IBM

developerWorks®

Connecting all the things in the Internet of Things

A guide to selecting network technologies to solve your IoT networking challenges

Anna Gerber

January 03, 2018
(First published May 23, 2017)

In this guide for IoT connectivity, learn about widely adopted technologies and standards for IoT networking and why you might choose one network protocol over another. Also, learn about the key considerations and challenges related to networking in IoT.

IoT 101: Getting started with IoT development

This article is part of the IoT 101 learning path, a quick-start guide for IoT developers.

- IoT concepts and skills
- IoT hardware guide
- IoT networking guide (this article)
- IoT platforms
- Tutorial: Build a simple home automation system

Communication is central to the Internet of Things. Networking technologies enable IoT devices to communicate with other devices as well as with applications and services that are running in the cloud. The internet relies on standardized protocols to ensure that communication between heterogeneous devices can occur securely and reliably. Standard protocols specify the rules and formats that devices use for establishing and managing networks, as well as for transmission of data across those networks.

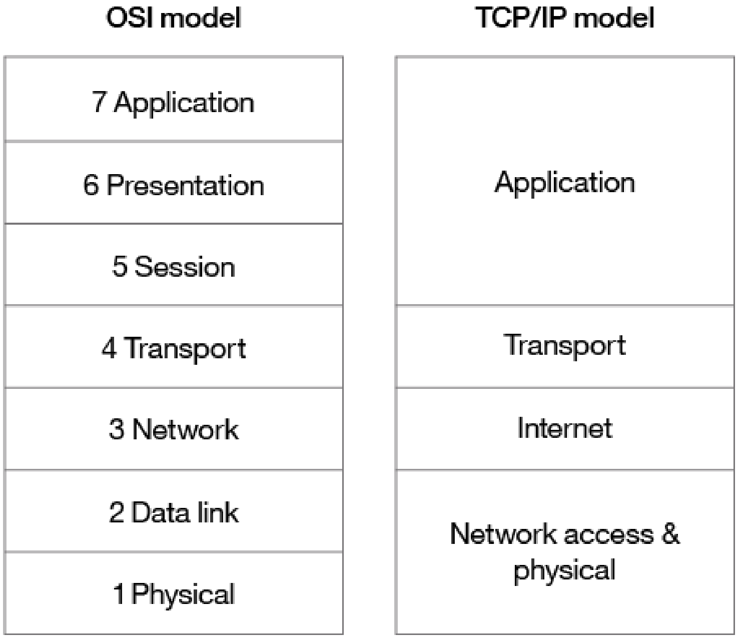
We often describe networks as being built up from a stack of technologies, with technologies at the bottom of the stack, such as Bluetooth LE, relating to physically connecting devices, while technologies further up the stack, such as IPv6, relating to logical device addressing and routing of network traffic. Technologies at the top of the stack are used by the applications that are running on top of those layers, for example, message queuing technologies.

In this article, I describe some widely adopted technologies and standards for IoT networking. I also explain when you might want to choose one network protocol over another. I then discuss key considerations and challenges that are related to networking within IoT, including range, bandwidth, power usage, intermittent connectivity, interoperability, and security.

Networking standards and technologies

The Open Systems Interconnection (OSI) model is an ISO-standard abstract model that describes a stack of seven protocol layers. From the top down, these layers are: application, presentation, session, transport, network, data link and physical. TCP/IP, or the Internet Protocol suite, underpins the internet, and it provides a simplified concrete implementation of these layers in the OSI model.

Figure 1. OSI and TCP/IP networking models



The TCP/IP model includes only four layers, merging some of the OSI model layers (see Figure 1):

- **Network Access & Physical Layer**
  This TCP/IP Layer subsumes both OSI layers 1 and 2. The physical (PHY) layer (Layer 1 of OSI) is concerned with how each device is physically connected to the network with hardware, for example with an optic cable, wires, or radio in the case of wireless network like wifi (IEEE 802.11 a/b/g/n). At the link layer (Layer 2 of OSI), devices are identified by a MAC address, and protocols at this level are concerned with physical addressing, such as how switches deliver frames to devices on the network.
- **Internet Layer**
  This layer maps to the OSI Layer 3 (network layer), which relates to logical addressing. Protocols at this layer define how routers deliver packets of data between source and destination hosts identified by IP addresses. IPv6 is commonly adopted for IoT device addressing.
- **Transport Layer**
  The transport layer (Layer 4 in OSI) is focused on end-to-end communication and provides features including reliability, congestion avoidance, and guaranteeing that packets will be delivered in the same order that they were sent. UDP (User Datagram protocol) is often adopted for IoT transport for performance reasons.
- **Application Layer**

