Essentials of
Short Range Wireless Standards

Nick Hunn

WiFore Consulting

What's out there?

Bluetooth
Bluetooth low energy
Wi-Fi (a,b,g,n)
Wi-Fi Direct
ZigBee
ZigBee PRO
ANT+
Wireless M-Bus
Z-Wave
Wireless USB
NFC
UWB

Insteon
RF4CE
6LoWPAN
Synkro
Amimon
UWB
Wireless HART
TransferJet
DASH7

And Proprietary

And don't forget cellular - they want the M2M market as well.

In praise of cables

- Range is usually not an issue – just add more cable.
- Latency is excellent – what goes in one end appears immediately at the other.
- They're transparent to data protocols and formats
- Throughput is excellent
- No issue with Security – you know what you plug it into.
- Interoperability is excellent. At most, you only need to change the plug.
- Power consumption may be higher, but the cable can carry power.
- They can be specified on a single page.

As well as…

- Topology is simple – it's typically one-to-one.
- Robustness to interference is generally a minor issue.
- Backwards Compatibility is normally no more difficult than changing a plug, and
- There's generally no License agreement, no Qualification Requirements and no Export Controls.

Replacing cables with wireless standards gives us

- Thousands of pages of specifications, purely to make up for the fact they're not as good as a cable.
- A lot of cost.
- Some difficult choices.

- A lot of flexibility
- The ability to design products differently.

What do we get from standards?

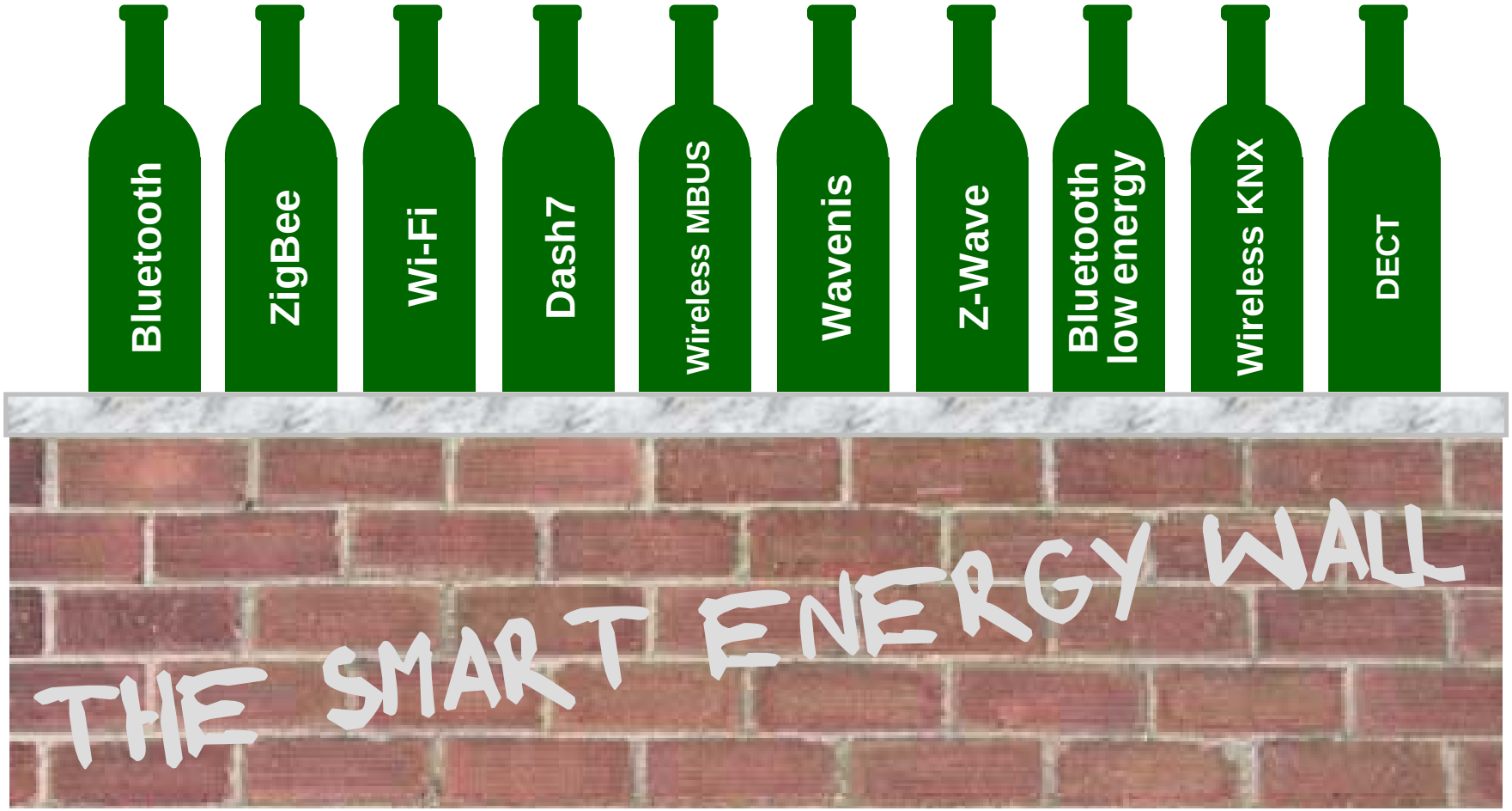
The Advantages

- Economies of Scale
- Multiple Suppliers
- Broad Industry Support
- Better Security
- Interoperability
- User Perception
- Industry Marketing
- Being part of an Ecosystem

The Disadvantages

- Complexity
- They’re a compromise
- Limited Modification Ability
- May attract hackers
- Qualification Cost
- Membership Requirements

For every application there are multiple contenders…



The billion unit markets for wireless.

	TAM*
• Phone accessories (internet / apps centric devices)	> 10 billion
• Smart Energy (meters & displays). *Which will drive:*	~ 1 billion
• Home Automation (white goods and HVAC)	> 5 billion
• Health, Wellness, Sports & Fitness	> 10 billion
• Assisted Living	> 5 billion
• Animal Tagging (food assurance)	~ 3 billion
• Intelligent Transport Systems	> 1 billion
• M2M (Internet connected devices)	> 10 billion

* TAM – Total Addressable Market

How do standards differ?

Not by as much as most people imagine.

Regulators control which RF frequencies a standard can operate at.

Physics dictates a lot of the radio performance – there are trade-offs between range, throughput and power consumption. These determine which market spaces each can play in.

Higher layer stacks can tune the performance to a particular application area.

Industry Alliances dictate in which markets a standard may be accepted.

Marketing helps to determine which standards are accepted in each.

There is growing competition between the standards for each new market.

Often that has little to do with their applicability

What is a standard?

- It is defined by a group, not a single company
- There are two or more silicon and stack suppliers
- It owns some or all of its Intellectual Property
- It offers interoperability
- It imposes qualification requirements and enforces them

Otherwise it's a proprietary implementation with ideas above its station.

Which means it may not exist in five year's time.

Wireless standards

Standard	Application Profiles	Multiple Suppliers	Qualification Program	Enforcement Program	Annual Shipments (millions)
Bluetooth	Yes	Yes	Yes	Yes	1,000
802.11	n/a	Yes	No	No	100
Wi-Fi	Yes	Yes	Yes	Yes	250
802.15.4	n/a	Yes	No	No	35
ZigBee / ZigBee PRO	Yes	Yes	Yes	Not active	5
Bluetooth low energy	Yes	Yes	Yes	Yes	0**
Wireless HART	n/a	Yes	No	No	2
6LoWPAN	n/a	Yes	No	No	0**
Z-Wave	Yes	No	Yes	No	2
ANT	Yes	Yes (2)	No*	No	2
DASH7	No	Yes	In Dev	No	0**
Wireless M-Bus	No	Yes	No	No	1

** The ANT qualification is a self-certification.*
*** Not yet shipping in volume.*

Choosing a wireless standard

The primary concerns of a designer are normally:

- Range
- Throughput
- Latency
- Power Consumption
- Cost
- The interoperable Ecosystem

Equally important are:

- Topology
- Security
- Licensing
- Robustness
- Backwards Compatibility

With a cable they come as standard.

With wireless they determine your choice of standard.

Range and Throughput

Throughput is intimately linked to range

Standard	Spectrum	Typical Throughput	Symbol Rate	Typical Range
802.11	2.4 GHz	~ 0.8 Mbps	2 Mbps	100 meters
802.11a	5.1 GHz	~ 24 Mbps	54 Mbps	15 meters
802.11b	2.4 GHz	~ 5 Mbps	11 Mbps	45 meters
802.11g	2.4 GHz	~ 22 Mbps	54 Mbps	25 meters
802.11n	2.4 GHz / 5.1 GHz	~ 130 Mbps	600 Mbps	50 meters (2.4 GHz)

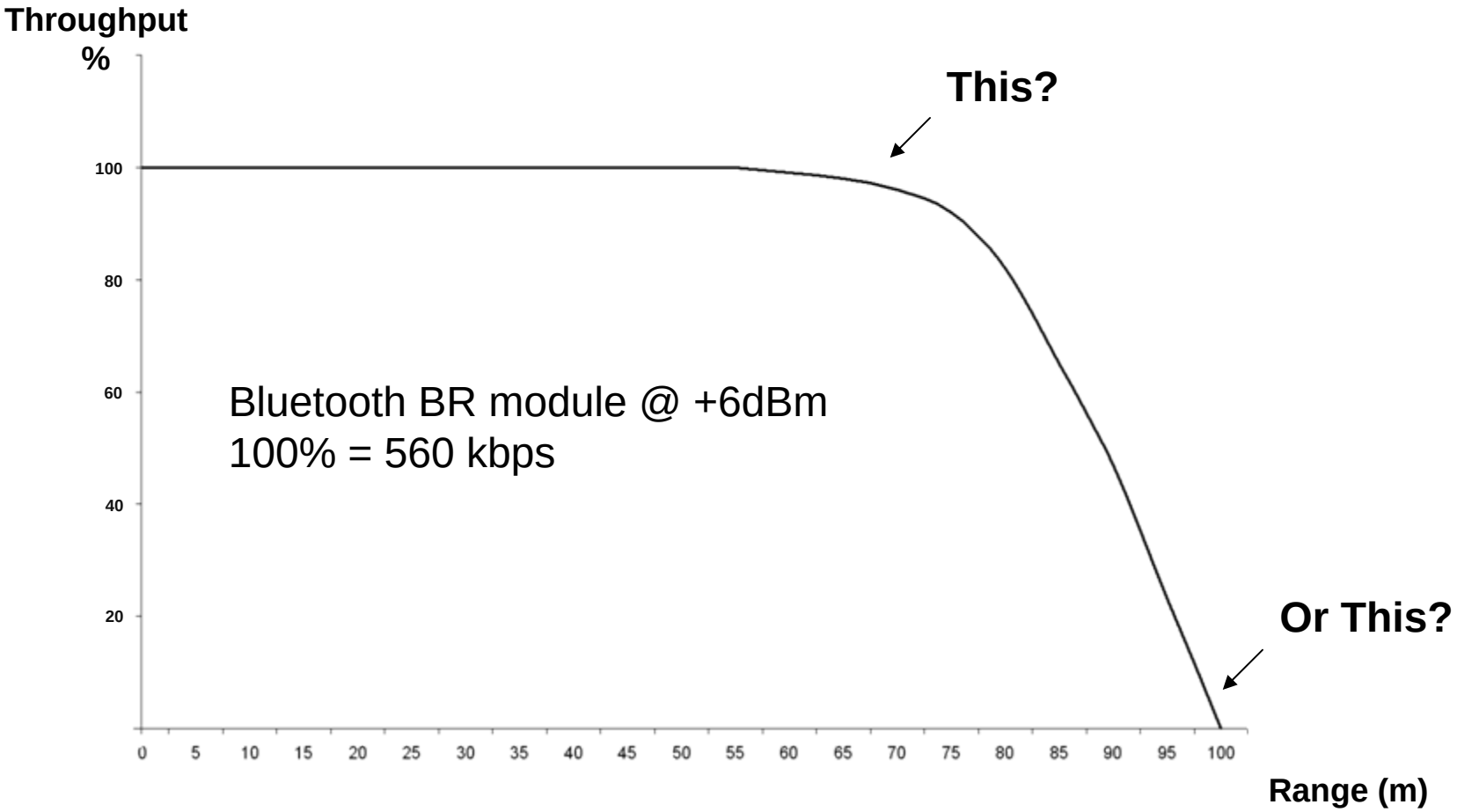
Every radio standard has the same underlying issue.

More throughput at the same symbol rate means more complex coding. Which increases the bit error rate, which reduces the range.

The alternative, of increasing the transmit power or the symbol rate, or transmitting and receiving multiple streams (MIMO), all increase the current consumption…

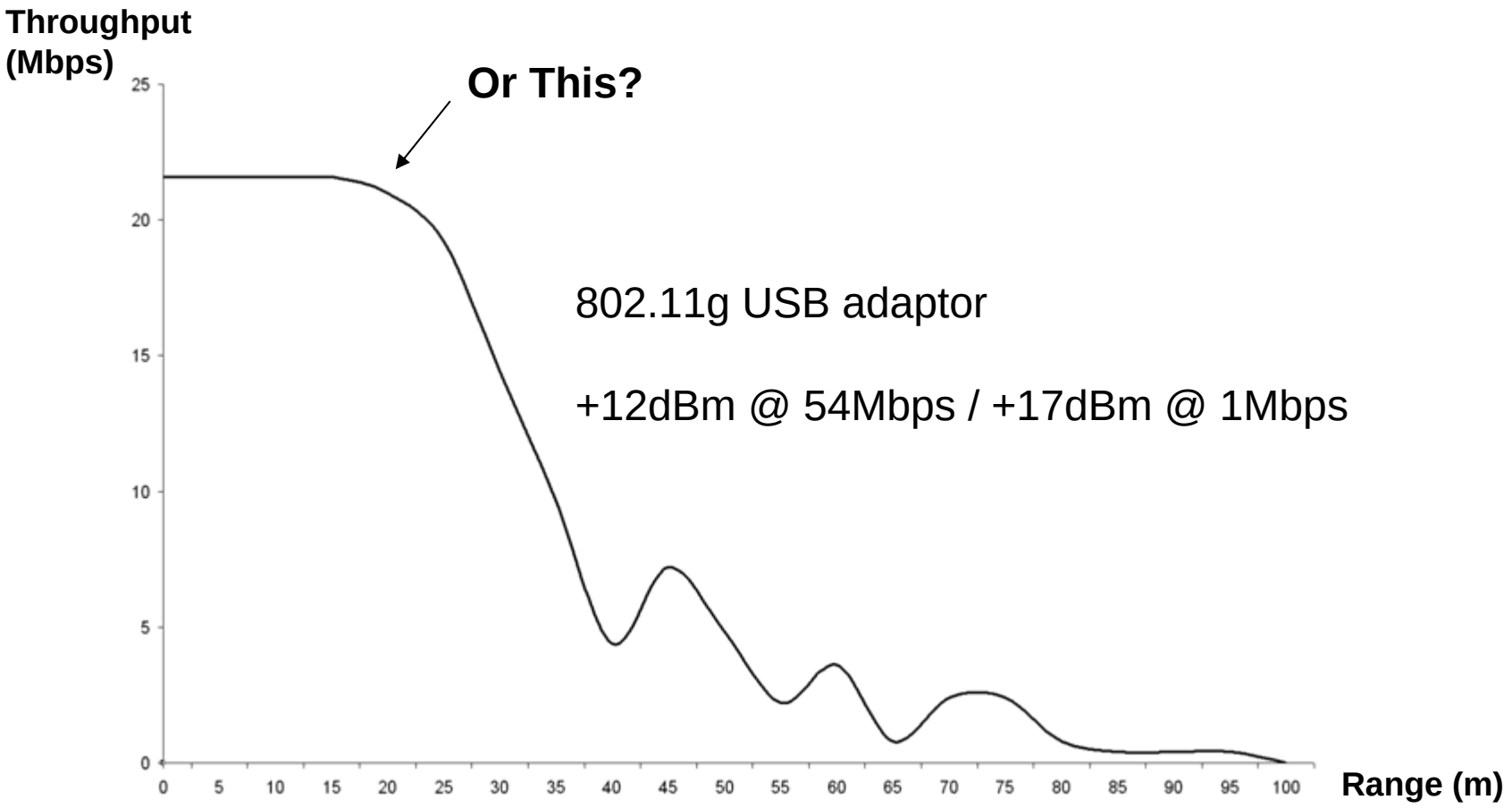
What do we mean by range?

Bluetooth is normally described as having a 10 metre range…

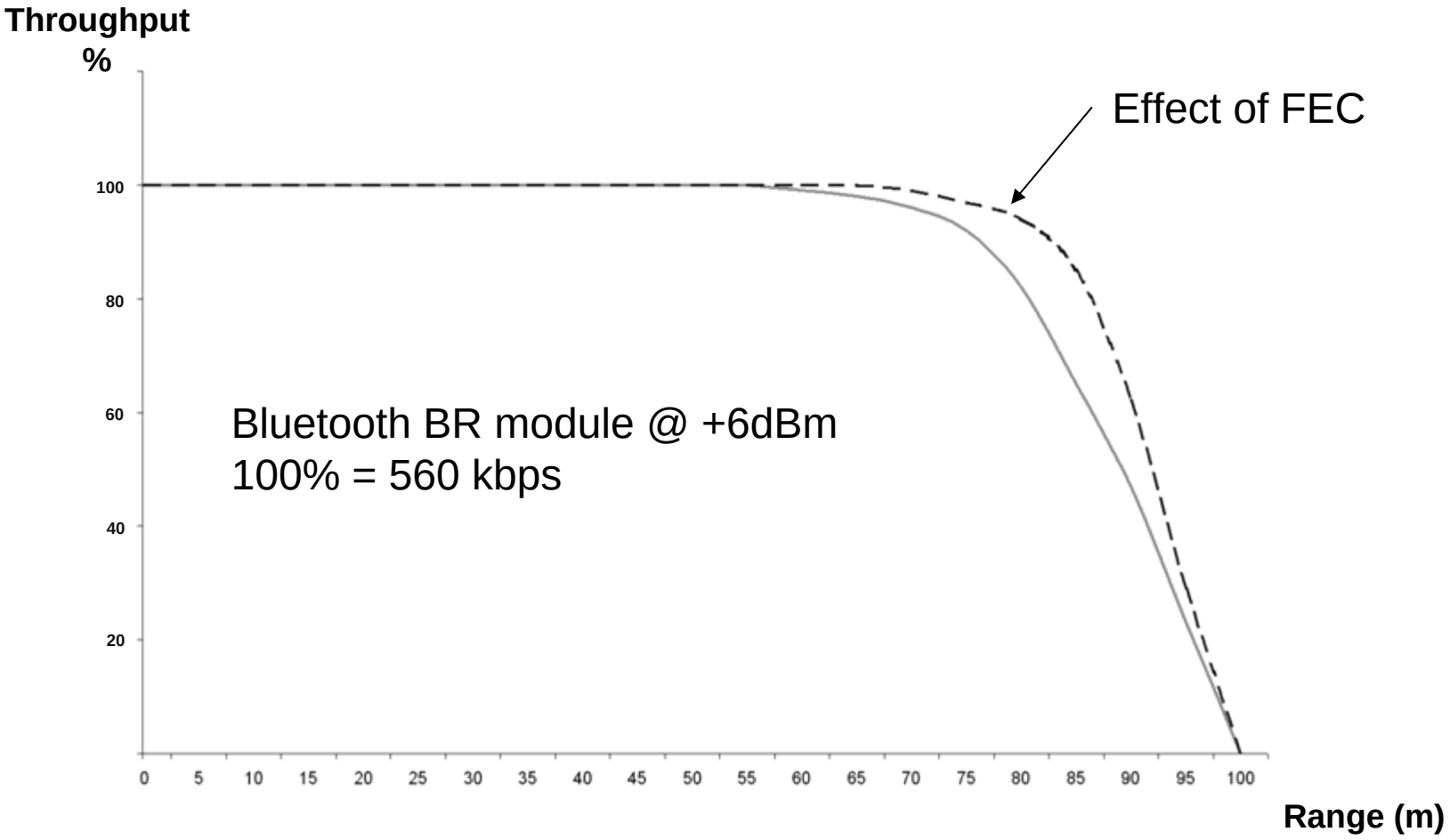


Alternatively…

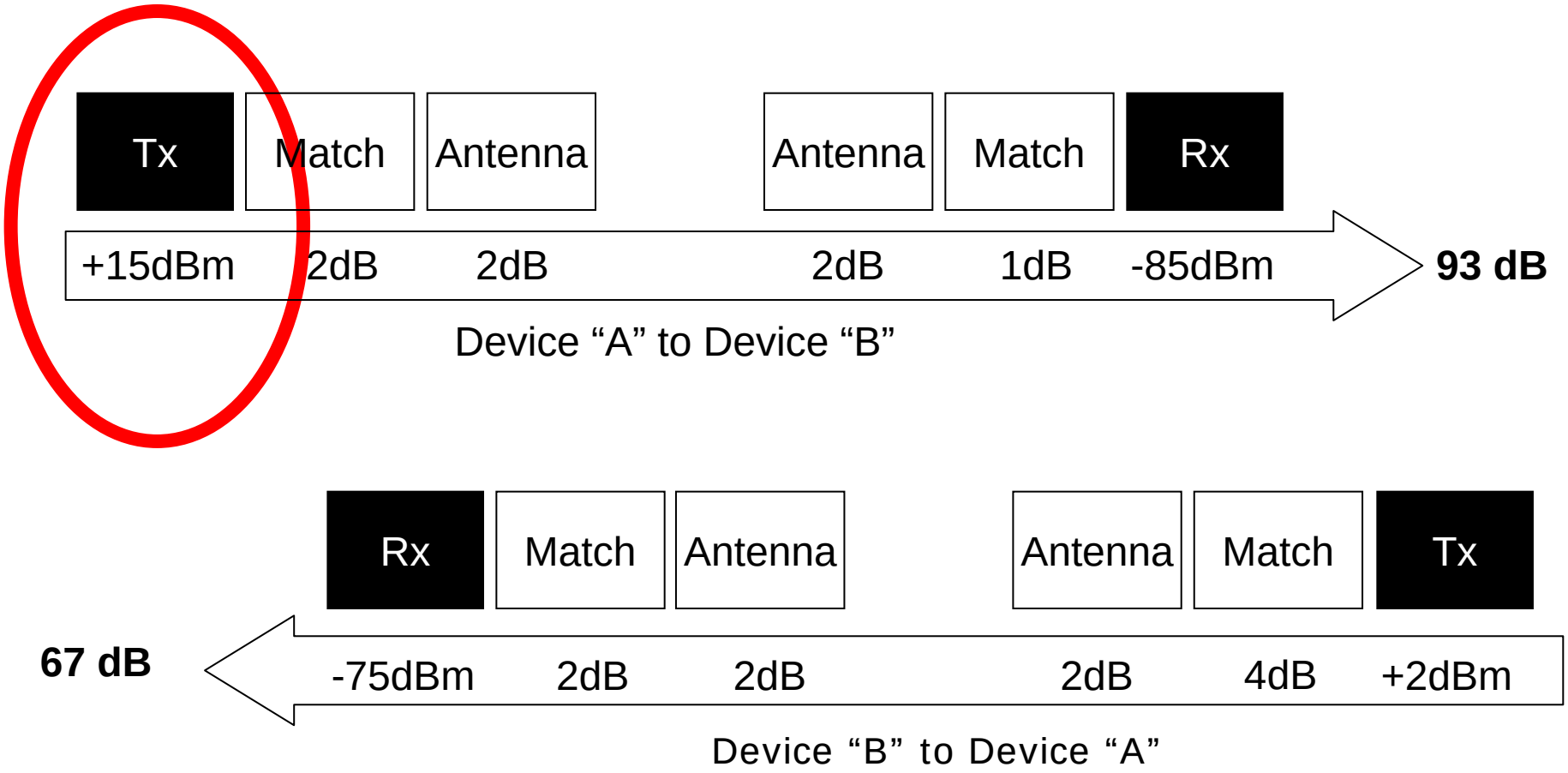
Whereas Wi-Fi is described as having a 100 metre range…



