Network Support Infrastructure For Pod-Based Systems

Mark DePietro
Motorola Broadband Communications Sector

Abstract

The FCC Report and Order of June 1998 called for the availability of retail navigation devices and PODs in the July 2000 timeframe. In order to enable a set of services in a POD-based set top or digital TV, it is necessary to consider corresponding changes that must be made to the supporting digital network infrastructure. This paper examines those changes in the context of the feature set that has been defined by the OpenCable process for July of 2000. In addition, other system level considerations that affect the success of OpenCable systems are discussed.

BACKGROUND

In order to be able to declare that PODs and Hosts have been successfully deployed, it is necessary to establish criteria by which to measure success. In the OpenCable process, success has been defined as the ability of the entire system, consisting of Headend, POD, and Host, to exhibit a set of behaviors identified as the J2K Feature set. In this context, J2K stands for "July 2000."

J2K Feature Set

The following elements comprise the feature set associated with the J2K rollout of PODs. This feature set was derived as a result of OpenCable discussions that took place in the summer and fall of 1999.

- Clear Analog Services
- Clear Digital Services
- Subscription Digital Services
- Call Ahead Pay Per View
- Impulse Pay Per View
- Support for HDTV Passthrough via 1394
- Copy Protection on the 1394 Interface
- Copy Protection on the POD-Host Interface
- System Information in Accordance with DVS-234 Profile 1
- Emergency Alerts Based on DVS-208
- Closed Captions Based on DVS-157 and DVS-053
- Parental Control Supported by Content Advisories in the PMT
- Electronic Program Guides

Multiple Deployment Scenarios

Three distinct POD/Host deployment scenarios have been identified to date. In the ***Native Network*** scenario, the Host manufacturer and the POD manufacturer coincide. In the ***Foreign Network*** scenario, the Host manufacturer and the POD manufacturer differ. Finally, in the ***POD-less Host*** scenario, a Host is deployed without a corresponding POD.

Each scenario enables completion of a different range of features in the overall feature set. The POD-less Host scenario enables the smallest set of features for obvious reasons. Without a POD, the Host has no access to the out-of-band data feed, nor does it have access to encrypted channels. As a result, a PODless host can not access anything

other than clear analog and clear digital services.

Code Download and Foreign Network Constraints

In the foreign network scenario, the POD and Host are from different manufacturers. Because code download was not part of the J2K feature list, Hosts are generally not able to participate in code download operations in foreign networks. Since hosts are sold at retail, they can not be assumed to possess an electronic program guide that is suitable for use in the subscriber's cable system. This is true because retailers typically serve consumers whose dwelling locations span multiple MSO service areas, and it is not practical for a manufacturer to pre-load every conceivable EPG into a host. If suitable business relationships between the Host manufacturer, retailer, and MSO have been established, it is possible to envision a solution to this problem wherein the retailer performs the service of downloading an EPG into the Host on behalf of the other two parties.

Alternatively, the manufacturer may establish a private mechanism to obtain EPG downloads and data feeds that bypasses the MSO (e.g., through a manufacturer-specific telephone dialup service). Because these solutions are beyond the scope of OpenCable, they are not considered further. Other features that rely on the existence of either a download mechanism, either directly or indirectly, are not available in the foreign network scenario for J2K.

In the remainder of this paper, all features being described should be assumed as required in both the native network and foreign network scenarios, unless explicitly stated otherwise.

SYSTEM LEVEL IMPACT ANALYSIS

There are 5 specific features in the J2K Feature set that drive a need for systemwide changes. these features, and the required system changes to support them, are described below.

COPY PROTECTION

The design of the copy protection system for OpenCable has had significant systemwide development impacts. This section describes the reason why copy protection is needed in the system, and discusses the related issues of certificates, certificate revocation lists, content tagging, and ultimate limitations of any copy protection solution.

