5:02:34
192.168.247.41

To the DS

- This additional mac address can be seen in the wireless frame in wireshark

To the DS


Flags: 0x01
.... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
.0.. .... = Protected flag: Data is not protected
0... .... = +HTC/Order flag: Not strictly ordered
.000 0000 0011 0000 = Duration: 48 microseconds
Receiver address: Routerboardc_64:eb:7f (48:a9:8a:64:eb:7f)
Transmitter address: Intel_ea:22:07 (74:d8:3e:ea:22:07)
Destination address: 2e:c8:1b:c5:02:33 (2e:c8:1b:c5:02:33)
Source address: Intel_ea:22:07 (74:d8:3e:ea:22:07)
BSS Id: Routerboardc_64:eb:7f (48:a9:8a:64:eb:7f)
STA address: Intel_ea:22:07 (74:d8:3e:ea:22:07)
.... 0000 = Fragment number: 0
1001 0110 1000 .... = Sequence number: 2408
Frame check sequence: 0xef848d28 [unverified]
[FCS Status: Unverified]
[WLAN Flags: ....TC]
Qos Control: 0x0000
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.247.35, Dst: 192.168.247.41
Internet Control Message Protocol
0010 10 96 3c 14 40 01 d9 a4 00 00 08 00 af 1d 00 00
0020 08 00 00 00 ff 01 16 01 92 00 00 00 01 00 ff 00
0030 00 10 18 03 04 00 00 0f 46 02 88 01 30 00 48 a9
0040 8a 64 eb 7f 74 d8 3e ea 22 07 2e c8 1b c5 02 33
0050 80 96 00 00 aa aa 03 00 00 00 08 00 45 00 00 3c
0060 db 9f 00 00 80 01 ef 82 c0 a8 f7 23 c0 a8 f7 29
0070 08 00 4d 4c 00 01 00 0f 61 62 63 64 65 66 67 68
0080 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61
0090 62 63 64 65 66 67 68 69 28 8d 84 ef
Address 1
Address 2
Address 3

From the DS

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	1	Dst Address	Transmitter Address	Src Address	N/A
1	0	Receiver Address	Src Address	Dst Address	N/A

Adress 3 Src MAC Address

2E:C8:1B:C5:02:34
192.168.247.41

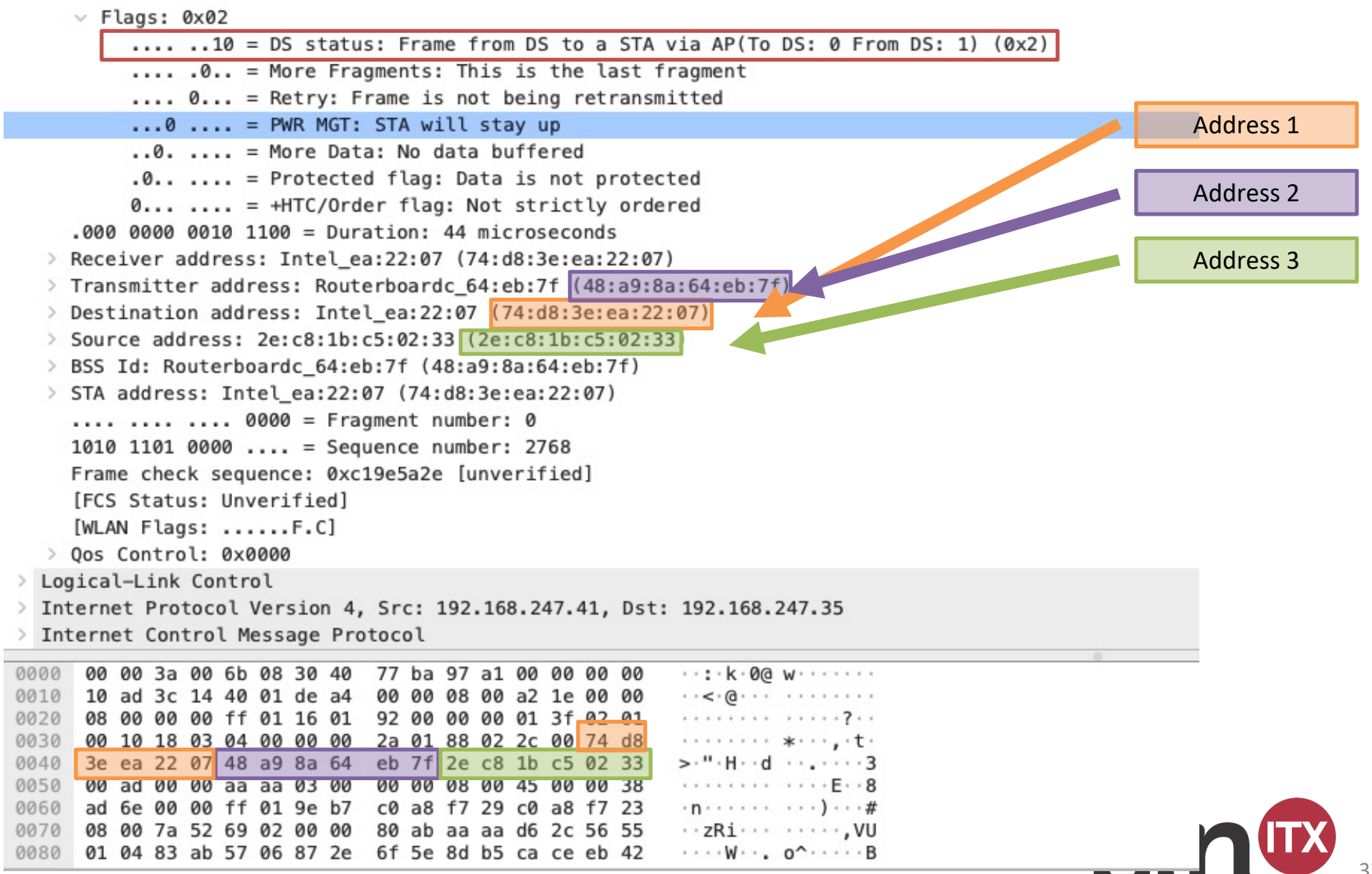
Address 2 Transmitter MAC Address

48:A9:8A:64:EB:7F
192.168.247.34

Address 1 Dst MAC Address

74:D8:3E:EA:22:07
192.168.247.35

From DS


Flags: 0x02
.... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
.0.. .... = Protected flag: Data is not protected
0... .... = +HTC/Order flag: Not strictly ordered
.000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: Intel_ea:22:07 (74:d8:3e:ea:22:07)
Transmitter address: Routerboardc_64:eb:7f (48:a9:8a:64:eb:7f)
Destination address: Intel_ea:22:07 (74:d8:3e:ea:22:07)
Source address: 2e:c8:1b:c5:02:33 (2e:c8:1b:c5:02:33)
BSS Id: Routerboardc_64:eb:7f (48:a9:8a:64:eb:7f)
STA address: Intel_ea:22:07 (74:d8:3e:ea:22:07)
.... 0000 = Fragment number: 0
1010 1101 0000 .... = Sequence number: 2768
Frame check sequence: 0xc19e5a2e [unverified]
[FCS Status: Unverified]
[WLAN Flags: ......F.C]
Qos Control: 0x0000
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.247.41, Dst: 192.168.247.35
Internet Control Message Protocol
0000 00 00 3a 00 6b 08 30 40 77 ba 97 a1 00 00 00 00
0010 10 ad 3c 14 40 01 de a4 00 00 08 00 a2 1e 00 00
0020 08 00 00 00 ff 01 16 01 92 00 00 00 01 3f 02 01
0030 00 10 18 03 04 00 00 00 2a 01 88 02 2c 00 74 d8
0040 3e ea 22 07 48 a9 8a 64 eb 7f 2e c8 1b c5 02 33
0050 00 ad 00 00 aa aa 03 00 00 00 08 00 45 00 00 38
0060 ad 6e 00 00 ff 01 9e b7 c0 a8 f7 29 c0 a8 f7 23
0070 08 00 7a 52 69 02 00 00 80 ab aa aa d6 2c 56 55
0080 01 04 83 ab 57 06 87 2e 6f 5e 8d b5 ca ce eb 42
Address 1
Address 2
Address 3

From the DS or To the DS ?

- Now with a wireless AP and a wireless station creating a bridge between two DS's

From the DS or To the DS ?

- Is this from the Distribution System (DS) ?
- Or
- Is this to the Distribution System (DS)?
- The packet will show….

From the DS or To the DS ?

```
Flags: 0x01
    .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
    .... .0.. = More Fragments: This is the last fragment
    .... 0... = Retry: Frame is not being retransmitted
    ...0 .... = PWR MGT: STA will stay up
    ..0. .... = More Data: No data buffered
    .0.. .... = Protected flag: Data is not protected
    0... .... = +HTC/Order flag: Not strictly ordered
.000 0000 0011 0000 = Duration: 48 microseconds
> Receiver address: Routerboardc_64:eb:7f (48:a9:8a:64:eb:7f)
> Transmitter address: 66:d1:54:a4:60:7e (66:d1:54:a4:60:7e)
> Destination address: 2e:c8:1b:c5:02:33 (2e:c8:1b:c5:02:33)
> Source address: 66:d1:54:a4:60:7e (66:d1:54:a4:60:7e)
> BSS Id: Routerboardc_64:eb:7f (48:a9:8a:64:eb:7f)
> STA address: 66:d1:54:a4:60:7e (66:d1:54:a4:60:7e)
  .... .... .... 0000 = Fragment number: 0
  0000 1100 1010 .... = Sequence number: 202
  Frame check sequence: 0xdedc839e [unverified]
  [FCS Status: Unverified]
  [WLAN Flags: .......TC]
> Qos Control: 0x0000
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.247.40, Dst: 192.168.247.41
> Internet Control Message Protocol
```

```
0000  00 00 3a 00 6b 08 30 40  84 c5 aa 45 00 00 00 00   ··:·k·0@ ···E····
0010  10 0c 3c 14 40 01 d5 a4  00 00 08 00 ad 1a 00 00   ··<·@··· ········
0020  08 00 00 00 ff 01 16 01  92 00 00 00 01 3f 00 00   ········ ·····?··
0030  00 10 18 03 04 00 03 00  aa 00 88 01 30 00 48 a9   ········ ····0·H·
0040  8a 64 eb 7f 66 d1 54 a4  60 7e 2e c8 1b c5 02 33   ·d··f·T· `~.····3
0050  a0 0c 00 00 aa aa 03 00  00 00 08 00 45 00 00 38   ········ ····E··8
0060  5c c0 00 00 ff 01 ef 60  c0 a8 f7 28 c0 a8 f7 29   \·····`· ···(···)
0070  08 00 5d fd 60 01 03 00  83 ae aa aa d9 32 59 55   ··]·`··· ·····2YU
0080  04 0d 8c ae 5c 12 99 3a  7a 6f ab d3 e4 ea 1a 7f   ····\··: zo·····
```

Address 1

Address 2

Address 3

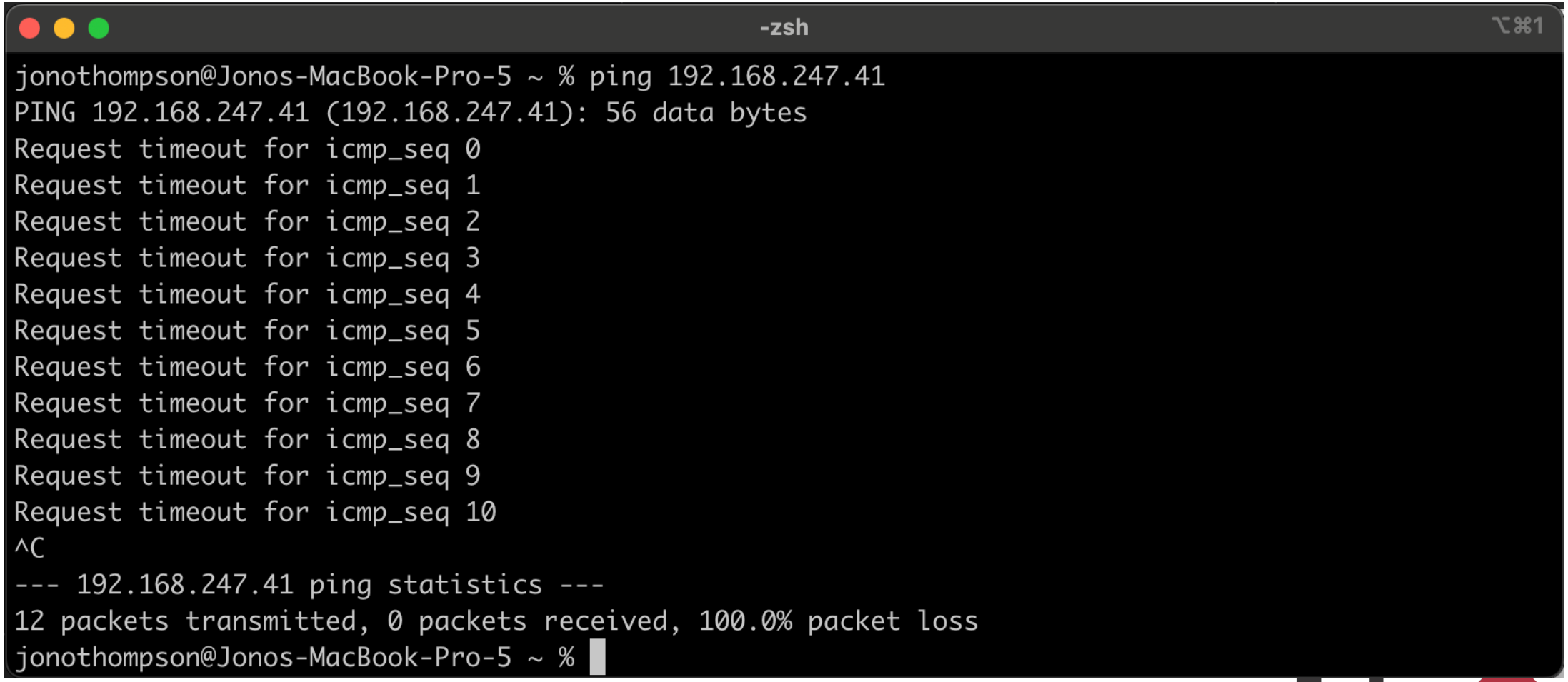
To the DS

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	1	Dst Address	Transmitter Address	Src Address	N/A
1	0	Receiver Address	Src Address	Dst Address	N/A