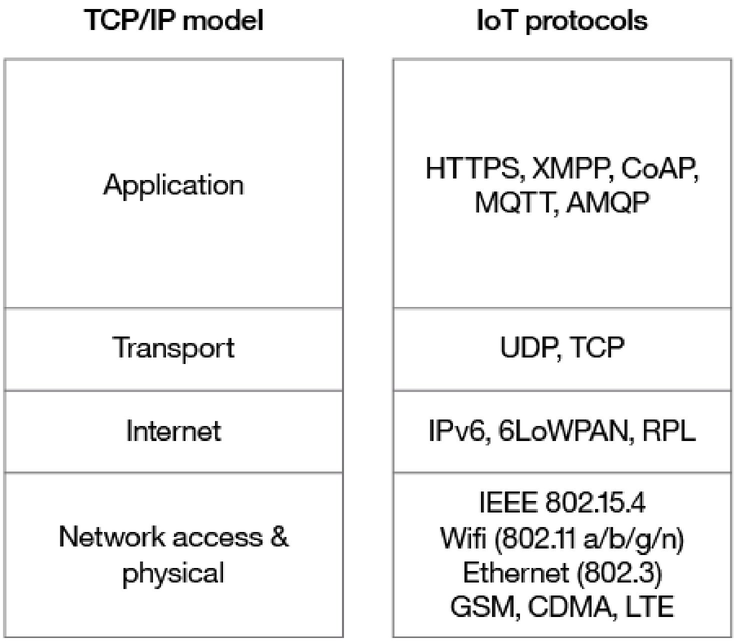
> The application layer (Layers 5, 6, and 7 in OSI) covers application-level messaging. HTTP/S is an example of an application layer protocol that is widely adopted across the internet.

Although the TCP/IP and OSI models provide you with useful abstractions for discussing networking protocols, and the specific technologies that implement each protocol, in practice, some protocols don't fit neatly into these layered models. For example, the Transport Layer Security (TLS) protocol that implements encryption to ensure privacy and data integrity of network traffic can be considered to operate across OSI layers 4, 5, and 6.

IoT networking protocols

Some of the networking protocols that are widely adopted within IoT and where they fit within the TCP/IP layers are shown in Figure 2.

Figure 2. IoT network protocols mapped to the TCP/IP model



TCP/IP model	IoT protocols
Application	HTTPS, XMPP, CoAP, MQTT, AMQP
Transport	UDP, TCP
Internet	IPv6, 6LoWPAN, RPL
Network access & physical	IEEE 802.15.4 Wifi (802.11 a/b/g/n) Ethernet (802.3) GSM, CDMA, LTE

Many emerging and competing networking technologies are being adopted within the IoT space. Multiple technologies are offered by different vendors or are aimed at different vertical markets like home automation, healthcare, or industrial IoT, often provide alternative implementations of the same standard protocols. For example, IEEE 802.15.4 describes the operation of low-rate wireless personal area networks (LR-WPANs) and is implemented by several competing technologies including ZigBee, Z-Wave, EnOcean, SNAP, and 6LoWPAN.

Technologies used for internet connectivity, like Ethernet, for example, can often be applied within the IoT; however, new technologies are being developed specifically to meet the challenges of IoT. As you look further down the stack toward physical transmission technologies, you face more challenges that are specific to IoT devices and IoT contexts.

The structure of a network is known as its topology. The most common network topologies that are adopted within IoT are star and mesh topologies. In a star topology, each IoT device is directly connected to a central hub (gateway) that communicates the data from the connected devices upstream. In mesh topologies, devices connect to other devices within range, and nodes within the network can act as simple sensor nodes, as sensor nodes that also route traffic, or as gateway nodes. Mesh networks are more complex than networks with star topologies, but have the advantage of being more resilient to failure because they don't rely on a single central gateway.

Network access and physical layer IoT network technologies

IoT network technologies to be aware of toward the bottom of the protocol stack include cellular, wifi, and Ethernet, as well as more specialized solutions such as LPWAN, Bluetooth Low Energy (BLE), ZigBee, NFC, and RFID.

