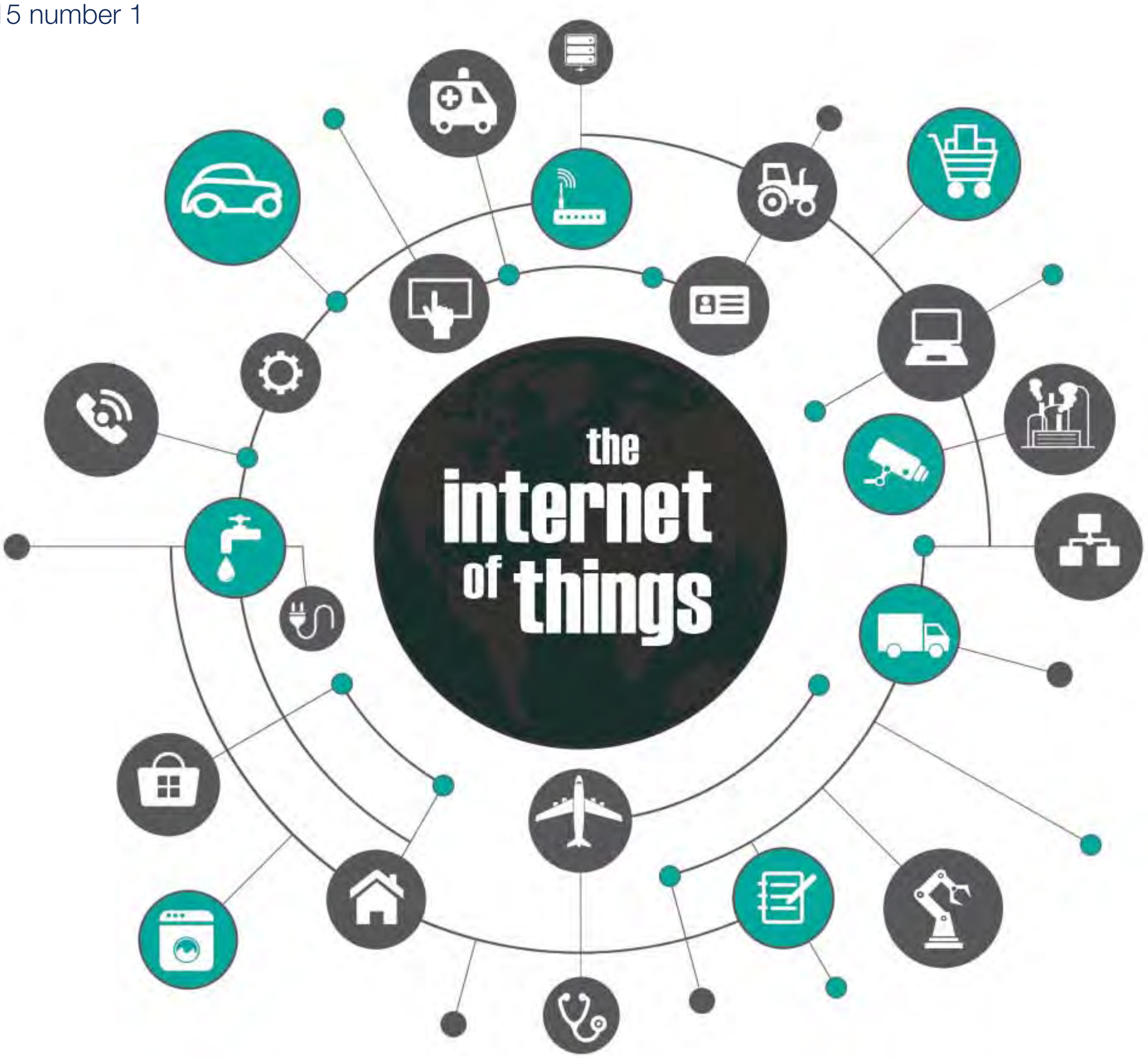
special edition

SIGMA
A PIVOT COMPANY

SigmaUptime

volume 15 number 1



A look at the challenges and opportunities presented by the emerging IoT.

