TECHNICAL REPORT

TR-356
Alternate Management Path for Broadband

Issue: 1
Issue Date: October 2016

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Technical Report has been approved by members of the Forum. This Technical Report is subject to change. 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.

Intellectual Property

Recipients of this Technical Report are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of this Technical Report, or use of any software code normatively referenced in this Technical Report, and to provide supporting documentation.

Terms of Use

1. License

Broadband Forum hereby grants you the right, without charge, on a perpetual, non-exclusive and worldwide basis, to utilize the Technical Report for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, products complying with the Technical Report, in all cases subject to the conditions set forth in this notice and any relevant patent and other intellectual property rights of third parties (which may include members of Broadband Forum). This license grant does not include the right to sublicense, modify or create derivative works based upon the Technical Report except to the extent this Technical Report includes text implementable in computer code, in which case your right under this License to create and modify derivative works is limited to modifying and creating derivative works of such code. For the avoidance of doubt, except as qualified by the preceding sentence, products implementing this Technical Report are not deemed to be derivative works of the Technical Report.

2. NO WARRANTIES

THIS TECHNICAL REPORT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS TECHNICAL REPORT SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE BROADBAND 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 TECHNICAL REPORT.

3. THIRD PARTY RIGHTS

Without limiting the generality of Section 2 above, BROADBAND FORUM ASSUMES NO RESPONSIBILITY TO COMPILE, CONFIRM, UPDATE OR MAKE PUBLIC ANY THIRD PARTY ASSERTIONS OF PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS THAT MIGHT NOW OR IN THE FUTURE BE INFRINGED BY AN IMPLEMENTATION OF THE TECHNICAL REPORT IN ITS CURRENT, OR IN ANY FUTURE FORM. IF ANY SUCH

Issue History

Issue Number	Approval Date	Publication Date	Issue Editor	Changes
1	17 October 2016	14 December 2016	Peter Silverman ASSIA Inc.	Original

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

Editor	Peter Silverman	ASSIA Inc.	psilverman@assia-inc.com
Broadband User Services Work Area	John Blackford Jason Walls	ARRIS QA Cafe	john.blackford@arris.com jason@qacafe.com
Alternative Management Path Project Stream	Peter Silverman,	ASSIA Inc	psilverman@assia-inc.com

TABLE OF CONTENTS

LIST OF FIGURES

Executive Summary

This Technical Report describes managing Customer Premises Equipment (CPE) using an alternate management path when the CPE's primary management path is unavailable (e.g., initial installation of the CPE, faulty broadband connection). For example, an alternate management path can be established by connecting a smartphone to the CPE via the CPE's LAN interface and connecting the smartphone to a network-based management system over a cellular data network, in order to troubleshoot an unavailable broadband connection. This Technical Report contains a reference functional architecture, descriptive use cases, security and privacy considerations, and requirements.

1 Purpose and Scope

1.1 Purpose

Faults or impairments on a broadband connection can disable or restrict remote management of the CPE. In such cases a network technician typically cannot perform management actions remotely (e.g., root-cause diagnosis of the impairment) and must dispatch an outside plant technician to the customer premises. This category of "truck rolls" represents a major component of the access network operational expense for many service providers, and so ways of reducing the number of these service calls are actively sought. This Technical Report supports both service providers deploying, and developers of, CPE and management systems. This Technical Report describes the use of alternate communications devices, such as smartphones or wireless-enabled tablets, to provide an alternate channel or data path for remote management of CPE in cases of a faulty or impaired broadband connection.

1.2 Scope

This Technical Report provides the reference model and functional architecture for use of the alternate management path between the CPE's management system and the CPE in the context of the TR-169 Network Management Architecture as well as TR-178 [2], ITU-T G.997.1 [3] and ITU-T G.997.2 [4]. Use cases that focus on diagnosing and (re-)establishing a CPE's broadband interface are defined using the reference architecture described in this Technical Report when communication between the CPE's management entity and the CPE is unavailable using the primary management path. Impacts to the functions of affected components, including privacy and security impacts, defined by reference architecture are described and requirements are identified for the impacted areas. Requirements are defined for communications over an alternate management path between an alternate communication device and CPE management system, and between that alternate communication device and the impacted CPE. Additionally, requirements are provided for the alternate communication device.

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.

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-169 EMS to NMS Interface Requirements for Access Nodes Supporting TR-101	BBF	2008
[2]	TR-178 Multi-service Broadband Network Architecture and Nodal Requirements	BBF	2014
[3]	G.997.1 Physical layer management for digital subscriber line transceivers	ITU-T	2012
[4]	G.997.2 Physical layer management for G.fast transceivers	ITU-T	2015

[5]	TR-064 Issue 2 - *LAN-Side CPE Configuration*	Broadband Forum	2015
[6]	TR-069 Amendment 5 - *CPE WAN Management Protocol*	Broadband Forum	2013
[7]	TR-330 TR-069 UPnP DM Proxy Management Guidelines	Broadband Forum	2015

2.3 Definitions

The following terminology is used throughout this Technical Report.

