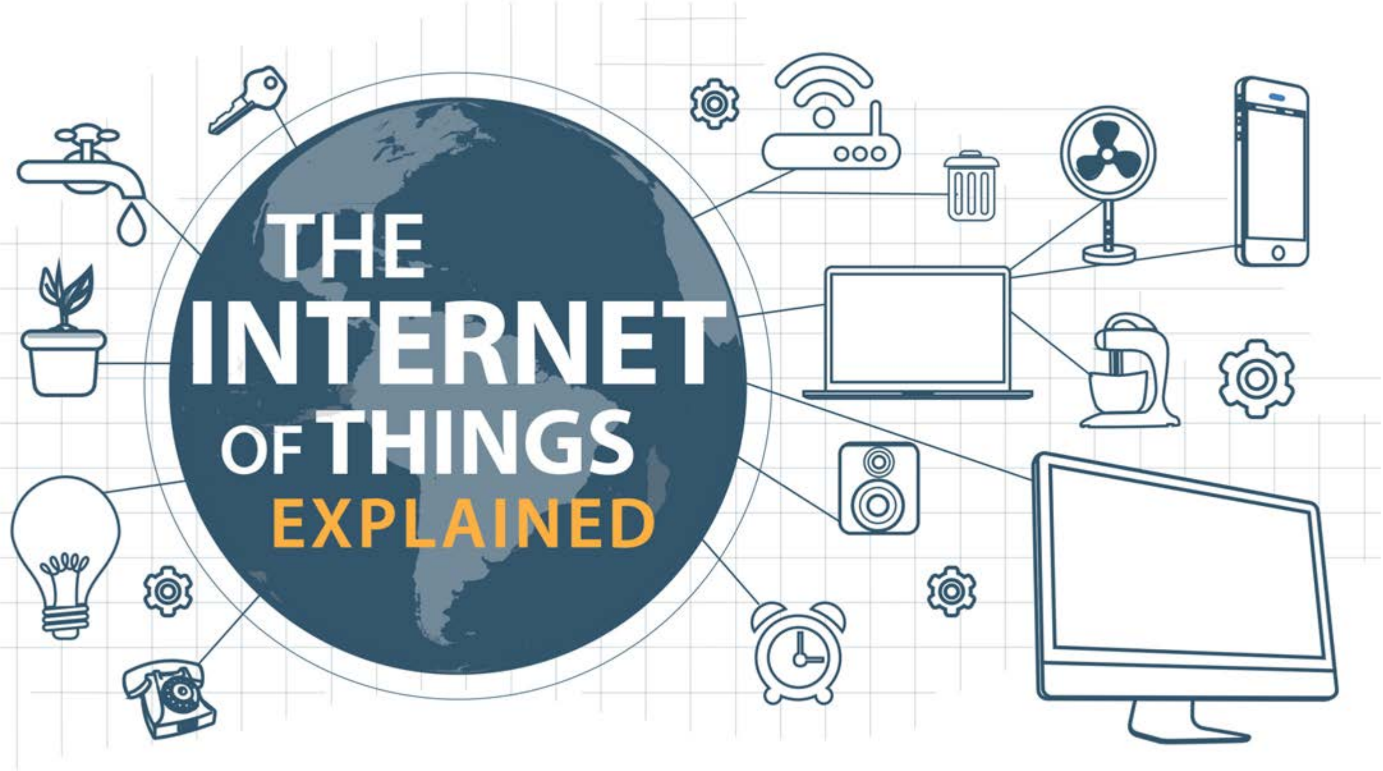


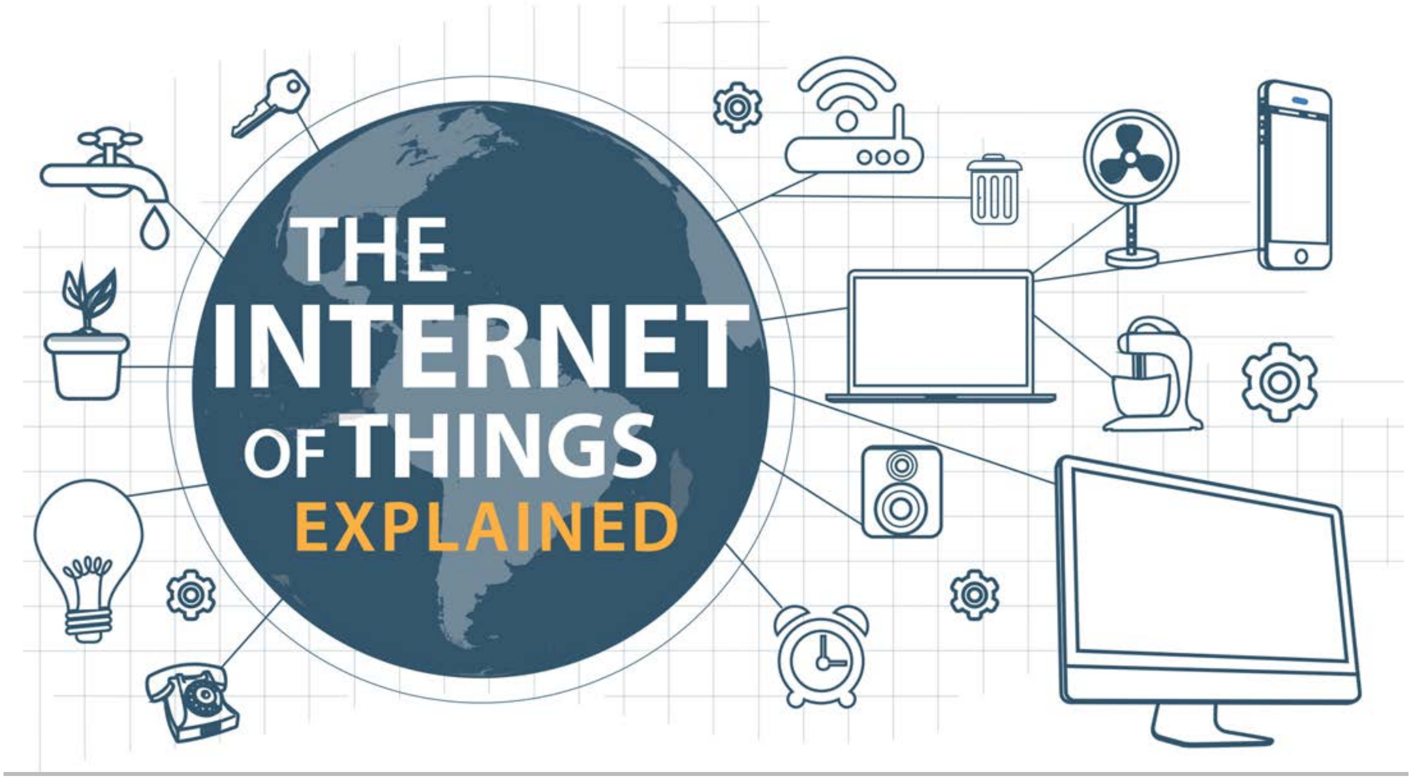
THE INTERNET OF THINGS EXPLAINED

The Internet of Things Explained

A ZCorum eBook

Editor: Marsha Hemmerich

Contents



INTRODUCTION

We think of it as the “Next Big Thing” but the idea of an Internet of Things goes back a lot further than we imagine. Way back in 1926 Nikola Tesla said in an interview: “When wireless is perfectly applied, the whole earth will be converted into a huge brain...and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket.“

Tesla's prediction sounds like an idea brought to life by Hollywood and science fiction. But if the current explosion of devices already connected to the Internet is any indication, then we're on our way to creating Tesla's smart Earth. So let's have a look into the origin of the Internet of Things:

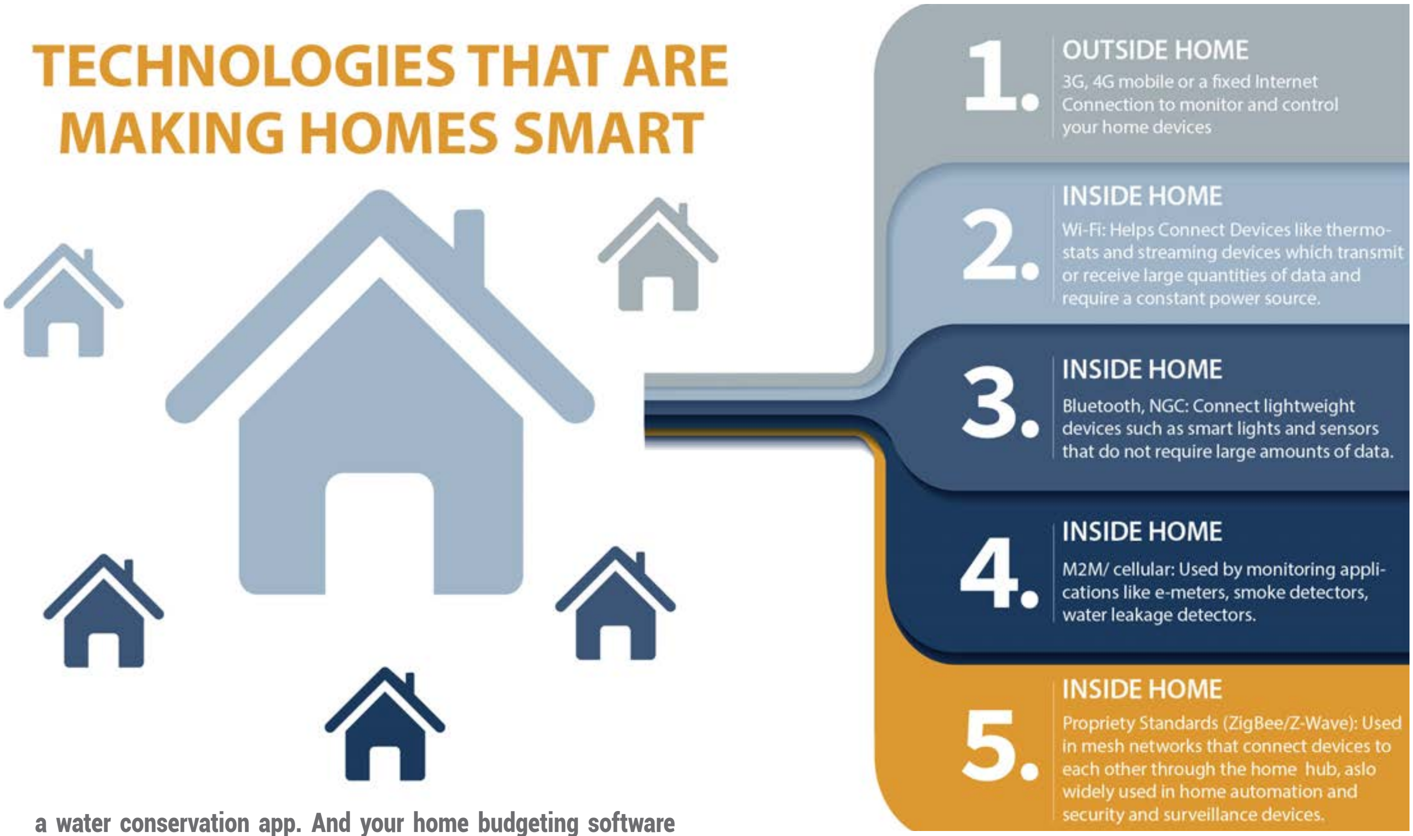
So What is the Internet of Things?

The Internet of Things (IoT) refers to smart, connected devices, in homes, businesses and our surroundings that have the ability to communicate with other devices over a network. These devices are outfitted with data-collecting sensors so they can communicate with one another as a way to determine the health and status of things, inanimate or living.

While some think the IoT is device to device communication over a closed network, like your app for changing channels on your cable box, or your Fit Bit app that tells you how many steps you took today, that operation is really just an internal net or intranet, not the wider sensor-enabled network that connects a multitude of things to a multitude of other things.

To explain further, currently apps are deployed for a specific purpose. Your lawn sprinkler app turns the water on and off and your step counter app counts your steps and calories burned, but these apps don't interact outside of that closed network. That's why presently we end up with a separate app for every “smart” thing. One app controls your garage door, another for the lawn sprinkler, still another for your fitness tracking and so on. Managing all these apps is the equivalent to having multiple remote controls on your coffee table, one for your TV, another for your DVD player, and still another for your cable box.

