



ABSTRACT TEST PLAN

ATP-069
TR-069 Abstract Test Plan

Issue: 2 Corrigendum 1
Issue Date: May 2017

Notice

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment. This Abstract Test Plan has been approved by members of the Forum. This Abstract Test Plan is subject to change. This Abstract Test Plan is copyrighted by the Broadband Forum, and all rights are reserved. Portions of this Abstract Test Plan may be copyrighted by Broadband Forum members.

Intellectual Property

Recipients of this Abstract Test Plan 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 Abstract Test Plan, or use of any software code normatively referenced in this Abstract Test Plan, 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 Abstract Test Plan 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 Abstract Test Plan, 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 Abstract Test Plan except to the extent this Abstract Test Plan 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 Abstract Test Plan are not deemed to be derivative works of the Abstract Test Plan.

2. NO WARRANTIES

THIS ABSTRACT TEST PLAN IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NONINFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS ABSTRACT TEST PLAN 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 ABSTRACT TEST PLAN.

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 ABSTRACT TEST PLAN IN ITS CURRENT, OR IN ANY FUTURE FORM. IF ANY SUCH RIGHTS ARE DESCRIBED ON THE ABSTRACT TEST PLAN, BROADBAND FORUM TAKES NO POSITION AS TO THE VALIDITY OR INVALIDITY OF SUCH ASSERTIONS, OR THAT ALL SUCH ASSERTIONS THAT HAVE OR MAY BE MADE ARE SO LISTED.

The text of this notice must be included in all copies of this Abstract Test Plan.

© 2017, The Broadband Forum. All rights reserved. This Broadband Forum document (ATP-069) specifies the Test Plan on which is based the BBF.069 Certification Program for TR-069-enabled products. Through an open selection process, the Broadband Forum entered into an agreement with one or more independent Test Agencies to offer commercial testing services against this Test Plan and to confirm results to the Broadband Forum in connection with the Forum's delivery of BBF.069 Certification. Offering Certification testing services against this Test Plan is reserved to the Test Agencies duly authorized by the Broadband Forum. Broadband Forum members can independently test against ATP-069, but may only produce limited reports which only detail where a given product has failed a test case

NOTE: The right to display a Broadband Forum Certification Logo may only be granted by the Broadband Forum, and that right is available only to Broadband Forum members that have successfully passed certification testing by a duly authorized Test Agency. Further details on the Broadband Forum Certification Programs can be found at <http://www.broadband-forum.org/technical/certification.php>

Issue History

Issue Number	Approval Date	Publication Date	Issue Editor	Changes
1	16 October 2012	17 October 2012	Tim Sheehan UNH-IOL	Original
2	9 January 2017	30 January 2017	Marion Dillon UNH-IOL	<ul style="list-style-type: none"> • 5.3-5.4 – Added Factory Reset step to Test Setup. • 5.10 – Corrected order of test setup and added an additional RPC from the ACS with “Connection:close” in the header. • 5.46 – Expanded this into three parts: Single-Instance Object, Multi-Instance Object (Empty), and Multi-Instance Object (Non-Empty). Multi-Instance Object (Empty) may be omitted if such an object doesn’t exist. • 5.47 – Expanded this into three parts: Single-Instance Object, Multi-Instance Object (Empty), and Multi-Instance Object (Non-Empty). Multi-Instance Object (Empty) may be omitted if such an object doesn’t exist. • 5.81 – Specified that Download RPC DelaySeconds arguments should be set so RPCs are run out of order, and added a Test Metric to check that Downloads are performed at the correct time. • 5.103-5.104 – Changed from Mandatory to Conditionally Mandatory • 5.108 – Altered the procedure to disable the network time server and deliver an expired certificate. Added a note to omit this test for CPEs that do not acquire their accurate absolute time on the network. • 5.110 – Added Mandatory test case to test Boolean Parameter Configuration. • 5.111-5.122 – Added Conditionally Mandatory tests for XMPP Connection Request.
2 Corrigendum 1	8 May 2017	9 June 2017	Marion Dillon UNH-IOL	<ul style="list-style-type: none"> • 5.114 – Removed test case.

Comments or questions about this Broadband Forum Abstract Test Plan should be directed to help@broadband-forum.org.

Editor

Marion Dillon

UNH-IOL

Broadband User Services

Jason Walls

Qacafe

Work Area Directors

John Blackford

Arris

Table of Contents

EXECUTIVE SUMMARY	10
1 PURPOSE AND SCOPE	11
1.1 PURPOSE	11
1.2 SCOPE	11
2 REFERENCES AND TERMINOLOGY.....	12
2.1 CONVENTIONS	12
2.2 REFERENCES	13
2.3 DEFINITIONS	14
2.4 ABBREVIATIONS	14
3 ABSTRACT TEST PLAN IMPACT	16
3.1 ENERGY EFFICIENCY.....	16
3.2 IPV6.....	16
3.3 SECURITY.....	16
3.4 PRIVACY	16
4 TEST SETUP	17
4.1 TEST EQUIPMENT.....	17
4.2 TEST SETUP AND EXECUTION	17
4.3 CPE TEST REQUIREMENTS.....	20
4.4 CPE OPTIONAL FUNCTIONALITY TEST REQUIREMENTS	21
4.5 TEST VALIDATION	21
4.6 OPTIONAL FUNCTIONALITY TAG.....	21
4.6.1 <i>Optional Functionality Tests</i>	21
5 TEST PROCEDURES.....	23
5.1 ACS DISCOVERY USING DHCPv4.....	23
5.2 ACS DISCOVERY USING DHCPv6.....	24
5.3 ACS REDISCOVERY USING DHCPv4.....	25
5.4 ACS REDISCOVERY USING DHCPv6.....	26
5.5 DHCP RETRY TO THE DHCPv4 SERVER	27
5.6 DHCP RETRY TO THE DHCPv6 SERVER	28
5.7 SESSION INITIATION AND TERMINATION	29
5.8 SESSION INITIATION AND TERMINATION WITH NO RPC	31
5.9 PERSISTENT TCP CONNECTION ACROSS A SINGLE CWMP SESSION.....	32
5.10 MULTIPLE TCP CONNECTIONS ACROSS A SINGLE CWMP SESSION	33
5.11 CONNECTION TO ACS USES SAME MECHANISM AFTER FACTORY RESET.....	34
5.12 HANDLING NULL TERMINATED ACS URL OBTAINED FROM DHCPv4SERVER.....	35
5.13 HANDLING NULL TERMINATED ACS URL OBTAINED FROM DHCPv6 SERVER	36
5.14 HANDLING DNS SERVER RESPONSE.....	37
5.15 ACS MODIFIES URL	38
5.16 ACS URL CHANGE ON THE DUT BY THIRD PARTY MEANS.....	39
5.17 PARAMETERS MODIFIED BY ACS DO NOT CREATE A “4 VALUE CHANGE INFORM EVENT TO THE ACS.....	40

5.18	EVENT DISCARD AFTER BOOTSTRAP INFORM	41
5.19	CONNECTION AFTER CONNECTION REQUEST	42
5.20	CONNECTION REQUEST WHILE SESSION EXISTS.....	43
5.21	CONNECTION AFTER PERIODICINFORMINTERVAL	44
5.22	CONNECTION ESTABLISHMENT USING SSL 3.0	45
5.23	CONNECTION ESTABLISHMENT USING TLS 1.0	46
5.24	CONNECTION ESTABLISHMENT USING TLS 1.2	47
5.25	COMMON NAME CERTIFICATE VALIDATION	48
5.26	REJECTION OF INVALID CERTIFICATE	49
5.27	USE OF MULTIPLE SESSION COOKIES ACROSS TRANSACTIONS IN A SESSION	50
5.28	SESSION RETRY	51
5.29	SOAP RESPONSE IN AN HTTP REQUEST	53
5.30	HTTP REDIRECTION TEST – 302 REDIRECT.....	54
5.31	HTTP REDIRECTION TEST – 307 REDIRECT.....	55
5.32	HTTP REDIRECTION – MULTIPLE REDIRECTIONS.....	56
5.33	HTTP REDIRECTION – HTTPS WITH URL MATCHING CERTIFICATE	57
5.34	HTTP REDIRECTION – HTTPS WITH URL/CERTIFICATE MISMATCH.....	58
5.35	REDIRECTION AT ANY POINT IN A SESSION	59
5.36	HTTP REDIRECTION – USE OF SESSION COOKIES.....	60
5.37	REDIRECT HTTP RESPONSE CONTAINS DATA.....	61
5.38	HTTP AUTHENTICATION - BASIC AUTHENTICATION	62
5.39	QOP AUTHENTICATION SETTING	63
5.40	HTTP AUTHENTICATION - DIGEST AUTHENTICATION	64
5.41	MAXIMUM SOAP MESSAGE SIZE	65
5.42	SETPARAMETERVALUES SOAP FAULT FORMAT.....	66
5.43	GETRPCMETHODS AND REQUIRED RPCS	68
5.44	GETPARAMETERNAMES – COMPLETE PATH	69
5.45	GETPARAMETERNAMES – COMPLETE PATH, NEXTLEVEL TRUE	70
5.46	GETPARAMETERNAMES – PARTIAL PATH – NEXT LEVEL TRUE	71
	5.46.A Single-Instance Object.....	71
	5.46.B Multi-Instance Object (Empty)	72
	5.46.C Multi-Instance Object (Non-Empty).....	73
5.47	GETPARAMETERNAMES – PARTIAL PATH – NEXT LEVEL FALSE – SINGLE-INSTANCE OBJECT	74
	5.47.A Single-Instance Object.....	74
	5.47.B Multi-Instance Object (Empty)	75
	5.47.C Multi-Instance Object (Non-Empty).....	76
5.48	GETPARAMETERNAMES – INVALID PATH.....	77
5.49	GETPARAMETERNAMES – ENTIRE OBJECT MODEL	78
5.50	GETPARAMETERVALUES – SIMPLE COMPLETE PATH	79
5.51	GETPARAMETERVALUES – MULTIPLE COMPLETE PATHS.....	80
5.52	GETPARAMETERVALUES – PARTIAL PATH	81
5.53	GETPARAMETERVALUES – COMPLETE AND PARTIAL PATHS.....	82
5.54	GETPARAMETERVALUES – ENTIRE OBJECT MODEL	83
5.55	GETPARAMETERVALUES – FAULT CONDITION	84
5.56	SETPARAMETERVALUES – SINGLE PARAMETER	85

5.57	SETPARAMETERVALUES – MULTIPLE PARAMETERS	86
5.58	SETPARAMETERVALUES – SAME PARAMETER MULTIPLE TIMES	87
5.59	SETPARAMETERVALUES – ATOMIC TEST	88
5.60	GETPARAMETERATTRIBUTES – COMPLETE PATH.....	89
5.61	GETPARAMETERATTRIBUTES – MULTIPLE COMPLETE PATHS.....	90
5.62	GETPARAMETERATTRIBUTES – PARTIAL PATH	91
5.63	GETPARAMETERATTRIBUTES – COMPLETE AND PARTIAL PATH.....	92
5.64	GETPARAMETERATTRIBUTES – INVALID PARAMETER NAME	93
5.65	GETPARAMETERATTRIBUTES – PARTIAL PATH EMPTY	94
5.66	SETPARAMETERATTRIBUTES – ACTIVE NOTIFICATIONS.....	95
5.67	SETPARAMETERATTRIBUTES – ACTIVE NOTIFICATIONS PERSISTENCE.....	96
5.68	SETPARAMETERATTRIBUTES – ATOMIC	97
5.69	SETPARAMETERATTRIBUTES – PASSIVE NOTIFICATION – COMPLETE PATH.....	98
5.70	SETPARAMETERATTRIBUTES – PASSIVE NOTIFICATION – PARTIAL PATH	99
5.71	SETPARAMETERATTRIBUTES – PASSIVE NOTIFICATION – COMPLETE AND PARTIAL PATH 100	
5.72	SETPARAMETERATTRIBUTES – DISABLE NOTIFICATION.....	101
5.73	SETPARAMETERATTRIBUTES – INCORRECT PARAMETER NAME	102
5.74	ADDOBJECT	103
5.75	ADDOBJECT – ERROR CONDITIONS	104
5.76	DELETEOBJECT	105
5.77	DELETEOBJECT – ERROR CONDITIONS	106
5.78	REBOOT	107
5.79	MANUAL REBOOT	108
5.80	DOWNLOAD TEST – BASIC VERSION UPGRADE	109
5.81	DOWNLOAD TEST – QUEUING	111
5.82	DOWNLOAD TEST – DELAY	112
5.83	DOWNLOAD TEST – RETRY	113
5.84	CANCELTRANSFER.....	114
5.85	UPLOAD	115
5.86	UPLOAD – QUEUING	116
5.87	UPLOAD – DELAY	117
5.88	SCHEDULEINFORM TEST	118
5.89	FACTORYRESET	119
5.90	CWMP FAULTS – BASIC RPC FAULTS	120
5.91	CWMP FAULTS – DOWNLOAD FAILURE.....	121
5.92	CWMP FAULTS – UPLOAD FAILURE	122
5.93	RUN DIAGNOSTICS.....	123
5.94	GETALLQUEUEDTRANFERS.....	124
5.95	XML NAMESPACE PREFIX VALIDATION.....	125
5.96	DUT RECEIVES CHUNKED TRANSFER ENCODING.....	126
5.97	DUT PROPERLY ENCODES AND DECODES XML ENTITIES.....	127
5.98	INFORM ON IP ADDRESS CHANGE	128
5.99	NO INFORM ON RECONNECT WITH NO IP ADDRESS CHANGE.....	129
5.100	ENABLECWMP SET TO FALSE	130
5.101	CHANGE ACS USERNAME AND PASSWORD.....	131

5.102 PERIODINFORMENABLE ENABLES PERIODIC INFORMS 132

5.103 PERIODICINFORMTIME IN THE PAST CONTROLS PERIODIC INFORM..... 133

5.104 PERIODICINFORMTIME IN THE FUTURE CONTROLS PERIODIC INFORM 134

5.105 DEFAULTACTIVENOTIFICATIONTHROTTLE THROTTLES ACTIVE NOTIFICATIONS.... 135

5.106 INFORM PARAMETERS SHOULD MATCH DEVICEINFO 136

5.107 DEVICE TIMES OUT IF ACS IS SLOW 137

5.108 USE OF CERTIFICATES IN THE ABSENCE OF NETWORK TIME 138

5.109 DUT RECEIVES CONTENT-LENGTH ENCODING 139

5.110 BOOLEAN PARAMETER CONFIGURATION 140

5.111 ESTABLISH SECURED CONNECTION TO XMPP SERVER 141

5.112 MAINTAIN CONNECTION TO XMPP SERVER..... 142

5.113 SRV LOOKUP OF XMPP SERVER..... 143

5.114 PROCESSING OF WEIGHTED SRV ENTRIES FOR XMPP SERVERS 144

5.115 RE-ESTABLISH CONNECTION TO XMPP SERVER 145

5.116 ESTABLISH XMPP CONNECTION BEFORE CWMP SESSION 146

5.117 SUCCESSFUL XMPP CONNECTION REQUEST 147

5.118 INVALID XMPP CONNECTION REQUEST 148

5.119 CONNREQALLOWEDJABBERIDS PARAMETER MATCHES..... 149

5.120 CONNREQALLOWEDJABBERIDS PARAMETER DOES NOT MATCH..... 150

5.121 CONNECTIONREQUESTUSERNAME PARAMETER DOES NOT MATCH..... 151

5.122 CONNECTIONREQUESTPASSWORD PARAMETER DOES NOT MATCH 152

APPENDIX I. OPEN ISSUES..... 153

APPENDIX II. TEST PROCEDURES REMOVED FROM THIS TEST PLAN 154

APPENDIX III. TEST CERTIFICATE GENERATION 155

List of Figures

Figure 1: RG Test Setup via Ethernet 17

Figure 2: End Device Test Setup via Ethernet through an RG 18

Figure 3: RG Test Setup via DSL/PON/Cable 18

Figure 4: End Device Test Setup via Ethernet through an RG connected via DSL/PON/Cable.. 18

List of Tables

Table 1: Required Test Equipment 17

Executive Summary

In order to ensure the continued growth of the TR-069 market and further the interoperability of the protocol, the Broadband Forum is creating a TR-069 Certification Program. Within this program, devices implementing a TR-069 management interface may be tested for their conformance to the TR-069 specification and various data-models. The TR-069 Certification Program will be released in differing phases, with the initial focus of verifying the conformance of a CPE device to the TR-069 base specification. To provide a consistent scope for this verification, the Broadband Forum developed test plans that are to be used by the testing agencies in the verification process.

