



Introduction to CableCARD™: History, Technology, Applications and Future

Craig Gwydir
Principal Architect
BitRouter

What is a CableCARD?

A special purpose PCMCIA card



Source: CableCARD Wikipedia



What does a CableCARD do?

Navigation and Security

- **Navigation** – Provides the ability to view and record digital and analog cable channels without the use of a cable settop box.
- **Security** – Provides the ability to view and record “premium” (encrypted) digital cable channels.



CableCARD and Host

- A “Host” generally refers to a television or a Digital Video Recorder (DVR) that can accept a CableCARD.
- A CableCARD plugs into a “Host.”
- Provides direct connection to cable system using a CableCARD – Digital Cable Ready.

Digital Cable Ready (DCR) Host



Source: Panasonic

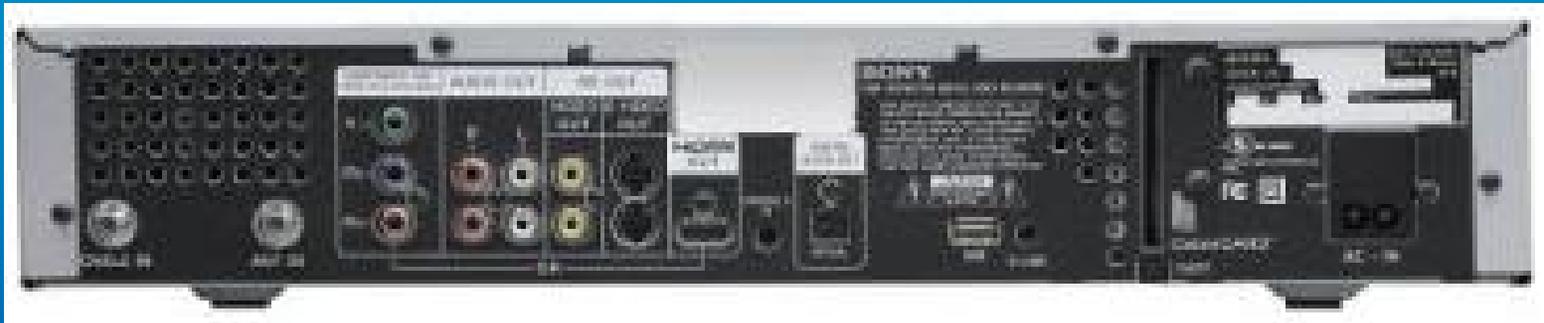
Digital Cable Ready Host - DVR

SONY DHG CableCARD(tm) HD DVR series

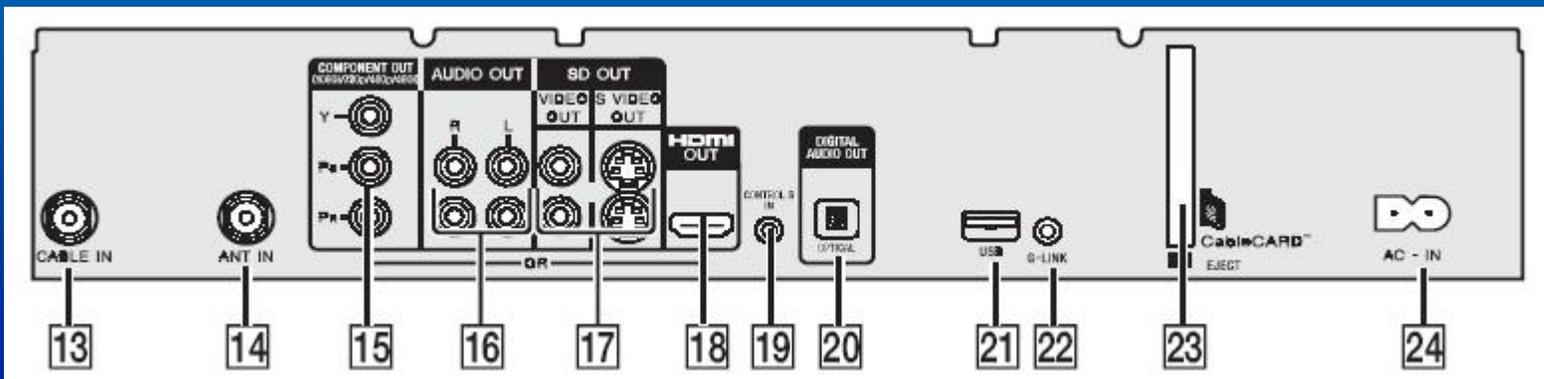


Source: Sony

SONY CableCARD DVR – Back Panel



Source: Sony



Source: Sony

Why do we have CableCARDs?

To open the market, allowing consumer electronic companies to produce and sell navigation devices for digital cable networks via retail channels.

Navigation devices include:

- Digital Video Recorders (DVRs)
- Digital Cable Ready TVs (DCR)
- Third party set-top boxes
- TIVO Series 3



Question...

Question: Has CableCARD technology enabled this open market of digital cable-ready consumer electronics devices via retail channels?



The answer is in the numbers..

The good news: As of June 15, 2007, some 271,000 CableCARDs have been deployed by cable operators.

The bad news: There are over 65 million basic cable subscribers.

Answer: CableCARDs have not done much to open the market for digital cable-ready CE devices via retail channels.



A Bit of History...

Telecommunications Act of 1996 (Section 304)

- Initiated by Congress
- Allowed non-cable company devices to access cable networks
- Provided wider number of choices for consumers in choosing consumer electronics devices for cable (and satellite) networks
- Analogous to Carterfone ruling allowing consumers to purchase third-party telephones to attach to telephone networks
- Resulted in the creation of CableCARDs

More History...

FCC – Federal Communications Commission

- Charged with working in concert with the cable industry to carry out and enforce the 1996 law
- “Integration Ban” – Create regulations to separate security and navigation within access devices—original deadline was July 1, 2000
- First reference to “POD” – Point of Deployment Module



A Massive Effort...

- NCTA – represented cable companies
- CEA – represented consumer electronics companies

Differing goals – various standards created

Development handed to CableLabs – R&D arm of cable companies

The result – a massive engineering effort to create the POD (Point of Deployment Module, or CableCARD)



CableCARD Cooks in the Pot

- Congress – Passed Telecommunications Act of 1996
- FCC – Charged to create a competitive market for 3rd party STBs
- Consumer Electronics Manufacturers – Create high end DTV and STB products that are CableCARD enabled
- CableLabs – Develop the CableCARD specifications and define certification/testing
- Motorola and Scientific Atlanta – Create the CableCARDS – available in 2003
- Cable Companies – Prepare to deploy them



Why wasn't CableCARD successful?

- Cable companies prefer to lease proprietary settops rather than CableCARDs.
- Proprietary integrated settops have more functions than CableCARDs.
- CableCARDs suffer from “V1.0” glitches.
- CableCARDs supported only on expensive third-party settops and high end DCR TVs.



CableCARD v1.0

- Implemented from a hodgepodge of standards:
 - SCTE 28
 - SCTE 41
 - CEA-679B
- No interactive program guide (IPG)
- No Pay Per View (PPV), no VOD
- No interactive services
- Decrypt one program at a time

CableCARD v1.0 Deployed

All cable providers **MUST** support
CableCARD v1.0 (as of July 2004).

First High end Digital Cable Ready (DCR)
TVs available in August 2004.

The good news: CableCARD v1.0
deployed!



CableCARD v1.0 – The bad news

- Cable companies advertised their STBs over CableCARDs
- CableCARDs were difficult to install, requiring a technician to come out to home
- Suffered from “Version 1.0” issues
- CableCARD technology – a “one-way” implementation



One way vs Two-way

- One way – Communication between the cable company and the DCR TV goes in one direction only—from cable company to CableCARD. No communication path is available from the CableCARD back to the cable company infrastructure.

What does this mean?



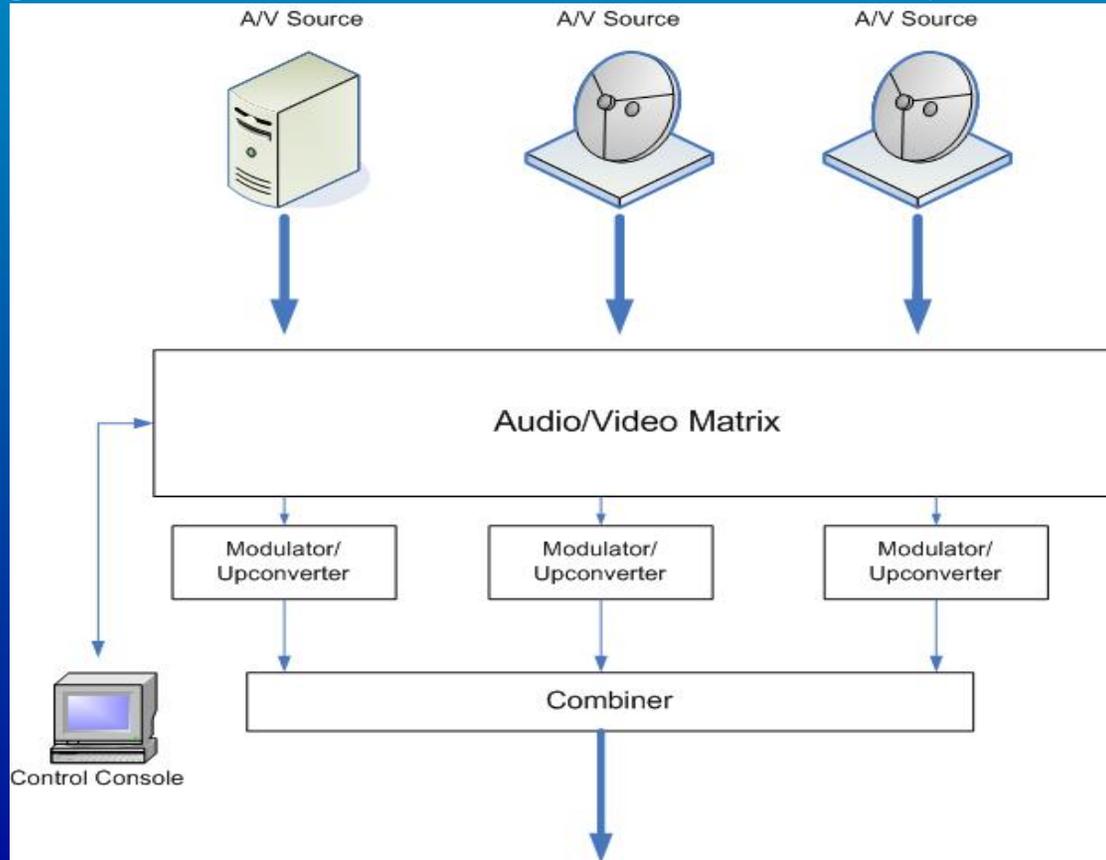
“One-way” Implementation

- No interactive program guide
- No Impulse Pay-Per-View (IPPV)
- No Video on Demand
- No Interactive Services
- CableCARD is “paired” with DCR device

Less than what is currently offered in today’s proprietary set-top boxes!

CableCARD Infrastructure

Cable Headend – Facility for receiving TV signals for processing and distribution over a cable system.