Alternate Communication Device (ACD)	The Alternate Communication Device (ACD) is responsible for mediating communications between elements at the customer premises over the T reference point and the communications with the CPE Management System over the G´-reference point.
Alternate Management Application	The alternate management application on the ACD establishes and maintains the alternate management path and proxies management functions between the CPE Management System and the target CPE or LAN CPE.
Alternate Management Path	Alternate management path is a communication path, separate from the broadband line, that relays diagnostics data, instructions, and control signals between network management systems and CPE, premises networks, or subscribers.
CPE Management System	The management system that communicates with the CPE across the primary or alternate management paths, performs analyses, and provides outputs. This is located in the broadband network outside of the customer premises. The CPE Management System can be implemented by an ACS.
Management Agent	The Management agent in the CPE (i.e., LAN Management Agent, Management Agent) that provides management capabilities in the CPE.

2.4 Abbreviations

This Technical Report uses the following abbreviations:

ACD	Alternate Communication Device
ACS	Auto-Configuration Server
AN	Access Node
AP	Access Point
app	Application
B-NT	Broadband-Network Termination

CPE	Customer Premises Equipment
CWMP	CPE WAN Management Protocol
DPU	Distribution Point Unit
DQM	DSL Quality Management
DSL	Digital Subscriber Line
DSM	Dynamic Spectrum Management
EM	Element Management
EMS	Element Management System
FCAPS	Fault, Configuration, Accounting, Performance, Security
FTTdp	Fiber to the Distribution Point
GUI	Graphical User Interface
GPON	Gigabit Passive Optical Network
RG	Residential Gateway
LAN	Local Area Network
LED	Light Emitting Diode
M2M	Machine to Machine
MELT	Metallic Line Test
NE	Network Element
NMS	Network Management System
OAM	Operations, Administration, and Management
ONU	Optical Network Unit
PMA	Persistent Management Agent
RPF	Reverse Power Feed
SELT	Single-Ended Line Test
TR	Technical Report
UPnP	Universal Plug and Play
VDSL	Very high rate Digital Subscriber Line
WAN	Wide-Area Network

3 Technical Report Impact

3.1 Energy Efficiency

TR-356 has no impact on energy efficiency.

3.2 IPv6

TR-356 has no impact on IPv6.

3.3 Security

TR-356 may have issues related to security as the alternate management path and its elements must be secured to prevent tampering with existing management functionality, breaches in confidentiality, theft of service, and unauthorized access. See Section 7.1 for details.

3.4 Privacy

TR-356 may have issues related to privacy as the distinction between private and network data must be upheld and use of the alternate management path must not allow access to the users' private data. See Section 7.2 for details.

4 Introduction

The management of CPEs utilizes the following network management architecture that was first described in TR-169[1] for management of access nodes and is extended in this Technical Report for the management of CPEs where Auto-Configuration Server (ACS) and access node EMS provide the Element Management (EM) functions and the CPEs in the Premises Network provides the necessary Network Element (NE) functions. The management path between the ACS/access node EMS and the CPE is established using the broadband line across the TR-178 *U-reference point [2]*. The access node EMS to CPE management path functions is typically limited to the management of the broadband connection between access node and the CPE (e.g., management of GPON ONU, xDSL OAM). In some cases the NMS may communicate directly to the access node without going through an access node EMS.

