NETWORKWORLD
FROM IDG

THE CONNECTED ENTERPRISE

INSIDER EXCLUSIVE

GETTING GROUNDED *in* IoT

NETWORKING & SECURITY

A guide to the basics enterprises need to know about the **INTERNET OF THINGS**

INTRO

THE INTERNET OF THINGS already consists of nearly triple the number of devices as there are people in the world, and as more and more of these devices creep into enterprise networks it's important to understand their requirements and how they differ from other IT gear.

The major difference is that so far they are designed with little or no thought to security. That stems from having comparatively little memory and compute power to support security but also because often they are designed with time-to-market, price and features as top considerations to the exclusion of security.

IoT devices use a varied set of communications protocols, so in an enterprise environment it's essential that there's support for whatever means they use to transfer the data they gather. They are also built around a small set of recent standards or no standards at all, which can complicate interoperability.

Vendors, service providers and practitioners are working on these problems, but in the meantime, it's important for networking pros to come up to speed with the challenges they face when the time comes to integrate IoT.

That's where this guide comes in. It starts off with an article about what to consider when networking IoT devices. This includes linking up and communicating, but also the impact that the volumes of data they produce will have on networking infrastructure, delay, congestion, storage and analytics. IoT can even have an impact on network architecture, pushing more computing power to the network edge to deal with this data close to its source. Management is yet another challenge.

This is followed up by an article about how the network itself might have to become the place where IoT security is implemented. Given that the most desirable aspects of IoT – cost, density of deployments, mobility – cannot be forfeited, and compute power is limited, something else has to pick up the slack. That something else could be the network and how it's segmented to isolate IoT devices from attackers.

This is followed up with 10 quick tips that help enhance IoT security.

A major subcategory of IoT is industrial IoT, which includes robots, sensors and other specialized equipment commonly found in industrial settings. They come with their own set of challenges and security concerns that are the topic of the fourth article in this package.

Finally, there's a glossary of IoT terms that are essential to understand if you're going to tackle the challenge of embracing IoT in the enterprise.

INSIDE

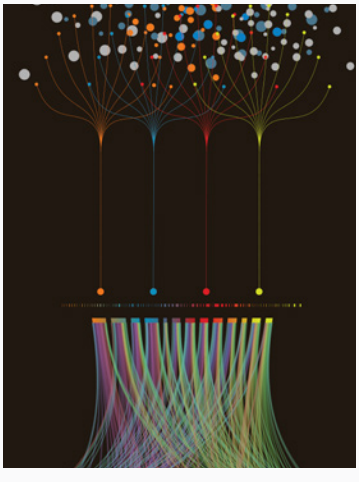
How to deal with networking IoT devices 3

IoT needs to be secured by the network 6

10 tips to minimize IoT security vulnerabilities 8

What is the Industrial IoT? [And why the stakes are so high] 9

Internet of things definitions: A handy guide to essential IoT terms 12



GETTY IMAGES

How to deal with networking IoT devices

The internet of things has such a **wide range of use cases and individual devices** that network architects have to pay attention to a wide combination of variables for **communication, power, bandwidth, reliability, cost and more.** BY LEE DOYLE

NETWORKING IOT DEVICES CAN BE challenging for IT managers because the communications requirements can be very different from those for typical PCs, tablets and smartphones currently connected to corporate networks.

In addition, there is an incredible diversity of IoT devices and how they are used. For example:

- A police car is now an IT-intensive mobile office. It has multiple IT systems (PCs, local tracking, cameras, sensors), which need bi-directional high speed, secure and reliable connectivity.
- Manufacturing sites rely on a wide range of sensors and video cameras to monitor the manufacturing processes and ensure safe, continuous operations. These sensors are often in hard-to-reach locations and require reliable, secure communications.
- Deployment of surveillance cameras in public settings is now widespread due to security concerns. These cameras need high-speed, reliable communications to relay video (largely upstream) to a central location.
- Many hospitals rely on connected medical devices to track their location and rapidly find the nearest device. This use case calls for low-speed reliable connections for a wide range of devices.

