Version	Date	Changes	Description
V1	6/24/2015	Initial version	Initial version
V2	6/29/2015	Edited section “Technologies (Network) that enable the reception of MVPD or OTT service” to remove redundancies to WG2 Report #1, Table 1 Section 1 edited, comments added to	Co-editor Version plus edits on 6/24 call
V3	6/29/2015	Consolidated edits from multiple sources	Distributed to WG4
V4	7/1/2015	Added RVU [Zerbe], proposed changes from CableVision (marked as username PG), Part III Section II, and use cases from V7 document. Accepted formatting changes (all but 2, can’t find 1,other won’t accept)	For call on July 1st
V5	7/1/2015	Removed large scale deletions that duplicated WG2	Edited during July 1 call

REPORT OF WORKING GROUP 4 TO DSTAC

DRAFT

July 7, 2015

Part I: Existing Devices and Technologies

Identify the salient differences important to implementation of the non-security elements of a system of such devices based on downloadable security.

EXPECTATIONS: SECTION I

As most members generally understand the functionality of the devices listed in Part I, it is expected that information would be provided as to how the devices discover and receive content.

As content is coming in on different input ports and through different applications running on the devices, the mechanisms for each should be detailed.

Various points have been captured in the "Part I section I Table".

Part I: Section I. Devices that receive MVPD or OTT service

Description	Supports Direct Attach to MVPD Network	Supports Direct Attach to Managed IP Network	Supports Direct Attach to OTT Network	Supports Local Network Connectivity	Uses Custom Apps	Uses HTML 5 Apps	Uses Local MVPD Guide	Uses Remote UI	Allows User to Make Local Recordings	Provides Access to Network PVR from Competitive Navigation UI	Supports Navigation of MVPD Linear Service by 3rd Party UI App	Supports 3rd Party Apps	Supports 3rd Party Access Not listed	Works across MVPD Network Technologies (Cable, IPTV, Satellite)	Portable across MVPDs (within Cable or within Satellite)	Supports ATSC Tuner and Guide Integration	Supports National EAS	Universal Remote Control Support	Supports Multiple Tuner Management and Conflict Resolution	Supports archiving customer-recorded content to external storage
MVPD provided Set-top Box	Yes	YES**	Yes	YES	Yes	(Some) YES	Yes, if PVR	No	Yes	No	No	(Some) YES	(Some) YES	No, MVPD Network Technology specific	(Some) YES	(Some) YES	Yes	Yes	Yes, in whole home DVR	No
High Definition and 4K Ultra HD TV – for IP and other delivery paths	No (assumes Clear QAM no longer possible)	No	Yes, smart TV	DLNA	Yes (OTT) No (Next Gen Android TV)	No	No for MVPD, creates one for over-the-air Broadcasts	No	No	N/A	No	Yes, smart TV	Yes, smart TV based on Android	HDMI, VidiPath, Rvu	HDMI, VidiPath, Rvu	Yes, a guide can be generated by scanning channels and using event information tables	Yes	Yes	Usually a single tuner now, PiP feature is gone	Japanese, European Models
RVU certified TV	Home Network	No	Yes, smart TV	DLNA	Yes, RVU	No	Remotely	Yes, with RVU application	No	N/A	with DirecTV SHEF protocol	Yes	TBD	if RVU used	if RVU	Not RVU Feature	Yes	Yes	Same	Not RVU Feature
VidiPath certified TV	Home Network	Yes	Yes, smart TV	DLNA	Yes, VidiPath (DLNA)	Yes, VidiPath for RUI, VidiPath 2.0 will have cloud/DRM capability	Remotely	Yes, DLNA + HTML 5	Spec provides a recordable DTCP-IP output. Not yet implemented in TVs.	No	No	Yes	TBD	if VidiPath used	if VidiPath	Not VidiPath feature	Yes	Yes	Same	Not VidiPath feature
Home Media Server (Content Server on Home Network)	Yes	Yes	Yes	Yes	Yes	Yes	Yes, plus additional guide data provided via broadband	Yes, for serving client devices	Yes	Yes for various cable systems, No for current satellite delivered services	Yes (custom MVPD-provided custom API)	Yes (custom MVPD-provided custom API)	TBD ??? - unsure of the purpose of this column	No, except for certain OTT-provided services	No	Yes	Yes	Yes	Yes	Yes
Home Video Gateway from MVPD, Residential Gateways (RG)	Yes	Yes	Yes	Yes	No	Yes (some)	Yes	Yes (some)	Yes	No	No	No	No	No	No	No	No	No	No	No
AT&T DSL gateway includes wifi access																				

Digital Transport Adapter (DTA)	Yes	No	Yes	Not currently	Yes	Not currently	No	No	Not currently	No	No	No	No	No, cable specific technology	Yes	No	Yes	Yes	No	No
Simple Digital Video Recorder from MVPD	see above	see above	see above	see above	see above	see above	see above	see above	see above	see above	see above	see above	see above	see above	see above	see above	see above	see above	see above	see above
Retail Whole Home DVR Ecosystem (Tivo)	Yes	No	Yes	Yes	Yes	Yes	No	Yes, for VOD and OTT	Yes	N/A	Yes	Yes	Yes	No	All Cable	Yes	Yes	Yes	Yes	Yes
Media Player Box from Retail (Roku, Apple TV, Amazon, WD)	No	Yes	Yes	Yes	Yes	Yes	No	No	Some - This is software dependent and highly variable, but coming to more current-run devices via software.	No, access via MVPD /OTT app	No, access via MVPD /OTT app	Yes	Yes	HDMI, local or network gateway	HDMI, local or network gateway	With ATSC gateway	Software (and gateway) dependent.	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	Variable (software and hardware specific)
Media Player Sticks (USB/HDMI)	No	Yes	Yes	Yes	Yes	Yes	No	No	Some - This is software dependent and highly variable, but coming to more current-run devices via software.	No, access via MVPD /OTT app	No, access via MVPD /OTT app	Yes	Yes	HDMI, local or network gateway	HDMI, local or network gateway	With ATSC gateway	Software (and gateway) dependent.	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	Variable (generally not local storage, but network storage)
Connected Tablet with Data Plan	No	Yes	Yes	Yes	Yes	Yes	No	No	Software dependent (rare)	No, access via MVPD /OTT app	No, access via MVPD /OTT app	Yes	Yes	HDMI, local or network gateway	HDMI, local or network gateway	With ATSC gateway	Software (and gateway) dependent. (May also support WEA)	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	Variable (local MMC/SD or network storage)
Connected Tablet with Wi-Fi	No	Yes	Yes	Yes	Yes	Yes	No	No	Software dependent (rare)	No, access via MVPD /OTT app	No, access via MVPD /OTT app	Yes	Yes	HDMI, local or network gateway	HDMI, local or network gateway	With ATSC gateway	Software (and gateway) dependent.	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	Variable (local MMC/SD or network storage)
Connected Smart Phone with Data Plan	No	Yes	Yes	Yes	Yes	Yes	No	No	Software dependent (rare)	No, access via MVPD /OTT app	No, access via MVPD /OTT app	Yes	Yes	HDMI, local or network gateway	HDMI, local or network gateway	With ATSC gateway	Software (and gateway) dependent. Generally required to support WEA.	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	Variable (local MMC/SD or network storage)
Connected Smart Phone with Wi-Fi	No	Yes	Yes	Yes	Yes	Yes	No	No	Software dependent (rare)	No, access via MVPD /OTT app	No, access via MVPD /OTT app	Yes	Yes	HDMI, local or network gateway	HDMI, local or network gateway	With ATSC gateway	Software (and gateway) dependent. May still support WEA.	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	Variable (local MMC/SD or network storage)

Broadband Connected Blu-Ray Players	No	Yes	Some	Some	Some	Some	No	Yes	No	No, access via MVPD /OTT app	No, access via MVPD /OTT app	Yes	Yes	HDMI, local or network gateway	HDMI, local or network gateway	With ATSC gateway	Software (and gateway) dependent.	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	With computer/gateway assistance (e.g. Plex, Kodi)
Notebook or Laptop Computer (Apple, Windows, Linux)	No	Yes	Yes	Yes	Yes, but less common usage	Yes	No	No	Yes	No, access via MVPD /OTT app, except w/Windows /OCUR	No, access via MVPD /OTT app, except w/Windows /OCUR	Yes	Yes	HDMI, local or network gateway	HDMI, local or network gateway	With ATSC gateway or built-in/optional tuner (PCIe, USB, etc)	Software (and gateway) dependent.	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	Yes
All-in-One or Desktop Computer (Apple, Windows, Linux)	No	Yes	Yes	Yes	Yes, but less common usage	Yes	No	No	Yes	No, access via MVPD /OTT app, except w/Windows /OCUR	No, access via MVPD /OTT app, except w/Windows /OCUR	Yes	Yes	HDMI, local or network gateway	HDMI, local or network gateway	With ATSC gateway or built-in/optional tuner (PCIe, USB, etc)	Software (and gateway) dependent.	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	Yes
Gaming Consoles (PS4, Xbox)	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes (Some)	No, access via MVPD /OTT app, except w/Windows /OCUR	No, access via MVPD /OTT app, except w/Windows /OCUR	Yes	Yes	HDMI, local or network gateway, or HDMI passthrough	HDMI, local or network gateway	With ATSC gateway or USB tuner	Software (and gateway) dependent.	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	Yes
Connected AV Receivers	Yes, radio No, AV	Some	Some	Yes	Some	No	No	No	No	No	N/A	N/A	N/A	HDMI	HDMI	N/A	N/A	N/A	N/A	N/A
Internal/External Tuners (Hauppauge, Silicon Dust, Sat-IP)	Yes	No	no	Via 3rd party service*	Via 3rd party service*	Via 3rd party service*	Not from MVPD Guide, sourced externally via 3rd party service	Via 3rd party service*	Via 3rd party service*	no, Linear only	Via 3rd party service*	requires 3rd party app...	NA	Some tuners support more than one DBS/terrestrial/Cable standard	OCUR on Cable					
External/External Tuners (Hauppauge, Silicon Dust, Sat-IP)	Yes	No	no	Yes; DLNA, DTCP-IP, OCUR/DRI, or custom protocols	3rd party client apps supported	Via 3rd party client	Not from MVPD Guide, sourced externally via 3rd party service	Via 3rd party client implementation	Via 3rd party client	no, linear only	Via 3rd party client using dlna or OCUR/DRI	requires a client	NA	Some tuners support more than one DBS/terrestrial/Cable standard???	OCUR on Cable					
	(*) 3rd party services for internal/external tuners can be protocol based servers or direct clients such as:																			
	- VLC media player client																			

	- DLNA Digital Media Servers																			
	- Windows Media Center																			
	- Windows Media Player																			
	- Command line tools																			
	- Custom applications (Hauppauge WinTV, etc)																			

[

Part I: Section II. Technologies (Network) that enable the reception of MVPD or OTT service (see WG2 report):

Discussion of important features of specific technologies

A. Operator Network Technologies

SUMMARY

As noted in WG2 Report Section III starting on page 3, there is variation in current video providers' distribution technologies and platforms. Across all service providers, an approach that has developed for delivering video service to customer owned devices is through "apps."

Diversity of Access Network Technologies [45]

As noted in WG2 Report in Section III starting on page 4, the larger US Cable operators and Verizon mostly use one or both of two the two primary CAS (Conditional Access Systems) vendors, and all support CableCARD for limited services. Both US Cable and Verizon use Quadrature Amplitude Modulation (QAM) for broadcast signals while over Hybrid Fiber Coax (HFC) or B/GPON (Broadband-/Gigabit-capable Passive Optical Networks) fiber networks. Verizon adds hybrid QAM/IP for on-demand content and two-way services. Direct Broadcast Satellite (DBS) also has two major variants for transport and CAS. AT&T uses IP unicast and multicast over DSL or B/GPON fiber, with a Digital Rights Management (DRM) approach instead of CAS.

Despite this diversity in network technologies, several MVPDs have demonstrated gateway devices that can translate these various technologies into common IP protocols. An MVPD could provide a device that converts their transmission method into a common IP protocol over the home network, for example as is done in VidiPath servers. Furthermore, MVPDs have stated they are moving towards transmission of services over IP, as OTT providers already do. Therefore these different network technologies are converging onto IP. **Diversity Of Customer Equipment Installation, Provisioning, And Configuration Methods [45]**

The diversity of network technologies across and within MVPDs is associated with a diversity of Customer Premise Equipment (CPE) installation, provisioning, and configuration methods. Table 1 shows the equipment necessary for network termination at the premise, the CPE deployed for the Pay TV service and the technologies used for in-home distribution of the service.

MVPD	Network Termination	Customer Premise Equipment (CPE)	In-Home Distribution
Cable	Coax & RFoG Optical Network Termination (ONT)	DVR & Non-DVR set-tops, DTA and Cloud Based systems IPTV Set tops	Cable RF & MoCA Wi-Fi
Satellite	Out Door Unit (ODU) – Satellite Dish Low noise block down-converter (LNB) Multiswitch (RF switching unit)	Genie Server (DVR) & Genie Mini clients Hopper (DVR) & Joey clients	802.11 & MoCA MoCA Wi-Fi
Telco	VDSL Modem or Gateway B/GPON Optical Network Termination (ONT)	DVR & Non-DVR IPTV set-tops	802.11 Cable RF & MoCA Wi-Fi
Google Fiber TV	GPON Optical Network Termination (ONT)	Network Box, Storage Box, TV Box	802.11 & MoCA

Table 1 - Diversity of MVPD Customer Premise Equipment

Cable networks are typically terminated at the house at the point of entry with coax cabling. In some instances cable networks use RF over Glass (RFoG), an analog RF fiber to the premise technology. The RFoG Optical Network Termination (ONT) converts the optical RF to an electrical RF signal over coax permitting the use of traditional cable QAM based CPE. Cable systems make use of both DVR and non-DVR set-top boxes that receive broadcast signals and use MoCA technology to link them together for a whole home DVR solution.

Satellite networks terminate in Out Door Units (ODU) satellite dishes. Low Noise Block down-converters shift the satellite signals to a frequency band that can be switched by a Multiswitch unit and distributed via coax cables to the various satellite CPE. Satellite systems make use of both DVR and non-DVR set-tops and use both MoCA and 802.11 Wi-Fi for distribution in the home for a whole home DVR solution. The satellite MVPDs also have client software available in some LG, Samsung, Sony and Toshiba TVs that allow them to access services through their home network either using RVU or Virtual Joey technology.

Telco networks are typically either traditional telephone twisted-pair copper or B/GPON FTTP networks. In the case of twisted-pair, the network is terminated by a VDSL modem or

gateway in an IPTV solution making use of both DVR and non-DVR IPTV set-tops and use 802.11 Wi-Fi for distribution in the home for a whole home DVR solution. Twisted-pair networks also need a filter installed to block the VDSL signal from telephones in the home. In the case of fiber networks, the network is terminated in an ONT and, in the case of FiOS, the optical RF spectrum is converted to electrical RF spectrum and distributed over coax, similar to the cable RFOG case. Fiber networks may use either Hybrid IP/QAM based set-tops (DVR and non-DVR) and MoCA for distribution in the home for a whole home DVR solution or the same IPTV based set-tops and 802.11 Wi-Fi distribution as in the twisted-pair case. In Hybrid IP/QAM based set-tops, each set-top box includes two interfaces: an interface to the overlay wavelength for linear services and certain control signaling; and an IP interface for IP VOD, widgets, guide data, gaming, and certain control plane signaling. All of these are integrated into a single service within the set-top box.

While all MVPDs would like for consumers to be able to self-install the necessary equipment to receive the MVPD service, this is not always a practical option for a number of reasons. First, if this is the first time a customer has subscribed to an MVPD service, it may be necessary to install the necessary network termination equipment, whether this is a cable drop, a fiber drop and an ONT, a VDSL modem/gateway and filters, or a satellite ODU, LNB, and Multiswitch. In addition to this, it may be necessary to wire the home with coax cable to distribute the signal from the point of entry to the various rooms in which service is desired. Even if the home has been previously wired for cable service, the need to insure that signal levels are appropriate or alignment of the satellite ODU is correct is still required.

Provisioning of set-top boxes also varies across and within MVPDs. There are two basic kinds of provisioning necessary in an MVPD system. The first is network provisioning so that the set-tops are properly connected to the network and can communicate properly. The second is provisioning of entitlements so that subscribers can access the services to which they are subscribed. Network provisioning is typically specific to the type of network and CAS system deployed, while provisioning of entitlements is exclusively the domain of the CAS system deployed. Configuration methods are also specific to the type of network and CAS system deployed.

Common Approaches to Retail Devices [45]

As detailed in the DSTAC Working Group 2 Report #1 [45] the As noted in WG2 Report in Section VI starting on page 12, for some service providers an approach for delivering video service to customer owned devices is through “apps.” However some DSTAC members do not believe the App approach meets the requirement of enabling a competitive navigation device as the only choice for consumers is the user interface of the MVPD’s app. It is the user experience and application features that enable competition, not simply the ability to launch the MVPD’s app.

MVPDs are remarkably similar in their approach to supporting retail devices, following the successful model that OTT video distributors such as Netflix, Hulu, and others use. See WG2 Report Section IV Part B on page 7, and Section XII on page 24 which describe CAS and DRM Trust Infrastructures.

CABLE TECHNOLOGIES AND ARCHITECTURES [46]

Cable systems have evolved over the decades since the first cable systems in 1940s. Most cable operators have upgraded their networks to two-way, Hybrid Fiber Coax (HFC). However, this evolution was not uniform across the United States and there is some diversity across cable operators. Figure 5 shows the typical HFC cable network architecture.

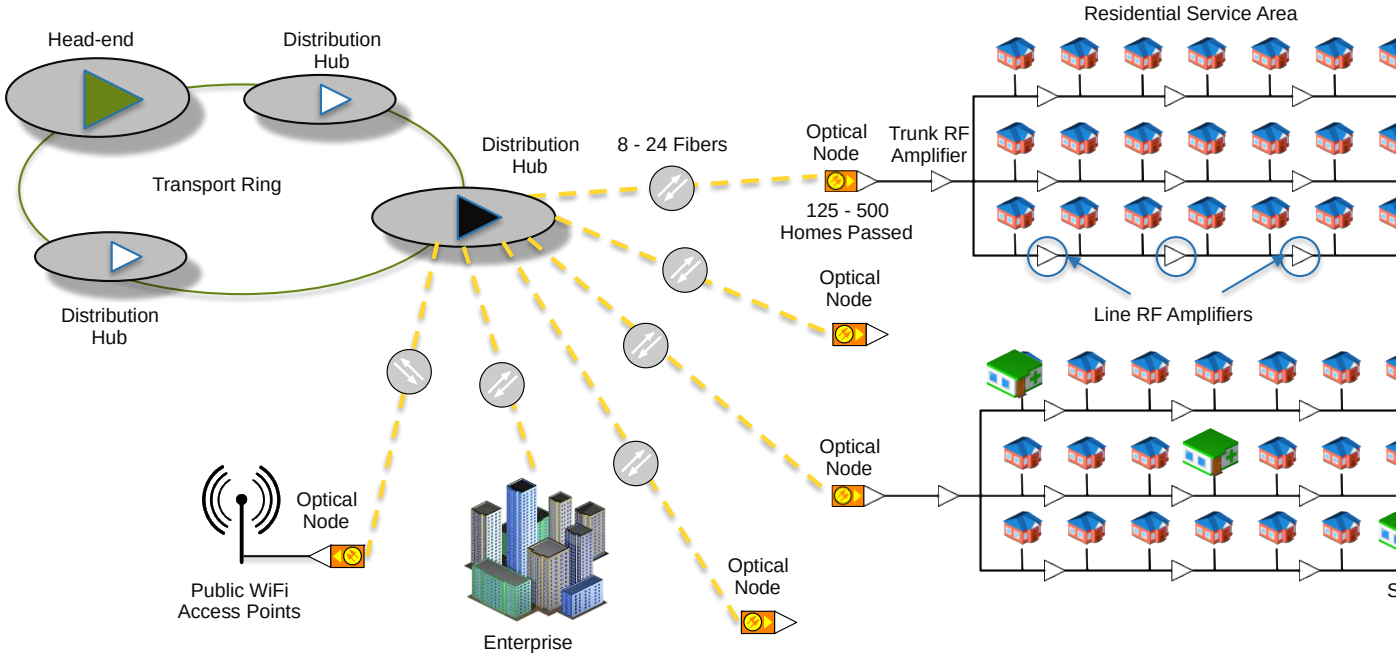


Figure 1 - Typical Cable System Network Architecture

Cable system architectures reflect fundamental differences dating from the original design goals based on different vendors and different owners. The General Instruments (now ARRIS) design was tailored primarily for the more rural and less clustered systems owned by Tele-Communications, Inc., with a focus on increased channel capacity, minimized head-end cost, and centralized set-top control and authorization. The Scientific-Atlanta (now Cisco) design was tailored primarily for the more urban and clustered systems primarily owned by Time Warner Cable, with a focus on two-way interactive services such as Video-on-Demand (VoD), the ability to add applications and services to set-top boxes over time, and local control and authorization. Thus, even though there are some shared elements, such as MPEG-2 video compression, there are fundamental differences in technologies for CAS, controllers, the out-of-band (OOB) communications channels used for command and control of the set-top box, network transports, QAM modulation, video codecs, core ciphers, advanced system information such as network configuration, session management, operating system, processor instruction set, interactive services, billing systems, applications necessary for presentation of services and in the set-top boxes. [3]

The respective design objectives resulted in proprietary systems that had different system architectures and network configurations, as well as different CAS systems, as described above. Despite these different design goals there were also a significant number of common elements:

- The GI and SA systems used MPEG-2 video compression and Dolby® AC-3 audio compression [6,7].
- Both systems have added support for MPEG-4/AVC in the intervening years [8].
- Both systems used QAM modulation for transmission of MPEG-2 transport streams carrying the audio/video signal [9].
- Both systems used variants of Data Encryption Standard (DES-64) [10] encryption as the working cipher for their CA systems and in particular both were capable of supporting the SCTE 52 2008 DES-CBC variant [11].
- Both systems used a common Service Information format to communicate channel line-up information [12].

However, because of the different design goals, there were many proprietary components remaining in each system.

The proprietary aspects of the two systems largely lay in following areas:

- The CAS system (DigiCipher™ II in the case of GI and PowerKey™ in the case of SA) used to control subscriber entitlements and manage access to digital channels.
- Their out-of-band (OOB) communications channels used for command and control of the set-top box:
    - GI's system implemented the DigiCipher II OOB utilizing an MPEG structure for transporting OOB messaging downstream, standardized as ANSI/SCTE 55-1 2009 [13]. The GI OOB channel provided 2Mbps downstream bandwidth and 256Kbps upstream bandwidth through an Aloha, polled communication protocol.
    - SA's system implemented a DAVIC based OOB utilizing an ATM/IP structure for transporting OOB messaging downstream, standardized as ANSI/SCTE 55-2 2009 [14]. The SA OOB channel provided 1.5 Mbps bandwidth in both the downstream and upstream using a real-time, two-way protocol.
- Operating system (OS) and processor instruction set:
    - GI's system initially implemented a proprietary kernel on a Motorola 6800 processor instruction set.
    - SA's system initially implemented the PowerTV™ OS on a Sun SPARC™ processor instruction set.
    - Subsequently, both system providers have introduced other OS (e.g. Linux) and processor instruction sets (e.g. MIPS).
- Network control architecture in support of interactive applications, such as VoD and Switched Digital Video (SDV):
    - GI's network control architecture lacked the concept of an interactive session manager, requiring third-parties to provide this component when integrating session-based services, such as VoD.
    - SA's network control architecture implemented an interactive session manager, supporting DSM-CC User-to-Network commands for support of dynamic MPEG transport sessions.

- Electronic Program Guide (EPG) application and EPG metadata format.

Integration of interactive service components, such as a VoD application and corresponding video streaming servers, required tight integration with either GI or SA's network. This resulted in pair-wise integrations between VoD vendors, set-top applications vendors, and the digital video systems providers.

Existing cable systems have now evolved in ways that vary widely from the legacy system architectures that were just described. One major difference is the use of the Common Scrambling Algorithm (CSA) in some systems, rather than core ciphers based on DES. In addition, many systems incorporated content delivery components from multiple vendors, which has lead to much more diversity in session control, bandwidth management, maintenance, commercial insertion, VOD and other critical system hardware and software.

To attempt to address the issue of interoperability across cable systems, CableLabs developed a set of specifications under the OpenCable program [15]. These specifications isolate the proprietary system specific aspects of these systems into separable components. The systems specific aspects fall into two general categories:

- Hardware – These included, the core hardware components of the CA system (working cipher and key hierarchy) and the key components of the OOB communications network (e.g. forward error correction and MAC layer processing)
- Software – These included, Operating System (OS) and applications (both cable operator specific and potentially third-party applications)

Figure 2 provides a block diagram identifying the key interfaces in the OpenCable architecture.

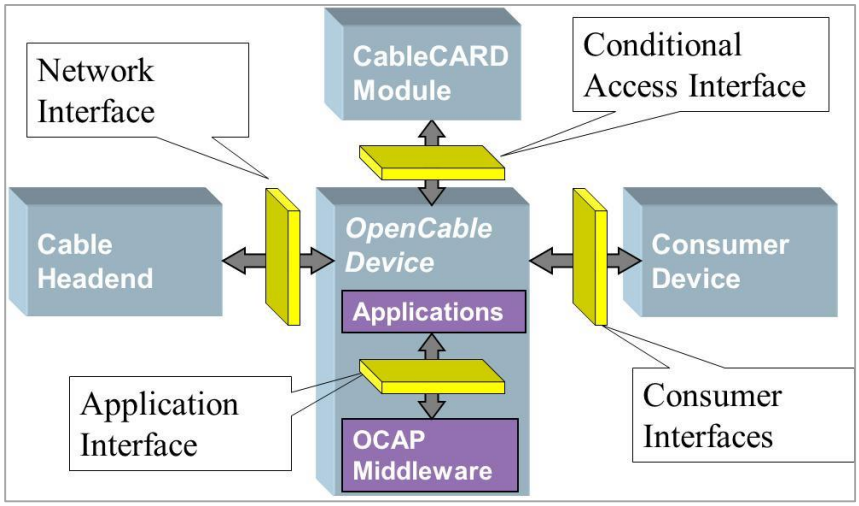


Figure 2 - OpenCable/tru2way Interface Diagram

The four interfaces specified by OpenCable:

- The Network Interface – This is the interface that connects to the cable network at the consumer's home and is specified as part of the OpenCable Host Specification.
- The Consumer Interfaces – These are the interfaces that connect to the consumer's TV or other entertainment devices (e.g. HDMI, component analog, composite analog, etc.) and are also specified as part of the OpenCable Host Specification[16].
- The Conditional Access Interface – This is the interface to the system-specific CA and OOB channel and is specified in the CableCARD™ Specifications.
- The Application Interface – These are the Application Program Interfaces (APIs) that applications use to perform the desired functions using the Host and CableCARD components and are specified by the Open Cable Application Platform (OCAP) specification.

In this architecture, an OpenCable Host device is enabled to connect to the cable network by providing a hardware component, the CableCARD, which is specific to the proprietary system deployed in that cable network. Originally, this would be either a GI or SA CableCARD; however other CA systems, such as NDS and Conax, have been added to this list over time. The CableCARD cryptographically binds to the Host for security and copy protection purposes and instructs the Host how to acquire the OOB communications channel, register on the network, and receive the OOB command and control signals appropriate for the CA system. The Host is then able to acquire the list of applications, for example the EPG, which are supported on the cable system, securely download them if necessary, and begin execution.

The CableCARD is the hardware module in the OpenCable system that achieves this isolation through a physical encapsulation of the cryptographic CA component and some portions of the OOB communications channel. The CableCARD by necessity had to be a separable or removable module that could be delivered independently from the Host device. In practice, the local cable operator provides the CableCARD.

The only commonality the two proprietary OOB channels have is the use of QPSK modulation; they differed in the frequency band and bandwidth, the Forward Error Correction (FEC), the framing, and the transport protocol used. Consequently, the QPSK front-end (modulation and demodulation) was placed in the OpenCable Host and all of the higher layers of the proprietary OOB communications protocol stack were placed in the CableCARD. Raw QPSK symbols and their timing passed across the PCMCIA interface through the use of redefined pins in the physical interface. The CableCARD is responsible for instructing the Host what mode of operation the system requires. OpenCable also enabled the cable operator to migrate the proprietary messaging carried on these proprietary OOB channels to a standard two-way communications channel, such as Data-Over-Cable Service Interface Specification (DOCSIS®). This was accomplished through the DOCSIS Set-top Gateway (DSG) with the appropriate modifications to the CableCARD [19]. Since DOCSIS provides an efficient two-way IP connection for devices, the DSG specification focused on extending the DOCSIS specification to perform two key functions:

- Encapsulate the downstream proprietary messaging in an IP transport using a broadcast or multicast transmission so that all set-tops could access it concurrently.

- Provide a one-way mode of operation so that the set-top could continue to function in a one-way mode in cases of network disruption.

EIA-679 Part B only permitted the decryption and processing of a single MPEG Multi-Program Transport Stream (MPTS), equivalent to a single set-top tuner. The original CableCARD specification followed this model with single stream mode, or S-Mode, of operation. As Digital Video Recorders (DVRs), picture-in-picture, and other multi-tuner features were developed, it was realized that the original S-Mode CableCARD had inadequate bandwidth for these features. It would require multiple S-Mode CableCARDs to provide this capability and could not grow to support multi-tuner gateway scenarios. Subsequently, the M-Mode (or Multi-stream mode) CableCARD specification was developed and has its origin in SCTE 28 [20]. M-Mode provides the higher transport data throughput rates that are required to support features, such as multiple-tuner Hosts, Hosts with DVRs, and Hosts with picture-in-picture capability.As described inSee also DSTAC Working Group 2 Report #1 [45].

SATELLITE TECHNOLOGIES AND ARCHITECTURES [52]

As was summarized in DSTAC Working Group 2 Report #1 [45], there are two primary Direct Broadcast Satellite (DBS) providers in the United States, DISH and DirecTV. While they use similar technologies and architectures to deliver the DBS portion of their service, there are still sufficient differences in the two systems as to prevent a set-top box designed for one system from working on the network of the other. As described in more detail below, both the SAT-IP project under DVB and the VidiPath initiative demonstrate that it is possible to convert the differences in broadcast systems into a common IP format for in-home devices, terminating the network variances at a gateway device.

Figure 3 shows the general DBS architecture for distribution of the television signal from program source to the subscriber's home. The video programming is distributed from the program source via satellite (indicated by "a" in the diagram) or fiber (indicated by "c" in the diagram) to the satellite up-link facility where it may be re-encoded, multiplexed, and encrypted for transmission via the DBS satellite to the subscriber's home. Local Receive Facilities (LRF) or Local Collection Facilities (LCF) are used to receive programming from local broadcast stations (indicated by "b" in the diagram), where these channels are then decoded, re-encoded, multiplexed, and transmitted via satellite or fiber to the satellite up-link facility. In some instances, an antenna at the subscriber's home receives local broadcast stations directly (indicated by "d" in the diagram).

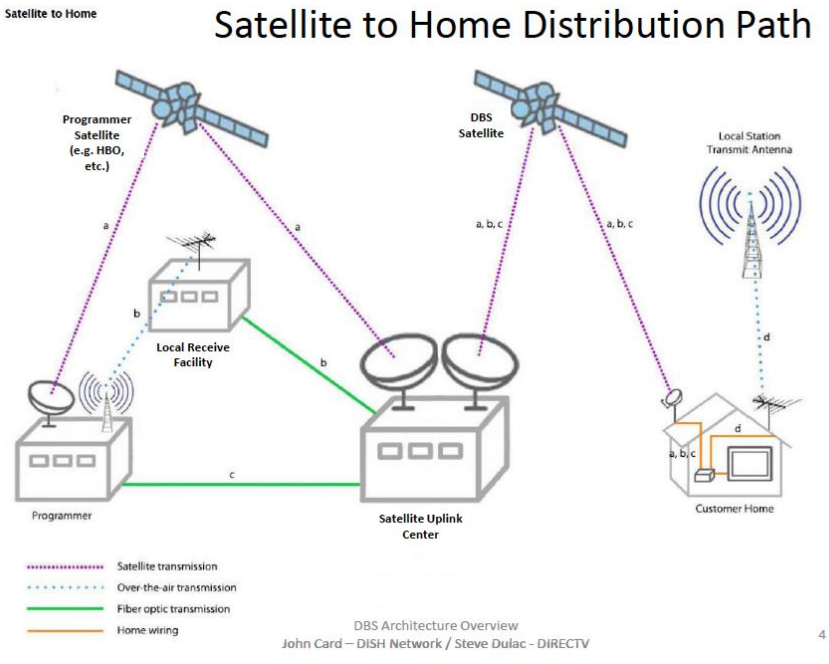


Figure 3 - DBS Architecture – Satellite to Home Distribution Path

Multiple satellites are used in each system to carry the diversity of programming offered by each provider. The Out Door Units (ODUs) and Low Noise Block (LNB) down-converters

receive the satellite signals and down-convert the signal to a lower frequency for distribution over coax cable throughout the subscriber's home. Because there are multiple satellite signals received by the ODU and LNB and there are potentially multiple tuners and/or set-tops in the home, a Multiswitch unit is used to switch the specific signal source to the requesting tuner.

