ATIS STANDARD

ATIS-0800017.v002

ATIS Standard on -

NETWORK ATTACHMENT AND INITIALIZATION OF DEVICES AND CLIENT DISCOVERY OF 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-0800017.v002, *Network Attachment and Initialization of Devices and Client Discovery of 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.

ATIS-0800017.v002

ATIS Standard on

NETWORK ATTACHMENT AND INITIALIZATION OF DEVICES AND CLIENT DISCOVERY OF IPTV SERVICES

Secretariat

Alliance for Telecommunications Industry Solutions

Approved March 17, 2009

Abstract

This document specifies the initial set of activities that prepare devices in the consumer domain to receive and consume IPTV services. The document describes the initialization and attachment phases for the Delivery Network Gateway (DNG) and the IPTV Terminal Function (ITF), covering network attachment, service provider discovery, service provider attachment, and services discovery procedures.

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-Chair
S. Wright, ARCH Committee Co-Chair
O. Levin, Technical Editor
M. Midani, Technical Editor
C.A. Underkoffler, ATIS Chief Editor
A. Blasgen, IIF Committee Administrator

CONTRIBUTORS

Gary Hanson, Alcatel-Lucent
Randy Sharpe, Alcatel-Lucent
Rajesh Vale, Alcatel-Lucent
Phyllis Anderson, AT&T
Steven Wright, AT&T
Simon Jones, BT
Nadine Guillaume, Cisco
Mark Watson, Digital Fountain
Mike Dolan, Microsoft
George Foti, Ericsson
Joe Lenart, Hitachi
Scott Shoaf, Juniper Networks
Robert Sprouse, Juniper Networks
Nandhu Nandhakumar, LG Electronics
Orit Levin, Microsoft
James Van Loo, Microsoft
Mowaffak Midani, Motorola
Shan Wey, Nokia Siemens Networks
Kevin Boyle, Nortel
Richard Brand, Nortel
Michael Fargano, Qwest
Jean-Yves Bernard, Rogers Communications
Mark Eyer, Sony
Matthew Goldman, Tandberg Television, part of the Ericsson Group
Bhumip Khasnabish, Verizon
Dan O'Callaghan, Verizon

TABLE OF CONTENTS

1 INTRODUCTION 1

1.1 NETWORK VIEW 1
1.2 ABBREVIATIONS 2

2 REFERENCES 4

3 DNG ATTACHMENT & INITIALIZATION 5

3.1 DNG SETUP AND INITIAL CONFIGURATION (PRE-CONFIGURATION) 5
3.2 DNG NETWORK ATTACHMENT 6

4 OVERVIEW OF ITF DEVICE ATTACHMENT & INITIALIZATION 9

5 ITF DEVICE SETUP & INITIAL CONFIGURATION (PRE-CONFIGURATION) 10

6 ITF DEVICE NETWORK ATTACHMENT 10

6.1 LOCAL DHCP SERVER ON THE DNG 11
6.2 REMOTE DHCP SERVER ACROSS THE NETWORK 12

7 ITF SERVICE PROVIDER DISCOVERY 15

7.1 ALTERNATIVE 1: PRECONFIGURED OR MANUAL SP DISCOVERY METHOD 17
7.2 ALTERNATIVE 2: DHCP-BASED SP DISCOVERY METHOD 17
7.3 ALTERNATIVE 3: DOWNLOAD OF THE DISCOVERY INFORMATION FROM THE NETWORK PROVIDER DOMAIN METHOD 17
7.4 ALTERNATIVE 4: TR-069 PROTOCOL-BASED SP DISCOVERY METHOD 18
7.5 ALTERNATIVE 5: STREAMING OF THE SPS INFORMATION TO A MULTICAST ADDRESS METHOD 18
7.6 ALTERNATIVE 6: IMS-BASED SP DISCOVERY METHOD 18
7.6.1 ITF Authentication & Registration 18

8 ITF ATTACHMENT TO A SERVICE PROVIDER & QUERY OF SPECIFIC SERVERS 19

8.1 THICK & THIN CLIENTS 19
8.2 CLIENT SIGN-ON 20
8.3 ATTACHMENT TO SP BY A THICK CLIENT THROUGH SIGN-ON 21
8.4 ATTACHMENT TO SP BY A THICK CLIENT USING A UNICAST-BASED PULL MECHANISM 22
8.5 ATTACHMENT TO IMS-BASED SP 24
8.5.1 Public Service Identifier (PSI) for Service Provider Attachment 25
8.5.2 Acquiring the Public Service Identifier (PSI) 26

9 ITF SERVICES DISCOVERY & SELECTION 26

9.1 INTRODUCTION TO ITF SERVICES DISCOVERY & BASIC DEFINITIONS 26
9.2 ITF SERVICES DISCOVERY AND SELECTION BY A THICK CLIENT USING A MULTICAST-BASED PUSH MECHANISM 27
9.3 ITF SERVICES DISCOVERY & SELECTION BY A THICK CLIENT USING A UNICAST-BASED PULL MECHANISM 28
9.4 ITF SERVICES DISCOVERY & SELECTION FOR IMS-BASED NETWORKS 29
9.4.1 ITF Services Discovery & Selection using the SIP Notification Framework 30
9.4.2 ITF Services Discovery & Selection using SOAP-based Pull Mechanism with IMS (Thick Client) 30
9.4.3 ITF Services Discovery & Selection using Pull Mechanism utilizing http with IMS (Thin Client) 30
9.4.4 ITF Services Discovery & Selection using Push Mechanism with IMS (Thick Client) 31

10 ITF SERVICE ATTACHMENT 31

A DHCP CONFORMANCE FOR IPTV DEVICES IN THE CONSUMER DOMAIN 32

A.1 INTRODUCTION TO DHCP 32
A.2 DHCP MESSAGE CONFORMANCE [NORMATIVE] 32
A.3 DHCP OPTIONS LIST [INFORMATIVE] 33
A.4 DHCP OPTIONS SENT FROM THE DHCP CLIENT TO THE DHCP SERVER [NORMATIVE] 41
A.5 DHCP OPTIONS SENT FROM THE DHCP SERVER TO THE DHCP CLIENT [NORMATIVE] 42
A.6 DHCP REFERENCES 44
A.6.1 Normative References 44
A.6.2 Informative References 44

B DNG BORDER FUNCTIONS 46

B.1 DNG FUNCTION REQUIREMENTS 46
B.2 NON-MANDATORY REQUIREMENTS FOR DNG FUNCTIONS 47

B.3 M-DNG AND S-DNG INTERFACE REQUIREMENTS 49
B.4 REFERENCES 50

C ALTERNATIVE METHOD FOR SERVICE PROVIDER DISCOVERY USING DHCP CONTAINER OPTION 51

C.1 INTRODUCTION AND MOTIVATION 51
C.2 METHOD 51
C.3 ILLUSTRATION OF THE CONTAINER OPTION IN THE CONTEXT OF IPTV 51

D DEVICE & USER AUTHENTICATION 56

D.1 AUTHENTICATION TYPES DEFINITION 56
D.1.1 Access Level Authentication 56
D.1.2 Service Level Authentication 56
D.1.3 Implicit Authentication 56
D.1.4 Explicit Authentication 56
D.2 DNG AUTHENTICATION 56
D.3 ITF DEVICE AUTHENTICATION 57
D.4 ITF USER AUTHENTICATION 57
D.4.1 Using Provider NGN Authentication 57
D.4.2 Using Application Server Integrated Authentication 58

E SIGN-ON DURING DHCP-BASED ATTACHMENT 60

E.1 REFERENCES: 61

F GBA ARCHITECTURE & SINGLE SIGN-ON OVERVIEW 62

G DETAILED IMS EXAMPLE 64

G.1 APPLICATION SERVER REGISTRATION WITH IMS 64
G.2 SUBSCRIBER PROVISIONING ON IMS 64
G.3 SUBSCRIBER SIP REGISTRATION 64
G.4 CONTENT CATALOGUE RETRIEVAL 65

H POTENTIAL OPTIMIZATIONS FOR SUBSCRIBE/NOTIFY SIGNALING EVENT PACKAGE 67

I ITF SERVICES DISCOVERY & SELECTION BY A THICK CLIENT USING A MULTICAST-BASED PUSH MECHANISM 68

TABLE OF FIGURES

FIGURE 1: NETWORK VIEW 1
FIGURE 2: DNG NETWORK ATTACHMENT 6
FIGURE 3: PHASES OF ITF DEVICE ATTACHMENT & INITIALIZATION SEQUENCE 9
FIGURE 4: ITF DEVICE NETWORK ATTACHMENT WITH A LOCAL DHCP SERVER IN THE DNG 12
FIGURE 5: ITF DEVICE NETWORK ATTACHMENT WITH A REMOTE DHCP SERVER 13
FIGURE 6: SERVICE PROVIDER DISCOVERY PROCEDURES SUMMARY 17
FIGURE 7: ITF AUTHENTICATION AND REGISTRATION STEPS 19
FIGURE 8: ATTACHMENT TO A SERVICE PROVIDER THROUGH SIGN-ON 22
FIGURE 9: ATTACHMENT TO A SERVICE PROVIDER USING A PULL MECHANISM 24
FIGURE 10: SERVICES DISCOVERY AND SELECTION USING A MULTICAST-BASED PUSH MECHANISM 27
FIGURE 11: SERVICES DISCOVERY AND SELECTION USING A PULL MECHANISM 28
FIGURE 12: IMS-BASED ATTACHMENT TO A SERVICE DISCOVERY AS, GENERIC SERVICE INFORMATION DATA RETRIEVAL AND SERVICE DISCOVERY EXAMPLE 29

FIGURE B.1 : POSSIBLE FUNCTIONAL ENTITIES (FES) IN A DNG 46

FIGURE C.1 : POSSIBLE FUNCTIONAL ENTITIES (FES) IN A DNG 52
FIGURE C.2: POSSIBLE FUNCTIONAL ENTITIES (FES) IN A DNG 53
FIGURE C.3: POSSIBLE FUNCTIONAL ENTITIES (FES) IN A DNG 54
FIGURE C.4: POSSIBLE FUNCTIONAL ENTITIES (FES) IN A DNG 55

FIGURE D.1 : PROVIDER AUTHENTICATION FOR ALL THREE MODES 58
FIGURE D.2: AS-INTEGRATED AUTHENTICATION 59

FIGURE E.1 : AUTHENTICATION OPTIONS 60

FIGURE F.1 : BOOTSTRAPPING PROCEDURE 63

FIGURE G.1 : IPTV CLIENT REGISTRATION 65
FIGURE G.2: IPTV THIN CLIENT CONTENT CATALOG RETRIEVAL 66

FIGURE I.1 : SIGNALING FLOWS HIERARCHICAL CLASSIFICATION 69
FIGURE I.2: ITF SERVICES DISCOVERY AND SELECTION FLOW 71

TABLE OF TABLES

TABLE A.1 : DHCP MESSAGES 32
TABLE A.2: DHCP OPTIONS LIST PER IETF SPECIFICATIONS 33
TABLE A.3: MANDATORY DHCP CLIENT OPTIONS 42
TABLE A.4: MANDATORY DHCP SERVER OPTIONS 42

TABLE B.1 : FEATURES REQUIRED IN M-DNG 47
TABLE B.2: FEATURES REQUIRED IN S-DNG 47
TABLE B.3: OPTIONAL FEATURES OF M-DNG 48
TABLE B.4: OPTIONAL FEATURES OF S-SDNG 48

ATIS Standard on –

Network Attachment and Initialization of Devices and Client Discovery of IPTV Services

1 INTRODUCTION

This document specifies the initial set of activities that prepare devices in the consumer domain to receive and consume IPTV services. The document describes the initialization and attachment phases for the Delivery Network Gateway (DNG) and the IPTV Terminal Function (ITF), covering network attachment, service provider discovery, service provider attachment, and services discovery procedures.

1.1 Network View

Figure 1 below depicts a simplified view of the IPTV network where only the devices, systems, and components that participate in the initialization and attachment functions are shown. These devices, systems, and components are positioned within their corresponding logical domains, per previous IIF specifications. The Domain Name Server (DNS) function/server, however, could reside in either the Network Provider domain or the Service Provider domain, so it is shown to overlap the two domains in the figure.

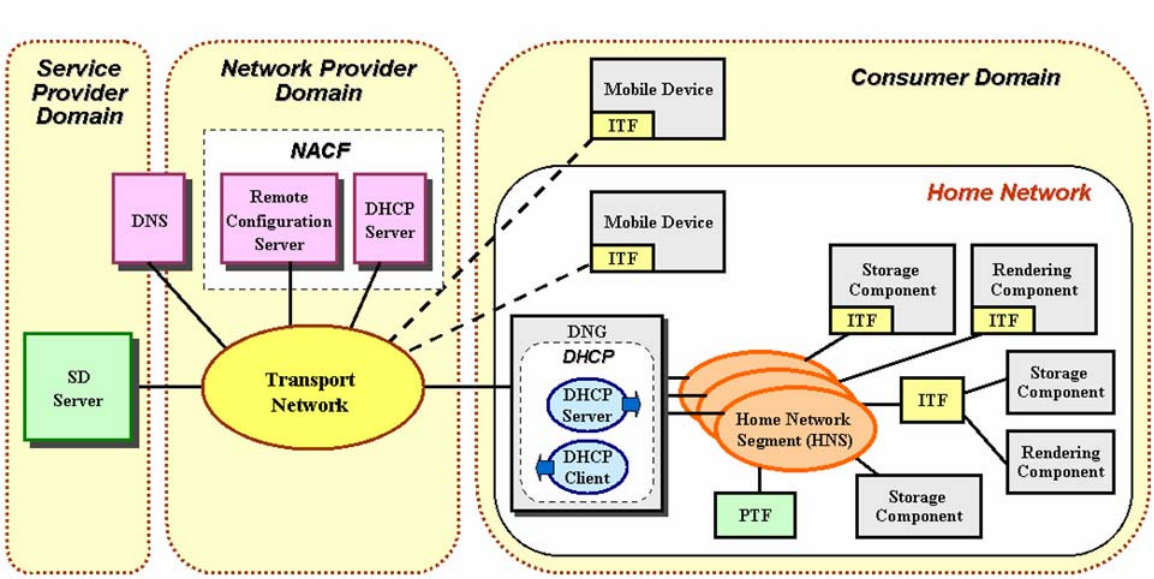

Figure 1: Network View

There are at least two types of devices in the consumer domain that need to attach to the network to establish IP layer connectivity, over which management, control, and user plane data can flow. The two types of devices are 1) *Delivery Network Gateways (DNG)* and 2) *IPTV Terminal Function (ITF) devices*.

An ITF device is a device that implements the ITF such as a set-top box. The term ITF is used to describe IPTV terminal functionality regardless of its physical embodiment. The term "ITF device" will be used when referring to a physical device.

The DNG can contain a Dynamic Host Configuration Protocol (DHCP) subsystem with two components:

1) DHCP server toward the home network and the ITF devices.
2) DHCP client toward the access network.

A detailed description of these functions is provided in subsequent sections.

In turn, there are two cases for ITF device attachment to the network. The first is the case where the ITF device resides behind the DNG, and the second is the case where the ITF resides on a mobile device and is attaching to the network without passing through the DNG.

The following procedures are within the scope of this document:

a) DNG initialization and attachment to the network.
b) Initialization and attachment for an ITF device (wired or wireless) residing behind the DNG.
c) Initialization and attachment for a mobile ITF device bypassing the DNG.

Procedure "a" will be covered in section 3 of this document, procedure "b" will be covered in section 4 of this document, and procedure "c" will be covered in future releases of this document.

It is assumed that the DNG and ITF devices pass one or more authentication phases described in Appendix D and Appendix F during the device initialization procedure described in sections 3 and 4 of this document.

