# WHAT IS THE ROLE OF CONNECTED HOME GATEWAYS AND SET-TOPS IN THE IOT?

A TECHNICAL PAPER PREPARED FOR THE
SOCIETY OF CABLE TELECOMMUNICATIONS ENGINEERS

MARK BUGAJSKI- ARRIS

# TABLE OF CONTENTS

# INTRODUCTION

The Internet of Things (IoT) is about creating ecosystems consisting of smart, "enchanted objects" connected to the cloud, where they interact with service intelligence in data centers.

IoT devices connect to the cloud using Internet Protocols over mobile networks, in-home wireless or physical wires via home gateways. The information from the gadgets can be processed locally or in the cloud. The result is translated into actionable information or real activities back in the location where IoT devices reside. IoT promises to improve our productivity, enhance what surrounds us and positively impact almost everything that we do.

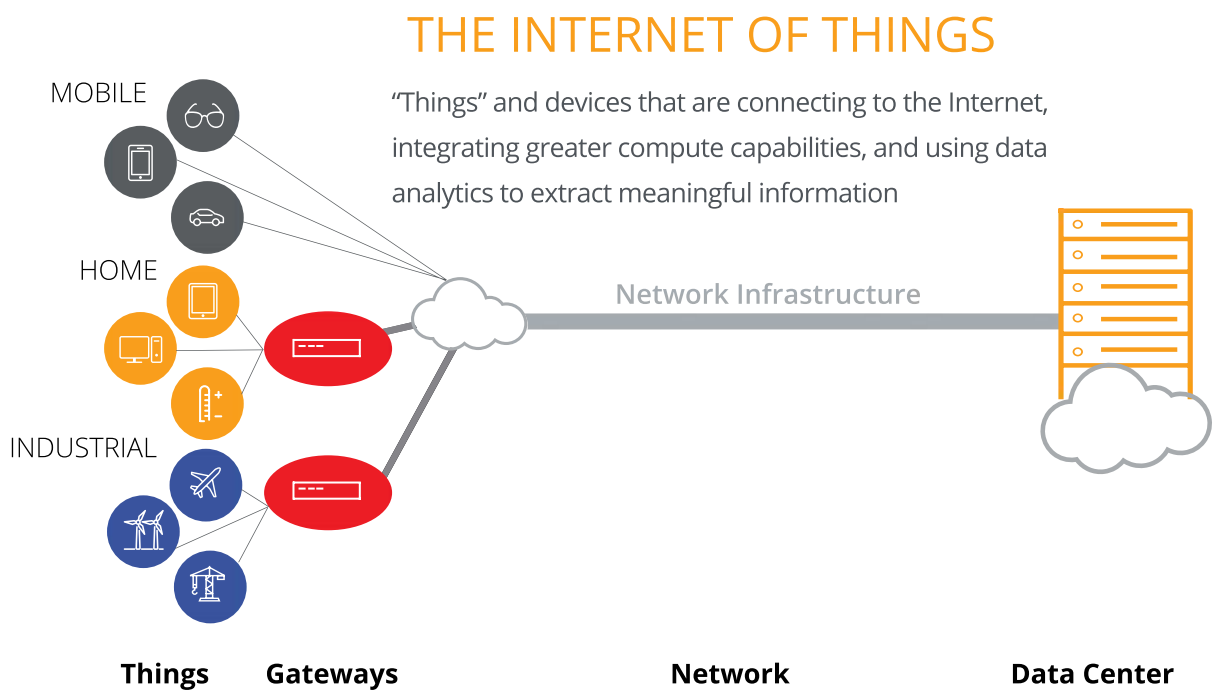


**Figure 1 - IoT**

Based on earlier studies, NCTA estimates that by the year 2020, there will be more than 50 billion IoT devices in use worldwide. [NCTA] These devices will range from simple - one or two function sensors - to quite complex automation subsystems. 50 billion devices means that there will be almost seven times as many IoT devices as there will be people on the planet - an estimated 7.7 billion in 2020.

