Global Knowledge®

Expert Reference Series of White Papers

The Internet of Things: A Primer for the Curious

The Internet of Things: A Primer for the Curious

Rich Hummel, CCNA, CCNAW, CCSI

Introduction

If the second wave of the Internet was the introduction of ubiquitous mobile devices, the Internet of Things (IoT), or Internet of Everything, is the third. It introduces billions of new sensors and devices to an already crowded global network. According to a recent study by IDC, the worldwide IoT install base will see a compound annual growth rate of 17.5 percent from 2013 to 2020.

A technical discussion about the IoT is limited because there is a standards war afoot that would make an in-depth discussion too cumbersome at this time. Instead we will look at what the IoT is; some key vertical markets where it can affect the most short-term change; the impact on existing networks; and some business, cultural, and ethical considerations.

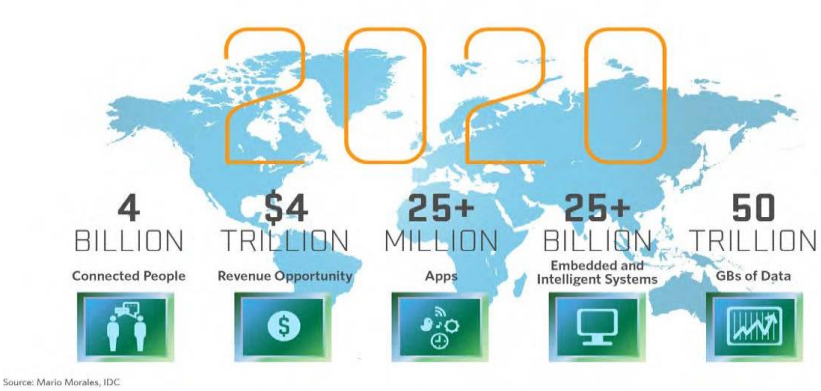
The Internet of Things Defined

Few people, even those in the information technology business, realize that we are quickly running out of Internet Protocol Version 4 (IPv4) addresses. The exact date when that happens is up for debate, but it is coming soon, with the number of Internet-connected devices exceeding the number of people on the planet.

Why do I bring this up in a white paper about the IoT? Because the IoT would not be possible without an almost **limitless supply** of addresses. It would be like a contractor building houses for which there are no more street addresses. Since IPv6 provides enough addresses (340 undecilion or $3.4X10^{38}$) to cover every square inch of the planet, including the ocean floor, we now have enough addresses to justify a discussion of the IoT.

Maybe you've heard of Machine-to-Machine (M2M) technology, which is the ability of machines to speak to each other and perform actions based on those conversations without human involvement. Think of your power utility monitoring your thermostat and adjusting the temperature based on its setting. If you can picture that concept, you have a good basis for a discussion of the IoT.

To give you an idea of how fast this technology is accelerating, in 2012, I had a discussion with an executive at the largest wireless provider in America. We discussed M2M at length, and a subsequent Internet search provided just a few results of companies involved in development projects. A year later, the CEO of a large networking manufacturer introduced the IoT to his channel partners at their annual summit. Today, just two years later, the number of companies involved in developing IoT applications has increased exponentially. And if discussion boards are the real indicator of activity in a particular industry, the IoT is ready to explode.