BitRouter's Portable Cable Headend

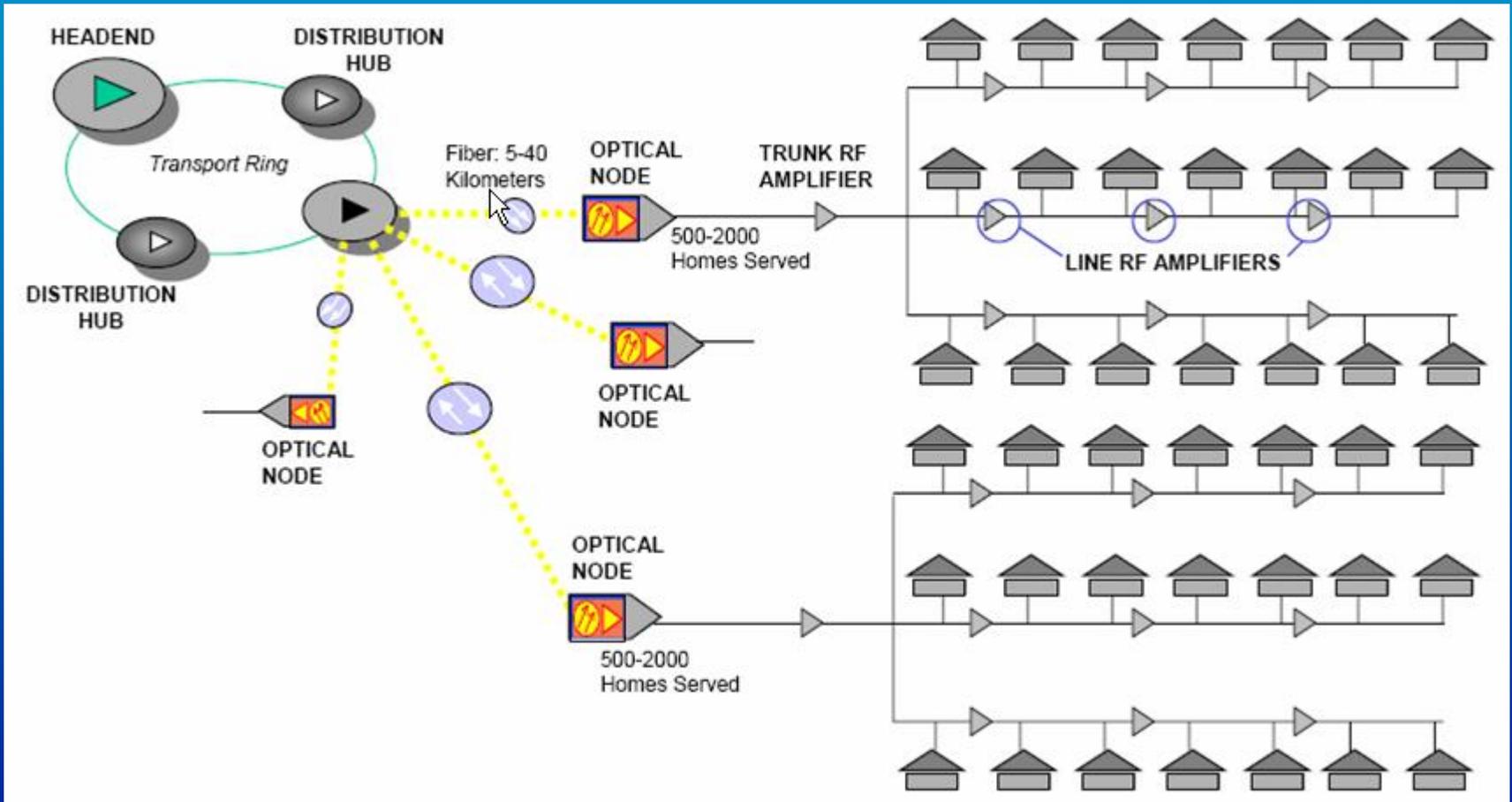




CableCARD Infrastructure

- Hybrid Fiber Coaxial Network (HFC)
 - Broadband network that combines optical fiber and coaxial cable
 - Used by US and Canadian operators
 - Tree and branch formation
 - Extends the headend output to cable customers
 - Bi-directional network

Typical HFC Network



Source: Wikipedia



CableCARD Infrastructure

- Fiber Optic network connects headend to local nodes.
- Local nodes connect optical signals to electrical signals going to the homes (25 to 2000 homes for each node).
- HFC network is non-symmetrical—one direction has more data-carrying capacity than the other direction



Example CableCARD Install

- Buy a DCR TV or STB
- Call the cable provider for a CableCARD install
- Wait for a technician to show up
- Technician “installs” CableCARD
 - Gets unique ID from CableCARD
 - Reports it to the main office
 - Main office sends EMM (Entitlement Management Message) to enable premium channels paid for
 - CableCARD receives EMM



Example CableCARD install

- **Step 1: Purchase Digital Cable Ready device:**
 - High end Digital TV (26 inches or larger)
 - Set-top box (SONY DHG HD DVR)
 - Tivo Series 3 (\$799)
 - Cable company set-top
 - Vista PC/ATI TV Wonder Digital Cable Tuner



Example CableCARD install

- **Step 2:** Buy a CableCARD subscription from your local cable company
 - Digital TV subscription
 - Monthly rental for CableCARD provided by cable company



Example CableCARD install

- **Step 3:** Schedule a technician to come out to home and install the CableCARD
 - Technician brings CableCARD to home
 - Cable subscriber provides Digital Cable Ready device



Example CableCARD install

- **Step 4: Technician visit – setup**
 - Plug CableCARD into DCR device.
 - Record unique ID displayed on screen by CableCARD after initialization. CableCARD uses host to display identification on screen:



Initial CableCARD Screen

In order to start cable service
for this device, please contact
your cable provider
1-800-555-1234

CableCARD(tm): 000-385-880-105-4

Host: 071-848-735-181-5

Data: 245-312-199-64

UnitAddress: 000-03858-80105-238



Example CableCARD install

- **Step 5: Technician visit – call headend office**
 - Technician calls the headend office and reports CableCARD ID.
 - Technician requests a “hit” to the CableCARD. A hit is slang for an Entitlement Management Message (EMM) sent over the cable network to the CableCARD. Tells CableCARD what programming package(s) you are paid for and are entitled to watch.
 - EMM authorizes a specific host/CableCARD combination.



Example CableCARD install

- **Step 6: Technician visit – wait for success**
 - Technician waits for EMM to reach CableCARD.
 - CableCARD receives EMM and becomes entitled to decrypt programming packages.
 - EMM only sent at request of technician – generally sent once.
 - CableCARD receives ECM messages (Entitlement Control Messages) over the cable network, which contain key(s) to decrypt premium channels.
 - ECM messages are sent continuously.

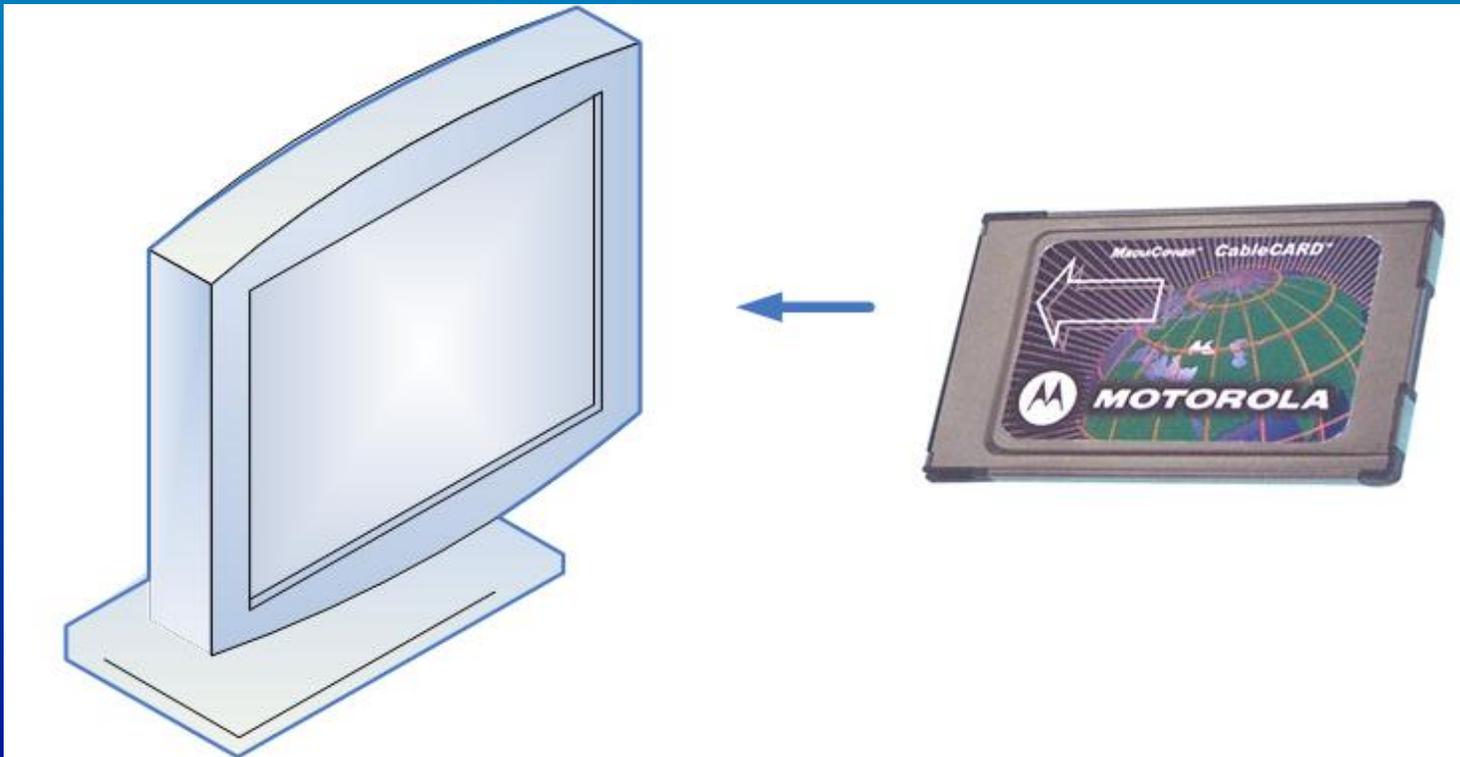


CableCARD install issues

- Cable company may not have CableCARDs in stock.
- EMM may not reach CableCARD.
- Firmware version on CableCARD may not match operational network.
- Pairing between CableCARD and host may not work correctly, causing initialization failure.
- CableCARD cannot be moved to another DCR host without a technician visit.