To learn more about NB-IoT, which according to a Gartner report is becoming the standard for LPWAN networks, read this IoT for All article.

- **LPWAN**
  (Low Power Wide Area Network) is a category of technologies that are designed for low-power, long-range wireless communication, and so they are ideal for use within large-scale deployments of low-power IoT devices like wireless sensors. LPWAN technologies include LoRa (LongRange physical layer protocol), Haystack, SigFox, LTE-M, and NB-IoT(Narrow-Band IoT).
- **Cellular**
  The LPWAN NB-IoT and LTE-M standards are aimed at providing low-power, low-cost IoT communication options using existing cellular networks. NB-IoT is the newest of these standards and is focused on long-range communication between large numbers of primarily indoor devices. LTE-M and NB-IoT were developed specifically for IoT, however existing cellular technologies are also frequently adopted for long-range wireless communication. These include 2G (GSM), which is mostly used in legacy devices, and which is currently being phased out, as well as CDMA, 3G, and 4G.
- **Bluetooth Low Energy (BLE)**
  BLE is a low-power version of the popular Bluetooth 2.4 GHz wireless communication protocol. It is designed for short-range (no more than 100 meters) communication, typically in a star configuration, with a single primary device that controls several secondary devices. Bluetooth operates across both layers 1 (PHY) and 2 (MAC) of the OSI model, which is shown in Figure 1. BLE is best suited to devices that transmit low volumes of data in bursts, as the devices are designed to sleep to save power when they are not transmitting data. Personal IoT devices like wearable health and fitness trackers often use BLE.

- **ZigBee**
  ZigBee also operates on 2.4GHz wireless communication spectrum, but it has a longer range than BLE of up to 100 meters. It also has a slightly lower data rate (250 kbps maximum compared to 270 kbps for BLE) than BLE. ZigBee is a mesh network protocol, and unlike BLE, not all devices can sleep between bursts, depending on their position in the mesh and whether they need to act as routers or controllers within the mesh. ZigBee was designed for building and home automation applications, like controlling lights. Another closely related technology to ZigBee is Z-Wave, which is also based on IEEE 802.15.4 MAC. Z-Wave was also designed for home automation, and it was a proprietary technology that was recently released as a public domain specification.
- **NFC**
  The near field communication (NFC) protocol is used for very small range communication (up to 4 cm), such as holding an NFC card or tag next to a reader. NFC is often used for payment systems, but it is also useful for check-in systems and smart labels in asset tracking in Industrial IoT applications.
- **RFID**
  RFID stands for Radio Frequency Identification. RFID tags store identifiers and data and are attached to devices for reading by an RFID reader. The typical range of RFID is less than a meter. RFID tags can be active, passive, or assisted passive. Passive tags are ideal for devices without batteries, as the ID is passively read by the reader. Active tags periodically broadcast their ID, while assisted passive tags become active when RFID reader is present. **Dash7** is a communication protocol that uses active RFID that is designed to be used within Industrial IoT applications for secure long-range communication. Similar to NFC, a typical use case for RFID is tracking inventory items within retail and industrial IoT applications.
- **Wifi**
  Wifi is standard wireless networking based on IEEE 802.11a/b/g/n specifications. 802.11n offers the highest data throughput, but at the cost of high power consumption, so IoT devices might only use 802.11b or g for power conservation reasons. Although wifi is adopted within many prototype and current generation IoT devices, as longer-range and lower-power solutions become more widely available, it is likely that wifi will be superseded by these lower-power alternatives.
- **Ethernet**
  Widely deployed for wired connectivity within local area networks, Ethernet implements the IEEE 802.3 standard. Not all IoT devices need to be wireless devices that are designed to be stationery. For example, sensor units that are installed within a building automation system can use wired networking technologies like Ethernet. Power line communication (PLC) is an alternative hard-wired solution that uses existing electrical wiring instead of dedicated network cables.

Internet layer IoT network technologies

Internet layer technologies (OSI Layer 3) are concerned with identifying and routing packets of data. Technologies that are commonly adopted for IoT that are related to this layer include IPv6, 6LoWPAN, and RPL.