But the true IoT, as it's envisioned, is a network of deployed “smart” devices like your rain gauge or lighting system that will collect data. That collected data is then made available to many other “smart” applications. So your rain gauge tells your lawn sprinkler there was an inch of rain last night and to stay turned off today and conserve water. This water conservation data could then be relayed to your municipal water company and noted on your record for possible discounts on your bill for using



TECHNOLOGIES THAT ARE MAKING HOMES SMART

1. OUTSIDE HOME
3G, 4G mobile or a fixed Internet Connection to monitor and control your home devices

2. INSIDE HOME
Wi-Fi: Helps Connect Devices like thermostats and streaming devices which transmit or receive large quantities of data and require a constant power source.

3. INSIDE HOME
Bluetooth, NGC: Connect lightweight devices such as smart lights and sensors that do not require large amounts of data.

4. INSIDE HOME
M2M/ cellular: Used by monitoring applications like e-meters, smoke detectors, water leakage detectors.

5. INSIDE HOME
Propriety Standards (ZigBee/Z-Wave): Used in mesh networks that connect devices to each other through the home hub, aslo widely used in home automation and security and surveillance devices.

a water conservation app. And your home budgeting software could receive the data on how much water you saved and predict the amount of your next month's water bill. There are endless combinations and the expectation is that this true version of IoT will provide much more value than what can be derived from the secluded islands of information, the individual apps, like we now have.

Where Did it Come From?

The concept of a network of smart devices was tested in 1982, with a modified Coke machine at Carnegie Mellon University. That machine became the first internet-connected appliance able to report its inventory and whether newly loaded drinks were cold. But the actual phrase 'Internet of Things' was coined by Kevin Ashton in 1999. While at Proctor & Gamble, Ashton got assigned to help launch a line of cosmetics. It began to bother him that he'd go into a local store to look at the cosmetics lines he controlled and find that there was one particular shade of lipstick that always seemed to be sold out. He checked with P&G's supply chain people, who told him they had plenty of that color in the warehouse and suggested that Ashton had just happened to go into a store that couldn't keep that color in stock. But Ashton didn't buy it: He wanted to know where his lipstick was, and what was happening to it. No one could tell him.

Ashton then got the idea of applying Radio-frequency identification (RFID) chips or sensors, which can hold a multitude of data and share that data through a wireless network. These sensors were seen as a prerequisite for the Internet of Things. If all objects and people in daily life were equipped with identifiers, computers could manage and inventory them. Like a lot of innovations, the IoT grew out of a new solution to an old problem, and now it's opening up new solutions to a whole host of problems. And like a lot of innovations, the IoT happened less by magic and genius than by a lot of small steps and bits of luck.

How Does it Work?

A device or object becomes "smart" when technology, such as a sensor, is embedded inside it. That object then becomes "connected" when it is connected to other devices all collecting and sending data somewhere to be processed. This becomes a network of sensors that communicate with each other. The goal is automating processes without any human interaction.

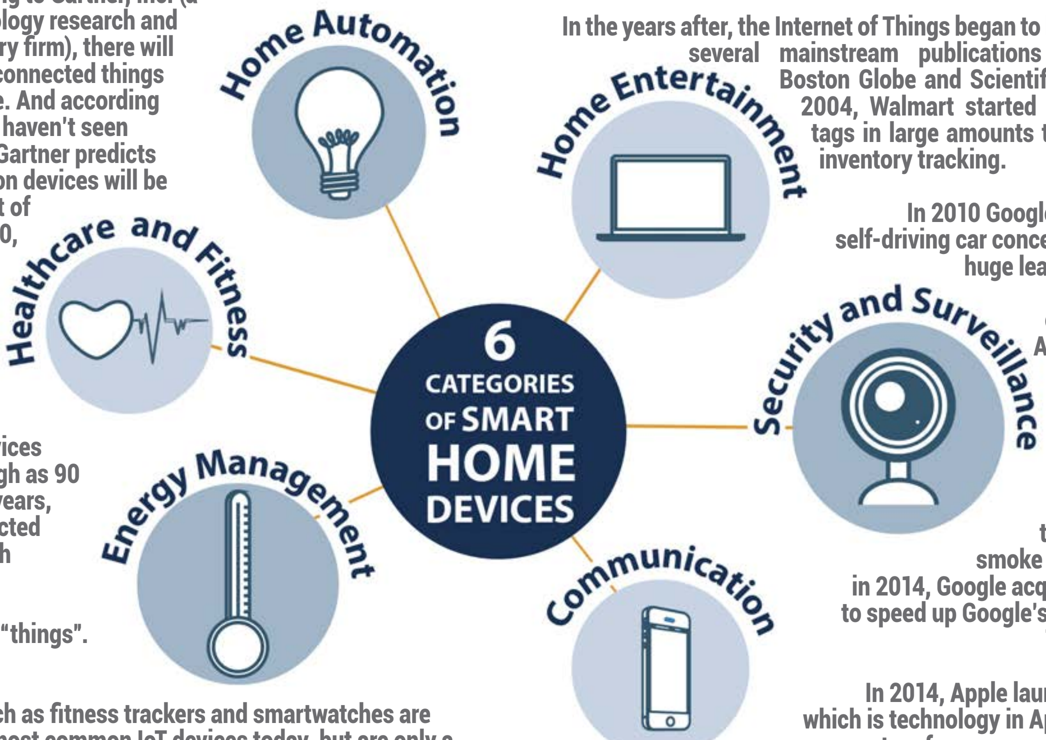
This network of sensors as it relates to the IoT is referred to as a Wireless Sensor Network (WSN). A WSN is a group of specialized sensors that monitor and record the physical conditions of their environment like temperature, light levels, sound levels, bodily functions, humidity, pressure etc. and organize that data at a central location or gateway. That organized data in the gateway can then be used to communicate and trigger an action. For instance, a video surveillance camera or pressure-sensitive welcome mat at your front door sends a signal to lock your doors if it detects a presence. At the same time it also sends an alert to your TV that there is someone at the front door.

