1. 背景・目的

Technical Report 069(TR-069)は、Broadband Forum が 2004 年 5 月に策定した技術規格であり、HTTP/SOAP プロトコル通信と XML 形式ファイル送受信により、DSL モデムなどの加入者宅内 CPE を遠隔から管理・監視する方式を定めている。

日本ケーブルラボの定める次世代 STB 技術仕様(SPEC-023)では、STB の管理・監視プロトコルとして、従来の SNMP 方式に加え、TR-069 の CWMP 方式を採用した。

CWMP は SNMP に対し、①HTTP のため原則的にはファイアウォールを通過可能　②SSL/TLS により高強度の暗号化が可能　③プロビジョニングを包含　④STUN による NAT/NAPT 越えが可能　といった利点があるが、DOCS 端末（CM, STB, MTA）とヘッドエンド間の通信はそもそも　①ファイアウォールが不要　②DOCSIS 暗号化で十分　③DHCP/TFTP によるプロビジョニング方式が既に確立・普及済　④NAT/NAPT が不要であり、SNMP から CWMP への置換は、必ずしも必須という訳ではない。

しかしながら、非 DOCSIS 網による IP-STB 収容や、IP-STB を介したタブレットやスマホ・ネット家電と外部間の通信では、インターネットやゲートウェイを通過できる CWMP の方が、SNMP よりも柔軟性が高い。

本 Tips では、TR-069 と CWMP の概要、SPEC-023 による TR-069 対応、留意事項について説明する。

2. 対象読者

OPEN STM シリーズのサーバー系プログラム開発者

3. 参考文献・関連文書

Broadband Forum TR-069 Amendment 3 (以降、「TR-069」)
Broadband Forum TR-106 Amendment 4 (以降、「TR-106」)
Broadband Forum TR-157 Amendment 3 (以降、「TR-157」)
Broadband Forum TR-135 Amendment 1 (以降、「TR-135」)
Broadband Forum TR-140 Amendment 1 (以降、「TR-140」)
Broadband Forum TR-098 Amendment 2 (以降、「TR-098」)
Broadband Forum TR-181 Issue 1 (以降、「TR-181/1」)
Broadband Forum TR-181 Issue 2 Amendment 2 (以降、「TR-181/2」)
JLabs SPEC-023 次世代 STB 技術仕様 1.2 版 (以降、「SPEC-023」)

4. その他

本 Tips 中の図表番号につき、参考文献・関連文書からの抜粋には原文の番号をそのまま流用し、独自に作成した図表には”Tips-*”の形式で番号を付与した。

5. 最終更新日

2013 年 10 月 9 日

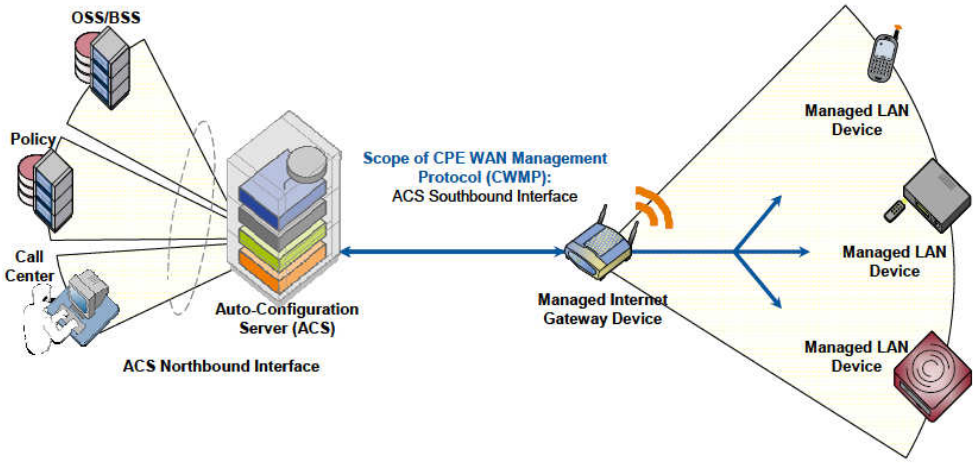
6. 詳細

6.1 TR-069 と CWMP の概要

(1) 基本アーキテクチャ

TR-069 のエンド-エンドアーキテクチャ構成を TR-069 Figure-1 に示す。

Figure 1 – Positioning in the End-to-End Architecture



TR-069 では ACS (Auto Configuration Server)が、携帯端末・STB・外付 HDD などの各 CPE (Customer Premises Equipment)と中間に配置される GW(Gateway)を管理する。
図中の青線は、TR-069 が定める CWMP (CPE WAN Management Protocol)の対応範囲を示す。
CWMP では、STUN による GW の NAT/NAPT 通過も可能である。STUN に関連する仕様の詳細は、TR-069 Annex F/G および、TR-111 を参照されたい。
TR-069 により SPEC-023 の次世代 STB を管理する場合、STB が GW 機能を供える場合には CPE+GW、ない場合には単純な CPE として取り扱われる。
ACS の上位には SMS/Billing・CRM・NMS 等の OSS/BSS、ポリシー制御、コールセンター設備などが配置される。各上位システムは、必要時に ACS の上位向け API を呼び出す。
上位向け API は TR-131 に定義され、TR-069 の対象外である。

CWMP のプロトコルスタックを Tips-001 に示す。

CPE/ACS 管理アプリケーション
RPC Methods (CWMP Annex A)
SOAP1.1
HTTP1.1
TLS1.2
TCP/IP

Tips-001 CWMP のプロトコルスタック

プロトコルバージョンは、SPEC-023 が参照する TR-069 バージョンである Amendment 3 に基づく。Amendment バージョンが変わると、対応するプロトコルのバージョンが異なる点に注意が必要である。具体的な例を挙げると、Amendment 2 以前のバージョンの TLS バージョンは 1.0 である。また、2013 年 10 月現在の TR-069 の最新バージョンは Amendment 4 であり、動作仕様が SPEC-023 と相違する。特に SPEC-023 の次世代 STB 管理に TR-069 を使う場合、Amendment 4 でなく、一世代前の Amendment 3 を参照する必要がある。本 Tips は SPEC-023 への応用を目的としているため、敢えて TR-069 Amendment 3 に同期する各 TR 規格を抽出・整理・参照している。

(2) TR-069 の機能
TR-069 の機能は、以下の 5 通りに分類される。

- 自動構成設定&動的サービスプロビジョニング
- ソフトウェア/ファームウェアイメージ管理
- ソフトウェアモジュール管理
- 状態&性能監視
- 障害診断

(3) CWMP の RPC メソッド

CWMP ではTR-069 の定義する RPC(Remote Procedure Call: 遠隔プロシージャ呼出)により、CPE または ACS のいずれかより他方を遠隔操作できる。CWMP の RPC メソッドは、概ね SNMP の各 PDU(Get/Set/Trap 等)に対応する。