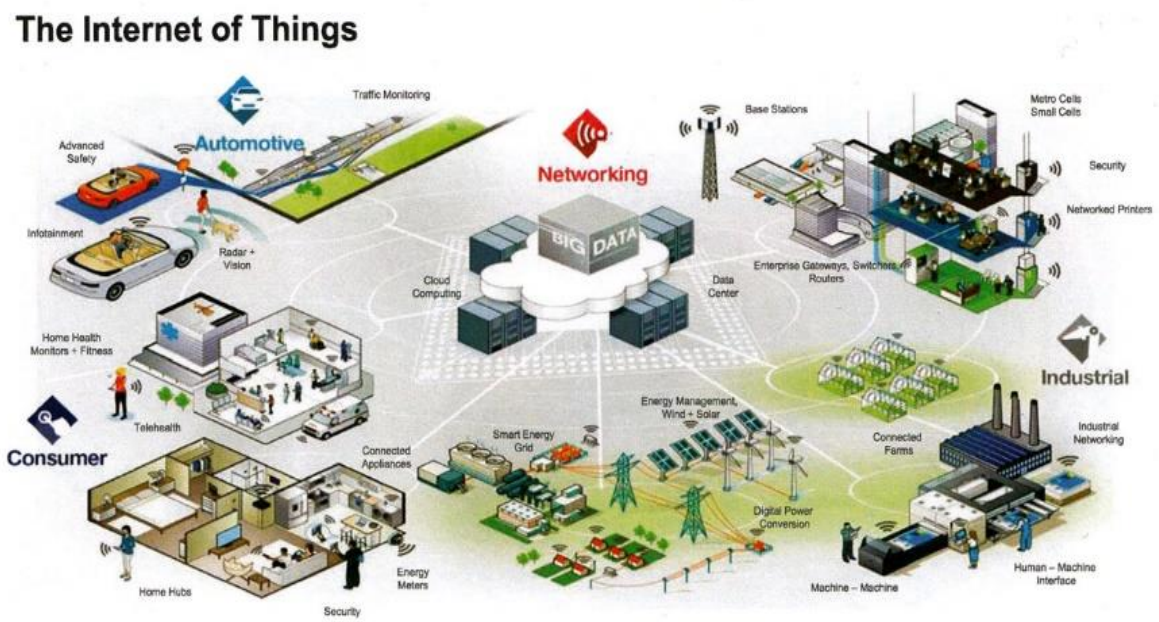
Source: Mario Morales, IDC

According to Wikipedia, "The **Internet of Things** (**IoT**) is the network of physical objects or 'things' embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator, and/or other connected devices." While that may seem broadly defined, it's accurate. The IoT will mean different things to different people. And once you accept this definition, you can see that there are almost limitless applications. Our homes, our businesses, our cars, our appliances, even our bodies themselves are potentially going to be connected to the Internet.

The purpose of this white paper is to provide a look at the present, a view into the future, and to consider the potential benefits and hazards of the IoT. If you come away with as many questions as answers, then this paper will have achieved its goals. Much of what is needed to make the IoT truly viable (e.g., technical standards) is still in development, and there is bound to be much contention before everything reaches a stable state where even early adopters are comfortable deploying a particular application into production.

How It Works and Its Applications

The IoT works the same way the Internet works. If you were to research the topic, what you would get back is information on how the Internet works. Applying simple logic tells you this makes sense. So what's the difference between how the Internet works and how the IoT works? As they say, the devil's in the details. It's the **application** that makes it different. What do you do with the information provided by all of these things we've connected to the Internet?



Even a cursory investigation into the IoT will produce a discussion of sensors, microcontrollers, actuators, micro-pumps, mobile communication devices, etc. For example, sensors designed to detect everything from the availability of parking spaces in urban environments to measuring the vital signs of athletes are used. These sensors will wirelessly connect to the Internet and provide data to be stored and analyzed. What we do with that data and its analysis is going to spark both technological and philosophical discussions worldwide.

Let's take a look at some simple examples in a handful of vertical markets to get your mind working on the limitless number of applications in every vertical market out there. These simple examples should allow you to go to work tomorrow armed with a variety of applications that make the place you work better.

Types of Applications

Commercial/Industrial

You're in charge of a large food processing plant. Some of your products require refrigeration at a very narrow range of temperatures. Someone does not completely close the door to the refrigeration unit and the temperature starts to slowly rise. The cooling system automatically adjusts the temperature, but it continues to rise over a thirty-minute period. Suddenly one of your employees receives a text message alerting them to this fact and they close the door, saving you energy costs and spoiled food.

Now use that same algorithm and apply it to any manufacturing facility, logistics company, or any industry or commercial building you imagine. Processes are controlled and adjusted automatically or remotely, lights are dimmed, and faults are detected. Now you might say a lot of that can be done today, but it's the level of granularity that will change.

Think of it this way: anything you'd like to monitor and control now has the possibility of being connected to the Internet. The only limitation is the human mind.

