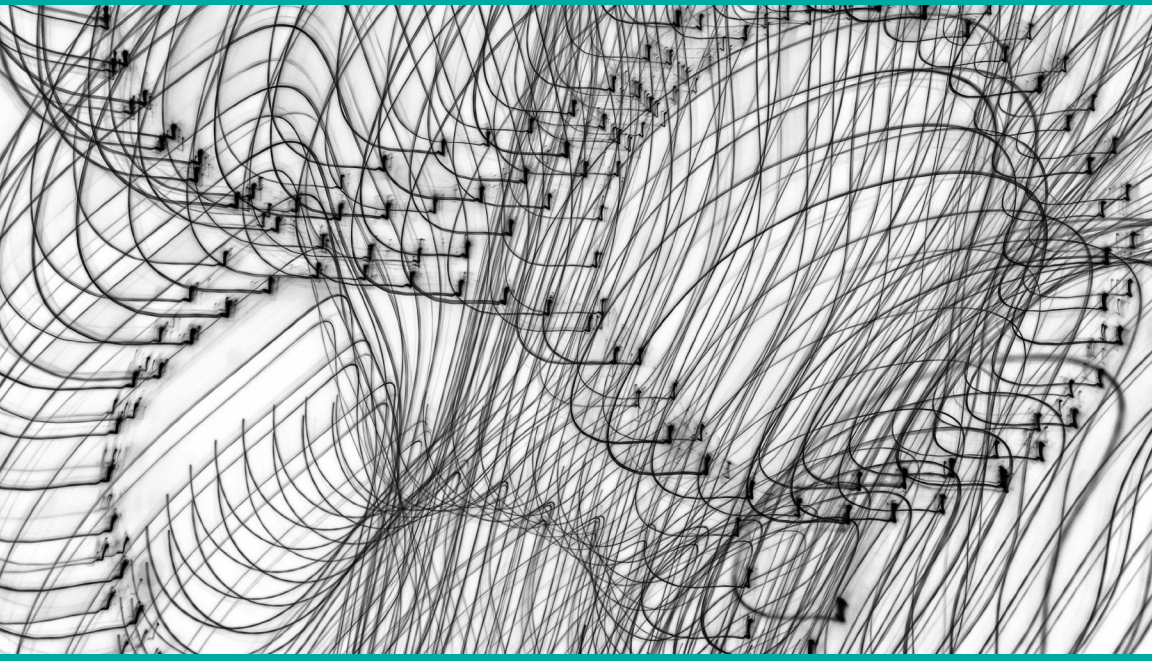
O'REILLY®

Are Your Networks Ready for the IoT?



Mike Barlow

4 Easy Ways to Stay Ahead of the Game

The world of web ops and performance is constantly changing. Here's how you can keep up:

1. **Download free reports** on the current and trending state of web operations, dev ops, business, mobile, and web performance. http://oreil.ly/free_resources
2. **Watch free videos and webcasts** from some of the best minds in the field—watch what you like, when you like, where you like. http://oreil.ly/free_resources
3. **Subscribe** to the weekly O'Reilly Web Ops and Performance newsletter. http://oreil.ly/getnews
4. **Attend the O'Reilly Velocity Conference**, the must-attend gathering for web operations and performance professionals, with events in California, New York, Europe, and China. http://velocityconf.com

For more information and additional Web Ops and Performance resources, visit **http://oreil.ly/Web_Ops**.

O'REILLY®

Are Your Networks Ready for the IoT?

Billions of Smart Machines and Sensors Place New Burdens on Systems for Sharing Data

Mike Barlow

Beijing • Boston • Farnham • Sebastopol • Tokyo O'REILLY®

Are Your Networks Ready for the IoT?
by Mike Barlow

Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*http://safaribooksonline.com*). For more information, contact our corporate/institutional sales department: 800-998-9938 or *corporate@oreilly.com*.

Editor: Courtney Allen
Production Editor: Shiny Kalapurakkel
Interior Designer: David Futato
Cover Designer: Karen Montgomery

January 2016: First Edition

Revision History for the First Edition
2016-03-04: First Release

978-1-491-94243-7

[LSI]

Table of Contents

Are Your Networks Ready for the IoT?

