International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.9980

(11/2012)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Access networks – In premises networks

Remote management of customer premises equipment over broadband networks – Customer premises equipment WAN management protocol

Recommendation ITU-T G.9980

International Telecommunication Union

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
ACCESS NETWORKS	G.9000–G.9999
In premises networks	**G.9900–G.9999**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T G.9980

Remote management of customer premises equipment over broadband networks – Customer premises equipment WAN management protocol

Summary

Recommendation ITU-T G.9980 defines 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. It describes how the various technical specifications in this family are related. A glossary of the terms and definitions used in the technical specifications is included in clauses 3 and 4.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T G.9980	2012-11-23	15

Keywords

CWMP, TR-069.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

The basis of this Recommendation is the Broadband Forum CPE WAN management protocol (CWMP), commonly referred to as TR-069.

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 specifies the generic requirements of the management protocol, and methods that can be applied to any TR-069 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.

Recommendation ITU-T G.9980

Remote management of customer premises equipment over broadband networks – Customer premises equipment WAN management protocol

1 Scope

This Recommendation 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.

CPE such as G-PON ONUs may be partially managed by OMCI, as specified in [b-ITU-T G.988]. [b-ITU-T G.988] defines options for shared management of such devices. These options, and the OMCI management of CPE, are outside the scope of this Recommendation.

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.

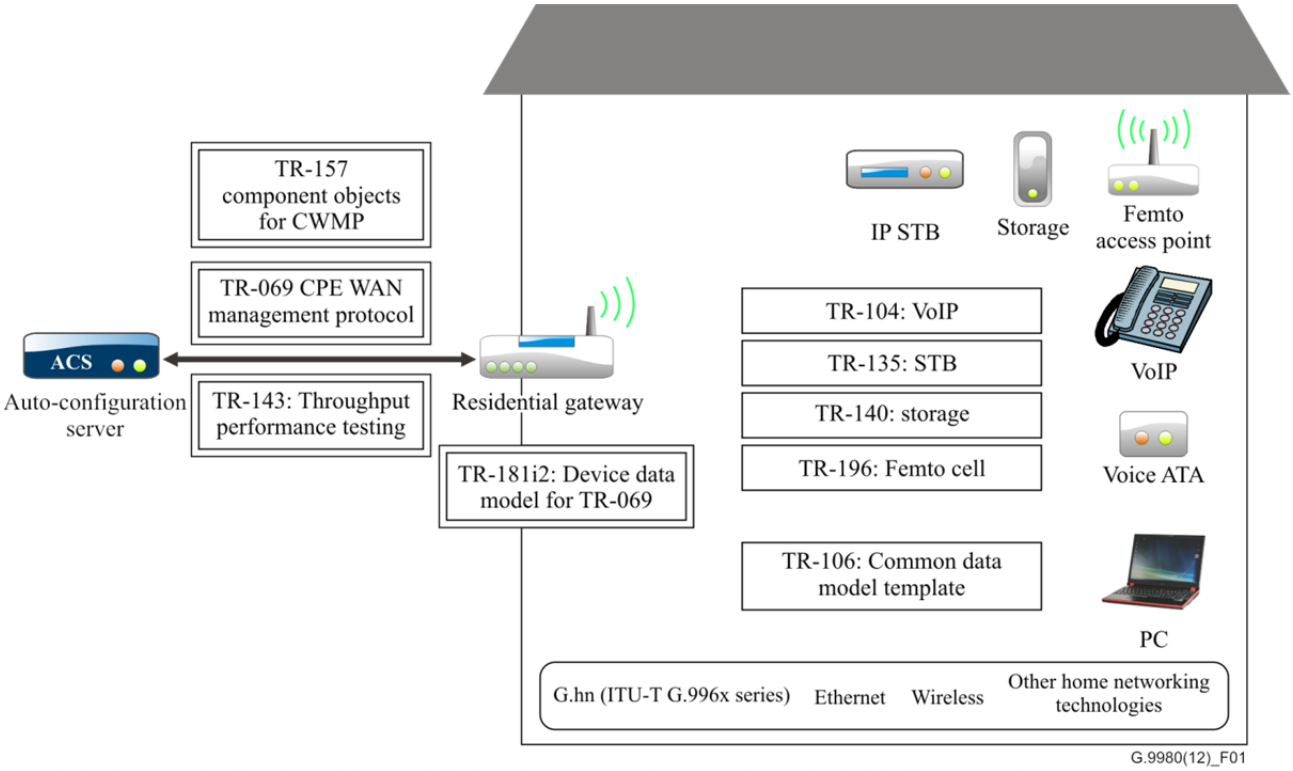
The protocol allows an ACS to control and monitor various parameters associated with a CPE. The mechanisms provided to access these parameters are designed with the following premises.

