The Internet Of Things Comes Together

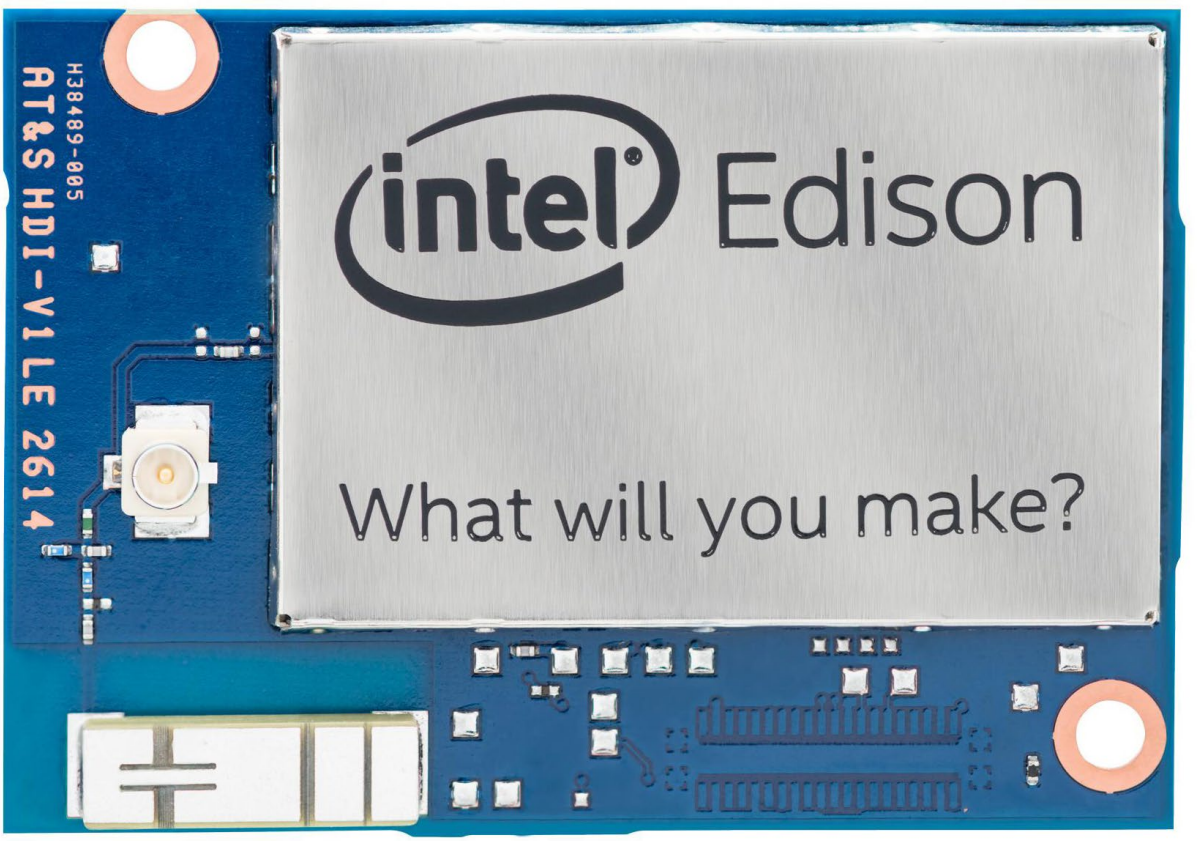
All Your Electronics, Connected

The hype around the Internet of Things is starting to reach a fever pitch. Here at CPU, our inbox has been flooded with press releases about the next generation of smart home devices, wearable electronics, and other IoT products that promise to make our lives easier. But how close are we to a world where the coffee maker is linked to your smartphone's alarm clock (helping us to avoid those torturous two minutes waiting for the coffee to brew), or where a smart HDTV recognizes when you're watching a movie and can automatically dim the lights?