ATP-069 provides a test plan that may be used to verify conformance of a CPE Device to the requirements defined in TR-069.

1 Purpose and Scope

1.1 Purpose

The purpose of ATP-069 is to provide a set of test cases, which will be used as a common testing language during CWMP CPE Conformance certification. The certification program is defined in BBF Document OD-361.

1.2 Scope

The tests detailed in ATP-069 are only intended to facilitate TR-069 conformance testing. The tests in ATP-069 are limited to CWMP-enabled CPE devices.

All tests specified in ATP-069 are directly derived from the TR-069 specification.

2 References and Terminology

2.1 Conventions

In this Abstract Test Plan, several words are used to signify the requirements of the specification. These words are always capitalized. More information can be found 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 Abstract Test Plan. At the time of publication, the editions indicated were valid.

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

Document	Title	Source	Year
[1] TR-069 Amendment 4	<i>CPE WAN Management Protocol</i>	BBF	July 2011
[2] TR-098 Amendment 2	<i>Internet Gateway Device Data Model for TR-069</i>	BBF	Sept 2011
[3] TR-104	<i>Provisioning Parameters for VoIP CPE</i>	BBF	Sept 2005
[4] TR-106 Amendment 6	<i>Data Model Template for TR-069-Enabled Devices</i>	BBF	July 2011
[5] TR-135 Amendment 1	<i>Data Model for a TR-069 Enabled STB</i>	BBF	Nov 2010
[6] TR-140 Amendment 1	<i>TR-069 Data Model for Storage Service Enabled Devices</i>	BBF	April 2010
[7] TR-143 Corrigendum1	<i>Enabling Network Throughput Performance Test and Statistical Monitoring</i>	BBF	Dec 2008
[8] TR-157 Amendment 5	<i>Component Objects for CWMP</i>	BBF	Nov 2011
[9] TR-181 Issue 2 Amendment 2	<i>Device Data Model for TR-069</i>	BBF	Feb 2011
[10] TR-196 Issue2	<i>Femto Access Point Service Data Model</i>	BBF	Nov 2011
[11] RFC 2119	<i>Key words for use in RFCs to Indicate Requirement Levels</i>	IETF	March 1997
[12] RFC 2131	<i>Dynamic Host Configuration Protocol</i>	IETF	March 1997
[13] RFC 2132	<i>DHCP Options and BOOTP Vendor Extensions</i>	IETF	March 1997
[14] RFC 3315	<i>Dynamic Host Configuration Protocol for IPv6 (DHCPv6)</i>	IETF	July 2003
[15] RFC 3489	<i>Session Traversal Utilities for NAT (STUN)</i>	IETF	March 2003
[16] RFC 5246	<i>The Transport Layer Security (TLS) Protocol</i>	IETF	Aug 2008
[17] RFC 6120	<i>Extensible Messaging and Presence Protocol (XMPP): Core</i>	IETF	March 2011

2.3 Definitions

Auto-Configuration Server	This is a component in the broadband network responsible for auto-configuration of the CPE for advanced services.
Access Node	DSL Access Multiplexer

2.4 Abbreviations

This Abstract Test Plan uses the following abbreviations:

ACS	Auto-Configuration Server
CN	Common Name
CPE	Customer Premise Equipment
CWMP	CPE WAN Management Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DUT	Device Under Test
FTP	File transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
ID	Identifier
IGD	Internet Gateway Device
IP	Internet Protocol
IPv6	Internet Protocol version 6
LAN	Local Area Network
NAT	Network Address Translation
NTP	Network Time Protocol
RFC	Request for Proposal
RG	Residential Gateway
RPC	Remote Procedure Call
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer

STB	Set Top Box
STUN	Session Traversal Utilities for NAT
TCP	Transmission Control Protocol
TFTP	Tiny File transfer Protocol
TLS	Transport Layer Security
TR	Technical Report
TTL	Time to Live
UDP	User Datagram Protocol,
URL	Universal Resource Locator
URN	Uniform Resource Name
UTC	Coordinated Universal Time
UTF	Universal Multiple-Octet Coded Character Set Transformation Format
UUID	Universally Unique Identifier
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
XML	Extensible Markup Language
TR	Technical Report
WG	Working Group

3 Abstract Test Plan Impact

3.1 Energy Efficiency

ATP-069 has no impact on Energy Efficiency.

3.2 IPv6

ATP-069 is required to support the IPv6 protocol. DHCPv6 is used by the TR-069 protocol on the WAN to discover the CPE. DHCPv6 is also used on the LAN to determine Device Identity when testing gateways.

3.3 Security

ATP-069 requires the use of authentication when connecting CPE to an ACS. Use of an HTTPS URL indicates that the CPE can establish an SSL or TLS connection to the ACS.

Appendix B contains the steps that will be used to generate the Certificate of Authentication for this Certification Test Plan.

3.4 Privacy

ATP-069 has no direct impact on user data privacy.

4 Test Setup

4.1 Test Equipment

The necessary set of test equipment to deliver reliable and repeatable test results is specified in Table 1.

Table 1: Required Test Equipment

Test Equipment	Description and Functional Capabilities
CWMP Analyzer	For infrastructure needs, an CWMP Analyzer will be provided to emulate the connections from CPE under test to a WAN. This device will allow control of ACS protocol requests and responses.
Traffic Analyzer	To verify certain test metrics, Analyzers will be provided dependent upon the connection between the CPE and CWMP Analyzer.
Access Node	For infrastructure needs, a Access Node will be provided to bridge connections from the CPE under test to the CWMP Analyzer.
File Server	In order to facilitate testing the Download RPC and other RPCs, a file server will be provided on which firmware files are loaded that can then be accessed via HTTP and/or FTP.
CPE	Customer Premise Equipment are devices under test in this conformance test plan

4.2 Test Setup and Execution

A typical basic test setup is shown below in Figure 1, this setup requires no media conversion. Figure 2 depicts a Basic IGD test setup that requires no media conversion. Figure 3 depicts a test setup that requires an access node and router to allow connection of ACS and CPE. Figure 4 shows the same access node test setup for IGD testing.

It is assumed that in the course of the testing, unless otherwise noted, that the network test setup remains in place for the duration of the entire test period. That is, though each test case specifies “connect the DUT and ACS to the test network” it is presumed that this setup remains connected in between test cases.



Figure 1: RG Test Setup via Ethernet

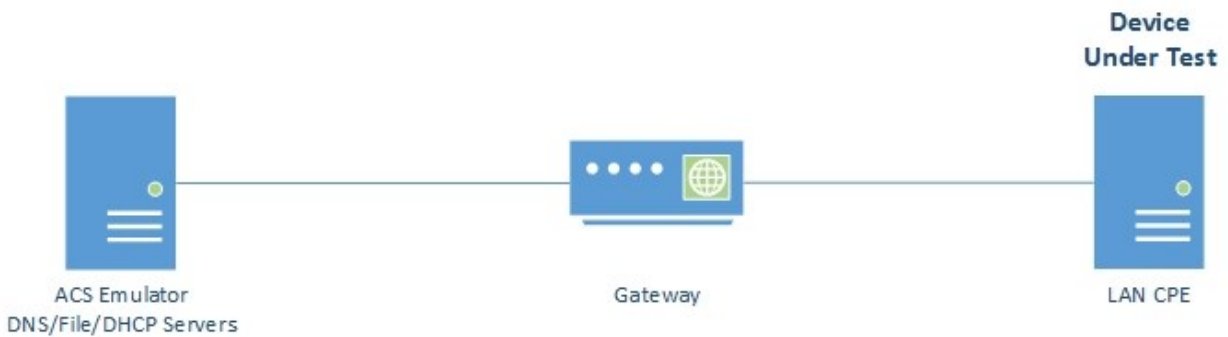


Figure 2: End Device Test Setup via Ethernet through an RG

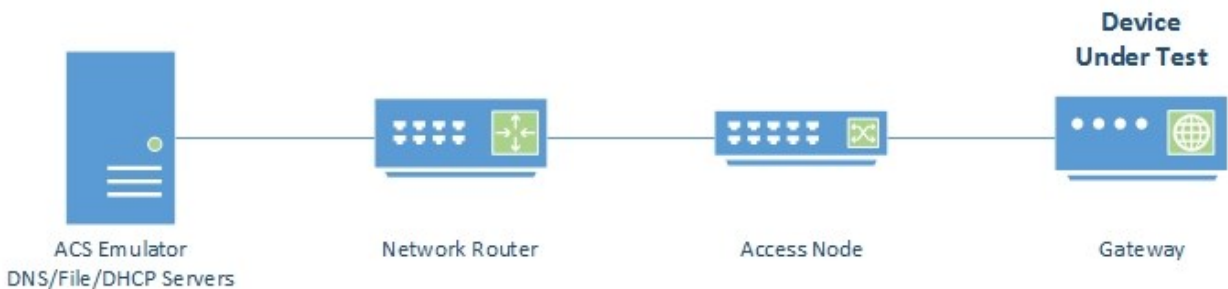


Figure 3: RG Test Setup via DSL/PON/Cable

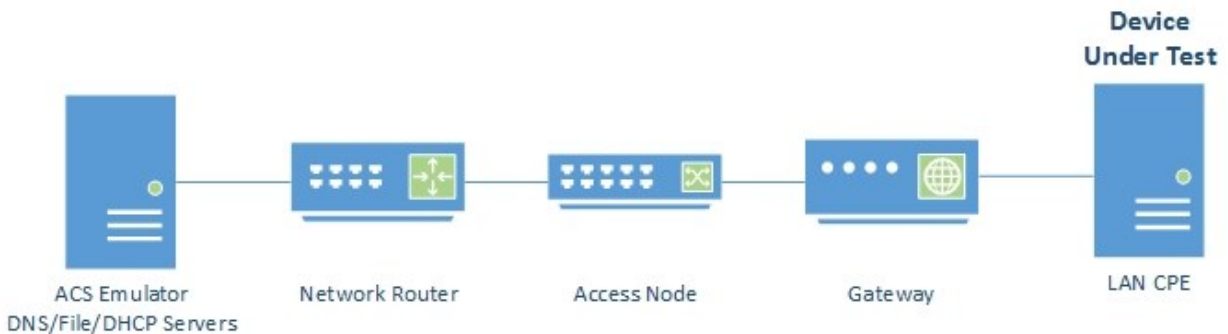


Figure 4: End Device Test Setup via Ethernet through an RG connected via DSL/PON/Cable

Test Execution

Each test is defined as either “automated” or “manual intervention required”. Automated tests are able to be performed sequentially by the test setup, through a test automation environment that is outside the scope of this document. These tests, performed sequentially, may causes

changes to the DUT's state during the course of testing. It is recommended to perform all automated tests independently of those requiring manual intervention.

Those requiring manual intervention require some type of interaction between the performers of the test and the DUT's interface in order to stimulate certain behavior as necessary in the test procedures. These interventions, and the tests themselves, may cause changes to the DUT's state during the course of testing. It is recommended to perform all manual tests independently of those that are able to be automated.

Validation of Underlying Protocols and Universal Test Metrics

CWMP, as defined in TR-069, relies on several underlying protocols. While it is outside the scope of this document to exhaustively test the requirements of these underlying protocols, it is necessary to test the functionality that will be required in order to have a functional CWMP system.

For each test for which a CWMP transaction occurs, the following metrics apply:

1. Validate that the HTTP sent by the DUT conforms to RFC 2616, HTTP 1.1.
 - Verify that the first line matches POST <URI> HTTP/1.1 CRLF. (Section 5.1)
 - Verify that headers are terminated with CRLF and there is a double CRLF between the headers and the body (Section 5)
 - Headers are formed field-name ":" value (Section 4.2)
 - The Host Header is present and properly formed. (Section 14.23)
 - Validate that either the Content-Length or the Transfer-Encoding: chunked header is present. All TR-69 messages require a message body, sometimes it must be empty. (Section 4.3, 4.4)
 - If Content-Length is present, validate that the body of the message matches the content length specified. (Section 14.13)
 - If Transfer-Encoding: chunked is present, validate the chunks are properly formed. (Section 3.6.1, 14.41)
2. Verify that the DUT conforms to the requirements in TR-69 section 3.4.1 Encoding SOAP over HTTP and section 3.4.6 Additional HTTP requirements, specifically:
 - Verify that the DUT's SOAP responses to requests made during test execution are sent over a subsequent HTTP POST.
 - Verify that when an HTTP response from the DUT contains a SOAP Envelope, the HTTP Content-Type header has a type/subtype of "text/xml".
 - Verify that any empty HTTP POST from the DUT does not contain a SOAPAction header.

- Verify that any empty HTTP POST from the DUT does not contain a Content-Type header.
3. Validate the cookie handling requirements of TR-69 section 3.4.2. All tests in this document will use cookies marked for Discard.
 4. Validate the SOAP body against the appropriate version of the TR-69 schema.
 - The SOAP message uses SOAP 1.1 envelope namespace identifier:
“<http://schemas.xmlsoap.org/soap/envelope>”
 - The SOAP message uses SOAP 1.1 serialization namespace identifier:
“<http://schemas.xmlsoap.org/soap/encoding>”
 - The SOAP message uses a namespace identifier compliant with the CWMP Protocol version.

4.3 CPE Test Requirements

In order to test the conformance of a CPE device, it MUST meet some requirements:

1. The CPE should be configurable, through non CWMP means, to allow modification of SSL, ACS usernames and passwords, ACS URL, and provide a means to change parameters for Active Notification tests.
2. The CPE MUST have two/three firmware images that are identical except for versioning to perform download testing.
3. The firmware images provided for certification MUST have “acs1.broadband-forum.org” as the default ACS URL. When a FactoryReset is performed this ACS URL value will persist.
4. The CPE should provide the means to monitor or configure the following:
 - a. Implemented RPCs
 - b. Implemented Optional RPCs
 - c. At least one Parameter that supports Active Notification and value can be modified by non-CWMP methods
 - d. At least one Parameter that supports Passive Notification and value can be modified by non-CWMP methods
 - e. Detailed steps to change ACS URL, ACS Username/Password, ConnectionRequest Username/Password, PeriodicInformInterval, PeriodicInformEnable, and CWMPEnable, via non-CWMP methods.
 - f. Parameters that can have Objects created and deleted
 - g. TR-069 container parameter (full path) that contains no leafs
 - h. Steps to perform FactoryReset and bring the device back to working order
 - i. Detailed steps to download files
 - j. Detailed steps to provision Primary WAN Connection
 - k. Detailed steps on activating any debug/logging feature
 - l. Detailed Recovery steps to bring the device back to working order

4.4 CPE Optional Functionality Test Requirements

If the CPE supports any of the following optional functionality, it **MUST** support the means to monitor or configure the corresponding test requirement outlined in [4.6.1 Optional Functionality Tests](#).

