THE SWITCH E-BOOK

Why Wires Matter More Than Ever

www.primex.com

primex

THE SWITCH E-BOOK

Contents

primex

Connecting the Intelligent Home

For many years 'home automation' was the field of a few hobbyists or wealthy homeowners that were willing to pay for the novelty that early and sometimes custom automation products offered.

The recent consumer availability of intelligent, voice controlled Smart Home Hubs by major vendors such as the Amazon Echo Dot, Apple HomePod, Google Home, Samsung SmartThings, and Wink Hub have generated renewed and broad interest in the ability to control sound systems, smart lights, digital locks, security cameras, thermostats, lawn sprinkler systems, and more, especially with hubs priced as low as $49.

When you add to that—waking up to your favorite tunes, the weather forecast, your stock prices, news headlines, message dictation, voice assisted internet searches, ordering and booking, fitness and health management, even playing online video games—then you have an entirely new dimension to Internet enabled 'convenience'.

Home automation defines a rapidly changing world in which everyday objects are connected to the Internet through IoT (Internet of Things) technology. It is as much about people as the inanimate connected objects. It is an expression of lifestyles, individuality, and striving for more knowledge, entertainment, comfort, and security.

Connecting to the Smart Home Hubs are a broad variety of what the industry calls constrained and high capacity IoT (Internet of Things) devices. Constrained devices have narrowly defined functions, comparatively low capacities in terms of processing power, memory storage, and functionality, have limited security, and also require less power—and are usually battery powered. Examples are simple sensors and switches.

High-capacity devices have significant processing power, are typically powered with an external power supply, and have stronger security features. Examples are media streaming devices (e.g. for Netflix, Amazon Prime, Hulu, etc.), smart sprinkler controllers, etc.

Energy and resource efficiency management is one of the first key areas where IoT devices show huge benefits by controlling smart heating thermostats, lawn sprinkler systems, refrigerators, and lighting sensors, optimized for time of day, seasonality, and home occupancy patterns.

Vendors are offering sensors and power switching modules that can monitor and control what used to be simple household items into powered, Internet-connected devices. They range from smart LED lightbulbs that not only turn on or off, but change color hue based on the homeowners mood or time of day, automated curtains, even remotely controlled pet feeders.

Over time, more and more home appliances and 'convenience' will be intelligently managed without requiring any human intervention or control. McKinsey estimates that in 2025, IoT devices will, on average, reduce labor by 100 hours per year (or 17 percent)[1] in a typical household by automating chores such as vacuum cleaning or lawn mowing. For now, growth for the intelligent home market continues to be driven by energy management and security solutions.

In a recent survey of 3,965 primarily North American respondents[2] 31% of all respondents say they use smart home tech, 37% having 3 or more devices. Smart thermostats (12%) are the most widely adopted device, followed by security cameras (9%), motion sensors (9%) and smart speakers (8%).

As to planned Smart Home Device purchases, 31% of respondents say they plan on buying at least one specific type of smart home device in the future. Another 14% are unsure if they will purchase any smart home tech, and 55% do not plan on buying. Smart cameras (12%) and thermostats (11%) show the biggest upside.

[1] The internet of things: Mapping the value beyond the hype - McKinsey Global Institute (MGI) — June 2015

[2] 451 Research — Changewave 2017

More Devices. More Bandwidth. More Connectivity.

More than 75% of U.S. homes currently on broadband use Wi-Fi within their unit to connect to the internet.[3]

According to the Consumer Technology Association[4] 4K UHD TVs will make up half of all total digital displays sold in 2018, with unit sales forecast to hit 22 million units (27 percent increase over 2017 data) generating $15.9 billion in revenue (14 percent increase).

In home bandwidth consumption will continue to grow with most homes not only adding smart home devices, but also streaming media to more D/UHD/3DTV TVs, playing high resolution multi-player games, and adding more digital assistants.

