


Contents

A decorative network diagram in the top right corner, featuring a series of interconnected nodes and lines, with some nodes highlighted in blue and others in grey.

- Introduction
- Physical and Link Layers Protocols (IoT Access Technologies)
 - Physical Layer Issues
 - Communication Technologies Criteria
 - Communication Technologies and Protocols

A decorative network diagram in the bottom left corner, featuring a series of interconnected nodes and lines, with some nodes highlighted in blue and others in grey.

Mostly adopted from Chapters 4, 5, and 6 of **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017

Physical and Link Layers Protocols- IEEE 802.15.4

- Two main sections divide this lecture:
 - “Communications Criteria,”
 - Describes the characteristics and attributes you should consider when selecting and dealing with connecting smart objects
 - “IoT Access Technologies,”
 - Provides an in-depth look at some of the technologies that are considered when connecting smart objects.

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017

Communication Technologies Criteria




- Currently, the number of technologies (available or under development) connecting smart objects is quite extensive,
 - but you should expect consolidation, with certain protocols eventually winning out over others in the various IoT market segments.
- Before reviewing some of these access technologies, it is important to talk about the criteria to use in evaluating them for various use cases and system solutions.

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017



Communication Technologies Criteria

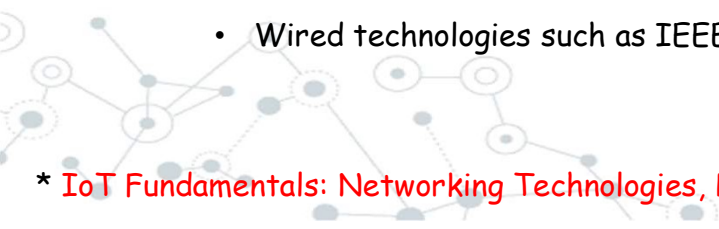


- 1- Range
 - 2- Frequency Bands
 - 3- Power Consumption
 - 4- Topology
 - 5- Constrained Devices
 - 6- Constrained-Node Networks
- 

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017

Communication Technologies Criteria: 1-Range



- **Short range:**
 - Tens of meters of maximum distance between two device
 - Example:
 - The classical wired example is a serial cable!
 - Wireless Examples: IEEE 802.15.1, Bluetooth and IEEE 802.15.7 Visible Light Communications (VLC).
 - **Medium range:**
 - Tens to hundreds of meters
 - Examples:
 - IEEE 802.11 Wi-Fi, IEEE 802.15.4, and 802.15.4g WPAN.
 - Wired technologies such as IEEE 802.3 Ethernet and IEEE 1901.2 Narrowband PLC
- 

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017

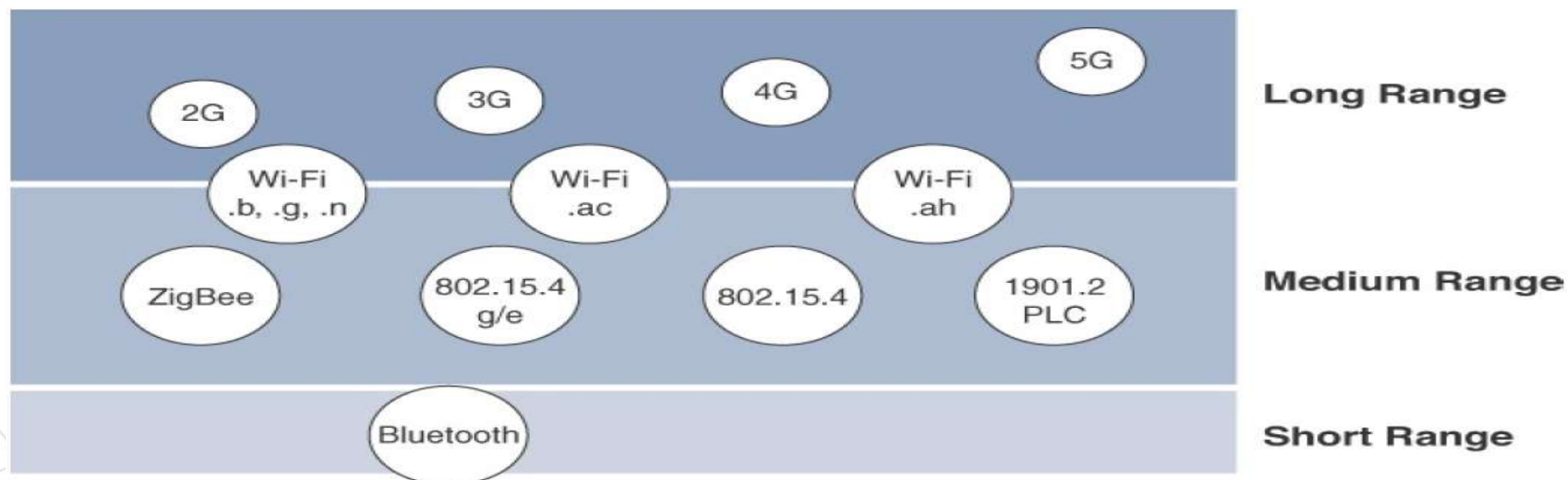
Communication Technologies Criteria: 1- Range