Medicine

The medical field is potentially where the greatest impact could be seen. Imagine wearing a sensor, or having one implanted, that would monitor all of your vital signs and all of your body's functions. Now imagine getting a text message telling you that you've taken in too much sugar or fat, or that you're lacking in vitamin D. If you're a pre- or post-operative patient, medicine could be released into your body through a transdermal nanopump on a prescribed schedule, rather than having a nurse come in and give you a shot or a pill.

Now imagine those body sensors in your connected home. You're lacking in specific vitamins? Your body sensor communicates with an application on your refrigerator, which recommends a shopping list containing foods high in that particular vitamin, or deletes the gallon of ice cream because your cholesterol is high.

Education

The potential exists for a significant paradigm shift in education, based on the adoption of the IoT. The traditional classroom, and the role of teachers in it, face dramatic changes in a completely connected world. Students will have access to new sources of traditional information, as well as the analyzed data gathered from the IoT.

Student data can also be gathered and analyzed to record attendance and performance. From a performance aspect, students' strength and weaknesses in particular areas of study can then be analyzed to indicate potential careers where they could be most successful.

Facility data can also be gathered and analyzed to reduce energy consumption and other operating expenses to extend historically strained educational budgets, or to reduce them, resulting in property tax reductions.

Agriculture

Irrigation systems up to this point have been pretty much an all-or-nothing proposition. Sensors placed in the soil at specific intervals could measure the moisture content and direct small, mobile irrigation systems to very specific parts of the farm to make sure that moisture content is kept at a level to produce the largest yielding plants.

Once the plants are harvested and ready for market, all of the logistics in getting those crops to market will be connected so that they arrive at stores at the appropriate time to ensure the best possible shelf life.

Retail/Consumer

The IoT will not only connect retail employees to each other and large amounts of product data through the use of wearable technology, but the products they sell will be connected as well.

The connected or smart home saw some of the earliest developments ion M2M and the IoT. Smart phones will talk to appliances, and appliances will talk to each other. This will provide automated and remote control of every electronic device in the home.

Smart Cities

When I first moved to San Antonio, Texas, I thought I was the luckiest driver in the city. Every time I came to a traffic light at an uncongested intersection, the light would turn green in matter of seconds. Then I noticed the cameras and access points mounted on the cross beam. This was my first introduction to a smart city.

That was over ten years ago. Today, all cities—large and small—will have the ability to monitor not only traffic intersections, but also traffic patterns all over the city. Then with the use of message boards and the exiting traffic light infrastructure, they can alter the flow of traffic to less congested streets.

And as previously mentioned, imagine driving in New York City and knowing where every available empty parking space is at any given moment in time. This alone would alleviate traffic problems in areas where people crawl down the street looking for an available space. For paid parking, rates could be posted as well, allowing you to find a spot within your budget.

Standards and the Lack Thereof

Remember the VHS-Betamax battle? OK, too '80s. How about the Blu-ray-HD DVD battle? There's a similar battle waging within the IoT. In order for our world to be truly connected, these devices must be able to speak the same language. The IEEE has all kinds of IoT *related* standards. But if you research those standards, you'll see they are all existing Internet standards. Whether its power, security, or network protocol standards, there are competing camps, led by the biggest players in the game.

Thread

Google and Samsung lead a group of big dogs leading the Thread camp. Google acquired Nest, a company that makes smart thermometers, and the Nest group is leading Thread's development. It sets Wi-Fi as well as security and power standards and is **IPv6 based**. What differentiates Thread from some of the previous wireless network protocols is its ability to operate at low power.

Thread uses IPv6 over Low power Wireless Personal Area Networks, or 6LoWPAN. Unlike network protocols for PCs, which are general purpose, 6LoWPAN is designed for a very specific purpose, in this case, home automation. It uses little memory and is low power. On the negative side, it has short range, low speed, and limited message size.

Don't expect to see Thread products until a certification program is in place. It should be noted that this effort is focused on the connected home vertical. As the IoT rolls out, we may see different standards in different verticals until a single standard can be agreed upon.

AllJoyn

AllJoyn is a protocol originally developed by Qualcomm, which then passed it on to the Linux Foundations. Qualcomm and The Linux Foundation then formed the AllSeen Alliance, bringing in Cisco, Microsoft, LG, and HTC as members, along with smaller company members. As of February 2015, AllJoyn has more than 120 members.