In-Band vs Out-of-Band

- Cable network in the home (split into in-band vs out-of-band)



In-Band Path

Data coming from the headend – MPEG-2 streams:

In-Band signals

- Contain content you wish to watch – HBO, ESPN
- May be encrypted
- Each “channel” is transferred on 6Mhz of bandwidth, between 54Mhz and possibly up to 1Ghz
- Multiple “programs” can be multiplexed on a “channel” if there is enough space on the frequency
- Emergency Alert Information



Out-of-Band Path

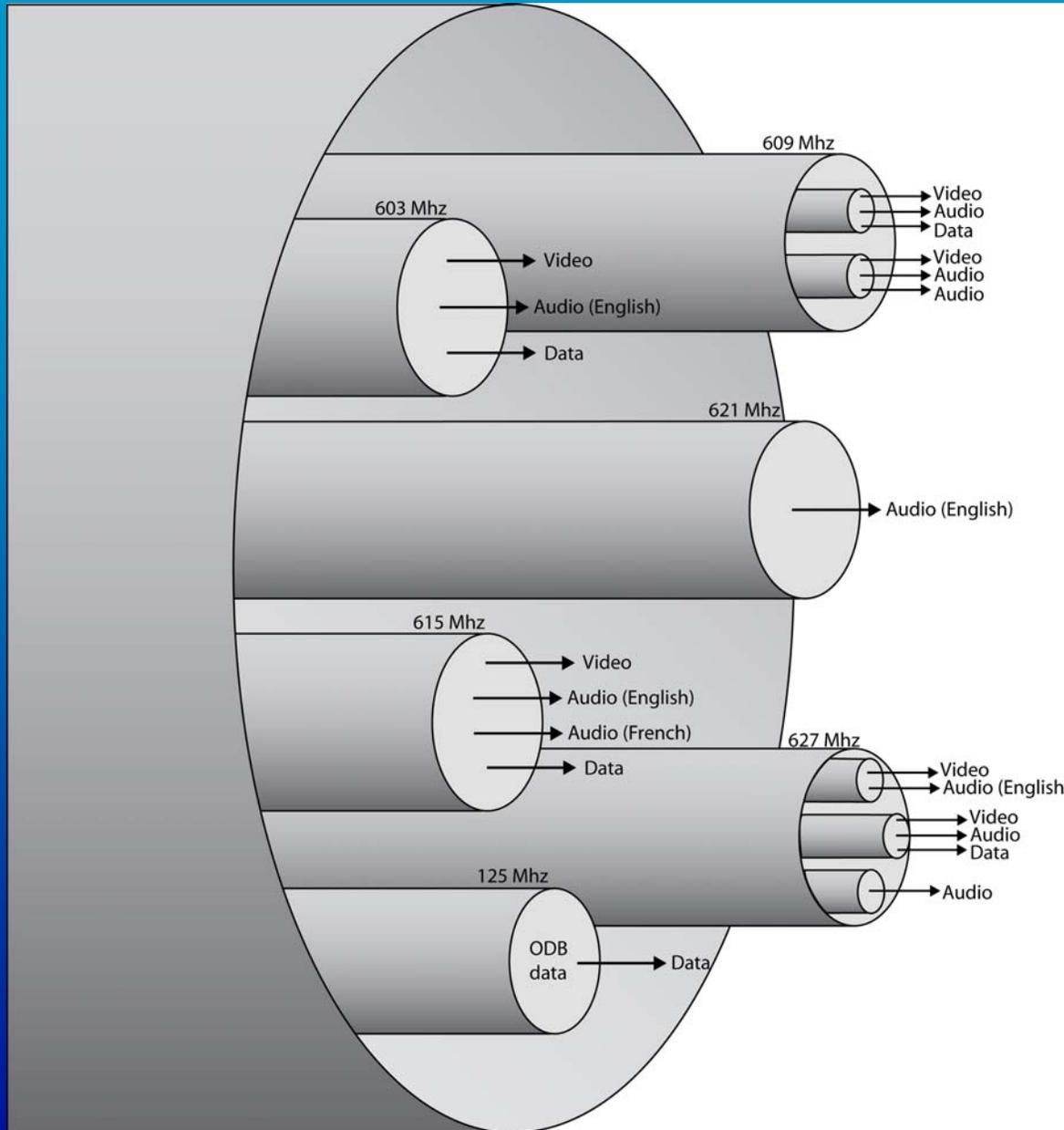
More data in MPEG-2 pipe:

Out-of-Band signals:

- Contain data, not video
- EMM (Entitlement Management Message)
- ECM (Entitlement Control Message) – keys, encrypted by a proprietary mechanism (known by headend and CableCARD only)
- Channel Map
- Emergency Alert Information (sent on both in-band and out-of-band paths)