Varying IoT connectivity requirements

In addition to the range of IoT use cases, there are literally hundreds of different types of IoT devices and sensors. Each has its unique requirements including the number of connections, the cost per connection, power availability and the amount of data transfer required, both upstream and downstream.

Depending on application, networks of IoT devices will require scalable, reliable, secure connectivity for remote devices and sensors. Perhaps the biggest challenge is providing low-cost connections to remote devices – some of which will use batteries and have no AC power supply.

IoT network requirements

Depending on the specific devices and applications involved, an IoT network may require:

- The ability to connect large numbers of heterogeneous IoT elements

THINKSTOCK

- High reliability
- Real-time awareness with low latency
- The ability to secure all traffic flows
- Programmability for application customization
- Traffic monitoring and management at the device level
- Low-cost connectivity for large number of devices/sensors

This list of requirements is challenging and may require IT managers to implement multiple network connections depending on the IoT application.

Impact of SDN and NFV on IoT network design

The advent of software-based networking technologies, such as SDN, NFV and SD-WAN, give network architects new tools to design flexible networks. NFV and SDN provide technology to customize the network to IoT requirements. NFV offers many virtual network functions (VNFs), including routing, security, gateways and traffic management that can be combined to deliver the customized network services required by IoT. SDN delivers the centralized, managed capabilities to orchestrate and manage the data flows on highly distributed IoT networks.

The big-data challenge

Networks of IoT devices can create a tremendous amount of data – some of which needs to be analyzed in near-real-time. Due to latency and bandwidth limitations, not all data analysis can or should occur in a centralized location. IoT networks will need distributed analytics and business intelligence, often at or near the edge of the network.

Design considerations for IoT networks

There are a number of factors IT managers should consider when planning for IoT networks. The first level of questions is: What type of device or sensor will be connected? How many devices are there? What is the expected amount of traffic?

> The advent of software-based networking technologies, such as **SDN, NFV** and **SD-WAN**, give network architects new tools to design flexible networks.

The answers to these questions will drive the connectivity options along with overall network budgets for CAPEX and OPEX.

Other key questions include:

- Is the device/sensor fixed or mobile?
- What is the level of security required at the device level?
- Does the IoT data need to be analyzed in real time?
- Do the network and IT system need to control activity at the device or is it mainly passive?
- Does the device or sensor have access to AC power?

IoT connectivity technologies

IT managers have a wide range of options to connect IoT devices and sensors. Each option has specific advantages and disadvantages, depending on application.

Four networking technologies that have widespread commercial adoption today are candidates for IoT networks:

- Bluetooth provides built-in wireless communications for many devices such as smartphones but has a limited range and reliability challenges.
- Wi-Fi is universally available for PCs, phones and tablets but requires a lot of power for ongoing connectivity.
- 4G LTE is pervasive and fast but can be expensive for high data use and power hungry.
- Ethernet enables high-speed LAN connections in almost all campus and branch locations but requires a physical cable to connect to IoT devices.

In addition, the communications industry has invented a number of new networking technologies designed specifically for connecting IoT devices. These include:

- IoT cellular, for which there are several standards such as LTE-M, NB LTE-M, and NB-IOT.
- Low-power wide area networks, such as SigFox and LoRa, which are built specifically to address the requirements of low power (battery only) IoT devices.
- ZigBee is a wireless standard

designed to connect machine-to-machine networks at low cost and low power requirements.

Impact of IoT on campus and branch networks

A significant consideration for many IT organizations is the impact of new IoT networks on existing campus, branch and wide area networks. IoT devices can create new traffic patterns, have large data flows and unique latency requirements.

BRANCH NETWORK

The branch network typically has a moderate number of devices connected via Ethernet and Wi-Fi. Most branch locations do not have trained IT personnel and must be administered remotely. IT organizations are migrating to SD-WAN and SD-Branch technologies to cost effectively meet the increasing need for WAN bandwidth and to simplify remote network installation and administration. Connection of IoT devices at branch locations can mean new network technology to manage, challenges for remote troubleshooting, device-management issues and requirements for increased WAN bandwidth. Certain types of IoT applications may require significant local compute/storage capacity.