Technology services to help you streamline operations, reduce costs and improve business processes.

Companies today must align IT strategy with their corporate objectives, strategy and business model. Pivot has created a portfolio of operating companies and partners with a focus on helping you enhance and extend the capabilities of your technology assets.

Pivot provides technology services ranging from initial needs assessment and design, through procurement and implementation, to on-going support. As an adjunct to your IT team, we provide the resources that allow your team to offload some of the day-to-day operational challenges and focus on innovations that will drive business value and competitive advantage.

Contact us to learn more.

PIVOT
TECHNOLOGY SERVICES

www.pivotts.com 888-895-0495

Contents

4

Sigma Uptime

Editorial Correspondence:

10221 E. 61st Street
Tulsa, OK 74133

Phone (800) 726-7667 • Fax (918) 270-7134

Change of Address: Send corrected address label to the above address.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission.

Sigma UPTIME is published bimonthly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.

a Smarter World

A look at the challenges and opportunities presented by the emergence of the Internet of Things.

In an interview with *Collier's* magazine 90 years ago, engineer and inventor Nikola Tesla described his vision of a future in which "the whole earth will be converted into a huge brain" by "perfectly applied" wireless technologies that would create a mesh of connections between humans, machines and processes. Furthermore, Tesla said, these connections could be controlled through telephone-like devices so small "a man will be able to carry one in his vest pocket."

That sounds an awful lot like today's Internet of Things (IoT).

In the IoT, all manner of objects can be embedded with sensors that allow them to collect and share data across wired and wireless networks — essentially integrating digital and physical worlds to create the "huge brain" Tesla described in 1926. Leveraging cloud, mobile and big data technologies, organizations can collect, access and analyze data from this fabric to gain insight, resolve problems and create opportunities across a broad spectrum of use cases.

The IoT has been called "the next Industrial Revolution" and "the biggest business opportunity in the history of people." Hyperbole? Perhaps. But the IoT has clearly become a mega technology trend with far-reaching implications for everything from commerce and computing to healthcare and housing.

Industry analysts generate staggering numbers around IoT. Gartner estimates there will be 26 billion connected devices by 2020. Cisco says there will be 50 billion. Intel says it will be 200 billion. IDC says 212 billion. According to Forrester Research, 82 percent of all companies will have implemented some type of IoT application by 2017. Research firm BI Intelligence says the IoT market will surpass the PC, tablet and phone markets — *combined* — by 2017.

Development of the IoT has been spurred by a number of factors, including improvements in wireless networking technology and the development of low-power, small-core microchips that deliver more processing capabilities for smaller devices. However, adoption remains inhibited by factors such as a lack of standards, questions about security and new requirements for network infrastructure. In this issue, we'll look at how Cisco is addressing those challenges with integrated solutions covering everything from the network to the cloud and endpoint devices.

IoT Infrastructure

Fog computing and other Cisco innovations set a foundation for deployment.

Although the Internet of Things is still in its infancy, there is widespread belief it could become the next great engine of economic growth. MachNation, a market research firm focused exclusively on IoT, estimates it will generate $4 trillion in technology and communications spending by 2024.

However, the IoT also creates key challenges at the core technology level. Organizations must address fundamental issues with existing infrastructure, hardware and software in order to fully reap the benefits of IoT.

"For the time being, widespread IoT adoption will be inhibited by factors such as a lack of standards, questions about global scalability and a nascent ecosystem for application development," said Michael Hritz, Business Development Manager, Pivot. "Privacy and security concerns also must be addressed.

"Perhaps the biggest challenge of all will be developing the capabilities for capturing, storing, managing, analyzing and retaining the massive amounts of data that will be generated by all of these connected objects. Think of it as big data on steroids."