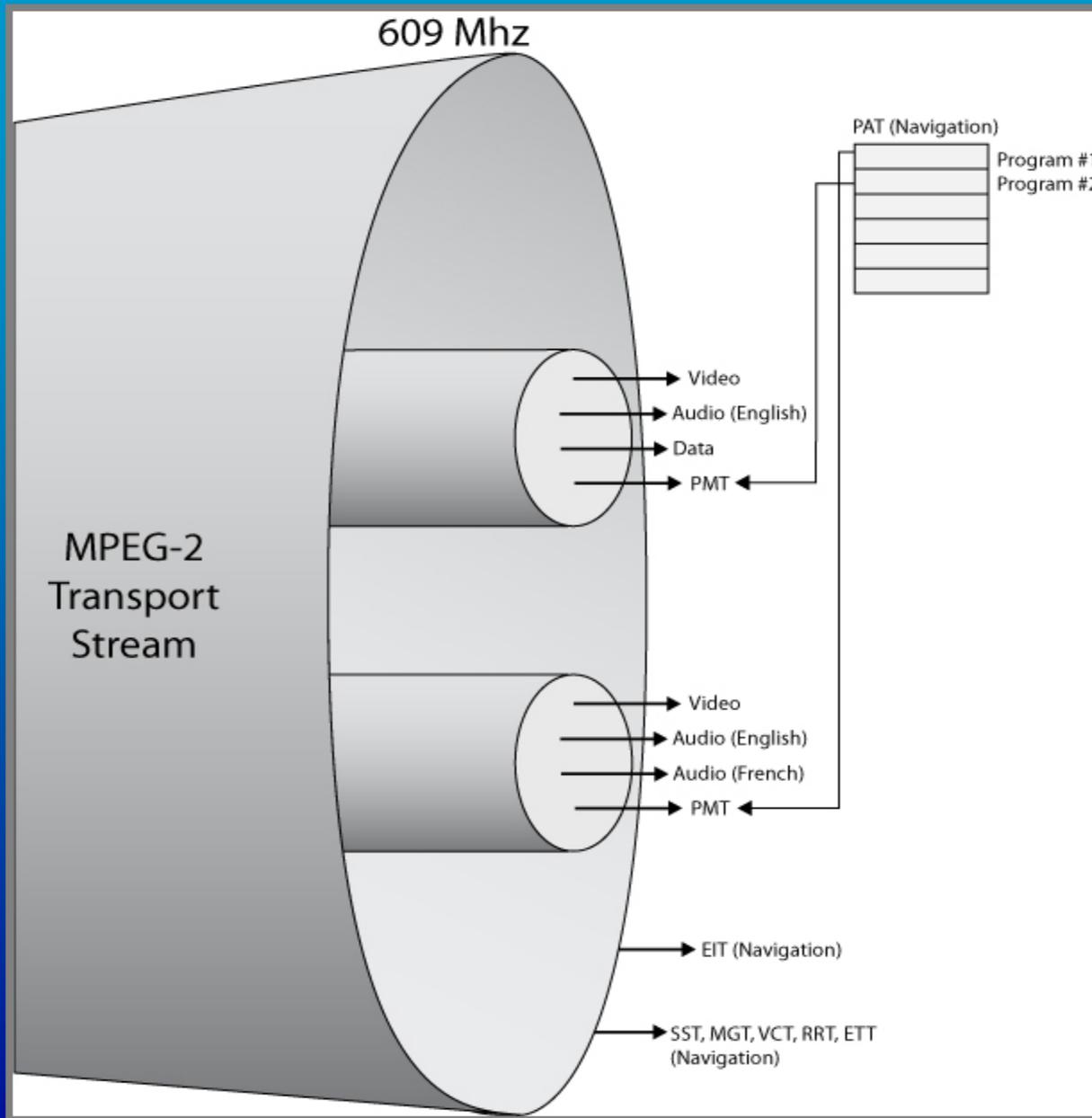


MPEG-2 Pipe

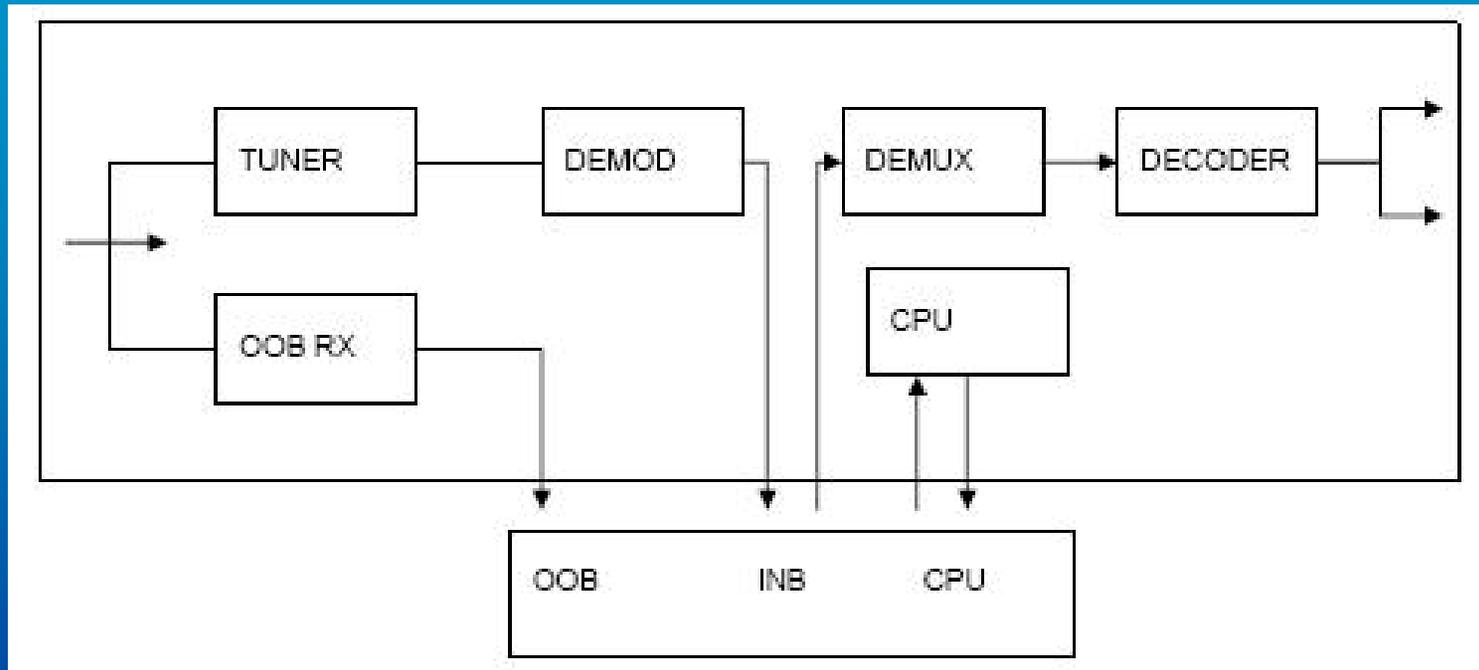


MPEG-2 Pipe

MPEG-2 Transport Stream



Inside a Digital Cable Ready TV



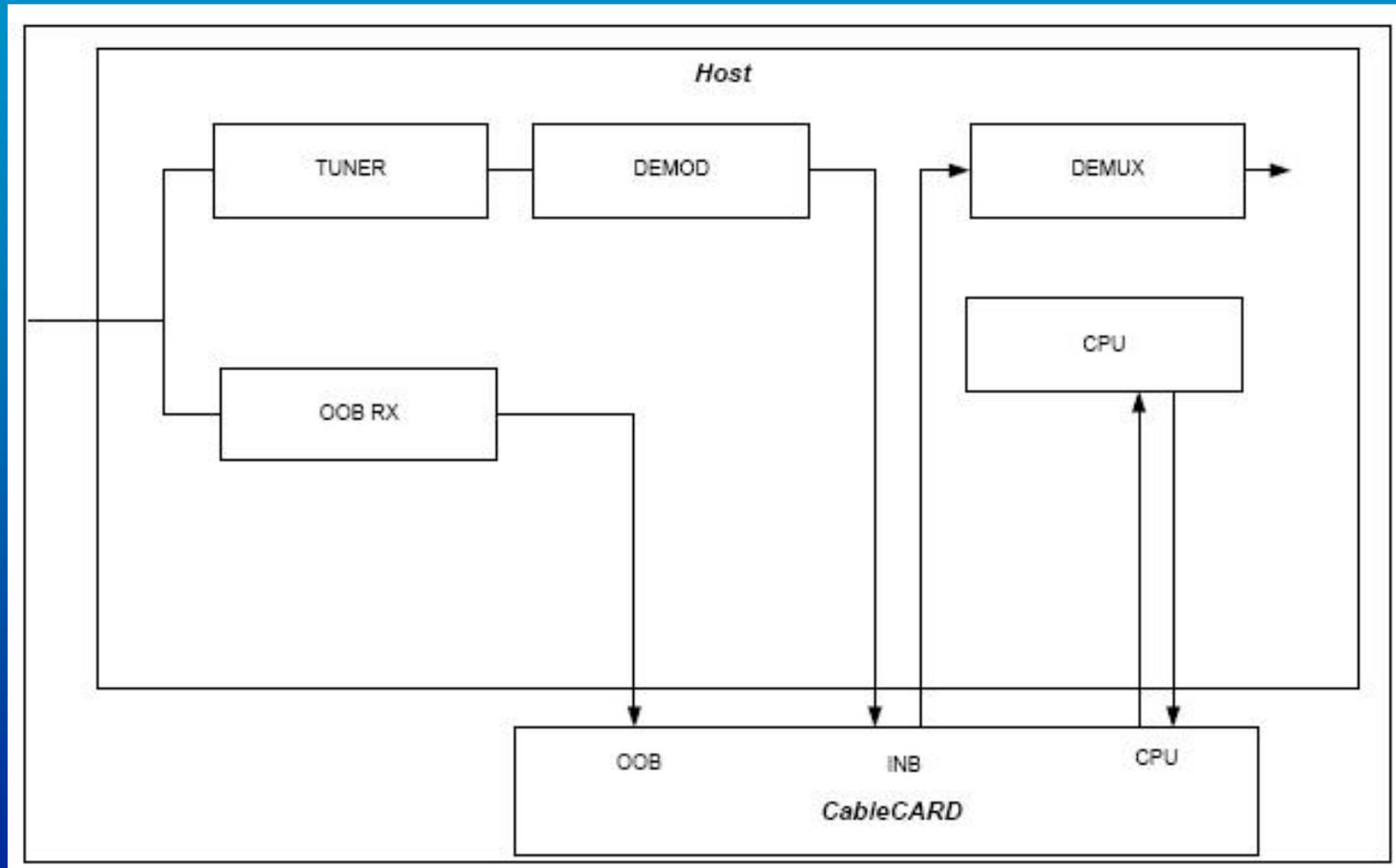
Source: BitRouter



One-way vs two-way

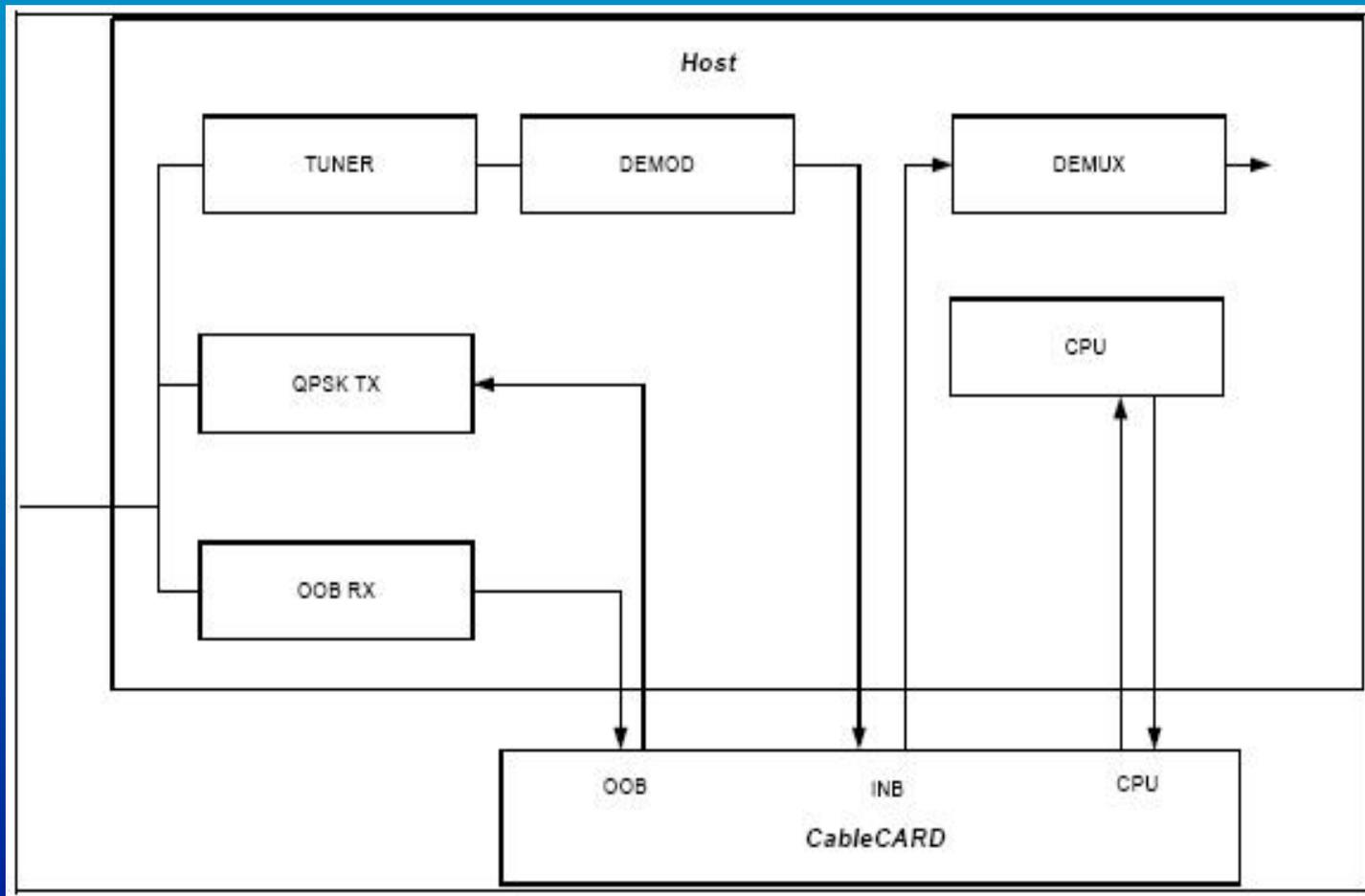
- **One way** – Communication between the cable company and the DCR TV goes in one direction only—from cable company to CableCARD. No communication path back to the cable company infrastructure.
- **Two way** – Communication path in “both directions”—from headend to CableCARD and from CableCARD to headend.

One-way network example



Source: CableLabs documentation

Two-way network example



Source: CableLabs documentation



Little known fact...

- All CableCARDs are TWO-WAY – have ability to send data back to headend.
- However, manufacturers of digital TVs requested the first standard be one-way.
- FCC defined elements of a one-way receiver.



CableCARD 1.0

- CableCARD 1.0 – what we have been taking about:
 - Current deployment
 - One-way implementation on hosts
 - No interactive services
 - No extended programming guide (EPG)
 - No Video On Demand
 - No Interactive Pay-Per-View



CableCARD 2.0

- CableCARD 2.0: Latest implementation of CableCARD technology
 - Two-way implementation for card and host
 - Fixes many limitations of CableCARD 1.0
 - Decrypt multiple streams at a time (DVR, PIP)
 - CableLabs responsible for specification and certification
 - No current deployment yet



CableCARD 2.0

- Operational Modes:
 - M-CARD – capable of processing multiple streams
 - S-CARD – v1.0 legacy mode – single stream

	Single Stream Host (S-Host)	Multi-Stream Host (M-Host)
S-CARD	S-Mode	Host may reject S-CARD
M-CARD	S-Mode	M-Mode



Motorola M-CARD



Scientific Atlanta M-CARD





M-CARD Capable Host

- M-Host – Multi-Stream Multi-Tuner capable device
- Can be Settop or Digital TV
- Specified by CableLabs – OpenCable Host Device Version 2.X, where “X” is “0” or “1”
- Support non-scrambled analog channels
- Support in-the-clear digital channels
- Support digital premium (scrambled) channels using a CableCARD
- Support interactive and two-way services (VOD, IPPV, EPG)



CableLabs

- Research and Development arm of cable industry
- Located in Louisville, Colorado
- Owns CableCARD specifications
- Developed test procedures for CableCARDs and Hosts
- OpenCable Project – Promote “Plug and Play” availability for deploying interactive cable services in North America
- Specifications available at <http://www.cablelabs.com>

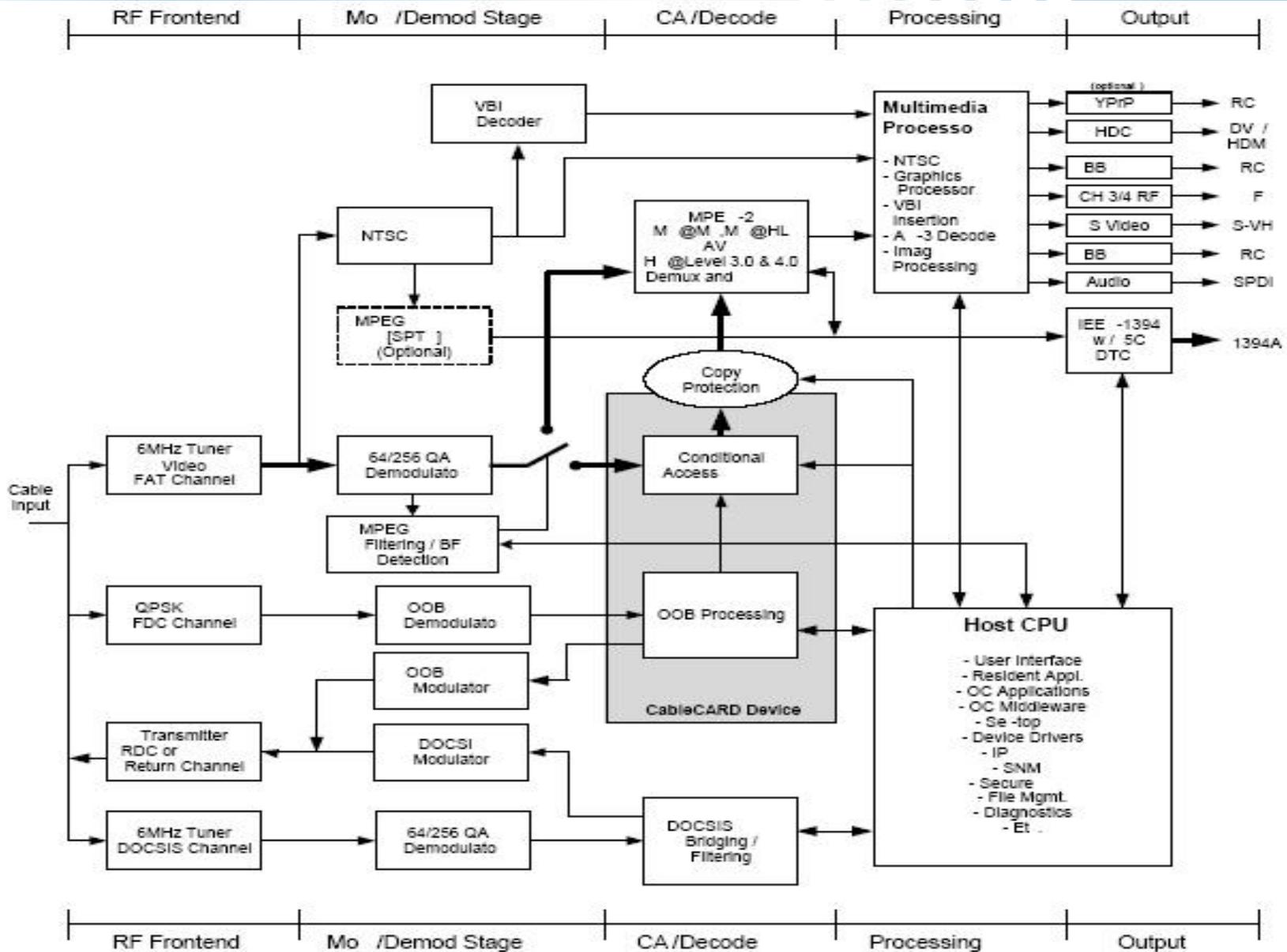


OpenCable Host Device Overview

- OpenCable Host Devices (OCHD2.1)
 - OCS2.1 – OpenCable Set-top
 - OCT2.1 – OpenCable Terminal

<http://www.opencable.com/specifications/host.html>

HOST2.1-CFR – OpenCable Host Device 2.1
Core Functional Requirements





Signal Path Within DTV

- Tuner – Locks onto in-band signal of MPEG-2 stream you want to watch
- Passed through demodulator – recovers data from the signal (premium channel – encrypted)
- Passed to CableCARD
- CableCARD checks EMMs for authorization
- If entitled, then pulls ECM out of in-band signal (ECM is encrypted in proprietary manner)
- CableCARD uses the DES key to re-encrypt the decrypted stream and sends the stream back to the Host
- Host uses DES key to decrypt stream coming from CableCARD and then plays stream.