Networks of IoT devices can create a tremendous amount of data - some of which needs to be analyzed in near-real-time.

CAMPUS NETWORK

The campus network can have large numbers of devices (PCs, tablets, smartphones, printers, etc.) connected via Wi-Fi and Ethernet with a high-capacity Ethernet backbone for high-speed connections to the organization's data center. The campus network typically has trained IT personnel on-site to address networking issues – slow downs, interruptions in service, etc. For the campus network, IoT implementations can mean new networks to link remote sensors, vast increases in the number of connected devices, challenges for device management and authentication, and congestion on the existing Wi-Fi network.

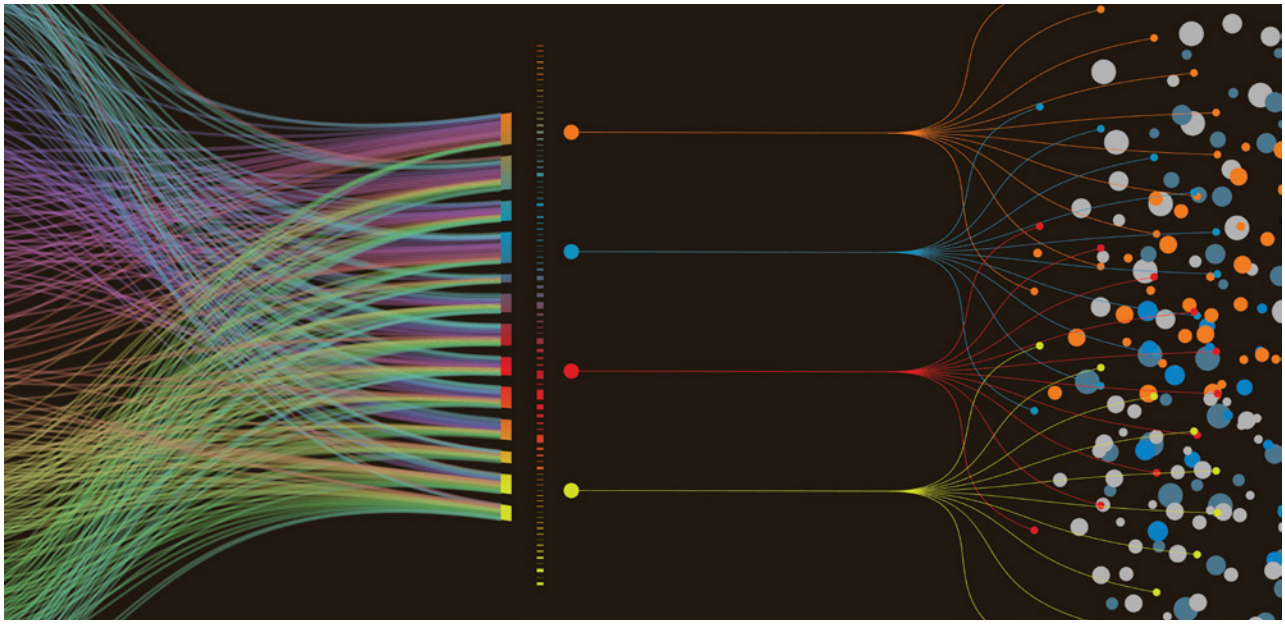
The IT intelligence enabled by connecting IoT devices and sensors is enabling organizations to provide better customer service, deliver goods faster and to reduce costs via more efficient operations. The network, both local and wide area, is a critical element in the implementation of secure, reliable and responsive IoT systems. The unique requirements of individual types of IoT systems require new forms of network connectivity and impact the existing branch and campus networks. Many IT organizations have found it challenging to implement IoT platforms that meet the requirements of high reliability, low latency, security and centralized control.

To comment on this story, visit Network World's Facebook page.

Architecting for IoT connectivity requires IT organizations to sift through a wide number of networking options.