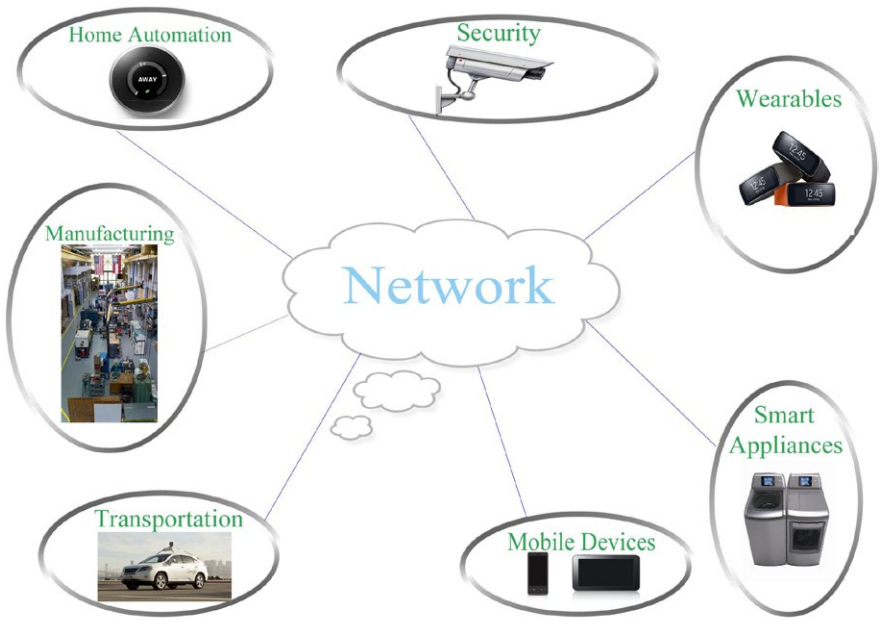
The quick answer is that the infrastructure and supporting technologies, such as cloud integration, RFID tags, motion sensors, and software standards, are in place. But there's still work to be done to make the IoT function transparently in the background. There are also big questions about how IoT devices will be secured. Here, we'll examine the current state of the IoT and where it's headed.

What Exactly Is The IoT?

The Internet of Things isn't the most descriptive term. Sure, we can infer that it covers technologies that are capable of connecting to and communicating via the Internet, but there's more to the process. Tom Kerber, director of research



Intel's Edison is a platform that makes it easy to add IoT connectivity to everyday technology.



The IoT consists of many different types of devices, many of which will be able to communicate with each other.

at Parks Associates, provides us with a breakdown. "The term 'IoT' is defined as a device that is connected to the Internet and has an accompanying virtual object in software." The virtual object is a digital representation of the real-word object. For example, it could be a digital identity or data gathered from a physical attribute, such as environmental conditions from sensors in your home, geolocation from smartphones and cars, and power consumption from heavy-load appliances.

"Consumers are able to view and manipulate the virtual object through an interface, such as a smartphone, tablet, or computer," says Kerber. "The device may also be queried or managed by other platforms, controllers, or applications that coordinate multiple objects." Management software can be either built into the device or delivered via cloud-based processing over the online connection.

The combination of the actual hardware (the thing), integrated software, and communication services can be used to powerful effect. For example, "wearable devices can indicate when a person is falling asleep and do things like lock doors or turn off lights and appliances," says Jonathan Collins, principal analyst at ABI Research.

Intelligent IoT devices often function in background, so you won't need to do anything to enjoy the benefits. For example, IoT devices can automate heating and cooling based on the outdoor temperature, turn on or off house lights when you get home and leave, and set your dishwasher and laundry to run during off-peak hours to reduce your bills. Wearable devices can connect to the web and keep a record of your exercise habits, as well as estimate how many calories you're burning during the course of a day. Of course, the Internet connection can also be utilized to remotely manage a device, if allowed.

