SCTE STANDARDS JOURNAL

VOLUME 1 NO. 2 SEPTEMBER 2021

SCTE TECHNICAL JOURNAL

SCTE
a subsidiary of CableLabs®

SCTE STANDARDS JOURNAL

SCTE TECHNICAL JOURNAL

VOLUME 1, NUMBER 2

September 2021

Society of Cable Telecommunications Engineers, Inc.
140 Philips Road, Exton, PA 19341-1318

Table of Contents

Editorial Correspondence: If there are errors or omissions to the information provided in this journal, corrections may be sent to our editorial department. Address to: SCTE Journals, SCTE, 140 Philips Road, Exton, PA 19341-1318 or email journals@scte.org.

Submissions: If you have ideas or topics for future journal articles, please let us know. All submissions will be peer reviewed and published at the discretion of SCTE. Electronic submissions are preferred, and should be submitted to SCTE Journals ,journals@scte.org.

Foreword

One of our industry's biggest success stories in recent years is how cable broadband has become the preeminent foundational platform that makes Internet communications, information and applications possible. More and more, the innovations of cable and Silicon Valley have worked in parallel to enrich the lives of consumers.

Like SCTE Cable-Tec Expo next month, our SCTE Technical Journal reflects that enormity of purpose with a diverse mix of topics covering existing infrastructure, emerging technologies, and the applications that will run across our networks. This latest edition of the quarterly volume includes articles on cable's bread-and-butter sectors – the access network and video – as well as next-generation data and AI/ML capabilities and the layers of new services they enable. Here's how the lineup shapes up:

- **Drivenets' Clayton Wager** takes you deep inside Distributed Disaggregated Chassis networks, including technical and business impacts and physical placement and power consumption advantages.
- Longtime contributor **Robert Cruickshank and the team at GRIDIoT** explain how electric load sensing, forecasting and sharing can open up new markets for the industry.
- **NCTA's Matt Tooley, Piracy Monitor's Steve Hawley, and Charter's Kei Foo** outline how AI/ML can arm the industry against piracy.
- **Charter's Srilal Weera** bridges cable's present and future with a piece on the technical intricacies of digital advertising and video metadata
- **CableLabs' Andy Dolan** discusses how Wi-Fi Alliance Easy Connect can streamline onboarding for Open Connectivity Foundation IoT specification devices.
- **Sudheer Dharanikota, his team at Duke Tech Solutions, and Cox Communications' Bruce McLeod** weigh in with two articles on telehealth: the business case and the market landscape for cable operators.

There is also a letter to the editor from **Cox Communications' Kristina Waters** and **Ubuntu's Ananya Gupta** posing novel ideas regarding the age-old problem of recycling coaxial cable.

We'd like to express my gratitude to all those who contributed to this month's edition, as well as those who will be speaking on scores of relevant topics next month at Cable-Tec Expo. We urge you to take advantage of this Journal, the virtual Expo program, and all of the resources that make SCTE so valuable to our industry. At the same time, we hope you will consider authorship in a future edition of the SCTE Technical Journal. Working together and sharing expertise is vital to the continued ability of our technical workforce to achieve new objectives.

Thanks for your participation in SCTE; we look forward to connecting with you during Expo and in the future.

The SCTE Editorial Staff

SCTE STANDARDS JOURNAL

A Technical Analysis Of A Distributed Disaggregated Chassis Architecture For Cable Aggregation Networks

A Technical Paper prepared for SCTE by

Clayton Wagar, Senior System Engineer, DriveNets, SCTE Member
125 Half Mile Road, Suite 200
Red Bank, New Jersey 07701
cwagar@drivenets.com

Table of Contents

List of Figures

List of Tables

1. Introduction

In 2020, broadband service providers (cable, DSL, fiber providers) experienced their best year since 2008, with a net addition of almost 4.9 million subscriber units. Among them, cable operators have reached 69% market share (up from 67% in 2019 and 65% in 2018) making the most of the broadband acceleration due to the COVID-19 pandemic[i].

Nonetheless, cable operators face many challenges to support the traffic growth originating from their commercial success. Network scale, resource efficiency, network availability, quality of service (QoS) and operational efficiency are key elements, especially at the IP aggregation layer.

Current IP aggregation architectures are built on monolithic chassis solutions, where configurations match specific requirements for each geographical site: three- to five-year growth forecasts, power limitations, space, and more. When a chassis solution reaches its capacity limit, there are two options that are usually considered. Option 1 is to replace the current chassis solution with a higher capacity solution (“forklifting”). Option 2 is to introduce hierarchy into the site using spine-leaf (Clos) architectures. However, both lead to multiple technical, operational, and business challenges that cable operators are keen to minimize.

To address these issues, the Open Compute Project, or OCP, has defined another alternative based on a new architecture: the distributed disaggregated chassis (DDC) white box architecture – developed by Tier-1 service providers, and supported by a wide community of operators and vendors through the Open Compute Project.

This paper discusses the DDC architecture, how it compares to a spine-leaf architecture, and the benefits cable operators can expect from it at the aggregation layer.

2. A typical cable aggregation network architecture

2.1. Overview

Cable networks are facing growing demand for residential services’ aggregation, driven by the expansion of cable modem termination system (CMTS) services, virtual CPE (customer premises equipment) and video, while:

- Minimizing impact between residential and business services
- Reducing north-south traffic for east-west traffic within primary hubs
- Ensuring N+1 redundancy

In parallel, the multiplication of distributed access architecture (DAA)/deep fiber locations often require super-aggregation layers to minimize impact on the transport layer. Although optical and packet transport grooming technologies allow for some flexibility in the overall size of the aggregation domain, the growth of consumer broadband traffic continues to drive very high-density aggregation.

Additionally, trends in network and service delivery design point to the continued consolidation of connectivity and service delivery domains. While most network-based services have become virtualized over the last decade, resulting in greatly expanded data center footprints, the logical (and often geographical) placement of those services continues to evolve. Services which were served from mega-scale data centers only a few years ago now demand placement nearer the edge of the network, for performance and optimization reasons. Examples of these network-based services include virtualized access workloads, content-delivery, instrumentation and analytics, and value-added network services delivered to subscribers.

As these edge cloud-delivered services expand, alongside the growth in aggregation connectivity, operators are finding an acute need for scale-out architectures that allow high-fidelity packet connectivity in the aggregation domain across both underlay (access network aggregation, metro, and core connectivity) as well as overlay (cloud connectivity between compute/storage clusters). In fact, some operators are developing collapsed aggregation domains, which serve both underlay and overlay through the same network element.

2.2. Aggregation network architecture

Access infrastructures (both legacy and virtualized access nodes) are aggregated through the use of either a) home-run connections through a metro optical network to the IP aggregation point, or b) ring-based aggregation subtended off of a mesh of nodes connected to the aggregation point.

This architecture has served the cable industry extremely well over the past two decades:

- Initially piggybacking on the existing ring-shaped paths that cable operators installed when video was the primary service and IP backhaul was not a first-class product;
- Building the packet mesh between "hot spots" in the metro domain, shortcutting the rings where necessary to optimize IP traffic; and
- Supporting a full mesh (where needed or desired), allowing minimal oversubscription for subscribers and a high degree of control for additional services (business, partner, etc.)

Interestingly, because most cable operators continue to use IP transport for their legacy video services, many of them continue to treat partially- or fully-meshed portions of their network as pseudo-rings. This is largely due to operational simplicity surrounding dual IP multicast feeds to the edge-QAM devices.

The demand on these aggregation architectures, both physical and logical, will continue to grow. As access capacity rides the year-over-year growth curve, and as edge cloud services assimilate into the same part of the network, we can predict that aggregation layers will drive both the physical port count as well as the logical complexity of this unique part of the network.

2.3. Services

Historically, cable operators have not typically deployed an overly complex set of protocols in their IP networks, compared to their service provider peers in the telco domain. While IP routing protocols cannot be considered "simple," cable operators have had the good fortune to be fast movers behind the early adopters in this field, adopting protocols after they mature and prove their usefulness.

Nearly all current cable operators rely on a very well-supported mix of the following in the packet domain:

- BGP for both external and internal propagation of routes
- IS-IS (and sometimes OSPF) as the Internal Gateway Protocol (IGP)

- MPLS, with label distribution for both internal traffic engineering and business services
- Coarse QoS models, with most of the end-user QoS management left to the highly capable DOCSIS domain

Furthermore, cable operators are developing and deploying edge cloud services which allow for IT workloads (x86-based network services) to be deployed across the network, including near- and far-edge locations. These edge clouds often rely on the previously mentioned protocols, with the addition of encapsulation or tunneling to virtually expand the connectivity domain when needed.

The result of this service blend is an aggregation layer with a primary focus on scale and resiliency. The largest cable operators are forecasting 100 gigabit Ethernet (GE) aggregation sites with over 1,000 connections to access, cloud, peers, and operations systems.

3. The DDC model

3.1. Overview

The DDC builds on the same well-known concepts that have served us well in the networking industry over the last four decades:

- Network processor-based, distributed forwarding;
- Scalable control-plane functions, often now on a general purpose x86 CPU complex;
- Interconnection between elements using a deterministic fabric; and
- Highly interoperable, standards-based optical connectivity.

At a very high level, the DDC specification simply documents any given chassis-based router on the market today, with a key difference: DDC systems are composed of discrete, interoperable units. Each of these units, described below, serves a specific function. They are also standards-based, and multiple vendors can be mixed-and-matched to assemble a system.

Table 1 - Comparison between Chassis and DDC models

Chassis model	DDC model
Line card - proprietary	Standalone white box based on Broadcom Jericho2 chipset – multiple ODM vendors
Fabric card - proprietary	Standalone white box based on Broadcom Jericho2 chipset – multiple ODM vendors
Backplane connectivity - proprietary	Standard external cabling – multiple vendors
Proprietary power, fan, controllers common for all cards	Each white box comes with its own power and fan
Proprietary rails	Standard rails
16 SKUs on average	Six SKUs on average

3.2. Key building blocks

The DDC white box design calls for three key building blocks:

- A packet unit, the "line card," which supports external connectivity through standard optics, and has high-capacity packet-forwarding capabilities.
- A fabric unit, used solely for interconnecting packet chassis in the system. The fabric in a DDC architecture is cell-based, deterministic, and input-queued. This ensures that no hierarchy of buffering is introduced into the network, and the resulting fabric does not require overspeed to meet the needs of the system.
- A control unit, standard high-performance x86 server(s), running protocol operations and maintaining system functions.

These building blocks can be used to build a hyperscale aggregation layer, while allowing physical flexibility for the space and power concerns that are typical for most data centers or hub locations. Additionally, these building blocks provide 100% coverage of the technology, protocols, and use cases compared to existing chassis-based systems and designs.

Further, using these building blocks in a DDC system relieves operators from the existing constraints of chassis-based solutions, like proprietary hardware sourced from only one vendor, which leads to a vendor-constrained environment. The DDC model enables supply-chain diversity across manufacturers, and procurement leverage in pricing and discounting.

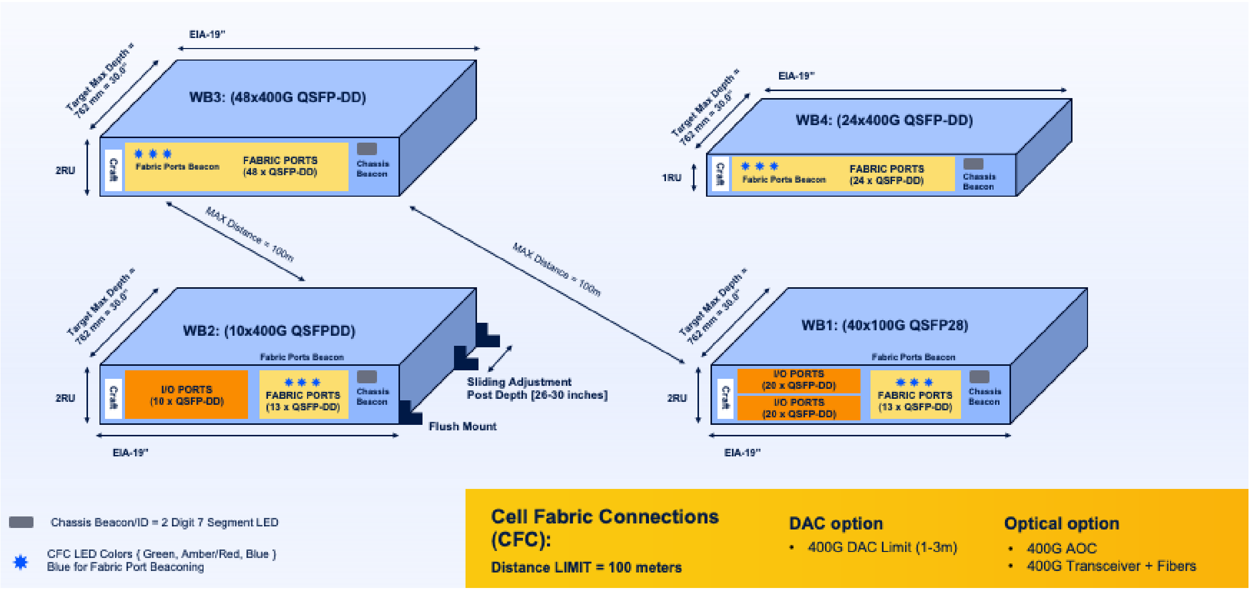


Figure 1 - The DDC building blocks

3.3. Configurations

Like many hyperscale technologies, the DDC model is evolving quickly and according to market demand. Currently, DDC specifications formally define four different sizes, or models:

- A single line card system that supports 4 Tbps of capacity, and houses all control plane functions in a single, typically 2 RU system.
- A small cluster that supports16 Tbps of capacity, by leveraging 1+1 fabric systems and up to four-line card systems.
- A medium cluster that consists of seven fabric systems and up to 24-line card systems. This configuration supports 96 Tbps of capacity.
- A large cluster that consists of 13 fabric systems and up to 48-line card systems. This configuration supports 192 Tbps of capacity.

With the introduction of new systems based on evolving network processors, the DDC architecture can be deployed in configurations supporting over 650 Tbps.

3.4. Other hardware components

Other components in the DDC system are standards-based and easily deployed and maintained. They include:

- An Ethernet-based interconnection underlay, primarily used to deploy and configure the system, and establish logical connectivity among the various elements in the cluster.
- Client-side optics based on MSA form factors and well-defined optical standards.

Fabric connections, based on optics standards, ensure speedup-free passage of traffic between packet systems. These fabric connections can also make use of evolving technologies, greatly reducing expenses and physical constraints on scale-out systems.

In practice, DDC systems look and operate nearly identically to legacy, chassis-based systems once installed. The operational models are highly similar as DDC systems can operate as a virtual single entity through system orchestrators. While the physical form might be different, the maintenance and troubleshooting are even simpler through component-based visibility and advanced automation.

3.5. NOS software

A key enabler for the DDC architecture is the network operating system. In addition to the hardware components of the DDC system, the NOS provides full lifecycle management of the individual components, interacts with the network with standard routing protocols, and provides the operational interface for managing the system. Multiple commercial NOS vendors support DDC architectures today, and open-source projects are planning to add support in the coming years.

A modern NOS supporting the DDC architecture is typically based on software best practices – orchestrated container-based microservices, publish/subscribe interfaces for instrumentation and analytics, support for standard operational interfaces, and full visualization of the system with operational dashboards.

One of the most important challenges for the DDC NOS is the orchestration of capabilities in the system. The initial software loading and configuration of the white boxes, through system verification and turnup, and into day zero and day 1+ operations, are all important and complex functions. These functions are required to scale with the underlying hardware. This orchestration capability can also interact in real-time with compute and storage orchestrators to give the operator fine-tuned control over the entire service delivery stack.

One important distinction between DDC and legacy monolithic architectures is the specialization of vendors in the hardware and software domains. The vendor that supplies DDC NOS will almost certainly be different from the hardware vendor that supplies the chassis, optics, and cabling. In this way, vendors can focus, specialize, and deliver at a more natural cadence, versus a vertically integrated system, in which hardware and software must be developed together.

4. Analyzing the DDC architecture in aggregation use cases

4.1. Software and services

A key element of analysis is the ability of the DDC solution to perform the necessary network services for the operator. While the underlying network processor has a great deal of capability, it still requires a robust NOS to power the tasks.

Aggregation routing typically does not require complex configuration or protocol support. Usually, only light-touch policies, traffic engineering, and coarse QoS enforcement are needed.

The DDC architecture defines the hardware and layout of the cluster. However, the specification does not define a particular software stack to power the system. As of this writing, at least two vendors supply DDC NOS, with open-source projects underway as well. These vendors are responsible for developing an entire routing protocol stack, in addition to the lifecycle and orchestration necessary to maintain the DDC hardware.

DDC NOS solutions focus on modern and common protocol stacks, for core and aggregation routing, as well as peering applications. DDC NOS solutions have the luxury of a modern operating system, best practices software engineering, and modern technology like containers and microservices.

Even though there are variations among vendors, one hallmark of the DDC ecosystem is that software companies can (and do) develop features at a pace not found in legacy chassis solutions. This has direct impact on technology lifecycles and technical debt. Network architects can expect new features (including boutique, customized features) from DDC NOS vendors within months rather than years.

4.2. Hardware

Analysis of routing hardware solutions typically focuses on the quantitative aspects of the solutions: types and quantities of interfaces; interface density; power consumption; and physical characteristics. Service providers compile requirements for specific use cases in the network, and compare different routing platforms based on their needs. These requirements vary significantly between operators.

Interfaces and density – DDC solutions in the market today focus almost exclusively on 100 GE and 400 GE interface types. Service providers have begun migrating to 100 GE in aggregation layers over the last several years, so DDC is well positioned for this wave of growth. For operators needing lower speed interfaces, DDC solutions typically can also break out to 50, 25, or 10 GE, although with reduced density. In the aggregation use case, DDC solutions allow for very high scale-out without the complexity of spine-leaf protocol operations and expense.

Additionally, DDC solutions offer density at least equal to, and in most cases higher than, chassis-based solutions. With the ability to add significant numbers of client interfaces without adding more common equipment, operators find DDC to have the best interface density for scaling out.

Physical characteristics – As previously discussed, DDC is typically deployed as a constellation of 2 RU boxes, each with a specific function (line card, fabric, control). These boxes are interconnected with a management ethernet network as well as dedicated fabric connections between all line cards. When fully installed, the DDC system resembles a compute cluster with external optical connections.

The ability to position these 2 RU elements is not arbitrary – there are some cable length requirements. However, there is significant freedom on how these elements are physically installed. The control elements might be installed with similar x86 compute servers, and the packet elements might be deployed closer to their client connections. Fabrics might be centrally located in the hub. This capability gives planners significant new freedom in the installation and layout of a high-density aggregation cluster.

Power consumption – The networking industry has had a keen focus on power consumption for several decades. Products are often designed with power consumption as a first-tier priority. Operators demand the lowest possible operational cost, looking at per-gig metrics as indicators. DDC solutions compare very favorably vis-à-vis their legacy chassis counterparts in this respect. Within a given generation of equipment, vendors typically have access to the same technologies and design patterns, leading to a variety of solutions with similar power consumption needs. DDC technologies achieve similar, or better, capacity, with equal power consumption.

Where DDC solutions outshine their chassis counterparts, however, is in *power distribution* – specifically, the ability to distribute the elements of a DDC chassis across many racks. Since the elements are interconnected with cables instead of a metal cage (chassis), network architects have new freedoms to design their physical footprint within a location. Per-rack power constraints are among the most frequent problems to solve during deployment. DDC solutions allow planners to 'spread out' the power consumption as needed. Whether to fit within older power distribution constraints, or to use leftover capacities within a bay, DDC uniquely provides this power distribution benefit.

4.3. QoS versus spine-leaf

Quality of service capabilities of routing platforms always get significant attention. Vendors have, over the last several decades, used QoS as a key point of differentiation in their products. Products based on merchant silicon, like DDC, have historically been viewed as inferior to custom-built, vertically integrated solutions from traditional vendors.

Any meaningful limitations on QoS capabilities are no longer applicable in today's world of network processing. Major vendors have adopted merchant silicon for their product lines, and the capabilities of those NPUs have improved with every generation.

DDC NOSs can implement any QoS algorithm and buffer significant amounts of traffic at granular levels. Aggregation use cases generally have only modest queueing requirements, and the silicon powering DDC brings no problems here.

One very interesting and key differentiator of DDC is the use of a single-stage QoS model throughout the system. Even fully scaled-out systems with thousands of 100 GE ports use a single point of QoS enforcement. This is done through the use of two key technologies:

- Ingress virtual output queuing for the entire system, ensuring that traffic destined for any given outgoing interface is managed on the ingress device. It guarantees that any QoS action is performed before transiting over the fabric and egress devices.
- Cell-based fabric interconnect is deterministic, load balancing, and full-mesh. There is only transient buffering of cells – no additional queueing or QoS is performed in the fabric. And because the traffic has already been QoS-processed, the fabric does not need significant speedup to prevent head-of-line blocking.

In contrast, spine leaf architectures (used for scale-out) with legacy chassis suffer from two key weaknesses. First and foremost, architects must use client ports to interconnect the many chassis, reducing service density and adding costs. Where QoS is concerned, spine-leaf adds an additional layer of buffering, and more importantly, operational complexity in traffic surges, when buffering works against application layer recovery.

5. Conclusions

The DDC architecture, only two years old now, shows significant capabilities for many use cases. In this paper, we have discussed the technical features of DDC, and how those line up well with aggregation and scale-out use cases.

Among the key findings:

1. DDC compares favorably, or even surpasses, chassis-based solutions in quantitative areas such as port density and power consumption.
2. A white box software ecosystem exists not only for aggregation and core, but also for more complex solutions such as mobile aggregation, peering, and BNG/BRAS.
3. DDC solutions offer best-in-class capabilities including robust protocol support and rich QoS capabilities.
4. There are significant technical (architectural) and business impacts thanks to DDC, including rule-breaking flexibility in physical placement and power consumption planning.

Operators looking at scaled-out architectures should seriously evaluate DDC. With significant and positive impact on the design and architecture of the network, DDC and white-box solutions offer compelling, valuable alternatives for the future of networks.

6. Abbreviations and Definitions

6.1. Abbreviations

BGP	Border Gateway Protocol
BNG	broadband network gateway
BRAS	broadband remote access server
CMTS	cable modem termination system
CPE	customer premises equipment
CPU	central processing unit
DAA	distributed access architecture
DDC	distributed disaggregated chassis
DOCSIS	Data-Over-Cable Service Interface Specifications
DSL	digital subscriber line
GE	gigabit Ethernet
IGP	Internet Gateway Protocol
IP	Internet Protocol
IS-IS	intermediate system-to-intermediate system
IT	information technology
MPLS	multiprotocol label switching
MSA	multiple source agreement
NOS	network operating system
NPU	network processing unit
OCP	Open Compute Project
ODM	original design manufacturer
OSPF	open shortest path first
QAM	quadrature amplitude modulation
QoS	quality of service
RU	rack unit
SCTE	Society of Cable Telecommunications Engineers
SKU	stock keeping unit
Tbps	terabits per second

[i] Leichtman Research Group https://www.leichtmanresearch.com/ – Analyst on the Broadband, Media and Entertainment Industries since 2002

SCTE STANDARDS JOURNAL

Optimization of Electric Load Shaping, Sensing, and Forecasting

A Guide to Operational Savings and New Business Models

A Technical Paper prepared for SCTE by

Dr. Robert F. Cruickshank, III, CTO, GRIDIoT® by RCA, SCTE Member
132 Cruickshank Rd #269
Big Indian, NY 12410
rfciii@cruickshank.org
+1-703-568-8379

Laurie Asperas-Valayer, CSO, GRIDIoT by RCA, SCTE Member
AsperasValayer@gmail.com
+1-631-335-9197

Francis R. Sandoval, Principal, GRIDIoT by RCA, SCTE Member
francisrsandoval@gmail.com
+1-720-338-1988

James Sandoval, Architect, GRIDIoT by RCA
sandoval.jim@gmail.com
+1-435-602-0046

Table of Contents

List of Figures

List of Tables

Abstract

In the face of increasing demand for electricity and extreme weather events, the aging electric grid is increasingly failing to provide broadband operators and society at large with safe, low-cost, reliable power. During droughts, sparks from failing power lines start wildfires that disrupt operations and result in loss of life and property. Similarly, during severe heat waves and cold snaps, electricity supply can't meet increased demand and utilities are forced to use rolling blackouts that interrupt broadband services and result in catastrophic losses. Building more power generation, transmission, and distribution infrastructure hasn't resulted in a more resilient grid or more reliable power—but it has raised the cost of electricity. To reliably support broadband operations and enable new business models, what's needed are new solutions that monitor the grid and enable the demand for electricity to be shifted in time to follow the cleanest and lowest-cost supply. Time-shifting creates economic value by discouraging consumption at certain times and encouraging consumption at other times, thereby creating virtual power plants that optimize and extend the life of existing grid assets. Furthermore, time-shifting reverses the supply-follows-demand relationship by allowing flexible demand, such as battery storage, to anticipate and follow supply. The goal of this work is to empower the broadband industry with software-centric technologies that increase network reliability and reduce the cost of broadband operations while spearheading profitable business models that scale quickly to modernize the global electric utility ecosystem while reducing harmful heat and carbon emissions.

1. Introduction

It is evident that severe weather and the ongoing electrification of the world will cause the global demand for electricity to increase by nearly 2/3 through 2040.[i] One might argue that the increased use of renewable generation will decrease the cost of electricity, but there is mounting evidence that without modifying the way electricity is distributed and used, increases in renewables can lead to higher costs.[ii] [iii] [iv] [v]

Case in point, today's energy management technology uses storage and time-of-use pricing to control load. Yet, the increased demand for cheap electricity can cause grid congestion when prices are low and then raise prices to unreasonable highs when energy is less available, as in the February 2021 Texas Power Crisis.[vi] It has become evident that load control technologies need to evolve to provide cost effective energy management. Moreover, it has been suggested that network-enabled virtual power plants that aggregate renewables, batteries, and flexible loads could be orchestrated to mitigate grid congestion.[vii] [viii] [ix]

Indeed, in a multi-industry approach, all stakeholders will have to take measures to better manage energy generation, procurement, distribution, and use. Furthermore, the U.S. Department of Energy's latest play for connected communities and consumer-side energy management will necessitate new communications tools to orchestrate operation of the grid. The broadband industry is strategically positioned to help monitor and manage the grid, identify congestion, improve load forecasts, optimize loads, and provide benefits directly to its operations, other industries, and utilities.

2. Load Shaping for Broadband Operations

Much of the increase in the cost of electricity for operations will come from the construction of backup power systems and from charging the exponentially increasing number of batteries throughout the broadband operator infrastructure in electric vehicles, depots, data centers, customer care facilities, and neighborhood power supplies.

2.1. Batteries and Thermal Storage: A Partial Solution

Batteries are increasingly taking on the role of grid-interactive flexible distributed energy resources (DERs). In an instant, and without prior planning, batteries can flexibly switch from charging to discharging, taking power from the grid, or giving power back. Yet, as the broadband industry increases its use of batteries and thermal energy storage, such as water heating and air conditioning, to reduce electricity costs, a new problem will emerge: Without supervisory control, batteries can be charged using any energy resource, not necessarily a least expensive or renewable resource.[x]

2.2. Status Quo in Orchestrating Supply and Demand

To date, the status quo in the orchestration of supply has focused on faster automatic transfer switches that ensure uninterrupted power will be available to many loads in broadband operations such as servers, air conditioning, hybrid fiber-coax (HFC) nodes, and amplifiers. Transfer switches allow backup power to come online quickly in the event of grid outages but do so in a binary on/off fashion, switching batteries and generators on whenever the grid shuts off—and vice versa.

To date, the technology to manage demand has focused on powering only critical loads during grid outages. As such, non-critical loads remain unpowered during outages, thus reducing the loads on batteries and local standby generators. So-called “transactive energy” and “automatic demand response” often have complexities that require close cooperation with utilities, and have promise, but have only seen very limited deployment since their introduction nearly 20 years ago. What’s been missing until now is rapidly scalable technology to continuously orchestrate both supply and demand in real-time across DERs to cost-optimize purchases of electricity from utilities and reduce carbon footprint while improving the resiliency of broadband microgrids.

2.3. Continuous Load Shaping

It should be noted that a distinction in jointly optimizing supply and demand is that the flow of electricity should be considered infinitely variable in time, as opposed to the binary instantaneous on/off operation of emergency backup power that is in widespread use today. More specifically, using an infinitely variable 24/7 paradigm, the load from charging storage is continuously modulated—and even reversed to aid in supply—as batteries cycle between charging and discharging to meet the emergency and the non-emergency day-to-day needs for electricity.

2.4. Wholesale Time-of-Use (TOU) Electricity Pricing

Today, in the U.S. there are some 3,200 electric grid distribution system operators (DSOs) that deliver power to residential, commercial, and industrial consumers. Most DSOs and other large consumers of electricity do not have generation assets and must purchase wholesale electricity from one or more independent system operators/regional transmission operators (ISOs/RTOs) shown in Figure 1.