Architecting for IoT connectivity requires IT organizations to sift through a wide number of networking options. IT leaders must carefully evaluate their current IoT networking requirements in terms of bandwidth (upstream and down), reliability, security and budget (costs). IoT networking requirements and the technology to connect to devices and things will continue to evolve. Networking architectures should be designed with flexibility and adaptability to meet changing business requirements.

Lee Doyle is Principal Analyst at Doyle Research, with more than 25 years' experience analyzing the IT, network and telecom markets.)



IoT needs to be secured by the network

Economics don't allow all internet of things devices to have baked-in security, so it has to be addressed elsewhere. BY JON GOLD

EVERYONE WHO HAS A STAKE in the internet of things, from device manufacturers to network service providers to implementers to customers themselves, makes important contributions to the security or lack thereof in enterprise IoT.

"The key to all [IoT devices] is that they are networked," Jamison Utter, senior business development manager at Palo Alto Networks told a group at the Security of Things World conference. "It's not just a single thing sitting on the counter like my toaster. It participates with the network because it provides value back to business."

"I think the media focuses a lot on consumer, because people reading their articles and watching the news ... think about it, but they're not thinking about the impact of the factory that built that consumer device, that has 10,000 or 20,000 robots and sensors that are all IoT and made this happen."

The fact that IoT has security issues is well-known. Utter likens it to the case of Windows 95, which suffered from infamous security problems in large part because it

> **It's not just a single thing sitting on the counter like my toaster.** It participates with the network because it provides value back to business.
>
> **JAMISON UTTER,**
> SENIOR BUSINESS DEVELOPMENT MANAGER AT PALO ALTO NETWORKS

GETTY IMAGES

wasn't designed from the ground up to be secure.

"What we have is simplistic operating systems, running on simplistic hardware, that were not designed for security – just like Windows 95," he said.

Sharing responsibility for security

IoT security isn't qualitatively different than securing any other broad category of computing device, said Utter, it's just the scale of the device pool and their computing limitations that makes the task challenging.

"Would you accept the same level of security on a car as on a sensor that opens the door? It's just not appropriate, right? The asset is not as valuable. So what we have to accept is that endpoints will have varying levels of security."

At the device, network, data and in the cloud, a patchwork of security implementations will be at play. "That's why we have to design our security as holistically as possible, rather than trying to pass it off and saying, 'You guys take care of it.'"

The network, Utter said, is the key battleground for future IoT security, largely because of economics – some endpoints simply aren't able to be secured sufficiently without an unreasonable investment of money. If shipping crates with highly secure IoT endpoints attached to them cost too much, for example, that throws off a company's entire business model.

"We need to start framing IoT in a slightly different way," he said. "Everyone focuses on the endpoint ... but I believe the network can actually be an enforcement point for IoT, because some devices will never be appropriate to have high-level security, it's just not right in the economic model."

> **"That's why we have to design our security as holistically as possible,** rather than trying to pass it off and saying, 'You guys take care of it.'"
>
> **JAMISON UTTER,**
> SENIOR BUSINESS DEVELOPMENT MANAGER AT PALO ALTO NETWORKS

Major mobile data carriers, Utter argued, have a substantive part to play in keeping IoT secure. Given that an increasing number of IoT devices use LTE, LoRaWAN and even 3G to connect, the carriers can make a contribution by scrubbing data, blocking malicious devices and other active security measures.

"They need to stop being simply a conduit for information, but also participate and help us be better about how to keep the pipes clean and keep the right things on our networks," he said.

Visibility, analysis, automation, repeatability

According to Utter, there are four pillars of security for IoT. "The first is visibility, which needs to go beyond, "Which devices are on the network?" and delve more deeply into questions like, "What are these devices actually doing?" and "Who is receiving the data they're sending?"

"I can't have blindness to what's happening on my network," he said.

The second is analysis, and since smart companies are already doing this in the name of business value, it shouldn't be a major stretch to extend that analysis to security. Following naturally from that, automation to decrease the human workload of managing IoT networks can be implemented.

Doing all of this in a repeatable way leads to the final pillar, consistency. The major obstacle here is the patchwork of IoT standards in use across the industry and the challenge of getting them all to talk to each other.