Imagine if you live in a country that has cars and roads, but no highways. Your car would be useful, but it would be much *more* useful if there were highways.

Imagine the Internet of Things as systems of highways. What should we expect from those systems?

Naturally, we would want them to be safe, secure, and resilient at every level. In addition to providing seamless and reliable connectivity, they would be scalable and cost-effective.

It's important for us to discuss and delineate our expectations of IoT systems, because the universe of connected smart devices and sensors is expanding rapidly. Four years from now, according to several estimates, there will be 20 billion to 50 billion connected devices and the IoT will add between $7 trillion and $19 trillion to the global GDP.[1]

Growth at that scale will create challenges and opportunities for businesses, organizations, and individuals in every sector of the economy. William Ruh, chief digital officer at GE, describes the IoT as a vast network of "chatty machines," generating data at speeds and volumes that would have seemed unimaginable just a few years ago.

The looming transformation raises a critical question: are existing networks ready for the data traffic that will be created by a vibrant and growing IoT economy?

1 *http://onforb.es/1QmGf1I*

A Symphony of Networks

Because practically all of us carry mobile phones, we tend to perceive our communications network as exclusively wireless. But moving signals around the planet requires an ensemble of multiple networks. There's a physical layer consisting of copper wire, coaxial cable, and optical fiber. Signals are conveyed by cellular wireless wide area network (WWAN) systems such as 2G, 3G, 4G, and coming soon, 5G. A small portion of signal traffic is handled by satellites orbiting the Earth.

Generally, however, we do not access signals directly from those large-scale systems. Most of the time, our mobile phones and devices are pulling data from wireless local area networks (WLANs) such as Wi-Fi, or wireless personal area networks (WPANs), such as Bluetooth or ZigBee.

Since WLANS and WPANs are low-power, short-range networks, telecom companies are pushing optical fiber closer to users in an effort to reduce the distance signals need to travel through the air. Those efforts are sometimes referred to as *fiber to the curb* (FTTC) and *fiber to the home* (FTTH).

The push to shorten the gap between users and access points creates the illusion of a completely wireless network, when in actuality, the network we perceive is a complex orchestration of wires, transmitters, and various mobile devices.

We'll Need Another Closet

Peter Winzer currently heads the Optical Transmission Systems and Networks Research Department at Bell Labs in Holmdel, NJ. For the past seven years, he's been exploring spatial multiplexing as an option for scaling optical fiber systems to transport more data. The impetus for his work is based on a simple premise: data networks are running out of capacity.

"Data traffic has been growing at roughly 60 percent annually for well over two decades, and that was before the Internet of Things," says Winzer. "The truth is we don't have enough network capacity to support the future of data traffic. There won't be enough bandwidth within the existing network."

Part of the challenge is human nature. "It's like filling up your closet and then building a second one. Pretty soon, you'll fill that one too," he says.

From Winzer's perspective, the solution requires a combination of evolution, innovation, and integration. "When optical fiber came along in the 1970s, we ripped out most of the coaxial cable or twisted-pair copper wire and replaced it with glass. Since then, little has fundamentally changed. There isn't another medium on the horizon that's likely to replace optical fiber," he says. "The next likely step will be inventing highly-integrated parallel optical paths and transmission systems."

Even if they aren't as dramatic as shifting from copper wire to optical fiber, upgrades will be necessary. The Shannon Limit is a theoretical barrier limiting the amount of data that can be sent across a network. As predicted by Moore's Law, the capabilities of microprocessors are growing and their costs are declining. Since computing processes generate data, it's fair to assume that data traffic will continue climbing toward the Shannon Limit—with or without the IoT.

Which Half of the Chess Game Are We In?

The "original" Internet was built initially for sharing static information such as email messages, documents, and photographic images. While it's true that Internet traffic has grown steadily over the past two decades, the increases have been relatively modest compared to the leaps in data traffic that are expected when the IoT and its larger cousin, the Industrial Internet, kick into high gear.

"Industrial assets such as jet engines and wind turbines produce tremendous amounts of data," says Benjamin Beckmann, lead scientist at the Complex Systems Engineering Lab in GE Global Research. Applying machine learning and predictive analytics to data generated by industrial equipment requires collecting and aggregating the data in a processing center. "An airliner creates more than a terabyte of data during a flight. Transmitting data of that size back to a data center is a huge challenge."