Figure 1 - U.S. Independent System Operators/Regional Transmission Operators

It is important for broadband providers to understand that within an ISO/RTO geographic area, the wholesale price of electricity varies spatiotemporally by hour and day across tens of thousands of nodal locations in the grid. For example, Figure 2 shows average hourly pricing across all nodes in the Southwest Power Pool (SPP).

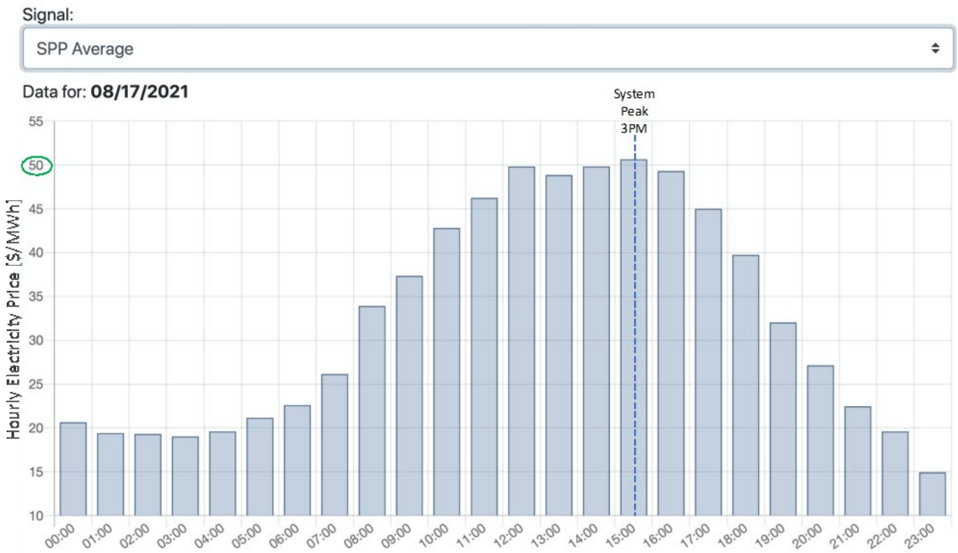


Figure 2 - Hourly Wholesale Electricity Pricing in the Southwest Power Pool

In Figure 2, note the roughly $50/MWh peak price of electricity at 3 PM. Local times are shown in Figure 2 and Figure 3. To provide a sense of spatiotemporal differences across the U.S., Figure 3 shows average pricing in 9 different U.S. regions with peak pricing reaching nearly $100/MWh during the evening in California. In Figure 3, a miniature of Figure 2 is included at the upper left for reference, and the vertical lines at 3 PM aid in comparing differences in regional pricing.

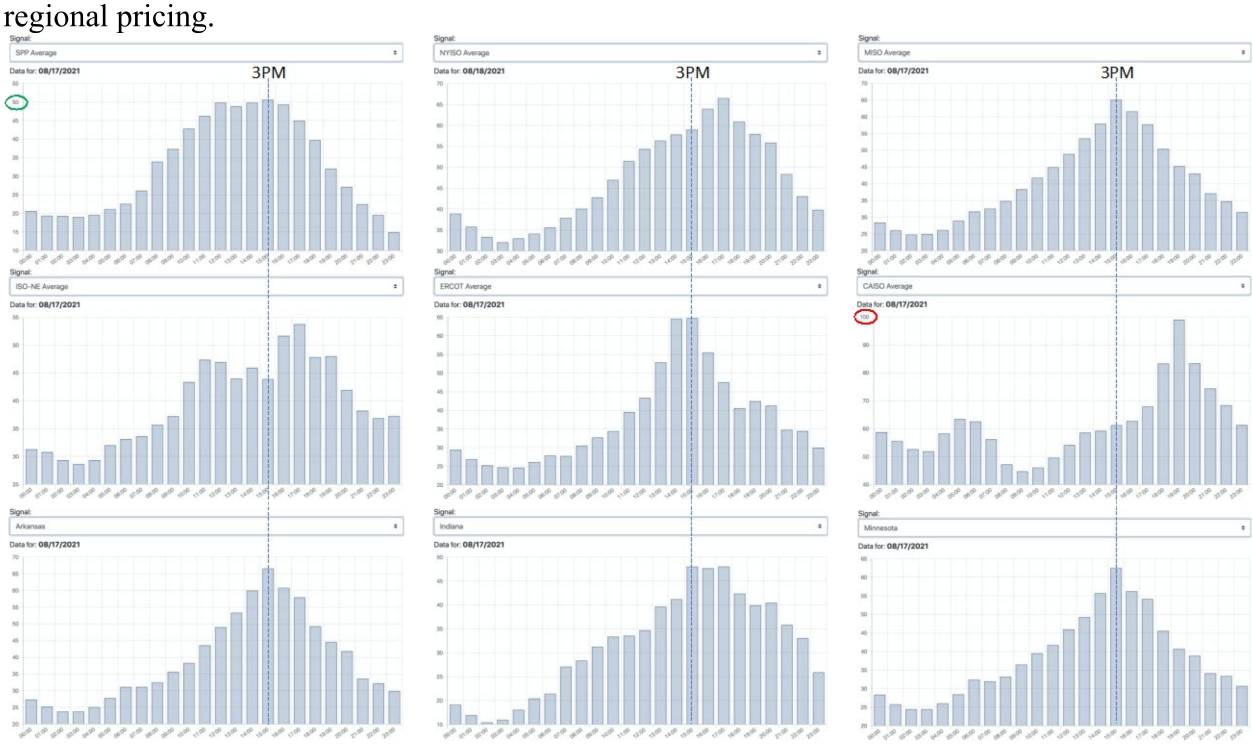


Figure 3 - Hourly Wholesale Electricity Pricing Across 9 U.S. Regions

In Figure 3, note the different shapes and times of peak pricing. By modulating individual loads, broadband operators can shift demand to the times of the day with lower electricity prices and/or lower carbon emissions.

2.5. ANSI SCTE 267 2021 Cost-Optimized Load Shaping

Referring to Figure 2, broadband providers can reduce their electricity cost by purchasing less electricity during the day and more electricity in the overnight, early morning, and late evening hours. To reduce cost, what is needed is a simple and scalable way to shift load away from peak hours to off-peak hours using a cost-optimized load shape as shown in Figure 4.

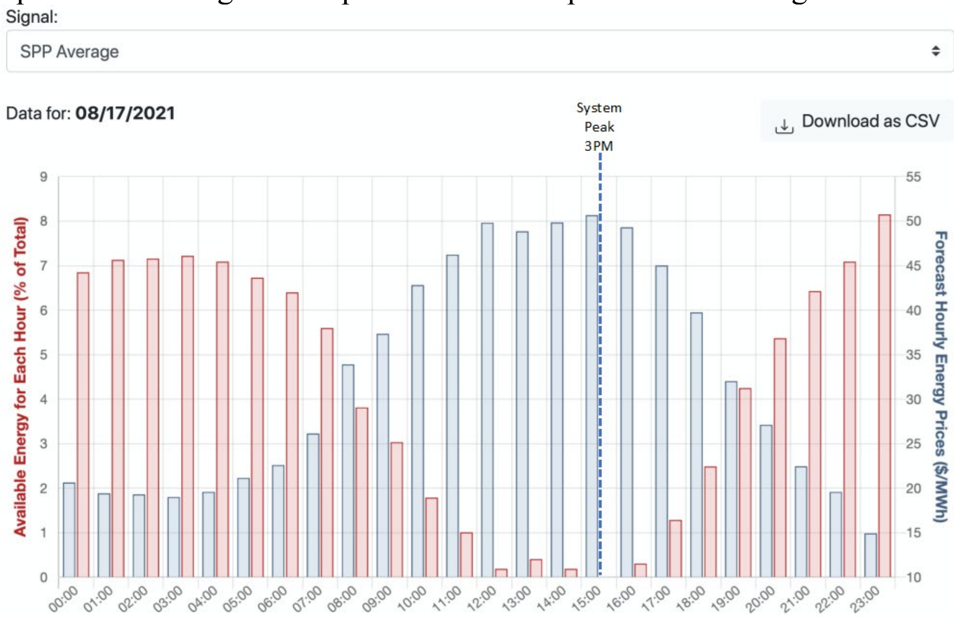


Figure 4 - Example Cost-Optimized Load Shape Based on Hourly Pricing

In Figure 4, the red bars (with the scale at left) denote an example of one possible cost-optimized load shape and blue bars (with scale at right) denote the same hourly wholesale electricity price in the Southwest Power Pool shown in Figure 2. *In* Figure 4*, note the minimization of load during peak hours, which reduces electricity costs.*

Figure 2, Figure 3, and Figure 4 provide insights as to how broadband providers can orchestrate demand to follow the lowest cost supply. To rapidly reduce the cost of electricity for all stakeholders in the energy value chain, a programmable infrastructure was created to harvest ISO data and convert it to an Optimum Load Shape (OLS) signal that complies with the U.S. National Standard ANSI SCTE 267 2021.[xi] For the cost-optimized use case in Figure 4, the newly created OLS server uses ISO day-ahead pricing forecasts to produce a signal that orchestrates demand to follow the lowest cost supply. To simplify and accelerate cross-industry adoption of OLS technology, wholesale pricing and cost-optimized load shapes for nearly 22,000 grid transmission interconnection points covering the vast majority of the U.S. are now available at a single IP Address via an OLS Signal interactive viewer and application programming interface (API).[xii]

For example, broadband providers may use any number of OLS clients that interface with the OLS API, to retrieve forecast optimum load shapes and then autonomously shape their load to reduce their electricity bills and carbon footprint—while also reducing their utilities' electricity production costs and extending the life expectancy of the generation, transmission, and distribution infrastructure.

OLS signals will be increasingly important in the charging of broadband's emerging fleet of electric vehicles (EVs).[xiii] An example of OLS-enabled savings in charging EVs shown in Table 1.

Table 1 - OLS-Enabled Savings

	EV Optimum Load Shape →	Shaped EV Load	Unshaped EV Load	Retail ¢/kWh	Shaped ¢/h	Unshaped ¢/h
Midnight	7.3%	0.73	-	15.1	11.1	0.0
1	7.3%	0.73	-	14.4	10.5	0.0
2	7.2%	0.72	-	14.2	10.2	0.0
3	7.1%	0.71	-	14.4	10.2	0.0
4	7.0%	0.70	-	15.2	10.7	0.0
5	7.5%	0.75	-	15.4	11.5	0.0
6	7.1%	0.71	-	16.8	11.9	0.0
7	The vehicle is in use and unavailable for charging from 0700 - 1800 hours. The charger takes unavailability into consideration and autonomously adjusts the Optimum Load Shape that it received from the supply-side.			19.8	0.0	0.0
8				19.4	0.0	0.0
9				19.6	0.0	0.0
10				18.2	0.0	0.0
11				17.9	0.0	0.0
Noon				16.5	0.0	0.0
13				16.7	0.0	0.0
14				17.5	0.0	0.0
15				18.4	0.0	0.0
16				19.9	0.0	0.0
17				20.1	0.0	0.0
18	8.3%	0.83	7.00	22.2	18.5	155.3
19	9.2%	0.92	3.00	19.1	17.7	57.4
20	8.9%	0.89	-	18.7	16.7	0.0
21	8.3%	0.83	-	18.0	15.0	0.0
22	7.4%	0.74	-	18.4	13.5	0.0
23	7.3%	0.73	-	16.8	12.3	0.0
Totals →	100%	10.00	10.00	Cost→	$ 1.70	$ 2.13
		kWh	kWh	Savings→	$ 0.43	$ 157.03
				20%	per/day	per/year

In Table 1, the EV requires a total of 10 kilowatt-hours (kWh) per charge. Starting at the left of Table 1, using an OLS signal (in purple), the charge controller modulates the rate of charge during all the hours that the vehicle is plugged in and available for charging. Multiplying the rate of charge for shaped load (in blue) and unshaped load (in black) by the hourly retail electricity price results in costs at right. An estimated per vehicle charging savings of 20% is shown at bottom right. Table 1 savings are based on the OLS example in Figure 2 of ANSI SCTE 267 2021.[xi]

3. A New Lucrative Triple Play: Optimization of Load Shaping, Sensing, and Forecasting

Looking beyond broadband operations to new business models, the importance of OLS is that its cost-saving benefits dramatically increase with scale. Soon, most companies and homes will have EV charging stations, and broadband is a logical choice to ensure OLS signals are delivered to these and other electrical devices. In traditional cable TV parlance, think of broadcasting: Time, temperature, and OLS. Table 2 provides a sense of the far-reaching applications of OLS in grid and microgrid use cases.

Table 2 - OLS Use Cases in the Utility Ecosystem

Use Case	Min Gen Cost	Max Asset Utilization	Max RES	Min Energy Charges	Min Demand Charges
1. Generation	●	●	●		
2. Transmission		●			
3. Wholesale Purchaser			●	●	●
4. Distributor		●			
5. End User				●	●
6. Utility-tied Microgrid	●	●	●	●	●

In Table 2, green dots denote the many objectives of OLS such as: minimizing cost and/or carbon emissions; maximizing utilization of generation, transmission and distribution assets; maximizing the use of renewables; and minimizing energy and demand charges. In all use cases, a primary benefit is that OLS client devices can achieve the objectives of any OLS use case, as each client device operates independently of the OLS source.

3.1. Business Model 1: Sell Delivery of Load Shaping Signals

In a new service offering that extends the reach of OLS, broadband operators can distribute the ISO cost-optimized OLS signals (the same signals that are used in broadband operations) across broad geographic areas to commercial and residential consumers, so they can reduce their cost of electricity. Without adding new software or special logic, broadband operators can leverage their existing processes to use managed Wi-Fi routers to confirm that shapes are delivered to connected devices such as batteries, vehicle chargers, water heaters, air conditioners, and commercial refrigeration systems. Like managing DERs in broadband operations, OLS signals modulate the charge and discharge of batteries and other forms of energy storage. In addition, widely distributed OLS signals will allow for new applications, such as OLS-managed battery-backed EV chargers that ensure vehicles are always charged with renewable energy. The "Extending OLS" business model reduces energy costs throughout the energy value chain, and broadband operators can get a portion of savings from utilities.

3.2. Business Model 2: Sell Sensing for Distribution Grid Segments

The distribution portion of the global power grid is sensor-starved and ill-equipped to monitor changes in load that result in grid congestion, overheating, outages, and costly hardware upgrades. What is needed for coordination and control are robust and secure communications which rapidly propagate changes in load to provide utilities with real-time data that quantify grid congestion. Distribution networks are vastly distributed infrastructures; their place in the overall grid is shown in Figure 5, which does not reflect their enormity.

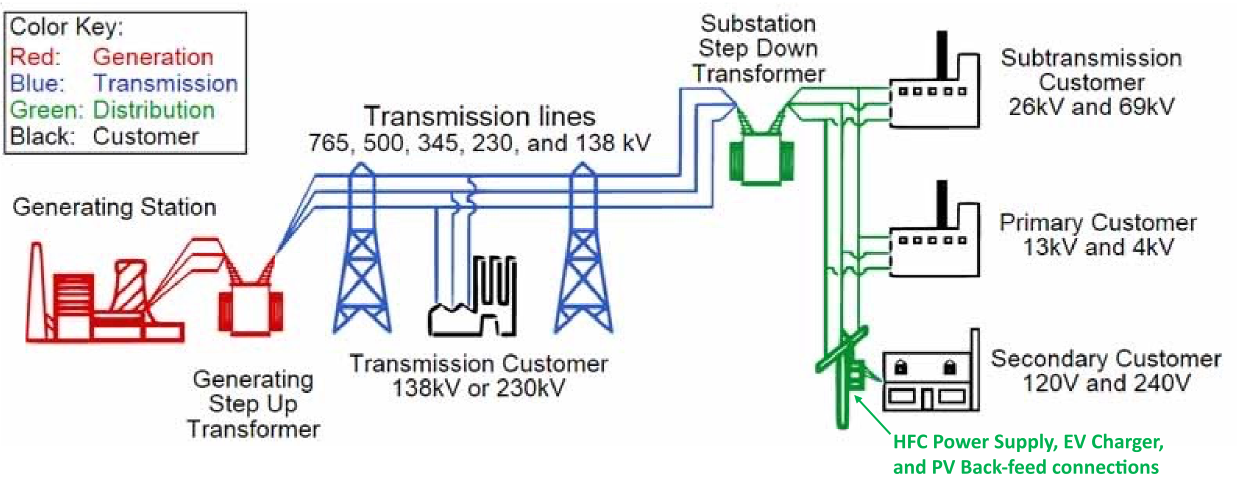


Figure 5 - Grid Pictorial[xiv]

In Figure 5, red depicts generation, blue depicts transmission networks that make up 3.5 % of the grid, and green depicts distribution networks that make up 96.5% of the grid—and require continuous load monitoring as DERs are added. Fortunately, broadband providers have relationships with thousands of utilities each of which maintains distribution networks. In the U.S. alone there are nearly 3,200 distribution networks spanning 5 million miles. Figure 6 provides a sense of the relative shapes and sizes of distribution networks.

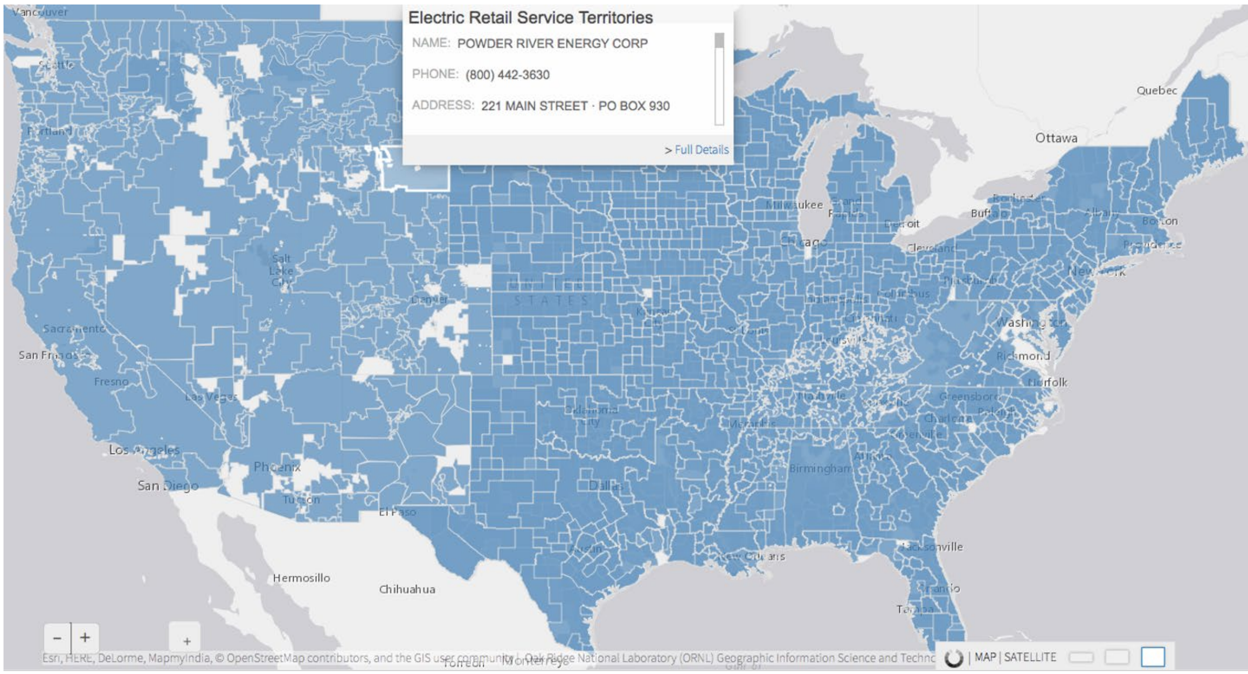


Figure 6 - U.S. Distribution System Operator Territories[xv]

Broadband's capability to provide real-time notification of voltage changes is a perfect complement to the wireless mesh and other network technologies that utilities use to monitor and manage the grid. For example, in the face of increasing cyberattacks designed to cause voltage fluctuations that destabilize and bring down the grid, broadband is the highest-performance out-of-band alternative to assist utilities in monitoring the grid in real-time.

Like canaries accompanying coal miners, the broadband network follows the grid's secondary distribution network everywhere it goes—and already provides early warning signs of some grid issues. Today, all broadband network elements are plugged in to the grid and battery backed, and many act as grid power quality sensors. For example, there are already nearly a million HFC power supply voltage and inverter sensors in the Americas and another million or so throughout the world. A new commercially available innovative grid monitoring application based on existing broadband sensors is already providing tremendous value and is drawing attention from multiple industries and government entities.[xvi]

3.3. Business Model 3: Sell Forecasts of Loads, Flexibility, and Congestion

To efficiently manage grid infrastructure capital expenditures, utilities will increasingly need comprehensive spatiotemporal forecasts of load, flexibility, and congestion at millions of points throughout the distribution network. Broadband operators can leverage the data from sensors to create hyper-local forecasts to sell to DSOs, for example, identifying where EV chargers will be causing dangerous grid overloads and brownouts. Using machine learning—in hierarchical edge and cloud-based signal processing of sensor readings—broadband operators can identify the impact of weather, local habits, and myriad other factors. Forecast errors can be reduced over time, year over year to create Optimal Load Forecasts.

4. Conclusion

The broadband industry faces increasing energy costs and decreasing grid reliability—and can seize the opportunity to implement load shaping to improve network reliability and technical operations. In addition, the broadband industry can build lucrative businesses in load sensing and forecasting that redefine energy management on a global scale. Moreover, as more residences and businesses produce as well as consume electricity (i.e., become prosumers), the connectivity and sensing capabilities of broadband will enable seamless management of efficient energy transactions and uses—thereby supporting current trends in connected communities and customer-side energy management.

The development of new business models will allow for more onsite energy production, distribution, and use of renewable energy sources like wind, solar, hydro, and geothermal power. New business models provide direct tangible economic value in a) load shaping (selling virtual energy and capacity as well as the delivery of OLS signals to the masses), b) hyper-local load sensing (selling data to DSOs), and c) hyper-local load forecasting (selling forecasts to DSOs). New business models also allow utilities to avoid capital upgrades and extend the life of the grid, thereby improving the reliability of broadband and energy services.

It's now or never. New broadband standards and innovations are paving the way for lucrative opportunities in both operations and business development. First, load shaping creates clean and mighty virtual power plants that create economic value by mitigating congestion, favoring renewables, and raising the efficiency of generation to achieve 20% savings in charging EV and facility batteries. Second, sensing of power quality in the grid and HFC networks aids in outage prediction and coordination between utilities and broadband providers—and improves the customer experience and network reliability by streamlining troubleshooting and restoration efforts. Third, forecasting predicts load, flexibility, and voltage sags due to congested power flows. With the right investments and Federal and State grants, standards-based broadband innovations can reduce broadband and other industries' operational and capital expenditures. Indeed, broadband can outperform proprietary solutions in modernizing the grid.

5. Abbreviations and Definitions

5.1. Abbreviations

API	application programming interface
CAISO	California Independent System Operator
DER	distributed energy resource
DSO	distribution system operators
ERCOT	Electric Reliability Council of Texas
EV	electric vehicle
HFC	hybrid fiber-coax
ISO	independent system operator

ISO-NE	Independent System Operator – New England
kWh	kilowatt-hour
MISO	Midcontinent Independent System Operator
NYISO	New York Independent System Operator
OLS	Optimum Load Shape
PJM	Pennsylvania, Jersey, Maryland Independent System Operator
MWh	megawatt-hour
RTO	regional transmission operator
SCTE	Society of Cable Telecommunications Engineers
SPP	Southwest Power Pool
TOU	time-of-use

5.2. Definitions

Optimum Load Shape	A set of numbers that specify the percent of total energy to be used in each time period
time-of-use	A rate for electricity with cost that varies, e.g., by hour of day

6. References

[i] International Energy Agency, World Energy Outlook, 2019, Stated Policies Scenario, https://www.iea.org/reports/world-energy-outlook-2019/electricity

[ii] Getting the Rates Right for a Public EV Charging Build-Out, https://www.greentechmedia.com/articles/read/getting-the-rates-right-for-a-public-electric-vehicle-charging-buildout

[iii] The Paradox of Declining Renewable Costs and Rising Electricity Prices, https://www.forbes.com/sites/brianmurray1/2019/06/17/the-paradox-of-declining-renewable-costs-and-rising-electricity-prices/?sh=7866599861d5

[iv] Why Aren't Falling Renewables Costs Cutting European Energy Market Prices? https://www.greentechmedia.com/articles/read/why-arent-lower-renewable-costs-cutting-european-energy-market-prices

[v] Residential electricity price growth US 2022, https://www.statista.com/statistics/201714/growth-in-us-residential-electricity-prices-since-2000/

[vi] Fix Texas electricity — and hurry! https://www.utilitydive.com/news/fix-texas-electricity-and-hurry/603159/

[vii] Global EV Outlook 2020 – Analysis, https://www.iea.org/reports/global-ev-outlook-2020

[viii] Summary Report on EVs at Scale and the US Electric Power System, https://www.energy.gov/sites/prod/files/2019/12/f69/GITT%20ISATT%20EVs%20at%20Scale%20Grid%20Summary%20Report%20FINAL%20Nov2019.pdf

[ix] Propelling the transition: The battle for control of virtual power plants is just beginning, https://www.utilitydive.com/news/propelling-the-transition-the-battle-for-control-of-virtual-power-plants-i/581875/?%3A+2020-+12-+30+Top+Utility+Trends+%5Bissue%3A31552%5D=

[x] Electric Cars Would Save America Huge Amounts of Energy, https://www.bloomberg.com/graphics/2021-opinion-renewables-will-power-future-of-us-energy/

[xi] Optimum Load Shaping for Electric Vehicle and Battery Charging, https://www.scte.org/standards-development/library/standards-catalog/optimum-load-shaping-for-electric-vehicle-and-battery-charging/

[xii] OLS Blog, https://optimumloadshape.com/

[xiii] Summary Report on EVs at Scale and the US Electric Power System, https://www.energy.gov/sites/prod/files/2019/12/f69/GITT%20ISATT%20EVs%20at%20Scale%20Grid%20Summary%20Report%20FINAL%20Nov2019.pdf

[xiv] Adapted from https://www.researchgate.net/figure/Overview-of-the-traditional-electric-power-system_fig1_321722658

[xv] Cable TV Opportunities in Electric Grid Modernization, Robert Cruickshank, Anthony Florita, Bri-Mathias Hodge., U.S. Department of Energy, National Renewable Energy Laboratory, 2017

[xvi] Gridmetrics Inc., https://gridmetrics.io/

SCTE STANDARDS JOURNAL

Best Practices for the Use of AI/ML in the Mitigation of Video Piracy

An Operational Practice prepared for SCTE by

Matthew Tooley, Vice President of Broadband Technology, NCTA, SCTE Member
25 Massachusetts Ave NW
Washington DC 20001
mtooley@ncta.com
(202) 222-2479

Steve Hawley, Founder & Managing Director, Piracy Monitor, SCTE Member
Seattle WA
steve@tvstrategies.com
(360) 897-6677

Kei Foo, Director of Advanced Video Engineering, Charter Communications, SCTE Member
Denver CO
Kei.Foo@charter.com

Table of Contents

1. Introduction

This is a report on best practices in the use of artificial intelligence (AI) and machine learning (ML) for the reduction of video piracy by consumers. A best practice is a method or technique that has been generally accepted as superior to any alternatives as it produces results that are superior to those achieved by other means.

AI is the broader concept of machines being able to carry out tasks in a way that would be considered 'smart'. ML is a subset of AI-based on the concept of getting AI to accomplish tasks without being given specific instructions. In other words, it is about teaching machines how to learn. There are a few distinct ways that machines can learn – supervised learning, unsupervised learning, and reinforcement learning.

Video piracy is the act of copying[1] video images and sounds that are protected by copyright without the permission or consent of the copyright owner. Video piracy occurs in many forms that include unauthorized sharing of copyrighted video files, unauthorized access to video distribution systems, and unauthorized distribution of copyrighted videos.

Anti-video piracy are the mitigation tools, techniques, and procedures to mitigate video piracy. Anti-video piracy focuses on either identifying the sources of video piracy to prevent the distribution of pirated content or the consumption of video piracy to prevent the end-user from accessing the pirated content.

2. Overview Machine Learning

Machine learning is a subset of artificial intelligence. Machine learning algorithms build a model based upon training data to make predictions without being explicitly programmed to do so. Machine learning approaches or methods fall into three categories – 1) supervised machine learning, 2) unsupervised machine learning, and 3) semi-supervised machine learning.

This report focuses on supervised machine learning as supervised machine lends itself to classifying data and making decisions. Supervised machine learning trains itself on a labeled data set. The training data is labeled with information that the machine learning algorithm uses to build the machine learning model. The labels used by the algorithm to teach the model how to classify data. For example, an anti-video piracy model might be trained on a data set that has data sets that are labeled as pirated video or unauthorized use of a copy and benign video.

Supervised machine learning requires less training data than other machine learning methods. It also makes training easier because the results of the model can be compared to actual labeled results.

Figure 1 is a schematic for a supervised machine learning system. As shown in the figure, a key step is data cleaning to avoid garbage in/garbage out. The next step is feature extraction. From the cleaned data, the data scientist has to identify the individual properties or characteristics in the data set for the machine learning algorithm to use to build the model. A set of features is a feature vector, and the feature matrix is a collection of the feature vectors from the training set for the machine learning algorithm to use to build the model.