"It's my belief that in order to give IoT security the same level of security I give to financial or to your PCI systems or to your ERP, I have to be able to deliver consistently to the networks and endpoints that run inside the IoT network," he said.

Businesses can help secure their own IoT networks in a number of different ways, including vendor selection. By making sure that vendors know security is a priority and doing business with those that take it seriously, companies can contribute to safer IoT, according to Utter.

"Manufacturers have to understand that they have a stake in the security posture," he said. "And the security posture is really the business posture of their companies."

Jon Gold is a Senior Writer for Network World and covers IoT and wireless networking.

10 tips to minimize IoT security vulnerabilities

Here's a handy list of tips that can help you avoid the most common mistakes that business IT pros make when bringing IoT devices onto enterprise networks. **BY JON GOLD**

THE ONLINE TRUST ALLIANCE HAS compiled a list that lays out 10 suggestions for using IoT tech in the enterprise without making the enterprise more vulnerable to security threats. The list centers on awareness and minimizing access to less-secure devices. Having a strong understanding of what devices are actually on the network, what they're allowed to do and how secure they are at the outset is key to a successful IoT security strategy.

Here's the list:

1 Every password on every device should be updated from the default, and any device that has an unchangeable default password shouldn't be used at all. Permissions need to be as minimal as possible to allow devices to function.

2 Do your homework – everything that goes on your network, as well as any associated back-end or cloud services that work with it, needs to be carefully researched before it's put into production.

3 It's a good idea to have a separate network, behind a firewall and under careful monitoring, for IoT devices whenever possible. This helps keep potentially insecure devices away from core networks and resources.

4 Don't use features you don't need. The OTA gives the example of a smart TV used for display only, which means you can definitely deactivate its microphone and even its connectivity.

5 Look for the physical compromise. Anything with a hardware "factory reset" switch, open port or default password is vulnerable.

6 Gizmos that connect automatically to open Wi-Fi networks are a bad idea. Make sure they don't do that.

7 If you can't block all incoming traffic to your IoT devices, make sure that there aren't open software ports that a malefactor could use to control them.

8 Encryption is a great thing. If there's any way you can get your IoT devices to send and receive their data using encryption, do it.

9 Updates are also a great thing. Whether you've got to manually check every month or your devices update on their own, make sure they're getting patches." Don't use equipment that can't get updates.

10 Underlining the above, don't use products that are no longer supported by their manufacturers or that can no longer be secured.

(The Online Trust Alliance was founded as a loosely confederated industry group in 2005, mostly as a response to email-based security threats and spam. The group's aims have evolved substantially since then, to encompass a much wider range of technologies, including IoT. After becoming a recognized 501(c)3 organization in 2012, the OTA was absorbed by the larger Internet Society, and became a subordinate arm of that group as of October 2017.)

> **Every password on every device should be updated from the default,** and any device that has an unchangeable default password shouldn't be used at all.

Jon Gold is a Senior Writer for Network World and covers IoT and wireless networking.

What is the Industrial IoT? [And why the stakes are so high]

The Industrial Internet of Things, or IIoT, **connects machines and devices in industries such as transportation, power generation and healthcare.** The potential is high and so are the risks. **BY JON GOLD**

EVERYONE'S HEARD OF THE IOT – smart thermostats, Internet-connected refrigerators, connected lightbulbs – but there's a subset called industrial IoT that has a much more significant day-to-day impact on businesses, safety and even lives.

The term IIoT refers to the Industrial Internet of Things. In broad strokes, it's the application of instrumentation and connected sensors and other devices to machinery and vehicles in the transport, energy and industrial sectors.

What that means in practice varies widely. One IIoT system could be as simple as a connected rat trap that texts home to say that it's been activated, while another might be as complicated as a fully automated mass production line that tracks maintenance, productivity and even ordering and shipping information across a huge, multi-layered network.

How the industrial internet of things is different from IoT

The industrial internet of things is also referred to as the industrial internet, a term coined by GE, and Internet of Industrial Things. Whatever you call it, the IIoT is different from other IoT applications in that it focuses on connecting machines and devices in industries such as oil-and-gas, power utilities and healthcare.

