InfoWorld DeepDive

What the 'Internet of things' really means

SHUTTERSTOCK/STEPHEN SAUER

Deep Dive

What the 'Internet of things' really means

Get past the confusion caused by all those technologies claiming to be in the Internet of things BY GALEN GRUMAN

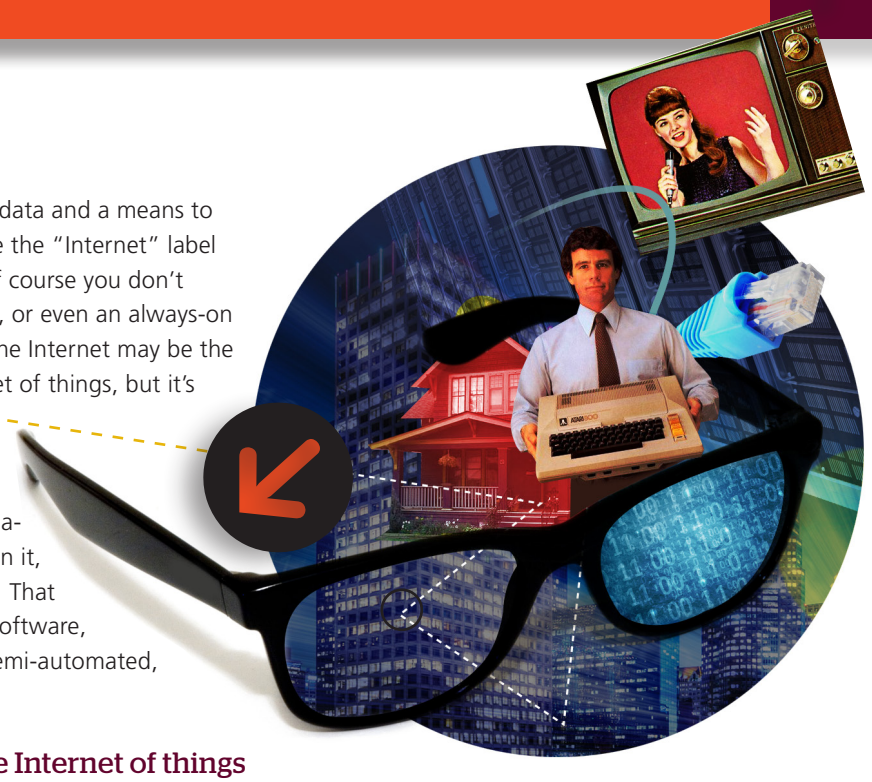
In some cases, the Internet of things is simply a buzz phrase that companies use to sell whatever they've long had -- just as the cloud, green, Internet, e-, and mobile labels have long been abused.

Answer a call or go to a conference these days, and someone is likely trying to sell you on the concept of the Internet of things. However, the Internet of things doesn't necessarily involve the Internet, and sometimes things aren't actually on it, either.

In some cases, the Internet of things is simply a buzz phrase that companies use to sell whatever they've long had -- just as the cloud, green, Internet, e-, and mobile labels have long been abused. But there is a there there: The Internet of things has a real meaning that's useful to understand, as it will affect nearly every corner of both IT and consumer technology.

At its core, the Internet of things means just an environment that gathers information from multiple devices (computers, vehicles, smartphones, traffic lights, and almost anything with a sensor) and applications (anything from a social media app like Twitter to an e-commerce platform, from a manufacturing system to a traffic control system).

Deep Dive



Basically, you need data and a means to access it -- that's where the "Internet" label comes from, though of course you don't need the Internet itself, or even an always-on network connection. The Internet may be the backbone of an Internet of things, but it's not the only bone in that body. Then you need something that works with that information to analyze it, act on it, or otherwise process it. That something is typically software, whether automated, semi-automated, or human-controlled.

The intrigue of the Internet of things

Where the Internet of things gets interesting is when you combine information from devices and other systems in novel ways, tapping into the huge processing capabilities available today to do the kinds of expansive analysis usually associated with the concept of big data -- meaning analysis of data not necessarily designed to be analyzed together.

Otherwise, you're talking about sensor networks and machine-to-machine (M2M) networks common in factories, hospitals, warehouses, and even streets (think the streetlights and "next bus" electronic signs) or network-connected product systems (like an Apple TV-based entertainment system, the Bluetooth stereo in your car, or iPod Touch-based cash registers in retailers) -- useful but not profoundly new.