---

[1] Note: the copying of video images and sounds are protected by copyright without the permission or consent of copyright owners unless otherwise permitted by law such as fair use or archival purposes.

Once the machine learning model is generated, the data scientist then runs it on a new labeled data set to evaluate how well it performs and tunes the model by selecting different features and/or a different machine learning algorithm. There are many different machine learning algorithms including linear regression, logistic regression, decision tree, random forest, and K-nearest neighbor to name a few.

Once the data scientist is happy with the performance of the machine learning model it can be used to score new data. Again, the new raw data must be processed to extract and generate a feature vector that is then inputted to the machine learning model which scores the feature vector to predict or classify the result. The score is typically a probability between 0 and 1 for the likelihood the new data matches what the machine learning model has been trained to classify.

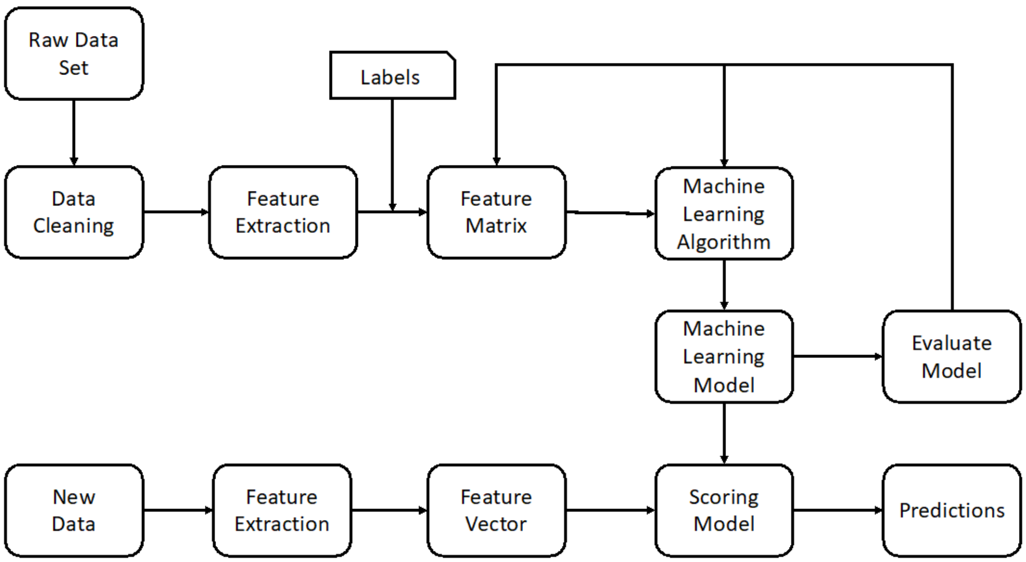


Figure 1 - Supervised Machine Learning System

3. Use Cases

In this report, we describe a set of use cases to illustrate how AI/ML can be used to mitigate video piracy. The list of use cases is by no means exhaustive, nor should they be viewed as normative. The examples described here are to illustrate some of the concepts to provide better context for the best practices described later in this report.

3.1. Fraud Detection

Fraud is one form of video piracy. A subscriber's video credentials can become compromised by video pirates providing the video pirates unauthorized access to the video delivery system. An AI/ML system can be used to monitor and analyze data from the video delivery platform to detect out-of-the-ordinary behavior that is indicative of video piracy. The AI/ML system is trained to look for deviations from defined models. The detected events may then be fed into an operator's Security Information and Event

Management (SIEM) tool for further processing by the operator's security operation center. (Orange - Hello Future, 2020)

Data for the analysis by the AI/ML system could include data associated with users, devices, logins, licenses, and subscriber traffic patterns as means to identify anomalous and suspicious behavior.

3.2. Credential Stuffing/Password Sharing

Another form of video piracy involves multiple users using the same account either due to the sharing of passwords or stolen account credentials from some other data breach as part of a credential stuffing cyber attack. An AI/ML system can be used to monitor and analyze video usage data from the video delivery platform to detect the sharing of logins and passwords outside the home. (Orange - Hello Future, 2020) Indicators of a shared password may include: 1) bandwidth usage that does not match the profile of the customer or out of the ordinary bandwidth usage associated with the customer account; 2) a high number of concurrent video streams for the customer's account; 3) a higher than the normal number of devices associated with the customer's account; and 4) logins from higher than the normal number of geo-locations or from out of the ordinary geo-locations. Other parameters may also be indicative of a credential stuffing or password sharing. It should be noted that some operator's Terms of Service allow for 'whole family' access (such as a family member away at college), which may result in 'false positives' in locations or consumed bandwidth (see section 4.8).

3.3. Identifying Servers Hosting Illegally Sourced Content

Pirated video is hosted and sourced from many locations across the Internet. A repository of URLs can be scanned by an AI/ML system to identify websites that are or likely to be hosting and serving illegally source content. Convolutional neural networks trained with millions of images can identify illegal content by tracking broadcaster logos, producer watermarks, sports jerseys, and various other data points. (Dar, 2018)

3.4. Identifying Pirated Video Streams

Many IP flows have unique fingerprints that are a function of the distribution of packet lengths and inter-packet spacings. Pirated video streams are no exception. The AI/ML system is used to identify IP video streams sourced from pirate servers by analyzing the IP flow's packet lengths and inter-packet timings for patterns that match known pirated video servers. (Tooley & Belford, 2019)

4. Best Practices

4.1. AI/ML Governance

AI/ML development and deployments should have an AI/ML governance plan in place.

The AI/ML governance plan is a framework for how an organization controls access, implements policy, and tracks activities for its models. This includes setting the rules and controls for the machine learning models in production, such as access control, testing, validations, tracing of model results, explainability, model monitoring, reproducibility, and effective documentation and versioning of models.

4.2. Data Governance

AI/ML development and deployments should have a data governance plan in place.

Data governance explains a set of regulations procedures governing the input, manipulation, and use of data in an organization. The governance plan entails the entire life cycle of data processing; which entails data collection, storing, and processing. The data governance process should include policies on the use of data with regards to privacy (e.g., personally identifiable information PII) and security. The governance plan should include classifications that describe the sensitivity of a whole of data asset to help data citizens across the organization understand the business terms, data classes, reference data sets, and governance rules. And finally, the data governance plan should include processes for tracking data lineage to track the data's lifecycle, where it originated, and how it is consumed. In extreme cases of piracy, the data lifecycle could be considered a 'chain of custody' in the event that civil or criminal actions are undertaken against alleged pirates.

4.3. Standards

AI/ML development and deployments should follow applicable, when possible, AI/ML standards.

AI/ML is an emerging technology, and the standards are still being developed in many cases. There are a few standards that have been published and a number of others that are under development.

4.4. Explainability

AI/ML models and their outputs should be explainable. There should be no black box solutions.

All AI/ML models and their outputs should be easily explained. The features that the model used and did NOT take into account in predicting the outcome should be documented and easily understood and validated. One method for validating the features is the use of SHAP (Shapley Additive explanations).

Explaining the features used by the ML model is important as it aids in preventing bias (sampling, exclusion, cultural or stereotype, and measurement).

4.5. Model Monitoring

AI/ML deployments should include model monitoring to protect against data drift.

Model monitoring measures model performance against the actual outcomes to ensure the deployed model works as expected in a real-world environment. ML models should be monitored for data drift. Video piracy is fluid and therefore over time the models can become stale due to shifts in operator product offering Terms and Conditions, environments, changes in consumer behavior, and the behavior of the video pirates.

4.6. Security

AI/ML deployments should be secured using a defense-in-depth approach to secure every level of the application and environment.

A defense-in-depth approach (MovieLabs, 2019) (Streaming Video Alliance, 2020) should be used to secure the AI/ML system both while in development and when deployed. Many ML systems may use sensitive data and may include intellectual property and therefore any data used by the system should be secured both while in transit and while at rest.

4.7. ML Training

Anti-piracy ML systems should use supervised training to minimize false positives.

Supervised training is done using ground truth data. To minimize false positives, the ML model should use supervised training as it is best for classifying data as either pirated or not-pirated.

4.8. Minimize False Positive

The ML model should be optimized to minimize false positives (e.g., maximize the F-score).

To minimize any collateral damage from machine-learning-based anti-video piracy systems, the ML model should be optimized to minimize the false positive or in other words, maximize the F-score.

4.9. Reference Parameters

The ML model should include a set of reference parameters that include account and usage data

Account parameters and usage parameters can be used to tailor and improve the detection of video piracy to identify subscriber behavior that is outside the norms of the subscriber.

4.10. Anomalous situations

The ML model should be able to determine anomalous situations that are outside of reference parameters

As part of training the ML model, the ML model should be trained to look for anomalous behavior that is inconsistent with the account's reference parameters

4.11. Borderline conditions

The ML model should be able to accommodate "gray areas," to accommodate permissible anomalies.

The AI/ML system should score each event and not treat each event as binary. The scoring of the event allows for a human analyst to identify and analyze events that are in the gray areas.

5. Abbreviations and Definitions

5.1. Abbreviations

AI	artificial intelligence
IP	Internet Protocol
ML	machine learning
SCTE	Society of Cable Telecommunications Engineers
SHAP	Shapley Additive exPlanations

6. Bibliography and References

Dar, P. (2018, January 23). *Irdeto is Using Machine Learning in the Fight Against Piracy.* Retrieved May 4, 2021, from https://www.analyticsvidhya.com/blog/2018/01/irdeto-using-machine-learning-piracy/

MovieLabs. (2019). *The Evolution of Production Security - Securing the 10-Year Vision for the Future of Media Production, Post and Creative Technologies.* Retrieved May 4, 2021, from https://movielabs.com/prodtech/security/ML_Securing_the_Vision.pdf

Orange - Hello Future. (2020, March 9). *A control tower against illegal streaming, supported by AI.* Retrieved May 4, 2021, from https://hellofuture.orange.com/en/a-control-tower-against-illegal-streaming-supported-by-ai/

Streaming Video Alliance. (2020, December 14). *Securing Streaming Video.* Retrieved May 4, 2021, from https://www.streamingvideoalliance.org/document/securing-streaming-video/

Tooley, M., & Belford, T. (2019). *Detecting Video Piracy with Machine Learning.* Retrieved May 4, 2021, from https://www.nctatechnicalpapers.com/Paper/2019/2019-detecting-video-piracy-with-machine-learning

SCTE STANDARDS JOURNAL

Video Metadata Extraction in Digital Advertising

A Technical Paper prepared for SCTE by

Srilal Weera PhD
Principal Engineer
Charter Communications
8560 Upland Drive, Englewood, CO 80112-7138
720-699-5079
Srilal.weera@charter.com

Table of Contents

List of Figures

List of Tables

1. Introduction

Video is a ubiquitous medium. From TV and movies to social media and mobile platforms, its applications are numerous in the entertainment sector. The ability to describe what's happening in a video without human intervention is the eventual goal of an AI/ML engine. The usual definition of metadata is "data about data." However, in the context of machine learning, metadata are the "content descriptors" of video/audio/textual data elements extracted from a video. Video metadata extraction is the process of auto-identifying video content.

An emerging trend is the application of AI technology for TV advertising. In this best practices guide, we discuss the unique challenges in applying machine learning to carrier-class video advertising. To illustrate the point, the discussion is focused on a specific use case that is common to all ad supported TV services.

The selected use case is Ad Ingest Quality Control (QC). TV commercials are subjected to various rules and regulations. For example, ads containing specific content (e.g. alcohol, firearms) are barred from airing during certain TV programs. Identifying these categories may pose a challenge to a machine learning tool, as off-the-shelf products are more oriented towards facial recognition. That is to be expected perhaps, as the video ML products were primarily intended for surveillance and sports applications. However, by judiciously combining metadata from multiple data streams, ML based analysis can be enhanced.

This best practices guide consists of two parts. The solution description section contains recommendations based on our experience and the lessons learned. The requirements section defines features a machine learning tool would need to perform for specified tasks.

Machine learning based video analysis is a burgeoning field. As the technology matures, its applications in broadband industry will be far and wide. Network operators and service providers may find the guidelines useful in solution development. Vendor partners who are developing carrier-class machine learning solutions may embody these in product specifications.

2. Broadcast Advertising – Constraints

Multi-channel video programming distributors (MVPD) are highly regulated in the US. The term covers not only traditional cable companies, but any entity that provides TV service to consumers via fiber, coax, satellite, DSL or wireless. With the advent of internet-based TV service (also known as OTT), the moniker is modified as V-MVPD (virtual MVPD). Note that in all cases, the content distributors could be responsible for the displayed video content, including advertisements [1]. This places the onus on the content distributor (also known as service provider/network operator), to prevent the "non-compliant" content from reaching the TV audience.

In the context of the present discussion, there is a distinction between TV content and ads. While movies/episodes etc. are originated from mainstream studios (and thus properly vetted), TV ads could originate from a multitude of sources. Therefore it is necessary to identify any non-compliant ads at the Ad Ingest Quality Control (QC) prior to airing. Today, this is done manually by trained individuals. They examine tens of thousands of ads a month and quarantine the failed ones. The challenge is to automate that process with an AI/ML engine embedded within the workflow.

First, we examine the basis for non-compliancy of ads. While reference is made to the US regulatory framework, similar laws apply in other countries. When a TV commercial is deemed non-compliant, the restriction usually stems from one of the three categories below.

a) Regulatory Compliance

The Regulatory constraints are primarily stipulated by FCC [1], but could also be under the purview of FTC, FEC and FDA [2] [3] and [4]. Listed below are some examples of regulatory requirements overseen by federal agencies. See the references cited above for full requirements.

Examples:

- "Broadcasters are responsible for selecting the broadcast material that airs,…including advertisements." [1]
- Ads related to alcohol, tobacco, firearms, gambling, etc. must meet federal guidelines.
- A political ad is required to display a statement from the sponsor for at least 4 seconds.
- An ad may be deemed deceptive for misleading/missing information (truth-in-advertising).
- Ads promoting certain lotteries, cigarettes or smokeless tobacco products are not allowed.
- Ads must comply with loudness mitigation requirements of the CALM Act.

b) Contractual Compliance

Contractual constraints are imposed by content providers such as ESPN. An example would be the restriction on alcohol ads during ESPN Little League World Series program. For a complete list of applicable restrictions, see reference [5].

c) Business/Operational Compliance

These are generally operational guidelines and best practices established by the broadcasters. Being sensitive to audience needs as well as delivering quality content could enhance a company's credibility. One example is "frequency capping" or limiting the display of the same ad multiple times.

3. ML Challenges in Carrier-Class Video Analysis

Identifying the above categories programmatically may pose a challenge to ML tools, as off-the-shelf products are more oriented towards facial recognition. A familiar ML application is creating a "bounding box" around a face and tracking it through a video clip (Fig. 1). Such applications are useful in sports and surveillance; however they are not directly applicable to the MVPD market. The latter requires comprehensive ML analyses of multiple streams (video, audio and textual metadata).

Figure 1- Bounding Box Example
(Photo Credit: Pexels.Com)

3.1. ML Based Video Metadata Extraction – Tool Capabilities

Use of machine learning (ML) for image and video analysis often include face recognition, personalization and recommendations. The list below shows the general capabilities of ML tools in the market.

a) Video/Image

- Face recognition
- Object detection
- Activity identification
- Emotions (smiling/frowning)
- Celebrity identification

b) Audio

- Specific phrases
- Sentiment (positive or negative)

c) Text/OCR

- Transcription of the audio
- Generation of text from product labels

In common usage, machine learning video products do a multi-pass analysis with each pass identifying specific characteristics, such as faces, common objects, celebrities etc. The results are presented as content descriptor metadata (labels). An accompanying “confidence level” indicates the accuracy of prediction. Off-the-shelf ML tools may not meet needs right out of the box, as the video content/ad detection is still a nascent technology. Customizing such products for carrier-class video applications requires a certain amount of post-processing. Otherwise, the results could be tainted with false positives or the tool may fail to identify content adequately (false negatives).

4. Deep Learning Algorithms for Video Classification

Object detection and recognition are classification problems in machine learning. Compared to image analysis, video is inherently complex. While image analysis has only spatial dependence, video analysis involves the temporal component. The statistical algorithms used mainly are support vector machines (SVM), decision trees and k-nearest neighbor (KNN). The current trend however is for neural network-based algorithms. This is mainly due to two drivers: prevalence of large amounts of data for training and the availability of high speed GPUs for parallel computing.

The generic artificial neural networks (ANN) models suffer from accuracy and training time issues and are not able to meet carrier-class video classification requirements. Hence more sophisticated deep neural networks have become the standard. Of these, the convolutional neural network (CNN) is the workhorse and is a powerful image classification tool. While a video is composed of a succession of images, the time dimension makes the analysis more complex.

Recurrent neural networks (RNN) algorithms have been successfully applied to this task. There have been several variants of RNN over the years. For time series analysis, RNN-based deep learning models are the standard technique due to the ability to store events happened in the past. While RNN is capable of analyzing sequences of data, training a machine learning model based on RNN is a formidable task. That's because it is susceptible to "vanishing/exploding gradient" problems during the training phase, when a back-propagation technique is applied. The root cause is the exceedingly small derivative of the "loss function" (or error) during back propagation. To avoid extreme values of the gradients, it is necessary to disregard certain intermediate steps. A solution for this problem is a Long Short-Term Memory (LSTM) algorithm, which is a modified version of RNN. LSTM adds the capability to remember longer time steps without issues, via the use of multiple gates. The flip side is that LSTM is complex to compute.

AI/ML-based video analysis is a burgeoning field with new and improved algorithms. New algorithms are routinely being developed (Fast R-CNN, Faster R-CNN, etc.). These are mainly for improving the speed of analysis as updating millions of parameters (weights and biases) associated with hidden states takes a lot of time.

4.1. Machine Learning Paradigms

Several machine learning paradigms are discussed below.

Transfer Learning – Transfer learning is the reuse of a pre-trained model on a similar, but new problem. The ML engine is first trained with a publicly available dataset and then fine-tuned to suit the specific application. This technique speeds up the weight initialization process and reduces training time of the neural network model.

Federated Learning – The core concept of Federated learning is decentralized learning, meaning that the data stays within each device/domain. This new paradigm is especially suited for training wireless devices as it seems to address the privacy concerns. The algorithm is trained incrementally and locally on the device. The updates are sent periodically to a central server.

Understanding the intricacies of Federated Learning (Fed-ML) would be crucial for service providers. Some of the pertinent questions one may ask are:

- What are the privacy/security loopholes?
- What is the defense against backdoor attacks?
- Are certain models more susceptible for data breaches?
- What are the risks of data reconstruction?
- What service provider obligations exist in a multi-domain Fed-ML model?
- What are the patent encumbrances for operators that deploy Fed-ML?

Explainable AI (XAI) – Deep learning models function more or less as black boxes. A neural network may easily classify a photo of an animal as a cat but may be reticent about why it made that decision. A recent development is explainable AI (XAI), also known as interpretable-AI (with different nuances). The intent is to help open up the black box model. For example, XAI may provide the justification as to why an ML engine has declined a loan application or why a specific product was recommended for a specific customer.

In the case of video metadata usage, the applications span a wide range. The extracted video metadata should align with the aforementioned machine learning paradigms.

4.2. Training a Neural Network

To train a neural network, a good selection of examples and counter-examples is needed, else the machine learning model would be susceptible to overfitting. That is, the model will fit the existing data well, but is likely to fail when it encounters a new instance of the target data. While this is not an issue with common objects (e.g. cars) due to the abundance of examples, it is a challenge for objects with ambiguous signatures (such as fireworks or alcohol). Distinguishing fireworks from similar signatures (bright lights in a dark background), is not an easy task. Similarly, an image classifier may find it hard to differentiate beer from a similarly colored liquid in a bottle (e.g. olive oil).

The need for proper counter-examples becomes more acute as we move from image analysis to video activity identification. This is discussed in detail in the Error Analysis section.

4.3. Test Planning

During the test planning stage, an assessment needs to be made on the number of classes and samples. The similarities and variations/imbalances in classes can affect the engine performance. Generally, the dataset is split in 70:20:10 ratio among the training, test and validation data. It is also possible to forego a separate data set for validation (only 80:20) via k-fold cross-validation with the training dataset.

Fine tuning the model and hyper-parameters yields improved performance of the ML engine. A model-parameter example is neural network weights optimization. Hyper-parameters would include the number of layers, learning rate, number of neurons per hidden layer, etc.

5. Machine Learning Tool Performance

While ML engine performances continue to improve, current detection speeds are slower than real time. For certain tasks, the ML engine may take excessive time for the video analysis (e.g. many minutes for a 30-second ad). One reason could be that the ML engines operate in multi-pass mode. This is necessary because at Ad-Ingest Quality Control, the ML engine works as a gate-keeper. On the other hand, if the intent is to find a single signature (e.g. either guns or alcohol), a single pass would be sufficient.

To improve the speed, one approach would be to reduce the number of categories selected for detection. The ML engine has to perform a classification task per each category. Some categories may not be relevant to the task at hand, although each task consumes time for detection. Another option would be to use faster GPU processors.

5.1. Hardware Considerations

Machine learning engines can be appliances or reside in the cloud. The cloud-based implementation is preferred if the data also resides in the cloud. The appliances would be GPU-based (as opposed to CPU), due to the large number of cores which facilitate parallel computing.

When it comes to benchmarking, NVidia GTX (or similar) products are general purpose engines. For specialized applications NVidia DGX (with thousand TFLOPs of computing speed) could be a choice. Benchmarking a cloud product is trickier due to multiple factors that can affect the performance. Analysis based on statistical results is recommended.

6. Resurgence of Contextual Advertising

In the last two decades, cookie-based user tracking was the primary mode for targeted advertising in digital media. However, the latest privacy regulations (GDPR, CCPA) are making such data collection practices unacceptable. Therefore, advertisers are eager to find alternative means to promote their brands. Contextual advertising is a suitable option as it protects consumer data. However, that necessitates powerful AI/ML capabilities to describe a scene in a video image. Generating descriptive metadata is a challenge. For example, instead of generic labels such as "person/human," the ML tool needs to identify whether a person is young/old, male/female, mood, activity, etc.

6.1. Video Analysis for Contextual Advertising

Activity identification is a burgeoning field of research [6]. Though steadily improving, it is a challenge for the ML tools. Content descriptors (labels) need to be sufficiently descriptive for effective contextual analysis. For the MVPD space, "activity identification" would open up new applications such as identifying a car chase from a video (as opposed to cars in a still image) would offer new ad opportunities. Table 1 below depicts sample activities that are relevant to contextual advertising.

Table 1 - Activity Identification for TV Advertising (Examples)

Dominant Activity	Possible Ad Usage
Cooking	Utensils, cooking classes, kitchen appliances
Car chase	Car ads/repairs, auto insurance
Shopping	Retail store ads
Eating	Food ads, restaurant
Dancing	Clothing, personal care, alcohol ads
Drinking	Alcohol ads
Social gathering	Multiple products
Kids playing	Toys, food and drink ads, medicines, clothing
Sports activities	Sports-related products
Anxiety, Arguing	Pain medications, lawyer ads

7. Error Analysis of the ML Classifier

Measuring the accuracy of an ML classifier is not a straightforward task. The usual definition of accuracy (the number of correct results divided by the total results) may not yield a useful measure. This is due to imbalances in the dataset. To understand this better we need to look at the types of errors to which classifiers are susceptible.

- False Positive – Incorrectly identifying something as a true signature. Examples include: misidentifying a cat as a dog; claiming a file is infected, though it is clean; or categorizing someone as having cancer, when they do not.
- False Negative – Missing a true signature. Examples include: not identifying a picture of a dog as a dog; or failing to identify beer, and misidentifying it as olive oil.

Contrast these with the ideal case of a properly working ML identifier:

- True Positive – Correct identification of an actual signature/object
- True Negative – Correct identification of a false signature/object

In statistical data analysis, False Positives (FP) and False Negatives (FN) are also known as Type-I and Type-II errors. Note the interplay between the error types. Each case is unique, and the severity may depend on business objectives. A compromise may need to be reached between FP vs. FN detection. The ML engine can be trained accordingly.

Confusion Matrix

Confusion or error matrix compares the correct and incorrect predictions made by the machine learning classifier. The entries in the matrix show at a glance how the engine performs.

Table 2 – Confusion Matrix

	ACTUAL VALUE: Positive	ACTUAL VALUE: Negaitive
PREDICTED VALUE: Positive	TP True Positive	FP False Positive
PREDICTED VALUE: Negative	FN False Negative	TN True Negative

With the above definitions, Accuracy becomes

Accuracy = true/ total = (TP + TN) /total

If the training sample batch is not evenly distributed, then the above formula will give skewed results.

Therefore other measures need to be considered.

Recall

Recall measures the prediction rate of true positives, out of all the correct predictions.

Recall = TP / (TP+FN)

Recall is a measure of the sensitivity of the ML classifier.

Precision

Precision is a measure of confidence of the positive predictions of the tool.

Precision = TP / (TP+FP)

The above measures can be adjusted by tuning the parameters of the ML engine. However, increasing one measure will decrease the other.

7.1. False Positives Example

In this example, the tool misidentifies the bright light in the dark background as fireworks (with a high confidence level).

Figure 2 - False Positive – Fireworks

Table 3 – Machine Learning Detection and Error Mitigation

Detected Category	Initial Confidence Level	New Confidence Level
Fireworks have been detected from 00:00:02 to 00:00:03	90%	< 30%

In the appendix a methodology to mitigate this issue is discussed. The third column indicates the updated confidence level after the mitigation is applied.

7.2. False Negatives Example

In this example, the tool fails to identify the alcoholic beverages in the image analysis. However, the term "cocktails" is noted in the audio transcript as depicted in the JSON file (Fig. 3).

In the appendix a methodology to mitigate this issue is discussed.

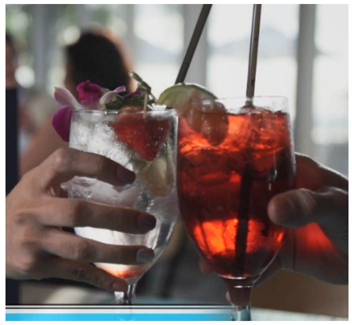


Figure 3 - False Negative - Alcoholic Beverage


```
{
        "id": 4,
        "text": "You can enjoy our hot tub cocktails and R Florida.",
        "confidence": 0.9069,
        "language": "en-US",
        "instances": [
         {
           "Start": "0:00:16.74",
           "End": "0:00:19.82",
         }
        ]
}
```


Figure 4 - JSON file of audio script of the parsed ad

The JSON file in Fig. 4 indicates the word “cocktails” as parsed from the audio transcript. This data is available even though the image analysis failed to recognize that alcoholic beverages were in the video.

False Positives vs. False Negatives – Which is Worse?

The answer actually depends on the specific use case. The ML team needs to assess which is more critical -- missing a signature or tainted results?

The approach we recommend is to treat the former as critical. An example would be accidentally playing an alcohol or casino ad during a children’s program. But at the same time we recognize that a deluge of false positives would make the ML tool unpopular and the users would lose trust.

Another practical consideration is the nature of the output from the ML engine. Usually, it is a lengthy JSON formatted file containing a very large number of entries. Not all predicted values, though accurate, may be significant. In such a case, the calculated errors would be marginally small, leading to inflated accuracy claims. A clear methodology needs to be established before performing the error analysis. A rule-of-thumb would be to count only the events relevant to the task and above a pre-defined threshold value (e.g. 60%).

7.3. Limitations of Current Machine Learning Tools

To improve the detection accuracy, machine learning tools tend to use increasingly sophisticated algorithms. However, the algorithmic approach alone did not seem to produce expected results. Obtaining optimal results within a reasonable time is a challenge. Searching each video frame for a multitude of categories (alcohol, gambling, drugs, violence, trademarks, copyrighted content, explicit content, political content etc.) is time consuming. It could also be irrelevant (i.e. searching for all manners of firearms or medications within a beer ad would be wasteful,).

The appendix section details a method to add a software engine to the workflow to perform additional analyses to enhance the results.

8. Conclusions

Machine learning applications in carrier-class video services is still a nascent field. This best practices guide is to help ML practitioners in the field to appreciate the constraints involved, as well as to develop technical requirements.

Video metadata extraction involves the analysis of multiple streams: image (spatial), video (temporal), audio and textual components. This is because visual analysis alone is not sufficient to make meaningful recommendations for carrier-class video (unlike surveillance or sports use cases). A multi-stream analysis provides a better contextual interpretation.

9. Abbreviations

AI/ML	artificial intelligence/machine learning
DL	deep learning
ANN	artificial neural network
CNN	convolutional neural network
RNN	recurrent neural network
LSTM	Long Short Term Memory
R-CNN	region based convolutional neural tetwork
TFLOP	Trillion floating-point operations per second
JSON	JavaScript Object Notation

10. Bibliography and References

[1] FCC Guidelines for Ads - https://www.fcc.gov/consumers/guides/complaints-about-broadcast-advertising

[2] FTC Guidelines for Ads - https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking

[3] FEC Guidelines for Ads - https://www.fec.gov/help-candidates-and-committees/making-disbursements/advertising/

[4] FDA Guidelines for Ads - https://www.fda.gov/media/82590/download

[5] ESPN Advertising Guidelines - http://www.espn.com/adspecs/guidelines/en/ESPN_AdStandardsGuidelines.pdf

[6] MIT AI Lab research - http://moments.csail.mit.edu/explore.html

Appendix

Machine Learning Tool Requirements for Advertising Use Cases

A.1 Overview

Below is a collection of optional requirements specific to MVPD advertising applications. Network operators and service providers may use these for solution development and RFC preparation. The vendor partners may find these helpful in developing product specs for carrier-class machine learning solutions.