IoT includes consumer-level devices such as fitness bands or smart appliances and other applications that don't typically create emergency situations if something goes wrong.

Simply stated, there is more at stake with IIoT deployments where system failures and downtime can result in life-threatening or high-risk situations.

The IIoT brings computers from IT to operational technology, opening up vast possibilities for instrumentation, leading to major efficiency and productivity gains for almost any industrial operation.

To comment on this story, visit Network World's Facebook page.

Is IIoT its own category?

Technologically, IIoT works on similar principals to any other piece of IoT tech – automated instrumentation and reporting being applied to stuff that didn't have those capabilities before. That said, the scale of it is much different than a simple system that lets you mess with your thermostat from your phone. Hundreds, perhaps thousands or even tens and hundreds of thousands of individual endpoints can be present in an IIoT deployment."

What are businesses doing with the industrial IoT?

Instrumentation for production lines can let companies track and analyze their processes on an enormously granular level: asset tracking can give a quick, accessible overview of huge amounts of material; predictive maintenance can save

> Whatever you call it, **the IIoT is different from other IoT applications** in that it focuses on connecting machines and devices in industries such as **oil and gas, power utilities and healthcare.**

companies big money by addressing problems before they have a chance to become serious. The number of potential use cases is vast and growing by the day."

The Industrial IoT Consortium lists these 15 possible uses of IIoT:

1. Smart factory warehousing applications
2. Predictive and remote maintenance
3. Freight, goods and transportation monitoring
4. Connected logistics
5. Smart metering and smart grid
6. Smart city applications
7. Smart farming and livestock monitoring
8. Industrial security systems
9. Energy consumption optimization
10. Industrial heating, ventilation and air conditioning
11. Manufacturing equipment monitoring
12. Asset tracking and smart logistics
13. Ozone, gas and temperature monitoring in industrial environments
14. Safety and health (conditions) monitoring of workers
15. Asset performance management

Do you need to implement IIoT differently?

Yes, because IIoT devices can have much longer service lives than consumer gadgetry – Canonical executive vice president of IoT and devices Mike Bell estimates the average at seven to 10 years – so any implementation has to be built to last.

Even beyond the raw scale and longevity involved, the implementation process can be convoluted. The kind of back end necessary to make the most of data gleaned from instrumentation is a considerable undertaking in and of itself, and has to be undertaken in close coordina-

GETTY IMAGES

tion with the rest of the enterprise. It requires a dedicated strategy for collecting data from endpoints, storing it in an accessible format – whether in a data center or in the cloud – feeding it to the analysis engine and having a way to turn insights from that analysis into actionable and timely information.

How does machine-to-machine communication let the IIot talk to everything?

There's a wide range of different formats and technologies that address different parts of the need for machine-to-machine communication among connected devices. Physical layer technology like Sigfox and Zigbee, software layers like Weave and IoTivity — all of it is necessary for a fully functioning IIoT environment, and it all has to be interoperable.

What about IIoTsecurity and other concerns?

Just like consumer IoT, IIoT has a lot of security issues. Recall the Mirai botnet, which leveraged poorly secured security cameras and other gadgets into a huge DDoS weapon.

Beyond the possible use of compromised IIoT devices to create massive botnets, there's also the issue that vulnerabilities can be exploited to allow theft of valuable data already on your network – yet another attack vector.

One thing that might help keep IIoT secure, according to Bell, would be to borrow the increasingly common practice of automatic, silent downloading and patching from the consumer side of IoT. Some companies won't like this, preferring to have absolute control over the software running on their machines, but it could be a big help from a security perspective.

Other factors that IT leaders are concerned about include the following:

■ **Lack of standardization.** As an attempt to graft newer technology onto old, there's a huge range of different designs and standards for everything from transmission protocols to ingestion formats. Simply put, if the gizmo that sends operational information about the temperature of a blast furnace isn't made by the same company that makes the network or the data ingestion engine, they might not work together.

■ **Integration with legacy technology.** Lots of older equipment isn't designed to provide data in a format that's legible for modern IIoT tech, so getting a decades-old power station controller to talk to a sophisticated new IIoT infrastructure could require some translation.