1.2 Abbreviations

Abbreviation	Expansion
3GPP	3rd Generation Partnership Project
ACS	Automatic Configuration Server
AKA	Authentication and Key Agreement
AS	Application Server
B2BUA	Back-to-Back User Agent
BOOTP	Bootstrap Protocol
BSF	Bootstrap Server Function
CA	Conditional Access
CAC	Connection Admission Control
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DoS	Denial of Service
DRM	Digital Rights Management
DSCP	Differentiated Service Code Point

Abbreviation	Expansion
DSP	Digital Signal Processing
DTMF	Dual Tone Multi-Frequency
DVR	Digital Video Recorder
EAP	Extensible Authentication Protocol
EAS	Emergency Alert Service
EPG	Electronic Program Guide
FLUTE	FiLe delivery over Unidirectional Transport
FQDN	Fully Qualified Domain Name
FW/NAT	Firewall / Network Address Translation
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GUP	Generic User Profile
HD	High Definition
HFC	Hybrid Fiber Coax
HNS	Home Network Segment
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
IANA	Internet Assigned Numbers Authority
I-CSCF	Intermediate-Call Session Control Function
IGMP	Internet Group management Protocol
IIF	IPTV Interoperability Forum
IMS	IP Multimedia System
IPTV	Internet Protocol TeleVision
ISIM	IMS Identity Module
LAN	Local Area Network
M-DNG	Media - Delivery Network Gateway
MTF	Multicast Transport Function
NACF	Network Access Control Function
NAPT	Network Address and Protocol Translation
NASS	Network Attachment Sub System
NE	Network Element
NGN	Next Generation Network
NP	Network Provider
OTA	Over The Air
PANA	Protocol for carrying Authentication for Network Access
PCON	Parental Control
P-CSCF	Proxy-Call Session Control Function
PKI	Public Key Infrastructure
PON	Passive Optical network
PSI	Public Service Identifier
QoS	Quality of Service

Abbreviation	Expansion
RACF	Resource Admission Control Function
RCMS	Remote Configuration and Management Server
RPC	Remote Procedure Call
RTSP	Real Time Streaming Protocol
S-CSCF	Serving-Call Session Control Function
SCF	Session Control Function
SD	Service Discovery
SD	Standard Definition
SDAS	Service Discovery Application Server
S-DNG	Signaling - Delivery Network Gateway
SI	System Information
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SP	Service Provider
SPID	Service Provider Identifier
Srce	Source
SRV	SeRVice record (see DNS)
Srvr	Server
SSM	Source Specific Multicast
STB	Set Top Box
TLS	Transport Layer Security
UDDI	Universal Description Discovery and Integration
UE	User Element
UPSF	User Profile Service Function
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
WS	Web Services
WSDL	Web Services Description Language
XML	eXtensible Markup Language

2 REFERENCES

[1] 3GPP TS 23.218, *IP Multimedia (IM) session handling; IM call model; Stage 2*, V8.1.0, 2008.[1]

[2] 3GPP TS 23.228, *IP Multimedia Subsystem (IMS); Stage 2*, V8.4.0, 2008. [1]

[1] This document is available from the Third Generation Partnership Project (3GPP) at < http://www.3gpp.org/specs/specs.htm >.

[3] 3GPP TS 24.229, *Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3*, V8.3.0, 2008.[1]

[4] 3GPP TS 29.228, *IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents*, V8.1.0, 2008. [1]

[5] 3GPP TS 33.203, *3G Security; Access Security for IP-based services*, V8.2.0, 2008. [1]

[6] 3GPP TS 33.220, *Generic Authentication Architecture (GAA); Generic bootstrapping architecture*, V8.3.0, 2008. [1]

[7] ATIS-0800002, *IPTV Architecture Requirements*, 2006.[2]

[8] ATIS-0800003, *IPTV Architecture Roadmap*, 2006.[2]

[9] ATIS-0800007, *IPTV High Level Architecture*, 2007. [2]

[10] ATIS-0800009, *Remote Management of Devices in the Consumer Domain for IPTV Services*, 2008. [2]

[11] ATIS-0800013, *Media Protocols Specification*, work in progress. [2]

[12] ATIS-0800020, *IPTV EPG Metadata Specification*, 2008. [2]

[13] ATIS-0800022, *Consumer Domain Device Configuration Metadata*, work in progress. [2]

[14] Broadband Forum TR-069, *CPE WAN Management Protocol v1.1*, Issue 1 Amendment 2, 2007.[3]

[15] Broadband Forum TR-101, *Migration to Ethernet Based DSL Aggregation*, 2006.[3]

[16] IETF RFC 1884, *IP Version 6 Addressing Architecture*, 1995.[4]

[17] IETF RFC 2131, *Dynamic Host Configuration Protocol*, 1997.[4]

[18] IETF RFC 2132, *DHCP Options and BOOTP Vendor Extensions*, 1997. [4]

[19] IETF RFC 2365, *Administratively-Scoped IP Multicast*, 1998. [4]

[20] IETF RFC 2782, *A DNS RR for specifying the location of services (DNS SRV)*, 2000. [4]

[21] IETF RFC 3265, *Session Initiation Protocol (SIP)-Specific Event Notification*, 2002. [4]

3 DNG ATTACHMENT & INITIALIZATION

The DNG could be a Layer 2 or a Layer 3 device. In either case, the DNG *shall* have its own IP address so it can be addressable by the network for device management purposes. When operating as a Layer 3 device, the DNG generally provides routing, QoS, firewall, NAT, policy enforcement, DHCP Server, and other border functions for the home network. This section details how the DNG initializes and attaches to the service provider network. For additional details on the border function requirements of a DNG, see Appendix B.

3.1 DNG Setup and Initial Configuration (Pre-Configuration)

In some network deployments, the DNG is *pre-configured* with all or part of the network attachment information. For example, a DNG could use the procedure described below to get its own IP address, and then proceed directly to communicate with a Remote Configuration and Management Server

[2] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

[3] This document is available from the Broadband Forum. < http://www.broadband-forum.org >

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

(RCMS) based on hard-coded addressing information, or based on plug-in methods (such as smart card).

3.2 DNG Network Attachment

DNG network attachment refers to the activities associated with the DNG establishing Layer 3 connectivity to an IP network. Once the network attachment activities have been completed, the DNG will be capable of transmitting and receiving IP packets and establishing a management session with an RCMS. Subsequently, the RCMS is used to provision the DNG with access-network specific parameters.

This specification document uses DHCP as a mechanism for network attachment. Using this protocol, the DNG acquires its WAN IP address, and can also learn the address of the RCMS. Figure 2 below shows the sequence of events that take place when the DNG is powered up or initialized.

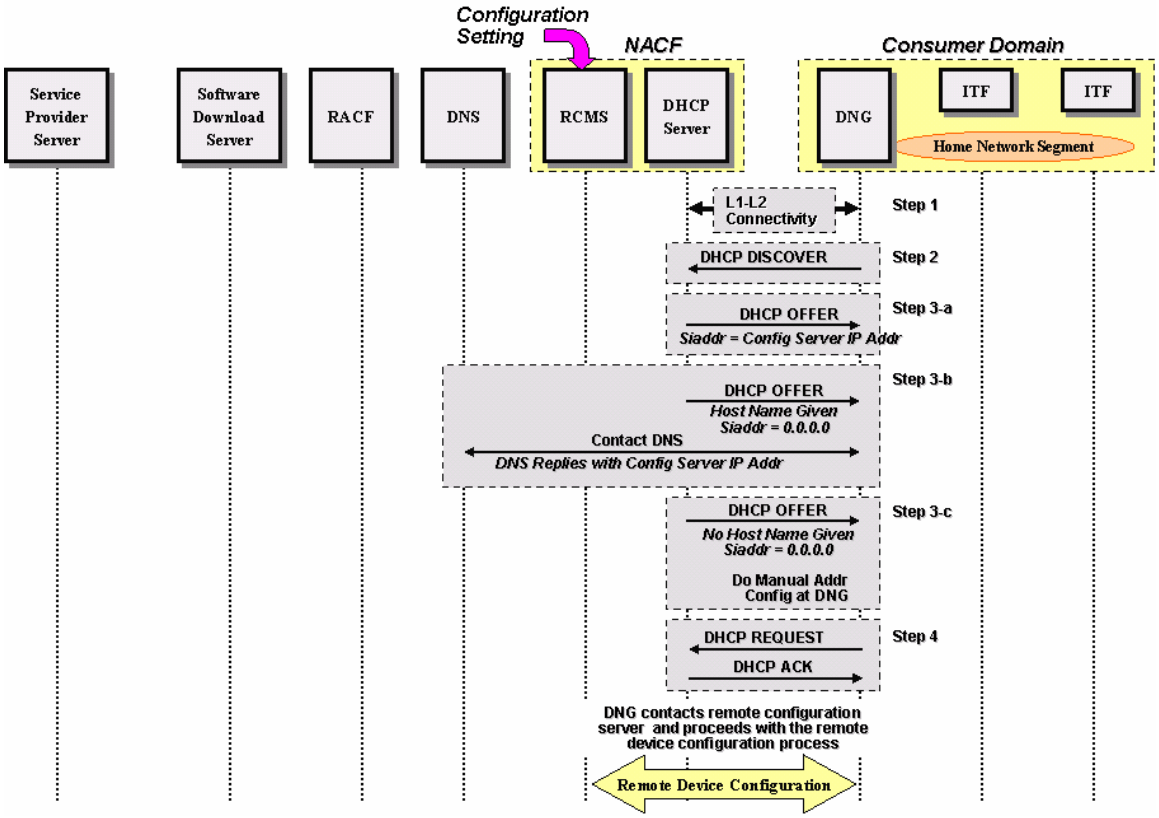

Figure 2: DNG Network Attachment

NOTE -- The DNS operation, if executed per step 3-b, is asynchronous with the completion of the DHCP REQUEST and ACK messages: that is, the DNG may chose to complete the entire DHCP DISCOVER-OFFER-REQUEST-ACK sequence and then perform the DNS operation.

Specifically, the following procedure takes place:

1) *The DNG establishes L1 and L2 connectivity with the network*. The specific steps depend on the type of the access network (DSL, PON, HFC, or Wireless) and are beyond the scope of this document. It could be assumed that the L1 and L2 connectivity procedure and/or associated authentication mechanism collects and stores in the network unique information associated with a physical DNG such as the DNG MAC address, DNG ID, or DNG Certificate and Access Port (in case of DSL

access). This information could be made available for use in future authentication process by various network entities.

2) *The DNG issues a DHCP DISCOVER message toward the network that* ***shall*** *include all the mandatory DHCP client options, as specified in Table A.3 in Appendix A*. An intermediate DHCP relay, if used, *may* also insert additional options such as DHCP Option 82, per Broadband Forum TR-101.

   If the DNG device were to support the Container Option[5], it would request it in Option 55 (parameter request list). This would be performed in step 2 in the figure above.

3) *The network provider DHCP server replies to the DNG with a DHCP OFFER message that* ***shall*** *include all the mandatory DHCP server options, as specified in Table A.4 in Appendix A*. The DHCP server *shall* provide the following information to the DNG:

   a) DNG WAN IP address in the "yiaddr" field of the DHCP OFFER message.
   b) DNG WAN IP address in the "yiaddr" field of the DHCP OFFER message.
   c) DNG network subnet mask, in the subnet mask Option 1.
   d) DNS Server IP address(es) in the DNS Option 6.
   e) Default gateway IP address in the Default Router Option 3.
   f) The Container Option, if requested in Option 55 (step 2 above) and configured by the network provider, to convey other options to the ITF device.
   g) The RCMS addressing information, in the "siaddr" field of the DHCP OFFER message.

There are three possibilities based on the value returned in the "siaddr" field at this point:

a) If the DHCP server is provisioned with the RCMS IP address, then it *shall* include it in the "siaddr" field of the OFFER message. This is shown as step 3-a in the figure above.

   Since a complete RCMS URL is required per TR-069 specifications to reach the RCMS, the DNG shall construct the RCMS URL based on the following URL syntax:

   URL = protocol://host:port/path

   Where:

   - The "protocol" could be "http" or "https".
   - The "host" portion of the URL may be in general the IP address or the Fully Qualified Domain Name (FQDN[6]) of the RCMS, and in this case it is the RCMS IP address that is included in the "siaddr" field of the OFFER message.
   - The "path" could be the default path '/'.

   In this specification document, the DNG *shall* assume that the RCMS is deployed under the default path '/' and *shall* construct the RCMS URL as follows:

   RCMS URL = http(s)://ip:port/.

[5] See Appendix C for more details.

[6] FQDN is the complete absolute (not relative) domain name for a specific computer or host on the Internet. The FQDN consists of two parts: the hostname and the domain name. For example, an FQDN for a hypothetical mail server might be mymail.somecollege.edu. The hostname is mymail, and the host is located within the domain somecollege.edu.

In this specification document, the DNG SHALL assume that the RCMS is deployed under the default TR-069 port number 7547, and SHALL construct the RCMS URL as follows:

RCMS URL = http://ip:7547/. (for the http protocol)

or

RCMS URL = https://ip:7547/. (for the https protocol)

To resolve the two protocols issue, the DNG *shall* attempt to contact the RCMS using https protocol first, then attempt the http protocol if the first attempt fails.

b) If the DHCP server is provisioned with the RCMS FQDN but not with the RCMS IP address, then it *shall* set siaddr = 0.0.0.0 and provide the DNG with the RCMS FQDN using one of the following three DHCP options:
   1) Option 43 with a complete RCMS URL per TR-069 specification
   2) Option 43 with an RCMS FQDN, as specified in Appendix A, Table A.4.
   3) Option 15, as extended by the ATIS IIF, in Appendix A, Table A.4, use case b.

In case 1 the URL is provided, and can be used directly by the DNG to contact the RCMS.

In case 2 or case 3, the DNG can construct the RCMS URL from the FQDN as follows:

RCMS URL = http(s)://FQDN:7547/.

Or can perform a DNS query first to obtain the RCMS IP address, and then construct the RCMS URL from the IP address, as follows:

RCMS URL = http(s)://ip:7547/.

Option 43 takes precedence over Option 15 for the RCMS FQDN case. That is, if Option 43 (with an RCMS FQDN) and Option 15 are both received, then the client *shall* use the RCMS FQDN specified in Option 43. Please refer to the DHCP conformance table in Appendix A for more details.

The DNG *shall* interact with the DNS to resolve the RCMS IP address. This is shown as step 3-b in the figure above.

c) If the DHCP server is not provisioned with the RCMS address information (IP address or FQDN) and therefore does not provide the RCMS IP address or its FQDN, then there *shall* be a mechanism in place to allow the end user to manually configure the DNG. This is shown as step 3-c in the figure above.

4) *The DHCP protocol sequence completes with the standard DHCP REQUEST and DHCP ACK messages.*

NOTE -- It is possible for the DNG DHCP client to request additional information from the DHCP server across the network via the use of the DHCP INFORM operation as described in RFC 2131. The DHCP INFORM operation, which usually includes the parameter list Option 55, can be invoked by a DHCP client at any time to request configuration information from the DHCP server.

After acquiring the IP address of the RCMS, the DNG interacts with the RCMS to acquire needed configuration parameters, per ATIS-0800009, *Remote Configuration of Devices in the Consumer Domain for IPTV Services*.

NOTE -- The RCMS discovered in any of the previous steps could be designated by the network provider as the initial RCMS. Consequently, and per TR-069 specifications, this discovered RCMS, upon its first contact with the DNG, can set the following element in the DNG data model:

InternetGatewayDevice.ManagementServer.URL

to re-direct it to its operational RCMS. From that point on the DNG interacts with the RCMS based on the URL specified by this object.

4 Overview of ITF Device Attachment & Initialization

This procedure is comprised of six high level functional steps (or phases) listed below:

0. Setup and pre-configuration phase.
1. Network attachment phase.
2. Service provider discovery phase.
3. Service provider attachment phase and query of specific servers.
4. Services discovery and selection phase.
5. Service attachment (and operation) phase.

Phase 0 is the basic setup and pre-configuration phase described in section 5. Phases 1 to 5 are depicted in Figure 3, and are covered in sections 6 to 10 of this specification document.

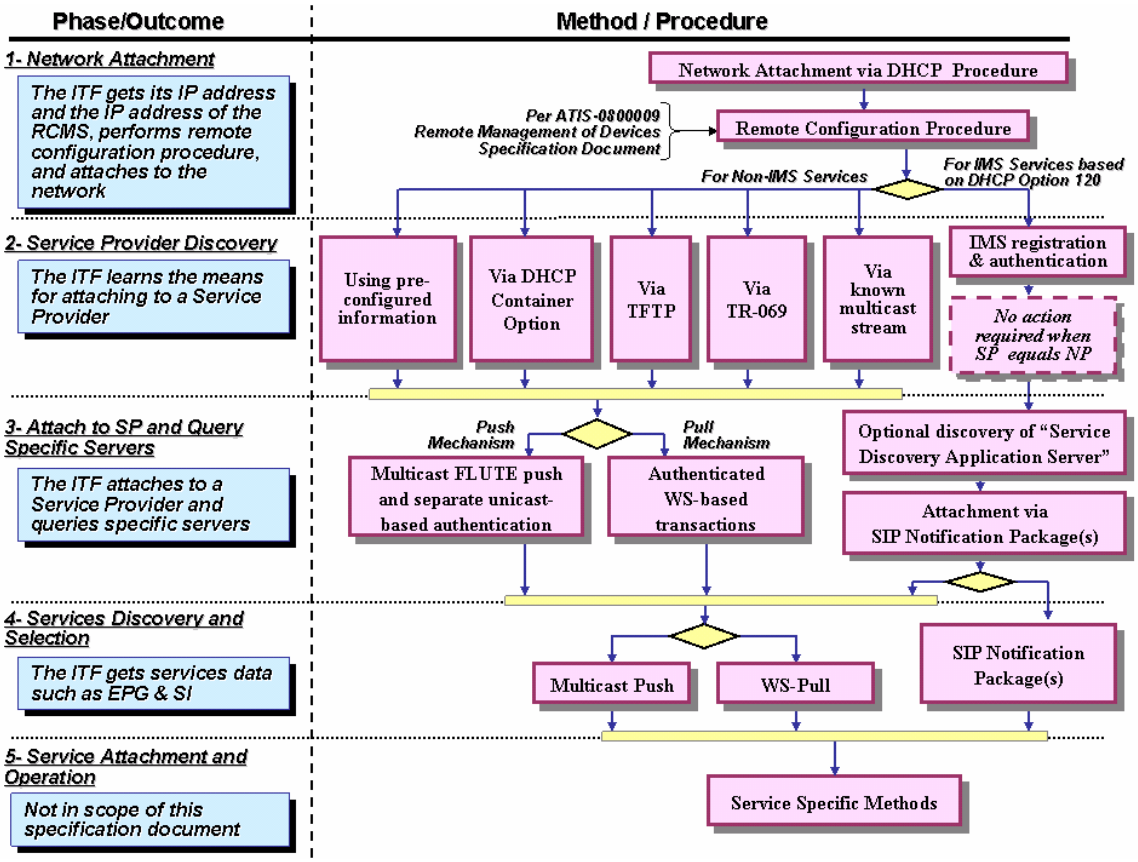

Figure 3: Phases of ITF Device Attachment & Initialization Sequence

In order to receive and consume an IPTV service, it is necessary to perform each one of the specified steps. Nevertheless, this specification identifies multiple alternatives for implementing each of the identified steps, so that succeeding at one of them will satisfy the functional requirement.