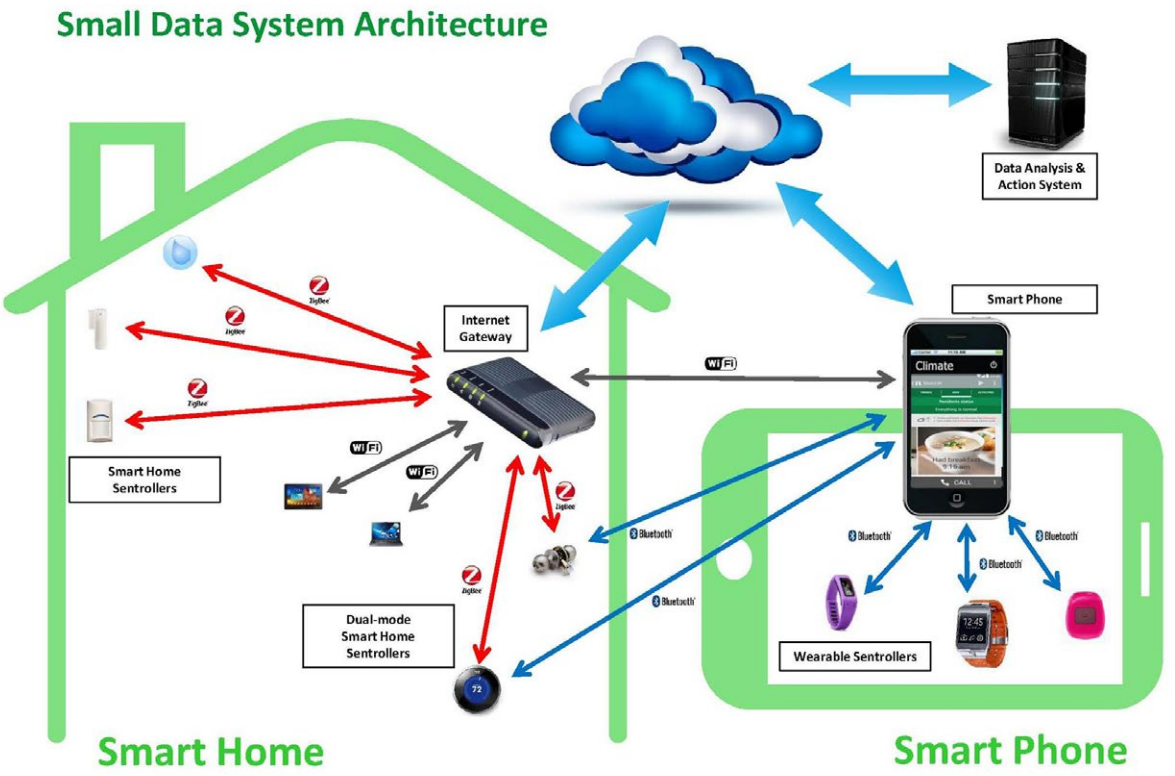
Bigger picture, the IoT is about smart technology that can share data to enhance capabilities and operation. "The IoT is creating a new world, a quantifiable and measureable world, where people and businesses can manage their assets in better informed ways to make timely and correct decisions of what they want or need to do," says Cees Links, founder and CEO of GreenPeak. "The rise of the IoT will create many practical improvements in our world, leading to more comfort and lower energy cost, better security, and more convenience."

IoT Tech

With the rapidly improving capabilities of SoCs and other pint-sized hardware, it's easier than ever for IoT developers to adapt environmental sensors, home electronics, monitoring systems,

"These are consumer-heavy environments, where individuals increasingly want devices to exhibit the same ease of use and connectivity as their smartphone."

-Jonathan Collins, principal analyst, ABI Research



The ZigBee standard can work with a wide variety of IoT devices in the home.

connected cars, etc. for IoT tasks. For example, Intel's Edison is a small module that lets IoT manufacturers easily integrate machine-to-machine communication and collaboration with smart devices.

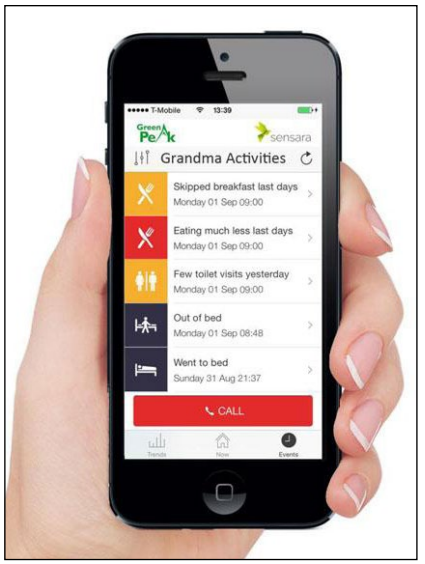
The Edison board measures just 1.4 inches long by 1 inch wide and comes with an Intel SoC featuring a 500MHz dual-core Intel Atom processor. Intel has also packed a 100MHz Quark microcontroller, 1GB of LPDDR3 POP memory, and dual-band Wi-Fi and Bluetooth connectivity. Intel's Edison is a complete platform, too. Intel uses open firmware and currently supports development on Arduino and C/C++. In the near future, Edison will support Node.JS, Python, RTOS, and Visual Programming.