Host 2.0 Devices and Cable Modems

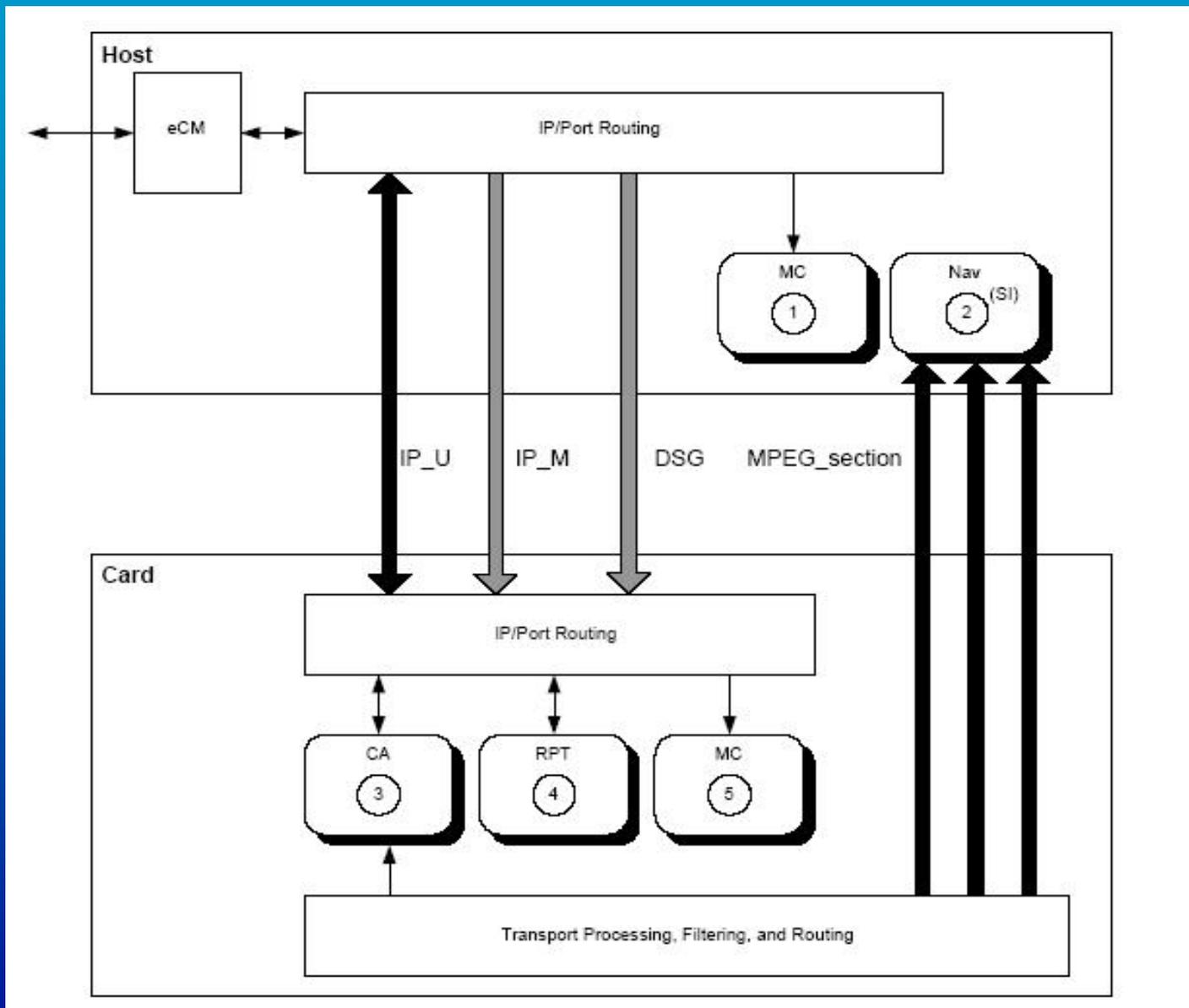
- Host 2.0 Devices MUST contain an embedded cable modem (eCM)
- eCM must be DOCSIS compliant
- DOCSIS specified by CableLabs
- Provides network connectivity to the Host 2.0 device for transmission of out-of-band data
- Allows for bidirectional communication to/from headend



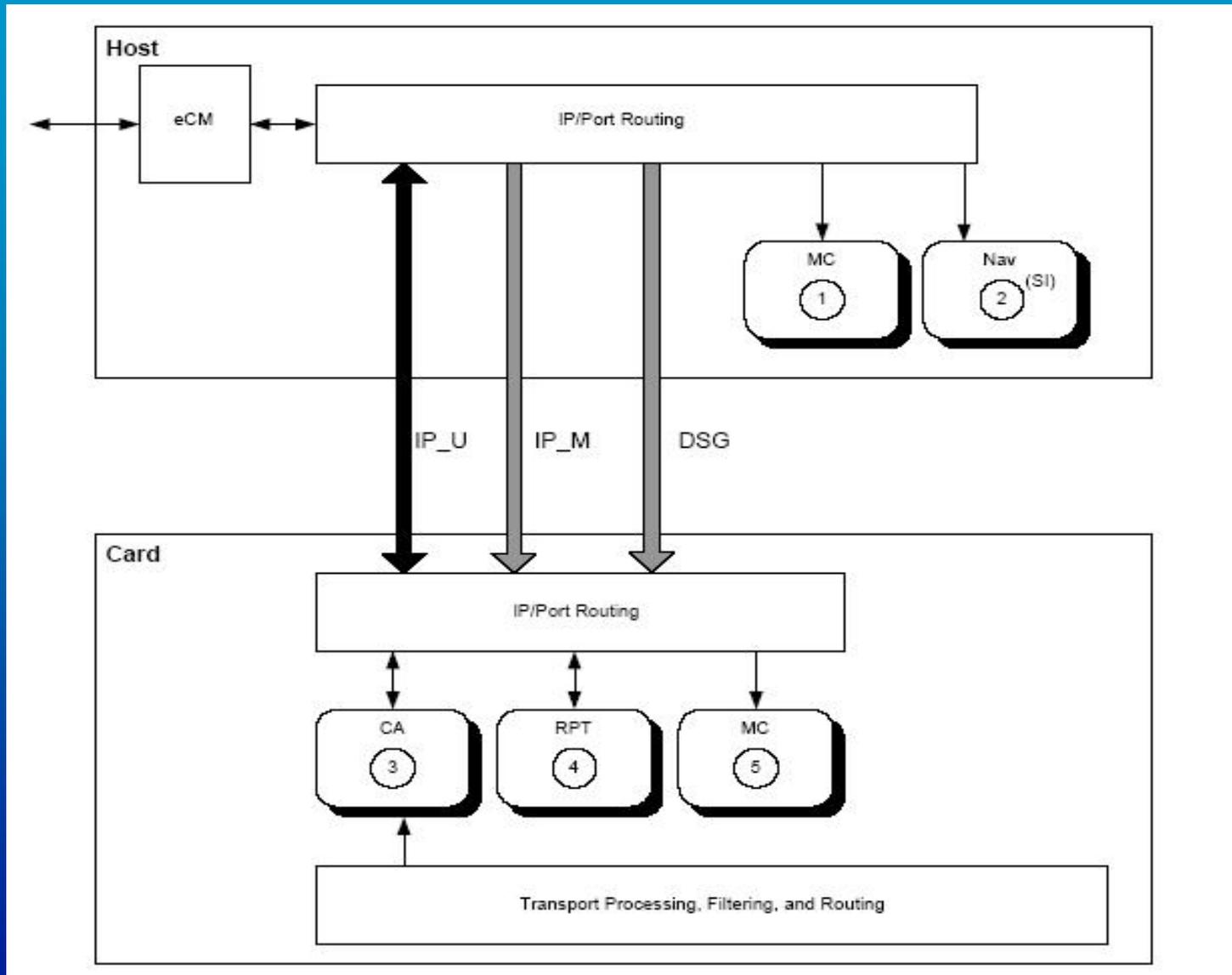
Host 2.0 Devices and Cable Modems

- DSG – DOCSIS Settop Gateway
 - Required extension of Cable Modem technology
 - Added feature above that found in on-the-shelf DOCSIS cable modems
 - Programmable network packet filter
 - Two different DSG modes – **Basic** and **Advanced**

Basic DSG Mode



Advanced DSG Mode





DFAST

- Encryption algorithm allowing both host and CableCARD to derive the same cryptography key without transmitting the key over the interface.
- Encryption algorithm is DES for S-CARD and 3DES for M-CARD
- Licensed from CableLabs as C source code



Copy Control Information (CCI)

- Information describing duplication rules associated with digital content
- Indicates “low value” and “high value” digital video and audio content
- “High value” content must be encrypted across the Host-CableCARD interface or any digital output
- Encryption and decryption specified by CableLabs
- Encryption key rotated per CableLabs spec

CCI Values

CCI Value	Meaning
Copy Freely	Any number of copies can be produced.
Copy No More	A copy of the content already made, no more copies permitted.
Copy Once	Only one copy of the content is permitted.
Copy Never	Copy never permitted for this content.

CCI Value

CCI Value	Name	Content Value	Encrypted across Host-CableCARD Interface?
0x00	Copy Freely	Low Value	No
0x01	Copy No More	High Value	Yes
0x10	Copy Once	High Value	Yes
0x11	Copy Never	High Value	Yes

NOTE: “Copy Once” CCI value is changed to “0x01” after copy is made.