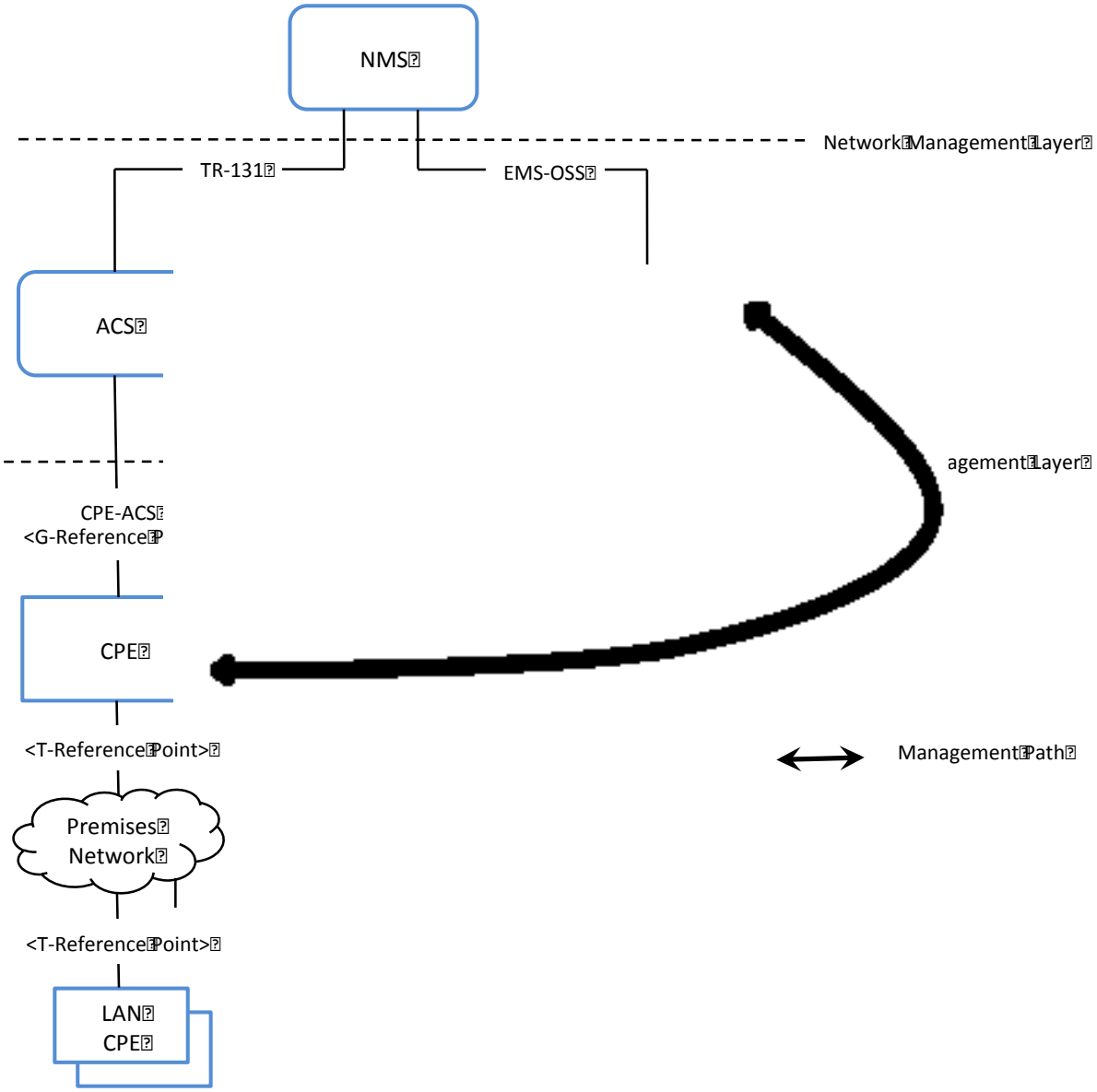

Figure 1 CPE Management - Primary Path

Figure 1 shows the primary path for CPE management. When the connectivity between the CPE and its management systems (i.e. ACS, access node EMS) is unavailable an alternate management path can be established using an alternate communication device that acts as a communications proxy between the management system and CPE as shown in Figure 2.

