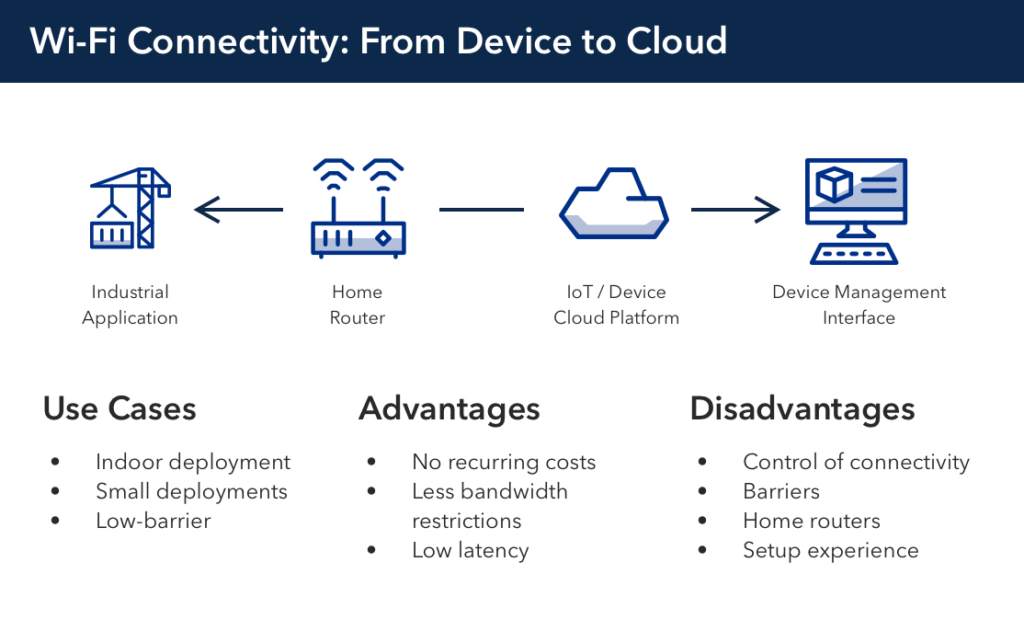
# How to Choose the Right IoT Connectivity Protocol for Your Connected Device

Choosing the right IoT connectivity protocol for your device can feel pretty straight-forward. Most assume that Wi-Fi is best for indoor deployments, while cellular connectivity is best for outdoor deployments.

However, it’s not so black and white. Our team finds that customers underestimate the advantages and disadvantages for certain radio technologies. In some cases, we actually recommend cellular protocols to companies who are planning to deploy indoors. That’s because cellular IoT connectivity protocols can be easier to set up, provide better reliability, and allow the maker of the device to be in control of the data.

Many other decisions can impact the type of radio you should choose, such as availability of infrastructure (cellular network and Wi-Fi networks), or the price sensitivity of your customers. That’s why in this guide, we’ll discuss different IoT connectivity protocols, and which one could be the best connectivity option for your IoT solution.