For the initial phase the following limited work-scope could be considered.

- **Ad Ingest QC** – Identify restricted ad content per defined criteria. Develop interfaces to insert/integrate ML engine to the current workflow. The annotated results in the JSON file can be used to generate human readable reports.

- **Ad Classification** – Scan ads in the ad repository and generate metadata for ad cataloging and search. The search criteria and results display mechanism are discussed below.

See Fig. 5 and Fig. 6 for workflows.

A.2 General Requirements

a) Auto-detect and tag the media content by analyzing Video/Audio/Text components.
b) Identify following signatures and supply content descriptors with timestamps as applicable:
   b.1. People, animals and other general objects appearing in the media
   b.2. Provision to add user-defined objects/logos/emblems for the search criteria
   b.3. Sentiment and emotions, underlying topics as well as any anomalies detected
   b.4. Activities happening in the media
   b.5. Copyrighted content and popular trademarks
   b.6. Word phrases, sounds and other audio content that describe the media
   b.7. Length of the video content (e.g. 30 sec ad)
   b.8. Language(s) spoken/displayed
c) Create a searchable index of the metadata derived by Machine Learning (ML) tool.
d) Provide a dashboard with user friendly UI for the Ops staff to search content metadata.
e) Create a workflow to seamlessly integrate machine learning results and data analytics.
f) Support multiple content types and formats. Note that the content can be file-based, stored in an archive, or streaming media.

A.3 Ad Ingest QC – Identifying Non-Compliant Content

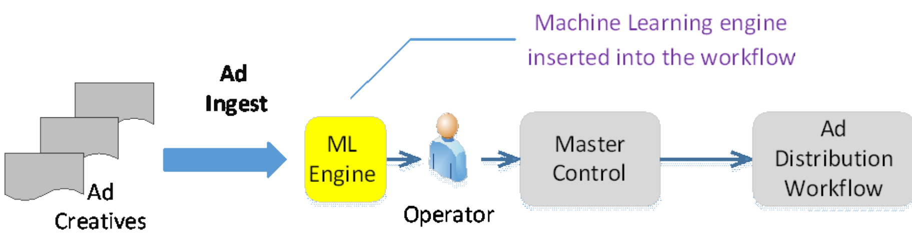


Figure 5 - ML tool usage in ad ingest QC and classification

a) Scan ads at ingest and generate descriptive metadata.
b) Create a summary of each ad content.
c) Tag the identified ads per IAB Content Taxonomy Mapping system: www.iab.com/guidelines/taxonomy . Use the hierarchical JSON format.

```
"26.3.3.7":{
   "Technology & Computing":{
     "Computing":{
        "Computer Software and Applications": "Digital Audio"            }
    }
  }
```

d) Screen ads for restricted content. Flag the non-compliant ads for further processing: The table below shows restricted content in a typical (hypothetical) case.

Table 4 – Non-Compliant/ Restricted Content

Restricted Category	Requirement Importance	Comments/Examples
Alcohol	High	Beer, wine, hard liquor or variants, including those with non-descriptive names (“***Bud Light Lemon Tea***”).
Tobacco	High	Cigarettes, E-cigarettes, cigars, vaping
Drugs	High	Includes drug paraphernalia
Gambling, Casino	High	
Copyrighted content	High	Visual and/or audio track (songs, movie soundtracks)
Trademarked content	High	College brand T-shirts, logos and emblems
Explicit Content	High	
Curse/Swear words	High	Profanity in ads is not allowed
Sexual products	High	
Violence	High	Guns, explosives, physical violence
Competitor content	Medium	
Political Content	Medium	(Hard to detect, but see below for plausible signatures*)

<u>Note</u>: For political content the following FEC requirement may apply: "…a "clearly readable" written statement that appears at the end of the communication, for a period of at least four seconds"*.
https://www.fec.gov/help-candidates-and-committees/making-disbursements/advertising/

e) Screen ads for quality issues (video jitter, macro blocking, audio clipping etc.)
f) Provide audio transcript of the media content emphasizing key words/phrases.

A.4 Ad Classification – Cataloging Ads in a Repository

a) Scan ads in the repository and generate descriptive metadata to classify the ads.
b) The metadata may be in the form of human readable "labels" in the UI/Dashboard.
c) The metadata may be in the form of JSON/text output files for programmatic analysis.
d) The metadata may summarize the ad content to enable cataloging.
e) The labels may be prioritized to better describe the ad content, as appropriate.
f) Use a search engine capability to parse ad metadata.
g) Given specified criteria, locate and retrieve matching ads from the ad repository.

A.5 Video Content Analysis Pertaining to Ads

a) Descriptive Metadata – Scan videos and generate descriptive metadata. Identify sentiments, underlying topics as well as any anomalies in the media content.
b) Searchable Catalog – Create a searchable catalog of videos based on tagged content.
c) Ad Recommender – Analyze video content and recommend ad opportunities for Contextual Advertising, including sentiment analysis.
d) Segmentation – Generate logical video segmentation boundaries and identify dominant activity (e.g. fight scenes, car chases, songs).
e) Thematic advertising – Given an ad-campaign theme (e.g. eco-tourism), find matching videos from the collection. Find effectiveness of ads by different demographics/audiences.
f) Video Tagging – Screen video content for quality issues and tag accordingly.
g) Celebrities - Find videos of a given actor, including duration/time stamps, from a collection.
h) Closed captions – Translate speech to text for assets that currently do not have captions.

A.6 Reporting Requirements

a) Generate a pdf file containing the detected instances marked with screenshots, bounding boxes and time stamps.
b) The report may provide high-level and detailed-level data.

High Level – Aggregate and summarize the detections. Provide video, shot and frame level annotations. Provide audio transcript and summary of visually identified text (optical character recognition).

Detailed Level – Provide detections with counts (number of occurrences), durations or presence percentages (e.g. the occurrences per GoP (group of pictures) expressed as a percentage). Provide a detailed report of each identified signature (e.g. alcohol) along with thumbnail photos, start/end times, durations and confidence levels. The screen shots of interest may contain annotated bounding boxes to indicate the detections.

c) In addition to the above, a low-resolution version of the annotated video, with overlay bounding boxes is recommended (useful when a quick view of the detections is needed).
d) In addition to static reports, an active dashboard GUI with clickable labels (to indicate each occurrence on a time line).

A.7 Performance Requirements

a) Ability to process video content in near real-time (or within a specified delay).
b) Ability to process multiple files simultaneously.
c) Ability to prioritize ML job processing (beyond best effort/round robin modes).
d) Ability to meet specified latency requirements.
c) Ability to meet audio/video quality requirements, such as MOS, PSNR, SSIM as well as perceptual video quality.

A.8 Product Integration and Workflow Requirements

The machine learning classifier engines in the MVPD space are usually vendor developed and then customized for clients. One pitfall is that usually more emphasis is given to fine tuning the ML engine and less consideration is given to product integration. Both aspects are important.

A detailed assessment of ML module integration into the ad processing workflow is necessary prior to the production testing stage. Generally, this would cover interfaces, reliability/failover scenarios, data processing, performance and CDN integration. Fig. 6 depicts this at high-level.

The output of the ML engine (audio, video and textual analyses results) is usually in JSON format. This raw data need to be converted to a more presentable format for human consumption. APIs also need to be configured for M2M communication with analytics engines, dashboards, etc.

a) **Report generation** – A pdf file containing the detected instances marked with screenshots and time stamps is recommended. A video overlay with bounding boxes is also desirable. An active dashboard GUI with clickable (hyper-linked) labels (depict each occurrence with time stamps) is a nice-to-have feature.

b) **Workflow integration** – Interfaces should be developed to insert/integrate ML engine to the existing workflows. A parallel process (vs. in-line), is recommended since the ML analysis speed is not close to real-time. The intent is to prevent any impact to the normal (non-ML) workflow functioning. While the workflows are generally in a single provider cloud, a hybrid-cloud scenario could also be envisioned (see Fig. 7).

c) **Interface development** – Interfaces should be developed to transfer JSON metadata to another module such as ad campaign manager or analytics engine.

API/Interfaces should be created as necessary for ad ingest and ad database classification scenarios:

- Auto-ingest feed of video clips to ML classifier engine
- Metadata output from ML engine to an ad campaign manager
- Ad Ingest – Metadata output from ML engine to GUI dashboard and other analytics systems
- Ad Classification Use Case – ML output metadata to be linked to an analytics/search system

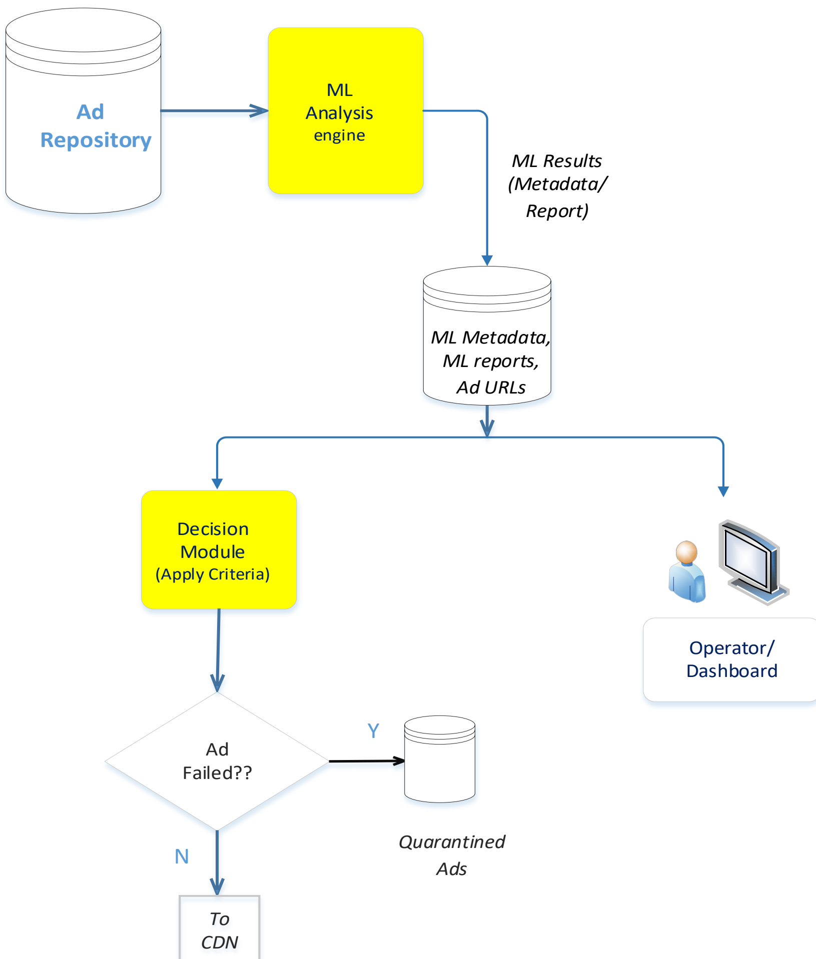


Figure 6 - Ad Classification Workflow

A.9 Cloud and API Requirements

a) Automated ML engine workflow integration should be configured for the following cloud scenarios:
   - Single cloud – Data resides on the cloud (or copied to). ML engine is located on the same provider cloud.
   - Hybrid (multi-cloud) – Data resides on the provider-1 cloud and copied to a different provider-2 cloud where the ML analysis is performed.

In each case the results are sent back to specified local servers.

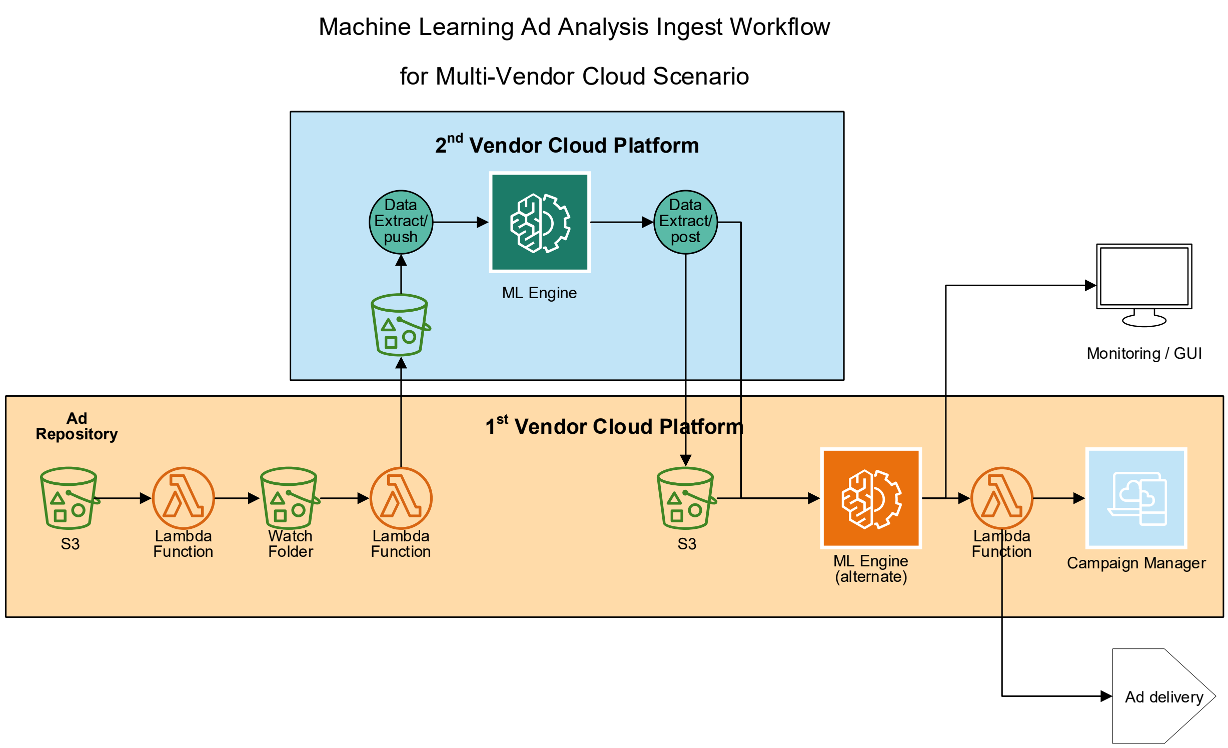


Figure 7- ML Ingest Workflow for Multi-Vendor Cloud analysis

(Note – The diagram shows AWS components for illustrative purposes, however it is applicable to any other cloud vendor product)

A.10 User Customization

a) It is important that the user is able to add custom objects to the ML analysis criteria. Examples would be product logos, new type of beer in the market, drug paraphernalia for detection.
b) If the tool has no provision for user customization, then the option for the modification to be effected via the vendor ML team may be provided.

SCTE STANDARDS JOURNAL

Streamlined Onboarding: Simplified and Secure IoT Device Management

Leveraging Wi-Fi Easy Connect to Onboard Open Connectivity Foundation Devices

A Technical Paper prepared for SCTE by

Andy Dolan, Senior Security Engineer, CableLabs, SCTE Member
858 Coal Creek Circle
Louisville, Colorado 80027
a.dolan@cablelabs.com

Kyle Haefner, Ph.D., Lead Security Architect, CableLabs, SCTE Member
858 Coal Creek Circle
Louisville, Colorado 80027
k.haefner@cablelabs.com

Darshak Thakore, Principal Architect, CableLabs, SCTE Member
858 Coal Creek Circle
Louisville, Colorado 80027
d.thakore@cablelabs.com

Craig Pratt, Lead Security Engineer, CableLabs, SCTE Member
858 Coal Creek Circle
Louisville, Colorado 80027
c.pratt@cablelabs.com

Table of Contents

List of Figures

List of Tables

1. Introduction

The widespread adoption of the Internet of Things (IoT) has made smart devices ubiquitous in many different environments, including homes, offices, and industrial settings. As has been the case over the last decade, more IoT devices continue to be brought into these environments each year, with current projections predicting that over 14 billion IoT devices will be installed and connected by 2023, 17 billion by 2025, and over 25 billion by 2030 [1], [2]. There are well-known sets of security topics now inherently associated with IoT, from distributed denial of service attacks (botnets) that have had major impacts on large portions of the Internet to privacy and network intrusion risks. There is accordingly a well-established body of research that addresses these concerns, as well as emerging solutions in the IoT market that aim to improve the security aspects of IoT for end users and practitioners of IoT applications [3]–[5].

1.1. Problem Space

Amidst these changes, however, exists the persistent challenge of end user experience in device setup and management, which is often complicated by the variety of management solutions that are specific to the ecosystems of individual devices. Each of these management solutions may offer different capabilities and approach the initial bootstrapping of trust differently. To set up two devices from different vendors, users are commonly required to download two separate management applications. Each of these applications may implement a different method for bringing the respective device onto the user's Wi-Fi network separately; for example, one may provide the device with Wi-Fi credentials directly over Bluetooth, while another may first leverage the user's mobile device to act as a temporary access point (AP) across which it can provide these details. Apart from the setup and management of devices, it is also often the case that different devices are not interoperable with one another, adding yet another challenge.

From the user perspective, managing and maintaining a home IoT environment with various devices can be overwhelming, and maintaining a consistent security posture in the home is accordingly difficult.

Existing work has aimed to address individual aspects of these challenges. To facilitate more secure and simplified association to Wi-Fi networks, the Wi-Fi Alliance has recently developed Wi-Fi Easy Connect, also known as Device Provisioning Protocol (DPP) [6]. Under this new standard method of Wi-Fi network association, a device can easily be connected to a Wi-Fi network by the user through a single action, such as the scanning of a QR code. A brief overview of the Easy Connect protocol is detailed in section 2.2. The Open Connectivity Foundation (OCF) has created a standard framework for the secure management and interoperability of IoT devices, including the introduction of devices into an OCF ecosystem [7]. Further details on OCF are provided in section 2.3.

1.2. Use Case

While these new approaches to IoT device onboarding and management provide better user experiences that also prioritize security, they operate at independent layers and still require the user to apply onboarding actions at each layer. Ideally, users should be able to start seamlessly and securely interacting with new devices almost immediately after introducing them into their home environment, with a minimal set of actions required. This should take the form of a single administrative action taken by the user to introduce a new device into their home IoT ecosystem, both in terms of connecting it to their home network and onboarding it into their established IoT management domain. Not only should this single action be simple and intuitive for a user to execute without requiring any additional applications, it should also provide sufficient security that ensures that each device is provisioned with unique credentials for the network and the IoT ecosystem.

To drive support for this style of IoT device onboarding and management among a diverse set of IoT devices and home network systems, this solution should manifest as an open standard and be built upon other open standards and protocols. This can ensure that IoT devices and networks that implement these mechanisms are able to provide a streamlined onboarding experience without any need of additional applications or proprietary integrations.

1.3. Solution Overview

In this paper, we describe the fundamental procedure of *streamlined onboarding*, and present the specific architecture that combines Easy Connect and OCF as an example implementation. We first provide a brief overview of the current practices in IoT device onboarding, as well as background on both Wi-Fi Easy Connect and OCF. We then provide an overview of streamlined onboarding in generalized terms, as well as the specific example of streamlined onboarding that combines Easy Connect and OCF, including an implementation overview. Finally, we offer some discussion on the core benefits of this architecture, as well as other areas that this approach to bootstrapping of device trust could also be applied.

2. Background

2.1. Current State of IoT Device Onboarding

In the current home IoT market, the installation and setup process for any particular device often requires a significant amount of direct interaction from the user. Once a device has entered its operating environment, a user needs to provide the device with their home network details so that it can associate to the Wi-Fi network, as well as other device-specific configuration information, including provisioning for interactions with other compatible devices.

As many devices have limited (if any) inputs and outputs for users to provide or receive information, a common solution has been to require that users interact with the device through their smart phone, which acts as a proximal interface to the device. However, this interface is often a specific application released by the device vendor, requiring the user to download and install a new application before being able to use the device. Once installed, the connection made from the phone to the device often takes the form of a Bluetooth connection established with the device, or a temporary Wi-Fi network broadcast by the device to which the user's phone can connect. Over this established connection, the user is able to enter Wi-Fi network information through the app and bring the device onto the network. Once the device has associated to the Wi-Fi network, the user is able to provision the device, which may include associating it with a user account, configuring operational settings, and configuring permissions for other devices to interact with it. This is also typically done through the vendor-specific application.

The reality of this current state of IoT onboarding is the inevitable requirement for users to navigate several different applications to manage IoT devices of different vendors, as well as a significant amount of overhead to provision network credentials to devices before they can even be configured at the IoT application level. Even though these extra requirements exist for the user, they still commonly result in sharing a single Wi-Fi passphrase across many different devices. This implies that the compromise of one device necessitates resetting the passphrase for all other devices on the network, yet another burdensome task for the end user.

2.2. Wi-Fi Easy Connect (Device Provisioning Protocol)

The Wi-Fi Alliance (WFA) has developed the Wi-Fi CERTIFIED Easy Connect™ protocol to reduce the complexity and enhance the user experience of connecting devices to Wi-Fi networks and incorporates latest cryptography to provide the highest available standard of security. The WFA Easy Connect protocol enables secure transfer of device credentials and additional configuration data to new devices on both home and enterprise networks without requiring complex infrastructure. The WFA Easy Connect protocol also provides per-device credentials, mutual authentication, and secure device-and-group level identification. The protocol is specifically targeted for headless IoT type devices (e.g. door bells, light bulbs, cameras etc.) but it can also be used for onboarding general purpose devices like tablets and laptops. We have provided a more detailed overview of Easy Connect and its benefits in [8].

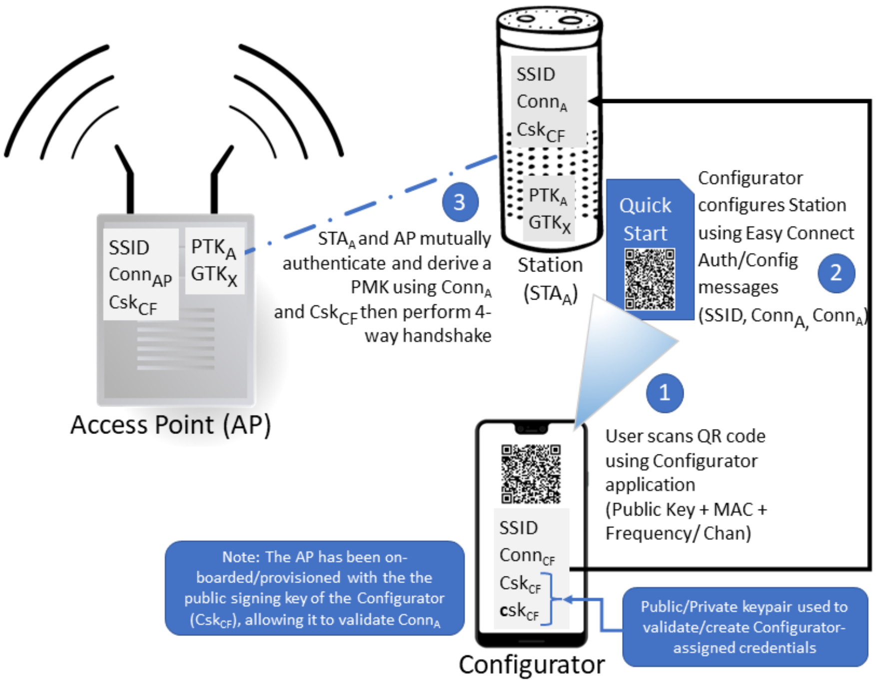


Figure 1 - Overview of QR code-based Easy Connect Protocol

Figure 1 provides an overview of the Easy Connect protocol. In the Easy Connect framework, the device that needs to be onboarded is called the "Enrollee" and another device or entity performs the role of a "Configurator." The Configurator communicates with the Enrollee using the Easy Connect protocol to establish a secure channel and then provision the Enrollee with the Wi-Fi credentials and any additional configuration data that the Enrollee needs to become operational on the network. In order for the Configurator to discover the Enrollee and to ensure that it is communicating with the correct Enrollee device, the Easy Connect protocol specifies a "bootstrapping" step by which some information about the Enrollee is provided to the Configurator. The bootstrapping step can be performed in a number of different ways depending on the type of Enrollee, but the most common mechanism is to scan a QR code on the Enrollee through a mobile app and retrieve the bootstrapping information from the QR code. This simplifies the way by which users can initiate the Easy Connect protocol and then automatically have the device connect to their network.

The Easy Connect protocol itself has been designed to be extensible and allows for additional data besides the Wi-Fi configuration to be exchanged securely between the Enrollee and the Configurator. This provides a flexible mechanism for other protocols and applications to "piggyback" over the secure channel provided by Easy Connect to transfer application specific information securely.

2.3. Open Connectivity Foundation (OCF)

The Open Connectivity Foundation (OCF) is a certified International Standards Organization (ISO) and International Electrotechnical Commission (IEC) internet of things (IoT) standard that focuses on secure interoperability of devices across all vertical industries. The OCF specification is the result of several years of work from hundreds of companies that span the industry from device manufacturers and software vendors, and Internet service providers.

OCF is an application layer protocol and builds on lower layers that provide message transport, session, encryption, and discovery. Because OCF is agnostic to the underlying physical layer and transport layer it can run over anything that supports IPv6 connectivity including Wi-Fi, Bluetooth, and Thread [9].

OCF uses the well-established client-server architecture in which a device can act as a client (requestor of information) and/or a server (supplier of information or actions). Servers have resources (information or actions) that can be requested by clients. Seen in the example depicted in Figure 2, a lightbulb can act as a server in which its resources are the states of the light, on/off, dimming, color etc. A client in the form of a light switch acts on the lightbulb's resources through requests to issue commands to the lightbulb.

All communication between clients and servers is accomplished using a REpresentational State Transfer (REST) approach by which the client requests information from, or sends a command to a particular resource, e.g. the state of the light – true (on) or false (off). All operations are done using the Create, Retrieve, Update, Delete, Notify (CRUDN) conventions to interact with resources. All requests are constructed in JSON and transferred over the wire using Concise Binary Object Representation (CBOR) encoding to reduce the size of the message payloads, and OCF uses the constrained application protocol (CoAP) [10] for transport of messages. CoAP is a service-layer protocol that is suitable for resource-constrained internet devices.

In the OCF model every request after a device has been onboarded is encrypted and all connections between clients and servers are mutually authenticated. Additionally, each request is authorized by sets of access control lists on the server that check to verify that the client has the correct permissions to access the resource. If everything checks out, then the server responds with the requested information or performs the requested action.

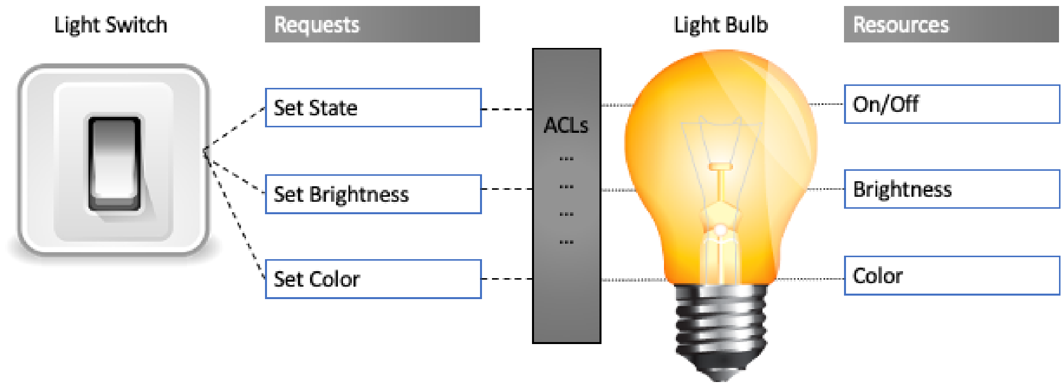


Figure 2 - Example of OCF Device Operations

2.3.1. *Lifecyle of a Secure IoT Device*

The lifecycle of an IoT device, illustrated in Figure 3, can be broken into two main stages, unowned and owned. An unowned device is like a device that has just been removed from its packaging. To add the device to your smart home you must take ownership of the device, i.e. bring it onto your network and give it credentials and permissions so that it can interact with your other devices.