To the DS

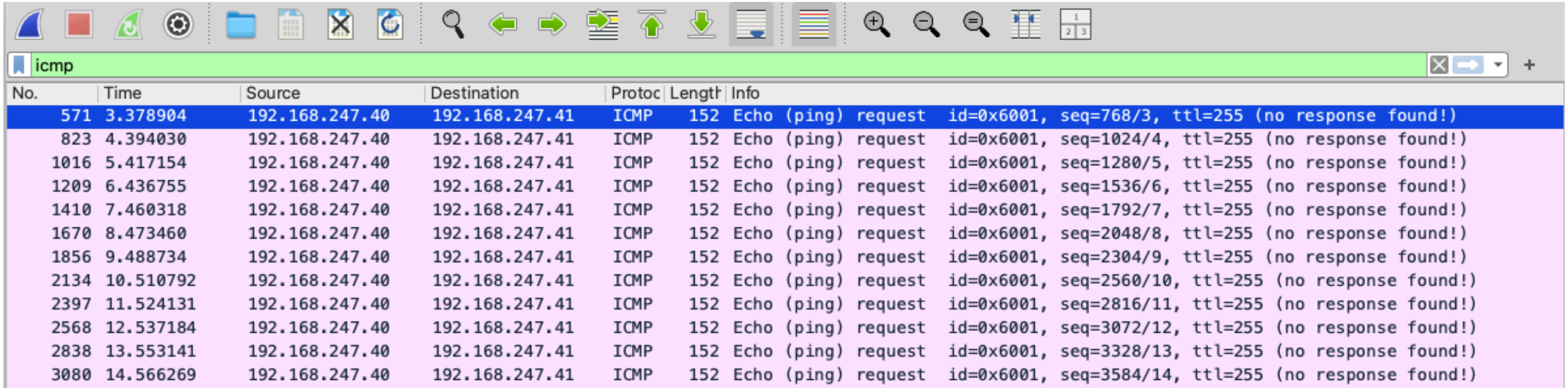
- This is seen as To the DS
- And the SRC address is correctly the source of the packet

It didn’t work



It didn’t work!

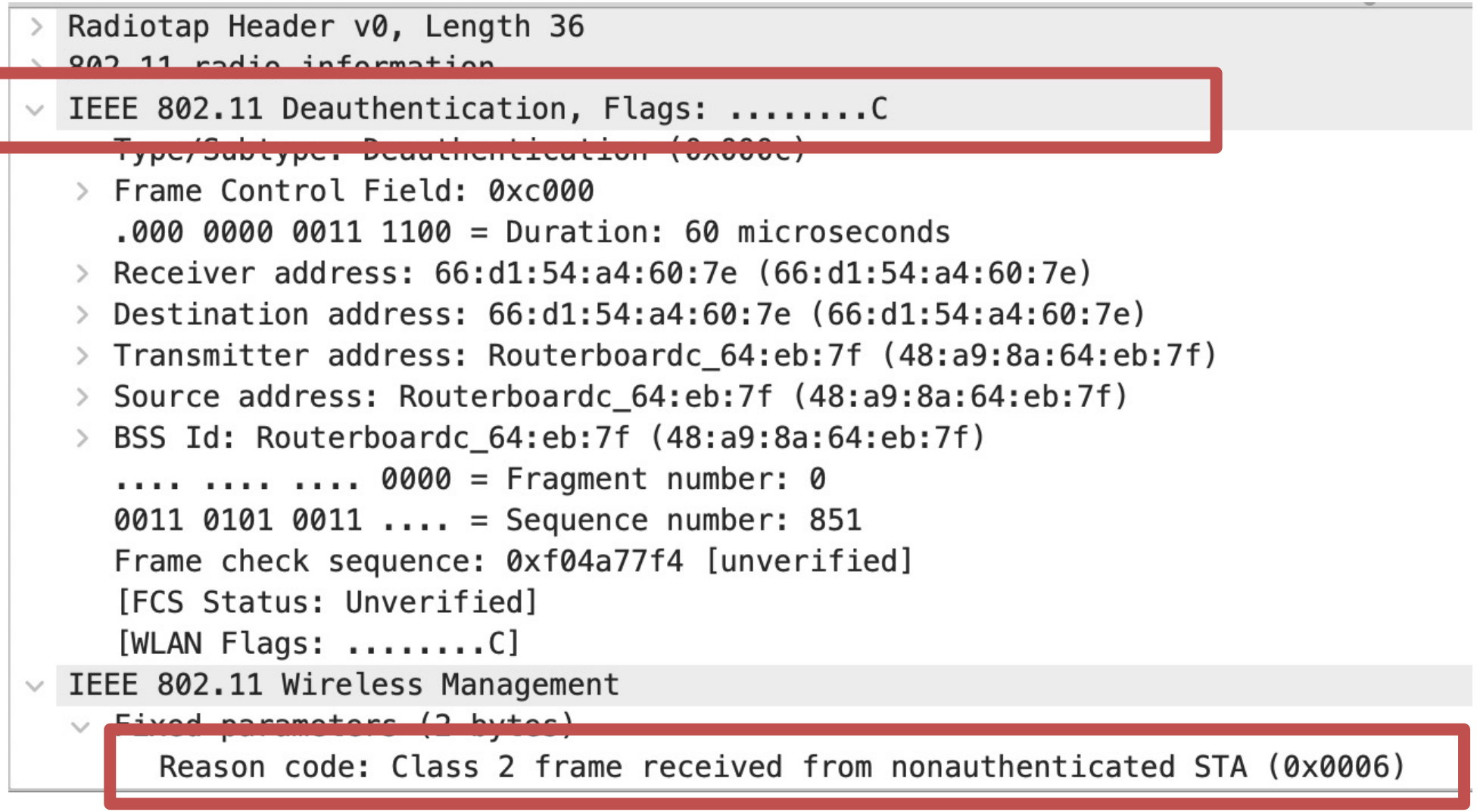
- Just incuse laptop was lying check the packet



Why?

- The packets never lie……

Why


Radiotap Header v0, Length 36
802.11 radio information
IEEE 802.11 Deauthentication, Flags: C
Type/Subtype: Deauthentication (0x000c)
Frame Control Field: 0xc000
.000 0000 0011 1100 = Duration: 60 microseconds
Receiver address: 66:d1:54:a4:60:7e (66:d1:54:a4:60:7e)
Destination address: 66:d1:54:a4:60:7e (66:d1:54:a4:60:7e)
Transmitter address: Routerboardc_64:eb:7f (48:a9:8a:64:eb:7f)
Source address: Routerboardc_64:eb:7f (48:a9:8a:64:eb:7f)
BSS Id: Routerboardc_64:eb:7f (48:a9:8a:64:eb:7f)
.... 0000 = Fragment number: 0
0011 0101 0011 .... = Sequence number: 851
Frame check sequence: 0xf04a77f4 [unverified]
[FCS Status: Unverified]
[WLAN Flags: ....C]
IEEE 802.11 Wireless Management
Fixed parameters (2 bytes)
Reason code: Class 2 frame received from nonauthenticated STA (0x0006)

Why?

- As can be seen from the packet, the wireless access point does not accept the packet from a src address which which is not an authenticated client
- The Access point also attempts to de-auth the none authenticated client
- As every frame must include radio transmitter and receiver address. This does not

Why?

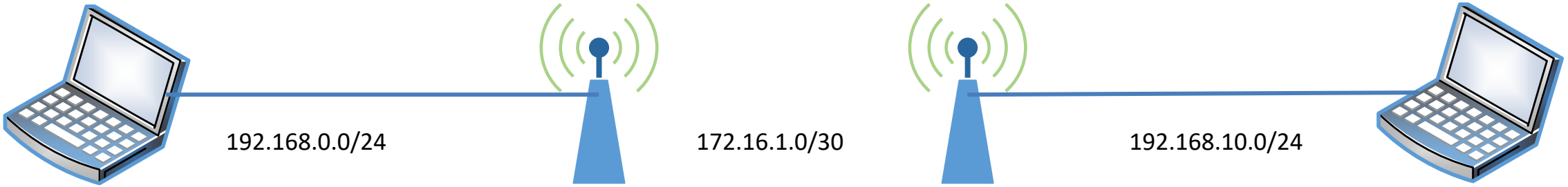
- As every frame must include radio transmitter and receiver address. This does not
- This means A transparent L2 bridge over WiFi the *3 address* frame format is not suitable

How to Resolve

- There are a number of ways this can be resolved….

Wireless Bridges - Options

- NAT
  - Loses end to end communications
- Routing
  - More Complicated Network design
  - Potentially more secure – depending on deployment



Wireless Bridges - Options

- WDS
  - Supports 4th MAC Address
  - Limited inter-vendor support as different vendors implement this differently
  - Requires support on both client and AP
- Vendor priority bridging
  - No Inter-vendor support
- MAC Spoofing

Wireless Bridges

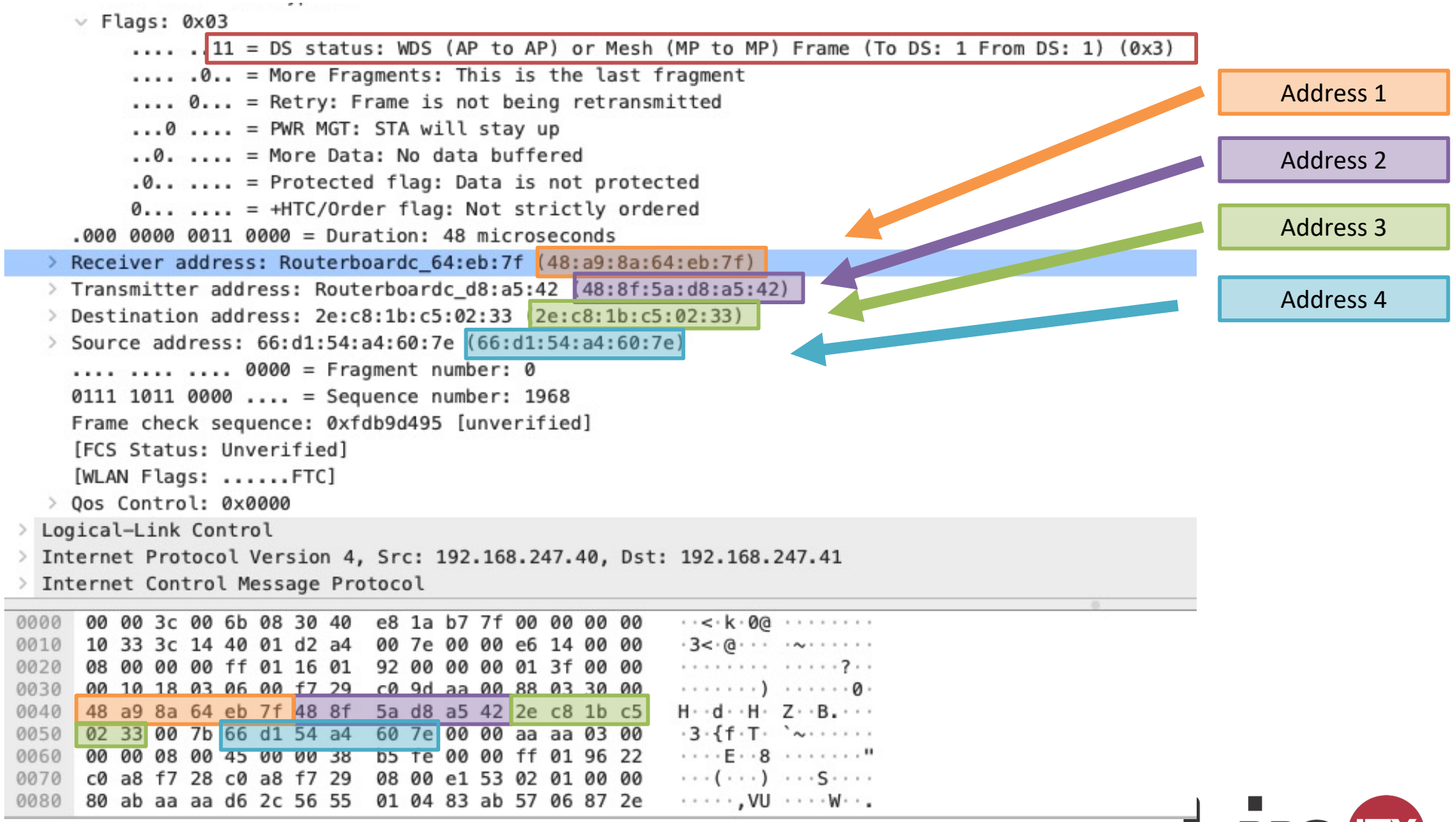
- 802.11 standard allows for an optional 4th MAC address in the header and this can be used to transmit this missing mac-address to make wireless link work