Into the Fog

Present-day infrastructure — from the wireless carrier to the data center and all points in between — simply wasn't built to handle the enormous amount of data the IoT will generate. It is generally assumed that the large-scale data collection and analytics required for the IoT will take place in the cloud, but even the cloud model presents some issues.

"Moving data back and forth to cloud-based applications for analysis is generally a very efficient process today, but the game changes when you start talking about having millions and billions of connected devices," said Hritz. "The vast numbers of transactions taking place in the IoT make this model of distributed processing expensive, and the latency involved will be a problem for time-sensitive applications such as healthcare monitoring devices."

The solution may lie in a new cloud-like model for distributed computing in which data processing and analysis take place closer to data sources. Extending the cloud metaphor, Cisco calls this model "fog computing" — an approach that brings the cloud closer to the ground. The architecture calls for the use of "fog nodes" such as routers at the network edge to process data, reducing latency by eliminating the need to send raw sensor data back to the cloud for processing.

Supporting the IoT Load

The fog computing model is one of the six technology elements or "pillars" in Cisco's IoT System, a comprehensive set of technologies and products for enterprises to help them accelerate and innovate with the IoT. Much like its Unified Computing System integrates all the components required for data center architecture, Cisco's IoT System combines networking gear, security devices, analytics, application management and more in a cohesive platform.

The six pillars of the Cisco IoT System are:

Network connectivity. This pillar includes purpose-built routing, switching and wireless products available in ruggedized and non-ruggedized form factors.

Fog computing. To equip its routers for edge processing, Cisco has combined its Internetworking Operating System (IOS) with Linux to create its IOx architecture. This allows edge routers to collect data from devices using a wide range of wireless communication protocols including cellular, WLAN, Bluetooth low energy, ZigBee, Z-Wave, NFC, RFID and more.

Security. This pillar includes cloud-based threat protection, operations-specific security appliances, network and perimeter security, data security, user- and group-based identity services, video analytics, and secure physical access.

Data analytics. IoT-specific APIs allow analytics to run directly on fog nodes for real-time data collection and analysis. Also included are the tools necessary to integrate IoT analytics with other business analytics programs.

Management and automation. Cisco IoT Field Network Director and Cisco Prime Management Portfolio deliver intuitive management solutions and allow centralized management of device configuration.

Application enablement. This platform provides infrastructure for application hosting and application mobility between cloud, fog and middleware services to support app development and lifecycle management.

"The Internet of Things represents a significant opportunity, but organizations have to understand the demands it will make on their networks," said Hritz. "When you consider the challenges the BYOD trend created, you can imagine what will happen when you increase the number of endpoints coming online by an order of magnitude.

"The six pillars Cisco has established with its IoT System will serve as a strong foundation for companies to build IoT solutions. By integrating key technologies and products, it will simplify and accelerate the deployment of IoT solutions in order to deliver tangible benefits."

Reducing IoT Risk

The network carries more of the security workload in Cisco's approach.

From connected cars and wearable healthcare, to smart homes and more, the Internet of Things (IoT) offers endless possibilities for fascinating and life-changing applications. At the same time, it creates the potential for truly frightening security breaches.

Imagine if someone were able to remotely stop your pacemaker, turn off your home security system or cut the engine of your self-driving vehicle. In fact, researchers recently discovered a flaw in Fiat Chrysler's connectivity software that would allow hackers to take control of some vehicles' engines and brakes from thousands of miles away.

The potential for such malice makes securing all IoT devices, sensors and systems imperative.

"The emerging world of IoT has the potential to be a transformational technology. To reap its many benefits, the world of IoT must be safe, secure and trusted," said Michael Kaiser, executive director of the National Cyber Security Alliance (NCSA). "Individuals and businesses that adopt IoT should be sure they know how to keep the devices secure, understand what data is being collected and where it is being stored, and how to take advantage of any available user controls for the device."

