Home Networking Subsystem

Introduction

RDK Home networking provides features for enabling the next-generation home networks which is not only limited to interaction with our home entertainment systems but also provides a medium to control wide range of activities such as our home's security, energy, health monitoring and environmental systems.

In general RDK Home network provides a set of interconnected devices tasked to carry out activities ranging from home entertainment to more interesting features such as home automation.

Features

- User can connect multiple connected devices such as DTV, tablets, smartphones, and laptops to the Ethernet port or over Wi-Fi. The connected devices with supported clients can watch same or different HD or SD QAM linear TV programs simultaneously.
- User can connect multiple IP over MoCA devices such as IP Clients to access Gateway services
- User will not experience service degradation when watching any video program via supported TV or supported connected devices due to bandwidth constrain.
- User MUST be able to access cloud services from all client devices supported by the Gateway device
- Supports trans-coding linear TV programs into DTCP-IP protected video with adaptive streaming and uni-cast to all operator supported connected devices over WiFi and Ethernet in real time.
- Support Time of Day synchronization as per DOCSIS ToD with network program guide server using a public time server such as time.nist.gov.
- Must function as DMS to support DLNA certified DMP connected devices

Home Networking Interfaces

- Wi-Fi
- MoCA
- Bluetooth
- Ethernet

Home Networking Protocols

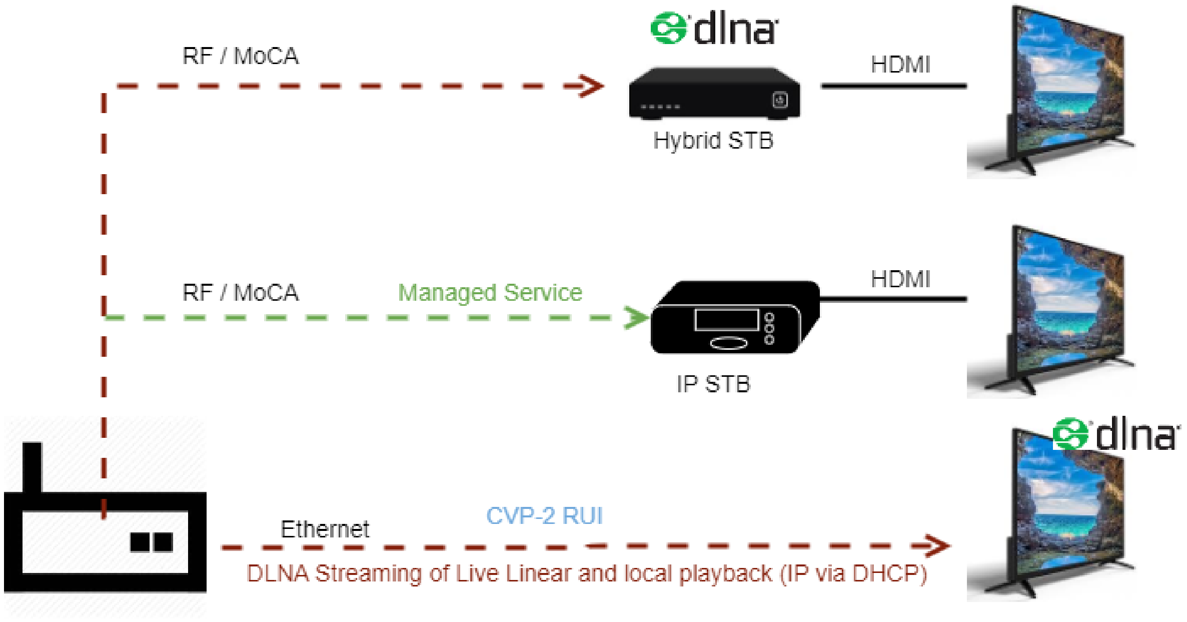
RDK Supports several Home networking protocols for features such as device discovery, multimedia streaming.