With miniaturization and universal connectivity, it is possible to make all types of products smart and connected. Applications of sensor networks include automated and smart homes, medical device monitoring, traffic and weather conditions, and even robot control.

What are the "Things"?

According to Gartner, Inc. (a technology research and advisory firm), there will be 4.9 billion connected things this year alone. And according to Gartner, we haven't seen anything yet. Gartner predicts nearly 26 billion devices will be on the Internet of Things by 2020, including a quarter billion vehicles. Some research claims the number of devices could be as high as 90 billion in five years, with 10 connected devices in each household.

That's a lot of "things".



Wearables such as fitness trackers and smartwatches are probably the most common IoT devices today, but are only a small part of the overall trend. Many products and services are already into the IoT market, including kitchen and home appliances, lighting and heating products, and insurance company-issued car monitoring devices that allow motorists to pay insurance based on the amount of driving they do.

The First Connected Things

Decades before that first connected Coke vending machine in 1989, automated "homes of the future" were standard exhibits at World's Fairs and backgrounds in science fiction. Home automation included the control of home entertainment systems, houseplant and yard watering, pet feeding, and changing the lighting for different moods.

In 1989 a new 'House of the Future' was built in The Netherlands. The house had multiple smart devices in every room and focused on the interaction between man and device. Voice recognition was an important aspect of the house.

In 1990 the first toaster was connected to the Internet. Developed for a trade show exhibition, the only thing that could be done was turning it on and off, but in 1991 the private developers added an automatic crane to also insert a slice of bread automatically.

In 2000, the smart refrigerator made its entry. For many years, the smart refrigerator has been the example of the Internet of Things and it was developed by LG. It had an LCD screen that was capable of showing information such as inside temperature, the freshness of stored foods, nutrition information and recipes. The refrigerator cost $ 20,000.00 and not surprisingly, did not sell as well as LG had hoped.

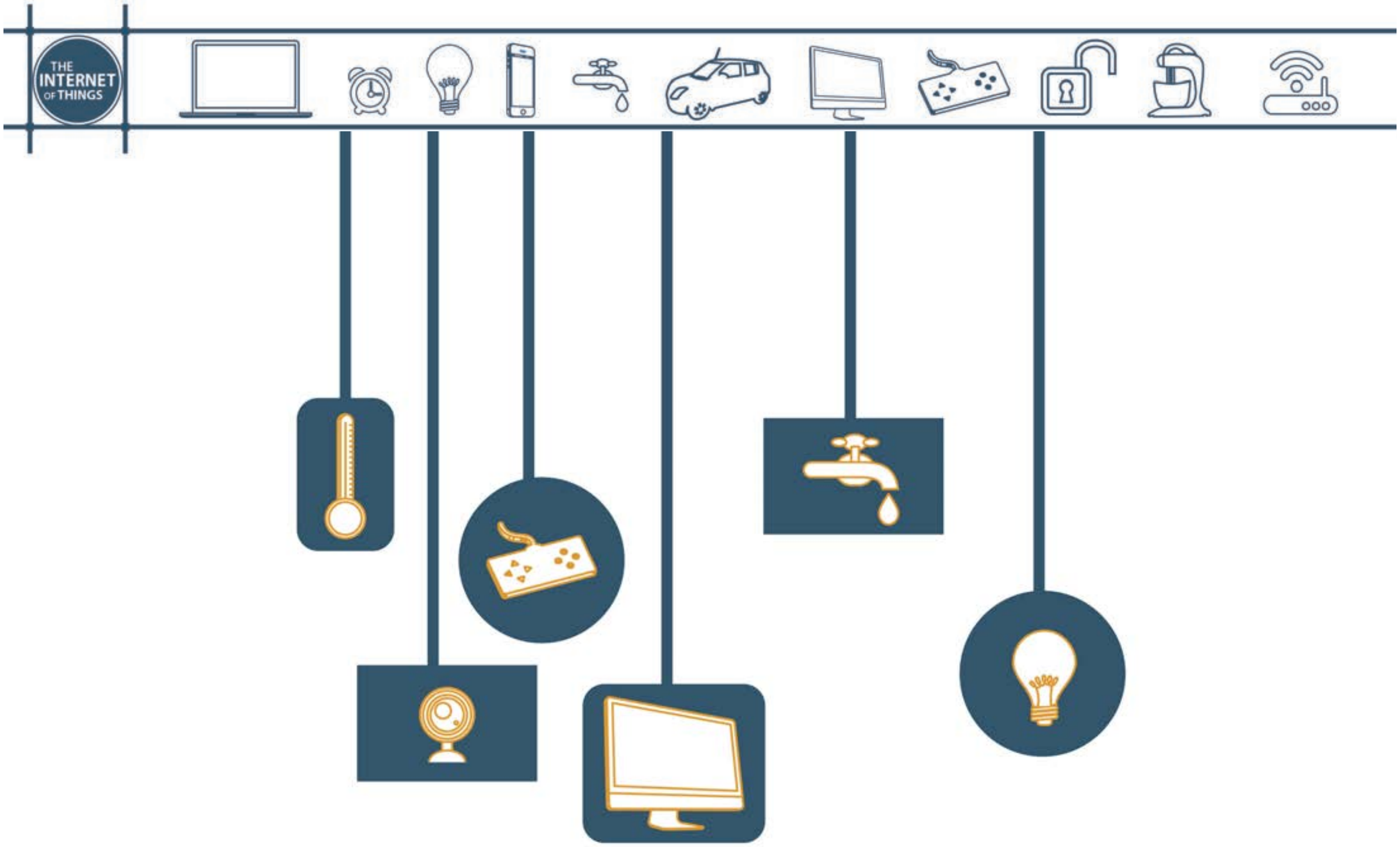
In the years after, the Internet of Things began to be mentioned in several mainstream publications such as the Boston Globe and Scientific American. In 2004, Walmart started to deploy RFID tags in large amounts to improve their inventory tracking.

In 2010 Google launched their self-driving car concept, which was a huge leap forward in the development of connected cars. Also in 2010, two former Apple engineers started Nest Labs, the company that produces smart thermostats and smoke detectors. Then in 2014, Google acquired Nest Labs to speed up Google's own Internet of Things division.

In 2014, Apple launched HomeKit, which is technology in Apple's operating system for communicating with and controlling connected smart devices in the home.