CWMP がサポートする RPC メソッドの一覧を TR-069 Table-5 に示す。

Table 5 – RPC message requirements

Method name	CPE requirement	ACS requirement
CPE methods	**Responding**	**Calling**
GetRPCMethods	REQUIRED	OPTIONAL
SetParameterValues	REQUIRED	REQUIRED
GetParameterValues	REQUIRED	REQUIRED
GetParameterNames	REQUIRED	REQUIRED
SetParameterAttributes	REQUIRED	OPTIONAL
GetParameterAttributes	REQUIRED	OPTIONAL
AddObject	REQUIRED	OPTIONAL
DeleteObject	REQUIRED	OPTIONAL
Reboot	REQUIRED	OPTIONAL
Download	REQUIRED[7]	REQUIRED[7]
ScheduleDownload	OPTIONAL	OPTIONAL
Upload	OPTIONAL	OPTIONAL
FactoryReset	OPTIONAL	OPTIONAL
GetQueuedTransfers (DEPRECATED)	OPTIONAL[8]	OPTIONAL
GetAllQueuedTransfers	OPTIONAL	OPTIONAL
CancelTransfer	OPTIONAL	OPTIONAL
ScheduleInform	OPTIONAL	OPTIONAL
ChangeDUState	OPTIONAL	OPTIONAL
SetVouchers (DEPRECATED)	OPTIONAL[9]	OPTIONAL
GetOptions (DEPRECATED)	OPTIONAL[9]	OPTIONAL
ACS methods	**Calling**	**Responding**
GetRPCMethods	OPTIONAL	REQUIRED
Inform	REQUIRED	REQUIRED
TransferComplete	REQUIRED[10]	REQUIRED[11]
AutonomousTransferComplete	OPTIONAL	REQUIRED
DUStateChangeComplete	OPTIONAL[12]	OPTIONAL[13]

Method name	CPE requirement	ACS requirement
AutonomousDUStateChangeComplete	OPTIONAL	OPTIONAL
RequestDownload	OPTIONAL	OPTIONAL
Kicked (DEPRECATED)	OPTIONAL	OPTIONAL[14]

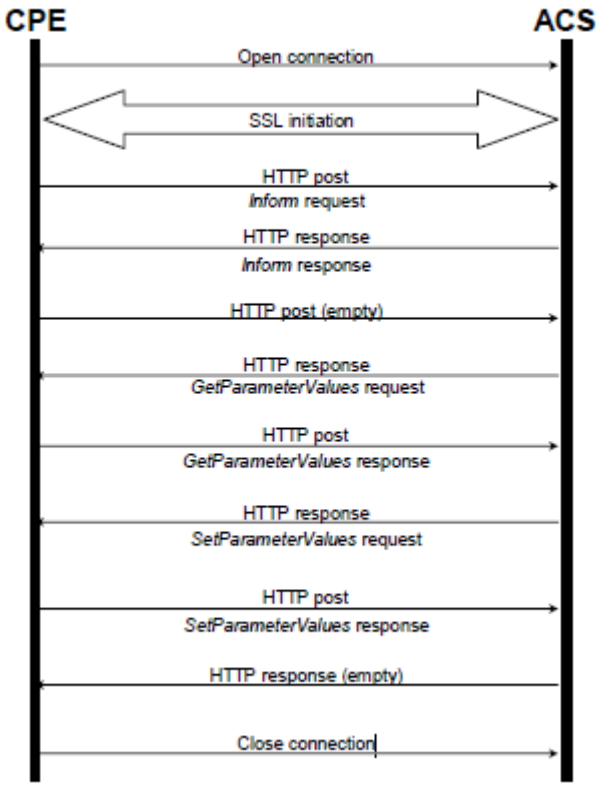
CPE メソッドは CPE の CWMP エージェントに、ACS メソッドは ACS マネージャに実装される。CPE 要件(CPE requirement)は対象メソッドに対する CPE への対応要件を、ACS 要件(ACS requirement)は ACS への対応要件を表す。

例えば CPE メソッドの”GetRPCMethods”の場合、CPE 要件は Responding=応答が”Required”すなわち必須対応、ACS 要件は Calling=呼出が”Optional”すなわち任意対応である。

(4) CPE による CWMP セッションの開始

CPE イニシエーション（CPE から ACS に通信を開始）によるトランザクションの典型例を TR-069 Figure 3 に示す。

Figure 3 – Transaction Session Example



TR-069 Figure 3 では、CPE から ACS への TCP コネクションオープンからトランザクションが開始する。TLS/SSL を使う場合、SSL イニシエーションが実行され、コネクションが開設される。

CWMP トランザクションは、CPE から ACS への HTTP POST による”Inform”送信と、ACS から CPE への HTTP POST RESPONSE による”Inform response”送信により開始される。

TR-069 Figure 3 では、具体的な操作内容が ACS による CPE への GetParameterValues と SetParameterValues の RPC 要求のため、最初に CPE から送信される HTTP POST が empty(空)すなわちダミーとなり、続く ACS からの HTTP POST RESPONSE で RPC メソッドの REQUEST が送信される点に注意が必要である。

すなわち、HTTP レベルでの REQUEST/RESPONSE と、CWMP アプリケーションレベルでの REQUEST/RESPONSE が逆転する。

CPE は ACS の HTTP RESPONSE が empty(空)となる場合、トランザクション終了を判断し、TCP コネクションをクローズする。

CPE から ACS への HTTP セッションには、全て HTTP POST が使われる。

なおセキュリティ上の要件がある場合、全ての HTTP を HTTPS に置換可能である。

(5) ACS による CWMP セッションの開始
ACS イニシエーション（ACS から CPE に通信を開始）によるトランザクションの典型例は、(6)の TR-157 Figure 4 を参照されたい。(5)との違いは、ACS から CPE へのコネクションオープンに、HTTP GET を使う点である。TR-157 Figure 4 では、ACS からの HTTP GET に対し、204(No Content)の http ステータスコードを返している。ACS が 204 または 200(OK)の HTTP GET RESPONSE を受信時、ACS と CPE 間の TCP コネクションがオープンとなり、続く CWMP トランザクションが開始される。
コネクションオープン時の GET は HTTP のみであり、HTTPS の使用は TR-069 により禁止されているが、以降の HTTP POST は全て、(4)同様に HTTPS への置換が可能である。
HTTP GET 時の認証には、HTTP ダイジェスト認証が使われる。
CWMP トランザクションは(4)同様、CPE から ACS への HTTP POST による”Inform”送信と、以降、CPE から ACS への HTTP RESPONSE が empty(空)となる場合にトランザクション終了する迄の流れは、(4)と同じである。

CPE から ACS への HTTP セッションには全て HTTP POST が使われるのに対し、ACS から CPE への HTTP セッションには HTTP GET が使われる点に注意されたい。

なお CWMP が使用する SOAP は元来、Web サービスを前提としたプロトコルであり、SOAP ではインターネット上の任意のクライアント≒CPE から特定の Web サービス≒ACS に処理を要求する仕様のため、TR-069 の定める ACS イニシエーションすなわち、ACS から特定 CPE に対して通信を開始する業務上の要件と矛盾する。この矛盾を解消するために、CWMP では empty(空) の HTTP RESPONSE を応用した HTTP レベルでの REQUEST/RESPONSE と CWMP アプリケーションレベルでの REQUEST/RESPONSE の逆転という、Web サービスの常識的な基本形から少々逸脱する特殊な工夫・拡張を行っている点に注意が必要である。
更に、CWMP のポート番号として IANA により 7547 が割り当てられているが、TR-069 では CPE の Connection Request URL に本ポートを使うか否かは MAY 規定であり、MUST までは規定されていない点にも注意が必要である。

(6) TR-069 のデータモデル

TR-069 のデータモデルは、TR-106 の定めるベースライン標準テンプレートに、各機種固有のデータモデルを表す様々な TR 規格が追加される形で構成される。