4.5 Test Validation

A test is considered successful (or passed) when the corresponding test procedure has been completed and the specified success metrics are attained. Tests can be validated by observing functional changes in the DUTs, through feedback interfaces on the devices under test, results attained from the CWMP Analyzer, and via an in-line protocol analyzer.

Latency in the network or discrepancies in the clocks of the CPE and ACS can cause minor variations in the time values associated with each test case that contain metrics dealing with exact time values. Due to this variance, tests that have metrics dealing with exact times also have a latency time value associated that is either a plus(+) or minus(-) time value in the test metric.

4.6 Optional Functionality Tag

The Optional Functionality Tag labels a test as Mandatory or Conditionally Mandatory. Mandatory tests are tests that are required to be run against all DUTs being certified. Conditionally Mandatory tests are only run against DUTs that support stated functionality of the specific test. Supported functionality is communicated to the test lab at the beginning of testing. Every supported RPC **MUST** be returned in the GetRPCMethodsResponse in test case 5.43, and any Optional RPC that is returned in that test case **MUST** be considered supported for the purpose of this test plan.

4.6.1 Optional Functionality Tests

Optional Functionality Tag	Test Case Number	Required Configuration
DHCP ACS URL Discovery (At least one of the following MUST be run)	5.11	Ability to set the ACS URL to null
DHCPv4 ACS URL Discovery	5.1, 5.3, 5.5, 5.12	
DHCPv6 ACS URL Discovery	5.2, 5.4, 5.6, 5.13	
Optional CWMP Configuration – ACS URL change on the DUT by third party means	5.16	Detailed steps to change the ACS URL on the CPE.
Secure CWMP Session (At least one of the following MUST be run)	5.25, 5.26, 5.33, 5.34	Detailed steps to load a new Certificate of authentication
Secure CWMP Session – SSL 3.0	5.22	
Secure CWMP Session – TLS 1.0	5.23	

	Secure CWMP Session – TLS 1.2	5.24	
Optional RPC – Cancel Transfer		5.84	
Optional RPC – Upload		5.85, 5.86, 5.87, 5.92	
Optional RPC – ScheduleInform		5.88	
Optional RPC – FactoryReset		5.89	
Optional RPC – GetAllQueuedTransfers		5.94	
Optional Parameter – EnableCWMP		5.100	
Absolute Time		5.103, 5.104	
Optional Parameter – NotificationThrottle		5.105	
XMPP Connection Request		5.111 – 5.122	

5 Test Procedures

5.1 ACS Discovery using DHCPv4

Purpose:

This test is designed to verify that the DUT attempts to use DHCPv4 to discover the ACS URL when the DUT has no value for the ManagementServer.URL

Optional Functionality Tag:

Conditionally Mandatory - DHCPv4 ACS URL Discovery

References:

Section 3.1/TR-069a1 or later
RFC 2132

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-069 specification, a CWMP enabled CPE must use DHCP to attempt to discover the ACS URL when the CPE has no value (empty or null) for the parameter ManagementServer.URL. A CPE identifies itself to the DHCP server as supporting this method by including the string “dslforum.org” (all lower case) anywhere in the Vendor Class Identifier (DHCP option 60). The CPE may then use the values received from the DHCP server in the Vendor Specific Information (DHCP option 43) to set the URL of the ACS and the Provisioning Code.

Test Setup:

1. Configure the DHCPv4 server or simulator to include the ACS URL in its DHCPv4 option 43.
2. Configure the DUT to have an empty or null value for the ManagementServer.URL parameter.
3. Connect the DUT, DHCPv4 server or simulator, and CWMP Analyzer to the network infrastructure

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.2 ACS Discovery using DHCPv6

Purpose:

This test is designed to verify that the DUT attempts to use DHCPv6 to discover the ACS URL when the DUT has no value for the ManagementServer.URL.

Optional Functionality Tag:

Conditionally Mandatory - DHCPv6 ACS URL Discovery

References:

Section 3.1/TR-069a3 or later
RFC 3315

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-069 specification, a CWMP enabled CPE must use DHCP to attempt to discover the ACS URL when the CPE has no value (empty or null) for the parameter ManagementServer.URL . A CPE identifies itself to the DHCP server as supporting this method by including the string “dslforum.org” (all lower case) anywhere in the Vendor Class (DHCP option 16). The CPE may then use the values received from the DHCP server in the Vendor Specific Information (DHCPv6 option 17) to set the URL of the ACS and the Provisioning Code.

Test Setup:

1. Configure the DHCPv6 server or simulator to include the ACS URL in its DHCPv6 options.
2. Configure the DUT to have an empty or null value for the ManagementServer.URL parameter.
3. Connect the DUT, DHCPv6 server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.3 ACS Rediscovery using DHCPv4

Purpose:

This test is designed to verify that the DUT consistently utilizes DHCPv4 to discover the ACS URL.

Optional Functionality Tag:

Conditionally Mandatory - DHCPv4 ACS URL Discovery

References:

Section 3.1/TR-069a1 or later
RFC 2131

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-069 specification, a CWMP enabled CPE must utilize the same method for acquiring an ACS URL that it was originally configured to use, regardless of the mechanism used to change the ACS URL at a later point.

Test Setup:

1. Configure the DHCP server or simulator to include a valid ACS URL in its DHCPv4 options.
2. Configure the DUT so that it must use DHCP to obtain an ACS URL the first time after its most recent factory default.
3. Connect the DUT, DHCPv4 server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.4 ACS Rediscovery using DHCPv6

Purpose:

This test is designed to verify that the DUT consistently utilizes DHCPv6 to discover the ACS URL.

Optional Functionality Tag:

Conditionally Mandatory - DHCPv6 ACS URL Discovery

References:

Section 3.1/TR-069a3 or later
RFC 3315

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-069 specification, a CWMP enabled CPE must utilize the same method for acquiring an ACS URL that it was originally configured to use, regardless of the mechanism used to change the ACS URL at a later point.

Test Setup:

1. Configure the DHCPv6 server or simulator to include a valid ACS URL in its DHCPv6 options.
2. Configure the DUT so that it must use DHCP to obtain an ACS URL the first time after its most recent factory default.
3. Connect the DUT, DHCPv6 server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.5 DHCP Retry to the DHCPv4 server

Purpose:

This test is designed to verify that the DUT retries its DHCP message when it does not receive a reply from the DHCP server.

Optional Functionality Tag:

Conditionally Mandatory - DHCPv4 ACS URL Discovery

References:

Section 3.1/TR-069a1 or later
RFC 2131

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CWMP enabled CPE must send a DHCP packet if it cannot communicate with the ACS indicated by the negotiated ACS URL value. Further, it must retry its DHCP packet if it does not receive a DHCPACK from the DHCP server within a reasonable time. This requirement is in accordance with RFC 2131.

Test Setup:

1. Configure the DHCP server or simulator to include the ACS URL in its DHCP options.
2. Configure the DUT to have an empty or null value for the ManagementServer.URL parameter.
3. Connect the DUT, DHCP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.6 DHCP Retry to the DHCPv6 server

Purpose:

This test is designed to verify that the DUT retries its DHCPv6 message when it does not receive a reply from the DHCP server.

Optional Functionality Tag:

Conditionally Mandatory - DHCPv6 ACS URL Discovery

References:

Section 3.1/TR-069a3 or later
RFC 3315

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CWMP enabled CPE must send a DHCPv6 packet if it cannot communicate with the ACS indicated by the negotiated ACS URL value. Further, it must retry its DHCPv6 packet if it does not receive a DHCPACK from the DHCP server within a reasonable time. This requirement is in accordance with RFC 3315.

Test Setup:

1. Configure the DHCP server or simulator to include the ACS URL in its DHCPv6 options.
2. Configure the DUT to have an empty or null value for the ManagementServer.URL parameter.
3. Connect the DUT, DHCPv6 server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.7 Session Initiation and Termination

Purpose:

This test is designed to verify that the CPE is able to initiate and terminate a session properly.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Sections 3.4.2, 3.7.1.1, 3.7.1.4/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

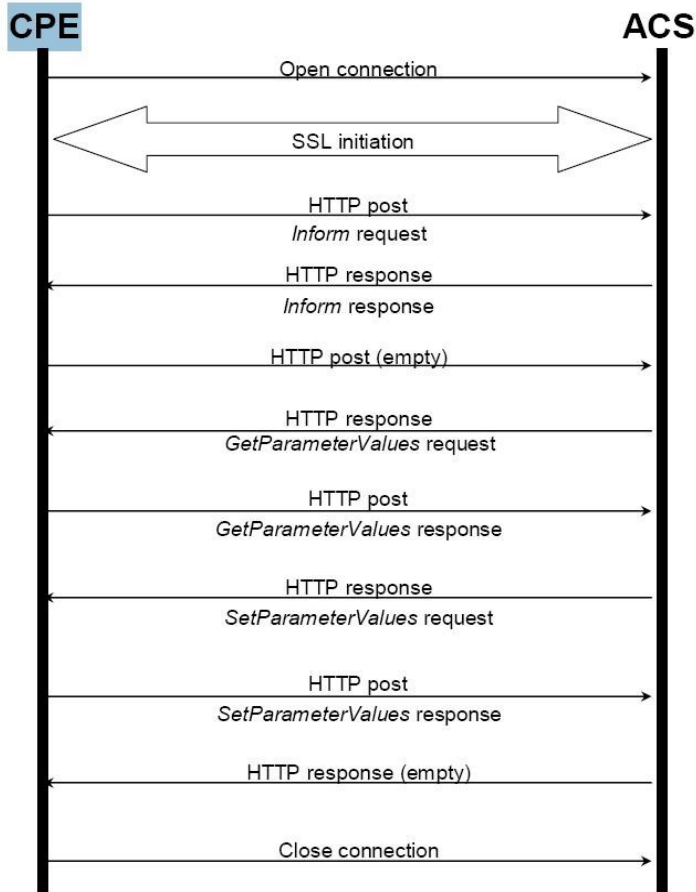
According to Broadband Forum TR-069 specification, once a connection between a CPE and an ACS is established, the CPE initiates a session by sending an initial Inform RPC on the ACS in an HTTP POST message. If and only if the CPE receives a successful Inform response to the Inform Request, the CPE considers the session to have been successfully initiated. Once initiated, the CPE must terminate the transaction session only when all of the following conditions are met:

The ACS has no further requests to send the CPE. The CPE concludes this if and only if the most recent HTTP response from the ACS was empty.

The CPE has no further requests to send to the ACS and the CPE has issued an empty HTTP POST to the ACS while HoldRequests is false (which indicates to the ACS that the CPE has no further requests for the remainder of the session). As defined in Table 6, if this condition has not been met but the CPE has no further requests or responses, it MUST send an empty HTTP POST, which will then fulfill this condition.

The CPE has received all outstanding response messages from the ACS.

The CPE has sent all outstanding response messages to the ACS resulting from prior requests. Figure below is an example of a session.



Test Setup:

1. Configure the CPE to use the ACS URL set on the CWMP Analyzer.
1. Connect the CPE, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.8 Session Initiation and Termination With no RPC

Purpose:

This test is designed to verify that the CPE is able to initiate and terminate a session properly.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Sections 3.4.2, 3.7.1.1, 3.7.1.4/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, once a connection between a CPE and an ACS is established, the CPE initiates a session by sending an initial Inform RPC on the ACS in an HTTP POST message. If and only if the CPE receives a successful Inform response to the Inform Request, the CPE considers the session to have been successfully initiated. Once initiated, the CPE must terminate the transaction session only when all of the following conditions are met:

- The ACS has no further requests to send the CPE. The CPE concludes this if and only if the most recent HTTP response from the ACS was empty.
- The CPE has no further requests to send to the ACS and the CPE has issued an empty HTTP POST to the ACS while HoldRequests is false (which indicates to the ACS that the CPE has no further requests for the remainder of the session). As defined in Table 6, if this condition has not been met but the CPE has no further requests or responses, it MUST send an empty HTTP POST, which will then fulfill this condition.
- The CPE has received all outstanding response messages from the ACS.
- The CPE has sent all outstanding response messages to the ACS resulting from prior requests.

Test Setup:

1. Configure the CPE to use the ACS URL set on the CWMP Analyzer.
2. Connect the CPE, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.9 Persistent TCP Connection Across a Single CWMP session

Purpose:

The purpose of this test is to verify that the ACS and CPE can maintain a persistent TCP connection across a single CWMP sessions.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, when a CPE receives an authentication challenge from ACS, the CPE must send the next HTTP request (including the “Authorization” HTTP header) in the same TCP connection unless the ACS specifically requested, via a “Connection: close” HTTP header, that the TCP connection be closed.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.10 Multiple TCP Connections Across a Single CWMP session

Purpose:

This test is designed to verify that ACS and CPE can maintain multiple TCP connections over a single CWMP session.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, for a sequence of transactions forming a single session, a CPE should maintain a TCP connection that persists throughout the duration of the session. However, if the TCP connection is cleanly closed after an HTTP request/response round trip, and if the session has not otherwise terminated (either successfully or unsuccessfully) at the time of the last HTTP response, the CPE MUST continue the session by sending the next HTTP request in a new TCP connection.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.11 Connection to ACS uses same mechanism after factory reset

Purpose:

This test is designed to verify that the DUT correctly connects to an ACS using the same connection mechanism as was used prior to the DUT being reset to factory defaults.

Optional Functionality Tag:

Conditionally Mandatory - DHCP ACS URL Discovery

References:

Section 3.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, the CPE MUST remember the mechanism it used to locate the ACS after each factory reset. If the CPE did not use DHCP to discover the ACS URL, then it SHOULD NOT fall back to using DHCP for ACS discovery. If the CPE originally used DHCP for ACS discovery, then when it fails to contact the ACS, it MUST perform re-discovery via DHCP.

Test Setup:

1. Configure the DUT to have an empty ACS URL.
2. Configure the DUT to use DHCP to discover the ACS
3. Connect the DUT, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.12 Handling Null Terminated ACS URL obtained from DHCPv4Server

Purpose:

This test is designed to verify that the DUT correctly interprets and acts upon the ACS URL used.

Optional Functionality Tag:

Conditionally Mandatory - DHCPv4 ACS URL Discovery

References:

Section 3.1/TR-069a1 or later
RFC 2131

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-069 specification, a CWMP enabled CPE must handle a null terminated ACS URL by accepting the URL as valid, without including the null terminating character in the URL.

Test Setup:

1. Configure the DHCPv4 server or simulator to include the ACS URL in its DHCPv4 options.
2. Configure the DUT to have an empty or null value for the ManagementServer.URL parameter.
3. Connect the DUT, DHCPv4 server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.13 Handling Null Terminated ACS URL obtained from DHCPv6 Server

Purpose:

This test is designed to verify that the DUT correctly interprets and acts upon the ACS URL used.

Optional Functionality Tag:

Conditionally Mandatory - DHCPv6 ACS URL Discovery

References:

Section 3.1/TR-069a3 or later
RFC 3315

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-069 specification, a CWMP enabled CPE must handle a null terminated ACS URL by accepting the URL as valid, without including the null terminating character in the URL.

Test Setup:

1. Configure the DHCPv6 server or simulator to include the ACS URL in its DHCPv6 options.
2. Configure the DUT to have an empty or null value for the ManagementServer.URL parameter.
3. Connect the DUT, DHCPv6 server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.14 Handling DNS server response

Purpose:

This test is designed to verify that the DUT does not cache the DNS server response beyond the duration of time to live (TTL) returned by DNS server.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.1/TR-069a1 or later
DNS RFC 1034

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, the CPE must not cache the DNS server response beyond the duration of time to live (TTL) returned by DNS server unless it cannot contact the DNS server for an update. This behavior is required by DNS RFC 1034 and provides an opportunity for the DNS Server to update stale data.

