



ATIS-0800009

ATIS Standard on -

**REMOTE MANAGEMENT OF DEVICES IN THE CONSUMER DOMAIN
FOR IPTV SERVICES**



The Alliance for Telecommunication Industry Solutions (ATIS) is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from over 300 communications companies are active in ATIS' 22 industry committees and its Incubator Solutions Program.

< <http://www.atis.org/> >

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith.
--

ATIS-0800009, *Remote Management of Devices in the Consumer Domain for IPTV Services*

Is an American National Standard developed by the **Architecture (ARCH)** Committee under the **ATIS IPTV Interoperability Forum (IIF)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Copyright © 2008 by Alliance for Telecommunications Industry Solutions
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < http://www.atis.org >.

Printed in the United States of America.

REMOTE MANAGEMENT OF DEVICES IN THE CONSUMER DOMAIN FOR IPTV SERVICES

Secretariat

Alliance for Telecommunications Industry Solutions

Approved March 2008

Abstract

This document covers remote device management architecture, remote device management protocols, software download, provisioning, configuration, and monitoring of devices in the consumer domain for IPTV services.

FOREWORD

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The IPTV Interoperability Forum (IIF) develops requirements, standards, and specifications that will determine the industry's end-to-end solution for Internet Protocol Television (IPTV).

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, IIF Secretariat, 1200 G Street NW, Suite 500, Washington, DC 20005.

The Architecture (ARCH) Committee was responsible for the development of this document, with the leadership of the following people:

- D. O'Callaghan, IIF Chair
- R. Brand, IIF Vice Chair
- R. Sharpe, ARCH Committee Co-Chairs
- S. Wright, ARCH Committee Co-Chair
- R. Jagannathan, Technical Editor
- M. Midani, Technical Editor
- C.A. Underkoffler, ATIS Chief Editor
- A. Blasgen, IIF Committee Administrator

CONTRIBUTORS

Rajesh Jagannathan, Alcatel-Lucent
 Randy Sharpe, Alcatel-Lucent
 Rick Townsend, Alcatel-Lucent
 Amit Kleinmann, Amdocs
 Phyllis Anderson, AT&T
 Al Morton, AT&T
 Steven Wright, AT&T
 Simon Jones, BT
 Mark Watson, Digital Fountain
 George Foti, Ericsson
 Joe Lenart, Hitachi
 Rajendra Bopardikar, Intel
 Scott Shoaf, Juniper Networks
 Nandhu Nandhakumar, LG Electronics
 Mike Dolan, Microsoft
 Orit Levin, Microsoft

James Van Loo, Microsoft
 Mowaffak Midani, Motorola, Technical Editor
 Joe Rodolico, Nielsen Media
 Kevin Boyle, Nortel
 Richard Brand, Nortel
 Ronnie Dhaliwal, Qwest
 Michael Fargano, Qwest
 Jean-Yves Bernard, Rogers Communications
 Nadine Guillaume, Cisco
 Mark Eyer, Sony
 Matthew Goldman, Tandberg Television
 Ken Kerpez, Telcordia
 Kurt Melden, Verivue
 Bhumi Khasnabish, Verizon
 Dan O'Callaghan, Verizon
 Reza Shafiee, Verizon

TABLE OF CONTENTS

1 INTRODUCTION1

2 SCOPE.....3

3 REMOTE DEVICE MANAGEMENT ARCHITECTURE.....3

4 SOFTWARE DOWNLOAD MANAGEMENT5

 4.1 SOFTWARE DOWNLOAD DEFINITION5

 4.2 SOFTWARE DOWNLOAD ARCHITECTURE6

 4.3 SOFTWARE DOWNLOAD MECHANISM.....9

5 REMOTE DEVICE MANAGEMENT PROCEDURE.....10

 5.1 DNG REMOTE DEVICE MANAGEMENT PROCEDURE10

 5.2 ITF DEVICE REMOTE DEVICE MANAGEMENT PROCEDURE.....10

 5.3 MOBILE DEVICE MANAGEMENT PROCEDURE.....10

 5.4 MULTI-TECHNOLOGY APPLICATION DEVICE MANAGEMENT PROCEDURE11

6 REMOTE DEVICE MONITORING.....11

 6.1 REMOTE DEVICE MONITORING ARCHITECTURE12

 6.2 DNG MONITORING13

 6.3 ITF DEVICE MONITORING14

7 REMOTE DEVICE DATA MODEL FOR MANAGEMENT14

 7.1 DNG PROFILES15

 7.2 ITF PROFILES.....15

 7.3 ACCESS RESTRICTIONS15

8 REFERENCES16

TABLE OF FIGURES

FIGURE 1: REMOTE DEVICE MANAGEMENT ARCHITECTURE.....4

FIGURE 2: SOFTWARE DOWNLOAD ARCHITECTURE6

FIGURE 3: VIDEO INSERTION AT DIFFERENT POINTS IN THE NETWORK12

FIGURE 4: VIDEO FLOWS ON TOP OF THE IP LAYER12

FIGURE 5: LAYERED REMOTE DEVICE MONITORING ARCHITECTURE.....13

TABLE OF TABLES

TABLE 1: REMOTE MANAGEMENT PROTOCOL STACK, PER TR-0694

TABLE 2: SOFTWARE DOWNLOAD INTERFACES8

ATIS Standard on

Remote Management of Devices in the Consumer Domain for IPTV Services

1 INTRODUCTION

Internet Protocol Television (IPTV) is defined as a “managed service” providing the secure and reliable delivery of entertainment video and related services over an Internet Protocol (IP) network. In order to provide a secure and reliable service, the Service Provider (SP) may require access to manage several aspects of the functions in the home network relevant to the IPTV service [1].