TR 規格構造の概要を TR-106 Figure 2 に示す。

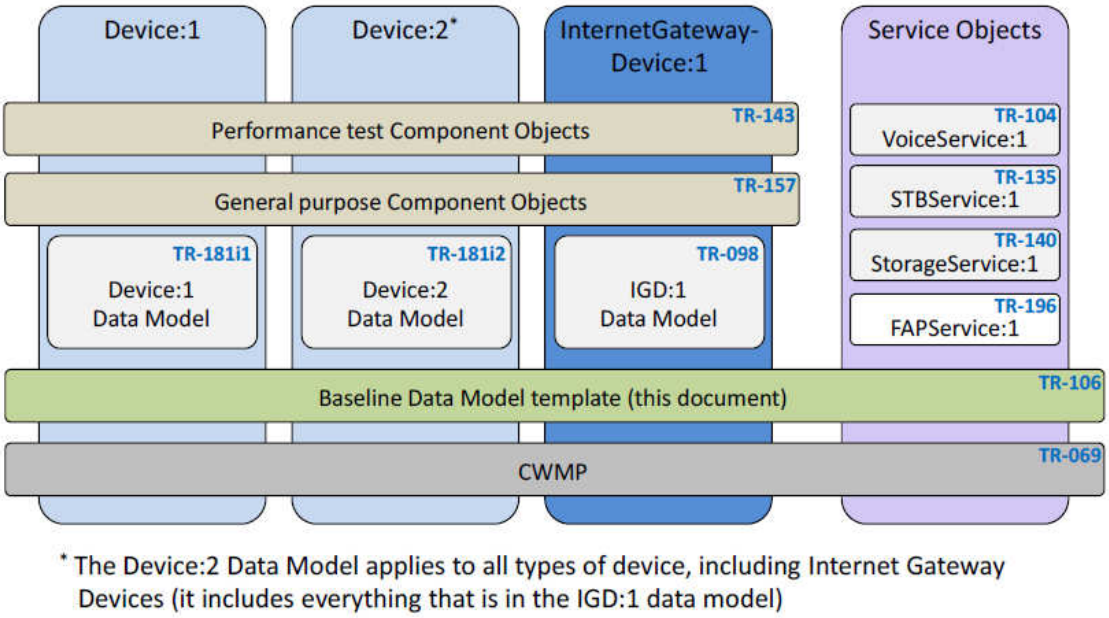


Figure 2 – Specification Structure

TR-069 は CWMP の基本仕様、TR-106 は TR-069 を実装する全機器に共通のベースラインオブジェクト構造を定義する。

TR-106 は、特定機器・サービスの状態を設定・診断・監視するための基本メソッドが操作するオブジェクト・項目の集合で構成され、全機器に対する TR-106 の遵守が義務付けられている。TR-106 には更に、適正なデータハイアラーキーを構成するための追加データモデルの構造上の要件、データモデルのバージョン管理ルール、プロファイルの定義ルールが定められている。

各項目は、SNMP の MIB 同様、オブジェクト名と”.”(ドット)の連結文字列で表現される。(例: InternetGatewayDevice.Time.NTPServer1 .)

各項目は、データ型や更新可/読出のみ等の属性情報を持つ。

各項目に使用可能なデータ型は、Object（他項目または他オブジェクトの集合）, string, int, long, unsignedInt, unsignedLong, boolean, dateTime, base64, hexBinary の 10 通りである。

CWMP 管理対象機器が複数の CPE を含む場合、例えば、複数の仮想音声端末を含む場合、各仮想端末に管理対象機器内で一意のインスタンス番号が付与され、ACS によりインスタンス別に管理される。

全機器はルート配下に共通オブジェクト（TR-181/1,TR-181/2 または TR-098）、共通コンポーネント（TR-157 および TR-143）および個別サービス（TR-135 等）の 3 構成要素を含み、TR-181/1 の表す Device:1、TR-181/2 の表す Device:2、ないしは TR-098 の表す InternetGatewayDevice のいずれかに分類され、それぞれ Device:1, Device:2, IGD の略称で表現される。
Device:1 は網末梢に配置されルーティング等のネットワーク層機能を持たないシンプルな機器を、Device:2 は Device:1 と IGD の双方を上位互換する汎用的な機器を表現する。
TR-181/2 には、機器の基本情報、ToD の設定、ネットワークインタフェースとプロトコルスタックの設定、ルーティングとブリッジングの管理、スループット指標、診断テスト、およびデータプロファイルの最小セットが定義される。TR-181/1 と TR-098 は、データモデルの定義範囲上は TR-181/2 のサブセットである。
Device:1 と Device:2 の場合、“Device”という名称のルートオブジェクト、ルート直下に“DeviceSummary”項目、“Services”オブジェクトがそれぞれ一つ含まれる。IGD の場合、ルートオブジェクトが”InternetGatewayDevice”になる。

”Services”には、対象機器がサポートする各サービスオブジェクトが含まれる。TR-106 Figure-2 の例では、サービスオブジェクトとして IP 電話サービスを表す VoiceService (TR-104)、セットトップボックスを現す STBService (TR-135)、NAS を表す StorageService (TR-140)、フェムトセルを表す FAPService (TR-196)が含まれている。