- 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 shown in double line rectangles.
Technical reports that define service data models (see clauses 6.2.1) are shown in rectangles.

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

Any protocol describing remote configuration or software-/firmware modification of CPEs must provide the capabilities to comply with all applicable national and regional laws, regulations and policies. The implementation of mechanisms to ensure the explicit endorsement of the customer by means of opt-in permissions before remotely initiating any procedures on the CPE may be required by some specific national and regional laws, regulations and policies. Implementers and users of the described CWMP shall comply with all applicable national and regional laws, regulations and policies.

Implementers and users of all ITU-T Recommendations, including ITU-T G.9980 and the underlying techniques, shall comply with all applicable national and regional laws, regulations and policies.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[BBF TR-069] Broadband Forum TR-069 Amendment 2 (2007), *CPE WAN Management Protocol v1.1*.
<http://www.broadband-forum.org/technical/download/TR-069_Amendment-2.pdf>

[BBF TR-104] Broadband Forum TR-104 (2005), *DSLHome Provisioning Parameters for VOIP CPE*.
<http://www.broadband-forum.org/technical/download/TR-104.pdf>

[BBF TR-106] Broadband Forum TR-106 Amendment 4 (2010), *Data Model Template for TR-069-Enabled Devices.*
<http://www.broadband-forum.org/technical/download/TR-106_Amendment-4.pdf>

[BBF TR-135] Broadband Forum TR-135 (2007), *Data Model for a TR-069 Enabled STB.*
<http://www.broadband-forum.org/technical/download/TR-135.pdf>

[BBF TR-140] Broadband Forum TR-140 (2007), *TR-069 Data Model for Storage Service Enabled Devices.*
<http://www.broadband-forum.org/technical/download/TR-140_Issue1.1.pdf>

[BBF TR-143] Broadband Forum TR-143 Corrigendum 1 (2008), *Enabling Network Throughput Performance Tests and Statistical Monitoring.*
<http://www.broadband-forum.org/technical/download/TR-143_Corrigendum-1.pdf>

[BBF TR-157] Broadband Forum TR-157 Amendment 1 (2009), *Component Objects for CWMP*.
<http://www.broadband-forum.org/technical/download/TR-157_Amendment-1.pdf>

[BBF TR-181 Issue 2] Broadband Forum TR-181 Issue 2 (2010), *Device Data Model for TR-069.*
<http://www.broadband-forum.org/technical/download/TR-181_Issue-2.pdf>

[BBF TR-196] Broadband Forum TR-196 (2009), *Femto Access Point Service Data Model.*
<http://www.broadband-forum.org/technical/download/TR-196.pdf>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 customer premises equipment (CPE) [b-ITU-T Y.101]: End-use system including private network elements connecting the customer applications to the access line.

3.1.2 technical report (TR): An approved technical specification of the Broadband Forum in accordance with [b-BBF01].

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 remote management: Management of CPE over a WAN by a service provider.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACS Auto-Configuration Server

CPE Customer Premises Equipment

CWMP CPE WAN Management Protocol

FAP Femto Access Point

FDD Frequency-Division Duplexing

IPTV Internet Protocol Television

NAS Network Attached Storage

NAT Network Address Translation

PVR Personal Video Recorder

QoE Quality of Experience

QoS Quality of Service

RG Residential Gateway

RPC Remote Procedure Call

SIP Session Initiation Protocol

SSL/TLS Secure Socket Layer/Transport Layer Security

STB Set-Top Box

TR Technical Report

UMTS Universal Mobile Telecommunication System

VoIP Voice over Internet Protocol

WAN Wide Area Network

5 Conventions

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

6 Remote management of CPE over broadband networks

This clause lists the elements of the CPE WAN management protocol (see clause 6.1) and the data models for specific devices (see clause 6.2), which constitute a normative part of this Recommendation.

6.1 Elements of the CPE WAN management protocol

The requirements for the CPE WAN management protocol are defined in [BBF TR-069].