Covering All Bases

One reason security is so challenging is that IoT solutions are highly complex, involving the entire technology stack from hardware to cloud infrastructure and all points in between. Common vulnerabilities in IoT devices include weak passwords, insufficient authorization, lack of transport encryption, insecure web interfaces and inadequate software protection. Because of this, the Open Web Application Security Project (OWASP) recommends a layered security approach that covers devices, cloud infrastructure, mobile applications, network interfaces, software, encryption, authentication, physical security and USB ports.

This is the approach Cisco has taken with the "Security Everywhere" strategy it announced in 2015. Already a leader in network security solutions, Cisco recently expanded its portfolio with a variety of new product launches and strategic acquisitions designed to embed security throughout the extended network.

"Over time, most organizations have developed a rather fragmented organizational and architectural approach to security. It isn't unusual to see a company with a stitched-together framework of products from dozens of different security vendors," said Michael Hrtiz, Business Development Manager, Pivot. "These systems aren't going to hold up under the strain created by the sheer numbers of connected IoT devices. A unified, single-platform approach like

continued on page 8

Continued from page 7

Cisco has developed will improve visibility across the entire network — not just on a piecemeal, device-by-device basis."

A key tenet of Cisco's approach to IoT security is that the network itself should serve as both a powerful security sensor and policy enforcer. By adding more sensors to network devices, tightly integrating established network tools and incorporating them with new solutions, Cisco seeks to make the network itself a security device that both identifies and remediates threats.

Automated Responses

Cisco achieves this through the integration of its existing tools with the recently acquired Lancope StealthWatch. Cisco NetFlow collects and records information about IP traffic flows from all network devices, and Cisco Identity Services Engine (ISE) generates contextual information about those network activities. This information is then shared with StealthWatch, which conducts sophisticated behavioral analysis. Together, these tools help organizations identify behaviors linked to a wide range of attacks, including advanced persistent threats, distributed denial of service attacks and insider threats.

Once threats are identified, the "network as enforcer" strategy imposes security policies, quarantines threats and segments traffic through the integration of NetFlow, ISE, StealthWatch and TrustSec software-defined segmentation. Embedded in Cisco switches, routers, wireless LAN controllers and security devices, TrustSec classifies traffic flows based upon identity information to enforce policy-based rules across the entire network. TrustSec grants the right levels of access to the right users and devices, while preventing the lateral movement of network threats.

"With this approach, your network can detect what was previously undetectable through deep and broad visibility into unknown devices, unusual traffic patterns and unexpected behavior," said Hritz. "But it doesn't stop there. Your network can contain an attack by enforcing segmentation and user access control.

"The threat landscape is constantly evolving, and the Internet of Things multiplies the points of infiltration into the network. Standard security measures involving human intervention to identify and remediate threats can't possibly keep up. By embedding security into the network, Cisco is automating much of that workload to greatly reduce complexity and risk."

Building a Smart City

In a scene from the Rodgers and Hammerstein musical *Oklahoma!,* a cowboy returns home from a trip to the big city flabbergasted by all the modern wonders of the early 1900s, captivating his friends with tales of gas-powered buggies, telephones, indoor plumbing, a seven-story skyscraper and more.

"Everything's up to date in Kansas City," the character sings. "They've gone about as fer as they can go."

Turns out, they're still pushing the limits in Kansas City.