Frame Control	Duration ID	Address 1 (Receiver)	Address 2 (Sender)	Address 3 (Filtering)	seq-ctl	Address 4 (Optional)	Frame body

WDS / Wireless Bridge / Mesh

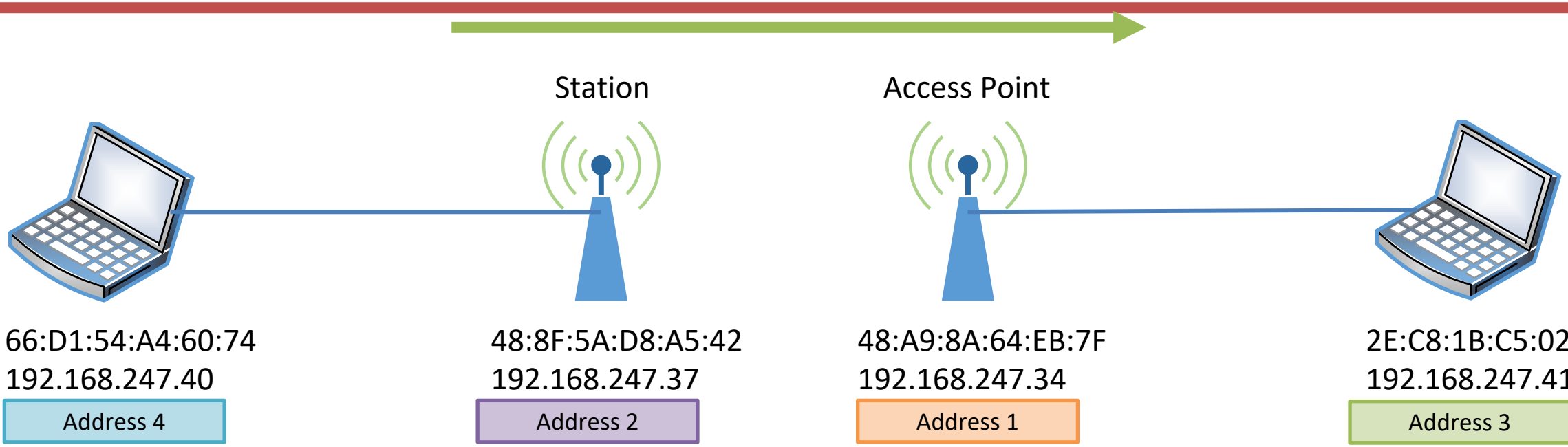
- Supports the use of the optional additional 4th mac address
- This can be seen when a vendor bridge mode is used.
- Now the wireless frame has the mac address of the wireless client.
- The example on the next slide has been taken using MikroTik Proprietary Bridge mode.

WDS or Mesh


Flags: 0x03
.... ..11 = DS status: WDS (AP to AP) or Mesh (MP to MP) Frame (To DS: 1 From DS: 1) (0x3)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
..0. .... = More Data: No data buffered
.0.. .... = Protected flag: Data is not protected
0... .... = +HTC/Order flag: Not strictly ordered
.000 0000 0011 0000 = Duration: 48 microseconds
Receiver address: Routerboardc_64:eb:7f (48:a9:8a:64:eb:7f)
Transmitter address: Routerboardc_d8:a5:42 (48:8f:5a:d8:a5:42)
Destination address: 2e:c8:1b:c5:02:33 (2e:c8:1b:c5:02:33)
Source address: 66:d1:54:a4:60:7e (66:d1:54:a4:60:7e)
.... 0000 = Fragment number: 0
0111 1011 0000 .... = Sequence number: 1968
Frame check sequence: 0xfdb9d495 [unverified]
[FCS Status: Unverified]
[WLAN Flags: ......FTC]
Qos Control: 0x0000
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.247.40, Dst: 192.168.247.41
Internet Control Message Protocol
0000 00 00 3c 00 6b 08 30 40 e8 1a b7 7f 00 00 00 00
0010 10 33 3c 14 40 01 d2 a4 00 7e 00 00 e6 14 00 00
0020 08 00 00 00 ff 01 16 01 92 00 00 00 01 3f 00 00
0030 00 10 18 03 06 00 f7 29 c0 9d aa 00 88 03 30 00
0040 48 a9 8a 64 eb 7f 48 8f 5a d8 a5 42 2e c8 1b c5
0050 02 33 00 7b 66 d1 54 a4 60 7e 00 00 aa aa 03 00
0060 00 00 08 00 45 00 00 38 b5 fe 00 00 ff 01 96 22
0070 c0 a8 f7 28 c0 a8 f7 29 08 00 e1 53 02 01 00 00
0080 80 ab aa aa d6 2c 56 55 01 04 83 ab 57 06 87 2e
Address 1
Address 2
Address 3
Address 4

WDS

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	1	Dst Address	Transmitter Address	Src Address	N/A
1	0	Receiver Address	Src Address	Dst Address	N/A
1	1	Receiver Address	Transmitter Address	Dst Address	Src Address

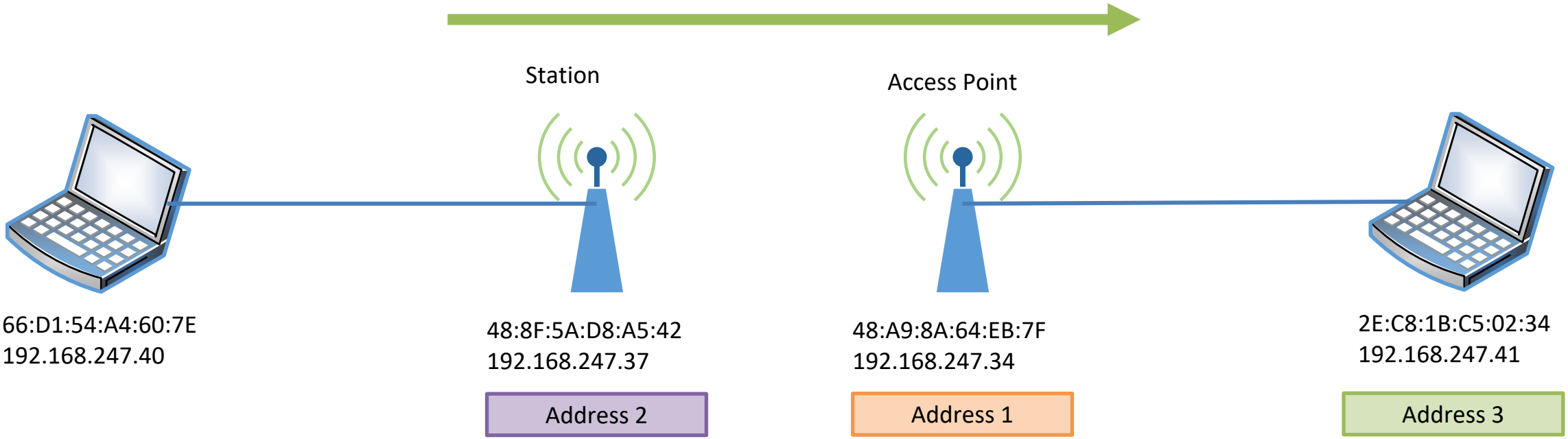


802.11 Wireless Bridges – MAC Spoofing

- Another way round this is change the SRC mac address to the MAC address of the Wireless client.
- This enables a wireless bridge to be created to any vendor Access point with no additional configuration on the access point
- The example on the next slide uses MikroTik station-pseudobridge wireless mode

802.11 Wireless Bridges – MAC Spoofing

- This bridge mode solves the problem by spoofing all src-mac addresses to the mac-address of the wireless station



Proprietary Bridge mode

```
Flags: 0x01
    .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
    .... .0.. = More Fragments: This is the last fragment
    .... 0... = Retry: Frame is not being retransmitted
    ...0 .... = PWR MGT: STA will stay up
    ..0. .... = More Data: No data buffered
    .0.. .... = Protected flag: Data is not protected
    0... .... = +HTC/Order flag: Not strictly ordered
  .000 0000 0011 0000 = Duration: 48 microseconds
> Receiver address: Routerboardc_64:eb:7f (48:a9:8a:64:eb:7f)
> Transmitter address: Routerboardc_d8:a5:42 (48:8f:5a:d8:a5:42)
> Destination address: 2e:c8:1b:c5:02:33 (2e:c8:1b:c5:02:33)
> Source address: Routerboardc_d8:a5:42 (48:8f:5a:d8:a5:42)
> BSS Id: Routerboardc_64:eb:7f (48:a9:8a:64:eb:7f)
> STA address: Routerboardc_d8:a5:42 (48:8f:5a:d8:a5:42)
  .... .... .... 0000 = Fragment number: 0
  0100 1000 1011 .... = Sequence number: 1163
  Frame check sequence: 0xf05220bf [unverified]
  [FCS Status: Unverified]
  [WLAN Flags: .......TC]
> Qos Control: 0x0000
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.247.40, Dst: 192.168.247.41
> Internet Control Message Protocol
```

```
0000  00 00 3a 00 6b 08 30 40  96 46 bf 0e 00 00 00 00   ··:·k·0@ ·F·····
0010  10 48 3c 14 40 01 d5 a4  00 00 08 00 ef 15 00 00   ·H<·@··· ········
0020  08 00 00 00 ff 01 16 01  92 00 00 00 01 3f 00 00   ········ ·····?··
0030  00 10 18 03 04 00 00 00  aa 00 88 01 30 00 48 a9   ········ ····0·H·
0040  8a 64 eb 7f 48 8f 5a d8  a5 42 2e c8 1b c5 02 33   ·d··H·Z· ·B.····3
0050  b0 48 00 00 aa aa 03 00  00 00 08 00 45 00 00 38   ·H····· ····E··8
0060  5f 05 00 00 ff 01 ed 1b  c0 a8 f7 28 c0 a8 f7 29   _····... ···(···)
0070  08 00 b5 53 2e 01 00 00  80 ab aa aa d6 2c 56 55   ···S.··· ·····,VU
0080  01 04 83 ab 57 06 87 2e  6f 5e 8d b5 ca ce eb 42   ····W··. o^·····B
```

Address 1

Address 2

Address 3

802.11 Wireless Bridges – MAC Spoofing

- As can be seen in the packet, this is using the standard wireless frame of 3 mac addresses
- The wireless client has changed the src mac address address to the mac address of the wireless client
- This now means the wireless bridge is working