**Everything You Need to Know About Wi-Fi Connectivity**



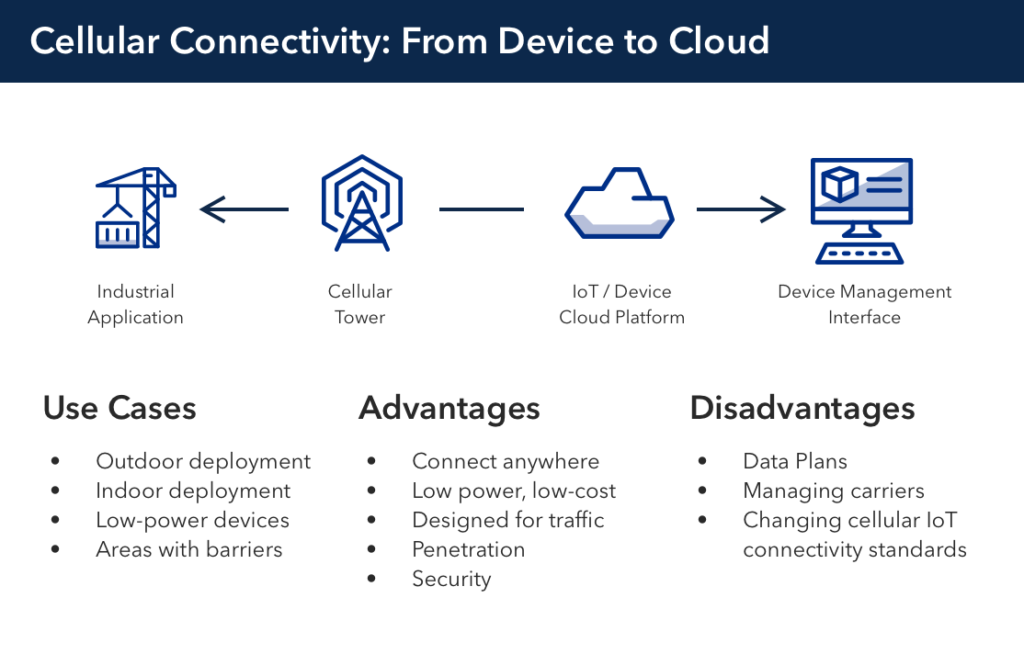
**Advantages**

* **Minimal to no recurring cost —**Unlike cellular devices, Wi-Fi connected devices come with no recurring costs. That’s because cellular devices require a SIM card and carry the cost of a data plan from a cellular provider. Wi-Fi also tends to be cheaper because you don’t have to pay to access the network infrastructure (i.e. the Wi-Fi network). It should be noted that IoT platforms often charge a small recurring fee for connectivity usage, including Wi-Fi. However, this recurring fee is much cheaper than your typical cellular connectivity data plan.
* **No bandwidth restrictions —**No bandwidth restrictions make Wi-Fi a good choice for high bandwidth applications (like audio and video streaming). If you intend to stream security video footage from one place to another, Wi-Fi may be the way to go. For businesses, you don’t need to consider the cost of bandwidth because your devices will leverage your customers’ existing Wi-Fi networks.
* **Low latency** — Due to complex carrier networking infrastructure, cellular devices typically have to transmit data through more systems than Wi-Fi. If the device is roaming, messages must go even farther and are often given lower priority. Additionally, in order to reach long distances from the tower, cellular radio protocols have to tolerate significant message loss by taking extra time to retransmit. As a result, Wi-Fi based devices exhibit lower latency than cellular devices.

**Disadvantages**

* **Control of IoT connectivity —**Wi-Fi connected devices are dependent on the router’s connection to the Internet. If your home router provides a weak Wi-Fi signal, your device will have a poor connection. Unlike cellular, a Wi-Fi device requires that your customers know how to configure the device for access to their network. Wi-Fi connectivity also puts device data in the hands of your customer, and that is less than optimal if the value of the solution resides in the data.
* **Barriers —**Wall construction material (such as drywall, metal framing, and building materials) often interfere with Wi-Fi signals.
* **Home Routers —**Wi-Fi is great for many indoor connected products, as the devices are generally close to the router. Although, outdoor smart products (like connected hot tubs) are often too far from the home router to establish a reliable connection. Many products are available to help extend a Wi-Fi signal. However, this requires extra setup to get started. For outdoor coverage, Wi-Fi extenders or special outdoor access points are necessary, which also require power and add additional points of possible failure, plus additional costs.
* **Setup experience —**Users constantly change SSIDs and passwords, which can easily disrupt a device’s connection to a router. Certain firewalls and other connection filtering solutions also require IT administration to configure a “work-around”, creating more setup complications. Cellular simply ‘works’ without any end-user configuration.

**Everything You Need to Know About Cellular Connectivity**



**Advantages**

* **Connect anywhere, anytime —** Cellular networks cover 90 percent of the world’s population, allowing you to connect your IoT device pretty much anywhere.
* **Low power, low-cost —** In recent years, the power and cost of cellular chips have reduced dramatically, meaning you can swap out cellular for Wi-Fi at a similar cost and power consumption. Cellular is now comparable in cost and power to Wi-FI, so you can consider them for more use cases.
* **Designed for traffic —**Existing cellular infrastructures are designed to handle constant communication. Unlike Wi-Fi networks, cellular network quality is going to be more consistent across the United States. That’s because you’re essentially paying a company (like AT&T or Verizon) to manage and provide a strong connection. You’re also are not limited by how much data you can send over a cellular network due to no limiting regulations.
* **Penetration —** Cellular communication protocols are better at reaching hard to reach or underground places because they can penetrate solid barriers easier.
* **Security**— With a cellular network, you are paying another company to manage security for you, which makes security breaches less likely. On the other hand, Wi-Fi networks can easily be hacked if end-users don’t properly update and patch their home Wi-Fi networks.