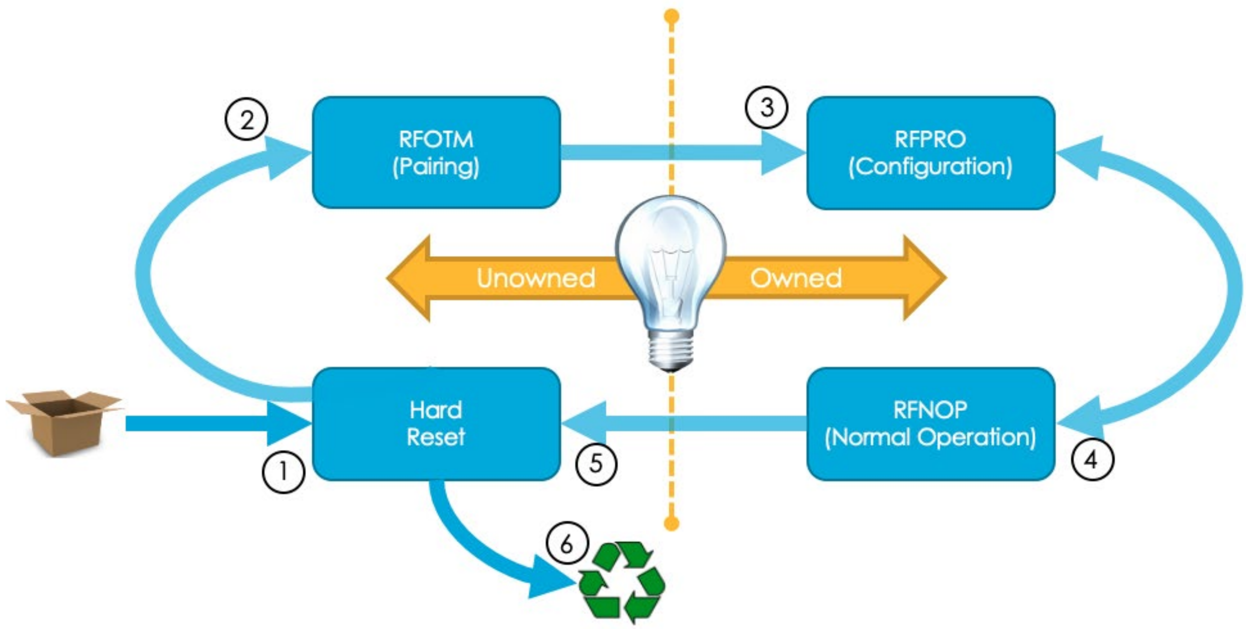


Figure 3 - Overview of OCF Device Lifecycle

This step is also referred to as onboarding. The complete lifecycle states of an OCF device is listed below:

1. **Factory New/Reset**
   When you bring home a new device, take it out of the box, and plug it in the device starts in a clean-slate mode where all settings are the manufacturer defaults.
2. **Pairing Mode**
   Once the device boots up, it enters a pairing mode called Ready For Ownership Transfer Method (RFOTM). This pairing mode allows you to scan the network and see (discover) the new device. Once you find the new device, you can select it and set it up. This setup configuration is done with a configuration tool called the Onboarding Tool (OBT) which is the primary piece of software that is used to configure an OCF network. Once the device exits pairing mode, it is considered "owned" and has all of the necessary credentials for the administrator to configure it.
3. **Configuration**
   Once ownership of the device is established, the device can then be configured. This configuration is done in the Ready for Provisioning (RFPRO) state. This is the state where further operational credentials are configured, and access control is defined. The device can return to this state as necessary when additional configuration is needed.
4. **Normal Operation**
   After the device is configured, then the device transitions to the Ready for Normal Operation (RFNOP) state. The device will spend the majority of its time in this state. As described above, when the device requires additional configuration (e.g., provisioning to operate with other devices, starting software updates), it is first transitioned back to the RFPRO state, and then transitioned back to the RFNOP state when configuration is complete.
5. **Hard Reset**
   When the device has reached end-of-life or ownership of the device will be transferred, the device should be hard reset. This erases all of the configuration on the device, including Wi-Fi and operational credentials, roles, routines, etc. Hard reset is a clean erasure of the device.
6. **Transfer or Recycle**
   The device has now returned to a factory default state where it is unowned and can be re-owned and incorporated into a new smart-home environment or safely recycled.

3. Streamlined Onboarding

In this paper we propose and demonstrate the concept of streamlined onboarding in which the network layer onboarding process and the application layer onboarding process work in unison to provide a seamless and secure onboarding experience to the user. From the user's perspective, their "out-of-the-box" to "device operational" setup is a single-step experience.

At its core, streamlined onboarding involves conveying streamlined onboarding information for use by the IoT management system across a separate layer that is referred to as an Out of Band (OOB) channel. While this OOB channel can take a variety of forms, we focus on the network onboarding process as the OOB channel. This information that is provided over the OOB channel is used to identify and authenticate the new device as it is added to the IoT management system. Under this scheme, a device automatically provides its streamlined onboarding information while joining the network, effectively making the components that provision the network aware that the device is ready to be onboarded into the IoT management system.

The network components relay this information to the IoT management system through a special component known as a diplomat, which understands how to communicate with both the OOB channel and the IoT management system. Once the information is received from the diplomat, the IoT management system discovers the device using the identifying information provided over the OOB channel and onboards the device, authenticating it using the authentication information provided over the OOB channel. For the user, the single action of starting the network onboarding process brings the device onto both the network and the IoT management system, ready for further configuration and use.

To achieve this concept of streamlined onboarding applied to IoT device management in the home context, we combine the secure provisioning of Wi-Fi network credentials via the Easy Connect protocol with the secure IoT management and interoperability framework of OCF. In our architecture, Wi-Fi Easy Connect serves as the OOB channel that communicates, as part of the network association of a device, application-level OCF information that is used to establish trust between that device and an existing OCF domain. Easy Connect provides an excellent example of an OOB channel for streamlined onboarding for three reasons: it is secure; the device is first authenticated before the channel is established; and no additional steps are required of the user to facilitate the channel. The resulting architecture allows a user with an established OCF domain to simply scan a QR code to bring a new device both onto their network and into their IoT ecosystem. With this single action, the new device is provisioned with credentials for the network, and brought into the OCF domain where it can be managed through the OCF standard. To bring streamlined onboarding to fruition, CableLabs has contributed to the open specifications for both Easy Connect and OCF, creating a solution that is seamless, simple, and more secure for the user.

4. Detailed Architecture

4.1. OCF Streamlined Onboarding

4.1.1. OCF Components

Under OCF, streamlined onboarding information is transferred over the OOB channel (and any facilitators of the OOB channel) to the diplomat, which is modeled as an OCF resource. The diplomat conveys the information received from the OOB channel to the domain's onboarding tool (OBT) in a publish/subscribe fashion. In OCF terms, the streamlined onboarding information for a single device consists of the device's universally unique identifier (UUID) to identify the device, as well as a credential that the OBT can use to authenticate the device when taking ownership of it.

The diplomat can be architecturally implemented in a number of different ways. It can be a component of the OBT application or a standalone entity. In the architecture described in this paper, we have implemented the diplomat as a standalone entity; in practice, the diplomat can be thought of as the OCF-aware component of the OOB channel. For example, a diplomat may be a software component of a Wi-Fi access point. When the diplomat is a standalone entity, a one-time configuration step is needed to establish a trust relationship between the OBT and the diplomat. To achieve this, the diplomat is onboarded, as any other OCF device is, into the OCF domain through the process described in section 2.3.1. The OBT then indicates to the diplomat that it would like to receive notifications of new devices to onboard by subscribing to updates from the diplomat resource through an OCF OBSERVE request. Once this configuration is complete, the diplomat will notify the OBT of all new devices that should be onboarded going forward.

The diplomat serves as a translator between the OOB channel and the OCF standard. The way in which the diplomat receives information from a particular OOB channel is an implementation detail of the specific diplomat. For example, a Wi-Fi access point may send a software-based event with streamlined onboarding information that the diplomat component of the access point detects. Once the diplomat retrieves the information about the device to be onboarded from the OOB channel side, it provides the information to the OBT through an OCF NOTIFY message. OCF leverages confirmable messages to ensure that the new device notification will be reliably delivered to the OBT, even if the OBT is absent or unreachable for a period of time (e.g. OBT is out of the home).

4.1.2. Streamlined Onboarding Flow

As described in section 2.3.1, the standalone OCF device enters pairing mode (RFOTM) after booting up and waits for the OBT to discover the device. This requires the user to initiate the discovery and choose the correct device on the network. This adds more steps for the user to perform and more opportunities for the user to make a mistake. Under streamlined onboarding, the UUID that was provided over the OOB channel is used by the OBT to automatically discover the correct device, obviating the need for the user to manually select the correct device. This filtered discovery is also robust against cases in which other devices may attempt to masquerade as the actual device during discovery.

Once the OBT has discovered the device through this filtered discovery process, it prompts the user for confirmation before proceeding with the ownership transfer process. This provides the user with feedback that confirms that the device that was added to the network was successfully found, and gives the user an opportunity to cancel the OCF onboarding process. This may be useful for cases in which the user wants instead to onboard the device to a different domain, or not to onboard the device at all. Should the user confirm that the device is to be onboarded, the OBT initiates an ownership transfer method with the device to onboard it into the OCF domain.

As part of the execution of an ownership transfer method in OCF, the OBT establishes a secure channel with the device through datagram transport layer security (DTLS). While this channel is encrypted, it can be either authenticated (provide attestation of device identity) or unauthenticated (provide no attestation of device identity). Some ownership transfer methods defined in OCF, particularly those that are least difficult for users to execute, do not provide authentication. Streamlined onboarding does provide authentication, because the OBT leverages the credential provided by the device over the OOB channel as part of this handshake to ensure that the device that is onboarded is the same device that initially communicated over the OOB channel. In other words, the session established between the OBT and the device during onboarding can be trusted because the credential used to establish that session was exchanged ahead of time over the (separate) OOB channel, making streamlined onboarding more robust against on-path attackers.

Under the current architecture, the credential takes the form of a randomly generated passphrase that is used to derive a pre-shared key (PSK) for use in the DTLS handshake. However, our architecture allows for exchanging other types of credentials as well, including raw asymmetric public keys and X.509 certificates. In any of these cases, the OBT uses the credential to cryptographically verify that the device being onboarded is the device whose information was provided over the OOB channel. After the device is authenticated, the OBT takes ownership of the device, and the device transitions to the RFPRO state for further provisioning and use, as described in section 2.3.1.

4.2. Integration with Easy Connect

As described in section 2.2, Wi-Fi Easy Connect uses a series of Layer 2 messages to authenticate a device and provision it credentials for the Wi-Fi network. During this exchange, the Configurator first establishes a secure channel with the Enrollee. After establishing this secure channel, a set of configuration messages are exchanged to provision the network credentials to the Enrollee. The Enrollee first asks for these details with a configuration request message. The configuration messages that are exchanged during this process are formatted with JSON and are extensible through the addition of new fields. To accommodate the OCF streamlined onboarding information described in section 4.1, a new field “org.openconnectivity” is added to the configuration request message that is sent from the Enrollee to the Configurator. The Enrollee populates this field with its OCF device UUID and credential to be used during ownership transfer. When this configuration request message is received by the Configurator, the Configurator relays the streamlined onboarding information in the “org.openconnectivity” field to the diplomat in an implementation-specific fashion.

Because Easy Connect and OCF operate at entirely different layers, it should be noted that this method of providing application-level information through Easy Connect could apply to other IoT management frameworks and the OCF form of streamlined onboarding could be facilitated with OOB channels other than Easy Connect.

5. Implementation

To build an example implementation of streamlined onboarding, we integrate existing open-source implementations of both the OCF and WFA standards. Respectively, these are IoTivity-Lite [11] and HostAP (hostapd & wpa_supplicant) [12], with modifications that introduce the generation and use of streamlined onboarding information. In our implementation, a Wi-Fi AP is instantiated on one Linux system using hostapd. On the same system, we host an OCF onboarding tool and a diplomat implemented with IoTivity-Lite. Example OCF devices are implemented with IoTivity-Lite as well and are instantiated on other Linux systems that act as Wi-Fi stations through the use of wpa_supplicant. Figure 4 illustrates a logical overview of our implementation.

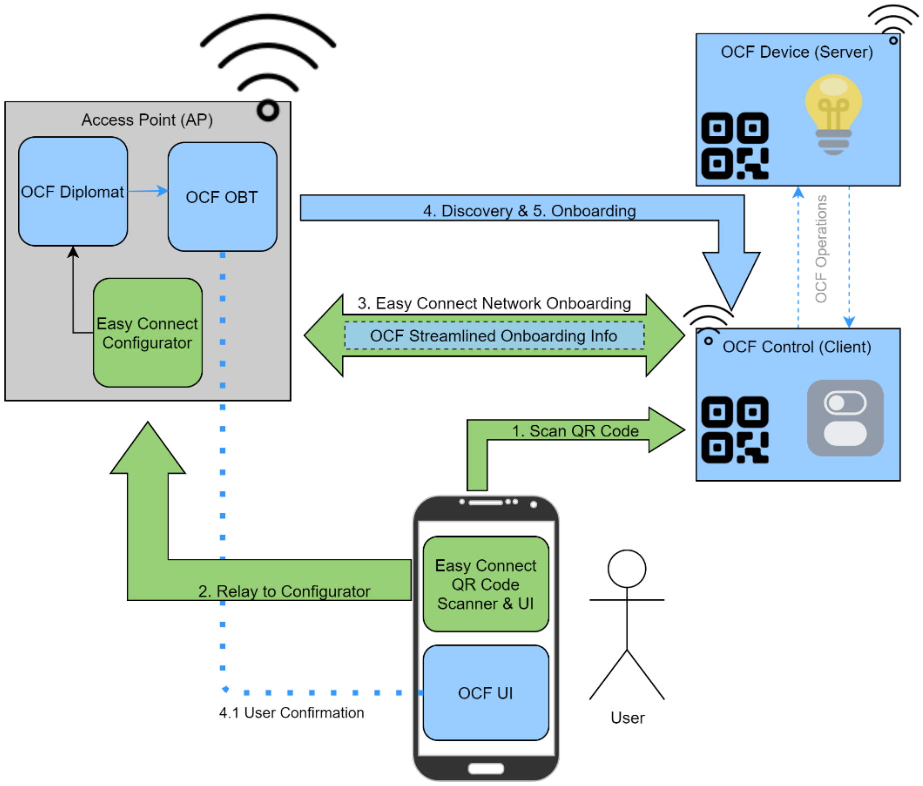


Figure 4 - Overview of Streamlined Onboarding Implementation

A description of the high-level steps outlined in Figure 4 appears below in Table 1.

Table 1 - Enumeration of Streamlined Onboarding Flow

Step	Description
1. Scan QR Code	The user leverages an application or web interface to scan the QR code presented by the device (e.g., on a display, printed on the manual, or printed on the device chassis).
2. Relay to Configurator	The application that scans the QR code relays the decoded URI to the Easy Connect Configurator (e.g., through a web request).
3. Easy Connect Network Onboarding	The Easy Connect Configurator contacts the Enrollee (the device) and provisions it Wi-Fi credentials so that it may join the network. OCF information is included in the configuration request, as described in section 4.2, and is provided to the OBT by way of the diplomat.
4. Discovery	Once the OBT has received the streamlined onboarding information from the diplomat, it

Step	Description
	discovers the relevant device (which is now on the network).
5. Onboarding	Before proceeding, the OBT prompts the user for confirmation (step 4.1). If the user confirms that the OBT should proceed, the OBT takes ownership of the device, using the credential provided over the Easy Connect exchange to authenticate the device.

At a high level, our implementation uses Linux-based inter-process communication sockets exposed by the Wi-Fi stack for two purposes:

- For IoTivity-Lite devices to inform wpa_supplicant of newly generated streamlined onboarding information.
- For hostapd to inform an IoTivity-Lite diplomat of streamlined onboarding information that was received as part of the Easy Connect configuration request message.

This section describes these various components and their implementations in further detail. In practice, our implementation is run on Raspberry Pis equipped with external USB Wi-Fi adapters.

5.1. Example OCF Devices (Stations/Enrollees)

To provide examples of OCF devices that can be onboarded in our architecture, we have implemented an example lighting device (e.g., a smart light bulb) and its corresponding controller (e.g., a smart switch). Each device is hosted on a separate Linux system, and the smart switch can interact with the smart bulb through OCF controls described in section 2.3. Each of these devices is implemented with our modified version of IoTivity-Lite and runs our modified version of wpa_supplicant for its Wi-Fi connectivity.

On each individual host, the OCF component offers streamlined onboarding information to the Wi-Fi component through HostAP's inter-process communication interface. This information is initially generated when the device is booted and no domain has yet taken ownership of it (i.e., when the device is booted for the first time after being reset). The streamlined onboarding credential generated by the device is a passphrase consisting of a sequence of random bytes. The device is able to provide this streamlined onboarding information directly to wpa_supplicant on startup, where it is kept in the Wi-Fi context until Easy Connect is executed. If the device has a display interface, it may display its Easy Connect QR code directly. Otherwise, the QR code may be preconfigured (e.g., using a static public key that was generated during manufacturing) and printed on the box, manual, or physical chassis of the device. At this point, the device simply waits both for network connectivity and to be onboarded into an OCF domain.

When an Easy Connect Configurator contacts the device, the Easy Connect exchange is carried out as usual, with the exception of the configuration request message that is sent from the device (acting as the Enrollee) to the Configurator. In this message, the device's instance of wpa_supplicant has been implemented to populate an additional field, "org.openconnectivity," with the contents of its streamlined onboarding information, as described in section 4.2.

5.2. Access Point and Administrative Components

The access point is implemented on a Linux system and hosts a few components that are used for the administrative aspects of both the Wi-Fi network and the OCF domain. These include:

- The hostapd access point – This AP broadcasts a Wi-Fi network and additionally acts as the Easy Connect Configurator. To interact with the Configurator, a user either interacts with this host directly, or may use an interface (e.g., a webserver offered by the host) to relay the information to the Configurator.
- The OCF diplomat – This diplomat is configured to receive streamlined onboarding information from hostapd through inter-process communication. When it does, it uses an OCF NOTIFY message to inform an OBT that has subscribed to it.
- The OCF OBT – This onboarding tool acts as the root of trust in the OCF domain. The OBT is configured to subscribe to updates on streamlined onboarding information from the (local) diplomat, and to perform onboarding when those updates are received. The user can also interact directly with this OBT (e.g., by way of a web-based interface) to discover, onboard, and provision devices.

The hostapd-based AP acts as a typical Wi-Fi network, on which any device (OCF or otherwise) can associate and gain network access. The AP additionally provides the Easy Connect Configurator with which a user interacts by presenting the contents of an Easy Connect QR code to initiate the Easy Connect network onboarding process. In our implementation, this interaction is performed when the user scans the QR code with a web-based interface, and that interface relays the contents of the QR code to the Configurator. Once received, the Configurator initiates Easy Connect, contacting the device that presented the QR code over Layer 2 and establishing a secure channel. When the device being onboarded sends its Easy Connect configuration request message as part of the Easy Connect exchange, the hostapd component of the AP sends a software event that contains any streamlined onboarding information that was present in the “org.openconnectivity” field of the configuration request.

The diplomat is implemented with IoTivity-Lite, and simply notifies any subscribers of streamlined onboarding information when it receives it. The diplomat’s primary function is to poll for the streamlined onboarding events that are sent by hostapd, as described above. When such an event is received, the diplomat encodes the streamlined onboarding information and notifies the OBT.

The OBT is also implemented with IoTivity-Lite, and is designed to subscribe to the diplomat and process streamlined onboarding information received through NOTIFY messages. When these messages are received, the OBT uses its filtered discovery mechanism and the UUID received from the diplomat to first discover the new device, then takes ownership of it through the streamlined onboarding ownership transfer method. In this method, the OBT extracts the credential from the streamlined onboarding information and uses it to derive a PSK. The OBT then initiates a DTLS handshake with the device, using the PSK to authenticate the device.

Once a device has joined the network and the OCF domain through this streamlined onboarding process, it can be configured further with OCF operations described in section 2.3. In our demo implementation, once both OCF devices are onboarded, they can be configured to interact with each other, such that the switch device can control the lighting device. In all, for a user to configure these two devices, only 3 steps are required: scanning the QR code of each device to execute streamlined onboarding, and configuration of the devices so that they may interact with each other.

6. Discussion

Streamlined onboarding provides a method for onboarding IoT devices that is both more intuitive and more secure. This has many advantages for users, vendors, and operators.

6.1. Users

End users, those who will be purchasing and provisioning devices, will benefit from a simple one-step process that requires only one application to onboard their new device onto the network and integrate it into their smart home. By making contributions to open standards, our goal is to establish streamlined onboarding as a well-known process that end users can come to expect from IoT devices, greatly reducing up-front effort that is required to configure new devices.

Streamlined onboarding also provides extra security with no extra effort, as each device will have a unique credential on the user's Wi-Fi network. No longer will the homeowner need to provide the same password to each device on their network. On the IoT management front, streamlined onboarding provides a more secure process for provisioning ownership information to IoT devices, and a framework such as OCF can enable consistent security and better interoperability for devices.

6.2. Vendors

Vendors that implement streamlined onboarding will save the development costs required to build an application for managing the device. Because this solution uses standard protocols and there is an open-source reference implementation, a vendor can rapidly bring a device to market, complete with the tools to manage that device. Additionally, vendors can limit costs that might have been spent on additional radios (e.g., Bluetooth) that would only be used to provision onboarding information before a device was connected to the network. Vendors that support streamlined onboarding also offer the desirable feature of a simplified process for users to start using a new device.

6.3. Operators

Operators that offer customer-premises equipment (CPE) with Wi-Fi AP capabilities can support a better subscriber experience when it comes to adding IoT devices to the network, leading to less frequent support calls directed to operators on how to get devices connected. Additionally, support of the streamlined onboarding flow can be applicable to several different IoT management frameworks, enabling support for a variety of IoT ecosystems that a user may introduce into the home.

For operators of managed IoT solutions, streamlined onboarding will allow an installer to quickly, consistently, and securely onboard the device to the subscriber's network. The provisioned device will be guaranteed to interoperate with the subscribers' other devices. This will result in more consistent behavior with fewer errors experienced by users resulting in fewer support calls.

6.4. Conclusion

The current state of IoT device management continues to pose challenges in the realms of security and user experience. As IoT adoption continues to expand rapidly, there is a growing need for solutions that provide improvements to both these critical facets. Streamlined onboarding offers a consistent and secure way to bring IoT devices onto the network and into an IoT management domain with minimal user interaction or prerequisites. Aimed to be built upon open standards, streamlined onboarding can provide a consistent experience that is easy for operators and vendors to adopt, and simpler for end users to execute.

Conceptually, streamlined onboarding could be implemented with a variety of different IoT management frameworks and lower-layer protocols to serve as an OOB channel. This paper describes our method for streamlined onboarding using WFA Easy Connect as the OOB channel to onboard Open Connectivity Foundation IoT specification devices. Our example implementation is built with open-source libraries for both Easy Connect and OCF, which are respectively HostAP and IoTivity-Lite.

In the future, we hope to pursue streamlined onboarding under additional IoT management frameworks and demonstrate the use of other OOB channels. As part of these efforts, we also have the goal of demonstrating the use of streamlined onboarding in market segments other than home IoT, such as business and industrial settings or smart cities. An important aspect of driving security in any solution is to ensure that the secure method is also simple to use; streamlined onboarding presents an opportunity to provide such a path for IoT device management.

7. Abbreviations and Definitions

7.1. Abbreviations

AP	access point
CPE	customer premises equipment
CBOR	concise binary object representation
CoAP	constrained application protocol
CRUDN	create, retrieve, update, delete, notify
DPP	device provisioning protocol
DTLS	datagram transport layer security
IoT	internet of things
ISO	International Standards Organization
IEC	International Electrotechnical Commission
JSON	JavaScript object notation
OBT	onboarding tool
OCF	Open Connectivity Foundation
OOB	out of band
PSK	pre-shared key
QR code	quick response code
REST	representational state transfer
RFOTM	ready for ownership transfer
RFPRO	ready for provisioning
RFNOP	ready for normal operation
UUID	universally unique identifier
WFA	Wi-Fi Alliance

7.2. Definitions

Onboarding	The process of establishing trust in a device for operation in a network and/or ecosystem (e.g., Wi-Fi, OCF) by provisioning credentials that the device uses in that ecosystem.

8. Bibliography and References

[1] "Current Forecast Highlights - Transforma Insights," Jul. 20, 2021. https://transformainsights.com/research/forecast/highlights (accessed Aug. 04, 2021).

[2] "Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper," *Cisco*. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (accessed Aug. 23, 2021).

[3] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[4] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019, doi: 10.1109/JIOT.2019.2935189.

[5] S. Imtiaz, R. Sadre, and V. Vlassov, "On the Case of Privacy in the IoT Ecosystem: A Survey," in *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Jul. 2019, pp. 1015–1024. doi: 10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00177.

[6] *Wi-Fi Easy Connect Specification*. Wi-Fi Alliance, 2020. [Online]. Available: https://www.wi-fi.org/file/wi-fi-easy-connect-specification

[7] "OCF - Specifications," *Open Connectivity Foundation (OCF)*. https://openconnectivity.org/developer/specifications/ (accessed Aug. 22, 2021).

[8] Craig Pratt, Darshak Thakore, and Jacob Gladish, "WiFi Passwords: The Evolving Battle Between Usability and Security," presented at the SCTE Cable-Tec Expo, 2020. [Online]. Available: https://www.scte.org/documents/3070/1742_Pratt_3216_paper.pdf

[9] "Thread Benefits." https://www.threadgroup.org/What-is-Thread/Thread-Benefits (accessed Aug. 25, 2021).

[10] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," Internet Engineering Task Force, Request for Comments RFC 7252, Jun. 2014. doi: 10.17487/RFC7252.

[11] "Home | IoTivity." https://iotivity.org/ (accessed Aug. 23, 2021).

[12] "hostapd and wpa_supplicant." http://w1.fi/ (accessed Aug. 23, 2021).

SCTE STANDARDS JOURNAL

Telehealth Business Case for Cable Operators

A Technical Paper prepared for SCTE by

Dr. Sudheer Dharanikota, Managing Director, Duke Tech Solutions, Inc., SCTE Member
Sudheer@duketechsolutions.com
+1-919-961-6175

Ayarah Dharanikota, Healthcare Strategy Consultant, Duke Tech Solutions Inc.
ayarah.dharanikota@duketechsolutions.com
+1-919-376-5657

Dennis Edens, Senior Manager, Duke Tech Solutions Inc.
dennis.edens@duketechsolutions.com
+1-919-332-9681

Bruce McLeod, Executive Director, Cox Communications,
bruce.mcleod@cox.com
+1-678-300-1700

Table of Contents

List of Figures

List of Tables

1. Document Overview

What is the problem?

How big is the Telehealth opportunity for cable operators? What are the financial considerations from revenue and cost points of view?

Key Takeaways
We make the following recommendations to operators:

- Telehealth opens door for multiple stakeholders
- Profitability will reach 100s of billions of dollars
- Operators need to build inter-industry collaborations.
- Their reward depends on the amount of risk the operators are willing to take.

Key words: Telehealth, Telecom for Healthcare, Unified Communications, Data Hosting

2. Executive Summary

As the years have progressed, the amount of healthcare spending in the US has also significantly risen. In 2018, it reached upwards of $3.6 trillion [1]. One way to combat that spending is the use of telehealth (TH) solutions. Telehealth is the idea of using telecommunication services to provide healthcare to any individual regardless of location. It can encompass everything from physician visits to educational tools, but at its heart telehealth depends on the progress telecom operators have made.

This past year during COVID-19, we have seen a 175x increase in telehealth adoption [2]. COVID has highlighted the many benefits of telehealth conducted from home:

- Saving travel/visit cost;
- Reducing travel time; and
- Reducing risk for patients and physicians.

Telehealth not only impacts the individual patients, but also family homes, elders, caregivers, and healthcare providers. Each of these stakeholders has its place in telehealth and are key players when considering how to enter the market or when creating solutions. However, with the explosion in telehealth needs during the pandemic the space has also become highly fragmented with few unifying solutions. MSOs have a chance to **unify the telehealth space**.

Since MSOs have already developed infrastructure for audio/video communication, smart devices, IoT, etc. they already have a leg up on other companies. To expand beyond just the basic needs, we have defined four offerings for MSOs to consider:

- **Basic Telehealth:** *Basic Telehealth* services would help maintain audio or video communication between patients and providers. The goal would be to provide services to users regardless of location.
- **Security:** A *Security* offering would be dependent on the security level needed. One needs to consider if Health Insurance Portability and Accountability Act (HIPAA) or Protected Health Information (PHI) would play a role in the offering.
- **Analytics:** The *Analytics* offering would provide analysis and visualization of medical data.

- **Install and Support (IandS):** Providing an *IandS* offering is dependent on the individual stakeholders' needs.

Each of these offerings considers MSOs' current and future capabilities while addressing the need of the market. They are innately flexible so that they can be changed to fit whatever model the MSO sees fit for itself. From our research, we were able to project the market size, revenue, cost, and profits. The cost areas we considered were premise, service offering, operations, training, and overhead cost. From these projections in 2030, operators could see around $109.5B in profits.

MSOs have a competitive advantage with their established customer bases, communication infrastructures, hosting/analytics capabilities, and support structures. With strategic partnerships in the telehealth space, operators have a low barrier to entry while being able quickly to capture a large telehealth market. Not only will operators have a chance to expand their portfolio, but also to create a valuable healthcare impact in this growing market space.

