

Home Device Manager

Dipayan Chaudhuri, Nitika Kapoor

Abstract: Home Device Manager offers a standardized CPE integration layer that enables providers to manage CPE that support either the Broadband Forum's TR-069 protocol or other protocols such as SNMP or Telnet. It Integrates and deploys a Broadband management platform within existing IT environment to interact efficiently with your OSS and BSS environment for transaction billing, Customer support, ERP and business intelligence.

Keywords: Activation ,Auto Configuration Server(ACS) ,Customer Premises Equipment(CPE) ,home device manager ,TR-069 Amendments ,TR -069 devices ,Zero-Touch

I. INTRODUCTION

Purpose of Home Device Manager-Home Device Manager allows broadband providers to remotely manage CPE (customer premises equipment), such as residential gateways, DSL and cable modems, femtocell access points, IP set-top boxes, and VoIP terminal adapters.

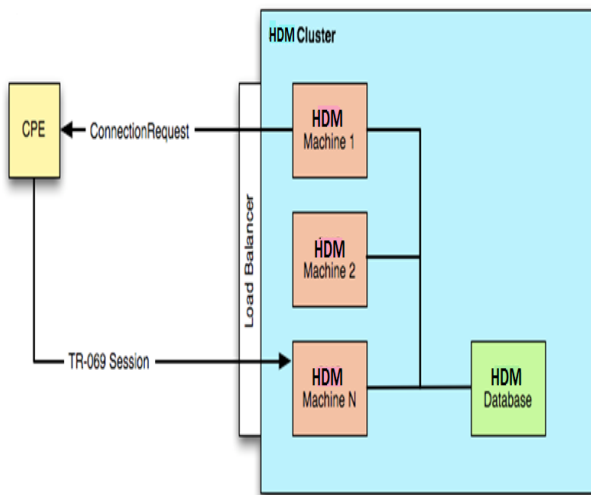


Fig -1: CPE and HDM Logical Block Diagram

II. What is TR-069 ?

TR-069 is the document number of the technical report, defined by the Broadband Forum, that specifies the "CPE WAN Management Protocol" or "CWMP". It provides the communication between the CPE & ACS. ACS (Auto Configuration Server) can manage the a device, trouble shoot, configure, upgrade etc.

HDM is also called ACS (Auto Configuration Server).

Issue 1 Amendment 1	Nov, 2006	Clarification of original document
Issue 1 Amendment 2	Nov, 2007	CWMP v1.1: Multicast Download support, 10 AUTONOMOUS TRANSFER COMPLETE event, AutonomousTransferComplete method, additional Download fault codes, interoperability clarifications, minor editorial changes.
Issue 1 Amendment 3	Nov. 2010	CWMP v1.2: Small updates for IPv6 related to DHCP, Additions for Software Module Management support (including new RPCs, Inform Event Codes, fault codes, and an Annex on UUIDs), ScheduleDownload RPC, and CancelTransfer RPC.
Issue 1 Amendment 4	July 2011	CWMP v1.3 Added Proxy management support and added Annex J and Appendix I. Table 4 Session timeout updated. Removed xsd Section A.6. Added Alias-Based Addressing additions, Section 3.6.1, Appendix II, and RPC Definition updates.

Table -1: TR-069 Amendments

III. HDM Activation Overview Process and it's types

A. Purpose: Device activation is initiating and configuring CPE devices to become fully operational in the provider's network.

B. Pre-activation

- Preprovisions the device with the appropriate authentication parameters. Preprovisioning can be done before activation by the CPE manufacturer, distributor, or retailer.
- If a device is not preprovisioned, HDM will provision the device with a BootstrapServer. In this scenario, HDM uses OSS to pre- provision the device, which prepares it for the next phase of configuration.

C. Activation

- Configuring the device, with SPV (Set Parameter Value) actions. Device configuration can range from a simple configuration change to a complex series of parameter value changes allowing the device to be operable in the provider's environment.
- Downloading firmware (optional). The firmware download configures the device with current updates from the manufacturer.
- Configuration download (optional), which downloads an initial configuration from a file to the device.

D. Fully Pre-Provisioned Activation

- Provisioning data store and unique CPE credentials,
- The OSS contains device and subscriber data that must be imported into the HDM provisioning data store before starting activation of devices.
- HDM provisioning data store and CPE must be pre-provisioned as follows:

1. The HDM provisioning data store must contain:

- CPE ID (OUI, product class, serial number),
- PPP credentials (if PPPoE required),
- HTTP credentials
- Optionally, subscriber ID and user-defined tags.

2. The CPE must be pre-provisioned with:

- Permanent ACS URL that enables it to communicate with the Device Management (DM) Server.
- Unique PPP (if PPPoE required) and HTTP credentials.