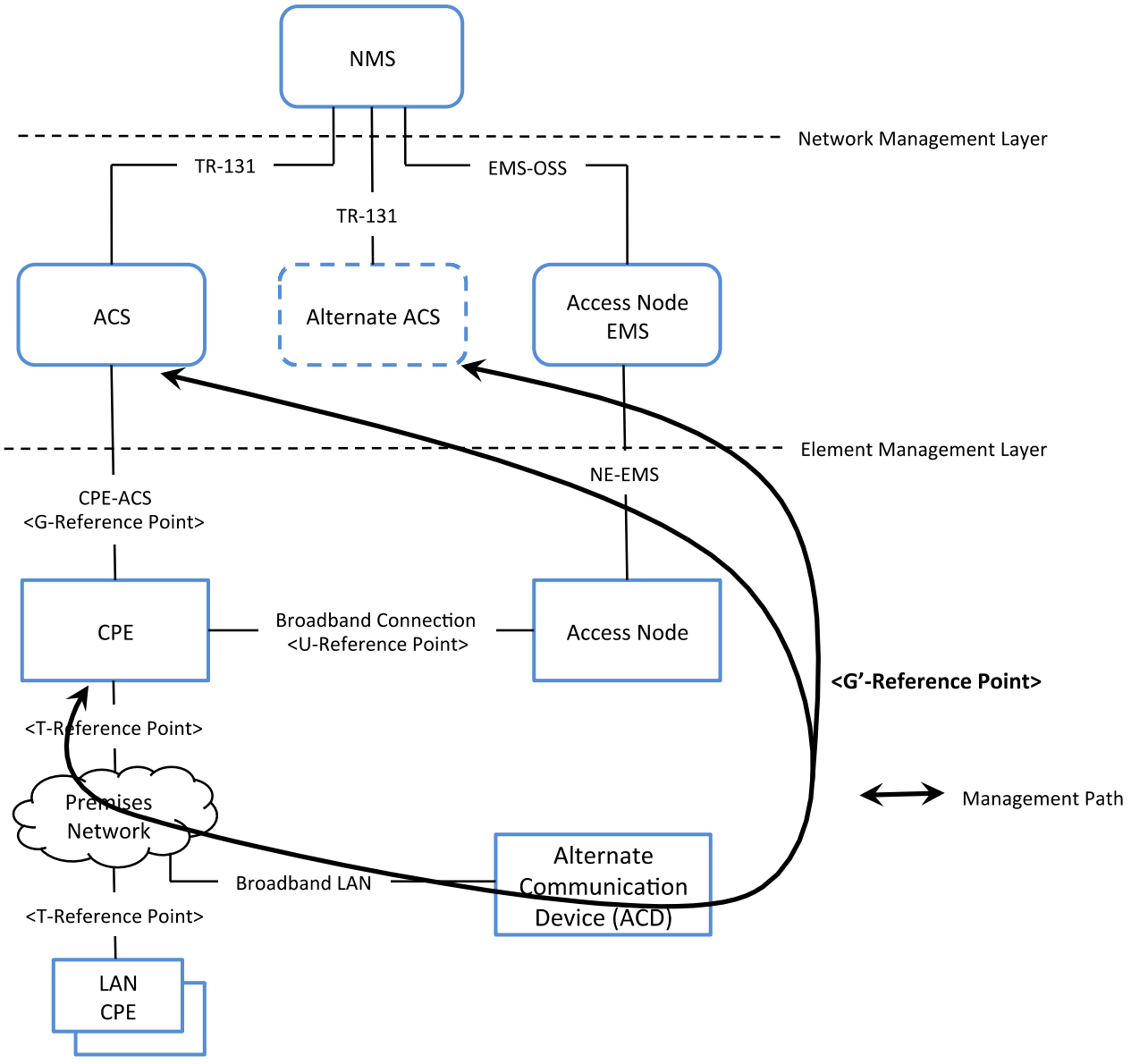

Figure 2 CPE Management - Alternate Path

Figure 2 depicts how an alternate communication device is used within the customer premises network to establish a management path between the CPE and the CPE's management system. Reference points in the figures include:

U-reference point: The reference point that describes the broadband connection between the CPE and the access node.

T-reference point: Premises network reference point between the CPE and other elements in the Premises Network.

G-reference point: Management reference point between the CPE and management systems (including ACS) for which the management flow is not mediated by the management entity on the access node. The *G-reference point* utilizes the primary broadband connection.

G´-reference point: Management reference point between the ACD and management systems (including the ACS) that traverses the alternate management path. The G´-*reference point* is distinguished from the *G-reference point* in that the primary broadband connection is not utilized for the management traffic.