ATIS-0800002, *IPTV Architecture Requirements* [1], specifically states the following requirements for the remote management of devices in the home environment:

IIF.ARCH.HOME.56	The IPTV Architecture shall support the ability to provision the DNG and ITF remotely.
-------------------------	---

IIF.ARCH.HOME.57	The IPTV Architecture shall support the ability to collect status information from the DNG and ITF remotely.
-------------------------	---

Remote management of fixed or mobile devices is defined as an access-agnostic, secure, and reliable mechanism to configure, monitor, and manage the devices in the consumer domain, including software download and/or upgrade. There are differences based on whether the device is mobile or not. Protocols for management of remote devices are also access-technology agnostic within the fixed or mobile domains. Obviously, the device should be able to attach (or connect) to a Network/Service Provider to allow for the remote management task to take place.

1.2 Acronyms

CA	Conditional Access
CDMA	Code Division Multiple Access
CPE	Customer Premise Equipment
DM	Device Management
DNG	Delivery Network Gateway
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DVB	Digital Video Broadcast
DVR	Digital Video Recorder

ATIS-0800009

EPG	Electronic Program Guide
FLUTE	File Delivery over Unidirectional Transport
GSM	Groupe Spécial Mobile
HN	Home Network
HNS	Home Network Segment
HTTP	Hyper Text Transport Protocol
IGD	Internet Gateway Device
IGMP	Internet Group Management Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPTV	Internet Protocol Television
ITF	IPTV Terminal Function
LAN	Local Area Network
MPEG	Moving Picture Experts Group
MPEG TS	MPEG Transport Stream
NAT	Network Address Translation
NGN	Next Generation Network
NP	Network Provider
OMA	Open Mobile Alliance
PAT	Program Association Table
PIM	Protocol-Independent Multicast
PMT	Program Map Table
PTF	Protocol Translation Function
PVR	Personal Video Recorder
QoE	Quality of Experience
QoS	Quality of Service
QoS M	Quality of Service Metrics
RCMS	Remote Configuration and Management Server
RMS-FUS	Remote Management and Firmware Update System
RPC	Remote Procedure Call
RTP	Real Time Protocol
SDS	Software Download Server
SHE	Super Head End
SP	Service Provider
SSL	Secure Sockets Layer
STB	Set Top Box
TCP	Transport Control Protocol
TDMA	Time Division Multiple Access
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VHO	Video Hub Office

VoD	Video on Demand
VSO	Video Site Observer
WAN	Wide Area Network

2 SCOPE

This document discusses the remote management of devices in the consumer domain, focusing initially on the Delivery Network Gateway (DNG) and IPTV Terminal Function (ITF) devices. Other devices -- such as handheld devices, storage devices, etc. -- are under consideration for future releases of this document.

This document covers remote Device Management (DM) architecture, software download, provisioning of parameters, status monitoring, remote diagnostics, fault recovery, and security management.

This document builds upon DSL Forum TR-069 [3] remote management methods, protocols, and related DSL Forum data models to the extent possible. It also builds upon enhancements to TR-069 developed by DVB in their Remote Management and Firmware Update System (RMS-FUS) for DVB IP Services [10]. However, additional enhancements to the TR-069 protocol and data models will be provided when deemed necessary to accommodate the specific needs of the IIF IPTV service and architecture.

3 REMOTE DEVICE MANAGEMENT ARCHITECTURE

The IPTV architecture defines a rich consumer domain environment that includes a variety of consumer devices of varying degrees of sophistication. This typically includes a DNG with routing and firewall capability; multiple ITF devices, such as Set Top Boxes (STBs) and storage devices that terminate the IPTV streams; and mobile devices that are likely to communicate with the network directly rather than through the DNG.

Remote management for each of these devices is required for the proper operation of the managed IPTV service. Due to the topology of the home network, different management flows are required to fully meet the remote management requirements for the IPTV service. As shown in the figure below, the following flows are required:

- ◆ Flow (1) for the remote management between the network and the DNG.
- ◆ Flow (2) for the remote management between the network and the ITF devices.
- ◆ Flow (3) for the remote management between the network and the mobile devices.