Manufacturers are creating entire smart home systems, too. For example, GreenPeak has designed a network of sensors, called the Family Lifestyle System, that can connect to the Internet and be monitored or controlled by a device in your house or remotely via a smartphone. The Family LifeStyle System connects all of the GreenPeak sentrollers (a sensor, controller, and actuator combo) in your smart home to a cloud application. And based on the data provided by the smart home devices, the Family Lifestyle System can learn a household's daily routines, such as when people leave and come back, automatically lighting the rooms where people tend to hang out.

IoT devices don't need much onboard logic to deliver machine-to-machine communications. "Devices don't need to be too smart, just connected to processing power in the cloud," says Collins. "The cost of providing appliance connectivity has fallen significantly, and the infrastructure to connect, share, and use the data collected has all developed and gained wide adoption." The ability to use tiny, affordable IoT controllers makes it relatively easy to enable IoT connectivity on all kinds of devices. IoT principles can be used on a mass scale, too, empowering more efficient energy grids, transportation systems, and manufacturing facilities.

Putting It All Together

The physicals tools are readily available to make the IoT a reality, and the growing interest in the IoT has helped to quickly evolve IoT software and standards. For example, ZigBee is a wireless language that's popular for communication between smart home devices. The ZigBee communication protocols are based on the IEEE802.15.4 standard. Known for its support of wireless personal area networks, the ZigBee standard is particularly ideal for use with low-power, low-bandwidth devices—a requirement for many IoT devices. ZigBee recently announced its latest wireless standard, called 3.0, that's designed to unify the



GreenPeak's Senior Lifestyle System lets children and elderly privately and securely share lifestyle information.

various ZigBee standards and support all device types, commands, and functionality among the current ZigBee standards.

"Smart home devices usually connect via ZigBee and the home router to the Internet," says Links. "They include all the devices in the home, from lights and light switches to motion sensors, thermostats, door locks, automated curtains, sun shades, etc." Best of all, ZigBee can work with your smartphone to control all of the devices, assuming you have a compatible app to serve as an online dashboard or control utility.

The ZigBee protocol typically functions as a mesh network, where every IoT device can connect to every other IoT device in range. One or more of the IoT devices can serve as the Internet gateway. Wi-Fi networks, by comparison, typically have a star topology, where every device connects to an access point, rather than directly with each other. The star topology adds complexity to the network and makes it less ideal for IoT devices. Another possible issue with Wi-Fi is that the standard calls for higher power requirements, which might prevent developers from using it with battery-powered devices, such as home automation, remote controls, and monitoring equipment.

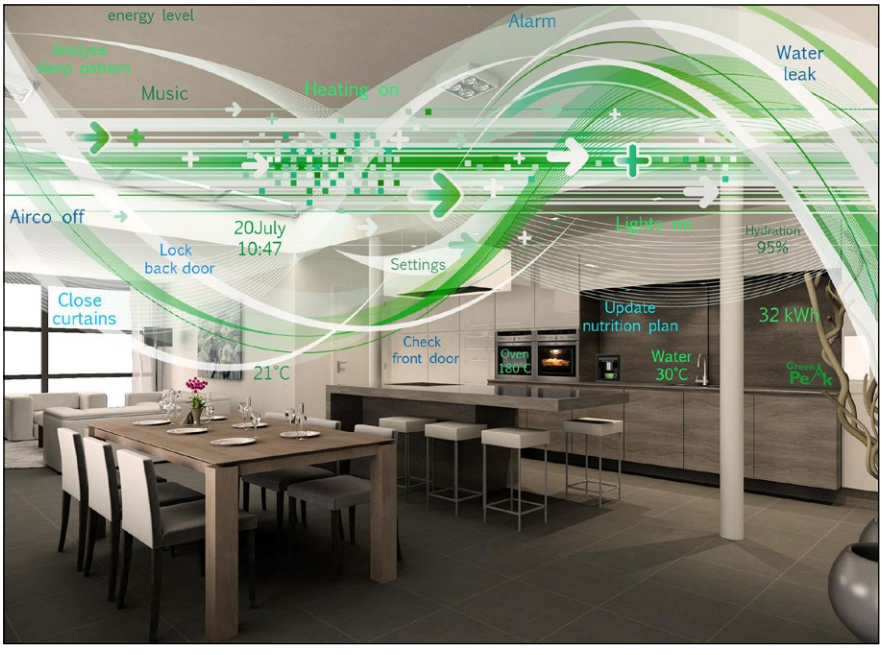
When comparing ZigBee to Bluetooth, ZigBee also boasts a strong advantage in power consumption. (There's a good reason why many people turn off Bluetooth on their mobile device when not in use.) Device support is another potential limitation for Bluetooth, as the standard can only support up to 20 connections. ZigBee, on the other hand, can support thousands of connections. In short, the various benefits of ZigBee make it the preferred communication protocol for many IoT devices.