The two operators' systems differ in a number of respects, including:

- The number and location of up-link facilities
- The orbital positions of the satellites used by each
- The satellite frequency plans used
- The Out Door Units (ODUs), Low Noise Block (LNB) down-converters, and Multiswitch units used
- The Conditional Access Systems (CAS) used
- The whole home DVR architectures and technologies used

Figure 4 shows the number and location of the uplink facilities for the two DBS providers. As can be seen the number and location of uplink facilities differs significantly.

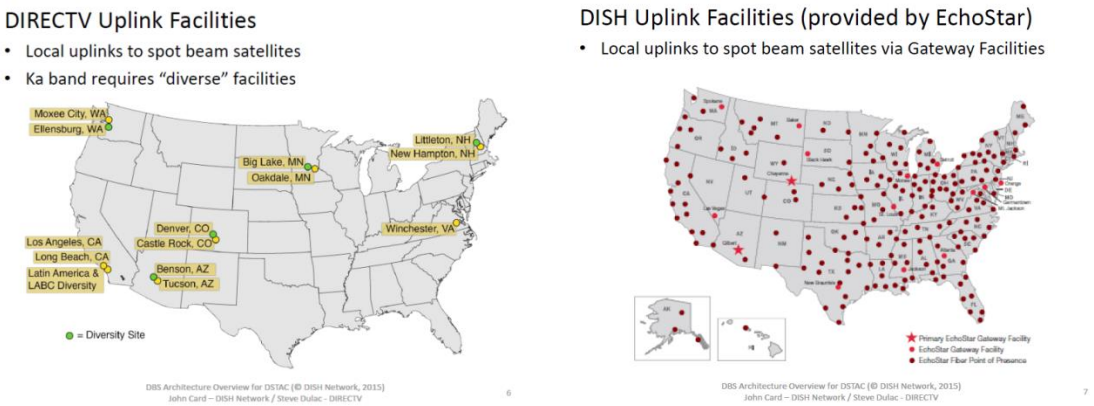


Figure 4 - DirecTV and DISH Uplink Facilities

The orbital positions for the two providers differ and this directly affects the orientation of the satellite dish and configuration of the ODU, LNB, and Multiswitch at the subscriber's home. The orbital positions for the two providers currently are:

- DirecTV – 99W, 101W, 103W as well as 110W, 119W & 95W
- DISH – Eastern US Arc – 61.5W, 72.7W, 77W, Western US Arc – 110W, 119W, 129W and shared 118.7W

The satellite frequency plans of the two providers differ as well. This impacts the configuration of the LNB and Multiswitch at the subscriber's home, as well as the

implementation of the Integrated Receiver Decoder (IRD) or set-top box. Figure 5 shows the respective satellite and in-home frequency plans of the two providers.

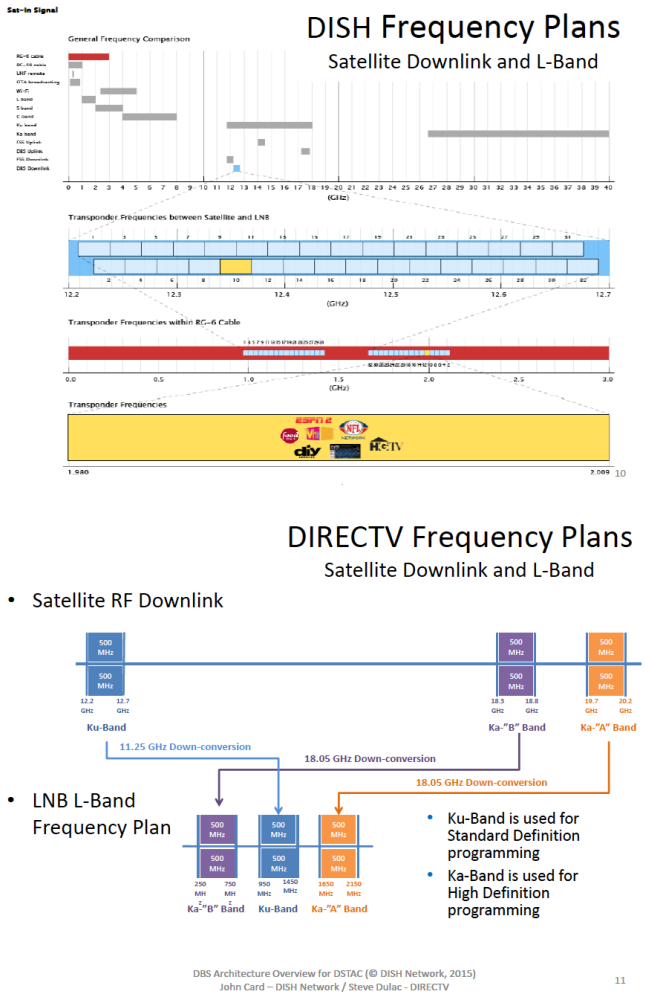


Figure 5 - DBS Satellite Frequency Plans

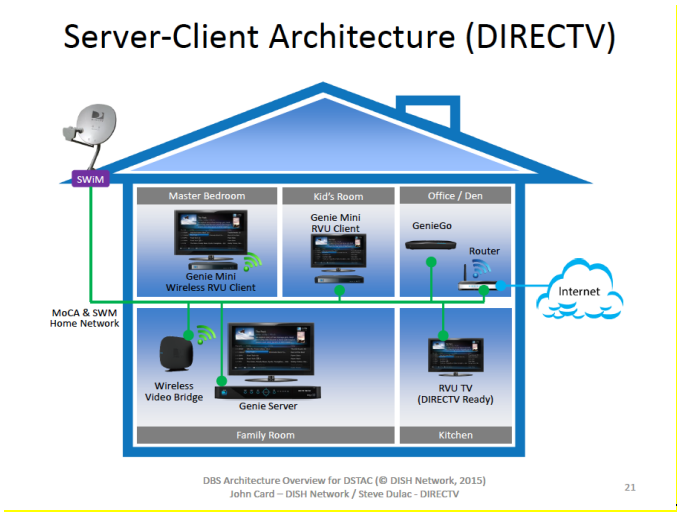
The ODUs and LNBs differ depending on the DBS operator and type of service being provided. For example, the current DirecTV ODUs include: an 18" Round (SD only), an 18x20" Triple-Sat (SD only), or a Slimline ODU (HD) which can be used with a Slimline-3 or a Slimline-5 LNB. The LNBs also differ in their powering. DISH LNBs are typically powered by one set-top in the home, while all DirecTV and some DISH LNBs have a dedicated external power supply. The Multiswitch unit allows a set-top to select between the multiple input signals received by the LNB. Because LNBs receive signals from multiple satellite transponders, it is necessary to switch the input signal for the requested channel to the requesting set-top tuner. The set-top sends a signal to the Multiswitch unit identifying the desired input and the Multiswitch unit switches the input signal onto the coax cable to the requesting set-top.

The two DBS providers differ in their implementations of their respective Multiswitch units. The control signaling between the two systems differs. Specifically, DIRECTV uses a Pulse-Width Modulated (PWM) control scheme; with simple 3-byte messages to identify desired input

port, which does not strictly conform to the DiSEqC (Digital Satellite Equipment Control) standard. DISH uses system based on and conforming to DiSEqC but extending the standard with additional commands. There are Single Wire Multiswitch units, which allow multiple, independent set-tops to share a single coaxial cable and multi-wire switch units that use separate coax cables for each set-top. Set-tops, Multiswitch units, ODUs and LNBs from the two providers do not interoperate.

The DIRECTV set-top boxes receive SD satellite signals using the 130-byte "DSS" transport format, while DISH uses the 188-byte MPEG transport format for its SD satellite signals. Both MVPDs use MPEG transport format for HD satellite signals. The two DBS providers utilize Digital Video Recorders (DVR) in the home to deliver a more interactive and personalized experience to subscribers: each have proprietary implementations that leverage MVPD-controlled content storage to deliver features including VOD and targeted Dynamic Ad Insertion (DAI). The set-top boxes from both providers offer common television outputs (e.g. analog component and composite, digital HDMI), but have deployed non-interoperable approaches for IP-networked outputs. The two DBS providers also differ in the CAS and DRM solutions used in their respective DBS systems. DirecTV uses NDS CAS/DRM systems and DISH uses Nagra CAS/DRM systems. Both providers support additional DRM systems for their internet-delivered services.

While both DBS providers use a client-server architecture and MoCA for in-home distribution of their whole home DVR solutions, they differ in their specific implementations. Figure 6 shows the two whole home DVR server-client solutions. DirecTV uses the RVU Remote User Interface technology, which has been integrated into a number of retail televisions (see rvualliance.org/products). Like other MVPDs, both providers participate in the Digital Living Network Alliance (DLNA) and make use of some DLNA protocols in their whole home DVR solutions.



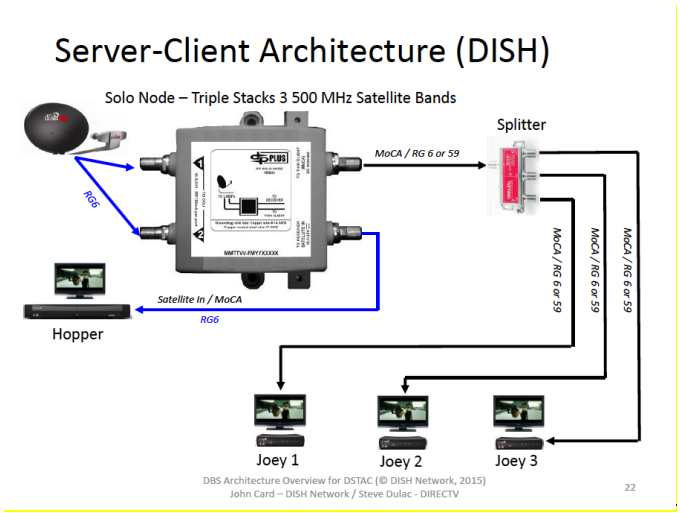


Figure 6 - DBS Server-Client Whole Home DVR Solutions

TELCO TECHNOLOGIES AND ARCHITECTURES

Telephone companies have used a number of different technologies and architectures for delivery of their MVPD service. Some have partnered with satellite providers to deliver an MVPD service, others have deployed fiber with an RF overlay network, and others have deployed IPTV systems over VDSL and fiber networks. This section covers the systems deployed by AT&T and Verizon.

AT&T and Verizon have taken different approaches to deploying an MVPD service. AT&T largely leveraged its twisted pair network using VDSL technology to deliver an IP-based TV service. AT&T has also deployed an FTTP PON network to carry this IPTV service. Verizon deployed a PON fiber network (FiOS) from the start, but chose to leverage cable technology to deliver its MVPD service to the point that they also make use of CableCARD in their set-top boxes as well as in support of retail devices. To accomplish this, Verizon used a separate wavelength to carry an RF spectrum with broadcast TV channels. The two-way PON network is used to carry two-way services, including VoD. This is sometimes referred to as a Hybrid QAM/IP implementation, as QAM is used to carry the broadcast channels and IP is used to carry VoD services.

AT&T Technologies and Architectures [43]

In 2004 SBC/AT&T participated in the Microsoft IPTV Early Adopters Program (EAP). The IPTV Mediaroom system was designed as an application platform to support the IPTV service and evolution of service features. The platform is now owned and maintained by Ericsson. AT&T offers this service over both copper (VDSL) and Fiber (FTTP) networks. The service is based on an all Internet Protocol (IP) delivery for Linear/Live, and VOD. The network encompasses a number of proprietary features such as Instant Channel Change (ICC), Multiview, and a large number of interactive applications. The Microsoft Mediaroom DRM is used for content protection on AT&T U-verse STBs with an embedded secure SOC. U-verse is offered to third party devices such as smart phones (iOS, Android), tablets, PCs and laptops through AT&T U-verse applications. PlayReady DRM is used for content protection on these devices.

Figure 7 is a diagram of the AT&T U-verse Architecture. U-verse content is acquired and gathered at a central location, the Super Hub Office (SHO), for national linear channels and VOD assets. Linear content is encoded to AT&T's unique specifications and distributed via multicast from the SHO to Video Hub Offices (VHOs). The content is then multicast to the end user, when requested. Local channels are acquired locally and encoded to AT&T's unique specifications at the VHOs. VOD assets are encoded to AT&T's unique specifications and transported to the SHO[1]. From there they are distributed to the VHOs via multicast, and stored locally at the VHOs. The assets are then streamed from the VHOs to the end user via unicast, when requested.

Linear channels are encoded using H.264 video compression and Dolby Digital Plus (DD+) converted to AC-3 by the STB or AAC audio, and contained within an MPEG-2 transport stream. When ingested into Mediaroom, the channels are encrypted and encapsulated as RTP streams via the Acquisition Servers (A-servers), and distributed via multicast to the local VHOs.

[1] Note that AT&T does not use the CableLabs encoding specifications to encode content.

Linear channels are also acquired by a Distribution Server (D-server), which is at the VHO and used for instant channel change. When a user switches to a live channel, a proprietary ICC enables a fast channel change implementation.

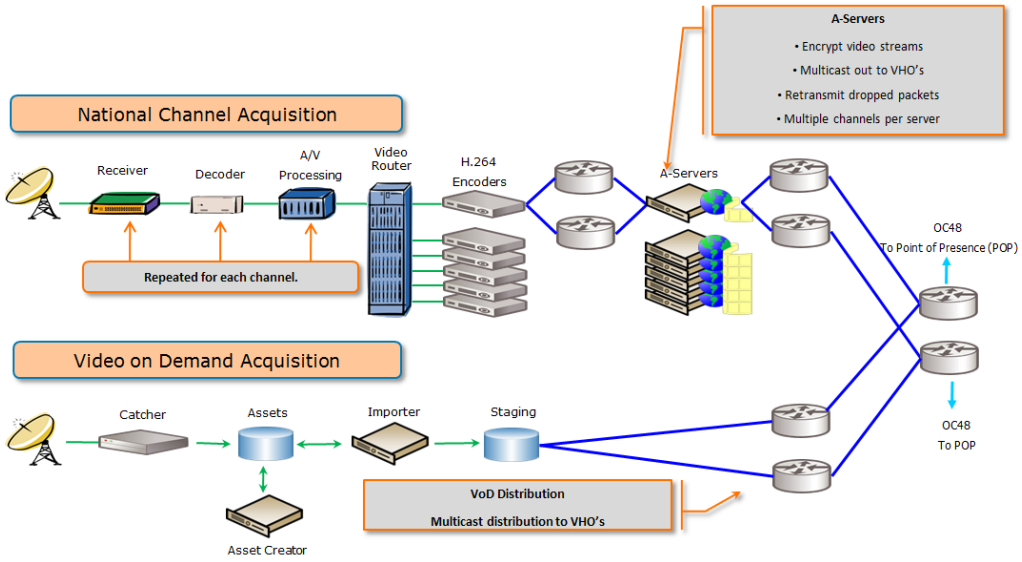


Figure 7 - AT&T U-verse Architecture

VOD assets are encoded using H.264 video and AC-3 audio, and contained within an MPEG-2 transport stream. When ingested into Mediaroom, the assets are encrypted, encapsulated as an RTP stream, then distributed and stored at the local VHOs on VOD Servers (V-servers). When initiated by the user, VOD assets are streamed from the VHO V-servers to the user's receiver over HTTP.

The U-verse Mediaroom DRM is used to enforce license restrictions from content agreements and provides overall content protection. The DRM is based on 128-bit AES and 2048-bit RSA encryption. Linear content is encrypted either at the SHO, or at the local VHO (for local channels). The encrypted channels are distributed to the end user's STB where they are decrypted using an embedded secure SOC. VOD assets are encrypted at the SHO after being acquired from the content provider. The encrypted assets are then distributed through the network and only decrypted once it is streamed to the end user's STB. Content outputs are also protected via HDCP, CGMS-A, and Macrovision. The output controls are implemented through the client application.

AT&T U-verse is also available online at uverse.com, and on tablets and smart phones via the U-verse mobile application. Uverse.com offers a web site where users can login and view services. Some content flows through an internal process and other content is hosted directly through third parties like Hulu, Turner, etc. Content is protected via PlayReady DRM. The U-verse mobile app for phones and tablets are developed internally and content is encoded and hosted using a third party. Content is protected via PlayReady DRM.

AT&T is planning to deploy 4K and HEVC, more advanced STBs to provide more value-added services to U-verse customers. Access bandwidth is improving with the provisioning of more bandwidth over VDSL and the deployment of more fiber (GigaPower). AT&T will be

deploying more advanced Wi-Fi technologies (i.e. 802.11ac) for both video and data distribution and expanding U-verse applications to reach more and more third-party devices, and offering more interactive applications.

Verizon Technologies and Architectures [44]

Verizon took an alternate approach to AT&T by deploying a FTTP network known as FiOS. The Verizon FiOS network is a Passive Optical Network (PON) either B-PON or G-PON with the addition of an "overlay" wavelength (1550nm) to transmit broadcast video over RF. VOD is distributed over IP using data/voice wavelengths (1490nm & 1310nm). Figure 8 shows the Optical Spectrum on the PON network based on ITU G.98x PON standards. Figure 19 provides a diagram of the FiOS access network showing the B/G-PON OLT for two-way voice, data, and VoD traffic, the Erbium Doped Fiber Amplifier (EDFA) used to inject the broadcast RF on the fiber, the ONT at the customer premise. This diagram also shows the optical wavelengths used for the FiOS service. This architecture provides full support for both cable style RF video as well as emerging IPTV video technologies. Moving the VOD traffic to the B/G-PON IP network freed up RF spectrum for broadcast HDTV growth and provides greater scale as demand for voice, data, and VoD increases. The network protocols used on the B/G-PON network are ATM AAL1&2 for Plain Old Telephone Service (POTS) and ATM AAL5 for Broadband Internet and VoD.

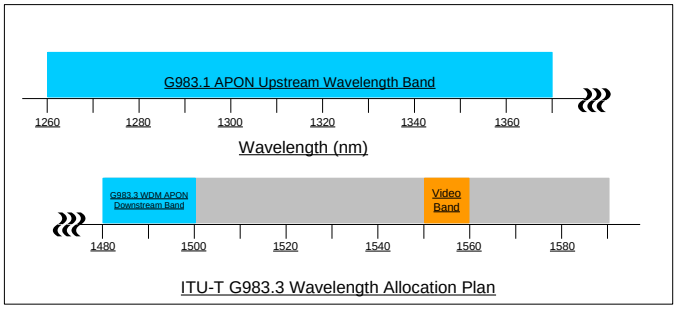


Figure 8 - ITU G.98x PON Optical Spectrum

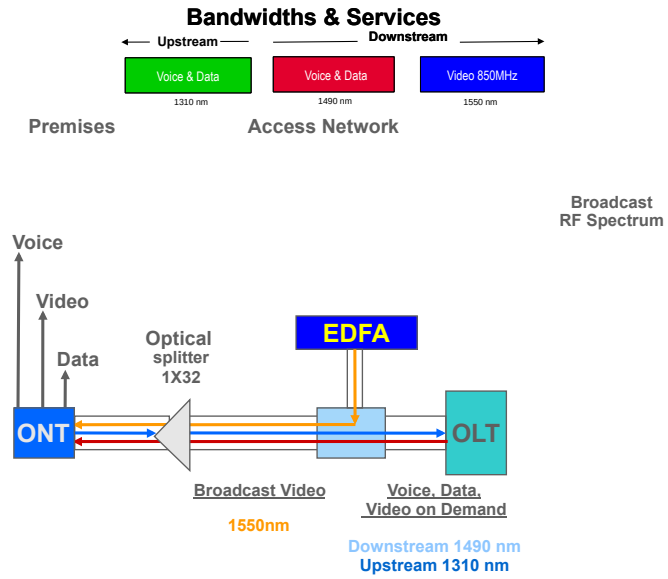


Figure 9 - Verizon FiOS Access Network

Figure 10Figure 10 shows the high-level Verizon architecture. Content is received at two Super Head Ends (SHE) for purposes of redundancy. A Long Haul Network (LHN) is used for the National Video Distribution Network to carry the video traffic from a SHE to multiple Video Hub Offices (VHO), each of which serves a major metropolitan or franchise area. The Metro Video Distribution Network distributes the video traffic from a VHO to multiple Video Serving Offices (VSO) where it is then distributed over the PON access network to the customer premise. This diagram also shows which network protocols used at which points in the overall architecture.

Figure 21 shows the FiOS Hybrid QAM/IP set-top box and dual networks over which it connects to the VSO. First, there is the one-way overlay interface that carries broadcast video using 256 QAM and MPEG-2 Transport Streams (TS). In addition, there are two OOB downstream channels: SCTE-55-1 for the MediaCipher CAS system and SCTE-55-2 for the PowerKey CAS system, the same used by most US Cable operators. These OOB channels carry System Information (SI), Entitlement Management Messages (EMM) and other control plane signaling for box control and configuration. The IP Interface carries VOD content, duplicates some of the OOB signaling and carries additional application data including widgets, guide data, and gaming traffic.

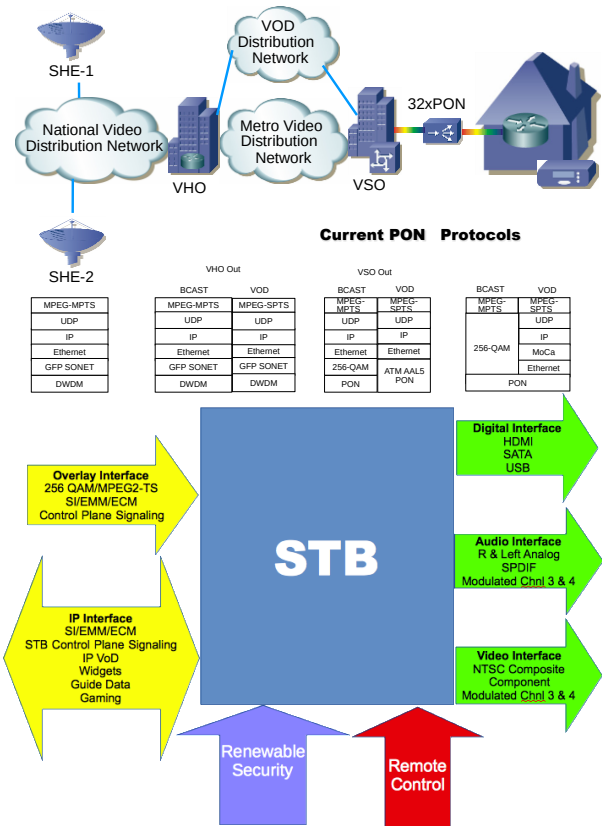


Figure 10 - Verizon FiOS High-Level Architecture **Figure 11 -** Verizon FiOS Dual-Network Hybrid STB Architecture

The Verizon FiOS system uses both MediaCipher and PowerKey CAS systems in all markets via a Simulcrypt compliant architecture. All channels are encrypted using the DVB Common Scrambling Algorithm (CSA) cipher. The system also fully supports the CableCARD

interface with different CableCARDs provided for MediaCipher and PowerKey. To support CableCARD, it was necessary to dual carry System Information, EMMs, ECMs, and set-top box control plane signaling on both the IP and Overlay Interfaces.In order to support simulcrypt, the FiOS headends comply with the DVB Simulcrypt standard. In the FiOS simulcrypt implementation, the MediaCipher CAS has the sole Code Word Generator (CWG) function. Simulcrypt also increased the complexity of the system. Both the Mediacipher and PowerKey CAS systems are accessing the same commonly encrypted version of the content. In addition, many other channels and VoD content are available through alternate IP communications channels.

Verizon supports retail devices such as Smart Phones, Tablets, Smart-TVs, and Gaming Platforms. Non-FiOS access networks make use of DRM rather than CAS for content protection. The DRM solutions are based on 128 bit AES/CTR mode cipher.

References

[1] Louis D. Williamson, "FSN Technology," Proceedings: Society of Cable Television Engineers 1995 Conference on Emerging Technologies, Jan. 4-6, 1995, Orlando, FL, pp. 27-35.

[2] Michael B. Adams, "MPEG and ATM in the Full Service Network," Proceedings: Society of Cable Television Engineers 1995 Conference on Emerging Technologies, Jan. 4-6, 1995, Orlando, FL, pp. 13-26.

[3] Ralph Brown and John Callahan, “Software Architecture for Broadband CATV Interactive Systems,” NCTA Cable ’95 Proceedings, Dallas, TX, May 1995.

[4] PEGASUS PROGRAM, Request For Proposal and Functional Requirements Specification, V1.0, Time Warner Cable - Engineering & Technology, March 6, 1996.

[5] ISO/IEC 13818-6:1998 - Information technology -- Generic coding of moving pictures and associated audio information - Part 6: Extensions for DSM-CC.

[6] ISO/IEC 13818-2, 2000: Information technology—Generic coding of moving pictures and associated audio (MPEG): Video.

[7] ATSC Digital Audio Compression Standard (AC-3, E-AC-3), Revision B.

[8] ISO/IEC 14496-10:2005: Information technology - Coding of audio-visual objects - Part 10: Advanced Video Coding.

[9] ISO/IEC 13818-1, 2000: Information technology—Generic coding of moving pictures and associated audio (MPEG): Systems.

[10] Federal Information Processing Standards Publication (FIPS PUB) 46-3, Data Encryption Standard.

[11] ANSI/SCTE 52 2008, Data Encryption Standard – Cipher Block Chaining Packet Encryption Specification.

[12] ANSI/SCTE 65 2008, Service Information Delivered Out-Of-Band For Digital Cable Television.

[13] ANSI/SCTE 55-1 2002, Digital Broadband Delivery System: Out Of Band Transport Part 1: Mode A.

[14] ANSI/SCTE 55-2 2002, Digital Broadband Delivery System: Out Of Band Transport Part 2: Mode B.

[15] CableLabs Press Release, “Cable Industry Creates 'OpenCable™' Goal is Interoperable Set-top Boxes”, September 4, 1997.

[16] OpenCable Host Device 2.1 Core Functional Requirements, OC-SP-HOST2.1-CFR-I15-120112, January 12, 2012, Cable Television Laboratories, Inc.

[17] CEA-679-C Part B, National Renewable Security Standard (July 2005). A joint work of NCTA and CEMA Technology and Standards.
[18] EN 50221-1997, EN 50221: "Common interface specification for conditional access and other digital video broadcasting decoder applications".
[19] DOCSIS Set-top Gateway (DSG) Interface Specification, CM-SP-DSG-I20-120329, March 29, 2012, Cable Television Laboratories, Inc.
[20] ANSI/SCTE 28 2007, HOST-POD Interface Standard
[21] OpenCable™ Software Request For Proposals, OC-RFP-990914, September 14, 1999, Cable Television Laboratories, Inc.
[22] DVB Multimedia Home Platform 1.1.3, DVB-MHP 1.1.3, ETSI TS 102 812 V1.3.1 (2007-03), Blue book A068r3.
[23] OpenCable Application Platform Specifications, OC-SP-OCAP1.2.2-120224, February 24, 2012, Cable Television Laboratories, Inc.
[24] DVB Globally Executable MHP version 1.0.2, (GEM 1.0.2), ETSI TS 102 819 V1.3.1 (2005-10).
[25] Advanced Common Application Platform (ACAP), ATSC Document A/101A, February 12, 2009.
[26] Application Execution Engine Platform For Digital Broad Casting, ARIB STD-B23, Version 1.1, Association of Radio Industries and Businesses, February 5, 2004.
[27] System Description, Blu-ray Disc Read-Only Format, Part 3-2: BD-J Specifications, version 2.4. Blu-ray Disc Association, 2009.
[28] Host 2.0 DVR Extension, OC-SP-HOST2-DVREXT-I03-110512, May 12, 2011, Cable Television Laboratories, Inc.
[29] OCAP Digital Video Recorder (DVR), OC-SP-OCAP-DVR-I08-120112, January 12, 2012, Cable Television Laboratories, Inc.
[30] OpenCable Host Home Networking Extension 2.0, OC-SP-HOST-HN2.0-I06-120112, January 12, 2012, Cable Television Laboratories, Inc.
[31] Home Networking Protocol 2.0, OC-SP-HNP2.0-I07-120224, February 24, 2012, Cable Television Laboratories, Inc.
[32] Reserved Services Domain Protocols Specification, OC-SP-RSD-PROT-I01-080828, August 28, 2008, Cable Television Laboratories, Inc.
[33] Reserved Services Domain Technology Specification, OC-SP-RSD-TECH-I01-080630, June 30, 2008, Cable Television Laboratories, Inc.
[34] OCAP Home Networking Extension, OC-SP-OCAP-HNEXT-I08-120112, January 12, 2012, Cable Television Laboratories, Inc.
[35] Home Networking Security Specification, OC-SP-HN-SEC-I03-120112, January 12, 2012, Cable Television Laboratories, Inc.
[36] Enhanced TV Application Messaging Protocol 1.0, OC-SP-ETV-AM1.0-I06-110128, January 28, 2011, Cable Television Laboratories, Inc.
[37] Enhanced TV Binary Interchange Format 1.0, OC-SP-ETV-BIF1.0-I06-110128, January 28, 2011, Cable Television Laboratories, Inc.
[38] HTTP Live Streaming, Internet Draft, http://tools.ietf.org/html/draft-pantos-http-live-streaming-08.
[39] HTML5 - A vocabulary and associated APIs for HTML and XHTML, W3C Working Draft, World Wide Web Consortium, http://www.w3.org/TR/html5/.
[40] ISO/IEC 23009-1:2012: Information technology -- Dynamic adaptive streaming over HTTP (DASH) -- Part 1: Media presentation description and segment formats.

[41] *ISO/IEC 23001-7:2012, Information technology -- MPEG systems technologies -- Part 7: Common encryption in ISO base media file format files*. International Standard. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:23001:-7:ed-1:v1
[42] CAS / DRM Reality Check, Robin Wilson, Nagra, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 19, 2015.
[43] AT&T IPTV Technologies and Architectures, AhmadAnsari, AT&T, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[44] Verizon Technologies and Architectures, Dan O'Callaghan, Verizon, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[45] Downloadable Security Technology Advisory Committee (DSTAC) Working Group 2 Report #1, April 21, 2015, https://transition.fcc.gov/dstac/wg2-report-01-04212015.docx.
[46] Cable Technologies And Architectures Overview, Ralph Brown, CableLabs, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[47] MPEG & IP Video Comparisons, Mark Vickers, Comcast, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[48] DSTAC Presentation OMS and Optimum Services, Ken Silver, Cablevision, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[49] Charter DCAS Environment, Jim Alexander, Charter, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[50] TWC IP Video Architecture, George Sarosi, Time Warner Cable, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[51] Bright House Overview, Jeff Chen, Bright House, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[52] DBS Architecture Overview, John Card II, DISH & Steve Dulac, DirecTV, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[53] Cable Risk and Threats, Ralph Brown, CableLabs, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 19, 2015.
[54] MVPD CAS and DRM Trust Infrastructures, Ralph Brown, CableLabs, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), April 14, 2015.

5. Direct-to-Home (DTH) Satellite Dish (small dish)

Alaska special case

8. Over-the-Air Network Antenna Tuners (ATSC)

B. Home Network Technologies

EXPECTATIONS: SECTION B

List protocols … if trying to build competitive device, what do I need to build? Physical connection. Anything that was done that is proprietary. This appears to be Layer 1 and 2.