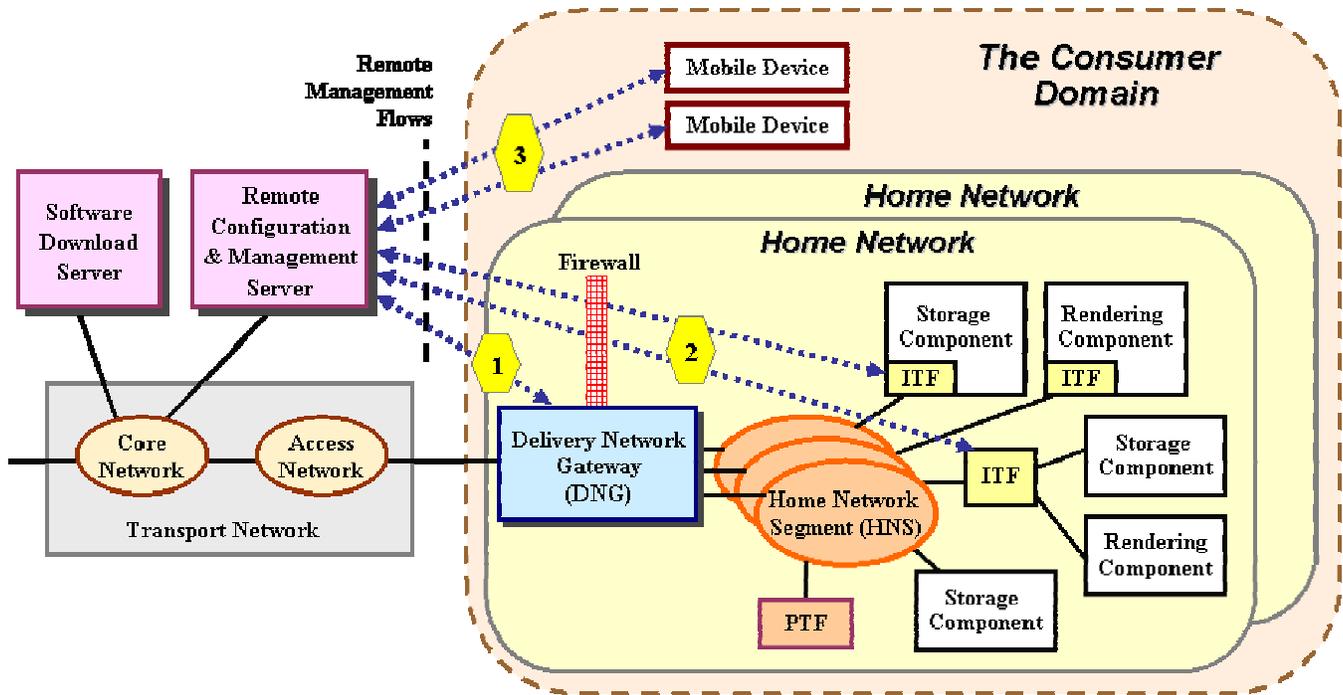


Figure 1: Remote Device Management Architecture

Management flows 1 and 2 are based on the DSL Forum TR-069 architecture and protocol specifications [3], with specific additions and enhancements deemed necessary to better satisfy the remote management needs of the IPTV consumer domain environment.

The protocol stack is based on invoking Remote Procedure Call (RPC) methods, expressed in a SOAP presentation layer, communicated in Hyper Text Transport Protocol (HTTP) [13] over a Secure Sockets Layer (SSL) [14] or Transport Layer Security (TLS)[15], and carried over Transport Control Protocol (TCP) over IP, as shown below.

Management Applications
RPC Methods
SOAP (presentation layer)
HTTP
SSL (or TLS)
TCP
IP

Table 1: Remote Management Protocol Stack, per TR-069

The architecture proposed above takes into account the reference model of the home network specified in ATIS-0800002, *IPTV Architecture Requirements* [1], the separation between layers and domains specified in the Next Generation Network (NGN), and the need to allow both the Network Provider (NP) and Service Provider (SP) to download software images and other information to the home devices.

This architecture accommodates IP Multimedia Subsystem (IMS)-based IPTV networks and non-IMS-based IPTV networks. There is a common sequence that takes place between a home device (when it first attaches to the network) and the Remote Configuration and Management Server (RCMS) for both IMS and non-IMS networks described in ATIS-0800017, *Attachment and Initialization Specification for IPTV Services in the Consumer Domain* [2].

For Groupe Spécial Mobile (GSM), Time Division Multiple Access (TDMA), and Code Division Multiple Access (CDMA) Mobile Devices, management flow 3 is to be based on the Open Mobile Alliance (OMA) Device Management specifications [4], including device authentication, device bootstrapping, and device management.

If a software download -- including possible user profiles -- is deemed necessary during the initial configuration phase, the RCMS will pass the Uniform Resource Locator (URL) of the appropriate Software Download Server (SDS) to the device, and files will be downloaded to the target device using any of the mechanisms stated in the Software Download Management section below.

4 SOFTWARE DOWNLOAD MANAGEMENT

Software download service is part of remote device management service in the remote device management architecture.

The software download service is based on the DSL Forum TR-069 Amendment 2 [12] as extended for multicast delivery and other reasons in DVB Remote Management and Firmware Update System for DVB IP Services [10], with exceptions and additions noted. Some of the major distinctions are:

- ◆ This specification only applies to managed devices in the consumer domain (DVB RMS-only and RMS-FUS modes are endorsed; FUS-only mode is not endorsed).
- ◆ This specification makes a distinction between DNGs and ITFs. DVB treats them the same and refers to them both as Customer Premise Equipment (CPE).
- ◆ DNG and ITF bootstrapping for software downloading is accomplished as specified by TR-069 Amendment 2 [12] (the additional DVB method involving a FUS stub file and multicast boot sequence is *not* endorsed).

Completely new software and updates to previously installed software in a DNG or ITF are downloaded from a SDS with the active participation of a RCMS.

The software download service provides a notification service that announces the availability of software updates to DNGs and ITFs. The DNG or ITF is provisioned or is able to acquire information that will help it to identify, attach to, and monitor this service, as well as interpret the information provided.

4.1 Software Download Definition

Software to be downloaded is defined in a broad term that includes the following:

- ◆ An executable (image) running on the device.
- ◆ Updates to certain modules of the executable.
- ◆ Applications/modules running on top of the basic executable image.
- ◆ Profile files for the customization of certain features and services on the managed device.

It shall be possible to download run-time applications without the need to re-boot the ITF device after the updates are made effective. Such a capability is highly desirable for the DNG.

Note that media file downloads are out of the scope of this document.

4.2 Software Download Architecture

The SDS is a separate entity that is under the control of the RCMS, as shown in Figure 2.