This document does not specify the order in which the listed alternatives within a phase can be attempted. It *shall* be possible to configure and manage the activation logic in order to meet various deployment models.

5 ITF DEVICE SETUP & INITIAL CONFIGURATION (PRE-CONFIGURATION)

ITF device setup and initial configuration phase (identified as phase 0 above) refers to the pre-configuration information related to acquiring and configuring a physical ITF device. The initial device configuration *may* be performed at manufacturing time or manually entered by the user. The completion of this phase is prerequisite for other phases in the overall ITF initialization and attachment sequence.

For an ITF to properly function in different environments, its setup and pre-configuration phase provides means for determining the following:

- The identity and authentication credentials to be established for the ITF. *Identity credentials* are data elements maintained on the ITF that are used to identify the ITF device.
- Service provider(s) identities and any additional information necessary for establishing a service account with one or more service providers.
- Other device and service options.

Note that the mechanisms for implementing the ITF setup and pre-configuration procedure are outside the scope of the ATIS IIF. However, the data elements, such as identity and authentication credentials and their default values, are in scope for the ATIS IIF.

6 ITF DEVICE NETWORK ATTACHMENT

ITF device network attachment refers to the activities associated with the ITF device establishing Layer 3 connectivity to an IP network and obtaining network configuration data.

During the network attachment phase the following information *may* be obtained or otherwise established by the ITF device:

- IPv4 or v6 address, network mask, default route.
- DNS server(s), local network domain name, SIP proxies, etc.

Once network attachment activities have been completed, the ITF device will be capable of transmitting and receiving IP packets and establishing a management session with the RCMS. This specification document uses DHCP as a mechanism for network attachment.

The profiles and the details for each of the mechanisms as applicable for various IPTV use cases are described in the following sections.

There are two cases to consider for ITF attachment to the network:

1) The DNG supports DHCP server capability and thus acts as the network DHCP server for the ITF devices on the home network.
2) The DNG passes DHCP messages through transparently.

Note that while the second case can still be found in today's deployments, home networks are moving toward self-contained IP domains, with the network DHCP server located in the DNG.

6.1 Local DHCP Server on the DNG

In this case, it is assumed that the DNG has already attached to the network and acquired its Layer 3 networking information. The following sequence takes place when an ITF device is powered up or initialized:

1) The ITF device establishes Layer 1 and Layer 2 connectivity with the DNG across the home network, which could be over a copper network, a coaxial network, fiber network, or wireless network.
2) The ITF device issues a DHCP DISCOVER message toward the DNG that *shall* include all mandatory DHCP client options, as specified in Table A.3 in Appendix A. This includes Option 60 to allow it to identify itself to the DNG.

If the ITF device were to support the option(s)[7] carried in the Container Option, it would request those options in DHCP Option 55.

3) The DNG, as a DHCP server, replies to the ITF device with a DHCP OFFER message that *shall* include all mandatory DHCP server options, as specified in Table A.4 in Appendix A. The DNG *shall* provide the following information to the ITF device:
    a) ITF device IP address in the "yiaddr" field of the DHCP OFFER message.
    b) ITF device network mask in the subnet mask Option 1.
    c) DNS server IP address(es) in the DNS Option 6.
    d) RCMS IP address (same as the one assigned to the DNG) in the "siaddr" field of the DHCP OFFER message.
    e) Default gateway IP address in the "Default Router" Option 3.
    f) If configured, the DHCP options requested in step 2 above (carried in the Container Option) to convey specific information to the ITF, such as Service Provider Discovery information.
4) The ITF device continues the DHCP message exchange with the standard DHCP REQUEST message.
5) The DNG completes the DHCP message exchange with the standard DHCP ACK message sent to the ITF device.

At the end of the DHCP sequence, and in the cases when the DNG does not provide the ITF with the RCMS IP address or when the ITF wishes to discover its own RCMS, one of the following can take place:

- The ITF device can issue a DNS query to discover the IP address of its RCMS, assuming that the ITF was pre-provisioned with the RCMS FQDN.

[7] See Appendix C for more details.

- The ITF device can be configured locally with RCMS addressing information.
- ITF device can obtain the configuration information from its Service Provider (during *Attachment to SP* phase in section 8).

The flow is shown in Figure 4 below.

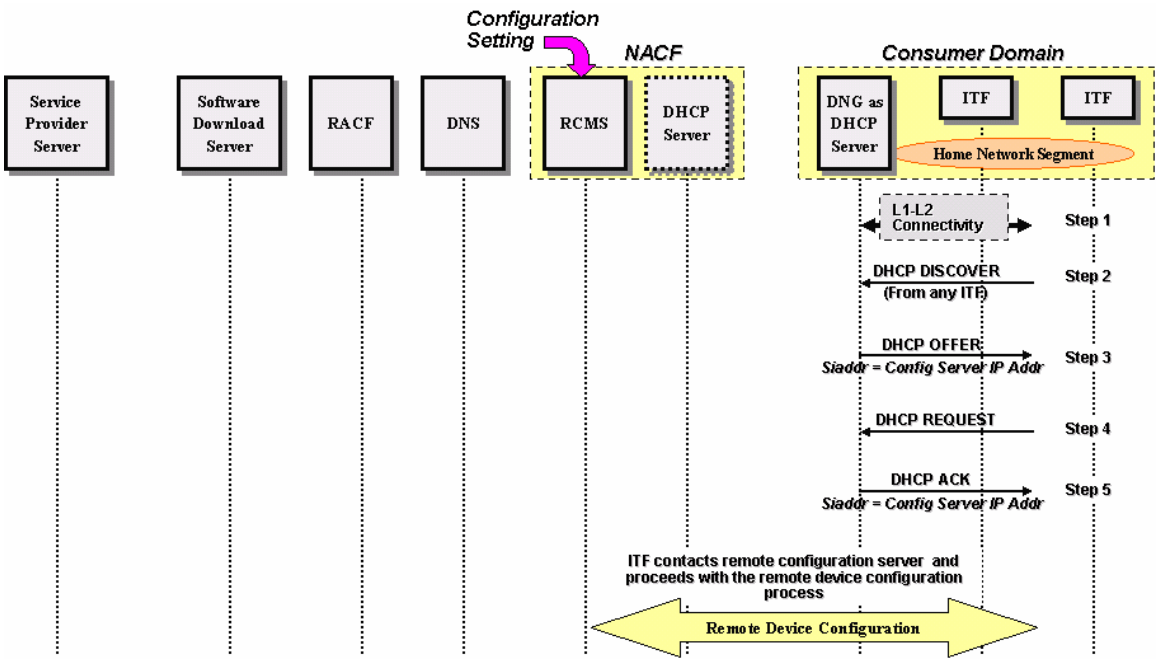

Figure 4: ITF Device Network Attachment with a Local DHCP Server in the DNG

After acquiring the IP address of the RCMS, the ITF device interacts with the RCMS to acquire needed configuration parameters, per ATIS-0800009, *Remote Configuration of Devices in the Consumer Domain for IPTV Services*.

6.2 Remote DHCP Server across the network

In this case, the DNG passes all DHCP messages transparently to the network. As the DHCP messages pass transparently through the DNG, the DHCP messages shall not be altered by the DNG in any way. Depending on the access network technology, the DHCP messages/packets may be encapsulated, but this is outside the scope of this document.

Figure 5 shows the sequence of events that take place when the ITF device is powered up or initialized.

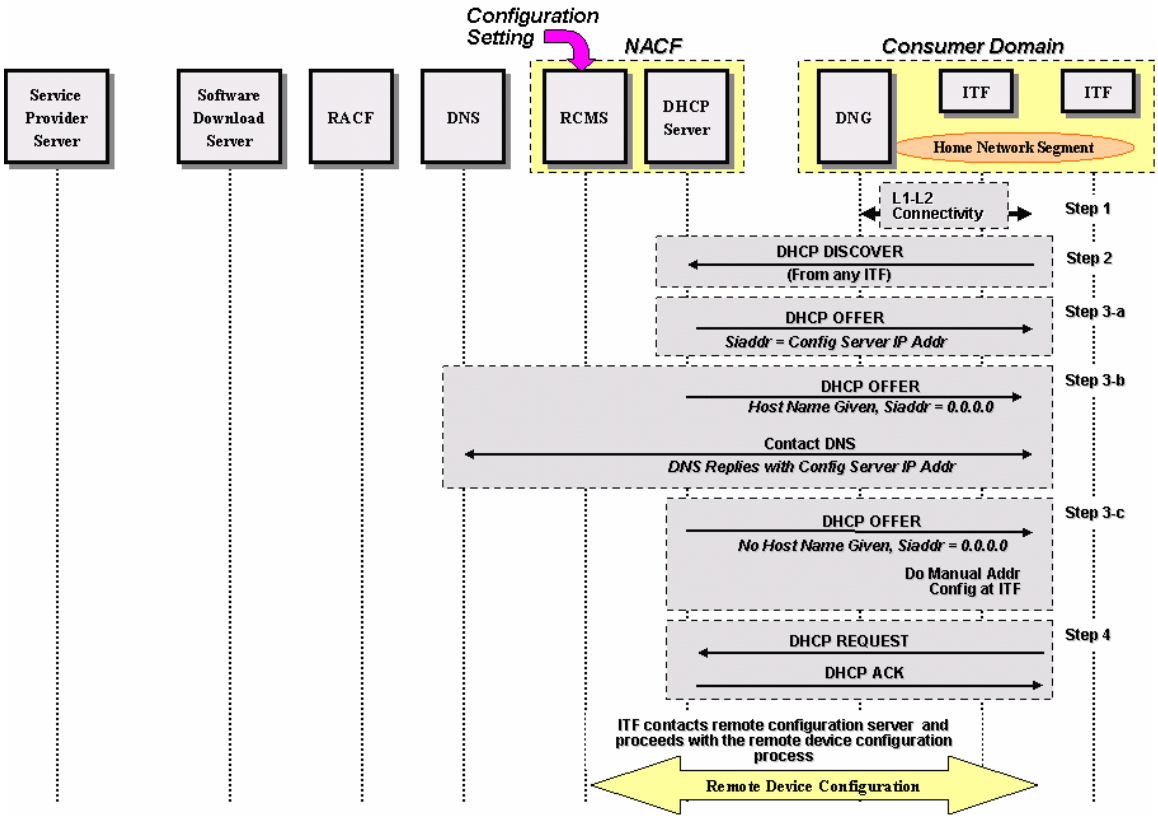

Figure 5: ITF Device Network Attachment with a Remote DHCP Server

NOTE -- The DNS operation, if executed per step 3-b, is asynchronous with the completion of the DHCP REQUEST and ACK messages; that is, the ITF device may chose to complete the entire DHCP DISCOVER-OFFER-REQUEST-ACK sequence and then perform the DNS operation.

Specifically, the following takes place:

1) The ITF device establishes Layer 1 and Layer 2 connectivity with the DNG across the home network, which could be a copper network, coaxial network, fiber network, or wireless network.

2) The ITF device issues a DHCP DISCOVER message toward the DNG that *shall* include all mandatory DHCP client options, as specified in Table A.3 in Appendix A. The ITF device *shall* also include Option 60 to allow it to identify itself to the network. The DNG passes this DISCOVER message to the core/access network transparently.

3) The network provider DHCP server replies to the ITF device with a DHCP OFFER message that *shall* include all mandatory DHCP server options, as specified in Table A.4 in Appendix A. The DHCP server *shall* provide the following information to the ITF device:

   a) ITF device IP address in the "yiaddr" field of the DHCP OFFER message.
   b) ITF device network mask in the subnet mask Option 1.
   c) DNS Server IP address(es) in the DNS Option 6.
   d) If available, the RCMS IP address in the "siaddr" field of the DHCP OFFER message.
   e) Default gateway IP address in the Default Router Option 3.

The DNG *shall* pass the DHCP OFFER message to the ITF device transparently.

There are three possibilities at this point reflected in the content of the DHCP OFFER message:

a) If the DHCP server is provisioned with the RCMS IP address, then it *shall* include it in the siaddr field of the OFFER message. This is shown as step 3-a in the figure above.

   Since a complete RCMS URL is required per TR-069 specifications to reach the RCMS, the ITF device shall construct the RCMS URL based on the following URL syntax:

   URL = protocol://host:port/path

   where,

   - The "protocol" could be "http" or "https"
   - The "host" portion of the URL may be the IP address or the FQDN of the RCMS, and in this case it is the RCMS IP address that is included in the "siaddr" field of the OFFER message.
   - The "path" could be the default path '/'

   In this specification document, the ITF device *shall* assume that the RCMS is deployed under the default path '/' and SHALL construct the RCMS URL as follows:

   RCMS URL = http(s)://ip:port/.

   In this specification document, the ITF device *shall* assume that the RCMS is deployed under the default TR-069 port number 7547, and *shall* construct the RCMS URL as follows:

   RCMS URL = http://ip:7547/. (for the http protocol)

   or

   RCMS URL = https://ip:7547/. (for the https protocol)

   To resolve the two protocols issue, the ITF device *shall* attempt to contact the RCMS using https protocol first, then attempt the http protocol if the first attempt fails.

b) If the DHCP server is provisioned with the RCMS FQDN but not with the RCMS IP address, then it *shall* set siaddr = 0.0.0.0 and provide the ITF with the RCMS FQDN using one of the following three options:

   1) Option 43 with a complete RCMS URL per TR-069 specification
   2) Option 43 with an RCMS FQDN, as specified in Appendix A, Table A.4.
   3) Option 15, as extended by the ATIS IIF, in Appendix A, Table A.4, use case b.

   In case 1 the URL is provided, and can be used directly by the ITF device to contact the RCMS.

   In case 2 or case 3, the ITF device can construct the RCMS URL from the FQDN as follows:

   RCMS URL = http(s)://FQDN:7547/.

   or can perform a DNS query first to obtain the RCMS IP address, and then construct the RCMS URL from the IP address, as follows:

   RCMS URL = http(s)://ip:7547/.

   Option 43 takes precedence over Option 15 for the RCMS FQDN case. That is, if Option 43 (with an RCMS FQDN) and Option 15 are both received, then the client *shall* use the RCMS FQDN

specified in Option 43. Please refer to the DHCP conformance table in Appendix A for more details.

The ITF device *shall* interact with the DNS to resolve the RCMS IP address. This is shown as step 3-b in Figure 5 above.

c) If the DHCP server is not provisioned with the RCMS address information (IP address or FQDN) and therefore does not provide the RCMS IP address or its FQDN, then there *shall* be a mechanism in place to allow the end user to manually configure the ITF device, or the ITF device can obtain the configuration information directly from its Service Provider during the *Attachment to SP* phase, per section 8.

4) The DHCP protocol sequence completes with the standard DHCP REQUEST and DHCP ACK messages.

Note -- It is possible for the ITF device DHCP client to request additional information from the DHCP server via the use of the DHCP INFORM operation as described in RFC 2131. The DHCP INFORM operation, which usually includes the parameter list Option 55, can be invoked by a DHCP client at any time to request configuration information from the DHCP server.

After acquiring the IP address of the RCMS, the ITF device interacts with the RCMS to acquire needed configuration parameters, per ATIS-0800009, *Remote Configuration of Devices in the Consumer Domain for IPTV Services*.

NOTE -- The RCMS discovered in any of the previous steps could be designated by the network provider as the initial RCMS. Consequently, and per TR-069 specifications, this discovered RCMS, upon its first contact with the ITF device, can set the following element in the ITF device data model:

Device.ManagementServer.URL

to re-direct it to its operational RCMS. From that point on the ITF device interacts with the RCMS based on the URL specified by this object.