It is recognized that service provider policies or local regulations may restrict the use of CPE WAN management and its partner specifications for privacy and security reasons. Such restrictions could encompass one or more of the following:

- CWMP communications only via mutually authenticated SSL/TLS channels;
- restrictions on the type of CPE to be managed remotely;

- requirement for explicit individual endorsement by the subscriber, which must take place before remote management is established to retrieve information about the CPE configuration;
- requirement for asking of an explicit endorsement by the subscriber, which must take place before changing the CPE configuration;
- other.

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

[BBF TR-069] 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.

To aid the technical alignment of the Recommendation with [BBF TR-069], the remainder of this clause (shown within a frame) is structured in accordance with [BBF TR-069]. The numbered titles refer to section numbers in [BBF TR-069] itself.

1 Introduction

The CWMP generic requirements of the management protocol methods may be applied to any CWMP enabled CPE.

From a purely functional perspective, CWMP 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.

1.2 Positioning in the end-to-end architecture

The ACS is a server that resides in the network. It manages devices in or at the subscriber premises via the CPE WAN management protocol. CWMP is agnostic to the specific access medium utilized by the service provider, although it does depend on IP-layer connectivity having been established.

1.3 Security goals

CWMP security is intended to be scalable to match a range of CPE, from very simple to very sophisticated. The security goals are:

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

2 Architecture

2.1 Protocol components

CWMP applications are defined atop a stack that respectively comprises RPC methods, SOAP, HTTP, SSL/TLS, TCP and IP as specified in [BBF TR-069].

2.2 Security mechanisms

Mechanisms available to CWMP include SSL/TLS and HTTP shared secrets.

2.3 Architectural components

CWMP is designed around the fundamental idea of remotely setting and retrieving named variables, creating and deleting remote objects, and invoking a small set of predefined methods. It builds on this foundation to support auto-discovery, notifications and file transfer mechanisms.

Standard CWMP information models are specified in clause 6.2 of this Recommendation. The information model may also be extended in vendor-specific ways.

CWMP sessions may be initiated by either ACS or CPE. When a CPE initializes, it may contact an ACS to obtain part or essentially all of its configuration, possibly even including its firmware load.

3 Procedures and requirements

3.1 ACS discovery

The CPE may have a default ACS URL built into its configuration. The CPE may also learn the identity of the ACS through local configuration, or through a DHCP option. DHCP may also provide a provisioning code, to be used by the CPE in further identifying itself to the ACS. The ACS may itself modify the URL to be used by the CPE for subsequent contact with a different ACS.

If the ACS URL specifies HTTPS, the CPE must use SSL/TLS to establish the session with the ACS.

3.2 Connection establishment

The CPE may initiate a session with the ACS when it initializes, when an ACS-configured periodic or scheduled inform time arrives, when it needs to send a provisioned value or state change notification or to recover a prematurely terminated earlier session. The CPE does not maintain an open session when it has no information to exchange with the ACS.

The ACS may indirectly initiate a session with the CPE through an HTTP request that the CPE open a session with the ACS.

3.3 Use of SSL/TLS and TCP

SSL/TLS is recommended for all sessions, but not required. If SSL/TLS is used, the CPE must authenticate the ACS through certificate-based authentication. The ACS is also encouraged to authenticate the CPE.

Other paragraphs in section 3 describe the details of message coding (SOAP), session establishment, operation and termination and file transfer operations. Additional authentication requirements are defined, including ACS HTTP authentication of CPE, if CPE authentication has not already been performed during the SSL/TLS negotiation.

Annex A – RPC methods

The data types and messages defined for CWMP remote procedure calls (RPC) are defined in Annex A of [BBF TR-069]. As well as the syntax of each message and its response, the annex specifies any special behavioural constraints that may apply to either ACS or CPE.

A generic XML schema is included as part of this annex.

Annex B – Removed

(Removed from this edition of TR-069.)

Annex C – Signed vouchers

Annex D – Web identity management

Annex E – Signed package format

Annex F – Device-gateway association

CWMP can be used to remotely manage CPE devices that are connected via a LAN through a gateway. When an ACS manages both a device and the gateway through which the device is connected, it can be useful for the ACS to be able to determine the identity of that particular gateway.

The procedures defined in this annex allow an ACS to determine the identity of the gateway through which a given device is connected. The mechanism relies on the use of DHCP by both the device and the gateway.

In an exemplary use case, an ACS establishing QoS for a particular service might need to provision both the device as well as the gateway through which that device is connected. To do the latter, the ACS would need to determine the identity of that particular gateway.