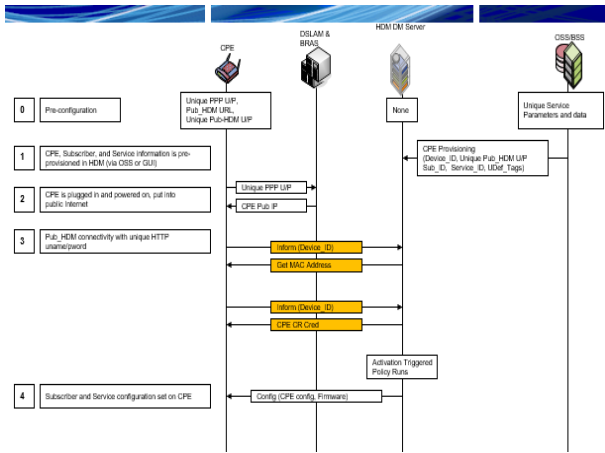


Fig -2: Fully Pre-Provision Activation

E. Pre-Provision HTTP Activation

HDM Server must be provisioned with HTTP credential:

- In this scenario, the HDM provisioning data store is preprovisioned only with unique HTTP credentials for CPE; the database does not contain the CPE ID. When activating

F. Zero-Touch Activation

- OSS system contains subscriber information, but no CPE information.
- The HDM provisioning data store contains no CPE and subscriber information. The HDM provisioning data store is not preprovisioned with subscriber data from the OSS system.
- The CPE must be preprovisioned with a default, temporary ACS URL that enables it to communicate with an HDM Bootstrap Server within the walled garden.
- The CPE must also contain default ACS HTTP credentials. If PPP is used and walled garden is used, it must contain default PPP credential.

devices with a partially preprovisioned HDM provisioning data store and unique CPE credentials, the OSS must contain subscriber data.

The CPE must be preprovisioned as follows:

- The HDM provisioning data store must contain a set of the unique public HTTP user names and passwords for each CPE.
- The CPE must be preprovisioned with a permanent ACS URL that enables it to communicate with the Device Management (DM) Server.
- The CPE must also contain unique PPP and unique, public HTTP credentials.