The Need for Copy Protection

One side effect of partitioning a set top into Host and POD is the creation of an easily accessible interface over which all inband content flows. In the absence of a copy protection scheme, this provides an easy point of attack for pirates wishing to make unauthorized digital copies. To remove this deficiency, it is necessary to encrypt the interface between the POD and the Host. This requires the selection of:

(1) An encryption algorithm, and
(2) A key management scheme

If both of these selections are completely known in the public domain, the resulting solution strength is ultimately equivalent to having a clear interface. To avoid this weakness, it is useful to introduce a set of secrets that are known a-priori only to legitimate Hosts and PODs. This introduces the need for a secret access-granting authority. CableLabs plays this role with respect to POD-Host interface encryption system

parameters. Finally, even with the existence of such an authority, it is not wise to assume that these secrets will be maintained (as evidenced by the various DVD breaches that have emerged). Thus, it is also desirable to have in place an intellectual property barrier whose violation can be used as the basis for litigation against an interface attacker. The use of DFAST in the key generation process plays this role in the POD-Host interface, and CableLabs administers access to the DFAST intellectual property.

The Role of Certificates

By putting encryption and key management in place across the POD Host interface, attacks mounted by third parties against the interface are effectively thwarted. However, this level of protection was not considered adequate during the OpenCable requirements analysis phase. It was also desirable to know ahead of time that Hosts would not make inappropriate use of content once it traverses the interface from the POD. To receive assurances in this area, the Host is required to possess a certificate that ensures it will behave as a "good citizen" with respect to handling of high value content. Furthermore, the POD is required to: (a) validate the authenticity of the Host certificate, and (b) report the results of the authenticity check (in a non-spoofable fashion) back to an entity in the control system. The control system receives the authenticity verification from the POD, and compares the Host ID against a list of known bad hosts - the so-called ***Certificate Revocation List*** (CRL). If the germane Host ID is not present on the CRL, the Host is considered to be well behaved with respect to protection of high value content. As a result, the control system sends a "Host Validation" message to the POD. The Host Validation message is protected by a digital signature to prevent spoofing attacks. Until the POD receives a Host validation message from the control system, it will not decrypt any content that has been tagged as "high value."

Tagging Content in the Control System

To complete the copy protection solution, it is necessary to have a facility in the system that provides a distinction between low value content and high value content. In the OpenCable solution, a data element known as Copy Control Information (CCI) plays this role. Four values of CCI have been defined to date. ***Copy Freely*** content requires no protection. The other three values, ***Copy Once***, ***Copy Never***, and ***No Further Copying***, all require protection in the form of POD-Host interface encryption. The CCI value "No Further Copying Permitted" is typically a source of confusion. This particular CCI value is only used as a designation on second generation material where the ancestral content was tagged as "Copy Once".

In addition to tagging content, cable operators participating in the OpenCable process wanted to put in place an infrastructure that enabled price differentiated purchase opportunities for a single item of content. As an example, suppose an item was marked "Copy Freely". The OpenCable participants wanted to have a way to offer the content for purchase at two different prices. At the lower price, the content would appear to have a more restrictive "Copy Never" tag from the perspective of the Host. At the higher price, the content would appear to have the less restrictive "Copy Freely" tag, again from the perspective of the Host. In order to provide this capability in the system, each individual POD needs to have the capability to present a different tag to the Host based on criteria associated with the mode of purchase. As a result, the access control system was required to be involved in the CCI delivery chain. This caused a ripple effect back to the Billing systems, because these systems act as

the point of entry for pay per view schedule data into cable access control systems. The ripple effect also extends to the Electronic Program Guide (EPG) providers, who will need to develop user interface screens that are capable of presenting the purchase options to the subscriber.