7 ITF SERVICE PROVIDER DISCOVERY

Service Provider (SP) Discovery is the process by which an ITF becomes aware of the available IPTV Service Provider(s), and learns the means for attaching to a Service Provider over a secure managed network.

The list of one or more Service Provider(s) available to the consumer is offered by the Network Provider (NP). The information will be represented in the manner appropriate for each service discovery method.

Six Service Provider Discovery methods are defined in this section. The discovery methods differ in the number of steps to be performed by an ITF to obtain the SPs' information. A method can obtain the Service Provider discovery information directly in a single step or indirectly by first obtaining a pointer to the information and then obtaining the information. The details are described in the sections below.

Each method concludes with the ITF obtaining the following information for each service provider:

- Attachment addressing information (required), in one of the following forms:
  - SP P-CSCF URL through which to connect to the IMS registrar (IMS case).
  - Application Server URL/IP address along with basic common configuration required by all ITFs.

- SP ID (Note: not required for IMS and whether this is required for non-IMS is for further study).
- SP name (optional, multi-lingual).
- SP description (optional, multi-lingual).
- SP logo (optional).
- Version number of SP information (optional).

This information is used by an ITF to perform the subsequent attachment to the Service Provider (see section 8) and Services Discovery and Selection (see section 9) procedures.

The information retrieved in this stage is typically not secured -- i.e., a non-authenticated client can perform the discovery process, and it is possible that the retrieved information would contain no data to authenticate the "publisher" of the information.

The attachment information for each Service Provider is specific to the attachment method and *shall* be sufficient for attachment using at least one of the following methods: *multicast push*, *unicast pull*, or *IMS*. The methods are described in section 8.

The discovery methods described below differ in the representation of the discovery information retrieved. The discovery data is represented in a format specific to the protocol in use as specified in each section below. The details of the service provider attachment data will be defined in ATIS-0800022, *IPTV Consumer Domain Device Configuration Metadata*, using XML format.

The Service Provider Discovery procedures for the different alternatives are summarized in the following figure.

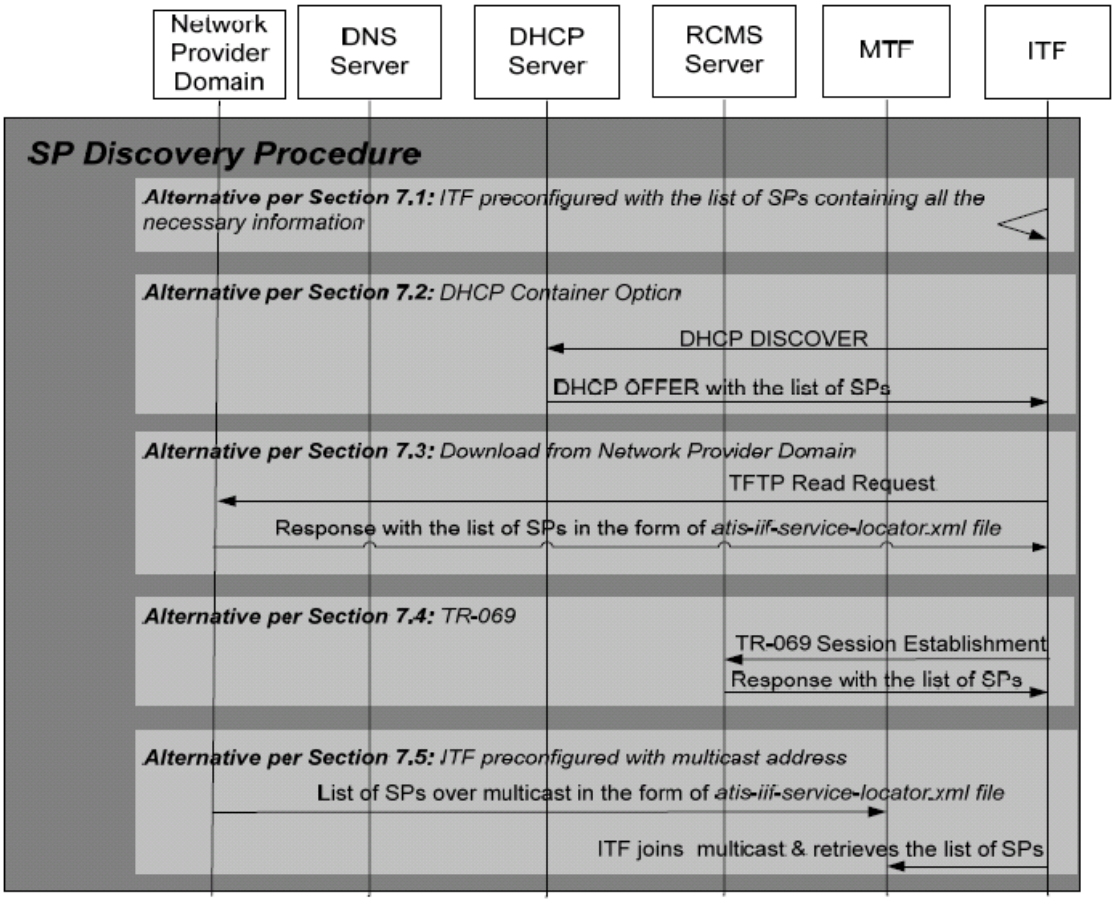

Figure 6: Service Provider Discovery Procedures Summary

7.1 Alternative 1: Preconfigured or Manual SP Discovery Method

The ITF *may* be preconfigured (as described in section 5) with a list of one or more SPs containing all the necessary information as specified in section 7.

7.2 Alternative 2: DHCP-based SP Discovery Method

In addition to acquiring its own IP address and the IP address of the RCMS from the DHCP server, the ITF can acquire a list of one or more SPs containing all the necessary information as specified in section 7 through the DHCP Container Option as described in Appendix C. The format of the list is for further study.

7.3 Alternative 3: Download of the Discovery Information from the Network Provider Domain Method

In this case, the client uses an FQDN defined by the network provider as the location from which to download the atis-iif-service-provider-locator.xml file using TFTP. This file contains the service provider(s) attachment information in XML format as described in ATIS-0800022, *IPTV Consumer Domain Device Configuration Metadata*. The network provider's DNS is used to resolve the available FQDN to an IP address.

7.4 Alternative 4: TR-069 Protocol-based SP Discovery Method

In this case, the discovery is performed by the ITF using the TR-069 protocol during phase 1 of the ITF device initialization and attachment sequence. Specifically, upon a successful ITF device network attachment and successful establishment of a management session between the ITF and the RCMS, the RCMS provides the ITF with a list that contains the SP information.

It is possible that the RCMS is aware of addressing information of a single IPTV SP, multiple IPTV SPs, or no IPTV SPs at all. For each known IPTV SP, however, the RCMS *shall* provide the ITF with the information as stated at the beginning of this section.

The details of the data structure (list of SP information) and its formal representation *shall* be compliant with TR-069 data model syntax, and will be defined in ATIS-0800022, *IPTV Consumer Domain Device Configuration Metadata*.

7.5 Alternative 5: Streaming of the SPs Information to a Multicast Address Method

In this case, the atis-iif-service-provider-locator.xml file is streamed over a FLUTE multicast stream as defined elsewhere in the ATIS IIF. This file contains the service provider(s) attachment information in XML format as described in ATIS-0800022, *IPTV Consumer Domain Device Configuration Metadata*. The ITF listens to an administratively scoped (per RFC 2365) multicast address as identified by a Network Provider. The allocated multicast address is either preconfigured by the manufacturer of the ITF device or retrieved using other means.

RFC 2365 defines the "administratively scoped IPv4 multicast space" to be the range 239.0.0.0 to 239.255.255.255. In addition, it describes a simple set of semantics for the implementation of Administratively Scoped IP Multicast addresses. Finally, it provides a mapping between the IPv6 multicast address classes and IPv4 multicast address classes. RFC 2365 *should* be used as a guide by Network Providers that choose to administratively manage IP multicast Addresses.

7.6 Alternative 6: IMS-based SP Discovery Method

IMS-based networks advertise the use of SIP by using DHCP Option 120 during the network attachment phase. Option 120 provides the ITF with the identity (i.e., FQDN or IP address) of the P-CSCF through which it connects to the IMS registrar and allows the client to utilize IMS registration and attachment to discover an IPTV service provider and subsequently attach to it.

It is assumed in this phase that the IPTV SP is the same as the IMS service provider. Hence, no specific action is required in this case. It is important to note that the IMS registrar and the IPTV Service Discovery Application server are two separate entities. The discovery of the address of the Service Discovery Application server is described in section 8.5.

Prior to any action, the ITF *shall* perform IMS registration and authentication, as described below.

7.6.1 ITF Authentication & Registration

Once the ITF acquires the entry point (i.e., the P-CSCF) to the IMS network, it performs IMS registration and authentication to attach to a service provider. Figure 7 shows the actions involved in the ITF authentication and registration process

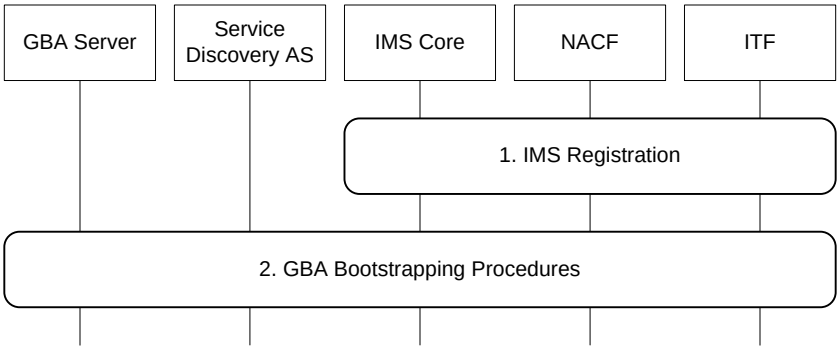

Figure 7: ITF Authentication and Registration Steps

Step 1 of Figure 7 is performed through regular IMS registration with the IMS network per 3GPP TS 23.228 and 3GPP TS 24.229.

In step 2, the ITF performs the generic bootstrap procedure as described in 3GPP TS 33.203. This procedure utilizes the Authentication and Key Agreement (AKA)-based generic bootstrapping architecture (GBA) described in 3GPP TS 33.220, and uses the same credentials used for IMS registration. A high-level overview of GBA, and its goal, is provided in Appendix E for the convenience of the reader.

Once the ITF has completed authentication and registration, it will attach to a Service Discovery Application Server to retrieve its generic service information, as described in section 8.5.

8 ITF Attachment to a Service Provider & Query of Specific Servers

The ITF attaches to and interacts with one or more Service Provider servers (discovered earlier) in order to acquire information about specific services (e.g., EAS, linear TV, VoD).

The output of section 7 can contain one or more records that indicate ways to attach to different service providers. For each output record, if the address is discovered or resolved to a FLUTE type or a multicast IP address, then attachment to that Service Provider uses the push mechanism as described in section 8.3.

8.1 Thick & Thin Clients

Thick Client and *Thin Client* architectures are not precisely specified in this document, but these are general terms for categories of clients that are reasonably well understood in the industry. The differentiation is primarily based on whether service logic is executing locally on the client hardware.

In general, the ITF contains several clients for different services. Even though they can be multiple clients from a logical perspective, this does not constrain the implementation within the ITF. The selection of a client type is likely to be specific to the service and the hardware supporting the client. The attachment procedures in this specification are intended to be generic for a wide variety of client hardware from "set-top box" to portable "cell phone" type implementations of the ITF. These devices implementing the ITF are likely to support a variety of services -- Linear TV, VoD, Communications Services, Internet services, etc.

For example, ATIS-0800007, *IPTV High Level Architecture*, identifies in section 9 several different clients including the Program Guide Client, DRM Client, Media Client, On-Demand Client, etc. The categorization of ITF devices and the specific sets of client functionality they may contain are beyond the scope of this specification.

Therefore, for service attachment purposes we distinguish two general categories of client that can be implemented with the ITF. These are:

- *Thin Client:* A thin client-based service executes most of its service logic on an application server accessed over the network. The thin ITF client concentrates on the presentation of the user interface and the interaction with the user. A thin client is effectively a web browser when retrieving the configuration data and providing the content data to the user.
- *Thick Client:* A thick client-based service executes most of its service logic in the ITF client. The client also performs the presentation of the user interfaces and the interaction with the user.

8.2 Client Sign-on

In order for the Service Provider to authorize the client for acquiring or using any IPTV services (EPG, EAS, Linear TV, VoD, DVR, etc.), the client *shall* sign-on and authenticate with the SP Authentication Server function before proceeding to Services Discovery and Selection phase (as described further in section 9).

The sign-on procedure *shall* be carried in a secure manner. The details of this procedure (including the protocol, format, and the authentication details) are being developed elsewhere by the ATIS IIF. It is envisioned that the information will be expressed in XML format and exchanged over HTTP(S).

The defined sign-on procedure *shall* allow for subsequent secure Web Services (WS) communications to be established between the ITF and the IPTV system if desired.

This step can, for example, include verification against disabled accounts. ATIS-0800022 defines the values sent from the ITF to the Service Provider during Service Provider attachment. Section 9.2.2.1 of ATIS-0800022 addresses the Non-IMS case and section 9.2.3 addresses the IMS case. Included in the Client Sign-On is the following set of parameters:

- ITF device identifier (e.g., the device MAC address or the MAC address of the active WAN interface on the device).
- Model.
- Vendor.

Note that some of the ITF information (e.g., MAC address) could have already been pre-provisioned on the IPTV Application Server. The use of components of access control or encryption such as shared secrets, PKI certificates, and keys is outside of the scope of this document. However, it is useful to note that they could be preloaded on the ITF at manufacture time. Also note that the SD Server and the Authentication Server functions can reside on the same IPTV Application server.

In response to the ITF sign-on, the IPTV Application Server sends all the information needed for subsequent services discovery and attachment by the client, such as:

- Channel Map Identifier (required)
- Location information (using multicast and/or unicast means) of the:

  - SI data (required) (see ATIS-0800022, *IPTV Consumer Domain Device Configuration Metadata*)
  - Electronic Program Guide data (optional) (see ATIS-0800020, *IPTV EPG Metadata Specification)*
  - Emergency Alert Service (EAS) data (if regionally required)
- Additional IPTV multicast stream location or server functions location to contact (in case the services are deployed on separate servers)

8.3 Attachment to SP by a Thick Client through Sign-on

Once the ITF chooses in step 7 an SP from the atis-iif-service-provider-locator.xml file defined in ATIS-0800022, *IPTV Consumer Domain Device Configuration Metadata*, it retrieves the SP associated initial provisioning information for Services Discovery and IPTV Application servers attachment such as:

- Authentication/Registration Server function URI.
- STUN information (STUN Server URI, keep-alive frequency, etc.).
- Software Download Directory (contains multicast location of software images, etc.).

In order for the Service Provider to authorize the client in acquiring any multicast IPTV service, the client must sign on and/or authenticate with the SP Authentication/Registration Server function before proceeding as described in section "Client Sign-on" above.

As a response to the sign-on request, the IPTV Application server sends localized provisioning information to the ITF -- i.e., the multicast location of the subsequent streams that are of interest to this particular ITF as detailed in section 8.2 above. The localized information will prepare the ITF to proceed to the next step, Services Discovery and Selection phase (as described in section 9). The details of provisioning information and authentication metadata (if required) are detailed in ATIS-0800022.