TR-181/2 のデータモデル構造を TR-181/2 Figure-1～Figure-4 に示す。

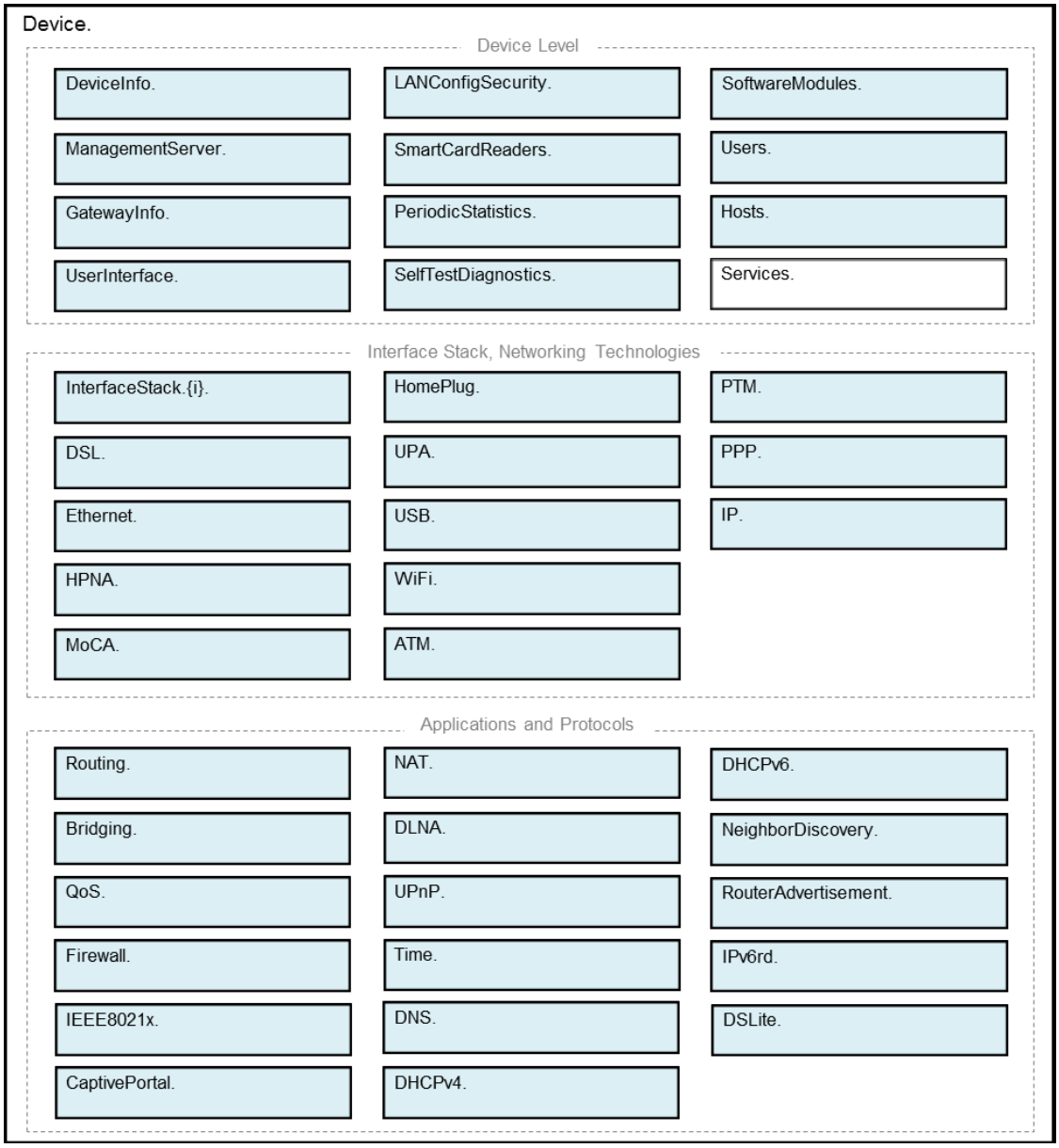


Figure 1 – Device:2 Data Model Structure – Overview

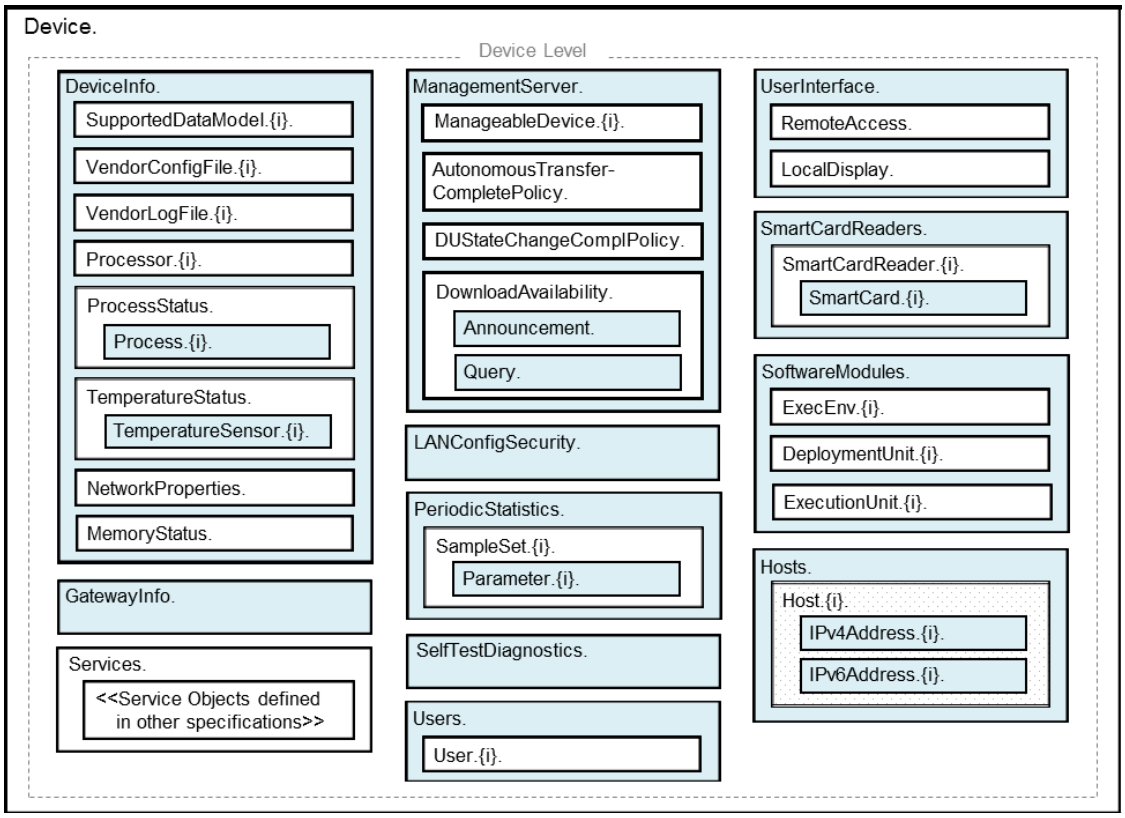


Figure 2 – Device:2 Data Model Structure – Device Level

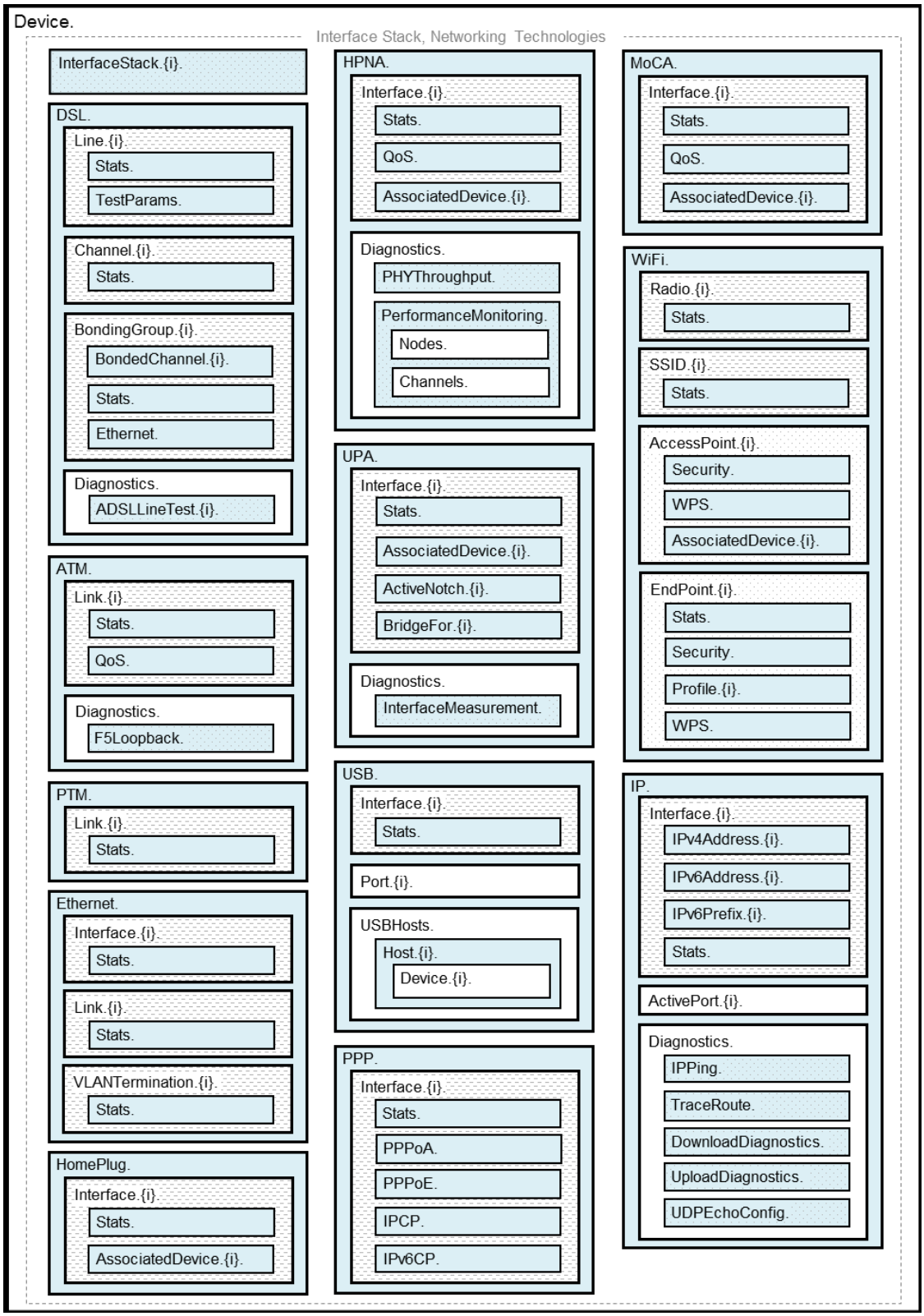


Figure 3 – Device:2 Data Model Structure – Interface Stack and Networking Technologies