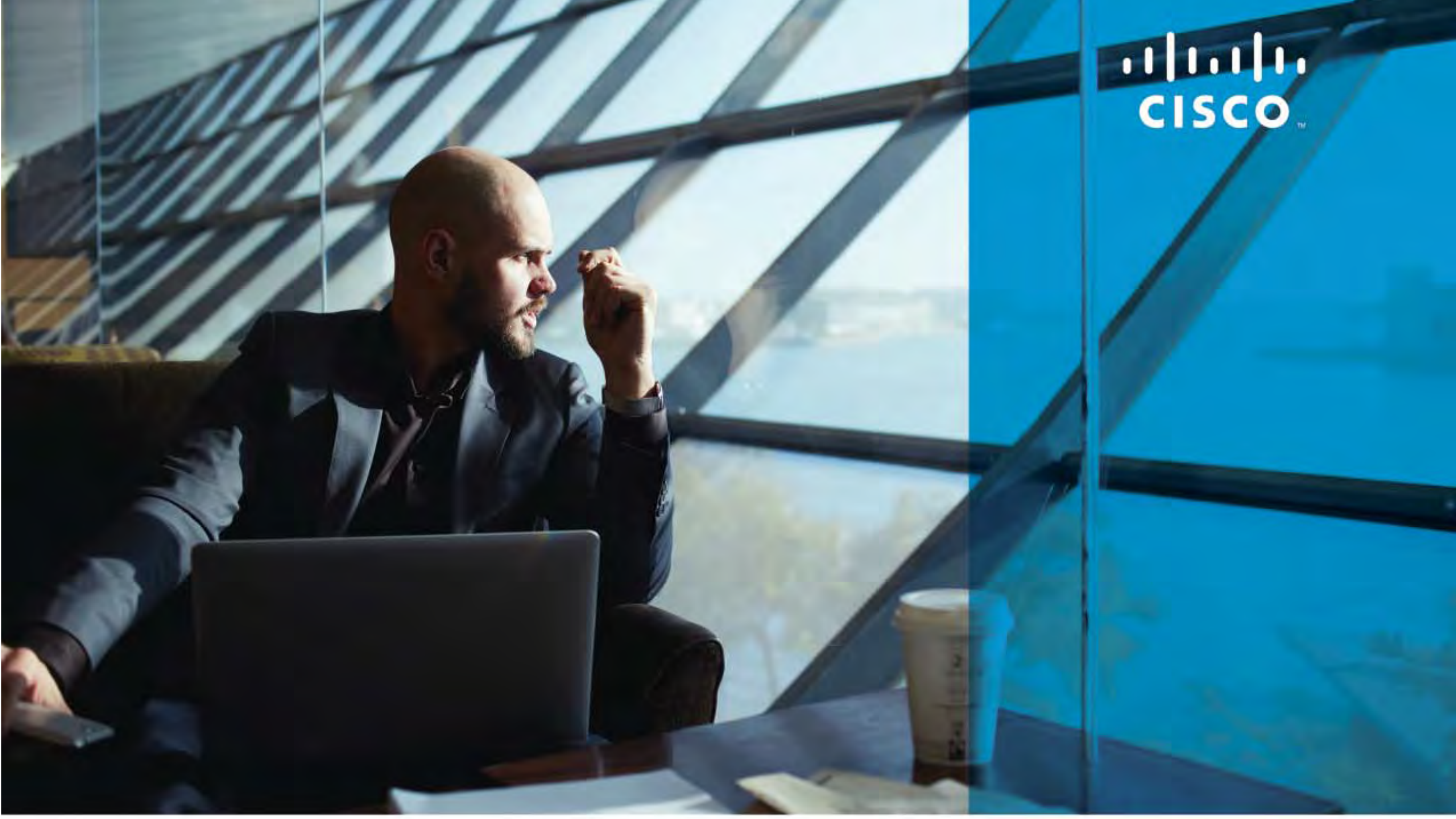
As part of a public-private partnership with Cisco Systems and Sprint, the city is currently involved in the widespread deployment of Internet of Things (IoT) technology that will make it the largest "smart city" in North America. The idea is to create a pervasive digital platform that can aggregate data from various sensors, solutions and applications, conduct advanced data analytics, and then use that information to support a wide spectrum of city services.

The project is an offshoot of Cisco's Smart+Connected Communities portfolio of solutions designed to improve the management of public facilities in urban centers. The initial piece of the Kansas City project is an intelligent Wi-Fi network, funded and managed by Sprint and built along a 2.2-mile corridor established for a new streetcar system that is scheduled to become operational this spring. This will allow the city to provide free public Wi-Fi in the area, but the network will also connect new technologies such as sensors and intelligent data management systems with existing technologies such as smartphones and smart devices.