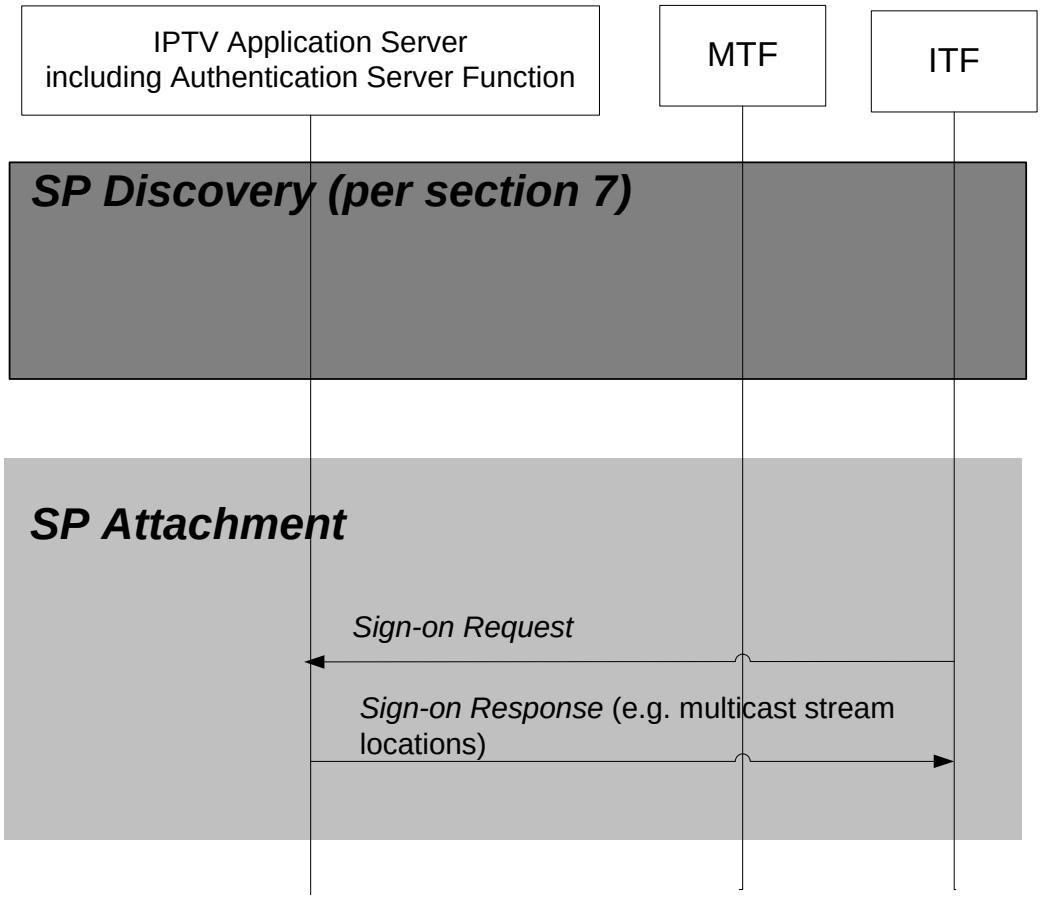

Figure 8: Attachment to a Service Provider Through Sign-On

8.4 Attachment to SP by a Thick Client using a Unicast-based Pull Mechanism

The SD contact information is known to the ITF as a result of the previous step. In the case of the Unicast-based Pull mechanism, the Service Provider attachment information (as retrieved per section 7) contains the URL(s) of the Authentication and SD Server function(s). By default, these server functions are collocated.

In order for the Service Provider to authorize the client for acquiring or using any IPTV services, the client must sign-on and authenticate to the SP Authentication Server function before proceeding to Services Discovery and Selection phase (as described further in section 9). From there, secure communications are established between the ITF and the IPTV system for securing subsequent Web Services (WS) signaling transactions. Details are being developed elsewhere by the ATIS IIF.

Note that functions 1 – 3 described below can be performed as a single WS request or as a sequence of separate secure WS requests. This mechanism allows the IPTV Service Provider to deliver information relevant only to a single ITF in a secure controlled manner.

(1) *Sign-on (Required)*

During this step the ITF logs into the IPTV SP Authentication Server function as described in section "Client Sign-on" above.

(2) *GetServicesList (Required)*

The IPTV services can physically reside on machines other than the original SD Server function. In this step, the ITF gets a list of the IPTV services that it needs to contact with the services' corresponding location information. The location information is defined using the ResourceLocator type, as defined in ATIS-0800013, *Media Protocols Specification*. It can point to specific IPTV Application Servers' URLs, location of specific IPTV services' multicast streams, etc.

(3) *GetSubscriberDevicesGroupList (Optional)*

In order to distribute information relevant only to a subset of ITFs in a system, a Service Provider can assign each ITF to one or more Devices Groups.

A *Devices Group* is a logical set of devices grouped according to some common attributes or a desired functionality as part of an operator configuration. Examples of Devices Groups would be the physical location of a set of devices, a subscription to a particular set of services (a.k.a., packages), etc.

Using the GetSubscriberDevicesGroupList request, the subscriber retrieves the list of Devices Groups to which it belongs.

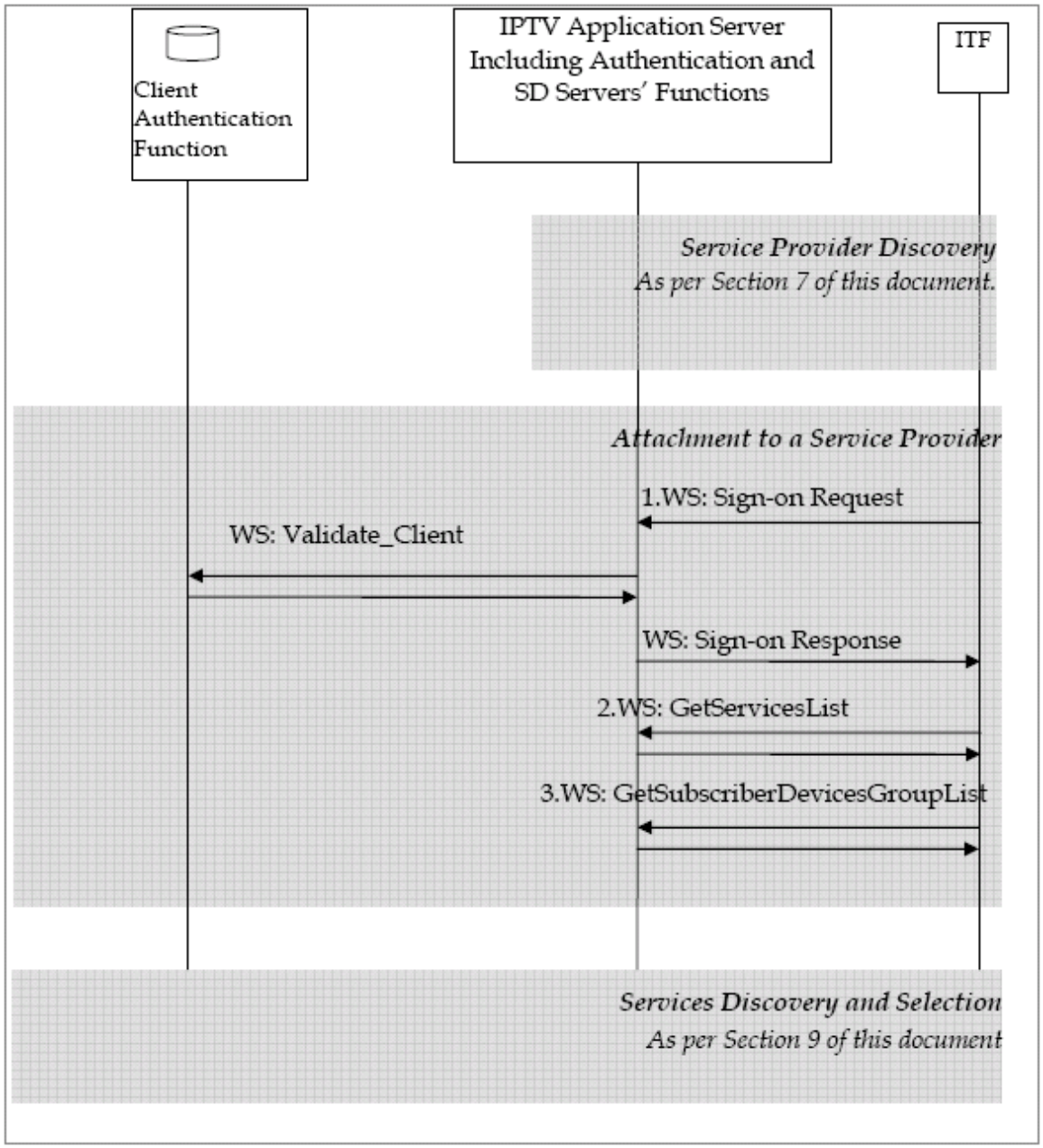

Figure 9: Attachment to a Service Provider using a Pull Mechanism

After the attachment procedure is successfully completed, the ITF automatically performs the "Services Discovery and Selection" procedure described in section 9.

8.5 Attachment to IMS-Based SP

Once the IMS client has authenticated and registered with the IMS network as described in section 7.6, the client needs to contact the Service Discovery Application Server. The methods for identification and retrieving the location of the Service Discovery Application Server (AS) are described in sections 8.5.1 and 8.5.2 below. Once the server location is known, in order to receive the initial service data (and subsequent notifications of updates to that data), the client attaches to the server by establishing a

standard SUBSCRIBE session based upon the IETF standard SIP Notification framework specified in RFC 3265, *Session Initiation Protocol (SIP)-Specific Event Notification*.

The framework provides a pull mechanism for initial data retrieval; when the data changes, it uses a push mechanism for notification of those changes through the use of a NOTIFY command.

For initial service discovery, there *shall* be a single event package related to IPTV for conveying information related to transport mechanisms in regard the different elements of the information model. The package *shall* be extensible so that support for new information elements in the information model can be accommodated.

The following is an example of an event package for the initial SUBSCRIBE to the Service Discovery AS. Some initial parameters defined for the ITF-Service-Data package are defined below for illustrative purposes only.

Example: Event Package Name: ITF-Service-Data

- Event header field present in SUBSCRIBE and NOTIFY requests for this package
- Event Package Parameters for use in SUBSCRIBE:
  - *ITF Vendor:* the vendor of the ITF. The implementer *should* use their DNS domain name (e.g. example.com) as the value of the "vendor" parameter so that it is known to be unique.
  - *ITF Version*: string text describing the version of the ITF.
  - *Other Device Characteristics*: other characteristics such as screen size, aspect ratio, RTSP support, IGMP support, over-the-air (OTA) broadcast support, etc. can be desirable in order to enable the IPTV Application Server to provide the most optimal service possible, however this is for future study.

    Other parameters can be envisaged. This is just a subset of potential parameters included in the SUBSCRIBE request.

SUBSCRIBE requests are routed by the IMS to the Service Discovery AS for processing using a PSI as discussed in sections 8.5.1 and 8.5.2 below. If the Service Discovery AS is willing to fulfill the request for service data, it returns a 200 OK and begins to construct or locate the requested data. When the data is ready, the Service Discovery AS sends a NOTIFY message to the ITF. The NOTIFY *shall* include a URI for every element in the information model described in section 9.1.

The NOTIFY *shall* also include the manner in which the data associated with the URI is to be retrieved. The retrieval methodology could be a multicast address where data is pushed to the client, an HTTP GET for browser-based data, FLUTE resource locator, etc. This can also include SIP URIs to be used with the SIP Notification Framework. The methods for retrieval of the service data are further described in section 9.4.

8.5.1 Public Service Identifier (PSI) for Service Provider Attachment

It is recommended that a *Public Service Identifier (PSI)* is allocated to the Service Discovery Application server.

The usage of this PSI simplifies pre-configuration of ITFs, and allows IMS features/functions to be fully exploited seamlessly. PSIs are essentially SIP URIs that are functionally equivalent to IMS public user

identities in that they identify services instead of users. In that capacity, they can be provisioned in an end-user profile as originating initial Filter Criteria (iFCs) for service access authorization. Users who don't have the PSI for a particular service provisioned in their originating iFC will not be allowed to access that service. This also requires that the Service Provider DNS does not include that PSI as an entry. This ensures that if no iFC including the PSI is detected, normal IMS routing using DNS will fail and result in an error message (4XX) to be returned to the ITF.

In applying the above principles, all users authorized to access the IPTV service will have within their originating iFC the Service Discovery AS PSI configured as a trigger point in conjunction with a SIP SUBSCRIBE. Furthermore, the Application Server to which the SUBSCRIBE request is routed will be configured in the iFC as the IPTV Service Discovery Application server.

Detailed information about PSIs can be found in 3GPP TS 23.228, 3GPP TS 24.229, and 3GPP TS 23.218.

8.5.2 Acquiring the Public Service Identifier (PSI)

There are two options for the ITF to acquire the Public Service Identifier (PSI) for the Service Discovery Application server of the service provider: 1) an ITF can be manually configured or pre-configured with the PSI; or 2) DNS SRV records can be used to obtain the PSI in accordance with RFC 2782 with the following input parameters:

a) *Service:* The symbolic name 'atis-iif-iptv-servicediscovery' of the desired service. The network provider DNS must include an entry for this symbolic name when using this method.

b) *Protocol:* SIP

c) *Domain name:* The domain for which the returned records are valid; the value is set to the IMS home domain.

The output of the DNS SRV lookup is the Service Discovery Application server PSI name, which is used later during the service discovery phase.

9 ITF SERVICES DISCOVERY & SELECTION

9.1 Introduction to ITF Services Discovery & Basic Definitions

Services Discovery is the process by which an ITF receives the necessary data elements which enable the ITF to access the available IPTV Services.

The data model and the XML schema of elements in the IPTV network are being defined elsewhere by the ATIS IIF. The main data elements are:

- EPG
- Service Information

The Services Discovery information can be retrieved in several ways. These retrieval mechanisms are described in the subsequent sections.

9.2 ITF Services Discovery and Selection by a Thick Client Using a Multicast-based Push Mechanism

Upon successful ITF registration/authentication and based on unique information (e.g., MAC address) provided by the ITF to the SP IPTV Application server during the Attachment to SD Server phase, the IPTV Application server provides to the ITF the location of different Service multicast flows (see sections 8.3 and 8.4). The ITF joins the appropriate multicast flows (e.g., SI, EPG, etc.) using SSM upon request from the associated application, as shown in Figure 11.

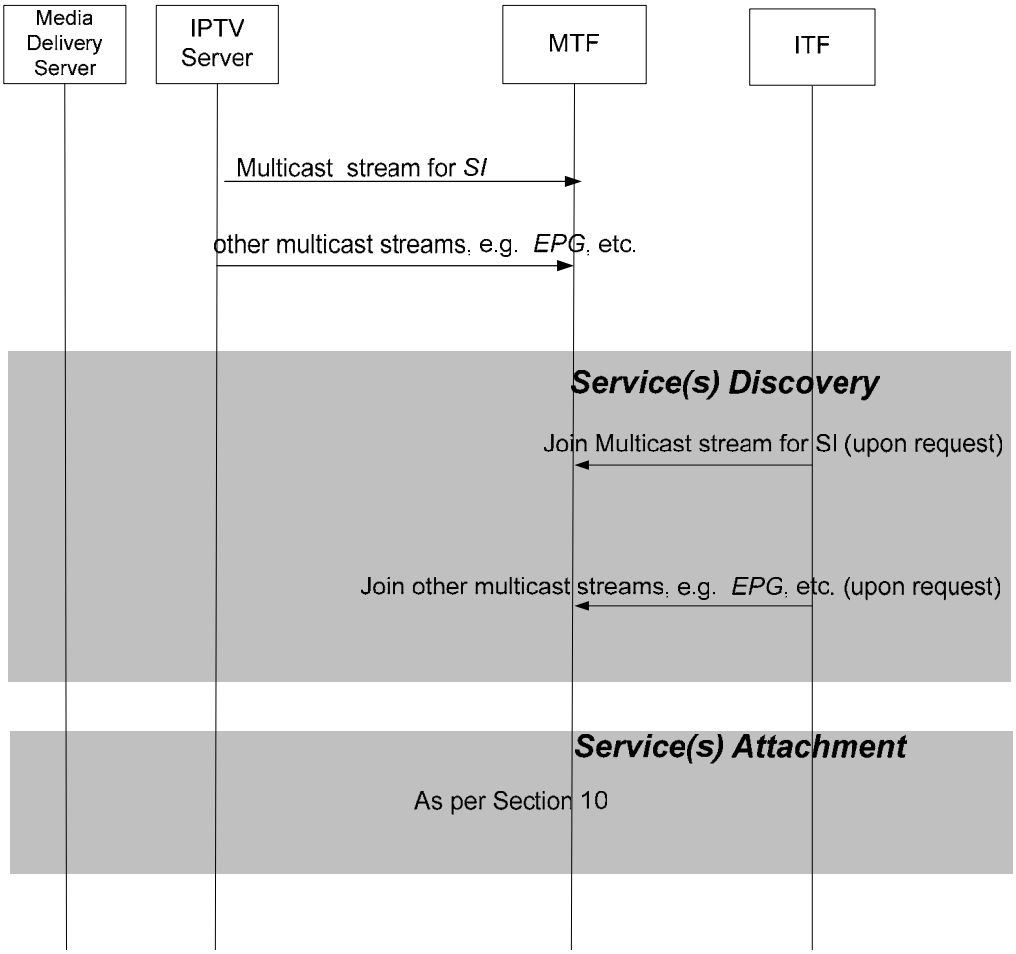

Figure 10: Services Discovery and Selection Using a Multicast-based Push Mechanism

The ITF can leave the multicast stream(s) once it is done receiving the SI, EPG, or other data information. Multicast flows that carry critical messages (e.g., EAS and/or notification messages) could be continuously monitored by the ITF -- i.e., the ITF would never leave the flow(s).

Service Attachment is outside the scope of this document. Once the ITF collects all the necessary signaling information, it is ready to join any Media Stream selected by the user.