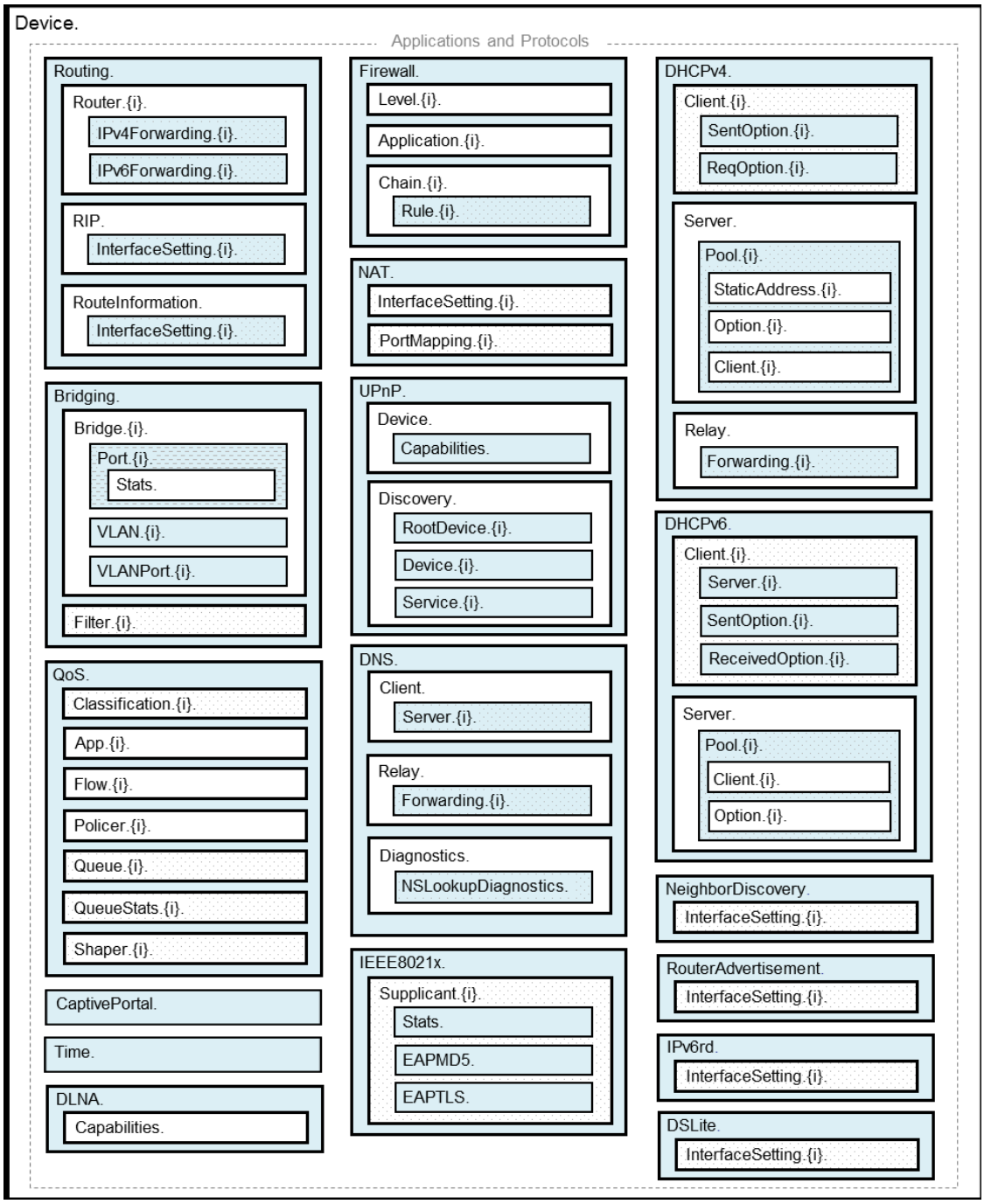


Figure 4 – Device:2 Data Model Structure – Applications and Protocols

TR-157 は、TR-181/1, TR-181/2, TR-098 の定義する Device:1, Device:2, IGD のデータモデルに基づく応用概念であり、TR-069 の管理対象機器に実装される共通データオブジェクトを定義する。
TR-157 の共通データオブジェクトサマリーを TR-157 Table 2 に示す。

Table 2 – Summary of Common Data Objects

Object Name	Allowed Location in Hierarchy	Description
Capabilities	Root and Service Objects	Device capabilities.
DeviceInfo	Root and Service Objects	General information about the device, including its identity and version information.
ManagementServer	Root	Parameters associated with the communication between the CPE and an ACS.
GatewayInfo	Root	Information to identify an Internet Gateway Device through which the CPE is connected.
Time	Root and Service Objects	Parameters associated with an NTP or SNTP time client on the CPE.
Config	Root and Service Objects	Contains general configuration state.
UserInterface	Root and Service Objects	Parameters related to the user interface of the CPE.
LAN	Root and Service Objects	Parameters related to IP-based LAN connectivity of the CPE.

本 Tips が参照する TR-157 Amendment 3 の共通データオブジェクト定義の最新バージョンは 1.7 である。バージョン 1.7 の共通オブジェクト定義は以下の URL から取得できる。

<Device:1 (DM instance: tr-157-1-3.xml)>
http://broadband-forum.org/cwmp/tr-157-1-3.xml
http://broadband-forum.org/cwmp/tr-157-1-3-dev.html
http://broadband-forum.org/cwmp/tr-157-1-3-dev-last.html

<IGD:1 (DM instance: tr-157-1-3.xml)>
http://broadband-forum.org/cwmp/tr-157-1-3.xml
http://broadband-forum.org/cwmp/tr-157-1-3-igd.html
http://broadband-forum.org/cwmp/tr-157-1-3-igd-last.html

TR-157 では更に、Device, IGD を対象としたソフトウェアモジュールの管理方法（ライフサイクル、転送方式、転送失敗時の取扱）を Appendix II に定義している。
ACS からのリクエストによる CPE の DU(Deployment Unit: デプロイメント単位)更新手順例を TR-157 Figure 4 に、CPE から ACS への更新終了通知例を TR-157 Figure 5 に示す。