A decorative network diagram in the top right corner, featuring a series of interconnected nodes (circles) and lines, representing a communication network.

- **Long range:**
 - Greater than 1 mile (1.6 km) between two devices require long-range technologies.
 - Examples: cellular (2G, 3G, 4G) and some applications of outdoor IEEE 802.11 Wi-Fi and Low-Power Wide-Area (LPWA) technologies.

Communication Technologies Criteria: 1- Range

- How far does the signal need to be propagated?
 - the area of coverage for a selected wireless technology



* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Communication Technologies Criteria: 2-Frequency Bands

- **Licensed:**

- Generally applicable to IoT long-range access technologies and allocated to communications infrastructures deployed by services providers, public services (for example, first responders, military), broadcasters, and utilities.
- Examples: cellular, WiMAX, and Narrowband IoT (NB-IoT) technologies.

- **Unlicensed:**

- For the industrial, scientific, and medical (ISM) portions of the radio bands, and they are used in many communications technologies for short-range devices (SRDs).
- Examples: 2.4 GHz band as used by IEEE 802.11b/g/n Wi-Fi, IEEE 802.15.1 Bluetooth, and IEEE 802.15.4 WPAN.

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017

Communication Technologies Criteria: 2-Frequency Bands



- **Licensed Frequency Bands**

- Users must subscribe to services when connecting their IoT devices.
 - This adds more complexity to a deployment involving large numbers of sensors and other IoT devices,
- The network operator can guarantee the exclusivity of the frequency usage over the target area and can therefore sell a better guarantee of service

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017



Communication Technologies Criteria: 2-Frequency Bands

- **Unlicensed Frequency Bands**

- An unlicensed band is not unregulated.

- National and regional regulations exist for each of the allocated frequency bands (much as with the licensed bands).
 - These regulations mandate device compliance on parameters such as transmit power, duty cycle, channel bandwidth, and channel hopping.

- It does not require a service provider.

- However, it can suffer from more interference

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017

Communication Technologies Criteria: 2-Frequency Bands

- **Unlicensed Frequency Bands**

- The frequency of transmission directly impacts how a signal propagates and its practical maximum range.
 - Range and its importance to IoT access are discussed earlier
- Either for indoor or outdoor deployments, the sub-GHz frequency bands
 - allow greater distances between devices
 - have a better ability than the 2.4 GHz ISM band to penetrate building infrastructures or go around obstacles, while keeping the transmit power within regulation.

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017

Communication Technologies Criteria: 2-Frequency Bands



- **Unlicensed Frequency Bands**

- The disadvantage of sub-GHz frequency bands is their lower rate of data delivery compared to higher frequencies.
- However, most IoT sensors do not need to send data at high rates.
- Therefore, the lower transmission speeds of sub-GHz technologies are usually not a concern for IoT sensor deployments

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017



Communication Technologies Criteria: 2-Frequency Bands

- **Unlicensed Frequency Bands**

- In most European countries, the 169 MHz band is often considered best suited for wireless water and gas metering applications.
 - This is due to its good deep building basement signal penetration.
- In addition, the low data rate of this frequency matches the low volume of data that needs to be transmitted.
- Several sub-GHz ranges have been defined in the ISM band.
 - The most well known ranges are centered on 169 MHz, 433 MHz, 868 MHz, and 915 MHz.
 - However, most IoT access technologies tend to focus on the two sub-GHz frequency regions around 868 MHz and 915 MHz.