Wireless Point to Point Deployment Considerations

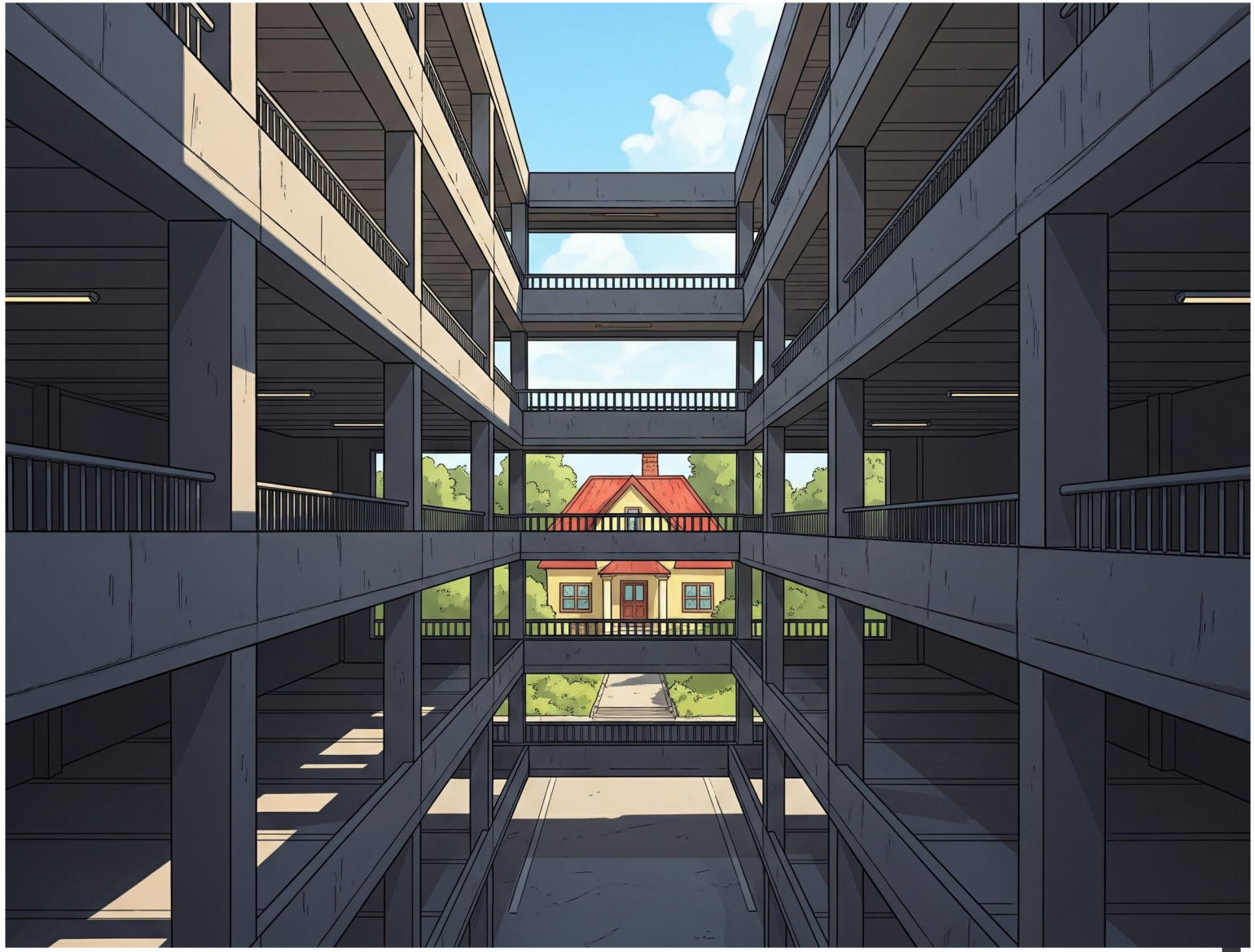
Wireless PtP Deployment Considerations

- The next few slides look at a few Deployment considerations that should be taken into account
- These are only a few and are covered in a very basic way.
- There is much more to delivering good wireless point to point links than I have time to cover today

Line of sight

- Is there clear line of sight?

Not Clear Line of Sight



Line of Sight (LOS)

- Wireless signals are not sent out in a laser like beam but an elliptical shape
- Clear Line of site requires the whole of this elliptical shape to be clear
- 5GHz links require a min of 60% clear for a reliable link
- The shape is also 3d not a flat 2d so all directions need to be clear

Obstructions in Fresnel Zone

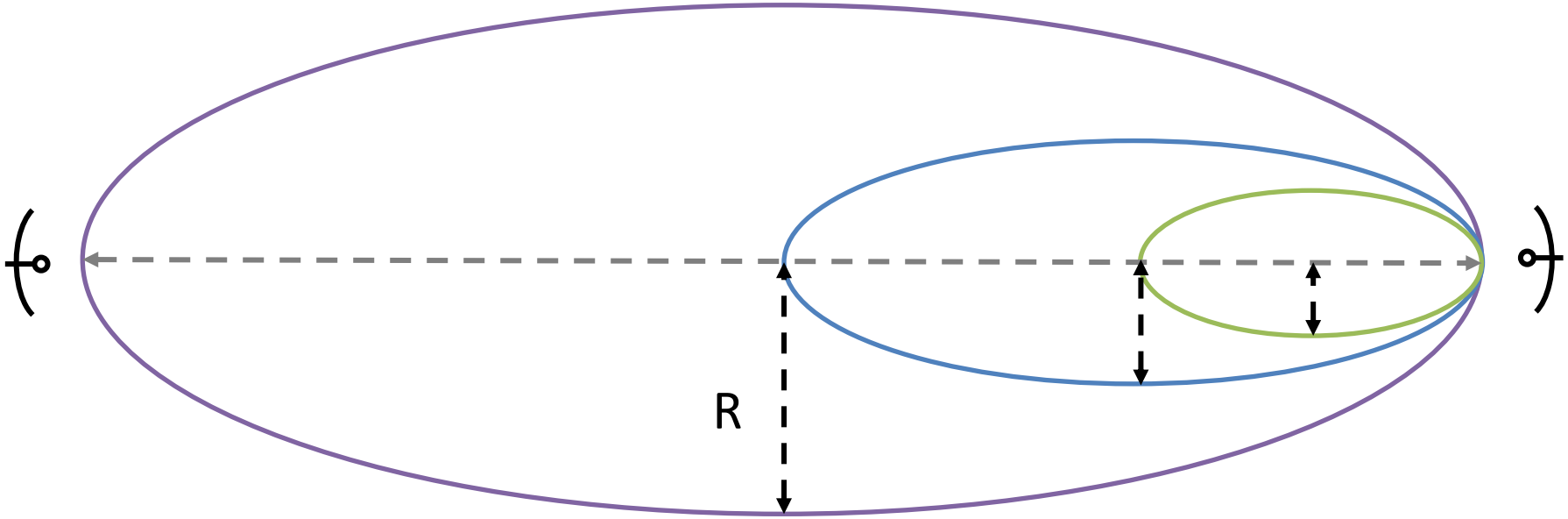
Obstructions in Fresnel Zone

- Objects in the Fresnel Zone cause attenuation to the signal
- Trees grow
- Trees get leaves in summer
- Water levels rise

WiFi Engineers toolbox

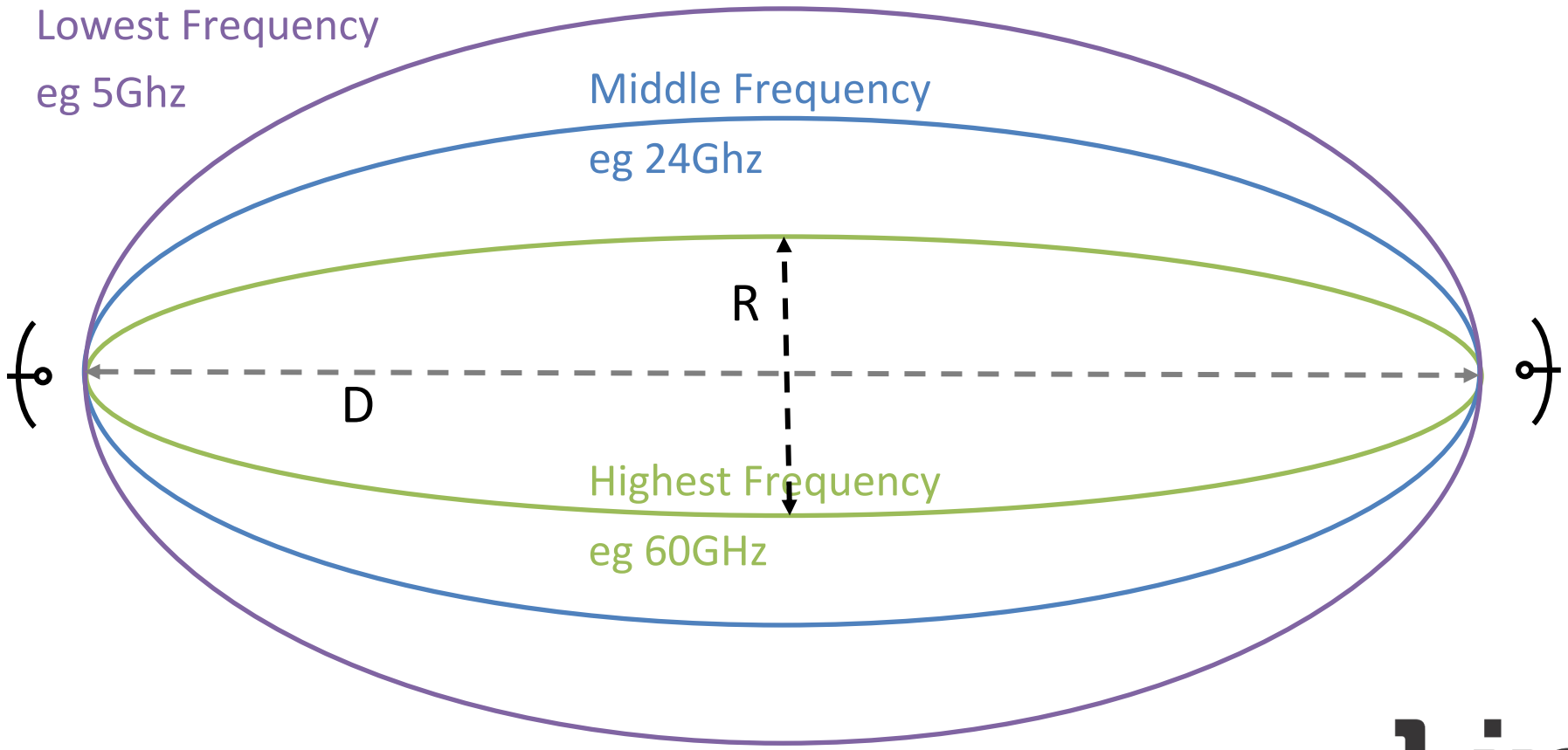
Distance vs. Radius

- Fresnel Zone radius increases with Distance

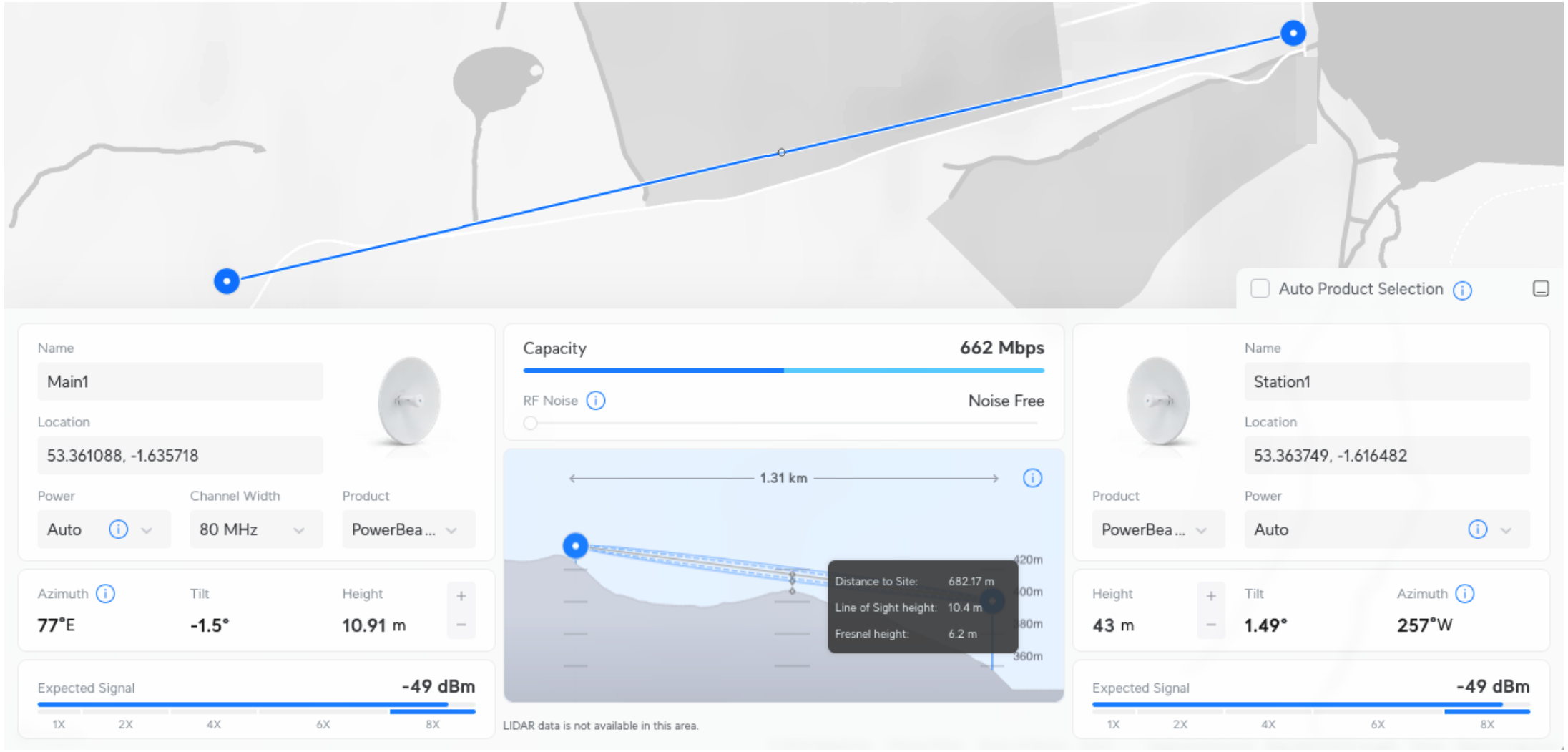


Frequency vs. Radius

- Fresnel Zone reduces with higher frequency
- “Fresnel Zone radius & Frequency inversely correlated”