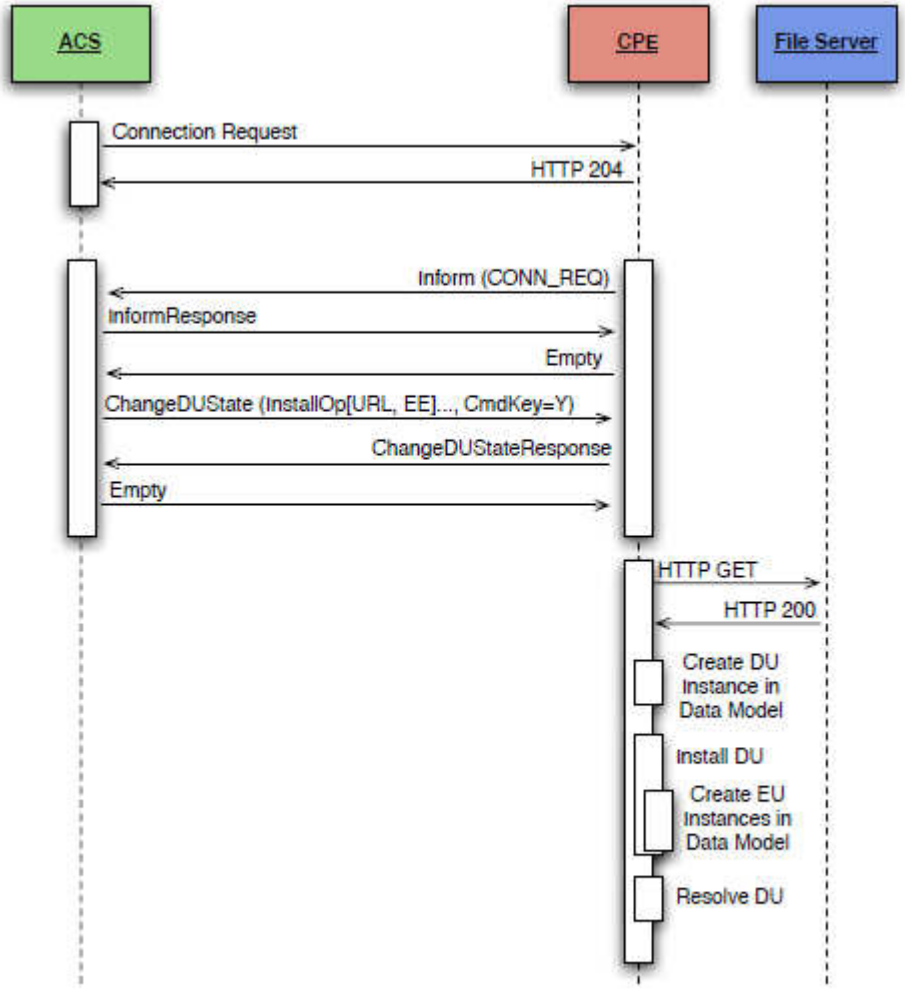


Figure 4 – Installation of a Deployment Unit - CWMP Session #1

TR-157 Figure 4 では、ACS が CPE の ChangeDUState RPC を遠隔実行している。
シーケンス中に出てくる DU、EU(Execution Unit: 実行単位)だが、Java で例えるならば、DU が jar, war, ear アーガイブ、EU がクラスファイルに近い概念である。
すなわち DU がダウンロード・デプロイされるアーガイブファイル、EU が DU にアーガイブされ、EE(Execution Environment: 実行環境)上でインスタンス化・実行される実装クラスに相当する。
なお本例では DU 取得に HTTP GET を使用しているが、TR-069 では HTTP、HTTPS、FTP、SFTP、TFTP のいずれかから任意のファイル転送プロトコルを選択できる。

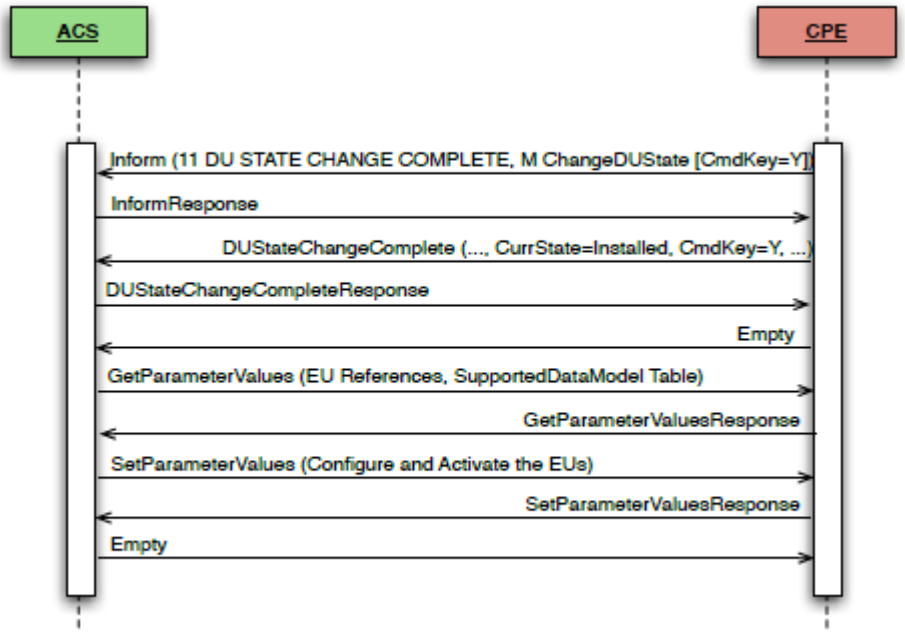


Figure 5 – Configuring and Starting the Execution Units - CWMP Session #2

TR-157 Figure 5 では、CPE が ACS の ChangeDUStateComplete を遠隔実行する形で完了を通知している。

6.2 SPEC-023 による TR-069 対応

(1) CWMP RPC メソッドへの対応

SPEC-023 では TR-069 Table-5 に示した RPC メソッド中、Required(必須)メソッドに加え、SPEC-023 表 7-3 に示す各 Optional(任意)メソッドの実装を求めている。

CPE メソッド	ACS メソッド
Upload	AutonomousTransferComplete
FactoryReset	DUStateChangeComplete
ChangeDUState	AutonomousDUStateChangeComplete
	RequestDownload

SPEC-023 表 7-3: BBF TR-069 OPTIONAL RPC メソッドへの対応

更に SPEC-023 では、CPE すなわち STB は、SPEC-023 表 7-4 に示すファイル転送への準拠を求めている。

ファイル種別	メソッド	主導	備考
Firmware Upgrade Image	Download ScheduleDownload	ACS	
Vendor Configuration File	Download ScheduleDownload	ACS	
Vendor Log File	Upload	ACS	

SPEC-023 表 7-4: BBF TR-069 におけるファイル転送の対応

ファイル転送プロトコルとしては、TR-069 のサポートする HTTP、HTTPS、FTP、SFTP、TFTP のうち、HTTP(TLS の利用も含む)および IP マルチキャスト(FLUTE)への対応を求めている。

(2) TR-069 データモデルへの対応

SPEC-023 では、CPE に以下のデータモデル定義の実装を求めている。

- Device:1 Version 1.7 (TR-157 Amendment 3)
- STB Service Version 1.1 (TR-135 Amendment 1)
- Storage Service (TR-140 Amendment 1)