To achieve the notion of the Internet of things, you need most of the following pieces in place:

- Network connectivity, which is typically wireless
- Sensors and/or user input that capture or generate data
- Computational capabilities, at the device and/or back end

I say "most" because you could have a store-and-forward connectivity approach such as plugging a device into a USB port on a computer. Store-and-forward is essential in any case, because connectivity is not ubiquitous, so you need a way to send data captured when offline. That's a hallmark of the Internet, which was initially designed to allow communications even after a nuclear war through store-and-forward and auto-rerouting.

There are thousands of possible purposes -- perhaps millions. That is why the Internet of things is not a thing but a concept that can be applied to all sorts of things.

Putting the things in the Internet of things

You need things, but they need not be independent items like printers or earbuds or sneakers or golf clubs. A thing in an Internet of things could be simply status information, such as where you are or where the temperature is at a certain location or the engine temperature -- that may be collected through a general-purpose device such as a computer or smartphone. In other words, the thing itself need not be in an Internet of things, though data about it must.

And you need a purpose for having all these connected devices. There are thousands of possible purposes -- perhaps millions. That is why the Internet of things is not a thing but a concept that can be applied to all sorts of things. In most cases, those purposes are expressed through applications or services -- whether local, cloud-based, data center-based, or a combination of any or all of those.

In some cases, the services sift through huge amounts of data, which Hadoop and other big data technologies in combination with cloud services now makes possible. But an Internet of things doesn't have to involve big data -- there are small-data uses too, such

SHUTTERSTOCK

Deep Dive

as the Web of sensors on highways to detect chemical and nuclear weapons that are always monitoring but transmit only when an anomaly is detected. Combine that sensor network with traffic management systems, electronic highway signage and perhaps emergency broadcast notices, first-responder deployments, and so on, and you get a public-safety Internet of things.

Its versatility is what opens up so many possibilities for the Internet of things. For example, running an app like Foursquare or Google Now that monitors user locations takes an existing set of devices (smartphones), their sensors (location data), and their network connectivity to aggregate information to a data center somewhere in the cloud that uses that information for, in this case, ad delivery and market research. It's an example of how the Internet of things can simply be an application taking advantage of today's connected environment.

But an Internet of things can be more purpose-built, such as the devices that plug into your car's computer to transmit engine, speed, and other readings to your insurer (a bad idea!) or your smartphone (a better idea). At its most basic, this is just a sensor network in your car tying into a central transmitter. But the Internet of things twist is that some of that data would go to the government and private agencies that monitor traffic, feeding in real-time travel data to augment what they collect via in-road sensors and highway cameras.

Two (or more) is better than one

An Internet of things can enable hybrid uses. For the car example, multiple services might get pieces of that automobile and travel data for everything from traffic management to insurance rate-setting, from mechanics' diagnostics to road-repair prioritization.

As another hybrid example, think of all those health sensors available, like the Fitbit and Nike+ for personal health management, or like the Worthings blood pressure monitor or Agamatrix glucose monitor for medical monitoring. The personal ones expand the capabilities of the connected mobile world with a new sensor that sends data to an app in the cloud. But the medical ones may expand that same connected mobile world but send it to a medical provider's electronic health records (EHR) system. It's even possible that the two types of health sensors could cross-deliver, with your Fitbit data also going to the EHR and your physician-prescribed medical sensor also going to your personal health vault -- with each subset serving multiple purposes.

That notion of multiple purposes is probably the best reason for using the term "Internet of things," as the Internet is more than a resilient network but a conduit for any combination and collection of digital activities. The Internet started as a way for the government to communicate after nuclear war but has evolved to be much more than a network.

In many ways, the Internet has become a digital world that has gateways into our physical world. The Internet of things takes that concept to the next level, allowing multiple worlds -- some connected to others, some not -- that mash up physical and digital in all sorts of ways. ■

InfoWorld executive editor Galen Gruman *analyzes the latest issues in mobile technology.*

Deep Dive

The 3 ways the Internet of things will unfold

The three key segments of the real IoT are on different paths, so don't think of them as one entity BY GALEN GRUMAN

Despite the tech industry's fierce attempts to scrub all meaning from the IoT label, something real and valuable is occurring in the Internet of things.