Launch of IPV6

But the biggest enabler of the Internet of Things was the launch of IPV6 in 2011. Integration with the Internet requires that devices have an IP address as a unique identifier. However, due to the depleted address space of IPv4, objects in the IoT must use IPv6 to accommodate the extremely large number of IP addresses required. Where IPV4 had only 4 billion addresses, IPV6 has a total of 340 undecillion IP addresses. This is more than enough to cope with the expanding Internet of Things in the coming years, even if projections are correct that predict by 2030 we will have 100 trillion connected devices in the world. The future of the Internet of Things will not be possible without the support of IPv6; and consequently the global adoption of IPv6 in the coming years will be a critical necessity for the successful development of the IoT.



So Why Should Operators Care About the IoT?

Everywhere you look there's new information about IoT from technology specialists, hardware manufacturers, and software creators. It's like chasing a moving target. But the projected explosion of the IoT is forcing some industries to rethink their network architecture. R & D departments are beginning to explore new communication methods that could potentially bypass the Internet entirely. The idea is that by the use of peer-to-peer communication between the wireless sensor network clusters, they can form a new Internet made up of just WSNs. These sensor networks could have a central gateway of Internet access, and thereby offer Internet access in one-hop.

The creation of these interconnected WSNs would use wireless network technologies such as Bluetooth, Wi-Fi and Wireless Personal Area Networks (WPAN). Over time, as people opt in to allow their personal area networks to communicate with the wireless sensor networks, communication could occur directly between WSNs rather than through the Internet.

The concern for internet service providers is that a network of 50 billion connected devices could potentially bypass, to a degree, the provider's broadband network to communicate with each other through a peer-to-peer model via these WSNs. This could translate into revenue loss for ISP's as more subscribers sidestep the connection with carrier gateways to avoid the cost of broadband plans.

Initially, the trend would lean towards open Wi-Fi outside the home that WPANs could gateway through to the Internet. Eventually, a critical mass of WSNs within a densely populated metro region could open the door for seamless wireless communication among WSNs.

The Early Bird

The important key is for operators to get the first foot in the door, establish themselves as the gateway, connect all the devices and become an indispensable and hopefully inseparable part of the subscriber's home. Because the devices for smart homes are still in early stages of development, ISPs are set to position themselves as leaders in the IoT market now.

In addition to their high data capacity networks that are already supporting OTT entertainment and gaming, ISPs have a unique advantage with the equipment that's already in the home. Providers are in a unique position to serve as the central gateway and IoT hub in the future smart home, and "cutting the cord" from this position would become less likely if nearly impossible. Once set, a homeowner disconnecting their entire home and lifestyle

> "THE CABLE INDUSTRY , AS A PRIMARY PROVIDER OF CONSUMER INTERNET SERVICES , IS IN A POSITION TO HELP DEFINE THE INTERNET OF THINGS IN THE HOME ENVIRONMENT."
>
> **-Clarke Stevens**
> ***Principle Architect in Applications Technologies***
> ***Cablelabs***

from the "gateway" would be a major disruption and costly in time and expense. Current internet service providers are set to possibly solve the Internet of Things' biggest problem, the lack of a central processing gateway.

The Gateway

Research firm Gartner notes the absence of a gateway device to help homes control and connect all these devices safely to the web and is seeing developments in internet service providers, cable companies, alarm manufacturers and mobile phone companies as they try to build devices and develop the ecosystems to get them into homes. Although the market is in its infancy and business models are not quite established yet, that's not stopping the development of IoT gateway products. Several have been created and more are coming. The key consideration will be how those gateways enable the user to connect any of their devices to a corporate network.

Gartner is tapping ISPs to get the majority of the market and be in a position to fend off a challenge from mobile phone operators, but the race is only starting and there could be plenty of opportunities for those that put together an IoT solution first. The fact that operators have equipment in a household that is already connected to the smart pipe means that a central gateway is already in place.

This equipment could become an "all protocols" Internet of Things hub. It could bring all the home's devices together into a single ecosystem that lets your security camera talk to your garage door that talks to your lights that talk to your oven and your shower. Everything working together like a truly connected home but with a single managing app. The TV, when in use, could also become a giant notification center. Providers that deliver internet access could add IoT functions to the modems, WiFi extenders, or remote controls they provide to their customers and pull in extra revenue.

> "IOT APPLICATIONS ARE TRIGGERED BY SENSORS AND NEED DATA MANAGEMENT, BUT THERE IS NO SINGLE IOT GATEWAY TO THE HOME. AS INTERNET-CONNECTED HOMES BECOME INCREASINGLY SMARTER, THE GATEWAY IS BECOMING THE CENTER FOR CONNECTING THE DIFFERENT DEVICES AND HOME APPLIANCES."
>
> **- Paul O'Donovan**
> *Principle Research Analyst*
> *Gartner*

The need for a central point of control will also become glaring to the subscriber in short order. A primary gateway would provide better management of the data collection from devices. A gateway would offer opportunities for an operator to add and test new devices and services with the television acting as a dashboard for all the IoT services in the home. Instead of having an app for every IoT device, those apps can be assembled and controlled from the remote on the couch or the cellphone when away from the home. In addition, the television can act as a smart thing' itself, so when a trigger comes in, say the doorbell rings, the television can not only display the video of the person at the door, it can also pause the programming on the tv.

The Interoperability of the Internet of Things

Various research firms estimate the number of connected devices to reach into the billions by the year 2020. And the number keeps rising. Everything from your shower water to your toothbrush to your weekly pizza order will be automated, connected and collecting data. But the hot IoT talk is centered on the ongoing standards war between the consortiums and alliances that have formed to try and come up with standards for all those billions of devices.

Among the challenges for a successful IoT is the unusually high dependence on cooperation. What has become the biggest challenge for smart devices and the systems providers is ensuring interoperability for all the different technologies and standards. But so far device makers would rather create their own closed ecosystems with their own internal protocols.

The IoT will run in data centers. And for the IoT to work in data centers, platforms from competing vendors need to be able to communicate with one another. "This requires standard APIs that all vendors and equipment can plug into," said Mike Sapien, a principal analyst with the research and consulting firm Ovum.