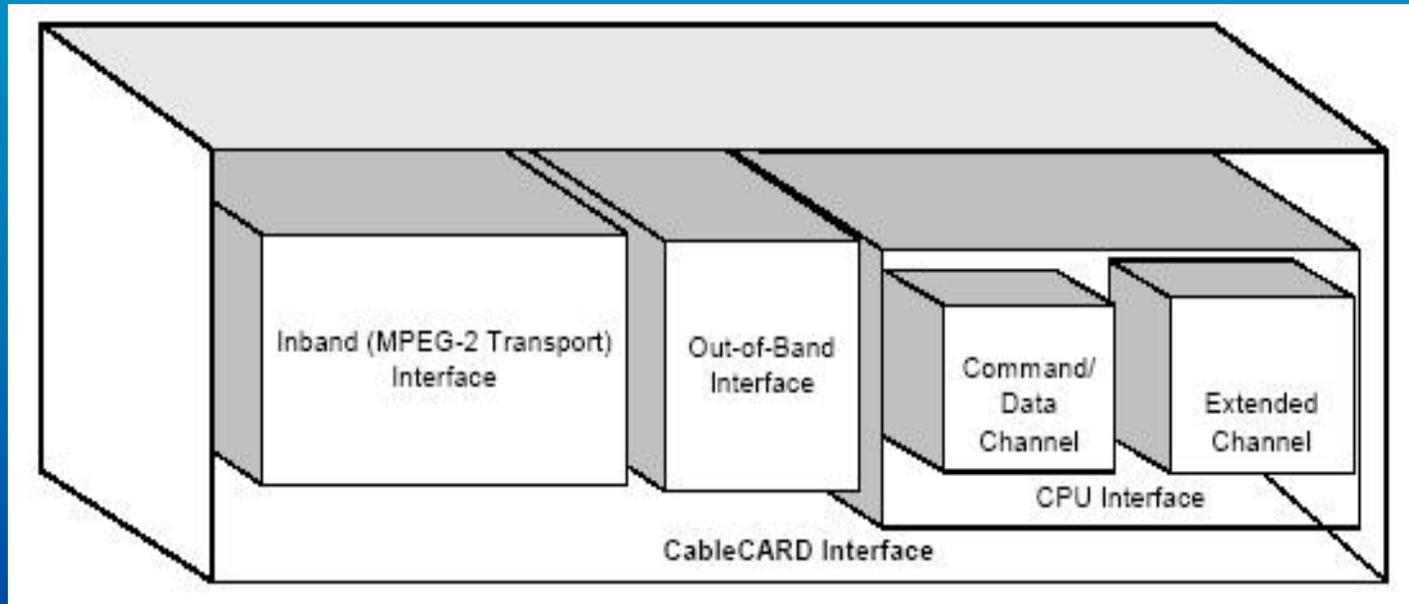


Encryption and DVR

- DVR and set-tops do not have a display device
- Audio/Video outputs on Cable Ready DVR and Set-tops must have encryption
- HDMI/HDCP
- Analog – Macrovision

Prevent illegal copying of protected content

CableCARD Interface



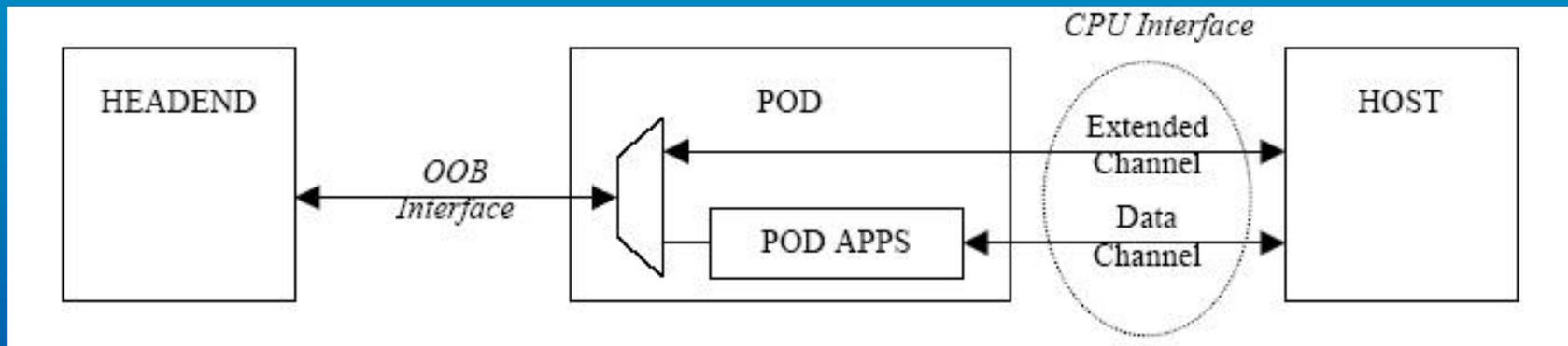
Source: CableLabs documentation



CableCARD Interfaces

- In-band (INB) Transport Stream Interface – Carries MPEG-2 packets in both directions.
- Out-of-band (OOB) Interface – Provides a data communication path between cable system and host in both directions.
- Command Interface – Communication packets transferred between CableCARD and Host.
- Extended Channel Interface – Communication path between the CableCARD and Host.

System Overview



Source: CableLabs documentation

Command Interface

- Carries communication between applications running on CableCARD and Host
- Layered architecture

Application			
Resources:			
User Interface	Low-Speed Communications	System	Optional extensions
Session Layer			
Generic Transport Sublayer			
PC Card Transport Sublayer			
PC Card Link Layer			
PC Card Physical Layer			

Source: CableLabs documentation

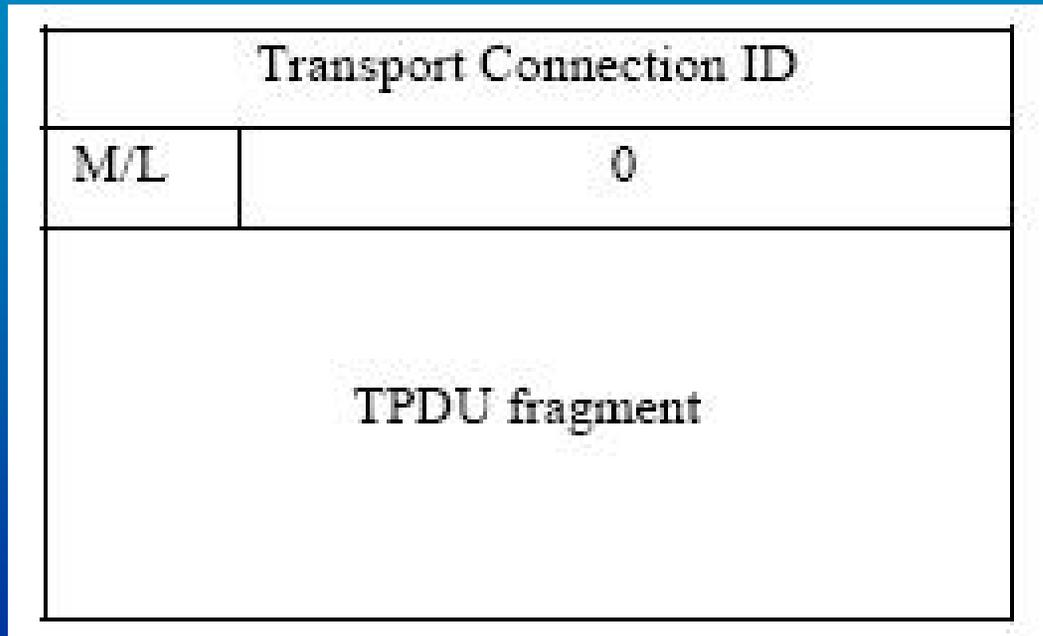


Architecture

- Physical Layer – Hardware interface
- Link Layer – Fragments and reassembles data objects passed over physical layer
- Transport Layer – Data objects associated with a particular transport connection
- Session Layer – Provides a logical means for the CableCARD to use “resources” on the Host

Link Layer Packet

- Data Channel

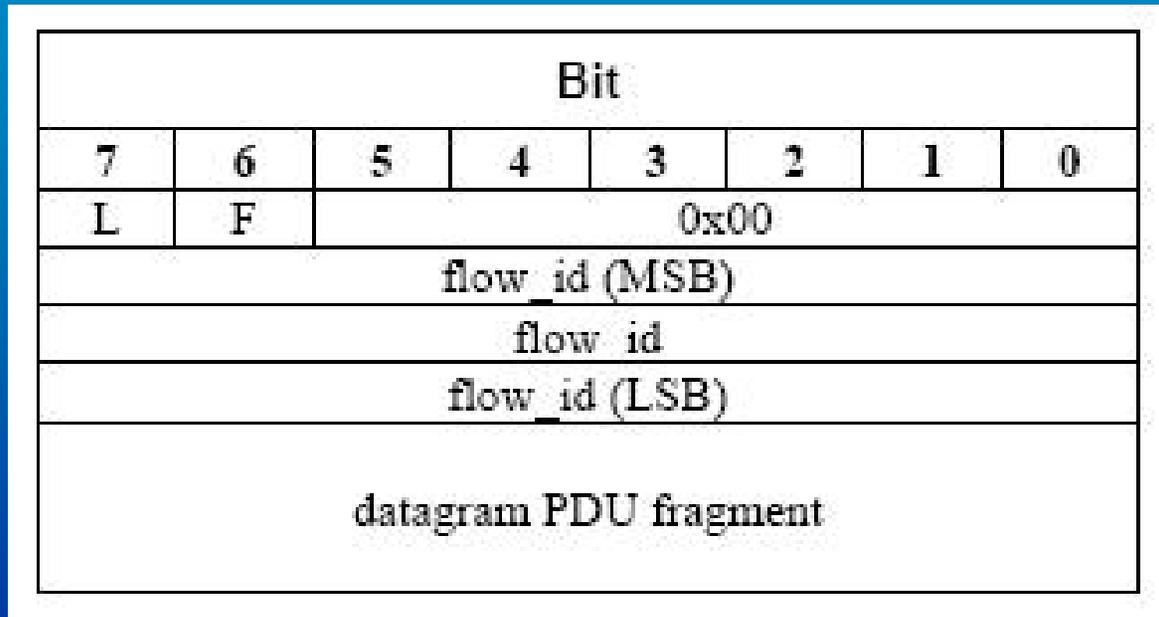


Source: CableLabs documentation



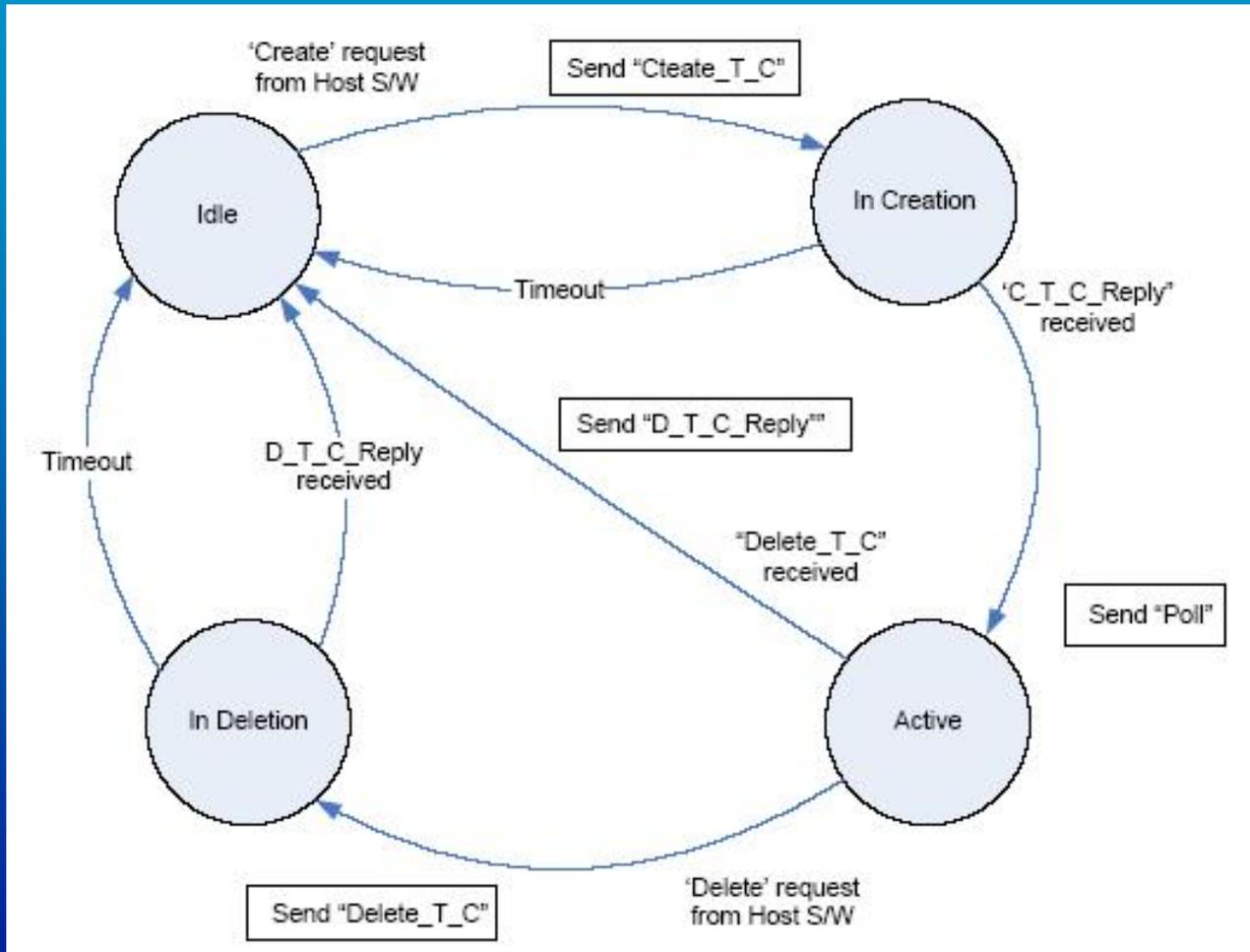
Link Layer Packet

- Extended Channel



Source: CableLabs documentation

Transport Layer



Source: CableLabs documentation



Transport Layer

- Logical connection state
- Transport Layer only allows one transport connection maximum for S-CARD
- Transport Layer was removed from M-CARD architecture



Session Layer

- Connects CableCARD “applications” to “resources” on the Host

What is a “resource”?