- **IPv6**

At the Internet Layer, devices are identified by IP addresses. IPv6 is typically used for IoT applications over legacy IPv4 addressing. IPv4 is limited to 32-bit addresses, which only provide around 4.3 billion addresses in total, which is less than the current number of IoT devices that are connected, while IPv6 uses 128 bits, and so provides 2^{128} addresses (around 3.4×10^{38} or 340 billion billion billion billion) addresses. In practice, not all IoT devices need public addresses. Of the tens of billions of devices that are expected to connect to the IoT over the next few years, many will be deployed in private networks that will use private address ranges and only communicate out to other devices or services on external networks by using gateways.

- **6LoWPAN**
  The IPv6 Low Power Wireless Personal Area Network (6LoWPAN) standard allows IPv6 to be used over 802.15.4 wireless networks. 6LoWPAN is often used for wireless sensor networks, and the Thread protocol for home automation devices also runs over 6LoWPAN.
- **RPL**
  The Internet Layer also covers routing. IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is designed for routing IPv6 traffic over low-power networks like those networks implemented over 6LoWPAN. RPL (pronounced "ripple") is designed for routing packets within constrained networks such as wireless sensor networks, where not all devices are reachable at all times and where there are high or unpredictable amounts of packet loss. RPL can compute the optimal path by building up a graph of the nodes in the network based on dynamic metrics and constraints like minimizing energy consumption or latency.

Application layer IoT network technologies

HTTP and HTTPS are ubiquitous across internet applications, which is true also within IoT, with RESTful HTTP and HTTPS interfaces widely deployed. CoAP (Constrained Application Protocol) is like a lightweight HTTP that is often used in combination with 6LoWPAN over UDP. Messaging protocols like MQTT, AMQP, and XMPP are also frequently used within IoT applications:

- **MQTT**
  Message Queue Telemetry Transport (MQTT) is a publish/subscribe-based messaging protocol that was designed for use in low bandwidth situations, particularly for sensors and mobile devices on unreliable networks.
- **AMQP**
  Advanced Message Queuing Protocol (AMQP) is an open standard messaging protocol that is used for message-oriented middleware. Most notably, AMQP is implemented by RabbitMQ.
- **XMPP**
  The Extensible Messaging and Presence Protocol (XMPP) was originally designed for real-time human-to-human communication including instant messaging. This protocol has been adapted for machine-to-machine (M2M) communication to implement lightweight middleware and for routing XML data. XMPP is primarily used with smart appliances.

Your choice of technologies at this layer will depend on the specific application requirements of your IoT project. For example, for a budget home automation system that involves several sensors, MQTT would be a good choice as it is great for implementing messaging on devices without much storage or processing power because the protocol is simple and lightweight to implement.

IoT networking considerations and challenges

When you consider which networking technologies to adopt within your IoT application, be mindful of the following constraints:

- Range
- Bandwidth
- Power usage
- Intermittent connectivity
- Interoperability
- Security

Range

Networks can be described in terms of the distances over which data is typically transmitted by the IoT devices attached to the network:

- **PAN (Personal Area Network)**
  PAN is short-range, where distances can be measured in meters, such as a wearable fitness tracker device that communicates with an app on a cell phone over BLE.
- **LAN (Local Area Network)**
  LAN is short- to medium-range, where distances can be up to hundreds of meters, such as home automation or sensors that are installed within a factory production line that communicate over wifi with a gateway device that is installed within the same building.
- **MAN (Metropolitan Area Network)**
  MAN is long-range (city wide), where distances are measured up to a few kilometers, such as smart parking sensors installed throughout a city that are connected in a mesh network topology.
- **WAN (Wide Area Network)**
  WAN is long-range, where distances can be measured in kilometers, such as agricultural sensors that are installed across a large farm or ranch that are used to monitor micro-climate environmental conditions across the property.

Your network should be designed to get the data from the IoT devices to where it will be used. So, make sure that you select a network protocol that matches the range that is required for your use case. For example, you shouldn't choose BLE for a WAN application that needs to operate over a range of several kilometers. If transmitting data over the required range presents a challenge, consider edge computing, which moves the analysis to the data out to the devices, rather than moving the data elsewhere for processing.