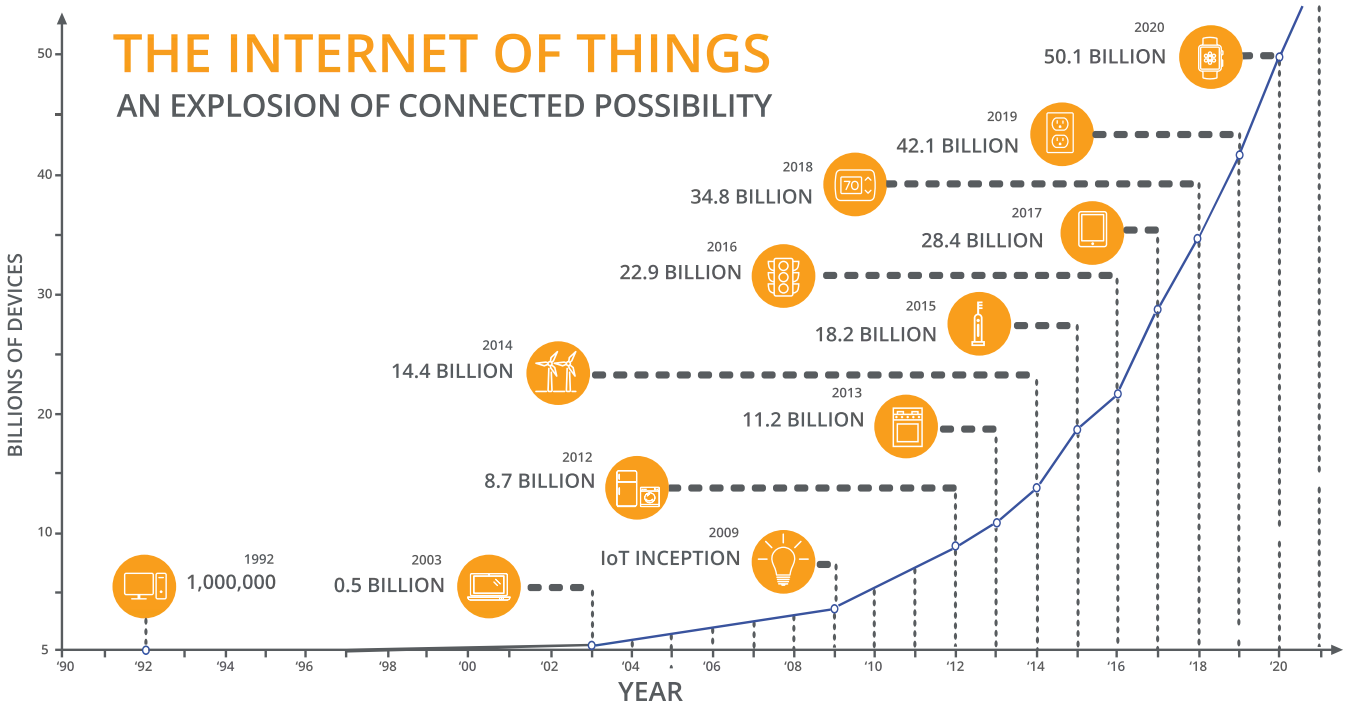


Figure 2 - Growth of 'IoT' Devices

In regards to overall IoT spectrum of devices and services, the connected home represents 27% of the overall opportunity. Of the connected home, energy management and home automation/security accounted for 72% of the device shipments, according to data from 2014.

Personal devices, wearables, industrial and machine-to-machine (M2M) as well as smart cars, cities and other IoT opportunities represent the 73% growth opportunity.

BI Intelligence [BI] forecasts that connected home revenues will grow at 52% compound annual growth rate (CAGR) to $500 billion between the years 2014 and 2020. The volume of shipments will grow from 142 million in 2014 to 1.8 billion in 2020.

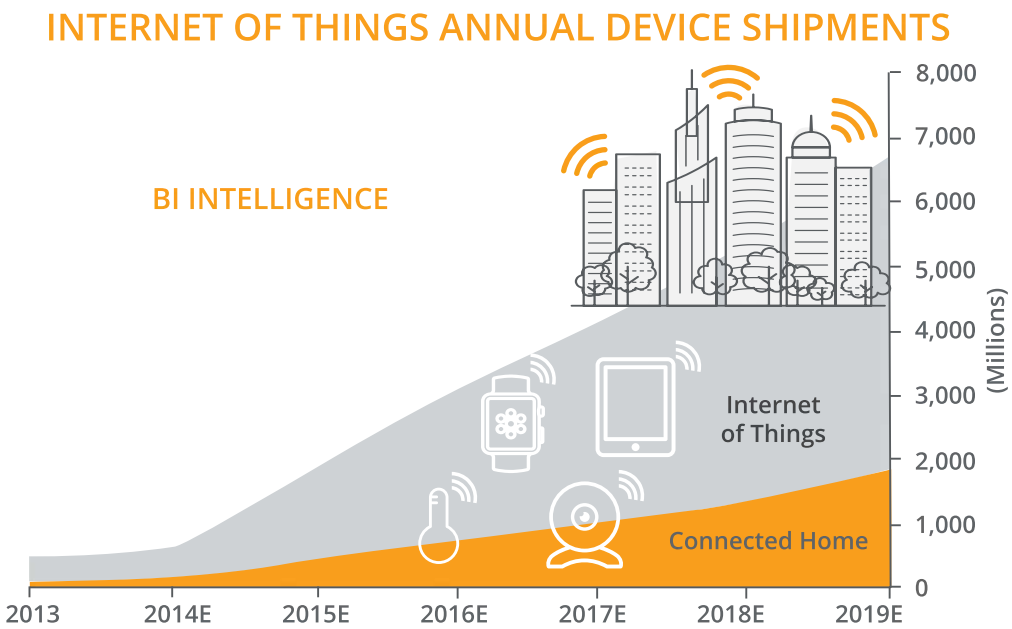


Figure 3 - IoT Annual Shipments

Why is IoT important to Multiple System Operators (MSOs)? Because billions of connected devices will connect to the gateways inside their subscribers' home networks and to the cloud through the broadband access pipes owned and operated by the MSOs. Today, many of the devices that fall into the IoT category already operate on the MSOs' networks and are already causing the number of subscriber complaint calls to increase, in particular for wireless devices. An exponential growth of wireless devices, all occupying the unlicensed Wi-Fi™ spectrum, will result in even more 2.4 GHz and 5 GHz RF spectrum congestion. If left unmanaged, it will interfere with MSO owned devices and degrade adjacent home Wi-Fi networks in high-density residential areas.

# THE ROLE OF HOME GATEWAYS IN THE IOT

## Reliability and cost benefits from using MSO gateways as IoT service hubs

In most recent surveys, consumers who were asked about their concerns related to emerging IoT services, revealed three key areas that need to be addressed to accelerate adoption of these

services. As depicted in Figure 4, consumers identified cost, complexity and the lack of security of these systems as the top barriers to adoption of IoT.