Home Networking Overview

AT&T U-verse supports both wired and wireless home networking for video distribution. In homes with structured wiring/Ethernet cable wiring (i.e. CAT-5 wiring), the Residential Gateway (RG) and STBs are connected using the available structured wiring. If structured wiring is not available, AT&T is using HPNA over coax for wired video distribution. AT&T is also offering a

Wireless STBs (WSTBs) and a dedicated Wireless Access Point (WAP) using the 802.11n Wi-Fi technology for video distribution. Figure 1 shows an example of home networking diagram.

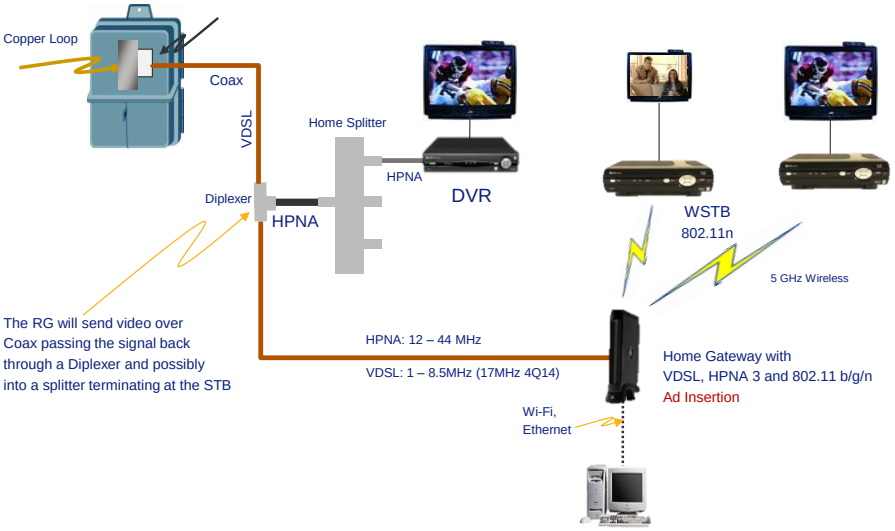


Figure 12: Example of Home Networking

Typically, VDSL is terminated at the RG using a coaxial cable or a twisted pair copper cable. Content is distributed to wired STBs via either HPNA over coax, or standard Ethernet cables, or wireless networks. In terms of Access network technology, AT&T is offering broadband services over both copper and fiber to the home networks. For the U-verse copper-based customers, AT&T is using VDSL speeds of up to 100Mbps and for fiber-based customers, AT&T is offering broadband speeds of up to 1Gbps.

Wireless Network Connectivity

Over the last decade wireless performance has improved exponentially as a result of technologies and features such as Multiple Input Multiple Output (MIMO), Transmit Beamforming (TxBF) and availability of additional spectrum. A number of wireless vendors are working on optimizing Wi-Fi silicon for in- home high definition video streaming. Figure 2 shows some of the current in home wireless technologies.

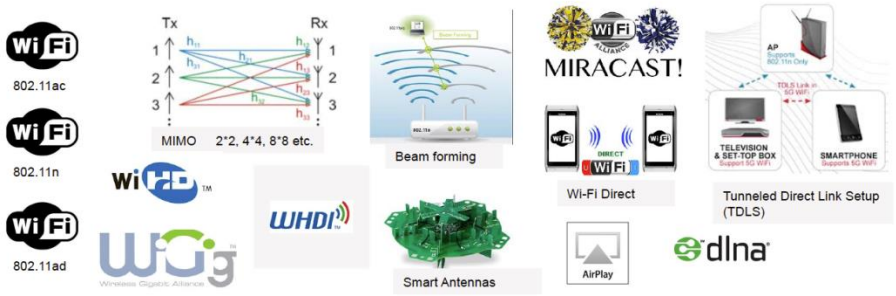


Figure 13: Current in Home Wireless Technologies

Both 802.11ac and 802.11n claim enough capacity to support in-home video streaming. Many Wi-Fi products, including 802.11n, support Multiple Input Multiple Output (MIMO), digital Beamforming and operations in 5GHz spectrum. These technologies promise greater reliability

and even better performance than legacy Wi-Fi technologies. These technologies are application agnostic and allow operators to use device and service discovery technologies defined in DLNA.

Tunnel Direct Link Setup (TDLS) and Wi-Fi Direct are efficient methods for video streaming between two Wi-Fi clients. MSOs should consider these technologies for in-home video streaming if the cable video source (e.g. cable video gateway) in the home can be configured as a Wi-Fi client. The service discovery methods defined in Digital Life Living Alliance (DLNA) can be used while the TDLS clients are connected through an AP. A new Wi-Fi Direct Application Service Platform (ASP) to advertise and discover cable video services is required before Wi-Fi Direct can be used for in-home cable video streaming.

Miracast uses TDLS or Wi-Fi Direct as underlying transport. Unlike TDLS and Wi-Fi Direct, Miracast also defines application specific procedures such as content security methods and media streaming protocols to support screen mirroring and video streaming between two Wi-Fi clients. Miracast currently does not require support for High Definition video streaming using MPEG-2.

Use of Wi-Fi for in-home video streaming introduces a number of factors that influence the design of home network architecture. Some of these factors are:

- Does the customer subscribe to both video and Internet services from the same of different service provider?
- Is the video source (e.g. video gateway) connected to the home network LAN using wired or wireless network?
- Are there separate IP networks in the home for video and data services? An architecture using separate Wireless LAN for video and data can result in confusion for the customer since a device connected to the Wi-Fi AP for video services will not be able to access data services without first disconnecting from the video Wi-Fi network, and then connecting to the data Wi-Fi network. WiGig (802.11ad) supports data rate up to 7 Gbps using 60 GHz frequency band. The indoor coverage range for WiGig is about 10 meters, which is good for communication between two devices in the same or next room.

802.11ac versus 802.11n

802.11ac delivers higher throughput than 802.11n, as a result of the support for 80 MHz channels and 256 QAM. This advantage is more obvious when Wi-Fi clients are at close range to the Wi-Fi AP. The throughput performance of the two technologies is comparable at long range (e.g., < -70 dBm RSSI).

While either 802.11n or 802.11ac can be used for video streaming, 802.11ac is the current generation Wi-Fi technology, and it supports some features that were not part of the 802.11n standard. Table 1 below provides a highlight of some of the differences between 802.11n and 802.11ac.

Table 2: Comparison 802.11n and 802.11ac features

Features	802.11n	802.11ac
Frequency Band	2.4 or 5 GHz	5 GHz only
Channel Bandwidth	20, 40 MHz	20, 40, 80, 160, 80+80 MHz
Modulation & Coding Scheme	64 QAM	256 QAM
Spatial Streams	Up to 4	Up to 8
Transmit Beamforming	Optional	Standardized
Max Throughput	600 Mbps	3.2 Gbps
MU-MIMO	No	Yes
Availability	Available for some time now	First generation available now

In addition to the features in Table 1, 802.11ac also includes support for features such as Dynamic Bandwidth Management, which can be very handy in mitigating interference and improving spectral efficiency. This feature allows an AP to dynamically choose channel bandwidth to each client on a frame-to-frame basis.

The first generation 802.11ac products support only 20, 40 and 80 MHz channel bandwidth. The current FCC spectrum rules do not allow for a 160 MHz channel. Channel bandwidth of 80 MHz+80 MHz and 160 MHz are expected in the second-generation 802.11ac products. Support for MU-MIMO and Dynamic Bandwidth Management are also expected in the second-generation 802.11ac products.

AT&T is deploying a dedicated video Wireless AP (WAP) that is based on 4x4 802.11n. The video WAP is strictly used for video distribution to wireless standalone STBs that are based on 802.11n Wi-Fi standard.

TUNNEL DIRECT LINK SETUP (TDLS)

TDLS allows network-connected client devices to create a secure, direct link to transfer data more efficiently. The client devices first establish a control channel between them through the AP. The control channel is then used to negotiate parameters (e.g., channel) for the direct link. APs are not required to support any new functionality for two TDLS compliant devices to negotiate a direct link.

TDLS offers multiple benefits, including efficient data transmission between client devices by removing the AP from the communication link. Use of direct communication channel also allows the client to negotiate capabilities independent of the AP. For example, clients can choose a wider channel, efficient modulation scheme, security and channel that are more suitable for direct link between the client devices.

TDLS devices, communicating with each other over a direct link, are also allowed to maintain full access to the Wi-Fi network simultaneously, which for example, allows the client device to stream video to another device in the home over the direct link; and at the same time allow user

to surf Internet via connectivity to the AP. If the TDLS direct link is switched to another channel, the stations periodically switch back to the home channel to maintain connectivity with the Wi-Fi network.

The WFA has certified multiple products for TDLS, including Broadcom and Marvel. TDLS is based on IEEE 802.11z, and is one of the optional features of Miracast (Wi-Fi Display).

WI-FI DIRECT

Wi-Fi Direct allows Wi-Fi client devices to connect directly without use of an AP. Unlike TDLS, Wi-Fi client devices are not required to be connected to an AP to establish a Wi-Fi Direct link. Wi-Fi Direct also includes support for device and service discovery. Wi-Fi Direct devices can establish a one-to-one connection, or a group of several Wi-Fi Direct devices can connect simultaneously.

Wi-Fi Direct offers multiple benefits, including ease of use and immediate utility and enables applications such as printing by establishing a peer to peer connection between the Wi-Fi Direct enabled printer and client device, content sharing between two Wi-Fi Direct enabled devices, and displaying content from one Wi-Fi Direct device to another without requiring any Wi-Fi network infrastructure.

Wi-Fi Direct certifies products, which implement technology defined in the WFA Peer-to-Peer Technical Specification. The WFA has certified multiple products for Wi-Fi Direct. As of 2012, there are over 1100 Wi-Fi Direct certified products.

Wi-Fi Direct is the core transport mechanism for Miracast (Wi-Fi Display).

MIRACAST

Miracast provides seamless display of content between devices using Wi-Fi Direct as the transport mechanism. Miracast also includes optional support TDLS as a transport mechanism.

The key features supported in Miracast include device and service discovery, connection establishment and management, security and content protection, and content transmission optimization. Similar to Wi-Fi Direct and TDLS, Miracast is client functionality and does not require updates to AP devices.

Primary use cases for Miracast are screen mirroring and video streaming.

Miracast certifies products, which implement technology defined in the Wi-Fi Display Technical Specification. As of this writing many devices (e.g., Smart phones) have been certified for Miracast.

WIRELESS GIGABIT (WIGIG)

WiGig was originally developed in WiGig Alliance. In 2013, WiGig Alliance and Wi-Fi Alliance united, consolidating WiGig technology and certification development in Wi-Fi Alliance. The WiGig technology offers short-range multi-gigabit connections for wide variety of applications including video, audio and data. The following is a list of applications that WFA is focusing on:

- WiGig Display Extension
- WiGig Serial Extension
- WiGig Bus Extension
- WiGig SD Extension

The WiGig technology is the basis of IEEE 802.11ad amendment and supports Beamforming and data rates up to 7 Gbps in 60 GHz frequency band. Many WiGig products are also expected to support Wi-Fi, along with mechanisms for smooth handovers from 60 GHz to 2.4 GHz and 5 GHz band. The indoor coverage range is about 10 meters, which is adequate for communication between two devices in the same or next room. A number of vendors, including Atheros, Marvell and Broadcom, Dell, Intel, Panasonic and Samsung are working with the WFA in the development of technology and certification testing program. The WFA currently expects to launch WiGig certification program in 2016.

Ethernet Network Connectivity:

Some MVPD provided STB also have wired Ethernet connectivity. All U-verse STBs are equipped with a Fast Ethernet connector enabling the 10/100-base fast Ethernet home networking. This enables consumers with Ethernet wired homes to directly connect the STBs to the network termination units or RGs inside the home without the need for extensive rewiring or setup of high-fidelity wireless networks.

Bluetooth

Increasingly Bluetooth networking is being utilized by many CE devices and applications to extend their functionality to support new features and capabilities. These include [among others] remote controls, game controllers, and audio streamers.

ZigBee® RF4CE Remote Control Specification

Traditionally, remote controls for set-top boxes and CE devices have made use of InfraRed (IR) protocols that have relied on line of sight between the remote control and the device itself. Increasingly, these devices have been installed in entertainment centers or equipment closets that preclude line of sight use by IR remote controls. As a result the use of RF protocols like ZigBee RF4CE are being used in remote controls for set-top boxes. The cable industry has adopted a profile of RF4CE that is published by CableLabs[2].

HPNA Network Connectivity:

AT&T is using the HPNA V3 over Coax that is based on the ITU G.9954-2006 standard. HPNA operates in the 12-44 MHz frequency band and offers a data throughput of up to 320 Mbps. The HPNA technology also supports Quality of Service (QoS), Differentiated Services Code Point

[2] Cable Profile for the ZigBee® RF4CE Remote Control Specification, OC-SP-RF4CE-I01-120924, September 24, 2012.

(DSCP) with 8 priority queues. The technology also supports dynamic bandwidth allocation and coexists with VDSL.

MoCA 2.0 Technology Overview

Used for whole-home DVR, IP networking (IPVOD, CAS call-home for PPV/VOD purchase reporting, diagnostics, application data, diagnostics), software download and client control

Please refer to http://www.mocalliance.org/ for more information.

A typical in-home coaxial cable architecture consists of a tree-and-branch network topology using RF splitters and coaxial RG-6 or RG-59 cables. The multimedia signal enters the home via an Optical Network Unit (ONU) or via Cable gateway, Digital Subscriber Line (DSL) gateway, or via a satellite dish. Multimedia content is distributed to each room in the home using the in-home coaxial network. The home must support multiple simultaneous HDTV, SDTV, audio, data, voice-over IP, gaming, and other multimedia usages both from the broadcast network and from the in-home DVR or storage devices. Each wired room and device may be either, or both, a source or sink of multimedia content both to and from multiple simultaneous entertainment devices in the home. Although the in-home coax is a relatively static channel, the presence of coaxial splitters creates a highly dispersive multipath channel that can cause significant echoes in addition to high signal attenuation when communicating between various networking devices.

The in-home coaxial network connectivity must provide a reliable room-to-room, peer-to-peer, full-mesh connectivity among all sources and sinks in the home. In order to support at least three simultaneous HDTV and SDTV multimedia streams, the in-home network is required to have at least 60 Mb/s, and in many cases greater than 100 Mb/s data throughput with low packet error rate and low average latency. These network performance requirements, adopted by MoCA, must be satisfied when other services are added or when a neighbor or a family member runs services in the home.

The initial MoCA technology using the existing in-home coaxial cables was based on the MoCA 1.1 standard ratified in 2007. It uses bit-loaded Orthogonal Frequency Division Multiplexing (OFDM) modulation with 224 subcarriers in a 50 MHz channel. Bit-loaded OFDM was selected for MoCA because it is robust against static or slowly changing multipath and optimizes the modulation between every pair of devices. When bit loading, each MoCA device probes the channel between itself and every other MoCA device in the network and selects the modulation on each of the 224 subcarriers based on the probe results: the better the signal-to-noise ratio (SNR) on a subcarrier, the higher the modulation assigned to that subcarrier. MoCA 1.1 uses a maximum subcarrier modulation of 256 QAM. Since the MoCA PHY layer adapts each link between node pairs independently, the channel capacity can be different between different nodes, as well as between the forward and reverse directions of the same node. The bit-loading parameters for a particular path are called a PHY profile. It enables a maximum PHY rate of 275 Mbps, and network throughput rate of 175 Mbps at low Packet Error Rate (PER ≤ 10^{-5}) and low average one-way latency (≤ 3.5 milliseconds) in defined frequency bands from 475 MHz to 1550 MHz. The latest MoCA 2.0 standard, which was ratified in June 2010, includes the following key features:

- Increased channel bandwidth from 50 MHz to 100 MHz (225 MHz) for bonded channels with increased maximum modulation density from 256-QAM to 1024-QAM
- Forward-Error-Correction (FEC) was changed from Reed-Solomon (RS) to Quasi-Cyclic (QC)-LDPC
- Expanded MoCA channel plan from 400 MHz to 1675 MHz in defined frequency bands to support bonded channels operation, and two simultaneous independent networks
- Total MAC network throughput of 430 Mbps, and 860 Mbps with a bonded-channel in a 16-node network
- Full backward interoperability with MoCA 1.1 devices
- Turbo-mode for two-node network with network throughput > 1 Gbps
- Using Orthogonal Frequency Division Multiple Access (OFDMA) for Reservation Requests (RRs) from each MoCA device to the NC
- Four new power states ('Active', 'Idle', 'Standby', 'Sleep') for energy savings were defined
- New multicast Parameterized QoS (PQoS) flows with reduced one-way average latency
- Enhanced link privacy using Advanced Encryption Standard (AES) in Cipher-Block Chaining (CBC) mode using 128-bit AES key length

Table 3 summarizes the MoCA 2.0 PHY and Medium Access Control (MAC) layer key parameters.

Table 3 - Summary of MoCA 2.0 PHY and MAC Layer Parameters

PARAMETER NAME	PARAMETER VALUE	NOTES
Bandwidth	100 MHz, 225 MHz (bonded channels)	
Modulation Type	OFDM	
Modulation Density	BPSK up to 1024-QAM	
Subcarrier Spacing	195.3125 kHz	
Cyclic Prefix	0.2 to 1.28 µs	In increments of 0.2 µs for data
FEC	QC-LDPC with code rate 39/46	LDPC = Low-Density Parity Code
Maximum PHY Rate (theoretical)	733 Mbps, 1466 Mbps (bonded channels)	
Maximum MAC Rate	430 Mbps, 860 Mbps (w/bonded channel)	
Medium Access Control (MAC)	TDD Scheduled MAC with Tx opportunities by NC	
QoS	Contention-free service with low-latency multicast flows	
Network Management	SNMP MIBs for MoCA 1.1	TR-069 support for MoCA 1.1
Maximum Network Size	16 adapters	
Power Save	'Active, 'Idle', 'Standby', and 'Sleep'	

PARAMETER NAME	PARAMETER VALUE	NOTES
	modes	
Security	128-bit AES encryption in CBC mode Two sets of static and dynamic keys for data encryption	CBC = Cipher Block Chaining

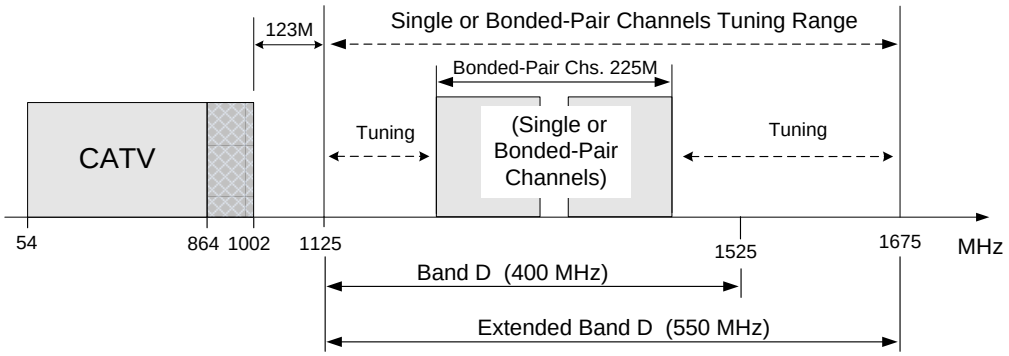


Figure 14 - MoCA 2.0 Extended Band D Frequency Plan

MoCA 2.0 PHY layer operates in defined frequency bands from 400 MHz to 1675 MHz. Figure 14 shows the MoCA 2.0 Extended band D (ExD) frequency plan, which is used by most of the Cable operators in North America. Band D defined for MoCA 1.1 devices was extended from 1125 MHz to 1675 MHz, introducing two D sub-bands (D-low and D-high) so that two independent MoCA 2.0 networks can be supported. The MoCA 2.0 channels (100 MHz) are centered on a 25 MHz grid, and can be tuned in 25 MHz increments. Bonded channels (225 MHz) consist of 100 MHz primary and secondary channels centered on the 25 MHz grid with a 25 MHz gap between them. The ExD frequency plan supports mix-mode operation with MoCA 2.0 and MoCA 1.1 devices. Other frequency bands include Band E (400 MHz to 700 MHz) and band F (650 MHz to 875 MHz) used primarily by the satellite operators.

In some use cases, when a higher MAC throughput is required, MoCA 2.0 added a turbo mode support in a two-node network. In this network nodes may eliminate some MAC overhead in order to maximize the MAC throughput. The MAC throughput in a turbo mode is required to be > 500 Mbps using a 100 MHz channel, and > 1 Gbps using bonded-channels.

The MAC layer uses Time-Division-Duplexing (TDD) scheme where all the nodes on the network transmit on the same frequency, but at different time slots or transmit opportunities. All the transmit opportunities are coordinated by a single node called the Network Coordinator (NC). The NC is dynamically selected from all the nodes in the network based on which node has the best broadcast bitloading capability. The NC broadcasts to all the nodes a Media Access Plan (MAP) message approximately every 1ms, defining when each node can transmit in the upcoming time period called a MAP cycle. Thus, the NC ensures that there is no contention for the allocated transmit opportunities. During each MAP cycle, the MoCA nodes are given the opportunity to send RRs to the NC. The NC responds to all the RRs it receives in the MAP cycle by granting time

slots in the next MAP cycle to as many transmissions it can. These transmission grants are sent in the next MAP message. Thus, the nodes 'know' when they should send and receive data during the upcoming MAP cycle. The MoCA 1.1 network throughput is reduced as the MoCA network expands from two nodes to more nodes due to increased overhead since the NC must schedule additional RRs, which reduces transmission time. This issue was addressed by MoCA 2.0 using OFDMA, allowing eight nodes simultaneously to send their RRs to the NC where each node is transmitting its RR on a different set of subcarriers. Not only does this reduce the overhead for the RRs, but also it reduces latency by allowing a MoCA 2.0 NC to grant RR opportunities to all the nodes every MAP cycle.[3]

MoCA defines two methods to protect video traffic from other type of traffic on the in-home coaxial network. In the first method, video is sent as prioritized traffic based on the VLAN tag. Thus, the MoCA device will provide preference to video streams with high MoCA priority compared with low-priority or untagged traffic. The second method is to send video streams using Parameterized Quality of Service (PQoS). A traffic flow with specific Traffic Specification (TSPEC) parameters is configured based on link metrics of the flow. Once the PQoS flow is admitted to the network, its bandwidth is guaranteed to be transported across the network. MoCA 2.0 defines additional TSPEC parameters for greater flow control such as maximum latency, classification rule, in-order packet delivery and retransmission.

Energy efficiency of consumer products, particularly Set-Top Boxes (STBs) and networking devices is an important requirement. U.S. Federal government and the European Commission have initiatives to regulate the maximum allowed energy consumption of STBs and networking devices.[4] To address this issue, MoCA 2.0 defined four power states as shown in Table 4, allowing the MoCA node under the control of its host processor to move in and out of low-power states in coordination with other MoCA devices in the network. In addition, the MoCA 2.0 specifies the rules for transitioning the MoCA device from active state to any other power states, and from the other power states back to the active state.

Table 4 - MoCA 2.0 Power Mode Names and Description

POWER MODE	POWER MODE NAME	DESCRIPTION
M0	Active	Normal operation of the MoCA interface; full power consumption.
M1	Idle	MoCA interface is unable to transmit data traffic, but can receive broadcast and unicast traffic; fast wake-up time.
M2	Standby	MoCA interface is unable to transmit data traffic, but can receive

[3] A. Monk, R. Lee, and Y. Hebron, "The Multimedia over Coax Alliance," Proceedings of the IEEE vol.101 (2013).

[4] European Commission, ICT Codes of Conduct – Please see http://re.jrc.ec.europa.eu/energyefficiency/html/standby_initiative_main.htm

		broadcast traffic; slower wake-up time.
M3	Sleep	MoCA interface is disconnected from the network.

MoCA 1.1 uses 56-bit Data Encryption Standard (DES) encryption for data traffic. The privacy of MoCA 2.0 was upgraded to 128-bit Advanced Encryption Standard (AES) encryption in Cipher Block Chaining mode. Two sets of static and dynamic keys are used for data encryption. In addition, each MoCA device has a programmable password, which is used for distinguishing between MoCA networks either in the same home or adjacent homes.

HomePlug AV and other powerline transmissions

Used for IP networking (IPVOD, CAS call-home for PPV/VOD purchase reporting, application data, and diagnostics).

Please refer to http://www.homeplug.org/ **for more information.**

Part I: Section III. Modes of end-subscriber Use Cases reception of MVPD or OTT service

Discussion of both transport layer details and user experience:

EXPECTATIONS: SECTION III

See Part I: Section VII for expanded Use Case Topics.

A. Streaming – Multicast, Unicast, and Broadcast

B. Download-to-go

C. DVR Purchase

D. TV Everywhere

Part I: Section IV. Technologies (Functional) that enable the reception of MVPD or OTT service:

These are usage of devices technologies from above as applied to MVPD or OTT service reception.

EXPECTATIONS: SECTION IV Part A

Discuss high level description of the function.

Broadcast services.

A. Gateways and MVPD Provided Devices and Environments

Home Network Video Gateways (includes RG)

Key components and features of the RG are:

- xDSL Modem: terminates single-pair and/or bonded-pair copper connections. The modem detects the appropriate xDSL profile automatically and connects customers to the correct VDSL profile.
- Support for local network connectivity:
    - Wired: Ethernet, HPNA
    - Wireless: 2.4GHz 802.11n, 5GHz 802.11ac
- Supports integrated VoIP
- TR-069 Compliant, Integrated Firewall, NAT/PAT support, Diagnostics support
- Supports Ad Insertion
- Provides Battery backup for the VoIP service
- Other key interfaces are:
    - DSL Modem, Gigabit Ethernet WAN, HPNA V3.1 Coax port, up to 4 Gigabit Ethernet LAN ports
    - 5GHz, 802.11 ac, 4x4 MIMO Wi-Fi, 2.4GHz 802.11n MIMO Wi-Fi
    - 2 VoIP lines
    - USB host support

Broadband Gateways (Modems/Routers)

Standalone STBs

AT&T is offering standalone wired and wireless STBs to U-verse customers. The U-verse standalone STBs are designed with a dedicated video System on Chip (SoC) with a secure core to support identification, authentication, and provisioning of services as well as Digital Right Management security system that is used for content security and protection. All of AT&T U-verse STBs are HD capable STBs and the U-verse content is encoded using the H.264/AC3/DD+ compression standards. Some of the key components of the standalone non-DVR U-verse STBs are:

- Dedicated DRAM
- Application Flash
- Boot ROM (or Secure Flash)
- 10/100 Ethernet Port bridged with HPNA – Internal Ethernet switch
- HPNA V3
- USB 2.0 port
- Composite, Component, S-Video, HDMI, Optical TOSLINK Audio outputs
- Infra-Red (IR) Remote Control
- Status LEDs

Digital Video Recorder

AT&T is offering a local Digital Video Recorder (DVR) STB with up to 1TB of HDD. Other features of the DVR STB hardware are similar to the standalone non-DVR STBs. In conjunction with the Mediaroom client software application, AT&T is using the DVR STB to offer Total Home DVR (THDVR) and Remote Pause Buffer services. The THDVR service enables customers to record and playback multiple HD channels (up to 6-record and 3 Playback) simultaneously. Customers can initiate recording sessions and playback of recorded content from any STBs within the home. In addition, the Mediaroom software along with the DVR STB, enables pausing of live TV as well as the use of trick modes on live streams from any STBs within the home. These features are based on proprietary implementations of THDVR and Remote Pause Buffer in the Mediaroom software that is licensed by AT&T. The DVR also supports the storage of ad assets and serving of these assets to other STBs within the home.

Cloud or Network DVRs

MVPD's offer a Network/Multi-Room Digital Video Recording (MR-DVR) platform. Cablevision's system uses the existing STB within the home with no HDD. Other features of the MR-DVR STB are similar to the standalone DVR STBs without a pause buffer. This cloud service becomes a total Multi-Room Home DVR solution. This service enables customers to record and playback multiple HD channels (up to 15-recordings) simultaneously. Customers can initiate recording sessions and playback of recorded content from any STBs within the home. These features are based on proprietary implementations of MR-DVR based on VOD protocols. The MR-DVR system also supports the storage of ad assets and serving of these assets to other STBs within the home.

Mediaroom Applications Software

The Mediaroom application software is a proprietary IPTV application software licensed by AT&T for the U-verse service. The IPTV Mediaroom system was designed as an application platform to support the IPTV services and evolution of service features. The platform is now owned and maintained by Ericsson. The U-verse IPTV service is based on an all Internet Protocol (IP) delivery for Linear/Live and VOD. The service also encompasses a large number proprietary features and value-added services such as Instant Channel Change (ICC), Multiview, and a large number of interactive applications. The Microsoft Mediaroom DRM is used for content protection on AT&T U-verse STBs with an embedded secure SOC. U-verse is offered to third party devices such as smart phones (iOS, Android), tablets, PCs and laptops through AT&T U-verse applications. PlayReady DRM is used for content protection on these devices. Key implementation details of the AT&T U-verse IPTV features are confidential/proprietary.

EXPECTATIONS: SECTION IV Part B

Discuss general function of the application for content discovery and selection. And how the application got on the Retail Device.

OTT services

A. Direct Connect Devices

1. CableCARD Devices

As noted in WG2 Report Section III starting on page 17, CableCARDs and the FCC's "UDCP" rules were originally designed for retail UDCPs that receive one-way linear cable services, but not services that required interactivity, such as VOD and interactive program guides. Cable operators were later required to use CableCARDs in most of their fully featured set-top boxes, and have designed those leased set- top boxes to present their full service offering in set-tops with CableCARDs by tightly integrating the experience into an interactive app. For some providers, that app runs on a particular middleware. UDCPs are not utilizing that app or that middleware. Through bilateral negotiated agreements between the cable operator and the CableCARD device manufacturer, like the one between TiVo and several cable operators, the TiVo "one-way" CableCARD device has access to two-way cable services.

CableCARDs are currently not required or used by current major video distributors like DISH, DIRECTV, AT&T, or over-the-top providers.

B. Application on Retail Device

B.1. Applications deployed to the Apple App Store for operation on iOS devices are written against an Apple-provided iOS SDK. These applications may incorporate code written in any of a number of languages, but Objective-C and HTML5 are historically the most common. Video applications in the iOS context are modal, though this may be changing somewhat in iOS 9. This means that content-provider library discovery, search, and browsing are typically executed in the user-interface context of the application. Developer deployment of applications and application updates is generally managed via the Apple App Store for everyday users. Applications are submitted to Apple for review and distribution.

B.2. Android device applications may be delivered to a device by a number of means ranging from side-loading (direct installation) to various application stores (e.g. Amazon appstore, Samsung Galaxy Apps, etc.), the Google Play store being the most popular. In the case of the Google Play store, applications are submitted to the store and made available at the discretion of the application developer. Google may remove application availability if an application is found to be malicious or otherwise harmful.

Video applications distributed on the Google Play store *may* be modal and isolated, as with iOS applications, but this is not the only mechanism for browsing integration. Instead, Android applications may expose their video programming via software interfaces that allow for system-integrated browsing, searching, discovery, and selection. Amazon's Fire TV provides similar functionality for 3rd party applications, allowing for integrated browsing, search, and discovery. Playback in both cases is handled by the 3rd party's application, but this integration between the 1st party browsing UI and 3rd party video playback UI does not require any service-specific user action.

B.3 With a number of available Smart TV platforms (e.g. Android TV, WebOS, Tizen, Yahoo! Connected TV, Google TV, Google Cast), the approaches for application distribution and content discovery and playback are varied. Approaches to distribution and display range from generally open to curated to closed.

Generally open systems (e.g. Android TV) provide APIs and distribution mechanisms that allow for distribution control but remain largely unrestricted by their platform vendors, resorting to application restriction, for example, in cases of user harm.

More curated Smart TV platforms (e.g. LG's WebOS) provide APIs and distribution mechanisms but require platform vendor approval (typically after extensive testing and validation) before an application may be made available for use.

Further restriction is possible, leaving platform APIs and distribution mechanisms restricted by explicit agreement between platform and service vendors. At present, this group is not aware of any Smart TV platforms still using this approach to application distribution.

B.4 HTML5 with EME encompasses a wide range of use cases for content discovery, search, navigation, and playback, as HTML5 with EME is merely a technology stack allowing for host-based provisioning negotiation. Though HTML5 "applications" may be delivered in a number of ways, the most common approach is to receive the code and content in a browser context while interacting with a server.