Sensors along the streetcar route will collect data from the lights, traffic signals, pavement, water pipes and more to help the city improve traffic flow and public safety, and to deliver more efficient city services. They will enable smart lighting through a series of energy-efficient LED streetlights that get brighter or dimmer depending on conditions. Sensors will also feed data to interactive digital kiosks at streetcar stops, providing information about local cultural events, food and entertainment, other businesses, and city services.

Another potential application is the use of sensor information to develop a smart water network that would provide usage information, leak detection, predictive maintenance and more. This and other innovative applications will be developed in the marketplace over time through the city's "Living Lab" partnership with Cisco and Think Big Partners.

The Living Lab is a development data portal that connects entrepreneurs to smart city data for rapid innovation of new applications that can be developed, built, tested and validated in a full-scale, industrial-user environment.



Security matters more than ever. That's why we're putting Security Everywhere.

Traditional approaches to network security were designed for a single purpose: to protect resources inside the network from threats and malware coming from outside the network. Today's businesses must consider smartphones, tablets and consumerization of IT, combined with telecommuters, contractors, partners and business-critical services hosted in the cloud. Security is more important than ever — and far more complex.

Through our Security Everywhere strategy, Cisco is acknowledging this new threat landscape and addressing it in a far more comprehensive and integrated manner than ever before. The value of Cisco architecture is its emphasis on embedding security spanning the extended network — from the data center to the cloud to every endpoint — closing gaps across the attack continuum and significantly reducing time to detection and remediation.

Contact your Sigma representative for a more in-depth discussion of the product, solution and services enhancements comprising a Security Everywhere approach, and how they can enhance your protection against a growing array of security threats.

www.sigmasol.com
888.895.0495

SIGMA
A PIVOT COMPANY

Prescription for Success

Cisco portfolio enables medical-grade infrastructure for IoT.

Glucose-sensing contact lenses allow diabetics to monitor blood-sugar levels without painful finger pricks. Prescription bottles automatically trigger refill orders when they become empty. Refrigerators monitor contents and generate reports on the health impact of eating habits. Smart toilets analyze samples to measure everything from vitamin deficiencies to hormone levels. Smart pills transmit a wide range of physiological information after being swallowed.

Such items would have seemed like science fiction even a few months ago, but they are now very close to reaching the marketplace through the rapid emergence of Internet of Things technologies. While the IoT is sparking innovation in many markets, no industry is being impacted more than healthcare.

Healthcare has always been a data-driven industry, with patient outcomes, operational efficiency and financial performance dependent upon quality information getting to the right person at the right time in the right place. IoT creates the opportunity to reshape healthcare by delivering a connected architecture that can seamlessly communicate among distributed data sources and provide real-time information when required.

Many Benefits

From a clinical perspective, patient data collected and analyzed in IoT systems can be used to improve patient outcomes, manage chronic diseases, enable home care, improve quality of life and avoid preventable deaths. Additionally, IoT data can drive big operational improvements in building maintenance, staffing allocation, inventory management, supply chain processes, equipment maintenance and more.

A recent investment research report from Goldman Sachs finds that the U.S. currently spends more than $3 trillion on healthcare each year — nearly 20 percent of the country's total GNP. The report, titled "The Digital Revolution Comes to US Healthcare," estimates IoT will become a $32.4 billion market in the near term, and will deliver savings of up to $305 billion.

"Availability of information is one of the major challenges in healthcare because of a fragmented infrastructure in which data is scattered across several repositories," said Frank Hughes, Healthcare Practice Manager, Sigma Solutions. "The

IoT creates an opportunity to consolidate data in ways that dramatically improve both clinical and operational efficiency.