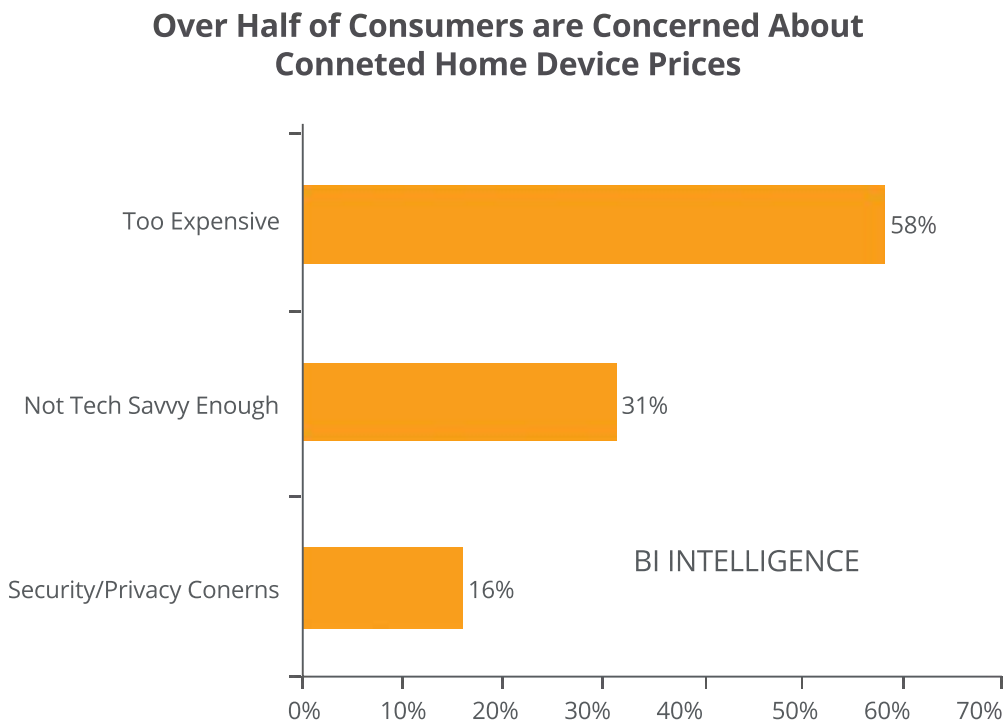


Figure 4 - Barriers to Scaling of IoT Services

Security and privacy concerns are steadily increasing as a result of frequent news reports of malicious hacking into home devices, poor security of cheap devices and identity and financial information theft. What can MSOs do to allay these concerns while opening up opportunities to monetize along the way?

On the high cost side of the 'IoT adoption challenge', the functionality of the wireless hub can be easily integrated into the home gateway, in addition to the Wi-Fi and Ethernet connections, in a form of (802.15.4) Zigbee and Bluetooth interfaces. The Bluetooth communication to/from IoT devices can also be delegated/extended to the set-top box devices that are distributed throughout the home to improve reach to IoT devices. The electronic components needed to implement this functionality are already on the very high volume curve of usage in consumer electronics (CE) and mobile devices.

The addition and implementation of emerging IoT communication standards into the gateway and set-top software stacks will ensure cross-vendor device compatibility, and encourage healthy competition that will drive costs down.

MSOs can reduce the initial cost burden (sticker shock) to the subscriber by leasing the IoT equipment on a monthly fee basis, especially for home security and people-monitoring applications. They can also integrate services from the "application roulette" into one package and bundle service fees together with the broadband and multimedia offerings.

When it comes to dealing with lack of technical competencies required to install the devices and setup the applications, MSOs have a much greater opportunity to make a difference – particularly for the older generations of our society. The key for MSOs is to simplify IoT for the masses. A major step in this direction lies in turning the MSOs' set-tops, which are connected to the TV screens into interactive, intuitive, and user-friendly IoT services portals.

On the connection security and data privacy of IoT services side of the discussion, the franchised local MSOs have historically had outstanding reputations when it comes to preventing theft of programming and breaches on their networks. The connections from the MSOs' cloud to the in-home gateway is very secure and features built-in quality of service (QoS) mechanisms that ensure that "life-line" IoT service packets are never dropped or lost even in the most congested times of the day or week. MSOs can put IoT services at the same priority level as their life-line telephone services offered to residential and business subscribers.

Since the connection between modern MSOs' set-tops and the cloud use the same DOCSIS infrastructure and home gateway, as well as protocols like baseline privacy interface (BPI), it's next to impossible to breach. Both the set-top and gateway connections are also much more reliable than any other consumer Wi-Fi device. The health of both the gateway and the set-top is constantly monitored and managed via TR-69/181 IEEE interfaces and other standardized means such as Simple Network Management Protocol (SNMP).

The variety of set-tops within one service area is limited, and as such, can be easily managed via portals to future IoT services. In contrast, there are thousands of types of CE tablets, PCs and mobile devices with unique  limitations and reliability issues that may increase the complexity of the overall IoT service issues.

Monitoring and troubleshooting of the gateway (which can also host the IoT hub functionality) and set-top is not performed over the same connection as CE devices. Therefore, issues with CE devices are very unlikely to impact the performance of either the gateway or the set-top box.

# IoT CHALLENGES FOR THE CONSUMERS AND HOW THEY CREATE OPPORTUNITIES FOR MSOs

## Installation of IoT devices and interaction with services

Today, the IoT retail CE industry creates verticals of individual services. The device manufacturers want to own the service and "ride" the MSOs' service networks in a totally Over-the-Top (OTT) style. Devices of similar functionality are not compatible or interchangeable with devices from other manufacturers. Most devices come with their own rather pricey hub and companion mobile app.

Additionally, these vertical services are not integrated with each other, creating "IoT application roulette" as depicted in Figure 5.

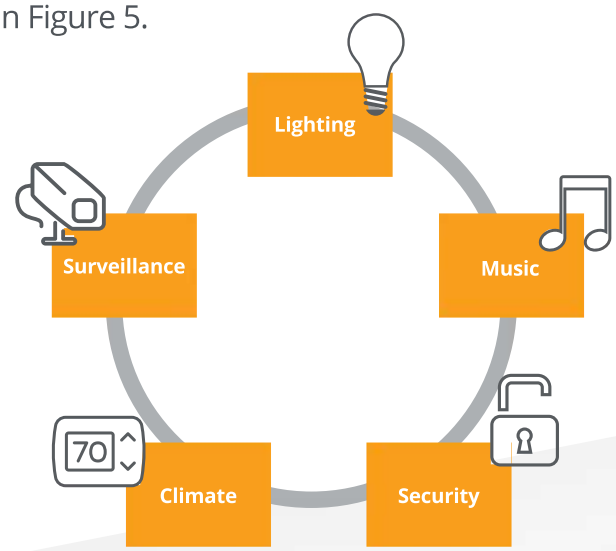


Figure 5 - IoT Services Application Roulette

Today, most retail home automation and security devices come with their own service apps that are often challenging to learn and remember how to operate. Each has its own user interface (UI) and cloud-based service intelligence that does not communicate with other devices or services. Inside this home automation space, the lighting, energy and monitoring devices often come with their own hubs and apps. If bought at different times, these services may be impossible to integrate and operate in full unison.