AllJoyn is a peer-to-peer protocol that discovers nearby devices (proximity detection) and manages the communication between those devices, including secure exchange of information. It is a distributed software bus using the existing D-Bus Wire Protocol, which is object-oriented and language neutral (C, Java, Perl, etc).

Other Protocols

There are other efforts out there. There's the **Open Interconnect Consortium, The Industrial Internet Consortium**, and what would a standards war be without **Apple or Android**? The bottom line is this: the battle will continue until there is a victor or a treaty. Until then, while the development of devices and applications for the IoT continues, adoption will be slow at best.

Network Impacts and Considerations

The impact on your network by implementing the IoT should be fairly obvious by now. Here are the new factors you should consider before implementing the IoT in your network:

1. Pervasive IPv6 deployment
2. A significant number of new devices and protocols
3. Massive amounts of new data
4. Irregular traffic generation
5. Increased cloud dependency

The level of impact on your network is going to be dependent upon how and to what extent you deploy the IoT.

IPv6

Obviously, since the IoT is dependent upon IPv6, you should be running a dual stack with IPv4, and be well on your way to a single-stack, IPv6 deployment. This eliminates the need to subnet, and simplifies what is going to become a much larger, more complicated network environment.

New Devices, More Data

Let's take a look at these issues from the outside in.

Internet Access

Chances are, the current pipe you have is sufficient, but with all of the traffic generated with the implementation of the IoT, it's going to have to be bigger.

Wireless Network

You're introducing potentially hundreds or thousands of new clients into the wireless network. If you would prefer that its performance is not negatively impacted, you're looking at more access points and more controllers to manage those access points. The new 802.11 standards can help here, but they are not going to make up for all of the new clients.

Data Center

Regardless of which protocol you end up deploying, if you are bringing all of these devices into your network, it is for a justifiable business reason. Each new device is going to be transmitting data into the network, which then needs to be stored and analyzed. Chances are, no matter how much future growth was built into your last data center upgrade, it won't be nearly enough. This is why if you speak to most people involved in technology sales, they see the data center as one of the greatest potential areas for growth. It may be time to consider that hybrid data center/cloud solution you've been discussing for the last few years.

Performance Monitoring

The way you monitor performance is going to change to accommodate this new data. If not properly planned for, the massive amounts of new data stored on your network is bound to create performance issues. If your performance monitoring platform does not scale well, you could find yourself monitoring certain things less frequently, monitoring only those things you deem most important, or using average metrics to produce capacity forecasts, which presents problems down the road.

Monitoring platforms will now be measured by **speed at scale**. In other words, as the size of your network increases geometrically, your monitoring platform is able to perform at the same speed as previously needed.

Irregular Traffic Generation

These new devices we've introduced are going to generate traffic **in short bursts on irregular schedules**. That is, only when they have to. Polling your network at five-minute, or even one-minute, intervals is no longer going to work. It may be necessary to poll every second to allow for the billions of devices that will be communicating over the IoT.

Short-burst traffic like this, when monitored at five-minute intervals, may be flattened out. This could create problems with latency-sensitive applications like VOIP and video. The difference between polling your network at five-minute intervals versus sub-one-minute intervals is like the difference between a standard DVD and a Blu-Ray disc. All of those imperfections you see on a high definition disc are not visible on a standard disc.

If you want a true view into your network's performance, make sure your monitoring platform supports high-frequency polling. This will make troubleshooting performance issues in the IoT world much more efficient and effective.

Increased Cloud Dependency

We've discussed the potential impacts of the IoT on your network. What now? Do you make that difficult trip to your CFO's office and present him with next year's IT budget, which would likely result in a trip to the cardiac unit of your local hospital? Or maybe you need to make that presentation to the local planning board to convince them that if they really want to keep up with the school system in the town next door, that everyone's property taxes are going up.

If those are things you'd rather not do, you're likely to consider other options, the most obvious one being transferring some of your IT operations to the cloud. Of course, surrendering even a small part of your operations to the cloud limits the amount of control you have over that part of your operations.

