ETSI ES 203 069 V1.1.1 (2011-03)

ETSI Standard

Access, Terminals, Transmission and Multiplexing (ATTM); Remote management of CPE over broadband networks; CPE WAN Management Protocol (CWMP)

Reference

DES/ATTM-02012

Keywords

configuration, management, xDSL

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Standard (ES) has been produced by ETSI Technical Committee Access, Terminals, Transmission and Multiplexing (ATTM).

Introduction

The basis of the present document is the Broadband Forum CPE WAN management protocol (CWMP), commonly referred to as TR-069 [1].

The protocol is intended for communication between a CPE and an Auto-Configuration Server (ACS). The CPE WAN management protocol defines a mechanism that encompasses secure auto-configuration of a CPE, and also incorporates other CPE management functions into a common framework.

TR-069 [1] specifies the generic requirements of the management protocol, and methods that can be applied to any TR-069 [1] CPE. Other Broadband Forum Technical Reports (TRs) specify the managed objects, or data models, for specific types of devices or services.

The protocol may be used to manage various types of CPE, including stand-alone routers and LAN-side client devices. It is agnostic to the specific access medium utilized by the service provider, although it does depend on IP-layer connectivity having first been established by the device.

1 Scope

The present document defines the requirements for the remote management of networked devices by a service provider in a consumer's home. It provides an overview of and the necessary normative references to a family of technical specifications (see figure 1). It describes how the various technical specifications in this family are related.

The protocol is intended to provide flexibility in the connectivity model:

- The protocol allows both CPE and ACS initiated connection establishment, avoiding the need for a persistent connection to be maintained between each CPE and an ACS.
- The functional interactions between the ACS and CPE should be independent of which end initiated the establishment of the connection. In particular, even where ACS initiated connectivity is not supported, all ACS initiated transactions should be able to take place over a connection initiated by the CPE.
- The protocol allows one or more ACSs to serve a population of CPE. Each CPE can only be associated with one ACS, while each ACS may be associated with one or more service providers. However, a single physical device may present more than one logical CPE device, each of which may be associated with a different ACS.
- The protocol provides mechanisms for a CPE to discover the appropriate ACS for a given service provider.
- The protocol provides mechanisms to allow an ACS to securely identify a CPE and associate it with a user/customer.

Processes to support such association support models that incorporate user interaction as well as those that are fully automatic.

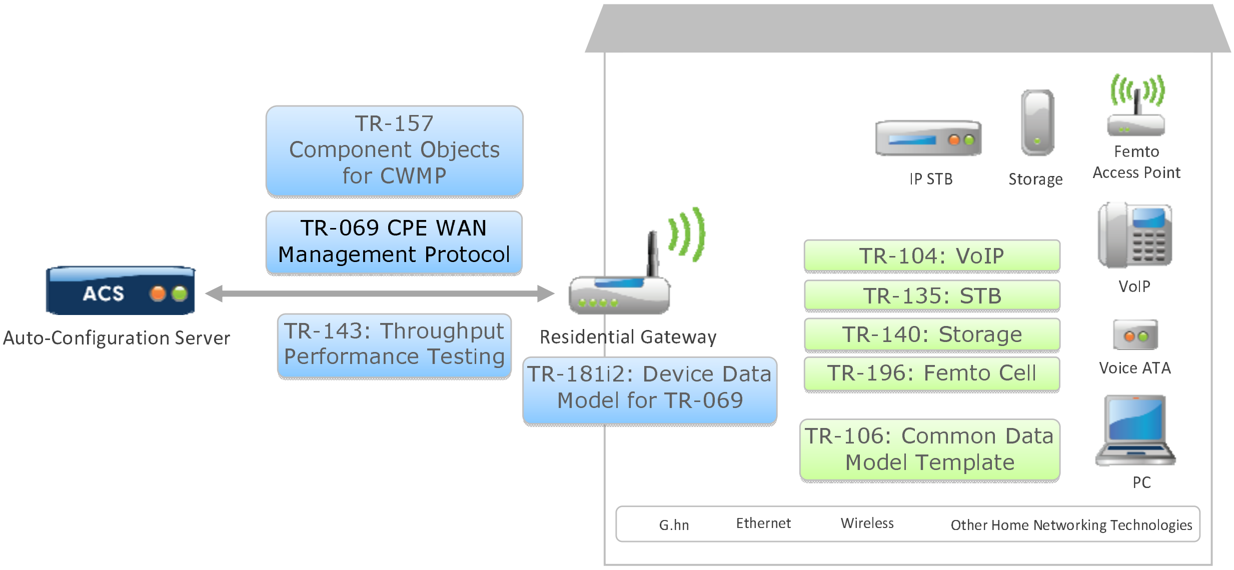
The protocol allows an ACS to control and monitor various parameters associated with a CPE. The mechanisms provided to access these parameters are designed with the following premises:

- Different CPE may have differing capability levels, implementing different subsets of optional functionality. Additionally, an ACS may manage a range of different device types delivering a range of different services. As a result, an ACS must be able to discover the capabilities of a particular CPE.
- An ACS must be able to control and monitor the current configuration of a CPE.
- Other entities besides an ACS may be able to control some parameters of a CPE's configuration (e.g. via LAN-side auto-configuration). As a result, the protocol must allow an ACS to account for external changes to a CPE's configuration. The ACS should also be able to control which configuration parameters can be controlled via means other than by the ACS.
- The protocol should allow vendor-specific parameters to be defined and accessed.

The protocol is intended to minimize implementation complexity, while providing flexibility in trading off complexity vs. functionality. The protocol incorporates a number of optional components that come into play only if specific functionality is required. The protocol incorporates existing standards where appropriate, allowing leverage of off-the-shelf implementations.

The protocol is agnostic to the underlying access network.

The protocol is also extensible. It includes mechanisms to support future extensions to the standard, as well as explicit mechanisms for vendor-specific extensions.



Technical Reports for CWMP and Data Models (see clauses 6.1 and 6.2) are coloured blue.
Technical Reports that define Service Data Models (see clause 6.2.1) are coloured green.

Figure 1: CPE WAN management protocol and its related technical specifications

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] Broadband Forum TR-069 (Amendment 2 - December 2007): "CPE WAN Management Protocol (CWMP) v1.1".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-069_Amendment-2.pdf.

[2] Broadband Forum TR-104 (September 2005): "DSLHomeTM Provisioning Parameters for VoIP CPE".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-104.pdf.

[3] Broadband Forum TR-106 (Amendment 4 - February 2010): "Data Model Template for TR-069-Enabled Devices".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-106_Amendment-4.pdf.

[4] Broadband Forum TR-135 (December 2007): "Data Model for a TR-069 Enabled STB".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-135.pdf.

[5] Broadband Forum TR-140 (Issue 1.1 - December 2007): "TR-069 Data Model for Storage Service Enabled Device".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-140_Issue1.1.pdf.

[6] Broadband Forum TR-143 (Corrigendum 1 - December 2008): "Enabling Network Throughput Performance Tests and Statistical Monitoring".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-143_Corrigendum-1.pdf.

[7] Broadband Forum TR-157 (Amendment 1 - September 2009): "Component Objects for CWMP".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-157_Amendment-1.pdf.

[8] Broadband Forum TR-181 (Issue 2 - May 2010): "Device Data Model for TR-069".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-181_Issue-2.pdf.

[9] Broadband Forum TR-196 (April 2009): "Femto Access Point Service Data Model".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-196.pdf.

[10] ITU-T Recommendation Y.101 (2000): "Global Information Infrastructure terminology: Terms and definitions".

[11] Broadband Forum Technical Report Approval Process.

NOTE: Available at http://www.broadbandforum.org/about/download/trapprovalprocess.pdf.