Home entertainment is currently not integrated with IoT services. Therefore, it is next to impossible to have it complement home automation to augment music or video applications. This creates an environment in which subscribers have to host multiple apps for IoT sub-services, learn and remember their unique navigation schemas, and use them for independent operations. The complexities and costs of separate hubs, devices and service fees may add-up rather quickly.

The opportunity for MSOs in this area lies in converging multiple mobile apps into a single application. The apps will need to be simple and intuitive, and "listen to" and control most of the retail devices, while maintaining compliance with the IoT communication standards. MSOs can create web apps for their set-tops that can be rendered on the TV screen by the built-in browser.

## The "greying" of the population will force simplification of IoT services

According to estimates from the US Census Bureau, by the year 2040, the segment of Americans older than 65 years will increase by 80% and the segment over 85 years will increase by almost 50%. In that same timeframe, the US total population will rise only 25% as illustrated in Figure 6.

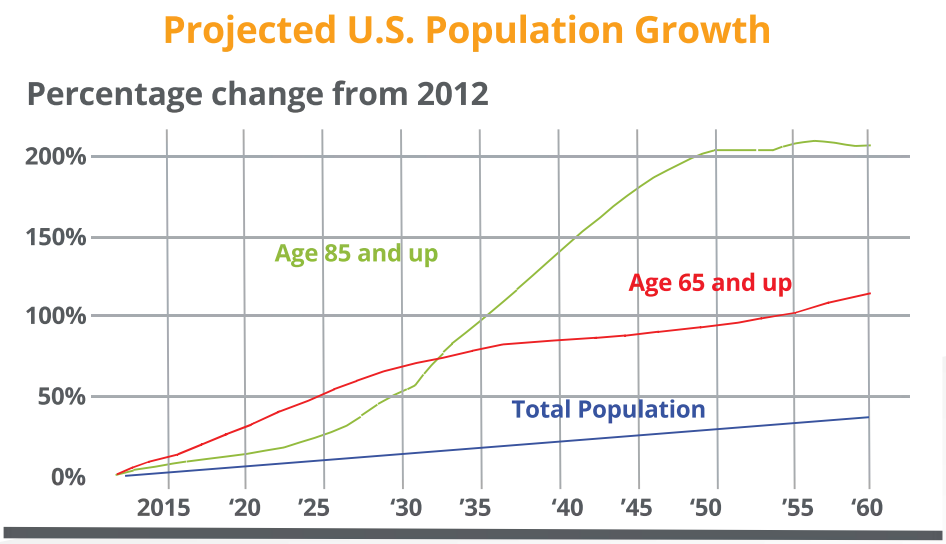


Figure 6 - Aging of US Population

As we age, our tolerance of complex and new technology diminishes. We tend to spend more time in front of the TV rather than interacting with mobile devices or PCs. The role of the set-top as a portal to the external world is likely to increase in this rapidly growing segment of the population. Therefore, it is important that the user experience (UX) in front of the TV be tailored towards the skills of the individual subscriber. UI personalization will be the key feature that allows subscribers to interact with their home entertainment system via their navigation and set-top interactivity.

Family Caregiver Alliance's [CAREGIVER] data estimates that 30% of US households have someone in the family who is either care-giving or care-receiving. The emerging IoT aims to automate and simplify how we monitor someone's vital signs, enforce patient compliance with medical self-testing, and ensure that the patients are taking prescribed medications on schedule.

Industry experts have already coined the term "Internet of Healthy Things" (IoHT) to better describe connected devices that, for example, monitor blood glucose levels, blood pressure and heart rates. New devices work as connected stethoscopes, as scales to measure weight and to collect data from wearables.

According to predictions by Infonetics [INFON], the Connected Health Market is expected to grow from under $1 billion in service revenue today to $2.4 billion in 2018 with a CAGR of 35.5%.


Figure 7 - Internet of Healthy Things

Infonetics [INFON] predicts that the machine-to-machine (M2M) connections for healthcare will continue to be principally be made over licensed spectrum services to the cloud/WAN. Current M2M connections at the device level are over Bluetooth low energy (BTLE) and Wi-Fi. It is predicted that the number of M2M customer side connections will be 211 million by 2018.

The older subscriber will most likely be able to interact with emerging IoT services using the TV screen - an already-familiar device. Therefore the installation of IoHT devices and the turn-up of medicine and care services need to be simple and intuitive. There is no better and larger screen in the household than the TV screen to act as a guide and interactive portal for these services. It is our belief that the aging population will greatly benefit from the use of the TV screen as a portal for virtual visits to doctors, family communication and wellness monitoring services.

To ensure plug and play (PnP) on-boarding of the IoT devices to the services offered by the MSO, partnerships with the IoT device manufacturers will be required. Products will be 'curated' on the factory floor and they'll also provide the needed device information (i.e. Wi-Fi, Zigbee and BT MAC) to the service cloud. This will ensure operational compatibility across multiple devices and integrity of IoT service. Using TV screens to guide subscribers through self-installation and on-boarding will significantly increase service turn-up and increase success rates.