5 CPE Management Reference Functional Architecture

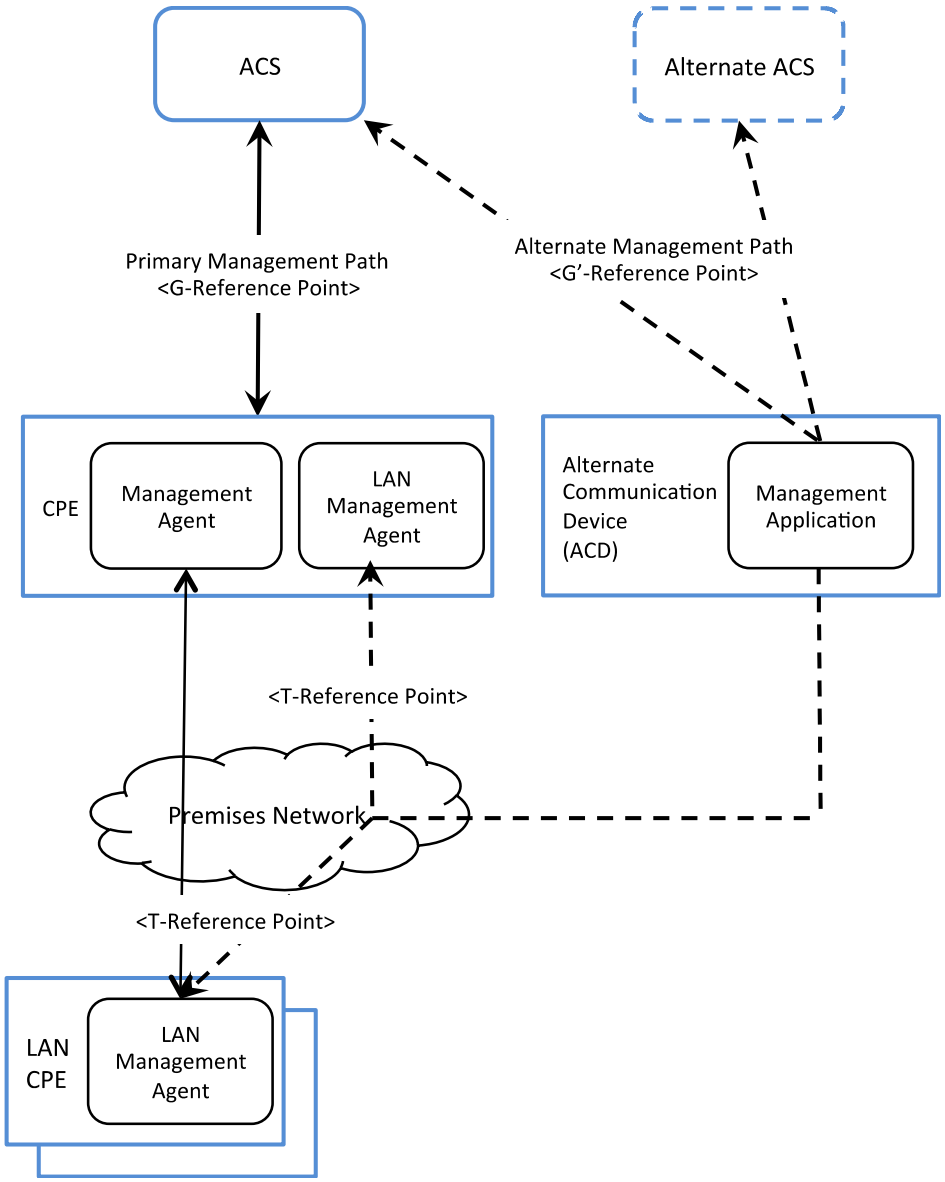

Figure 3 CPE Management Reference Architecture

The CPE management reference architecture is shown in Figure 3. The *primary management path* operates over the *G-reference point*, and normally management messages flow between the ACS and the CPE over this path. For managed CPE in the LAN, the LAN CPE is managed across the *T-reference point*. The *alternate management path* operates from one side of the *Alternate Communication Device* (ACD) across the G′*-reference point* to the ACS or the Alternate ACS. On the other side of the ACD, the *alternate management path* operates between the ACD and the CPE across the *T-reference point*. Essentially the G′*-reference point* represents the use of a physical path to transport management traffic that is distinct from the physical path that the primary management path utilizes. The alternate management path can be used to transmit diagnostics data from the CPE

through the *ACD* to the *CPE Management System*, as well as to transmit control data or guidance back down from the *CPE Management System* through the *ACD* to the CPE.

Using the alternate management path the *ACD* can communicate with systems other than the *CPE Management System* (i.e. ACS) that is used with the primary management path. For example, the *ACD* could communicate with an alternative ACS that is used for purposes such as troubleshooting, self-install, etc.

The *ACD* allows the managed CPEs in the customer premises network to exchange data with a *CPE Management System* located in the broadband network outside the customer premises across the G´-*reference point*. The functionality of the *ACD* could be implemented within the CPE that also supports the *G-reference point*, another LAN CPE or a device attached to the Premises Network.

The *alternate management application* on the *ACD* establishes and maintains the alternate management path and proxies management functions between the *CPE Management System* and the target CPE or LAN CPE. In addition, the *alternate management application* on the *ACD* can facilitate the monitoring and diagnostics of the premises network and LAN CPEs, including troubleshooting an impaired primary broadband connection. The *alternate management application* could perform some diagnostics analyses locally, and analyses can be performed jointly between the *alternate management application* and *CPE Management System*. The *alternate management application* on the ACD can provide a user interface to accept user inputs and output data and instructions.

The *CPE Management System* can perform analyses and decide what steps may help remediate the impairment (e.g., initiate re-configurations, issue trouble tickets, issue troubleshooting instructions). Historical diagnostics and configuration data can also be stored by the *CPE Management System* and used for analysis, particularly for repetitive or chronic troubles. The *CPE Management System* can work in conjunction with other management systems within the service provider domain (e.g. work force management, call center technicians).

The *Management Agent* in the CPE (i.e. LAN Management Agent, Management Agent) provides some FCAPS management capabilities within the CPE. As shown in Figure 3, the distinction between the Management Agent and the LAN Management Agent is dependent on the reference point (e.g., G-reference point, G´-reference point) over which the *CPE Management System* connects with the CPE.

6 Descriptive Use Cases

6.1 Descriptive Use Case 1 - Remediate Broadband Line Failure

In this use case, a broadband line experiences a failure that renders the primary broadband connection inoperable (e.g. failed WAN interface on the CPE, copper or fiber access link failure, failure of the backhaul link from an access node). Once the failure is detected, the alternate management connection is then set up and used to enable remote management. A specific example of an alternate management path is shown in Figure 4, where an alternate management application in an ACD is connected to the CPE using WiFi across the T-Reference Point, and is also connected to management systems in the network using LTE across the G´-Reference Point. The ACD is an application that can reside on a smartphone, tablet, personal computer or other CPE. The management application could include a TR-069 UPnP DM proxy function as defined in TR-330 [7] which enables the CPE Management System to manage the RG; this arrangement is described in TR-064i2 [5].