To support this feature, both the gateway and device are expected to be managed via CWMP, and both managed by the same ACS, or by distinct ACSs that are appropriately coupled.

Annex G – Connection request via NAT gateway

Network address translation (NAT) in a gateway isolates the LAN-side IP address space from the WAN-side IP space. CPE behind a NAT gateway can use the previously defined methods to initiate sessions, but the procedures defined in this annex are needed for the ACS to be able to request a connection from the CPE. The NAT gateway does not need to support CWMP.

6.1.2 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 this version.

6.1.3 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.

6.1.4 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. [BBF TR-143] facilitates throughput testing to be able to assess the subscribers experience in terms of broadband speed.

6.1.5 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.

6.1.6 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;
- allow for mutual strong authentication of CPE and ACS;
- provide confidentiality for transactions between CPE and ACS;
- allow appropriate authentication for each type of transaction;
- prevent theft of service.

6.2 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, among 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 [BBF TR-106], [BBF TR-143], [BBF TR-157], [BBF TR-181 Issue 2], [BBF TR-104], [BBF TR-135], [BBF TR-140] and [BBF TR-196].

[BBF TR-106] 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:

- [BBF TR-181 Issue 2]: Device data model for TR-069
- [BBF TR-157]: Component objects for CWMP
- [BBF TR-143]: Enabling network throughput performance tests and statistical monitoring

Technical reports that define service data models are:

- [BBF TR-104]: DSLHome provisioning parameters for VOIP CPE
- [BBF TR-135]: Data model for a TR-069 enabled STB
- [BBF TR-140]: TR-069 data model for storage service enabled devices
- [BBF TR-196]: Femto access point service data model

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

[BBF TR-181 Issue 2] defines version 2 of the TR-069 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 [b-BBF TR-181 Issue 1] (not included in the Recommendation) and [b-BBF TR-098] amendment 2 (not included in the Recommendation). Legacy installations may 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 [BBF TR-181 Issue 2] 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.

To aid the technical alignment of the Recommendation with [BBF TR-181 Issue 2], the remainder of this clause (shown inside a frame) is structured in accordance with [BBF TR-181 Issue 2]. The numbered titles refer to section numbers in [BBF TR-181 Issue 2] itself.

4 Architecture

4.1 Interface layers

This Technical Report models network interfaces and protocol layers as independent data objects, generally referred to as interface objects (or interfaces). Interface objects can be stacked, one on top of the other, using path references in order to dynamically define the relationships between interfaces.

The interface object and interface stack are concepts inspired by [b-IETF RFC 2863].

Within the Device:2 data model, interface objects are arbitrarily restricted to definitions that operate at or below the IP network layer (i.e., layers 1 through 3 of the OSI model). However, vendor specific interface objects MAY be defined which fall outside this restricted scope.

4.2 Interface objects

An interface object is a type of network interface or protocol layer. Each type of interface is modelled by a Device:2 data model table, with a row per interface instance (e.g., IP.Interface.{i} for IP Interfaces).

Each interface object contains a core set of parameters and objects, which serves as the template for defining interface objects within the data model. Interface objects can also contain other parameters and sub-objects specific to the type of interface.

4.3 InterfaceStack table

Although the interface stack can be traversed via LowerLayers parameters (as described in section 4.2.1 *Lower Layers*), an alternate mechanism is provided to aid in visualizing the overall stacking relationships and to quickly access objects within the stack.

The InterfaceStack table is a Device:2 data model object, namely *Device.InterfaceStack.{i}*. This is a read-only table whose rows are auto-generated by the CPE based on the current relationships that are configured between interface objects (via each interface instance's LowerLayers parameter). Each table row represents a "link" between a higher-layer interface object (referenced by its HigherLayer parameter) and a lower-layer interface object (referenced by its LowerLayer parameter). This means that an InterfaceStack table row's HigherLayer and LowerLayer parameters will always both be non-null.

NOTE – As a consequence, interface instances that have been stranded will not be represented within the InterfaceStack table. It is also likely that multiple, disjoint groups of stacked interface objects will coexist within the table (for example, each IP interface will be the root of a disjoint group; unused "fragments", e.g., a secondary DSL channel with a configured ATM PVC that is not attached to anything above, will linger if they remain interconnected; and finally, partially configured "fragments" can be present when an interface stack is being set up).