Error correction and coding can have major effects

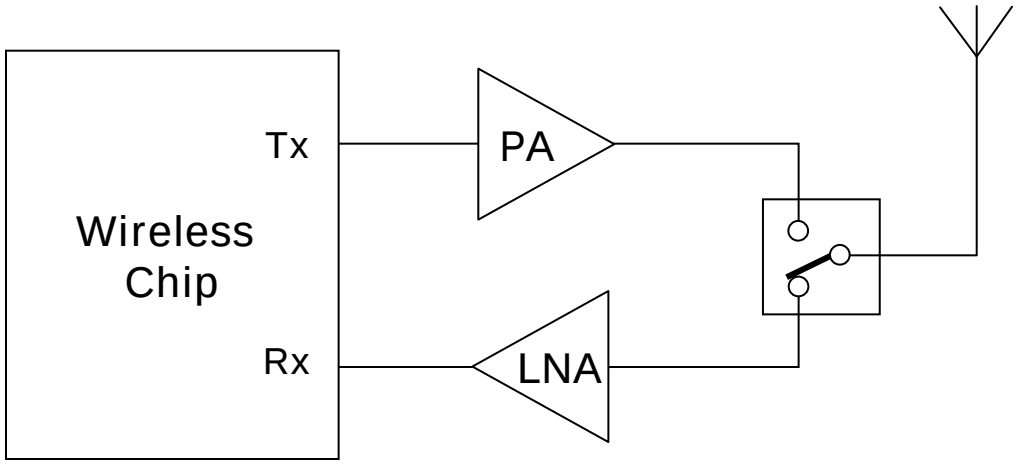


Range – the importance of link budget

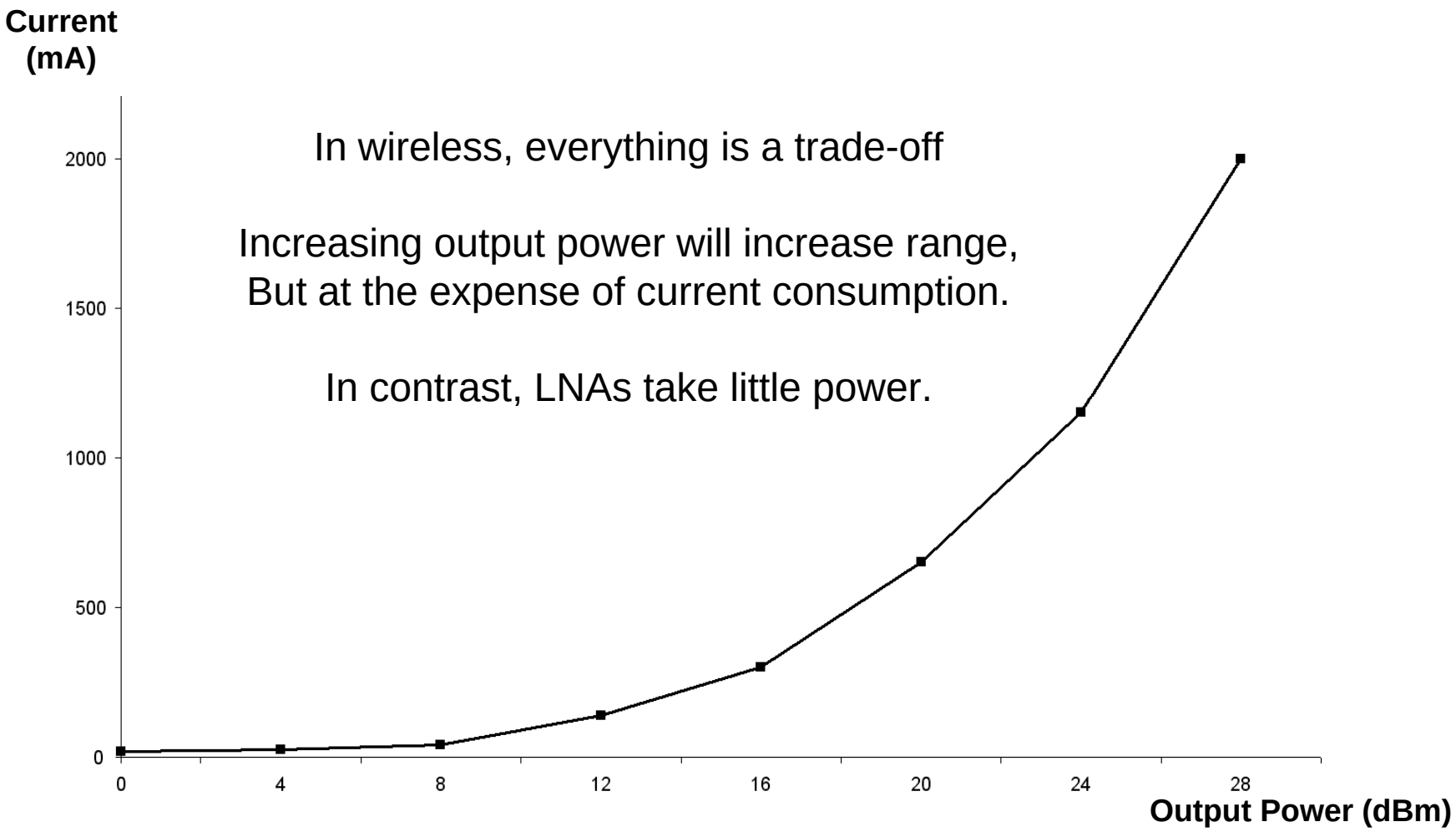


Regardless of topology, the range is determined by the poorer link budget

You can listen better as well as shout…



Range and current consumption



In wireless, everything is a trade-off

Increasing output power will increase range,
But at the expense of current consumption.

In contrast, LNAs take little power.

Basic parameters for the main standards

	Range	**Throughput**	**Latency**	**Current Consumption**	**Relative Cost**	**Secure** (3)
Bluetooth ACL	100m	2 Mbps	50ms	35mA	1	Yes
Bluetooth SCO	50m	64 kbps	10ms	30mA	1	Yes
Bluetooth HS	20m	10 Mbps	200ms	200mA	3	Yes
Bluetooth low energy	100m	50 kbps	3ms	15mA	0.5	Yes
Wi-Fi / 802.11	100m	20 Mbps	200ms	200mA	3	Yes(1)
ZigBee PRO	100m	75 kbps	5ms	25mA	1.5	Yes
ANT	100m	20 kbps	2ms	20mA	1	Maybe(2)

(1) Wi-Fi is not secure in ad-hoc mode. Wi-Fi direct should be.

(2) ANT security is defined in higher layer ANT+ profiles. ANT itself has no security.

(3) Security is determined by the level of hacking. Standards with small numbers of deployed devices don't really know whether they're secure or not.

These are maximum values. Not all can be achieved at the same time.

Security

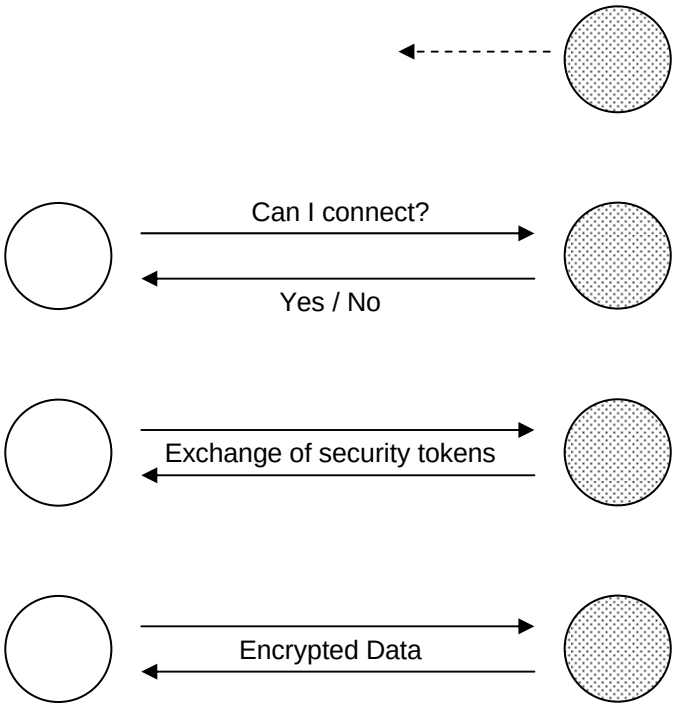
Security processes

Discovery

Authorisation

Authentication

Encryption



Is your standard secure?

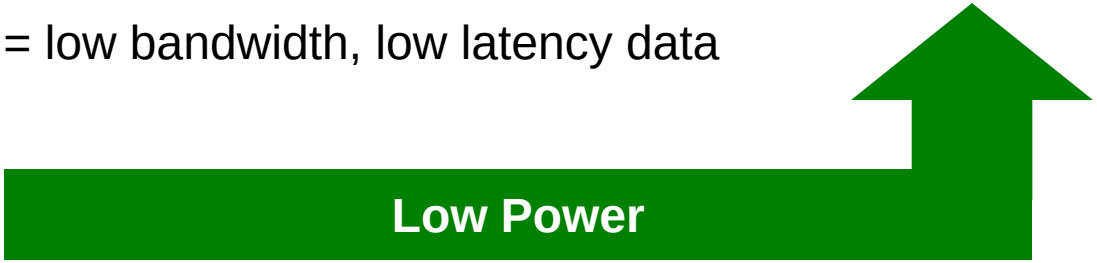
- Bluetooth, Wi-Fi and ZigBee PRO all have respectable security solutions.
- Implementations need to match the latest version of the standard.
- Security is a running battle with hackers, and will remain so.
- Until someone tries to hack it, you don't know whether it is secure.

www.wi-foo.com/ViewPagea038.html?siteNodeId=56&languageId=1&contentId=-1 - Bluetooth hacking tools.
www.wi-foo.com/index-3.html - Wi-Fi hacking tools.
www.willhackforsushi.com/presentations/toorcon11-wright.pdf - ZigBee hacking tools

Application areas

	Voice	Data	Audio	Video	State
Bluetooth ACL / HS	*x*	Y	Y	*x*	*x*
Bluetooth SCO	Y	*x*	*x*	*x*	*x*
Bluetooth low energy	*x*	*x*	*x*	*x*	Y
Wi-Fi	(VoIP)	Y	Y	Y	*x*
Wi-Fi Direct	Y	Y	Y	*x*	*x*
ZigBee	*x*	*x*	*x*	*x*	Y
ANT	*x*	*x*	*x*	*x*	Y

State = low bandwidth, low latency data

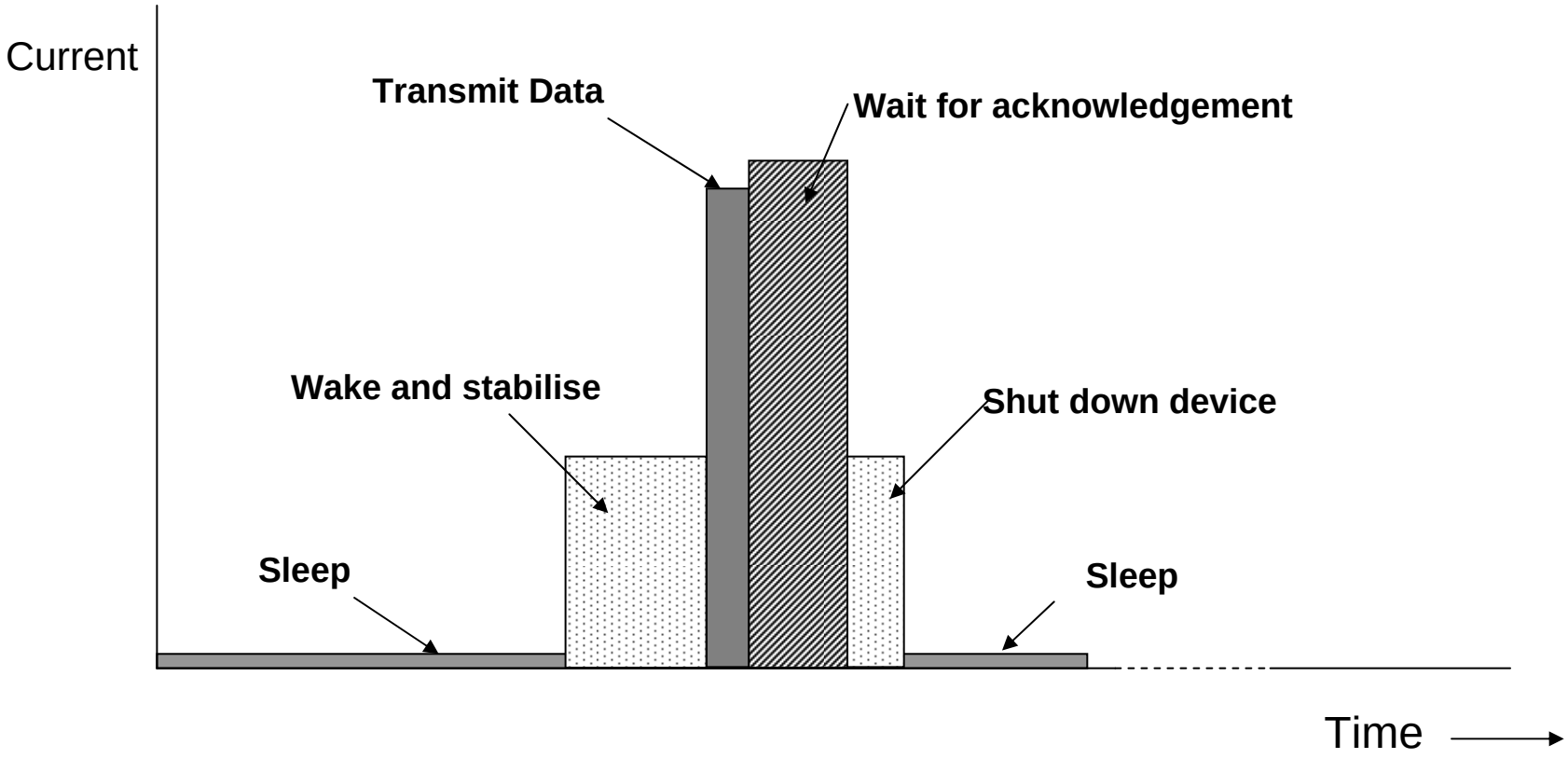


Low Power

Low power

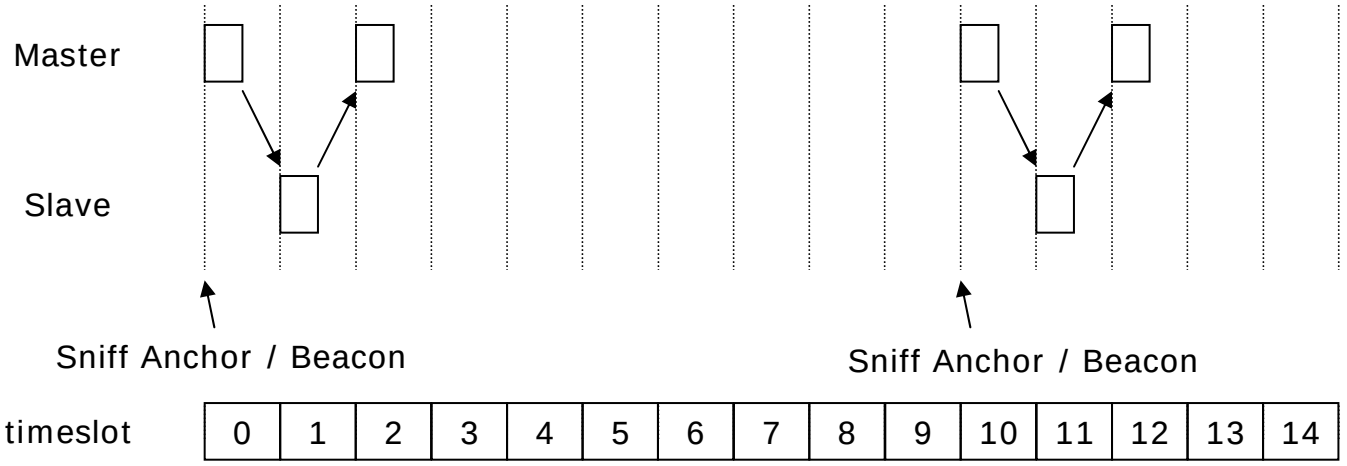
- Low power is the ability to be OFF most of the time.
- Devices are told:
  - When to be awake, or
  - What local event will wake them
- Key is the ability to wake up quickly, perform a transaction and return to deep sleep.
- It’s easier when the link is asymmetric, with one end powered.
- It also means low duty cycles.

Low power – the critical elements



Low power systems strive for a duty cycle where the ON period is less than 1%.

Programmed sleep



The master tells the slave when to wake up,
The slave listens for information or sends data at this point,
The transaction may update the sleep / sniff / beacon interval, then
The slave goes back to sleep.
Sniff subratings allow the slave to skip some events.

Get the power hierarchy right

In a well designed system, with low duty cycle, the power budget may look like this:

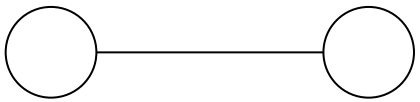
Battery Leakage	10%
Sleep Current	45%
Application	30%
Wireless Link	15%

Designing the power management and getting it right can be as challenging as designing the radio.

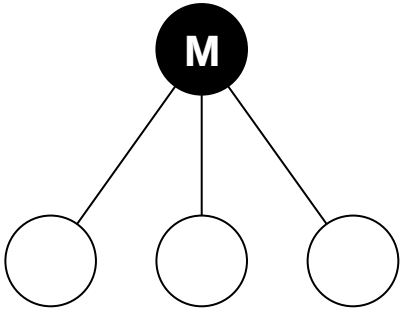
It does not come as part of the wireless standard – you need to design it into your product.

Topologies

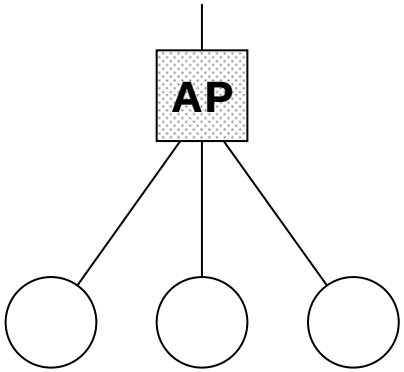
Simple topologies



Point to Point (cable replacement)



Point to Multipoint (piconet)



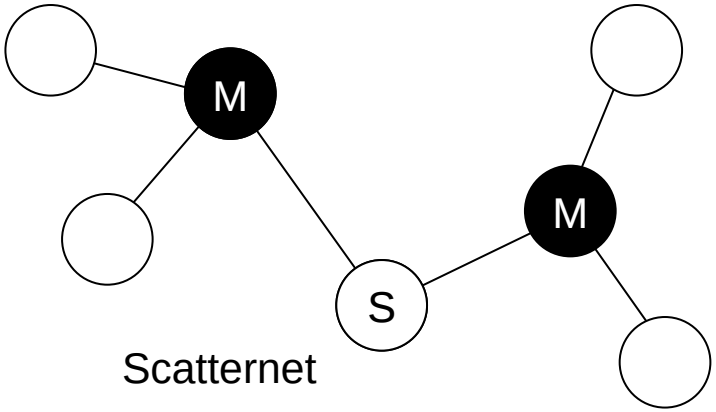
Point to Multipoint (infrastructure)

Maximum Connections per node

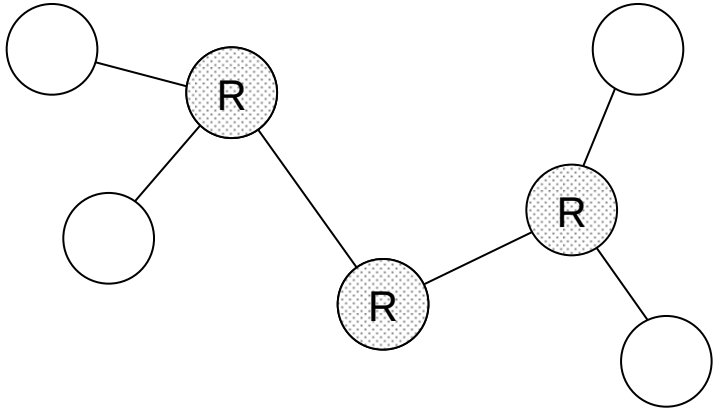
Bluetooth technology	802.11 / Wi-Fi	802.15.4 / ZigBee	Bluetooth low energy	ANT
7	255	20	2 billion	2 billion

In practice, the limit is generally determined by memory constraints

Linear topologies

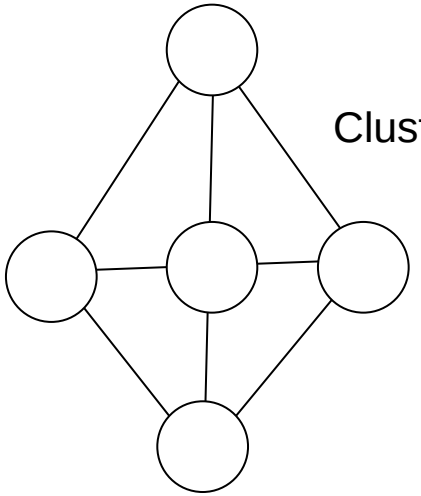


Scatternet

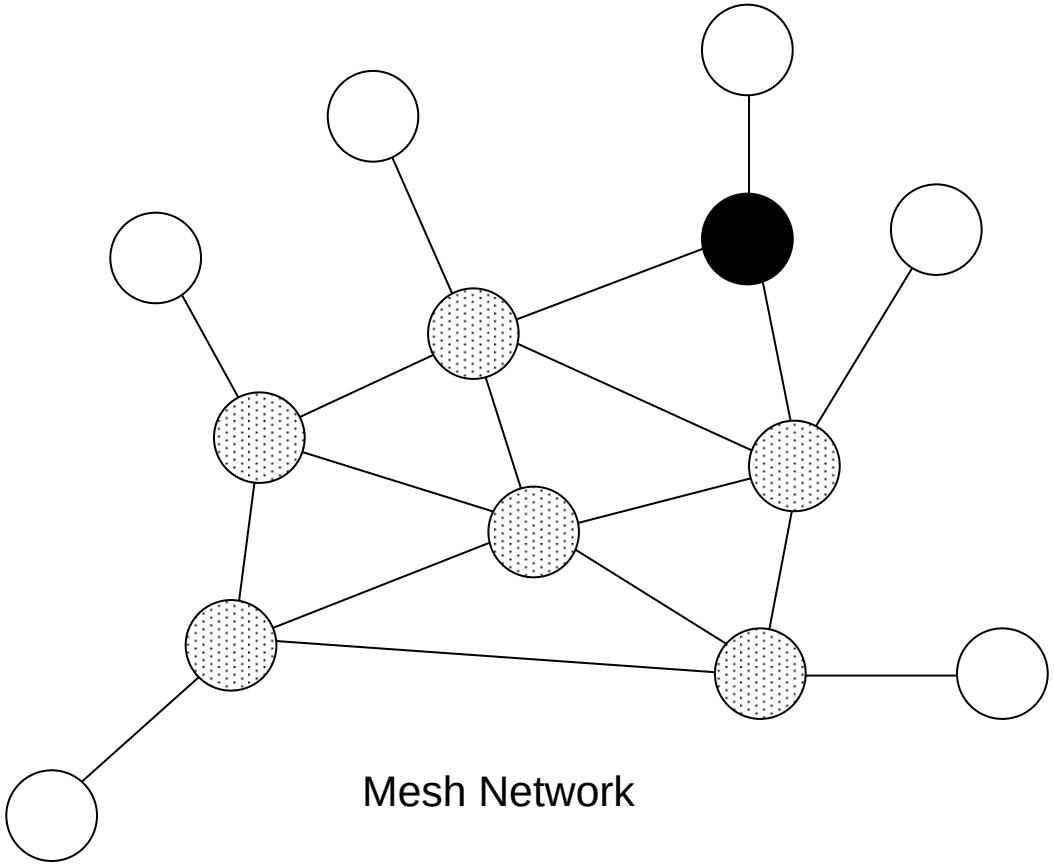


Tree Network

Mesh topologies



Cluster



Mesh Network

Topologies

	Peer-peer	Piconet	Cluster Tree	Infra-structure	Mesh
Bluetooth BR/EDR/HS	Y	Y	(scatternet)	*x*	*x*
Bluetooth low energy	Y	Y	*x*	*x*	*x*
Wi-Fi	(802.11)*	(802.11)*	*x*	Y	x
Wi-Fi Direct	Y	Y	*x*	*x*	x
ZigBee	Y*	Y	Y	*x*	Y
ANT	Y*	Y	Y	*x*	*x*

* Limited security in this topology

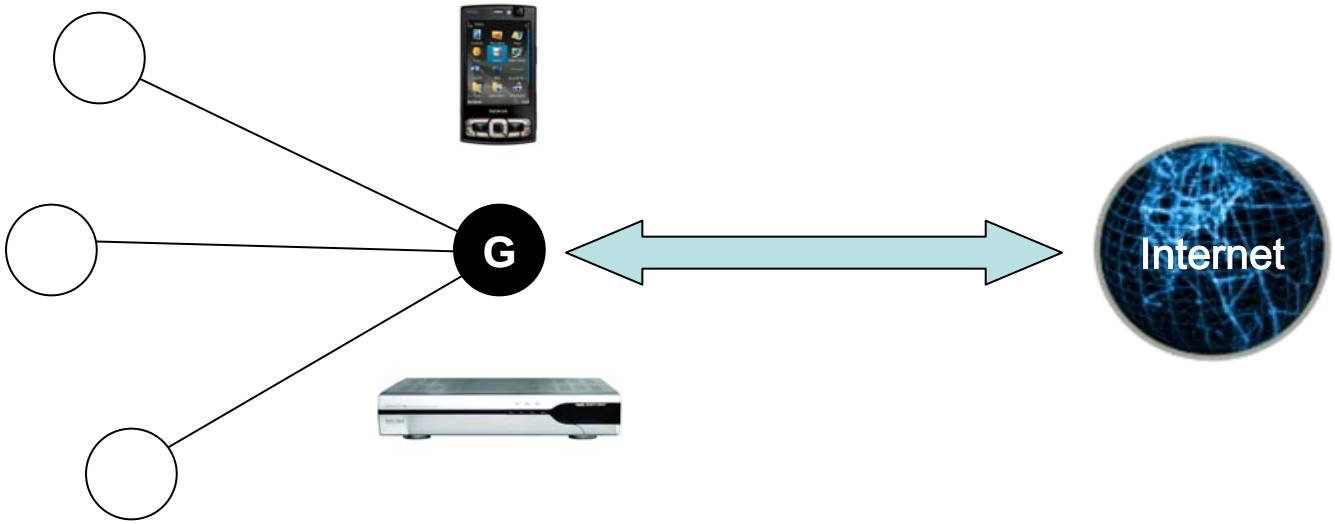
Most applications are still cable replacement (peer-peer) or infrastructure.