[12] Broadband Forum TR-181 (Issue 1 - February 2010): "Device Data Model TR-069" (superseded by BBF TR-181 Issue 2).

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-181_Issue-1.pdf.

[13] Broadband Forum TR-098 (Amendment 2 - September 2008): "Internet Gateway Device Data Model for TR-069" (superseded by BBF TR-181 Issue 2).

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-098_Amendment-2.pdf.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

Not applicable.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ITU-T Recommendation Y.101 [10], [11] and the following apply:

Customer Premises Equipment (CPE): end use system including private network elements connecting the customer applications to the access line

remote management: management of CPE over a WAN by a service provider

Technical Report (TR): approved technical specification of the Broadband Forum [11]

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3G	Third Generation Mobile
ACS	Auto-Configuration Server
CPE	Customer Premises Equipment
CWMP	CPE WAN Management Protocol
FAP	Femto Access Point
FDD	Frequency Division Duplex
HNB	3G Home NodeB (aka femtocell)
IPTV	Internet Protocol TeleVision
LAN	Local Area Network
MGCP	Media Gateway Control Protocol
NAS	Network Attached Storage
PVR	Personal Video Recorder
QoE	Quality of Experience
QoS	Quality of Service
RG	Residential Gateway
SIP	Session Initiation Protocol
STB	Set-Top Box
TR	Technical Report
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WEP	Wireless Encryption Protocol

4 Conventions

There are no particular notations, styles, presentations, etc., used within the present document.

5 Remote management of CPE over broadband networks

This clause lists the elements of the CPE WAN management protocol (see clause 5.1) and the data models for specific devices (see clause 5.2) each of which is a normative part of the present document.

5.1 Elements of the CPE WAN management protocol

The requirements for the CPE WAN management protocol are defined in [1].

5.1.1 TR-069: CPE WAN management protocol (CWMP)

TR-069 [1] is intended for communication between a CPE and an auto-configuration server (ACS). The CPE WAN management protocol defines a mechanism that encompasses secure auto-configuration of a CPE, and incorporates other CPE management functions into a common framework.

TR-069 [1] specifies the generic requirements of the management protocol methods, which can be applied to any TR-069 [1] enabled CPE.

From a purely functional perspective, TR-069 [1] supports a variety of functionalities to manage a collection of CPE, including the following primary capabilities:

- Auto-configuration and dynamic service provisioning.

- Software/firmware image management.

- Status and performance monitoring.
- Diagnostics.

5.1.2 Auto-configuration and dynamic service provisioning

CWMP allows an ACS to provision a CPE or collection of CPE based on a variety of criteria.

The provisioning mechanism allows CPE provisioning at the time of initial connection to the broadband access network, and the ability to re-provision or re-configure at any subsequent time. This includes support for asynchronous ACS-initiated re-provisioning of a CPE.

The identification mechanisms included in the protocol allow CPE provisioning based either on the requirements of each specific CPE, or on collective criteria such as the CPE vendor, model, or software version.

The protocol also provides optional tools to manage the CPE-specific components of optional applications or services for which an additional level of security is required, such as those involving payments.

The provisioning mechanism allows straightforward future extension to allow provisioning of services and capabilities not yet included in the present document.

5.1.3 Software/firmware image management

CWMP provides a framework for managing the downloading of CPE software/firmware image files. The protocol provides mechanisms for version identification, file download initiation (ACS initiated downloads and optional CPE initiated downloads), and notification of the ACS of the success or failure of a file download.

5.1.4 Status and performance monitoring

CWMP provides support for a CPE to make available information that the ACS may use to monitor the CPE's status and performance statistics. It also defines a set of mechanisms that allow the CPE to actively notify the ACS of changes to its state. TR-143 [6] facilitates throughput testing to be able to assess the subscribers experience in terms of broadband speed.