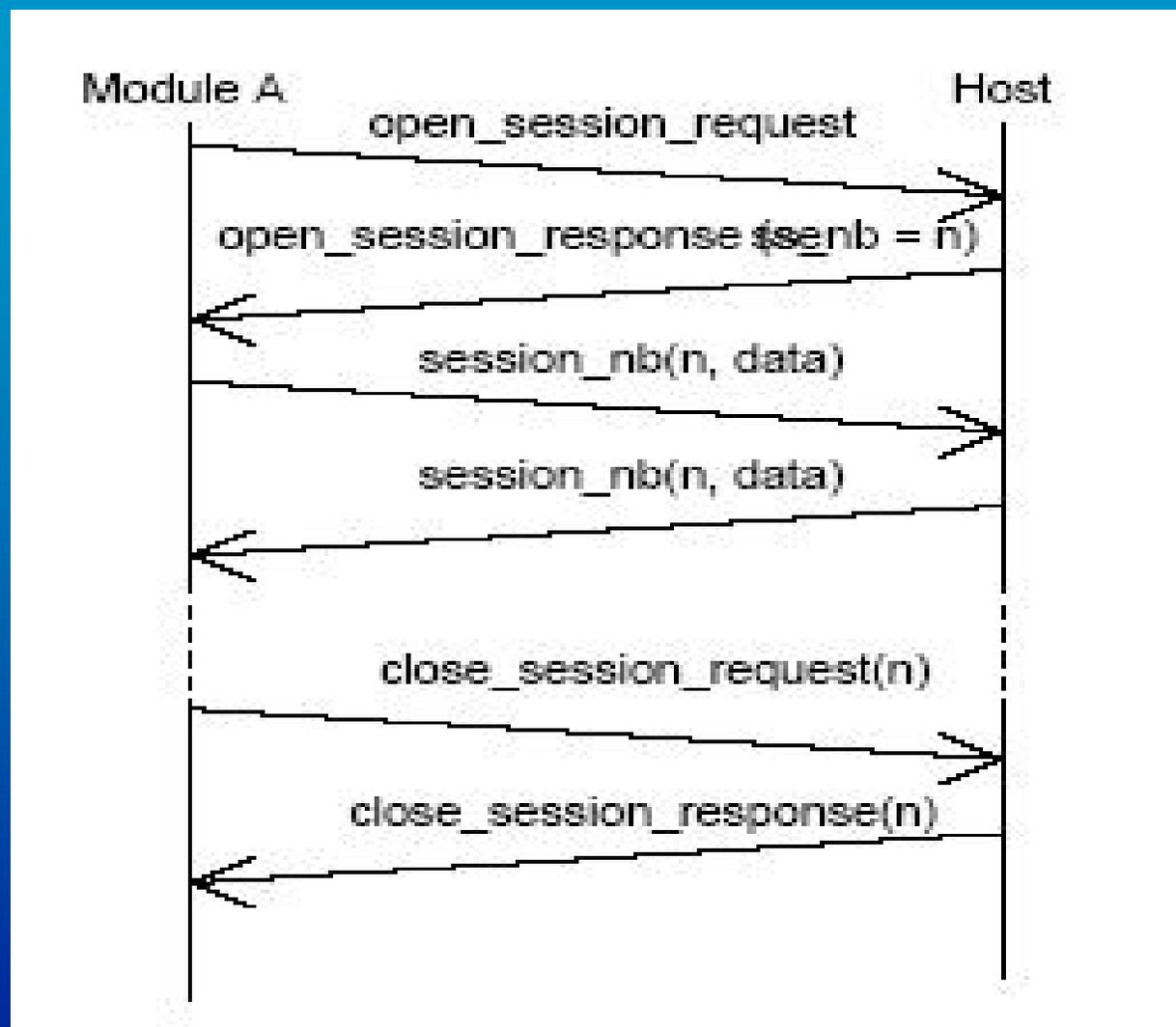
- A resource is a defined set of functionality that provides a service to the CableCARD.
- Sessions and Resources are defined by CableCARD specification.



Sessions

- Types of resources available on Host for use by CableCARD – examples:
 - System Time
 - Resource Manager – Provides resource list on Host
 - MMI - Displays HTML pages on Host
 - Copy Protection – Key rotation
 - Receive Extended Channel “flows” – Such as cable channel list and channel navigation

Session Protocol



Source: CableLabs documentation



Resources

- Resources exist on the Host only.
- CableCARD opens a “session” to a particular resource on the Host.
- Application Protocol Data Units (APDUs) are wrapped in a Session Protocol Data Unit structure (SPDUs).
- Resources define a unit of functionality available to a CableCARD.



Session Protocol Data Unit



Source: CableLabs documentation

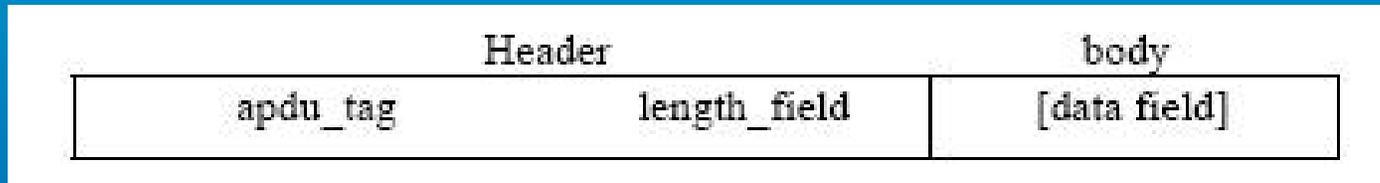


Application Protocol Data Units

- APDUs are data objects defined by the CableCARD specification.
- APDUs send application data between CableCARD and Host.
- APDUs are wrapped in a SPDU.



Application Protocol Data Units



Source: CableLabs documentation

Example Resource: Resource Manager

Resource	Mode	Class	Type	Version	Identifier (hex)
Resource Manager	S-Mode/M-Mode	1	1	1	0x00010041

The Resource Manager includes three APDUs as described in the following table:

Table 9.4-2 - Resource Manager APDU List

APDU Name	Tag Value	Resource	Direction Host ↔ Card
profile_inq()	0x9F8010	Resource Manager	↔
profile_reply()	0x9F8011	Resource Manager	↔
profile_changed()	0x9F8012	Resource Manager	↔