9.3 ITF Services Discovery & Selection by a Thick Client Using a Unicast-based Pull Mechanism

Figure 12 shows different ways in which the EPG and the SI data can be distributed to the ITF. The details of these mechanisms will be defined in ATIS-0800022, *IPTV Consumer Domain Device Configuration Metadata*.

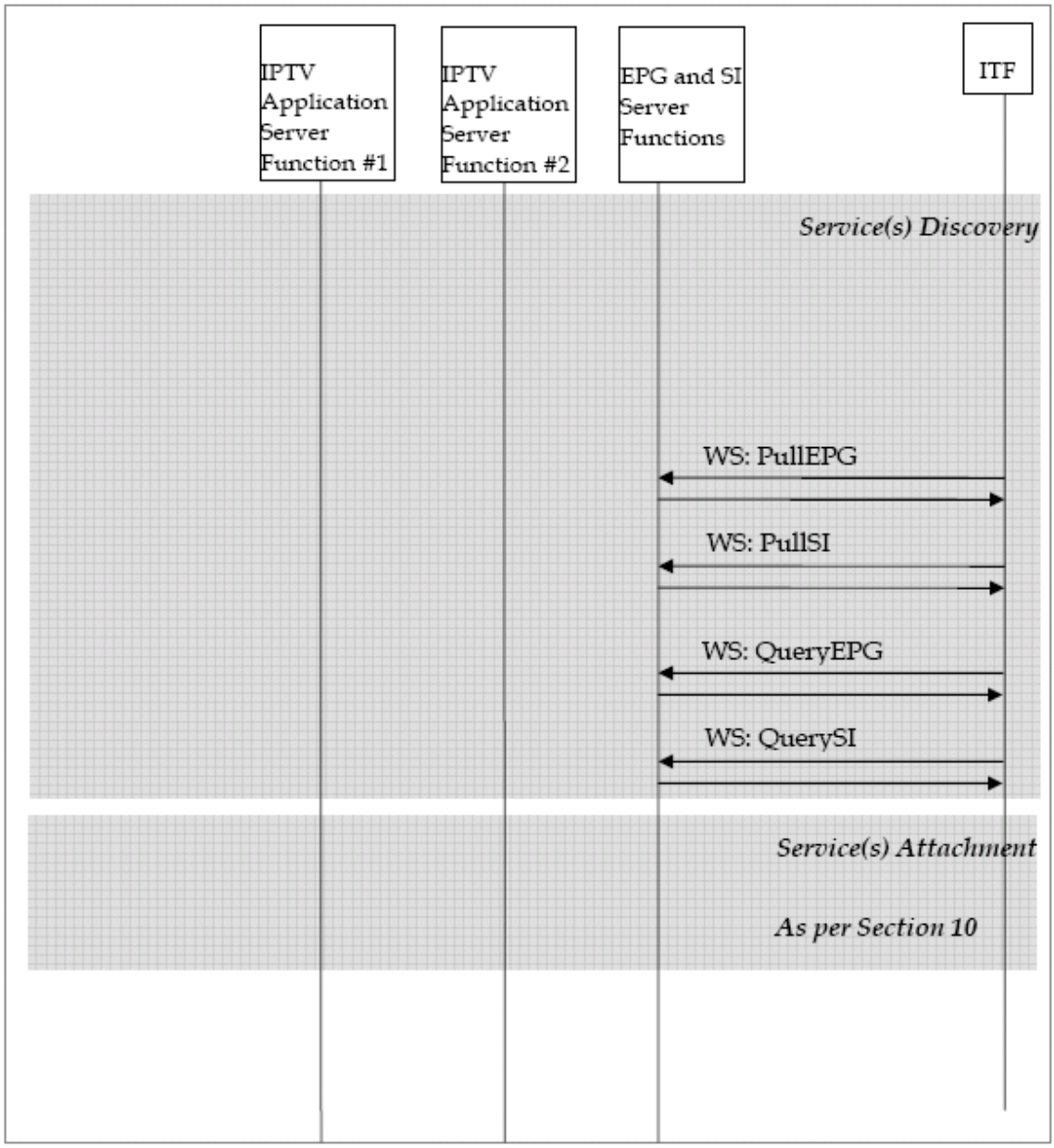

Figure 11: Services Discovery and Selection using a Pull Mechanism

As shown, the following mechanisms for retrieving the EPG and the SI can take place:

- *PullEPG*: The subscriber retrieves the EPG using predefined XML file structures.
- *PullSI*: The subscriber retrieves the SI tables using predefined XML file structures. Retrieval of this information can be performed in multiple steps.

- *QueryEPG*: The subscriber retrieves the EPG using customized request.
- *QuerySI*: The subscriber retrieves the SI tables using customized request.

9.4 ITF Services Discovery & Selection for IMS-based Networks

The SIP Notification framework based upon the IETF standard SIP Notification framework specified in RFC 3265 enables transport of service data via wide range of mechanisms that can cater to thin or thick client models. Examples of additional mechanisms for thick clients are IP Multicast (e.g., data carousel), URI addresses for SOAP based pull requests, URI addresses for HTTP GET for XML data, etc. Examples of additional mechanisms for thin clients include URI addresses for portals and for channel information.

Three IMS-based ITF options for implementing the Services Discovery and Selection procedure are described in the sections below:

- Use of the SIP Notification Framework outlined in section 9.4.1.
- Use of a pull mechanism similar to that described in section 9.3.
- Use of a push mechanism similar to that described in section 9.2.

An exemplary flow illustrating the attachment to the Service Discovery AS and the retrieval of the generic service information data as outlined in section 8.5, along with services discovery and selection as discussed in this section is shown below in Figure 13.

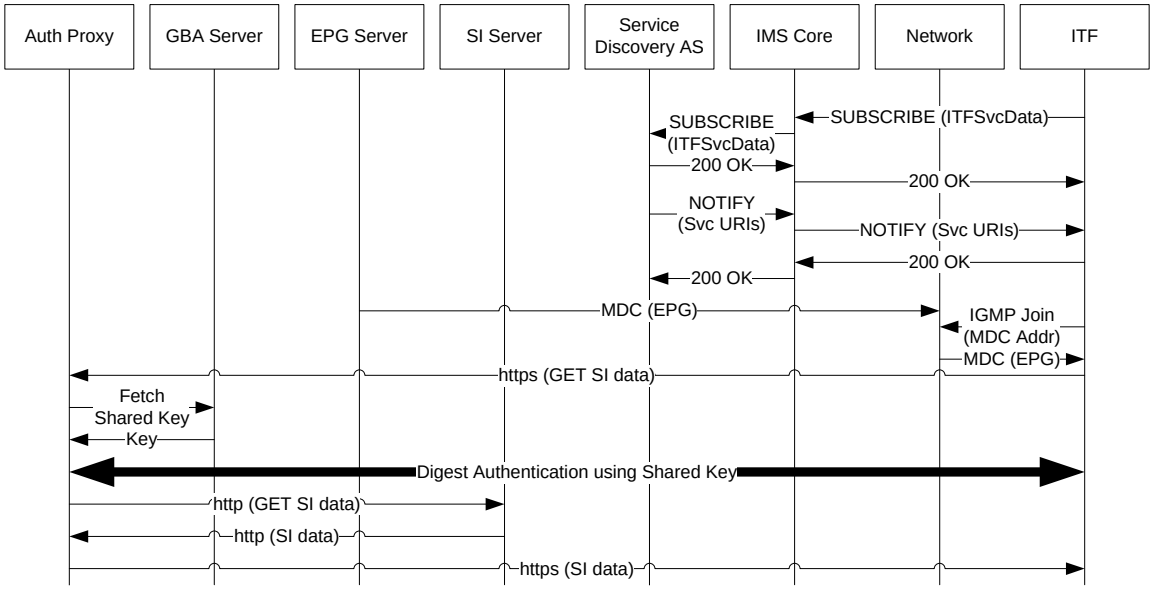

Figure 12: IMS-Based Attachment to a Service Discovery AS, Generic Service Information Data Retrieval and Service Discovery Example

The behavior and progressions shown in the figure above are explained further below:

- *First, the ITF sends a SUBSCRIBE to the Service Discovery AS for the ITF-Service-Data event package*. The ITF provides information about itself which the SDAS uses to select the service data URIs for the ITF.
- *Once the Service Discovery AS decides to accept the request, it returns a 200 OK*. Note that if the ITF was not authorized to access the Service Discovery AS, the IMS core would return an appropriate failure code in response to the request.
- *The Service Discovery AS then returns a NOTIFY message including retrieval information related to all information elements*. In this example, the ITF indicates that the EPG is contained in a multicast data carousel. The IP address of the carousel is returned to the ITF in the NOTIFY message.
- *The ITF then joins the IP multicast address to retrieve the EPG*.
- *The same NOTIFY from the Service Discovery AS also indicates to the ITF that SI is to be retrieved from the SI URI using HTTP GET*. The SI URI is a secure URI and is handled via the GBA architecture described previously. Ultimately, the SI server receives the request and returns the requested information in a secure manner.

Exchanges related to retrieval of remaining information elements have been removed for brevity.

Utilizing this methodology to retrieve service attachment data will almost certainly require some of the potential optimizations outlined in Appendix G.

9.4.1 ITF Services Discovery & Selection using the SIP Notification Framework

The necessary IPTV service address data *shall* be retrieved through URIs included in the NOTIFY response to the SUBSCRIBE sent to the Service Discovery AS as described in section 8.5. If a SIP URI to be used with the SIP Notification Framework is provided for a specific information element, an event package definition for that information element is required.

9.4.2 ITF Services Discovery & Selection using SOAP-based Pull Mechanism with IMS (Thick Client)

NOTE -- While this section discusses a client utilizing SOAP to retrieve data, it is certainly possible for other protocols to be utilized for this purpose.

Section 9.3 discusses a pull mechanism for the ITF to utilize web services interfaces to retrieve its configuration data for the services to which it is subscribed. In particular, the section implies a thick client model utilizing SOAP based Remote Procedure Calls (RPCs).

The use of the mechanism is equally applicable to the IMS case. There is no difference in the use of this mechanism between the IMS and non-IMS cases.

9.4.3 ITF Services Discovery & Selection using Pull Mechanism utilizing http with IMS (Thin Client)

Thin clients are useful for clients which do not have the processing capabilities to handle a thick client model. In this case, a network portal retrieves the actual configuration XML data, stores it locally, then converts the XML data to web pages that can be rendered through a web browser when accessing the portal.

The use of the mechanism remains the same. For a thin client, the Services Discovery function returns URIs specifying the Portal http address for the web service calls while the IMS case embeds the same http address definitions in the SIP Notify response.

9.4.4 ITF Services Discovery & Selection using Push Mechanism with IMS (Thick Client)

Just as the use of the pull mechanism with IMS is functionally equivalent to non-IMS implementations, the push mechanism use with IMS is fairly straightforward. The ITF would join the multicast streams from which it will derive its service attachment data following the procedure outlined in section 9.2.

10 ITF SERVICE ATTACHMENT

The Service Attachment procedure to be used to acquire a particular IPTV service (e.g., Linear TV, VoD) is typically service-specific, and is beyond the scope of this specification document.

Appendix A
(normative)

A DHCP CONFORMANCE FOR IPTV DEVICES IN THE CONSUMER DOMAIN

This appendix specifies the required and recommended DHCP Options for the DNG and ITF devices. DHCP client compliance with Table A.3 is mandatory, and DHCP server compliance with Table A.4 is mandatory.

A.1 Introduction to DHCP

The DHCP, defined by IETF, provides a framework for passing configuration information between the network (DHCP Servers) and hosts (DHCP Clients) over a TCP/IP network by including predefined structures, referred to as Options, within the DHCP messages.

There are 9 messages and 255 Options defined (or reserved) by numerous IETF RFCs, and used for different purposes and applications. Only a subset of these Options is usually supported based on the host device type and supported services. Some of these Options overlap in functionality, and some are conditional on other Options.

According to the ATIS IPTV architecture, the DNG behaves as a DHCP server toward the LAN side (toward the ITF devices), and as a DHCP client toward the access/core network. The ITF device behaves only as a DHCP client on the LAN network.

A.2 DHCP Message Conformance [Normative]

DHCP messages are identified by their Message Code. The table below lists the DHCP messages, and sender/receiver party for each. All references to the specifications are listed at the end of this Appendix.

Table A.1 : DHCP Messages

Message Code	*Message Name*	*Spec*	*DHCP Client*	*DHCP Server*
1	DHCP_DISCOVER	RFC 2131	Send	Receive
2	DHCP_OFFER	RFC 2131	Receive	Send
3	DHCP_REQUEST	RFC 2131	Send	Receive
4	DHCP_DECLINE	RFC 2131	Send	Receive
5	DHCP_ACK	RFC 2131	Receive	Send
6	DHCP_NAK	RFC 2131	Receive	Send
7	DHCP_RELEASE	RFC 2131	Send	Receive
8	DHCP_INFORM	RFC 2131	Send	Receive
9	DHCP_FORCE_RENEW	RFC 2131	Receive	Send

Both server and client *shall* support all of these messages, either by sending them, or by receiving and processing them.

A.3 DHCP Options List [Informative]

The ***informative*** table below summarizes known standard DHCP Options as defined by IETF. The table also shows the roles the DHCP client and the DHCP server play in implementing each Option, if a particular Option is supported by the network.

Support for DHCP Options relevant to implementing an ATIS IIF-compliant IPTV system is specified in sections A.4 and A.5 below. DHCP Options are identified by their Option number/code. All references to the specifications are found at the end of this Appendix.

Table A.2: DHCP Options List per IETF Specifications

Option Code/ Number	*Option Name & Explanation*	*Spec*	*Client*	*Server*
0	PAD_OPTION	RFC 2132 TS-102034 HGTR-R1	Must	Must
1	SUBNET_MASK_OPTION	RFC 2132 TS-102034 HGTR-R1 CH1.1	Must	Must
2	TIME_OFFSET_OPTION	RFC 2132 HGTR-R1 CH1.1	May	Must
3	ROUTER_OPTION	RFC 2132 TS-102034 HGTR-R1 CH1.1	Must	Must
4	TIME_SERVICE_OPTION	RFC 2132 TS-102034 CH1.1	May	May
5	NAME_SERVICE_OPTION	RFC 2132	May	May
6	DOMAIN_NAME_SERVICE_OPTION Note: The domain name server option specifies one (or more) Domain Name System IP addresses available to the client. If more than one DNS address is provided, the servers' IP addresses *should* be listed in order of preference.	RFC 2132 TS-102034 HGTR-R1 CH1.1	Must	Must
7	LOG_SERVICE_OPTION	RFC 2132 HGTR-R1 CH1.1	May	May

Option Code / Number	*Option Name & Explanation*	*Spec*	*Client*	*Server*
8	COOKIE_SERVICE_OPTION	RFC 2132	May	May
9	LINE_PRINT_SERVICE_OPTION	RFC 2132	May	May
10	IMPRESS_SERVICE_OPTION	RFC 2132	May	May
11	RESOURCE_LOCATION_SERVICE_OPTION	RFC 2132	May	May
12	HOST_NAME_OPTION	RFC 2132 HGTR-R1 CH1.1	May	May
13	BOOT_FILE_SIZE_OPTION	RFC 2132	May	Must
14	MERIT_DUMP_FILE_OPTION	RFC 2132	May	May
15	CLIENT_DOMAIN_NAME_OPTION	RFC 2132 TR-044 TS-102034 HGTR-R1 CH1.1	May	May
16	SWAP_SERVICE_OPTION	RFC 2132	May	May
17	ROOT_DISK_PATH_OPTION	RFC 2132	May	May
18	EXTENSION_PATH_OPTION	RFC 2132	May	May
19	INTERNET_PROTOCOL_FORWARD_OPTION	RFC 2132	May	May
20	SOURCE_ROUTE_OPTION	RFC 2132	May	May
21	ROUTE_POLICY_FILTER_OPTION	RFC 2132	May	May
22	MAXIMUM_DATAGRAM_ASSEMBLE_OPTION	RFC 2132	May	May
23	DEFAULT_TIME_TO_LIVE_OPTION	RFC 2132 CH1.1	May	May
24	MAX_TRANS_UNIT_TIMEOUT_OPTION	RFC 2132	May	May
25	MAX_TRANS_UNIT_PLATEAU_OPTION	RFC 2132	May	May
26	MAX_TRANS_UNIT_INTERFACE_OPTION	RFC 2132 CH1.1	May	May
27	MAX_TRANS_UNIT_SUBNET_OPTION	RFC 2132	May	May
28	BROADCAST_ADDRESS_OPTION	RFC 2132	May	May
29	SUBNET_MASK_DISCOVER_OPTION	RFC 2132	May	May