Beckmann and others are concerned by the sheer quantity of data flowing from sensors and smart machines operating in critical industries such as aviation, healthcare, manufacturing, mining, and power generation. He compares the situation to the 3,000-year-old

story about a man who teaches his king to play chess. He asks the king to reward him by placing a grain of wheat on a corner square of a chessboard and then doubling the number of grains on each successive square. The deal seems reasonable until the first half of the chessboard is filled, at which point the king realizes that it would take more than the entire's world supply of wheat to fill the second half of the chessboard.

"We're on the second half of the chessboard now," says Beckmann. It's not all bad news, however. Thanks again to Moore's Law, it's becoming increasingly feasible to move computing processes closer to the devices at the edges of your network. Instead of transporting data from a remote location to a data center for processing, "you've got processing power near the asset that's producing the data," he says. Beckmann is optimistic about the prospects for a new generation of intelligent machines that can analyze the data they produce and generate usable insights for optimizing their performance in real time.

All IoT Data is Not Created Equal

Rod Anliker is director, OEM Server Architecture, at Hewlett-Packard Enterprise. Like Winzer and Beckmann, he's concerned by the amount of data the IoT will generate. From his perspective, however, part of the challenge arises from thinking about IoT data as a static or uniform phenomenon.

"The value of IoT data changes over time," Anliker says. "Much of it is perishable. The value of some IoT data disappears within a few seconds." Let's say, for example, that a smart device mounted on an oil rig begins overheating. A sensor on the device will send a signal across an IoT network, alerting an operator to the possibility that the device is overheating and that action is required. If the signal is delayed, its value diminishes.

"In some cases, you might also need to know why the device is overheating so you can take the right action," Anliker says. "But you can't wait five hours for the data to arrive. You might not be able to wait even five seconds."

There can be multiple reasons for a machine or device to begin overheating. The problem could be internal, or it could be caused by another component in the system. "If it's a complex problem, you

need to find the source of the problem to make the right decision," he says. "When you only have a few seconds to make a decision, edge computing is extremely valuable."

Edge computing (which encompasses fog, grid, and mesh computing) enables you to run analytics at or near devices and machines connected to IoT networks. With edge computing, you don't need to send all the data back to a central data center for analysis. In effect, edge computing eliminates or reduces latency issues that would drive down the value of IoT data.

"Even Moore's Law can't overcome the speed of light," Anliker says. "Connectivity is expensive and it reduces the return on investment (ROI) of the system. The cost of storage can also be quite significant."

That doesn't necessarily mean that edge computing is the solution for all IoT network challenges. Pushing analytics to the edge of the network requires fine-tuning servers and applications to function in real-time, often in harsh or unforgiving environments.

"If you want to get the maximum value from your data, you need to configure your servers for IoT edge-computing workloads," he says. "The servers must be tailored to the workloads. You can't simply use general-purpose computers for this."

Monitoring machines, equipment, and even people is another challenging IoT scenario. It often involves processing streams of live video data from arrays of high-resolution cameras. "Video processing is a highly demanding use case where you're trying to correlate multiple images in real time. The signals are digitized, compressed, and then decompressed. It's a lot more complicated than your smart thermostat at home sending JSON data packets into the cloud," Anliker says.

More Than a Matter of Bandwidth

"Generally speaking, it's fair to say existing networks are ready for IoT traffic, because IoT traffic isn't all that different from normal IP (Internet Protocol) traffic," says Xiaofan (Fred) Jiang, an assistant professor in the Department of Electrical Engineering and the Data Science Institute at Columbia University. "The current trend is making IoT devices IP-compatible, so I don't think we're going to see a

sudden change in IoT traffic. We'll likely see a gradual increase in traffic as IoT devices become more commonly used."

Jiang's research covers cyber-physical systems and data analytics, smart and sustainable buildings, mobile and wearable systems, environmental monitoring and control, and connected health and fitness applications. Although he does not believe network capacity will pose a direct obstacle to IoT growth, there are subsidiary issues that could prove troublesome.

"For example, the number of IP endpoints will increase," he says, noting that every connected device and sensor on the network will have its own IP address. Upgrading IP networks from IPv4 to IPv6 would accommodate more endpoints, he says.

