TECHNICAL REPORT

TR-064
LAN-Side CPE Configuration

Issue: 2
Issue Date: August 2015

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Broadband Forum Technical Report has been approved by members of the Forum. This Broadband Forum Technical Report is not binding on the Broadband Forum, any of its members, or any developer or service provider. This Broadband Forum Technical Report is subject to change, but only with approval of members of the Forum. This Technical Report is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Technical Report may be copyrighted by Broadband Forum members.

THIS SPECIFICATION IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS SPECIFICATION.

Broadband Forum Technical Reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only, and may not be modified without the advance written permission of the Broadband Forum.

The text of this notice must be included in all copies of this Broadband Forum Technical Report.

Issue History

Issue Number	Approval Date	Publication Date	Issue Editor	Changes
1	May 2004	May 2004	Barbara Stark, BellSouth	Original
1 Corrigendum 1	24 August 2015	11 September 2015	Steven Nicolai, Arris Barbara Stark, AT&T	Deprecate the original
2	24 August 2015	11 September 2015	Steven Nicolai, Arris Barbara Stark, AT&T	Describe use of UPnP DM services to do LAN-side configuration

Comments or questions about this Broadband Forum Technical Report should be directed to help@broadband-forum.org.

Editors	Barbara Stark	AT&T
	Steve Nicolai	Arris
BroadbandHome™ WG Chairs	Jason Walls	QA Cafe
	John Blackford	Pace

TABLE OF CONTENTS

List of Figures

Executive Summary

When deploying broadband services for a customer, it is often necessary to perform some manner of configuration in order to provision the initial conditions necessary for the broadband connection to exist and connect to the provider's network before being managed by other means. It's in the interest of service providers to make this as automated as possible.

While providers can use Broadband Forum TR-069 [1] to perform Customer Premises Equipment (CPE) provisioning, management, and diagnostics, it is not always the case that broadband CPE is in a state that allows it to reach a TR-069 Auto-Configuration Server (ACS). Some means of configuring customer premises equipment from the LAN side is desired that can still make use of TR-069's extensive data model.

This Technical Report describes a specific mechanism using UPnP Forum's BasicManagement:2 (BMS:2) and ConfigurationManagement:2 (CMS:2) Device Management (DM) specifications to be used for LAN-side CPE configuration, while still leveraging TR-069 data models to configure the CPE. When properly executed, the installation software provided by the service provider can be used to initially provision the CPE and activate the broadband services.

Issue 2 includes:

- Requirements to support UPnP DM BMS:2 [8] and UPnP DM CMS:2 [9] for LAN-side CPE configuration
- Usage examples
- An updated title of "LAN-Side CPE Configuration Specification". [Note that the Issue 1 title was "LAN-Side DSL CPE Configuration Specification".]

1 Purpose and Scope

1.1 Purpose

This Technical Report describes a specific mechanism using the UPnP Forum's BasicManagement:2 (BMS:2) service (defined in UPnP DM BMS:2 [8]) and ConfigurationManagement:2 (CMS:2) service (defined in UPnP DM CMS:2 [9]) to be used for LAN-side CPE configuration.

1.2 Scope

This Technical Report provides requirements and usages examples for the use of UPnP DM BMS:2 [8] and UPnP DM CMS:2 [9] for LAN-side CPE configuration of devices using the TR-181 Issue 1 Device:1 [3], TR-098 InternetGatewayDevice:1 [2] (DEPRECATED), or TR-181 Issue 2 Device:2 [4] root data models. It does not attempt to address WAN-side configuration, although the described mechanisms can be proxied from the WAN using techniques described in TR-330 [5]. Usage examples that show the sequence of communication are included in Appendix I.

2 References and Terminology

2.1 Conventions

In this Technical Report, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found be in RFC 2119 [6].

MUST	This word, or the term “REQUIRED”, means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the term “RECOMMENDED”, means that there could exist valid reasons in particular circumstances to ignore this item, but the full implications need to be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" means that there could exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications need to be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the term “OPTIONAL”, means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option.

2.2 References

The following references are of relevance to this Technical Report. At the time of publication, the editions indicated were valid. All references are subject to revision; users of this Technical Report are therefore encouraged to investigate the possibility of applying the most recent edition of the references listed below.

A list of currently valid Broadband Forum Technical Reports is published at www.broadband-forum.org.