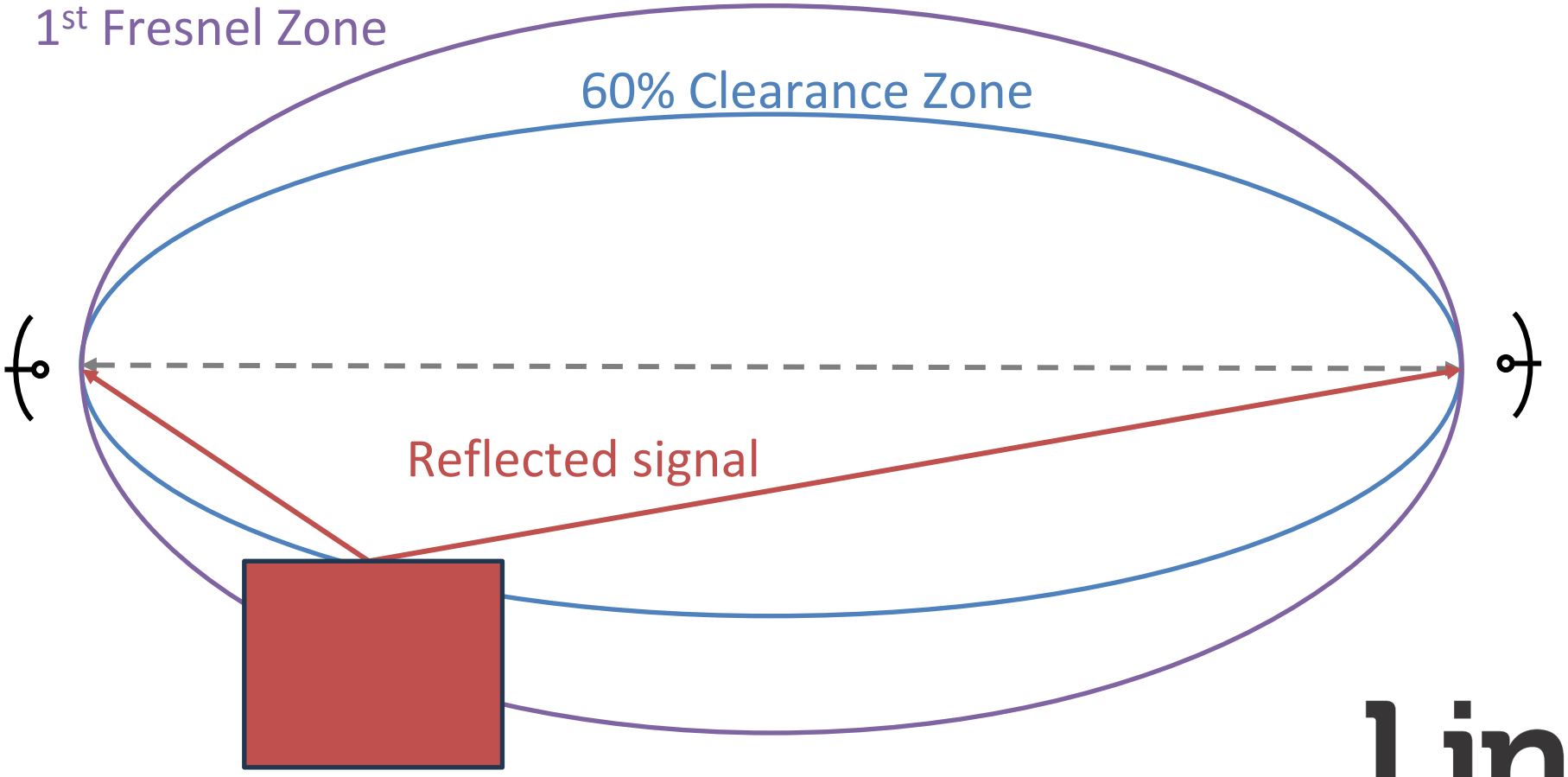


Link Planning tools



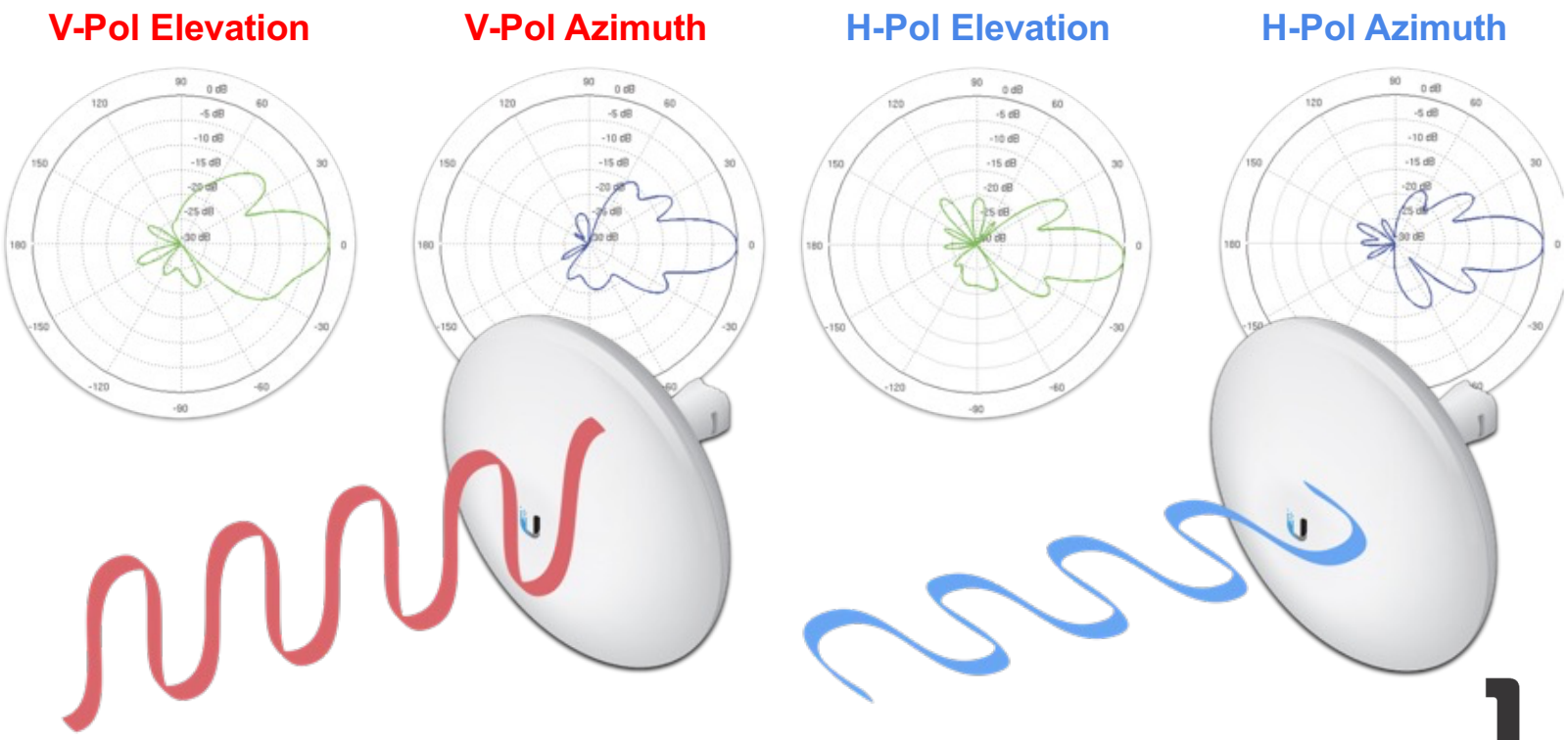
Multipath in Outdoor

- Multipath in the indoor is good. Multipath outdoor is bad
- Signal Reduction from out-of-phase main/reflected waves



MIMO in the Outdoors

- Outdoor antennas polarised with each antenna 90^{o} apart.
- Waveforms are vertical and horizontal polarised
- Outdoor antennas must be correctly aligned



Slant Polarisation

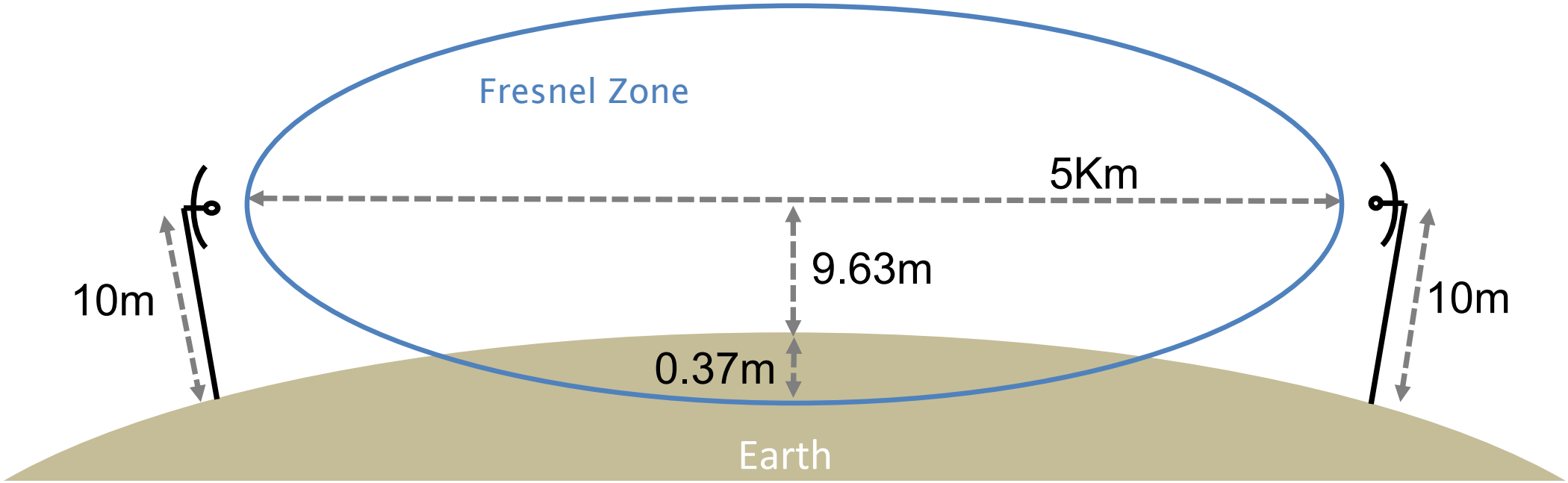
- Most obstructions are either horizonal or vertical.
- This means they cause maximum impact to the signal
- Slanting the whole orthogonal polarisation so the antennas are +/- 45^{o} and not at 0^{o} and 90^{o}
- Slant polarisation reduces the problem caused by reflections of Horizonal or Vertical obstructions

Unfortunately, the Earth is not flat….