The use of a set-top and the MSO gateway (in contrast with CE devices) will alleviate subscribers' concerns with security and privacy shown in Figure 4. A large segment of subscribers, especially the older generations, are fearful of personal data theft and do not trust Internet-based companies. OTT IoT devices may create an additional fear that someone, via the Internet, is snooping inside their home. These fears are not unfounded, as we have seen cases of connected TVs listening to sounds inside a room and even sending pictures to the Internet from built-in cameras. Almost on a weekly basis, we read news reports about hacker attacks into retail home routers, along with massive identity and financial data thefts. Consequently, subscribers feel more insecure about interacting with the Internet.

In contrast, subscribers generally trust their traditional TV and Internet Service Providers (ISPs). These Service Providers' set-tops have never snooped or stolen information from the home. They do not leak sensitive content to the Internet. Also, there is no built-in camera or microphone that could be the culprit for snooping on cable subscribers. It can be safely assumed that, the gateways and set-tops generate a high level of comfort and security when introducing new IoT services.

A survey of consumers conducted by Vanson Bourne [reference] on behalf of ARRIS shows that TV Service Providers are at the top of the list of companies trusted to supply, setup and manage home automation services.

## Who out of the following would you trust most to supply this sort of remote management or automated home service to you?

Base: asked of respondents that are either interested in, or already have the ability to manage or automate parts of their home remotely (sheet q35)

| | Total | Male | Female |
|---|---|---|---|
| TV service provider | 25% | 25% | 24% |
| Home security company | 21% | 19% | 24% |
| Internet service provider | 18% | 19% | 16% |
| Utilities company | 13% | 14% | 13% |
| Insurance provider | 6% | 6% | 7% |
| Electronics manufacturer (e.g. the manufacturer of your TV or games console) | 4% | 5% | 2% |
| Home improvement store/DIY retailer | 3% | 4% | 3% |
| Healthcare provider | 1% | 1% | 1% |
| Would not trust any of the above to supply a connected home service | 8% | 6% | 10% |
| **Base** | 405 | 220 | 185 |

Base: asked of respondents that are either interested in, or already have the ability to manage or automate parts of their home remotely (sheet q35)

| | Total | 16-24 years old | 25-34 years old | 35-44 years old | 45-54 years old | 55-64 years old | 65 years old and over |
|---|---|---|---|---|---|---|---|
| TV service provider | 25% | 22% | 30% | 30% | 25% | 13% | 21% |
| Home security company | 21% | 18% | 16% | 15% | 25% | 3% | 43% |
| Internet service provider | 18% | 13% | 16% | 15% | 25% | 24% | 21% |
| Utilities company | 13% | 15% | 18% | 18% | 4% | 7% | 7% |
| Insurance provider | 6% | 10% | 8% | 3% | 7% | 4% | 0% |
| Electronics manufacturer (e.g. the manufacturer of your TV or games console) | 4% | 5% | 4% | 7% | 2% | 2% | 0% |
| Home improvement store/DIY retailer | 3% | 3% | 3% | 3% | 4% | 4% | 4% |
| Healthcare provider | 1% | 3% | 1% | 0% | 0% | 0% | 0% |
| Would not trust any of the above to supply a connected home service | 8% | 11% | 3% | 8% | 11% | 13% | 4% |
| **Base** | 405 | 88 | 99 | 87 | 57 | 46 | 28 |

## Rationale for MSOs to use set-tops as IoT portals and gateways as service hubs

The connection between set-tops and an MSO's cloud is extremely secure and content theft on this link is rare. This very connection is also much more reliable than to any other CE device. As mentioned earlier, the link to the set-top is monitored and managed via TR-69 and other standards such as SNMP, with a limited variety for easy management. In contrast, there are thousands of types of CE tablets, PCs and mobile devices with unique limitations and reliability issues.

## The benefits to the subscriber from using set-tops as an IoT services portal

Subscribers are already familiar with set-top remotes (aka. pilots) as a tool to interact with TV-based services. TV screens are getting larger, and are well-suited to display, monitor and manage the ever-increasing number of devices inside the home network that can be leveraged to control IoT services. Navigation inside the IoT applications on the TV screen can be made simple and intuitive. This will be demonstrated in several examples later in this paper. In contrast, when using a mobile app, the subscriber has to find the right device that hosts the desired IoT management app, find and launch the app and recall how to navigate it. This also restricts the subscriber to interacting with only one app at a time.

As mentioned previously, set-tops are perceived as more secure than any CE device. Since the set-top is always authenticated with the MSO's cloud, there is no need to remember credentials and enter them into the device in order to interact with the services. There is also no spyware or phishing software on the gateway or set-top waiting to steal subscriber information. The connection to the MSO's cloud from a home set-top and gateway is already secure, making theft unlikely.

## MSOs' incremental revenue opportunities from IoT

The following tables illustrate a number of opportunities for MSOs to leverage their infrastructure and augment their systems to take a larger share of future IoT service revenues.

| Potential Steps | Benefits |
|---|---|
| Integrate more functionality into gateway, Wi-Fi extenders, and set-tops especially for IoT. Eliminate the need for IoT hubs | Reduce the overall CapEx cost of home security and automation systems to accelerate service adoption |
| Train and use own field installers to roll- out IoT services | Accelerate service adoption and improve subscriber satisfaction |
| Retrain the technician staff to sell connected home devices and upsell additional IoT service features | Teach staff to upsell additional features for higher subscription fees |

| Potential Steps | Benefits |
|---|---|
| Offer gateway functionality to large OTT providers of IoT services (utilities, etc.) | Improve own ROI or decrease the monthly charge to the subscriber to scale |
| Collaborate with device manufacturers to "curate" IoT devices that will support integrated applications | Provide a better, owned brand of connected whole-home offerings to increase the subscription revenue. Gain margin from selling a range of own devices |
| Use standards-compatible software in the gateway self-installation, on-boarding and monitoring of subscriber purchased devices | Integrate subscriber purchased devices with connected whole-home service offerings |
| Develop a range of service tiers that meet a variety of subscribers' budgets | Develop a set of tiered applications that rely on subscriber's own device in the range from $5 to $10 per month<br><br>Upsell the subscriber to richer services in the $20+ monthly fee range |
| Partner with healthcare monitoring companies to host, manage and monitor their services | Share revenue |