B.5 Personal computer-based streaming applications from individual service providers are more rare. Some, like Kodi and Boxee exist, but these are 3rd party aggregation applications often

built without direct input from service providers. As such, service support is inconsistent. We can look to music navigation applications (e.g. WinAmp, iTunes, Songbird, Amazon MP3) as a possible design example, but there are many distinct differences, including local library collection, high title count, and short title (track) duration. Instead, video services are more commonly deployed to computers via HTML with either EME or embedded plug-in viewing mechanisms (e.g. Flash, Silverlight).

C. Standalone Retail Devices

C.1 What can be called an HDTV ranges in function from a dumb monitor to a display-integrated computer. HDTV devices generally incorporate external digital, analog, and tuner inputs, and HDTV endpoint devices may incorporate other interfaces such as USB, TOSLINK, Ethernet, etc. Generally, HDTV devices may receive MVPD content via tuning unencrypted channels (e.g. ClearQAM). "Smart TV" HDTV devices may also access video content over WiFi, Ethernet, or local storage connections.

C.2 DVR – Update shortly.

C.3 Portable media storage devices (e.g. SD Cards, external Hard Disk Drives) may be used to store video content for later playback. These devices can be connected via a number of interfaces, the most common being USB. Content stored on these devices may be cryptographically "keyed" to be decodable on a single device or limited group of devices.

Part I: Section V. Technologies (Standards/Protocols) that enable the reception of MVPD or OTT service:

WG4 collecting list of technologies for now. This section may become list of references, or may include necessary analysis.

EXPECTATIONS: SECTION V

Discuss how Protocols enable reception of content.

Google Fiber IPTV System Overview

Summary

This outlines the various components of the Google Fiber IPTV service. It's purpose is to explain how we may operate differently than other MVPDs and also to explain how it's service could be adapted to work with a market for 3rd party retail navigation devices. Overall, Google Fiber operates like most MVPDs do with regards to having installers, CSRs, headends, content ingestion/transcoding/distribution and in home STBs.

Linear TV Feeds

Linear TV channels are sent out over IPTV multicast. The channels use H264 video encoding and either MPEG or Dolby Digital audio encoding. The transport layer is a single program MPEG2 Transport Stream. They carry multiple audio tracks when present. Closed captioning and AFD information is also retained in these streams. Retransmitted local broadcast channels are sent without encryption. All other channels are encrypted using Widevine with EMM/ECM data present in the stream. Households that do not subscribe to the TV service have the IPTV multicast signal blocked at the network level.

Video on Demand

Google Fiber has all types of VOD content; free, subscription based and transactional. VOD content is served over HTTP and encrypted using Widevine. The streaming format is specific to the Widevine VOD implementation that is used. We also provide VOD content served over the DASH protocol; which is currently utilized by our mobile/tablet clients and will likely transition to this protocol for all VOD streaming in the near future. VOD streamed via DASH supports playback using standard EME.

Metadata

Metadata relating to the program guide information and VOD content is delivered via HTTP to the clients. This data also contains the mappings of logical TV channels to their actual multicast IP:port. It comes down as a compressed BLOB of data which is a delta of the information from the last retrieval. It is also possible to download the full set of information, which is what occurs for a newly provisioned STB. The data is in a proprietary format. Imagery associated with the metadata has URLs specified in the metadata so those images can be retrieved for presentation in the user interface.

Content Authorization

A secure HTTP RPC service is provided for clients to retrieve information relating to content authorization and subscribed channels. Connection to this service requires validation of security certificates in a bi-directional manner (i.e. SSL where both client & server certificates are validated). This service provides the information on what specific channel lineup the device should be using (so it can then request the proper metadata). It also provides a list of all the devices in the home that our whole home DVR storage box is allowed to communicate with. It also lists all of the channels that the user is authorized for viewing. The DRM components in the client also connect to this same service in order to obtain the data they need in order to enable decryption of the subscribed linear TV channels and authorized/purchased VOD content and know the output protection rules associated with that content. (NOTE: These are not the

actual encryption keys, but keys that in conjunction with the DRM secrets loaded into the device along with the ECM/EMM information in the MPEG stream allows it to generate the decryption keys for the content. Keys are rotated on a regular basis for the linear TV channels.)

Emergency Alert

EAS information is sent out over an IPTV multicast feed and contains all the information the device would need in order to properly respond to an EAS/EAN event.

Monitoring & Logging

Device logs are uploaded regularly to Google servers for analysis and processing. We use the TR-069 protocol for management, provisioning, remote configuration and other types of data collection.

K. Adaptive Bit-Rate Streaming (DASH)

Slingbox

The Slingbox is a TV placeshifting device that allows users to watch their live TV or DVR content anywhere via an IP connection. It is able to connect to virtually any MVPD's STB. Connections are only 1-1, meaning a single session per Slingbox. Please refer to http://www.slingbox.com/ for more information.

Real-Time Transport Protocol (RTP)

In order for a third party to implement the Mediaroom features, they need to license the Mediaroom platform. The following provides a high level overview of the two key features:

ICC: instant channel change is achieved by a combination of TCP and UDP IP traffic for a specific channel and detailed implementation of ICC is confidential

RUDP: Resilient UDP is another technology used by Microsoft to provide reliability. This is also a proprietary Microsoft technology.

Part I: Section VI. OTT Services

WG4 creating an exhaustive list during its work, and then WG4 will pare down and group the list for the final report into those services that matter in their salient features.

EXPECTATIONS: SECTION VI

Some OTT services have different applications on different platforms. Describe the operation of each application for the discovery and reception of content.

Part I: Section VII. Essential Customer Experiences

Include messaging and protocols that enable these experiences during analysis.

PURPOSE

Through a series of Use Cases, specify the content subscription service elements that are currently available and used by the market.

INTRODUCTION

These Use Cases serve to identify and describe the current service features that an end-subscriber (consumer) may gain access to when they have a subscription to a content service.

Examples of a content subscription service would be a subscription to a Multichannel Video Programming Distributor (MVPD) or an Over-The-Top (OTT) service. The dissemination of these services can be transmitted through a series of paths, such as cable, satellite or via an Internet connection or a combination thereof.

It is important to note that these subscriptions are bound by agreements made amongst several parties. For the User, traditionally, this agreement is between themselves and the content subscription service. For the content subscription service provider, there are multiple agreements, including those with content providers, advertisers, metadata providers, CAS and DRM vendors, set-top box manufacturers, and others. These agreements are important to note as they govern the content ecosystem that is being accessed by the subscriber.

The following Uses Cases recognize these agreements; making no attempts to circumvent such business agreements.

Outlining and categorizing virtually every service feature available aids in the identification of the salient differences amongst the categories and service offerings. Some of the devices reviewed by the DSTAC Working Group support only some use cases or only some features within a use case. The report analyzes the features and use cases that are or should be supported. That analysis may assist in evaluating alternative systems and features that are or should be baseline requirements for service providers and device manufactures, as well as the evaluation of platforms or devices in the marketplace that are able to satisfy these Use Cases.

It should also be noted that these Uses Cases may change over time. The purpose of this document is to relay Use Cases based on current market availability.

END-USER Precondition: Consumer already has a subscription with an MVPD or OTT provider.

USE CASE #1 - Tuning and Viewing a Linear Channel

USE CASE DESCRIPTION

This use case covers when a subscriber tunes to a new channel using channel up/down, direct channel entry, or from other navigation (the linear and on-demand navigation use case is covered below).

TRANSMISSION METHODS

While an MVPD device must only support the transmission methods for the MVPD's network, a retail device for this use case should be able to support methods for transmission of linear channels, including:

TRANSMISSION METHOD	ACTIVE EXAMPLE
Analog	There are a small amount of Cable operators in the country who still transmit some channels using analog transmission methods.
QAM broadcast	Quadrature Amplitude Modulation (QAM) is the standard for broadcast of digital video on cable networks today. In the United States, the QAM standard used is ANSI/SCTE 07, 2000: Digital Video Transmission Standard for Cable Television.
QPSK DVB-S2	Quadra-phase Shift Keying (QPSK) is a modulation system used in DNBS broadcast systems. DVB-S2 is an advanced coding system defined by DVB.
QPSK DSS broadcast	See {ref}
DVB-S2 broadcast	. DVB-S2 is an advanced coding system defined by DVB. See {ref}
QPSK and 8-PSK Turbo broadcast	8-way-phase Shift keying 8-PSK
Multicast User Datagram Protocol (UDP)	?:Milo]
Multicast Real-Time Protocol (RTP with custom adaptation layer) over UDP	?:Milo]
Unicast RTP (with custom adaptation layer) over UDP	The U-verse TV system uses unicast RTP based messages to deliver instant channel change video payload to the client. When booted, each STB receives a listing of video

	session assignments to a specific Distribution server (D-Server) from the D-Server cluster. The Payload is delivered vis Unicast RTP over UDP by the D-Server. The RTP adaptation fields contain information that identifies various real-time events such as Blackout markers and tables, Random Access Points (RAP) among others. In addition to this, the D-Server may add event specific markers to the RTP extension for a specific request. The unicast RTP delivery is also used for delivering error correction payloads for lost or corrupted packets as part of the resilient UDP (RUDP) mechanism.
QAM switched digital video (SDV)	Switched Digital Video (SDV) for QAM networks is a method of implementing IP multicast using broadcast QAM transport rather than IP. This permits only those broadcast channels in a service group that are being watched to be transmitted to that service group. Those channels which are not being watched in a service group are not transmitted and thus save bandwidth enabling more channels to be carried in the same amount of bandwidth as a purely broadcast system. The two-way out-of-band channel used on the particular system provides the two-way communication path necessary for a set-top to request a particular SDV channel using a proprietary protocol.
NACK-Oriented Reliable Multicast (NORM) Transport Protocol	NORM is an IETF RFC for a protocol that can provide end-to-end reliable transport of video streams over generic IP multicast routing and forwarding services. CableLabs recently issued several specifications that use NORM for transport of Adaptive Bit-Rate video streams over IP multicast. The relevant specifications are: • IP Multicast Server – Client Interface Specification, OC-SP-MS-EMCI, Cable Television Laboratories, Inc. • IP Multicast Controller-Server Interface Specification, OC-SP-MC-MSI, Cable Television Laboratories, Inc. • IP Multicast Controller-Client Interface

	Specification, OC-SP-MC-EMCI, Cable Television Laboratories, Inc. IETF RFC 5740, NACK-Oriented Reliable Multicast (NORM) Transport Protocol, November 2009.

As some MVPDs transition to converged IP networks, new transmission methods will be introduced and some transmission methods will be deprecated. Examples of IP streaming include HLS (https://developer.apple.com/streaming/) and DASH (http://mpeg.chiariglione.org/standards/mpeg-dash).

CODEC SUPPORT

While an MVPD device must only support the codecs used by the MVPD's network, a retail device for this use case should support audio and video codecs, including:

- MPEG-2 Note that DBS systems will typically use GOP structures lasting multiple seconds.
- MPEG-4 AVC/H.264
- HEVC/H.265
- MPEG-1 Audio
- Dolby AC3
- Dolby Digital Plus
- AAC
- AAC Plus

The following table lists examples of codecs and how they are currently being used by the listed entities.

MVPD	CAS	Core Cipher	Transport	Control Channel	Video Codec
Cable	• DigiCipher 2 • MediaCipher • PowerKey • NDS VideoGuard • Conax • Nagravision • DTA • OMS • BBT • Verimatrix VCAS for Broadcast-Hybrid	• DES-CBC • DES-CBC • DES-ECB • CSA • CSA • CSA • DES-CBC/ECB • CSA/DES/AES • AES • AES/DES/CSA	• QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/IP/MPEG-2 TS	• SCTE-55-1 • SCTE-55-1/DOCSIS • SCTE-55-2/DOCSIS • Generic IP • Generic IP • SCTE-55-2/DOCSIS • In-Band • DOCSIS • Generic IP • Generic IP	• MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2, MPEG-4/H.264
Satellite	• NDS VideoGuard • Nagravision • Terrestrial free-to-air	• DES/AES • CSA/DES/AES • N/A	• QPSK/DSS TS, DVB-S2/MPEG-2 TS • QPSK, 8-PSK Turbo/MPEG-2 TS • 8-VSB/MPEG-2 TS	• In-Band • In-Band • N/A	• MPEG-2/AVC • MPEG-2/AVC • MPEG-2
Telco	• Mediaroom DRM • MediaCipher/PowerKey • Verimatrix VCAS for IPTV	• AES • CSA • AES/DES/CSA	• Multicast/Unicast-IP/VDSL/FTTP • QAM/MPEG-2 TS & IP/BPON or IP/GPON • IP Multicast MPEG-2 TS	• IP/VDSL/FTTP • SCTE-55-1/SCTE-55-2 • Generic IP	• AVC • MPEG-2/AVC • MPEG-2, MPEG-4/H.264
Google Fiber TV	• Widevine	• AES	• IP/GPON	• IP/GPON	• AVC

NOTE: This table was cited within the DSTAC Working Group 2 report {ref} and was described as a summary of known, deployed CAS systems, each of which has its own unique licensing and trust infrastructure, along with the associated core ciphers, transports, control channels, and video codecs in use.

As new video and audio codecs are introduced, MVPDs will take advantage of them. Over time some codecs will be deprecated. In instances where a separate decoder is used these aforementioned codecs may not be called upon for use. For example, a gateway device might

not have an HDMI output, and therefore have no decoders on board. The device with the decoder would be the end point client device, such as a tablet or RUI client.

IMAGE QUALITY

While an MVPD device must only support the picture resolutions and formats used on the MVPD's network, a retail device for this use case should be capable of supporting common picture resolutions and formats, including:

- SD 480i/480p
- HD 720p (30 and 60 fps)
- HD 1080i
- HD 1080p (24 and 30 fps)
- 4K and UltraHD (High Dynamic Range (HDR), Wide Color Gamut, deep pixel depth)
- 3D frame compatible (Side-by-side, Top-and-Bottom, Interlace)

As new picture resolutions and formats are introduced, MVPDs will take advantage of them. Over time some resolutions and formats will be deprecated.

Because content may be decoded to various resolutions and refresh rates, devices displaying content to different target resolutions and rates should be capable of spatially and temporally resampling supplied content to maintain spatial and temporal consistency. Example algorithms include, but are not limited to, nearest-neighbor, bilinear, Lanczos.

Normative References:

- ARIB STD-B56, "UHDTV System Parameters for Programme Production"
- …

STREAM MANAGEMENT (Resource Allocation)

Stream management is the allocation of stream resources within a defined network. Where necessary, a device for this use case must support the concurrent stream management required to limit the number of concurrent streams that a subscriber can receive and/or view. Stream management is also used to manage the number of simultaneous ingress and egress streams for THDVR.

The device shall limit streams to be consistent with the number of authorized access points. Note that stream management is not limited to solely HD and SD streams.

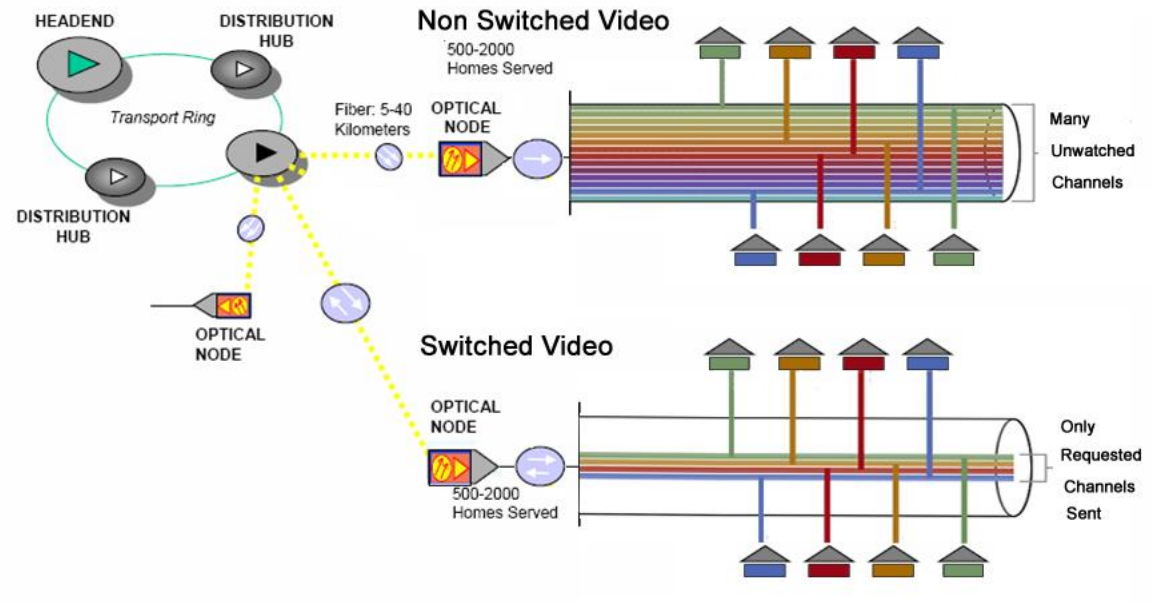
Stream management is necessary when addressing access network bandwidth limitations, tuner limitations (in particular in the case of satellite) or fraud prevention (credential or password sharing).

Examples of Stream Management include:

SYSTEM	ACTIVE EXAMPLE
AT&T U-Verse	Stream management used by Mediaroom is a proprietary implementation that manages the number concurrent WAN streams (coming to the home) and DVR record and playback streams. This feature is part of the Mediaroom application software running on the STBs.
DBS	DBS receivers typically have limited numbers of tuners that are distributed among DVR recordings, attached displays, and network displays. Management of tuner resources is a task for the main server in a DBS installation.

SWITCHED DIGITAL VIDEO

Switched Digital Video (SDV) allows an MVPD to make efficient use of bandwidth by only broadcasting those channels that are currently being watched within a given area, e.g., a node, or neighborhood. This allows the MVDP to use the reclaimed bandwidth for other services, including higher data speeds. The network looks for tell-tale signs of viewer inactivity, asks the viewer if he or she is still watching, and recovers the channel if there is no response. The exact SDV techniques vary by vendor, but they rely upon SDV client software in the customer device or a tuning adapter. For SDV to work with retail devices, all current implementations would need to be ported, a predictable software client would need to be present in the retail device, the solutions would need to be tested for operability and for functional tuning performance across MVPDs, and room would need to be left for the implementations to continue to evolve and improve. If there is no client to communicate viewing status upstream, there is no recovery of bandwidth, and SDV would fail in its essential purpose of opening bandwidth for more channels, more high-definition, faster broadband and more advanced services. See below for high level overview of SDV.



Some of the key elements of SDV are:

- Dynamic channel mapping information identifying the current channels being transmitted into a service group and their tuning information.
- Tuning requirements (methods).
- Keep-alive messages, indicating that a channel is still being watched.
- Time-outs, indicating that a channel may potentially no longer being viewed based on the lack of viewer activity via the remote control.

Customer notifications (e.g., tear-down of channel), to insure that the viewer is in fact no longer watching the channel, before actually taking down the channel.

APPLICATIONS

Applications provide additional information or access to additional services, as selected by or subscribed to, by the User. A device with the ability to support integrated or program synchronous applications, should ensure that integrated applications or applications associated with the tuned channel, are presented and accessible to the User. Currently, some technologies used are Widgets, Enhanced TV (EBIF), and MediaRoom. Other proprietary applications, such as those related to OTT services, may also be supported by the device.

Examples of integrated or program synchronous applications include:

- Headlines ticker
- Instant local weather
- Sports scores and statistics
- Shop by remote
- Bookmarking ads
- Social networks (Twitter, IM, SMS, etc.)
- Mosaic channels
- Telescoping
- Auto-tune HD
- “Mix” channels (mosaic of multiple channels / camera angles)
- Set timers (e.g. for future sport events or tune to current events)
- Communication service compatibility
    - Voicemail, CallerID requires integration with telephone networks
    - May be used for home automation and home security networks

ADVERTISING

Advertising messaging, when part of a service, should not be deliberately filtered out. The following advertising models must be supported:

- Local insertion of broadcast advertising into linear television
- Local insertion of zoned or targeted advertising into linear television
  i) Must receive if delivered from network
  ii) Must securely store & delete in device and insert if managed by the device
- Interactive Request For Information (RFI)
- Telescoping to on-demand advertising
- Must honor and be compliant with advertising rules, such as:
  i) Rules about ads in conjunction with a network's video
  ii) Rules preventing interference, substitution or removal of ads
  iii) Limitations on web links when programming is directed to children
  iv) Rules about the inclusion of advertisements, promotions, sponsorships, and/or overlays that are displayed, in or around, a network's video window (linear & VOD) while the guide experience is engaged.
  v) Support for availability windows (e.g., C3 or Post-C3 ad loads)
- Ad measurement and reporting
  i) Report back the display of an ad for frequency limits or analytics of reach of the ad campaign
- Protection of ad boundaries, especially as it relates to substitute programming or downstream devices
- Ad asset storage and lifecycle management
- Integration with Ad Decision Management (ADM) and Ad Decision Systems (ADS)
- Honor C+3, C+7, etc. ad insertion rules for DVR content playback

This use case also requires support for an audit trail to validate that the advertising has been presented as relayed.

DEVICE REQUIREMENTS

1) A device must ensure that blackouts are supported.
    a. Content delivered to the device (e.g., from satellite or cable distribution hub or IPTV super hub office) must be blacked out if not authorized (e.g., in-home vs. out-of-home, in-market vs. out-of-market, in-region vs. out-of-region, domestic vs. international).
    b. Customer notifications, including messaging, signaling & placement (e.g., notifying customers of blackout restrictions or alternate programming requirements).

2) A device must support parental control.
    a. Content delivered to the device must not be tuned or presented if restricted by Parental Control (PIN setting and resetting both via device and through customer support, PIN enabling and disabling, PIN entry).
    b. Adult title blocks.
    c. Requirements: 47 U.S.C. §§ 624(d)(2) and 640
    d. Supporting standards: CEA-608, CEA-708, CEA-766.

3) A device should support Alternative Content.
    a. The device must receive and insert appropriate content as alternate to regional blackouts (sports, network non-duplication, syndicated exclusivity) or other programming rights restrictions (e.g., in-home vs. out-of-home).
    b. Customer notifications, including messaging, signaling & placement.
    c. Advertising substitutions to accommodate content and channel ratings.

4) The device must support messaging and redirection for unauthorized channels.

5) The device must enforce copy control, image constraint, and selectable outputs control as indicated by CCI or on-demand applications.

6) The device must enforce copy count limitations.

7) The device must enforce pass-through/regeneration of copy control information on outputs (e.g., CGMS-a, APS).

8) The device must enforce/allow transit, delay/latency and round-trip time restrictions beyond those defined by standards such as DTCP or HDCP.

9) The device must not deliberately filter out watermarks (video, audio, other). Watermarks, in this case, are forensic markers embedded into a piece of content to permit after-the-fact detection of the source of security breaches.

10) The device must enforce geo-filtering and geo-fencing requirements & restrictions beyond blackouts (e.g., alternate programming).

a. E.g., restrictions/requirement for what can be displayed in common areas, commercial/university properties

11) The device should support and must tolerate the presence of Active Format Descriptor (AFD) signaling (e.g., letterbox, center-cut an HD signal to fit SD presentation).
    a. Normative references: CEA-805, ATSC (A/65, A/81), SMPTE AFD.

12) The device must support transcoding or down-res'ing restrictions or requirements (e.g., minimum encoding bitrates/quality).

13) The device should support the feature of HD channel preferred.
    a. When the subscriber tunes to a simulcast SD channel the device suggests tuning to the HD version, or does so automatically if configured accordingly.

AUDIENCE MEASUREMENT

Audience measurement is the ability to report back viewing metrics based on anonymized census-level audience data derived from set-tops. This is a non-intrusive service. Current audience measurement techniques enable MVPDs to measure audiences for channels and when viewers tune in and tune out. This helps to determine which programs are most popular, how many people watch a program to its conclusion, what viewership to report to advertisers, which programs and channels to carry, how to optimize programming to meet changing viewer demand, and how to sell advertising that underwrites the programming and networks provider to consumers. Examples include: Audience measurement of long tail and small market programming; Audience measurement to allow ad buyers to buy advertising in specific dayparts and networks; DBS delivery of targeted ads based on household characteristics; Consumer-packaged-goods companies measuring ROI by correlating campaigns with lift in sales.

PLAYBACK

This use case requires the activation of trick play capability of live TV, e.g. pause, fast forward, and rewind, each at multiple speeds and may be enacted through the following methods:

- Time shift buffer
- Using local DVR
- Using network DVR

Pause and Resume are currently available and traditional features. The device and system should support pausing content on one device and resuming from another device.

INSTANT CHANNEL CHANGE

Some MVPD devices support Instant Channel Change (ICC), a feature that minimizes or eliminates channel change latency, depending on the MVPD's network. A retail device for this use case should support and include a variety of different methods of implementing ICC, including:

- IPTV – multicast and unicast RTP/UDP/IP
- QAM SDV
- Broadband tuners and demodulators
- Opportunistic device caching
- Pre-decoding of adjacent channels, with associated stream count limitations enforced.

REGULATORY REQUIREMENTS

There are a number of regulatory requirements for this use case. A device should support all service provider and device regulatory requirements, as obligated by law. Examples of regulations include:

- Safety and interference requirements.
- Emergency Information
    - Emergency Alert System (EAS) local and regional. Receives EAS on all channels. Supports force tune and text crawls with audio replacement.
    - Emergency Information: When emergency information is conveyed visually during non-newscasts (such as in on-screen crawl), the secondary audio stream must be used to convey such emergency information aurally, preempting any other use of SAP, such as DVS or foreign-language.
- Accessibility Access (e.g., top-level vs. lower-level; ease of access)
- Advanced Communications Services (ACS), such as two way electronic messaging services (e.g., real-time text and video chat applications), must be accessible to and usable by persons who are blind or have limited vision
    - On July 1, 2016, the waiver of the ACS requirement is set to expire. The waiver includes IP-TVs, IP-Digital Video Players (DVPs), and Set-Top-Boxes leased by cable operators.
- Nielsen
    - Audio watermark pass-through
    - ID3 tag pass-through and/or regeneration
- Commercial Advertising Loudness Mitigation (CALM) Act
- Pass-through of VBI (analog) (e.g., V-Chip, CC, VITC, etc.) and regeneration of digital counterpart.

Normative References:

- Accessibility: 47 C.F.R. Parts 14, 79; SMPTE ST 2052-1-2010, Timed Text Format (SMPTE-TT)
- CALM: 47 CFR §76.607; ATSC Recommended Practice (RP) A/85
- EAS: 47 C.F.R. Part 11
- Nielsen: 47 C.F.R. §§76.62; Carriage of Digital Broadcast Signals, 16 FCC Rcd 2598 ¶ 61 (2001).
- Privacy: 47 U.S.C. §§ 338(i), 551
- Pass-through & V-Chip: 47 U.S.C. § 534(b)(3); 47 C.F.R. §§76.62; 76.606; ATSC A/65 PSIP standard; Carriage of Digital Broadcast Signals, 16 FCC Rcd 2598 ¶ 61 (2001); Second Periodic Review of the Commission's Rules and Policies Affecting the Conversion to Digital Television, 19 FCC Rcd 18279, ¶¶ 154-159 (2004).
- Parental control: 47 U.S.C. §§ 624(d)(2) and 640

USE CASE #2 - Viewing On-Demand Content

USE CASE DESCRIPTION

This use case incorporates the features laid out within the Linear Content Use Case.

This use case also covers the multiple forms of on-demand content consumption, examples include:

- Transactional VoD (rental transaction, including purchase screen)
- Subscription VoD (premium subscription content, authorization only)
- Free VoD (non-premium content, no authorization or purchase screen)
- Electronic Sell Through (EST, purchase screen on first viewing only, authorization only on subsequent viewing)
- Start Over™ (similar to subscription VoD, but contextual)
- Look Back™ (similar to subscription VoD)
- Purchase PIN (PIN setting and resetting both on TV and through customer support, PIN enabling and disabling, PIN entry)
- Device meets trick play requirements, e.g. disables FF with OD content (typically during advertisements), per content provider condition, disable skip (e.g., 30-second skip) for full assets or intra-asset.
- 3rd party devices must support a purchase UI controlled by the MVPD system.

In satellite systems, each of these can furthermore be implemented via a priori staging of content on local DVR storage. Devices interacting with DBS systems must accept catalog information from the attached DBS gateway – depending on download history and broadband connectivity, any particular DBS gateway will have unique sets of VOD content available. The variations in content will include variations of resolution (1080p/3-D/UHD/HD (1080i & 720p)/SD, etc.) and pricing.

USE CASE #3 - Tuning and Viewing Pay Per View (PPV) events

USE CASE DESCRIPTION

This use case incorporates the features laid out within the Linear Content Use Case.

This use case covers the purchase and viewing of PPV events including the following PPV features:

- Free preview window – period of time subscriber can view PPV event without paying.
- Purchase window – period of time subscriber can purchase the PPV event.
- Cancellation window – period of time during which subscriber can cancel the purchase of the PPV event
- Secure purchase credits and purchase limits – In general, PPV event purchases are done on a store and forward basis, purchases are stored securely, set-tops are provisioned with limits on the number or amount of purchases that can be made before the purchases are collected
- User interface required to present time remaining in preview, purchase, and cancellation windows, as well as the transaction and when the purchase limit is exceeded, including messaging capabilities (e.g., call-in numbers, contact information)
- Purchase PIN (PIN setting and resetting both on TV and through customer support, PIN enabling and disabling, PIN entry)
- Auditing and reporting
- Devices interacting with DBS systems must accept guide data from the attached DBS gateway – accurate guide data is available for in-home use. The variations in content will include variations of resolution (1080p/3-D/UHD/HD (1080i & 720p)/SD, etc.) and pricing.
- Limited time recording of PPV events on 3rd party devices may be supported.
- 3rd party devices must support a purchase UI controlled by the MVPD system.

USE CASE #4 - Navigation

USE CASE DESCRIPTION

This use case covers the broad range of methods for navigating linear and on-demand content. Regardless of the method, the navigation must respect the content provider's license agreements about channel placement and neighborhoods. There is a significant effort that goes into the navigation to optimize consumer satisfaction and make it easy to use / enjoy features of the service.

There are many different methods of navigating linear and on-demand content that should be considered, some examples include:

- Provide a familiar or similar interface across the multiple devices consumers use to access the service
- Grid guide
- Cloud based guide variants / RUI
- Talking guide
- Emergency Information settings & accessibility
- Closed Captioning settings & accessibility
- Channel presentation in required neighborhoods (e.g., news channels) and channel assignments (e.g., broadcaster carriage on channel)
- Favorite channels, recent tuning history, bookmarks, etc.
- Recent tuning history across devices
- Mosaics & associated navigation
- Cover art
- Channel logos
- Thumbnails
- Search – including both locally-based and network-based
- Network-branded points of entry, e.g. content provider requires that their on-demand content be accessible through a network-branded folder labeled "Disney" or "HBO" rather than just being commingled with other on-demand content
- Multiple guide view…genre, by network
- Devices interacting with DBS systems must accept guide data from the attached DBS gateway – accurate guide data is available for in-home use. Variations between particular homes will include blackout and local channel availability, and will require a generated guide to accurately reflect conditions in any particular subscriber's home.
- Both HD and SD versions of channels may be available with otherwise identical service and event information. Standardized table structures may not distinguish between 3-D, UHD, HD and SD versions.
- Recommendations from user profile across devices
- Recommendations from what's trending or popular in neighborhood
- Trick play – fast forward and/or rewind, at multiple speeds, skip chaptering, etc.
- Navigating and Billing for VOD including:
    - Verification of purchase

    - Offer of multiple options (e.g., rent or EST)
    - Integration with billing system/account management
    - Record customer purchases
- Search, including:
    - Voice control via remote
    - Voice control smart phone, tablet or similar device
- Whole Home capabilities:
    - Ability to advertise services to the home network
    - Ability to discover services on the home network

Multiple features above may be combined in the navigation functions.

USE CASE #5 - Recording Linear Content

USE CASE DESCRIPTION

This use case includes all of the features of the Linear Content Use Case and also covers the recording of linear content via Digital Video Recording (DVR) capabilities. If recording rights are available for a particular channel or event, then also see linear tuning use case for additional features.