The Internet of things is hot. Practically every tech vendor is using the label for some of its products. Cisco Systems and PwC both predict that the market will be worth trillions of dollars. The Internet of things is also the tech industry's latest overhyped technology -- most of what is called IoT is not IoT, and the IoT market will never be worth trillions of dollars unless you declare that IoT includes anything that uses power, a chip, and some communications capability, which is a pointless definition.

Despite the tech industry's fierce attempts to scrub all meaning from the IoT label, something real and valuable is occurring in the Internet of things. But users and IT organizations can't take advantage of it without understanding what's going on, which is what this post explains.

Several technologies are making IoT widely possible, mostly from the mobile space.

One is the low-power processor, typically

Deep Dive

based on the ARM designs already in use by nearly all smartphones and tablets. They're much cheaper and smaller, as well as more power-efficient, compared to traditional Intel and AMD x86 chips. About 40 percent of them are used in devices you may not expect, says ARM Holding marketing VP Ian Ferguson, such as in-car infotainment systems. Companies like Texas Instruments also make a bevy of chips -- some based on ARM, others not -- that power everything from sensors to alarm clocks to garage door openers to beacons.

There are three clusters of real IoT activities, and each is on its own path. Some paths may cross, but understanding the three separately will help you strategize about your own IoT engagement.

Then there's Bluetooth and Wi-Fi, including the networkless Wi-Fi Direct (WiDi) variant standard in recent mobile devices and computers. (This is how Apple's AirDrop works, as well as Windows' and Android's Miracast.) The two networking standards are commoditized, so they're finding their ways into all sorts of devices.

Industry efforts like Thread are trying to develop a constrained communications standard that lets devices communicate over a common protocol (as opposed to a radio technology) without the full computation and energy consumption overhead of the typical IP stack. The Thread effort sees IP at the edge of the stack, so the low-requirements communications eventually can connect to the Internet and heavier-weight systems, but it doesn't force every component to be able to do so.

Basically, it's getting cheap and easy to put a chip in it. And it's getting easy to add coprocessors for everything from motion detection to radio connectivity, from graphics processing to encryption. More devices can compute and connect as a result. Power sources are shaping up as the limiting factor, so there's lots of research on everything from better batteries to converting radio waves or motion into power.

There are three clusters of real IoT activities, and each is on its own path. Some paths may cross, but understanding the three separately will help you strategize about your own IoT engagement:

- Machine-to-machine is simply about efficiency, not fundamental new opportunity
- The notion of smart systems will gain traction, with Bluetooth peripherals as the first step
- The ad hoc Internet of things is well under way

Machine-to-machine is simply about efficiency, not fundamental new opportunity

For decades, we've had industrial, medical, and office equipment that could talk to other equipment, such as thermostats that communicate temperature information to normalize HVAC settings, assembly-line sensors that let robots know to stop welding if the line is delayed or stopped, and EKG readers that alert a nursing station if worrisome readings occur. This is known as machine-to-machine (M2M) communications, and it's really useful.

These established M2M uses are now getting the IoT label, but they are not really changed by IoT. However, they're cheaper and easier to deploy because of greater technology standardization that is making the larger IoT trend

Deep Dive

possible. We'll thus see the "industrial Internet of things" (the new name for M2M) become more widespread, as smaller companies can afford to join in and larger companies can afford to bring the notion outside of expensive manufacturing systems.

It's like when PCs arrived in business: Suddenly, a computer didn't cost millions of dollars, so computing could go beyond the data center.

What's made M2M easier and cheaper to deploy? Bernie Anger, the general manager of General Electric's Intelligent Platforms division (a big M2M vendor for industrial automation) points to three factors.

- ODBC User Agent adoption: This version of the venerable database connectivity protocol is not Windows-dependent, so devices on all sorts of platforms can now share data through a known protocol, not just PCs or devices running Windows Embedded. Due to the relatively low cost -- ODBC UA-capable devices with local computation ability and network access cost just $200 -- it's affordable to have more devices connected.

Again, it's old-fashioned industrial computing made easier through modern technologies, then rebranded as IoT.

- Hadoop and similar mass-scale data processing technologies allows analysis of massive data in cost-effective way. When analytics was an expensive, scarce resource, companies limited what data they collected and analyzed to the most critical areas. Now they can apply analytics to more areas, and they're doing so.
- The ubiquity of the HTML5 Web standard in client devices: That means more than the use of iPads, smartphones, computers, and other off-the-shelf equipment -- it also means that specialty devices now use a client UI that's well understood and compatible with all the computing devices you have. The burden of writing to proprietary user interfaces is greatly reduced, and operator familiarity is greatly improved.