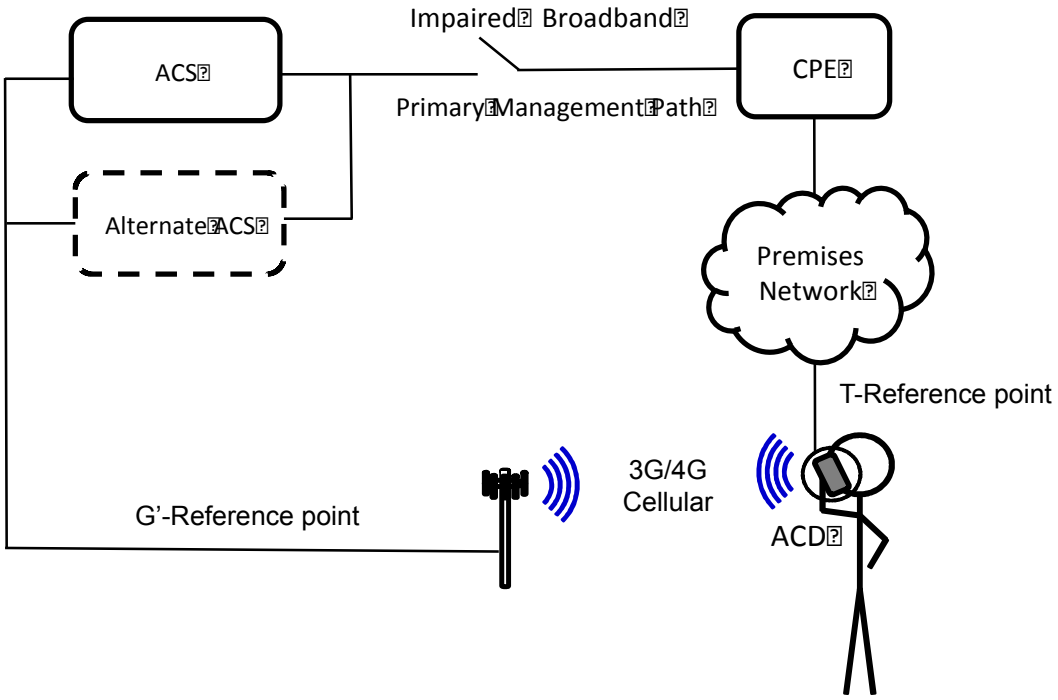

Figure 4 Using Local Wireless and Cellular Data to Enable Remote Management

Once the alternate management path between the ACD and the management system is established, the management system or management application on the ACD initiates remediation actions, such as:

- Provide instructions to guide the user or technician to resolve the trouble, which are tailored to repairing or improving the particular line or customer premises network depending on analyses of the diagnostics data. These can provide case-by-case guidance to the user, in the form of prompts, questions, and tasks to be executed.

- Automatically implement “repairs” or improve broadband performance with no manual intervention, by automatically re-configuring equipment, networks, and systems.
- Simple repair actions such as modem reboot, WiFi driver reboot, WiFi channel change can be attempted.
- Re-configure CPE or the premises network.
- Issue trouble tickets to dispatch to an identified area: inside, outside plant, customer premises, CPE configuration, or application.
- Invoke test modes and diagnostics for the broadband line. Single-Ended Line Test (SELT), Metallic Line Test (MELT), or other diagnostics modes can be performed by metallic CPE.
- Configure the CPE for enhanced capabilities such as noise cancellation.
- Capture and transmit images of the CPEs to the service provider, thus allowing the service provider to directly determine the status of LEDs or displays, check cabling, etc.
- Provide instructional videos (e.g., fault isolation, configuration) that can be downloaded and viewed by the customer;
- For FTTdp deployments, diagnose a Reverse Power Feed (RPF) disconnection or impaired operation.
- For the CPE management system, provide inputs to other network management systems, for example a trouble ticketing system, work-force management system, statistical analysis systems, monitoring system. The output can include alarms indicating faults, disconnections, poor performance, or monitoring anomalies.

6.2 Descriptive Use Case 2 - Initial Configuration of the Broadband Connection, the CPE, and Self Install

In this use case the broadband connection has never been established and the alternate management path is utilized to allow a network operator or other entity to remotely assist in the initial configuration, trouble-shooting, and diagnosis of the turn-up of the service. The user can be guided in the installation process by instructions issued over the alternate management path. The alternate management path also allows remote access to the CPE for configuration of the CPE to accept the connection, gather information, and run tests including tests from the CPE on the primary broadband physical connection such as SELT or MELT from the CPE. This use case may utilize the functionality described in Use Case 3 where a downloadable app communicating from a smart phone assists the end user based on information gathered over the alternate management path in setting up the connection.

This use case is distinguished from Use Case 1 in that the primary management path has never been established, thus there is no historical information or expectation how the management processes should operate. There is no certainty that the primary management path will be able to be established and the CPE may require initial configuration to establish this connection. Use case 2 helps enable customer self-install with its desirable reductions in operational complexity and time to bring up a service.