5.1.5 Diagnostics

CWMP provides support for a CPE to make available information that the ACS may use to diagnose and resolve connectivity or service issues as well as the ability to execute defined diagnostic tests.

5.1.6 Security

CWMP is designed to provide a high degree of security. The security model is also designed to be scalable. It allows for basic security to accommodate less robust CPE, while allowing greater security for CPE that can support more advanced security mechanisms. The security goals of the CPE WAN management protocol are as follows:

- Prevent tampering with the management functions of a CPE or ACS, or the transactions that take place between a CPE and ACS.
- Provide confidentiality for transactions between CPE and ACS.
- Allow appropriate authentication for each type of transaction.
- Prevent theft of service.

5.2 Data models

A key concept within CWMP is that of a data model. A data model provides objects and parameters that can be acted on by the CMWP generic method calls. These objects and parameters expose configuration, diagnostics, or status data for various types of services and devices. For example, the data model for a VoIP device exposes parameters related to SIP configuration, amongst other VoIP related capabilities. Data models define a superset of functionality that could be managed for a particular device or service; devices implement the portions of the data models that are relevant for their specific functionality.

The requirements for the CPE WAN management data models are defined in TR-106 [3], TR-143 [6], TR-157 [7], TR-181 [8], TR-104 [2], TR-135 [4], TR-140 [5] and TR-196 [9].

TR-106 [3] defines generic information for defining CWMP data models, including requirements around hierarchy, rules for obsolescence and deprecation, data types, and the CWMP-DM XML schema, which is used for defining all data models.

CPE, such as Residential Gateways (RG), Set-Top Boxes (STB) and Network Attached Storage (NAS) devices, are provisioned and managed using a common set of parameters, which make the device recognizable from the network ACS and allow auto-provisioning and ongoing management.

Technical reports that establish these parameters are:

- TR-181 Issue 2 [8].
- TR-157 [7].
- TR-143 [6].

Technical reports that define service data models are:

- TR-104 [2].
- TR-135 [4].
- TR-140 [5].
- TR-196 [9].

5.2.1 TR-181 Issue 2: Device data model for TR-069

TR-181 Issue 2 [8] defines version 2 of the TR-069 [1] device data model. The data model applies to all types of TR-069-enabled devices, including end devices, internet gateway devices, and other network infrastructure devices. It represents a next generation evolution that supersedes both TR-181 Issue 1 [12] and TR-098 amendment 2 [13]. Legacy installations can continue to make use of the InternetGatewayDevice:1 and Device:1 data models, which are still valid.

NOTE: The evolution to Device:2 was necessary in order resolve some fundamental limitations in the InternetGatewayDevice:1 data model, which proved to be inflexible and caused problems in representing complex device configurations. However, in defining this next generation data model, care has been taken to ensure that all InternetGatewayDevice:1 and Device:1 functionality has been covered.

The Device:2 data model defined in TR-181 Issue 2 [8] comprises a set of data objects covering things like basic device information, time-of-day configuration, network interface and protocol stack configuration, routing and bridging management and diagnostic tests. It also defines a baseline profile that specifies a minimum level of data model support.

The cornerstone of the Device:2 data model is the interface stacking mechanism. Network interfaces and protocol layers are modelled as independent data objects that can be stacked, one on top of the other, into whatever configuration a device might support.

5.2.2 TR-157: Component objects for CWMP

TR-157 [7] defines component objects for use in CWMP managed devices for all root data models. A component object is defined as an object and its contained parameters are intended for use in any applicable CWMP root data model. The object(s) may reside at the top level or an appropriate sub-object level.

5.2.3 TR-143: Enabling network throughput performance tests and statistical monitoring

TR-143 [6] defines an active monitoring test suite that can be leveraged by network service providers to monitor and/or diagnose the state of their broadband network paths serving populations of subscribers who have TR-069 [1] compliant CPE. Active monitoring supports both network initiated diagnostics and CPE initiated diagnostics for monitoring and characterization of service paths in either an ongoing or on-demand fashion. These generic tools provide a platform for the validation of QoS objectives and service level agreements.