TR-157 については、前節の説明を参照されたい。

TR-135 の STBService オブジェクト構造を TR-135 Figure 2 に示す。

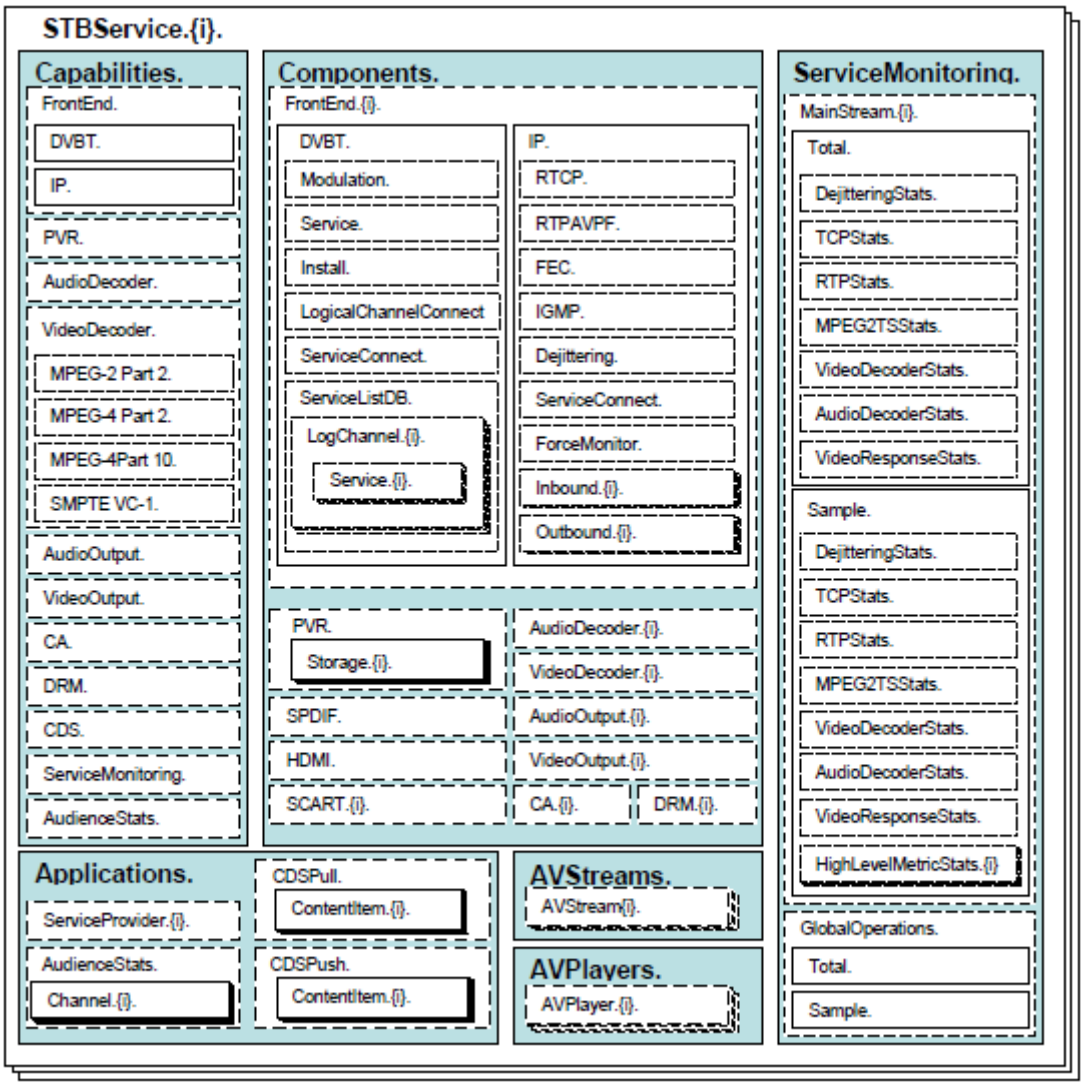


Figure 2– TR-135 – STBService object structure

TR-140 の StorageService オブジェクト構造を TR-140 Figure 1 に示す。

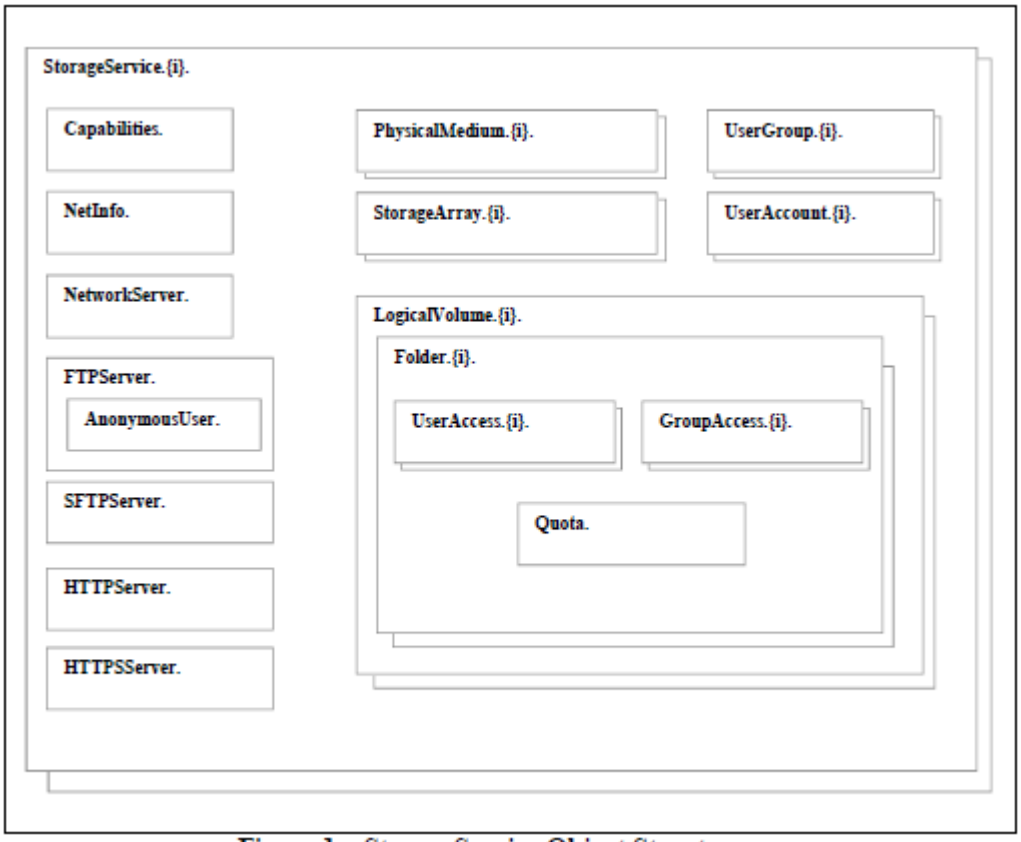


Figure 1 – StorageService Object Structure

(3) TR-069 データプロファイルへの対応

SPEC-023 では、CPE に Tips-003～005 に示すデータモデル定義の実装を求めている。
SPEC-023 が実装を求めているプロファイル中、TR-157 のプロファイルを Tips-003、TR-135 のプロファイルを Tips-004、TR-140 のプロファイルを Tips-005 に示す。
表中のバージョンは、対応するデータモデルのバージョン番号を表す。

プロファイル名	バージョン	備考
TR-157		
Baseline:1	1.0	
GatewayInfo:1	1.0	WAN-LAN gateway 有効時
Time:1	1.0	
LAN:1	1.0	
IPPing:1	1.0	
TraceRoute:1	1.0	
Download:1	1.2	
Upload:1	1.2	
MemoryStatus:1	1.3	
ProcessStatus:1	1.3	
TempStatus:1	1.3	
AutonXferComplPolicy:1	1.3	
UPnPDev:1	1.3	
UPnPDiscBasic:1	1.3	
UPnPDiscAdv:1	1.3	
SelfTestDiag:1	1.3	
NSLookupDiag:1	1.3	
SimpleFirewall:1	1.3	
USBHostsAdv:1	1.3	
PeriodicStatsBase:1	1.3	
PeriodicStatsAdv:1	1.3	
DownloadAnnounce:1	1.3	
DownloadQuery:1	1.3	
Processors:1	1.7	
VendorLogFiles:1	1.7	
DUStageChngComplPolicy:1	1.7	
SM_ExecEnvs:1	1.7	
Device.DLNA.		
Device.SmartCardReader.{i}.		