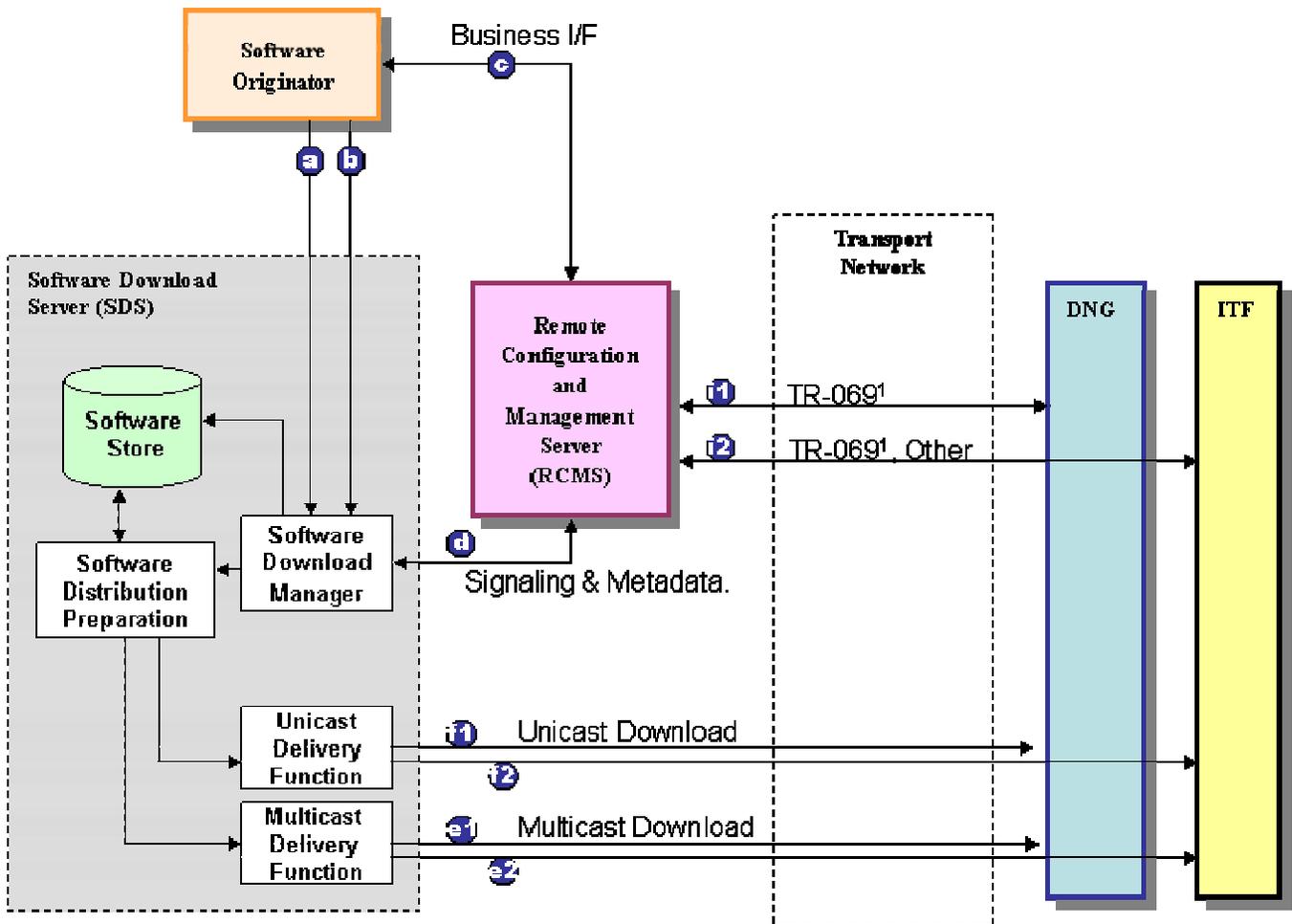


Figure 2: Software Download Architecture

Interfaces are defined so that the device hosting the software download service could be an integral part of RCMS or a separate device in the same or different domain. The SDS could be in a NP or SP domain.

¹ This interface for software downloads requires additional capability to be added to the TR-069 mechanism that is specified in Annex 1 of the DVB RMS-FUS (Annex 1: Extensions to TR-069 / CWMP required for DVB RMS-FUS).

4.2.1 Software Originator: A DNG or ITF manufacturer or an independent software vendor having a business relationship with the provider controlling remote configuration and management.

4.2.2 Software Download Server: A logical entity containing all the components required for a software download service. It is possible for all the components in the server to be physically co-located.

4.2.3 Software Download Manager: Coordinates the receiving and storage of software files and associated metadata from a software originator. It uses the metadata to add new entries to the notification service. It also uses the metadata to help in the formatting and packaging of the software file by the software distribution preparation function.

4.2.4 Software Store: Provides persistent storage of downloaded software from the software originator.

4.2.5 Notification Service: Notifies the availability of any software to a DNG or ITF device.

4.2.6 Software Distribution Preparation: A function that prepares the software files for delivery over an IP network. It includes fragmenting, adding headers, and adding parameters compatible with delivery format.

4.2.7 Unicast Delivery Function: The delivery function provided for IPTV content delivery, characterized by a 1:1 correspondence between a data source and a sink point.

4.2.8 Multicast Delivery Function: The delivery function provided for IPTV content delivery, characterized by a 1:N correspondence between a data source and a sink point.

The definitions of the depicted interfaces and the correspondence with DVB RMS/FUS [10] interfaces are shown in the table below:

Table 2: Software Download Interfaces

<i>Interface label</i>	<i>Equivalent DVB I/F²</i>	<i>Description</i>	<i>Standardization</i>
a	1	This interface carries the files containing the software from the software originator entity to the software download manager.	This interface is out of scope for this specification document.
b	2	This interface carries the files containing the metadata from the software originator entity to the software download manager.	This interface is out of scope for this specification document.
b	3	Business-to-business relationship between the software originator and the network operator.	This interface is out of scope for this specification document.
e	4	Signaling and metadata between RCMS and the software download manager.	Signaling based on DVB specs. Metadata to be specified by the ATIS IIF based on DVB specs.
e1	5	Multicast delivery to the DNG.	Based on DVB specs. Metadata to be specified by the ATIS IIF based on DVB specs.
e2	5	Multicast delivery to the ITF.	Transport protocols options based on DVB specs (e.g. FLUTE). Metadata to be specified by the ATIS IIF based on DVB specs.
f1	6	Unicast delivery to the DNG.	Based on DVB specs. Metadata to be specified by the ATIS IIF based on DVB specs.
f2	6	Unicast delivery to the ITF.	Transport protocols options based on DVB specs. Metadata to be specified by the ATIS IIF based on DVB specs.
i1	9	Download management signaling.	Based on TR-069 Amendment 2.
i2	9	Configuration and download management signaling.	Based on TR-069 Amendment 2.