Over the years, new construction home pre-wiring evolved from some to all rooms being wired with phone and coax for cable TV to the majority of builders now offering CAT5, in some cases CAT6 wiring throughout the home. CAT5 is capable of speeds up to 1 Gigabit, while CAT6 is capable of 10 Gigabit networking.

[3] Parks Associates — May 2017

[4] 2018 - U.S. Consumer Technology Sales and Forecasts — Consumer Technology Association

One of the newest options is fiber optic cable. It is made out of thin strands of pure glass that carry digital information with light instead of electrical currents. Not only can it carry a signal over longer distances, it has a much higher throughput capacity. With 4K deploying now, and 8K displays just around the corner, fiber will surely find itself inside the home in the future.

Consider this, a single 8K TV will require a sustained data rate of 48Gbps. Copper wire tops out at around 10 Gbps.

Builders are increasingly promoting WiFi only homes as it requires little or no up-front cost. While WiFi offers tremendous flexibility, it is unlikely that it will be able to handle the growing data throughput needs of all the home's media devices.

It also begs the question, why consume WiFi bandwidth on high throughput consumption devices such as media streaming TVs and security cameras that are essentially fix-mounted in a location?

Wi-Fi is also subject to interference and intermittency. We will cover that further on.

The Dangers of an 'All Wireless' Home

The convenience of whole home WiFi can come with significant risks. The WiFi network itself can be the primary exposure point.

Most people now understand that a password and enabling encryption are basic, yet, the 2017 KRACK attack revealed how vulnerable home networks can be. As a result, WPA2 (WiFi Protected Access), the encryption standard that secures most modern WiFi networks today is no longer secure.

A successful home network intrusion could provide a hacker with access to sensitive personal information, including financial and medical data. It also exposes your entire network and all connected devices.

In early 2018, the Wi-Fi Alliance announced the latest Wi-Fi security protocol, WPA3, which will better protect against brute-force attacks and also employ individualized data encryption, scrambling the connection between each device on the network and the router.

It is unlikely that all of today's network devices will be upgradeable to this new WPA3 protocol, or whatever may come thereafter.

A secure network is only as strong as its weakest link, with each wireless device added, a possible additional exposure point.

Most people don't necessarily realize that products they now buy and deploy for energy savings, security, and comfort are essentially 'IoT devices'. These devices not only control functions in the house, but also share data and tap into Internet-based data sources. For example, weather forecast services use the aggregated data and artificial intelligence to learn and adjust optimal settings to their associated devices.

For example, smart thermostats gather data on motion, temperature, humidity and light and combine that with data analysis to automate the control of the temperature based on the users' lifestyle and habits.

IoT devices are themselves prime targets for hack attacks, especially Constrained Devices. In the last few years, many well-publicized cyberattacks have demonstrated the risks of inadequate IoT security, as confirmed by recent Forrester's TechRadar research.

Compromised IoT devices are not only used to gain access to the network that it is connected to, they can also be clustered into large, global cyberattacks.

In one such hack attack a large number of internet-connected devices such as DVRs and security cameras were compromised and reconfigured to execute massive cyberattacks on popular websites.

Wireless IoT devices make security more challenging than traditional wired devices due to the many RF and wireless communication protocols and standards. Hackers are realizing that homes are very easy targets with many wireless IoT devices lacking basic security layers.

With increasingly more personal and sensitive data (including financial and personal health data) being kept on home networks, wireless IoT devices can be a system's weakest link.

The danger is not only in the access to sensitive information. Hackers expose consumers to costly ransomware attacks, locking them out of their computers and home servers that sometime hold their entire digital life footprint. There were 4.3x new ransomware variants in Q1 2017 than in Q1 2016.[5] Global ransomware damages are predicted to exceed $5 billion in 2017.[6]

In September of 2017, Researchers at the IT Security Infrastructures group, Friedrich-Alexander University Erlangen-Nürnberg (FAU) discovered new security weaknesses in the popular ZigBee wireless network technology, making it vulnerable to attacks to light, heating, door lock, and security alarm systems that use the standard.