5 Parameter definitions

The normative definition of the Device:2 data model is split between several DM instance documents (see [BBF TR-069] Annex A). Table 3 lists the Device:2 data model versions and DM instances that had been defined at the time of writing. It also indicates the corresponding technical reports and gives links to the associated XML and HTML files. The TR-181i2 XML document defines the Device:2 model itself, and imports additional components from the other XML documents listed. The TR-181i2 HTML document is a report generated from the XML files, and lists the entire Device:2 data model in human-readable form.

Annex A – Bridging and queuing

This annex defines the queuing and bridging model (the packet classification, the queuing and scheduling, and bridging), the default layer 2/3 QoS mapping and URN definitions for app and flow tables (App ProtocolIdentifier, Flow Type and Flow TypeParameters).

6.2.2 TR-157: Component objects for CWMP

[BBF TR-157] 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.

To support the functionality defined in [BBF TR-157], an extension to the device data model and InternetGatewayDevice data model is specified in Table 1 of [BBF TR-157]. For the device data model, this extension is considered part of Device:1.4 (version 1.4 of the device data model), which extends version 1.3 of the device data model defined in TR-157 Issue 1. For the InternetGatewayDevice data model, this extension is considered part of InternetGatewayDevice:1.6 (version 1.6 of the InternetGatewayDevice data model), which extends version 1.5 of the InternetGatewayDevice data model defined in TR-157 Issue 1.

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

[BBF TR-143] 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 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.

To aid the technical alignment of the Recommendation with [BBF TR-143], the remainder of this clause (shown inside a frame) is structured in accordance with [BBF TR-143]. The numbered titles refer to section numbers in [BBF TR-143] itself.

4 Active monitoring

Active monitoring is the concept of introducing dummy TCP or UDP traffic into a network, in this case, a broadband access network that includes TR-069-enabled CPE, for the purpose of evaluating QoS. Test traffic may originate in the network or at CPE that supports [BBF TR-143].

5 Parameter definitions

Section 5 defines the specific syntax and semantics of the parameters of a VoIP service. Parameters are grouped into packages, which are then further collected into profiles for various applications in section 7.

6 Notification requirements

7 Profile definitions

7.1 Notation

7.2 Download profile

The download profile configures CPE to execute a download test and to record the results. Ethernet priority and DSCP fields may be configured as part of the profile.

7.3 DownloadTCP profile

The download TCP profile extends the download profile to record TCP request and response times, when the download uses TCP.

7.4 Upload profile

The upload profile configures CPE to execute an upload test and to record the results. Ethernet priority and DSCP fields may be configured as part of the profile.

7.5 UploadTCP profile

The upload TCP profile extends the upload profile to record TCP request and response times, when the upload uses TCP.

7.6 UDPEcho profile

The UDP echo profile configures the CPE to execute a UDP echo test.

7.7 UDPEchoPlus profile

The UDP echoplus profile extends the UDP echo profile by adding an echo-plus enabling parameter.

Appendix A – Theory of operations

A.1 UDP echo plus

The UDP echoplus feature is an extension to the ordinary ICMP echo function. It allows both one way and round-trip measurements of packet performance. It is processed according to its DSCP or Ethernet priority markings, which makes a better measure of performance as seen by the subscriber.

A.2 DownloadDiagnostics utilizing FTP transport

This test is the FTP transfer of a test file from the test server to the CPE. It records the number of bytes received and several time stamps that allow evaluation of download performance.

A.3 UploadDiagnostics utilizing FTP transport

These tests are similar to the download test.

A.4 DownloadDiagnostics utilizing HTTP transport

These tests are similar to the corresponding FTP download test.

A.5 UploadDiagnostics utilizing HTTP transport

These tests are similar to the corresponding FTP upload test.

6.2.4 TR-104: DSLHome provisioning parameters for VOIP CPE

[BBF TR-104] 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 [BBF TR-069].

To aid the technical alignment of the Recommendation with [BBF TR-104], the remainder of this clause (shown inside a frame) is structured in accordance with [BBF TR-104]. The numbered titles refer to section numbers in [BBF TR-104] itself.

1 Introduction

TR-104:

- 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.

2 Architecture

[BBF TR-104] defines a VoiceService as the container associated with the provisioning objects for VoIP CPE. In the context of [BBF TR-106], the VoiceService object defined in [BBF TR-104] is a service object. Individual CPE devices may contain zero or more instances of the VoiceService object. The presence of more than one VoiceService object might be appropriate, for example, where a CPE device serves as a management proxy for other non-TR-069 capable VoIP CPE. For example, an Internet gateway device might serve as a management proxy for one or more non-TR-069 capable VoIP phones.