■ **Money.** As both of the above points highlight, fully embracing IIoT requires new hardware, new software and a new way of thinking about technology. The idea is to make money, but plenty of people are understandably worried by the up-front costs.

■ **People.** Getting the most out of IIoT often requires expertise in machine learning, real-time analytics, and data science — to say nothing of cutting-edge knowledge of networking technology.

> Getting the most out of IIoT often requires **expertise in machine learning, real-time analytics, and data science**–to say nothing of cutting-edge knowledge of networking technology.

Jon Gold is a Senior Writer for Network World and covers IoT and wireless networking.

BE SURE NOT TO MISS:

Review: Microsoft Azure IoT Suite
Hot IoT tech trends for 2018
What happens when an IoT implementation goes bad?
IoT expands its strengths

GETTY IMAGES

Internet of things definitions: A handy guide to essential IoT terms

IoT standards, protocols and technologies explained.

BY JON GOLD

There's an often-impenetrable alphabet soup of protocols, standards and technologies around the Internet of Things. Here's our attempt to wipe away some of the fog, in the hopes of making the language of IoT just a little bit clearer.

6LoWPAN – Possibly the most tortured acronym of even this distinguished group, 6LoWPAN is "IPv6 over low-power personal area networks." Sheesh. The idea is to placate people that say it's not really the "Internet" of Things without Internet protocol, so it's essentially the IPv6 version of Zigbee and Z-wave.

AMQP (Advanced Message Queuing Protocol) – AMQP is an open source standard that allows disparate applications to talk to each other across any network and from any device. AMQP is a part of numerous commercial middleware integration offerings, including Microsoft's Windows Azure Service Bus, VMware's RabbitMQ and IBM's

GETTY IMAGES

MQlight. It was initially developed by the financial sector for fast M2M communication but has begun to be used in IoT projects.

Bluetooth of various kinds (Blueteeth?) – There are two main forms of the ubiquitous Bluetooth wireless communication protocol used for IoT. The standard variety is used across great swaths of smart home gizmos, from connected refrigerators to shower speakers to door locks. Bluetooth Low Energy, often referred to simply as BLE, is a little bit more attractive for larger networks of constrained connected devices, since battery life is less of a limiting factor. Both formats got an update in December 2016 with Bluetooth 5, which expands the effective range of Bluetooth devices and boosts potential throughput.

Cellular data – It's not the most power-efficient way to do things, obviously, but there are plenty of IoT deployments out there that use wireless data from the cellular carriers as their transport layer.

CoAP (Constrained Application Protocol) – This is an Internet protocol designed for use with constrained devices, those without a lot of computing power. It's a part of the official Internet Engineering Task Force's standards, and as you'd imagine from the name, it works well with small-scale gizmos like digital signage and smart lighting.

DDS (Data Distribution Service) – It's another middleware standard, like AMQP, this one created by the Object Management Group, a tech industry consortium dating back to 1989 aimed at creating distributed object-management standards. DDS uses a system of "topics" – types of information known by the system, like "boiler temperature" or "conveyor belt speed" – to provide information to other nodes that have "declared" an interest in a given topic, ideally obviating the need for complicated network programming.

HomeKit – HomeKit is Apple's own-brand front-end and control apparatus for smart home devices. It's got the usual Apple issue of only working particularly well when the important parts of the system are all Apple-made, which could prove annoying if you don't already own an Apple TV or iPad, but it's also got the concomitant Apple virtue of being simple to set up and use.

IoTivity – IoTivity is an open-source project that's trying to create a standard software layer for IoT device connectivity, backed by a bunch of the tech world's heavy hitters, including Microsoft, Intel, Qualcomm, LG and Samsung. The project absorbed a group called the AllSeen Alliance, publishers of a rival standard called AllJoyn, in October 2016, and the two systems are mostly interoperable at this point.

JSON-LD (JavaScript Object Notation for Linked Data) – A lightweight outgrowth of the JSON file format intended to provide an easy way to move machine-readable data around a network of devices that might format their information differently.