Gartner analyst Fernando Elizalde says, "A number of alliances have sprung up in the last couple of years to attempt to sort out the interoperability issue. Each aims to provide a solution that integrates all the smart home categories."

IoT standards were established to manage four main areas: connectivity, interoperability, privacy, and security. So how do all the competing IoT standards groups stack up when it comes to these areas of IoT emphasis? Let's compare the five most popular and influential alliances.

The Alliances

Several groups have formed to try and sort out the technologies and create the mix of tools that will most likely succeed. One of the more popular alliances is AllSeen, which is backed by Qualcomm, Microsoft Corp. and LG. AllSeen uses an open-source technology that allows connected devices to communicate directly with one another, rather than through the cloud.

Other alliances include Thread, backed by Nest Labs; Open Interconnect Consortium, backed by Intel; Apple Inc. HomeKit; and Industrial Internet Consortium, founded by Intel, Cisco, AT&T, GE, and IBM. Samsung is a member of the Thread and OIC, but it also has its own solution, called SmartThings. Unfortunately, this profusion of industry groups, rather than solving the interoptibility issue, has only added to the fragmentation.

The AllSeen Alliance. The first IoT standards group, AllSeen was started by the nonprofit Linux Foundation. It now has more than 51 member organizations, including heavy hitters like Microsoft, Qualcomm, LG, Sharp, and Panasonic. AllSeen seeks to provide a secure, programmable software and services framework for applications that enable a connected home. The Alliance envisions connectivity taking place through transport layers such as WiFi, WiFi-Direct, Ethernet, Powerline, Bluetooth LE, 6LoWPAN, ZigBee, and Z-Wave. Interoperability is also a focus, with supported platforms including Android, iOS, Linux, OpenWRT, Windows, and OS X.

The Open Interconnect Consortium (OIC). The OIC, led by Intel, Atmel, Broadcom, Dell, and Samsung, is dedicated to defining requirements and ensuring interoperability of all devices in the IoT. Specifically, the OIC envisions a highway-like system of connectivity between IoT verticals, and it recently launched IoTivity, an open-source framework. The companies that make up the consortium also make security a top priority, though it's unclear how the group will address privacy.

The Thread Group. Formed by Google's Nest Labs, the Thread Group includes more than 80 members, including Samsung, ARM Holdings, Silicon Labs, and Freescale Semiconductor. The group's goal is to encourage manufacturers of smart-home devices to use the Thread standard for device communications through a network. Unlike other alliances that tout IoT platforms, Thread relies on a low-power radio protocol known as IPv6 over Low power Wireless Personal Area Networks (6LoWPAN). Thread sees this connectivity protocol as interoperable with the application layers provided by the other alliances.

HomeKit. Apple's entry into the consortium world wants to give third-party device makers approval under the "Made for iPhone" certification process already used for iOS accessories. HomeKit will supply toolkits for developers to make smart-home integration for developers and consumers. The HomeKit API features a common language designed to be interoperable with non-HomeKit devices that use protocols like ZigBee or Z-Wave.

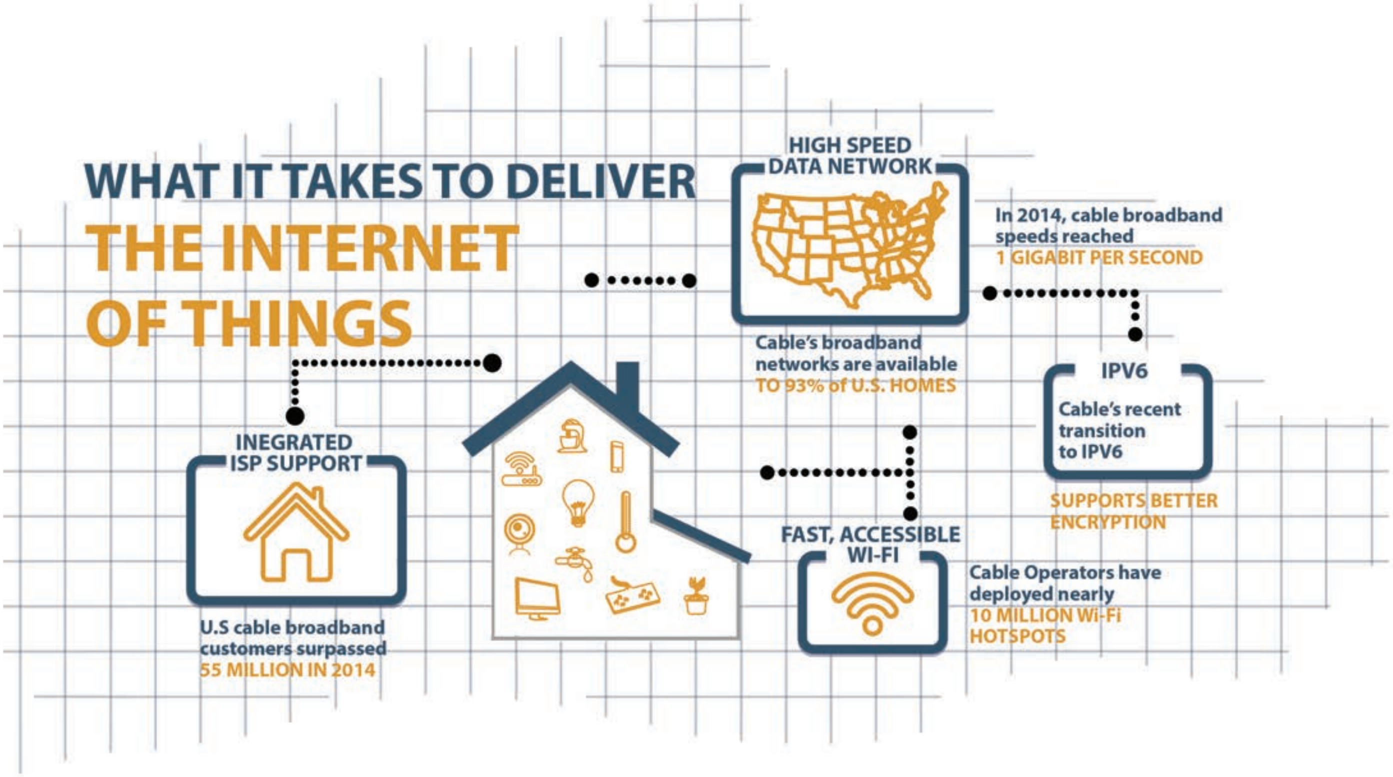
Industrial Internet Consortium. Founded by Intel, Cisco, AT&T, GE, and IBM, the 150-member IIC wants to accelerate IoT adoption while defining industry standards. The group's members are collaborating to develop connectivity standards, and the IIC has signed a strategic agreement with the OIC to share information to streamline IoT device interoperability. SAP recently announced it will partner with the IIC to deliver use cases, reference architecture and frameworks, and security for IoT applications.