3. Introduction

As healthcare spending increases in the US ($74B in 1970 to $3.6T in 2018), it opens up room for technology to reduce waste, decrease cost, and increase productivity [3]. In many cases, telehealth solutions have entered the space as a way to address some of the inefficiencies of the current healthcare system. For example:

- Access to quality medical care for all communities.
- Reduce time and money spent traveling to and from medical facilities.
- Providing continued care across different physicians for chronic disease patients.
- Controlling costs from no-show patients.

Telehealth is a virtual service that encompasses both telemedicine and telecare. Unlike telemedicine, telehealth goes beyond video/audio communication. It incorporates electronic health records (EHR), education, testing, etc. Telecare allows patients to take care of their medical needs virtually through medical devices or monitoring services. The diagram below (details available here) highlights how these three services interact in the realm of virtual healthcare.

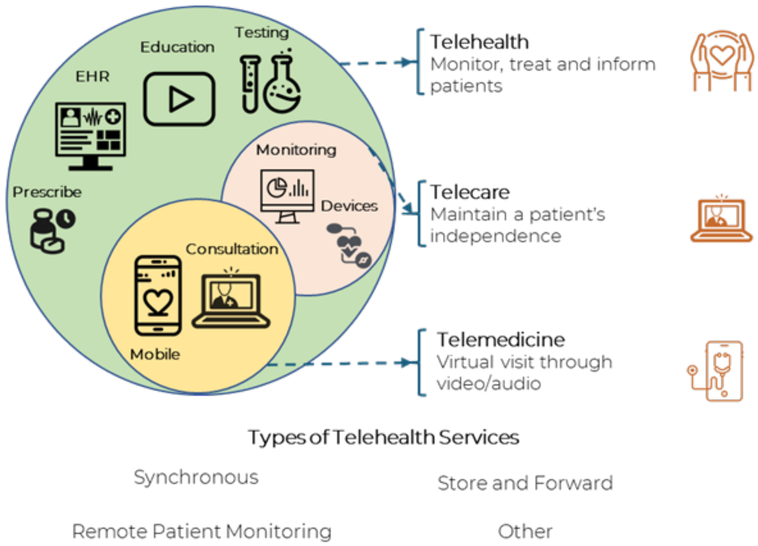


Figure 1 - Summary of Telehealth and other related services

Because of the COVID-19 pandemic, many telehealth legislative barriers were lifted to accommodate the social changes that were happening around us. Some such barriers included relaxing state physician licensing laws, CMS (Center for Medicare and Medicaid Services) restrictions on location, HIPAA flexibility on technology, etc. [4]. With these relaxations, telehealth technology has grown at an incredible rate; 2020 has seen a 175x [1] increase in telehealth adoption but it also has led to a fragmented market. As the benefits of telehealth become clearer, MSOs have an opportunity to expand their presence in the sector.

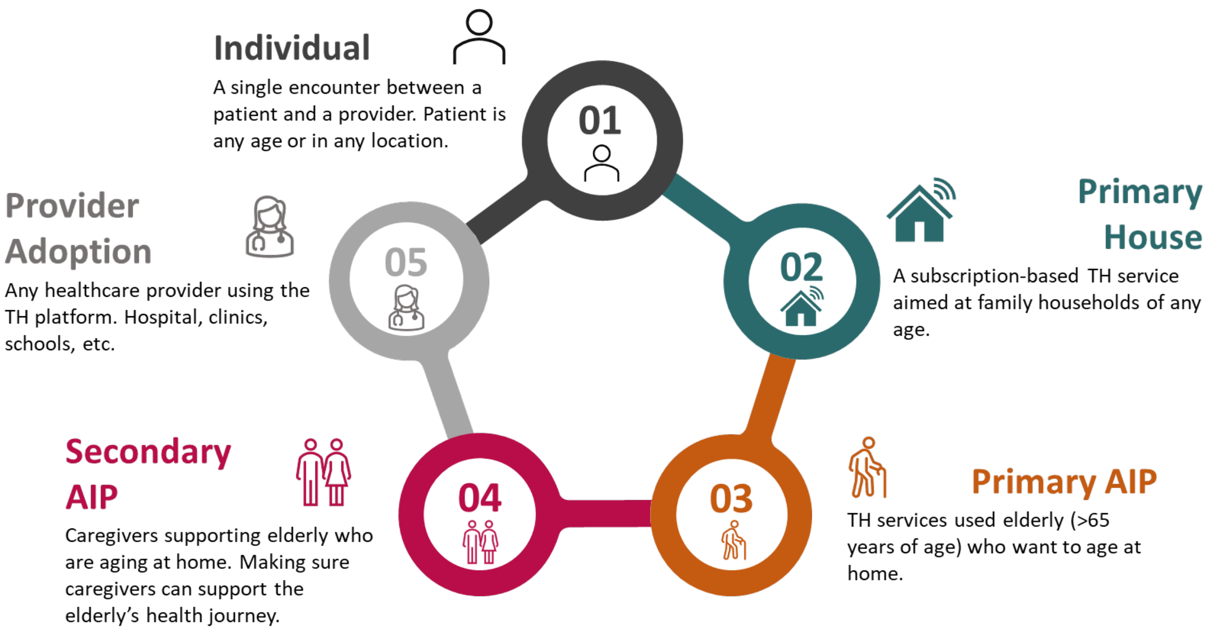
Telehealth has always used telecommunications, but with advancements in technology (5G wireless, 10G wireline access networks, etc.) and increased availability, MSOs can work to unify the telehealth space. With their expertise in broadband, established customer relations, hosting capabilities, and service management, MSOs can tailor telehealth solutions to their strengths while unifying existing solutions. This paper will focus on different potential business models that MSOs can follow to target the telehealth market, as well as make a case for why MSOs are a natural fit for advancing telehealth solutions.

4. Market Sizing

To understand the telehealth market, we identified a few key stakeholders: *individuals; primary house; primary AIP (Aging in Place), Secondary AIP; and Provider Adoption.* Figure 2 shows a variety of markets that operators can tap into to provide telehealth services.

Figure 2 - Different stakeholders an operator can address with their Telehealth solutions

Individual: Single encounters are the main target for stakeholders for telehealth solutions. Before the COVID-19 pandemic, CDC reported the number of telehealth visits was increasing at an average compound growth rate of 50% per year; however, during COVID-19 there was an increase in the need to shift to virtual care for safety and convenience sake. This shift pushed telehealth visits up 154% (approximately 1.6M Telehealth encounters) by the end of March 2020 when compared to that same time period in 2019 [5]. The number of individual patients who said they use telehealth went up from 11% in 2019 to 46% in 2020 [2]. While the number of overall telehealth visits is declining after the initial



excitement, many walls have been knocked down because of the pandemic. It opened the door for other markets/stakeholders to benefit from telehealth services. Some of the stakeholders we address are household families, the elderly, elderly caregivers, and providers.

Primary House: Primary house addresses how family households will use telehealth services. The 2020 census reported that households in the US with an average age of 50 years totalled 83.7M [6]. Since encounters typically involve just a single individual, we expect that only a fraction (estimated ~10-15%) of households will initially aim for a family telehealth plan.

Primary Aging In Place (AIP): Elderly individuals (65+ years) and their caregivers (Secondary AIP) also have a large stake in the progress of telehealth solutions. More and more elders are turning towards aging in their own homes, or AIP. With AIP comes technologies such as telehealth to make their stay at home safer and more convenient. As the elder population grows (from 45M in 2017 to 95M in 2060) and with 90% reporting that they want to age at home, telehealth will become a prime service for AIP [7].

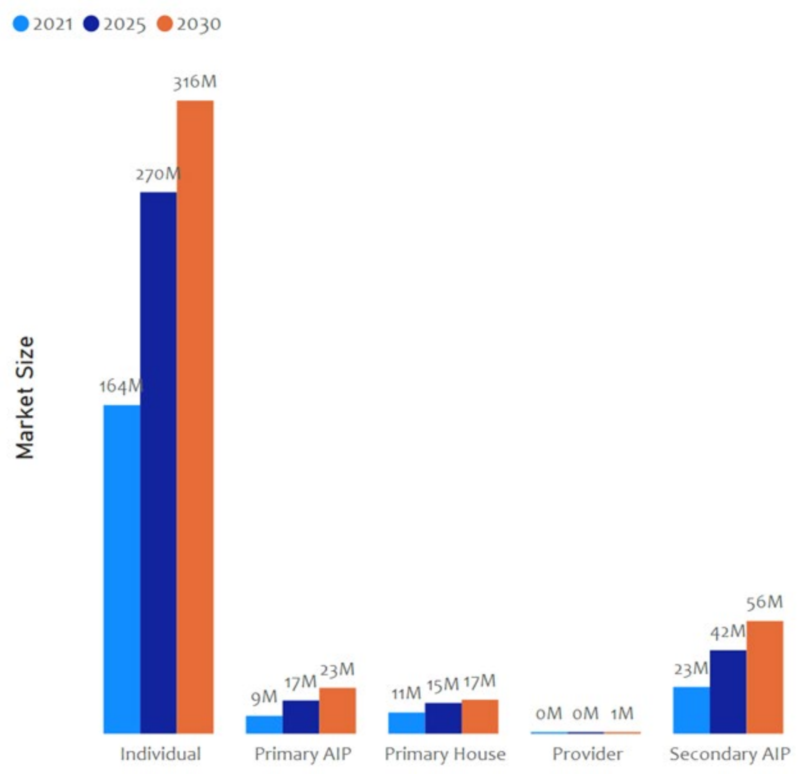


Figure 3 - Projected Telehealth market size for different stakeholders

Secondary AIP: Caregivers are also a big part of the elderly's care journeys. The 2020 AARP (American Association of Retired Persons) Caregiver report noted that 53M Americans acted as a caregiver sometime in the past 12 months [7]. 89% of those people were relatives and spent on average 23.7 hours per week caring for their elderly family members [7]. Since caregivers are providing significant care for the elderly, they need to be in the loop of the elder person's health care journey, including telehealth visits.

Provider Adoption: Physicians and other healthcare providers (categorized as provider adoption) are also growing more accustomed to using telehealth, with 80% of physicians who have used telehealth planning to continue using it after the pandemic [8]. Since restrictions have eased and clearer reimbursement pathways for telehealth have been established, more physicians will likely continue adding it to their practice. Physicians (from all types of specialties and locations) will be able to open their services to users of telehealth. A survey done by Amwell found that 96% of physicians would be willing to use telehealth for their practice and 93% said they would use it for chronic care management [9].

5. Business Model

5.1. Telecom offerings for telehealth

Before going into telehealth offerings, we need to understand some of the issues our identified stakeholders have with the current healthcare system.

Table 1 - Common problems in the healthcare industry and which stakeholders face them

	Healthcare Access	Unified Communication	Analytics	Monitoring	Trust/ Security
Individual	✓	✓	✓	✓	✓
Primary House	✓	✓	✓	✓	✓
Primary AIP	✓	✓	✓	✓	✓
Secondary AIP		✓	✓	✓	✓
Provider Adoption		✓	✓	✓	✓

The table above describes some common problems the stakeholders above have faced with our health system. Derived from these problems, we have created offerings that MSOs can offer to address those problems: Basic Telehealth, Security, Analytics, and Install and Support (IandS).

Basic Telehealth: Basic Telehealth offerings would address the basics of a medical encounter between patient and provider. This offering would include simple audio or video communication between the different parties. Hence it would address the need of making sure services are provided to anyone as long as they have a reliable connection. Operators could utilize their strength in broadband, in-home connectivity, and unified communications to offer services to telehealth stakeholders. By extending their current services they could add infrastructure to support telehealth services and address the needs of the consumer.

Security: This offering would be mainly dependent on the level of data security required in the service. If all the service operator would want to offer is simply video or audio communication, it may not need to be HIPAA (Health Insurance Portability and Accountability Act) compliant. However, if the service is more integrated with the patient data (personal information or other patient data), then having HIPAA and PHI (Protected Health Information) compliance would be necessary. Depending on the number of risks operators would want to take on, building trust in the service would be essential. Cable operators could provide secure connections and data transfer, making it easier to delve into the security offering. The challenge with providing healthcare security would be to maintain services that meet established regulations. Secure services might become table stakes at some point, but in the meantime, these services could be an additional offering.

Analytics: Analytical services would involve both analysis and visualization of different forms of patient or hospital data. It could help inform providers of lab trends, correlations that might help with diagnosis or chronic care management. Visualizations could assist with understanding telehealth trends in the hospital as a whole, whether it be for telehealth management, device operations, etc. With a wide range of analytical services that can be derived from hospital data, operators would have a chance to work with healthcare experts to provide metric-driven changes within the industry.

Installation and Support (IandS): IandS involves any form of install and support that telehealth services might require, given that each stakeholder likely would require different levels of support. For providers, this could involve restructuring their infrastructure to support telehealth. This could include repurposing their devices, installing software/hardware, new telehealth devices, servicing devices, software, etc. For the patients, there might not be as many devices to install, but there would be potential for servicing devices. Depending on the level of IandS, individuals would have to be specially trained to support the telehealth infrastructure. This service could be offered as an upsell package by the operators. Since operators have been integrated into telehealth since the beginning, IandS is another chance to enhance their telehealth portfolio.

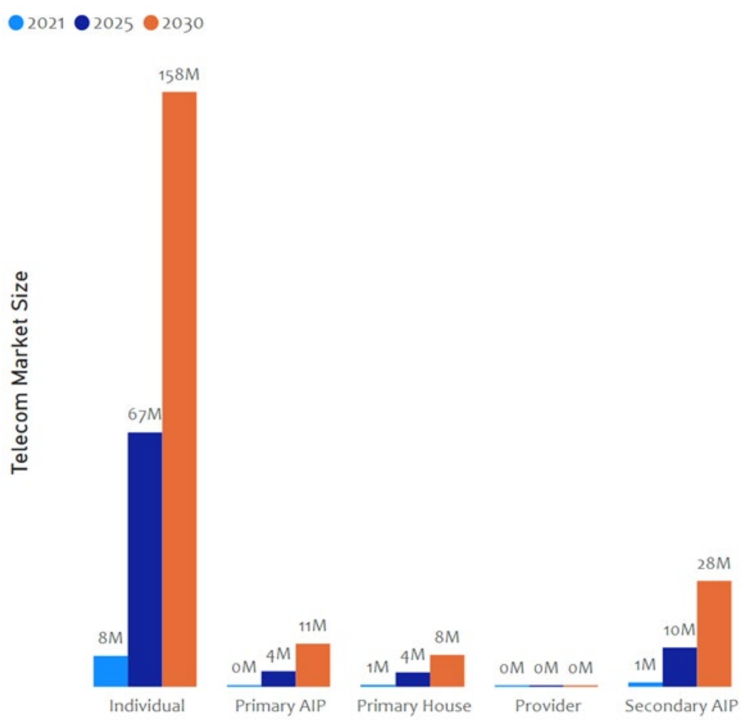


Figure 4 - Telecom operators projected market size by the stakeholder

In the following sections, we provide the telecom operator market size for the above product offerings, the revenue opportunities and cost, and profitability analysis.

5.2. Operators market size

With a very conservative initial size and growth assumption per market segment (Individual, Primary House, Secondary AIP, Primary AIP, and Provider) and a detailed breakdown of these segments into subsegments for an accurate forecast, we derived the next 10-year telecom operators telehealth forecast.

When looking at how the telehealth market is projected to grow, as shown in Figure 4, it is clear that there is consistent growth in most segments. The market segment seeing the most growth is the individual. We can attribute this amount of growth to increased acceptance of telehealth services. As telehealth builds its reputation as a reliable mode of healthcare, more individuals will turn to it for primary care visits, specialized treatment, chronic care management, etc.

Additionally, with Primary AIP and Secondary AIP, growth can be linked back to the move towards the elderly wanting to age in their own homes. As an increasing number of elderly individuals shift to AIP, there would be a need for them to receive healthcare services in their own homes. Hand-in-hand with that, the caregiver(s) for elderly will also increase their adoption as a result of a need for providing additional care.

5.3. Potential business models

While healthcare is a mature industry, telehealth has just begun to receive heavy attention; however, due to the pandemic, many companies have made a push to enter the market. This means operators need to utilize their strengths to create strong differentiators and a portfolio based on customer needs. Figure 5 below highlights a business model operators for extening capabilities within the realm of the four offerings.

Basic Telehealth Offering: Since the Basic Telehealth offering deals only with the essential video/audio communication MSOs would be working closely with healthcare providers. Other stakeholders (individual, primary house, primary AIP, and secondary AIP) wouldmore often than not engage with a provider rather than an MSO in the basic offering. By nature of this pathway, MSOs mostly would be receiving revenue directly from healthcare providers.

Security Offering: The majority of telehealth security efforts are incorporated into the telehealth platform, and for that reason revenue generated from a Security offering would primarily involve the healthcare provider. The other stakeholders would have security provided to them when they log in to the platform, but MSOs would not be gaining any direct revenue from them.

Analytics Offering: Similar to the security offering, providers would be the main stakeholder for an Analytics offering. While patients/caregivers may have access to certain pieces of data, the provider would actively be using/paying for the analytics. MSOs could take on a proactive approach to creating dashboards or analytical tools for providers to use in their practice. Hence, operators would receive revenue from the providers that use their analytical tools or services.

IandS Offering: Depending on the condition of the patient or the active role medicine plays in their daily lives, stakeholders might require more install and support of the medical device. We do, however, expect that majority of the revenue would be taken from the provider because of the variety of medical devices they already have. While other stakeholders may have closer to one-time cost or less frequent monthly IandS devices, providers would need more active device support.

These pathways are just a few of the possible ways MSO could interact with certain telehealth stakeholders. As operators grow their telehealth presence, they could expand their business models and how they reach out to stakeholders.

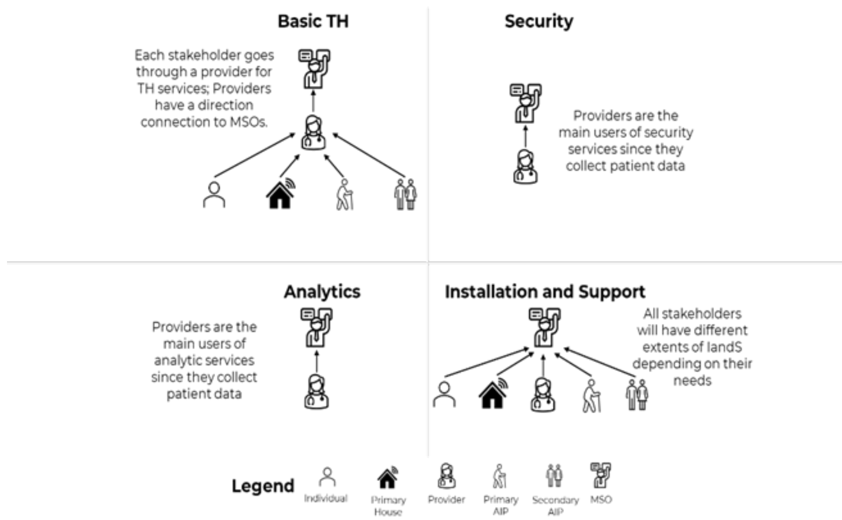


Figure 5 - High level business model assumed in the revenue, cost, and profitability analysis

6. Telehealth Business Case Analysis

6.1. Telehealth revenue forecast for operators

In this section, we provide an analysis of different telehealth revenue opportunities for operators. We have performed extensive stakeholder business cases and analyzed business models used by different vendors to identify potential operator revenue opportunities. The summary of this analysis is presented by market segments in Figures 6 and 7.

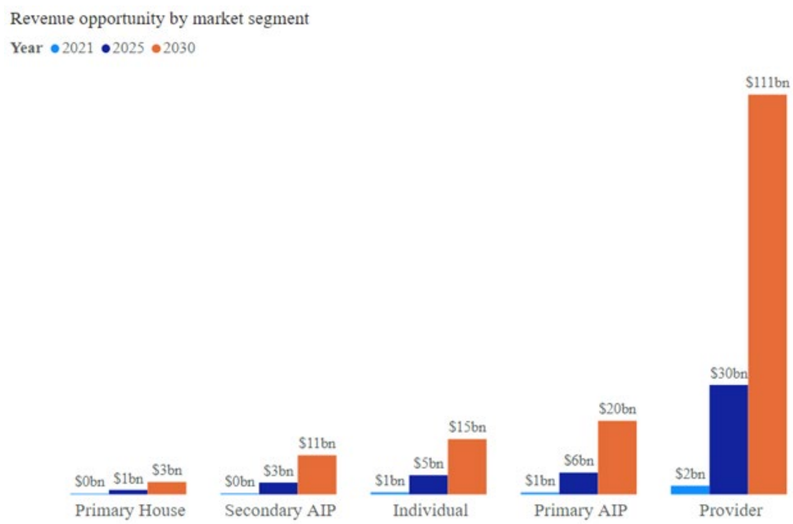


Figure 6 - 10-year revenue forecast for different market segments

Basic Telehealth: With the Basic Telehealth offering above, Telecom Operators could derive revenue from either telehealth visits, monthly revenue from package deals, or users/license charges. For the individual telehealth visit, the revenue would go from the provider to the telecom operator. For their pricing model, operators could consider that patients are gaining significant savings (from fuel expenses, lost wages, and other family expenses). Telecom operators could make money in a few ways with primary house such as taking revenue from the monthly and/or per visit charges. As a reference, we have seen two types of package deals: a) straight monthly charge and b) a reduced monthly charge with an additional per visit charge. With providers, revenue could be derived from monthly user charges, software license charges, etc. The stakeholder business case would include saving money on fuel spending, wages, and travel time. Per visit, patients could save roughly $280 [10]. In addition, the operator could partner with providers to create an integrated platform on which operators would take the majority of the revenue for running the back end. Monthly packages for homes would be another revenue pathway for operators.

Security: Since security would mainly focus on the provider end, operators could charge through various pricing models such as licensing, number of users, etc. Security also would be provided through EHR systems, thus there could be some revenue split with EHR systems or other partners. License charges could vary depending on the level of protection provided. Some estimate it to be between $1,000-$2,000 per year. A per-user charge could also change depending on the size of the institution or the amount of data being handled.

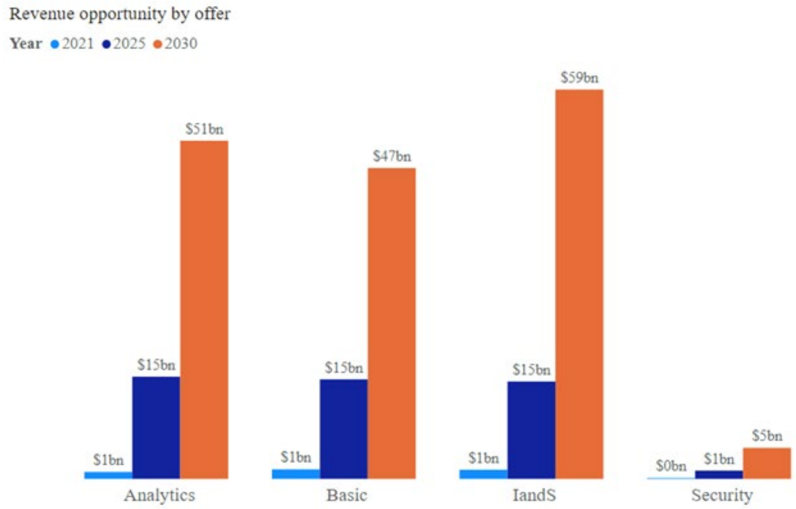


Figure 7 - 10-year revenue forecast by different offers

Analytics: Pricing for analytics and visualizations could be dependent on, a) the number of hospital claims or b) other metrics chosen by the operator. Because there is a wide range of types of visualizations and analytical services that could fall under this offer, we focused on conservative numbers to project the revenue. One such service was analyzing hospitals' claims.

Install and Support: IandS could become more complicated for certain stakeholders, but operators already have an infrastructure to handle this complexity! In the IandS models, operators could make revenue from installing technology for providers with monthly servicing costs; however, for an individual or primary house service, there may be little revenue from installations and servicing depending on the type of devices used. Provider installations could be upwards of $10,000/device with a fraction of that going to per month servicing.

Revenue Projection Summary: When comparing how different offering revenues are changing between stakeholders from 2025 to 2030, some clear trends emerge. In terms of revenue portion size, each stakeholder has relatively the same portion of the total revenue. The two largest segments in both 2025 and 2030 are the individual and primary AIP. With Individuals holding the largest market segment (~76% in 2025 and 2030) and most revenue generated through Basic Telehealth offerings, it is not a surprise that it is one of the larger revenue-generating stakeholders. As for primary AIP, while its market is not larger than secondary AIP, this group will directly be interacting with the offerings. For example, an elderly person will be the primary user for a Basic Telehealth solution while a caregiver may require pared-down monitoring functionality. As MSOs continue to explore telehealth, more revenue opportunities will emerge beyond just the stakeholders/offerings we have suggested.

6.2. Telehealth solution cost projection

End-to-end telehealth costs are grouped into five main categories: *new subscribers; service offering; operations and support; training*; and *overhead*. For the cost model, each of these costs is further categorized into:

- Initial one-time costs: These are the costs of building the initial telehealth infrastructure. This typically scales based on aggregation points and the scaling of the modular architecture per volume of customers (such as per thousand, per million customers, etc.)
- Net new customer costs: These are the costs of adding a new customer to the platform, such as costs from T4H hub etc. This typically depends on the type of service for which a customer is subscribing.
- Per subscriber costs: These are per subscriber maintenance costs.
- Installation and support costs: These costs include per customer installation and support costs.
- Overhead costs: These are for the additional management (i.e., Marketing, Sales, etc.) support overhead. These costs scale based on the number of markets and the number of resources supported per manager.

Each of the cost categories will be reviewed in more detail in the following sections.

New subscriber costs:

New subscriber costs are considered costs specific to adding a new customer. The demarcation point of the telehealth service is being defined as the telehealth hub (this could be a logical or a physical device). For any of the five market segments identified there would be a hub cost. The hub cost is expected to be different for the different market segments. For individuals, primary home, and primary AIP needs the hub and other relevant basic devices cost is around $80. A secondary AIP hub is ~$150 while a provider hub is ~$750. Subscribers are assumed either to pay for their premise equipment or to rent it for the time that they have the service. For this reason, no net new subscriber cost is applied for the premise equipment in the business case model.

The cost to support unified communications at the premise is projected to be the same on a per-user basis. Each user would have a licensing cost and would be required to download a communication application. The cost of the associated application and license is expected to decrease significantly over time. Initial costs are being estimated at $2 to $4 per month per subscriber, however, lower-cost may be achievable assuming volume discounts.

Premise sensor costs will vary based on the offering, market segment, and the specific condition targeted to be addressed by the telehealth solution. Some of the sensor packages for individuals with a basic package could be around $750, while a basic package for Primary AIP is ~$6,750. On top of this, a monitoring service charge of ~$1 - $5 per subscriber per month is also likely to be incurred. Like the premise equipment, the sensor packages would also be purchased or leased by the customer for at least the time that they have the service. For this reason, no cost is applied for the sensor packages in the business case model. Equipment installation and maintenance costs are being covered under operations and support costs.

Service offering costs:

The most significant impact to operators in supporting the telehealth market will be felt in providing the targeted services. Most of the charges will be one-time costs with some ongoing support and maintenance costs. Initial costs will be high as they are investments in the initial infrastructure, but these costs will significantly come down over time. Time to market is very important to capture market share, so where justified, forming partnerships or outsourcing necessary service offering requirements is recommended. Below is a list of the primary service offering support requirements.

- Unified communications for individual households
- Personal or electronic health record (PHR or EMR) integration
- Platform compliance to Health Insurance Portability and Accountability Act (HIPAA)
- Security (not considered unique to the telehealth offering) and privacy support
- Data hosting services and partitioning
- Analytical services

Note that these service offering costs are expected to decrease over time as systems and processes are put in place to address the offerings.

Operations and support costs:

Operations and support costs are the costs to cover order fulfillment and customer service. These costs tend to have the biggest impact on the cost model. By operators leveraging their existing order fulfillment and customer support organizations, they would have a significant competitive advantage in the early stage of this developing market. They would also be better equipped to be more accurate at estimating and controlling these costs. In the operating costs, we considered order fulfillment costs such as order entry and installation and customer services such as customer care and in-home service team costs.

Employee training will be critical to have a fast and smooth introduction of telehealth service offerings. Training is considered a one-time cost. However, additional training will need to be provided for onboarding new employees. Although the entire enterprise would need some form of training, primary training would be focused on five distinct areas of the organization:

- Sales;
- Installation and provisioning;
- Customer care;
- Field service and support; and
- Enterprise.

Enterprise training will include understanding the product offerings, which is key for all areas of the organization. Each organization will need to understand how these new offerings impact their job functions and any associated process changes that are made.

Overhead costs:

To cover the costs that are shared an additional overhead charge has been assumed. These costs account for personnel responsible for sales, marketing, and the dedicated engineering for telehealth solution support. An estimated headcount has been applied to the model. These overhead costs will be incurred year over year to support the product offerings and would be scaled based on the number of subscribers.

Summarized cost projections:

As stated earlier, each of these cost categories is further classified for the business case model. Figure 8 shows a high-level estimation of the costs per sub, net new subscribers addition, and support.