There are a number of implementations that should be considered:

- Record on local hard disk drive
- Record on whole home DVR and supporting home network protocols
- Record on Remote Pause Buffer (Pausing Live TV from any STBs within the house)
- Record on Network or Remote Storage DVR (similar to subscription VoD, but on a per subscriber basis, with associated database and navigation)
- Time-shift-buffering and limitations (e.g., restricted to 30 minutes)
- Record timers based on:
    - Content type: first time airing, reruns
- Content removal incited by the timed recording.
    - Content can be expunged based on settings related to number of recordings to keep, priority, etc.
- Record on mobile device, side car recording
- Move recorded content onto an authorized device(s)
    - A “move” removes the content from the source device. No copies are to be made in a “move” scenario.

To support accessibility requirements and choices made during playback, 3rd party devices must preserve all audio streams and associated metadata at the time of initial recording.

Recording rights may differ on a channel and/or event basis.

Recording rights may change over time and should be verified at the time of recording.

USE CASE #6 - Remote Management by Consumer

USE CASE DESCRIPTION

This use case covers management functions available to the subscriber remotely or on a network-connected mobile device.

RELATED REQUIREMENTS

Management of Tuning

Management of the service by the subscriber remotely, including by the primary display and by a network-connected mobile or second screen device:

- DVR scheduling
- Content search
- Remote control
- Parental controls, including device restrictions (e.g., by channel, rating, time-of-day, etc.)
- Management of some DBS gateways may require security certificates available from the MVPD.

Management of Account

Management of the account by the subscriber remotely, including by the primary display and by a network-connected mobile or second screen device:

- Account management, pay your bill via integration with billing system
- Subscription management – ability to upgrade or downgrade service packages on-screen with remote, requires access to service catalog and integration with the billing system
- Self-help customer service support items (e.g. schedule a service call or appointment)
- Subscriber Account Management may be supported on standard HTML5 web browsers that are connected to an MVPD's internet site.
- Account and password information should not be cached by an unsecure device or in unsecured/unencrypted storage.

USE CASE #7 - Set-Top Box set-up

USE CASE DESCRIPTION

This use case covers how a subscriber can set-up a number of preferences for the operation of their set-top box, including:

- Menu Preferences, such as changing the background darkness level and auto-tuning to HD channels, overscan of image, on-screen overlays and their positioning.
- Device Settings
    - Closed captioning
    - Audio settings
    - Light brightness of your set-top box
    - Inactivity standby options
    - Nightly reset time
    - EPG preferences (size, favorite channel list)
    - Remote control setup for 3rd party devices (TV, A/V receiver)
    - Audio output format and volume leveling settings
    - Control of HDMI-CEC for 3rd party devices (TV, AV Receiver)
    - Output video resolution to TV:
        - SD 480i
        - ED 480p
        - HD 720p
        - HD 1080i
        - HD 1080p
        - UHD 2160p
- Parental Controls, see above
- PIN Controls, see above
- Accessibility (e.g., Closed Captioning, audio track selection, etc. – see above)
- Many settings and options will only be available through the MVPD device UI.

Management of Device

Management of the device settings by the subscriber, including by the primary display and by a network-connected mobile or second screen device:

- Captioning
- Language selection
- Energy management
- Remote management and other tasks may require access to the video output or UI pages generated by an MVPD device.

USE CASE #8 - Customer Support and Remote Management by Service Provider

USE CASE DESCRIPTION

This use case covers customer support and remote management features provided by the MVPD.

- Remote diagnostics
- On-screen diagnostics
- Ability to disable a device and display a notification (e.g. Call your service provider)
- Backup of set-top box configuration in the network (e.g. preserves DVR scheduling, configuration preferences, etc.)
- Unified remote control experience
- Reporting back on statistics like signal level, device temperature and crash reports
- Software updates
- Some MVPD devices may save device and user settings in associated remote control devices.
- CSR support will require the subscriber to access the MVPD's device UI and may require access to raw video output of the MVPD device.

USE CASE #9 - Installation and Provisioning

USE CASE DESCRIPTION

[This use case should describe the installation and provisioning of the service and customer premise equipment necessary to receive the service. This use case should cover the range of installation from self-install to professional install, and should include home networking setup of multiple display devices (retail and MVPD/OTT) in the home.]

This use case includes functionality to verify the quality of an installation (e.g. correct orientation of a satellite dish) prior to allowing authorization of services.

- Ensure pre-reqs for service have been met by customer – i.e. network access setup and configuration, Wireless network, home wiring, etc.
- If Ethernet over Coax technologies (i.e. HPNA or MoCA) are used, coaxial home wiring should be tested before installing STBs to ensure proper network connectivity and throughput
- When wireless home networking is used, installers should verify rate, reach, Wi-Fi interference to ensure high quality of service over Wi-Fi
- Secure Register with unique Consumer Device ID with backend systems to receive service authentication and access data
- Ensure that customers are correctly provisioned for the services/packages they sign up for
- During installation verify the following:
    - Service is up and running
    - Remote control functions properly
    - All services features (i.e. ICC, THDVR, etc…) and interactive applications are operational
- Some in-home network technologies will not interoperate with more than one MVPD present. Parallel wiring may be required.

DBS-RELATED REQUIREMENTS

DBS systems need to be able to:

- identify the customer's satellite matrix (which satellites are visible, and how to connect and tune to them through a multiswitch),
- connect to "slim" clients within the house,
- prompt for STB authorization requests (e.g.,. call for authorization),
- Configure STB remote to control TVs, A/V Receivers, DVD/Blu-ray players that may be connected to the system, universal remote setup, and configuration of IR-Blasters for control of VCRs.

- Professional installation of service will require access to the video output (HDMI, Component, composite) of provided gateway device.
- MVPD provided devices will require access to DBS broadcast to download current device software.

USE CASE #10 - Device Operation Requirements

USE CASE DESCRIPTION

This use case covers additional features that normally run in the background, and are generally part of maintenance, security, and efficiency interests. Such interests place requirements on the device, for example:

Software Updates

Software updates for retail devices are typically the responsibility of the device manufacturer, while software updates for MVPD provided devices are typically the responsibility of the MVPD. There are some instances, for example DOCSIS cable modems purchased at retail, in which the cable operator may assume responsibility for software updates to insure that network interoperability is maintained. Methods by which software updates are disseminated and secured for retail devices is also typically determined by the retail device manufacturer. Frequently, software updates for retail devices are disseminated over the Internet, which assures two-way communication and permits validation of the receipt and successful, secure installation of the software update on the retail device. Methods by which software updates are disseminated and secured by MVPDs are specific to the MVPD, as well as performed over the MVPD's network. CableLabs specifies a secure software download mechanism as part of the DOCSIS and PacketCable (VoIP) specifications. Secure software download is tested as part of the certification of these devices.

Privacy and security

- Device secured against unauthorized access
- System requires court process for access by government
- Device must have required registered certificates for encrypted communications with backend systems.
- Device must comport to FCC and FTC rules on privacy.
- May need to access raw video output during countermeasure checks.

Energy Efficiency requirements (Voluntary Agreement for set-top boxes)

Including configurability of sleep timers, inactivity & turn-off notifications

Meet consumers' expectations of how well hardware and software should work together (i.e. performance requirements)

USE CASE #11 – User Authentication

This use case covers the minimum requirements a device must comport to in order to authorize transmission of content to an approved device.

In order for a device to receive specified content, the User and Device must abide by the following:

- Per the Precondition, the User has a subscription to a content service.
- The content service subscription authorizes connection to the content being accessed (e.g. conditional access).
- The device must abide by the rules invoked by the content usage and security settings. Examples include:
    - Permissions
        - Subscription will conform to region settings (neighborhoods, blackouts) and service settings (entitlements).
        - Device Authorization Access
        - Content or application enforces applicable usage restrictions
        - Rights Management
    - Devices are required to track current version of DRM and security updates.
        - Currently these updates are managed by the device and/or service provider network.

In the event the conditional access permissions do not align, then the User should see a notification message about this incompatibility and content will not be sent to the device.

USE CASE #12 – Renewability Management

In order to protect the user during an unscheduled event, a service provider must have the ability to contact the user through the device. This Use case covers the methods through which a service provider and/or device manufacturer may contact the User in order to resolve issues related to an unscheduled event.

During an unscheduled event, the user, service, and device are vulnerable to unintentional or unauthorized uses of the device and service.

Examples of unscheduled events may include: system outage, risk event, or compliance violation that results from an unintentional or unauthorized change to these systems.

In order to reduce these vulnerabilities, the device must be able to support the following:

- Revocation
    - Updates
    - Removal
- Change management processes: real-time monitoring, automated assessment, software updates
- Video interface to Hopper/Genie needed during process
- Smartcard replacement may be a co-task with DSTAC renewability

USE CASE #13 - Cloud VOD Delivery

Pre-Condition: Subscriber has access to the same or similar VOD content that is available through the primary Home Gateway or STB that the MVPD provides to the home subscriber.

USE CASE DESCRIPTION

This Use Case reviews the elements related to delivering content from a remote access, or cloud source to a supported device. This is described in WG2 Report Part VI.

To support this use case a device should provide one or more of the following:

1. An App platform that provides support for multiple App developers including video distributors, examples include: iOS, Android, Android TV, Tizen, WebOS, Yahoo Widgets, Xbox, and PlayStation. The robustness of the App platform may affect what content is available to devices that are supported by the the App platform.
2. An HTML5 based platform that supports Media Source Extensions (MSE) and Encrypted Media Extensions (EME) with one or more Content Decryption Modules (CDM). As with the App platform, the robustness of the implementation may affect what content is available to devices that support HTML5 MSE/EME.
3. A DLNA VidiPath compliant client that can connect to an MVPD VidiPath server.

SERVICE DESCRIPTION

A Cloud VOD library typically also includes expanded VOD, such as look back content or episodic content from previous weeks of a programmatic series. There may be different servers handling the home VOD compared to the Cloud VOD media assets, thus not all content in the Cloud is offered at home and vice versa.

Most implementations of Cloud VOD from MVPDs are growing to be a superset of the home use case for VOD. Divisions of titles tend to be categorized in areas such as:

- Free
- Genre-based
- Network specific
- Premium Subscription
- Event-driven titles.

As Pay TV operators deploy HTML5 based UI's, the MVPD subscriber can leverage a consistent UI across the TV, mobile device, or PC. Content is typically accessed over the Internet using a Browser or Web application. Platform dependent applications for iOS or Android are also being developed to provide this TV Everywhere experience.

See IP VOD, already cloud based

USE CASE #14 - Cloud Live Streaming

Pre-Condition: Subscriber has access to the same Live or Linear broadcast TV content that is available to the primary Home Gateway or STB that the MVPD provides to the home subscriber.

USE CASE DESCRIPTION

This Use Case reviews the elements related to streaming the delivered content from a remote access, or cloud source to a supported device.

To support this use case a device should provide one or more of the following:

1. An App platform that provides support for multiple App developers including video distributors, examples include: iOS, Android, Android TV, Tizen, WebOS, Yahoo Widgets, Xbox, and PlayStation. The robustness of the App platform may affect what content is available to devices that are supported by the the App platform.
2. An HTML5 based platform that supports Media Source Extensions (MSE) and Encrypted Media Extensions (EME) with one or more Content Decryption Modules (CDM). As with the App platform, the robustness of the implementation may affect what content is available to devices that support HTML5 MSE/EME.
3. A DLNA VidiPath compliant client that can connect to an MVPD VidiPath server.

Examples include:

- Would be proxied by Hopper and show up in guide data.

SERVICE DESCRIPTION

Live or linear content is delivered at the time that the originally schedule content is delivered to the subscriber's home video gateway or STB. Access to these TV video streams tends to be sought from mobile devices for the purpose of providing a TV Everywhere experience.

MVPDs offer applications that directly stream content from the Cloud using broadband access for home devices such as gaming consoles, Smart TVs, and Tablets. The home user can avoid having to connect to a STB with a wired HDMI cable. As MVPDs move to upgrade their network to a full IP distribution architecture, these directly attached networked devices can receive a complete lineup of linear and live TV content directly, without having to be tethered to a Gateway or STB.

USE CASE #15 – Cloud DVR Recording and Streaming

Pre-Condition: Subscriber has access to recorded content that is available from a Remote Storage DVR service offered by the Pay TV provider, or access to a copy of the DVR content located on a home DVR or Gateway device that is remotely stored in the Cloud.

USE CASE DESCRIPTION

This Use Case reviews the elements related to recording the delivered (via streaming) content from a remote access, or cloud, source to a supported device.

To support this use case a device should provide one or more of the following:

1. An App platform that provides support for multiple App developers including video distributors, examples include: iOS, Android, Android TV, Tizen, WebOS, Yahoo Widgets, Xbox, and PlayStation. The robustness of the App platform may affect what content is available to devices that are supported by the the App platform.
2. An HTML5 based platform that supports Media Source Extensions (MSE) and Encrypted Media Extensions (EME) with one or more Content Decryption Modules (CDM). As with the App platform, the robustness of the implementation may affect what content is available to devices that support HTML5 MSE/EME.
3. A DLNA VidiPath compliant client that can connect to an MVPD VidiPath server.

SERVICE DESCRIPTION

Live or Linear broadcast TV content can typically be recorded simultaneously on both a local DVR and on a remote server for access by a mobile device outside of the home. Control of the scheduling for recordings can be done though a Web browser application running on a networked enabled device with Internet access or using a Pay TV developed application, such as those downloaded for Android or iOS devices. Remote control of the home DVR or remote control of the Cloud DVR is available through these device MVPD applications. APIs may be provided by the MVPD for a retail device to use a third party guide to control DVR content recording.

USE CASE #16 - Cloud Content Downloading for Mobile Devices

Pre-Condition: Use Case #15 has been met

USE CASE DESCRIPTION

This Use Case reviews the elements related to managing download content that has been delivered from a remote access, or cloud, source to a supported device.

To support this use case a device must:

- Be an authorized device
- Maintain (i.e. no deliberately remove) content protection technologies that are inherent to the downloaded content, such as Digital Rights Management or watermarks).
- If the downloaded content is marked with an expiration date, then the device must make every reasonable effort to forbid playback of content once the expiration date has been reached.
- If the authorized device has a domain restriction imposed upon it, then the device must abide by that requirement.
    - Such a requirement is use to ensure that the device is tied to the subscriber's home network; protecting entitlements.

Provide one or more of the following:

1. An App platform that provides support for multiple App developers including video distributors, examples include: iOS, Android, Android TV, Tizen, WebOS, Yahoo Widgets, Xbox, and PlayStation. The robustness of the App platform may affect what content is available to devices that are supported by the the App platform.
2. An HTML5 based platform that supports Media Source Extensions (MSE) and Encrypted Media Extensions (EME) with one or more Content Decryption Modules (CDM). As with the App platform, the robustness of the implementation may affect what content is available to devices that support HTML5 MSE/EME.
3. A DLNA VidiPath compliant client that can connect to an MVPD VidiPath server.

The availability of download varies among content subscription services; rights are often content or programmer specific. Typically, the expiration date indicates how long the downloaded program is available for playback.

Examples include:

- Proxied by Hopper.

SERVICE DESCRIPTION

When available, a User has the ability to copy or move content from the Cloud for temporary storage and manage content playback on a mobile device. Examples of this content may be VOD content or copies of Live/Linear content stored in a Cloud DVR service. One reason that content is available for download is to allow for offline viewing of subscription content. A device is considered "offline" when it does not connect to a broadband network, wireless LTE service area or Wi-Fi access point.

Each service varies in how the downloaded content is managed. Examples of management methods are:

- Some require the device connect to a network after a certain number of days, in order to renew rights and confirm expiration dates
- , other services do not require such check ins.
- When required, such as through rights limitations, one title is allowed to be checked out or downloaded at a time per subscriber.

Part I: Section VIII. Salient Differences to implementation of non-security elements

EXPECTATIONS: SECTION VIII

This is a summary section. Analysis and conclusions will go here.

Part II: Systems that Enable Competitive Availability of Devices

Identify systems comprising minimum standards, protocols, and information other than security elements to enable competitive availability of devices that receive MVPD services.

Note: Part II will be covered in the face to face session

EXPECTATIONS: All Sections

As most members understand the functionality of the devices listed in Part I, it is expected that information would be provided as to how the devices DISCOVER and TUNE CONTENT.

Part II: Section I. Protocols and messages that enable competitive devices

Metadata, authorization, key management are included protocols and features

WG3??? TBD for discussion on July 7th, possibly independent of Wg3 report

Part II: Section II. SAT-IP

Description

SAT-IP is a remote tuner control protocol that provides a standardized way for IP clients to access live media broadcasts from satellite reception servers on IP networks. It separates distribution-specific elements such as tuners, dish LNBs, etc into a single device that then provides video services to over IP to client devices on the home network using common protocols. The client devices and protocols are agnostic to the physical layer differences between satellite service providers. Satellite services can be forwarded over all types of IP wired or wireless technologies to a range of IP client devices.

The protocol envisions a number of different possibilities for the server where it could be built-in to different devices such as consumer or commercial versions of LNBs, IP Multiswitches, or set-top boxes.

Protocols

The SAT-IP home network protocols are based on IP, RSTP, UPnP and HTTP. It was made to be integrated into DLNA as an option.

SAT>IP servers identify themselves on the IP network using standard UPnP mechanisms (SSDP). Stream Control in SAT>IP is done via RTSP or HTTP. SAT>IP clients request access to satellites, transponders and MPEG PID streams as needed. RTSP queries are used for requesting RTP unicast or multicast streams. HTTP queries are used for requesting HTTP streams.

In summary, the client can provide low level tuning functions with the reception servers using this protocol to translate to whatever specific technologies are used by the service provider.

Security

The solution current assumes either “Free-to-Air” unscrambled or a pass-through scenario that assumes that any CA or DRM descrambling will be done by the client. Because the protocols can be used under DLNA, DTCP-IP encryption could be applied to scrambled services. As a specification for use in Europe, there is an assumption that DVB Common Interface + (CI+) would be used.

Information

The following links provide useful information:

http://www.satip.info/

http://en.wikipedia.org/wiki/Sat-IP

Part II: Section IV. DVB CI+ - july 7 discussion about how to include necessary information

A. Standards

B. Protocols

C. Information

1. Regulatory environment – mandate on TVs

D. Applicable Devices

Part II: Section III. CableCARD

Description

The CableLabs CableCARD specification defines a one way interface used to decrypt and view one-way linear digital cable television in the United States. CableCARD only functions on Hybrid Fiber-Coax (HFC) based networks and does not function on DBS or IPTV systems. CableCARD uses a physical PCMCIA PC Card type II form factor device for all conditional access and provides copy protection of content across the PCMCIA interface. A CableCARD is able to decrypt up to six simultaneous programs from a service provider. A CableCARD set top box is comprised of the set top box, purchased at retail or rented from operator, as well as the CableCARD itself which must be provided by an operator, generally for a monthly fee.

At the core a set top box obtains a channel lineup from the CableCARD and then may request entitlement to decrypt and display a particular program in the lineup. The CableCARD emits Copyright Control Information (CCI) which the set top box Host is required to abide by, in cases such as recording. Premium content requires a one-to-one pairing of CableCARD to Host to protect against unauthorized viewing. Host binding requires an end user to contact

their service provider with unique information from both the Host device and the CableCARD, thus ensuring that all Hosts are licensed and certified devices.

CableCARDS provide a few other mechanisms besides merely decrypting signals. The CableCARD terminates and decodes the forward out-of-band channel which carries service information data such as channel lineups (SCTE 65 Profiles 1 through 3), optionally guide data (SCTE 65 Profiles 4 through 6), EMMs, software downloads, EAS messages, and other control data, and proprietary service data. In practice, only SCTE 65 Profiles 1 through 3 are used and retail UDCPs obtain guide data through third-parties other than the cable system. (reference to MOU required)

The CableCARD provides an application information interface, which can be used to obtain information about the CableCARD itself, including Host binding status, card manufacturer, card modes, packets/tables received, et cetera. CableCARDs also provide a Man Machine Interface (MMI) that provides a way to present messages on the display using HTML pages with URL's that are passed back to the CableCARD to request further data from the MMI. The CableCARD specification defines a baseline HTML profile that constrains the functionality required of the Host for the MMI. The Baseline HTML Profile only supports formatted text messages, in the form of HTML pages, with one hyperlink. In practice the MMI is only used for the Card/Host binding and diagnostic purposes.

Originally, CableCARD devices were either an integrated digital television with a CableCARD slot or a set top box with video outputs only. A subsequent OpenCable Unidirectional Receiver (OCUR) specification was developed to enable an interface to Microsoft

Windows Media Center PCs. The OCUR Digital Receiver Interface is discussed in another section of this document. The CableCARD ecosystem provides set top box implementors the ability to add features consistent with the DFAST license, such as enforcement of content protection.

Standards

Standards in use by CableCARD include:

- SCTE 28 – Host POD interface describes low level CableCARD interaction, like the Man Machine Interface (MMI), entitlement requests, application information, and other conditional access related operations.
- SCTE 41 – Copy protection standards, includes key and certificate exchanges, device authorization, content protection, Host binding, and algorithms in use.
- SCTE 65 – service information delivered out of band, such as channel lineups (Profiles 1 through 3) and basic guide data (Profiles 4 through 6).
- EIA-608/EIA-708/SCTE 21 – Embedded user data, such as CGMS-A content rights descriptor and captions.
- Joint Test Suite.

Information

http://www.cablelabs.com

http://en.wikipedia.org/wiki/CableCARD

OpenCable CableCARD Interface 2.0 Specification, OC-SP-CCIF2.0, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-CCIF2.0-I27-150330.pdf, Cable Television Laboratories, Inc.

OpenCable CableCARD Copy Protection 2.0 Specification, OC-SP-CCCP2.0, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-CCCP2.0-I13-130418.pdf, Cable Television Laboratories, Inc.

OpenCable Security Specification, OC-SP-SEC, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-SEC-I08-110512.pdf, Cable Television Laboratories, Inc.

Uni-Directional Cable Product Supporting M-Card: Multiple Profiles, Conformance Checklist: PICS, M-UDCP-PICS-I04-080225, http://www.cablelabs.com/wp-content/uploads/specdocs/DVC-RQ-M-UDCP-PICS-I04-080225.pdf, Cable Television Laboratories, Inc.

Applicable Devices

- Most MVPD supplied cable boxes, excluding DTA's, until 12/2015.
- TiVO's
- Hauppauge/SiliconDust/Ceton network CableCARD tuners (OCURs)
- Ceton internal CableCARD PCI card

Description

An OpenCable Unidirectional Receiver (OCUR) is designed to be interoperable across all CableCARD cable systems in the United States. The OCUR does not interoperate with DBS or IPTV MVPD systems. The OCUR is designed specifically to work with a Windows-based PC with PlayReady DRM. The PC may separately support OTT interactive applications, real time services, and other on demand services. OCUR devices are unidirectional CableCARD devices, but an OCUR is defined as having IP outputs only with DRM protection; physical video outputs are not allowed in this device model. The OCUR may optionally have a USB interface host interface for connection of a Tuning Resolver. OCUR IP outputs are specified by the Digital Receiver Interface (DRI). Various approved DRM systems are permitted to protect premium content across the network; Microsoft PlayReady is the only currently approved full DRM for the OCUR, while DTCP-IP is approved for link level security.

All client-server interaction leverages open standards and protocols, and adds additional DRI-specificed requirements, including a unique content protection layer (“DRI Security”) that must be supported in all DRMs. Signal source and other CableCARD details are mostly hidden from the receiving client, who only receives protected content streams and various ancillary information externally.

Protocols

OCUR devices advertise themselves on the network using UPNP SSDP announcements. OCUR devices offer two interfaces to obtain content using UPnP and DLNA protocols. An OCUR device supports the DRI Tuner UPnP protocol, and optionally the DLNA Digital Media Server (DMS) function.

A Tuner object is available for each physical tuner the OCUR has. This DRI Tuner exports a variety of operations and queries which closely resembles interacting with a physical tuner, this inferface allows direct manipulation in cases of clear QAM. The interface also offers high level operations a user might expect such as tuning to a linear digital cable channel. All data through this interface is transmitted via UDP unicast streams using RTP.

An OCUR might also export a DLNA digital media server (DMS) content directory service (CDS). This CDS allows for HTTP requests of streams and completely abstracts all details away from the tuner. The CDS approach allows clients without an approved DRM access only to programs with Copy Control Information (CCI) identifying them as Copy Freely, expanding the number of supported clients that can access Copy Freely content to any device that supports DLNA.

Security

OCUR devices use IP for all outputs. OCUR devices can use either PlayReady or DTCP-IP for RTP transmissions when using the DRI Tuner UPnP object model. OCUR devices encrypt all content that is

not Copy Freely, so the client is responsible for decrypting secure content. Programs accessed over DLNA, which are not marked Copy Freely, are secured using DTCP-IP. Any device which is licensed to use Windows/PlayReady or is DLNA/DTCP compliant can interact and get content from an OCUR device.

Certain additional license requirements applied to both OCUR manufacturers, DRMs and Windows Media Center OEMs, including adherence to the CHILA Compliance and Robustness Rules, warranties, and indemnities from Windows Media Center OEMs. DRM provider requirements include conformance to CHILA Compliance and Robustness Rules, approved outputs process, population of an Association Database of paired CableCARD-OCURs, QoS, carriage of System Renewability Messages (SRM), Breach Management, Revocation and Renewability, reasonable and non-discriminatory license terms, warranties and indemnity. When WMDRM was replaced with a self-contained Playready system, some of these requirements were relaxed.

Information

http://www.opencable.com

http://en.wikipedia.org/wiki/OpenCable

OpenCable CableCARD Interface 2.0 Specification, OC-SP-CCIF2.0, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-CCIF2.0-I27-150330.pdf, Cable Television Laboratories, Inc.

OpenCable CableCARD Copy Protection 2.0 Specification, OC-SP-CCCP2.0, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-CCCP2.0-I13-130418.pdf, Cable Television Laboratories, Inc.

OpenCable Unidirectional Receiver, OC-SP-OCCUR, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-OCUR-I11-130607.pdf, , Cable Television Laboratories, Inc.

OpenCable Digital Receiver Interface Protocol, OC-SP-DRI, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-DRI-I04-100910.pdf, Cable Television Laboratories, Inc.

OpenCable Security Specification, OC-SP-SEC, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-SEC-I08-110512.pdf, Cable Television Laboratories, Inc.

Applicable Devices

- Hauppauge WinTV network CableCARD tuners
- SiliconDust HDHomeRun network CableCARD tuners
- Ceton Windows Media Center Extenders

Part II: Section V. Android/iOS store device architectures from DEVELOPER point of View

Text from f2f coming

Part II: Section VII. VidiPath

Description

VidiPath is a home networking technology being promoted and certified by the DLNA organization. It assumes a home gateway which tunes, receives and descrambles premium content from service providers and outputs it to client devices over DTCP-IP in the home.

VidiPath service operator services can be forwarded to all types of devices attached to the home network over wired or wireless technologies. With DLNA VidiPath certification and a "CVP-2" status bit in the DTCP certificate, service providers are guaranteed pixel accurate rendition of their user interface on devices and with a good level of quality of service.

Protocols

VidiPath protocols consist of a number of DLNA guidelines which are implemented. Along with "basic" DLNA based on 2015 guidelines with improved trick play and response times, devices must conform to HTML5, Low Power, Diagnostics, and Authentication guidelines.

VidiPath servers identify themselves on the IP network using standard UPnP mechanisms (SSDP). Stream Control is done HTTP. Using the service operator's remote user interface which can be discovered, VidiPath clients request access to content as needed. HTTP queries are used for requesting HTTP streams.

Security

Conditional Access or DRM decryption (as well as RF tuning) is managed by the gateway device and out-of-scope for VidiPath.

Information

See the DLNA website for an overview of VidiPath:

Webinar/Videos: www.dlna.org/dlna-for-industry/newsroom/cvp2-webinar-series

Guidelines: www.dlna.org/dlna-for-industry/guidelines

Part II: Section VIII. HTML5 as a system

Investigation of HTML5 as a system in browser, dedicated application, or device

Text from f2f coming

Part II: Section IX. RVU

Description

RVU as illustrated in Figure 6 of Part 1 enables a simple solution for a Whole Home DVR using a single server and standard Consumer Electronics client devices. A DVR experience is offered at each client, including user interactions such as guide, DVR trick play, interactive applications and

VoD content. RVU can be implemented on a variety of CE devices from basic thin clients to Smart TVs and gaming platforms. RVU increases the CE device value by providing DVR functionality and access to subscriber based content on each client CE device. Low cost client devices with small memory footprints and low CPU performance are supported while enabling advanced 4K UHD video formats.

Standards

RVU is built on UPnP device discovery/control, DLNA media streaming, and DTCP-IP content protection.

Protocols

The RVU Remote User Interface (RUI) protocol sends commands and responses as XML strings on command channels, remote user interface vector and bitmap graphics are carried in TCP data frames, while A/V streams are passed via DLNA media streaming under DTCP-IP protection. Non-RVU protocols such as DIRECTV's SHEF can be used to directly command RVU servers (e.g. DIRECTV Genie servers) which in turn enables creation of a higher level non-RVU interface with deep links into service provider server originated content.

Information

The RVU Alliance maintains the RVU protocol specifications as developed by leading technology companies (http://rvualliance.org/specification-availability). RVU technology is field proven and integrated in millions of devices in the field today (http://rvualliance.org/products). The RVU Alliance further maintains a test & certification program to ensure device interoperability and compliance (http://rvualliance.org/certification).

Part II: Section X. Passage

Description

Passage is a technology that enables security interoperability similar to Simultcrypt. It is suitable for broadcast linear streams where a service provider supports simultaneous distribution to receivers with legacy Conditional Access (CA) and new security such as Digital Rights Management (DRM).

While the in-stream signaling for Simulcrypt and Passage are similar and the results are the same - allowing receivers with different security systems to receive the same transport stream - it is accomplished through different means.

Simulcrypt accomplishes interoperability through key sharing. The scramble key content is delivered separately through proprietary means to receivers with different security systems. The content is 100% encrypted and both systems share low-level descrambling capability.

However, key sharing may not always be possible or desirable. Legacy scrambling uses out-of-date algorithms such as DVB Common Scrambling Algorithm (CSA), DES or DES-CBC. Often the security extends into the descrambling by keeping certain information secret, e.g. Initialization Vectors for DES-CBC, to create a type of anti-cloning mechanism. Another anti-hacking feature of some legacy systems is very rapid key changes which makes sharing with other security systems problematic.

Passage accomplishes interoperability through selective multiple encryption. A small amount of critical content data, less than 2% of the bandwidth, essential for decompressing the rest of the content (sent in-the-clear), is duplicated and scrambled two ways – one for legacy CA and one for DRM. Each receiver gets the same transport stream, selects its respective scrambled content, and share the remaining clear common content.

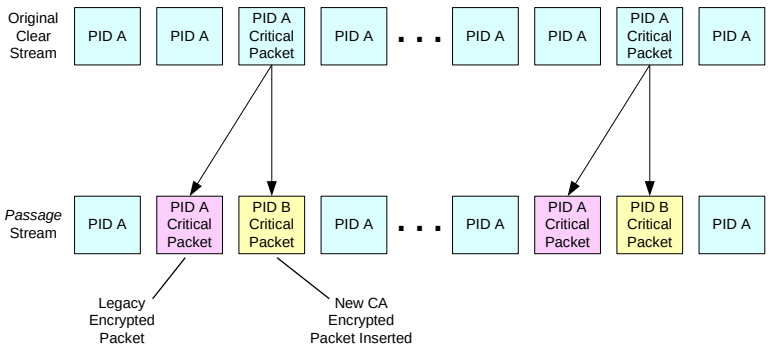


Figure 1 - Creation of Passage Selective Multiple Encrypted Stream

Unlike Simulcrypt, since Passage allows for the independent scrambling of critical packets of content, there are the following benefits:

- The security of the large base of legacy receivers in the field is not put at risk.
    - Divulging and licensing of the legacy descrambling know-how, e.g. Initialization Vectors, are not required. This lowers the risk of legacy clone hardware being available.
    - Knowledge of a scrambling key leaked from the alternate security system cannot be used to reverse engineer and attack the legacy security system.
    - There is no need to "slow" key changes on the legacy system or share a higher level of the legacy key derivation protocol thereby reducing overall resilience to a hack in order to be compatible with the alternate security.
- Since no secrets need to be shared between security systems, there should be no legacy CA provider security indemnity concern for the service operator.
    - Breaches should be readily identifiable as to which keys and which scrambled packets are being hacked.
- The alternate packet may be scrambled using efficient implementations of the AES-128 algorithm which may more readily supported by DRMs and mobile device platforms.
- As with Apple HTTP Live Streaming, Passage's use of selective encryption may make software-only implementations possible for new classes of devices.