Golgi IoT Cloud Service. Removes the complexity of developing a standards compliant IoT device by abstracting the standards compliance layer for developers and ensures forward and backwards compatibility for connectivity and data transport across AllSeen, OIC, and Thread with more standards being added in the future.

It's not clear which consortium will ultimately come out on top. And even if a winner is declared, it won't happen this year. According to a new IoT research paper published by Woodside Capital Partners, the most optimistic timeframe for a single standard to emerge is 2017.

Economic Advantages for the Operator

If the predictions hold true, the snowballing IoT world will grow dramatically in the next few years. When standards are identified and locked down, ISPs will be in the best position to offer a library of choices for the subscriber in a one stop shop.



WHAT IT TAKES TO DELIVER THE INTERNET OF THINGS

HIGH SPEED DATA NETWORK

In 2014, cable broadband speeds reached 1 GIGABIT PER SECOND

Cable's broadband networks are available TO 93% of U.S. HOMES

IPV6

Cable's recent transition to IPV6

SUPPORTS BETTER ENCRYPTION

INEGRATED ISP SUPPORT

U.S cable broadband customers surpassed 55 MILLION IN 2014

FAST, ACCESSIBLE WI-FI

Cable Operators have deployed nearly 10 MILLION Wi-Fi HOTSPOTS

In addition to the obvious stickiness of having the subscriber's home connected to a central gateway, operators can also use the gateway and TV as a dashboard for consumable and hardware purchases that expand IoT services. Whether selling light bulbs or sensors, having an easy way to add those devices through the same dashboard provides another way operators can expand services and revenue. The portal could let operators advertise new products and services directly. And as more devices become smart and connect to the internet, the average home will become a den of web linked goods. For internet service providers, this explosion in smart-home products represents additional opportunities to sell consumers on new services connected to their television or smartphone.

Security is an area of tremendous concern but also an opportunity for operators to leverage their wealth of experience in Internet security, firewalls, and digital rights management. One of the most important roles that the operator can play is to serve as a single point of security for the data that is passed not only around the home and between devices, but up to the cloud to enable communication with cellphones when the user is out of the home.

Creating a single point of security for all the data and devices controlled in a household can help reassure the subscriber about security concerns. No one wants the cameras they install to be available for anyone to see, or to disable their home security system or open their garage door. Security of IoT networks, data and devices will be a high priority feature of any system sold on the market. When services are collected together by the operator, intrusion points are consolidated in a single point of protection, reducing the number of places that are vulnerable to intruders.

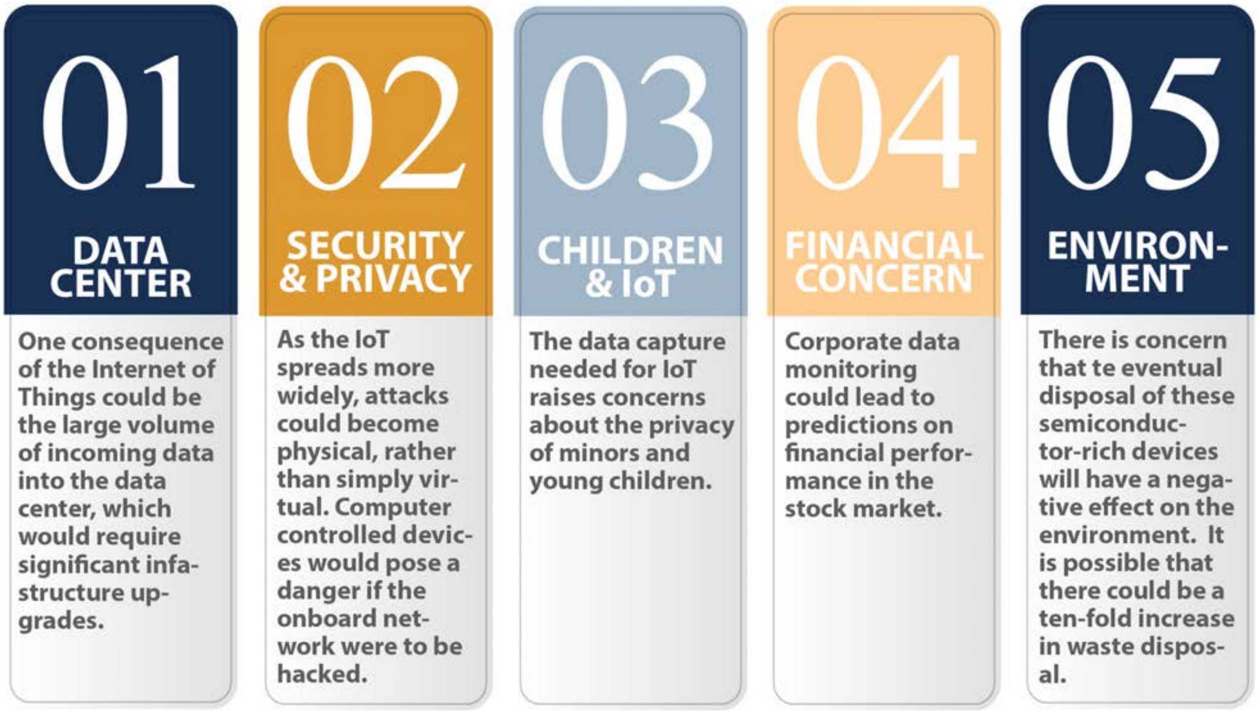
The Concerns

Reality is beginning to bite the Internet of Things and while the IoT will connect countless objects and systems, it also presents significant challenges. Many of those looking to enter into the IoT space are starting to look at the potential problems. So what challenges should operators be aware of when it comes to IoT?