Document		Title	Source	Year
[1]	TR-069 Amendment 5	*CPE WAN Management Protocol*	Broadband Forum	2013
[2]	TR-098 InternetGatewayDevice:1	*Internet Gateway Device Data Model for TR-069 (DEPRECATED)*	Broadband Forum	

[3]	TR-181 Issue 1 Device:1	*Device Data Model for TR-069*	Broadband Forum	
[4]	TR-181 Issue 2 Device:2	*Device Data Model for TR-069*	Broadband Forum	
[5]	TR-330	*TR-069 UPnP-DM Proxy Management Guidelines*	Broadband Forum	2015
[6]	RFC 2119	*Key words for use in RFCs to Indicate Requirement Levels*	IETF	1997
[7]	UPnP DeviceProtection:1	*DeviceProtection:1 Service*	UPnP Forum	2011
[8]	UPnP DM BMS:2	*BasicManagement:2 Service Template Version 1.01*	UPnP Forum	2012
[9]	UPnP DM CMS:2	*ConfigurationManagement:2 Service Template Version 1.01*	UPnP Forum	2013
[10]	UDA 2.0	*UPnP Device Architecture Version 2.0*	UPnP Forum	2014

2.3 Definitions

The following terminology is used throughout this Technical Report.

ACS	Auto-Configuration Server. This is a component in the broadband network responsible for auto-configuration of the CPE for advanced services.
BMS:2	BasicManagement service defined by UPnP Forum in UPnP DM BMS:2 [8]. This is one of the services that comprise UPnP Forum's Device Management (DM) device category.
CMS:2	ConfigurationManagement service defined by UPnP Forum in UPnP DM CMS:2 [9]. This is one of the services that comprise UPnP Forum's Device Management (DM) device category.
CPE	Customer Premises Equipment. Any device inside a customer's premises network that connects out over an ISP's network, including set-top boxes, Residential Gateways, telephony devices, home networking adaptors, and a variety of other devices.
DeviceProtection:1	DeviceProtection:1 service defined by UPnP Forum in the UPnP DeviceProtection:1 [7] specification. This is an add-on service that can be combined with other UPnP Forum Device Control Protocol specifications to provide secure operation of those protocols.
DM	Device Management is a device category of UPnP Forum's Device Control Protocol specifications. It identifies a group of UPnP device and service descriptions that includes BasicManagement service (BMS), ConfigurationManagement service (CMS), SoftwareManagement service, and ManageableDevice device.

UPnP CP	A UPnP Forum defined application that meets the Control Point requirements of the UPnP Device Architecture (UDA).
UPnP Device	A UPnP Forum defined application that meets the Device requirements of the UPnP Device Architecture.
TR-064 Managed Device	A piece of CPE that can be managed through the mechanisms defined in this Technical Report.
TR-064 Management Application	Software that can manage a TR-064 Managed Device through the mechanisms defined in this Technical Report.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

ACS	Auto-Configuration Server
ACL	Access Control List
BMS:2	BasicManagement:2 service
CD	Compact Disc
CMS:2	ConfigurationManagement:2 service
CP	Control Point
CPE	Customer Premises Equipment
CWMP	CPE WAN Management Protocol
DM	Device Management
IP	Internet Protocol
LAN	Local Area Network
PIN	Personal Identification Number
TR	Technical Report
UDA	UPnP Device Architecture
WAN	Wide Area Network

3 Technical Report Impact

3.1 Energy Efficiency

TR-064 has no impact on energy efficiency.

3.2 IPv6

TR-064 has no impact on IPv6.

3.3 Security

It is important that unauthorized individuals and applications are not able to modify the configuration of CPE. Security is provided through X.509 keys as described in UPnP DeviceProtection:1 [7]. See that document for a theory of operations and discussion of security considerations. Some example usages are in Appendix I.

In addition, UPnP DM CMS:2 [9] and UPnP DM BMS:2 [8] describe various aspects of Access Control Lists (ACLs) and requirements for ACLs within the context of DeviceProtection:1 as applied to CMS:2 and BMS:2 respectively. These documents also describe how additional access roles (beyond Basic, Public, and Admin) can be defined for a particular implementation. This allows service providers additional flexibility in defining who is authorized to configure specific parameters in their CPE.

3.4 Privacy

The mandatory security mechanisms provided by UPnP DeviceProtection:1 [7] provide for privacy by preventing unauthorized access to subscriber information in CPE devices, and encrypting transmission of information.