Additionally, he says, many IoT applications will require real-time data to function properly. That means network providers would have to offer run-time guarantees, which might require further infrastructure upgrades or modifications. "I'm not too worried about the networks right now, because none of this will happen overnight," says Jiang. "Instead of thinking about the networks themselves, it's more appropriate to look at the 'last mile' links."

A robust IoT ecosystem includes a wide range of devices relying on various types of links for connectivity. Jiang recommends planning ahead for a variety of wireless protocols. "We already see lots of IoT devices using Bluetooth and not Wi-Fi. Some devices are connected through ZigBee or Z-Wave. Google has released OnHub, a wireless router designed for a diverse set of user access points," says Jiang. "You need to consider which protocols to support at the link level and at the network level."

Volatility, Storage, and Special Cases

On the whole, IoT devices will be more diverse and less stable than most of the Internet devices we've grown accustomed to using. Unlike laptops and tablets, many IoT devices and sensors won't need continuous connectivity to a network. "They will connect for maybe two seconds and then disconnect," says Jiang. "From a temporal point of view, the connectivity of an IoT device is more volatile. So your 'last mile' infrastructure needs to support that volatility."

Environmental sensors, for example, will "sleep" most of the time, and "wake up" only long enough to send short bursts of informa-

tion. "From a network perspective, you'll see these devices connecting and disconnecting very rapidly. That's a very volatile paradigm and your network will need to handle it," says Jiang.

Data storage is likely to become an issue since most IoT data will be relatively "useless," according to Jiang. "You'll need to create a storage hierarchy and manage the data based on its value to you." Organizations will have to learn the best techniques for extracting value from raw IoT data in real time, and then storing the data inexpensively for future use.

Jiang agrees with the general notion that not all IoT data has equal value. But he is wary of creating special systems or protocols for different kinds of data. "Let's not group IoT devices into their own little networks. That is fundamentally contrary to the basic principles of the IoT. Instead, let's rely on the traditional idea of end-to-end reliability," he says. "If you're worried about enhanced security, focus on the endpoint, and not on creating a special virtual local area network (VLAN)."

In other words, don't treat the IoT as a special case. "That would be bad for the ecosystem," says Jiang. "Let's build on the same principles that made the Internet successful."

Forests of Sensors

Thomas Nicholls is executive vice president of communications at SIGFOX, a French company that provides cellular connectivity for low-power devices and sensors. Nicholls foresees a world in which common objects such as windows, washing machines, and trees are equipped with sensors capturing and relaying timely data about their environments. From his perspective, the question of network readiness should focus on capability rather than capacity.

"We're looking at a technology disruption that's on the scale of cell phones and possibly larger," says Nicholls. "I am completely convinced this is a revolution."

Nichols says he is less worried about handling data traffic from physical devices and more concerned about utilizing patterns of information emerging from the data. The challenge is representing data collected from physical devices in ways that makes it usable and valuable to companies, organizations, and ordinary citizens. "You

need cheap and dead simple approaches for representing 'things' from the IoT on the web," he says.

"For example, one of the companies using our network makes sensors they put on trees. The sensors don't need batteries; they use energy from natural light. They just measure temperature. If there's a huge increase, they activate another sensor that checks the wind speed and the wind direction," Nicholls says. "The information is sent to a fire station, where the firemen can see exactly where the forest fire started, where it's spreading to, and exactly how fast it's spreading. Then they go out and they stop the fire before it's too late."

Nicholls says connecting the tree-mounted sensors is "ridiculously cheap" and requires very little energy. "It's the type of use case that could never have existed before the IoT," he says.

The Role of SDNs

Another factor to consider is the role of software-defined networks (SDNs) in IoT ecosystems. Essentially, SDNs enable network administrators to program networks dynamically, rather than simply sending data across existing network architecture. "Networks will definitely need to be more dynamic," says Antonio "Ato" Sánchez-Monge, a network architect at Juniper Networks and coauthor of *MPLS in the SDN Era: Interoperable Scenarios to Make Networks Scale to New Services* (O'Reilly Media, 2015). "It will not be just about adding capacity, but about using that capacity more intelligently, and here is where software comes into play. It is paramount to count on more agile mechanisms that enable shifting or adapting capacity as required."