- Legacy CA can be bypassed in new devices. Content rights need not be limited to the Copy Control Information (CCI) bits. Content rights associated with the DRM encrypted alternate packets can maintain persistent control over content – enabling new use cases.

Implementations

Passage is proven technology. There have been a number of field and lab trials as well as deployments with the Cisco CA Overlay system.

The best way to deploy Passage seems to be the point of commercial distribution. That way a stream would be processed in one place, and then distributed throughout the US. There are 4 or 5 different headend configurations and they all can be accommodated by reconfiguring their existing equipment. Non-participating headends won't need to opt-out - they don't need to do anything. Participating headends will only require reconfiguration of existing equipment – stream groomers and multiplexers - with normal functions such PID filtering, PID remapping, and descrambling and re-scrambling.

Protocols

Passage utilizes the DVB Simulcrypt standard to standardize interfaces at the broadcast center as well as the signaling the security system in in-band stream. Additional messaging is required to signal the alternate video and audio packets in a program. This is described in the Passage Set-top Box Specification, available from Sony Electronics.

Security

While not a security system in and of itself, Passage use of selective encryption is approved by Merdan Associates and Sarnoff Laboratories. Reports are available under NDA from Sony Electronics.

Part III: Alternative Systems that Enable New Categories of Navigation Devices

Identify alternative systems as appropriate to promote the availability of different categories of navigation devices.

Part III: Section I. CE Device Competitive Navigation Alternative Systems:

Scott: When MVPD does not control interface, what needs to be defined so that the retail device has the information to implement a function

Part II protocols can be referenced

If you believe that a competitive device should do a function (e.g. local ad insertion), give us a way to do it.

What are interfaces and protocols needed for that functionality?

DCAS duties

Provide access to content

Service discovery

Easy for MVPD to provision

Protocol/webservice for listing all video service available to the subscriber and device

Provide service data to obtain content/asset/tuning informational

Tuning tables

PPV and VOD

Access is mandatory

Exported asset lists

Direct url's supported in RUI's
Decoding client negotiates DRM upon access

Defined CAS client APIs

requesting a stream for decrypting, request an asset for viewing, etcetera

Transcrypting content

MSO CA/DRM is widely differing

DCAS should terminate network CA/DRM and translate into interoperable format similar to DFAST currently

DFAST is proof this works across varying CA systems

Legacy systems do not require replacement in field, the DCAS transcrypting operation handles this

Applies to newly deployed devices

AT&T concern

If hardware available, CE device tunes and DCAS transcrypts to suitable output format

External tuning hardware may be required

DBS due to tuning complexities

ATT due to proprietary network and tuning methods

Others possibly due to architectural complexities

PPV and VOD

Access is required

Support Third Party Competitive User Interfaces

Separation of network CAS/DRM and UI application

Cannot be restricted

The key to 3rd party market differentiation and diversity

Competitive devices are key to DSTAC

Vidipath / CVP2

Doesn't support competitive user interface for access to premium content, can only, be done through the operator's HTML5
For example no DLNA content directory

Requires guarantees that the 'service provider bit' in DTCP cert will be informational only and not affect interoperation

Clients cannot record (quote from WG2 f2f)

No exported asset lists for side by side operation with MSO VidiPath server

RVU

SHEF requires externally licensing tribune data

Not clear if SHEF supports a competitive navigation UI

Exports asset list

Side by side RUI operation appears possible to a degree

Doesn't support recording by client device

User Experience Information/Metadata

Accurate and reliable

Content lists

Required to display all available content to end user

Guide data

Basic guide should be mandatory

Title and episode number
Enhanced guide data allows for market differentiation

Current methodologies

SCTE65 profile binary tables
CEA-2033 (?) xml data

Captions

Embedded in stream
Attached in container

Parental control

3rd party control and implementation

Blackouts

Provisioning data pushed to DCAS module

DCAS knows entitlement rights for blackouts

If not handled in the operator network, then DCAS responsibility

A 3rd party would require robust metadata and signaling to support this on device

'Instant channel change'

Proprietary feature, abstracted by the operator in their network or network terminating device, or 3rd party should be left to implementation at will

Public API must be made available and standardized

Usage limitations

DCAS internal operation, should not be left to 3rd party

If usage is over limits DCAS should respond with failure to entitlement request

Ad insertion/splicing

Not a 3rd parties business
Not done on cableCARD devices today

Should be a headend duty responsible by MSO
DCAS can manipulate streams internally how it pleases

Segmented content containing

Mosaic channels

APIs provided for 3rd party implementation allowing for market differentiation

'apps'

3rd party's decision if apps are desired to be supported

Anything from an MSO should be implemented in a generic interface to interoperate with competitive 3rd party user interfaces

MMI provides such a generic HTML interface to allow for 'app' widgets

audience measurement

Privacy concerns abound

Not responsibility of 3rd party to report metrics upstream

Not done currently with 3rd party cableCARD devices now

Playback

Trick modes must be allowed

Understand some exceptions in cases of PPV

Time skipping allowed

Recording

Should be allowed

Where content rights information permits

Hard drives should not be a requirement

Local and network DVR's must be supported

Recordings exportable to secure clients

Timeshifting

Timeshift/pause buffers should be allowed

Copyright Control Information – CCI

Embedded CGMS-A

Should be evented from DCAS

Support Messaging

Man machine interface (MMI)

Allow for status/information pages

Allow for HTML widgets to facilitate MSO applications

Display must be optional based on user input

Allows for single API to interact with the DCAS

DCAS can communicate upstream privately and respond

Suitable for all communication with head end

Billing
Upselling
Notifications
Must be more robust than current cableCARD MMI

EAS

Should be evented through MMI

Codecs

Baselines might be necessary

SD: MPEG2 + AC3

HD: SD + H264 + AAC

UHD: HD + HEVC + …

Use minimal amount of mainstream codecs and containers for least licensing issues

Home Network Delivery protocols

Secure local network outputs required

UPNP announcement of service for local clients

DLNA interfaces for operation by authorized clients

WAN streaming of permitted content

Supports Approved Digital Outputs post consumer device

DTCP-IP

Link protection

Ensures in house playback

Others as approved

Copy Free data should be viewable on clients without supported DRM's

Same as currently possible in cableCARD

Part III: Section II. MVPD User-Interface Controlled Alternative Systems:

F2F from Amazon

Part III: Section II. MVPD User-Interface Controlled Alternative Systems

SYSTEM 1: APPLICATION-BASED SERVICE WITH MVPD UI

Diversity, innovation, and choice are the hallmarks of today's device marketplace. As the Commission has recognized, consumers are able to access protected video content on a wide and growing array of devices, from smartphones, tablets, and other mobile devices, to smart TVs and PCs, to MVPD-supplied and retail set-top boxes. Retail devices and platforms vary in their capabilities, so there is no uniform technology for securing video across the device ecosystem. Furthermore, technologies for accessing video services are continually and rapidly changing due to underlying technology changes, delivery of new innovative services and competition from other MVPDs and OTTs. Technology trends over the past several years show how video providers (both MVPD and OTT) are adapting to these market and technical realities.

Applications (apps) are the most successful and widespread method for delivering service to retail devices and platforms today. In this regard, MVPD apps follow the same approach as the "apps" that Netflix, Amazon, and other OTT providers use for delivering service on retail devices and platforms. MVPD and OTT providers are implementing platform-specific native apps for all of the major mobile platforms, and are now turning to more portable approaches (e.g. HTML5 apps) to reach additional retail devices. In addition, MVPDs and retail device manufacturers have collaboratively developed standards for interoperability among MVPD and retail devices through the Digital Living Network Alliance (DLNA).

In summary, the app-based approaches currently being deployed by MVPDs to reach retail devices are:

- Device/Platform Specific Apps
- W3C HTML5 Web Browser
- DLNA VidiPath™
- RVU
- DISH Virtual Joey
- Slingbox Clients

The MVPD or OTT video provider can use a common cloud-based and/or LAN-based network infrastructure to deliver content in an optimal fashion to the broad diversity of retail devices and platforms using one or more of these app-based approaches. Device/Platform Specific Apps can take advantage of the latest features in the latest devices and tailor the user experience to the specific device, e.g. multi-touch, accelerometers, finger print identification, and speech

recognition. Web Apps executing on a standard HTML5 browser can reach a broad set of devices with a rich set of application features. DLNA VidiPath leverages the W3C HTML5 Web app model, but integrates with other devices on the home network offering a rich home user experience.

Collectively, the app model is the means for bridging the differences between varied and rapidly changing services and varied and rapidly changing consumer electronics platforms. These application approaches abstract the diversity and complexity of service providers' access network technologies and customer-owned IP devices and accommodate rapid change and innovation by both service providers and consumer electronics manufacturers. These application approaches may also make use of a combination of software-downloadable security and a hardware root of trust. This diversity and flexibility enables the broadest coverage of retail devices, optimizes the consumer experience on the latest devices and technologies, and takes advantage of a wide range of market-tested security measures including downloadable DRMs.

Table 5 shows how the major MVPDs currently support retail devices using this three-pronged approach. All of the major MVPDs support an iOS and Android App to access their service on smart phones and tablets. All of the major MVPDs support their service on Microsoft Windows and Apple Mac OS X either through an application or a Web app (using a plug-in model for content protection today and transitioning to an HTML5 EME Web App in the future). Some of the major MVPDs support Smart TVs (LG, Samsung, Sony, Toshiba), game consoles (PlayStation 3 & 4, Xbox 360 & One), and media adaptors (Roku). VidiPath Certification was launched in September 2014. Many of the major MVPDs either support DLNA VidiPath today or plan to in the near future. DLNA RVU, developed and maintained by the RVU Alliance, is supported by DirecTV. Certified VidiPath client devices are expected in the market later in 2015. Table 1 lists some of the currently supported devices, which continue to grow.

MVPD	Subs (M)[1]	Mobile Apps[2]	PC (Windows/Mac OS X)[3]
Comcast	22.6	✔	Web app
DirecTV	20.3	✔	Web app
DISH	14.1	✔	Native app (DishWorld)
TWC	11.4	✔	Web app
AT&T U-verse	5.7	✔	Web app
Verizon	5.3	✔	Web app
Charter	4.4	✔	Web app
Cox	4.3	✔	Native app (Cox TV Connect)
Cablevision	2.7	✔	Native app (Optimum)

Table 5 - MVPD Support For Mobile Devices & PCs

[1] SNL Kagan
[2] Android & iOS based smart phones & tablets
[3] Either as a browser plug-in or as a Windows & Mac OS X application (in the future HTML5 EME/MSE will deprecate browser plug-ins)

The following sections discuss each of the three solutions being deployed by MVPDs and OTT video providers today.

I. Device/Platform Specific Apps

A. Standards

By definition native apps are written specifically for a particular platform, e.g. iOS, Android, Tizen, Xbox, Playstation, etc. While these platforms and devices make use of many different standards, summarized below, the specific user interfaces, device features and

platform APIs enable differentiation and competition among them. This competitive marketplace for devices and platforms has resulted in an explosion of smart phones, tablets and more recently smart watches, with a large array of features and capabilities. Smart TVs are also offering application platforms that enable access to new service offerings, including applications such as Netflix, YouTube, and Amazon Prime Video, as well as some MVPD apps.

In general, these platforms offer some form of app marketplace (e.g. Apple's App Store or Google's Google Play App Store), where MVPD app developers can offer their apps and consumers can download them to their devices.

In order to support their App marketplace these platforms have developed various security capabilities to insure that the content and applications are protected appropriately.

MVPDs have focused their app development efforts thus far on those devices and platforms that enjoy the greatest consumer use and marketplace success. **Error! Reference source not found.** ranks particular devices/platforms by the number of units sold in the United States. As can be seen by this table, MVPDs broadly support device/platform specific apps on the most popular devices/platforms. MVPDs are also devising other ways to expand the range of devices and platforms that can support MVPD apps, such as via an HTML5 web browser, VidiPath, or RVU. Some observations that can be drawn from these and other marketplace facts:

- The total number of retail devices in the US that can be served by an MVPD app is over: **450 million devices**
- The percentage of these retail devices that can be served by one or more MVPD apps is: **96%**
- The percentage of these retail devices that can be served by an app from all of the top 10 MVPDs is: **67%**
- The average number of MVPD set-tops per subscriber is **2.4**
- The average number of these retail devices per US household is **4,** well exceeding the **2.4** MVPD set-tops per subscriber

Other devices can be supported by either an HTML5 web browser, VidiPath, or RVU.

Retail Device	United States Units	MVPD Apps
Android phones[1]	92,036,000	All top 10 MVPDs[7]
PCs & Macs w/Broadband[2]	85,358,000	All top 10 MVPDs
iOS phones[1]	71,449,000	All top 10 MVPDs
Xbox 360[3]	48,460,000	5 of the top 10 MVPDs

Android Tablets[4]	43,260,000	All top ten MVPDs
PlayStation 3[3]	29,160,000	2 of the top 10 MVPDs
iOS Tablets[4]	23,730,000	All top 10 MVPDs
Samsung TV[5]	14,740,800	4 of the top 10 MVPDs
Vizio TV[5]	12,151,200	0
Apple TV[6]	8,800,000	N/A
Sony TV[5]	8,764,800	1 of the top 10 MVPDs
PlayStation 4[3]	8,650,000	2 of the top 10 MVPDs
Xbox One[3]	7,790,000	2 of the top 10 MVPDs
LG TV[5]	6,500,000	2 of the top 10 MVPDs
Roku[6]	5,000,000	1 of the top 10 MVPDs
Chromecast[6]	4,000,000	1 of the top 10 MVPDs
Total Number of Retail Devices	469,849,800	

Table 6 – US Retail Device Numbers

[1] comScore Reports January 2015 U.S. Smartphone Subscriber Market Share, March 4, 2015 - http://www.comscore.com/Insights/Market-Rankings/comScore-Reports-January-2015-US-Smartphone-Subscriber-Market-Share

[2] Computer and Internet Use in the United States: 2013 *American Community Survey Reports,* U.S. Department of Commerce Economics and Statistics Administration U.S. CENSUS BUREAU, November 2014 - http://www.census.gov/history/pdf/2013computeruse.pdf

[3] Platform Totals, VGChartz Limited, http://www.vgchartz.com/analysis/platform_totals/ (accessed: 6/18/15)

[4] THE STATE OF THE TABLET MARKET - http://tabtimes.com/resources/the-state-of-the-tablet-market/ (accessed: 6/18/15)

[5] Majority of US Internet Users to Use a Connected TV by 2015, eMarketer, June 13, 2014 - http://www.emarketer.com/Article/Majority-of-US-Internet-Users-Use-Connected-TV-by-2015/1010908 and Samsung, Vizio Control US smart TV market, Broadband TV News, MARCH 10, 2014 - http://www.broadbandtvnews.com/2014/03/10/samsung-vizio-control-us-smart-tv-market/

[6] Streaming devices sales in the United States in 2014 (in million units), Statista Inc. - http://www.statista.com/statistics/296641/streaming-devices-sales-united-states/ (accessed: 6/18/15)

[7] Top 10 MVPDs – AT&T, Bright House, Cablevision, Charter, Comcast, Cox, DirecTV, DISH, Time Warner Cable, Verizon

B. Protocols

Some of the common standards that these platforms support include:

- IETF Internet Protocol Standards
- IEEE 802.11xx Standards
- 3GPP LTE Standards
- UPnP and DLNA Guidelines
- W3C Standards
- MPEG video and audio standards

C. Information

MVPDs and OTT providers have developed apps for the following devices and platforms, among others:

- Apple iOS
- Google Android
- Samsung Smart TV and Tizen
- LG WebOS
- Microsoft Xbox
- Sony PlayStation
- Roku

- Slingbox Client

The following sections discuss these platforms.

1. Apple iOS

Apple supports an app ecosystem for its mobile devices, smart phones, tablets, and smart watches based on its iOS platform.

Apple has an extensive developer program for Apple devices that is accessible under license (https://developer.apple.com/programs/). Apps can be submitted to the Apple iTunes Store for distribution to iOS devices.

The iTunes Store, originally the iTunes Music Store, is a software-based online digital media store operated by Apple Inc. It opened on April 28, 2003, and has been the largest music vendor in the United States since April 2008, and the largest music vendor in the world since February 2010.

iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware. It is the operating system that presently powers many of the company's mobile devices, including the iPhone, iPad, and iPod touch.

iOS was originally unveiled in 2007 for the iPhone and has been extended to support other Apple devices such as the iPod touch (September 2007), iPad (January 2010), iPad mini (November 2012) and second-generation Apple TV onward (September 2010).

The iTunes Store is accessible using a web browser, or using native applications on an iOS device. In order to complete a purchase, one is required to register an account with Apple. This is a secure process that every iOS customer needs to perform in order to be able to browse, download, install, and use any of applications published through the iTunes Store. In order to create an Apple ID, one would need to access the App Store and follow the steps that include entering contact information, email address, and billing information.

Once a user account is created, the customer can browse all available applications, video, and music, and make purchases. Applications are instantly available on the device.

Applications for the iTunes Store are developed, tested, and distributed using strict guidelines and tools that Apple provides to all developers. Apple regulates applications and their functionality by enforcing a testing process that occurs upon submission of an app to the iTunes Store. While there is no guaranteed maximum duration of this process, Apple tries to review all submitted

applications within a week. During this time, their testers evaluate the app against a strict set of requirements which ensures that the submitted applications perform as desired on selected platforms, do not violate any of Apple's terms and conditions, and do not provide an outlet for any illegal activity. The full set of the latest requirements can be found at: https://developer.apple.com/app-store/review/guidelines/

If an application fails any of the required guidelines, the developer is notified with an explanation and means of submitting another version that should fix the issues found. The explanation usually contains all reasons for failure. At the same time, Apple reserves the right to deny any application for a reason not specified in the guidelines. For example, if they find something that might violate their business model, but was not discovered before in any other app, and possibly not recorded in the guidelines, they would deny the request, and update the guidelines document. Over time, requirements have evolved as trends have appeared in application development. For example, applications accessing the user's location for advertising were valid prior to the fall of 2009. After this point, apps were rejected that did not provide more robust user experience beyond simply using location data for advertising. Other requirements, such as using undocumented APIs, have always led to rejection.

The first step in creating an application is to create a developer environment, which includes downloading, and installing specific software on specific hardware. Developers use special tools to develop, test, package, and sign their applications.

Special tools required for iOS development are:

- A Mac computer running OS X 10.9.4 or later (this is Apple's standard operating system)
- Xcode (latest version)
- iOS SDK (iOS Software Development Kit)

Xcode is Apple's integrated development environment (IDE). Xcode includes a source editor, a graphical user interface editor, and many other features. The iOS SDK extends Xcode to include the tools, compilers, and frameworks (software libraries, emulators, and command line utilities) you need specifically for iOS development. Xcode is distributed via Apple's Mac Store that is built in into Apple's Mac OS X operating system.

The second step in the process is to create a record on the iTunes store that will act as a placeholder for the application developed in the first step. In order to publish to the iTunes Store, developers need a paid iOS Developer account ($99/year). This applies to free or paid applications. Developers are also required to verify their identity, and in case of large organizations, only the Vice President level executives are allowed to create the account. Verification of their level is required.

Applications require a unique Application ID. This is used to uniquely identify them in the Store and associate the application developers build with the iTunes Store record of it.

A very important part of this step is a signing certificate that ensures security of the application. Developers first need to create a Distribution Certificate. This is a secure certificate stored on the developer's profile that confirms the developer identity and signs the code. This process is detailed on the *Distribution* tab of the Provisioning Portal (account created by developers in the first step).

After creating a Distribution Certificate, developers are required to create a Distribution Provisioning Profile. This profile limits the application to be executable only on specific devices. Three different profiles are permitted, to target a specific number of devices initially (used for development), devices belonging to the developer's organization (testing), or public devices (used for iTunes Store). Profiles are built into the application, which ensures that you are not submitting an application prematurely as the third level of this profile is required by the Store. During the process of archiving (creating a version that can be released to the Store), it is necessary to add the Distribution Profile to the application. Archiving is an automated process that is performed by Xcode, and the result is a file that can be uploaded to the Store.

The third step of making the application available in the Store is submitting it for internal Apple testing. iTunes Connect is the commercial side of the app store, which handles the actual sales of the finished app, which countries to sell in, description and screenshots etc. It's a relatively easy process and it's at this point that you'll decide whether to sell the app, give it away, enable iAds to be displayed, enter bank information, and sign any contracts needed for release.

Once a record of the application is created through iTunes Connect, Xcode will be able to upload the packaged application and associate it with that record through an automated process.

The App Review Guideline Document is a living document that Apple can change at any time. Essentially the guidelines are put in place to prevent problems with pornography, violence, legal issues, user experience, and other more specific app guidelines. Apple checks each app against these guidelines before approving it for sale and inclusion on the App Store.

Apple will promote apps that get featured in the App Store, typically within a specific app category.

As one of the integral parts of the iOS platform, Apple implemented capabilities for video and audio content streaming. In addition, Apple has implemented mechanisms for content rights management, as well as capabilities to bring third-party DRMs. iOS implements HTTP Live Streaming (HLS). The HLS architecture involves three main components:

- Server: Codifies and encapsulates the input video flow in a proper format for the delivery. Then, video is prepared for distribution by segmenting it into different files. In the process of intake, the video is coded and segmented to generate video fragments and index files. Service providers have a lot of range in developing these components, and often adjust location, capacity, and length of video files to account for changes in their own systems.
- Distributor: A standard Web Server accepts requests from clients and delivers all the resources needed for streaming.
- Client: Downloads all the files and resources, assembling them so that they can be presented to the user as a continuous flow video. The client software downloads first the index file through a URL and then the several media files available. The playback software assembles the sequence to provide continuous display to the user. This functionality is already built into iOS devices, and developers access this functionality using the video playback portion of the iOS SDK.

In order to satisfy content license agreements, Apple allows developers to either implement Apple's DRM (Digital Rights Management) called FairPlay or use a third-party DRM. Since many MVPDs have different content protection requirements that are based on their content license agreements, they may implement a third-party DRM that supports their own license agreements. Some MVPDs may need to support multiple DRM systems, which are permitted by Apple.

Apple allows the app developer to determine if the built-in media platform satisfies license and other requirements, and if not, developers can implement their own players and mechanisms to ensure better security. Implementing a new player allows MVPDs to have more control in implementing and maintaining capabilities, such as support regulatory requirements, e.g. EAS, parental control, accessibility, etc.

The iOS platform allows applications to use HDMI and Airplay outputs to stream video and audio. Content licenses may have different rules on allowing streaming over HDMI and/or Airplay. Given these requirements, MVPDs are left to decide on allowing or denying access to high definition devices over HDMI and/or Airplay. Requirements to manage HDMI and/or Airplay connections may be enforced by the chosen DRM system.

The iOS platform provides the means of utilizing the underlying hardware security. All iOS devices have a dedicated AES-256 crypto engine built into the DMA path between the flash storage and main system memory, making file decryption very

efficient. Application developers are free to use this mechanism or implement their own. A summary of iOS provided hardware security is available at: https://www.apple.com/business/docs/iOS_Security_Guide.pdf

2. Google Android

Google supports an App ecosystem for mobile devices, smart phones, tablets, and smart watches with its Android platform. Google supports an App ecosystem for smart TVs with its Android TV platform. Google also has an extensive developer program for Android Apps that is available under license to Google (http://developer.android.com/index.html).

Google Play is the app store for the Google Android App ecosystem. Android is the operating system created and developed by Google and, unlike Apple's iOS, is available via open source for any device manufacturer who chooses to use it. It is the operating system that powers many smart phones, tablets, and media players. Use of the Android OS does not mandate distribution of Android Apps through the Google Play Store. For example, Amazon has its own Amazon Fire Apps store for Android apps that run on Amazon tablets and Fire TV media players.

The Google Play Store and Amazon Fire App Store are both accessible using a web browser, or using native applications on an Android or Amazon device. In order to complete a purchase, one is required to register an account with Google Play or Amazon.

Once a user account is created, the customer can browse all available applications, video, and music, and make purchases. Applications are downloaded and made available on the device.

There are two integrated application development environments (IDEs) available for Android; Eclipse and Android Studio with Java as the development language.

Google also provides a set of developer guidelines to assist in the development of Android apps, as well as a set of design guidelines that help developers to make apps that not only work well but also look good.

The Android platform provides a secure boot process, as well as providing for signed application code, although sometimes this can be device manufacturer dependent. Android provides application sandbox support. However, Android does not provide a native secure media player, so an app developer must implement a secure media player to meet its content license and regulatory requirements. Miracast and/or HDCP protected output is often provided, but depends on the device manufacturer.

The Android App ecosystem is not as stringently managed as the Apple iOS app ecosystem. Android apps are not strictly approved by Google and are self-signed only. Apps can be delivered from the Google Play Store over Google protocols, or the Amazon Fire Store, or they can be side-loaded directly onto the device.

The Android platform does not provide access to unique keys or certificated identities through Android. However, access to the device MAC address is permitted.

3. Samsung Smart TV & Tizen

Samsung supports an App ecosystem for its smart TVs either with its Smart TV platform or more recently its Tizen platform initially released in March of 2015 (http://www.samsungdforum.com/). During 2015, Samsung Smart TV will fully migrate to the Tizen based ecosystem. The new Tizen platform will provide for Samsung Smart TV App developers a better performing and easier app development environment.The Smart TV platform supports Web applications, while Tizen supports Web applications, native applications and hybrid applications, but Samsung Tizen TV only provides a Web application environment for developers. App developers in Tizen develop applications based on Web technology (HTML5, CSS3, JavaScript). Tizen also supports Samsung's mobile devices, tablets, smart phones, and smart watches.

Samsung Smart TV is a web-based application that runs on an application engine installed on Samsung's digital TVs that are connected to the Internet. Smart TV applications are special web pages implemented in a web browser and displayed on a TV screen. Users can download *Smart TV Applications* from Samsung Apps and install them on their TVs, or even develop their own applications.

Consumers can view an application on the TV screen similar to how they view web pages in a web browser on a computer. However, the experience is adjusted to screen resolution, hardware specifications, using the TV remote control for user interaction, and typically only executing one application at a time..

The Smart TV platform supports HTML5, DOM3, CSS3, JSC, and a variety of DRMs including: PlayReady, Widevine, and Verimatrix. For transport the Smart TV platform supports DASH, HLS, Smooth Streaming, as well as Live Streaming. The Smart TV Platform is based on two engines: Gecko, for platforms from years 2011 and 2010 and WebKit for more recent years. It supports three resolutions

- 960 x 540 pixels
- 1280 x 720 pixels

- 1920 x 1080 pixels

Smart TV apps can be controlled by the following input devices:

- Remote control
- Mouse
- Gestures
- Voice

The Tizen platform supports HTML5, DOM3, CSS3, JSC, and a variety of DRMs including: PlayReady, Widevine, Verimatrix, SecureMedia, SDRM, and SCSA. For transport the Smart TV platform supports DASH, HLS, Smooth Streaming. Applications are signed with the developer certificate.

In order to distribute applications on Samsung TVs and make them available through the Samsung Smart Hub Apps TV store, it is necessary to register the application and it must go through a certification process provided by Samsung or its Affiliate at the Application Seller Office before being launched on the Samsung Apps TV store. To request certification, it is necessary to prepare the Tizen widget package and metadata and submit it in the Samsung Apps TV Seller Office.

Tizen widget packages are signed with the author's signature, so the system cannot modify the package contents in any way. Because of this, it is crucial that all app information and metadata in Tizen widget file are correct and match the information provided to the Seller Office. Otherwise, this may lead to problems in submitting the application or certification process itself.

The registration process, from generating an App ID to certification test , consists of four steps:

1. Basic information - provide general app metadata + icon and screenshot images. Information set in this step will be displayed in Samsung Apps store.

2. Test information - verification request details. These include target Tizen TV platforms, app documentation, login credentials and additional information useful for the application testers.

3. Pretest - submit the widget package file and check if it complies with Samsung policy. The system scans application code with an automatic tool and notifies about any warnings or errors.

4. Complete - confirm the request details and execute the Release Agreement.

To update existing applications, it is only necessary to complete steps 2.-4.

When all of these steps are completed, the app is sent to Samsung engineers for verification.

To aid development Samsung provides both a development guide and a UX guide.

4. LG WebOS

LG supports an app ecosystem for its smart TVs with its WebOS platform. Applications are packaged in IPK format and registered in the LG SmartWorld Seller Lounge. The LG application quality assurance team evaluates the performance, function, and UIs of submitted apps to verify the suitability for publishing on LG Content Store (LG STORE). Valid apps are published on LG Content Store (LG STORE).

LG has the following criteria for applications submitted to the LG Store:

1. Under no circumstances will any content containing offensive words/phrases/meaning toward other nations and cultures be tolerated.
2. Application should not contain any racially or sexually discriminating content.
3. Applications should not contain any user information retrieving malignant codes, and/or viruses, etc.
4. Applications should not contain any codes that can result in fatal device errors.
5. Applications should not contain any material that violates copyrights of anyone including pictures, videos, illustrations, programs, etc.
6. Applications should not contain extremely lewd and/or violent material including videos, phrases, images, etc.

LG also has a number of QA criteria for applications submitted to the LG Store:

Category	**Detail Checks**

Sound	1. Are there any problems with sound when the content is run? 2. Is there any unwanted noise or static in the sound? 3. Are the background music and/or sound effects playing back correctly? 4. Are the sound and video in sync?
Language	1. Does the app support the appropriate regional language? 2. Does the app display the appropriate language correctly? 3. Do special characters and emoticons display correctly? 4. Are there any spelling or word display errors?
Remote	1. Does the app support the use of regular LG Smart TV remote control correctly? 2. Does the app support the use of the LG Smart TV Magi Motion Remote Controller correctly? 3. When the content is run, are the movements of the Motion Remote Controller and its pointer working correctly?
Action	1. During the running of an app, does the pause function operate correctly? 2. From the paused point, does the app re-start correctly when it is un-paused? 3. Does the app shut down correctly? 4. Does the display change back to the previous screen correctly?
Performance	1. Does the app load without too long of a delay? 2. When run, does the app exhibit skipping or stopping problems?

3. Does the app shut-down without too long of a delay?

4. Does the app cause loading problems for the TV?

Every app submitted to LG Smart World will go through a Quality Assurance (QA) process before sale is permitted. Those Apps that do not meet the QA criteria can be rejected for sale.

The QA criteria applies to every app submitted but certain Apps such as game, video, education, etc, can be subjected to additional criteria by category.

Apps that cause TV errors, illegally collect user information, contains malignant codes, and/or contains viruses will be removed from the store, and the Seller can be held responsible.

5. Microsoft Xbox

Microsoft supports an app ecosystem for its Xbox game consoles, both Xbox 360 and Xbox One.

<Discussion of Microsoft Xbox platform goes here>

6. Sony PlayStation

Sony supports an app ecosystem for its PlayStation game consoles, both PlayStation 3 and 4.

<Discussion of Sony PlayStation platform goes here>

7. Roku

Roku supports an app ecosystem for its streaming video players, including its Roku 1, 2, 3, and Roku Streaming Sicks. There is no fee for joining the Roku Developer Program or for publishing a Roku app. Roku Channels are written in a Roku-specific language called BrightScript. BrightScript is a scripting language similar to VisualBasic and is quickly learned by experienced programmers. Communication with services and servers is done over HTTP using standard XML-based technologies like (M)RSS, RESTful APIs and JSON. For video, Roku recommends H.264 video with AAC-LC audio wrapped in a MP4 container. Roku also supports the VC-1 video codec, and the WMA and MP3 audio codecs. Roku supports the HTTP Live Streaming protocol (HLS), which is quickly becoming the standard across home entertainment and mobile devices. This technology provides adaptive streaming of either

live or on-demand content. Roku supports PlayReady for Smooth Streaming and AES-128 bit encryption for HLS. Roku reviews and approves all apps prior to publishing them to the Roku Channel Store to ensure that they are of high quality and function properly. Roku attempts to make this process as streamlined as possible. The specific restrictions and terms for publishing content to the Roku Channel Store are found in the Roku Developer Agreement. In a presentation to Working Group 4, Time Warner Cable commented that the Roku developer support team was skeptical about developing a grid based EPG app on Roku devices that would have acceptable performance. Based on Time Warner Cable's extensive experience in developing grid based EPG applications, they were able to provide an EPG app on Roku devices that performed very well. This Roku app was demonstrated at the June 2, 2015 Working Group 4 meeting. {Link to video}

D. Applicable Devices

As outlined above Apps can be developed for almost every class of retail device, including:

- Smart or connected TVs
- Game Consoles
- Retail set-top boxes or HDMI sticks
- Personal computers (both Windows and Mac)
- Tablets
- Smart phones

II. W3C HTML5 Web Browser

The World Wide Web Consortium (W3C - http://www.w3.org/) is an open standards body that defines the standards used to implement the Web today. HTML5 represents the latest version of the W3C standards and is being implemented by all commercial web browsers today. Web browsers for mobile devices are also implementing HTML5. Smart TVs and other connected entertainment devices are also implementing HTML5 capabilities.