5.2.4 TR-104: DSLHome provisioning parameters for VoIP CPE

TR-104 [2] defines the data model for provisioning of a voice-over-IP (VoIP) CPE device by an auto-configuration server (ACS) using the mechanism defined in TR-069 [1].

NOTE: TR-104 [2]:

- Accommodates VoIP devices that are either embedded in an internet gateway device or stand alone as independent devices.
- Accommodates VoIP devices that support multiple distinct VoIP services, each potentially with multiple distinct lines.
- Supports the use of both SIP and MGCP signalling protocols.
- Supports various types of VoIP CPE including VoIP endpoints, SIP outbound proxies, and SIP back-to-back user agents.

5.2.5 TR-135: Data model for a TR-069 enabled set-top box

TR-135 [4] provides the specifications for remote management of digital television (IPTV or broadcast) functionality on STB devices via CWMP. Access to network and PVR content is managed by an IPTV service platform, rather than by the ACS. The ACS may perform some initial configuration of a newly installed STB, but its main functions are configuration of STB parameters for trouble management and collection of statistics for QoS/QoE monitoring.

NOTE: TR-135 [4] defines the data model for describing a STB device as well as rules regarding notifications on parameter value change. This provides standard data model profiles that would typically be seen while remotely managing a device of this nature.

5.2.6 TR-140: TR-069 data model for storage service enabled devices

TR-140 [5] allows for a basic storage service to be managed by an ACS. The following is a sample list of support capabilities an ACS can provide using CWMP:

- Basic configuration and setup during device activation (addressed by TR-140 [5] and TR-181 Issue 2 [8]).
- User credentials setup and file privilege access (addressed by TR-140 [5] (folder access)).
- Retrieval of device status (addressed by TR-140 [5] (parameters) and TR-181 Issue 2 [8]).
- Wireless setup (e.g. WEP security) for a storage service device with Wi-Fi access.
- Network diagnostics and troubleshooting, e.g. network connectivity to the Internet gateway device and to the Internet (addressed by TR-181 Issue 2 [8] (connection parameters)).

NOTE: Not all of these capabilities are handled with this data model; some capabilities are part of the native CWMP protocol and some capabilities are handled via other data models.

5.2.7 TR-196: Femto access point service data model

TR-196 [9] specifies the data model for Femto Access Point (FAP) for remote management using CWMP.

The scope of this FAP data model is UMTS FDD home nodeB (3G HNB). However, the structure and organization of the data model takes it into consideration in such a way that it can be extended to cover other type(s) of FAP device based on other radio interface technologies.

Annex A (informative): Bibliography

- Broadband Forum TR-064 (May 2004): "LAN-side DSL CPE Configuration".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-064.pdf.

- Broadband Forum TR-133 (September 2005): "DSLHome TR-064 Extensions for Service Differentiation".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-133.pdf.

- Broadband Forum TR-068 (December 2006): "Base Requirements for an ADSL Modem with Routing".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-068_Issue-3.pdf.

- Broadband Forum TR-124 (December 2006): "Functional Requirements for Broadband Residential Gateway Devices".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-124.pdf.

- Broadband Forum TR-122 (Issue 1.01 - November 2006): "Base Requirements for Consumer-Oriented Analog Terminal Adapter Functionality".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-122v1.01.pdf.

- Broadband Forum TR-131 (November 2009): "ACS Northbound Interface Requirements".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-131.pdf.

- Broadband Forum TR-142 (Issue 2 - February 2010): "Framework for TR-069 enabled PON Devices".

NOTE: Available at http://www.broadband-forum.org/technical/download/TR-142_Issue-2.pdf.

History

Document history		
V1.1.0	January 2011	Membership Approval Procedure MV 20110306: 2011-01-05 to 2011-03-07
V1.1.1	March 2011	Publication