In addition to connected home services, MSOs should explore creating their own enhanced services or as a result of partnerships with other companies. Below are some examples:

| Potential Service | Description |
|---|---|
| Medicare and telemedicine services that use gateways and set-tops for communication with medication dispensing and monitoring devices. Using the set-top and TV screens as service portals for notifications | Partnerships with medical insurance companies and government agencies to provide monitoring and future medication administration services |
| Brokerage for services interfaces for utility companies and other Services Providers | Creation of a M2M or B2B2C interfaces where the subscriber can broker their utilities to different providers to get most competitive rates |
| Analytics and telemetry from the home devices and services | Selling telemetry data from the home including to big data companies |
| Use of location and presence detection information to improve effectiveness of targeted advertising | Improve advertising revenue from advertising brokers |
| Accessibility and voice controlled services | A specific market to create a more accessible home environment for the blind with voice controlled services |
| Education services | Leveraging entertainment, connectivity and multiscreen control to drive the creation of a home education service that includes task rewarding |

## Existing and emerging IoT standards

For IoT services to be successful in scaling and gaining rapid consumer acceptance, adoption of standards will be mandatory. This will drive device costs down, guarantee PnP on-boarding of devices to IoT hubs/gateways and the cloud, and ease the seamless integration of current vertical services into a fully integrated, whole-home IoT offering.

| Group | Founded | # of Members | Goal | Founding Members |
|---|---|---|---|---|
| Open Interconnect Consortium | 2014 | 62 | Define and promote open source standards and implementations to improve interoperablility across vertical markets and use cases | Atmel, Broadcom (no longer a member), Dell, Intel, Samsung, Wind River |
| AllSeen Alliance | 2011 | 133 | AllSeen's Alljoyn open source project is a universal framework promoting interoperable products that can connect with all types of devices, systems, and services | Haier, LG Electronics, Panasonic, Qualcomm, Sharp, SIlicon Image, Sony, TP-Link, and others |
| Thread Group | 2014 | 97 | Founded "to create the very best way to connect and control products in the home." | ARM, Freescale Semiconductor, Nest, Samsung, Silicon Labs, and others |
| Industrial Internet Consortium | 2014 | 148 | Founded to "identify the require-ments for open interoperability standards and define common architectures", case studies, and standard requirements | AT&T, Cisco, GE, IBM, Intel |
| IPSO Alliance | 2008 | 44 | This Alliance promotes IP as solution for Smart Objects by documenting the use of IP-based technologies defined at the standard organizations like IETF | Atmel, Cisco, Dust Networks, Emerson Climate Technologies, Freescale Semiconductor, SAP, SensinodeOy, SICS, SIlver Spring Networks, Sun Microsystems, and others |
| Intel IoT Solutions Alliance (formally Intel Intelligent Systems Alliance) | 2011 | 250+ | The Intel IoT Solutions Alliance "seeks to build a strong and sustainable market advantage through "solutions based on Intel architecture. "We work to drive revenue growth and market share for our members." | Intel<br>Premier (non-founding) members: ADLINK, Advantech, Dell OEM, Kontron, Portwell |
| Alliance for Internet of Things Innovation | 2015 | 20+ | Hoping to bring together different industries, sectors, and companies in Europe, the AIOTI builds "on ongoing Commission Initiatives to... foster European IoT Innovation ecosystems." | Bosch, Philips, Sigfox, EU Commission |

Figure 8 - IoT Standards [VDC]

Today, four physical layer (PHY) standards exist, and Google supports a relatively low speed (100 kbps 10 meters) 802.15.4 wireless personal area network (WPAN). Some of these standards are more open than the others, and some have hesitation about sharing intellectual property, which prevents certain silicon vendors from joining the consortia.

All PHYs of these standards share the congested, unlicensed 2.4 GHz band.

Here is an executive level summary of the key standards initiatives:

**OIC:** Intel set up the Open Internet Consortium to help create standards for the IoT

> Initially, the OIC was focused on developing use cases for smart home, office and automotive markets. The organization is membership driven.
>
> Intel is one of the founding members of OIC, opening up the possibility of working with other companies so its chipsets can be used in their IoT devices. OIC works to establish a single solution covering interoperability across multiple vertical markets (CE, enterprise, industrial, automotive, health, wearables, etc.), operations support systems (OSS), platforms, modes of communication, transports and use cases.
>
> Dell, Samsung and others are part of the alliance, which jointly estimates there will be 212 billion connected "things" globally by the end of 2020.

**AllJoyn/AllSeen Alliance:** Qualcomm holds 58% of global wireless baseband revenue in Q2 2014 [QCOM], and it only seems natural for it to parlay its strong wireless chip business in the IoT market.

> In 2013 Qualcomm turned over its AllJoyn protocol to the Linux Foundation and set up the AllSeen Alliance.
>
> The basis of the alliance is that technical companies use the standards Qualcomm created with AllJoyn to allow different companies to connect their IoT devices to one other. "It is not Qualcomm's intent to monetize, through a patent licensing program, our code contributions to the AllJoyn open source platform made in the Alliance."
>
> Qualcomm and its historical aggressiveness about intellectual property rights (IPR) have made it difficult for legal teams of MSOs to accept joining the AllJoyn consortium.

**Thread group:** Established July 2014, it is developing a networking protocol software stack for linking many types of devices in homes, such as lights, security systems, and heating and cooling equipment.