4 TR-064 Managed Device Requirements

R-1 The TR-064 Managed Device MUST implement UPnP Device requirements of UPnP Device Architecture (UDA) 2.0 [10].

R-2 The TR-064 Managed Device MUST implement a UPnP Device with the CMS:2 service defined in UPnP DM CMS:2 [9] (or any later and backward compatible version) with the Security Feature (which requires the DeviceProtection:1 service defined in UPnP DeviceProtection:1 [7]).

R-3 The objects and parameters of the CWMP data model that will be made available via the CMS:2 service MUST be mapped according to the rules defined in Appendix C.1 of UPnP DM CMS:2 [9].

R-4 All CWMP objects and parameters that are writable via the CMS:2 service MUST include "Subscriber" in their AccessList attribute, as described in TR-069 [1].

R-5 If reboot is necessary for successful application of a new configuration, the TR-064 Managed Device MUST implement BMS:2 service as defined in UPnP DM BMS:2 [8] (or later and backward compatible version) with the Security Feature (which requires the DeviceProtection:1 service defined in UPnP DeviceProtection:1 [7]).

It is possible that the set of parameters exposed or configurable through LAN management is a subset of those for WAN management. This is allowed, but not required.

R-6 In the absence of specific ISP requirements for data model and parameter support, the TR-064 Managed Device SHOULD at a minimum allow reading and configuration of parameters according to the following set of TR-181 Issue 2 Device:2 [4] profiles:

- Baseline:1
- Profiles appropriate to establishing and troubleshooting connectivity on all supported WAN interfaces, from the physical layer interface up to the IP interface (e.g., VDSL2:1, PTMLink:1, and IPInterface:1 for a VDSL2 connection).

5 TR-064 Management Application Requirements

R-7 The TR-064 Management Application MUST implement UPnP Control Point (CP) requirements of UDA 2.0 [10].

R-8 The TR-064 Management Application MUST implement CMS:2 CP functionality as defined in UPnP DM CMS:2 [9] (or any later and backward compatible version) with the Security Feature (which requires the DeviceProtection:1 CP functionality defined in DeviceProtection:1 [7]).

R-9 If the TR-064 Management Application expects to operate with TR-064 Managed Devices that use BMS:2 to support reboot, and a reboot is required to successfully complete configuration, then the UPnP CP MUST implement BMS:2 CP functionality as defined in UPnP DM BMS:2 [8] (or any later and backward compatible version) with the Security Feature (which requires the DeviceProtection:1 service defined in UPnP DeviceProtection:1 [7]).

R-10 If user interaction is needed to establish security, the TR-064 Management Application MUST provide a user interface that will allow for such interaction.

6 Potential Future Enhancements

If the reboot function is supported as a data model parameter, then BMS:2 will not be needed.

Appendix I. Usage Examples

All usages assume a TR-064 Managed Device (e.g., Residential Gateway, Set-Top Box) and device with a TR-064 Management Application (e.g., smartphone, tablet, personal computer) that can communicate via IP on a local area network (LAN).