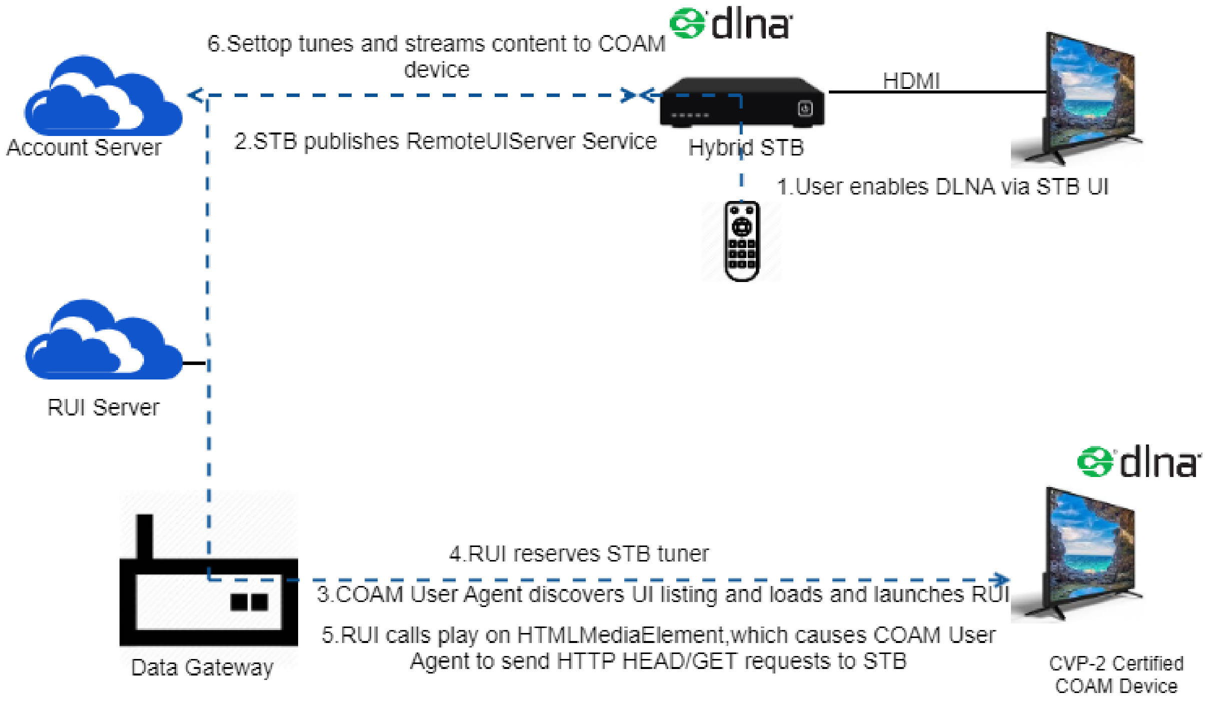
DLNA CVP-2

Feature Summary

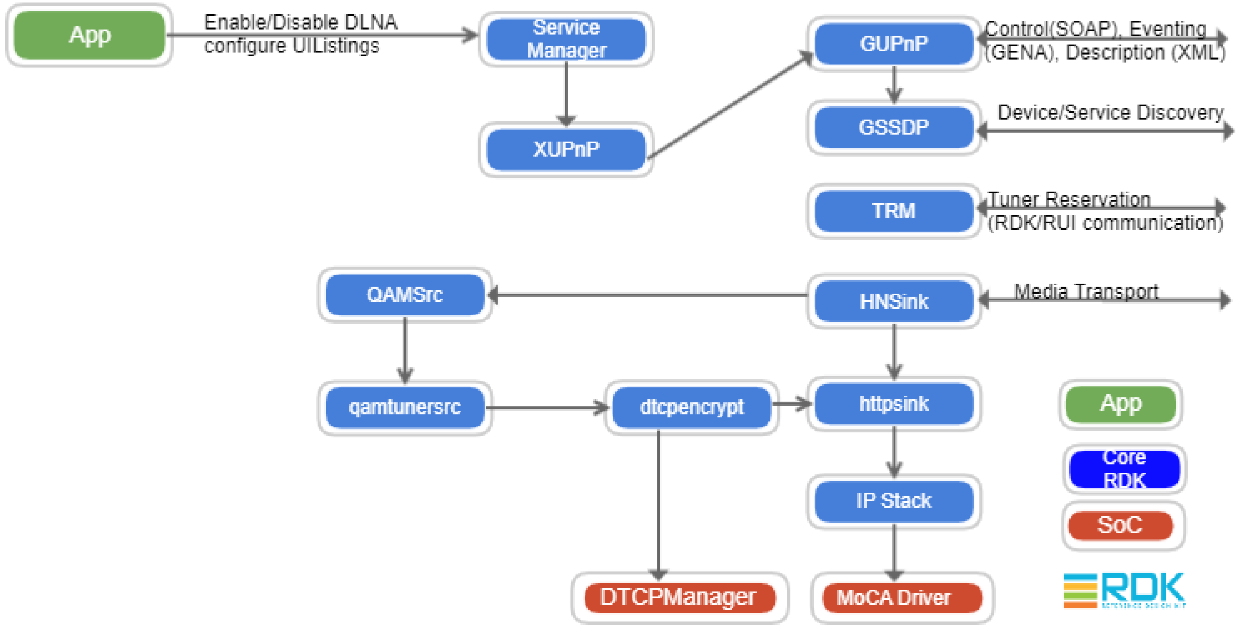
- Interoperability with CVP-2 clients
- Customer option to enable/disable DLNA
- 2 Box Model (DMP/DMS)
- MPEG-TS, AVC-TS
- DTCP-IP Link Protection
- RUI-H Discovery (UPnP RemoteUIServerDevice device and UPnP RemoteUIServer service)
- Playback with trick modes
- Live linear streaming

