

RDK-B Device Management

- User Specific Features
 - [WEBUI](#)
 - [SNMP](#)
 - [TR069](#)
 - [Logging](#)
- MSO Specific Features
 - [Dynamic DNS](#)
 - [Routing](#)
 - [HS Port Forwarding](#)
 - [Xconf Firmware upgrade](#)
 - [RDK Feature Control](#)
 - [RDK Telemetry](#)
 - [WEBPA](#)
 - [Captive Portal](#)

User Specific Features

WEBUI

- Easy monitoring and control of the device using the WebUI
- Enable, disable and modify various modes like Bridge mode, WiFi SSID and so on directly from WebUI
- Factory Reset the device
- Component : [WebUI](#)

SNMP

- Respond to Get requests from SNMP Management System
- Retrieve data from other RDK software components
- Component : [CcspSnmpPa](#)

TR069

- Register device to Auto-Configuration Server (ACS) using Inform notification
- Periodically send device information to ACS using Inform notification
- Allow ACS to configure periodic Inform interval
- Retrieve device diagnostics/parameters using GetParameterValues() method
- Set device parameters using SetParameterValues() method
- Factory reset using FactoryReset method
- Device reboot using Reboot method
- Component : [CcspTr069Pa](#)

Logging

- Generate logs for all the components and processes.
- Configuration of logging level per component
- Print formatted data to stdout and redirected to a local log file
- Aggregate logs locally on device
- Extract logs to server for analysis
- Component : [RDKLogger](#)

MSO Specific Features

MSO has some additional features on top of the features mentioned above.

Dynamic DNS

- Support for automatically updating a name server in the Domain Name System (DNS)
- Allows maximum of 4 host names
- Component : [CcspXDNS](#)

Routing

- Provides support for Routing Information Protocol using which MSO can monitor the routing information for the packets being interfaced from the device

HS Port Forwarding

- Supports port forwarding feature for home security network
- Component : CcspHomeSecurity

Xconf Firmware upgrade

- Single entity for managing firmware on set-top
- Provides set-top
 - Which firmware version
 - From where to download
 - How (protocol) to download
- Web interface for server side rule administration
- Key Highlights
 - Users can set download protocol
 - HTTPs as preferred method
 - Ability to decouple downloads from reboot
 - Ability to schedule firmware checks (During boot-up/Later), Configurable based on time zones, quiet times
 - Ability to redirect to secure download end points
 - Supports
 - Upgrade of Primary firmware
 - Remote Control
 - Disaster recovery images
 - Warehouse upgrades

Service & Scripts

Service Name : /lib/systemd/system/swupdate.service

Helper Script : /lib/rdk/swupdate_utility.sh

Main Script : /lib/rdk/deviceInitiatedFWDnld.sh

RDK Feature Control

- Operational limitations that lead to RFC
 - The only way to disable a new feature in the field was to rollback to the older firmware
 - Lack of options to do a feature deployment in a subset of devices
 - Lack of options to deliver dynamic configurations to the box
- Using RFC
 - Enables quicker roll out of features
 - Enables a secure channel for delivering runtime configurations to the device
 - Ability to control when the feature needs to be enabled/disabled ? Disable now/ Disable during reboot
- Component : [RDK Feature Control](#)

RDK Telemetry

- Telemetry is required to have more timely data about device health and status.
- With telemetry:
 - Data is more real-time
 - Metrics are available through configurable SLA policies
 - Critical matrix in real-time
 - Lower priority metrics in pre-scheduled interval
 - Real time metrics use terse key/value pairs.
- The log and telemetry upload process is controlled through dcm-log service
- Component : [Telemetry](#)

WEBPA

- WEBPA protocol provides this functionality of read/write access to device management parameters in an efficient manner as compared to TR-69 or SNMP.
- Component : [WebPA](#)

Captive Portal

- Feature of Smart Internet
- Account/Device activation
 - devices has to be first "activated" on the account and network

- On fresh boot up and factory reset, Captive Portal prompts to change the default SSID network name and password
- Allows user to personalize their WiFi SSIDs. This Step needs to be completed to connect to the internet.
- TR181 parameter for captive portal:
 - Device.DeviceInfo.X_RDKCENTRAL-COM_CaptivePortalEnable