Figure 2 defines ten interfaces and Table 2 maps nine of them to DVB RMS-FUS specifications. Not all interfaces need to be implemented in order for the system to be functional. DVB RMS-FUS specifies some interfaces as required and others as optional, however this document makes some of those options mandatory. Table 3 summarizes the required interfaces for ATIS IIF conformance. These are a subset of the cases specified in DVB RMS-FUS (RMS-FUS and managed CPE cases only).

² Figure 6, Architecture showing system interfaces of DVB Draft Specification IPI2384r11, Remote Management and Firmware Update System for DVB IP Services - Approved by DVB TM-IPI [10].

Table 3: Interface Conformance

Interface	Conformance
e1/e2	Required
f1/f2	Required
i1/i2	Required

4.3 Software Download Mechanism

Software downloads to, and required authentication for, a DNG and ITF may happen in several ways, and is different for unicast versus multicast transport.

The DSL Forum TR-069 and DVB RMS-FUS CPE software download methods do not consider some ATIS IIF requirements. The DSL Forum specifies authentication of the Auto-Configuration Server by CPE. The DVB RMS-FUS specification recommends authentication of source and sometimes destinations of the various interfaces but does not specify any particular method. They both have the same digitally-signed file formats for downloaded file authentication. A signed file is downloaded and its certificates verified, followed by storage of this file until required for execution. At the time of execution there is no guarantee that the original file has not been tampered with.

It is possible that there is a need to store an authenticated file for execution at a later time. Since the DSL Forum and DVB CPE specifications do not guarantee authenticity at the time of executing a downloaded file, the ATIS IIF shall specify additional methods to satisfy such a need.

The following is a list of requirements that specify the unicast and multicast software download methods to follow for DNG and ITF:

- ◆ The unicast download mechanism for a DNG shall follow the DSL Forum TR-069 and DVB RMS-FUS [10] specifications.
- ◆ The unicast download mechanism for an ITF shall follow the DSL Forum TR-069 and DVB RMS-FUS [10] specifications. Additional authentication mechanisms as defined by the ATIS IIF may be used for additional security by authenticating saved files loaded at runtime.
- ◆ The multicast download mechanism for a DNG shall follow the DVB RMS-FUS [10] specifications.
- ◆ The multicast download mechanism for an ITF shall follow the DVB RMS-FUS download specifications [10]. Additional authentication mechanisms as defined by the IIF may be used for additional security by authenticating saved files at runtime.

For the additional authentication mechanism for stored files, the ITF uses an authentication service rooted in a trust mechanism defined by the ATIS IIF to authenticate the files irrespective of the download protocols. This authentication mechanism is optional for the DNG.

The download may be initiated by the CPE, RCMS, or software originator. The first two cases are specified in TR-069. The case of a software originator initiating a download is for further study.

Irrespective of the initiator, all software downloads have to be authorized and controlled by the RCMS. DVB RMS-FUS Annex 1 describes extensions to the TR-069 CPE WAN Management Protocol to

support the multicast and other capabilities introduced by the DVB specification including additional RPCs and data model extensions.

Notifications for software download are provided over the i1 and i2 interfaces for both multicast and unicast downloads. In the case of multicast downloads to the DNG or ITF, the download RPC method provides a URL pointing to a resource locator file (XML that configures the FLUTE stack) using HTTP with the following naming convention:

```
atis-iif-resourcelocator.xml
```

It might be advantageous whenever multiple CPE devices are updated with the same software download that it be done via a multicast mechanism. There may be instances when the download is specific to a particular CPE and thus unicast methods would be more appropriate.

5 REMOTE DEVICE MANAGEMENT PROCEDURE

5.1 DNG Remote Device Management Procedure

Provisioning and configuration of the DNG shall follow the RPC methods stated in the DSL Forum TR-069 specifications for the Internet Gateway Device (IGD) and the protocol stack stated in Section 3.

5.2 ITF Device Remote Device Management Procedure

For ITF devices connected to the DNG, provisioning and configuration of ITF devices shall follow the RPC methods stated in the DSL Forum TR-069 and TR-111 [7] specifications for “CPE devices” residing behind the DNG. The specific parameters are specified in the corresponding data model of each device. TR-111 offers a method to associate a DNG with an ITF device from an RCMS’s point of view. It also allows an RCMS to initiate a connection request to an ITF device if the ITF device is operating behind a Network Address Translation (NAT) gateway function in the DNG. Other remote management protocols for ITFs are subject to further study.

5.3 Mobile Device Management Procedure

The OMA Device Management protocol shall be used for the management of 3GPP and 3GPP2 mobile devices.

The underlying transport is a request/response SyncML exchange between the OMA client (on the mobile device) and the OMA server. The protocol provides the functionality to pass one SyncML message or multiple SyncML messages (as packages) between the source and destination.

In order to avoid overwhelming an OMA client, an OMA server is not permitted to send new commands to a client that has not yet returned a status to previous commands. The following OMA DM packages/messages and procedures are defined by the OMA DM specifications:

- ◆ **Package 0: Management Initiation Alert from Server to Client:**

This package is required since some mobile devices cannot continuously listen for connections from a management server or do not wish to keep an open port for security reasons. Devices, however, can continue to receive unsolicited messages called *notifications*.

A management server can use this notification capability to alert the device to cause the client to initiate a connection back to the management server. OMA DM protocol specifies several management initiation notification bearers.

◆ **Package 1: Initialization from Client to Server:**

In this package the device sends the following to the server:

- Mobile device information (such as manufacturer, model, etc.). The client *shall* send device information in the first message of the management session.
- An indication as to whether the management session was initiated by the server (by sending a trigger in Package 0) or by the client (such as an end user selecting a menu item).
- Any optional client-generated alert.

◆ **Package 2: Initialization from Server to Client:**

In this package, the server needs to identify itself to the client and optionally send user-interaction commands and management data and commands.

◆ **Package 3: Client response to Server:**

This package contains:

- Results of management actions sent from server to client.
- Results of user interaction commands.
- New optional client-generated alerts.

This package is sent by the client if Package 2 contained management commands that required a response from the client.