**Disadvantages**

* **Data Plans** – Accessing cellular infrastructure carries a recurring cost that not all IoT business models can support.
* **Managing carriers** — Cellular carriers can be a pain to work with. It’s best to choose an IoT platform that takes care of the cellular carriers for you. Cellular carriers are more likely to respond to IoT providers faster because they are taking care of a larger amount of devices. If you’re a small business, you’re not going to be as high of a priority for cellular carriers. They will take care of larger clients before they take care of the smaller use cases, which is why IoT providers have an advantage to negotiate strong cellular carrier relationships.
* **Changing cellular IoT connectivity standards**— Newer and better cellular standards are always coming out. Once it was about 3G, now it’s all about LTE. Fortunately, current LTE standards are designed to be deployable for the next 10+ years. So, you don’t need to change any time soon. However, Wi-Fi formats and structures change frequently with changing technologies. Cellular infrastructure is regulated by governments and maintained by companies dedicated to uptime.

**How to Choose the Right Cellular Connectivity Option**

Unlike Wi-Fi, you have to make additional considerations on the type of cellular IoT connectivity you want for your IoT device. At the moment, 2G and 3G radio technologies are being phased out, so that eliminates some of the potential options. But there are still other radio technologies that need to be considered like Cat-M1 (LTE) and NB-IoT.

**Cat-M1**

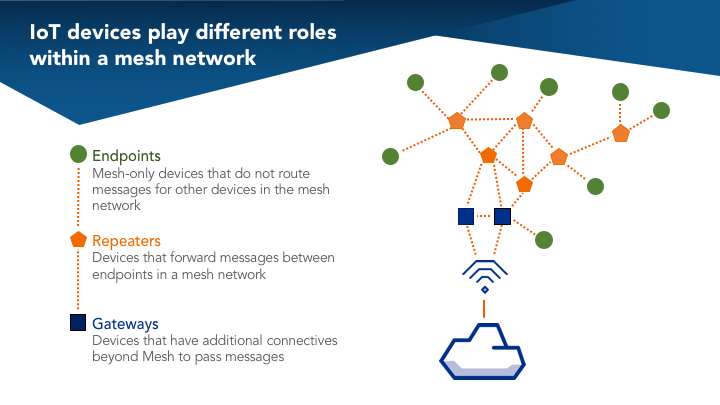
Category M1 (Cat-M1) is one of the newest cellular protocols available for IoT applications. Cat-M1 is an LTE chipset that is designed to integrate with sensors — it consumes less power, which means fewer truck visits and longer uptime. Verizon and AT&T just launched Cat-M1 networks a year ago, and IoT platforms  are starting to offer Cat-M1 as a part of their cellular connectivity offerings.

**Narrowband IoT**

Narrowband IoT (also known as NB-IoT or LTE-NB1) is a proposed Low Power Wide Area (LPWA) technology that is supposed to work anywhere. NB-IoT can be deployed within the existing LTE spectrum and carriers will be able to update their networks through firmware updates. NB-IoT can also be used as a standalone deployment within its own dedicated spectrum where deemed necessary.

**Everything You Need to Know About Mesh Connectivity**

As IoT platforms have matured, they have started to embrace a low-power, low-cost alternative that can bridge the gaps between these devices: wireless mesh networks.



A [wireless mesh network](https://blog.particle.io/2018/04/28/how-to-build-a-wireless-mesh-network/" \t "_blank) is an infrastructure of nodes (a mesh topology) that are wirelessly connected to each other. These nodes piggyback off each other to extend a radio signal (like a Wi-Fi or cellular connection) to route, relay, and proxy traffic to/from clients. Each node spreads the radio signal a little further than the last, minimizing the possibility of dead zones.