6.3 Descriptive Use Case 3 - Troubleshooting Problems Using a Downloadable Alternate Management Application

In this case, the customer has detected a problem with his service or network and has contacted the service provider using a smartphone. Contact can be via a voice call, email, text, or web interface, and support can be provided by a technician, web page, or expert system. In this case a fault in the wireline access network prevents the service provider's technical support function from using the primary management path carried by the fixed-line network to diagnose the customer's problem. To establish an alternate management path, the operator installs and activates an alternate management application on a smartphone. The alternate management application enables the alternate management path, provides a GUI that is accessible to the customer, and can also do some analysis of the network. The alternate management application can support contact with a call center via messaging or a telephone call.

6.4 Descriptive Use Case 4 - Stand-Alone Operation

Note: this use case is informative and is not reflected in normative requirements. In this case both the primary G-reference point and the alternate G′-reference point are disabled or unused. This could happen if there is no cellular data coverage, or with smartphones that don't support multiple simultaneous connections. This is a case of LAN-side CPE management, as described in TR-064i2 [5]. In this case, the alternate management path can operate only within the premises network, and the alternate management application can take emergency actions on its own. The alternate management application can retrieve data from the CPE, analyze the data, display it to the user, and possibly change some configurations. The user can read the data to call center agents via messaging or a telephone call. Or, the alternate management application can assist the user in resolving the trouble. In this use case, the ACD could store information for later transmission over the G' interface should a G' path be established at a later time.

6.5 Descriptive Use Case 5 - Support for Agent Access to CPE Graphical User Interface

This use case describes an operator that wishes to diagnose an issue where the G-Reference Point is unavailable (e.g. a CPE has misconfigured PPP credentials and a PPP tunnel cannot be established). The operator's customer service agent has the ability to establish a connection proxy via an ACD to the CPE in the customer's home. Through this connection the agent can then browse the CPE graphical user interface and the agent can then directly resolve the issue by adjusting the configuration on the GUI. Rather than the agent diagnosing the problem by looking at error logs and information from the device data model hosted on the ACS or other Operational Support System (OSS), it allows viewing the problem from the customer's perspective and can therefore lead to quicker resolution of the problem.

The implementation of this use case can be satisfied by following the architectural pattern defined for the alternate management path. As part of a diagnostics call with a customer service agent, the customer would be asked to run a diagnostics application (the *alternate management application*) on the ACD that will act as a proxy to the CPE in the customer premises. The alternate management application would register itself with a management service in the operator's OSS and notify that it is available to perform the proxying function. The customer service agent could then see the availability of the alternate management path and establish the G'-Reference Point connection from the service provider's OSS to the CPE. The ACD would proxy, in this case HTTP/S, traffic between the service and the CPE. The service would ensure that access was only restricted to the relevant

resources on the customer's LAN, and that the agent was logged in to the CPE (which may involve the secure transfer of credentials stored at the ACS). To allow real time browsing of the CPE GUI the ACD would need to support 2 simultaneous network interfaces.

As per section 7.1 Security Requirements the connection between the ACD and the CPE would be secured; in this case the connection would be encrypted via TLS and the ACD would check the authenticity of the operator service.

6.6 Description of Other Uses

Customer self-install, reverse-powering of the DPU from the customer's premises, and remote management from a Persistent Management Agent (PMA) are fundamental to FTTdp and these all present possible failure modes whose resolution can be assisted by an alternate management path.

The alternate management path provides a connection for management in situations where optimization, diagnosis or repair of the primary path requires a period without frequent interruptions, such as retrains, in the primary management path to accomplish these operations. The alternate path provides a continuous management channel during this period of intermittent operation of the primary path.

Additional uses of the alternate management path include use by a service provider who is not a network operator, such as a provider of a Machine-to-Machine (M2M) service. Also, the alternate management path could be part of a connection also used for user data, providing a failover connection, or even just to bolster the speed of the primary broadband connection. This is essentially hybrid access.

7 Issues Related to Access to Data over the Alternate Management Path

The alternate management path may access data within the CPE, possibly including the CWMP data model. Maintaining consistency of data between use of the alternate management path and use of the primary management path is critical, therefore access to this data, particularly write access, needs to be secure and private.

7.1 Security

There needs to be mechanism(s) to handle authentication, authorization and access to network resources and attached devices and their information (including the information that the device exists). The complexity and restrictions involved depend on the requirements of the applicable use cases, and in particular the use case with the greatest sensitivity to security risks.

Security goals include:

- Prevent tampering with the management functions of the CPE and network devices and systems.
- Provide confidentiality for the transactions that take place between the CPE and management system.
- Allow appropriate authentication for each type of transaction.
- Prevent theft of service.
- Block unauthorized intrusion into users' data and systems, particularly for the ACD and CPE Management System.
- Block unauthorized intrusion into a CPE Management System and other providers' systems, particularly from the LAN CPE, CPE, and ACD.

End-to-end trust can be established by securing the individual alternate management interfaces: the interface between the CPE and ACD (T-reference point), and the interface between the ACD and CPE Management System (G'-reference point). This may also extend to include the interface between the ACD and LAN CPE (T-reference point). Additionally the alternate management application would also need to be secured.