Each VoiceService object contains one or more VoiceProfile objects. A VoiceProfile corresponds to one or more phone lines that share the same basic configuration. Each VoiceProfile object contains one or more line objects, each of which represents a single distinct phone line.

The VoiceProfile object allows a multi-line voice device to group lines with common characteristics under a single profile. By allowing more than one VoiceProfile, the model allows a single multi-line voice device to have groups of lines that are configured differently from others. One possible use of this structure could be to associate distinct groups of lines with completely separate service providers, each with distinct VoIP servers and configuration requirements. Another possible use could be to distinguish between different levels of service from a single service provider. For example, a single device could provide some consumer lines plus some business lines, each associated with a distinct VoiceProfile, and distinguished by their quality characteristics.

3 VoiceService version 1.0 data model

Section 3 defines the specific syntax and semantics of the parameters of a VoIP service. Parameters are grouped into packages, which are then further collected into profiles for various applications in section 4.

4 Profile definitions

4.1 Notation

4.2 Endpoint profile

The endpoint profile collects parameters that are appropriate to a VoIP endpoint into several groups. The capabilities group includes bounds on choice of codec and bit rate, the number of simultaneous sessions, the available signalling protocols, fax and modem detection and pass-through, numbering plan, tone, ringing and button map customization. The voice profile group is subdivided into several smaller groups, dealing with RTP, line status, the parameters of the codec in use, session timers and far-end addresses, and PM counters.

The following three profiles contain similar information, but in forms tailored for their separate signalling protocols.

4.3 SIPEndpoint profile

The SIP endpoint profile extends the endpoint profile with specific parameters of importance to SIP signalling, specifically including SIP proxy, registration and subscriber authentication information.

4.4 MGCPEndpoint profile

The MGCP endpoint profile extends the endpoint profile with parameters of importance to MGCP signalling. Specifics include identity and registration information of the agent and the local user.

4.5 H323Endpoint profile

The H323 endpoint profile extends the endpoint profile with parameters of importance to ITU-T H.323 signalling. Specifics include identity and registration information of the gatekeeper and the local user.

4.6 TAEndpoint profile

The TA endpoint profile is intended to be used by a terminal endpoint. It extends the basic endpoint profile with lists of the associated physical ports and their identifiers that share the same parameters.

Appendix A – Facility actions

Appendix A defines the various VoIP signalling actions that can be triggered by subscriber dial plan prefixes or telephone set pushbuttons. Examples include activation or deactivation of features such as call forwarding, calling line identification, selective ringing and the like. Other actions include, for example, switching between multiple calls on hold.

Appendix B – Downloading tone and ringer files

Appendix B describes the details of using the TR-069 file download feature for the specific purpose of downloading VoIP tone and ringer files.

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

[BBF TR-135] 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, and is outside the scope of 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. Most parameters defined in [BBF TR-135] are therefore read-only to the ACS.

NOTE – [BBF TR-135] 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.

To aid the technical alignment of the Recommendation with [BBF TR-135], the remainder of this clause (shown inside a frame) is structured in accordance with [BBF TR-135]. The numbered titles refer to section numbers in [BBF TR-135] itself.

5 Architecture

A set-top box (STB) is modelled as a collection of functions and capabilities, most of which are optional, and most of which can exist in more than one instance. As well as the basic STB infrastructure, the other components are those whose profiles are defined below in section 7.

6 Parameter definitions

Section 6 defines the specific syntax and semantics of the parameters of a STB. Parameters are grouped into packages, which are further collected into profiles for various applications in section 7.

7 Profile definitions

7.1 Notation

7.2 Baseline profile

The baseline profile provides read-only information about the capabilities of the STB, including the standards it supports and the maximum number of streams of various types that it can support simultaneously. Writeable parameters are limited to mute control and choice of language for audio and subtitle streams.

7.3 PVR profile

The personal video recorder profile returns the status of a possible PVR application. PVR storage is supported through a reference to a storageService defined in [BBF TR-140].

7.4 DTT profile

The digital terrestrial television profile provides configuration parameters for digital video broadcasting, as well as read-only maintenance and PM parameters.

7.5 IPTVBaseline profile

The IPTV profile provides read-write QoS buffering parameters, and a set of read-only parameters that report the STB's capabilities and current status with regard to IPTV features.