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017

Communication Technologies Criteria: 3- Power Consumption




- **Powered nodes**
 - have a direct connection to a power source
- **Battery-powered nodes:**
 - are often classified by the required lifetimes of their batteries.
 - For devices under regular maintenance, a battery life of 2 to 3 years is an option.
- Evolution of a new wireless environment known as Low-Power Wide-Area (LPWA) for battery-powered nodes

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017



Communication Technologies Criteria: 4- Topology



- Topology (star, mesh, and peer-to-peer)
 - For long range and short-range technologies, a star topology is prevalent, as seen with cellular, LPWA, and Bluetooth networks.
 - Star topologies utilize a single central base station or controller to allow communications with endpoints.
 - For medium-range technologies, a star, peer-to-peer, or mesh topology is common, as shown in Figure 4-2. Peer-to-peer topologies allow any device to communicate with any other device as long as they are in range of each other.
- 

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017

Communication Technologies Criteria: 5- Constrained Devices

- Classes of Constrained Nodes, as Defined by RFC 7228
 - Constrained nodes have limited resources that impact their networking feature set and capabilities.
 - Classes of Constrained Nodes, as Defined by RFC 7228:
 - **Class 0:** are typically battery-powered nodes such as push button nodes that sends 1 byte of information when changing its status
 - Memory \ll 10 KB
 - Processing capability and storage \ll 100 KB
 - **Class 1:** are capable enough to use a protocol stack specifically designed for constrained nodes
 - Memory \sim 10 KB
 - Processing capability and storage \sim 100 KB
 - **Class 2:**
 - Memory $>$ 50 KB
 - Processing capability and storage $>$ 250 KB

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017

Communication Technologies Criteria: 5- Constrained Devices

Class	Definition
Class 0	<p>This class of nodes is severely constrained, with less than 10 KB of memory and less than 100 KB of Flash processing and storage capability. These nodes are typically battery powered. They do not have the resources required to directly implement an IP stack and associated security mechanisms.</p> <p>An example of a Class 0 node is a push button that sends 1 byte of information when changing its status. This class is particularly well suited to leveraging new unlicensed LPWA wireless technology.</p>
Class 1	<p>While greater than Class 0, the processing and code space characteristics (approximately 10 KB RAM and approximately 100 KB Flash) of Class 1 are still lower than expected for a complete IP stack implementation. They cannot easily communicate with nodes employing a full IP stack. However, these nodes can implement an optimized stack specifically designed for constrained nodes, such as Constrained Application Protocol (CoAP). This allows Class 1 nodes to engage in meaningful conversations with the network without the help of a gateway, and provides support for the necessary security functions. Environmental sensors are an example of Class 1 nodes.</p>
Class 2	<p>Class 2 nodes are characterized by running full implementations of an IP stack on embedded devices. They contain more than 50 KB of memory and 250 KB of Flash, so they can be fully integrated in IP networks. A smart power meter is an example of a Class 2 node.</p>

* *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing*, Cisco press, 2017

Communication Technologies Criteria: 6- Constrained-Node Networks



- Several of the IoT access technologies, such as Wi-Fi and cellular, are applicable to laptops, smart phones, and some IoT devices,
- Some IoT access technologies are more suited to specifically connect constrained nodes.
 - Typical examples are IEEE 802.15.4 and 802.15.4g RF, IEEE 1901.2a PLC,
 - LPWA, and IEEE 802.11ah access technologies.
 - These technologies are discussed in more detail later in this chapter.

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017



Communication Technologies Criteria: 6- Constrained-Node Networks



- Constrained-Node Networks are often referred to as low-power and lossy networks (LLNs).
- Low-power refers to the fact that nodes must cope with the requirements from powered and battery-powered constrained nodes.
- Lossy networks indicates that network performance may suffer from interference and variability due to harsh radio environments.