LoRaWAN – LoRa refers to a proprietary wireless-chip technology designed for use in low-power WAN implementation. LoRaWAN technology is similar to (and competes with) Sigfox, although the LoRa Alliance is a consortium of companies rather than a single corporation.

MQTT (MQ telemetry transport) – MQTT is a publish/subscribe messaging protocol, designed to be used in situations where the devices talking to each other have limited computing power or are connected by unreliable or delay-prone networks. It does what it's supposed to do very well, but it's hamstrung a bit by the fact that implementing tough security controls can be tricky and can undercut the lightweight nature of the protocol.

NFC (Near-field communication) – The lowest of low-power networks has been around for a long time and is unsurprisingly well-suited for use in IoT applications. Anything that can be placed close to what it's supposed to interact with and doesn't need to send or receive a great deal of information is a good fit for NFC.

Physical Web – The Physical Web is a Google-created concept that argues for "quick and seamless interactions with physical objects and locations." It uses a protocol called Eddystone to broadcast links via Bluetooth Low Energy, with the idea being that you can simply walk up to a parking meter and feed it digitally or get information about a store by scanning its kiosk with your phone.

SCADA (Supervisory Control and Data Acquisition) – SCADA has been around since the days of mainframes, and outlines the earliest attempts at systematic computerized control over industrial, manufacturing and heavy transport applica-

tions. Older-generation SCADA networks are frequently highly insecure, having been designed for ease of use, rather than security.

Sigfox – Sigfox is both the shorthand for a proprietary, narrowband, low-power WAN technology and the name of the French company that makes it. The proprietary nature of the technology is unusual (though not unique) for the LPWAN space, but Sigfox's business model is different than most other companies – the idea seems to be to act as a kind of IoT mobile operator, providing on-demand network coverage for anyone who wants to implement IoT.

SMS – Yep, regular old text messages can be a perfectly acceptable communications medium for certain kinds of IoT devices, particularly those that are spread out across a large geographic area and have a certain amount of delay tolerance. Sweden-based pest control company Anticimex, for example, has smart traps that update the company about rodent activity through SMS.

Thread – Thread is a low-power networking protocol incoporating 6LoWPAN that was created by a group led by Google subsidiary Nest Labs, which you'll doubtless remember for its Nest smart thermostat, arguably the first breakthrough smart home device. Since the summer of 2016, an open-source variant of the specification has been available to developers as OpenThread.

TR-069 (Technical Report 069) – This is a Broadband Forum specification document that outlines a protocol called CWMP designed to let users remotely configure and manage customer-premises equipment via an IP network. ("Consumer-premises equipment WAN Management Protocol," for those keeping score at home.) It dates back to the earlier part of the century and was originally designed to help cable network operators manage gizmos like set-top boxes remotely.

Weave – Weave is Google and Nest's software layer for smart homes. It's designed with flexibility and security in mind, even for particularly constrained devices, and it's based on Google's existing Android platform. It's also partially open source – Google has published what it calls "some of the core components" of Weave to GitHub.

Web Thing Model – This is the World Wide Web Consortium's idea for a physical IoT framework, which, unsurprisingly, leverages existing web technology to connect devices, rather than relying on custom, non-web protocols.

XMPP (eXtensible Messaging and Presence Protocol) – A clear case of acronym abuse, XMPP began life as Jabber, an open source standard for chat clients that gained minor notoriety among players of certain online role-playing games. It has since become an IETF standard, with a vast range of extensions and implementations, many of which are aimed at core IoT functionality like discovery and provisioning.

Zigbee – Zigbee is a wireless-mesh networking protocol that boasts the rare combination of good battery life and decent security, thanks to built-in 128-bit encryption. That's partially offset by a low maximum data rate and relatively short range, but there are plenty of constrained device applications for which it's well-suited. It's also an IEEE 802.15.4 standard, which provides a high degree of interoperability.

Z-wave – Like Zigbee, Z-wave is a low-power, short-range wireless network technology primarily used for applications like smart-home devices. It's standardized by the ITU.

Jon Gold is a Senior Writer for Network World and covers IoT and wireless networking.