Architecture Overview




6.Settop tunes and streams content to COAM device
dlna
HDMI
Account Server
2.STB publishes RemoteUIServer Service
Hybrid STB
1.User enables DLNA via STB UI
RUI Server
dlna
4.RUI reserves STB tuner
3.COAM User Agent discovers UI listing and loads and launches RUI
5.RUI calls play on HTMLMediaElement,which causes COAM User Agent to send HTTP HEAD/GET requests to STB
Data Gateway
CVP-2 Certified COAM Device

RDK DLNA Architecture



Component Impacts

XUPnP

- Advertise RemoteUIServerDevice device and UPnP RemoteUIServer service

TRM

- Support tuner reservation from RUI on CVP-2 client

HNSink

- Support linear to CVP-2 client

RDK UPnP protocol & Architecture

The Universal Plug 'n' Play (UPnP) architecture provides an in-home client server architecture where servers and the services they provide are discovered and utilized by client control points using service actions and the the general event notification architecture (GENA). UPnP has been absorbed by the Open Connectivity Forum (OCF) and the UPnP specifications can be found at https://openconnectivity.org/resources/specifications/upnp/specifications. In the initial Comcast use of UPnP the UPnP defined BasicDevice and vendor specific service, DiscoverFriendlies, is published by gateway devices for discovery by client devices. The gateway devices use an IPv4 link local address to publish (discovery, actions, events) for the device, BasicDevice, and service, DiscoverFriendlies.

Initial RDK UPnP Architecture

The initial RDK UPnP Architecture involves an Client device discovering configuration information in an Gateway. There is only one device model that implements a UPnP Server, that being the Gateway. The BasicDevice is the only UPnP device type used. It is a UPnP standard device, see http://upnp.org/specs/basic/UPnP-basic-Basic-v1-Device.pdf. The DiscoverFriendlies service is the only service used and is embedded in the BasicDevice, as seen in the BasicDevice device description file; BasicDevice.xml. DiscoverFriendlies is a Comcast specific service defined in the Comcast home networking specification attached to this page.

There are two attributes in the RDK UPnP Architecture that are not to UPnP specification. First, the BasicDevice embeds the DiscoverFriendlies, but the BasicDevice specification states that no services may be embedded. Second, DiscoverFriendlies does not follow the naming conventions defined by UPnP for vendor defined services.

Use Cases

UPnP can partially or entirely address various use cases.

1. Provide configuration parameters to client devices.
2. Differentiating a Operator gateway from a COAM router so that an client device can determine a preferred gateway.
3. Prevent a COAM device from accidental access to the internet through an Gateway.
4. Prevent accidental or malicious bridging of any client device through a MoCA bridge (ECB) to a neighbor’s home.

5. For quality of service, determine that a client connected to an router is a known client and mark WiFi packet priority accordingly.
6. Operator's gateway gathers information about the devices on a home network for diagnostics purposes.

UPnP Security

UPnP defines security mechanisms such as the DeviceProtection service, but does not mandate them. The DeviceProtection service includes a TLS handshake for UPnP traffic, as well as a number of state variables for actions that can be used for security setup, access control, etc. Within the SSDP discovery messages the LOCATION header is used to indicate the base URL used for device and service description XML file access, as well as the destination for service actions, events, etc. An unsecure control point can use that URL to access the description files. If the device is under DeviceProtection scope, then it also must provide a secure location header; SECURELOCATION.UPNP.ORG. A control point that wishes to use secure functionality of a server will initiate a TLS handshake to the base URL to create a secure connection. The UPnP DeviceProtection:1 specification calls for self-generated, self-signed certificates.

UPnP security does not protect SSDP discovery messages, nor does it protect device and service description file access when a control point uses the required LOCATION header.

Doxygen documentation

API Specification can be found under XUPnP API Specification