New markets imply new topologies

	TAM	Topology
• Phone accessories	> 10 billion	P2P / Gateway
• Smart Energy (meters & displays).	~ 1 billion	Gateway Hub
• Home Automation	> 5 billion	Gateway / Mesh
• Health, Wellness, Sports & Fitness	> 10 billion	P2P / Gateway
• Assisted Living	> 5 billion	Gateway
• Animal Tagging	~ 3 billion	P2P
• Intelligent Transport Systems	> 1 billion	?
• M2M (Internet connected devices)	> 10 billion	Gateway

Over 90% of the next 50 billion wireless devices may use a gateway topology

The gateway topology

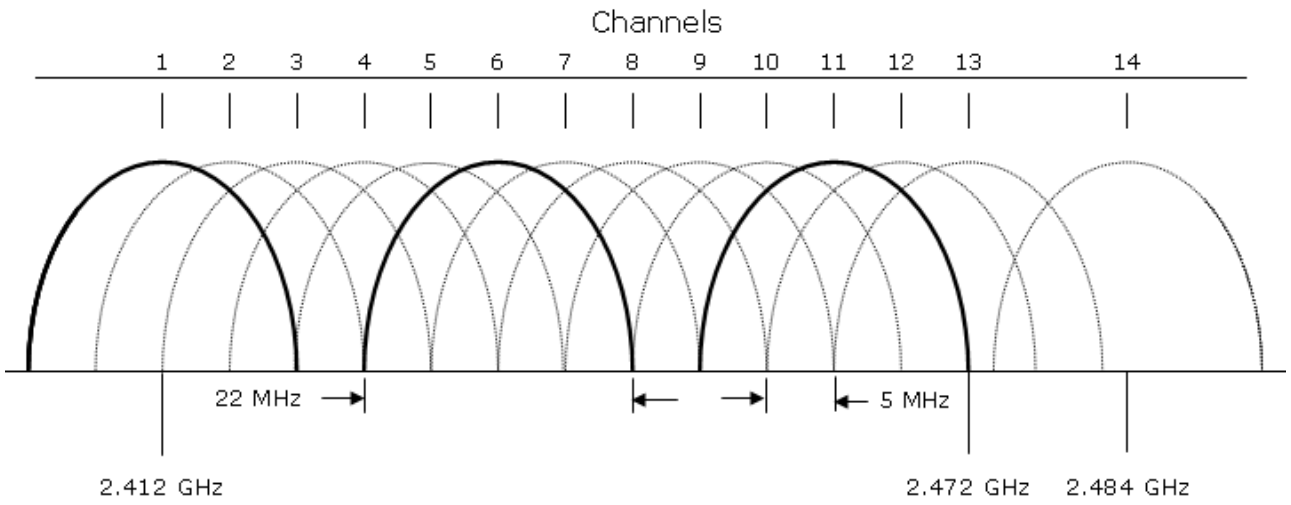


- Devices talk through gateways to web apps.
- They can cause specific apps to be loaded on a gateway device.
- Internet apps talk directly with the device – the gateway is just a tunnel.
- Gateways should be generic to enable interoperability.
- Bluetooth low energy technology supports this better than any other standard.

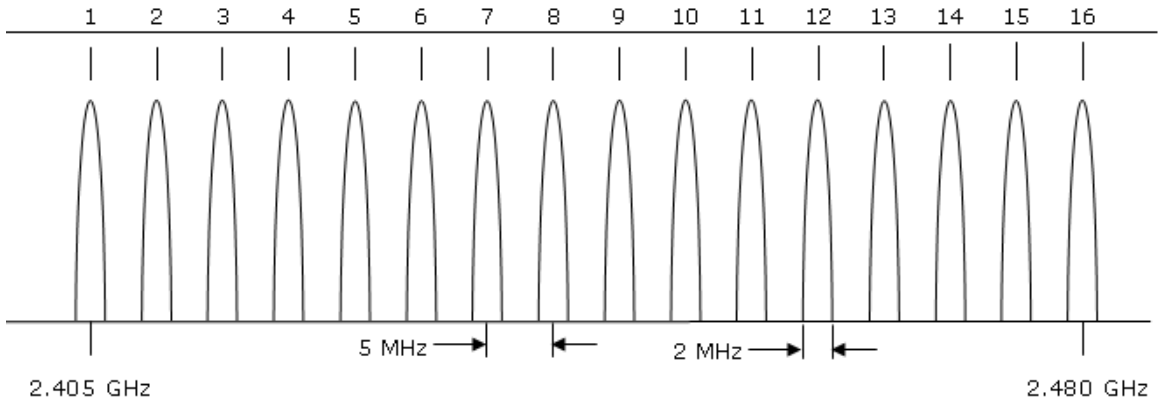
Robustness

Spectral usage – fixed channel standards

802.11
Wi-Fi

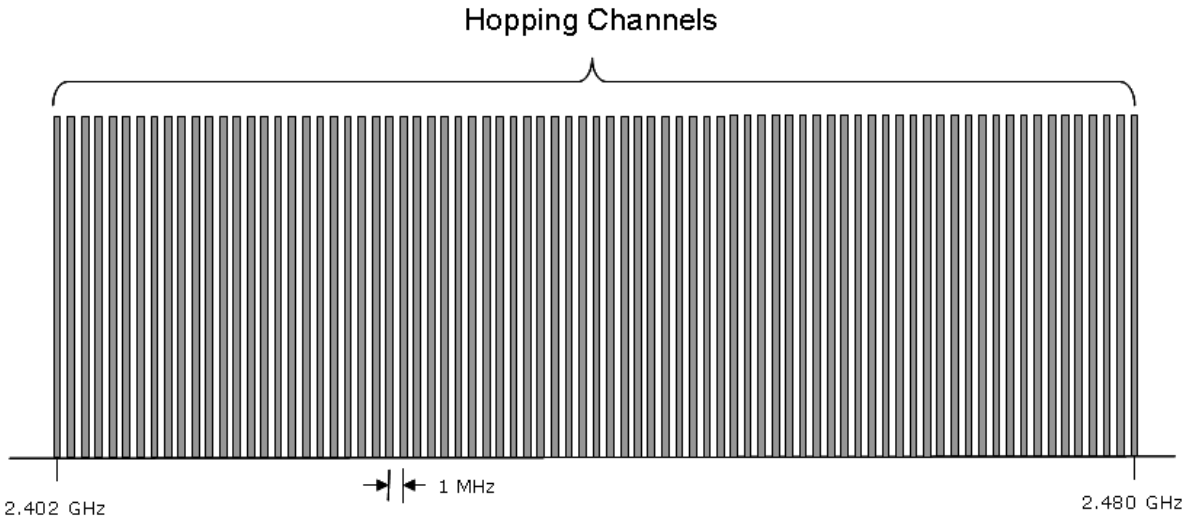


802.15.4
ZigBee

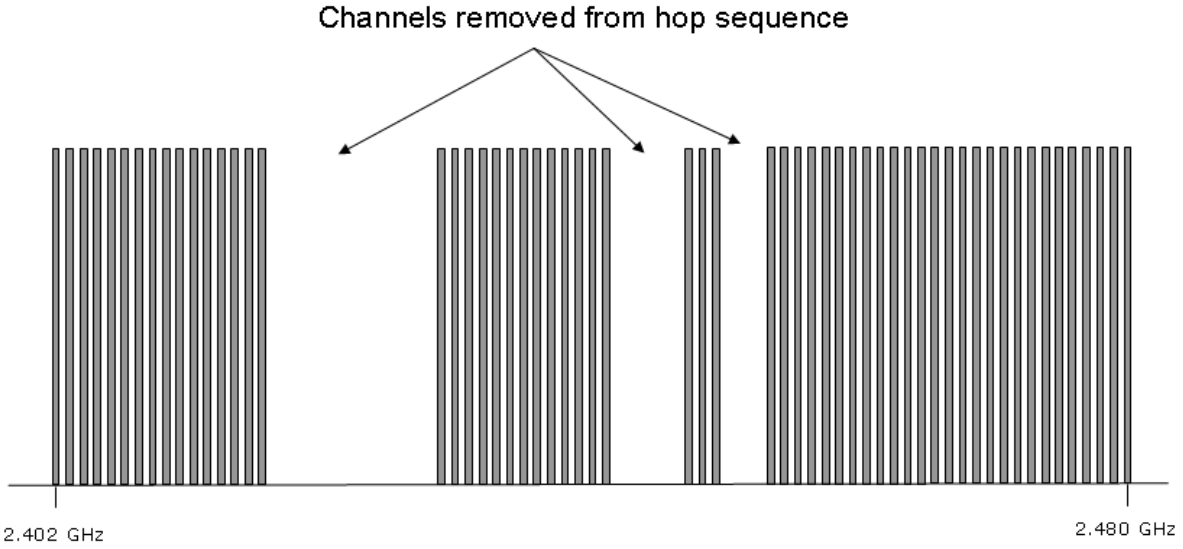


Spectral usage – frequency hopping standards

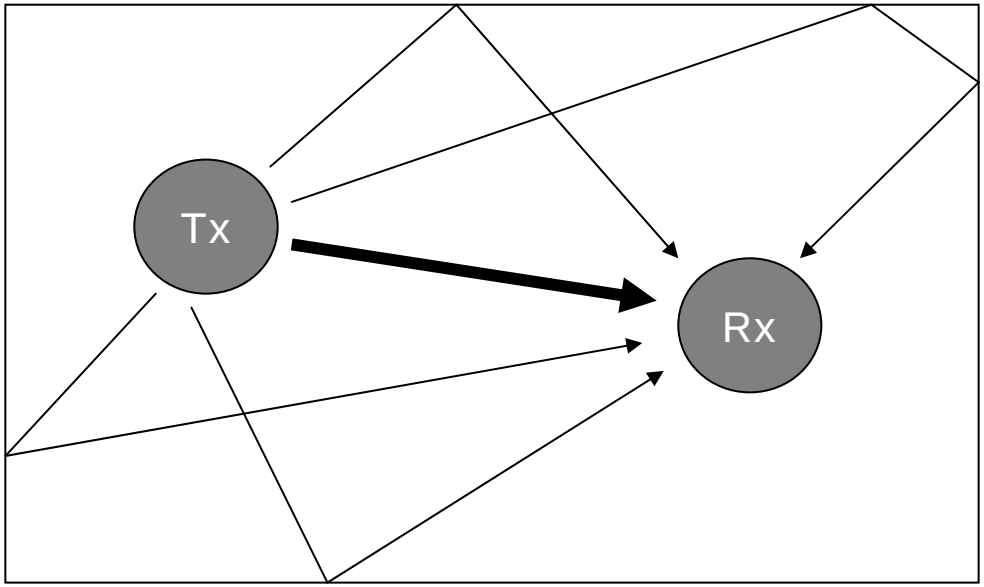
Bluetooth



Adaptive Frequency Hopping



Robustness - multipath



- Multiple reflected signals are also heard by the receiver.
- Frequency Hopping systems exhibit better resilience against multipath loss.
- This is a greater problem where both devices are static.

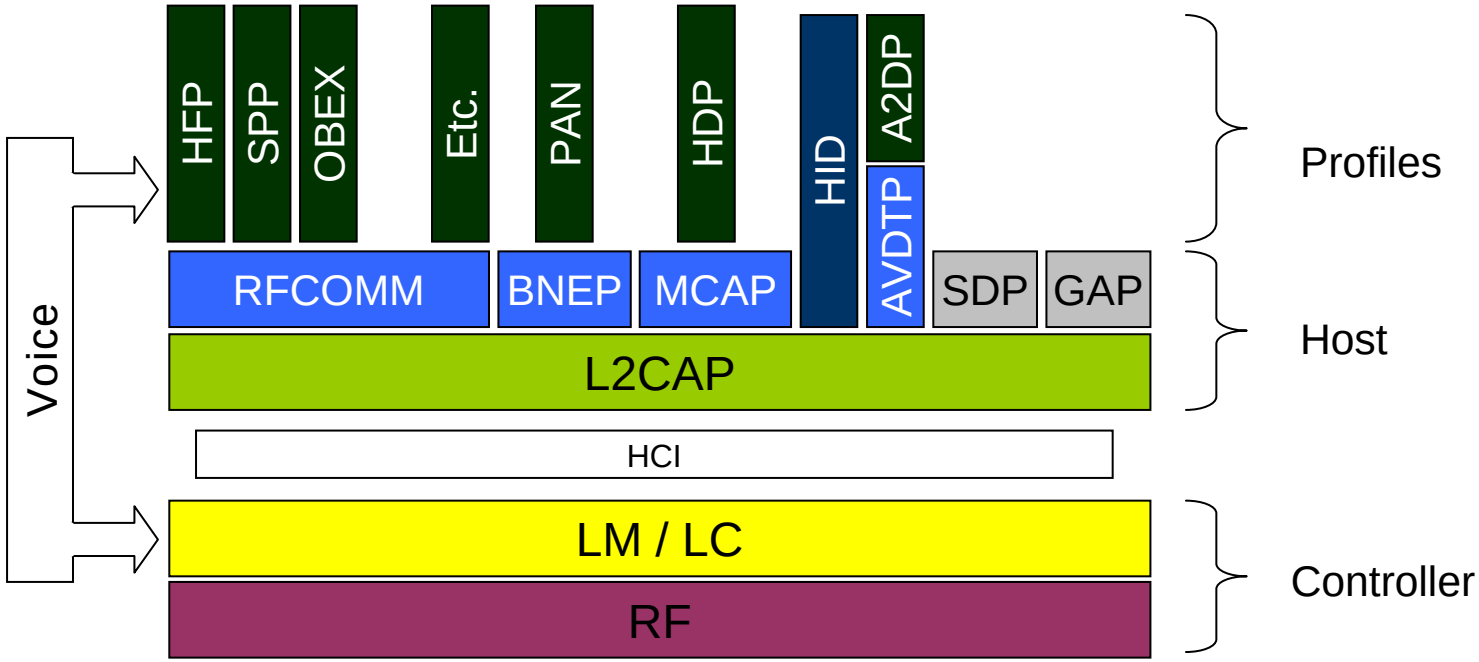
Robustness against interference

	Technique Used	Effectiveness against	
		Interference	Multipath Fading
Bluetooth	Adaptive Frequency Hopping	Excellent	Good
Bluetooth low energy	Adaptive Frequency Hopping	Excellent	Good
Wi-Fi	*None*	*None*	*None*
Wi-Fi Direct	n/a	n/a	n/a
ZigBee	None	*None*	*None*
ZigBee PRO	Frequency Agility (optional)	Limited	*None*

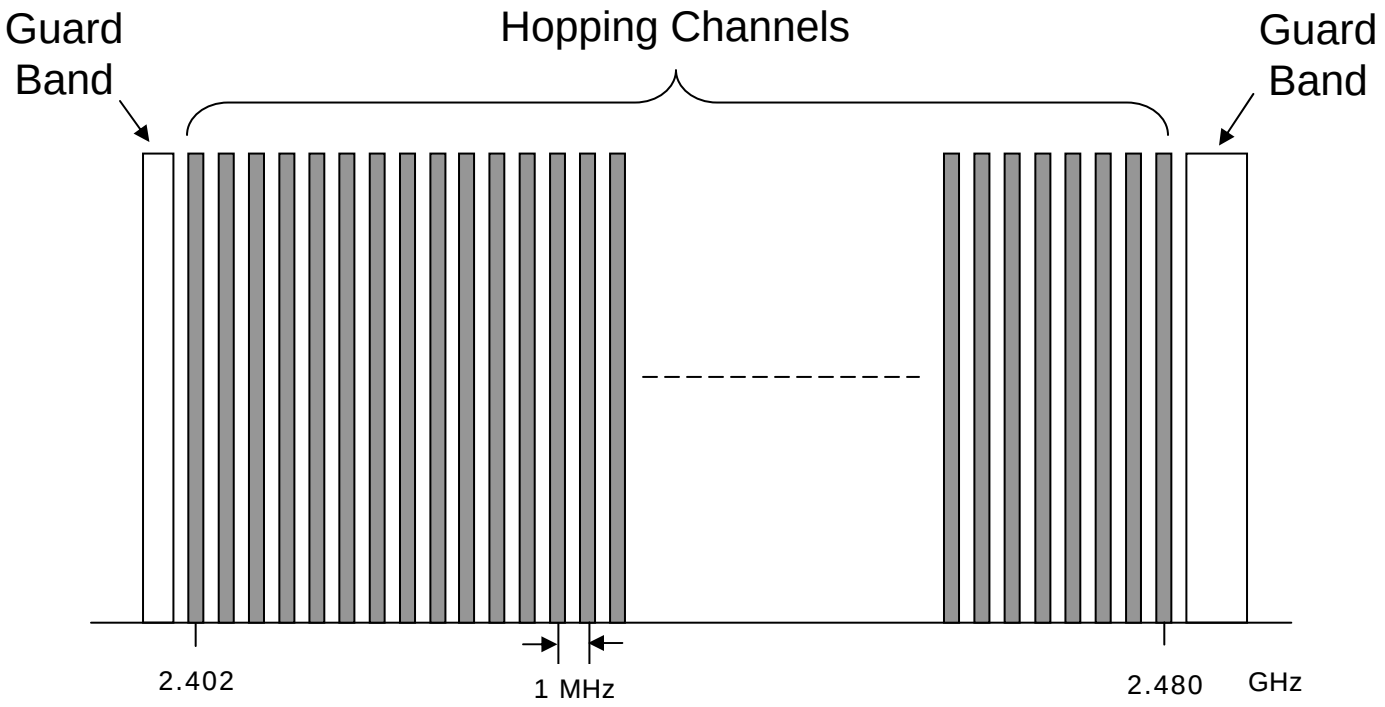
Applications like smart energy need a wireless technology to be robust for a lifetime of 20+ years. That requires adaptive intelligence to cope with conditions over that entire lifetime, not just at the time of installation.

Bluetooth

The Bluetooth stack

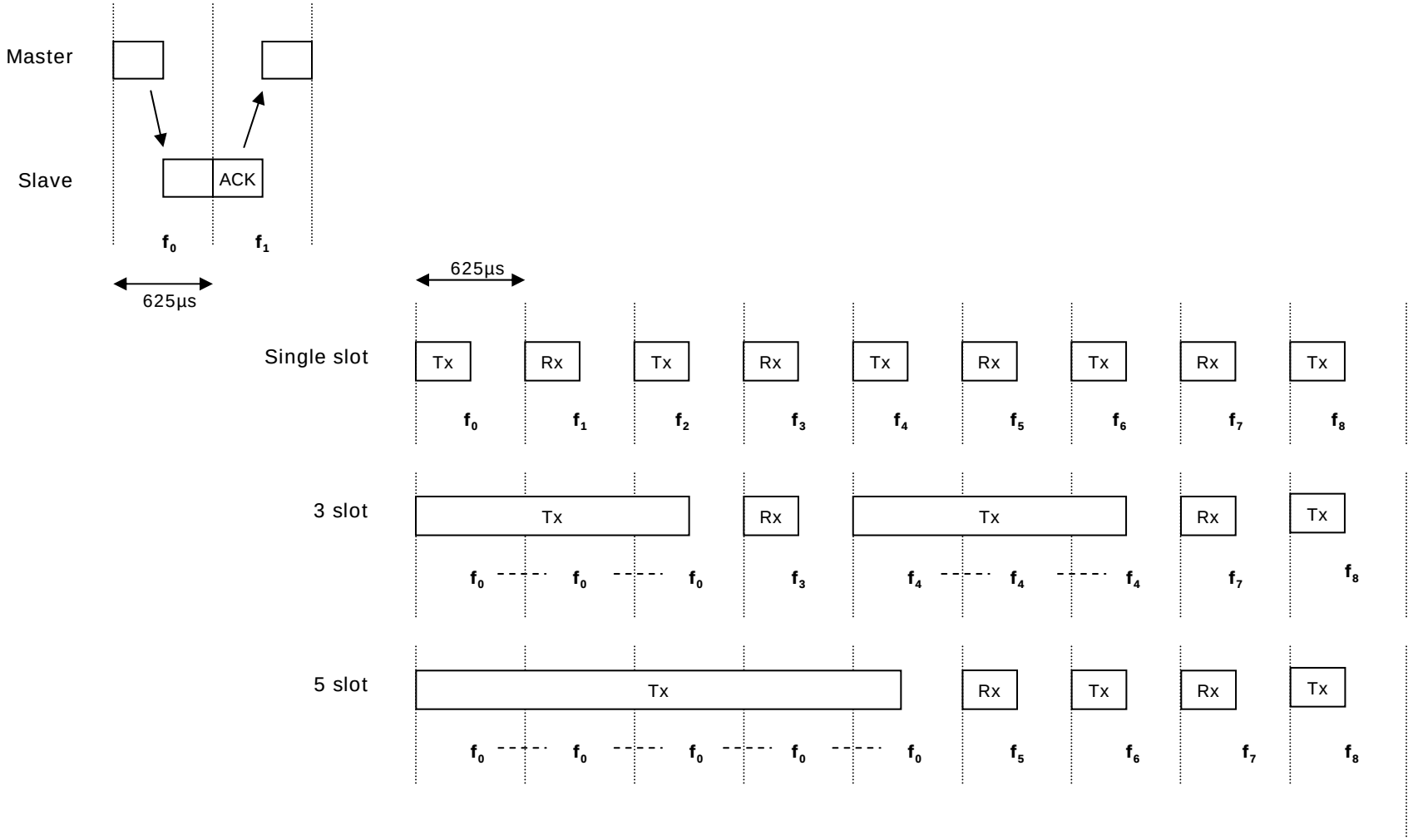


Bluetooth spectral usage

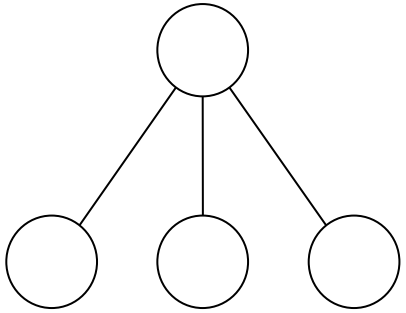


The radio hops 1600 times per second.
Hopping requires precise synchronisation and accurate clocks.