7.6 RTCP profile

The real-time control protocol profile provides simple configuration control (enable, interval setting) and a status report.

7.7 RTPAVPF profile

The RTP real-time feedback profile configures the real-time RTP feedback feature, and reports its current status.

7.8 IPTVHomeNetwork profile

The IPTV home network profile reports status and capabilities of the STB's home network interfaces, as translated from the WAN-side stream.

7.9 IGMP profile

The IGMP profile provides a way to configure IGMP parameters such as VLAN tagging, robustness and reporting interval, as well as read-only status and PM statistics.

7.10 BasicPerfmon profile

The basic PM profile supports configuration of high-level PM parameters, for example, global enable, time and interval reference times, etc. It reports statistics across the STB as a whole, and high-level statistics for the major components at various levels, for example, RTP, MPEG and video decoder.

7.11 ECPprofile

The error correction PM profile reports statistics related to the RTP error correction capability.

7.12 VideoPerfmon profile

The video PM profile reports statistics associated with the quality of video playback.

7.13 AudioPerfmon profile

The audio PM profile reports statistics associated with the quality of audio playback.

7.14 AudienceStats profile

The audience statistics profile collects channel count and time statistics.

7.15 AnalogOutput profile

The analogue output profile reports the STB's capabilities to support external devices such as video displays.

7.16 DigitalOutput profile

The digital output profile reports whether high-bandwidth digital content protection (HDCP) is in use on the particular video output.

7.17 CA profile

The conditional access profile reports the existence of conditional access, which is modelled through a smart card reader.

7.18 DRM profile

The digital rights management profile provides read-only parameters on the current status of media streams in progress.

Appendix I – Theory of operations

This appendix describes a large number of use cases and explains the way in which they employ the STB information model.

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

[BBF TR-140] 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 set up during device activation (addressed by [BBF TR-140] and [BBF TR-181 Issue 2]);
- user credentials set up and file privilege access (addressed by [BBF TR-140] (folder access));
- retrieval of device status (addressed by [BBF TR-140] (parameters) and [BBF TR-181 Issue 2]);
- wireless set up (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] (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.

4 Parameter definitions

Section 4 defines the specific syntax and semantics of the parameters of a storage device. Parameters are grouped into packages, which are further collected into profiles for various applications in section 6.

5 Notification requirements

6 Profile definitions

6.1 Notation

6.2 Baseline profile

The baseline profile provides read-only information about a storage service, including its storage and access capabilities, physical devices, file systems and top-level folders. Writeable parameters are limited to configuring the storage service's external network identity.

6.3 User access profile

The user access profile allows the configuration of network and local users, together with their access rights and login credentials.

6.4 Group access profile

The group access profile extends the user access profile to user groups, and allows the definition of access privileges at the group level.

6.5 FTP server profile

The FTP server profile configures a possible FTP server associated with the storage service, including its willingness to serve anonymous users.

6.6 SFTP server profile

The SFTP server profile extends the FTP server profile to also configure a possible SFTP server associated with the storage service.

6.7 HTTP server profile

The HTTP server profile configures a possible HTTP server associated with the storage service, including its security policy.

6.8 HTTPS server profile

The HTTPS server profile extends the HTTP server profile to include additional HTTPS parameters.

6.9 Volume config profile

The volume config profile extends the baseline profile to manage logical volume and top-level folder configuration.

6.10 RAID profile

The RAID profile configures storage arrays and reports on the current status and capacity of the array.

6.11 Folder quota profile

The folder quota profile allows the configuration of folder capacity policies, including over-capacity warning threshold.

6.12 Volume threshold profile

The volume threshold profile configures capacity policies at the level of the logical volume.

6.13 Network server profile

The network server profile configures network access protocols that may be used to access the storage

service remotely.

7 Use cases

The basic purpose of TR-069-managed storage service is to off-load storage management from the subscriber's responsibility. At the same time, some or all of the storage is accessible externally for use by a nomadic subscriber or by external servers such as the ACS itself (software upgrade) or personal video recorder (PVR) storage (see [BBF TR-135]).

Annex A – Theory of operations

Annex A covers details of storage device operation, including removable device management, access security and details of the use cases.

Annex B – RAID type descriptions

Annex B is a tutorial on the various ways in which disks can be combined under the RAID moniker.