Curvature of earth

Curvature of earth

- Links over 5Km need to take into account curvature of the earth when calculating Fresnel zone



Curvature of Earth

- The formula for calculating the effect of the Earth's radius is as follows:

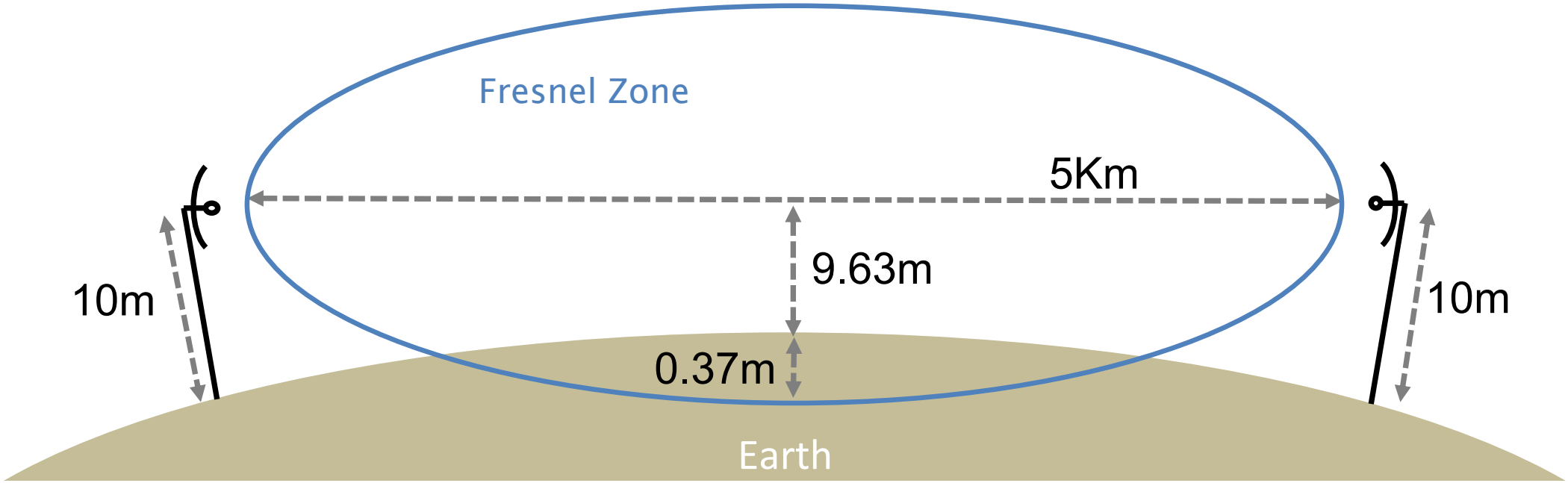
$$H = \frac{1000 \times D^2}{8 \times Er}$$

Where:-

- H = Height difference of Earth's Curvature at the mid-point between the two devices (m)
- D = Total Link Distance between the two devices (km)
- Er = Effective Radius of Earth (km). This is usually taken as 4/3 (1.333 rec.) actual radius to account for atmospheric refraction ie. 8,504km

Curvature of earth

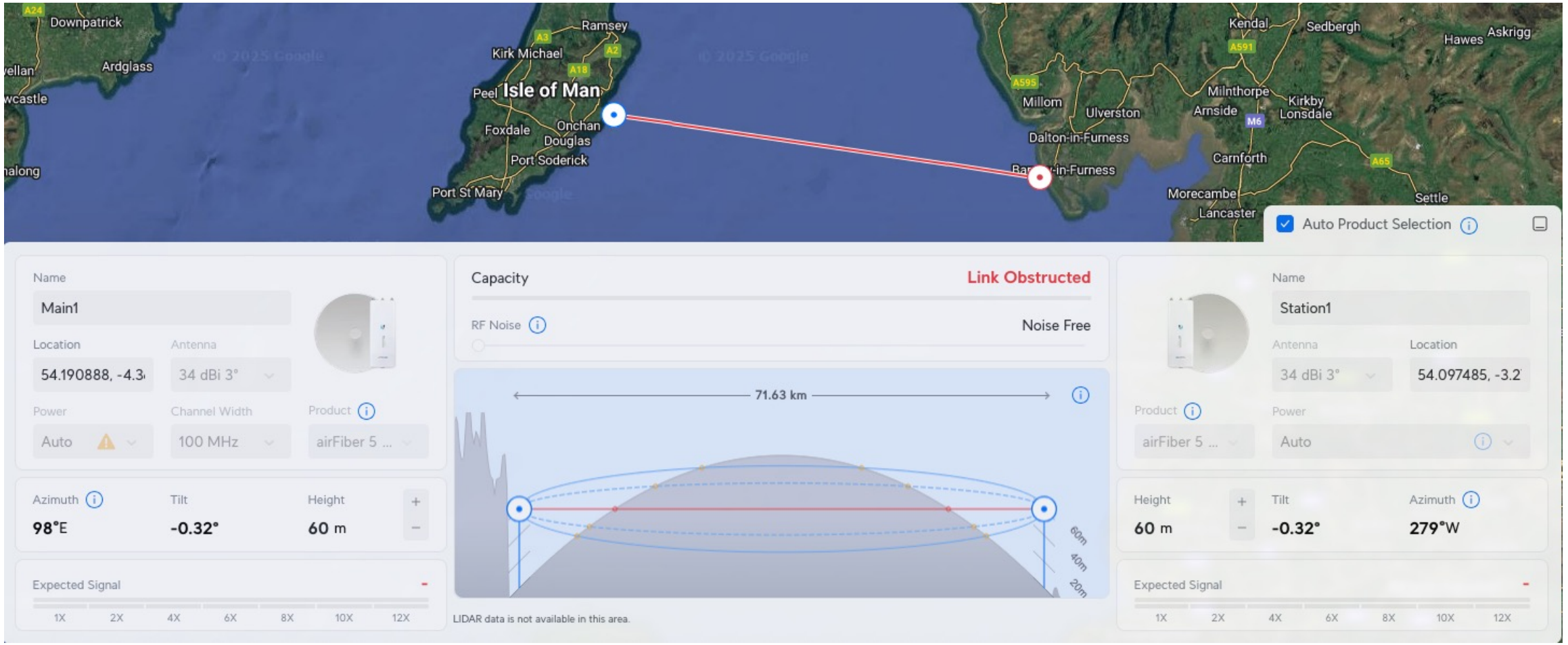
$$H = \frac{1000 \times 5^2}{8 \times 8504}$$
$$H = 0.37m$$



Wireless link planning tools

- There are a number of planning tools which mean we do not need to do the maths our self.
- Some also take LADAR building data too
- Vendor specific tools will calculate the expected link performance too
- The examples to follow have been made using the Ubiquiti planning tool
- https://ispdesign.ui.com

Curvature of earth

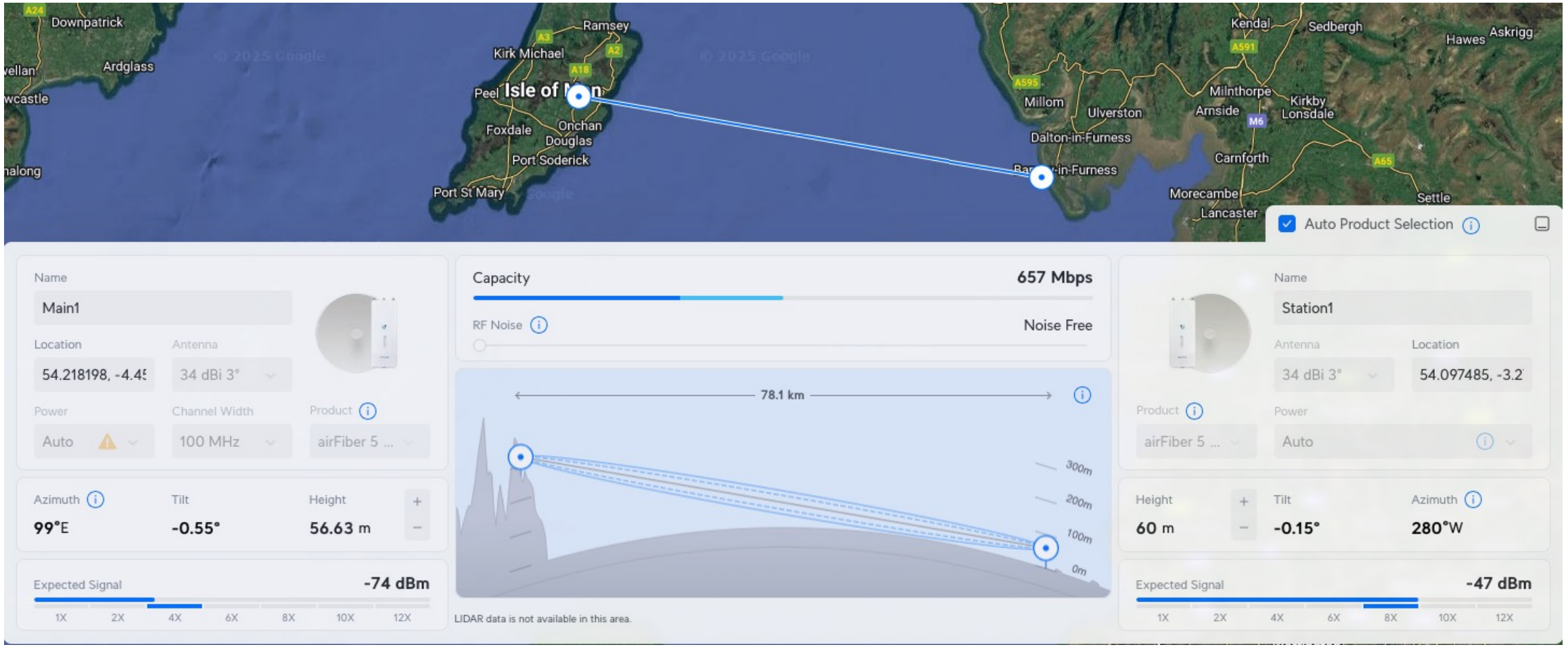


Curvature of earth

- It might not be practical to install a mast of 10’s of M or even 100m tall.

- Land features like Hills and mountains can be used to make long links possible!

Curvature of earth



DFS

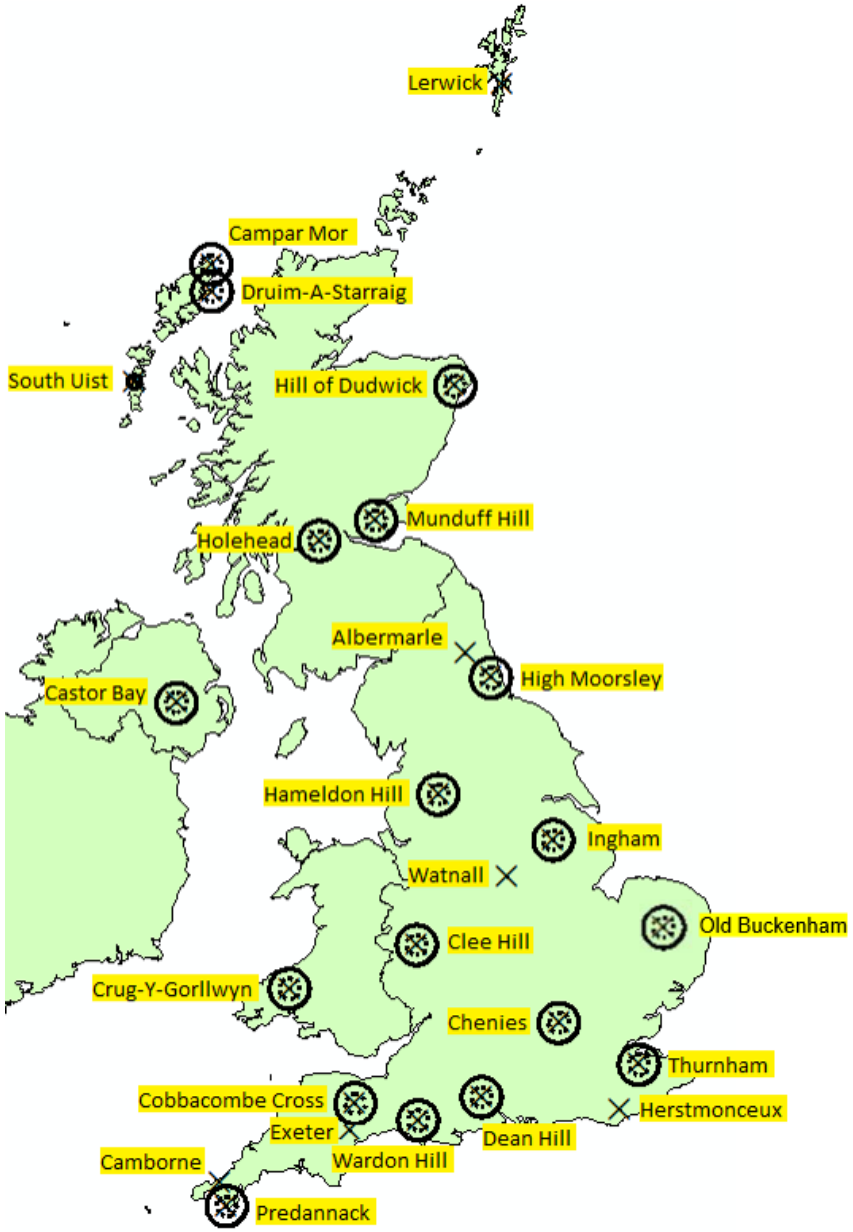
DFS

- Not discount furniture
- Dynamic Frequency Selection (DFS)
- Where a high % of DFS events indoors are often false positives outdoors these detections are more likely to be real.
- Channel selection and link planning needs to take into account the locations of weather radar station

Weather Radar

https://www.metoffice.gov.uk/research/weather/observations-research/raindrops-and-radar