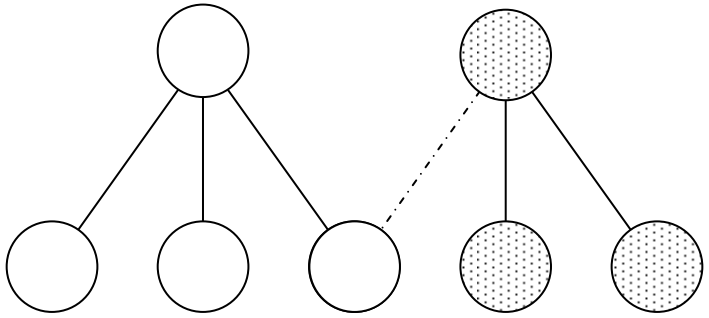
Bluetooth frequency hopping



Bluetooth topologies

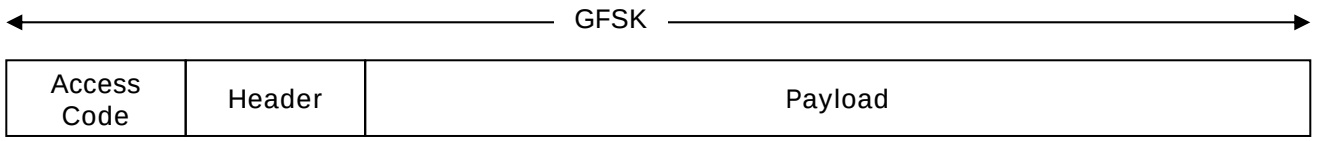


Point to Multipoint
(piconet)

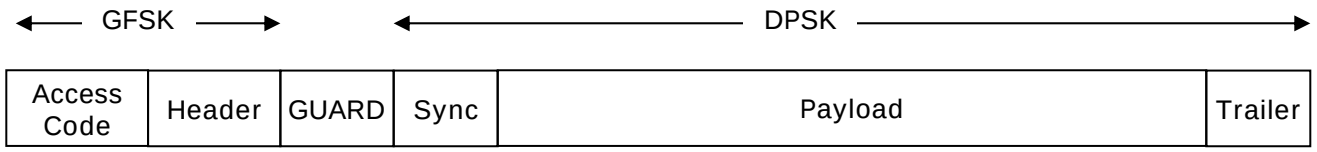


Scatternet

Simplified Bluetooth packet formats



Basic Rate Packet Format (BR) - 1Mbps symbol rate

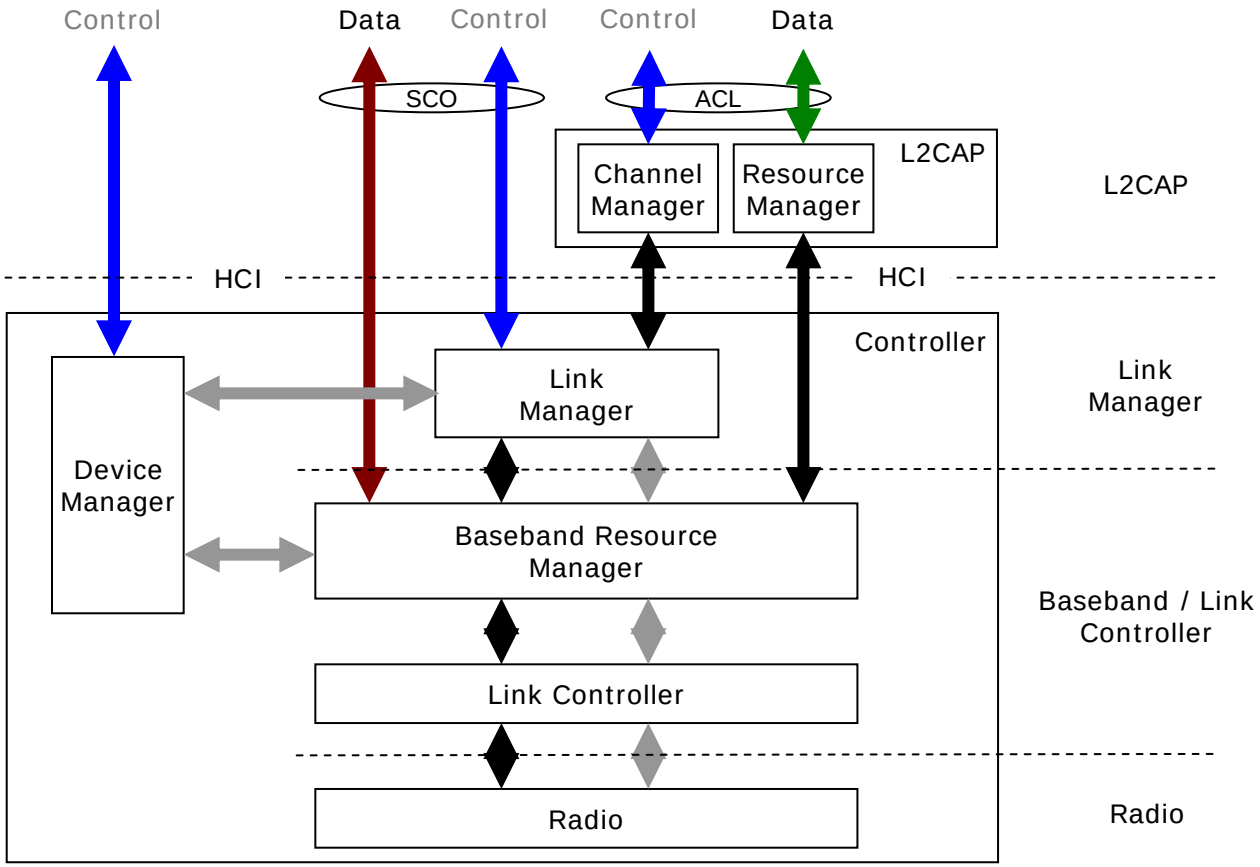


Enhanced Rate Packet Format (EDR) - 2 – 3 Mbps symbol rate

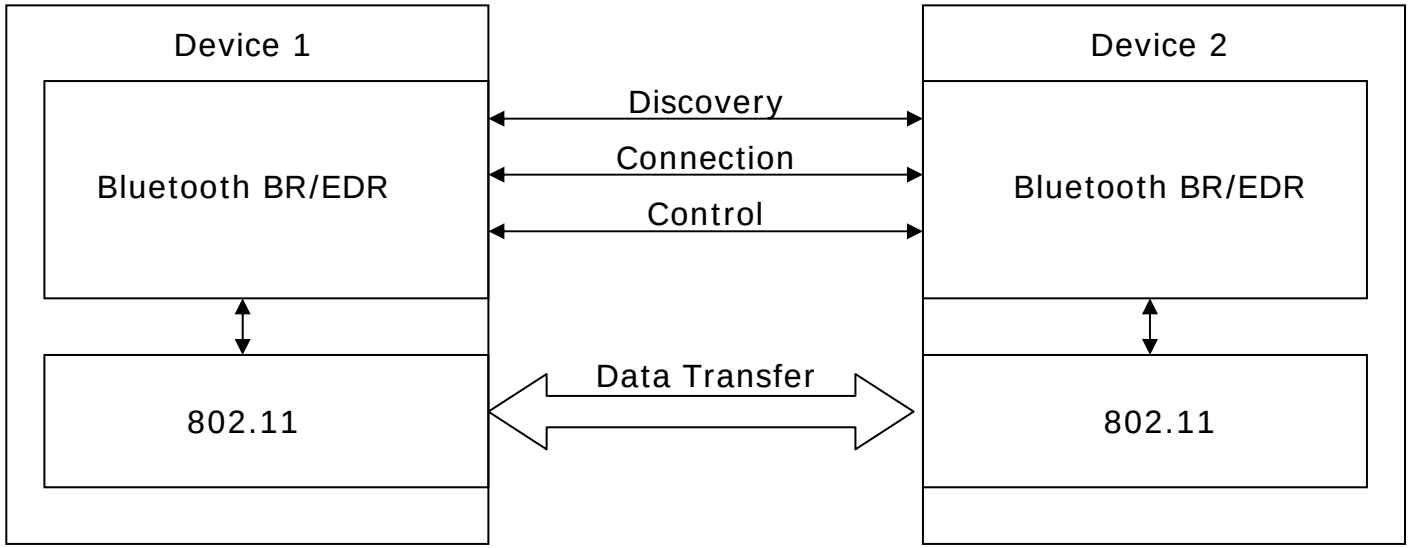
Packet types support:

- Asynchronous Connections (ACL) for data
- Synchronous Connections (SCO) for voice

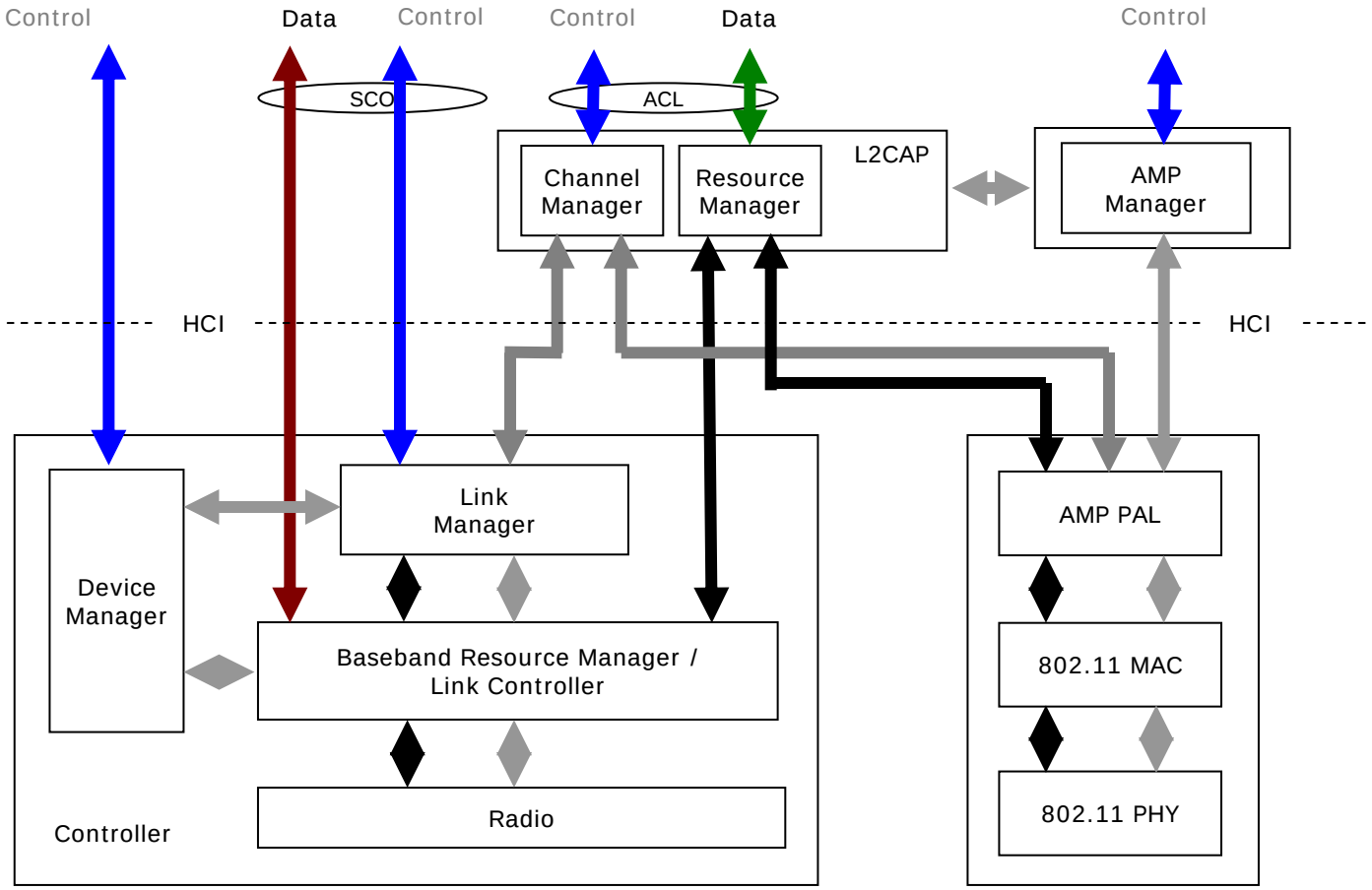
Control and data architecture



Bluetooth 3.0 – adding high speed



Bluetooth 3.0 – architecture

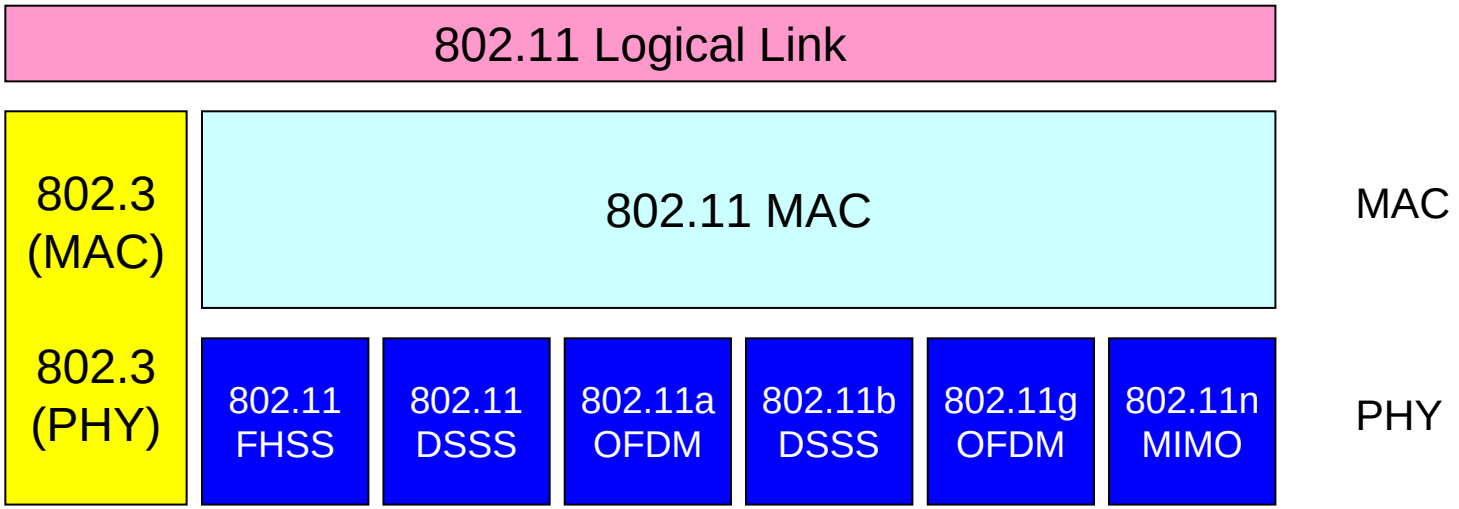


Profiles

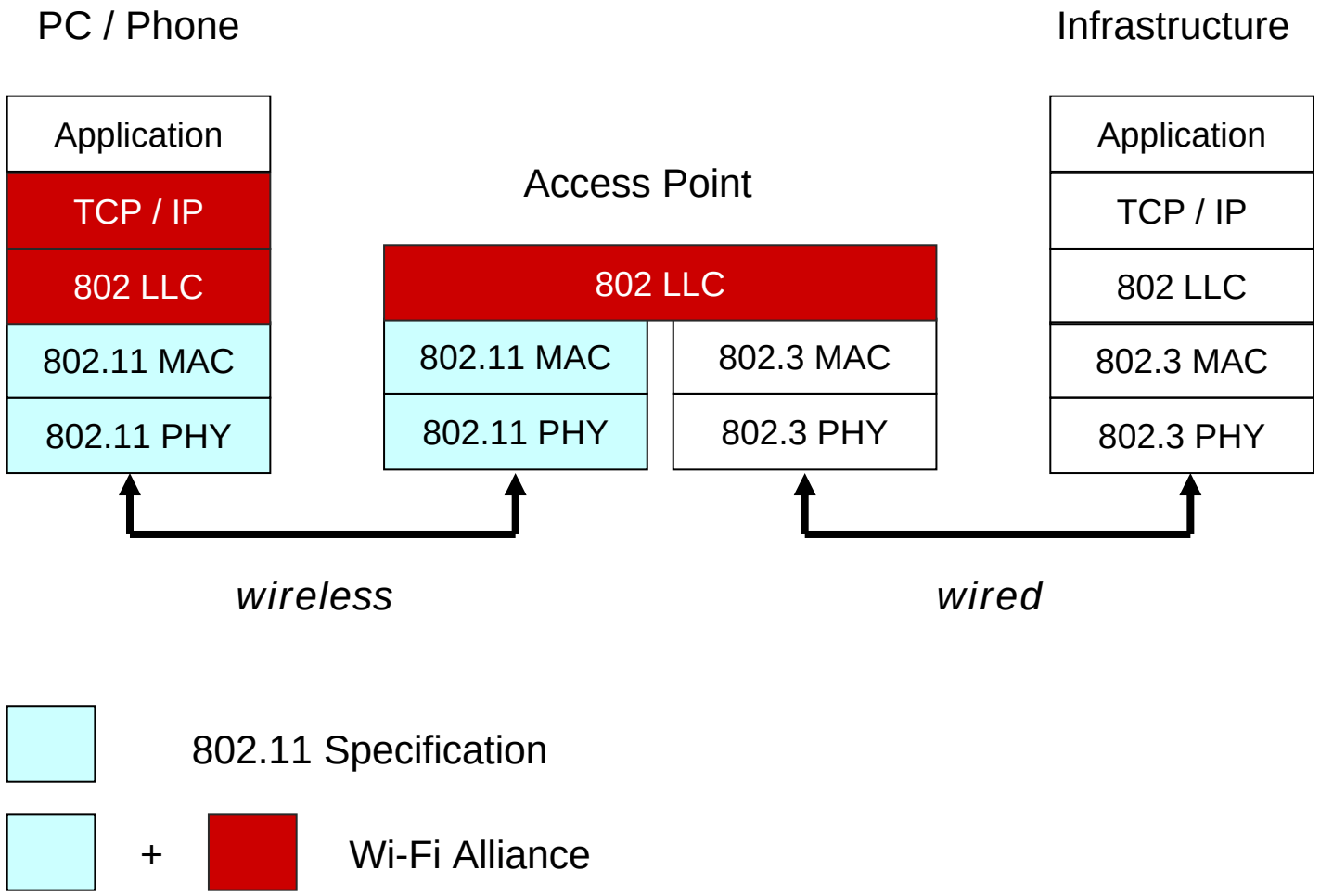
- Profiles provide application layer interoperability
  - Very few different profiles are used
    - Serial Port Profile (SPP)
      - Emulates an RS232 port. No application interoperability.
    - Hands Free Profile (HFP)
      - Headsets (supersedes Headset Profile) and voice applications.
    - Human Interface Profile (HID)
      - Mice, Keyboard, Gaming. Good for low latency and low power.
    - Object Exchange Profile (OBEX)
      - Picture and data transfer.
    - Advanced Audio Distribution Profile (A2DP)
      - Stereo Music.
    - Health Device Profile (HDP)
      - Continua Compliant Medical and Health devices

Wi-Fi & 802.11a,b,g,n,etc…

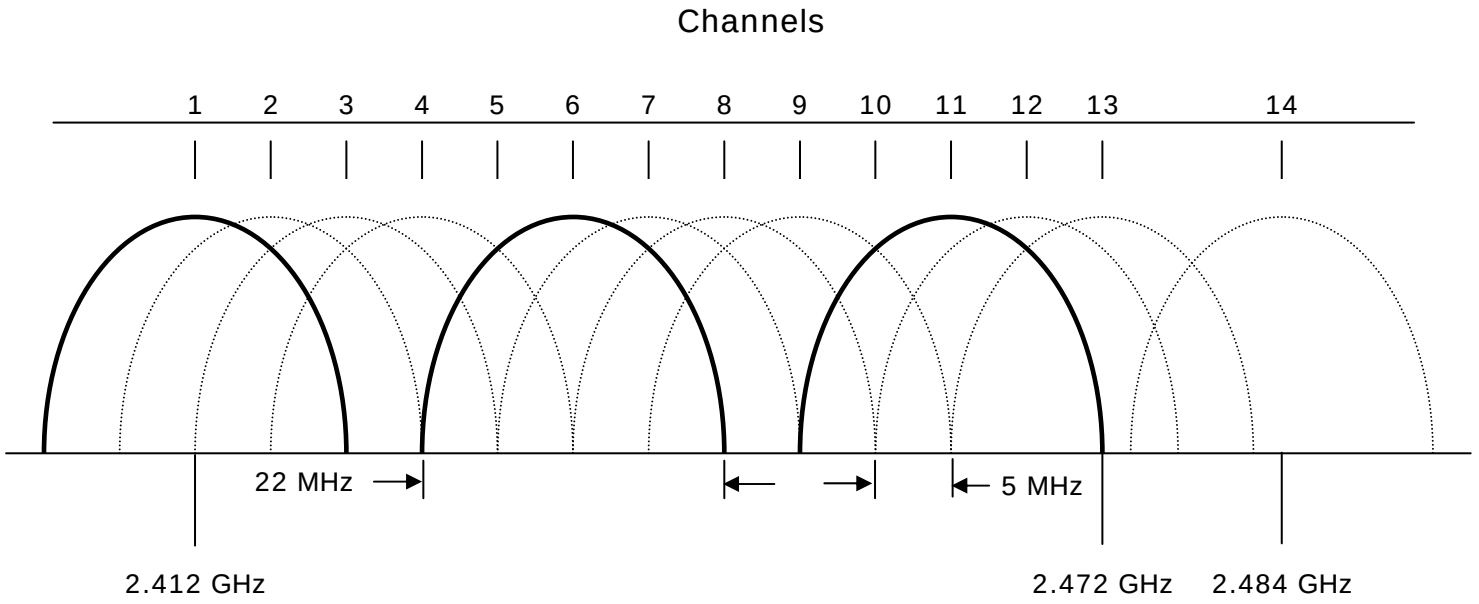
802.11 architecture



802.11, 802.3 and Wi-Fi relationships

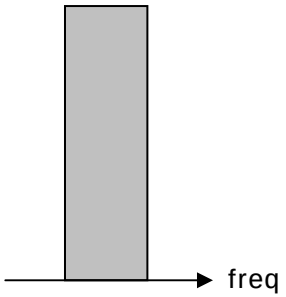


802.11 / Wi-Fi spectrum usage



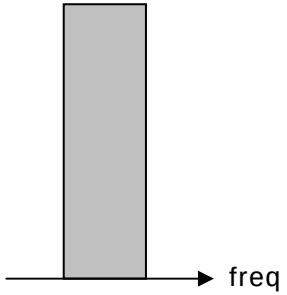
US	Channels 1-11
Europe	Channels 1-13
Japan	Channels 1-14

How DSSS works

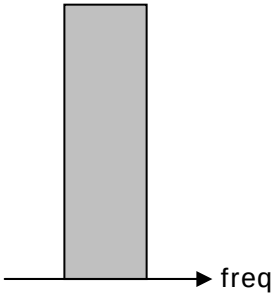


Original Signal

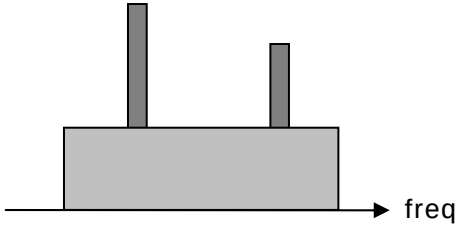
After Spreading



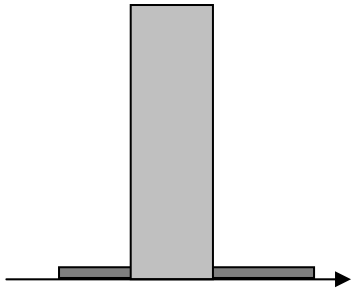
Received signal
after despreading.