A wired network is by definition a 'closed circuit' with its only external access point the gateway or modem and router combo, all of which can be firewalled to provide additional lines of defense.

[5] Source: Proofpoint Q1 2017 Quarterly Threat Report

[6] Source: Cybersecurity Ventures

Additional 'Wired' Benefits

Wired home networking holds other significant advantages over WiFi only configurations:

Capacity

In 2015, the Organization for Economic Cooperation and Development (OECD)[7] estimated that a family of four already had an average of 10 devices connected to the Internet in their household and that this average will increase five-fold to 50 devices by 2022. Between 2015 and 2020, U.S. households are expected to acquire more than 2.3 billion connected devices.[8]

Most of these devices exert little or no strain on the average home network, but as rapidly growing sales of 4K/UHD TVs make media streaming more prevalent, we can expect slowdowns.

According to Research Nester Pvt Ltd, [9] the global 4K TV market is expected to grow at a CAGR of 18.1% between 2017-2024, with the US as the second largest, but fastest growing region. Netflix recommends at least a 25Mbps connection for Premium subscribers to appreciate UHD content. Add several UHD content streams per home and you quickly reach the maximum sustained throughput of most wireless systems.

Although Wi-Fi throughput increased significantly in recent years, maximum speeds are still 866.7Mb/s for 802.11ac and only 150Mb/s for 802.11n, today's most utilized standards. In comparison a CAT6 wired Ethernet connections can handle speeds up to 10Gb/s, and unlike wireless, more consistently.

[7] This estimate applies to an average family of four located in OECD countries. OECD, OECD Digital Economy Outlook 2015 (Paris: OECD Publishing, 2015).

[8] Parks Associates – May 2017

[9] 4K TV's Market : Global Demand Analysis & Opportunity Outlook 2024 - Research Nester Pvt

Interference

Interference occurs when two communication signals are at or close to the same frequencies in the same vicinity, which may lead to degradation of device service or performance. There will be an enormous need for spectrum capacity as IoT device usage grows and electromagnetic spectrum interference management becomes more challenging.

There are many basic things that can interfere with the quality and reliability of a home WiFi network, including shielding by concrete or brick walls, microwave ovens, cordless phones and baby monitors that operate in the 2.4 GHz or 5 GHz spectrum, RF leakage from satellite coax cables, high voltage power installations near your home, and more.

Most neighborhoods now have homes with powerful routers that have at least one access point using 2.4GHz, and one in the 5GHz band, along with separate guest access. If you run a WiFi scan on the average apartment or even suburban home you see at least 10 to 30 signals continuously 'hopping' the fourteen available WiFi channels, competing to use their limited available bandwidth.

The devices themselves may also be the culprit. In January 2018, Google had to admit that Google Home devices and Chromecast dongles have a 'keep alive' feature that may crash most popular WiFi routers. As proprietary protocols and functionality gets added, so increases the risk of outages and performance degradation.

Whole Home Power Consumption

With environment and sustainability conscious Millennials[10] entering the home buying market, architects and builder look for solutions that not only meet their technology needs, but do so in an energy and space efficient manner.

With an increase in recent years of low power devices that use external power supplies and more consumers becoming aware of their overall energy consumption, the 'off' consumption of power supplies and devices is getting more attention. For example, a cellphone charger will consume 1 watt while plugged into the wall, even without a phone; a DVR set top box will consume 48.5 watts of power while turned off.

Network based technologies such Power over Ethernet (PoE) and USB Type-C hold the promise of low voltage power delivery throughout the home, eliminating the many energy wasting chargers and power converters. It also allows you to use a single cable to deliver both power and data, significantly reducing the installation labor and parts involved.

With more homes exploring solar power and power storage units, low voltage power distribution is also coming back in the forefront. Copper wiring is here to stay.

[10] Millennials – Breaking the Myths - The Nielsen Company - 2014

Wire it. Wire it right.

A heterogeneous ecosystem of both wired and wireless devices and services can appear difficult to secure, especially without clear guidance for consumers.