“However, for healthcare organizations to truly realize the benefits of IoT, they must have a network infrastructure with the capacity to gather and analyze this data in ways that produce meaningful results. Cisco has been a leader in developing both IoT technologies and a healthcare-specific framework that meets the industry’s unique requirements.”

Putting it All Together

Cisco has developed an ecosystem of solutions designed to facilitate healthcare organizations’ move to the IoT. Combining cloud, mobility, analytics and security solutions with its Connected Health portfolio and its Medical-Grade Network (MGN), Cisco has crafted a network of interoperable technologies that meet the healthcare community’s compliance, security, bandwidth and interoperability requirements.

The Medical-Grade Network is built upon a set of Cisco-recommended guidelines for building an optimal healthcare network. It is an intelligent network architecture that uses application awareness, incorporates application-specific security, and employs network segmentation and quality of service (QoS). The MGN was designed to enable quick and easy integration of key medical applications that make up the Connected Health portfolio. These include telehealth, video and web-conferencing applications that enable long-distance patient care, collaboration and training solutions, electronic health records, image archiving solutions, and more.

The MGN also supports Context-Aware Healthcare, Cisco’s wireless solution for keeping track of mobile assets and patients and improving the process of providing care with mobile resources. Adding the Cisco Wireless Location Appliance to a Cisco Unified Wireless Network gives organizations the ability to locate any Wi-Fi devices on the premises. This includes not only existing wireless devices on the network such as laptops or phones, but also anything that’s been fitted with a Wi-Fi tag.

This application allows a facility to instantly locate mobile assets such as wheelchairs or infusion pumps, track medical staff to help identify bottlenecks and adapt workflow for more efficient use of resources, and ensure that certain at-risk patients remain in designated areas of the hospital. Additionally, Wi-Fi tags with sensor capabilities can transmit information about temperature, pressure and humidity to monitor environment conditions in specific locations.

“The Internet of Things has the potential to transform healthcare from a reactive discipline to a proactive field where the focus is on prevention rather than treatment,” said Hughes. “However, it demands an intelligent network — a secure, application-centric platform that connects people, processes, data and things in ways that weren’t possible before. With its portfolio of solutions, Cisco is delivering the infrastructure necessary to make those connections today.”

IoT Applications

SMART CITIES

- Monitors that sense both vehicle and pedestrian movement to optimize traffic signals.
- Automated street lights that adjust lighting levels based upon motion, traffic, weather and other factors.
- Embedded roadway sensors that prompt warning messages and diversions according to road conditions and unexpected events such as accidents or traffic jams.
- Water monitoring to measure the quality of tap water and detect leakages or pollutants.
- Electric grid sensors that monitor and manage energy consumption.

INDUSTRIAL

- Sensors to monitor heavy equipment and automatically diagnose mechanical problems.
- Sensors that measure levels of toxic gas and oxygen inside factories to ensure safety.
- Auto-adjusting temperature controls for facilities with sensitive equipment and products.
- Asset-tracking tags for inventory control.
- Access-control sensors to improve physical security

RETAIL

- Sensors for tracking materials throughout the supply chain.
- Shelf-based monitors that automate inventory and restocking processes.
- Intelligent vending machines, kiosks and digital signage that create highly targeted ads and offers.
- Tags and scanners that streamline checkout and payment processing.

AGRICULTURAL

- Sensors to monitor activity levels of cows, giving ranchers insights that can boost milk production, smooth the calving process and ensure healthier cows.
- Tracking devices to locate and identify animals grazing in open pastures.
- Sensors that track soil conditions to help improve crop yields.
- Devices that measure the humidity and temperature levels in alfalfa, hay, straw and other feed supplies to prevent fungus and other microbial contaminants.

SMART HOMES

- Sensors that measure energy and water consumption to provide insights on how to save on costs and resources.
- Remote-control appliances that can be switched on and off from a smartphone application to avoid accidents and save energy.
- Intrusion-detection systems that can be monitored from mobile devices to improve security and earn insurance discounts.