"None of these is a revolution, but they come together now to enable the scale and speed not possible a decade ago in the M2M/SOA worlds, when everything was essentially custom, nonstandard, and heavyweight," Anger notes.

Over time, the use of standard protocols and technologies will allow the "back end" M2M systems to interact with user-facing technologies, which will provide some white-knuckle moments for the guardians of the core systems while making them more valuable overall.

The notion of smart systems will gain traction, with Bluetooth peripherals as the first step

Connecting M2M systems to the rest of the world will scare many IT pros, though "rest of the world" really means "other parts of the world." But it's inevitable because it's so useful. I recently profiled a simple example of a utility company managing its systems via iPads to be able to respond to problems faster. That's the simple example we'll see first.

That example is not restricted to M2M systems. It's basic field service, and it's happening in all sorts of ways. For example, some oil rig equipment has sensors that a field engineer can tap into via an iPad, then communicate to home base over satellite or other communications systems to get diagnostics and proposed fixes, as well as interactive manuals. The same is true for airplane engine and copier repairs.

Deep Dive

This too is not a new area. What is new is using consumer-grade equipment like the iPad, standard communications technologies like Bluetooth and Wi-Fi, and standard application languages like JavaScript and environments like HTML5. Again, it's old-fashioned industrial computing made easier through modern technologies, then rebranded as IoT.

You'll see more of it. As an example, Motorola Solutions recently announced a Bluetooth barcode scanner that works with Android and iOS devices. Historically, such scanning equipment is proprietary and expensive. Special training is also required to use and maintain them. By making the scanner a Bluetooth peripheral for common mobile devices changes that equation. Now, your employees can use equipment they likely know how to operate, using Web or native apps that are familiar to them to control the peripheral.

There are many examples of using mobile devices as computing hubs to sensors and specialty peripherals, especially around Bluetooth. This is going to change the specialty-gear industry in profound ways. It's already altering the consumer sphere, with everything from fitness wearables to ice-fishing aides. But cheaper, easier-to-use equipment running on common devices is merely the first step.

What comes next is what I call smart systems. Because these peripherals are connected to, in essence, mobile computers and those in turn can be connected to the Internet and all available cloud resources, they form a network of both data and operation. This is where the "Internet of things" label rightfully applies.

What do I mean by that kind of network? Think of a delivery driver, who now has a signature pad that collects your signature and lets the driver input status like "addressee not home, package not delivered." The data could then be transmitted via a radio in the truck so that the shipping info is updated on the tracking website that both the sender and recipient can monitor.

That existing technology has proven quite useful, but imagine if the signature pad were a peripheral or used a tablet's touchscreen. If the addressee is not home, the driver could take a photo of where the package was left, so the person knows where to look for it -- or of the menacing dog preventing delivery or of the person who signed for the package (because they almost never ask for ID). That's just the camera. If Bluetooth-powered door locks ever take off, they could interact with a back-end service for which the addressee has door-lock access rights temporarily, so the driver could open the door to leave the package in a safe location.

As the day progresses, the status of deliveries could be compared for nearby trucks, allowing transfer of cargo to equalize workload -- or even shift packages to a second driver who can revisit an address that day knowing the person is now available, rather than ship the package back to the distribution center and try the whole process the next day.

All the pieces exist in some form today, but their distribution is uneven -- both the hardware and the cloud-connected apps. As they become more common, we'll get smarter interactions that let us improve service in a whole range of fields, not simply package delivery. A quick example: A smart pillbox coupled with the sensors in a wearable or smartphone could allow remote monitoring of patients anywhere and provide a way for the patient to engage back (show a photo of the pill -- is it the right one?).

Such technology is already in trial sessions. But

Deep Dive

these trials focus on the center monitoring the edge: the patient, the home alarm, and so on. They're not so focused on the reverse, which is letting the edge query the center -- the delivery service, the doctor's office, the alarm company.

That'll come after the center-to-edge uses are in place. Once a connection is set, exploiting it in two directions becomes much easier. Then we'll see connections across multiple systems in a federation, in the same vein we've seen in the Internet and the cloud.

The carriers all want to be the hub for such an ecosystem, too, so they can charge even more monthly access fees. Most large telephone and cable companies are trialing such subscription-based home-automation hubs, but they're likely to fail.