Advanced Tagging

For J2K, the four values of CCI defined above will be implemented. However, during OpenCable discussions, more esoteric forms of CCI were also considered and ultimately rejected for the J2K timeframe. Given the recent popularity of Personal Video Recorder systems, it is possible to envision a need to tag content with respect to even ephemeral copying that is required to support functions such as program pause and time-shifted viewing. This class of tagging has been considered in ATSC, and there are proposals on the table that extend CCI to include values such as "Pause No More", "Copy with a 15 Minute Lifetime", etc. These extended forms of CCI may be required in a later version of OpenCable, and are likely to have systemwide requirements ripples similar in nature to those induced by the current set of defined CCI values.

Choosing Content to Protect

It should be noted that the current copy protection system provides protection primarily for the content owner. During the course of the development of the OpenCable copy protection specification, there was a fair amount of discussion surrounding the choice of content that should be encrypted over the POD-Host interface. To protect against a re-distribution attack on the conditional access system, it would be necessary to encrypt content on the POD-Host interface whenever the content is encrypted as it traverses the HFC system. In addition, if a conditional access system employs a very long crypto-period, it is possible to use the clear content on the POD-Host interface as a point for mounting a plaintext/ciphertext attack on the CA system. Both re-distribution attacks and plaintext/ciphertext attacks were considered to be beyond the scope of the envisioned threat model. As a result, content is only encrypted over the POD-Host interface when it has been tagged as "high value", meaning that the CCI value is not set to "Copy Freely."

Other Copy Protection Considerations

It should be noted that the above described copy protection system provides protection against a pirate who wishes to make pristine first-generation digital copies of content. Digital copies of good quality can still be obtained by making a camera-based copy of a television image, by taking an analog output and digitizing it, etc. It should also be noted that in order for "bad hosts" to be shut down, it is necessary to place the hosts on the CRL. The current copy protection system provides no watermarking feature. As a result, there is no defined facility in the copy protection system that could be used to ascertain the point of origin of content that is discovered to be pirated. Thus, the creation and maintenance of the CRL will require the existence of an administrative process that is based on an approximate audit trail.

Summary of Copy Protection System Impacts

As a result of the considerations noted above, it is necessary to modify existing conditional access systems and interfaces, billing systems, and electronic program guides to support the OpenCable copy protection solution. In addition, it is necessary to implement the administrative processes that will be used to govern the content of Certificate Revocation Lists.

SYSTEM INFORMATION

One of the key elements required to support Hosts from a variety of manufacturers is a uniform facility for communicating channel lineups that are active in the system. In today's digital systems, channel lineups are typically communicated out-of-band in a data structure known as the ***Virtual Channel Map*** (VCM). The VCM is a logical view of the channel lineup that allows a subscriber to maintain a constant interpretation of channel map even when there is variation in the underlying physical channel lineup.

In digital systems from different vendors, these VCMs are often transported in non-uniform ways. For example, some systems use MPEG transport on the out-of-band, while others use ATM transport. In addition, some systems support multiple channel maps within the context of a single hub while others employ one channel map per hub. In OpenCable, it was necessary to hide these intersystem differences from the Hosts in order to avoid unnecessary complexity in Host out-of-band processing firmware. The POD plays a crucial role in hiding these inter-system differences from the Host. It strips off the transport headers that are used in a particular system, and accumulates sections of the VCM for delivery to Host. It also filters out any VCMs that are not relevant to the Host, giving the Host the illusion that it is operating in an single VCM environment. So, in addition to being the security element in the system, the POD also plays a key role in supporting the delivery of System Information in a uniform fashion.

EMERGENCY ALERTS

In currently deployed digital systems, different methods are used by different vendors to denote the occurrence of an emergency condition and to provide the cable subscriber with needed emergency information. Often, the solution involves the generation of a proprietary message on the OOB that redirects the set top's tuner to an analog station that is carrying the emergency information. When the emergency condition terminates, the set top is returned to the previously tuned channel. In OpenCable systems, the use of private mechanisms to communicate emergency conditions is not acceptable. As a result, it was necessary to develop a common emergency alert mechanism that relied on public domain messages. SCTE DVS-208 was developed to fulfill this role. For OpenCable Systems, it will be necessary to carry DVS-208 messages in addition to any existing private messages that might currently be in use. This requires an upgrade to each headend that normally takes the form of a firmware download to one or more headend components.