Bandwidth

Bandwidth, or the amount of data that can be transmitted in a specific period of time, limits the rate at which data can be collected from IoT devices and transmitted upstream. Consider these factors:

- The volume of data that each device is generating
- The number of devices that are deployed in a network
- Whether the data is being sent as a constant stream or in intermittent bursts, as the bandwidth that is available will need to cope with the peak periods

The packet size of the networking protocol that you choose should match up with the size of the data that is typically being transmitted. It is inefficient to send packets padded out with empty data, but on the flip side there are overheads in splitting larger chunks of data up across too many small packets. Data transmission rates are not always symmetrical (that is, upload rates might be slower than download rates). So, if there is two-way communication between devices, data transmission needs to be factored in. Wireless and cellular networks are traditionally low-bandwidth, so consider whether a wireless technology is the right choice for high-volume applications.

Also, consider whether all of the raw data needs to be transmitted. One solution might be to capture less data by sampling less frequently, capturing fewer variables, or performing some filtering on the device to drop insignificant data. If you aggregate the data before you transmit it, you help to reduce the volume of data to be transmitted, but then this process has implications on flexibility and granularity in the upstream analysis. Aggregation and bursting is not always suitable for time-sensitive or latency-sensitive data either. All of these techniques also increase the data processing and storage requirements for the IoT device.

Power usage

Transmitting data from a device consumes power, and transmitting data over long ranges requires more power than over a short range. You must consider the devices that operate on a battery to conserve power to prolong the life of the battery and reduce operating costs. To prolong the battery life, you can put the device into sleep mode whenever it is idle. It is a good idea to model the energy consumption of the device under different loads and different network conditions to ensure that the device's power supply and storage capacity matches with the power that is required to transmit the necessary data by using the networking technologies that you adopted.

Intermittent connectivity

IoT devices aren't always connected. In some cases, devices will connect periodically by design in order to save power or bandwidth. However, sometimes an unreliable network might cause devices to drop off due to connectivity issues. Sometimes quality of service issues, such as dealing with interference or channel contention on a wireless network using a shared spectrum.

Interoperability

With so many different devices connecting to the IoT, interoperability can be a challenge. Adopting standard protocols has been the traditional approach for maintaining interoperability on the internet. However, for the IoT, standardization processes sometimes struggle to keep up with the rapid pace of change and technologies are released based on upcoming versions of standards that are still subject to change. In these cases, consider the ecosystem around the technologies; that is, ask these questions: Are they widely adopted? Are they open versus proprietary? How many implementations are available?

Security

Security is always a priority, so be sure to select networking technologies that implement end-to-end security, including authentication, encryption, and open port protection. For example, IEEE 802.15.4 includes a security model that provides security features that include access control, message integrity, message confidentiality, and replay protection, which are implemented by technologies based on this standard such as ZigBee.

- **Authentication**
  Adopt secure protocols to support authentication at the device level, for gateways, users, and applications and services. For example, consider adopting the X.509 standard for device authentication.
- **Encryption**
  If you are using wifi, you can use Wireless Protected Access 2 (WPA2) for wireless network encryption or you might adopt a Private Pre-Shared Key (PPSK) approach. To ensure privacy and data integrity for communication between applications, be sure to adopt TLS or Datagram Transport-Layer Security (DTLS), which is based on TLS, but adapted for unreliable connections that run over UDP. TLS encrypts application data and ensures its integrity.
- **Port protection**
  Port protection ensures that only the ports that are required for communication with the gateway or upstream applications or services remain open to external connections. All other ports should be disabled or protected by firewalls. For example, device ports might be exposed when exploiting Universal Plug and Play (UPnP) vulnerabilities, so UPnP should be disabled on the router.

Conclusion

Selecting the IoT networking technologies to adopt involves compromise, across the board. Your choice of networking technologies will have an impact on the design of your IoT devices, and there are dependencies among most of the considerations that I discussed in this article. For example, network range, data rate, and power consumption are all directly related. If you increase the network range or rate and volume of data that is transmitted, your IoT devices will almost certainly require additional power to transmit the data under those conditions.

For a basic home automation project, the power consideration criterion is likely to be of low importance, as the device would most likely be powered directly from a wall socket. Bandwidth limitations and drop-outs in connectivity would be higher priorities, so you can adopt wifi because it provides reasonable bandwidth and also makes it easier to build the project by using commodity hardware. However, wifi is not optimized for low-power devices, so this choice might not be a good choice for a battery-powered device.

In this article, I've provided an overview of some of the most common networking protocols and technologies for IoT. You need to consider your requirements in light of these IoT networking challenges to find the technologies that will be the best fit for your IoT application.