It should be noted that not all wireless mesh solutions provide these benefits, but this is the complete list that is unique to Particle Mesh:

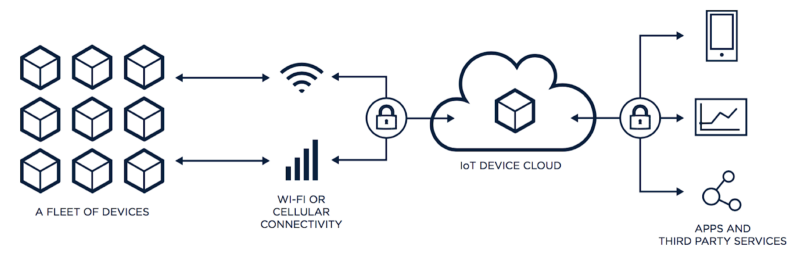
1. **No Single Point of Failure**– Build a local mesh network that is self-healing — if an individual device goes offline, the network can reconfigure itself to the closest connection. This means no data loss, no dead zones, no problems.
2. **Self-Extending** – Additionally, if you need to get more range out of a mesh system, you can add another node and the messages can hop through the mesh back to the gateway.
3. **Reliable Networks** – Interconnected devices can simultaneously transfer data smoothly and will not complicate the network connection. If one node goes down, another nearby node can pick up the connection and continue data communication.
4. **Low-cost, low-power** – Using wireless mesh networks eliminate the cost and complexity of installing fiber/wires between facilities. As more or less coverage is needed, wireless mesh nodes can be added or removed. Mesh uses comparable amounts of energy as Bluetooth, so you can design devices that last for 3-5 years then get tossed and replaced.

**Is Wireless Mesh Networking Right for You?**

When using wireless mesh networks for your IoT project, it is important that you consider these three core variables: installation, network management, and support.

1. **Installation —** This aspect entirely depends upon your intended application. You need to ask yourself if you actually needed a distributed set of mesh nodes for your use case. If you intend to implement wireless mesh networking for your home, this is relatively easy deployment that can be achieved with low-cost hardware. If you intend to implement mesh for commercial or industrial applications, you should setup a small-scale, prototype, mesh network to determine the efficiency of the system before deploying a mesh networking system at large.
2. **Device Management** — Most wireless mesh networking solutions come with some form of device or network management through a desktop or mobile application. When comparing solutions, it’s important to find one that allows you to manage fleets of devices, monitor event logs, perform diagnostics, and send updates wirelessly. The more control you have over your mesh-topography the better.
3. **Support —** When selecting a mesh-solution, it’s also important to consider the community surrounding it. Mesh networking solutions with limited adoption will have fewer resources available to aid you in development. For example, Particle’s development kits have a large developer community surrounding it, which makes it easier to find information and support when needed. Also, by selecting a more widely adopted wireless mesh networking solution, you will ensure that integrating your IoT device with existing cloud services will be easy.

**How to Choose the Right IoT Connectivity Platform**



When examining IoT connectivity protocols, you also need to examine the current IoT platforms on the market. You need to choose an IoT platform that provides the right IoT connectivity for your solution. It’s often difficult to choose the right IoT platform because they all market themselves in a different way and don’t provide the same solutions. So, here are some questions you should ask yourself when choosing an IoT platform for your connectivity needs:

* **IoT Connectivity** — How well does the vendor’s network coverage fit your business’s current and future initiatives?
* **Method of IoT connectivity** — What type of IoT connectivity do you need? Do you need a Wi-Fi or cellular solution for your IoT product? You need to assess these needs and see how the vendor can address them.
* **Geographic Coverage** — Do they provide embedded sim with global support? Does the IoT platform cover the regions your business needs?
* **Data Plan —**Does the vendor offer a fair data plan? You’ll want the ability to pause or suspend your data services at any time and the ability to control how much data that is used.
* **Data Access** **—** How will you integrate the data acquired through the IoT platform with your enterprise back ends and current cloud service? What do you plan to do with this data? Does the service match those needs?
* **Type of service** **—** How does the IoT platform describe and sell themselves? Some services are purely IoT connectivity platforms, while others are end-to-end solutions that offer the hardware, software, and connectivity. You need to assess what your business needs. How will your needs change over time?

**The Bottom Line**

Choosing the right IoT connectivity protocol for your business or connected project is an important decision. You must consider the advantages and disadvantages of each radio protocol before moving forward with your project. Taking the time to become acquainted with the benefits of each radio protocol will save you a lot of headache and heartache down the road.