Option Code / Number	*Option Name & Explanation*	*Spec*	*Client*	*Server*
30	SUBNET_MASK_PROVIDER_OPTION	RFC 2132	May	May
31	ROUTER_DISCOVER_OPTION	RFC 2132	May	May
32	ROUTER_SOLICIT_ADDRESS_OPTION	RFC 2132	May	May
33	STATIC_ROUTE_OPTION	RFC 2132 HGTR-R1	May	May
34	TRAILER_ENCAPSULATE_OPTION	RFC 2132	May	May
35	ADDRESS_RESOLUTION_CACHE_OPTION	RFC 2132	May	May
36	ETHERNET_ENCAPSULATE_OPTION	RFC 2132	May	May
37	TCP_DEFAULT_TIME_TO_LIVE_OPTION	RFC 2132	May	May
38	TCP_KEEP_ALIVE_INTERVAL_OPTION	RFC 2132	May	May
39	TCP_KEEP_ALIVE_PAYLOAD_OPTION	RFC 2132	May	May
40	NET_INFO_SRV_DOMAIN_OPTION	RFC 2132	May	May
41	NET_INFO_SRV_ADDRESS_OPTION	RFC 2132	May	May
42	NETWORK_TIME_SERVICE_OPTION	RFC 2132 TS-102034 HGTR-R1	May	May
43	VENDOR_SPECIFIC_DATA_OPTION Note: This option is used by clients and servers to exchange vendor-specific information. The information is an *opaque object* of "n" octets interpreted by vendor-specific code on the clients and servers. The definition of this information is vendor specific. This Option relates to Option 60.	RFC 2132 TR-069 HGTR-R1 CH1.1	May	May
44	NETBIOS_NAME_SERVICE_OPTION	RFC 2132	May	May
45	NETBIOS_DATAGRAM_OPTION	RFC 2132	May	May
46	NETBIOS_NODE_TYPE_OPTION	RFC 2132	May	May
47	NETBIOS_SCOPE_OPTION	RFC 2132	May	May
48	X_WINDOW_FONT_SERVICE_OPTION	RFC 2132	May	May
49	X_WINDOW_DISPLAY_SERVICE_OPTION	RFC 2132	May	May

Option Code / Number	*Option Name & Explanation*	*Spec*	*Client*	*Server*
50	INTERNET_ADDRESS_REQUEST_OPTION Note: This option allows the client to request that a particular IP address be assigned. It may not be needed or supported by every client, but it needs to be supported by the server. This Option is a requirement in Broadband Forum TR-44.	RFC 2132 TR-044 TS-102034 HGTR-R1 CH1.1	May	Must
51	INTERNET_ADDRESS_LEASE_OPTION Note: There are 2 uses for this option: ♦ In a client request (DHCPDISCOVER or DHCPREQUEST) to allow the client to request a lease time for its IP address. ♦ In a server reply (DHCPOFFER), a DHCP server uses this Option to specify the lease time it is willing to offer to the client	RFC 2132 TS-102034 HGTR-R1 CH1.1	Must	Must
52	OPTION_OVERLOAD_OPTION Note: A DHCP server sends this option to the client to indicate to the client that the DHCP 'sname' or 'file' fields are being overloaded by using them to carry DHCP options.	RFC 2132 TS-102034	May	May
53	DHCP_MESSAGE_TYPE_OPTION Note: This Option is mandatory by definition since it contains the DHCP message type	RFC 2132 TS-102034 HGTR-R1	Must	Must
54	DHCP_SERVER_IDENTIFIER	RFC 2132 TS-102034 HGTR-R1 CH1.1	Must	Must
55	DHCP_PARAMETER_REQUEST_OPTION Note: This Option is sent by a DHCP client to request values for specified configuration parameters. The list of requested parameters is specified as n octets, where each octet is a valid DHCP option code.	RFC 2132 TR-044 TS-102034 HGTR-R1 CH1.1	May	Must

Option Code / Number	*Option Name & Explanation*	*Spec*	*Client*	*Server*
56	DHCP_MESSAGE_OPTION Note: Sent by the Server. It provides an error message to a DHCP client in a DHCPNAK message in the event of a failure.	RFC 2132 TS-102034 HGTR-R1	Must	Must
57	DHCP_MESSAGE_SIZE_OPTION Note: This Option specifies the maximum DHCP message length that the client is willing to accept.	RFC 2132 TS-102034	May	Must
58	DHCP_RENEWAL_TIME_OPTION Note: This Option specifies the time interval (T1) from address assignment until the client transitions to the RENEWING state.	RFC 2132 TS-102034 HGTR-R1	Must	Must
59	DHCP_REBIND_TIME_OPTION Note: This Option specifies the time interval (T2) from address assignment until the client transitions to the REBINDING state.	RFC 2132 TS-102034	Must	Must
60	VENDOR_CLASS_IDENTIFIER_OPTION Note: This option is used by the client to identify the client vendor type and configuration of a DHCP client. Servers do NOT have to reply, but Servers that respond *should* use Option 43 to reply. So the sequence is as follows: - The client sends Option 60. - The Server replies with Option 43 (if it wishes to reply). Note: Per the ATIS IIF, this Option *shall* be sent by the client (also required by Broadband Forum TR-069 specs). The server's reply to this Option is optional, and it is via Option 43.	RFC 2132 TR-069 HGTR-R1 CH1.1	Must	Must

Option Code / Number	*Option Name & Explanation*	*Spec*	*Client*	*Server*
61	CLIENT_IDENTIFIER_OPTION Note: This option is sent by the DHCP client to the DHCP server. It serves as a unique client identifier.	RFC 2132 TR-044 TS-102034 HGTR-R1 CH1.1	Must	Must
62	NETWARE_INTERNET_DOMAIN_OPTION	RFC 2242	May	May
63	NETWARE_INTERNET_PROTOCOL_OPTION	RFC 2242	May	May
64	NET_INFO_SRV_PLUS_DOMAIN_OPTION	RFC 2132	May	May
65	NET_INFO_SRV_PLUS_ADDRESS_OPTION	RFC 2132	May	May
66	TRIVIAL_FILE_TRANSFER_OPTION	RFC 2132 HGTR-R1	May	May
67	BOOT_FILE_NAME_OPTION	RFC 2132 HGTR-R1	May	May
68	MOBILE_HOME_AGENT_OPTION	RFC 2132	May	May
69	SIMPLE_MAIL_TRANSPORT_OPTION	RFC 2132	May	May
70	POST_OFFICE_PROTOCOL_OPTION	RFC 2132	May	May
71	NETWORK_NEWS_TRANSPORT_OPTION	RFC 2132	May	May
72	DEFAULT_WEB_SERVICE_OPTION	RFC 2132 TR-044	May	May
73	DEFAULT_FINGER_SERVICE_OPTION	RFC 2132	May	May
74	DEFAULT_CHAT_SERVICE_OPTION	RFC 2132	May	May
75	STREET_TALK_SERVICE_OPTION	RFC 2132	May	May
76	STREET_TALK_DIRECT_ASSIST_OPTION	RFC 2132	May	May

Option Code / Number	*Option Name & Explanation*	*Spec*	*Client*	*Server*
77	USER_CLASS_DATA_OPTION Note: This Option is used by a DHCP client to ***optionally*** identify the type or category of user or applications it represents. A DHCP server uses the User Class option to choose the ***address pool*** it allocates an address from and/or to select any other configuration option. A server that is not equipped to interpret any given user class specified by a client *shall* ignore it.	RFC 3004 TR-044 TS-102034 HGTR-R1	May	May
78	SERVICE_LOCATION_PROTOCOL_OPTION	RFC 2610 TR-044	May	May
79	SERVICE_LOCATION_PROTOCOL_SCOPE	RFC 2610	May	May
80	RAPID_COMMIT_OPTION	RFC 4039	May	May
81	UNKNOWN / Not defined		NA	NA
82	DHCP_RELAY_AGENT_INFO_OPTION	RFC 3046	May	May
83	STORAGE_NAME_SERVICE_OPTION	RFC 4174	May	May
84	RESERVED	RFC 3679	Reserved	Reserved
85	NOVELL_DIR_SRV_OPTION	RFC 2241	May	May
86	NOVELL_DIR_SRV_TREE_NAME_OPTION	RFC 2241	May	May
87	NOVELL_DIR_SRV_CONTEXT_OPTION	RFC 2241	May	May
88-89	RESERVED	RFC 3679	Reserved	Reserved
90	DHCP_AUTHENTICATION_OPTION	RFC 3118	May	May
91-92	RESERVED	RFC 3679	Reserved	Reserved
93	CLIENT_SYSTEM_OPTION	RFC 3679	May	May
94	CLIENT_NET_DEVICE_OPTION	RFC 3679	May	May
95	LGHTWHT_DIRECT_ACCESS_OPTION	RFC 3679	May	May
96	RESERVED	RFC 3679	Reserved	Reserved
97	CLIENT_GRAPHIC_INTERFACE_OPTION	RFC 3679	May	May
98	OPEN_GROUP_AUTHENT_OPTION	RFC 2485	May	May

Option Code / Number	*Option Name & Explanation*	*Spec*	*Client*	*Server*
99-111	RESERVED	RFC 3679	Reserved	Reserved
112	NETINFO_OPTION	RFC 3679	May	May
113	NETINFO_TAG_OPTION	RFC 3679	May	May
114	UNIFORM_RESOURCE_LOCATOR_OPTION	RFC 3679	May	May
115	RESERVED	RFC 3697	Reserved	Reserved
116	AUTO_CONFIGURATION_OPTION	RFC 2563 TR-044 TS-102034	May	May
117	NAME_SERVICE_SEARCH_OPTION	RFC 2937 TR-044	May	May
118	SUBNET_SELECT_OPTION Note: This option allows the DHCP client to specify the subnet on which server to allocate an address. It should be optional for the client, and mandatory for the server.	RFC 3011 TR-044 TS-102034	May	Must
119	DOMAIN_SEARCH_OPTION	RFC 3397	May	May
120	SESSION_INIT_PROTOCOL_OPTION Note: This Option is required per ITF initialization sequence, for IMS/SIP networks.	RFC 3361	Must for IMS/SIP capable device.	Must for IMS/SIP capable network.
121	CLASSLESS_ROUTE_OPTION	RFC 3442 HGTR-R1	May	May
122	CABLELABS_CLIENT_CONFIG_OPTION	RFC 3495 CH1.1	May	May
123	LOCATION_CONFIG_INFO_OPTION	RFC 3825	May	May
124	VENDOR_CLASS_OPTION Note: A DHCP client may use this option to unambiguously identify the vendor that manufactured the hardware on which the client is running. The key word here is “Class”.	RFC 3925	May	Must

Option Code / Number	*Option Name & Explanation*	*Spec*	*Client*	*Server*
125	VENDOR_SPECIFIC_INFO_OPTION Note: DHCP clients and servers may use this option to exchange vendor-specific information. The key word here is "Info". The definition of the information carried in this option is vendor specific. This Option is required by Broadband Forum TR-111 to allow the remote configuration manager to associate the DNG with the devices behind it on the LAN. This option overlaps in functionality with Option 60 (which is required for the ATIS IIF).	RFC 3925 TR-111 HGTR-R1	Must	Must
126	OPTION_CODE_OPTION	RFC 3679	May	May
127	OPTION_CODE_EXTENSION_OPTION	RFC 3679	May	May
128	RESERVED	RFC 3942	Reserved	Reserved
129-222	RESERVED	RFC 2132	Reserved	Reserved
223	RESERVED	RFC 3942	Reserved	Reserved
224-254	RESERVED	RFC 2132	Reserved	Reserved
255	END_OPTION	RFC 2132 TS-102034 HGTR-R1	Must	Must

A.4 DHCP Options Sent from the DHCP Client to the DHCP Server [Normative]

The table below lists the DHCP Options that *shall* be sent by the DHCP client to the DHCP server.

Table A.3: Mandatory DHCP Client Options

Option Number	*Option Name*	*Explanation & Rationale*	*Qualification*
53	Message Type Option	Defines the message type of a DHCP exchange. Needed for basic DHCP operations.	Always
54	Server Identifier	DHCP Client includes this Option in the multicast DHCP REQUEST message to indicate which server's offer is being accepted. Note: DHCP clients use the content of the server identifier field (which is the IP address of the server) as the destination address for any DHCP messages unicast to the server.	Always
60	Vendor Class Identifier Option	Issued by the Client to identify device/host vendor information. Note: If the Client supports the Broadband Forum TR-069 ACS URL discovery method, it *shall* include the string *"dslforum.org"* (all lower case) in the Encapsulated Vendor-Specific list, per TR-069 section 3.2, table 2.	Always
125	Vendor Specific Info Option	DHCP client (ITF) sends this option to the server (DNG) if the client supports Broadband Forum TR-111.	Conditional

A.5 DHCP Options Sent from the DHCP Server to the DHCP Client [Normative]

The table below lists the DHCP Options that *shall* be sent by the DHCP server to the DHCP client. This includes:

- Options sent from the remote/network DHCP server to the DHCP client on the DNG; and,
- Options sent from the DHCP server on the DNG to the DHCP Client on the ITF device.

Table A.4: Mandatory DHCP Server Options

Option Number	*Option Name*	*Explanation & Rationale*	*Qualification*
1	Subnet Mask	The client subnet mask.	Always
3	Router	Default Gateway/Router	Always
6	Domain Name Server	One or more DNS IP addresses available to the client. Servers *should* be listed in order of preference.	Always

Option Number	*Option Name*	*Explanation & Rationale*	*Qualification*
15	Domain Name	There are two uses/cases for this Option: a) ***Original use case***, as the client domain name, for the following situations: o when the siaddr contains the RCMS IP address; or o when the siaddr is set to the null address (0.0.0.0) and Option 43 is providing the RCMS FQDN to the client. ***b)*** ***Extended use case***, specifying the RCMS FQDN, if the siaddr field in the DHCP message contains the null IP address ***and*** there is no conflict with Option 43 with regard to the RCMS FQDN. However, if there is a conflict, then Option 43 takes the precedence over this extended use of Option 15.	The use of this Option in case b is extended from its original definition (item a) to allow it to carry the FQDN of the RCMS.
43	Vendor-specific data	The server *may* send the RCMS URL to the client using this Option. This information, if sent, *shall* meet the specification stated in TR-069 section 3.2, table 2[8].	Conditional. This Option is used in support of one of the methods used by the server to inform the client of how to reach the RCMS. If other methods are used, this Option is not required.
53	Message Type	Defines the message type of a DHCP exchange. Needed for basic DHCP operations.	Always

[8] From Broadband Forum TR-069 section 3.2, table 2, for Option 43.

Encapsulated Option	*Encapsulated Vendor-Specific Option number*	*Parameter Name (per TR-069 IGD object model)*
URL of the ACS	1	InternetGatewayDevice.ManagementServer.URL
Provisioning code	2	InternetGatewayDevice.DeviceInfo.ProvisioningCode

Option Number	*Option Name*	*Explanation & Rationale*	*Qualification*
54	Server Identifier	DHCP servers *shall* include this option in the DHCP OFFER message in order to allow the client to distinguish between different lease offers coming from different servers. DHCP servers *may* include this option in the DHCP ACK and DHCP NACK messages. Note: The content of the server identifier field is the IP address of the server.	Always
Reply to Option 55		The DHCP server is required to reply to Option 55 (sent by the client) by sending the Options specified (listed) in Option 55.	Conditional, and if the server supports a particular option.
120	SIP Option	This Option is sent from the DHCP server to the DHCP client to allow a SIP client to locate a local SIP server that is to be used for all outbound SIP requests (outbound proxy server)	Conditional Required for an IMS capable network. The network DHCP Server *shall* send to the DNG, and the DNG DHCP Server *shall* forward to the ITF device.
125	Vendor Specific Info	DHCP server (DNG) sends this option to the client (ITF) if the server supports Broadband Forum TR-111.	Conditional

A.6 DHCP References

A.6.1 Normative References

[1] IETF RFC 2131, *Dynamic Host Configuration Protocol*, 1997.[4]

[2] IETF RFC 2132, *DHCP Options and BOOTP Vendor Extensions*, 1997. [4]

[3] IETF RFC 3203, *DHCP reconfigure extension*, 2001. [4]

[4] IETF RFC 3679, *Unused Dynamic Host Configuration Protocol (DHCP) Option Codes*, 2004. [4]

[5] IETF RFC 3942, *Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options*, 2004. [4]

[6] IETF RFC 3361, *Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers*, 2002. [4]

A.6.2 Informative References

[7] Broadband Forum TR-044, *Auto-Configuration for Basic Internet Services*, 2001.[3]

[8] Broadband Forum TR-069, *CPE WAN Management Protocol*, 2004. [3]

[9] Broadband Forum TR-111, *Applying TR-069 to Remote Management of Home Network Devices*, 2005. [3]

[10] ETSI TS 102 034, Digital Video Broadcast (DVB); *Transport of MPEG2 TS-based DVB Services over IP based networks*, V1.3.1, 2007.[9]

[11] Home Gateway Initiative, *Home Gateway Technical Requirements, Release 1*, 2006.[10]

[12] IETF RFC 2563, *DHCP Option to Disable Stateless Auto-Configuration in IPv4 Clients*, 1999. [4]

[13] IETF RFC 2610, *DHCP Options for Service Location Protocol*, 1999. [4]

[14] IETF RFC 2937, *The Name Service Search Option for DHCP*, 2000. [4]

[15] IETF RFC 3004, *The User Class Option for DHCP*, 2000. [4]

[16] IETF RFC 3011, *The IPv4 Subnet Selection Option for DHCP*, 2000. [4]

[17] IETF RFC 3925, *Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol Version 4 (DHCPv4)*, 2004. [4]

[18] CableLabs CH-SP-CH1.1-C01-060728, *CableHome® 1.1 Specification*, 2006. (Main reference is Table 7-9).[11]

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

[10] This document is available from the Home Gateway Initiative.< http://www.homegatewayinitiative.org/ >

[11] This document is available from CableLabs. < http://www.cablelabs.com/ >

Appendix B
(informative)

B DNG BORDER FUNCTIONS

B.1 DNG Function Requirements

This informative Appendix describes the media and signaling requirements for Border Functions in the DNG. The four informative tables, as defined by the MultiService Forum (MSF), show the requirements and their types for various features of the DNG components. In general, a DNG contains *signaling* and *media* processing functions: S-DNG and M-DNG. It could also be desirable to have a small resident database (DB) in the DNG to store *user*, *service,* and *attachment* configuration related *files*. This storage could also include a configurable number of earlier versions of those files. Figure B.1 shows a high-level block diagram of the functions typically required in a DNG.