An Access Control List (ACL) can determine which nodes, functions, or actors have read or write access to each parameter. The AccessList attribute as described in TR-069 [6] can grant write access to a subscriber or subscriber LAN interface (T-reference point) for specified parameters(s). If TR-064i2 [5] is used as the LAN interface, then CWMP objects and parameters that are writable via the CMS:2 service are required to include "Subscriber" in their AccessList attribute, as described in TR-069 [6].

7.2 Privacy

There is a distinction between private user data and network data that must be upheld. Subscribers' privacy must be upheld, and the ACD and CPE Management System (G'-reference point) are not to allow access to subscriber's private user data.

In addition, the alternate management path must not allow a subscriber unauthorized access to private data about the network or about other subscribers.

8 Requirements for an Alternate Management Path for Broadband

The following requirements apply to situations where the alternate management path is supported by CPE Management Systems and CPE.

8.1 General Requirements

R-1 A CPE Management System MUST be able to communicate with the CPE through the ACD when the primary management path is down.

R-2 A CPE Management System SHOULD be able to communicate with the CPE through the ACD when the primary management path is up

R-3 A CPE Management System MUST NOT use the alternate management path when the primary path is up unless it is communicating with an Alternate ACS.

R-4 A CPE Management System or ACD MUST be able to establish and use an alternate management path connection to the CPE.

R-5 The CPE MUST be able to transmit diagnostic data over the alternate management path.

R-6 A CPE Management System MUST be able to receive diagnostic data transmitted over the alternate management path from the CPE.

R-7 It MUST be possible to query for diagnostic data by a transaction initiated by a CPE Management System over the alternate management path.

R-8 Autonomous data SHOULD be able to be sent by the CPE during operation of an alternate management path.

R-9 A CPE Management System SHOULD be able to write CPE data model parameter(s) over the alternate management path to the CPE.

R-10 A CPE Management System SHOULD be able to initiate tests on the CPE, such as CPE Single-Ended Line Test (SELT) or LAN tests.

R-11 If the CPE initiates tests, then the CPE SHOULD be able to report the test results over the alternate management path to a CPE Management System.

R-12 The ACD SHOULD be able to proxy HTTP traffic between the CPE and a service hosted at the operator's ACS such that an agent at the operator can view and manipulate the CPE GUI.

8.2 Requirements relating to the T and G'- reference points

R-13 It MUST be possible to establish and use an alternate management path connection between a CPE Management System and an ACD across the G'-reference point.

R-14 The CPE Management System and the ACD SHOULD support proxying of HTTP traffic for communication across the G'-reference point to allow access to the CPE GUI.

R-15 The CPE Management System and the ACD MUST support TR-069[6] for communication across the G'-reference point.

R-16 It MUST be possible to establish and use an alternate management path connection between the CPE LAN Management Agent and ACD across the T-reference point.

R-17 The CPE LAN Management Agent and the ACD MUST support TR-064i2[5] for communication across the T-reference point.

R-18 Other LAN-side CPE management interfaces MAY be supported across the T-reference point in addition to TR-064i2[5].

8.3 Transaction Requirements

R-19 The CPE MUST only write parameters that are allowed and authorized for writing over the alternate management path into its data model.

R-20 A CPE Management System MAY be able to transmit guidance to users or technicians over the alternate management path.

R-21 The ACD SHOULD provide a local user interface for user access.

R-22 The CPE MAY expose a Graphical User Interface to the ACD to allow transactions to be made from the CPE Management System that allow agents secure access to the CPE Graphical User Interface.

R-23 It MUST be possible to transmit all CPE data that is exposed via CWMP data model objects and parameters across the alternate management path.

8.4 Security Requirements

R-24 All communications over the alternate management path MUST be able to be secured.

Note that all security requirements for TR-069[6] apply when communication across the G'-reference point uses TR-069. Access control to the CPE data models is supported by TR-69. Also, all security requirements for TR-064i2[5] apply when communication across the T-reference point uses TR-064i2.

R-25 In cases where protocols in addition to TR-064i2 are supported over the T–reference point, the following conditional security requirements MUST be supported for these additional protocols:

R-26 Communications between the CPE and ACD (T-reference point) MUST be able to be secured.

R-27 Communications between the ACD and LAN CPE (T-reference point) MUST be able to be secured.

R-28 Unauthorized network access to users' private data MUST NOT be allowed.

R-29 Unauthorized user access to network data MUST NOT be allowed.

R-30 When the ACD is proxying a HTTP connection for GUI access to the CPE, the connection between the ACD and the management systems MUST be secured.

R-31 When the ACD is proxying a HTTP connection for GUI access to the CPE, the connection between the ACD and the CPE MAY be secured.

R-32 When the ACD is proxying a HTTP connection for GUI access to the CPE, the ACD MUST have a secure mechanism for transferring credentials from the CPE management system such that the ACD can authenticate against the CPE GUI.

End of Broadband Forum Technical Report TR-356