> Thread devices connect through a mesh rather than a single hub in the center of the network, which could offer longer range and greater reliability, as well as avoid a single point of failure.
>
> Thread is meant to augment Wi-Fi supporting 802.15.4, forming a second network for small, power-sipping connected devices instead of laptops and tablets.
>
> Because the Thread stack only tells devices how to talk to one another and doesn't include an application layer, vendors can use different applications and UIs on top of it. Any application layer that uses IPv6, such as ZigBee smart energy and the Internet Engineering Task Force's constrained application protocol (CoAP), can run on top of Thread.
>
> Founding companies include: Yale Security, Silicon Labs, Samsung Electronics, Nest Labs, Freescale® Semiconductor, Big Ass Fans and ARM.

**HomeKit:** Apple's own HomeKit allows developers to control smart home devices like light switches, thermostats and garage doors.

> HomeKit compatible devices have to be a part of the made for iPhone (MFI) program, which requires a specific wireless chipset and Apple's software package to be integrated into the devices.
>
> HomeKit provides a way for every enabled app and accessory to access a single repository of information about a home's smart devices, with permission. This means that any new HomeKit-enabled app can instantly see all of the rooms, devices and homes that have been defined before.
>
> Siri-based voice control is considered a primary system interface of HomeKit, though individual apps may have their individual controls.
>
> Apple is positioning HomeKit as an open system that allows for creation and definition of any device or automation interaction. However, some experts think that HomeKit does not offer a truly open system that allows communication directly with any connected device, regardless of MFI status.

End-to-end encryption is enabled for HomeKit accessories to maintain what Apple calls "complete" privacy and strong security. Other standards advocate less proprietary solutions for addressing these issues. Cloud and device based security is being adopted from other existing standards

For legal reasons, cable companies use CableLabs® to represent them in both OIC and AllJoyn.

It is going to be very important for MSOs to be able to support on-boarding and in-IoT- service participation of devices that are compliant with different standards.

As illustrated in Figure 9, the gateway has to be able to support several on-boarding schemas and communication standards on the home side.

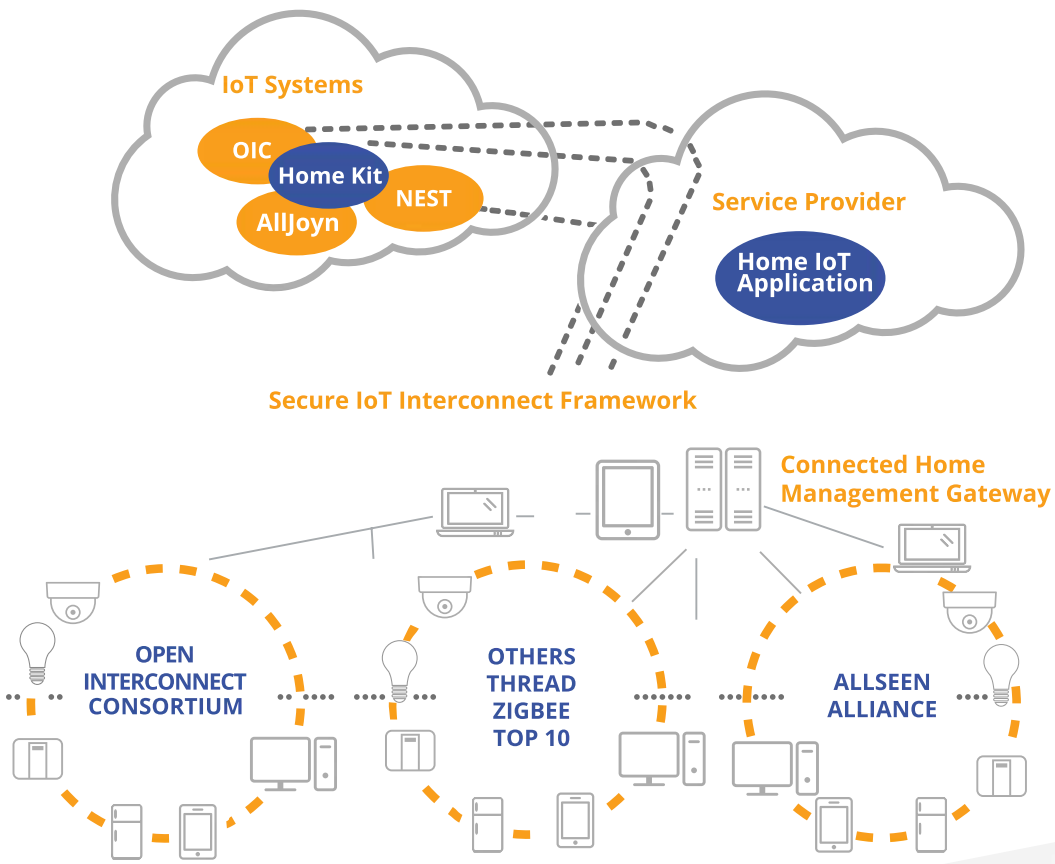


Figure 9 - IoT Standards and Home Gateway

The secure IoT interconnect framework software in the gateway forwards messages to the respective IoT OTT system in the cloud and then translates them for the MSO's own set of home IoT application(s). The former schema will enable support of legacy services whilst eliminating the service--specific hubs. The latter will allow for introduction of fully unified, all-encompassing services.

## Functionality of a future set-top box/TV IU for IoT services

On-boarding on the new IoT device:

Now consider the features that illustrate how average subscribers can on-board a simple IoT device and test/interact with it using the remote and their TV screen. We have this material thanks to extensive research done in the UX area.

The key attributes of IoT UI needed to on-board new devices are delivered by:

- Simplicity, often taken to the extreme
- Intuitiveness of navigation
- A limited number of steps to accomplish the desired action/effect
- Interactivity, triggered by system notifications

**Step 1.** We start with on-boarding a simple dimmable light bulb. The subscriber unwraps it, plugs into the light fixture and turns on the power. Next, the subscriber navigates inside the main set-top UI to the settings, then triggers a "connect device" app. A minimal set of keys is used to take these steps.