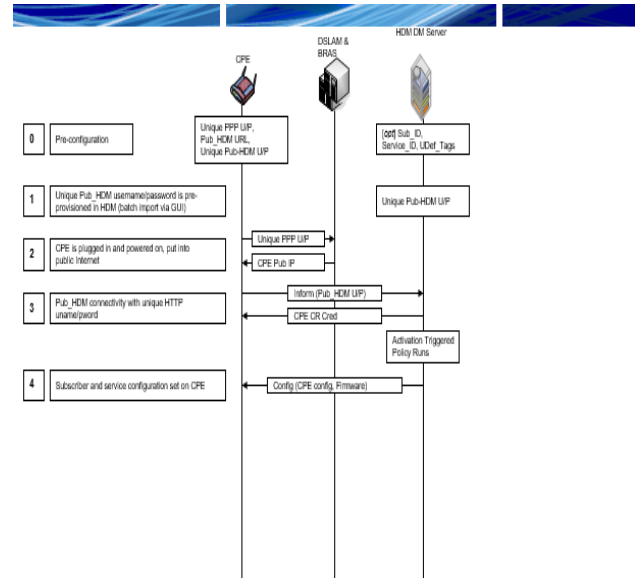


Fig -3: Pre-Provision HTTP Activation

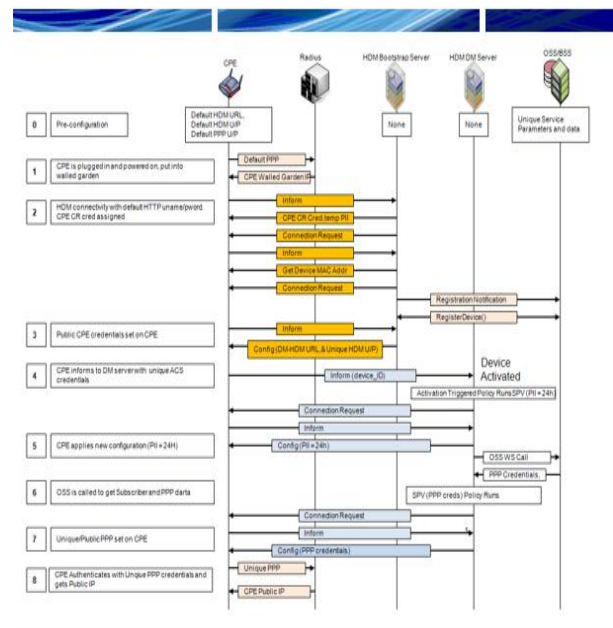


Fig -4: Zero-Touch Activation

- The subscriber receives the CPE and plugs the device into the DSL line.
- If the CPE uses the default PPP credentials to connect to the BRAS router, then BRAS router directs the CPE to an HDM Bootstrap Server within the walled garden.
- The CPE sends an Inform message with default ACS HTTP credentials to the Bootstrap Server (using the default ACS URL).
- The Bootstrap Server registers the device information in the HDM provisioning data store and sets its pre-activation state to “Initialized”.
- The Bootstrap Server marks the device as deactivated if any of the following conditions are true:
 - a) The device is new.
 - b) The Inform message is a BOOTSTRAP Inform message from an existing device.
 - c) The Inform message is non BOOTSTRAP (This situation can occur if the BOOTSTRAP Inform data was lost during or after factory reset of a device).

IV. Code for Creating Device using soap

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nbi2="http://nbi2.service.hdm.alcatel.com">
  <soap:Header/>
  <soap:Body>
    <nbi2:createDevice>
      <!--Optional:-->
      <arg0>
        <!--Optional:-->
        <community?></community>
        <!--Optional:-->
        <connectionRequestPassword?></connectionRequestPassword>
        <!--Optional:-->
        <connectionRequestUsername?></connectionRequestUsername>
        <!--Optional:-->
        <deviceId>
          <!--Optional:-->
          <OUI>00D112</OUI>
          <!--Optional:-->
          <productClass>HDM_Gateway_ProductClass8</productClass>
          <!--Optional:-->
          <protocol>DEVICE_PROTOCOL_DSLFTR069v1</protocol>
          <!--Optional:-->
          <serialNumber>T1</serialNumber>
        </deviceId>
        <disabled?></disabled>
        <!--Zero or more repetitions:-->
        <dynamicVariables>
          <encrypt?></encrypt>
        </dynamicVariables>
      </arg0>
    </nbi2:createDevice>
  </soap:Body>
</soap:Envelope>
```

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<S:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope" xmlns:S="http://www.w3.org/2003/05/soap-envelope">
  <env:Header/>
  <env:Body>
    <nbi2:createDeviceResponse xmlns:nbi2="http://nbi2.service.hdm.alcatel.com">
      <return>20009</return>
    </nbi2:createDeviceResponse>
  </env:Body>
</S:Envelope>
```

V. Results

The screenshot shows the 'Home Device Manager - Management Console' interface. At the top, there are tabs for Welcome, Devices, Policies, Actions, Device Types, Firmware, and Alarms. Below the tabs is a search bar for 'Find All TR-069 Devices'. The main area displays a table of devices with columns for Manage, Serial No., Subscriber Ref ID, Protocol, Device Type, Data Model Type, Gateway, Activated, Enabled, Awake, and Class. One device is highlighted in yellow, with its details shown in a form below. The form includes fields for Name (D1), Description, Template, Data Model Discoverable, Protocol (TR069), OUI (00D112), Product Class (HDM_Gateway_ProductClass8), Activation Settings, HTTP Default Password, Confirm HTTP Default Password, ACS URL, and Provisioning Mode (Pre-provision).

VI. Conclusion

- It has Worldwide distribution, services, and support.
- Improve new service time-to-market by defining the service once and leveraging that model in activation, self-service, call centers, and operations.
- Simplify the consumer experience and improve service adoption by using network-based service provisioning, activation and problem resolution.
- Empower NOC operators to monitor and take proactive actions on devices by automated alarm notifications from HDM.

REFERENCES

1. Sampriiti Sarkar, Alarms on Home Device Manager (IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH April – May 2016.
2. Stan Moyer and Simon Tsang ,Home Network Configuration Management & Service Assurance, Copyright 2001, Telcordia Technologies, Inc.
3. Vukasin Nuhijevic, Sasa Vukosavljev, Boris Radin, Nikola Teslic, Mirko Vucelja, An Intelligent Home Networking System, 978-1- 4577-0234-1/11 ©2011 IEEE.
4. Broadband forum, CPE WANMANAGEMENT PROTOCOL (CWMP), Available: <https://www.broadband-forum.org/cwmp.php>.
5. Home Device Manager Data Source API Reference Guide 3.0 Copyright 2005–2009 Alcatel-Lucent
6. André Ribeiro, Afonso Silva, Alberto Rodrigues da Silva Data Modeling and Data Analytics: A Survey from a Big Data Perspective Journal of Software Engineering an Applications, 2015, 8, 617-634
7. NAT Issues in the Remote Management of Home Network Devices, Choongul Park, Kitae Jeong, and Sungil Kim, KT Technology Lab, 0890-8044/08 © 2008 IEEE