What's Hot With IoT

You've probably noticed that many of the IoT applications we've covered are centered on home automation. "The home is a leading area for good reason," says Collins. "These are consumer-heavy environments, where individuals increasingly want devices to exhibit the same ease of use and connectivity as their smartphone." Home appliances in particular have been a major focus for IoT developers. Links says, "The so-called white goods can be easily connected to the Internet, enabled for remote control, allow for maintenance control (when does a filter need to be changed, for example), and alerts when they use more energy than desired."

Part of the attraction of the smart home is that there are a lot of extra benefits for connected appliances, HVAC, home security, and lighting. "Value-added services are most interesting when products are extended beyond their traditional boundaries," says Kerber. "Instead of thinking of an oven as an oven, think of it as a group of sensors and a controller. Adding sensors and controls that expand the functionality of the product provides new opportunities to sell value-added services."

Home security has been strong area of growth for IoT devices. A recent Parks Associates study found home safety and home security were the two most appealing smart home use cases. For example, 51% of respondents said it was "very appealing" to receive alerts via a mobile device or PC if there is smoke or fire inside their home. The next most appealing use cases were alerts for a gas



GreenPeak imagines a world where sensors and IoT devices will be installed throughout the home.

leak (or carbon monoxide), if the doors or windows are opened, if there is a medical emergency, and if there is a water leak.

There are a lot of IoT applications for outside the home, too. Wearable devices have been the subject of a lot of innovation in recent months. "Wearables are the devices that people carry with them, which usually connect via Bluetooth to the smartphone, and from there to the Internet," says Links. "Wearables include things like smart watches, fitness bands, step counters, and devices to help people to live more 'mindful.'" When you're aware of critical vital signs and how much you move around, for instance, it's much easier to accurately track calories and exercise habits.

Fitness bands are a good example of an IoT device that provides you with data that was previously difficult to quantify. "Fitness bands enable the person to be coached to live a healthier lifestyle, as well as to understand long-term trends," says Links. "It has all the ingredients of a typical consumer IoT application but also serves as a very good prototype of what other smart home applications will be able to do for the consumer: quantify our lives, measure how we are using our resources (such as the amount of energy consumption), how safe we live, and provide us feedback to change and improve."

A less popular category of IoT devices, at least from a consumer standpoint, are M2M (machine-to-machine) devices. Links says that these are devices that "are directly connected to the cellular network, like cars being able to report where they are (in case of an accident or theft), or a vending machine that calls when it is about to run out of stuff." These types of IoT device have huge potential for use in the manufacturing, utilities, and transportation sectors.

IoT Challenges

The IoT sounds great, but you'll want to temper expectations, as many devices are still at a stage that will appeal primarily to early adopters.

> "It does not make sense to build a cloud-based control structure for just a refrigerator."
>
> -Cees Links, GreenPeak founder and CEO

Kerber says, "Leading categories, such as lights, thermostats, door locks, and networked cameras, are in five to six percent of homes." And although the tremendous potential of the IoT looms, the advantages might not be readily apparent in a scenario of only a few connected devices.

"The problem that we are facing is a sort of chicken/egg problem," says Links. "It does not make sense to build a cloud-based control structure for just a refrigerator. But if that infrastructure would exist, then new equipment can be easily connected at small incremental cost."

Even in a house full of connected sensors and IoT devices, the technology might not yet work together. "The weather station does not provide information to the thermostat about the climate outside. The security system is not connected to the electronic door locks—not automatically locking the forgotten back door when it appears that nobody is in the home," says Links. A true IoT system will have all of the devices interconnected and communicating important information, which can be acted upon. Links adds, "We are currently in an emerging state of the IoT, with individual vertical applications that operate as islands and serve independent applications."

Security and privacy are also key concerns with IoT devices, especially since so many IoT devices are focused on the home. "Access control is a major concept that is addressed only peripherally in the wider development of the IoT," says Michela Menting, digital security practice director at ABI Research. "[Access control] requires some form of authorization, authentication, or identity management system in place with a suitable support infrastructure."

