IoT Basics:
The Ultimate Guide to
IoT Terminology

35 Top IoT Terms You Need to Know

LinkLabs

LinkLabs

35 Top IoT Terms You Need to Know

The Internet of Things (IoT) is the connectivity of physical objects such as vehicles, devices, buildings, and electronics, and the networks that allow them to interact, collect, and exchange data. After years of hype and enthusiasm, the IoT has finally gained legitimacy. Now a first step for enterprise and industry innovators looking to develop IoT solutions is knowing the top terms that explain this trend and IoT connectivity.

6LoWPAN

An acronym that combines the latest version of the Internet Protocol (IPv6) and Low-power Wireless Personal Area Networks (LoWPAN). 6LoWPAN is a protocol that allows power constrained IOT devices to avccess the TCP/IP internet directly.

Why it's important: 6LoWPAN allows for the smallest devices with limited processing ability to transmit information directly to the internet with a battery life that lasts for years.

Advanced Encryption Standard (AES)

Electronic data encryption specification, established in 2001, operating on a public/private key system. Planning for key management is important when implementing AES.

Why it's important: To date there are no known successful practical attacks having allowed illicit access of correctly implemented AES encrypted data. This is the standard for transport layer security in IOT devices.

Application Programming Interface (API)

A way for computers to talk to hardware or software platforms in a less complicated way.

Why it's important: Third parties use other company's API platforms as a point of integration. Designing applications to leverage APIs allows for faster development and easier paths to improve over time.

Big Data

A very large set of data that can be analyzed for patterns and trends. Big data provides valuable (and very profitable) insights that can be used to identify service or product opportunities and customer behaviors.

Why it's important: Analyzing big data moves enterprises away from making decisions by gut instinct into data-driven strategic choices. IOT devices have the potential to generate entirely new streams of data for big data processing.

Bluetooth Low Energy (BLE)

Also known as Bluetooth 4.0, this is a wireless, personal-area network with short-range and low-power consumption that allows for objects to transmit data.

Why it's important: This technology offers low-cost, safe, wireless connectivity and solves many of the earlier Bluetooth's pairing and performance headaches. This is the least expensive way to add short range wireless connectivity to devices.

Cloud Computing

"In the cloud" refers to a network of remote servers hosted online that store, manage, and process data.

Why it's important: Cloud computing is vital for large sets of data. It's great for those who need disaster recovery, collaboration controls, security, and an environmentally friendly way to store data.

Embedded Software
Instruction code that runs on hardware microcontrollers. Usually it is performing specific low-level functions, often without using an operating system.

Why it's important: Specialized for the particular hardware it runs on, embedded software often has time and memory constraints which must be addressed in IoT innovation. Most IOT devices leverage embedded software which can take longer to write than more abstracted server-side code.

Firmware Over-the-Air (FOTA)
A mobile technology enabling manufacturers to wirelessly repair bugs or remotely install new software, features, and services on a mobile device after product distribution.

Why it's important: FOTA is an efficient way to upgrade and update a mobile device wirelessly. Manufacturers can save resources on efficient and timely upgrades without having physical access to the device.

Gateway
A device that receives information from many other points on the network and transmits information to another network.

Why it's important: When multiple wireless protocols are mixed, a gateway is almost always requierd. The gateway is the stopping point for online communications, the hub through which data is sent back and forth.

General Packet Radio Service (GPRS)
A wireless communications standard on 2G and 3G cellular networks supporting a number of bandwidths and providing data rates of 56-114 kbps.

Why it's important: As cellular companies move to more advanced networks, GPRS networks may be more cost-effective for IoT networks. NB-IOT and LTE-M1 networks are being touted as replacements for these older cellular standards.

Industrial IoT (IIoT)
M2M communication for machinery and other industrial applications.

Why it's important: The IIoT enables machinery and equipment to transmit real-time information to an application. This allows operators to better understand equipment efficiency and identify preventative maintenance needs.

Industrial, Scientific, and Medical (ISM) Band
An unlicensed part of the RF spectrum used for general purpose data communications. In the US, the ISM bands are 915MHz, 2.4 GHz, and 5.5 GHz, whereas 2.4 GHz is the global unlicensed frequency, and has increasing amounts of interference.

Why it's important: This part of the radio spectrum can be used without a license in most countries.

Link Budget
An accounting of all of the losses (e.g. from antennas, structural attenuation, propagation loss) in a wireless communication system.

Why it's important: In order to "close the link," enough RF energy has to make it from the transmitter to the receiver.

Low-Power Wide Area (LPWA)
LPWA networks are built specifically for M2M communications and offer long-range, low-power consumption.

Why it's important: LPWANs solve cost and battery life issues that cellular technology cannot, and solve range issues that technologies like Bluetooth or BLE struggle with.

Low-Power Wireless Sensor Network
A group of spatially distributed, independent devices that collect data by measuring physical or environmental conditions with minimal power consumption.

Why it's important: Minimizing power consumption is key to achieving a longer lifetime for devices on wireless sensor networks.

LoRa Protocol (LoRaWAN)
A LPWAN specification deployed internationally to enable IoT and M2M, intended for carrier networks of wireless, battery-operated things.

Why it's important: Many carriers are testing LoRaWAN as a possible technology to support IOT networks.

LTE-M
An abbreviation for LTE-MTC (or machine-type communications), LTE-M is a more energy efficient part of the LTE system. Because of its extended discontinuous repetition cycle (eDRX) an endpoint can communicate with the tower or network on how often it will wake up to listen for the downlink.