Weather Radar sites



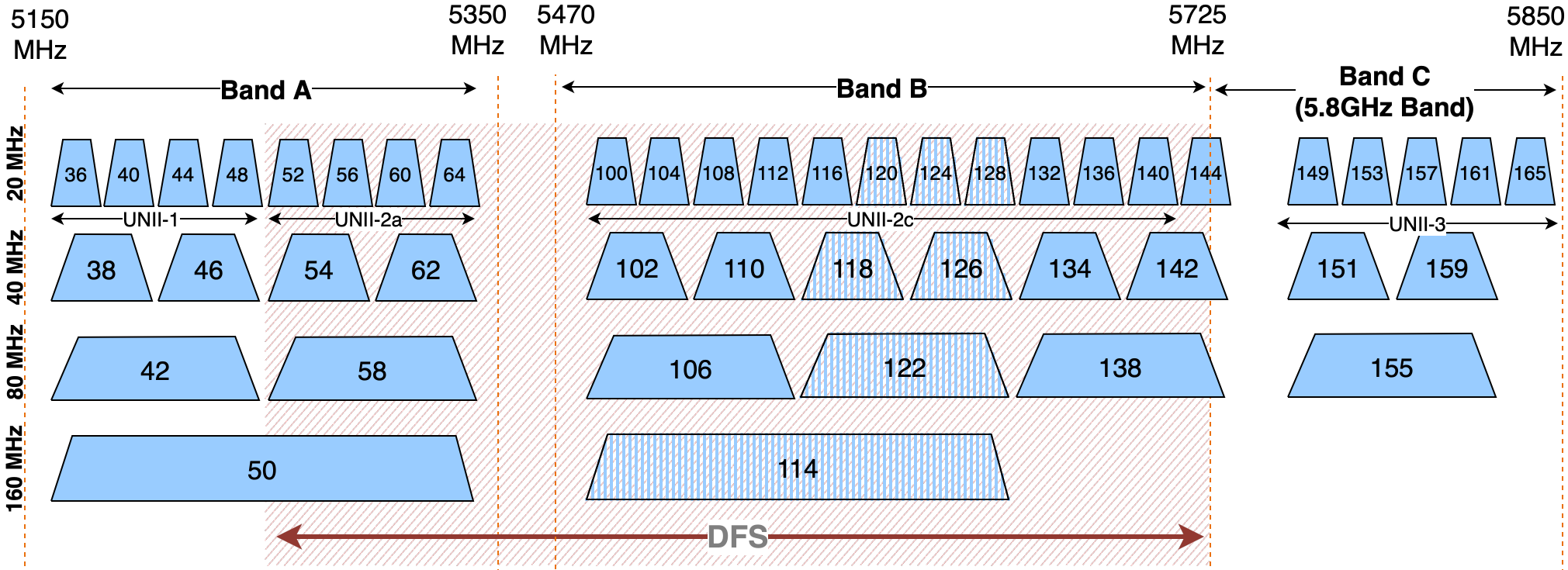
- Campar Mor-proposed radar
- Castor Bay
- Chenies
- Clee Hill
- Cobbacombe Cross
- Crug-y-Gorllwyn
- Dean Hill
- Drium-a-Starraig
- Hameldon Hill
- High Moorsley
- Hill of Dudwick
- Holehead
- Ingham
- Munduff
- Old Buckenham
- Predannack
- Thurnham
- Wardon Hill

5GHz Channel usage Outdoors

UK 5GHz WLAN Spectrum (Nov 2024)

WifiNigel.com

Channel	Centre Freq (MHz)
36	5180
40	5200
44	5220
48	5240
52	5260
56	5280
60	5300
64	5320
100	5500
104	5520
108	5540
112	5560
116	5580
120	5600
124	5620
128	5640
132	5660
136	5680
140	5700
144	5720
149	5745
153	5765
157	5785
161	5805
165	5825



5150-5350Mhz
Max EIRP = 200mW
Indoor only

5470 – 5725 Mhz
Max EIRP = 1W
Indoor/Outdoor

5725 - 5850Mhz
Max EIRP = 200mW
Indoor/(Outdoor? Restriction: No Fixed Outdoor*)

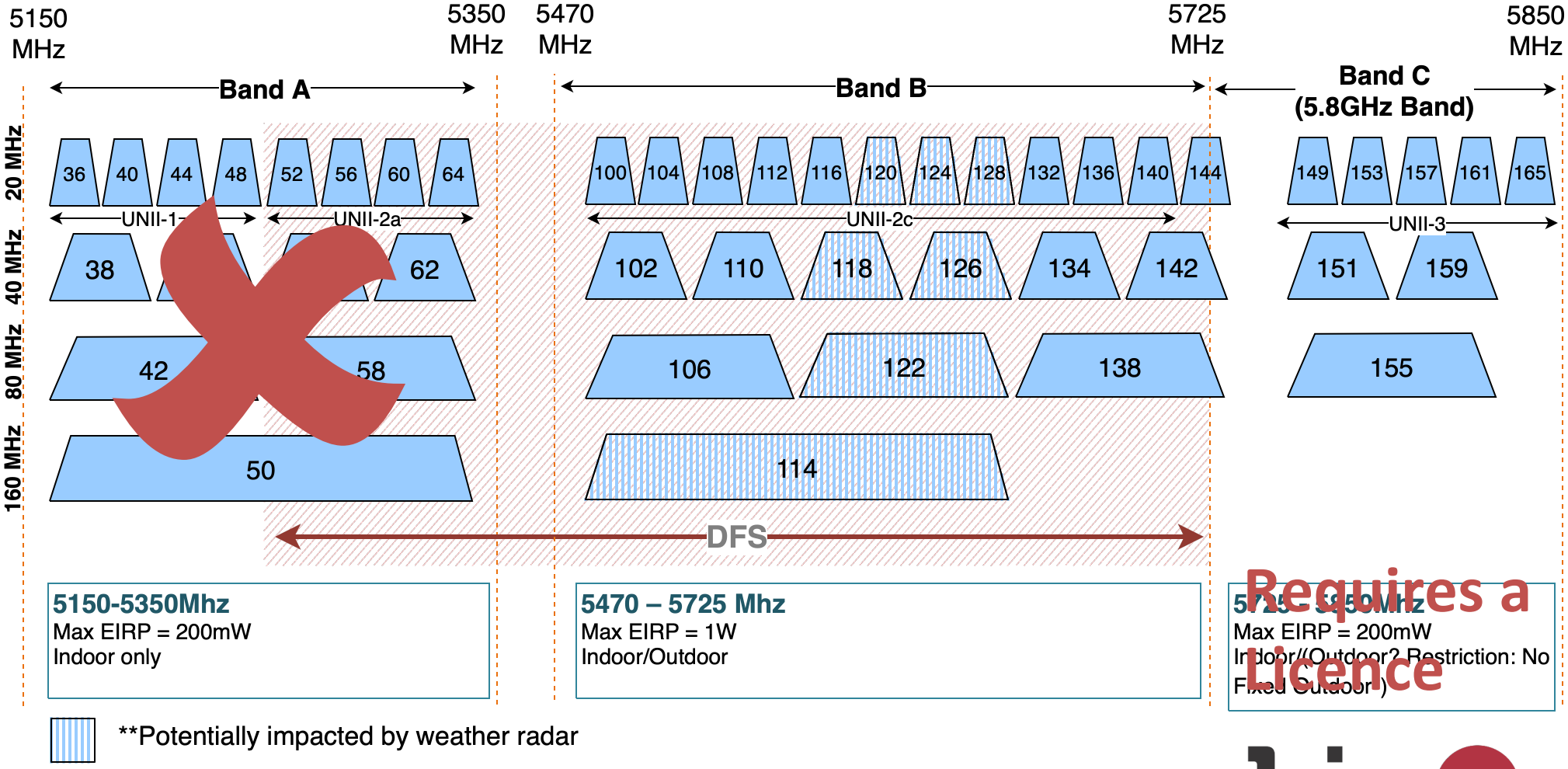
**Potentially impacted by weather radar

5GHz Channel usage Outdoors

UK 5GHz WLAN Spectrum (Nov 2024)

WifiNigel.com

Channel	Centre Freq (MHz)
36	5180
40	5200
44	5220
48	5240
52	5260
56	5280
60	5300
64	5320
100	5500
104	5520
108	5540
112	5560
116	5580
120	5600
124	5620
128	5640
132	5660
136	5680
140	5700
144	5720
149	5745
153	5765
157	5785
161	5805
165	5825

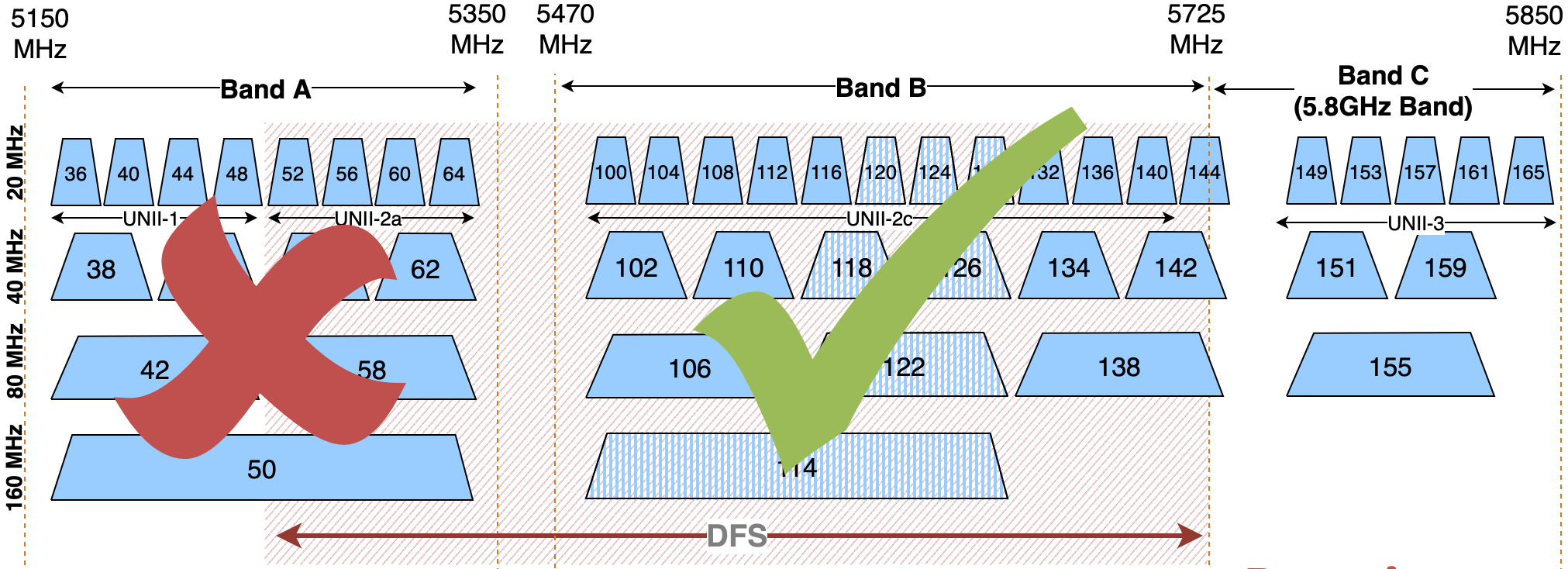


5GHz Channel usage Outdoors

UK 5GHz WLAN Spectrum (Nov 2024)

WifiNigel.com

Channel	Centre Freq (MHz)
36	5180
40	5200
44	5220
48	5240
52	5260
56	5280
60	5300
64	5320
100	5500
104	5520
108	5540
112	5560
116	5580
120	5600
124	5620
128	5640
132	5660
136	5680
140	5700
144	5720
149	5745
153	5765
157	5785
161	5805
165	5825