With computers, digital certificates are a popular way to validate devices, but this might not be possible with some IoT devices. "Digital certificates need key management frameworks and/or PKIs (public key infrastructures) in place to work effectively," says Menting. "These frameworks are not always compatible with low-power passive sensors and other integrated circuits with limited computational abilities." Without a strong authentication mechanism, IoT devices could make good targets for cybercriminals. "It can be relatively easy for an attacker to place a fake node and through that input malware, intercept, or tamper with data coming from other nodes," says Menting.

Securing IoT devices and communications is no simple matter. Kerber says, "The product firmware, the communication link to the cloud, and the cloud infrastructure must all be carefully designed and tested." The fragmentation of the various protocols and device types mean each device is often secured differently. Menting says, "In terms of regulation or standards, there is no unified security standard that can apply to all the IoT communication protocols uniformly due to this complexity." Without a single standard, IoT manufacturers must work with standardization organizations, industry collaborators, and vendors to effectively secure individual devices.

"Security issues already exist for the Internet of people," says Links. "The

industry and governmental bodies are just slowly starting to recognize these issues and take action. The exploding IoT makes these issues more explicit and accelerates the requirements to take these actions." Without an end-to-end security standard, manufacturers must take great care to secure the IoT devices. The task is even more difficult, because things like thermostats, dishwashers, and HDTVs didn't previously require any security. An IoT device might be a manufacturer's first experience protecting the product against online threats.

A Bright Future

The IoT can only grow from here, as the potential to reduce energy costs, improve safety, and enhance functionality is too great to ignore. Experts predict a huge increase in the number of IoT devices in the future. For example, Gartner forecasts that the IoT will grow to 26 billion units by 2020 (up from 0.9 billion in 2009). By comparison, the total number of smartphones, tablets, and PC in 2020 is only expected to be 7.3 billion units.

"The fact is that today many categories of connected things in 2020 don't yet exist," says Peter Middleton, research director at Gartner. "As product designers dream up ways to exploit the inherent connectivity that will be offered in intelligent products, we expect the variety of devices offered to explode."

The key industries leading to increased adoption, according to Gartner, include manufacturing, healthcare, and insurance. For example, real-time data from connected cars could allow insurance companies to offer usage-based car policies. Gartner also expects that connected sensors will provide new options to improve efficiency in utilities, transportation, and agriculture.

The adoption rate of the IoT will likely depend on how easily we can utilize the information provided by the technology. "The real key component of the IoT, whether wearables or the smart home, is the application, not the sensor," says Links. "Useful information extracted from the data can coach people in reaffirming what goes right, alerting or taking action if something goes wrong, and using data analytics to compare situations."

To support an explosion of IoT devices, IDC expects that within the next five years 90% of all IoT data will be hosted on service providers' cloud computing platforms. IDC's FutureScape report indicates that 50% of current IoT activity is focused around manufacturing, transportation, smart city, and consumer applications. In five years, IDC forecasts that all industries will have IoT initiatives.

Baby Steps

We expect you'll see a lot of intriguing, new IoT applications over the course of this year, based on the huge amount of IoT products being released at this year's CES. And as people discover the useful features of IoT devices, there will be greater demand. "The transition to the Internet of Things will transform our lives incrementally," says Kerber. "As consumers add smart devices to their home and manufacturers add layer after layer of value-added services, the home will start to work on the owner's behalf, automatically performing tasks in the background and enhancing the lifestyle of the consumer."

When it comes to ease of use, Links expects that the IoT will soon become simple to configure. "Problems that have to do with complexity needs to be broken down in 'digestible modules' that can be resolved, implemented, and connected. This is similar to what occurred with Wi-Fi. When Wi-Fi networking first appeared, it was quite complex and difficult to configure." Now, it's relatively easy for anyone to set up and connect to a Wi-Fi network, and hopefully, IoT devices will be just as simple to configure.

Right now, the IoT is a buzzword that doesn't have much bearing on our current lifestyle. It won't be that way for long, as the evolution of IoT devices and data analytics make it a "must have." Links gives us this example: "If we ask our children how the world existed before Internet, they are speechless, because they have no comprehension of how people can communicate without the commonplace tools we have today. The same will happen with the IoT." ■

Wearable devices also fall within the scope of the IoT.