6.2.7 TR-196: Femto access point service data model

[BBF TR-196] specifies the data model for femto access point (FAP) for remote management using CWMP. The purpose of [BBF TR-196] is to permit an operator to offer a managed femto access service to subscribers. As such, most aspects of the service are controlled by the ACS.

The scope of this FAP data model is UMTS FDD home nodeB (3G HNB). However, the structure and organization of the data model can be extended to cover other type(s) of FAP devices, based on other radio interface technologies.

To aid the technical alignment of the Recommendation with [BBF TR-196], the remainder of this clause (shown inside a frame) is structured in accordance with [BBF TR-196]. The numbered titles refer to section numbers in [BBF TR-196] itself.

4 Data model definition

Section 4 defines the specific syntax and semantics of the parameters of a FAP. Parameters are grouped into packages, which are further collected into profiles for various applications in section 5.

5 Profile definitions

TR-196 defines a large number of profiles to group FAP features. A baseline profile specifies configuration details that are expected in any FAP. Additional profiles describe local access policies, security policy, the various wireless protocols that may be supported, and PM, alarm and diagnostics capabilities.

The list of profiles includes:

2. Baseline profile
3. ACL profile
4. Local IP access profile
5. REM WCDMA FDD profile
6. REM GSM profile
7. GPS profile
8. Transport SCTP profile
9. Transport real time profile
10. IPSec tunnel profile
11. UMTS baseline profile
12. UMTS self config profile
13. UMTS self config NL in use intra freq cell profile
14. UMTS self config NL in use inter freq cell profile
15. UMTS self config NL in use inter RAT cell profile
16. UMTS cell config baseline profile
17. UMTS cell config advanced profile
18. UMTS cell config freq measurement profile
19. UMTS cell config UE internal measurement profile
20. UMTS cell config NL intra freq cell profile
21. UMTS cell config NL inter freq cell profile
22. UMTS cell config NL inter RAT cell profile
23. Fault management supported alarms profile
24. Fault management active alarms profile
25. Fault management profile event history profile
26. Fault management profile expedited delivery profile
27. Fault management profile queued delivery profile
28. Performance management profile

Bibliography

[b-ITU-T G.988] Recommendation ITU T G.988 (2010), *ONU management and control interface (OMCI) specification.*

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

[b-BBF01] Broadband Forum Technical Report Approval Process.
<http://www.broadband-forum.org/about/download/trapprovalprocess.pdf>

[b-BBF TR-098] Broadband Forum TR-098 Amendment 2 (2008), *Internet Gateway Device Data Model for TR-069.*
<http://www.broadband-forum.org/technical/download/TR-098_Amendment-2.pdf>

[b-BBF TR-181 Issue 1] Broadband Forum TR-181 Issue 1 (2010), *Device Data Model for TR-069.*
<http://www.broadband-forum.org/technical/download/TR-181_Issue-1.pdf>

[b-IETF RFC 2863] IETF RFC 2863 (2000), *The Interfaces Group MIB.*

Other related documents

[b-BBF TR-064] Broadband Forum TR-064 (2004), *LAN-side DSL CPE Configuration.*
<http://www.broadband-forum.org/technical/download/TR-064.pdf>

[b-BBF TR-68] Broadband Forum TR-68 (2006), *Base Requirements for an ADSL Modem with Routing.*
<http://www.broadband-forum.org/technical/download/TR-068_Issue-3.pdf>

[b-BBF TR-122] Broadband Forum TR-122 Amendment 1 (2006), *Base Requirements for Consumer-Oriented Analog Terminal Adapter Functionality.*
<http://www.broadband-forum.org/technical/download/TR-122v1.01.pdf>

[b-BBF TR-124] Broadband Forum TR-124 (2006), *Functional Requirements for Broadband Residential Gateway Devices.*
<http://www.broadband-forum.org/technical/download/TR-124.pdf>

[b-BBF TR-131] Broadband Forum TR-131 (2009), *ACS Northbound Interface Requirements.*
<http://www.broadband-forum.org/technical/download/TR-131.pdf>

[b-BBF TR-133] Broadband Forum TR-133 (2005), *DSLHome TR-064 Extensions for Service Differentiation.*
<http://www.broadband-forum.org/technical/download/TR-133.pdf>

[b-BBF TR-142 Issue 2] Broadband Forum TR-142 Issue 2 (2010), *Framework for TR-069 enabled PON Devices.*
<http://www.broadband-forum.org/technical/download/TR-142_Issue-2.pdf>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013