◆ **Package 4: Further management operations**

This package is used to close a management session.

5.4 *Multi-technology Application Device Management Procedure*

In the case where the device would incorporate the capability of multiple technologies, such as for example Fixed Mobile Convergence (FMC), only one Device Management protocol should be used in the device at any particular time. In those kinds of applications, either DSL Forum TR-069 or OMA-DM protocols should be used for the remote management of devices in the consumer domain, per individual operator requirements.

6 REMOTE DEVICE MONITORING

The remote management of devices in the home serves several purposes. These include:

- ◆ Assessment of the user's Quality of Experience (QoE).
- ◆ Network performance management and diagnosis.
- ◆ Determination of consumer domain device capabilities.
- ◆ Configuration of consumer domain devices and their capabilities.

6.1 Remote Device Monitoring Architecture

Remote monitoring of devices in the consumer domain must take into account the fact that the IPTV network is a “hierarchical network” consisting of multiple segments and nodes. That is, while video content basically originates in the Super Head End (SHE), different video streams including programs, advertisements, emergency alert messages, etc., can be injected (or removed) at different points in the network, as shown below.

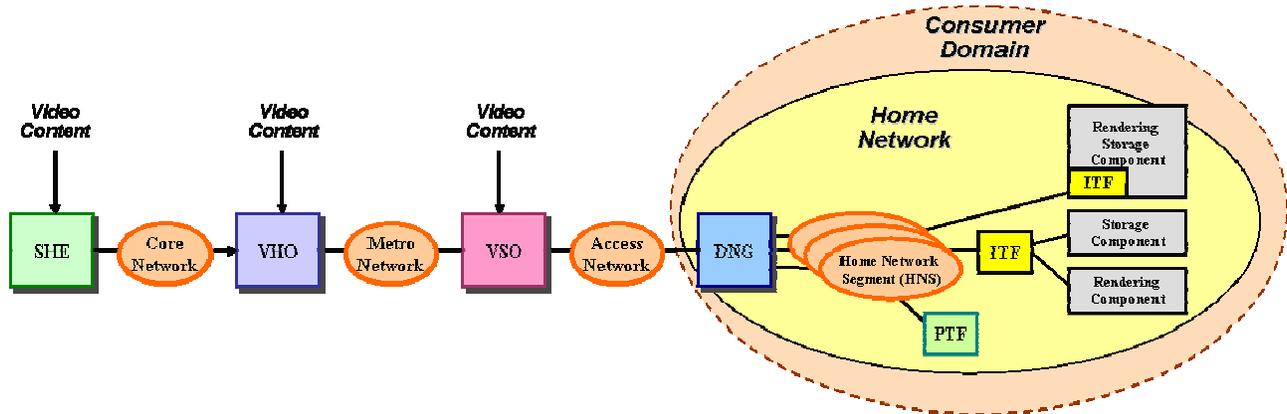


Figure 3: Video Insertion at Different Points in the Network

The video flows will therefore ride on top of an end-to-end IP transport layer, spanning multiple network segments, as shown below.

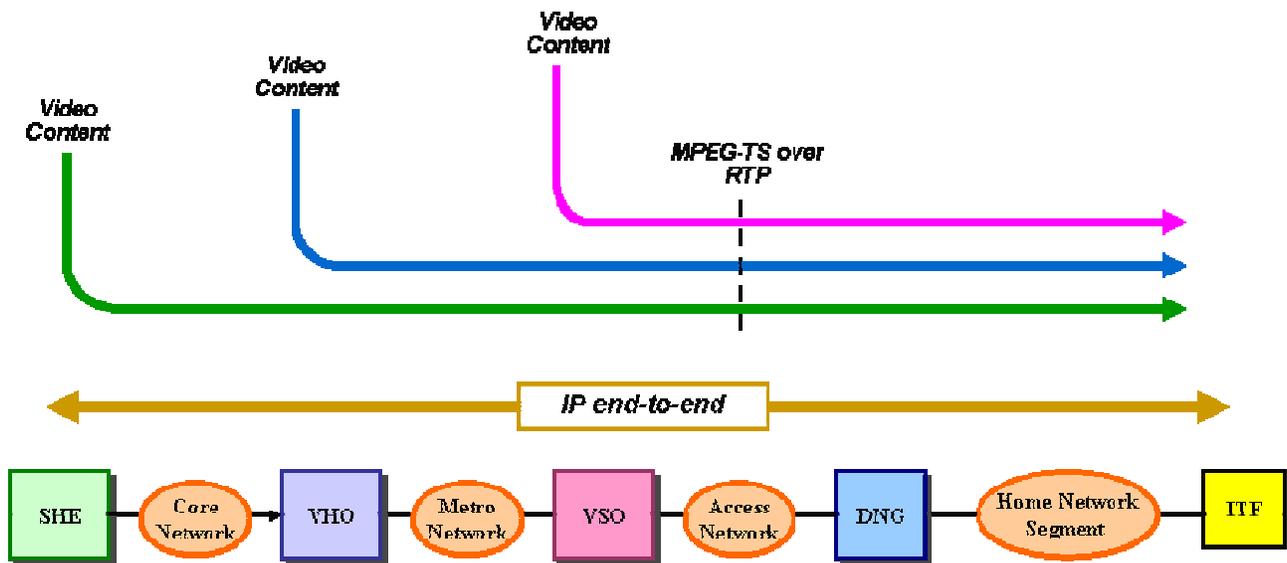


Figure 4: Video Flows on top of the IP Layer

The MPEG System Information tables (PAT, PMT), Electronic Program Guide (EPG), and other types of control, management, and metadata information may be modified at different points along the network; thus, an error could be introduced at any of these injection points.

An error in the MPEG layer may not be detectable at the IP layer. Moreover, with the advent of MPEG layer recovery techniques (such as MPEG error concealment), relying solely on the IP layer may not be sufficient to determine the impact of a network or service fault in the network.