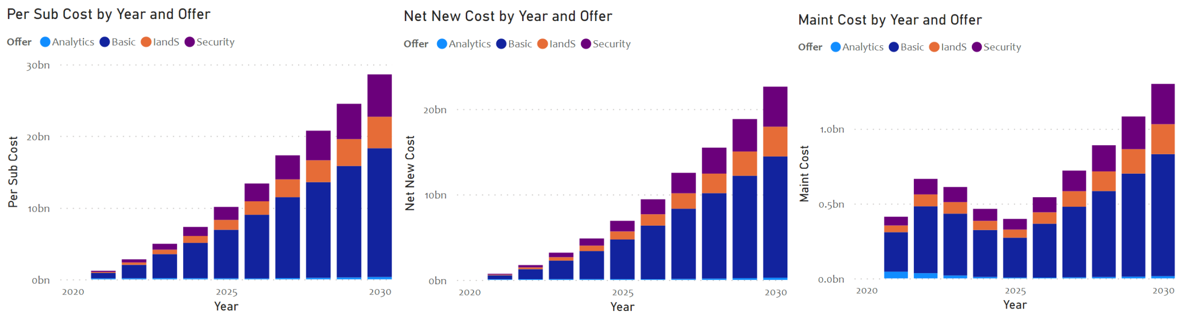


Figure 8 - High level estimated cost breakdown by AIP product offering

Per sub monthly costs are the highest due to revenue share agreements with the other solution component providers such as unified communications platform, PHR or EMR services, and specialized analytical services. Maintenance is the next major cost driver due to increased services. One can argue that the ROI of IandS may not be high enough to offer these services. But IandS, being the key differentiator for the operators, drives higher revenues through gaining more customers for the other services. The incremental cost for adding newer customers will diminish after the initial solution creation.

6.3. Profitability analysis

A shown in Figure 9, the telehealth opportunity for operators is going to reach 100s of billions of dollars in the US alone. We made a very conservative take rate assumption of 5% YOY growth in the market capture for operators. There is a significant upside to the profitability depending on the level of involvement an operator would want to have with the healthcare industry. We believe as both industries learn to trust each other, they will take more risks in solving complex telehealth problems and hence open doors for higher rewards than projected here

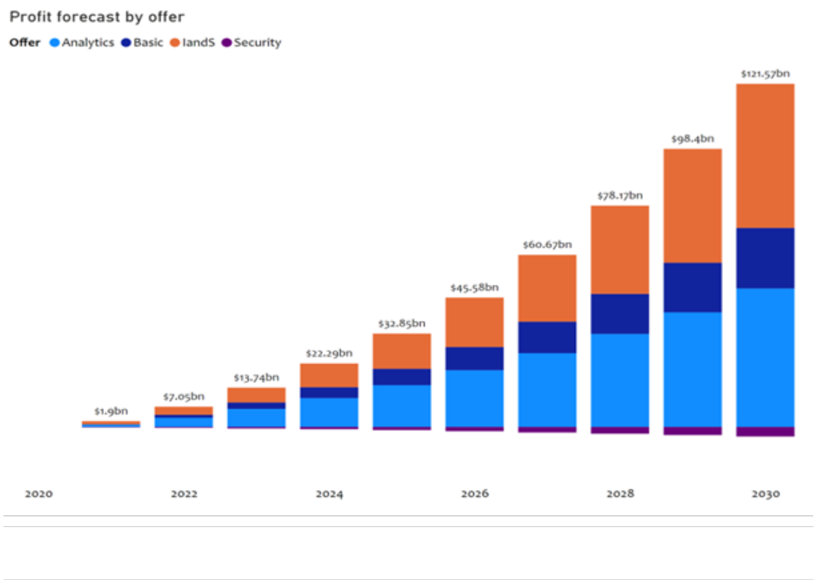


Figure 9 - Telehealth 10-year profitability forecast by offer

7. Conclusions and recommendations

This paper outlines our research of the telehealth market size and identified product offerings that are needed to fill the demand of a growing telehealth market. The result of our analysis reveals a compelling opportunity for MSOs to play a key role in fulfilling this market need by growing their product offerings and enabling end-to-end telehealth solutions.

As this paper points out, the healthcare industry is looking for innovations to help control exploding costs and address changing market needs. Operators are uniquely positioned to help address this telehealth market need. The cable operators have a competitive advantage in several key areas:

- Established relationships with the target customer base;
- Communication infrastructure ownership and control;
- Data hosting and analytics capabilities;
- Consolidated billing;
- Service provisioning and management experience; and
- Customer service and support (boots on the ground) organizations in place.

The key will be to use these competitive advantages to capture market share and grow operating profits quickly while the market is still fragmented. This market discontinuity is the optimum time to enter this expanding market.

To be most competitive, operators will also need to address their weaknesses. Healthcare is a new area for MSOs with some unique challenges. They not only need to support patients (i.e., subscribers), but also the assortment of healthcare providers and institutions. Health Insurance Portability and Accountability Act (HIPAA) regulations will also need to be addressed. From the market research and analysis, we estimated the **telecom market size**, the **projected revenue,** and the **estimated cost** to support making these telehealth offerings available. By modeling this data, we were able to calculate the projected profit. This model can be used by MSOs and other operators in developing their telehealth business cases.

Based on our extensive analysis, we provide the following observations and recommendations to cable operators:

- Telehealth gives way for cable operators to enter the lucrative inter-industry collaboration with the healthcare industry. The cable industry is uniquely positioned with its current capabilities (unified communication, broadband, and IoT devices).
- Partnerships can be developed with individuals, caregivers, and various healthcare providers to integrate different stakeholders.
- The development of integration partnerships and purchasing of key technologies will be crucial to bringing these offerings to the market quickly. The product offering strategy should focus on providing end-to-end telehealth solutions.
- Infrastructure can be repurposed to support telehealth offerings and HIPAA considerations.
- The offers presented here do not take into consideration the level of risk an operator is willing to take. We highly recommend exploring these during their internal strategic discussion.

Telehealth is not only a huge opportunity for operators to seize in the United States, but it is becoming a new addition to the ever-changing healthcare field around the world.

8. References

[1] Yusra Murd, *U.S. Health Spending Rose to $3.6 Trillion in 2018, Propelled by Health Insurance Tax*, article available here
[2] McKinsey & Company, *Telehealth: A quarter-trillion-dollar post-COVID-19 reality*, paper available here
[3] Peterson-KFF, *How has U.S. spending on healthcare changed over time?*, article available here
[4] Telehealth.HHS.Gov, *Policy changes during COVID-19*, article available here
[5] CDC, *Trends in the Use of Telehealth During the Emergence of the COVID-19 Pandemic*, paper available here
[6] United States Census, *Table HH-3. Households by Age of Holder*, table available here
[7] AARP, *Caregiving in the U.S. – 2020 Report*, report available here
[8] Michael Brookshire and Erin Ney, MD, *The Doctor is Online: Why Telehealth will Outlast the Pandemic*, article available here
[9] Amwell, *New Amwell Research Finds Telehealth Use Will Accelerate Post-Pandemic*, article available here
[10] Ann B Bynum, Cathy A Irwin, Charles O Cranford, George S Denny, *The impact of telemedicine on patients' cost savings: some preliminary findings*, paper available here

SCTE STANDARDS JOURNAL

Telehealth Market Landscape from a Cable Operators Perspective

A Technical Paper prepared for SCTE•ISBE by

Dr. Sudheer Dharanikota, Managing Director, Duke Tech Solutions Inc., SCTE Member
sudheer@duketechsolutions.com
+1-919-961-6175

Ayarah Dharanikota, Healthcare Strategy Consultant, Duke Tech Solutions Inc.
ayarah.dharanikota@duketechsolutions.com
+1-919-376-5657

Dennis Edens, Senior Manager, Duke Tech Solutions Inc.
dennis.edens@duketechsolutions.com
+1-919-332-9681

Bruce McLeod, Executive Director, Cox Communications, SCTE Member
bruce.mcleod@cox.com
+1-678-300-1700

Table of Contents

List of Figures

1. Document Overview

What is the problem?

How can cable operators address the telehealth market space? Who are the different telehealth players, and how can service providers differentiate themselves?

Key Takeaways

Based on our in-depth market survey surrounding telehealth, we proposed a seven-pronged approach: connectivity, infrastructure, security, quality metrics, analytics, serviceability, and support that operators should use to address basic telecom for healthcare services. We recommend that cable operators focus on the above services in the following order:

- Develop end to end ecosystem including labs and pharmacies;
- Build on existing capabilities such as connectivity, secure communications etc.; and
- Use the seven step differentiators as guiding principles for the rollout.

Key words: telehealth, market, service provider, telecom, MSO

2. Introduction

Telehealth is defined as using telecommunications technologies to support various healthcare services, such as long-distance healthcare, health education, public health administration, etc. The feature many of us are familiar with is the ability to connect patients and physicians who live in different geographical regions; this most commonly is called 'telemedicine.' Though this initial concept was conceived in the 1960s, only in the last decade has it started to gain ground. It is now projected to be valued at nearly $130.5 billion by 2025 [1]. With many advancements in telecommunications technologies, telehealth is becoming an increasingly important part of the worldwide healthcare infrastructure as healthcare starts to move away from paper records and in-person visits and towards virtual and more convenient healthcare.

Telehealth contains numerous benefits for the healthcare industry, not only for patients, but for other stakeholders. First, telehealth provides convenient and accessible care. Some of the biggest inhibitors to in-person patient care today are the distance and travel time between the patient and the care provider [2]. Telehealth overcomes these boundaries and provides care to rural and other areas where clinical shortages exist. It also allows for a healthcare professional to be just one call away, reducing the number of doctor visits, saving time, and preventing unnecessary costs [2]. Cisco reported 74% of patients prefer this easy access over in-person interactions [3] and a study by the American Hospital Association showed that telehealth care saved 11% in cost and tripled investors' ROI [4]. Additionally, telehealth has allowed for better care quality because timetables for medicine and prescriptions are more accurate. These timetables reduce stress and anxiety among patients as their health information is available to them at a moment's notice with the use of apps and other technologies.

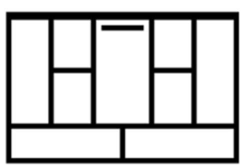
Over the last two decades, many existing healthcare systems and new companies have started to venture into the field of telehealth and telemedicine. Navigating through the products and services offered by these companies can get very tricky as they vary so drastically from company to company. Throughout the rest of this report, the SCTE team has conducted the technology, areas of focus, and business models of 19 companies around the world will be examined.

3. Framework of Analysis

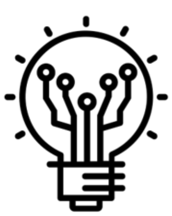
Over the years and with the introduction of COVID-19, telehealth companies have created their own niches in this expansive market. Some companies may focus solely on consultations for certain medical conditions; others will try to hit all areas of a patient's medical journey. With such a wide breadth of diversity within the market, we have created a framework in which to analyze these companies. The three overarching categories for analysis are Area of Focus, Business Model, and Technology. Using this framework, we have analyzed companies in the US, Canada, and internationally.

Area of Focus: Telehealth companies can provide a wide array of services with everything from consultations to educational material. But amongst these services differences, companies may also choose to focus on different disease states, different customers, or different demographics. NutriMedy is a good example of a telehealth company targeting a niche group. NutriMedy dietitians and other professionals give targeted advice to users with their chronic conditions. They mention helping with gastrointestinal, cardiovascular, nephrology, and oncology issues. With a plethora of avenues to follow, a successful service organization constantly has to find an optimized way to mix and match boots-on-the-ground efforts with technological innovation. Operators are quite familiar with such innovations from installation all the way to service support. When we analyzed these companies, we put on our operator's hat to see how these companies fare in their service evolution.

Business Model: As we looked at each company's business model, we were able to draw out the partnerships (EPIC, local pharmacies, etc.), value chain offerings, and work with other entities (labs, imaging, pharmacies, etc.) that were integrated into their model. For example, with the majority of health systems moving towards Electronic Medical Records (EMR), partnerships with EMR companies, such as EPIC, are becoming more attractive. Amwell is one of a few companies on this list that have formed that bridge. This integration allows for continuity of care and improved workflow. With a different approach to the telehealth market, many companies have been able to create unique value in the space; however, with the exponential growth this past year, the space has become heavily fragmented.



Technology: Telehealth companies have often used technology to differentiate themselves. Each company focuses on different stakeholders to provide basic consultations, diagnostics testing, or integrated front and back-end systems for end-to-end services. In this paper, we analyzed how companies integrate their technology, connect stakeholders, etc. For example, Amwell is one of the largest telehealth companies in the US. They have integrated a wide variety of technology over the years and have formed partnerships with companies such as EPIC. Their telemedicine carts and kiosks have also created flexibility in ways in which care can be provided.



With telecom operators playing an integral part in existing telehealth solutions and the growth of telehealth this past year, operators are uniquely placed to contribute more to this growing industry. This company compilation aims to inform operators of what already exists in the space and give a glimpse of how operators can play in the telehealth space.

4. Telehealth Companies

The goal of this survey is to give a 360-degree perspective on the companies in the telehealth market space before making any recommendations on what the service provider should or should not focus on. This company compilation takes a look at some companies from purely consultation based (Lemonaid Health) to high integration platforms (Amwell) in the telehealth space. The service provider should conduct such an analysis from their telehealth strategy perspective to evaluate where they have better opportunities and assess the best path for execution (such as partnership, build-operate-transfer, or pure build of the targeted solutions).

4.1. U.S. Companies

4.1.1. AMD Global Telemedicine

AMD Global Telemedicine focuses on providing solutions to organizations giving telehealth services while integrating into their current health IT systems. The products and services AMD Global Telemedicine offers can be split into four main categories: diagnostic telemedicine solutions, direct-to-consumer platform, employee on-site healthcare, and customer use cases.

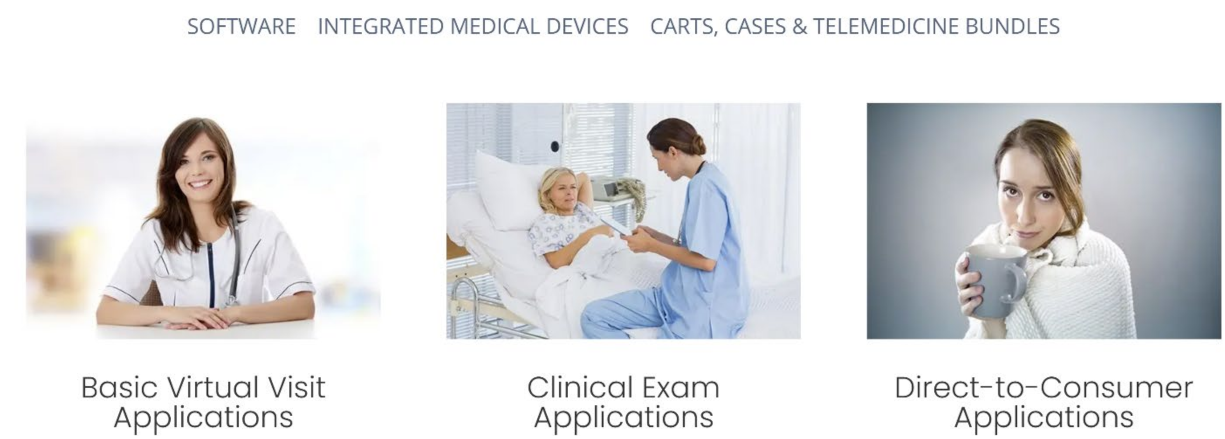


Figure 1 - Product categories that AMD targets

Company Website: https://amdtelemedicine.com/
Technology: Software, integrated medical devices, carts, cases & telemedicine bundles (**Figure 1**).
Area of Focus: Diagnostics, direct-to-consumer platform, on-site healthcare, and consumer use cases.
Business model: Partnerships with American Telemedicine Association, International Society of Telemedicine and eHealth, EMR systems. Most likely to charge for hardware and software programs. Pricing dependent on the product or software.

4.1.2. Amwell

Amwell is one of the leading Telehealth providers within the US and is working with more than 2,000 hospitals and health system partners. Amwell helps hospitals and health systems improve and expand their telehealth programs to offer more services to their patients. Amwell helps with telemedicine services throughout all of healthcare, from Urgent Care to Telestroke. They also provide specialty aid to hospitals in reducing the time patients spend in the ER by nearly 70%. They have additionally also implemented many of their services into inpatient and ambulatory care through the Wellstar Health system.

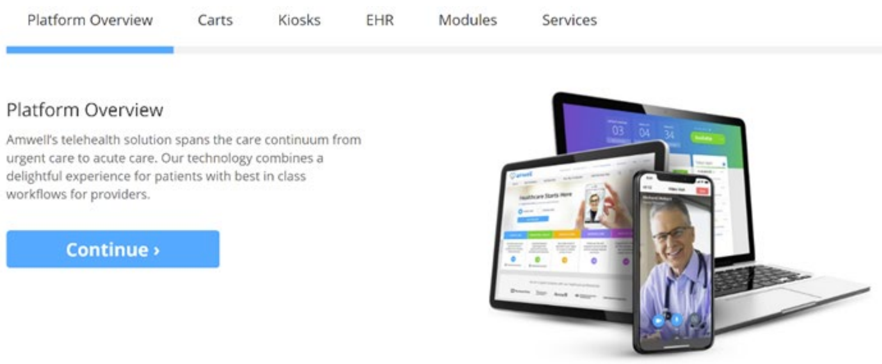


Figure 2 - Amwell simulated platform and forms of technology

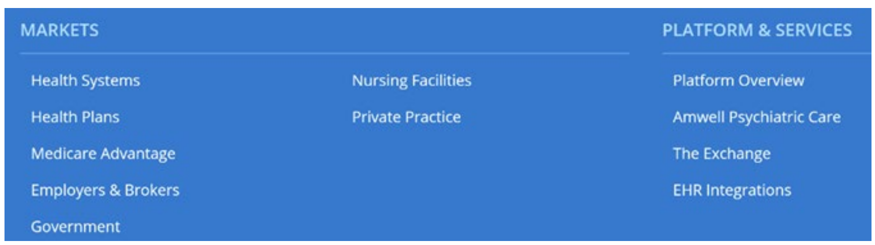


Figure 3 - Market segments that Amwell is currently working

Company Website: https://business.amwell.com/
Technology: Software, telemedicine carts, telemed kiosks, modules, etc. (Figure 2).
Area of Focus: Wide array including basic consultations, professional services, development of medical equipment, etc. (Figure 3).
Business model: Partnerships with health systems, EMR companies, payors, employers, labs, etc. Charge based on solution: consultation fee, software charges, hardware charges, or boots-on-the-ground.

4.1.3. Arista MD

Arista MD works as an e-consultant with various stakeholders within the telehealth field. These include payors, patients, health systems, and providers. Arista MD helps providers expand their specialty networks (Figure 4), which in-turn can reduce healthcare spending from services such as duplicate diagnostics, unnecessary testing, or emergency admissions. In addition to providing patients with primary care, they give access to specialists. Arista MD helps Health Systems by improving their network management between patients, providers (primary care physicians (PCP) vs. specialist), and others. Providers are supported by Arista MD's platform to ensure that patients are directed to the proper provider (PCP vs. specialist) while supporting PCPs.

Figure 4 - Arista MD aims to expand the customers health network

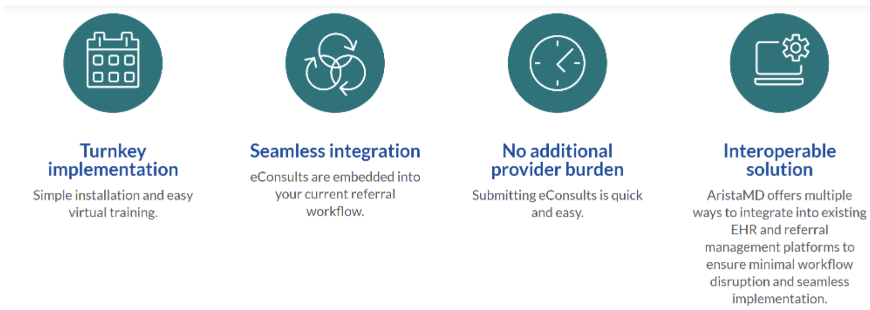


Figure 5 - AristaMD's eConsults system

Company Website: https://www.aristamd.com/
Technology: Store-and-forward, asynchronous telehealth platform.
Area of Focus: Expanding eConsults between primary care and specialists (Figure 5).
Business model: From website "At AristaMD, we envision a world where all patients have timely, cost-effective access to health care. Our mission is to use technology to facilitate collaboration between health care providers in order to expedite time to treatment, decrease costs and drive better patient outcomes."

4.1.4. BioTelemetry

BioTelemetry for the past 25 years has been focusing on providing cardiac and mobile blood-glucose monitoring, centralized medical imaging, and original equipment manufacturing. Their BioTel Heart sector provides remote cardiac monitoring diagnostic services and through their patient monitoring devices they have built the "world's largest cardiac network while making care more accurate, comprehensive and efficient." BioTel's services are also able to fully integrate into a hospital system existing EMR software using unidirectional or bidirectional integration. They have also expanded into the sectors shown in **Figure 6**.

Figure 6 - Different sectors of BioTelemetry

Company Website: https://www.gobio.com/

Technology: Mobile cardiac devices, corresponding software, remote INR.

Area of Focus: Cardiac management through device monitoring (Figure 7).
Business model: Partnerships with Apple, Philips, and others. Revenue from device and software sales. Devices covered by most insurances.
Latest News: Philips completes acquisition of BioTelemetry.

Figure 7 - Telehealth arrhythmia monitoring

4.1.5. Bright.MD

Bright.MD has created a platform to help hospital systems provide asynchronous care to their patients. Their SmartExam software connects the patients, health records, doctors, and status updates. They have also integrated physician SOAP notes, billing, communication, and prescription between SmartExam and EHR systems which is said to cut a company cost.

Figure 8 - Medtech breakthrough award

Company Website: https://bright.md/
Technology: Bright.MD platform that connects to EMR systems.
Area of Focus: Asynchronous care for patients.
Business model: Partnerships with EMR companies and health systems. Revenue coming in through software sales. Pricing could be per visit or dependent on insurance.
Latest News: Bright.MD named "Best Overall Telehealth Solution" in the 2021 MedTech Breakthrough Awards (Figure 8).

4.1.6. Doctors on Demand

Doctors on Demand connects patients to certified physicians regardless of insurance coverage. They cover services under urgent care, behavioral health, preventative health, and chronic care. For the physicians, they have connected their own EHR system. Their services are also covered under many insurances including United Healthcare, Aetna, Humana and Cigna and are covered under the health plans of many companies such as Walmart, American Airlines, and Comcast.

Figure 9 - Simulated Doctors on Demand platform

Company Website: https://www.doctorondemand.com/
Technology: Telehealth software (**Error! Reference source not found.**).
Area of Focus: Urgent care, behavioral health, preventive health, chronic care.
Business model: Partner with employers, labs, and health plans. Pricing can be dependent on insurance.

4.1.7. Lemonaid Health

Lemonaid Health works in three main steps: online questionnaire, doctor review, and medicine delivery (shown in Figure 10). After filling out the online questionnaire about prior health information, the information is reviewed from a US licensed physician in one of the 50 states. After identification of the diagnosis (labs have an additional cost), the patient is presribed medication which is delivered to their home. The patient may pay decreased prices depending on their condition.

Figure 10 - 3 steps Lemonaid health follows

Company Website: https://www.lemonaidhealth.com/
Technology: Application or telehealth platform.
Area of Focus: Cover a select list of conditions found on their website.
Business model: Partnership with pharmacies and labs. Cost of visits depend on reason for visit. Some conditions allow for a monthly subscription.

4.1.8. Livongo Health Inc.

Livongo works to assist patients with chronic conditions to help sustain healthy behavior (Figure *11*). Livongo also has done many clinical trials with all these conditions, yielding better treatment methods and plans. Additionally, Livongo does data analysis on all of its patients of similar chronic conditions to continue improving on its procedure and care.

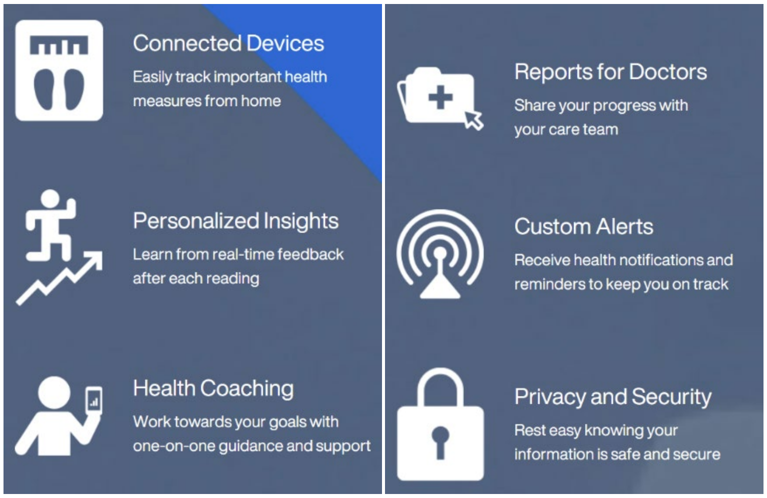


Figure 11 - Services Livongo provides through their platform

Company Website: https://www.livongo.com/
Technology: Software and health management devices (i.e. scale or glucose monitor).
Area of Focus: Patients with chronic conditions (mainly Diabetes).
Business model: Partnerships with other companies such as Teledoc. Potential hardware charges.
Latest News: Livongo is now part of Teladoc.

4.1.9. NutriMedy

NutriMedy is an app that connects users to dieticians and nutritionists. NutriMedy is said to have helped with gastrointestinal, cardiovascular, nephrological, and oncology related conditions (Figure 12). With the use of AI and ML they have been able to automate much of their processes, thus increasing efficiency.

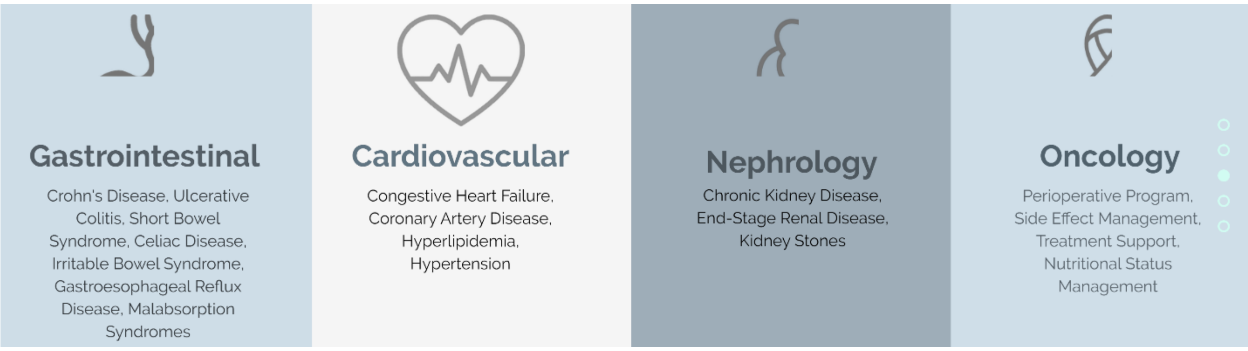


Figure 12 - Conditions NurtiMedy has targeted

Company Website: https://www.nutrimedy.com/
Technology: AI/ML software.
Area of Focus: Improvements to individuals' nutritional health.
Business model: Bringing together dietitians, nutritionaists, educational material, and personal care plans to help manage or prevent chronic conditions.

4.1.10. Philips

As a company with a large reach, Philips has touchpoints in both the hospital and at-home sectors of telehealth. For hospitals, they have intensive care, medical or curgical, eICU analytics and research, emergency department, and skilled nursing facility offerings. Their services are connected through Philips eCareManager. For patients, they offer remote patient monitoring services. Philips utilizes AI in many of their telehealth business, from many of their devices and at-home appliances to patient monitoring technologies.

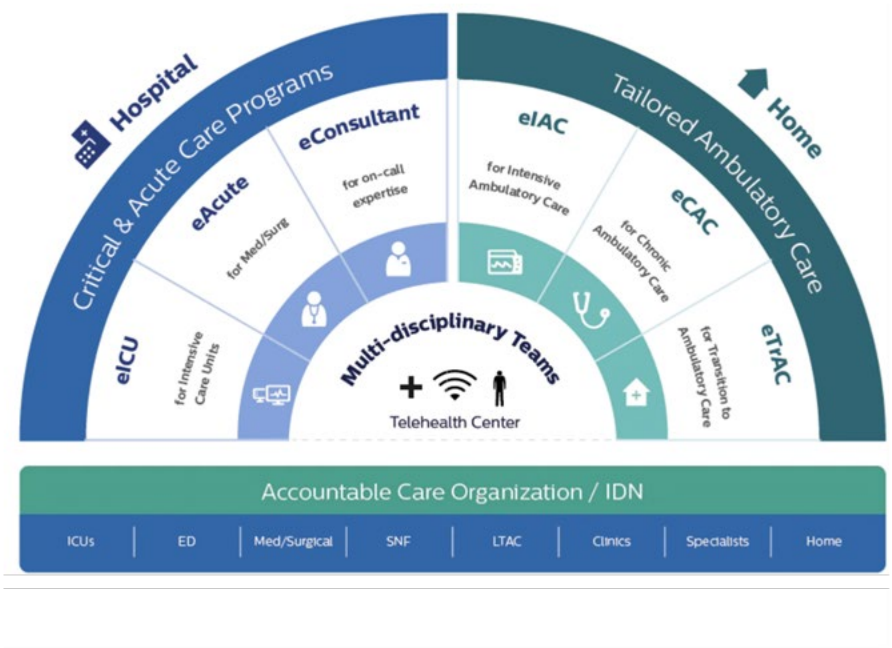


Figure 13 - Philip's enterprise telehealth guide for scaling their infrastructure

Company Website: https://www.usa.philips.com/healthcare/solutions/enterprise-telehealth
Technology: Different levels of technology depending on stakeholder. Hospital telehealth (ICU, surgical, etc.) verses home telehealth (chronic disease management).
Area of Focus: Hospital and home telehealth services for companies (Figure 13).
Business model: Software, hardware, device sales for companies to develop their portfolios. They also potentially provide install and support for their partners.