I.1 Basic Usage Example

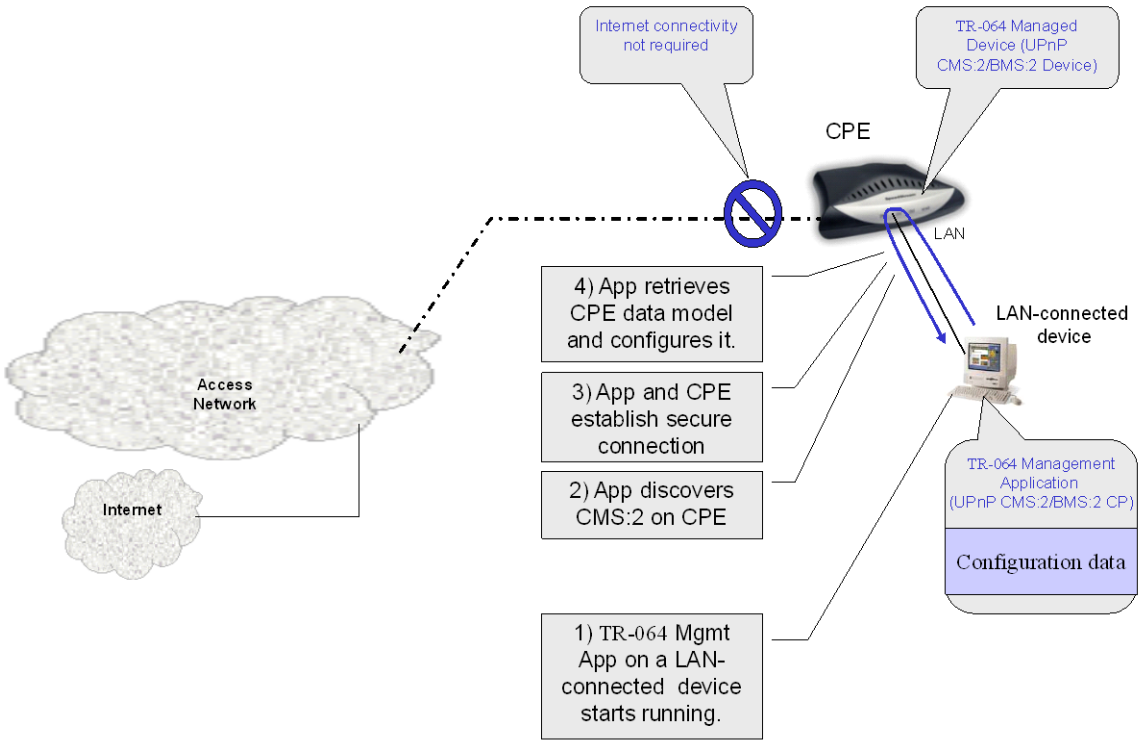

Figure 1: LAN-side CPE Management Example

Figure 1 shows a basic usage example. For this usage, no Internet connectivity is assumed. The steps involved in doing LAN-side configuration are:

Pre-requisite Step: TR-064 Management Application is placed on a LAN-connected device. Section I.1.1 lists examples of possible ways to accomplish this.

1. The TR-064 Management Application (which includes a UPnP CP with CMS:2 CP and DeviceProtection:1 CP functionality) starts running.
2. UPnP CP discovers the CPE's CMS:2 per UDA 2.0 [10] device discovery mechanisms. Section I.1.2 lists examples of possible ways to accomplish this.

3. TR-064 Managed Device and TR-064 Management Application use the security feature (UPnP DeviceProtection:1 service) to negotiate a secure connection. Section I.1.3 lists examples of possible ways to accomplish this.
4. TR-064 Management Application uses CMS:2 actions to retrieve the CPE data model and retrieve and configure parameter values.

Note: If reboot is needed, BMS:2 is used to invoke this function.

I.1.1 More Detailed Examples for Placing an Application on a Device

Following is an incomplete and non-exhaustive list of possible means for getting an application on a LAN-connected device. These are presented just to provide some ideas as to how this might be accomplished.

- Customer receives a CD, and runs the CD on a LAN-connected laptop or other general-purpose computing device.
- Technician is on the premises doing installation and connects a company laptop (with application already loaded) to the LAN.
- Customer downloads an app to a smartphone and subsequently connects it to the LAN.

I.1.2 More Detailed Step 2 Examples

If there are multiple CMS:2 implementations present on the LAN, it will be necessary for the TR-064 Management Application to identify the CMS:2 instance it is expected to configure. Following is an incomplete and non-exhaustive list of possible means for the TR-064 Management Application to identify the desired CMS:2 instance. These are presented just to provide some ideas as to how this might be accomplished.

- Use the UPnP Friendly Name (defined in UDA 2.0 [10]) to identify devices of interest. Whoever defines the default/factory configuration of the CPE can specify the UPnP Friendly Name it will use.
- If the CMS:2 implementation allows the *GetSupportedDataModels()* action to be invoked with the Public role (as recommended in UPnP DM CMS:2 [9]), then the TR-064 Management Application can see if the desired CWMP data model is supported, before trying to establish a secure connection.
- The TR-064 Management Application could go through the process of trying to establish a secure connection (described in UPnP DeviceProtection:1 [7]). The success of this process, or the credentials supplied during this process may be used to identify CPE that can be managed by this TR-064 Management Application.

I.1.3 More Detailed Step 3 Examples

The user interfaces that provide access to DeviceProtection:1 functionality (on both the TR-064 Managed Device and TR-064 Management Application), and the TR-064 Managed Device rules as to which actions and data require Admin role to invoke (and whether there are different rules depending on previous configuration state) are implementation-specific. Different Service Providers will want different user interfaces and different rules for the CPE they supply to their subscribers. Some possible behaviors are described in the following incomplete and non-exhaustive list.