Test Setup:

1. Configure the DUT to have a valid value for the ManagementServer.URL parameter.
The URL requires DNS resolution
2. Connect the DUT, DNS server, DHCP server, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.15 ACS Modifies URL

Purpose:

This test is designed to verify that the DUT accepts, interprets, and utilizes a new ACS URL set by the ACS via CWMP.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, once the CPE has established a connection to the ACS, the ACS may at any time modify the ACS address Parameter stored within the CPE. Once modified, the CPE must use the modified address for all subsequent connections to the ACS.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure an alternate instance or ACS URL on the CWMP Analyzer.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.16 ACS URL change on the DUT by third party means

Purpose:

This test is designed to verify that the DUT will send an Inform message when the ACS URL is modified by some third party means.

Optional Functionality Tag:

Conditionally Mandatory - Optional CWMP Configuration

References:

Section 3.7.1.5/TR-069a1 or later

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-069 specification, if the ACS URL is modified by third party means then the DUT must send an Inform with an event code "0 BOOTSTRAP".

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.17 Parameters modified by ACS do not create a “4 VALUE CHANGE Inform event to the ACS

Purpose:

This test is designed to verify that the DUT will not start a new session when a parameter is modified by the managing ACS.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.2.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, parameter changes made by the ACS itself via SetParameterValues MUST NOT cause a new session to be initiated.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure a parameter that is capable of being modified for “active notification” via SetParameterAttributes
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.18 Event Discard after BOOTSTRAP Inform

Purpose:

This test is designed to verify that the DUT correctly discards all undelivered events once a BOOTSTRAP has been sent.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.7.1.5/TR-069a1 or later

Test Execution Type:

Manual

Normative Description:

According to the Broadband Forum TR-069 specification, the CPE MUST NOT ever discard an undelivered BOOTSTRAP event. All other undelivered events MUST be discarded on BOOTSTRAP.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT, DHCP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.19 Connection after Connection Request

Purpose:

This test is designed to verify that the DUT attempts to establish a connection with the ACS upon receiving a valid connection request from the ACS.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Sections 3.2.1, 3.2.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, the CPE MUST establish connection to the ACS after a valid connection request is received from an ACS. This is differentiated from a CPE that is connecting to an ACS in all previous tests.

A connection request is an HTTP 1.1 GET to a URL designated by the CPE. The URL value is available as read-only Parameter on the CPE. The path of this URL value SHOULD be randomly generated by the CPE so that it is unique per CPE.

The CPE must use HTTP digest authentication [7] to authenticate the ACS before proceeding—the CPE MUST NOT initiate a connection to the ACS due to an unsuccessfully authenticated request.

All CWMP sessions begin with the use of the Inform RPC. Each Inform RPC contains event codes in its arguments that indicate the event that caused the session to be initiated. In this case, the behavior is indicated by the event code “6 CONNECTION REQUEST”.

Test Setup:

1. Configure the DUT with a connection request URL, connection request username, and connection request password.
2. Configure the CWMP Analyzer to use the pre-configured URL, username, and password for connection requests.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.20 Connection Request while session exists

Purpose:

This test is designed to verify that the DUT that is already in an established session with an ACS, but then receives a Connection Request, does not terminate the existing session and either rejects the Connection Request or establishes a new session immediately following the existing session.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Sections 3.2.1, 3.2.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if the CPE is already in a session with the ACS when it receives one or more Connection Requests, it MUST NOT terminate that session prematurely as a result.

The CPE MUST instead take one of the following alternative actions:

- Reject each Connection Request by responding with an HTTP 503 status code (Service Unavailable). In this case, the CPE SHOULD NOT include the HTTP Retry-After header in the response.
- Following the completion of the session, initiate exactly one new session (regardless of how many Connection Requests had been received during the previous session) in which it includes the “6 CONNECTION REQUEST” EventCode in the Inform. In this case, the CPE MUST initiate the session immediately after the existing session is complete and all changes from that session have been applied.

Test Setup:

1. Configure the DUT with a connection request URL, connection request username, and connection request password.
2. Configure the CWMP Analyzer to use the pre-configured URL, username, and password for connection requests.
3. Configure the CWMP Analyzer to set the ManagementServer.PeriodicInformInterval to 10 and the ManagementServer.PeriodicInformEnabled to 1.
4. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.21 Connection after PeriodicInformInterval

Purpose:

This test is designed to verify that the CPE attempts to establish a connection with the ACS after a time period equal to ManagementServer.PeriodicInformInterval.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.2.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, the CPE MUST establish connection to the ACS after PeriodicInformInterval (example, after every 60 seconds). This is differentiated from a CPE connecting to an ACS for the first time, or a CPE connecting to the ACS after reboot.

All CWMP sessions begin with the use of the Inform RPC. Each Inform RPC contains event codes in its arguments that indicate the event that caused the session to be initiated. In this case, the behavior is indicated by the event code "2 PERIODIC".

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a short value for the ManagementServer.PeriodicInformInterval, between 60 and 300 seconds. Configure the DUT to use this value for ManagementServer.PeriodicInformInterval.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.22 Connection Establishment using SSL 3.0

Purpose:

This test is designed to verify that the CPE is able to establish a connection with the ACS using SSL 3.0.

Optional Functionality Tag:

Conditionally Mandatory - Secure CWMP Session – SSL3.0

References:

Section 3.3/TR-069a1 and TR-069a2

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, The CPE MUST support SSL3.0, TLS 1.0 or both.

Test Setup:

1. Configure the CWMP Analyzer to use SSL 3.0.
2. Configure the DUT to use the HTTPS URL of the analyzer.
3. Configure the DUT with a pre-determined username and password for authentication.
4. Generate and install on the DUT a valid certificate for use in authentication with the CWMP Analyzer.
5. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.23 Connection Establishment using TLS 1.0

Purpose:

This test is designed to verify that the CPE is able to establish a connection with the ACS using TLS 1.0.

Optional Functionality Tag:

Conditionally Mandatory - Secure CWMP Session – TLS 1.0

References:

Section 3.3/TR-069a1 and TR-069a2

Test Execution Type:

Automated

Normative Description:

The CPE MUST support SSL3.0, TLS 1.0 or both.

Test Setup:

1. Configure the CWMP Analyzer to use TLS 1.0.
2. Configure the DUT to use the HTTPS URL of the analyzer.
3. Configure the DUT with a pre-determined username and password for authentication.
4. Generate and install on the DUT a valid certificate for use in authentication with the CWMP Analyzer.
5. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.24 Connection Establishment using TLS 1.2

Purpose:

This test is designed to verify that the CPE is able to establish a connection with the ACS using TLS 1.2.

Optional Functionality Tag:

Conditionally Mandatory - Secure CWMP Session – TLS 1.2

References:

Section 3.3/TR-069a3 or later

Test Execution Type:

Automated

Normative Description:

The CPE Should support TLS 1.2 (or a later version).

Test Setup:

1. Configure the CWMP Analyzer to use TLS 1.2.
2. Configure the DUT to use the HTTPS URL of the analyzer.
3. Configure the DUT with a pre-determined username and password for authentication.
4. Generate and install on the DUT a valid certificate for use in authentication with the CWMP Analyzer.
5. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.25 Common Name certificate validation

Purpose:

This test is designed to verify that the CPE is able to verify that the Common Name component of the subject field of the ACS certificate is the same as that in the host portion of the ACS URL.

Optional Functionality Tag:

Conditionally Mandatory - Secure CWMP Session

References:

Section 3.3/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, authentication of the ACS requires that the CPE MUST validate the certificate against a root certificate, and that the CPE MUST ensure that the value of the CN (Common Name) component of the Subject field in the certificate exactly matches the host portion of the ACS URL known to the CPE (even if the host portion of the ACS URL is an IP address).

Test Setup:

1. Configure the CWMP Analyzer to use SSL/TLS.
2. Configure the DUT and CWMP Analyzer with a pre-determined username and password for authentication.
3. Generate and install on the CWMP Analyzer a valid certificate for use in authentication with the CPE.
4. Configure the DUT to have a valid CA certificate.
5. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.26 Rejection of Invalid Certificate

Purpose:

This test is designed to verify that the CPE does not authenticate a Communication from the ACS when the certificate is invalid.

Optional Functionality Tag:

Conditionally Mandatory - Secure CWMP Session

References:

Section 3.3/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CPE MAY use certificate based authentication to validate Connection Requests from the ACS. If the DUT implements this functionality, it must not validate Connection Requests from the ACS when the certificate is invalid.

Test Setup:

1. Configure the CWMP Analyzer to use appropriate SSL/TLS.
2. Configure the DUT to use the HTTPS URL of the analyzer.
3. Configure the DUT with a pre-determined username and password for authentication.
4. Install mismatched certificates in the DUT and CWMP Analyzer.
5. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.27 Use of Multiple Session Cookies Across Transactions in a Session

Purpose:

This test is designed to verify that the CPE can successfully interact using cookies across multiple CWMP sessions.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CPE must support the use of cookies including the return of the cookie value in each subsequent HTTP POST, with the exception that a CPE need not support storage of cookies beyond the duration of a session. The CPE must support the compatibility requirements of section 9.1 of [7]. The CPE must support the use of multiple cookies by the ACS, and must make available at least 512 bytes for storage of cookies.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the CWMP Analyzer to use session cookies.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.28 Session Retry

Purpose:

This test is designed to verify that the DUT retries a failed session with the ACS.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.2.1.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CPE must retry failed sessions to attempt to redeliver events that it has previously failed to deliver and to allow the ACS to make additional requests in a timely fashion. The CPE MUST keep track of the number of times it has attempted to retry a failed session.

If the CPE fails to establish a session, this might be because the CPE supports CPE WAN Management Protocol v1.1 (or later) and the ACS supports only v1.0. If this situation is suspected, the CPE MUST revert to v1.0 when retrying the failed session.

A CPE MUST retry a failed session after waiting for an interval of time specified in the following Table or when a new event occurs, whichever comes first. The CPE MUST choose the wait interval by randomly selecting a number of seconds from a range given by the post-reboot session retry count. Beginning with the tenth post-reboot session retry attempt, the CPE MUST choose from a range between 2560 and 5120 seconds. The CPE MUST continue to retry a failed session until it is successfully terminated. Once a session terminates successfully, the CPE MUST reset the session retry count to zero and no longer applies the session retry policy to determine when to initiate the next session.

The CPE receives an HTTP layer fault from the ACS notifying it to revert back to CWMP v 1.0. It retries session with the ACS by reverting back to v1.0 when retrying the failed session.

Post reboot session retry count	Wait interval range (min-max seconds)
#1	5-10
#2	10-20
#3	20-40
#4	40-80
#5	80-160
#6	160-320
#7	320-640
#8	640-1280
#9	1280-2560
#10 and subsequent	2560-5120

Test Setup:

1. Configure the CPE to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.29 SOAP Response in an HTTP Request

Purpose:

This test is designed to verify that the SOAP Response is encoded properly in an HTTP Request Message.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, when there is a SOAP response in an HTTP Request, or when there is a SOAP Fault response in an HTTP Request, the SOAPAction header in the HTTP Request MUST have no value (with no quotes), indicating that this header provides no information as to the intent of the message. That is, it must appear as follows:

SOAPAction:

In addition to that, when an HTTP Request contains a SOAP Envelope, the HTTP Content-Type header must have a type/subtype of "text/xml"

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.30 HTTP Redirection Test – 302 Redirect

Purpose:

This test is designed to verify that the CPE supports the use of HTTP redirection by the ACS using the 302 (Found) status code.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CPE must support the use of HTTP redirection by the ACS. In doing so, the CPE must support the 302(Found) HTTP status code. In case of redirection, the CPE must attempt to continue the session using the URL provided in the HTTP redirect response. The CPE must resend the HTTP POST that resulted in the redirect response to the ACS at the redirected URL, and the CPE must then attempt to proceed with the session exactly as if no redirection had occurred. The redirected URL must not be saved by the CPE (i.e. as the value of the IGD.ManagementServer.URL) for use in any subsequent session or any subsequent retries of the session.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. If the CWMP Analyzer is capable of supporting multiple ACS URLs, configure an alternate ACS URL on the CWMP Analyzer.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.31 HTTP Redirection Test – 307 Redirect

Purpose:

This test is designed to verify that the CPE supports the use of HTTP redirection by the ACS using the 307 (Temporary Redirect) status code.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CPE must support the use of HTTP redirection by the ACS. In doing so, the CPE must support the 307(Temporary) HTTP status code. In case of redirection, the CPE must attempt to continue the session using the URL provided in the HTTP redirect response. The CPE must resend the HTTP POST that resulted in the redirect response to the ACS at the redirected URL, and the CPE must then attempt to proceed with the session exactly as if no redirection had occurred. The redirected URL must not be saved by the CPE (i.e. as the value of the IGD.ManagementServer.URL) for use in any subsequent session or any subsequent retries of the session.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. If the CWMP Analyzer is capable of supporting multiple ACS URLs, configure an alternate ACS URL on the CWMP Analyzer.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.32 HTTP Redirection – Multiple Redirections

Purpose:

This test is designed to verify that the CPE allows up to 5 consecutive redirections.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CPE must allow up to 5 consecutive redirections. If the CPE is redirected more than 5 times consecutively, it may consider the session unsuccessfully terminated.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure Two ACS URLs on the CWMP Analyzer.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.33 HTTP Redirection – HTTPS with URL Matching Certificate

Purpose:

This test is designed to verify that the CPE supports the use of HTTP redirection by the ACS to an HTTPS URL.

Optional Functionality Tag:

Conditionally Mandatory - Secure CWMP Session

References:

Section 3.4.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if an HTTPS URL is provided in the HTTP redirection, by the ACS, the CPE must use SSL/TLS as transport mechanism, and establish connection with the HTTPS URL.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. If the CWMP Analyzer is capable of supporting multiple ACS URLs, configure an alternate https ACS URL on the CWMP Analyzer.
3. Generate the proper certificates for the alternate https URL.
4. Install the proper certificates on the DUT
5. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.34 HTTP Redirection – HTTPS with URL/Certificate Mismatch

Purpose:

This test is designed to verify that, when redirected, the CPE does not connect to an ACS with an HTTPS URL when the certificate is invalid for the URL.