**Step 2.** Once the connect device app is triggered, the entire home IoT system indicates that a "dimmable light is connecting." Pressing another button on the remote permits the light bulb to be on-boarded next. Yet another button will abort the process. Only two buttons are needed.

**Step 3.** After the automated on-boarding step is complete, the notification changes to "dimmable light connected" and its background changes to indicate success. No button needs to be pressed in this step.

**Step 4.** Pressing another single button on the previous screen takes us to a screen where the device can be named based on its destination location.

**Step 5.** The subscriber is now able to view the entire IoT network with the kitchen light joined into the "halo" of all devices. Its functionality can be tested from the TV screen.

**Step 6.** By accepting the default on the screen in step 5, the subscriber enters the device test area where he can change the device's name and turn it on/off and dim lights, etc.

**Examples of notifications from IoT services and subscriber interaction:**

In this section, we will show examples of interactions with notifications from active IoT services. As with the on-boarding process, the subscriber's response to notifications are very simple and navigation is intuitive.

---

### Example 1. Notification from a home device (Xbox) about poor Wi-Fi connectivity

While navigating inside the main UI, the subscriber receives an on-screen notification indicating that the gaming console is experiencing problems with its connection to the Internet.

By pressing a button on the remote, the subscriber is taken to the screen showing the networked home devices and sees an Xbox in the center of the halo. The icon has a red background, which indicates major connection issues. The next step of network "self- healing" is then suggested to the subscriber.

---

### Example 2. Notification from the door webcam

While navigating inside the main UI, the subscriber receives an on-screen notification indicating that the webcam monitoring the front door has been triggered by an event.

By pressing a single button, the subscriber can see a recording of the event that triggered the notification.

---

### Example 3. Notification from the temperature sensor

The subscriber receives an on-screen notification indicating that one of the temperature sensors was triggered because it detected conditions outside of its programmed thresholds.

By pressing a single button, the subscriber can see the actual reading from this sensor and can take corrective action.

# CONCLUSION

We are still relatively early on the curve of IoT growth with traditional CE home automation companies and numerous start-ups vying for a piece of the action. MSOs and other traditional Service Providers are beginning to add home automation to their security services by using third-party, proprietary overlay hubs, and expensive tablet-portals. High CapEx and proprietary interfaces hamper these inroads. There is no major differentiation between MSO and OTT solutions at this point in time.

Subscribers are generally interested in automating their homes and remotely monitoring them via webcams and sensors. However, they are discouraged by the high initial cost of the systems. The survey of consumers mentioned earlier in this paper revealed that bundling fees for IoT with other services is the preferred way to pay for them. Other subscriber objections are the potential for technical challenges with installation, and the lack of security and data privacy capabilities of OTT IoT systems.

MSOs can shift gears and accelerate adoption of IoT by becoming a full Service Provider, and by partnering with healthcare, wellness, insurance, utilities and other entities to host their offerings in the cloud using gateways and set-top boxes that control the home devices. MSOs can easily add an interface to communicate with IoT devices to the gateways and set-tops and integrate standards-based communication protocols to on-board and manage them.

Lastly, MSOs have an opportunity to empower their set-tops to act as portals for IoT services. By taking advantage of built-in browsers, these set-tops can render simple and intuitive UIs to create and interact with the new services. They can also integrate existing services with IoT to create a seamless and rewarding UX.

# ABBREVIATIONS

| | |
|---|---|
| Apps | Applications |
| B2B2C | Business to Business to Consumer |
| BPI | Baseline Privacy Interface |
| BTLE | Bluetooth Low Energy |

| | |
|---|---|
| CAPEX | Capital Expenditures |
| CE | Consumer Electronics |
| CoAP | Constrained Application Protocol |
| DOCSIS | Data Over Cable System Interface Specification |
| IETF | Internet Engineering Task Force |
| IoHT | Internet of Healthy Things |
| IoT | Internet of Things |
| IPR | Intellectual Property Rights |
| M2M | Machine-to-Machine |
| MFI | Magnetic Field Imaging |
| MSO | Multiple System Operator |
| OIC | Open Internet Consortium |
| OSS | Operations Support Systems |
| OTT | Over-the-Top |
| PHY | Physical Layer |
| PnP | Plug and Play |
| QoS | Quality of Service |
| SNMP | Simple Network Management Protocol |
| UI | User Interface |
| UX | User Experience |
| WPAN | Wireless Personal Access Network |

# REFERENCES


Figure 2: [NCTA]
https://www.ncta.com/platform/industry-news/infographic- the-growth-of-the-internet-of-things

Figures 3 and 4: [BI]
http://www.businessinsider.com/connected-home-forecasts-and-growth-2014-9

Figure 5: [SAVANT] "Personalizing Home Control and Automation: Defining the Connected Home," by Mark Tubinis, SVP Connected Home, ARRIS. A Technical Paper prepared for the 2014 Society of Cable Telecommunications Engineers

Figure 7: [EDC] https://www-edc.eng.cam.ac.uk/projects/homeusedevices/

[CAREGIVER] https://caregiver.org/selected-long-term-care-statistics

[INFON] http://www.infonetics.com/pr/2014/Connected-Health-M2M-Market-Highlights.asp

[THREAD] http://threadgroup.org/About.aspx

[QCOM] https://www.strategyanalytics.com/access-services/components/handset-components/reports/report-detail/smartphone-apps-processor-market-share-q2-2014-qualcomm-captures-58-percent-revenue-share#.Vc3_wnh97lc

[VDC] http://blog.vdcresearch.com/.a/6a0115714871cc970c01bb0819dbaf970d-pi

[Z--WAVW] http://www.z-wave.com

[ZIGBEE] http://www.zigbee.org

[BT] http://www.bluetooth.com/Pages/low-energy-tech-info.aspx

[WI--FI] http://www.wi-fi.org

[OIC] http://openinterconnect.org