- The TR-064 Managed Device provides Admin privilege to any UPnP CP that establishes Public DeviceProtection:1 role (which does not involve user interaction) with it when the TR-064 Managed Device is unconfigured. After being configured by that UPnP CP, it assigns DeviceProtection Admin role to that UPnP CP.
- The TR-064 Managed Device has a PIN printed on its label that can be entered to allow Admin privilege.
- The TR-064 Managed Device has a screen that allows it to display a Personal Identification Number (PIN).
- The TR-064 Managed Device can provide a PIN from a https web page served by the TR-064 Managed Device.
- The TR-064 Managed Device has a https web page that allows the user to configure the role of authenticated UPnP CPs.

It is recommended that any https web pages served by the TR-064 Managed Device be appropriately secured. Securing such a web page is outside the scope of this document.

See Section 3, Theory of Operations, of UPnP DeviceProtection:1 [7] for additional information and usage scenarios for how to assign the Admin role to a TR-064 Management Application, for management of the TR-064 Managed Device.

I.2 Proxied Example

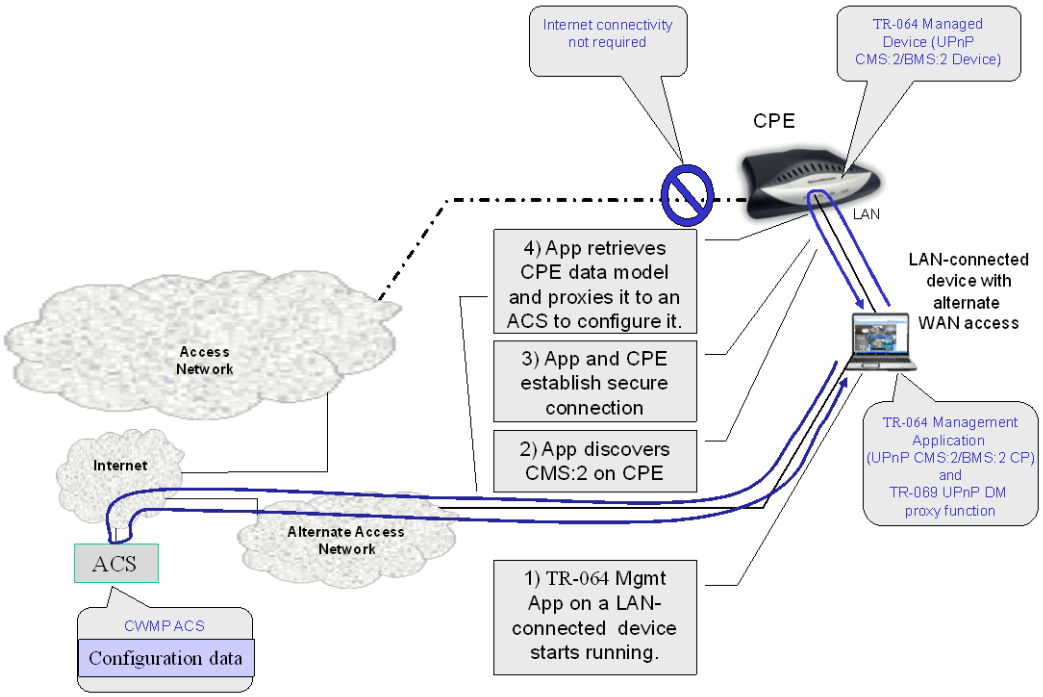

Figure 2: Proxied Example

The device with the TR-064 Management Application may have its own Internet connectivity (e.g., a smartphone or laptop with both Wi-Fi and cellular), and the application may include a TR-069 UPnP DM proxy function as defined in TR-330 [5]. This would allow the LAN management application to be used remotely for configuration and diagnostics. Figure 2 shows an example of proxied configuration. Note that this has a different Step 4 than the Basic Usage Example, because the configuration is proxied from the ACS.

If the Wi-Fi station functionality and mobile wireless data radio interface cannot be simultaneously active, it may be necessary for the application to be able to toggle use of the two connections.

Some devices (such as a laptop with Wi-Fi, Ethernet, and cellular) provided by the service provider to their installation technicians) may be able to have multiple network interfaces active simultaneously.

End of Broadband Forum Technical Report TR-064