Slowly the industry is advocating a Home Area Network (HAN) model with a wired residential gateway or router that provides firewalled access to the Internet through an Internet Service Provider. This model segregates out a resilient, firewalled, hard-wired sub-network for computers and devices with sensitive personal information, such as media servers, SANs, security systems, and home healthcare devices.

All wireless traffic is then put in additional sub-network(s), one for wireless devices that provide adequate security, and a second one for those devices that could pose a security risk to the HAN.

Wireless devices connected to the more secure sub-network can then be given full pass-through access to the HAN, whereas wireless devices with questionable security are kept outside of the firewall, in a similar fashion to providing 'guest' access to the Internet.

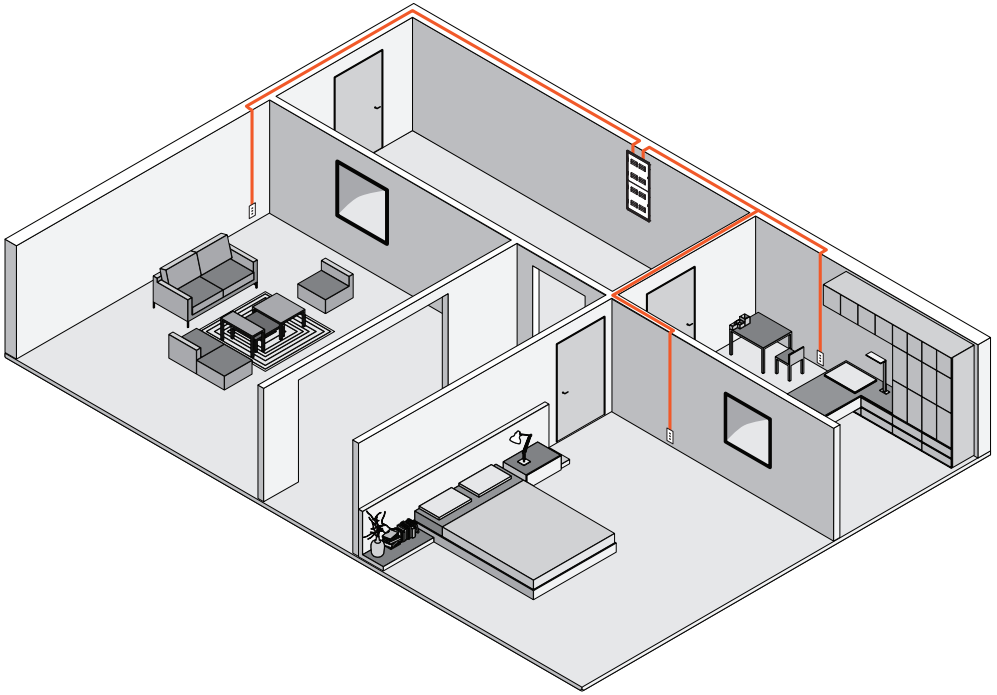
A Best Practice Approach to Wiring

A contemporary CAT6 wired home network starts with a media panel, the physical hub for all network and communications wiring throughout the home.

The hub and spoke model still provides the most efficient distribution model and therefore requires a media panel that can be placed central to its key outlet points. Traditionally media panels were mounted in storage closets and basements, accessible but out of sight.

Today, most homes will have at least two to three home network devices that are preferably placed inside or within proximity of the media panel. They include modems, routers, VOIP gateways (e.g. Ooma, MagicJack), and security systems.