Sánchez-Monge and his coauthor, Krzysztof Grzegorz Szarkowicz, describe two mechanisms for making networks more flexible, adaptable, and dynamic. "On the service-aware layer, we discuss service chaining, which allows steering an information flow at will. And on the core layer, we explain how a centralized controller can help to distribute traffic so that network links do not get congested. We believe that these are good examples of the dynamic and flexible networks that will be able to support IoT in the future," Sánchez-Monge writes in an email.

Moreover, he writes, SDNs have "triggered" the wider implementation of techniques for automating networks. "In the last decades we have been using pre-historic mechanisms and technologies to configure and manage networks. It is now the time to produce a shift that results in automated, intelligent infrastructures that can instantly be reconfigured, and … we can start applying artificial intelligence to the way networks behave. It is definitely the start of a new era."

GE's Beckmann agrees that SDNs will likely play a major role in the evolving IoT landscape. "SDNs are the next generation of networks," says Beckmann. "Traditionally, the network has a set of tables. Those tables decide where and how information flows. With an SDN, you can program the network on the fly to manage different requirements. If you need high levels of redundancy, you can program the network to give you multiple physically independent tasks. Or if you need low latency, you can program the network to give you the most direct route possible. If you need security, you can program the network to put encryption tunnels in place. You can combine these in any way you choose."

Frank Kobuszewski, vice president at CXtec, an IT infrastructure company, cautions that software-defined networks aren't a one-size-fits-all solution. "In large data centers, SDN can be one way to increase the scale of network capacity with less impact on the IT staff," he writes in an email. "The benefits of SDN seem to be more viable for larger organizations … For small or medium businesses, SDN is a different story. These organizations likely do not have the scalability issues of large data centers and may not need to jump in right away. As the SDN market continues to evolve and we see more solutions come into play, IT professionals in the small and medium-sized business space should evaluate their options and begin understanding how SDN can positively impact their organizations."

He recommends focusing on security issues posed by the IoT. "The most important aspect for organizations to consider is security," he writes. "With people connecting various devices to the enterprise network, security needs to be at maximum levels. Who is connecting what device? What information can they access and store? This seems like a no-brainer, but I don't believe we've scratched the surface of all the security implications of the IoT."

Playing Hide and Seek with IoT Devices

Discoverability is yet another issue that will become amplified as the IoT expands its footprint. Ideally, organizations should be able to find and identify the devices on their networks. IoT devices should be difficult to hide and easy to "discover." But that requires manufacturers of IoT devices to follow a set of standards, similar to the standards followed by manufacturers of electrical devices.

Henning Schulzrinne, the co-developer of key protocols enabling voice over Internet protocol (VoIP), was chief technology officer for the Federal Communications Commission (FCC). He is also a professor in the Department of Computer Science and the Data Science Institute at Columbia University.

"In the classic office environment, most network devices are installed by the IT department, which maintains an inventory of those devices," he says. "But IoT devices such as cameras and thermal sensors are installed by a wide range of people from various departments and companies. So it's more challenging making sure these devices don't just randomly show up on your network and nobody has any idea what the devices are doing. In that case, you're just hoping the device is there for a valid reason, but you can't really be sure."

Lurking within the discoverability challenge, he says, is another thorny problem: "How do you make sure the software for those IoT devices is updated? What if they're running older versions? What if they can't 'phone home' for updates? What if support for them has been discontinued by their manufacturer or the manufacturer has gone out of business? Those devices should have a way of sending a message saying, 'It's no longer safe for me to be on your network, so I'm taking myself offline.' But I'm not aware this capability exists for the IoT, at least not today."

IoT and Smart Cities

The smart city movement has emerged as the unofficial test bed for IoT development on a grand scale. Since smart city projects are often combinations of new and old technologies, they offer unique opportunities for exploring the potential of IoT ecosystems. The Dallas Innovation Alliance is a public-private partnership driving smart city initiatives for the City of Dallas. Alliance cofounders Jen-

nifer Sanders and Trey Bowles emphasized the foundational value of creating strong network infrastructures.