Tips-003 SPEC -023 の実装指定プロファイル一覧(TR-157)

プロファイル名	バージョン	備考
Baseline:1	1.0	
PVR:1	1.0	
DTT:1	1.0	
IPTVBaseline:1	1.0	
RTCP:1	1.0	
RTPAVPF:1	1.0	
RTPAVConfig:1	1.1	
ForceMonitoring:1	1.1	
IPTVHomeNetwork:1	1.0	
IGMP:1	1.0	
BasicPerfMon:1	1.0	
BasicPerfMon:2	1.1	
ECPerfMon:1	1.0	
VideoPerfMon:1	1.0	
AudioPerfMon:1	1.0	
DiagPerfMon:1	1.1	
AudienceStats:1	1.0	
AnalogOutput:1	1.0	
DigitalOutput:1	1.0	
DigitalOutput:2	1.1	
CA:1	1.0	
DRM:1	1.0	
CDS:1	1.1	

Tips-004 SPEC -023 の実装指定プロファイル一覧(TR-135)

プロファイル名	バージョン	備考
Baseline:1	1.0	
Baseline:2	1.1	
VolumeConfig:1	1.0	
UserAccess:1	1.0	
UserAccess:2	1.1	
GroupAccess:1	1.0	
GroupAccess:2	1.1	

Tips-005 SPEC -023 の実装指定プロファイル一覧(TR-140)

(4) プロビジョニング

ACS との通信に先立ち、CPE による ACS の発見が必要となる。

SPEC-023 は、TR-069 の ACS 自動発見を適用する。自動発見の優先順位は以下の通りである。

1. DHCP option 43 による自動設定(DHCP option 60 の”dslforum.org”の認識が必要)
2. STB プリセット URL
3. デフォルト URL(事業者による初期設定値)

(5) コネクション・認証

SPEC-023 では、CPE イニシエーションと ACS イニシエーションの双方への対応を求めている。ACS イニシエーションの場合、TE-069 では HTTP ダイジェスト認証によって CPE が ACS を認証するが、SPEC-023 では、認証に必要な ID、パスワードは、事業者側で設定された値を STB の出荷時、ないしはサービス開始時に STB に設定する前提である。

CPE による ACS 認証としては、SPEC-023 では TR-069 の定める Basic 認証、Digest 認証、証明書(TLS)の全方式への対応を求めている。特に証明書(TLS)方式については、SPEC-023 では TR-069 がオプション扱いとしているクライアント証明書による CPE 認証への対応を求めている。

受信機 ID が STB 本体に貼り付けられず事業者のみ参照可能である場合、SPEC-023 では JCL SPEC-001 5.3.9 記載の受信機 ID(6 バイト)をパスワードとして設定できる。ユーザーID については TR-069 3.4.4 記載の通り、<OUI>-<ProductClass>-<SerialNumber>とする。SerialNumber は、本受信機 ID とは異なるユニーク ID とし、JLabs で管理する。

なおコネクション開設後のメッセージ送受信には、TR-069 では共通秘密鍵認証および TLS 認証のいずれかの使用が求められているが、SPEC-023 では TLS1.2 を常に使用する。

(6) ファームウェア管理

SPEC-023 では、BS-TM 方式(JCL SPEC-001)によるエンジニアリング TS を用いたダウンロード方式に加え、TR-069 によるダウンロード制御（IP 経由または TS 警手、スキーム指定により区別）のサポートを求めている。

更新されたファームウェアは、利用者による CPE の再起動後に反映される。

再起動が必要となった場合、利用者に CPE の再起動を促すために、例えば「今すぐ再起動を行う」「一定時間再起動を保留する」などの選択等、適切な画面表示を行う。

ファームウェアダウンロードの開始は、以下の方式への対応を求めている。

- ACS からのダウンロード即時要求
- ACS からの遅延付きダウンロード指示
- ACS からのスケジュールドダウンロード指示

(7) ソフトウェアモジュール管理

ソフトウェアパッケージ(DU)の状態取得及び管理は、TR-157 の Device.SoftwareModules.DeploymentUnit.{i}.を利用し、実行モジュール(EU)の状態取得及び管理は、同 TR-157 の Device.SoftwareModules.ExecutionUnit.{i}.を利用する。

ソフトウェアパッケージの変更（インストール・アップデート・アンインストール）については、TR-157 の Appendix II に記載の方法に従う。

(8) 状態&性能監視

SPEC-023 では、従来方式である SNMP と新方式である TR-069 の並存を求めている。
DOCSIS 内蔵 STB の場合、HFC は事業者のプライベート網であり SNMP で運用可能であり、かつ SNMP による状態監視システムが既に存在するケースが殆どのため、状態&性能監視については、今後も引き続き SNMP が主流になると思われる。

(9) 動作ログ取得（障害診断）

SPEC-023 では、CPE の内部動作に関して、次に示す項目のログ記録と、TR-069/TR-106 による ACS からの遠隔参照を求めている。

- システムの起動およびエラーの履歴
- システムアップデートのダウンロード、適用およびエラーの履歴
- ネットワーク接続（DOCSIS, WAN, LAN）の動作およびエラーの履歴
- WAN-LAN 相互接続に係る機能の動作およびエラーの履歴
- アプリケーションのインストール、起動およびエラーの履歴
- 放送機能の動作およびエラーの履歴

(10)セキュリティ

SPEC-023 では、ソフトウェアの改ざん・特権昇格・内部情報読み取り・動作不能アタック、DoS 攻撃、外部からのコントロール権の乗っ取り、外部からの不正データ流入へのセキュリティ対策については詳細を定義せず、CPE の実装依存となっている。
更に、API への改ざん・不正アクセス・タッピング等へのセキュリティ対策についても同様に、CPE の実装依存となっている。
従って、TR-069 との関連・依存性は特にない。

6.3 留意事項

(1) 鍵配送問題と認証方式

SPEC-023 では、HTTP ダイジェスト認証に必要な ID、パスワードは、事業者側で設定された値を STB の出荷時、ないしはサービス開始時に STB に設定する前提である旨明記している。しかしながら一方で、ユーザーID 相当の<OUI>-<ProductClass>-<SerialNumber> の SerialNumber は JLabs 管理となっているし、パスワードについては JCL SPEC-001 5.3.9 記載の受信機 ID(6 バイト)をパスワードとして設定できる旨の記載もあり、事業者というよりは JLabs と STB メーカー主体の管理を前提としているようにも見え、ID・パスワードの位置付けと流通経路が必ずしも明確でない。

TR-069 では、HTTP ダイジェスト認証に使用するパスワードはいわゆる共有秘密鍵に相当する概念であり、流通経路については TR-069 の規定対象外として明確な定めがない。

このため、実商用サービスで STB を配布する場合には、いつ、誰が、どこで、どのように鍵を発行・配送するのか、事業者自身による具体的な検討が必須である。

更に、TR-069 では認証方式としてログイン認証・ダイジェスト認証および証明書認証のいずれかを選択できるが、SPEC-023 ではクライアント証明書への対応を義務付けている。

クライアント証明書を STB に記憶させる場合、上述の鍵配送問題に加え、CA 局による認証方式の検討が別途必要になる。例えば、ベリサイン等の商用 CA 局で認証する場合、クライアント証明書の発行に別途追加費用が発生する。

更に、STB の CPU・メモリ等が貧弱で処理能力が低い場合、クライアント証明書を前提とした RSA 等の公開鍵暗号方式は処理コストが高く、所要の通信性能を達成できない場合があるので注意が必要である。

(2) オーバーヘッド

TCP を採用している事、元来はアプリケーションレベルのセッション管理機構を持たないシンプルな HTTP で敢えて複雑なセッション管理を実装している事、既に Web サービスの主流から外れた SOAP を使っている事から、SNMP に比較した場合、処理コスト・通信の双方でオーバーヘッドがかなり大きい。このため、ACS, CPE 自身の処理負荷に加え、経路上のネットワーク機器に係る負荷にも注意が必要である。

(3) STUN による NAT 越え

NAT 配下に CPE が設置されている場合、SPEC-023 では TR-069 Annex G に規定する NAT 越え方式(STUN ベース)への対応を求めているが、NAT の種類によっては STUN が使えないケースも存在する。このため実際のネットワーク設計に際しては、まずは NAT の STUN 対応可否を確認し、場合によっては既存 NAT から TR-069 に対応した IGD(TR-069 Annex F 参照)への置換も含めた包括的な検討が必要である。

以上