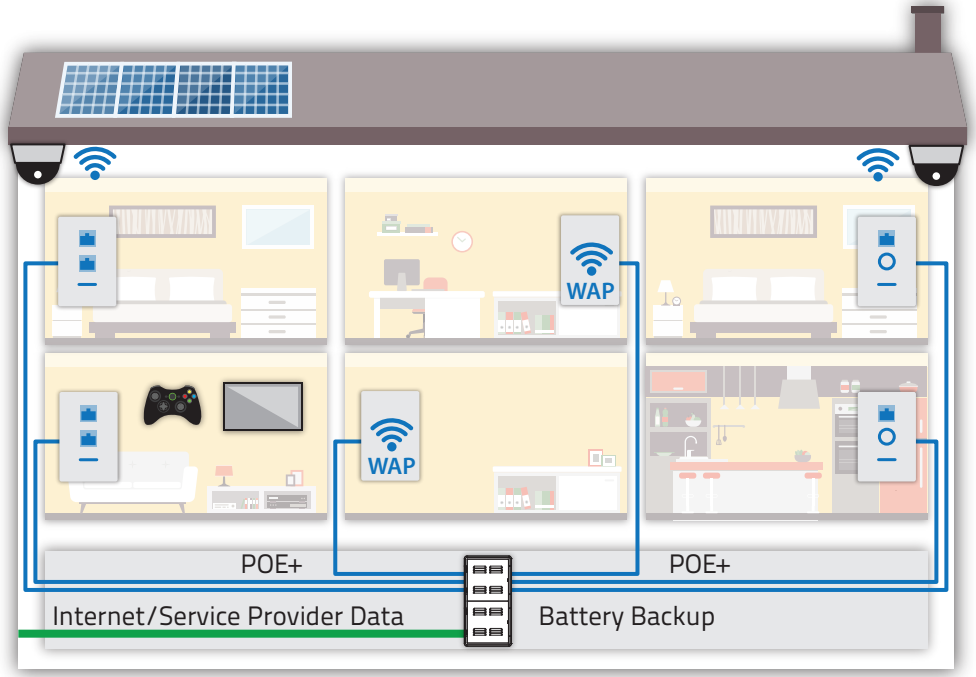
If a wireless router is to be placed in or near the media panel, it should be installed in a central location to assure even coverage throughout the home. Alternatively, WiFi extenders can be placed towards areas of the home that have poor coverage.



As to wiring the access points (CAT5/6 or fiber), high usage areas that require a secure wired connection would include a family room media center (if a media server is placed there), a home office, bedrooms and other rooms where you want to use UHD TVs or have high performance gaming.

For new construction, consideration should be given to pre-wiring CAT6, not only to obvious wall outlet locations, but also to provision both power and data to security cameras, home automation and home healthcare devices that currently depend on external power supplies. Whether they ultimately use Power over Ethernet (PoE) or USB Type-C, the wiring will at least be 'in the wall', secure and ready.

Avoid surrounding metal objects, concrete or brick walls that will absorb the signal, nearby microwave or wireless phone stations, even areas where there is continuous movement of people as water in the human body can cause radio wave interference.