4.1.11. Premier Health

Premier Health offers video consultation, urgent care, social work, and stroke evaluations within their telehealth services. Patients are also able to use the EPIC-powered MyChart account to set up appointments and connect with their provider.

Company Website: https://www.premierhealth.com/about-premier/about-us/what-is-premier-health/telehealth
Technology: Telehealth software.

Area of Focus: Providers, urgent care, telestroke, telesocial work.
Business model: Connecting patients to their physician's network. Pricing may depend on insurance.

4.2. Canadian Companies

4.2.1. InTouch Health

InTouch Health has integrated their Solo™ software (Figure *14*), medicine devices, and existing EMR systems into their telehealth platform. InTouch provides service covering behavior health, cardiology, convenient care, critical care, infectious disease, neonatology, operating room, specialty follow-up, and stroke. For hospitals they provide implementation, consulting, and physician capacity management.

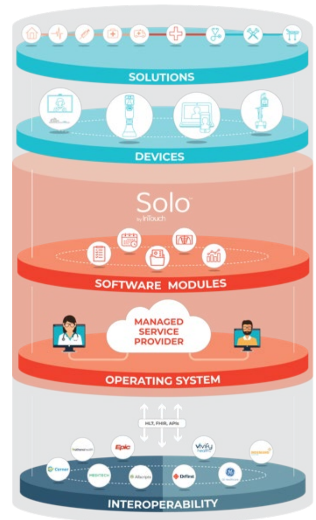


Figure 14 - InTouch Health's integrated platform called Solo

Company Website: https://intouchhealth.com/
Technology: Integrates medical devces, HER systems to offer a unified telehealth platform. Now part of TelaDoc Health.
Area of Focus: Work with hospitals, health systems, and industry vendors
Business model: Charge could be based on level of integration, software installed, or hardware necessary. Work with various hospital systems.

4.2.2. Maple

Maple is a telehealth company that links primary care or emergency medicine physicians to patients through the company's app. Patients are also able to request lab tests for various different conditions for a flat fee of $49. On the hospital end, Maple has integrated their system into existing EMR software while creating a telehospitalist system.

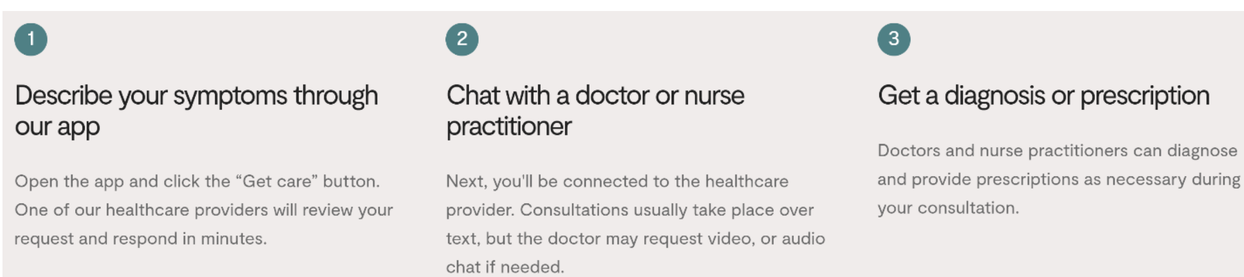


Figure 15 - Description of how Maple works

Company Website: https://www.getmaple.ca/
Technology: Virtual platform (Figure *15*) above highlights how a patient interacts with the platform.
Area of Focus: Various kinds of specialists available on their network.
Business model: Can pay per visit, membership plan, or credit packages. Work with businesses or hospitals.

4.3. International Companies

4.3.1. *Comarch*

Comarch has established itself in many sectors of software development, including healthcare. They have created offerings covering remote medical center, remote medical care, remote cardiac care, remote maternity care, remote care services, medical teleconsultation, and diagnostic points (Figure *16*). Comarch also employs the use of AI and cloud-based analysis within many of their healthcare solutions. Additionally, Comarch has developed their own EHR system to document medical data.

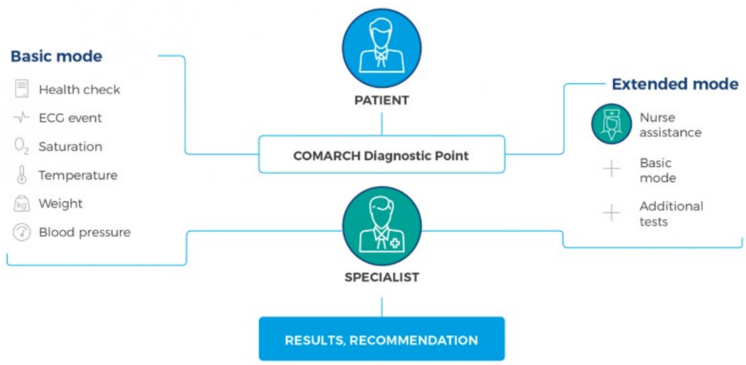


Figure 16 - Workflow of the diagnostic point

Company Website: https://www.comarch.com/healthcare/products/remote-medical-care/
Technology: Physical diagnostic points e-Care platform, heart monitoring software or devices, CTG monitoring device, LifeWristband (security device for patients), etc.
Area of Focus: Diagnostics, cardiology, obstetrics, senior care, pulmonology.
Business model: Selling ready-made solutions (equipment or software), leasing ready-made solutions, or service model.

4.3.2. *Focuscura*

FocusCura is aimed at helping elder people stay independent in their own homes (focusing on virtual homecare and hospital at home) while keeping caregivers, family, doctors, etc. in the loop. They have developed three primary products to support their mission: cAlarm Personal Alarm, cKey Home Access, and cMed Medication Support. The cAlarm is available as a pendant, wristband, or mobile alarm. The alarm system can also connect to a patient's at-home sensors. cKey assures clients that home care workers and healthcare professionals can enter their home when necessary. cMed assists clients take their medication independently with correct dosage and timing.

Figure 17 - Focuscura services

Company Website: https://www.focuscura.com/en
Technology: Personal alarm, home access, medication support, telemedicine (Figure 17**).**

Area of Focus: Supporting aging adult in their home while keeping family, caregivers, and providers informed.
Business model: Sales through devices and software. Also provides installation and support services.

4.3.3. StethoMe

StethoMe is funded through the EU and based in Poland. StethoMe utilizes a smart stethoscope that can monitor respiratory and heart metrics (records BMP and RR). AI and analytic software are used to provide an accurate diagnosis which is then reviewed by a doctor. The smart stethoscope has been clinically validated to be extremely effective in diagnosing conditions and can be used by patients at-home or even by doctors in conjunction with their own analysis. If used at-home in coordination with the app, the patient can send their results to a doctor who will determine what to do next.

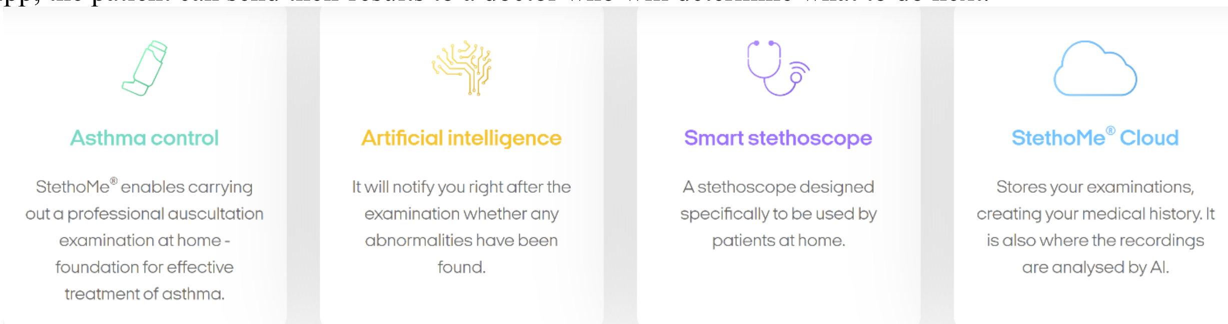


Figure 18 - SthethoMe's technology incorporated into the stethoscope

Company Website: https://stethome.com/en
Technology: Monitoring device, software, cloud storage (shown above in Figure *18*).
Area of Focus: Main focus is asthma monitoring.
Business model: Selling devices to patients while the data is saved in the StethoMe AI cloud Their quality is confirmed by the CE medical certificate and scientific research.

4.3.4. Resideo Life Care Solutions

Resideo Life Care Solutions is a spin-off company from Honeywell focusing on providing security, comfort, and care within someone's home. The main product offered by Resideo is its LifeStream Remote Patient Monitoring (RPM) Solution which connects video and peripherals, clinical dashboard, and Genesis Touch. Through Honeywell, Resideo provides training for organization on how to operate their platform, clinical consulting, and clinical support.

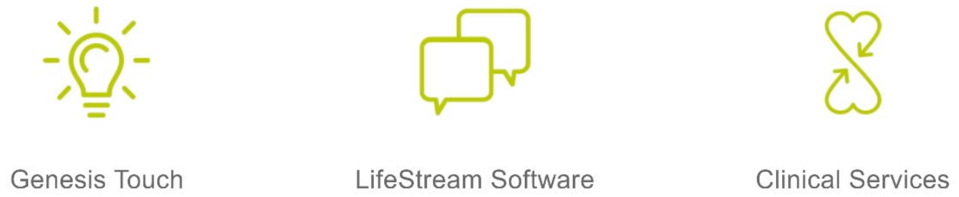


Figure 19 - Resideo Life Care Solution's platform components

Company Website: https://lifecaresolutions.resideo.com/resideo-telehealth-platform/
Technology: Remote patient monitoring software, integrated video communication, peripheral devices and accessories, integrated telemonitoring system.
Area of Focus: Monitoring patient condition in their home.
Business model: Improving patient outcomes using Genesis Touch, LifeStream Software, and clinical services (Figure *19*). They also provide clinical consulting, training, and support.

4.3.5. MyDoc

MyDoc, based in Singapore, offers multiple services to help with chronic care management from health data tracking and digital health screenings to a patient's own personal team of doctors, physicians, and health coaches available 24/7 and integrated chronic disease programs. Their platform allows for case note recording, health diary entry, automated reminders, etc.

Figure 20 - Best Practice Award given by Frost & Sullivan

Company Website: https://my-doc.com/
Technology: Telehealth platform with a wide range of integrated features such as case notes and health concierge services.
Area of Focus: Acute, chronic, and preventative medical services.
Business model: Integrates labs and physicians into the solution. Partners with insurers and their brokers. Works with employers as well.
Latest News: MyDoc was named 2020 Singapore Telehealth Company of the Year by Frost & Sullivan (Figure *20*).

4.3.6. Aerotel Medical System

Headquartered in Israel, Aerotel Medical Systems is a mobile and home-based company that focuses on ECG monitoring, medical parameters monitoring, telecare data hubs, and remote monitoring software. Their main focus is on the growing incident rate of heart related conditions.

Company Website: http://www.aerotel.com/index.php/en/
Technology: Remote ECG monitoring, medical parameter monitoring, telecare data hubs, remote monitoring software.
Area of Focus: Telehealth and ECG monitoring
Business model: Selling devices and software. They also have medical call centers and transtelephonic backup that transfers medical data.

4.4. Company Summaries

	Chronic Conditions	Acute Conditions	Technology	Existing EMR Integration
Labs	LMH **1**	LMH **1**	LMH BEAT MPL MDO **4**	
Pharmacy			LMH MPL MDO **3**	
Doc/ Hospital	ArMD LMD AMWL BMD NMD DonD PrH LOH MPL ITH CMR MDO KPH RLCS **14**	ArMD LMD AMWL BMD DonD MPL ITH MDO KPH RLCS **10**	AMD ArMD LMD BMD AMWL NMD DonD CMR LOH RLCS KPH **11**	AMWL PrH AMD BEAT MPL ITH BMD **7**
Patient	ArMD LMD AMWL NMD DonD PrH LOH BEAT MPL ITH CMR MDO AMS KPH **14**	ArMD LMD AMWL BMD DonD MPL ITH MDO KPH RLCS **10**	ArMD LMD AMWL NMD DonD PrH LOH BEAT MPL ITH CMR MDO AMS KPH STM FCA RLCS **17**	

Aerotel Medical Systems (AMS)	Bright MD (BMD)	Koninklijke Philips (KPH)	NutriMedy (NMD)
AMD Global Telemedicine (AMD)	Comarch (CMR)	Lemonaid Health (LMH)	Premier Health (PrH)
American Well (AMWL)	Doctor on Demand (DonD)	Livongo Health (LOH)	Resideo Life Care Solutions (RLCS)
Arista MD (ArMD)	FocusCura (FCA)	Maple (MPL)	StethoMe (STM)
BioTelemetry (BEAT)	InTouch Health (ITH)	MyDoc (MDO)	

The summary above looks at how companies we analyzed fit when compared against different stakeholders and a few elements of telehealth. We have also listed the companies as reference. When looking at this chart, we designated the green squares as the space where few or none of the companies we analyzed fit in.

After looking at the table above, we created a summary only looking at the spectrum of technology for each company when compared against the same stakeholders as above.

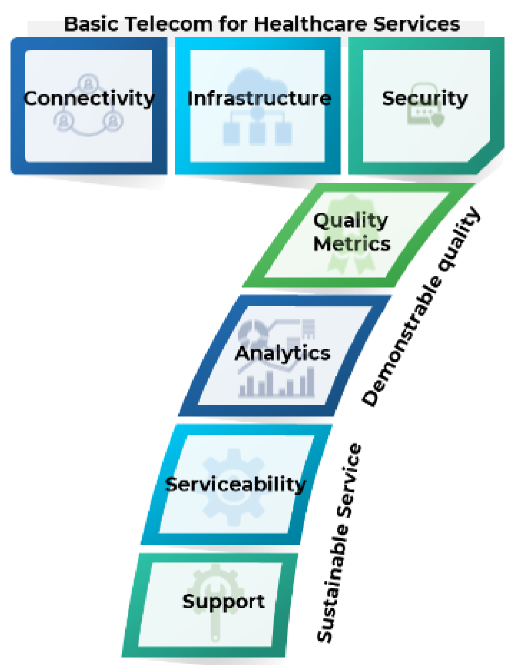
Technology Integration	Patient	Doc / Hospital	Pharmacy	Labs
High	AMWL PrH 2	KPH AMD CMR 3		
Med	ITH STM KPH BEAT RLCS FCA AMS LOH ArMD LMH 10	ArMD 1		LMH 1
Low	CMR DonD MPL NMD MDO 5	LOH BMD NMD RLCS LMH DonD 6	LMH MPL MDO 3	BEAT MPL MDO 3

5. Gaps and Recommendation

5.1. Gaps in Current Solutions

With the sudden growth of telehealth companies during 2020 due to the pandemic, the market made way for different business models; however, in turn the telehealth market became more fragmented. There are companies focusing solely on devices, platform, weight management, etc. The companies we highlighted above are but a fraction of the companies in the market.

After going through various types of Telehealth companies, the charts above highlight some clear gaps within the current market. Overall, there seems to be less intentional integration with lab, pharmacies, electronic health record platforms, and other external entities. On the technology end, we see a similar trend of platforms focusing less on pharmacy and lab services.



At a deeper level, there is room for growth within chronic care management, connection between physicians, device integration, and data analytics.

5.2. Recommendations for Cable Operators

While some cable operators may choose to address some of the aforementioned gaps, we propose a seven-pronged approach: connectivity, infrastructure, security, quality metrics, analytics, serviceability, and support. This approach is based on an in-depth DTS market report [5] we did surrounding the telehealth space. Below we talk at a surface level about how operators can impact the telehealth space with many tools already at their disposal.

Offer the basic Telecom for Healthcare services infrastructure
- Focus on providing highly available and standardized connectivity
- Provide standards-based T4H infrastructure for all stakeholders
- Keep security at the forefront of the solutions to mitigate any concerns of the Healthcare industry

Create a demonstrable quality infrastructure
- Identify, develop and measure the quality metrics for each of the T4H services
- Provide an analytical platform to assist in measuring quality provided by the operators' solutions

Develop a sustainable service infrastructure
- Develop and offer installation services support for the stakeholders
- Develop and offer service support, and maintenance for the stakeholders

6. Abbreviations

AI	artificial intelligence
BMP	beats per minute
ECG	electrocardiogram
ED	emergency department
EMR/EHR	electronic medical/health record
EU	European Union
ICU	intensive care unit
IT	information technology
ML	machine learning
PCP	primary care physician
ROI	return on investment
RPM	remote patient monitoring
RR	respiratory rate
SOAP	subjective, objective, assessment, and plan

7. References

[1] Dave Muoio, *Report: Global Telemedicine Market Will Hit $130B by 2025,* article found
[2] Chiron Health, *An Overview of Telehealth Technology*, article found here
[3] Cisco, *Cisco Study Reveals 47% of Consumers Open to Virtual Doctor Visit,* article found here
[4] American Hospital Association, *The Promise of Telehealth for Hospitals, Health Systems and Their Communities*, article found here
[5] Duke Tech Solutions market Research, *Telehealth market report – A Telecom based opportunity analysis*, available here

Could The Cable Industry Send Zero Waste To Landfill?

Circularity and The Coaxial Cable Recycling Challenge

Letter to the Editor prepared for SCTE by

Kristina Waters, Director, Cox Communications Sustainability, Cox Communications, SCTE Member
6205 Peachtree Dunwoody Road,
Atlanta, 30328
kris.waters@coxinc.com
404-269-1098

Ananya Gupta, Content Management, Ubuntoo Inc.
3365 Piedmont Road NE #1400
Atlanta, Georgia, 30305
ananya.g@ubuntoo.com
(404) 465-3485

Introduction

Building **a [circular economy]** is about regenerating natural systems by designing waste and pollution out of our economic operations and **keeping products and materials in reuse.**

While Cox Communications has actively participated in the circular economy through reuse, refurbishment, and recycling for many years, the cable telecommunications industry has an enormous opportunity for impact by expanding that focus to **entire recycling ecosystems**. With the scale and distribution at which we do business, we can have a major impact on the waste, water, and carbon footprints of our entire industry by re-evaluating how we can incorporate recycled content into new products.

One prime example of a practice that needs our urgent consideration is the estimated **25 million pounds of coaxial cable waste that the cable industry generates each year in the United States.**

Most multiple system operators (MSOs) work hard and responsibly to recycle every scrap of coaxial cable waste. However, many recyclers are only able to upcycle the metals in cables because of the bonded and specialized plastics. Coaxial cable is a composite containing polyvinyl chloride (PVC) or equivalent outer layer, metal braids, aluminum tape, copper or copper-coated steel core, and polyethylene (PE) insulation. These types of cables are most prevalently used in RG-6 and RG-11 cables, deployed across hybrid fiber-coax networks.

While extremely useful for the industry, the multi-material construction of coaxial cables makes upcycling and reuse – preferred elements of a circular economy – a challenge, especially when the cost to send this waste to landfill is so affordable.

The first challenge in achieving a circular economy for coaxial cable is to ensure the highest and best use of purchased materials, materials durability, and that MSOs are using as much purchased product as possible. In 2017, Cox Communications started a collaborative with suppliers and recyclers to begin understanding and addressing some of the systemic challenges that were driving high costs to recycle coaxial cable responsibly. One of several outputs of that collaboration was a new approach to packaging that made it easier for technicians to use 100% of the cable on each reel for interior RG6 coaxial cable.

In 2020, Cox Communications invited Ubuntoo, an environmental solutions platform, to take this challenge to the next level and began the search for technology solutions to **recycle, upcycle, or repurpose waste coaxial cable economically and at scale in the U.S.**

Through this project, we were able to identify four end-to-end recycling ecosystems inclusive of manufacturers (upcyclers) who could potentially accept the recycled plastic from coaxial waste and use it as a feedstock for the construction, asphalt, conduit, furniture, and other industries.

This letter intends to:

- Explain the various hurdles that are limiting the circular use and reuse of recoverable material in coaxial cable;
- Share the discovery process through which we were able to identify solutions to help solve this industry-wide opportunity; and
- Address the long-term systemic change needed in cable manufacturing to eliminate difficult-to-recycle components and achieve true circularity.

1. The Problem

1.1. New-Condition Discards

As Cox Communications began its journey toward circularity, the collaborative team, consisting of manufacturers, suppliers, and key internal stakeholders, completed a study of recoverable materials, identified the most challenging recycling elements, and mapped recycling source distribution. The team also assessed collection methods and gathered feedback from recyclers and downstream processors.

One of the first areas of opportunity identified was recycler feedback regarding the frequent disposal of 20-100 feet long, new-condition coaxial. After observations and interviews with technicians, vehicle space constraints and infrequent warehouse visits due to home start were identified as contributing factors.

1.2. Cable Composition

Coaxial cable is built to last, and with good reason, but our industry struggles to economically recycle up to **25 million pounds of cable waste a year** generated during new installations, rewiring, and network upgrades. The composition of these cables includes metal and different types of plastic (usually PVC), as well as adhesive substances that make the components difficult to separate, making it difficult for each recoverable material to achieve a desirable purity level suitable for reuse.

Figure 1 - Example of Coaxial Cable Composition. Image credit: Cox Communications

While durability cannot be compromised, the multi-material construction of coaxial cable makes it very hard for recyclers to process plastic components cost effectively to the level of purity required for manufacturer feedstock, especially when the expense for recyclers to send these components to landfill is so affordable at approximately **3 cents per pound**. Furthermore, the distributed footprint of these materials makes it even harder to economically collect and transport them to a scale-efficient recycler.

1.3. Recycling Ecosystems

While cable providers recycle coaxial cable waste, recyclers are often key decision-makers in deciding the volume of processed material that will be upcycled into raw materials for new products versus how much goes to landfills. Initiatives by MSOs to improve downstream upcycling rates have been met with several issues within the plastic and metal recycling vendor community. These issues, combined with low commodity values, create economic disincentives for recyclers to upcycle 100% of the content of this material.

First, there has been little done to connect a cohesive ecosystem of end-to-end recyclers of coaxial cable with manufacturing demand for associated plastic commodities. There are no known end-to-end recyclers in the U.S. who, either single-handedly or through partnerships, provide all the required services from start to finish for coaxial cable recycling including: Hauling; aggregation; material separation; chopping; shredding; plastics segregation; granulation; and compounding for upcycling in manufacturing new products.

Furthermore, according to interviews conducted with various stakeholders during the project, recyclers seemed to be far more interested in other materials sent by cable operators and tended to accept coaxial cables for limited periods of time, only as a courtesy. Once the metal is separated from the cable, the waste plastic is considered to have little to no known use and is expensive to process or purify; thus it is not a desirable commodity for recyclers in the U.S.

Such types of waste are therefore generally exported abroad where the purification and potential reuse of the waste plastic from coaxial cables is a more economically viable venture. However, exported waste is difficult to track in terms of the on-ground recycling and reuse. It is therefore a less desirable option from a regulatory standpoint, with a far larger carbon footprint due to the extensive transportation involved.

2. The Solution

2.1. Reduce Unnecessary Discards

The coaxial cable recycling collaborative first tackled the challenge of new-condition discards of interior RG6 in lengths between 20-100 feet. The team stayed true to the technician experience and sustainability as areas they could not compromise. With input from field operations teams and suppliers, the team identified a packaging and technician bag solution for 500-foot reels that reduced the volume of new-condition RG6 in recycling streams by 90%. This solution avoided the unnecessary recycling disposal of almost 300,000 pounds of coaxial cable annually, eliminated packaging waste from disposable 500 foot RG6 reels, and reduced shipping costs and materials, all while improving the technician experience.

2.2. Composition and Recycling Ecosystem Challenges

To find solutions to issues within the recycling ecosystem that were exacerbated by difficult-to-separate components, Ubuntoo conducted a comprehensive search for information about existing or potential solutions for recycling coaxial cable.

Figure 2 – Home page of Ubuntoo GreenHouse tool. Image credit: Ubuntoo

By conducting in-depth interviews with cable waste collectors, recyclers, and upcyclers, Ubuntoo mapped out the **landscape of stakeholders that must come together to achieve end-to-end recycling of coaxial cable waste**. This landscape is shown in **Ubuntoo's GreenHouse tool,** which helped document the information and keep the Cox team informed about progress in real time, with cloud-based access to an integrated feed of solutions, news, and knowledge uncovered through the discovery process.

Preview the platform [HERE.]

2.3 The Short-Term Solution: Recycling and Upcycling

Since coaxial cables in their current form are ubiquitous across the industry's hybrid fiber coax (HFC) plant, the priority of this project was to map out and connect end-to-end recycler ecosystems to responsibly address the waste associated with the cable industry.

Figure 3 – Cable Recycling Ecosystem. Image credit: Cox Communications & Ubuntoo

As part of the initiative, vendors were evaluated on the following criteria:

- **Accountability**: Vendors who — either single-handedly or through partnerships — were willing to take ownership of end-to-end coaxial cable recycling including logistics, recycling, and upcycling ranked higher than competitors during the evaluation.
- **Purity and Minimal Waste to Landfill:** Vendors with the equipment and capacity to minimize the cross-contamination of materials through the recycling process such that the resulting materials met upcycler requirements scored well during evaluation. The higher the purity percentage, the more likely the recycled product could be used in other products. Thus, recyclers who could promise lower levels of material contamination and therefore lower waste-to-landfill quantities scored higher. Furthermore, vendors who were open to transparent reporting, audits, and penalties upon failing to meet these commitments ranked better during evaluation.
- **Volume Capacity and Readiness:** Vendors who could commit to building the capacity to process large volumes of coax waste generated across multiple providers in multiple regions ranked better in the evaluation than others.

- **Location diversity:** Vendors who had recycling facilities that corresponded with Cox sites across the U.S. scored better during evaluation. Furthermore, vendors whose operations were exclusively in the U.S. were preferred from a regulatory and carbon footprint standpoint.
- **Industry commitment:** Vendors who could commit to having the coaxial recycling line be a stand-alone venture rather than an investment contingent upon gaining business in other recyclable asset categories scored better during evaluation than competitors.

Through this exercise we were able to identify four end-to-end recycling ecosystems across various stages of development. Additionally, the process also yielded a network of upcyclers who could potentially accept the recycled plastic and use it as a feedstock for the construction, asphalt, carpet, conduit, furniture, and other industries.

While some of these recyclers are already working on this solution, others are hesitant to make the necessary capital investments in this line of recycling without a sizable volume commitment from the cable industry. **We need the full force of the cable industry to incentivize end-to-end recyclers to build the capacity to address the entire scope of the coaxial cable waste problem.**

As part of this process at the time of this publication, Cox Communications is working on an RFP with these end-to-end recyclers to select vendors to achieve their zero waste-to-landfill commitment by 2024. However, Cox generates only a small fraction of the total coaxial waste in the United States. **With the support of other cable providers, this initiative can scale to address the entire weight of the coaxial cable waste problem.**

2.4 The Long-Term Solution: Manufacturing

It is no secret that the cable telecom industry has very addressable carbon footprints due to their high electricity and transportation costs. Significant efforts have been made to address the energy concerns over the last several years. However, nearly half of the industry's emissions are a result of the upstream supply chain including capital goods and other goods and services that produce upstream fuel emissions.

According to Economic Input-Output Life Cycle Analysis data, upstream supply chains drive up to 2.3x more carbon, 80 times more water, and 97 times more waste impact than internal Cox Communications operations. **This story is likely similar across the industry.**

While recycling and upcycling ecosystems are the necessary solution to solve the existing problem of coaxial waste, in the long run, it is important to envision a world in which the cable industry does not need to generate such waste.

Conclusion

If the cable industry is to achieve true circularity, **cable manufacturers must get involved.** Whether it is finding a way to use recycled cable waste as a feedstock within the industry itself, or re-engineering cable entirely to eliminate difficult-to-recycle components, this initiative has the potential to begin a new, sustainability-driven era for the cable telecom industry.

Cox Communications invites its peers, industry suppliers, and SCTE to support a movement toward circularity in the products we buy, use, and recycle, starting with one of our most challenging materials, coaxial cable so that we can all build a better future for the next generation while delivering the critical broadband and communications services on which the world depends.

SCTE STANDARDS
JOURNAL

SCTE
a subsidiary of CableLabs®

140 Philips Road | Exton, PA 19341-1318 | 800.542.5040 | scte.org