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017



Communication Technologies Criteria: 6- Constrained-Node Networks



- Layer 1 and Layer 2 protocols that can be used for constrained-node networks must be evaluated in the context of the following characteristics for use-case applicability:
 - **Data rate and throughput,**
 - **Latency,**
 - **Overhead and payload**

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017



Communication Technologies Criteria: 6- Constrained-Node Networks

- **Data rate and throughput**

- The data rates available from IoT access technologies range from 100 bps with protocols such as Sigfox to tens of megabits per second with technologies such as LTE and IEEE 802.11ac.
- However, the actual throughput is less sometimes much less than the data rate.
- Technologies not particularly designed for IoT, such as cellular and Wi-Fi, match up well to IoT applications with high rate requirements.
 - For example, nodes involved with video analytics have a need for high data rates.
 - These nodes are found in retail, airport, and smart cities environments for detecting events and driving actions.
 - Because these types of IoT endpoints are not constrained in terms of computing or network bandwidth, the design guidelines tend to focus on application requirements, such as latency

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017

Communication Technologies Criteria: 6- Constrained-Node Networks

- **Data rate and throughput,**

- While it may not be important for constrained nodes that send only one message a day, real throughput is often very important for constrained devices implementing an IP stack.
 - In this case, throughput is a lower percentage of the data rate, even if the node gets the full constrained network at a given time.
- For example, let's consider an IEEE 802.15.4g subnetwork implementing 2FSK modulation at 150 kbps for the 915 MHz frequency band. (The IEEE 802.15.4g protocol is covered in more detail later)
- To cover the border case of distance and radio signal quality, Forward Error Correction (FEC) will be turned on, which lowers the data rate from 150 kbps to 75 kbps.
- If you now add in the protocol stack overhead, the two-way communication handling, and the variable data payload size, you end up with a maximum throughput of 30 to 40 kbps.
- This must be considered as the best value because the number of devices simultaneously communicating along with the topology and control plane overhead will also impact the throughput.

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things**, Cisco press, 2017

Communication Technologies Criteria: 6- Constrained-Node Networks



- **Latency**
 - Much like throughput requirements, latency expectations of IoT applications should be known when selecting an access technology.
 - This is particularly true for wireless networks, where packet loss and retransmissions due to interference, collisions, and noise are normal behaviors.
 - On constrained networks, latency may range from a few milliseconds to seconds.
 - Applications and protocol stacks must cope with these wide ranging values.
 - For example, UDP at the transport layer is strongly recommended for IP endpoints communicating over LLNs.

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017



Communication Technologies Criteria: 6- Constrained-Node Networks

- **Overhead and payload**

- When considering constrained access network technologies, it is important to review the MAC payload size characteristics required by applications.
- In addition, you should be aware of any requirements for IP. The minimum IPv6 MTU size is expected to be 1280 bytes.
 - Therefore, the fragmentation of the IPv6 payload has to be taken into account by link layer access protocols with smaller MTUs.
- The use of IP on IoT devices is an open topic of discussion.
 - For the more constrained classes of devices, like Class 0 and Class 1 devices, it is usually not possible or optimal to implement a complete IP stack implementation.

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017


Communication Technologies Criteria: 6- Constrained-Node Networks

- **Overhead and payload**
 - For technologies that fall under the LLN definition but are able to transport IP, such as IEEE 802.15.4 and 802.15.4g, IEEE 1901.2, and IEEE 802.11ah, Layer 1 or Layer 2 fragmentation capabilities and/or IP optimization is important.
 - For example,
 - The payload size for IEEE 802.15.4 is 127 bytes and requires an IPv6 payload with a minimum MTU of 1280 bytes to be fragmented.
 - On the other hand, IEEE 802.15.4g enables payloads up to 2048 bytes, easing the support of the IPv6 minimum MTU of 1280 bytes.

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017

Communication Technologies Criteria: 6- Constrained-Node Networks



- **Overhead and payload**
 - Most LPWA technologies offer small payload sizes.
 - These small payload sizes are defined to cope with
 - Low data rate and
 - Low time over the air or duty cycle requirements of IoT nodes and sensors.
 - For example, payloads may be as little as 19 bytes using LoRaWAN technology or up to 250 bytes, depending on the adaptive data rate (ADR).
 - While this doesn't preclude the use of an IPv6/6LoWPAN payload, as seen on some endpoint implementations, these types of protocols are better suited to Class 0 and 1 nodes, as defined in RFC 7228.
- 

* **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017

Contents



- Introduction
- Physical and Link Layers Protocols (IoT Access Technologies)
 - Physical Layer Issues
 - Communication Technologies Criteria
 - Communication Technologies and Protocols
- Network Layer Protocols (IP as the IoT Network Layer)
- Transport Layer Protocols
- Application Layer Protocols

Mostly adopted from Chapters 4, 5, and 6 of **IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing**, Cisco press, 2017