Optional Functionality Tag:

Conditionally Mandatory - Secure CWMP Session

References:

Section 3.4.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if as a result of an HTTP redirect, the CPE is attempting to access an ACS at a URL different from its pre-configured ACS URL, the CPE MUST validate the CN component of the ACS certificate against the host portion of the redirected ACS URL rather than the pre-configured ACS URL.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP analyzer.
2. If the CWMP analyzer is capable of supporting multiple ACS URLs, configure an alternate https ACS URL on the CWMP analyzer.
3. Generate the proper certificates for the original ACS URL.
4. Install the certificates on the DUT.
5. Connect the DUT and CWMP analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.35 Redirection at any Point in a Session

Purpose:

This test is designed to verify that the DUT correctly interprets and acts upon a Redirection request during an open session

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, the CPE MUST allow redirection to occur at any point during a session (including the Inform response), and the ACS MAY issue a redirect at any point during a session.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT, DHCP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.36 HTTP Redirection – Use of session cookies

Purpose:

This test is designed to verify that the CPE can successfully communicate using cookies even after HTTP redirection.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CPE must include all cookies associated with the session in subsequent HTTP requests to the redirected ACS. The CPE must consider a redirect from an ACS to be a “verifiable transaction” and thus it must send cookies to the redirected ACS without performing domain validation of each cookie.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. If the CWMP Analyzer is capable of supporting multiple ACS URLs, configure an alternate ACS URL on the CWMP Analyzer.
3. Configure the CWMP Analyzer to use session cookies.
4. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.37 Redirect HTTP Response Contains Data

Purpose:

This test is designed to verify that the DUT correctly interprets and acts upon a non-empty HTTP Response sent from the ACS.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, in an HTTP response sent by the ACS containing a redirect status code, the length of the HTTP message-body MUST be zero. If the CPE receives an HTTP re-direct response with a non-empty message-body, it MUST ignore the content of the message-body.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the CWMP Analyzer to send an HTTP Response that contains data.
3. Connect the DUT, DHCP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.38 HTTP Authentication - Basic Authentication

Purpose:

This test is designed to verify that the CPE can successfully establish a CWMP session with the ACS using basic authentication.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4.4/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CPE must support Basic Authentication.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the CWMP Analyzer to use basic authentication.
3. The CWMP Analyzer is configured with proper credentials for the DUT.
4. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.39 Qop Authentication setting

Purpose:

This test is designed to verify that the DUT correctly sets the qop authentication field to “auth”

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4.5/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, the CPE and the ACS MUST support the RFC 2617 “qop” option containing the value “auth”.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the CWMP Analyzer to use Digest authentication.
3. The CWMP Analyzer is configured with proper credentials for the DUT.
4. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.40 HTTP Authentication - Digest Authentication

Purpose:

This test is designed to verify that the CPE can successfully establish a CWMP session with the ACS using digest authentication.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4.4/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CPE must support Digest Authentication.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the CWMP Analyzer to use Digest authentication.
3. The CWMP Analyzer is configured with proper credentials for the DUT.
4. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.41 Maximum SOAP Message Size

Purpose:

This test is designed to verify that the DUT can accept a SOAP message of 32768 bytes.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.5/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, a CPE MUST be able to accept a SOAP request with a total envelope size of at least 32 kilobytes (32768 bytes) without resulting in a “Resources Exceeded” response.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the CWMP Analyzer to create and send a 32768 byte SOAP message.
3. Connect the DUT, DHCP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.42 SetParameterValues SOAP Fault Format

Purpose:

This test is designed to verify that the SetParameterValuesFault element in a SOAP Fault response is formed properly.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.5/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, along with the SOAP fault requirements outlined in the SOAP Fault Format test case, a SOAP Fault error during SetParameterValues must contain a SetParameterValuesFault element. This element is to be used only in an error response to the SetParameterValues method, that contains a list of one or more structures indicating the specific fault associated with each parameter in error. The structure contains the following elements:

- A ParameterName element that contains the full path name of the parameter in error.
- A FaultCode element that contains a single numeric fault code that indicates the fault associated with the particular parameter in error.
- A FaultString element that contains a human readable description of the fault for the particular parameter in error.

```
<soap:Envelope
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:cwmp="urn:dslforum-org:cwmp-1-0">
  <soap:Header>
    <cwmp:ID soap:mustUnderstand="1">1234</cwmp:ID>
  </soap:Header>
  <soap:Body>
    <soap:Fault>
      <faultcode>Client</faultcode>
      <faultstring>CWMP fault</faultstring>
      <detail>
        <cwmp:Fault>
          <FaultCode>9003</FaultCode>
          <FaultString>Invalid arguments</FaultString>
          <SetParameterValuesFault>
            <ParameterName>
              InternetGatewayDevice.Time.LocalTimeZone
            </ParameterName>
            <FaultCode>9012</FaultCode>
            <FaultString>Not a valid time zone value</FaultString>
          </SetParameterValuesFault>
        </cwmp:Fault>
      </detail>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a valid, writable parameter from the DUT's supported data model.
3. Construct an invalid parameter name within the context of the DUT's supported data model.
4. Select a non-writable parameter from the DUT's supported data model.
5. Choose a parameter with a restrictive data type in the DUT's supported data model.
6. Choose a parameter with restricted possible values in the DUT's supported data model.
7. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.43 GetRPCMethods and Required RPCs

Purpose:

This test is designed to verify that the CPE supports all the required RPCs.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.1.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CPE must support the following required RPCs, and may optionally support other RPCs: GetRPCMethods, SetParameterValues, GetParameterValues, GetParameterNames, SetParameterAttributes, GetParameterAttributes, AddObject, DeleteObject, Reboot, Download.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.44 GetParameterNames – Complete Path

Purpose:

This test is designed to verify that the CPE is capable of responding to a simple complete path request made by the ACS to determine its accessibility.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.1.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CPE must support the following required RPCs, and may optionally support other RPCs: GetRPCMethods, SetParameterValues, SetParameterValues, GetParameterNames, SetParameterAttributes, GetParameterAttributes, AddObject, DeleteObject, Reboot, Download.

The GetParameterNames RPC is used to determine the availability of parameters in the CPEs data model and their access level. The RPC can a complete or partial path as its argument; this test exercises the ability to complete the GetParameterNames RPC using a complete parameter path.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.45 GetParameterNames – Complete Path, NextLevel True

Purpose:

This test is designed to verify that the CPE is capable of appropriately responding to a simple complete path request with the NextLevel set to True made by the ACS.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.3/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

If NextLevel is true and ParameterPath is a Parameter name rather than a partial path, the CPE MUST return a fault response with the Invalid Arguments fault code (9003).

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.46 GetParameterNames – Partial Path – Next Level True

5.46.A Single-Instance Object

Purpose:

This test is designed to verify that the CPE is capable of responding to a partial path request made by the ACS when next level is set to true and the partial path is of a single-instance object.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.3/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, when next level argument in GetParameterNames is set to true, the response from the DUT must contain all parameters and objects that are next-level children of the object given by the ParameterPath argument, if any. For example, if ParameterPath were “Device.Hosts.”, the response might include the following:

Device.Hosts.HostNumberOfEntries

Device.Hosts.Host.

Note: The next-level children of a single-instance object are its parameters, its single-instance object children and its multi-instance object children.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.46.B Multi-Instance Object (Empty)

Purpose:

This test is designed to verify that the CPE is capable of responding to a partial path request made by the ACS when next level is set to true and the partial path is of an empty multi-instance object.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.3/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, when next level argument in GetParameterNames is set to true, the response from the DUT must contain all parameters and objects that are next-level children of the object given by the ParameterPath argument, if any. For example, if ParameterPath were "Device.Hosts.Host." and there were no instances, the response would include an empty ParameterList.

Note:

If the DUT does not include an empty multi-instance object, this test case may be omitted.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.46.C Multi-Instance Object (Non-Empty)

Purpose:

This test is designed to verify that the CPE is capable of responding to a partial path request made by the ACS when next level is set to true and the partial path is of a non-empty multi-instance object.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.3/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, when next level argument in GetParameterNames is set to true, the response from the DUT must contain all parameters and objects that are next-level children of the object given by the ParameterPath argument, if any. For example, if ParameterPath were “Device.Hosts.Host.” and there were two instances, the response would include the following:

Device.Hosts.Host.1.

Device.Hosts.Host.2.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.47 GetParameterNames – Partial Path – Next Level False – Single-Instance Object

5.47.A Single-Instance Object

Purpose:

This test is designed to verify that the CPE is capable of responding to a partial path request made by the ACS when next level is set to false and the partial path is of a single-instance object.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.3/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, when next level argument in GetParameterNames is set to false, the response must contain the parameter or object whose name exactly matches the ParameterPath argument, if any (all levels below the specified object in the object hierarchy). For example, if ParameterPath were “Device.Hosts.”, the response might include the following:

- Device.Hosts.
- Device.Hosts.HostNumberOfEntries
- Device.Hosts.Host.
- Device.Hosts.Host.1.
- Device.Hosts.Host.1.PhysAddress
- Device.Hosts.Host.1.IPAddress
- Device.Hosts.Host.1.DHCPClient
- Device.Hosts.Host.1.AssociatedDevice
- Device.Hosts.Host.1.Layer1Interface
- Device.Hosts.Host.1.Layer3Interface
- Device.Hosts.Host.1.HostName
- Device.Hosts.Host.1.Active

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.47.B Multi-Instance Object (Empty)

Purpose:

This test is designed to verify that the CPE is capable of responding to a partial path request made by the ACS when next level is set to false and the partial path is of an empty multi-instance object.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.3/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, when next level argument in GetParameterNames is set to false, the response must contain the parameter or object whose name exactly matches the ParameterPath argument, if any (all levels below the specified object in the object hierarchy). For example, if ParameterPath were "Device.Hosts.Host." and there were no instances, the response would include the following:

Device.Hosts.Host.

Note:

If the DUT does not include an empty multi-instance object, this test case may be omitted.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.47.C Multi-Instance Object (Non-Empty)

Purpose:

This test is designed to verify that the CPE is capable of responding to a partial path request made by the ACS when next level is set to false and the partial path is of a non-empty multi-instance object.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.3/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, when next level argument in GetParameterNames is set to false, the response must contain the parameter or object whose name exactly matches the ParameterPath argument, if any (all levels below the specified object in the object hierarchy). For example, if ParameterPath were "Device.Hosts.Host.", and there was one instance, the response might include the following:

Device.Hosts.Host.
Device.Hosts.Host.1.
Device.Hosts.Host.1.PhysAddress
Device.Hosts.Host.1.IPAddress
Device.Hosts.Host.1.DHCPClient
Device.Hosts.Host.1.AssociatedDevice
Device.Hosts.Host.1.Layer1Interface
Device.Hosts.Host.1.Layer3Interface
Device.Hosts.Host.1.HostName
Device.Hosts.Host.1.Active

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.48 GetParameterNames – Invalid Path

Purpose:

This test is designed to verify that the CPE can identify an invalid path and respond with appropriate error message to a GetParameterNames request on an invalid parameter.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.3/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, when a GetParameterNames is attempted on an invalid parameter, the CPE must respond with a 9005 (Invalid Parameter Name) fault code.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose an incorrect parameter path name that has some contextual meaning to the DUT's supported data model. For example, "Device.DeviceInfo.Invalid."
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.49 GetParameterNames – Entire Object Model

Purpose:

This test is designed to verify that the CPE can communicate its entire object model to the ACS.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.3/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, when ParameterPath argument in the GetParameterNames is set to the root object in the DUT's data model (i.e., "InternetGatewayDevice.", or "Device."), and next level argument in GetParameterNames is set to false, the response must contain the entire object model supported by the DUT.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.50 GetParameterValues – Simple Complete Path

Purpose:

This test is designed to verify that the CPE can respond to a GetParameterValues request by the ACS on a simple complete path.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to BroadBand Forum TR-069 specification, a CPE must be able to respond to a GetParameterValues Request from an ACS when the argument is an array of strings, each representing the name of a requested parameter.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a valid parameter from the DUT's supported data model.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.51 GetParameterValues – Multiple Complete Paths

Purpose:

This test is designed to verify that the CPE can respond to a GetParameterValues request by the ACS on a complete path.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.2.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to BroadBand Forum TR-069 specification, a CPE must be able to respond to a GetParameterValues Request from an ACS when the argument is an array of strings, each representing the name of a requested parameter.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose two valid parameters from the DUTs supported data model.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.52 GetParameterValues – Partial Path

Purpose:

This test is designed to verify that the CPE can respond to a GetParameterValues request by the ACS on a partial path.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to BroadBand Forum TR-069 specification, a CPE must be able to respond to a GetParameterValues Request from an ACS when the argument is an array of strings, each representing the name of a requested parameter. If the parameter name argument is given as a partial path name, the request is to be interpreted as a RPC on return all of the Parameters in the branch of the naming hierarchy that shares the same prefix as the argument. A partial path name must end with a “.”(dot) after the last node name in the hierarchy. An empty string indicates the top of the name hierarchy.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a valid partial parameter path from the DUT's supported data model.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.53 GetParameterValues – Complete and Partial Paths

Purpose:

This test is designed to verify that the CPE can respond to a GetParameterValues request by the ACS on both complete and partial paths.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to BroadBand Forum TR-069 specification, a CPE must be able to respond to a GetParameterValues Request from an ACS when the argument is an array of strings, each representing the name of a requested parameter. If the parameter name argument is given as a partial path, the request is to be interpreted as a RPC to return all of the Parameters in the branch of the naming hierarchy that shares the same prefix as the argument. A partial path name must end with a “.”(dot) after the last node name in the hierarchy. An empty string indicates the top of the name hierarchy.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose two valid parameter paths from the DUT’s supported data model, one partial and one complete path.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.54 GetParameterValues – Entire Object Model

Purpose:

This test is designed to verify that the CPE can respond to a GetParameterValues request by the ACS on a partial path representing the top level in the data model with the entire object model.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to BroadBand Forum TR-069 specification, a CPE must be able to respond to a GetParameterValues Request from an ACS when the argument is an array of strings, each representing the name of a requested parameter. If the parameter name argument is given as a partial path name, the request is to be interpreted as a RPC on return all of the Parameters in the branch of the naming hierarchy that shares the same prefix as the argument. A partial path name must end with a “.”(dot) after the last node name in the hierarchy. An empty string indicates the top of the name hierarchy.

Unlike the GetParameterNames RPC, a CPE may reject a GetParameterValues call on the entire object model. However, it may only do so due to a “9004 Resources Exceeded” error.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.55 GetParameterValues – Fault condition

Purpose:

This test is designed to verify that the CPE can respond to a GetParameterValues appropriately if there is a fault condition with the ParameterNames element.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum Tr-069 specification, if the fault is caused by one or more invalid parameter names in the ParameterNames array, the Invalid Parameter Name fault code (9005) MUST be used instead of the more general Invalid Arguments fault code (9003). The value of a ParameterNames element MUST be considered invalid if it does not exactly match either the name of a parameter currently present in the CPE's data model (if the ParameterNames element does not end with a dot) or the name of an object currently present in the CPE's data model (if ParameterNames element ends with a dot).

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a valid parameter from the DUT's supported data model, but incorrectly modify the ParameterNames parameter.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.56 SetParameterValues – Single Parameter

Purpose:

This test is designed to verify that the CPE supports the required SetParameterValues RPC and can change a single parameter.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if an ACS calls SetParameterValues on a DUT, the DUT must support the request and respond appropriately. On successful receipt of a SetParameterValues RPC, the CPE must apply the changes to all of the specified Parameters atomically. That is, either all of the value changes are applied together, or none of the changes are applied at all. In the latter case, the CPE must return a fault response indicating the reason for the failure to apply the changes. The CPE must not apply any of the specified changes without applying all of them. This requirement must hold true even if the CPE experiences a crash during the process of applying the changes.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a valid, writable parameter from the DUT's supported data model.
3. Configure the CWMP Analyzer to set the ParameterKey argument in the GetParameterValues RPC to a unique value.
4. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.57 SetParameterValues – Multiple Parameters

Purpose:

This test is designed to verify that the CPE supports the required SetParameterValues RPC and can change multiple parameters in a single procedure call.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if an ACS calls SetParameterValues on a DUT, the DUT must support the request and respond appropriately. On successful receipt of a SetParameterValues RPC, the CPE must apply the changes to all of the specified Parameters atomically. That is, either all of the value changes are applied together, or none of the changes are applied at all. In the latter case, the CPE must return a fault response indicating the reason for the failure to apply the changes. The CPE must not apply any of the specified changes without applying all of them. This requirement must hold true even if the CPE experiences a crash during the process of applying the changes.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose at least two valid, writable parameters from the DUT's supported data model.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.58 SetParameterValues – Same Parameter Multiple Times

Purpose:

This test is designed to verify that the CPE supports the required SetParameterValues RPC and can respond back with the appropriate error code when a value for the same Parameter Name is set twice in the same SetParameterValues RPC.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, the ParameterList array, in the SetParameterValues RPC, MUST NOT contain more than one entry with the same Parameter name. If a given Parameter appears in this array more than once, the CPE MUST respond with fault 9003 (Invalid arguments).

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose at least one valid, writable parameters from the DUT's supported data model. Have the CWMP Analyzer set that parameter value twice in the same ParameterList of a SetParameterValues RPC.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.59 SetParameterValues – Atomic Test

Purpose:

This test is designed to verify that the CPE supports the required SetParameterValues RPC. When the SetParameterValues RPC contains multiple entries and one is incorrect that it will respond with the correct Fault code.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum Tr-069 specification, on successful receipt of a SetParameterValues RPC, the CPE MUST apply the changes to all of the specified Parameters atomically. That is, either all of the value changes are applied together, or none of the changes are applied at all. In the latter case, the CPE MUST return a fault response indicating the reason for the failure to apply the changes. The CPE MUST NOT apply any of the specified changes without applying all of them.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose at least two valid, writable parameters from the DUT's supported data model. Allow one of the Parameter Names to be set incorrectly.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.60 GetParameterAttributes – Complete Path

Purpose:

This test is designed to verify that the CPE can provide attribute information of a single complete path.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.5/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if an ACS requests for attribute information of a parameter using GetParameterAttributes method, the CPE must reply to the request with attribute information of the parameter.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a valid parameter path in the DUT's supported data model.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.61 GetParameterAttributes – Multiple Complete Paths

Purpose:

This test is designed to verify that the CPE can provide attribute information of multiple complete paths.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.5/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if an ACS requests for attribute information of an array of parameters using GetParameterAttributes method, the CPE must reply to the request with attribute information of all the parameters in the array.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose two valid parameter paths in the DUT's supported data model.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.62 GetParameterAttributes – Partial Path

Purpose:

This test is designed to verify that the CPE can return attribute information of all the parameters in the branch of the name hierarchy that shares the same prefix as the partial path argument.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if an ACS requests for attribute information of an array of parameters using GetParameterAttributes method, the CPE must reply to the request with attribute information of all the parameters in the array. If a parameter name argument is given as a partial path name, the request is to be interpreted as a RPC on return all of the Parameters in the branch of the naming hierarchy that shares the same prefix as the argument.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a valid partial parameter path from the DUT's supported data model.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.63 GetParameterAttributes – Complete and Partial Path

Purpose:

This test is designed to verify that the CPE can return attribute information of all the parameters in the branch of the name hierarchy that shares the same prefix as the partial path argument.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.5/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if an ACS requests for attribute information of an array of parameters using GetParameterAttributes method, the CPE must reply to the request with attribute information of all the parameters in the array. If a parameter name argument is given as a partial path name, the request is to be interpreted as a RPC on return all of the Parameters in the branch of the naming hierarchy that shares the same prefix as the argument.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a valid complete parameter path and a valid partial parameter path in the DUT's supported data model.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.64 GetParameterAttributes – Invalid Parameter Name

Purpose:

This test is designed to verify that the CPE can return the appropriate Fault code when the Parameter Name is invalid in a GetParameterAttributes RPC.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.5/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if an ACS requests for attribute information with an invalid Parameter Name using GetParameterAttributes method, the Invalid Parameter Name fault code (9005) MUST be used instead of the more general Invalid Arguments fault code (9003).

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the CWMP Analyzer with a GetParameterAttributes RPC method that contains an invalid Parameter Name
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.65 GetParameterAttributes – Partial Path empty

Purpose:

This test is designed to verify that the CPE can return the appropriate response when the Parameter Name of a partial path request does not have any sub objects in that partial path.

Note that for other CPE devices, although CWMP requires the ability to get parameter attributes on a partial path that is empty may not be widespread in implementation. If this is the case, those CPE devices should skip this test

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.5/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, if the ParameterNames argument in the request was a partial path, and if there are no Parameters within the object represented by that partial path (at any level below), the ParameterList MUST be empty, and this MUST NOT cause an error response. For example, if the PortMapping table contained zero instances and you perform a partial path GetParameterAttributes RPC on this table it would return an empty ParameterList in the GetParameterAttributesResponse RPC.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the CWMP Analyzer with a GetParameterAttributes RPC method that contains a partial path Parameter Name or an object that does not have any sub-objects populated
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.66 SetParameterAttributes – Active Notifications

Purpose:

This test is designed to verify that the CPE can successfully process SetParameterAttributes request from the ACS on a complete path with notification set to Active.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.4/TR-069a1 or later

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-069 specification, when the CPE receives a SetParameterAttributes request from the ACS on a complete path with notification set to Active, the CPE must initiate a session to the ACS, and include the new value in the ParameterList in the associated Inform message when the specified parameter value changes.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a parameter from the DUT's supported data model that can be altered locally from the DUT's interface and is capable of performing active notification.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.67 SetParameterAttributes – Active Notifications Persistence

Purpose:

This test is designed to verify that the CPE can successfully process SetParameterAttributes request from the ACS on a complete path with notification set to Active and that the setting persists across a device reboot.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.4/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, when the CPE receives a SetParameterAttributes request from the ACS on a complete path with notification set to Active, the CPE must initiate a session to the ACS, and include the new value in the ParameterList in the associated Inform message when the specified parameter value changes.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a parameter from the DUT's supported data model that can be altered locally from the DUT's interface and is capable of performing active notification.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.68 SetParameterAttributes – Atomic

Purpose:

This test is designed to verify that the CPE can successfully process SetParameterAttributes request from the ACS containing multiple attributes, one that is in error.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.4/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, on successful receipt of a SetParameterAttributes RPC, the CPE MUST apply the changes to all of the specified Parameters immediately and atomically. That is, either all of the attribute changes are applied together, or none of the changes are applied at all. In the latter case, the CPE MUST return a fault response indicating the reason for the failure to apply the changes. The CPE MUST NOT apply any of the specified changes without applying all of them. This requirement MUST hold even if the CPE experiences a crash during the process of applying the changes.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the CWMP Analyzer to send a SetParameterAttributes RPC containing two distinct attribute changes. One of the changes is in error (invalid ParameterName).