The ad hoc Internet of things is well under way

The third IoT segment is the least controlled. That's both good and bad.

Think of your home. If you're a techie, you probably have several IoT devices: an Apple TV or Google Chromecast, a Nest or Honeywell Lync thermostat, an Internet-connected Liftmaster garage door opener, your car's Bluetooth ignition lock, and so on. Some interact, some don't. Some should, some shouldn't. When they interact, and when they should, is often a personal choice for the user's context.

It's ad hoc and, thus, messy. If there's an integration point it's usually a smartphone or tablet, running apps for each service and collecting alerts into email or messaging apps. The user is the integrator.

What's changing here is the growing collection of ecosystems. Apple is the furthest along in this effort, with its three ecosystem integration APIs debuting this fall in iOS 8 and OS X Yosemite: HomeKit for home automation devices, CloudKit for cloud storage and sync, and HealthKit for fitness and medical devices. On iPhones, the new Health app in iOS 8 acts as a central repository, managed by the user, of health information provided by the compatible devices and cloud services that users choose. It can also be a conduit to other systems, whether an electronic health records (EHR) system or a weight-loss service.

Apple is using non-network connectivity to make its Macs and iOS devices federate on the fly in what I call "liquid computing," bringing IoT to more than small devices.

This integration is still ad hoc, but it's organized by a specific ecosystem. It's not so much a closed system as it is a compatible system, sort of like Windows was in the PC era for software and hardware. This native compatibility allows easier interoperability, which lets people create a custom IoT. That's powerful.

It's also why so many providers want to be the ecosystem of choice. Apple is the furthest along, but Google is also pushing hard on several fronts including its Nest purchase, its Chromecast effort, and its active participation in the Thread effort. Samsung has talked about similar efforts, but its execution has been, to be polite, uneven.

The carriers all want to be the hub for such an ecosystem, too, so they can charge even more monthly access fees. Most large telephone and cable companies are trialing such subscription-based home-automation hubs, but they're likely to fail. One reason is that users hate these companies and their log track record of arrogantly bad customer service. The other is that their vision is quite narrow, covering a small collection of things and in a way that is about user lock-in rather than empowerment. Only a fool would trap themselves in a carrier-based offering.

Deep Dive

Putting the carriers aside, we will end up with several large ecosystems for such individual-user devices. Some features will be proprietary to the ecosystem, such as Apple's restriction of AirDrop and AirPlay to its own hardware. Some will be partially open, such as Apple's iCloud, which offers iOS and OS X users full compatibility, Windows users limited compatibility, and none to Android users; or iBeacons, a protocol available to any beacons but whose client software runs only on Apple hardware.

Apple is the furthest along in this third IoT category, with its HomeKit APIs for home automation, CloudKit APIs for cloud storage and syncing, and HealthKit APIs for medical and fitness gear. Again, any service or device can use them. But only Apple devices run the client software, so they become the hub for all such devices. Developers can of course use others' APIs as well, such as Samsung's promised health APIs. (Assuming Samsung actually delivers; it's made lots of such promises for home automation but not executed well.) Beacons are a great example, with many equipment makers using Apple's APIs as well as their own, and waiting for Google to come up with its own.

Speaking of Google, the giant behind Android and Chrome OS hasn't come up with a cohesive set of technology like Apple's. But it's been investing in many of the pieces, including robotics and the Nest thermostat, and has been pushing Android for embedded systems as an alternative to Oracle's Java.

Then there's Microsoft, which keeps pushing its old Windows Compact Embedded, a full OS better suited to old-school computing devices and not IoT. Microsoft seems the least engaged in developing an IoT strategy, perhaps because its mobile position is so weak. Struggling mobile provider BlackBerry is also positioning its QNX kernel as an IoT basis. But it's in a better position because QNX is widely used for in-car infotainment systems and has the virtue of letting user-facing technologies like Apple's CarPlay ride on top -- so it can coexist with multiple user ecosystems.

Keep the three IoTs separate

Where all this leaves us is a set of distinct but overlapping markets all sharing the "Internet of things" label. They may share some technology underpinnings and some basic characteristics, but that's like thinking of PCs, networking, and databases as all the same because they are all computer technologies.

The Internet of things is many things. Understand the IoT that matters to you. ■

InfoWorld executive editor Galen Gruman *analyzes the latest issues in mobile technology.*

The Internet of things is many things. Understand the IoT that matters to you.

SHUTTERSTOCK