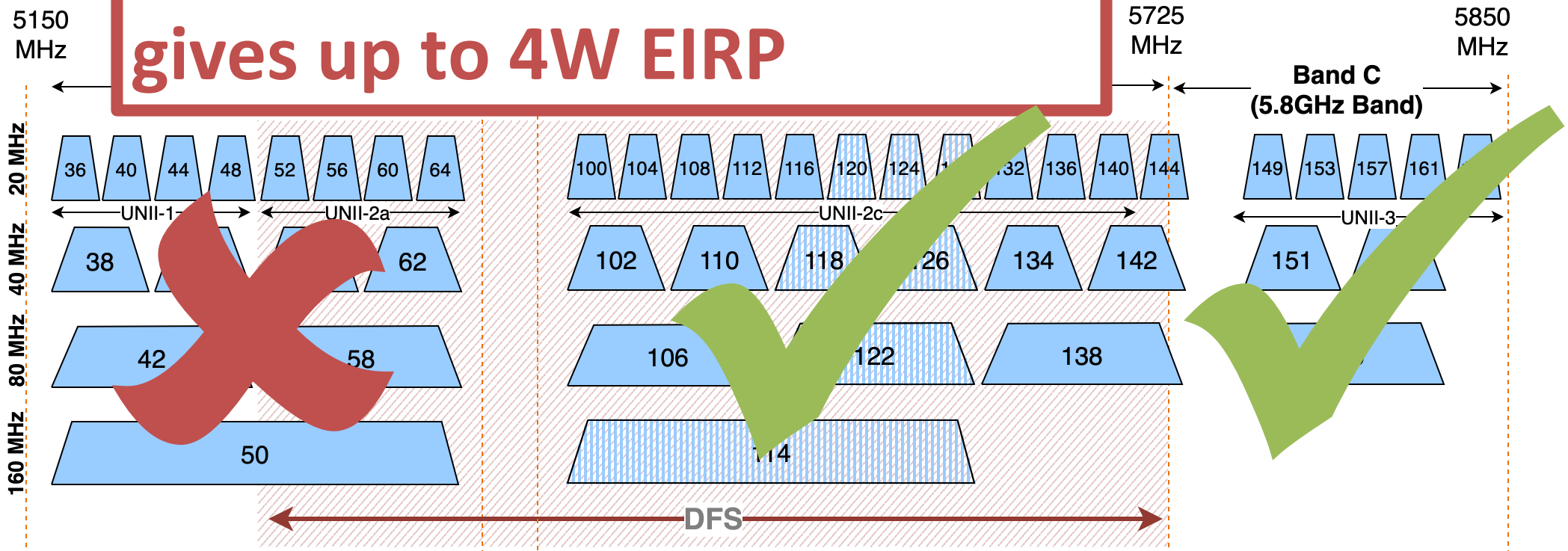
5GHz Channel usage Outdoors

UK 5GHz

Band C – Requires a Licence gives up to 4W EIRP

WifiNigel.com

Channel	Centre Freq (MHz)
36	5180
40	5200
44	5220
48	5240
52	5260
56	5280
60	5300
64	5320
100	5500
104	5520
108	5540
112	5560
116	5580
120	5600
124	5620
128	5640
132	5660
136	5680
140	5700
144	5720
149	5745
153	5765
157	5785
161	5805
165	5825



5150-5350Mhz
Max EIRP = 200mW
Indoor only

5470 – 5725 Mhz
Max EIRP = 1W
Indoor/Outdoor

5725 - 5850Mhz
Max EIRP = 200mW
Indoor/(Outdoor? Restriction: No Fixed Outdoor*)

**Potentially impacted by weather radar

5GHz Channel usage Outdoors

5GHz Band	Usage notes
Band A	Indoor only
Band B	Indoor and Outdoor upto 1W EIRP Requires DFS Potential Interference from Weather Radar
Band C	Outdoor fixed installations require licence from OFCOM Outdoor fixed installations upto 4W EIRP

5GHz Channel usage Outdoors

References:

- IR2030 section 8
- https://www.ofcom.org.uk/siteassets/resources/documents/spectrum/interface-requirements/ir-2030.pdf?v=335258

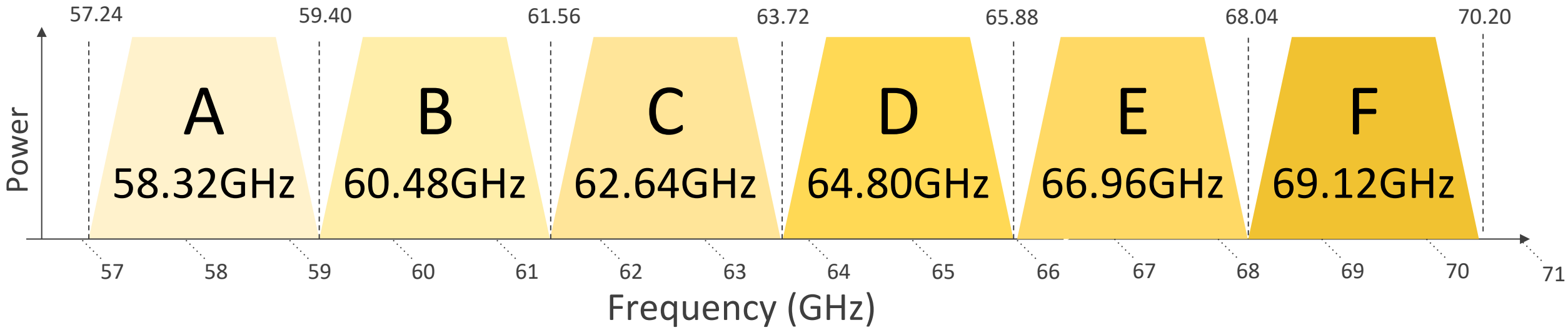
- IR2007
- https://www.ofcom.org.uk/siteassets/resources/documents/spectrum/interface-requirements/ir_2007.pdf?v=335252

When it is not fast enough

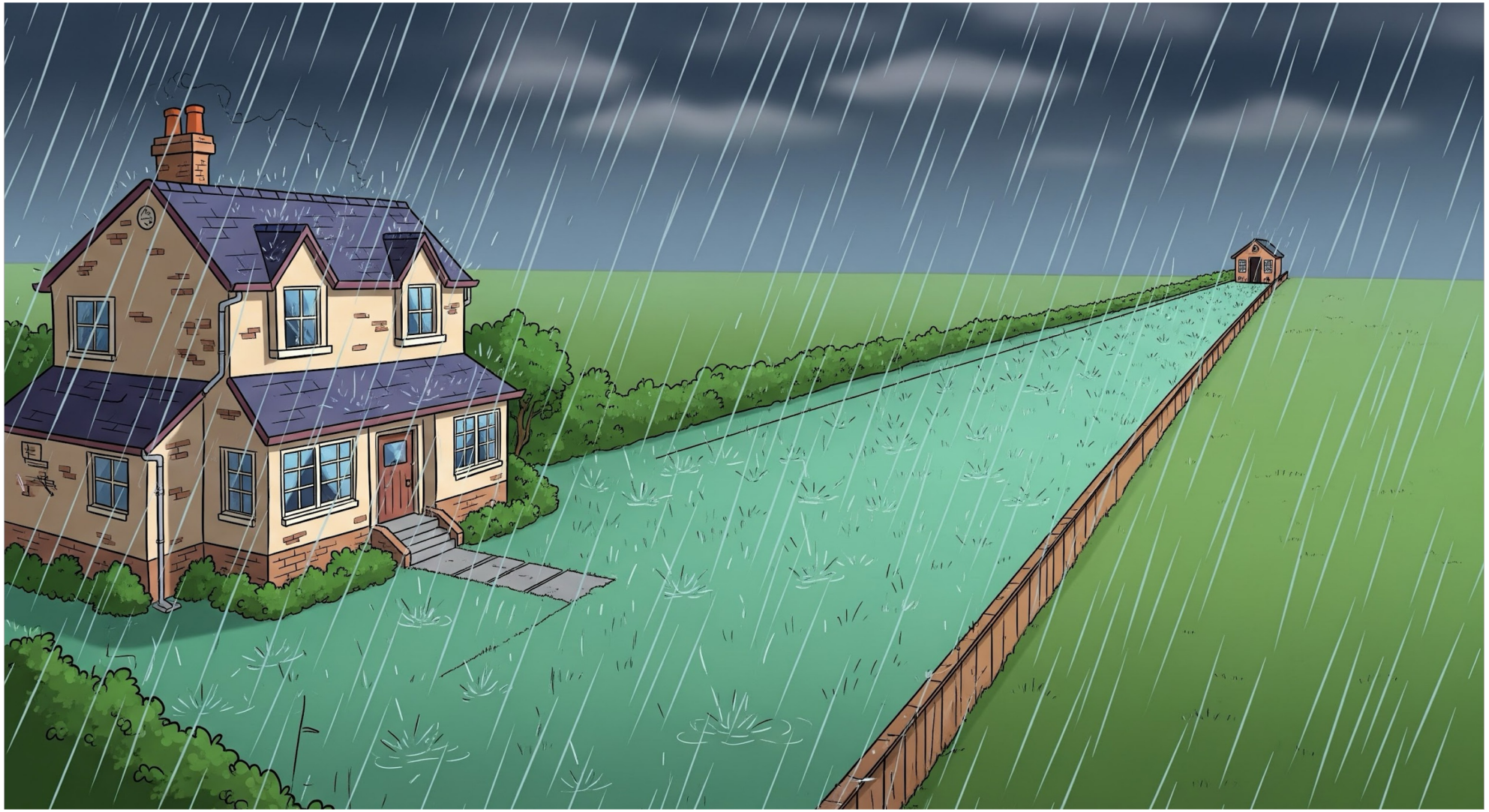
- 802.11ad and 802.11ay standards use 60GHz
- 60GHz can deliver multi-gigabit transmissions over short distances
- 60GHz has very narrow beamwidth
- 60GHz has virtually no in band interference
- 60GHz are more directional and less prone to interference
- No DFS regulations

60GHz Spectrum

Six 212MHz wide channels in the UK.

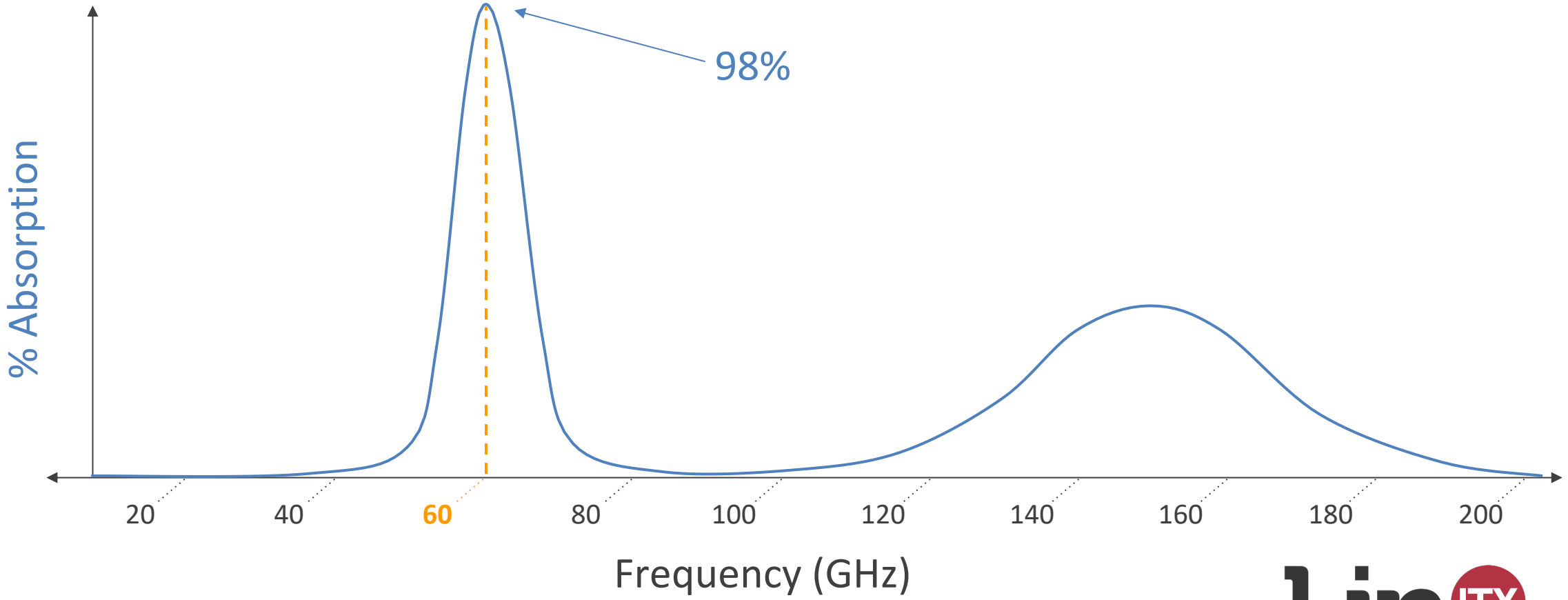


Typical British Weather



Oxygen Absorption

- "Highest concentration of energy absorbed by O_2 Molecules @60GHz"



When it is not fast enough

- Higher frequency subject to higher attenuation so does not penetration objects
- 60GHz is the resentment frequency of O_2 so subject to much higher attention though air
- Frequencies over 8GHz are also subject to rain fade
- Many vendors equip 60GHz radios with a 5GHz backup radio

OFCOM band V Regulations

- Radios with max power of 27dBm and max EIRP of 40dBm are licence exempt
- IR2030/7/4
- https://www.ofcom.org.uk/siteassets/resources/documents/spectrum/interface-requirements/ir-2030.pdf?v=335258

- Radios with max EIRP of 55dBm and max antenna gain of 30dBi require an EHF licence. £75 / 5 years

OFCOM band V Regulations

- Radios with max EIRP of 55dBm and max antenna gain of 30dBi require an EHF licence. £75 / 5 years

- IR2106 https://www.ofcom.org.uk/siteassets/resources/documents/spectrum/interface-requirements/ir-2106.pdf?v=325302

And if all else fails…. run a Cable

Thank you for Listening

LinITX Blog

Training

Linkedin