Why it's important: LTE-M is one of three new standards, along with NB-IoT, from the cellular industry allowing devices that operate on carrier networks to be less expensive and more power efficient.

Machine to Machine (M2M)
Connected devices exchanging information with other connected devices, without human assistance.

Why it's important: Machines monitoring other machines, without the need of human intervention, are transforming many industries. For example, a machine can alert when a new part is needed or broken down, eliminating manual monitoring, which eats up valuable time and resources.

Media Access Control (MAC)
One of two sublayers in a network, the MAC address is a unique identifier allowing the physical medium (radio waves or wire signals) to be organized to pass data back and forth.

Why it's important: Upper layer protocols rely on the MAC layer to produce complex, functioning networks.

Mote
Primarily used in North America, this is one way of referring to an "endpoint" in the IoT. Also known as a node, this usually refers to a generic sensor out in the physical world.

Why it's important: The sensor does the data gathering, some processing and communicates with other connected nodes in the IoT network.

NB-IoT
Even simpler than NB-LTE-M, this is a proposed narrowband (NB) technology not based on LTE. Instead it will likely be deployed on a side band or in deprecated GSM spectrum.

Why it's important: Although not available yet, with chipsets (if they exist) in the prototype stage, this may be an inexpensive option when rolled out.

Near-Field Communication (NFC)
Low-power, low-speed, short-range radio communication standard that allows two-way communication between endpoints within very close proximity.

Why it's important: Popular as a contactless communication between mobile devices, NFC is used to send information without physical device connection.

Quality of Service (QoS)
QoS manages network capabilities and resources to provide a reliable backbone to IoT connectivity. In order to offer secure and predictable services, QoS can manage delays, bandwidth and packet loss by classifying traffic and registering channel limits.

Why it's important: With effective QoS management in place, there is a much better chance of receiving warnings or other high priority messages in near real-time.

Radiofrequency (RF)
Radio waves. This term generally means "wireless communication" when referred to in IoT discussions.

Why it's important: RF is fundamental to IoT connectivity. Many IoT devices have RF transceiver chipsets to transmit data long distances using minimal power.

Radio Frequency Identification (RFID)
Generally speaking, this is the use of strong radio waves to "excite" enough current in a small tag to send a radio transmission back. It works over short range, and only for small amounts of data.

Why it's important: RFID tags can be used to detect and record data such as temperature, movement, radiation levels, and thus can be very useful in asset monitoring and supply chain management.

RF Geolocation
A general term that applies to "finding" a radio transceiver with another — GPS is a good example.

Why it's important: Location is a critical part of many IOT solutions. For systems that have GPS, location is easy. When GPS doesn't work for cost or because the node is indoors, WiFi fingerprinting or BLE proximity can be used.

Repeater
A device that receives and retransmits a digital signal to extend network reach.

Why it's important: Repeaters boost the distance a signal can travel and help a transmitted communication overcome obstructions.

Smart Meter
An electronic device that collects data about consumption of energy (gas, electric) and communicates it back to the energy company and/or consumer.

Why it's important: Enabling two-way communication, smart meters gather and transmit IoT device information to the central network.

Software-Defined Network (SDN)
An approach to networking that decouples control of information flow from the hardware and gives it to a software controller.

Why it's important: This allows for less data to travel wirelessly, making it a potential strategy for IoT networks.

Structure Attenuation
The loss in intensity of radio waves through a medium (like radio waves through a brick wall).

Why it's important: Structure attenuation can slow data transmission in the IoT. Repeaters can be used to address this issue.

Transmission Control Protocol/Internet Protocol (TCP/IP)
The core standard protocol for internet-based communications. Some wireless systems "break" TCP/IP in order to lower the overhead of the on-air signals.

Why it's important: This protocol manages data packets at the TCP layer and handles addressing of those packets at the IP layer. With this protocol, gateways can recognize and route data.

Ultra-Wide Band (UWB)
A "spark gap" transmitter that emits a very weak, very wide (in frequency) pulse of RF energy. This signal is used mostly for localizing signals. Wide signal bandwidths are good for measuring distance.

Why it's important: UWB operates by generating short, narrow pulses and can be an attractive option for asset tracking and fleet/inventory management.

ZigBee/Z-Wave
Short-range, low-power wireless standards used for sensing and control, typically used for personal or home area networks, or in a wireless mesh for longer-range networks. Like 6LoWPAN, designed for low data-rate and battery-powered applications, but Zigbee and Z-Wave technology can require more nodes to function successfully — which can increase costs.

Why it's important: Information from one sensor node continues to hop from node to node until it gets to the gateway. Often seen in security system, home automation and lighting control applications.

These 35 terms only scratch the surface of all the acronyms and applications the IoT introduces. Still, this primer provides a solid foundation to start with.

Let Link Labs Help

Selecting the right wireless technology for your IoT or M2M project or application is a tough process; it all depends on what you're trying accomplish. Link Labs has experience with wireless technology benefits, drawbacks and range calculations for industrial monitoring, asset tracking, commercial consumables, and a variety of other applications. We're here to help foster and enable your IoT innovation.

Learn more about our Symphony Link IoT Solutions

EXPLORE SOLUTIONS

Talk to a Symphony Link Expert about your project

CONTACT US

About Link Labs

Link Labs (www.link-labs.com) provides a wireless, low power consumption, wide-area network (LPWAN) that enables enterprises to gain insight, gather information, and take control of devices using Link Labs' robust connectivity solutions.