Remote monitoring of devices in the consumer domain must take into account the “layering principle” adopted by the NGN and the ATIS IIF. Therefore, the following layered remote monitoring architecture for IPTV is being adopted in these specifications, as shown in the figure below.

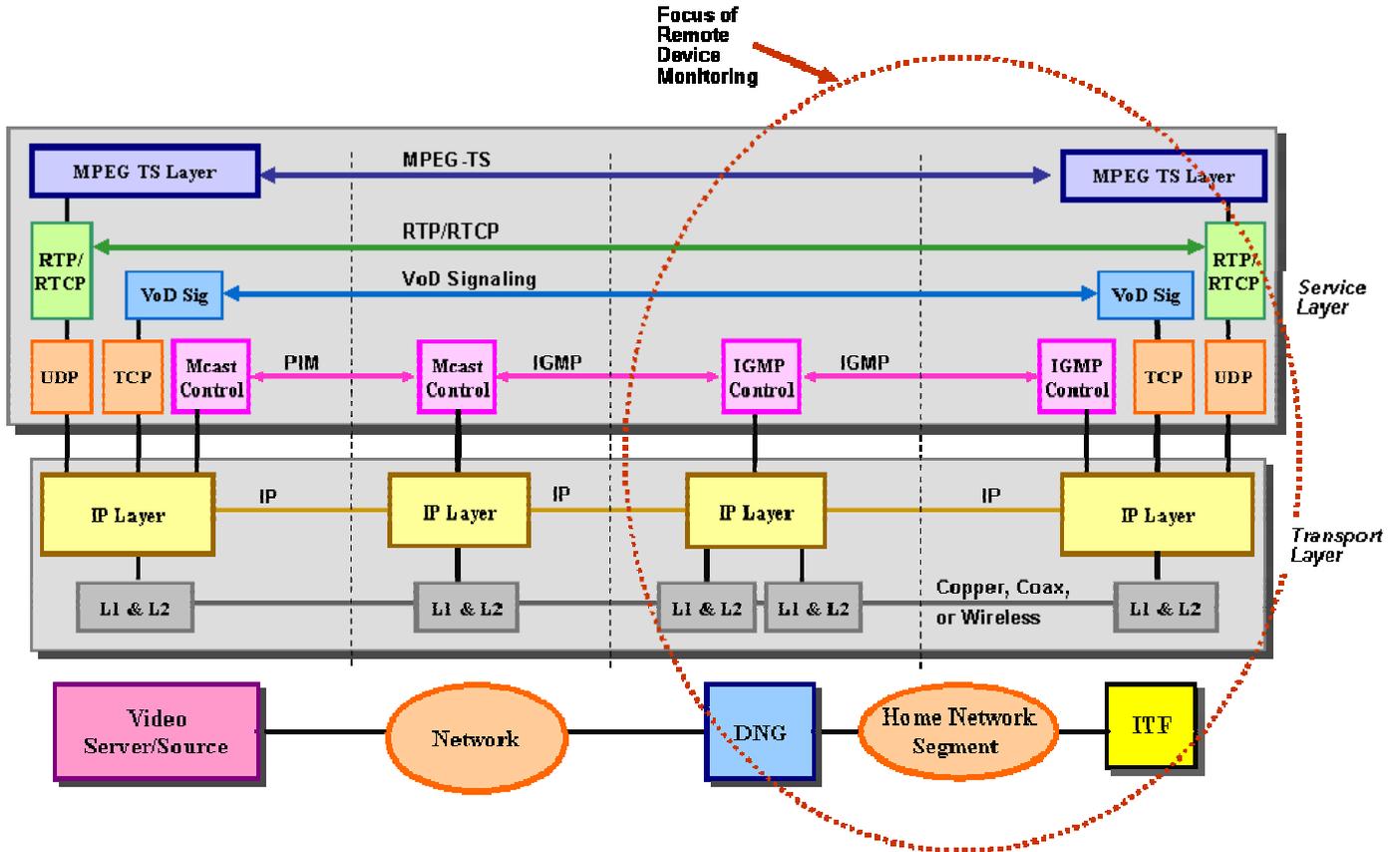


Figure 5: Layered Remote Device Monitoring Architecture

As shown, different network elements in the consumer domain have access and visibility to different layers along the network path, and therefore different and specific parameters need to be remotely monitored for each device to provide an adequate level of visibility/manageability by the network/service provider for IPTV services. The type of information to be monitored, on a per device basis, is shown in the next sections. ATIS-0800004, *Quality of Service Metrics (QoSM) Framework Document* [5], has detailed Quality of Service (QoS) measurement models with domains and metric layers.

6.2 DNG Monitoring

The DNG should allow remote monitoring by the network/service provider. This information could be classified into the following categories:

- ◆ DNG device information -- such as manufacturer, model, and software/firmware version.

- ◆ Information relating to the DNG's association with RCMS.
- ◆ Information relating to the SP -- such as URL for home page and help desk, logo, etc.
- ◆ Information relating to the packet forwarding behavior -- such as filtering, queue management, classification and marking, rate shaping, policing, etc.
- ◆ Information related to addressing/reachability information (IP addressing, port addressing).
- ◆ Statistical information of usage for the linear broadcast service (IGMP groups and counts).
- ◆ Service transaction-related information -- such as the user changing between linear IPTV channels.
- ◆ Information related to the DNG Local Area Network (LAN) interface -- such as type, status, packets sent and received, etc.
- ◆ Information related to the DNG Wide Area Network (WAN) interface -- such as status, downstream and upstream rates, noise margin, code violations, errored seconds, packets sent and received, etc.

Specific QoS and QoE related metrics for the linear IPTV service are specified in ATIS-0800008, *QoS Metrics for Linear Broadcast IPTV* [6].