Source: CableLabs documentation

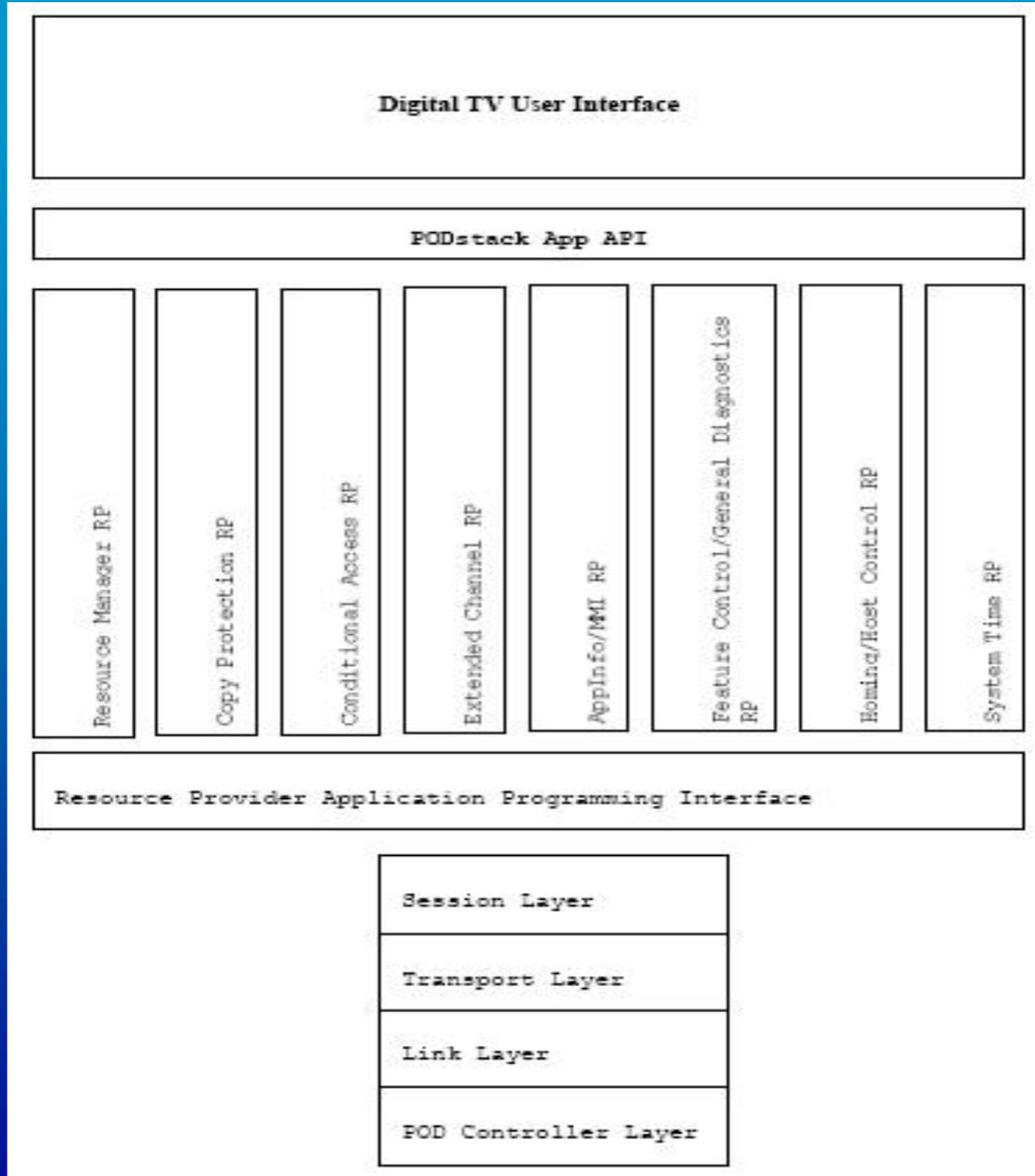


High Level Host Architecture

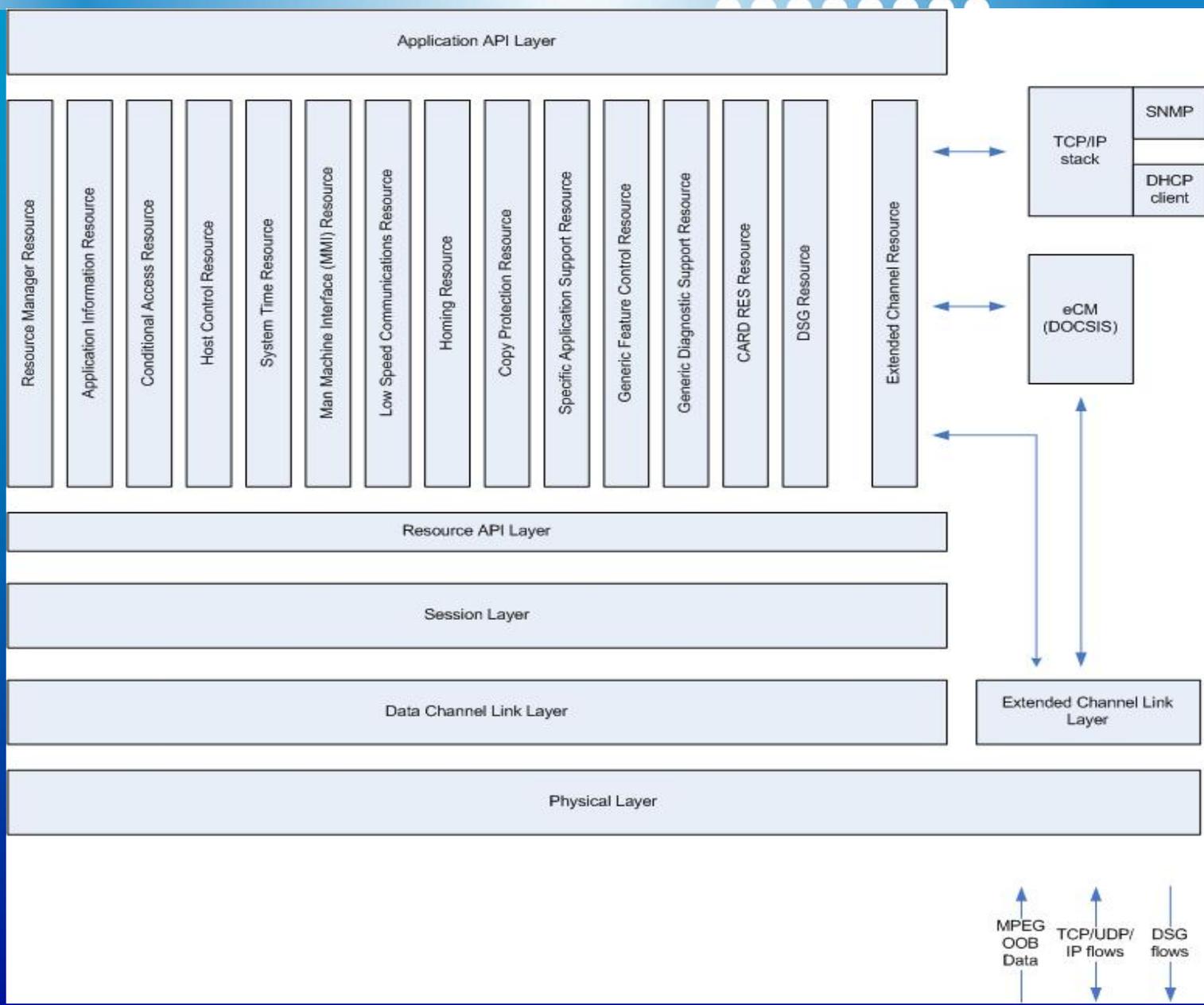




BitRouter's S-CARD Host Architecture



BitRouter's M-CARD Host Architecture





CableCARD Certification Process

- Certification process operated by CableLabs
- Certification processes for both Host and CableCARD devices
- Ensures interoperability of cable products as part of the OpenCable project
- Published test suite for Host and CableCARD devices



CableCARD Verification Process

- License DFAST technology from CableLabs
- Develop CableCARD stack
- Visit CableLabs for “Lab Development Use”
- Advise CableLabs of Expected Date to participate in Test Wave
- Sign DFAST Activation Notice
- Submit product to CableLabs for Test Wave



CableCARD Verification Process

- Purchase “production” digital certificates
- Go to manufacturing

Once a product passes certification within a Test Wave, it can be self-verified



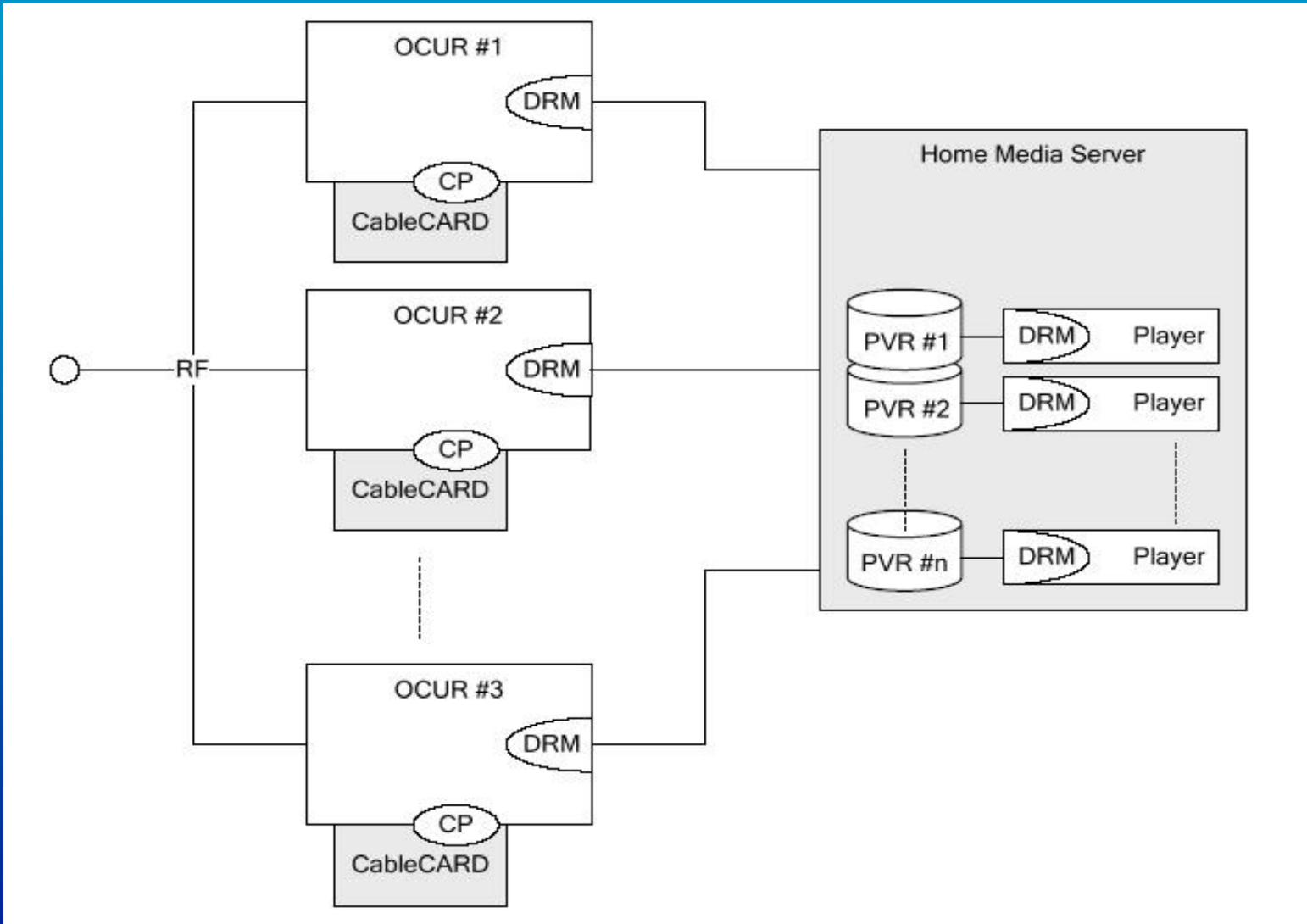
Types of CableCARD Hosts

- UDCP Device – Unidirectional Digital Cable Product or “Digital Cable Ready Receiver” (S-CARD)
- M-UDCP Device – Unidirectional Receiver using an M-Card
- Host 2.0 Device – Receiver that has support for two-way communication to headend
- OCUR – OpenCable Unidirectional Receiver



OCUR Device

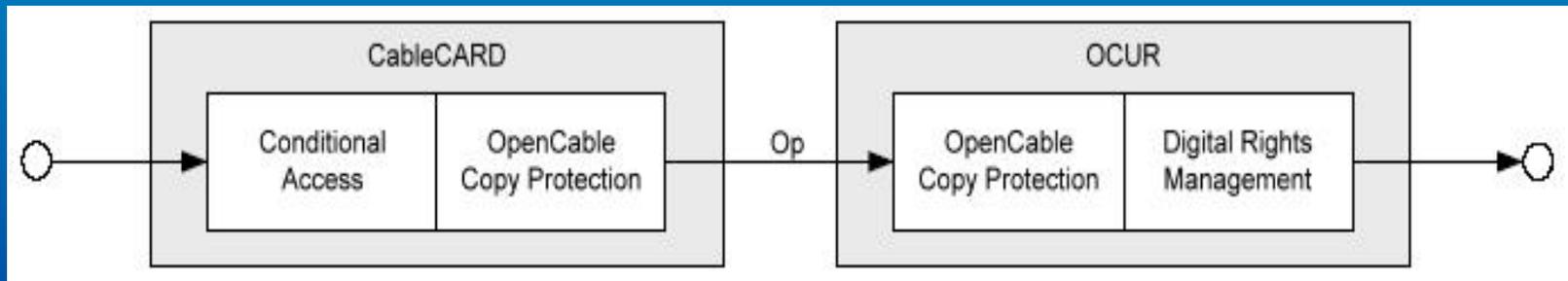
- Provides premium digital cable content to PCs
- Employs DRM technology (Digital Right Management)
- Specified by CableLabs
- Currently supports S-CARD only (one-way)
- Available on Microsoft Vista PCs certified as a OCUR device.



Source: CableLabs documentation

OCUR Technology

Protection Transitions:



Source: CableLabs documentation



FCC Roadmap

- 2003 – First S-CARDS certified
- 2004 – Availability of Digital Cable Ready Devices
- 2005 – CableCARD 2.0 specification available
- 2006 – Scientific Atlanta and Motorola M-CARDS certified
- 2007 – Availability of two-way Cable Ready Devices
- 2009-2010 – DCAS?



DCAS

- Downloadable Conditional Access System
- Future technology – replace CableCARD
- “Downloadable security” without a CableCARD
- For use in digital cable devices (set-tops, DVRs, etc.)
- Download any Conditional Access (CA) technology into a cable device in a secure way



DCAS, cont'd.

- DCAS – advantages to cable companies (MSOs):
 - No CableCARDS
 - No need to send technician
 - Complies with FCC integration ban
- DCAS – advantages to customer:
 - No need for a CableCARD
 - Two-way implementation – provides all features promised by CableCARD 2.0
 - No CableCARD monthly fee



Introduction to CableCARD™: History, Technology, Applications and Future

Craig Gwydir

Download latest tutorial version from:

www.bitrouter.com