CLOSED CAPTIONS

In today's digital systems, two closely related but different methods are used to carry closed caption data in digital streams. One method is based on DVS-157; the other is based on DVS-053. In some deployed hosts, there are hardware constraints that require DVS-157 to be present in order for closed captions to operate. As a result, in OpenCable, it will be necessary to dual carry DVS-157 and DVS-053 forms of closed captions, and it will be necessary for OpenCable Host devices to be prepared to process both forms. The Hosts are required to support both forms in order to facilitate any transition periods that may exist during which only one form of CC data is present in the system. To support dual carriage of DVS-157 and DVS-053, currently fielded encoder systems will need to be upgraded.

RATINGS AND PARENTAL CONTROL

In current systems, program ratings information is typically carried in the Electronic Program Guide data feed using proprietary data formats. In addition, parental control functions used to block access to undesirable programming are facilitated via the EPG. In OpenCable, it could not be assumed that any given EPG data feed would be present on all systems, nor was it desirable to mandate the presence of a single EPG. At the same time, it was considered essential to provide a uniform, public ratings conveyance mechanism, in part to achieve compliance with FCC rules related to V-Chip functionality in the digital domain.

In the OpenCable process, it was decided that ratings information will be carried with the content itself, and will be captured at the point of content encoding. The ratings information will be carried in the MPEG program map table (the PMT), using a ratings descriptor that is congruent with the one defined in EIA-766. OpenCable Hosts are required to monitor incoming PMTs, and must take appropriate actions (e.g., blank video and mute audio) whenever incoming content has ratings that violate established parental control constraints. Hosts must take these actions within 200 milliseconds.

PMT Version Change Considerations

As a result of these requirements, MPEG PMTs will undergo a version change at every program boundary to signify the presence of a new ratings descriptor. These PMTs are typically transmitted very frequently, on the order of 10 times per second in each multiplex, in order to facilitate rapid channel acquisition. Once a channel has been acquired, it is *usually* not necessary to examine the PMT again until a channel change operation occurs, since PMTs tend to be relatively static objects. Nevertheless, PMTs can change and when they do in current systems, they typically signify the occurrence of a disruptive change to the underlying PID structure of the transport multiplex. Thus, in most systems, when the PMT changes, set top firmware initiates a program re-acquisition cycle. In the future, when ratings information is carried in the PMT, a version change in the PMT will now most likely not signify a disruptive change to the PID structure.

As a result, it will be mandatory to rethink the logic used to respond to PMT changes, and put in place an ***Advanced PMT Monitor*** (APM). The APM will be responsible for analyzing the details of changes to an incoming PMT, and will need to avoid a reacquisition cycle when the PMT is only used to identify a ratings transition point.

Headend Remultiplexing Considerations

Set top firmware and encoder systems are not the only elements that are affected by a requirement to carry ratings information in the PMT. Every headend is also affected in some way, particularly when the headend supports remultiplexing operations. Whenever an MPEG remultiplexing operation occurs, it is necessary to tear down any incoming PMTs and reconstruct the new PMT to ensure consistency with the newly formed multiplex. In current systems, this normally means that pointers to video, audio, and data PIDs must be changed to complement any PID remapping that is occurring in the multiplex. However, with the addition of ratings information to the PMT, pointer preservation will not be adequate. It will also be necessary to preserve and re-insert incoming ratings descriptors. Thus, every deployed digital cable headend will need to be modified to support PMT ratings descriptor preservation functions.

ELECTRONIC PROGRAM GUIDES

For J2K, there will not be a single EPG that spans all systems. In addition, there is no OpenCable code download mechanism defined for J2K. As a result, EPG capabilities will exist only in the native network scenarios. Over the longer term, the cable industry and CEA have agreed that a certain base level of EPG data will be carried in the system in the form of inband PSIP. This, along with a future code download mechanism, will allow for future portability of EPGs.