The HTML5 Media elements, Media Source Extensions (MSE) and Encrypted Media Extensions (EME) are the W3C specifications for processing multi-media, including protected audio/video content. All major web browsers are implementing Media elements, MSE and EME to support both protected and unprotected video content. These specifications are being adopted by video distributors across the Web. For example, Netflix already uses HTML5 with EME to distribute protected content and other OTT distributers and MVPDs are following their lead. HTML EME can also be used in devices that do not have browsers.

HTML5 Media elements are used to present video and/or audio data to the user. HTML5 media resources can have multiple audio, video and data tracks. HTML5 includes standard definitions for special media tracks, including alternative media, captions, descriptive audio, sign language, subtitles, translation and commentary.

The MSE specification [MSE] defines an API that a web page can use to feed media data to the HTML5 video or audio element. This API enables JavaScript in the page to:

- Handle processing of an adaptive media manifest file.
- Fetch the media segments using the URL from the manifest file
- Append the media segments for playback by the browser's media player.

The MSE API can be used for insertion of other content like advertisements, alternative media or playback of a local media file.

While the MSE API is independent of any particular adaptive delivery protocol, MPEG DASH [DASH] has been a specific design and implementation focus. MPEG DASH takes advantage of the most recent MPEG technology to seamlessly adapt to changing network conditions, and provide high quality play back with fewer stalls or re-buffering events.

Media Source Extensions enables JavaScript to send byte streams to the various media codecs implemented in HTML5 web browsers. This allows the prefetching and buffering of media streams to be implemented in JavaScript providing greater flexibility and application control over these media streams. This flexibility allows the application to optimize the playback of media from multiple sources. Figure 15 is the diagram of the MSE architecture from the W3C MSE draft specification.

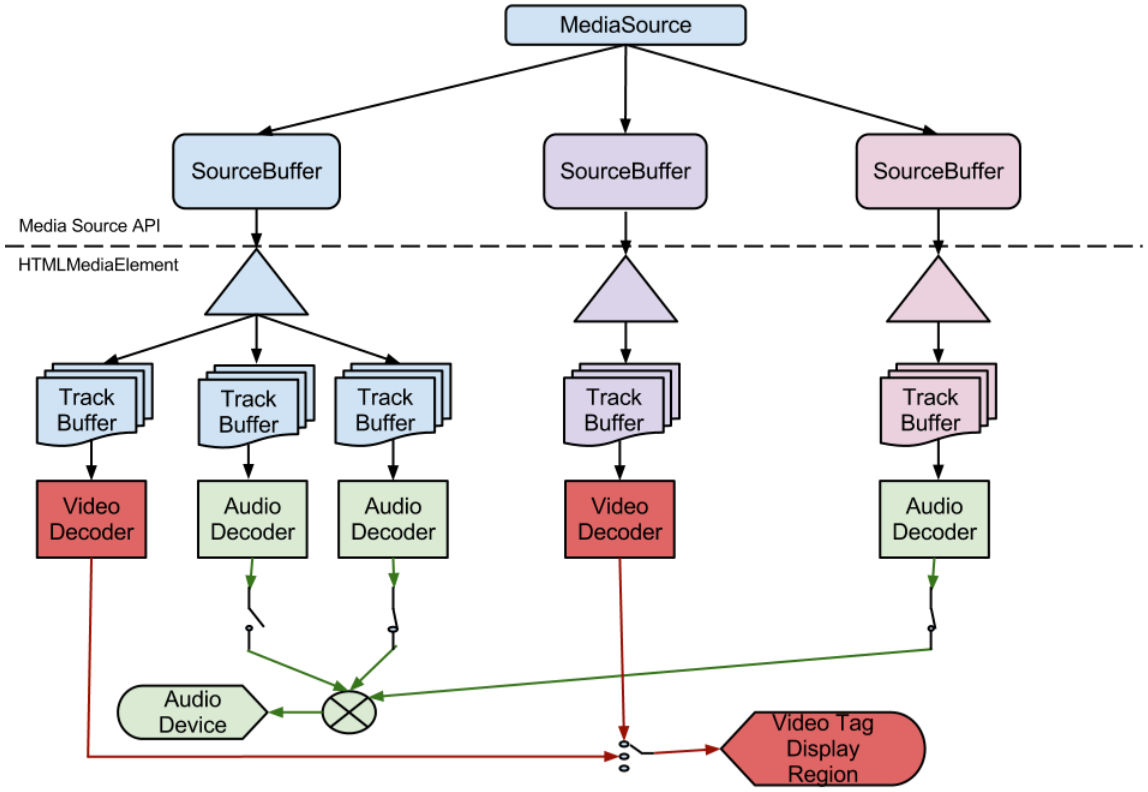


Figure 15 - Media Source Extensions Architecture

The EME specification [EME] defines an API that a web page can use to playback content, securely protected by any EME-compliant DRM system, using the video or audio element. The API enables the page to:

- Detect attempted playback of protected content.
- Learn what DRMs may be used to playback the content.

- Request the appropriate DRM license needed for content playback.
- Provide DRM licenses to the user agent for content decoding.

A browser may implement any number of DRM-specific content decryption modules (CDM) that handle license processing and content decryption. EME does not specify any particular content encryption or any set of DRMs, nor does it define how a CDM is implemented in the browser. EME does require support for the Clear Key [CLEAR] decryption so that browser EME implementations can be tested or used without a commercial DRM. EMEs is the W3C specification that defines the APIs necessary to control the playback of protected content. Per the EME specification:

"The API supports use cases ranging from simple clear key decryption to high value video (given an appropriate user agent implementation). License/key exchange is controlled by the application, facilitating the development of robust playback applications supporting a range of content decryption and protection technologies.

This specification does not define a content protection or Digital Rights Management system. Rather, it defines a common API that may be used to discover, select and interact with such systems as well as with simpler content encryption systems. Implementation of Digital Rights Management is not required for compliance with this specification: only the Clear Key system is required to be implemented as a common baseline.

The common API supports a simple set of content encryption capabilities, leaving application functions such as authentication and authorization to page authors. This is achieved by requiring content protection system-specific messaging to be mediated by the page rather than assuming out-of-band communication between the encryption system and a license or other server."

Figure 16 shows the high-level architecture of the EME specification. In this example, content is encrypted using Common Encryption Scheme (CENC) and is typically distributed from a Content Distribution Network (CDN).

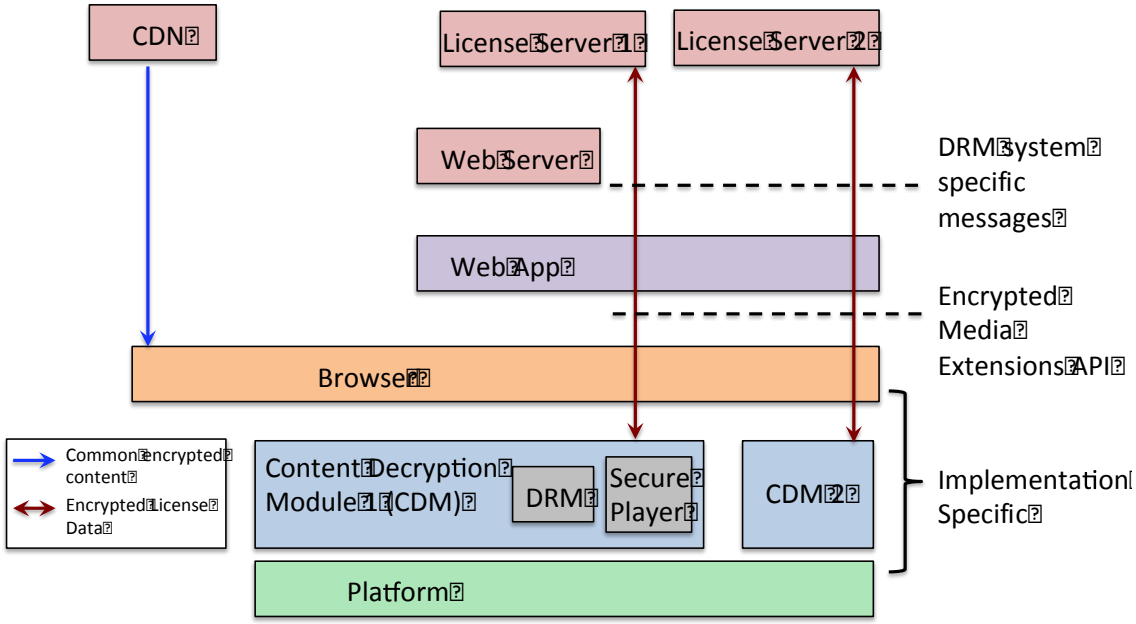
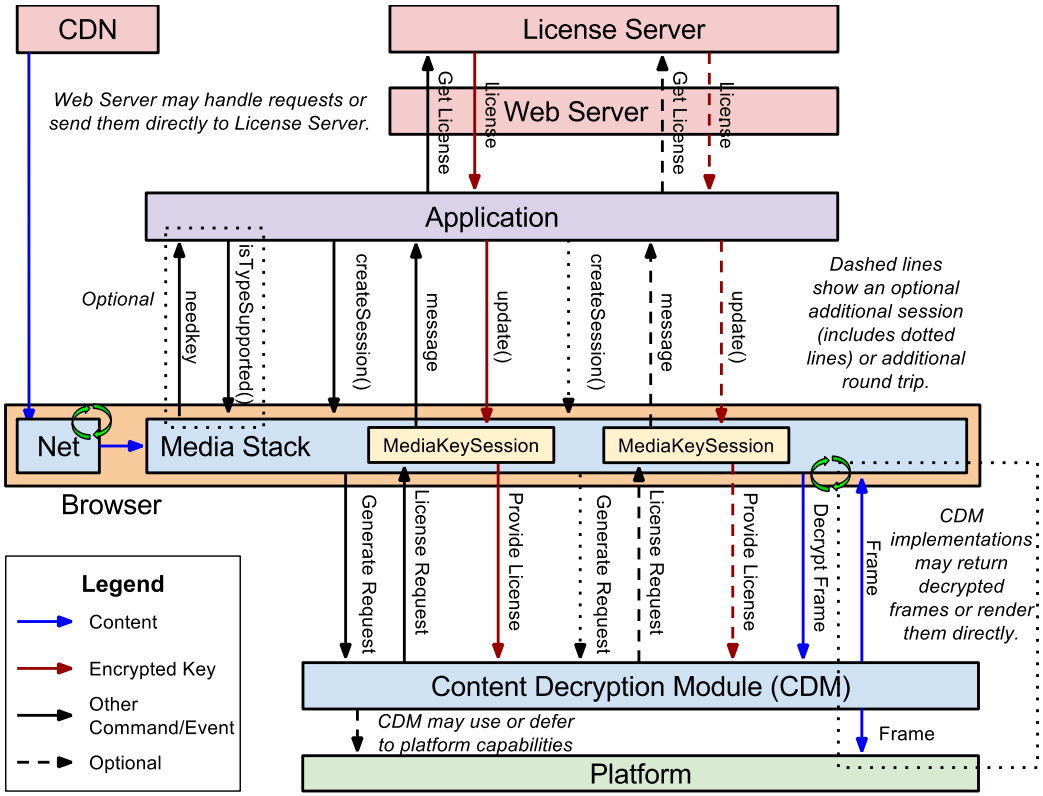


Figure 16 - Encrypted Media Extensions Architecture

Figure 17 is the detailed EME architecture from the EME draft specification and shows the APIs implemented to abstract the DRM



implementations.

Figure 17 - Detailed EME Architecture with APIs

All of the major browsers have implemented EME, including Google/Widevine, Apple/Fairplay, Microsoft/Playready, and Adobe/Access. Thus, there is competitive downloadable browser/DRM marketplace.

A. World Wide Web Consortium (W3C) Standards

The W3C Specifications are publicly available at: http://www.w3.org/TR/. The following W3C Specifications are relevant to enabling competitive availability of devices that receive MVPD services:

- W3C HTML5 Specification, *A vocabulary and associated APIs for HTML and XHTML*. http://dev.w3.org/html5/spec/
- W3C WOFF File Format 1.0. http://www.w3.org/TR/WOFF/
- W3C MSE, *Media Source Extensions*. http://www.w3.org/TR/media-source/
- W3C EME, *Encrypted Media Extensions*. http://www.w3.org/TR/encrypted-media/
- W3C Crypto, *Web Cryptography API*. http://www.w3.org/TR/WebCryptoAPI/

B. Protocols

The protocols used include:

- TCP/IP
- HTTP
- HTTPS
- MPEG DASH

C. Information

The W3C Specifications are publicly available at: http://www.w3.org/TR/.

D. Applicable Devices

HTML5 with EME and MSE is applicable to any device that implements these specifications including: smart/connected TVs, game consoles, PCs, tablets, and smart phones. HTML5 can support a browser user interface (e.g. Chrome or Firefox on a PC) or HTML5 can support an application environment that looks just like a native app environment (e.g. Smart TVs from Firefox OS, Tizen or WebOS). Consequently, HTML EME can be used in devices that do not have browsers.

III. DLNA VidiPath™

The Digital Living Network Alliance (DLNA) is a technology standards organization with participants from consumer electronics manufacturers, software developers, content providers, and MVPDs that builds industry consensus to advance the interoperability of

video products in consumers' connected homes. DLNA was founded in 2003 and currently has a membership of more than 200 companies. DLNA's multi-industry collaboration implements a set of guidelines utilized by service providers, electronics manufacturers, and software developers to provide consistent performance in a connected home environment. "VidiPath" enables MVPDs to deliver their service to retail devices by using an HTML5 app with extensions developed in the W3C standards body. VidiPath was developed in DLNA by major retail device manufacturers (including Samsung, Panasonic and Sony); major chip manufacturers (Intel and Broadcom) and major MVPDs (including Comcast, TWC, AT&T and DISH). The retail device can operate as a retail "mall" in which many different video providers can operate as retail stores presenting their own brands and experiences. The subscriber clicks on the app and receives the full service offered by the MVPD. VidiPath Certified devices, include mobile devices, PCs, set top boxes, AV receivers, game consoles, TVs. DLNA has also created a robust certification program which tests and verifies the interoperability of products built to its standards, ensuring consumers that devices branded with the DLNA Certified and VidiPath Certified marks will successfully connect and exchange content.

DLNA VidiPath enables both a home server model, or as MVPDs move more to the cloud, a cloud to ground model.

This section presents an overview of the VidiPath specifications that include features such as HTML5 Remote User Interface (RUI), Authentication, Diagnostics, Low Power, MPEG-DASH, and DTCP-IP [3]. Benefits offered by VidiPath to consumers, OEM manufacturers and service providers are also discussed. To support market adoption and implementation of VidiPath, CableLabs has developed an open source implementation of VidiPath Server and Client reference devices [4]. The Server and Client reference devices serve as reference platforms for retail device manufacturers and MVPDs and other MVPDs to test their VidiPath implementations.

A. DLNA VidiPath Media Formats

In order to support the full set of MVPD service features, retail devices need to support an appropriate set of audio and video codecs with specific resolution, bit rate, and frame rate. MVPD video content predominantly uses MPEG-2 video encapsulated in MPEG-2 TS, and H.264/AVC in MPEG-2 TS to a lesser degree. In addition, support for adaptive bit rate streaming needs to be considered as MVPDs may have a need to stream video over Wi-Fi networks to portable devices. Support for MVPD contractual and regulatory services (e.g., closed captions, parental control, EAS, SAP, and ad insertion) needs to be supported by this application framework. Information about these services for video content is carried in-band as elementary streams of the MPEG-2 transport streams (TS). So, the application framework needs to support mapping of these elementary streams to the application layer. In order to enable rapid application development cycle, the application framework needs to support a "write once and run anywhere" model.

B. DLNA VidiPath Quality of Service

MVPDs and content providers, want to ensure that their services are offered with the highest quality when the content is streamed over the home network from a video gateway to retail devices. Thus, it is necessary to avoid congestion or interference of home network traffic that could degrade the quality of user experience. Therefore, it is necessary to consider that a video gateway and retail devices support a home network technology with throughput in excess of 100 Mbps (enough to support 3 MPEG-2 video HD streams). In addition, support for either priority-based or parameterized quality of service (QoS) needs to be considered.

C. DLNA VidiPath Diagnostics

As premium video content is streamed over the home network from a video gateway to retail devices, MVPDs need a mechanism to diagnose and troubleshoot home network related issues remotely. Such a mechanism needs to support the ability to test the home network's connectivity between a video gateway and retail devices, provide network topology, and information about network throughput. In addition, the ability to query information about retail devices such as device model, manufacture, and, firmware version needs to be enabled by this mechanism.

D. DLNA Energy Efficiency

In order to meet consumer expectations and MVPD requirements for energy efficiency, MVPD STBs and gateways implement energy saving operations, including various types of sleep modes. To avoid a consumer having to explicitly wake up the video gateway when the consumer wants to watch video content on a retail device, it is necessary that the retail device is able to wake up the video gateway from sleep mode.

To enable secure distribution of premium content from an in-home video gateway to retail devices, major MVPDs in the U.S., CableLabs,retail device manufacturers and other service providers all over the world, led an effort to define VidiPath specifications within Digital Living Network Alliance (DLNA) [2].

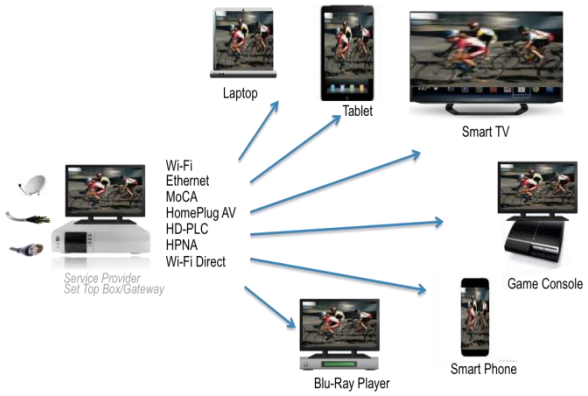


Figure-1: DLNA VidiPath Overview

Using VidiPath specifications, MVPDs can stream various content from a video gateway to retail devices, such as TVs, game consoles, tablets, mobile phones, and laptops, with a consistent MVPD user interface across different devices without the need of a dedicated MVPD supplied STB per device.

The DLNA VidiPath Specifications define the following set of features for VidiPath Server and Client [3]:

- HTML5 Remote User Interface (RUI)
- MPEG-2 and AVC media formats
- DTCP-IP Link Protection
- Diagnostics
- Low Power
- Authentication
- 3D Media formats; conditionally mandatory
- HTTP Adaptive Delivery; mandatory for Client, optional for Server

- Priority-based QoS
- Digital Media Server (DMS); mandatory for Server only
- Digital Media Player & Digital Media Renderer; mandatory for Client only

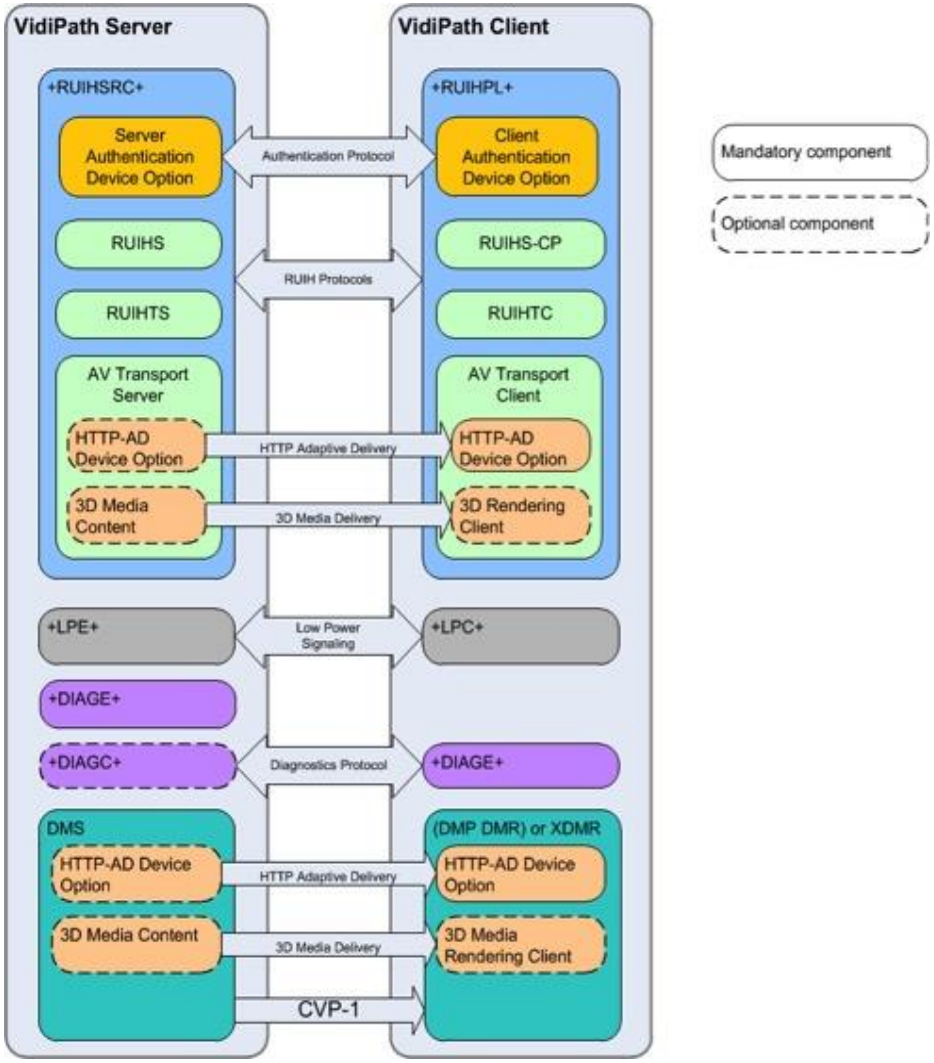


Figure-2: DLNA VidiPath Architecture

E. HTML5 Remote User Interface (RUI)

In order to support a consistent MVPD user interface to different form factors of retail devices (e.g., TVs, tablets, mobile phones, and, game consoles) and requirements identified in the Application Framework subsection, DLNA VidiPath specifications specify support for an HTML5-based Remote User Interface. DLNA HTML5 Remote RUI specification defines a profile of W3C's HTML5 specification [6] and other related specifications such as Cascading Style Sheets (CSS), Web Sockets, XMLHTTPRequest (Ajax), and FullScreen.

HTML5 is a widely adopted industry standard supported by a broad range of browsers on a wide variety of devices. Thus, it enables MVPDs to develop their guide once and offer it on a wide range of platforms resulting in reduced development costs and faster time to market for new services/applications. It also enables MVPDs to offer their guides directly from the cloud, thereby enabling them to rapidly evolve their services and applications to consumers.

An MVPD video gateway advertises that the Uniform Resource Locator (URL) of the MVPD HTML5 guide and VidiPath devices discover the URL using the UPnP RUI Discovery mechanism [7]. Cable operator's HTML5 guide can be served either from the in-home video gateway or from the cloud. Using the <video> tag defined in the HTML5 specification, MVPDs are able to display video within their guide user interface pages. DLNA HTML5 RUI Specification defines DLNA specific extensions to support playback of video content using <video> tag over an IP link protected by Digital Transmission Copy Protection (DTCP). In addition, the DLNA HTML5 RUI specification defines extensions to HTML5 <video> tag to support time-based seek and playspeed trick modes so that a consumer is able to pause, rewind and forward the video from the HTML5 guide page.

CableLabs developed a specification [8] that defines a standardized mechanism for exposing information about MVPD regulatory and contractual services, such as closed captions, content advisories, SAP, DVS, and ad insertion carried in the MPEG-2 TS video stream as HTML5 audio, video and text tracks, so that MVPD HTML5 Web applications can provide these services to consumers. DLNA HTML5 RUI requires implementation of this specification, so that MVPDs can fulfill their regulatory and contractual obligations while offering the full MVPD service to VidiPath devices. DLNA HTML5 RUI Specification also requires support for W3C's Server Sent Events (SSE) specification [9]. Using SSE, MVPDs are able to provide EAS messages to MVPD HTML5 RUI applications running on VidiPath devices. Figure-3 shows various HTML5 RUI entities and their functions.

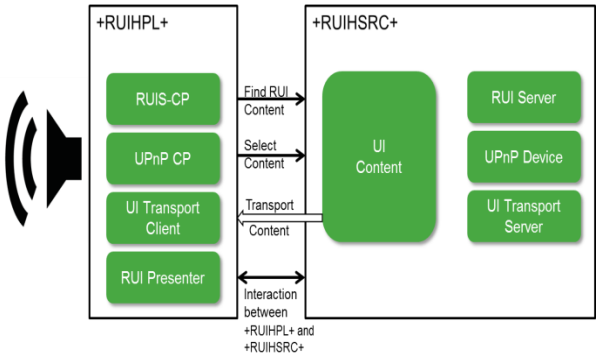


Figure-3: VidiPath HTML5 RUI Usage Model

HTML5 RUI (RUI-H) Source capability (+RUIHSRC+) has the role of exposing and sourcing RUI-H content and includes RUI-H Server (RUIHS), RUI-H Transport Server, and an optional DLNA Media Transport Server (for serving media content):

- RUIHS provides UPnP RUI Server device functionality, which enables VidiPath Servers to offer one or more remote UIs based on HTML5, and to handle UPnP RUI Server service actions.
- RUI-H Transport Server and RUI-H Transport Client are the device functions for transport of the RUI-H content between a client and server.
- RUI-H Pull Controller (+RUIHPL+) has the role of finding and loading RUI-H content that is exposed by a +RUIHSRC+ capability, rendering the UI content, and interacting with it. RUI-H Pull Controller includes RUI-H Server Control Point (RUIHS-CP), RUI-H Transport Client, RUI-H User Agent and an optional DLNA Media Transport Client.
- RUIHS-CP is a controller for browsing and selecting an HTML5 remote UI offered by a RUI-H Server.
- RUI-H User Agent functionality on a RUI-H Client is responsible for retrieving, decoding, presenting and interacting with the RUI-H content received from the RUI-H Server.

F. MPEG-2/AVC Media Formats

In order to ensure baseline interoperability between the VidiPath Server and the VidiPath Client, the DLNA VidiPath specifications define a required set of Media Format profiles for both VidiPath Server and Client for a particular geographic region (e.g., North America, Europe). This set of media format profiles is representative of premium content sourced by service providers in that particular region.

MPEG-2, as well as AVC/H.264 video encapsulated in MPEG-2 TS with resolutions up to 1080p, are required. Support for audio codecs such as AC-3, E-AC-3, AAC, MP3, and MPEG Layer-1 & 2 is required as a part of this media format profile set. Additionally, AVC video encapsulated in MP4 containers needs to be supported to enable interoperability with portable devices. VidiPath Server and Client devices are also required to support DLNA specified trick modes (byte seek, time seek and playspeed) and DTCP-IP link protection for this set of media format profiles. Due to this mandatory set of media format profiles, as long as MVPDs offer their content using one of the media format profiles from the VidiPath server implemented in the video gateway, a VidiPath Client device will be able to play back the content over the home network.

G. DTCP-IP Link Protection

In order to meet content provider expectations and requirements, DLNA VidiPath specifications leverage Digital Transmission Content Protection over Internet Protocol (DTCP-IP) Link Layer protection technology to secure content from unauthorized copying and misuse within the home as it is streamed from a MVPD video gateway to a VidiPath client device. DTCP-IP is a link protection specification published by Digital Transmission License Administrator [10].

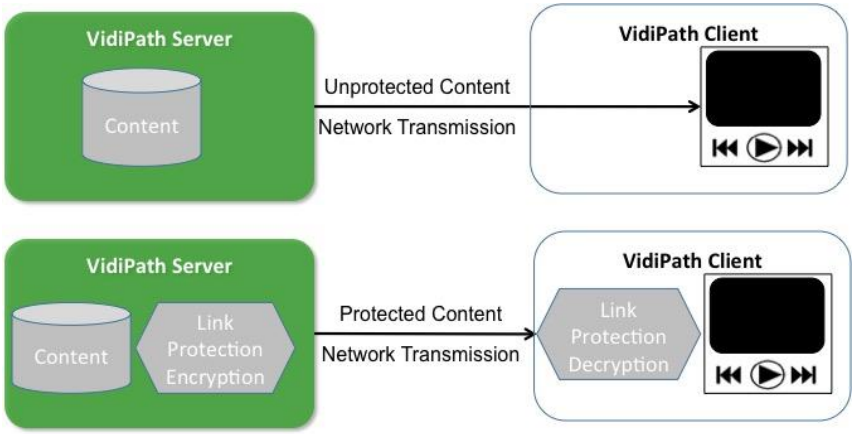


Figure-4: Secure content transmission using DTCP-IP

This is a critical enabler for multi-device viewing experiences involving premium subscription TV content. DTCP-IP is automatically negotiated between devices and has been designed to provide certain content protection as content moves across the local home network. In accordance with the VidiPath specifications, digital content can be shared securely between products in a user's home, but not with third parties outside the home network.

H. Diagnostics

The DLNA VidiPath Diagnostics feature focuses on the collection of data about the home network conditions and devices through a set of actions and queries, so that a MVPD or a user can take appropriate steps to troubleshoot and diagnose service-related issues. The VidiPath diagnostics feature relies on UPnP Device Management [11] as a required functionality, and IEEE 1905.1 [12] as an optional functionality. UPnP Device Management provides the ability to collect layer-3 & layer-4 diagnostics information such as IP-connectivity, network bandwidth, device information, and device status. IEEE P1905.1 provides layer-2 diagnostics information such as layer-2 link information, status, and layer-2 topology information.

Figure-5 shows various DLNA Diagnostics logical entities and their functions.

- A Diagnostics Endpoint (+DIAGE+) capability has the role of offering diagnostics services and responding to diagnostics action requests by implementing UPnP Basic Management Service v2 [13] as a required service and UPnP Configuration Management Service v2 [14] as an optional service. DLNA VidiPath Specifications requires certain actions to be implemented, such as Ping, Trace Route, and NSLookup. Both the VidiPath Servers and Clients are required to support diagnostic Endpoint capability.

- Diagnostics Controller (+DIAGC+) has the role of providing a diagnostics application and a control point for issuing action requests to a +DIAGE+. However, a Diagnostics Controller is optional for VidiPath device profiles, although it is expected that a Diagnostics Controller may be included on a VidiPath server to allow the service provider's support staff to diagnose issues within the consumer's home. The diagnostics application drives the Diagnostics Controller to access diagnostics data and capabilities. Cable operators remotely access the diagnostics application running on the VidiPath server using a TR-069 or SNMP management interface. Alternatively, a MVPD technician or end-user may access the diagnostics application through a browser or screen interface as shown in Figure-5.

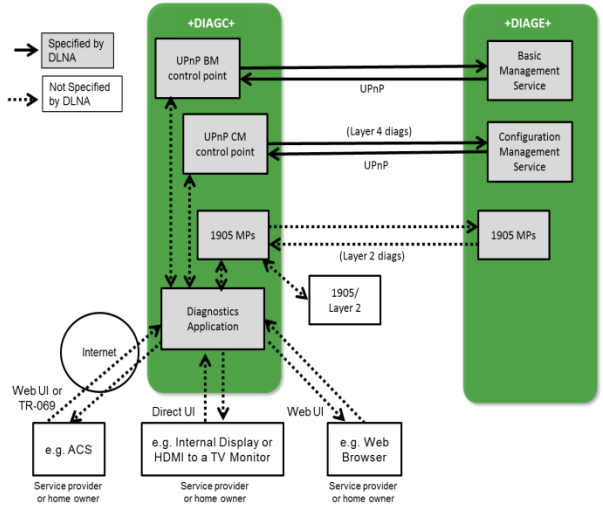


Figure-5: VidiPath Diagnostics Architecture

I. Low Power

To account for service provider STB/video gateway devices implementing energy saving operations, e.g., different levels of sleep modes, the DLNA VidiPath specifications provide wake-up or reservation mechanisms to VidiPath client devices. The specifications enable DLNA devices to convey energy management and sleep-mode capabilities for each of its network interfaces. This facilitates the awareness of the availability of DLNA functionality, even in the presence of power-saving mode operations. The VidiPath Low Power feature is based on the UPnP Energy Management Service [15].