Original Signal



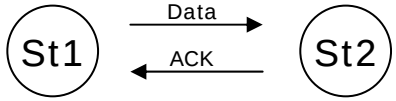
After Spreading,
with noise from
other emitters.



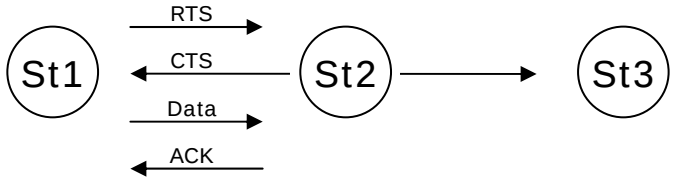
Received signal after
despreading. The original signal
is restored and noise reduced.

Accessing the medium

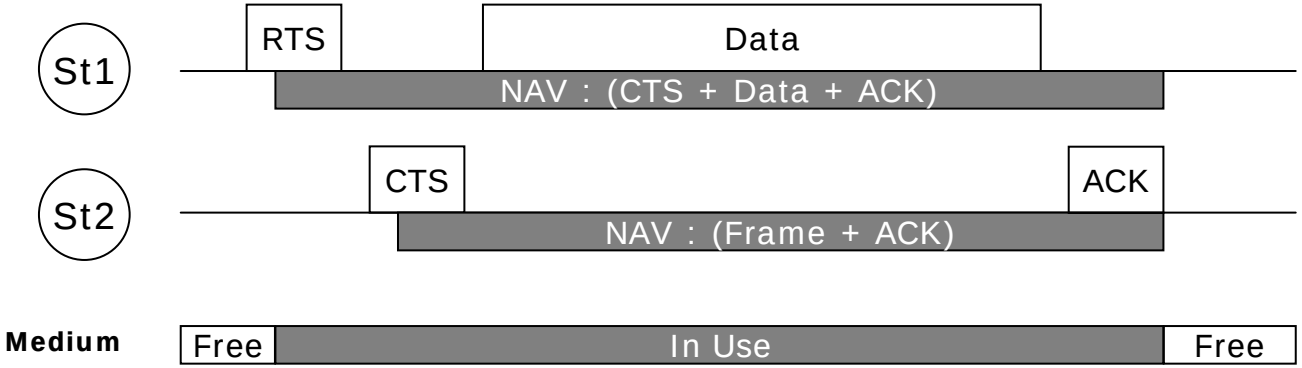
802.11 uses contention access – it needs to know the medium is clear before transmission.



a. Simple Transmission

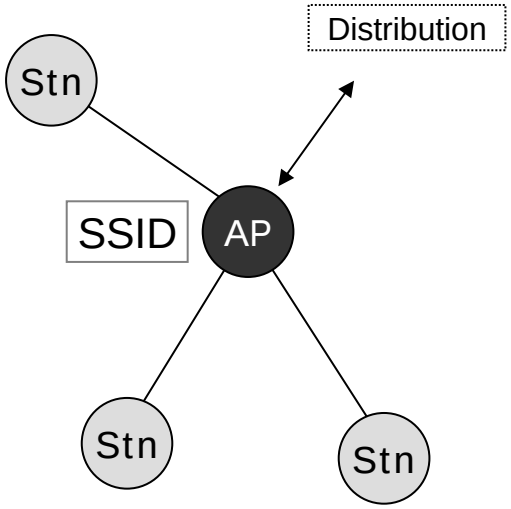


b. RTS / CTS

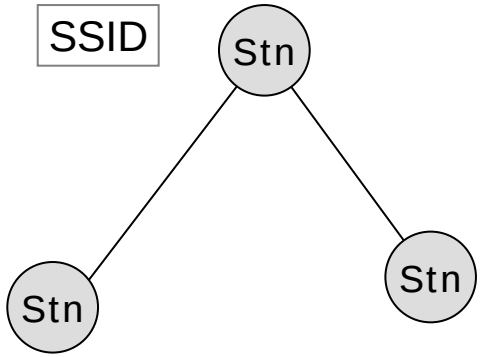


Use of NAV to signal wireless medium availability

802.11 topologies



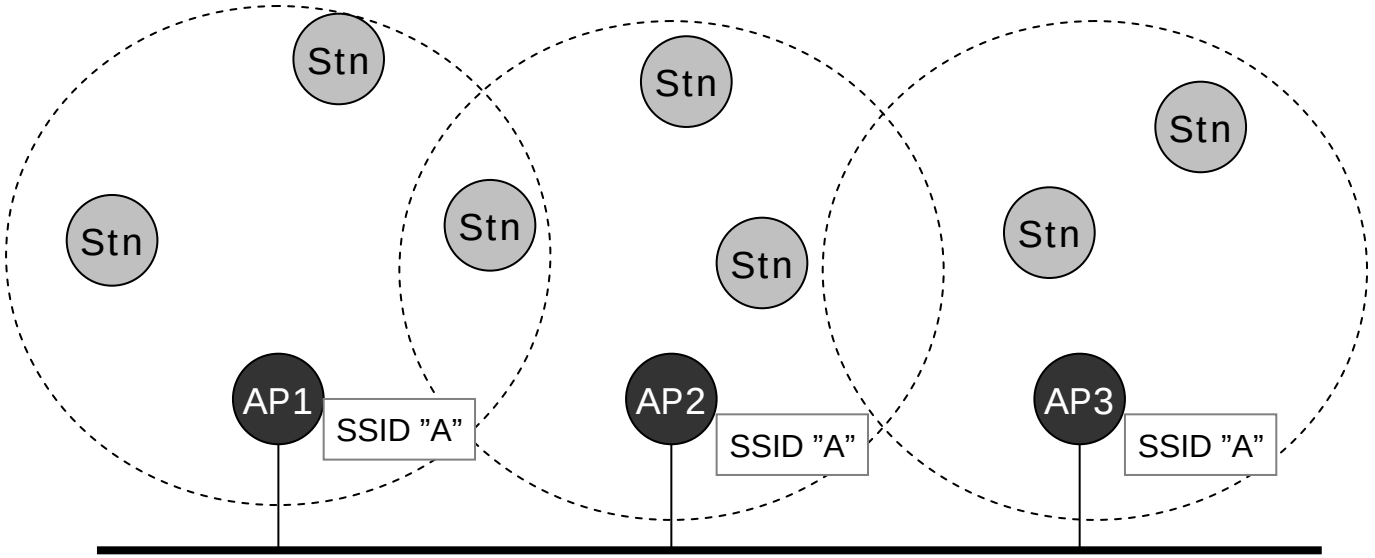
Infrastructure BSS



Independent BSS
(Ad-hoc or IBSS)

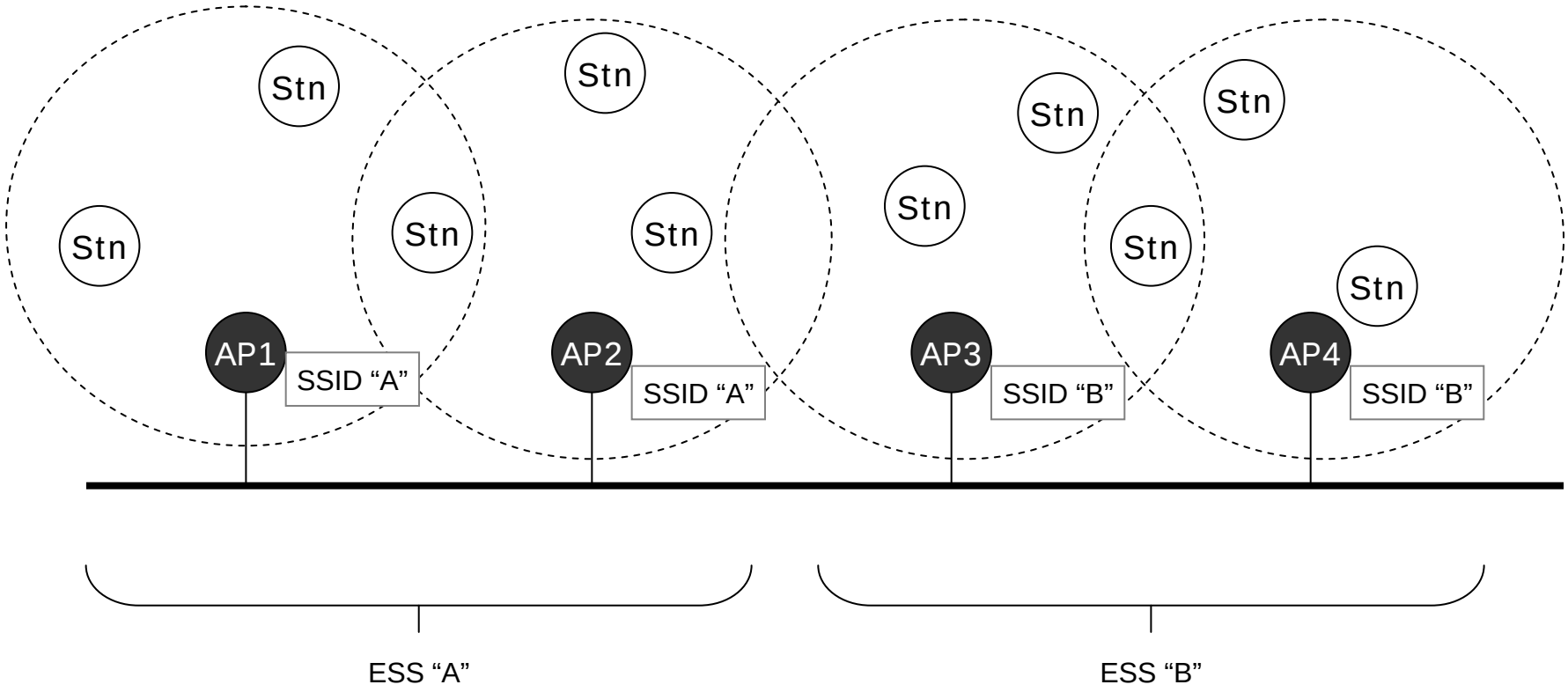
Soon to be Wi-Fi Direct

The extended service set (SSID)



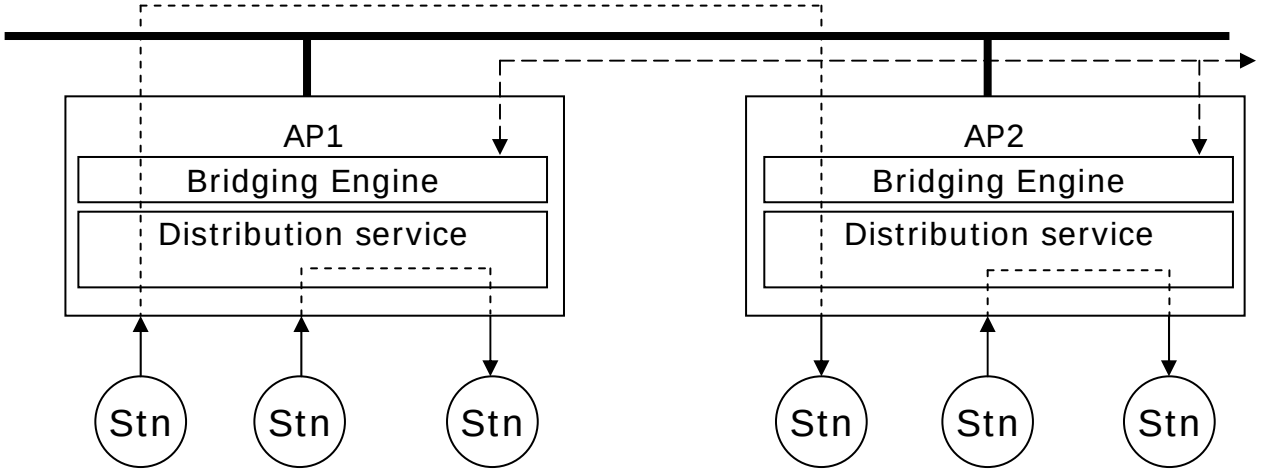
SSIDs are used to identify the access point in a Wi-Fi network.
802.11 displays its heritage as a network standard with a backbone connecting APs.
Outside the corporate office, this is rarely used.

Multiple extended service sets



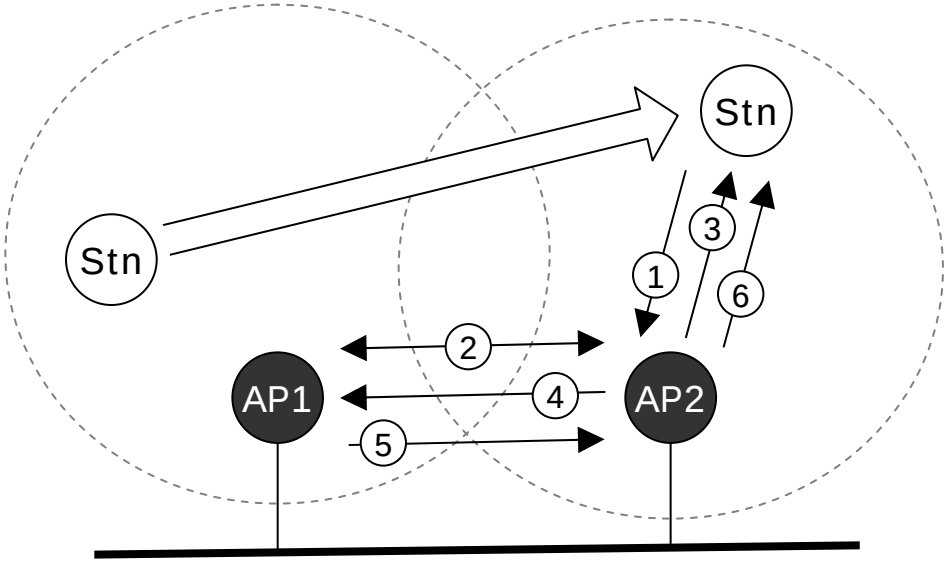
Overlapping Service sets will typically work on non-overlapping channels.

Bridging in an extended service set



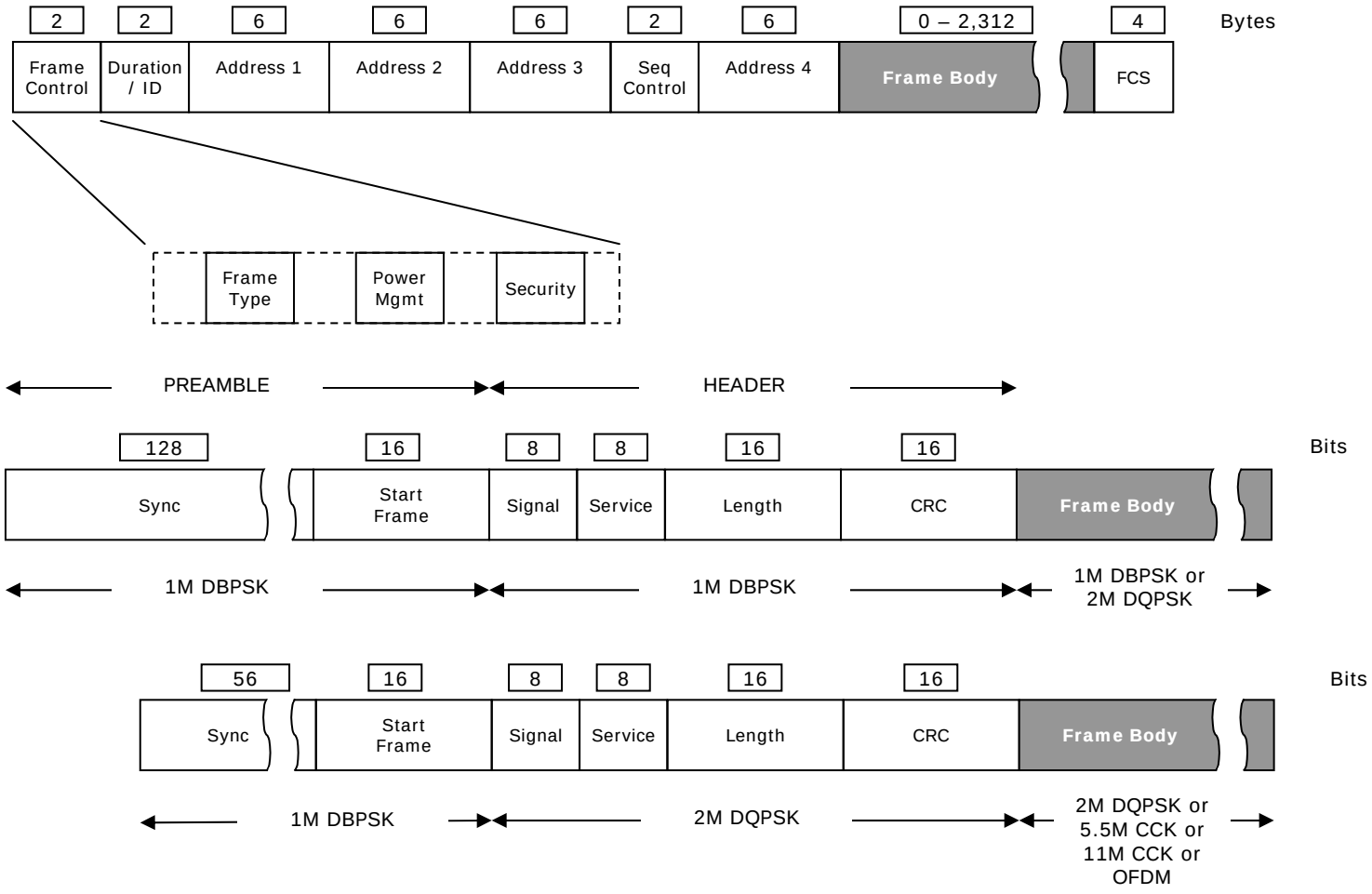
Connected Access Points allow connectivity across them.

Moving between access points

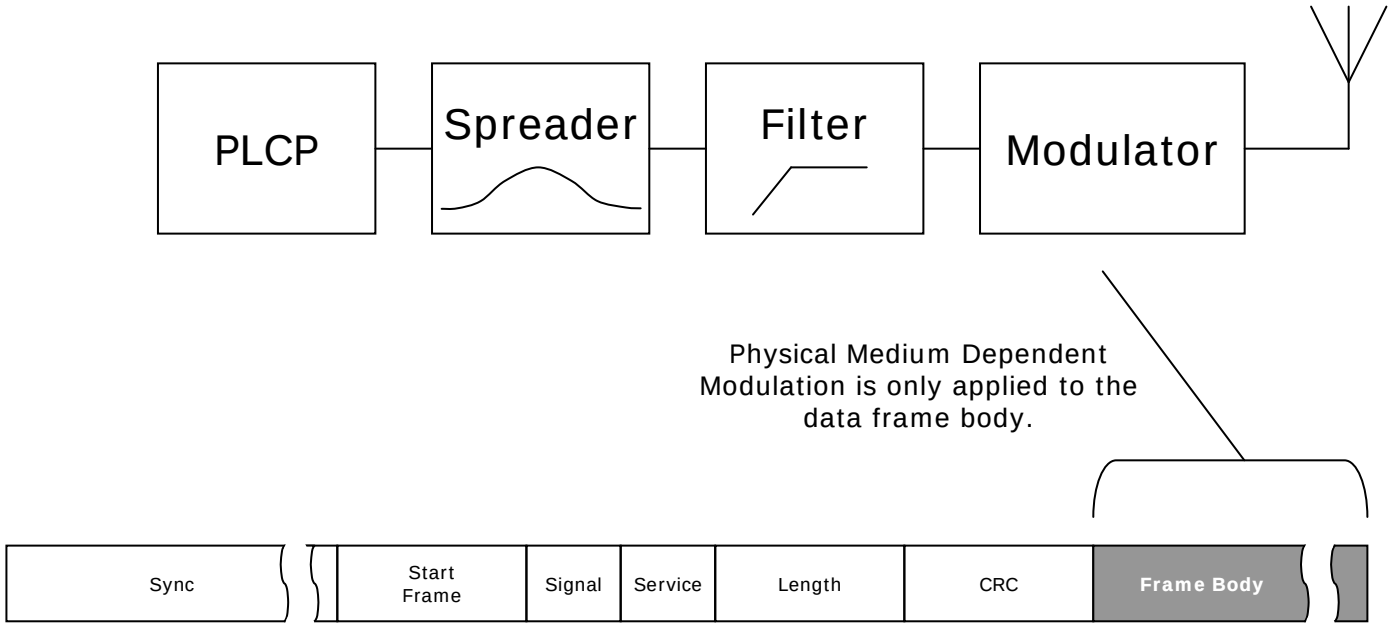


1. The station sends a Reassociation request to AP2, which includes the physical address of the old Access Point AP1.
2. The new Access Point uses this to check with AP1 to ensure that the station had a valid Association with it.
3. If this confirms that there was a valid Association with AP1, AP2 informs the station that it is now associated with itself (AP2), and the two Access Points update their bridging tables.
4. AP2 can optionally ask the original Access Point whether there is any buffered data for the station. This could be the case if the station was in a low power mode and had moved location before waking.
5. If any data is cached by AP1, it is transmitted to AP2, and
6. AP2 now transmits this on to the station.