Summary

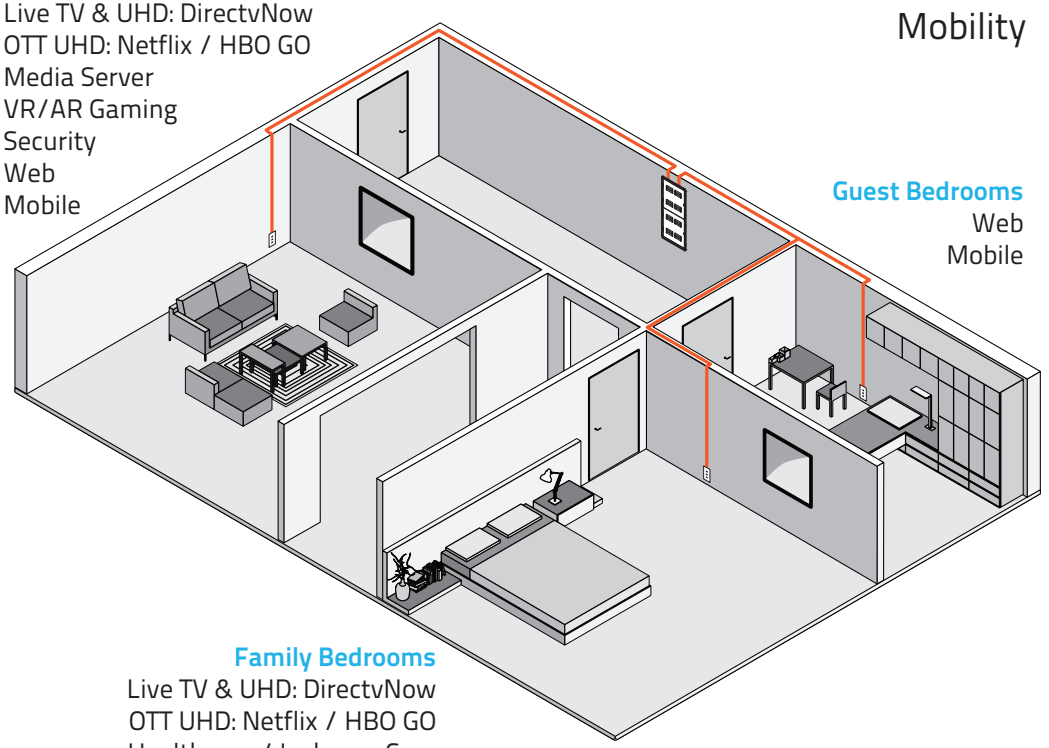
In home bandwidth needs will continue to grow dramatically in the coming years. Consumers want high speed, secure and reliable whole-home network coverage. While convenient, wireless (WiFi) is not as reliable, performant, and secure as wired networking.

A best practice approach calls for a heterogeneous Home Area Network (HAN) ecosystem of both wired and wireless connectivity, segregating a resilient, firewalled, hard-wired sub-network for computers and devices that need the highest level of security, bandwidth, and reliable uptime. All wireless traffic is directed through additional sub-networks, with or without access to devices and services behind the firewall. CAT6 wiring is also regaining attention for low power distribution throughout the home, while securely connecting devices to the Internet.

Wired Connectivity
Backup needs
Bandwidth / Low latency needs

Wired backhaul to wireless
Convenience
Mobility

Living Room / Game Room
Live TV & UHD: DirectvNow
OTT UHD: Netflix / HBO GO
Media Server
VR/AR Gaming
Security
Web
Mobile



Guest Bedrooms
Web
Mobile

Family Bedrooms
Live TV & UHD: DirectvNow
OTT UHD: Netflix / HBO GO
Healthcare / In-home Care
Web
Mobile

Resources

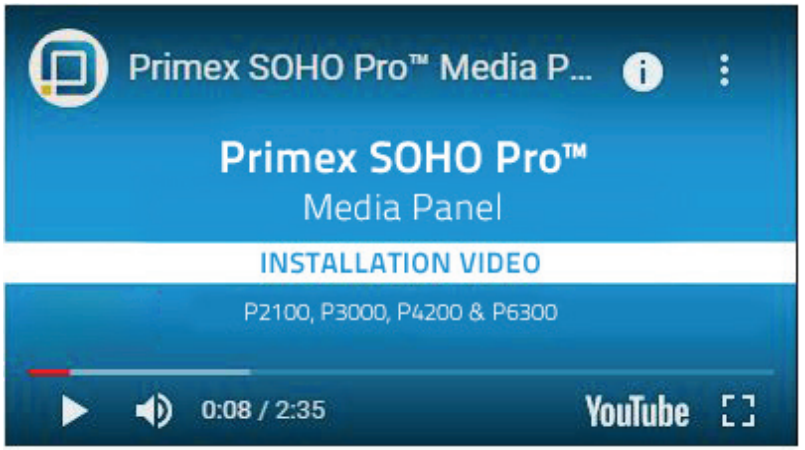
Smart Home Enclosures

PR1500

P3000

P4200

Installation Videos



Blog THE SWITCH BLOG

eNewsletter Sign up for The Switch

Social:

Website: www.primex.com

Contact: www.primex.com/contact

Toll Free Tel: 1 (877) 881-7875