Power savings is modular within a physical device. In the context of DLNA networked devices, as shown in Figure-6, each physical network interface can have various power modes. Some of these power modes can allow layer-2 or layer-3 connectivity to still be present even when many other device components are powered down. Other physical components, such as screens, hard drives and similar resources, can also support different power modes.

The VidiPath Low Power feature consists of the following entities:

- Low Power Endpoint (+LPE+) capability implements UPnP Energy Management Service and has the role of responding to action requests, including requests to provide information on network interface mode, and requests to access services based on subscriptions.

- Low Power Controller (+LPC+) capability implements a control point for the UPnP Energy Management Service and has the role of issuing action requests to a Low Power Endpoint or a Low Power Proxy.

The VidiPath Server is required to implement Low Power Endpoint (+LPE+) capability, and the VidiPath Client is required to implement Low Power Controller (+LPC+) capability. This enables VidiPath Clients to query information about power save mode operations of a service provider's VidiPath Server and invoke appropriate actions to wake-up the VidiPath Server when its services are needed for the consumer. Waking up a VidiPath Server from the low-power mode can introduce some latency and longer response time, so it is expected that a VidiPath Client provides appropriate messages to the user to provide a good user experience.

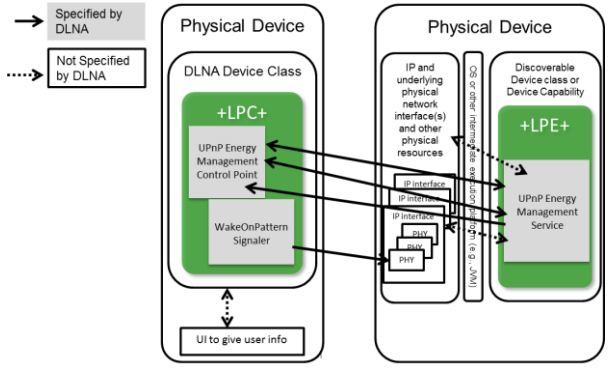


Figure-6: DLNA Low Power Architecture

J. HTTP Adaptive Delivery

The HTTP Adaptive Delivery feature of VidiPath enables service providers to describe content as adaptive content; i.e., in timed segments at various bit rates and in various media formats. In the event of network congestion, which is likely to happen over Wi-Fi, a client rendering devices can maintain smooth streaming of content for display by switching between streams at different bitrates. A Media Presentation Description (MPD) file provided by a server includes segment information such as timing, URL, and, media characteristics (e.g., video resolution and bit rates). This feature leverages Moving Picture Expert Group Dynamic Adaptive Streaming (MPEG-DASH), over HTTP (ISO/IEC 23009-1) standard [16]. Additionally, DLNA VidiPath specifications mandate support for ISO-based media file format (ISOBMFF) Live, ISOBMFF On-Demand, and MPEG-TS Simple profiles defined in the MPEG-DASH specification.

Different logical entities of the HTTP Adaptive Delivery feature are shown in Figure-7.

VidiPath Clients are required to support HTTP Adaptive Delivery device option and aforementioned HTTP Adaptive media format profile. Support for HTTP Adaptive delivery is optional for a VidiPath Servers, but if it is supported, then the VidiPath Server is required to support at least one of the HTTP Adaptive media format profiles.

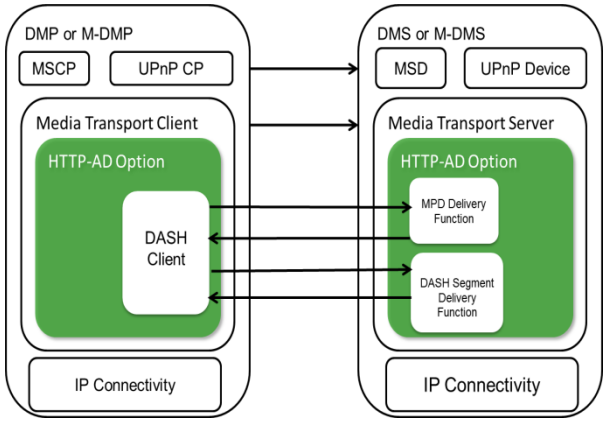


Figure-7: HTTP-Adaptive Delivery Entities

On the VidiPath Server, the HTTP Adaptive Delivery device option has the role of exposing and sourcing content using the HTTP Adaptive Delivery mode. This includes exposing and sourcing both the MPD and the media itself (segments for different representations). This functionality maps to the MPD delivery function and segment delivery function in MPEG-DASH. On the VidiPath client side, the HTTP Adaptive Delivery device option has the role of requesting appropriate content MPD and media representation (segments), and assembling and rendering the media while adapting to changing network conditions.

K. HTTP Adaptive Delivery

By utilizing the VidiPath Authentication feature, service providers can verify that the VidiPath client has been certified to the DLNA VidiPath specifications. This provides confidence to service providers that a VidiPath Client is able to display their HTML5 RUI guide, meet regulatory requirements, and deliver content services appropriately to meet consumer expectations.

The VidiPath authentication feature also supports authentication of a VidiPath Server by a VidiPath Client. A VidiPath Client can optionally authenticate a VidiPath Server to ensure that the Client is talking to a legitimate VidiPath Server to protect consumers from rogue servers.

Upon DLNA certification of a VidiPath device (Client or Server), a device manufacturer obtains a DTLA VidiPath Certificate, which has the same format as the legacy DTLA DTCP certificate used for DTCP-IP link protection, except that it has a special field that indicates the device is DLNA VidiPath certified. The same certificate is used by the device for VidiPath device authentication as well as for DTCP-IP link

protection. This avoids including additional certificates in the device and saves cost for the device manufacturer. If a service provider authentication server is located in the cloud, then it obtains a VidiPath X.509 certificate from DTLA.

DLNA VidiPath Authentication uses Transport Layer Security Supplemental Data (TLS-SD) extensions, defined in RFC 4680 [17], to carry VidiPath client's DTLA VidiPath certificate over Hypertext Transfer Protocol over Transport Layer Security (HTTPS). Standard Transport Layer Security [18] protocol only supports transport of X.509 certificates. A TLS-SD extension allows transport of arbitrary pieces of information over the TLS protocol.

The HTML5 RUI browser implemented by the VidiPath Client is responsible for performing authentication using HTTPS with MVPD Authentication Server. Cable operator Authentication Server verifies that the device requesting service is a DLNA Certified VidiPath device based on the DTCP VidiPath certificate supplied using the DLNA VidiPath authentication protocol.

Figure-8 shows various VidiPath authentication logical entities:

- Client Authentication is a device option that supports client credentials and the protocols to allow a client to be authenticated by an Authentication Server.

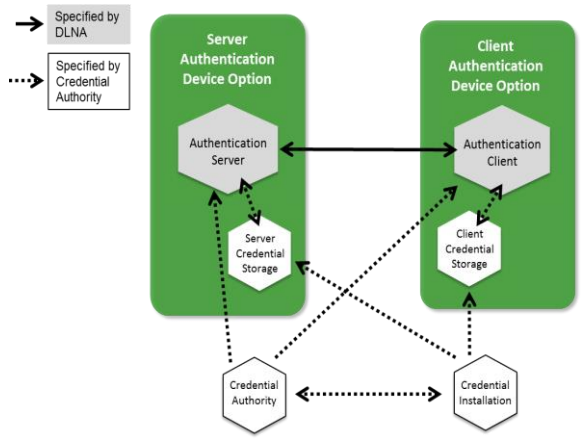


Figure-8: VidiPath Authentication Entities

- Server Authentication is a device option that supports server credentials and the protocols to allow a server to be authenticated by an Authentication Client.

The DLNA VidiPath Authentication supports two different scenarios for the Client/Server Authentication:

1. In the first scenario, shown in Figure-9, the Authentication Server is in the cloud and authentication must be accomplished with a cloud-based server. In this scenario, the server uses trusted X.509 VidiPath certificate and client uses DTLA VidiPath certificate.

2. The second scenario is shown in Figure-10, where the Authentication Server is located in the home (in a video gateway/STB) and all authentication protocol exchanges are performed within the home network. In this scenario, the server uses trusted or self-signed X.509 certificate signed with DTLA VidiPath certificate, and client uses DTLA VidiPath certificate.

L. Other VidiPath Features

- **Digital Media Server (DMS)**: VidiPath Server is required to support DLNA DMS device class. This provides essential functions of device discovery, content streaming with support for trick modes (pause, rewind, forward).

- **Digital Media Player (DMP)/Digital Media Renderer (DMR):** VidiPath Client is required to implement DLNA DMP and DMR device classes. These provide essential functionality for content streaming with support for trick modes. DMR provides device discovery and "Play To" scenario where a phone or tablet can establish and control content streaming between a DMS and DMR.

- **Priority-based Quality of Service (QoS):** DLNA VidiPath requires prioritized QoS solution where video streams are given a higher priority over data/background traffic over the home network. The majority, if not all, of home networking technologies (e.g., Ethernet, Wi-Fi, MoCA, HomePNA, and HomePlug) support traffic prioritization when packets are marked with layer-2 802.1 p/q tags. The VidiPath Server is required to mark video packets with diffserv codepoints (DSCP), as well as with layer-2 802.1 p/q tags, so that video traffic receives appropriate priority when streamed over the home network.

- **3D Media Formats:** DLNA VidiPath specifications conditionally mandate support for 3D media formats for VidiPath Clients and Servers. DLNA has defined a set of frame-compatible stereoscopic-3D media formats (Side-by-Side and Top-and-Bottom), which are representative of content supplied by service providers. If the VidiPath client supports rendering of 3D video, then it is required to implement support for these DLNA defined 3D media formats.

M. VidiPath Deployment Scenarios

The DLNA VidiPath Specifications support two deployment scenarios: Hybrid In-Home + Cloud scenario, and In-home only scenario.

In the hybrid In-home+Cloud Scenario, the MVPD's HTML5 RUI server and authentication server reside in the cloud, but all other functions of VidiPath server reside on an in-home video gateway or STB. A VidiPath

Client discovers URL of the MVPD's cloud guide from an in-home VidiPath gateway/STB. The VidiPath Client is authenticated with a cloud Authentication Server, which may be co-located with the cloud RUI server (server uses trusted X.509 VidiPath certificate). Upon authentication, the VidiPath Client downloads MVPD HTML5 guide from the cloud. The HTML5 guide has links to video content that point to the in-home gateway/STB. Thus, actual video content is served from in-home gateway/STB to the VidiPath Client.

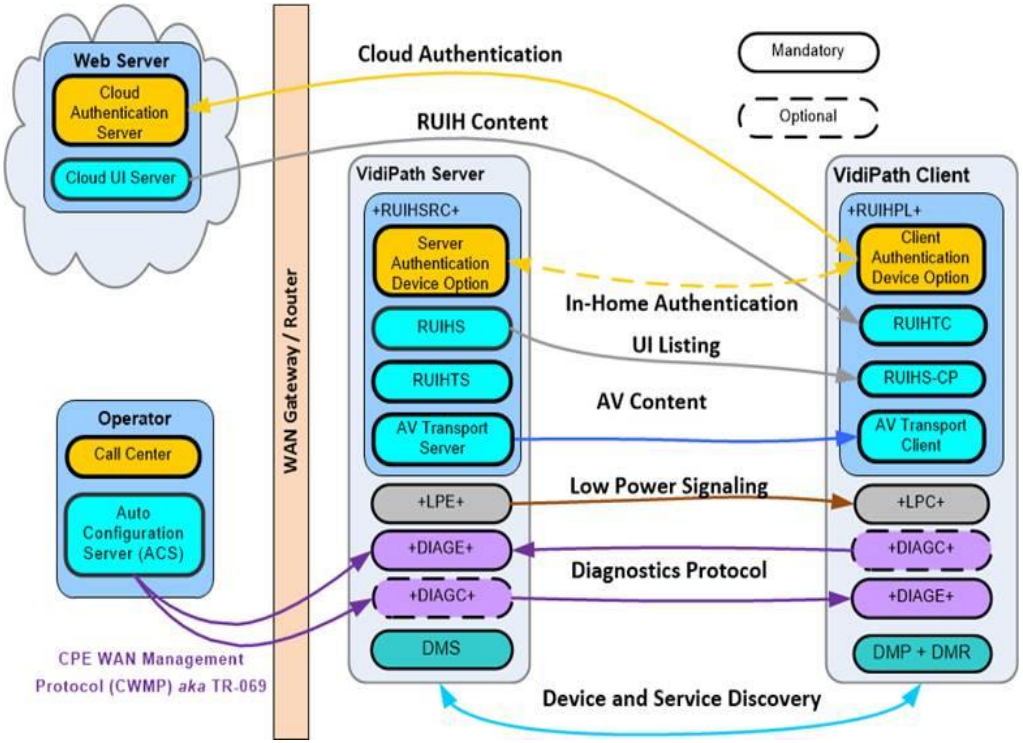


Figure-9: Hybrid In-home + Cloud Deployment

In the In-home only deployment scenario, the MVPD's HTML5 RUI server and Authentication Server reside in the in-home gateway/STB along with all other VidiPath Server functions. A VidiPath Client discovers URL of the MVPD's guide from an in-home VidiPath gateway/STB, which is served from within the home from the same gateway/STB. The same gateway/STB also hosts the Authentication Server.

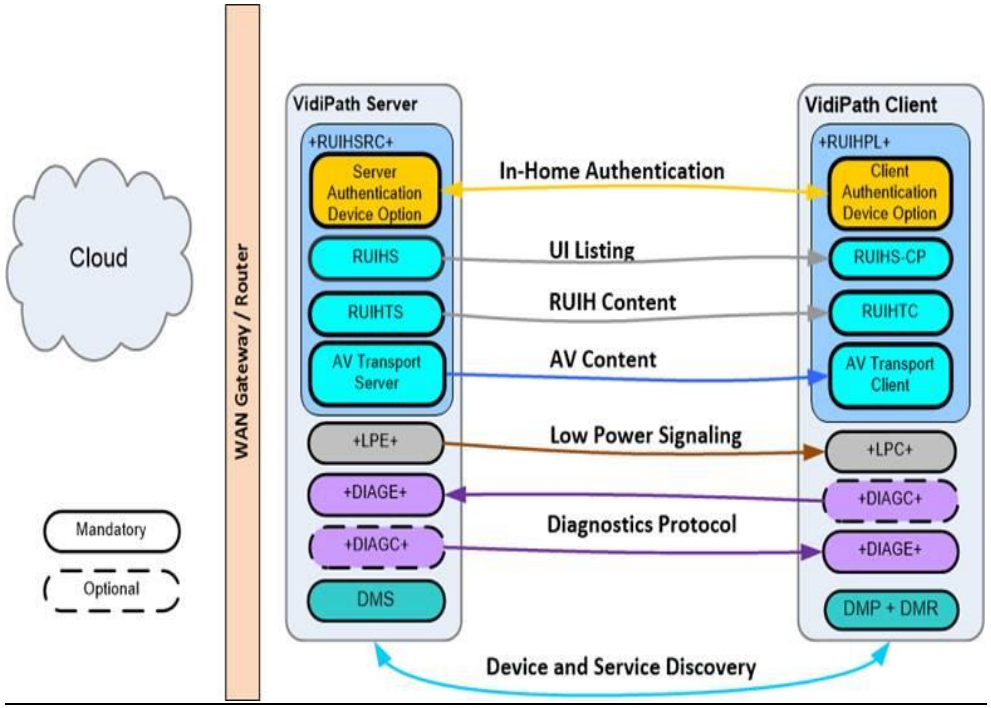


Figure-10: In-home only Deployment

The VidiPath Client is authenticated with the in-home Authentication Server (the server uses self- signed or trusted X.509 certificate signed with VidiPath certificate). Upon authentication, the VidiPath Client downloads MVPD HTML5 guide to access content services from the in-home gateway/STB VidiPath Server.

CableLabs, in partnership with industry participants such as Intel and ARM, has developed open source implementations of VidiPath Server and Client [4]. These implementations are aligned with libraries used by Reference Device Kit (RDK), an integrated software platform initiative for MVPD customer premise equipment (CPE) led by major MVPDs in the U.S. and Europe [5]. The main objectives for the VidiPath open source implementation efforts are as follows:

- Provide reference devices to DLNA to help launch VidiPath certification program
- Provide reference devices to the industry for testing and development of VidiPath products
- Foster VidiPath adoption and speed time to market

The VidiPath specifications enable consumers to consume premium subscription TV content on devices of their choice with a consistent user experience across all devices. Using VidiPath HTML5 RUI, service providers are able to evolve their services more rapidly and reduce time-to-market for new services and products. The auto service discovery feature supported by VidiPath facilitates easy installation and setup, which is a benefit to both consumers and service providers. The Diagnostics feature allows service providers to remotely diagnose and troubleshoot any service related issues.

VidiPath authentication provides assurance to service providers and content providers that only certified VidiPath devices access their services and provides assurance for their user experience on retail devices. VidiPath offers a single, interoperable solution to retail device manufacturers to enable premium subscription TV services from different service providers.

A. Standards

[2] DLNA CVP-2 Press Release, March 18, 2014, http://www.dlna.org/docs/default-source/press-releases/the-digital-living-network-alliance-releases-cvp-2-guidelines-for-viewing-subscription-tv-content-on-multiple-home-devices.pdf?sfvrsn=4

[3] DLNA Guidelines, http://www.dlna.org/dlna-for-industry/technical-overview/guidelines

[4] Open Source Implementations of CVP-2 Server and Client, CableLabs, http://html5.cablelabs.com/dlna-cvp-2/index.html

[5] Reference Device Kit, http://rdkcentral.com

[6] HTML5, A vocabulary and associated APIs for HTML and XHTML, W3C Candidate Recommendation 04 February 2014, http://www.w3.org/TR/2014/CR-html5-20140204/

[7] RemoteUIServer:1 Service Template Version 1.01, For UPnP™ Version 1.0, September, 2, 2004, http://upnp.org/specs/rui/UPnP-rui-RemoteUIServer-v1-Service.pdf

[8] Mapping from MPEG-2 Transport to HTML5, I03, CL-SP-HTML5-MAP-I03-140207, Cable Television Laboratories, Inc. Specifications, Web Technology, February, 7, 2014

[9] Server Sent Events, W3C Candidate Recommendation, 11 December 2012, http://www.w3.org/TR/eventsource/

[10] DTCP Volume 1 Supplement E, Mapping DTCP to IP, Revision 1.4 ED3, June 5, 2013, Digital Transmission License Administrator, http://www.dtcp.com/documents/dtcp/info-20130605-dtcp-v1se-ip-rev-1-4-ed3.pdf

[11] UPnP Device Management: 2, http://upnp.org/specs/dm/dm2/

[12] IEEE 1905.1, IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies, 2013, http://standards.ieee.org/findstds/standard/1905.1-2013.html

[13] BasicManagement:2, Service Template Version 1.01, For UPnP™ Version 1.0, February 16th, 2012, http://upnp.org/specs/dm/UPnP-dm-BasicManagement-v2-Service.pdf

[14] ConfigurationManagement:2, Service Template Version 1.01, For UPnP™ Version 1.0, March 4th, 2013,http://upnp.org/specs/dm/UPnP-dm-ConfigurationManagement-v2-Service.pdf

[15] EnergyManagement:1, Service Template Version 1.01, For UPnP™ Version 1.0, August 30, 2013, http://upnp.org/specs/lp/UPnP-lp-EnergyManagement-v1-Service.pdf

[16] ISO/IEC 23009-1:2012, Information technology -- Dynamic adaptive streaming over HTTP (DASH) -- Part 1: Media presentation description and segment formats, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=57623

[17] S. Santesson, TLS Handshake Message for Supplemental Data, IETF RFC 4680, September 2006, http://tools.ietf.org/html/rfc4680

[18] T. Dierks, et al, The Transport Layer Security (TLS) Protocol, Version 1.2, IETF RFC 5246, August 2008, http://tools.ietf.org/html/rfc5246

[19] Gnome's Rygel Project, https://wiki.gnome.org/action/show/Projects/Rygel?action=show&redirect=Rygel

[20] dLeyna Project, Intel Open Source Technology Center, https://01.org/dleyna

[21] The WebKit Open Source Project, http://www.webkit.org

[22] The GTK+ Project, http://www.gtk.org

[23] GStreamer, Open Source Multimedia Framework, http://gstreamer.freedesktop.org

[24] The Open SSL Project, https://www.openssl.org

B. Protocols

The protocols used include:

- UPnP
- TCP/IP
- HTTP
- HTTPS
- MPEG DASH

C. Information

The DLNA VidiPath Guidelines can be obtained at: DLNA Guidelines, http://www.dlna.org/dlna-for-industry/technical-overview/guidelines

D. Applicable Devices

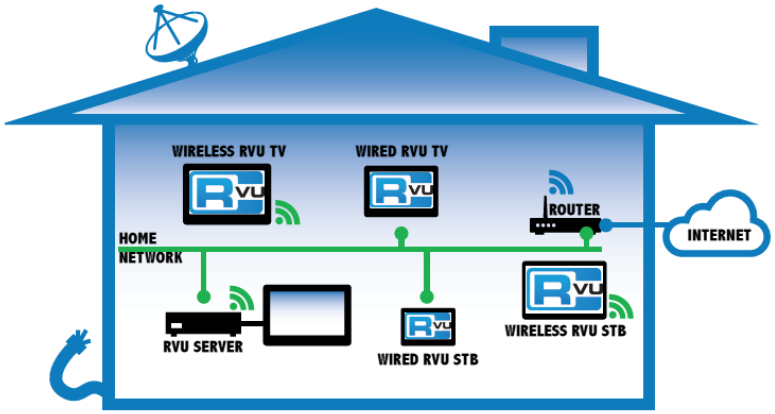
Any DLNA VidiPath certified device including: smart/connected TVs, game consoles, PCs, tablets, and smart phones.

IV. RVU™

The RVU protocol is available to consumer electronics (CE) manufacturers via the RVU Protocol Specification. RVU is based on open standards such as UPnP to simplify software integration and enable cost effective solutions that CE manufacturers can leverage to create RVU clients such as TVs.

RVU eases the provision of home networked commercial entertainment content while heightening the user experience. Viewers can access either pre-recorded or live content, premium content such as high definition or ultra-high definition video and multi-channel audio, or personal content such as photos and videos via the media server. RVU supports a novel process-light remote user interface that allows user interactions such as trick play (e.g., pause and rewind) and the running of interactive applications.

In addition to a full featured remote user interface that allows the user of a connect client device to navigate through user screens generated by a compatible RVU server, RVU technology provides Internet Protocol (IP) connectivity, service discovery built from UPnP and DLNA protocols, a remote commanding protocol, and industry standard media formats protected by DTCP-IP content protection.



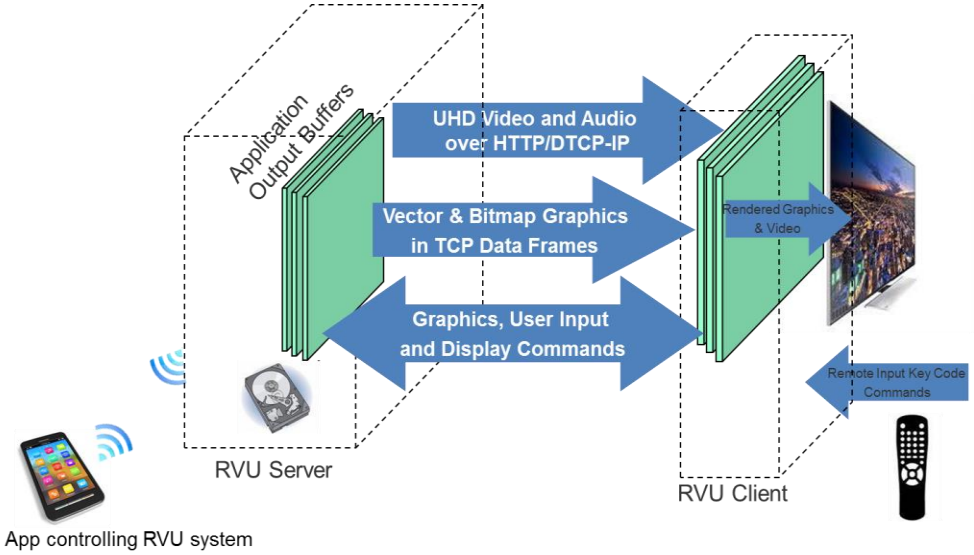
A. Standards

The RVU protocol specification is built upon UPnP device discovery, DLNA media streaming and DTCP-IP content protection.

B. Protocols

The RVU remote user interface (RUI) protocol complements devices implementing content streaming protocols of the DLNA guidelines. The concept of a remote user interface for clients is not new. However, the idea that clients should be able to provide a full-featured user interface by implementing minimal functionality, leaving most of the “hard work” to the server, is unique to RVU. The objective of RVU is to keep clients as process-light as possible. The RVU RUI delivers bitmapped and/or vector graphic user interface data for a robust, consistent UI experience throughout the home via thin clients as opposed to implementations with an entire UI via client-side

software. Clients implement relatively simple software to send key events to the server and display the RUI graphics and video/audio received in response.



C. Information

The Version 1.0 RVU Specification has been publically available since Fall 2009, Version 2.0 since Fall 2012, and a comprehensive certification program has been in place since Spring 2011. RVU is implemented on a wide variety of technology platforms, and has won awards at major trade shows and conferences around the world. RVU devices have been fielded to consumers nationwide since Fall 2012, in the form of 9 million DIRECTV Genie branded servers and several times the number of servers in Genie branded clients as well as RVU-certified Smart TVs from Samsung, Sony, LG and Toshiba. 4K/UHD services became available on RVU servers and Smart TVs from Samsung during 4Q/2014.

The RVU Alliance is a non-profit technology standards alliance comprised of service providers, consumer electronics manufacturers and technology providers to develop and maintain the RVU protocol specification for a small footprint full-featured Remote User Interface (RUI). Board level promoter members include Broadcom, Cisco, DIRECTV, Samsung and MaxLinear. Other members are LG, Sony, Toshiba, Sharp Electronics, Dolby Laboratories, Humax, JetHead Development Inc, Awox, MStar, Pace PLC, Sky Brasil, ST Microelectronics, Arris and Technicolor.

D. Applicable Devices

For a list of certified devices, including 4K/UHD clients, see www.rvualliance.org/products.

V. Virtual Joey

A. Standards

B. Protocols

C. Information

D. Applicable Devices

VI. Sling Box Client

A. Standards

B. Protocols

C. Information

D. Applicable Devices

VII. Use Cases Supported

Unlike CableCARD, which was designed only for reception of linear cable channels from digital cable systems for reception on cable-specific UDCP devices, applications are platform and technology neutral, allowing retail devices to operate across MVPD and OTT platforms, and support linear, on-demand, interactive, and other advanced features of the MVPD service, while respecting the usage limitations associated with licensed copyrighted content.

A. Tuning and Viewing a Linear Channel

The apps models abstract the transmission methods for the MVPD's network and deliver the service in IP, using the audio and video codecs and the picture resolutions and formats supported by the retail device. The robustness and capabilities of the App platform may affect what content is available to devices that are supported by the App platform. The application also handles any concurrent stream management required by the network or content agreements. The application supports any applicable switched digital video.

The application tunes the channel and presents integrated applications associated with the tuned channel, such as camera angles, as well as subscription applications such as sports statistics, interactive advertising, and caller ID on TV.

The application also presents the broadcast, zoned or targeted advertising inserted into the linear channel. Interactive request for information and telescoping ads are supported. All requirements for acceptable advertising, ad boundaries, ad lifecycle management, audience measurement, ad measurement and reporting are supported.

The application supports blackouts, geo-filtering and geo-fencing, alternate content, messaging and redirection for unauthorized channels, and parental control. The application manages copy controls and output restrictions.

The application supports trick play capability.

The application supports the network's technology to reduce channel change latency.

The application supports all regulatory requirements, including delivery of EAS and statutory privacy requirements.

B. On-Demand Content

In addition to supporting linear content and features, applications support transaction, subscription, and free VOD; EST; Start Over and Look Back. They also meet advertising requirements as required by content providers who license the content and advertisers who fund the dual-revenue MVPD business, e.g., dynamically inserting pre-roll advertising or disabling fast forward during advertisements included with VOD content.

C. Pay Per View (PPV) events

Applications also support PPV requirements such as free preview, purchase and cancellation windows, secure purchase credits and purchase limits.

D. Navigation

Apps use a UI designed by the MVPD for interacting with the MSO's experience. Consumers receive a common, familiar MVPD experience across devices, such as the ability to navigate and see recent tuning history regardless of which device was used. This is similar to how consumers experience Netflix and other OTT video services. Retail devices that host the application may continue to differentiate themselves with features, functions, networks, drives, speed, look, feel and price, and may have their own top level user interface, app store, and menu structure. This is consistent with the approach used by OTT video providers and with public pronouncements by Thomas Riedl, head of Google's Android TV, *"Content owners and distributors are one of the key stakeholders for us. For them, what's crucial is they want to deliver the best user experience and make sure that the content they provide to the user is displayed exactly as they broadcast it. Also in their role as app developer, they need to be able to completely control the experience. Android TV allows them to do all of these things based on our proven technology platform." IPTV News 4/21/15, http://www.iptv-news.com/2015/04/google-google-tv-has-evolved-into-android-tv/.*

Apps present the modern features of MVPD navigation, such as mosaics, recommendations from what's trending or popular in the neighborhood, view by genre, and recommendations from a user profile across devices. DLNA Vidipath offers the ability to navigate to and discover content or services on the home network.

Apps enforce content license requirements from content providers, including channel presentation in required neighborhoods (e.g., news channels) and channel assignments (e.g., broadcaster carriage on channel); channel logos; and search requirements (such as a network-branded point of entry)

There is no standard feature for a retail device to conduct deep search from outside of the MVPD app, just as YouTube no longer enables deep linking that bypasses the YouTube UI and experience, and Facebook and Twitter apps do not automatically enable deep search by web browsers. However, marketplace search deals can be done by mutual agreement, as Twitter agreed to do with Google and Netflix agreed to do with TiVo. Requiring negotiation is an established means for assuring that the "search" does not artificially raise or suppress rankings in search results. There are also opportunities for business-to-business deals for new user interfaces. For example, Xbox One uses a UI that was designed to be familiar to TWC subscribers and to Xbox users. It also integrates MSFT connect voice and gesture control. Likewise, TWC built a grid guide for Roku.

E. Recording Linear Content

The DLNA VidiPath spec provides a recordable DTCP-IP output, so that a retail DVR can record programming received by VidiPath. DLNA continues to evolve, and may augment this in the future.

Content providers generally do not (yet) permit apps on mobile devices to provide a recordable output. Similarly, Netflix does not present a recordable output to CE devices. Apps to Smart TVs may present recordable outputs. Content providers licensing terms may continue to evolve, and downloadable Apps//DRMs can be updated accordingly.

F. Remote Management by Consumer

Apps for the Smart TV and other devices enable consumers to change channels and manage their account via a network-connected mobile device. Such apps also allow consumers to manage their caption settings and other accessibility features and select their language through the mobile device.

G. Set-Top Box set-up

Apps for the Smart TV support establishing menu preferences, device settings, parental controls and accessibility.

H. Customer Support and Remote Management by Service Provider

Apps permit the service provider to troubleshoot and support device experiences.

As a common cross-platform MVPD experience is delivered across all retail devices via the MVPD App, MVPDs are able to offer better and consistent support and diagnostics to consumers.

I. Cloud Delivery

By using applications with popular device platforms, MVPDs can make VOD, live linear, recorded content, and download-to-go content available to customer-owned devices on a cloud-delivered basis, as permitted by content and distribution rights.

Part III: Section III. Implementation Analysis

Scott:

How the pieces from the other sections are tied together … whether done in Section I & II individually … or tied together here

Everything is discussed including device authorization

Note: Evaluation of burden might also appear in Part II

Section is both evaluation of burden and analysis of implementation on legacy devices for the systems described above in this part.

System 1

Implementation Details

Legacy Device Implementation

Evaluation of Burden