802.11 frames

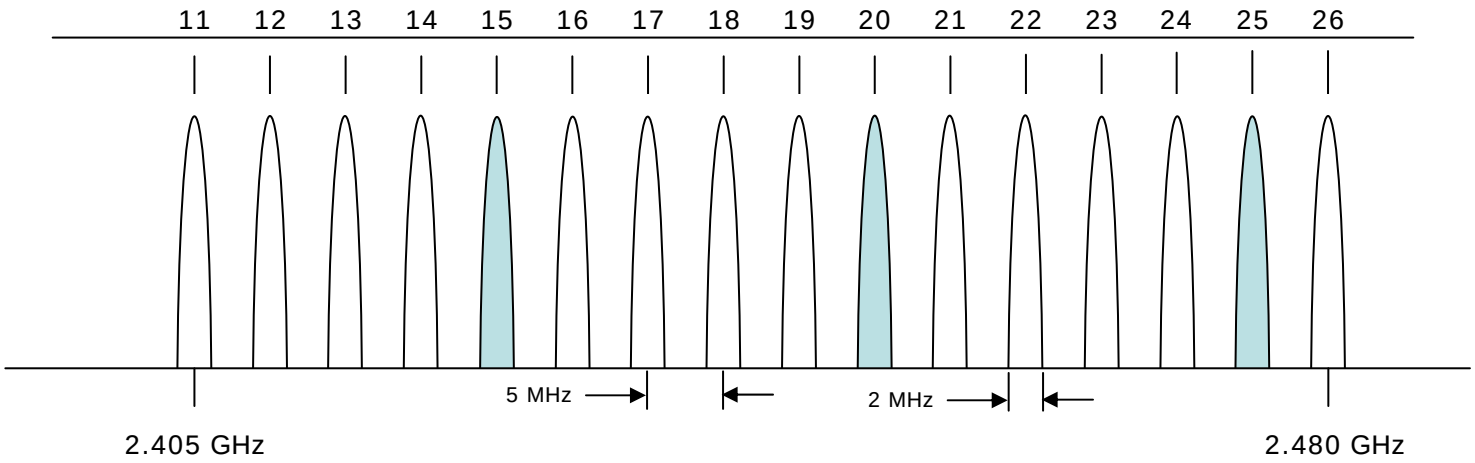


The PLCP – physical layer convergence procedure



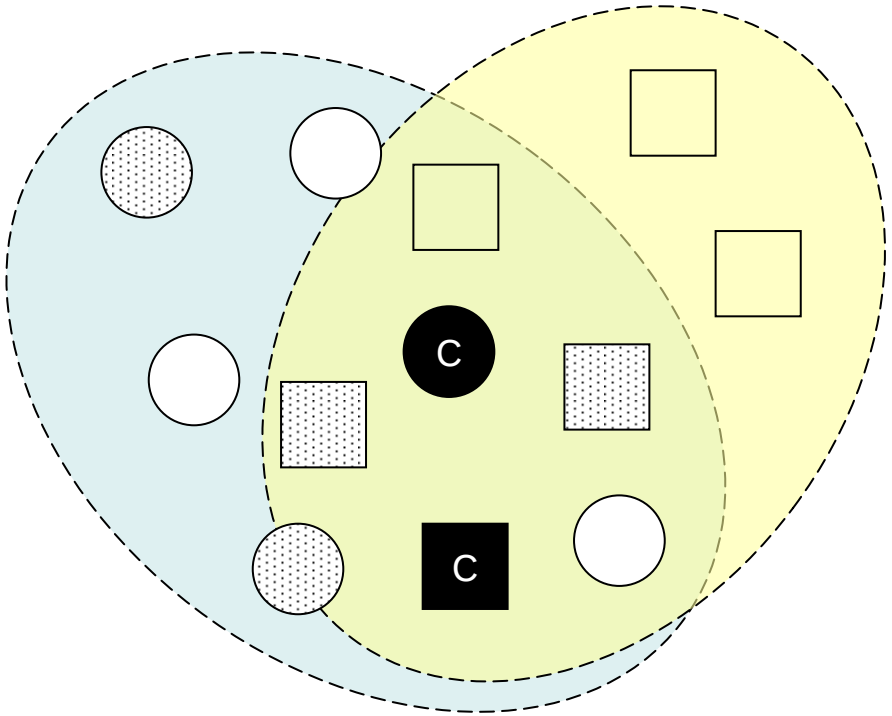
802.15, ZigBee, RF4CE and 6LoWPAN

Frequency usage for 802.15.4 / ZigBee



(RF4CE only uses channels 15, 20 & 25)

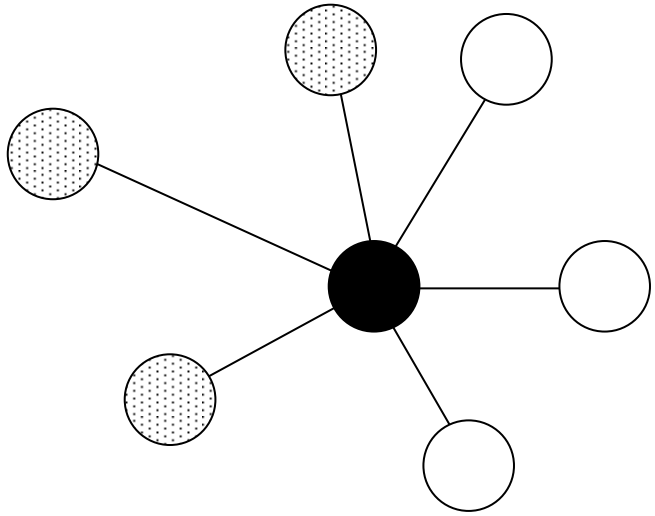
Overlapping networks



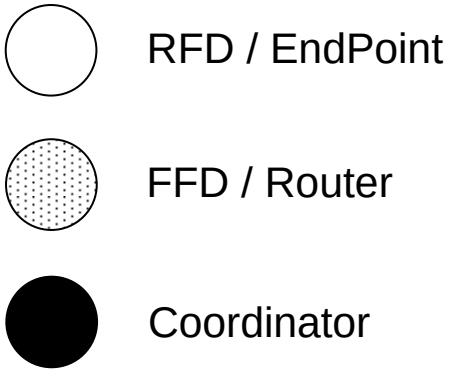
PAN “A” – Channel x

PAN “B” – Channel y

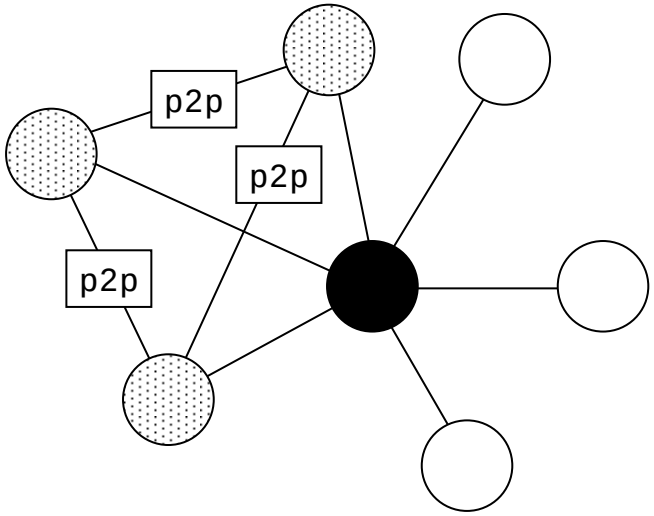
Basic topology of 802.15.4



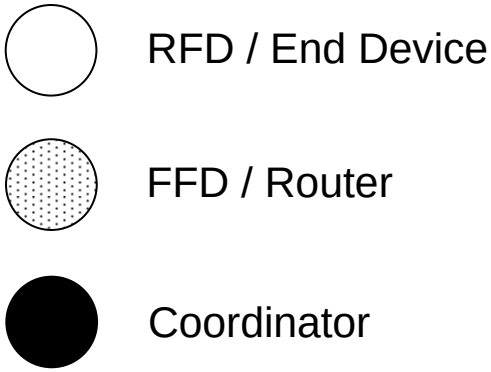
Star Network



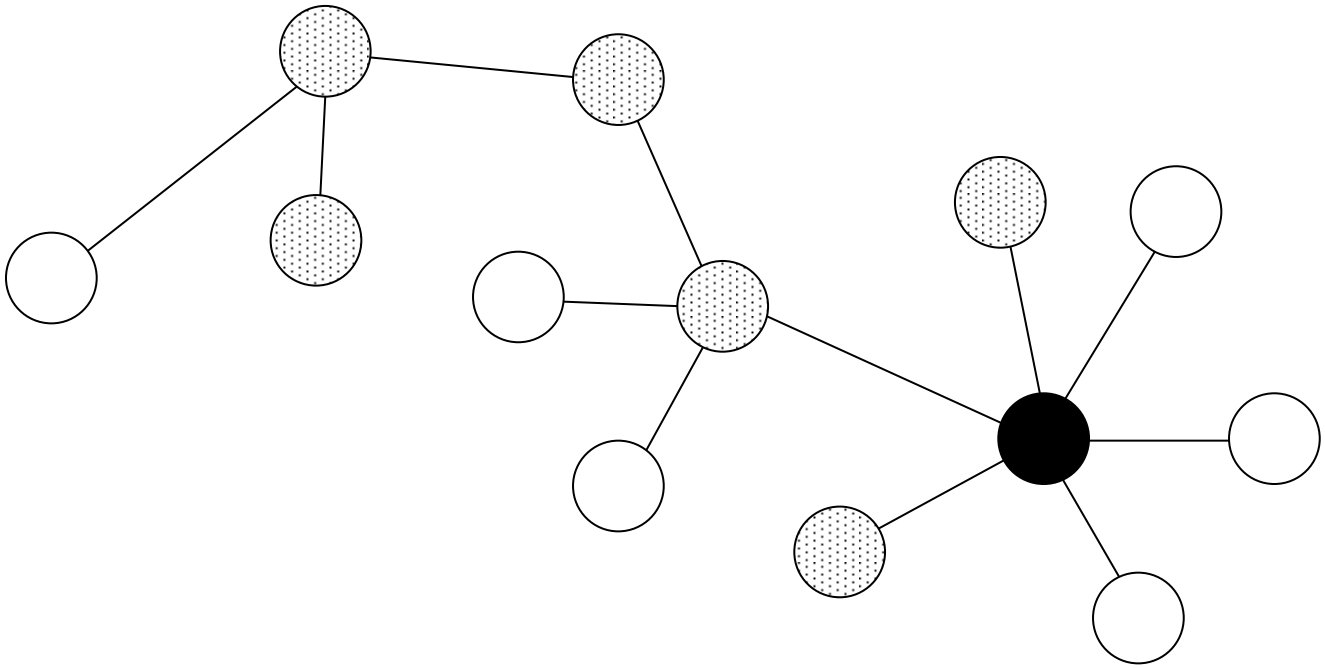
Peer-to-peer topology



Peer to peer

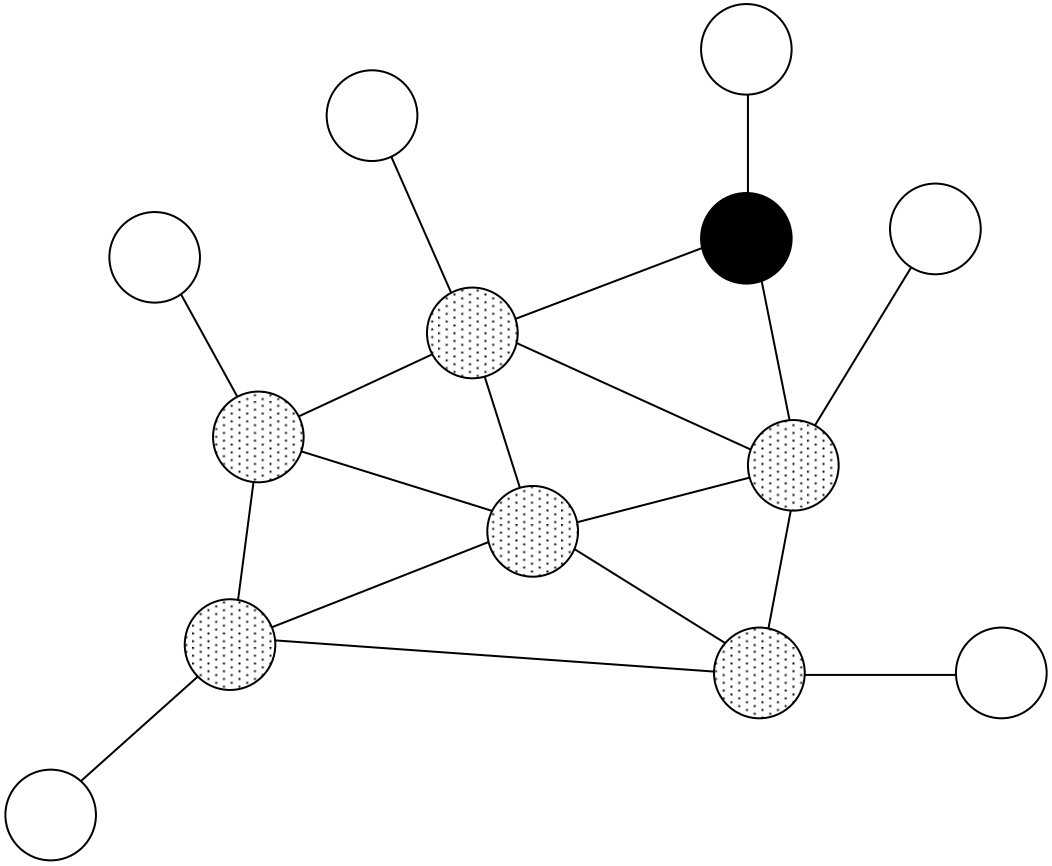


Cluster tree network (ZigBee)



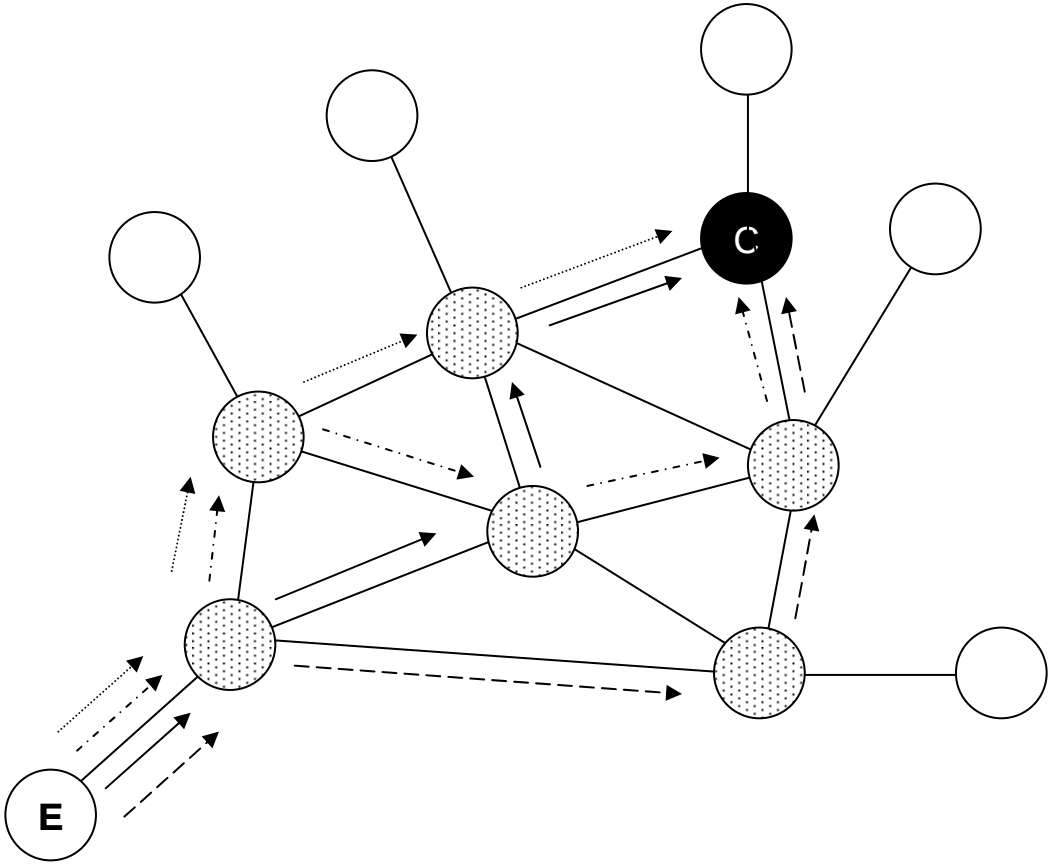
Cluster Tree Network

The full monty (mesh) – ZigBee PRO



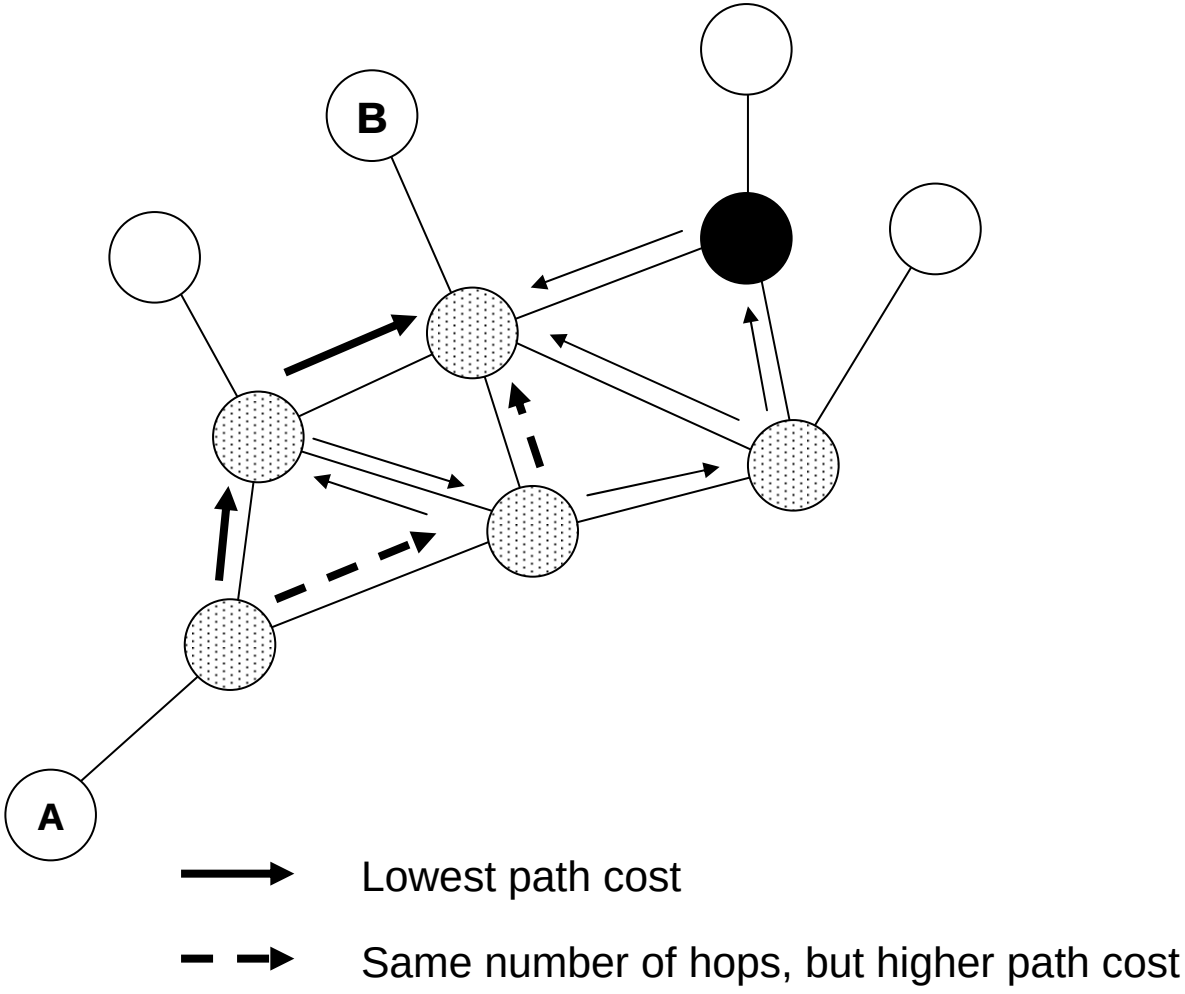
ZigBee Mesh Network

Data movement in a mesh

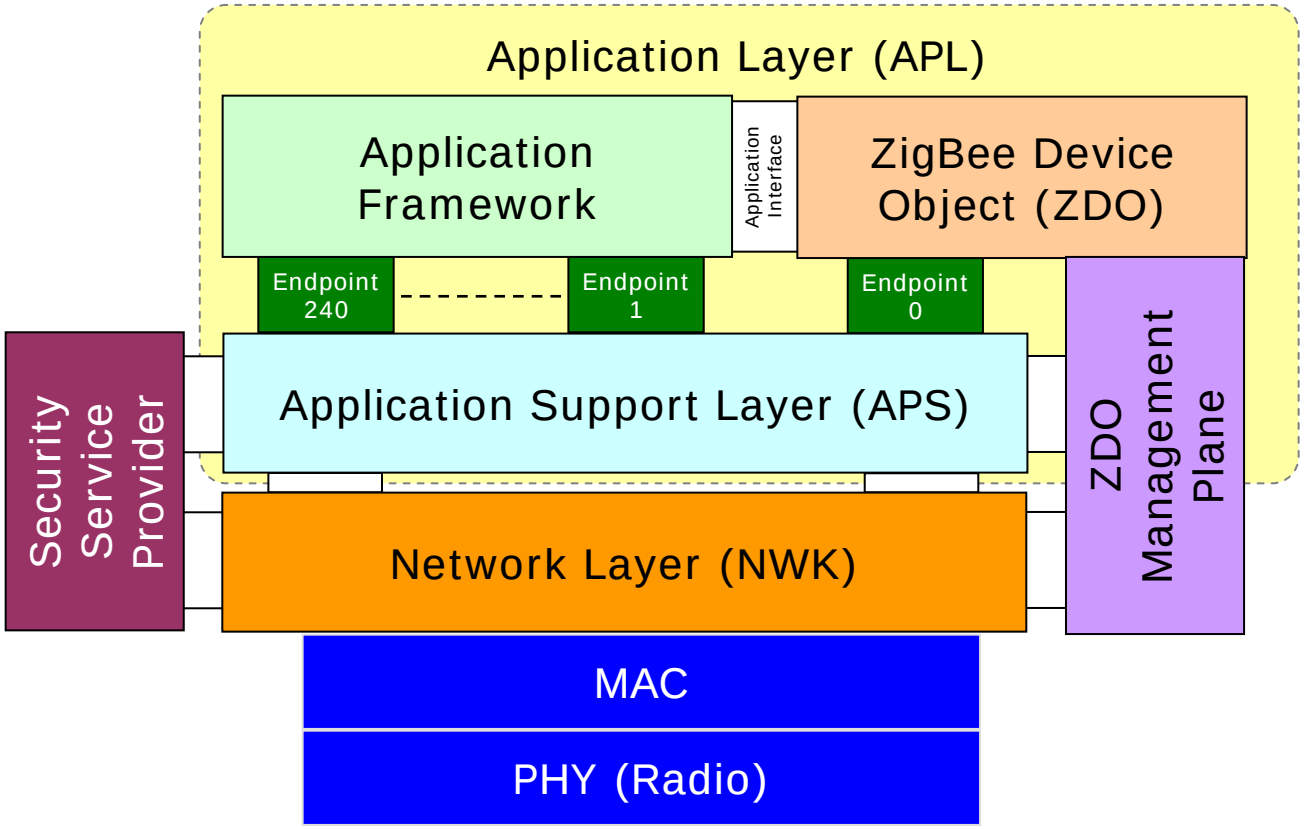


In ZigBee PRO, the send and return routes may be different

Route discovery

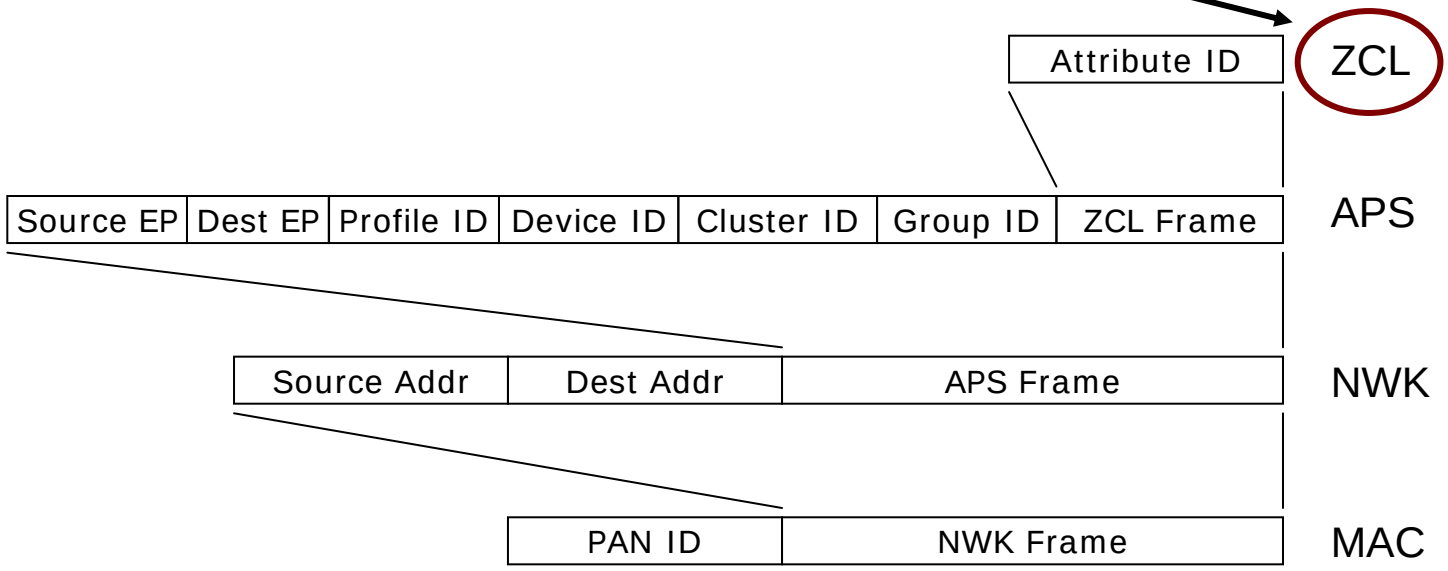


The ZigBee stack



ZigBee Framing Hierarchy

The ZigBee Cluster Library gives it great flexibility

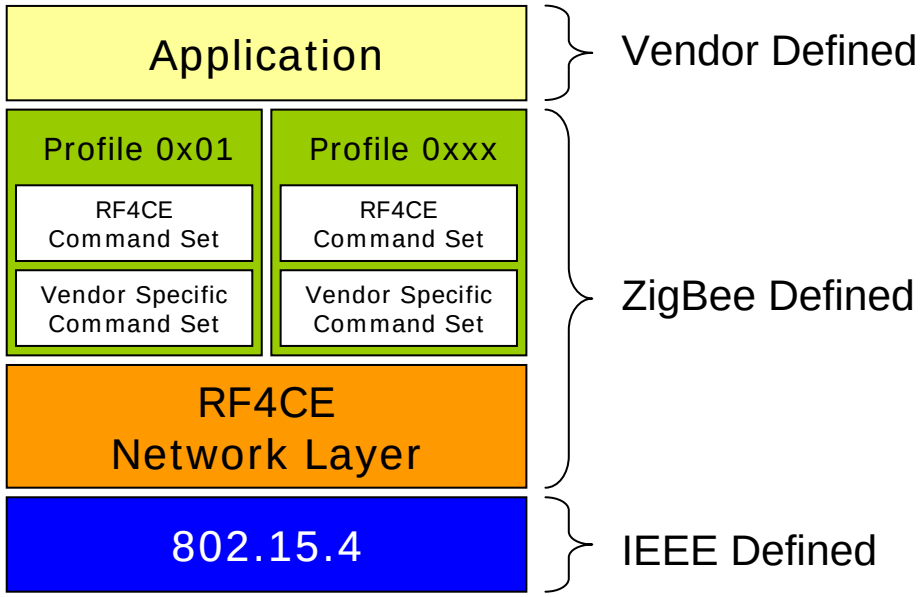


The ZigBee cluster library

Cluster ID	**0x0000**	**Basic Cluster**	
	Attribute ID	0x0000	ZCL Version
		0x0001	Application Version
		0x0002	Stack Version
		0x0003	HW Version
		0x0004	Manufacturer Name
		Etc…	
		0x0010	Location