"Our vision is to execute a multi-phased strategy, with its pilot phase focused in a downtown district called the West End," Bowles says. The West End is already equipped with optical fiber, making it an ideal area for beginning smart cities initiatives and "eliminating project delays based on the need for initial infrastructure development of the backbone of the network." The city also plans to continue improving networks across Dallas and will roll out best practices, developed in the West End, to other parts of the city, he says.

"Most cities are at varying points of 'network readiness' across a spectrum," says Bowles. Handling the massive amounts of data produced by citizens on a daily basis—independent of a robust smart cities initiative—requires solid partnerships with experienced service providers. Conducting a thorough audit of existing network capabilities and comparing them with projected needs are necessary steps in the evolution of smart cities.

"We believe most cities will need to take a close look at (their) existing network infrastructure and capacity," says Bowles. "We have learned from the experts that without a smart infrastructure as a foundation, a smart city initiative will not be successful. It is enormously important to learn from those who have walked this path before … there are clear best practices and lessons learned to be utilized as a foundation for new efforts."

Conversational Machines and Devices

A hypothetical scenario: Somewhere, on the windswept steppes of Asia, there's an automated wind farm, with three wind turbines generating low-cost electricity for the surrounding towns and villages. A fourth wind turbine is installed and within a few days, its embedded sensors and diagnostic analytics begin detecting anomalies in its performance.

All four wind turbines are connected to the IoT, so it won't be a problem for the new turbine to 'phone home' and ask for instructions. But is that the best solution? Home could be thousands of miles away and it could take days or weeks for a repair crew to arrive.

Wouldn't it be better if the new turbine could ask the older turbines how they handled similar situations? Maybe two of the turbines are also relatively new. They might advise the newest turbine to shut itself down and wait for the repair crew to arrive. But let's say the oldest of the turbines has experienced similar anomalies and knows they aren't likely to result in catastrophic damage. The old turbine might advise the newest turbine to stick it out and keep spinning its blades. And instead of listening to the two turbines that advised shutting down, the newest turbine would give added credence to the old turbine's advice.

That type of scenario is just around the corner. A similar scenario was described recently by Klaus Bauer, head of basic technology development at TRUMPF Werkzeugmaschinen. Speaking on a panel at the IoT Solutions World Congress in Barcelona in October 2015, Bauer offered a vision of "social machines" constantly sharing critical information about their current states and continually "helping" each other over time.

For that vision to become reality, networks of connected machines would need "semantic models" enabling the machines to "understand" each other and respond meaningfully in real time. How close are we to achieving that goal? It's probably only a few years away. The IoT is evolving swiftly, and networks won't be far behind.

"Today, the amount of data that flows across the Internet is primarily driven by human activities," says Sánchez-Monge. As a result, the growth of network capacity is aligned closely with the rate at which people gain access to the Internet, which in turn is closely aligned with world population growth.

The IoT, however, shifts the focus from people to machines. "The paradigm changes when the producers (and sometimes the consumers) of information are no longer humans, but machines," he says. "The rate at which the required capacity will grow year by year may be orders of magnitude higher in the future, because the number of devices will multiply and the nature of those devices will be more complex."

Evolutionary processes are nondeterministic by nature, so it's difficult to predict the future of IoT networks with precision. It's reasonable to assume that as data traffic grows in volume and variety, IoT networks will grow in capacity and capability, creating new areas of opportunity for organizations and people at every level of society.

About the Author

Mike Barlow is an award-winning journalist and author. He is coauthor of *The Executive's Guide to Enterprise Social Media Strategy* (Wiley, 2011), *Partnering with the CIO* (Wiley, 2007), and *Learning to Love Data Science* (O'Reilly, 2015). He is also the writer of many articles, reports, and white papers on marketing strategy, collaborative social networking, cloud computing, cyber security, machine learning, and big data analytics.

Over the course of a long career, Mike was a reporter and editor at several respected suburban daily newspapers, including *The Journal News* and the *Stamford Advocate*. His feature stories and columns appeared regularly in *The Los Angeles Times*, *Chicago Tribune*, *Miami Herald*, *Newsday*, and other major US dailies.

Mike is a graduate of Hamilton College. He is a licensed private pilot, an avid reader, and an enthusiastic ice hockey fan. Mike lives in Fairfield, Connecticut, with his wife and their two children.