OTHER SYSTEM LEVEL CONSIDERATIONS

In addition to the J2K feature list, it is worthwhile to consider some factors that will play a part in defining the evolution of OpenCable systems. Four relevant factors are briefly considered in the following sections.

Heterogeneity Of Security Features

Different conditional access systems have different features that present different experiences and system capabilities to the user. Examples of areas where CA systems differ include, but are not limited to:

(1) The quantity and nature of entitlements differ from system to system. In some systems, entitlements are conferred via service keys, in others the tier concept is used. Many other mechanisms are possible, and likely to exist.
(2) The method used to implement the concept of money differs from system to system. In some systems , there is no monetary concept. In other systems, a credit mechanism is used. In other systems, time is the element that equates to money.
(3) Some systems implement concepts such as free previews, program packages, and blackout areas, while others do not.

Given the existence of these differences, the following alternatives existed with respect to the interface between the host module and the security module:

(1) Account for the lowest common denominator features in the Host to POD functional interface.
(2) Define the interface to include all capabilities that could be encountered in any CA system, and use a profiling mechanism to identify differing levels of support.
(3) Define a very low-level host module to security module interface, and then require the existence of security module specific "driver firmware" to exist on the host device.

In OpenCable, a combination of alternatives (1) and (2) was chosen. As a result, applications developed for OpenCable will need to be aware of the existence of various security profiles, and will need to be designed "defensively" so that the lack of a particular feature in a given system can be recovered from in a graceful manner.

Firmware Distribution and Host Configuration Identification

In current digital systems, there is a primary vendor that provides both headend and set top equipment. Firmware destined for a particular population of set tops is distributed directly by the manufacturer to the MSO's site, often through the use of a field engineering organization. This direct distribution model does not scale well in an multi-host vendor to multi-MSO environment. Ultimately, there will be a need for a multi-hop distribution channel in which an

intermediate business entity facilitates the many-to-many distribution operations.

In addition, each delivered firmware object will be relevant to only a selected subset of Hosts in a given system. This is true even in the presence of a defined OpenCable middleware solution for the following reasons:

(1) The middleware engine implementation will be host specific.
(2) The middleware solution itself will be an object that is subject to evolution. Eventually, capability profiling or discrete forms of a middleware application will need to exist to distinguish between capability sets resident in different classes of Hosts.

As a result, there will ultimately be a need to have a Host configuration identification mechanism that spans multiple vendors. A two-tiered identification scheme, based on an organizationally unique identifier (OUI), makes the most sense. Some entity such as CableLabs will need to emerge as the OUI administrator.

Compatibility Matrix Generation and Maintenance

In current systems, features are added to deployed systems by making synchronized complementary changes to the headend and set top populations. The configuration management discipline of ***Compatibility Matrix*** generation is used to record information that defines version sets of various system elements that are known to operate properly together. In OpenCable systems, this discipline will become more important, since the number of different system elements that must be coordinated will increase. Some economic model must be developed to support large multi-vendor compatibility matrix generation efforts.

System Level Troubleshooting

In single vendor systems, or systems wherein a small number of vendors are involved, the locus of responsibility for performing system level troubleshooting is narrowly defined. In OpenCable systems, where multiple vendors supply PODs and Hosts, and where subscribers have a business relationship with both a retailer and an MSO, it is not at all clear what system level troubleshooting model or models will exist in order to ensure subscriber satisfaction. The emergence of clear, explicit models must occur in order to avoid customer confusion and dissatisfaction that would likely result otherwise.

CONCLUSIONS

This paper has examined the system level changes that are needed to support POD based systems. Significant progress has been made by the OpenCable community to ensure that systems will be ready to support PODs in the July 2000 timeframe. Additional work will be required to support portability of a compelling feature set.