6.3 ITF Device Monitoring

The ITF device should allow remote monitoring by the network/service provider. This information could be classified into the following categories:

- ◆ ITF device information -- such as manufacturer, model, and software/firmware version.
- ◆ Information relating to the service provider -- such as URL for home page and help desk, logo, etc.
- ◆ Audience measurements -- such as channels watched and duration.
- ◆ Information related to ITF capabilities -- such as the maximum number of streams that can be decoded, the audio and video formats and profile/levels supported, Conditional Access (CA) capabilities, the inclusion of a Personal Video Recorder (PVR), etc.
- ◆ The ability to enable or disable ITF capabilities.
- ◆ Parameters related to reachability (IP address and port address) and packet markings.
- ◆ Information related to the media streams (e.g., RTP, MPEG2 transport streams, or other) for both streams and mid/end-points (e.g., buffer related metrics).
- ◆ Transmission related metrics -- such as IP packets received, packets lost, jitter, etc.
- ◆ Service transaction related information -- such as the user changing between linear IPTV channels.
- ◆ Optionally, information related to the estimated quality of the content -- such as that of video and audio streams.

Specific QoS and QoE related metrics for the linear IPTV service are specified in ATIS-0800008, *QoS Metrics for Linear Broadcast IPTV* [6].

7 REMOTE DEVICE DATA MODEL FOR MANAGEMENT

A data model shall be adopted or developed by the ATIS IIF in order to address -- within a TR-069 framework -- software download management, device management, monitoring, diagnostics, and fault

management. The model allows the RCMS to read components and capabilities of the devices it is administering.

The data model shall specify objects and parameters for each object. In addition, the data model shall specify several service profiles. All service profiles shall contain a set of objects and parameters that are the minimum required for that service.

7.1 DNG Profiles

Source data models for the DNG may be based on the DSL Forum TR-098 [8] with extensions and profiles. The classification of candidate profiles for the DNG may include:

- ◆ *Base model*: This is the minimum dataset under which ATIS IIF IPTV services could be provided.
- ◆ *Extended model*: This model contains data capable of extending the basic IPTV service with some optional enhancements.
- ◆ *Monitoring service profile*: The data model would contain a profile of objects and parameters that would enable monitoring from the RCMS.

7.2 IIF Profiles

Source data models for the IIF device may be based on the DSL Forum TR-135 [9] with extensions and profiles. The classification of candidate profiles for the IIF may include:

- ◆ *Base profile for IPTV*: This is the minimum dataset under which the ATIS IIF IPTV services could be provided.
- ◆ *Extended profile for IPTV*: This profile will contain data capable of extending the basic IPTV service with some optional enhancements.
- ◆ *DRM service profile*: This profile will enable Digital Rights Management (DRM) and Conditional Access services. This is a topic for further study in the IIF.
- ◆ *Monitoring service profile*: This profile will include objects and parameters that would enable monitoring from the RCMS.
- ◆ *Diagnostics and fault management service profile*: This profile will enable remote as well as on-site diagnostics and fault management.
- ◆ *Software upgrade service profile*: This profile will define objects and parameters that enable software updates controlled by the RCMS.
- ◆ *Audience measurement service profile*: This profile will define objects and parameters that collect data on usage characteristics of IPTV service.

Other profiles to consider include RTP, MPEG Transport Stream (TS), MPEG, and Digital Video Recorder (DVR).

7.3 Access Restrictions

Objects and parameters can be subject to various levels of restrictions. The objects and parameters in the data model are categorized as:

- ◆ Mandatory
- ◆ Active Notification required (as in TR-069) to RCMS
- ◆ Passive Notification to RCMS

- ◆ Readable by RCMS
- ◆ Writable
- ◆ Creatable/Deletable

8 REFERENCES

- [1] ATIS-0800002, *IPTV Architecture Requirements*, April 2006.³
- [2] ATIS-0800017, *Attachment and Initialization Specification for IPTV Services in the Consumer Domain*, not yet published.³
- [3] DSL Forum TR-069, *CPE WAN Management Protocol*, May 2004, and Amendment 1, November 2006.⁴
- [4] Open Mobile Alliance, *OMA Device Management Protocol, Version 1.2, OMA-TS-DM_Protocol-V1_2*, February 9, 2007.⁵
- [5] ATIS-0800004, *QoS Framework*, November 2006.³
- [6] ATIS-0800008, *QoS Metrics for Linear Broadcast IPTV*, August 2007.³
- [7] DSL Forum TR-111, *Applying TR-069 to Remote Management of Home Networking Devices*, December 2005.⁴
- [8] DSL Forum TR-098, *Applying TR-069 to Remote Management of Home Networking Devices*, September 2005.⁴
- [9] DSL Forum TR-135, *Data Model for a TR-069-enabled STB*, December 2007.⁴
- [10] ETSI TS 102 824, *Remote Management and Firmware Update System for DVB IP Services*, February 2008.⁶
- [11] IETF RFC 3926, *FLUTE – File Delivery over Unidirectional Transport*.⁷
- [12] DSL Forum TR 069, *Amendment 2: CPE WAN Management Protocol*, December 2007.⁴
- [13] IETF RFC 2616, *Hypertext Transfer Protocol -- HTTP/1.1*.⁷
- [14] The SSL Protocol, Version 3.0.⁸
- [15] IETF RFC 2246, *The TLS Protocol, Version 1.0*.⁷

³ This document is/will be available from the Alliance for Telecommunications Industry Solutions, 1200 G Street N.W., Suite 500, Washington, DC 20005. < <http://www.atis.org> >

⁴ This document is available from the DSL Forum. < <http://www.dslforum.org/techwork/treports.shtml> >

⁵ This document is available from the Open Mobile Alliance (OMA). < <http://www.openmobilealliance.org/> >

⁶ This document is available from the European Telecommunications Standards Institute (ETSI). < <http://www.etsi.org/getastandard/home.htm> >

⁷ This document is available from the Internet Engineering Task Force (IETF). < <http://www.ietf.org> >

⁸ This document is available at < <http://wp.netscape.com/eng/ssl3/ssl-toc.html> >