The National Institute of Standards and Technology's (NIST) working definition of cloud computing cites five essential characteristics of cloud computing:

- **Broad Network Access** — Capabilities are available over the network and accessed across a varying set of platforms or end-user devices, such as mobile phones, tablets, laptops, etc.
- **Resource Pooling** — The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, whether we're talking about storage, processing, memory, or network bandwidth.

- **On-Demand Self-Service** — A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Rapid Elasticity** — You have capabilities that can be rapidly provisioned and released to scale in a manner that's commensurate with demand.
- **Measured Service** — Clouds leverage a metering capability at some level, so resource usage can be monitored, controlled, and reported, which provides transparency for both the provider and consumer of the cloud service.

These five areas provide an initiation point for the discussion. You may already be using some level of cloud services. How much more of your operations you want or need to turn over to the cloud is both a business and technical decision.

Security Considerations

The Open Web Application Security Project (OWASP) lists the top ten security issues for the IoT as:

1. Insecure Web Interface
2. Insufficient Authentication/Authorization
3. Insecure Network Services
4. Lack of Transport Encryption
5. Privacy Concerns
6. Insecure Cloud Interface
7. Insecure Mobile Interface
8. Insufficient Security Configurability
9. Insecure Software/Firmware
10. Poor Physical Security

Each one of these are provided as a link on the OWASP website should you choose to do a deeper dive into a specific area. Even a cursory investigation into any one of these areas will demonstrate that one of the primary considerations before allowing the IoT on your institution's (even your home's) network is security.

How serious is the threat? Last year it was revealed that Samsung smart televisions, while recording voice commands, could also record private conversations. This data was unencrypted and sent to third parties. Just last week, the United States Congress began hearings on security issues with the IoT.

The manufacturing of IoT devices is going to be done overseas to contain costs. This introduces the likelihood, however remote, that there will be security holes that malevolent entities can exploit. Like the IoT standards war, this will eventually be addressed and resolved. The decision needs to be made whether the benefits of incorporating the IoT outweighs the risk.

Big Data and Analytics

The impact of the IoT on big data and analytics is going to vary by industry. Obviously, health care, smart cities, and energy utilities are going to generate massive amounts of new data which is going to need to be stored, analyzed, and then have the results of that analysis stored as well. This is going to require significant core infrastructure updates, so as not to impact the performance of existing parts of the network.

Network designers are also going to need to make sure that all new data entering the network is worthy of being stored. So data management will be necessary to determine what data is to be stored, where it will be stored, and for how long. Some of this data may need to be discarded, or passed on to other locations to be stored and analyzed.

Business and Ethical Implications

Most discussions on the IoT are technical, or application based. But rest assured, as more and more people become aware of, then impacted by, the IoT, the discussions will turn to business and ethical considerations.

How much are people going to want retailers, utilities, and/or the government about their activities? Early on, people will be fascinated by the increased variety of information, the positive educational, and health care improvements. But the first time someone's personal information is compromised, it will be game on for litigators.

People may find it fascinating how much companies will know about them until some unscrupulous company uses it against them. The question to be answered is, if we cannot secure the personal information of individuals today, how are we going to do it when the number of devices potentially carrying that information increases by a factor of 100?

Business leaders from all industries are going to have to carefully consider what information they collect, how it is analyzed, and what is to be done with it. If they only focus on business efficiencies and profit margins, then they will likely finding themselves defending their decisions in court.

Exponential leaps in technologies rarely come without some impact on humanity. When 1984 came and went without Big Brother watching us, everyone let out a big sigh of relief. However, the IoT has the potential to bring us to that point, even if it is more than two decades late. There will be those who will point to improved security, but at what cost?

Conclusion

Like it or not, the IoT is upon us. There are a number of factors that will impact its adoption rate, and the inevitable privacy (or lack of) discussions will likely happen sooner than later. This is going to change the world as we know it, in many cases for the better. But we will need to keep an eye on the extent to which it invades out personal lives if it is going to be the positive force it has the potential to be.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

Cisco Data Center Curriculum

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Rich Hummel has a bachelor's degree in electrical engineering from New Jersey Institute of Technology, and a master's degree in technology management. He has worked extensively with wireless, video, and cloud technologies.