THE DATA CENTER

Over the long term, one consequence of the Internet of Things could be the large volume of incoming data to the data center, requiring significant infrastructure upgrades, particularly for data processing and storage. With the expectations of 26 billion things within four years, imagine what it will be like for the datacenter as the IoT rush begins. Operators will be challenged to keep their infrastructure investment apace with the explosion of data traffic. Deployments of IoT will bring about vast amounts of data that has to be received, analyzed and responded to in real time and instantaneously. Processing large quantities of IoT data in real time will increase the workloads of datacenters, leaving providers facing new security, capacity and analytics challenges.

The majority of datacenter traffic is self-generated and hosted on servers in the data center location or facility, with some traffic between facilities, whether these are co-location or public-cloud services. But, as IoT communication ramps up, datacenters will have to transform. The enormous number of devices, coupled with the sheer volume, acceleration and configuration of IoT data, creates challenges, particularly in the areas of security, data, storage management, servers and the data center network.



01 DATA CENTER

One consequence of the Internet of Things could be the large volume of incoming data into the data center, which would require significant infastructure upgrades.

02 SECURITY & PRIVACY

As the IoT spreads more widely, attacks could become physical, rather than simply virtual. Computer controlled devices would pose a danger if the onboard network were to be hacked.

03 CHILDREN & IoT

The data capture needed for IoT raises concerns about the privacy of minors and young children.

04 FINANCIAL CONCERN

Corporate data monitoring could lead to predictions on financial performance in the stock market.

05 ENVIRONMENT

There is concern that te eventual disposal of these semiconductor-rich devices will have a negative effect on the environment. It is possible that there could be a ten-fold increase in waste disposal.

“Data center managers will need to deploy more forward-looking capacity management in these areas to be able to proactively meet the business priorities associated with IoT,” said Joe Skorupa, Vice President at Gartner Research.

With the increases in data flow and the transformation of datacenters, the urgency for effective congestion management and automated policy enforcement will become a pressing issue. Operators will need a way to automatically enforce fair use policies during the heavy consumption periods, which will coincide with some of the same periods we see today such as prime evening and weekend times. Providers will be under pressure from subscribers to see that everyone on their network is receiving a fair share of bandwidth resources. Automated policy management systems will help alleviate some of that pressure.

These systems should identify top talkers, who are exceeding, or close to exceeding, their bandwidth quota. Providers can efficiently monetize high-traffic users by offering interim or short term upgrades or full service plan upgrades. Offering a speed reduction agreement for the remainder of a subscriber's billing cycle might also mitigate some of the bandwidth overindulging. But the tendency to overestimate actual bandwidth requirements is leaving many operators with capital expenditures that are underutilized and taking up space in their data center. At the same time, many operators are unsure what upgrades will be required, or when the best time is to upgrade to stay in front of the IoT storm.

By taking the time, operators can support and offer an abundance of OTT and IoT services without risking the subscribers' quality of experience. Internet Protocol Detail Record (IPDR) is the data collection by the CMTS about the IP-based usage on a per subscriber basis. This process can collect network insights, analyze the information and enable providers to:

- Lower network congestion by increasing visibility into the network when congestion occurs, enabling the activation of usage policies at those congestion points.
- Create and implement fair usage policies that enforce actions such as temporary speed reductions and throttling for heavy users during peak periods.
- Isolate repetitive top talkers that cost operators more than the revenue being gained from them and encourage these users to upgrade.

SECURITY AND PRIVACY

Concerns have been raised that the Internet of Things is being developed rapidly without appropriate consideration of the profound security challenges involved. In particular, as the Internet of Things spreads widely, attacks could become an increasingly physical, rather than simply virtual, threat. A January 2014 Forbes magazine article listed many Internet-connected appliances that can already “spy on people in their own homes” including televisions, kitchen appliances, cameras, and thermostats. Computer-controlled devices in automobiles such as brakes, engine, locks, hood and truck releases, horn, heat, and dashboard can be vulnerable to attackers who gain access to the onboard network.

Issues of security and privacy arise in connection with data coming from devices. Hackers could see when water flowing into a home has been shut down for conservation reasons and deduce that no one is home.

FINANCIAL MANIPULATION

If someone is monitoring the water data at a Coca-Cola plant, they could actually calculate their product output and from that information possibly predict financial performance in the stock market.

> “WHAT YOU’RE ABOUT TO LOSE IS YOUR PRIVACY”
>
> *-WIRED Magazine*

CHILDREN AND THE INTERNET OF THINGS

Data capture is a key starting point when considering the effects of the IoT on young people and raises key questions regarding identity, privacy, and risk issues in relation to IoT developments relating to children and young people.

ENVIRONMENTAL IMPACT

Another concern regarding IoT technologies is the environmental impact of the eventual disposal of all these semiconductor-rich devices. Because the concept of IoT entails adding electronics to everyday devices like simple light switches, it is reasonable to expect that items that previously were kept working for many decades would see an accelerated replacement cycle if they were part of the IoT. For example, a traditional house built with 30 light switches and 30 electrical outlets might stand for 50 years, but a modern house built with the same number of switches and outlets set up for IoT might see each switch and outlet replaced at five-year intervals in order to keep up to date with technological changes. This translates into a ten-fold increase in waste disposal.

Final Thoughts

The implications of IoT are far-reaching for broadband operators. There are many hurdles to overcome but it’s an interesting space full of promise. We are at the forefront of a connected world and the next few years will probably be the shaking out years for the Internet of Things, with a huge amount of connected devices being developed and announced and infrastructure and network upheavals to accommodate them.

In order to quickly and efficiently accommodate these new IoT-ready devices, and monetize the emerging IoT infrastructure, operators will pursue new partnerships with the myriad device vendors similar to the relationships they have experienced for years with content providers.

It may take some time to get the stars to align on IoT, but it seems clear that operators will be a central player in IoT home solutions.

ZCorum™

1.800.909.9441

4501 North Point Parkway, Suite 125
Alpharetta, GA 30022

ZCorum.com | TruVizion.com
Facebook.ZCorum.com
Twitter.com/ZCorum