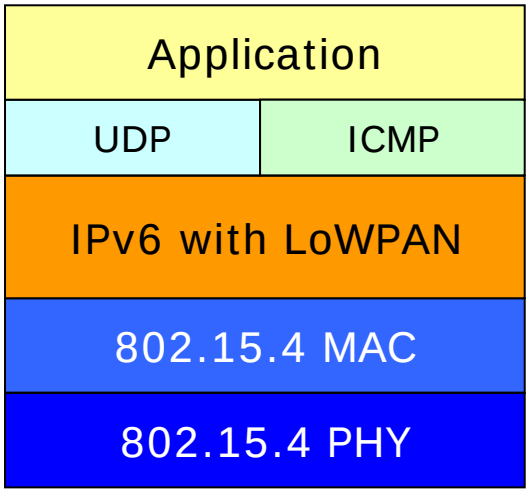
Cluster ID	**0x0002**	**Temperature**	
	Attribute ID	0x0000	Current Temperature
		0x0001	Minimum Temperature
		0x0002	Maximum temperature
		Etc…	
		0x0010	Temperature Alarm Mask

RF4CE



Targeted at Remote Control
Uses three channels only – 15, 20 & 25.

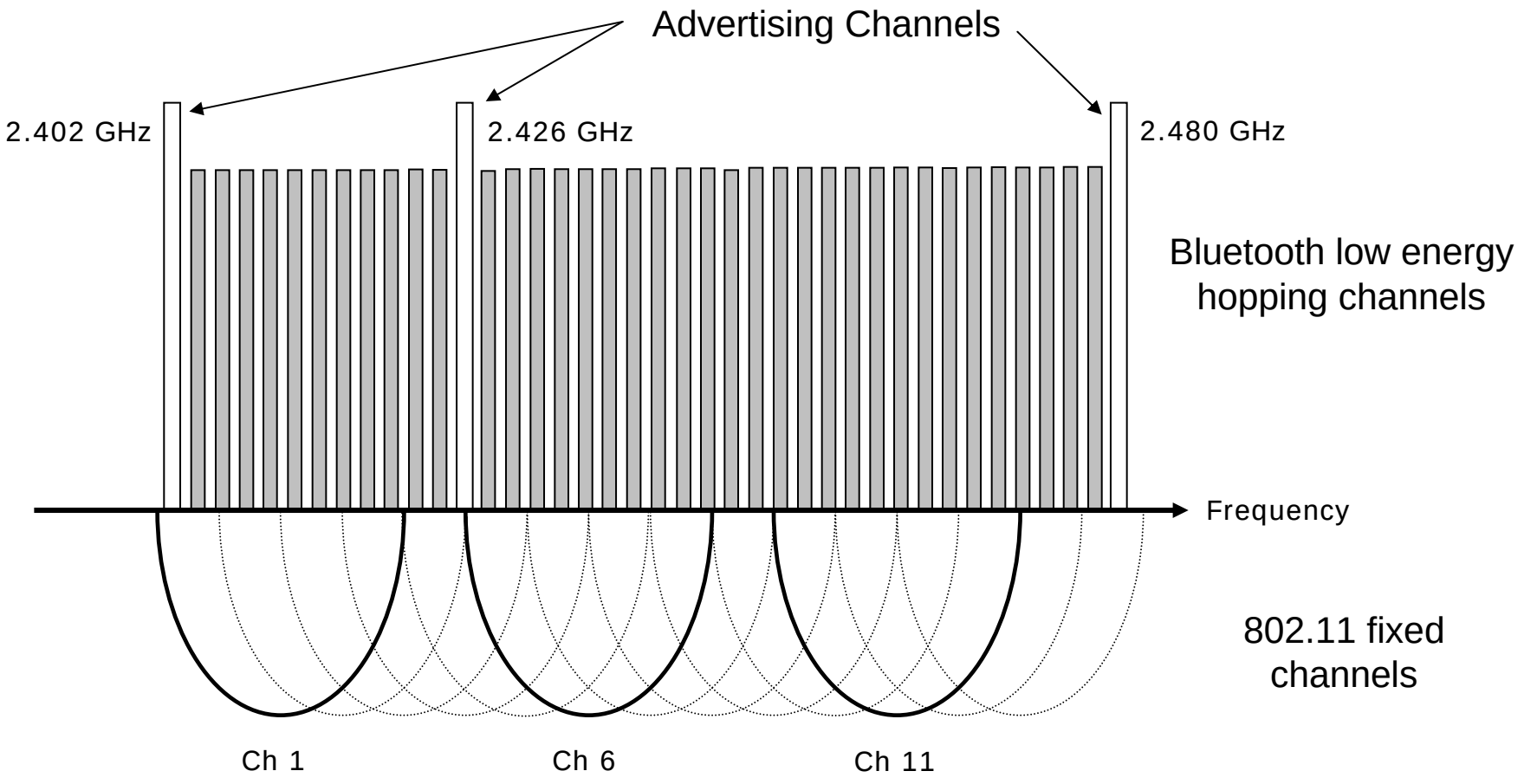
6LoWPAN



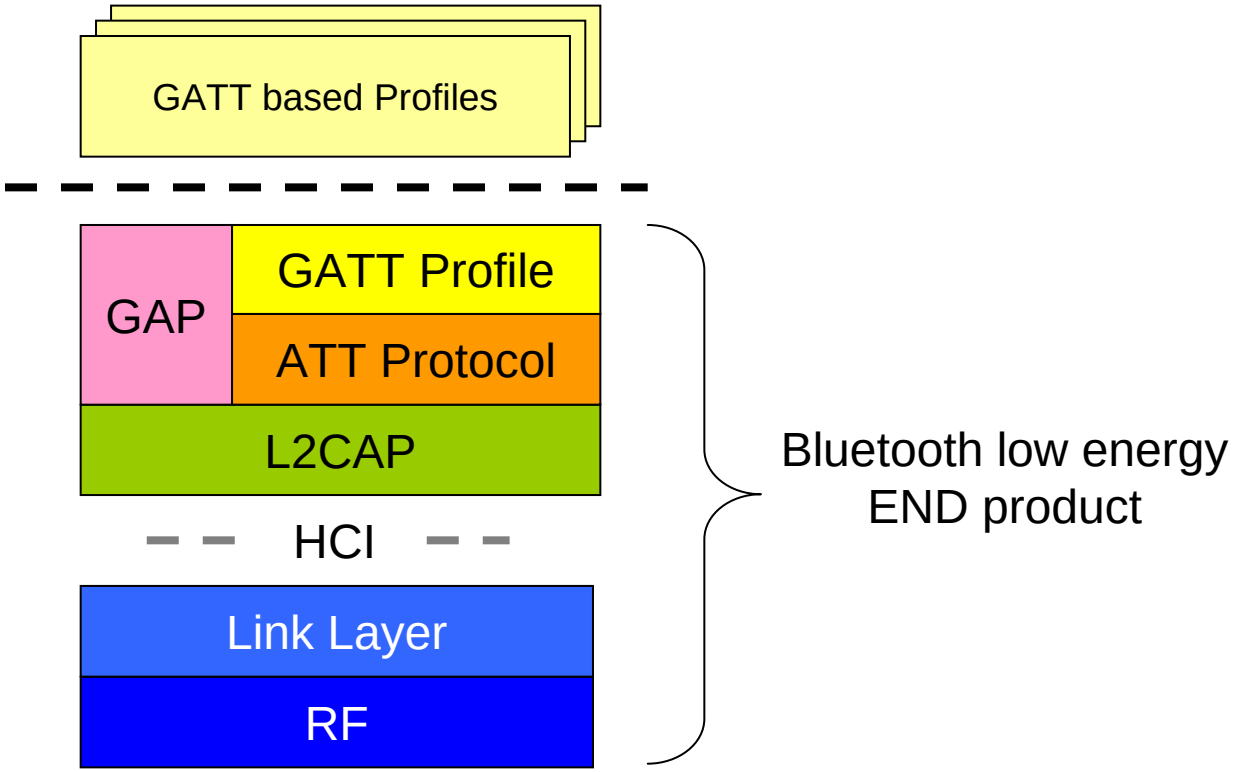
An initiative to “squeeze” IPv6 addressing into reasonably sized wireless packets.
Being adopted for ZigBee’s Smart Energy Profile 2.0

Bluetooth low energy

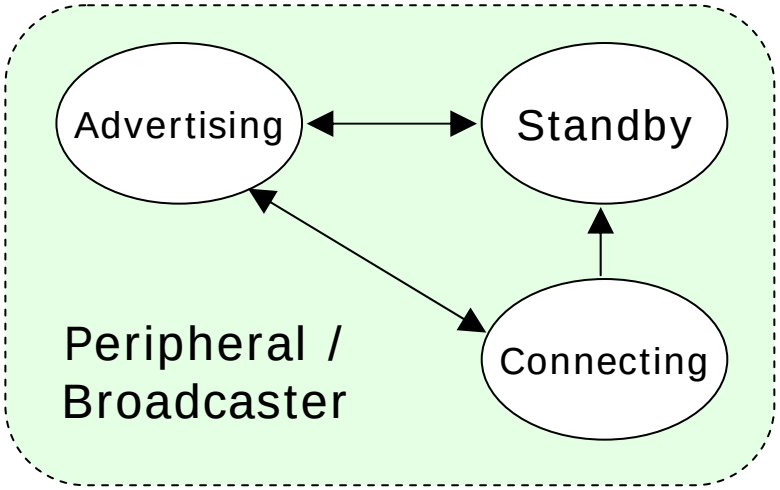
Bluetooth low energy frequency channels



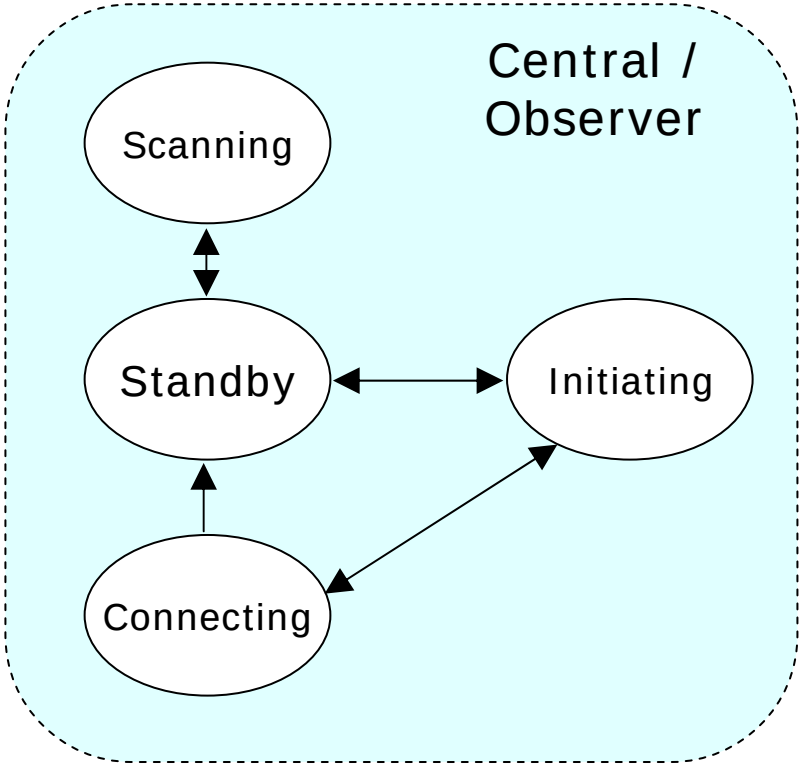
The Bluetooth low energy stack



An advertising and connected data model



A Broadcaster cannot enter the Connecting state.



An Observer cannot enter the Initiating State.

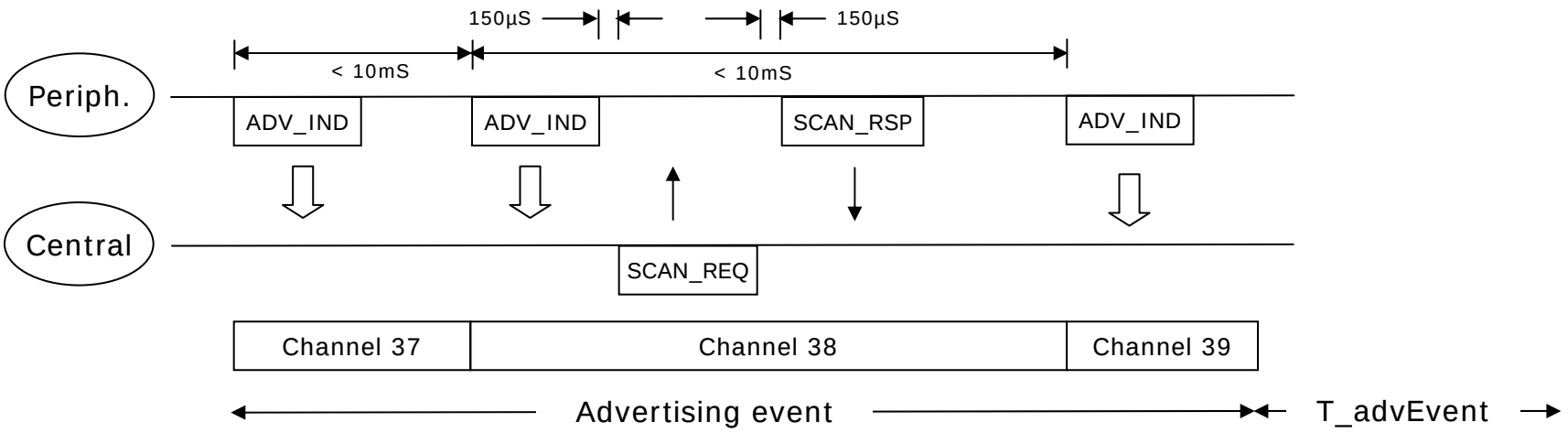
Designed to be simple

- A single, compact packet for all transmissions

Preamble	Access Address	Payload	CRC
1 octet	4 octets	2 – 39 octets	3 octets

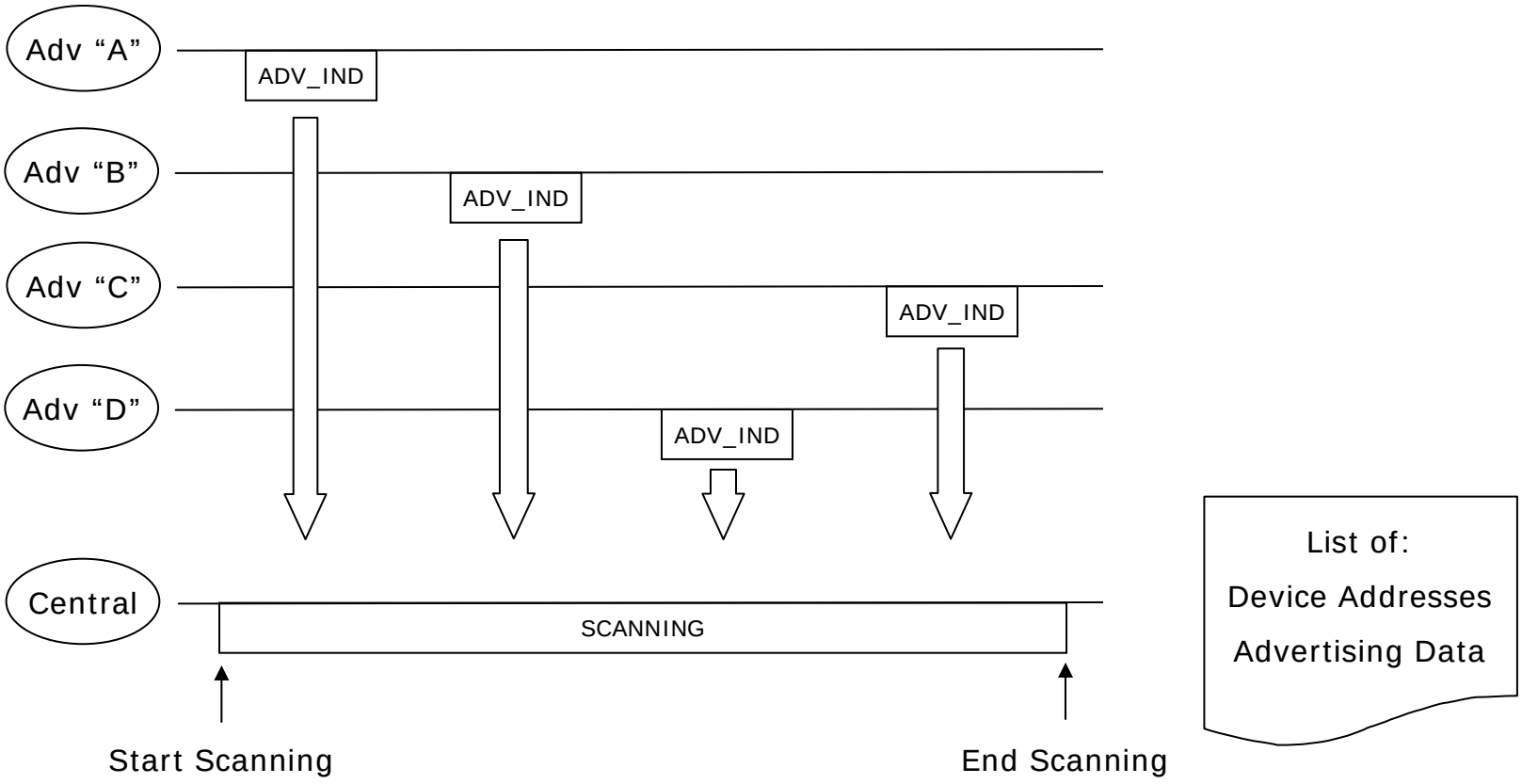
- Very simple profiles
  - One protocol – Attribute Protocol
  - Core data formats defined in the Generic Attribute Profile
  - Applications Profiles only define

Advertising



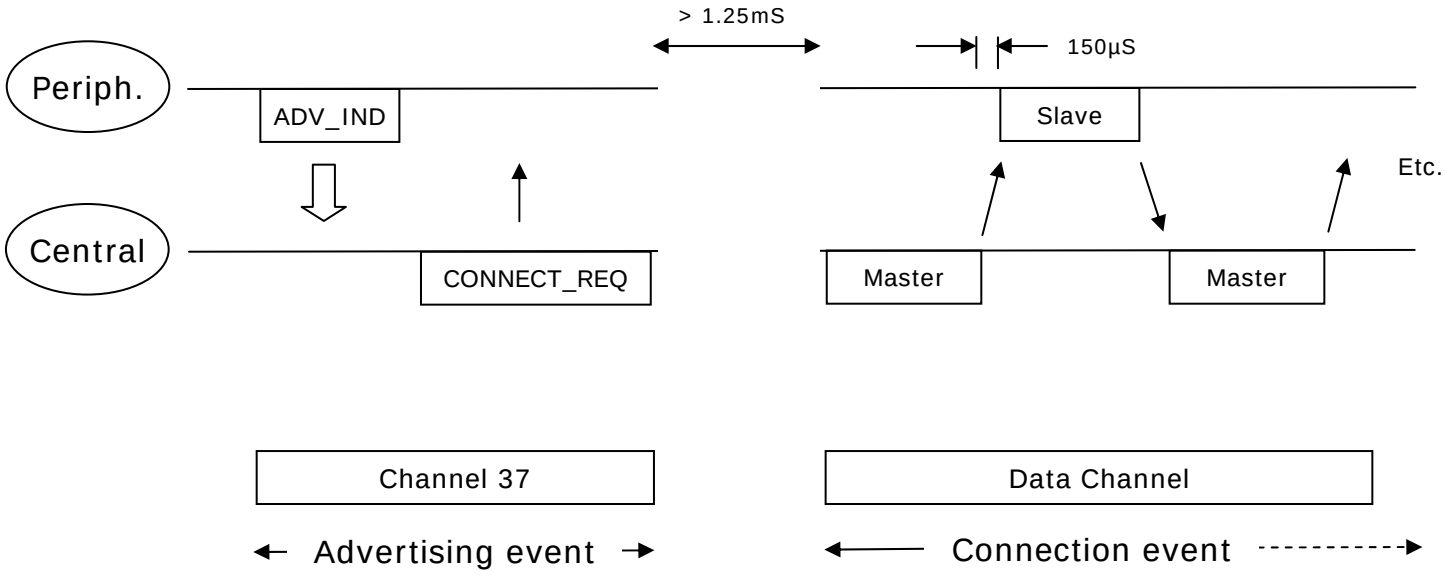
Devices can use advertising to send simple data as well as advertising their presence.