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.69 SetParameterAttributes – Passive Notification – Complete Path

Purpose:

This test is designed to verify that the CPE can successfully process SetParameterAttributes request from the ACS on a complete path with notification set to Passive.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.4/TR-069a1 or later

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-069 specification, when the CPE receives a SetParameterAttributes request from the ACS on a complete path with notification set to Passive, whenever the specified parameter value changes, the CPE must include the new value in the ParameterList in the Inform message that is sent the next time a session is established to the ACS. If the CPE has rebooted, or the URL of the ACS has changed since the last session, the CPE can choose to not include the changed parameter in the first session established with either the old ACS or the new ACS.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a parameter from the DUT's supported data model that can be altered locally from the DUT's interface.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.70 SetParameterAttributes – Passive Notification – Partial Path

Purpose:

This test is designed to verify that the CPE can successfully process SetParameterAttributes request from the ACS on a partial path with notification set to Passive.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.4/TR-069a1 or later

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-069 specification, when the CPE receives a SetParameterAttributes request from the ACS on a particular path with notification set to Passive, whenever the specified parameter value changes, the CPE must include the new value in the ParameterList in the Inform message that is sent the next time a session is established to the ACS. If the path is partial, the new attributes are to be applied to all Parameters below this point in the name hierarchy. If the CPE has rebooted, or the URL of the ACS has changed since the last session, the CPE can choose to not include the changed parameter in the first session established with either the old ACS or the new ACS.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a partial parameter path from the DUT's supported data model that contains parameters that can be altered locally from the DUT's interface.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.71 SetParameterAttributes – Passive Notification – Complete and Partial Path

Purpose:

This test is designed to verify that the CPE can successfully process SetParameterAttributes request from the ACS on both complete and partial paths with notification set to Passive.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.4/TR-069a1 or later

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-069 specification, when the CPE receives a SetParameterAttributes request from the ACS on a particular path with notification set to Passive, whenever the specified parameter value changes, the CPE must include the new value in the ParameterList in the Inform message that is sent the next time a session is established to the ACS. If the path is partial, the new attributes are to be applied to all Parameters below this point in the name hierarchy. If the CPE has rebooted, or the URL of the ACS has changed since the last session, the CPE can choose to not include the changed parameter in the first session established with either the old ACS or the new ACS.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose two parameter paths, one complete and one partial, from the DUT's supported data model that contain parameters that can be altered locally from the DUT's interface.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.72 SetParameterAttributes – Disable Notification

Purpose:

This test is designed to verify that the CPE is capable of disabling previously set notification attribute.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.4/TR-069a1 or later

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-069 specification, when the CPE receives a SetParameterAttributes request from the ACS on a particular path with notification set to 0 (disable notification), the CPE must cease informing the ACS of value change events on that parameter.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a parameter path (complete or partial) in the DUT's supported data model that is current set for either active or passive notification.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.73 SetParameterAttributes – Incorrect Parameter Name

Purpose:

This test is designed to verify that the CPE can successfully process SetParameterAttributes request from the ACS on an incorrect Parameter Name.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.4/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, when the CPE receives a SetParameterAttributes request from the ACS on a an incorrect Parameter Name, If the fault is caused by an invalid parameter name, the Invalid Parameter Name fault code (9005) MUST be used instead of the more general Invalid Arguments fault code (9003).

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a parameter from the DUT's supported data that is capable of being set to Active Notification.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.74 AddObject

Purpose:

This test is designed to verify that the CPE is capable of creating an instance of a multi-instance object. Note that for other CPE devices, although CWMP requires the ability to add objects, the creatable objects may not be widespread in implementation. If this is the case, those CPE devices should skip this test.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.6/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if an ACS uses AddObject RPC to create a new instance of a multi-instance object in the DUT, the DUT should honor the request, perform necessary action, create a new instance, and report back to ACS with the instanceNumber of the newly created object. The AddObject method call from the ACS takes as an argument the path name of the collection of objects for which a new instance is to be created. For example:

Top.Group.Object.

This path name does not include an instance number for the object to be created. The instance number is assigned by the CPE and returned in the response.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a multi-instance, writable object within the DUT's supported data model.
3. Configure the CWMP Analyzer to set the ParameterKey to a unique value in the AddObject RPC.
4. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.75 AddObject – Error Conditions

Purpose:

This test is designed to verify that the CPE is capable handling incorrect AddObject methods.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.6/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, addition of an object MUST be done atomically. That is, either all of the Parameters and sub-objects are added together, or none are added. In the latter case the CPE MUST return a fault response indicating the reason for the failure to add the object. The CPE MUST NOT add any contained Parameters or sub-objects as a result of this method call without adding all of them (all Parameters and sub-objects supported by that CPE).

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a multi-instance, writable object within the DUT's supported data model.
3. Configure the CWMP Analyzer to produce the following invalid AddObject parameter:
 - a. AddObject Request without a "." at the end of the Name.
4. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.76 DeleteObject

Purpose:

This test is designed to verify that the CPE is capable of removing a particular instance of an object. Note that for other CPE devices, although CWMP requires the ability to delete objects, the creatable objects may not be widespread in implementation. If this is the case, those CPE devices should skip this test.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.7/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if an ACS uses DeleteObject RPC to remove a particular instance of an object in the DUT, the DUT must honor the request, delete the particular instance of the object, and disregard the state previously associated with all Parameters (values and attributes) and sub-objects contained within this instance. The DeleteObject method call from the ACS takes as an argument the path name of the object instance including the instance number. For example:

Top.Group.Object.2.

When an object instance is deleted, the instance numbers associated with any other instances of the same collection of objects remain unchanged. Thus, the instance numbers of object instances in a collection might not be consecutive.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Add a known object to the DUT, if an object is not available.
3. Configure the CWMP Analyzer to set the ParameterKey in the DeleteObject RPC to a unique value.
4. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.77 DeleteObject – Error Conditions

Purpose:

This test is designed to verify that the CPE is capable of handling error conditions in the DeleteObject RPC.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.7/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if the fault is caused by an invalid ObjectName value, the Invalid Parameter Name fault code (9005) MUST be used instead of the more general Invalid Arguments fault code (9003). The ObjectName value MUST be considered invalid if it does not exactly match the name of a single instance of a multi-instance object currently present in the CPE's data model.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Add a known object to the DUT, if an object is not available.
3. Configure the CWMP Analyzer to send a DeleteObject RPC method without the "." at the end of the Object instance.
4. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.78 Reboot

Purpose:

This test is designed to verify that the CPE is capable of performing a reboot when instructed by the ACS.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.9/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, when an ACS instructs the CPE to perform a reboot by issuing the Reboot method call, the CPE must send a successful method response and complete the remainder of the session prior to rebooting.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.
3. Configure the CWMP Analyzer to set the CommandKey reboot argument in the Reboot RPC.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.79 Manual Reboot

Purpose:

This test is designed to verify that the CPE is capable of sending the BOOT eventcode in the first INFORM RPC after a manual reboot of the CPE.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.7.1.5/TR-069a1 or later

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-069 specification, “1 BOOT” indicates that the session was established due to the CPE being powered up or reset.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.80 Download Test – Basic Version Upgrade

Purpose:

This test is designed to verify that the CPE is capable of performing the Download RPC and apply the new software or firmware image.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.8/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, when Download method call is used by the ACS instructing the CPE to download a specified file from the designated location, the CPE must indicate successful or unsuccessful completion of the download using one of the following three means:

- A download Response with the status argument having a value of 0 (indicating success), or a fault response to the Download request (indicating failure).
- A TransferComplete RPC called later in the same session as the Download request (indicating either success or failure). In this case, the Status argument in the corresponding DownloadResponse must have a value of 1.
- A TransferComplete RPC made in a subsequent session (indicating either a success or failure). In this case, the Status argument in the corresponding DownloadResponse must have a value of 1.

Regardless of which mechanism is used, the CPE must only indicate successful completion of the download after the downloaded file has both been successfully transferred and applied. If the downloaded file is a software image, the CPE must consider the downloaded file to be successfully applied only after the new software image is actually installed and operational. If the software image replaces the overall software of the CPE (which would typically require a reboot to install and begin execution), the SoftwareVersion represented in the data model must already reflect the updated software image in the session in which the CPE makes a TransferComplete RPC on the ACS indicating successful download.

If the CPE requires a reboot to apply the downloaded file, then the only appropriate means of indicating successful completion is the third option listed above – a TransferComplete message sent in a subsequent session.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Obtain a firmware image for the DUT that, while structurally identical to the operating firmware under test, contains a different image version number.

3. Configure and provide a file server (i.e., http or ftp) that can be accessed by DUT through the network infrastructure. Authentication may or may not be configured on the file server.
4. Configure the CWMP Analyzer to set the CommandKey to a unique value in the Download RPC.
5. Copy the provided firmware image to the file server.
6. Connect all components of the test setup to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.81 Download Test – Queuing

Purpose:

This test is designed to verify that the CPE is capable of performing the Download RPC and Queuing up to a minimum of 3 separate download instances.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.8/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, if the CPE receives one or more Download or ScheduleDownload requests before performing a previously requested download, the CPE MUST queue all requested downloads and perform each of them as closely as possible to the requested time (based on the value of the DelaySeconds argument and the time of the request). Queued downloads MUST be retained across reboots of the CPE. The CPE MUST be able to queue a minimum of three file transfers (downloads and uploads). For each download performed, the CPE MUST send a distinct TransferComplete. If the CPE receives multiple Download requests with the same source URL, the CPE MUST perform each download as requested, and MUST NOT assume that the content of the file to be downloaded is the same each time.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Obtain a firmware image for the DUT that, while structurally identical to the operating firmware under test, contains a different image version number.
3. Configure and provide a file server (i.e., http or ftp) that can be accessed by DUT through the network infrastructure. Authentication may or may not be configured on the file server.
4. Copy the provided firmware image to the file server.
5. Connect all components of the test setup to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.82 Download Test – Delay

Purpose:

This test is designed to verify that the CPE is capable of performing the Download RPC with associated delay attribute.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.2.8/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, the CPE MUST perform and apply the download immediately after the time indicated by DelaySeconds, unless this is not possible for reasons outside the CPE's control, in which case the CPE MUST attempt to perform and apply the download within one hour after the time indicated by DelaySeconds. If the CPE cannot begin the download within this time window, the CPE MUST consider the download to have failed and report this failure to the ACS using the TransferComplete method.

The ACS MAY set the FileSize value to zero. The CPE MUST interpret a zero value to mean that the ACS has provided no information about the file size. In this case, the CPE MUST attempt to proceed with the download under the presumption that sufficient space is available, though during the course of download, the CPE might determine otherwise.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Obtain a firmware image for the DUT that, while structurally identical to the operating firmware under test, contains a different image version number.
3. Configure and provide a file server (i.e., http or ftp) that can be accessed by DUT through the network infrastructure. Authentication may or may not be configured on the file server.
4. Copy the provided firmware image to the file server.
5. Configure CWMP Analyzer to set the download FileSize to be zero.
6. Configure the CWMP Analyzer to set the DelaySeconds to one minute.
7. Connect all components of the test setup to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.83 Download Test – Retry

Purpose:

This test is designed to verify that the CPE is capable of resending the TransferComplete request after a download has occurred and the ACS has not responded to the first TransferComplete request.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Sections 3.2.1.1, 3.7.1.5/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, the URL Download argument MUST NOT include the “userinfo” component, as defined in RFC 3986. If the CPE rejects the Download request because the FileSize argument exceeds the available space on the device, it MUST use the Download Failure (9010) fault code.

If the CPE detects the presence of the “userinfo” component in the file destination URL, it SHOULD reject the Upload request with the fault code 9003 (Invalid arguments).

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Obtain a firmware image for the DUT that, while structurally identical to the operating firmware under test, contains a different image version number.
3. Configure and provide a file server (i.e., http or ftp) that can be accessed by DUT through the network infrastructure. Authentication may or may not be configured on the file server.
4. Copy the provided firmware image to the file server.
5. Connect all components of the test setup to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.84 CancelTransfer

Purpose:

This test is designed to verify that the DUT correctly performs Cancel Transfer via the CancelTransfer RPC method.

Optional Functionality Tag:

Conditionally Mandatory - Optional RPC - CancelTransfer

References:

Section A.4.1.9/TR-069a3 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, this method MAY be used by the ACS to cause the CPE to cancel a file transfer initiated by an earlier Download, ScheduleDownload or Upload method call. The TransferComplete method is not called for a file transfer that has successfully been canceled.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer
2. Configure the CWMP Analyzer to send a download request to start a Firmware image upgrade. Have the firmware image available on an accessible file server that is reachable by the DUT.
3. Connect the DUT, DHCP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.85 Upload

Purpose:

The purpose of this test is to verify DUT's upload functionality.

Optional Functionality Tag:

Conditionally Mandatory - Optional RPC – Upload

References:

Section A.4.1.5/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if an ACS issues an Upload RPC on the DUT, the DUT may choose to upload the specified file to the designated location. If the file cannot be successfully uploaded, the DUT must not attempt to retry the file upload on its own initiative, but instead must report the failure of the upload to the ACS via either the Upload response.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Install or acquire a vendor configuration or log file that is installed on the DUT.
3. Configure and provide a file server (i.e., http or ftp) that can be accessed by DUT through the network infrastructure. Authentication may or may not be configured on the file server.
4. Configure the CWMP Analyzer to set the CommandKey to a unique value in the Upload RPC.
5. Connect all components of the test setup to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.86 Upload – Queuing

Purpose:

The purpose of this test is to verify DUT's upload functionality and its ability to queue a minimum of 3 Upload File Transfers.

Optional Functionality Tag:

Conditionally Mandatory - Optional RPC - Upload

References:

Section A.4.1.5/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if the CPE receives one or more Upload requests before performing a previously requested upload, the CPE MUST queue all requested uploads and perform each of them as closely as possible to the requested time (based on the value of the DelaySeconds argument and the time of the request). Queued uploads MUST be retained across reboots of the CPE. The CPE MUST be able to queue a minimum of three file transfers (downloads and uploads).

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Install or acquire a vendor configuration or log file that is installed on the DUT.
3. Configure and provide a file server (i.e., http or ftp) that can be accessed by DUT through the network infrastructure. Authentication may or may not be configured on the file server.
4. Connect all components of the test setup to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.87 Upload – Delay

Purpose:

The purpose of this test is to verify DUT's upload functionality with respect to the DelaySeconds parameter being set.

Optional Functionality Tag:

Conditionally Mandatory - Optional RPC - Upload

References:

Section A.4.1.5/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, the CPE MUST perform the upload immediately after the time indicated by DelaySeconds, unless this is not possible for reasons outside the CPE's control, in which case the CPE MUST attempt to perform the upload within one hour after the time indicated by DelaySeconds. If the CPE cannot begin the upload within this time window, the CPE MUST consider the upload to have failed and report this failure to the ACS using the TransferComplete method.

This URL MUST NOT include the "userinfo" component, as defined in RFC 3986. If the CPE detects the presence of the "userinfo" component in the file destination URL, it SHOULD reject the Upload request with the fault code 9003 (Invalid arguments).

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Install or acquire a vendor configuration or log file that is installed on the DUT.
3. Configure and provide a file server (i.e., http or ftp) that can be accessed by DUT through the network infrastructure. Authentication may or may not be configured on the file server.
4. Configure the CWMP Analyzer to set the Upload URL with the Upload DelaySeconds parameter with a value of 60.
5. Connect all components of the test setup to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.88 ScheduleInform Test

Purpose:

The purpose of this test is to verify that the CPE is able to schedule a one-time Inform method call when requested by the CWMP Analyzer using ScheduleInform Test.

Optional Functionality Tag:

Conditionally Mandatory - Optional RPC – ScheduleInform

References:

Section A.4.1.2/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if an ACS issues a ScheduleInform RPC, the CPE MUST schedule a one-time Inform method call sometime in the future. The time the CPE must wait before issuing an Inform message is specified as a parameter in the ScheduleInform request.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a time interval between 60 and 300 seconds for the DUT to perform the scheduled inform.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.
4. Configure the CWMP Analyzer to set the CommandKey ScheduleInform RPC.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.89 FactoryReset

Purpose:

The purpose of this test is to verify that the DUT is capable of performing factory reset procedure upon receipt of FactoryReset RPC from the ACS.

Optional Functionality Tag:

Conditionally Mandatory - Optional RPC - FactoryReset

References:

Section A.4.1.6/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if an ACS issues a FactoryReset RPC to the DUT, the DUT can choose to perform factory reset. The DUT must initiate the FactoryReset procedure only after successful completion of the session.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.90 CWMP Faults – Basic RPC Faults

Purpose:

The purpose of this test is to verify that the DUT is capable of rejecting RPCs that it does not support.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.5.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

Section A.5.1 of Broadband Forum TR-069 specification, specifies the CWMP Fault codes that can be returned by the CPE in a variety of circumstances. These faults, listed in Table 65 of [1], consist of a fault code which must be used as the value of the SOAP fault code element, as well as arguments that may be required as part of the fault's functionality. Different fault codes are allowed or required for each of the RPCs described in CWMP.

This test exercises the basic fault, "9000 – Method not supported".

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a valid RPC that is not listed as supported by the DUT.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.91 CWMP Faults – Download Failure

Purpose:

The purpose of this test is to verify that the DUT is capable of notifying the ACS of a failed Download RPC and TransferComplete RPC.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.5.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

Section A.5.1 of Broadband Forum TR-069 specification, specifies the CWMP Fault codes that can be returned by the CPE in a variety of circumstances. These faults, listed in Table 65 of [1], consist of a fault code which must be used as the value of the SOAP fault code element, as well as arguments that may be required as part of the fault's functionality. Different fault codes are allowed or required for each of the RPCs described in CWMP.

This test exercises the faults that arise from a failed file transfer using the Upload and Download RPCs. The CPE attempts the transfer after the ACS makes an Upload or Download RPC on it, and makes the TransferComplete RPC on the ACS when the file transfer is completed or when an error occurs. The TransferComplete RPC contains a FaultStruct which includes any faults associated with the transfer. This test exercises faults 9010 through 9013, though the CPE may also include more detailed error codes for transfer errors (9014-9019).

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
1. Install or acquire a vendor configuration or log file that is installed on the DUT.
2. Configure and provide a file server (i.e., http or ftp) that can be accessed by DUT through the network infrastructure. Configure the file server both for unauthenticated and authenticated transfers.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.92 CWMP Faults – Upload Failure

Purpose:

The purpose of this test is to verify that the DUT is capable of notifying the ACS of a failed Upload RPC, TransferComplete RPC.

Optional Functionality Tag:

Conditionally Mandatory - Optional RPC - Upload

References:

Section A.5.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

Section A.5.1 of Broadband Forum TR-069 specification, specifies the CWMP Fault codes that can be returned by the CPE in a variety of circumstances. These faults, listed in Table 65 of [1], consist of a fault code which must be used as the value of the SOAP fault code element, as well as arguments that may be required as part of the fault's functionality. Different fault codes are allowed or required for each of the RPCs described in CWMP.

This test exercises the faults that arise from a failed file transfer using the Upload and Download RPCs. The CPE attempts the transfer after the ACS makes an Upload or Download RPC on it, and makes the TransferComplete RPC on the ACS when the file transfer is completed or when an error occurs. The TransferComplete RPC contains a FaultStruct which includes any faults associated with the transfer. This test exercises faults 9010 through 9013, though the CPE may also include more detailed error codes for transfer errors (9014-9019).

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Install or acquire a vendor configuration or log file that is installed on the DUT.
3. Configure and provide a file server (i.e., http or ftp) that can be accessed by DUT through the network infrastructure. Configure the file server both for unauthenticated and authenticated transfers.
4. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.93 Run Diagnostics

Purpose:

This test is designed to verify that the DUT correctly runs an IP Ping diagnostics Test (defined in Broadband Forum TR-098) and sends back the correct “8 DIAGNOSTICS COMPLETE” Inform event code.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.7.1.5/TR-069a1 or later

Broadband Forum TR-098

IETF RFC 792

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-098 specification, defines an object and set of parameters for performing a simple diagnostics test utilizing the ICMP [4] based “ping” application. The test is initiated by the ACS using a SetParameterValues remote procedure call that changes the value of the DiagnosticsState parameter in the IPPingDiagnostics object to a value of “Requested”. The CPE then performs the diagnostic test; generally after the CWMP session terminates successfully.

This test uses the following values for the write-enabled parameters in the IPPingDiagnostics object:

1. Host: set to the IP address of the CWMP Analyzer
2. NumberofRepetitions: 10
3. Timeout: 1000
4. DataBlockSize: 64
5. DSCP: 0

Upon conclusion of the test, the CPE initiates a CWMP session with an event code of “8 DIAGNOSTICS COMPLETE” in the Inform arguments.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer
2. Configure the CWMP Analyzer to correct Ping parameters for test
3. Connect the DUT, DHCP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.94 GetAllQueuedTranfers

Purpose:

The purpose of this test is to verify DUT's GetAllQueuedTransfers functionality.

Optional Functionality Tag:

Conditionally Mandatory - Optional RPC - GetAllQueuedTransfers

References:

Section A.4.1.7/TR-069a2 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, this method MAY be used by an ACS to determine the status of all queued downloads and uploads, including any that were not specifically requested by the ACS, i.e. autonomous transfers.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the DUT to have 2 distinct Download and Upload function queued for activity.
Use the DelaySeconds parameter to time the events.
3. Connect all components of the test setup to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.95 XML Namespace Prefix Validation

Purpose:

This test is designed to verify that the CPE doesn't require specific XML Namespace Prefixes.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.5/TR-069a1 or later

Namespaces in XML 1.0 [<http://www.w3.org/TR/REC-xml-names/>]

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, "Note – in the above examples, the XML namespace prefixes used are only examples. The actual namespace prefix values are arbitrary, and are used only to refer to a namespace declaration"

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP analyzer.
2. Configure the CWMP analyzer to use random (yet valid) namespace prefixes for SOAP and CWMP.
3. Connect the DUT and CWMP analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.96 DUT receives chunked transfer encoding

Purpose:

This test is designed to verify that the DUT can properly receive TR-69 messages sent by an ACS using HTTP 1.1 chunked transfer-encoding.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4/TR-069a1 or later
RFC 2616 section 3.6.1

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, the DUT must use HTTP 1.1. HTTP 1.1 allows the use of chunked Transfer-Encoding in both requests and responses. The Transfer-Encoding used by the ACS and the DUT do not need to match.

This test sends the InformResponse as a single chunk, and a GetParameterValuesRequest in multiple chunks.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.97 DUT properly encodes and decodes XML entities

Purpose:

This test is designed to verify that the DUT can properly send and receive data values that must be represented as XML entities such as '<', '&' and '>'.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.5/TR-069a1 or later

[1] Simple Object Access Protocol (SOAP) 1.1

[2] XML <http://www.w3.org/TR/REC-xml> section 2.4 and section 4.1

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, SOAP 1.1 is required, which is based on the XML specification. Section 2.4 of [2] states that character data MUST NOT include a literal '<' or '&'. A CDATA section must not include ']]>' unless it is the end of the CDATA section. If the CDATA section needs to include ']]>' the '>' must be escaped. This test identifies parameters that could contain these problematic characters and tests the behavior of the device when they do contain these characters. If a value is set on the device containing the problematic characters with SetParameterValues and then read back with GetParameterValues, it is possible that the device stored the escaped data. The test should independently verify the data value on the device to ensure that the device decoded the XML entity.

For example: Setting the SSID via the ACS to "foo<&]]>bar" will result in the SOAP XML containing a data value encoded as "foo<&]]>bar". The DUT should be checked to ensure that that the SSID is "foo<&]]>bar", not "foo<&]]>bar". Reading the SSID should result in a data value encoded in the SOAP XML as "foo<&]]>bar". Other writeable strings in the data model that could be used include username, password and PersistentData.

Section 4.1 of [2] states the DUT MUST be able to decode numerically escaped data such as "A" as hexadecimal and "A" as a decimal. Both represent the 'A' character.

If the DUT supports DeviceInfo.DeviceLog, the test should retrieve that parameter as it can be a source of problematic characters.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.98 Inform on IP address change

Purpose:

This test is designed to verify that the DUT sends an Inform when the IP address assigned to the DUT changes.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 2.3.3/TR-069a1 or later

Section 2.4.1/TR-098 or later

Section 3.5/TR-106a3 or earlier

Inform and Notification Requirements/TR-181 XML

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-098 specification, ConnectionRequestURL and ExternalIPAddress are required to be sent on every Inform. According to the Broadband Forum TR-181 specification, the ConnectionRequestURL parameter is required to be sent in every Inform. From TR-69 section 3.2.1, or section 2.3.3 in amendment 1 and newer, If the IP address changes, an Inform should be sent with Inform parameters reflecting the new IP address.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.99 No Inform on reconnect with no IP address change

Purpose:

This test is designed to verify that the DUT does NOT send an Inform when the IP address assigned to the DUT remains the same on reconnect.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4/TR-069a1 or later

Broadband Forum TR-098 section 2.4.1

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-098 section 2.4.1, ConnectionRequestURL and ExternalIPAddress are required to be sent on every Inform. From TR-69 section 3.2.1, or section 2.3.3 in amendment 1 and newer, If the IP address changes, an Inform should be sent with Inform parameters reflecting the new IP address. There is no need to send an Inform if there are no events to deliver upon reconnection.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.
3. Configure the DUT to disable periodic informs.
4. Configure the DUT to set Active Notifications to 0 for ConnectionRequestURL and ExternalIPAddress

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.100 EnableCWMP set to false

Purpose:

This test is designed to verify that the DUT no longer sends Informs after EnableCWMP is set to false.

Optional Functionality Tag:

Conditionally Mandatory - Optional Parameter - EnableCWMP

References:

TR-069a1 or later

TR-098a2 or later

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-098 specification, setting EnableCWMP to false means that CWMP support in the CPE is disabled, in which case the device MUST NOT send any Inform messages to the ACS or accept any Connection Request Notifications from the ACS. From TR-69 section A.2.1 the values “0” and “false” are considered interchangeable, where both equivalently represent the logical value false.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.101 Change ACS Username and password

Purpose:

This test is designed to verify that the ACS can change the username and password used to contact the ACS.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

TR-069a1 or later

TR-098a2 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-098 specification, the ACS can change the username and password used to contact the ACS.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.102 PeriodInformEnable enables periodic Informs

Purpose:

This test is designed to verify that the CPE does not send periodic Informs if PeriodicInformEnable is false.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

TR-069a1 or later

TR-098a2 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-098 specification, setting PeriodicInformEnable to 0 (false) will prevent the ACS from sending periodic Informs to the ACS. Setting PeriodicInformEnable to 1 (true) will allow the ACS to send periodic Informs to the ACS

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.103 PeriodicInformTime in The Past Controls Periodic Inform

Purpose:

This test is designed to verify that the CPE properly offsets periodic Informs based on PeriodicInformTime.

Optional Functionality Tag:

Conditionally Mandatory – Absolute Time

References:

TR-069a1 or later

TR-098a2 or later

TR-181i2 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-098 specification, periodic Informs must occur at integer multiples of PeriodicInformInterval either before or after PeriodicInformTime. This test sets PeriodicInformInterval to 2 minutes and sets PeriodicInformTime in UTC to 6 minutes behind the current time of the CPE. The CPE should issue at least one Periodic Inform within three minutes.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.104 PeriodicInformTime in the future controls periodic Inform

Purpose:

This test is designed to verify that the CPE properly offsets periodic Informs based on PeriodicInformTime.

Optional Functionality Tag:

Conditionally Mandatory – Absolute Time

References:

TR-069a1 or later

TR-098a2 or later

TR-181i2 or later

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-098 specification, periodic Informs must occur at integer multiples of PeriodicInformInterval either before or after PeriodicInformTime. This test sets PeriodicInformInterval to 2 minutes and sets PeriodicInformTime in UTC to 6 minutes ahead of the current time of the CPE. The CPE should issue at least one Periodic Inform within three minutes.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.105 DefaultActiveNotificationThrottle Throttles Active Notifications

Purpose:

This test is designed to verify that the CPE delays sending an active notification within the defined time window after the previous Inform.

Optional Functionality Tag:

Conditionally Mandatory - Optional Parameter - NotificationThrottle

References:

TR-069a1 or later

TR-098a2 or later

Test Execution Type:

Manual

Normative Description:

According to Broadband Forum TR-098 specification, the CPE MUST wait at least a specified number of seconds before initiating a session for the purpose of delivering an active notification event.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.106 Inform Parameters Should Match DeviceInfo

Purpose:

The parameter values included in the Inform should match the values returned by GetParameterValues, specifically the values in the DeviceInfo subtree.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section A.3.3.1/TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, a CPE MUST call the Inform method to initiate a transaction sequence whenever a session with an ACS is established. The calling arguments for this method are defined in Table 34.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.107 Device Times Out If ACS Is Slow

Purpose:

The purpose of this test is to verify that when the CPE does not receive an HTTP response from the ACS within a 30 second time period, it does not consider the session with an ACS to be unsuccessfully terminated until the 30 seconds have elapsed.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.7.1.4 /TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, the CPE MUST also consider a session unsuccessfully terminated if it has received no HTTP response from an ACS for a locally determined time period of not less than 30 seconds. If the CPE fails to receive an HTTP response, the CPE MUST NOT attempt to retransmit the corresponding HTTP request as part of the same session.

According to the Broadband Forum TR-069 specification, if the CPE for any reason fails to establish a TCP connection, fails to send an HTTP message, or fails to receive an HTTP response, the CPE MUST consider the session unsuccessfully terminated. The CPE MUST wait a minimum of 30 seconds before declaring a failure to establish a TCP connection, or failure to receive an HTTP response.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the CWMP Analyzer to not respond with an HTTP Response Inform Response.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.108 Use of Certificates in The Absence of Network Time

Purpose:

This test is designed to verify that the CPE can still make use of Certificate Authentication when unable to resolve time over the network

Optional Functionality Tag:

Conditionally Mandatory - Secure CWMP Session

References:

Section 3.3 /TR-069a1 or later

Test Execution Type:

Automated

Normative Description:

According to the Broadband Forum TR-069 specification, a CPE SHOULD wait until it has accurate absolute time before contacting the ACS. If a CPE chooses to contact the ACS before it has accurate absolute time (or if it does not support absolute time), it MUST ignore those components of the ACS certificate that involve absolute time, e.g. not-valid-before and not-valid-after certificate restrictions.

Note:

If the CPE does not support obtaining time over the network but obtains absolute time in another fashion (e.g. OLT, Satellite), this test case may be omitted.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Generate a certificate for the ACS URL that expired in 1969.
3. Generate and install on the DUT a valid certificate for use in authentication with the CWMP Analyzer.
4. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.109 DUT receives content-length encoding

Purpose:

This test is designed to verify that the DUT can properly receive TR-69 messages sent by an ACS using HTTP 1.1 using content-length.

Optional Functionality Tag:

Mandatory - Baseline Protocol

References:

Section 3.4 /TR-069a1 or later
RFC 2616 section 14.13

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, the DUT must use HTTP 1.1. HTTP 1.1 allows the use of content-length in both requests and responses. The Transfer-Encoding used by the ACS and the DUT do not need to match.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.110 Boolean Parameter Configuration

Purpose:

This test is designed to verify that a CPE can handle a Boolean parameter being set correctly.

Optional Functionality Tag:

Mandatory

References:

TR-069a1, Table 9 – Data Types and beyond

Test Execution Type:

Automated

Normative Description:

Table 9 : Boolean, where the allowed values are “0”, “1”, “true”, and “false”. The values “1” and “true” are considered interchangeable, where both equivalently represent the logical value true. Similarly, the values “0” and “false” are considered interchangeable, where both equivalently represent the logical value false.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Choose a valid parameter of type Boolean that is writable (PeriodicInformEnable) and verify it is set to “false”.
3. Connect the DUT and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.111 Establish Secured Connection to XMPP Server

Purpose:

This test is designed to verify that the DUT can establish a secure and authenticated connection with an XMPP Server.

Optional Functionality Tag:

Conditionally Mandatory – XMPP Connection Request

References:

Section K.2, K.2.1.1/TR-069a5 or later
RFC 6120

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, the CPE MUST be able to establish a secure and authenticated connection to an XMPP Server.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the DUT to have an XMPP.Connection object.
3. Configure the DUT's ManagementServer object to reference the XMPP.Connection object configured in step 2.
4. Connect the DUT, XMPP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.112 Maintain Connection to XMPP Server

Purpose:

This test is designed to verify that the DUT can maintain a secure and authenticated connection with an XMPP.

Optional Functionality Tag:

Conditionally Mandatory – XMPP Connection Request

References:

Section K.2.1/TR-069a5 or later

Section 4.6.1/RFC 6120

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, the CPE MUST maintain the TCP connection to the XMPP Server by utilizing the “whitespace keepalive” mechanism as defined in Section 4.6.1/RFC 6120 [37] and further described in Appendix III.5.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the DUT to have an XMPP.Connection object.
3. Configure the DUT’s ManagementServer object to reference the XMPP.Connection object configured in step 2.
4. Connect the DUT, XMPP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.113 SRV Lookup of XMPP Server

Purpose:

This test is designed to verify that the DUT can properly use the DNS SRV lookup mechanism to resolve the IP address and port number to be used to connect to the XMPP server.

Optional Functionality Tag:

Conditionally Mandatory – XMPP Connection Request

References:

Section K.2.1/TR-069a5 or later

Section 3.2.1/RFC 6120

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, the CPE MUST determine the public IP address of the XMPP Server using the rules defined in Section 3.2/RFC 6120 [37] and the recommendations described in Appendix III.4.1.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the DUT to have an XMPP.Connection object containing an XMPP server URI that uses a FQDN instead of an IP address.
3. Configure the DUT's ManagementServer object to reference the XMPP.Connection object configured in step 2.
4. Configure the DNS server to return a single FQDN and port for the requested XMPP server SRV record.
5. Connect the DUT, DNS Server, XMPP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.114 Processing of Weighted SRV Entries for XMPP Servers

Note:

This test case was removed.

5.115 Re-establish Connection to XMPP Server

Purpose:

This test is designed to verify that the DUT can reestablish the connection with the XMPP server in the event of a connection failure.

Optional Functionality Tag:

Conditionally Mandatory – XMPP Connection Request

References:

Section K.2.1/TR-069a5 or later
RFC 6120

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, if the connection to the XMPP Server is ever lost, the CPE MUST reestablish the connection as defined in Section 3.3/RFC 6120 [37] and further described in Appendix III.4.5.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the DUT to have an XMPP.Connection object.
3. Configure the DUT's ManagementServer object to reference the XMPP.Connection object configured in step 2.
4. Connect the DUT, XMPP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.116 Establish XMPP Connection before CWMP Session

Purpose:

This test is designed to verify that the DUT establishes a connection with the XMPP Server before initiating the CWMP Session.

Optional Functionality Tag:

Conditionally Mandatory – XMPP Connection Request

References:

Section K.2.1/TR-069a5 or later
RFC 6120

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, the CPE MUST establish the Connection Request XMPP connection before establishing the CWMP Session where the “1 BOOT” or “13 WAKEUP” event codes are to be delivered. In the event of a change to the ConnReqJabberID Parameter, this will allow the CPE to deliver the applicable “4 VALUE CHANGE” event code along with the “1 BOOT” or “13 WAKEUP” event code and remove the need for the CPE to immediately establish another CWMP Session for the delivery of said value change event code.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the DUT to have an XMPP.Connection object.
3. Configure the DUT’s ManagementServer object to reference the XMPP.Connection object configured in step 2.
4. Connect the DUT, XMPP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.117 Successful XMPP Connection Request

Purpose:

This test is designed to verify that the DUT can listen for and properly act upon XMPP Connection Request messages.

Optional Functionality Tag:

Conditionally Mandatory – XMPP Connection Request

References:

Section K.2.1.3/TR-069a5 or later
RFC 6120

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CPE conforming to this Annex MUST listen for XMPP Connection Request messages sent from an allowed list of Jabber IDs and generated by the XMPP Server specified by the XMPP.Connection instance referenced within the ManagementServer.ConnReq- XMPPConnection Parameter.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the DUT to have an XMPP.Connection object.
3. Configure the DUT's ManagementServer object to reference the XMPP.Connection object configured in step 2.
4. Connect the DUT, XMPP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.118 Invalid XMPP Connection Request

Purpose:

This test is designed to verify that the DUT properly handles receiving an XMPP Connection Request that is not validated against the cwmp-xmppConnReq-1-0.xsd schema.

Optional Functionality Tag:

Conditionally Mandatory – XMPP Connection Request

References:

Section K.2.1.3/TR-069a5 or later
RFC 6120

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, the XMPP Connection Request message MUST be well-formed XML and validated against the cwmp-xmppConnReq-1-0.xsd (<http://www.broadband-forum.org/cwmp/cwmp-xmppConnReq-1-0.xsd>).

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the DUT to have an XMPP.Connection object.
3. Configure the DUT's ManagementServer object to reference the XMPP.Connection object configured in step 2.
4. Connect the DUT, XMPP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.119 ConnReqAllowedJabberIDs Parameter Matches

Purpose:

This test is designed to verify that the DUT can listen for and properly act upon XMPP Connection Request messages based on the ManagementServer.ConnReqAllowedJabberIDs Parameter.

Optional Functionality Tag:

Conditionally Mandatory – XMPP Connection Request

References:

Section K.2.1.3/TR-069a5 or later
RFC 6120

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CPE conforming to this Annex MUST listen for XMPP Connection Request messages sent from an allowed list of Jabber IDs and generated by the XMPP Server specified by the XMPP.Connection instance referenced within the ManagementServer.ConnReq- XMPPConnection Parameter.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the DUT to have an XMPP.Connection object.
3. Configure the DUT's ManagementServer object to reference the XMPP.Connection object configured in step 2.
4. Configure the DUT's ManagementServer.ConnReqAllowedJabberIDs Parameter to contain a single value that matches the Jabber ID of the ACS server.
5. Connect the DUT, XMPP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.120 ConnReqAllowedJabberIDs Parameter Does Not Match

Purpose:

This test is designed to verify that the DUT can listen for and properly act upon XMPP Connection Request messages based on the ManagementServer.ConnReqAllowedJabberIDs Parameter.

Optional Functionality Tag:

Conditionally Mandatory – XMPP Connection Request

References:

Section K.2.1.3/TR-069a5 or later
RFC 6120

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, a CPE conforming to this Annex MUST listen for XMPP Connection Request messages sent from an allowed list of Jabber IDs and generated by the XMPP Server specified by the XMPP.Connection instance referenced within the ManagementServer.ConnReq- XMPPConnection Parameter.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the DUT to have an XMPP.Connection object.
3. Configure the DUT's ManagementServer object to reference the XMPP.Connection object configured in step 2.
4. Configure the DUT's ManagementServer.ConnReqAllowedJabberIDs Parameter to contain a single value that does not match the Jabber ID of the ACS server.
5. Connect the DUT, XMPP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.121 ConnectionRequestUsername Parameter Does Not Match

Purpose:

This test is designed to verify that the DUT can listen for and properly act upon XMPP Connection Request messages based on the ManagementServer.ConnectionRequestUsername Parameter.

Optional Functionality Tag:

Conditionally Mandatory – XMPP Connection Request

References:

Section K.2.1.3/TR-069a5 or later
RFC 6120

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, the value of the “username” element within the “connectionRequest” element MUST match the value of the ManagementServer.ConnectionRequestUsername Parameter.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the DUT to have an XMPP.Connection object.
3. Configure the DUT’s ManagementServer object to reference the XMPP.Connection object configured in step 2.
4. Configure the DUT’s ManagementServer.ConnectionRequestUsername to a valid value.
5. Connect the DUT, XMPP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

5.122 ConnectionRequestPassword Parameter Does Not Match

Purpose:

This test is designed to verify that the DUT can listen for and properly act upon XMPP Connection Request messages based on the ManagementServer.ConnectionRequestPassword Parameter.

Optional Functionality Tag:

Conditionally Mandatory – XMPP Connection Request

References:

Section K.2.1.3/TR-069a5 or later
RFC 6120

Test Execution Type:

Automated

Normative Description:

According to Broadband Forum TR-069 specification, the value of the “password” element within the “connectionRequest” element MUST match the value of the ManagementServer.ConnectionRequestPassword Parameter.

Test Setup:

1. Configure the DUT to use the ACS URL set on the CWMP Analyzer.
2. Configure the DUT to have an XMPP.Connection object.
3. Configure the DUT’s ManagementServer object to reference the XMPP.Connection object configured in step 2.
4. Configure the DUT’s ManagementServer.ConnectionRequestPassword to a valid value.
5. Connect the DUT, XMPP server or simulator, and CWMP Analyzer to the network infrastructure.

Procedure:

See IR-069i2

Test Metrics:

See IR-069i2

Appendix I. Open Issues

See IR-069i2

Appendix II. Test Procedures Removed from this Test Plan

See IR-069i2

Appendix III. Test Certificate Generation

See IR-069i2

End of Broadband Forum Abstract Test Plan ATP-069