Discovering



Scanners listen to advertising devices to discover what is available.

Connecting



Once connected, devices use AFH on the data channels for secure data communication.

Characteristics and services

- Characteristics describe data / state
  - They can be measurements (sensors)
  - They can perform control (actuators)
- Services add behaviour
  - When and how things happen
- Both reside on the Bluetooth low energy server

- Characteristics can be:
  - Read or Written
  - Indicated (sent with a host acknowledgement)
  - Notified (sent with a baseband acknowledgement)
  - Broadcast

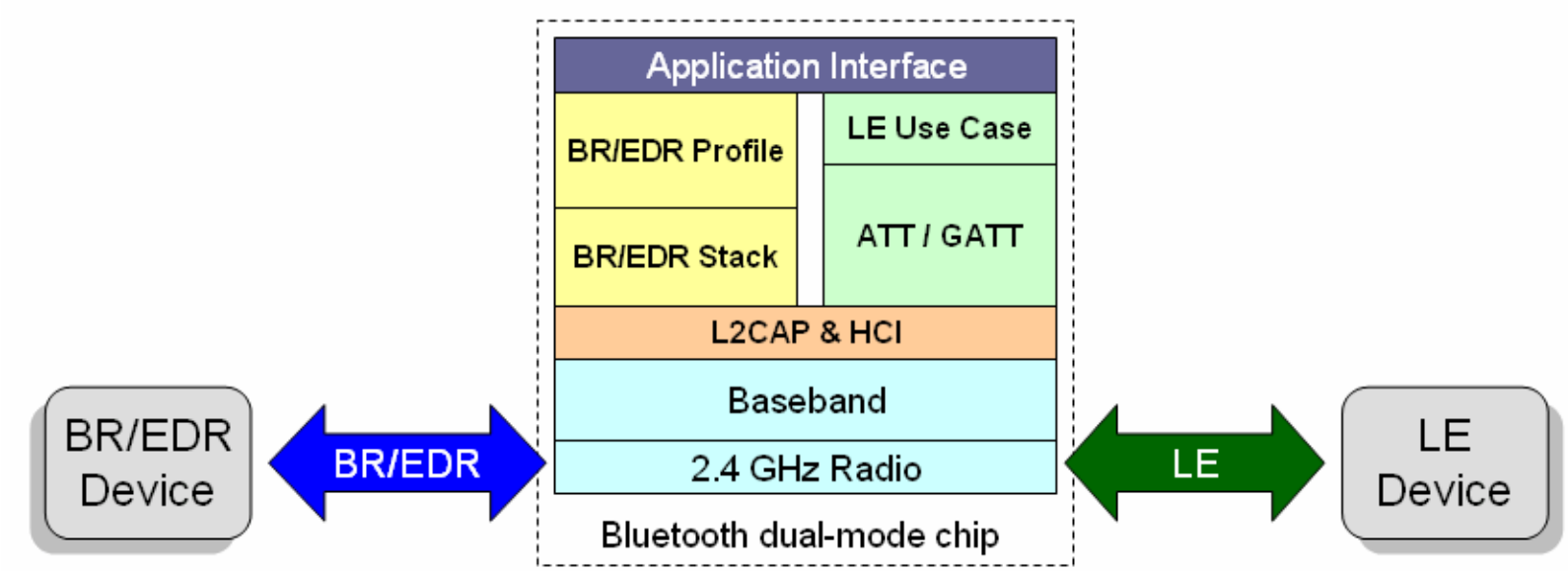
Profiles

- Profiles are a collection of services
- They are simple to write and use

Current Profiles in development include

- Battery Status
- Blood Glucose
- Weighing Scales
- HVAC
- Heart Rate Monitor
- Proximity
- Energy Services

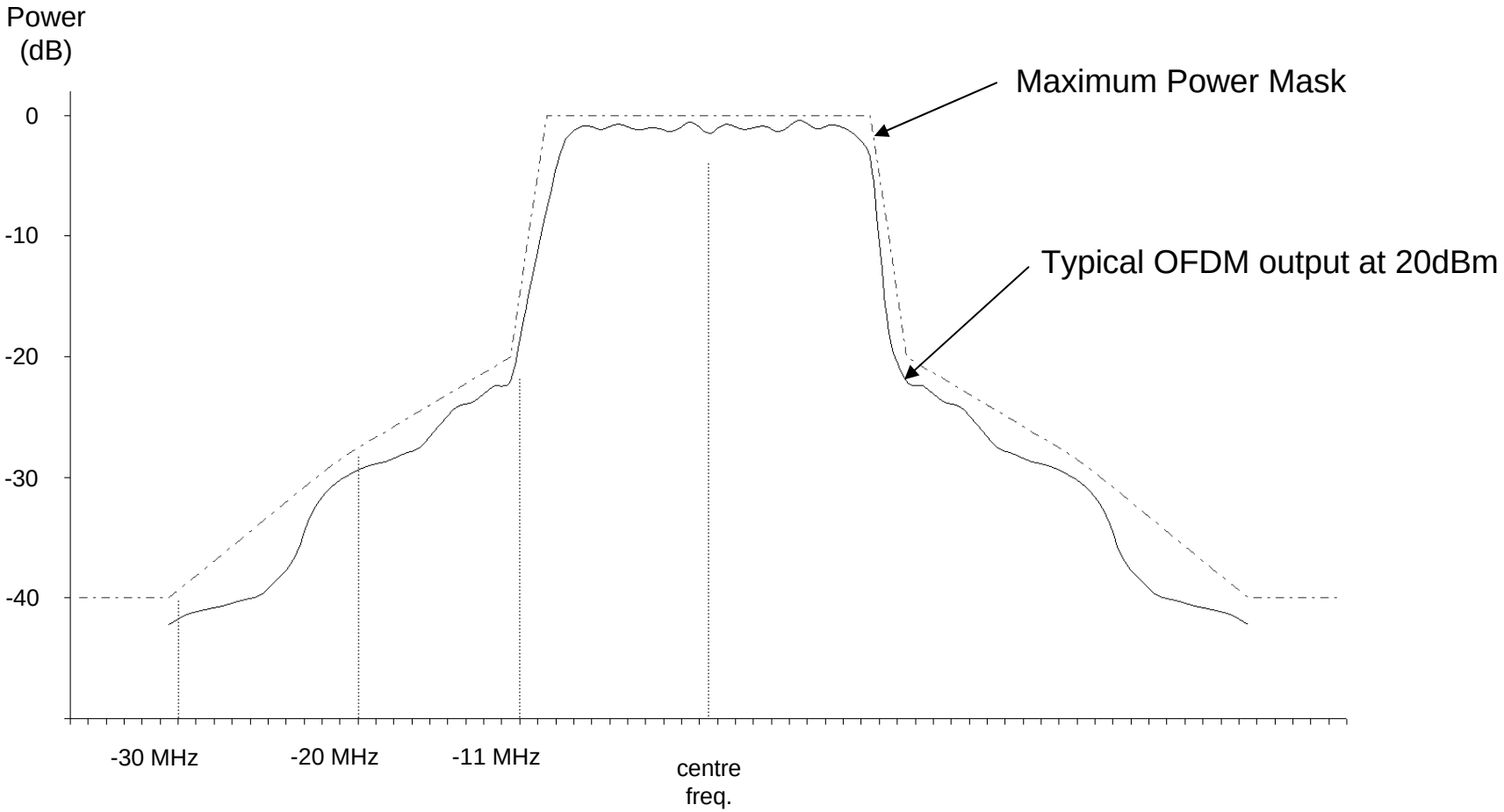
The dual mode stack



Bluetooth's Dual-mode advantage. One chip supports all types device.

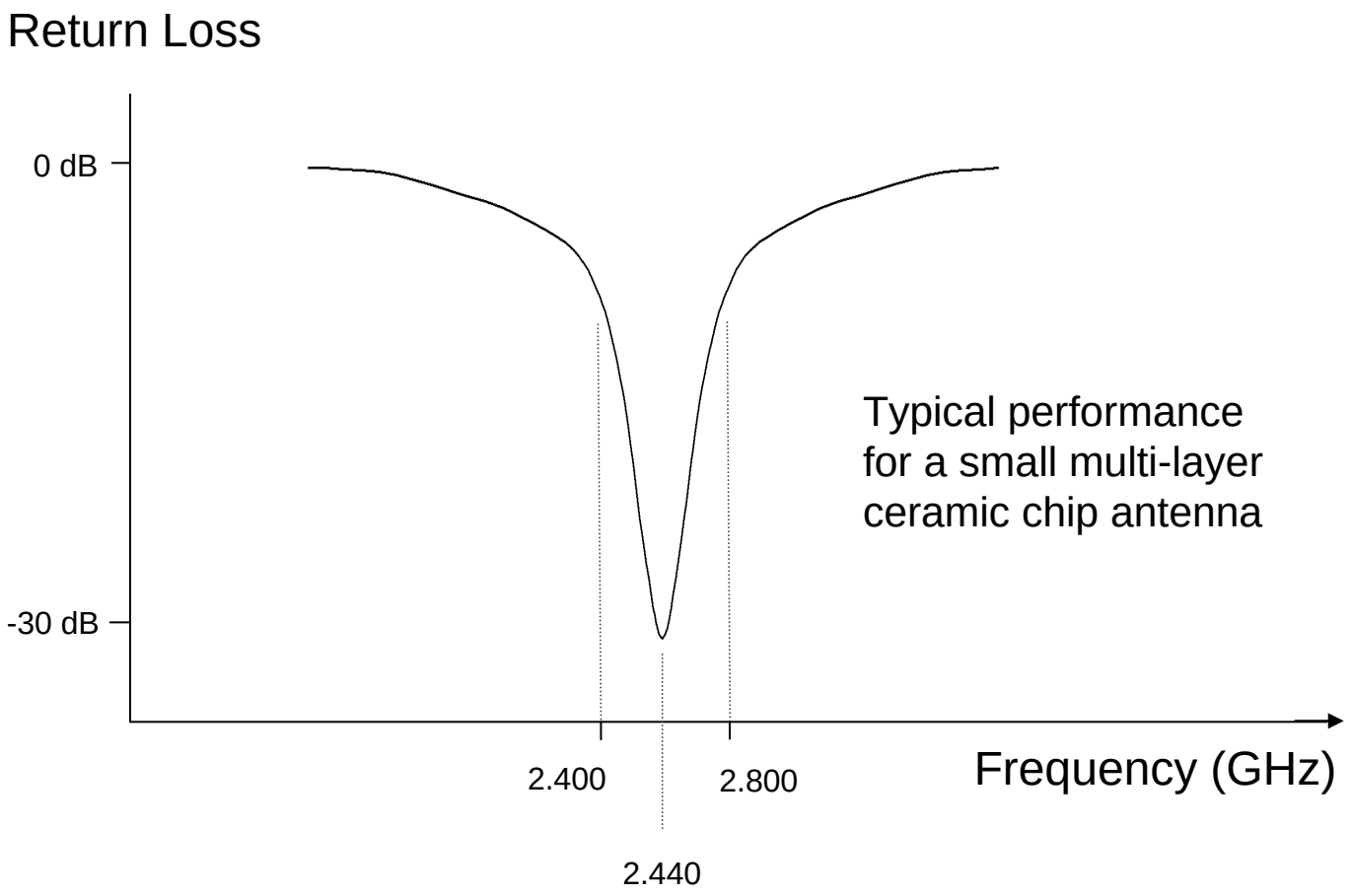
A few Gotchas

Meeting spectral masks

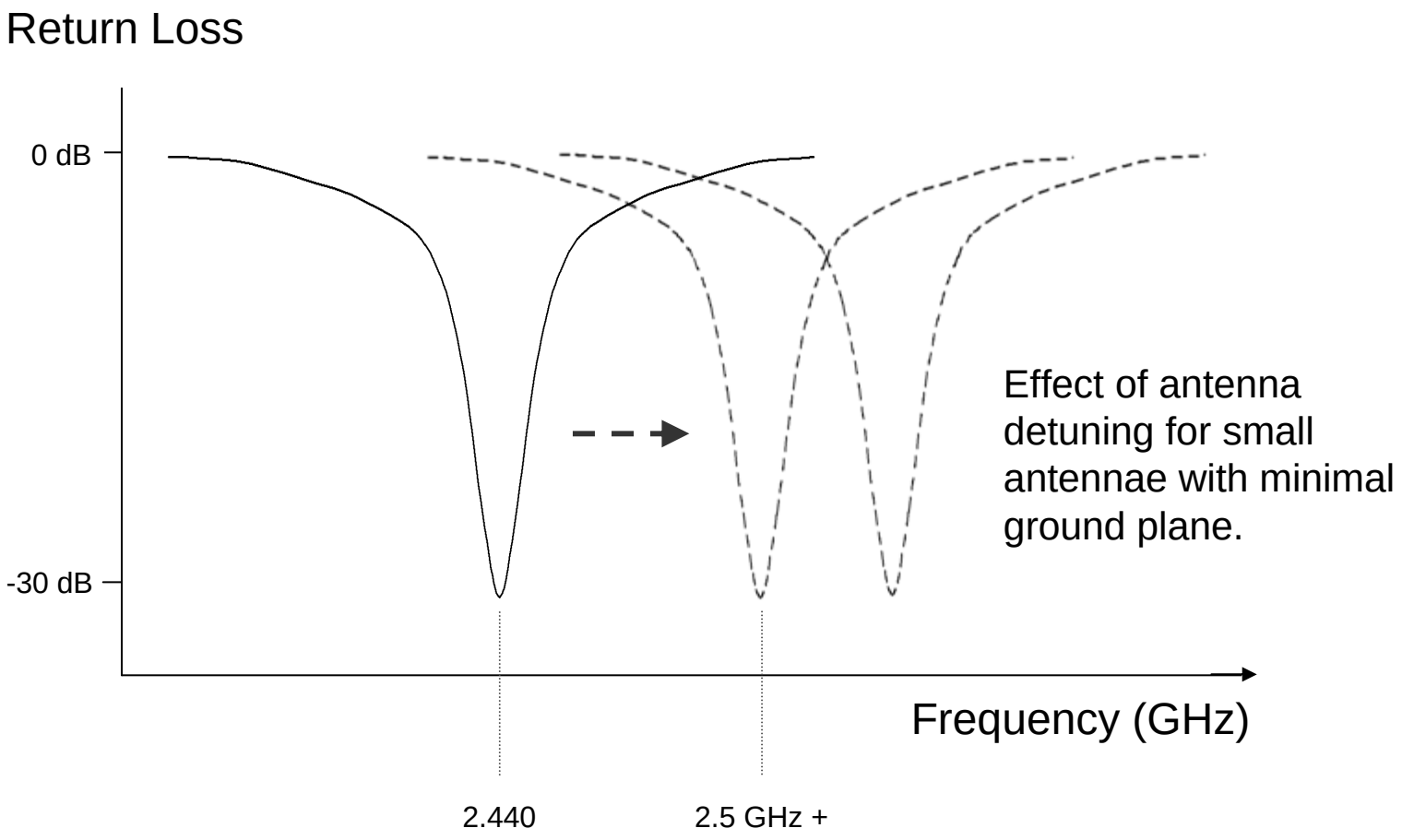


Can be difficult, especially at high power and complex coding schemes

Understanding antennae



Antenna detuning

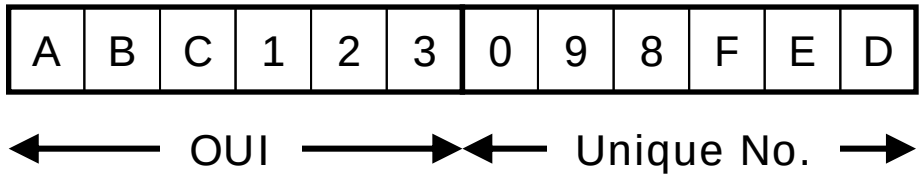


And…

- Temperature Range
  - Don’t expect it to work from -40°C to +85°C. Test it.
  - Radios can go deaf below 0°C and overheat above +50°C.
- Coexistence / Co-location
  - Radios don’t mix
- Upgrading over the wireless link
- Connection Hysterisis
- Feature Creep
- The User Interface
  - Finding and connecting to the right device

Other Practical Considerations and Costs

Buying your OUI

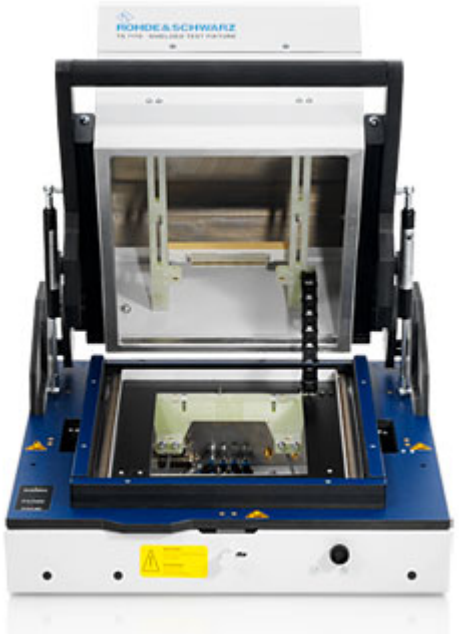


- You may need your own Organisationally Unique Identifier (aka Ethernet Address)
- $1,650 from the IEEE

http://standards.ieee.org/regauth/oui/forms/

Production test

- RF testing adds a new dimension to production, as devices can interfere with each other.
- Conducted tests require a connector, which adds cost.
- Transmitted tests require shielded test boxes.
- Both can cost upwards of $100k.
- Test equipment needs to be planned at design started at the beginning of the project, not left until the end.



Backwards compatibility and lifetime

	Availability	Backwards Compatibility
Bluetooth	11 years	Compatible with all previous versions at base 1Mbps
Bluetooth low energy	New	Will be compatible with Dual mode chips introduced in 2011
802.11	13 years	Security is compromised in mixed versions more than 3 years old
Wi-Fi	10 years	Security is compromised in mixed versions more than 3 years old. Two incompatible frequencies of operation – 2.4GHz and 5.1GHz
ZigBee	6 years	Three version – all with compatibility issues
ZigBee PRO	3 years	Incompatible with ZigBee
ZigBee PRO SEP2.0	New	Incompatible with other ZigBee stacks
ZigBee RF4CE	2 years	Incompatible with other ZigBee stacks
ANT	3 years	Only one version available.

Average years of compatibility

Bluetooth	11 years and still compatible
Wi-Fi	3 - 5 years (at which point security is compromised)
ZigBee	2 years

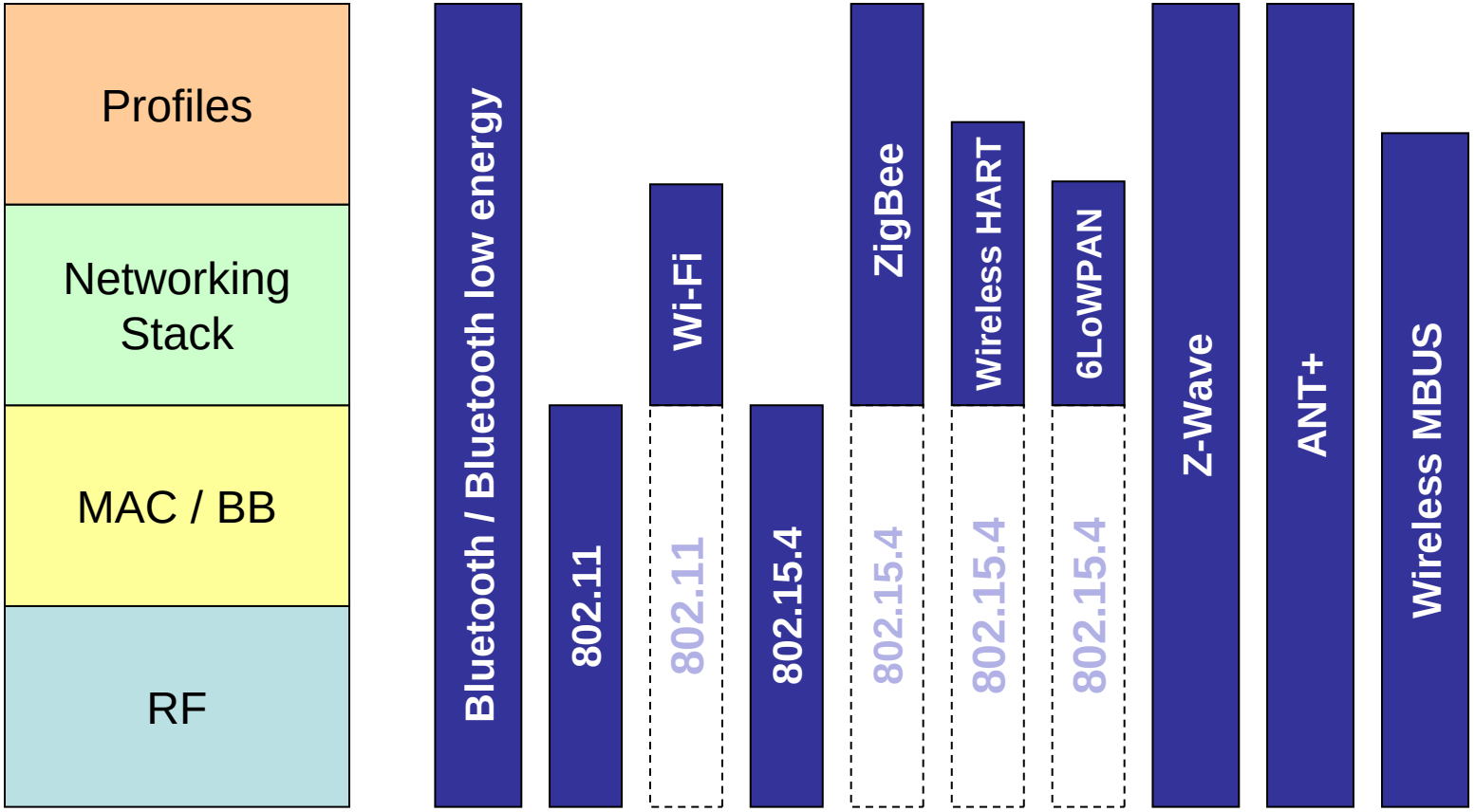
Licensing and qualification

	Bluetooth	Wi-Fi	ZigBee	ANT
License	RANDZ	RAND	RAND	No IP license
Annual Membership [1]	Free	$5k / $15k [2]	$3.5k [3]	$500 (5 yr)
Qualification Cost (per product)	~ $7.5k	~ $5 k	~ $3 k	$750 (5 yr)
Ownership of MAC/ PHY	Bluetooth	IEEE (802.11)	IEEE (802.15.4)	Dynastream

1 Minimum level of membership fee for use of trademark
2 To certify a Wi-Fi product, the minimum membership level is Regular.
3 Non commercial users may use the ZigBee standard without payment.
(Qualification costs can vary depending on membership level and use of prequalified components)

Plus CE, FCC, ICES, TELEC, CNCA, etc
Don't forget you need to perform R&TTE notification if your output power is greater than 10mW.

Not all standards cover the same elements



A standard can only offer IP protection for the parts it own.

Export controls

- If your device uses greater than 56bit encryption you may need to comply with Export Controls.
- These apply to every country involved in the design, manufacture, ship-through and supply.
- They also apply to downloadable firmware updates.
- Check with your local Government body and get any decisions in writing.

But…

Wireless can liberate your designs

My pulse is…

My blood glucose is…

My temperature is…

Thank You – Questions?

www.wireless-book.com

WiFore
Wireless Consulting

Nick Hunn
CTO

mob: +44 7768 890 148
email: nick@wifore.com
web: www.wifore.com

Creative Connectivity Blog
www.nickhunn.com

- Bluetooth low energy – aiming for the trillions.
- Smart Metering – the next Y2K bonanza?
- The need for Patient Accessible Medical Records.
- Who owns Smart Energy?