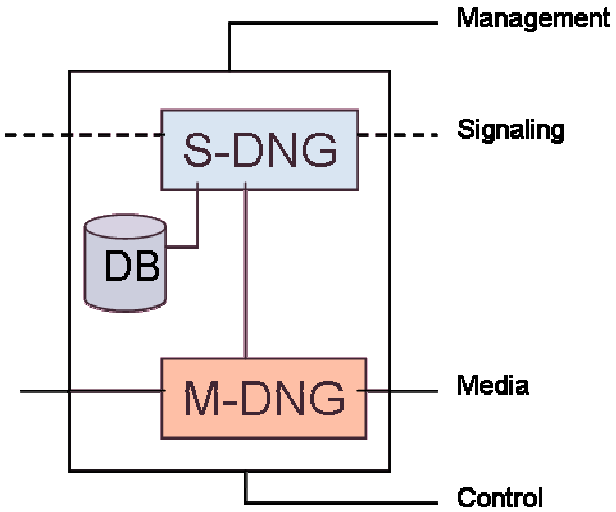

Figure B.1 : Possible Functional Entities (FEs) in a DNG

This section provides a summary of the different features required in the S-DNG and M-DNG functions. Table B.1 lists various features that are required in the M-DNG function. Table B.2 lists various features that are required in the S-DNG function.

Table B.1 : Features Required in M-DNG

M-DNG Features	Req. Type
FW/NAT	--
Firewall (Media Pinhole Control)	Mandatory
Network Address and Port translation (NAPT)	Mandatory
FW/NAT Traversal	Mandatory
Policy Enforcement	--
Protect the M-DNG and other NEs from DoS attack	Mandatory
Flow Reporting	--
Quality and SLA Monitoring (and recording)	Mandatory
Load Related Services	--
Protect the M-DNG and other NEs from DoS attack	Mandatory

Table B.2: Features REQUIRED in S-DNG

S-DNG Features	Req. Type
FW/NAT	--
Firewall (Signaling pinhole control)	Mandatory
Network Address and Port Translation (NAPT)	Mandatory
FW/NAT Traversal (e.g., support of ICE)	Mandatory
Policy Enforcement	--
Bandwidth and CAC Allocation functions	Mandatory
Interface to RACF Block (e.g., for bandwidth management)	Mandatory
Policing and Marking (DSCP)	Mandatory
Flow Reporting	--
Quality and SLA Monitoring (and recording)	Mandatory
Load Related Services	--
Protect the S-DNG and other NEs from DoS attack	Mandatory

B.2 Non-mandatory Requirements for DNG Functions

This section lists various optional requirements of the M-DNG (Table B.3) and S-DNG (Table B.4) functions. The following notations are used in the tables below:

- *CM:* This is an optional feature and if implemented is *Conditionally Mandatory*.

- *O:* Function is *Optional* for implementation.
- *NA:* Function is *Not Applicable*, and most likely it will not be implemented.

Table B.3: Optional Features of M-DNG

M-DNG Features	Req. Type
Policy Enforcement	--
Bandwidth Allocation and CAC functions	CM
Policing and Marking (DSCP)	CM
DSP Services (for both audio and video)	O
Deletion and notification of discontinued flow (media timers)	O
DTMF digit extraction and insertion (for voice service)	O
Encryption support for media flows	O
M-DNG Status Notification	NA

Table B.4: Optional Features of S-SDNG

S-DNG Features	Req. Type
Signaling Protocol Translation and Inter working	--
Perform Protocol translation between different signaling protocols	O
Signaling Interworking between v4 and v6 networks	O
Interworking between Transport protocols UDP-TCP and encryption protocols	NA
Protocol Verification and Repair	CM
Message Scrubbing for end-user Identity and Address Hiding	NA
Topology and Infrastructure Hiding	NA
Authentication Authorization Accounting	--
User/Endpoint Authentication	O
Session Record Generation and retention (local)	O
Privacy/Encryption	NA
Session Based Routing	---
User/Endpoint Registration	O
Session Routing	O
Load Related Services	--
Throttling	NA

S-DNG Features	Req. Type
Load Balancing	NA
DSP Service control	O
DTMF Digit Extraction/Insertion	O
Session statistics maintenance	O
Protect S-DNG and other NEs from DOS attack	CM
S-DNG Status Notification	NA
Handling of priority/emergency calls	O

B.3 M-DNG and S-DNG Interface Requirements

For informational purposes, this section reproduces the requirements and the capabilities of the interface between the M-DNG and S-DNG, when they operate in a distributed mode as defined in RFC 2119. Note that the usage of keywords *must*, *should, may* in this Appendix (B.3) is aligned with definitions from RFC 2119.

- *Secure Interface*: The interface *must* use cryptographically strong authentication between the M-DNG and the S-DNG and may use strong encryption for confidentiality.
- *Capabilities*: The interface *must* allow the S-DNG to request capabilities of the M-DNG (e.g., whether it is capable of doing QoS, NAT/media relay etc. functions).
- *Gate*: The interface *must* support the ability to enable/disable/modify a flow. Gating (i.e., firewall) should be available with or without media relay functionality.
- *Media Relay*: The interface *must* support the ability to insert a media relay/NAT function.
- *Source Filtering*: The interface *should* support the ability to perform source filtering. It should have the capability to relay black listed and/or white listed users.
- *CPE NAT*: The interface *must* be able to allow for signaling unaware CPE NAT devices (i.e., request behavior to update mapping when packets arrive from the CPE).
- *Virtual NAT*: The interface *should* be able to support multiple VPNs (L2, L3 based or other means) and multiple private address spaces (i.e., the ability to specify the address space and/or VPN on each side of the relay).
- *Rate limit*: The interface *must* support the ability to provide a rate limiter to limit bandwidth.
- *Marking*: The interface *must* support the ability to request marking of outgoing traffic (DSCP bits).
- *BW Allocate*: The interface *must* support the ability to allocate and modify bandwidth.
- *Replication*: The interface *should* support the ability to request a replication service (i.e., replicate packets and send them to a specific destination).
- *Statistics*: The interface *must* support the ability to provide flow statistics either at the end of the connection or else via audit whilst the flow is still active.

- *Notification*[12]: The interface *may* support the ability to inform the S-DNG that an error has occurred and a flow has been terminated.
- *DSP services*: The interface *may* support the ability to request DSP services (i.e. transcode packets from one codec to another).
- *Observed QoS information*: The interface *may* support the ability to request actual observed QoS information for each call/session.
- *DTMF digit extraction/insertion*: The interface *may* support the ability to request the extraction/insertion of DTMF digits in the media flows to support RFC 2833 devices.
- *Message Throttling*: The interface *may* provide ability to limit or throttle the number of control messages flowing through it.

B.4 References

[1] MSF-PS-SBG-001.00-FINAL, *MSF Session Border Gateway Requirements*, 2006.[13]

[12] In certain protocols, like H.248, notification is inherently supported and may be required.

[13] Available at < http://www.msforum.org/techinfo/approved/MSF-PS-SBG-001.00-FINAL.pdf >

Appendix C
(informative)

C ALTERNATIVE METHOD FOR SERVICE PROVIDER DISCOVERY USING DHCP CONTAINER OPTION

C.1 Introduction and Motivation

IPTV Service Providers often need to provide certain SP domain-specific information -- such as the entry point to SP Discovery process -- to IPTV devices located in the consumer domain.

It is desirable to pass configuration options from an SP/NP DHCP server to a Customer Premise Equipment (CPE). This appendix describes how this configuration information is passed from an SP/NP DHCP server, through the subscriber's gateway, to the CPE.

C.2 Method

Since the network attachment servers are homed in the Network Provider (NP) network, it is assumed that the SP(s) need to convey their associated discovery information to the NP. The NP DHCP server is configured with this information and provides it, upon request (using option 55), directly to the DNG DHCP server by encapsulating it in a container, the contents of which the DNG DHCP client does not process. The container option provides a mechanism through which the DNG DHCP client can pass DHCP options to the DNG DHCP server without explicit knowledge of the semantics of those options, i.e., as an opaque container. The multiple DHCP options are sent opaquely from the SP DHCP server to the DNG DHCP server (through the DNG DHCP client) and then the DNG DHCP server can explicitly process these options and pass them along to IPTV devices in the consumer network, upon request (using option 55). The details of the DHCP Container Option are being defined at the IETF. At the time of writing, the current draft was:

IETF draft-ietf-dhc-container-opt-00, *Container Option for Server Configuration*, 2008,
< http://tools.ietf.org/internet-drafts/draft-ietf-dhc-container-opt-00.txt >.

Additional information illustrating the Container Option in the context of IPTV is included in the following section.

C.3 Illustration of the Container Option in the Context of IPTV

There are 2 deployment scenarios to consider for DNG:

1) *DNG functions in bridge mode (DHCP relay)* – All DHCP messages from ITF device terminate on the SP/NP DHCP server.
2) *DNG functions in non-bridge mode* – All DHCP messages from ITF device terminate on the DHCP server located on the DNG.

The following preconditions need to be met between the Service Provider and the Network Provider if they are different entities:

- Contractual agreement exists between NP and SPs.

- SPs provide their configuration information (e.g. multicast address, ACS IP address or URL, etc.) to NP.
- NP provisions its DHCP server with the proper SP(s) configuration information.

The following network model is assumed:

- DNG supports both DHCP server and DHCP client.
- SP(s) provide configuration information to NP.

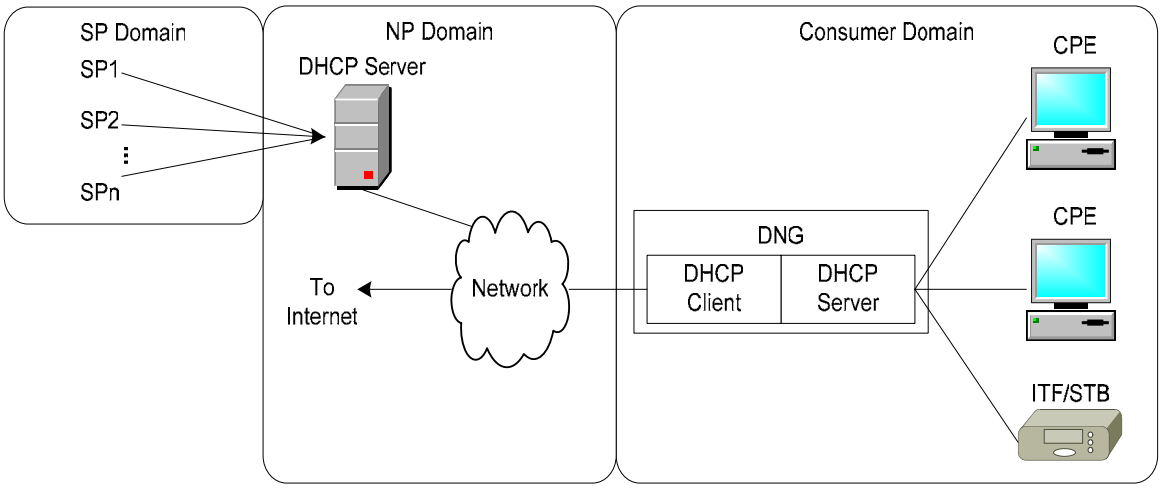

Figure C.1 : Possible Functional Entities (FEs) in a DNG

The following flow illustrates how the container option is passed through to the DNG to be delivered to the ITF device. It is assumed in this scenario that the SP and NP are the same entities and that the ITF is preconfigured with its SP information.

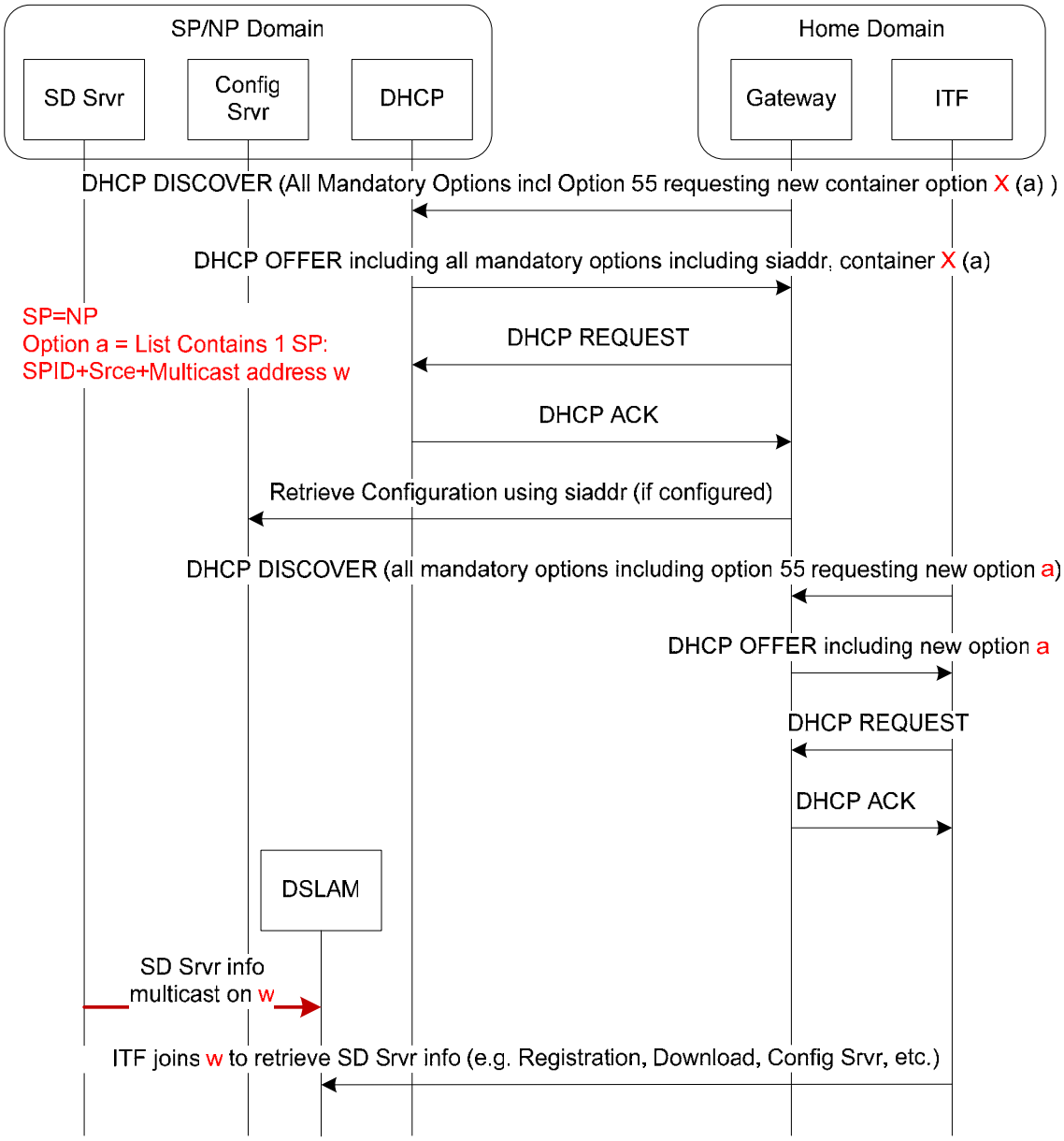

Figure C.2: Possible Functional Entities (FEs) in a DNG

The following flow illustrates how the container option is passed through to the DNG to be delivered to the ITF device. It is assumed in this scenario that the SP and NP are different entities and that the ITF is preconfigured with its SP information.

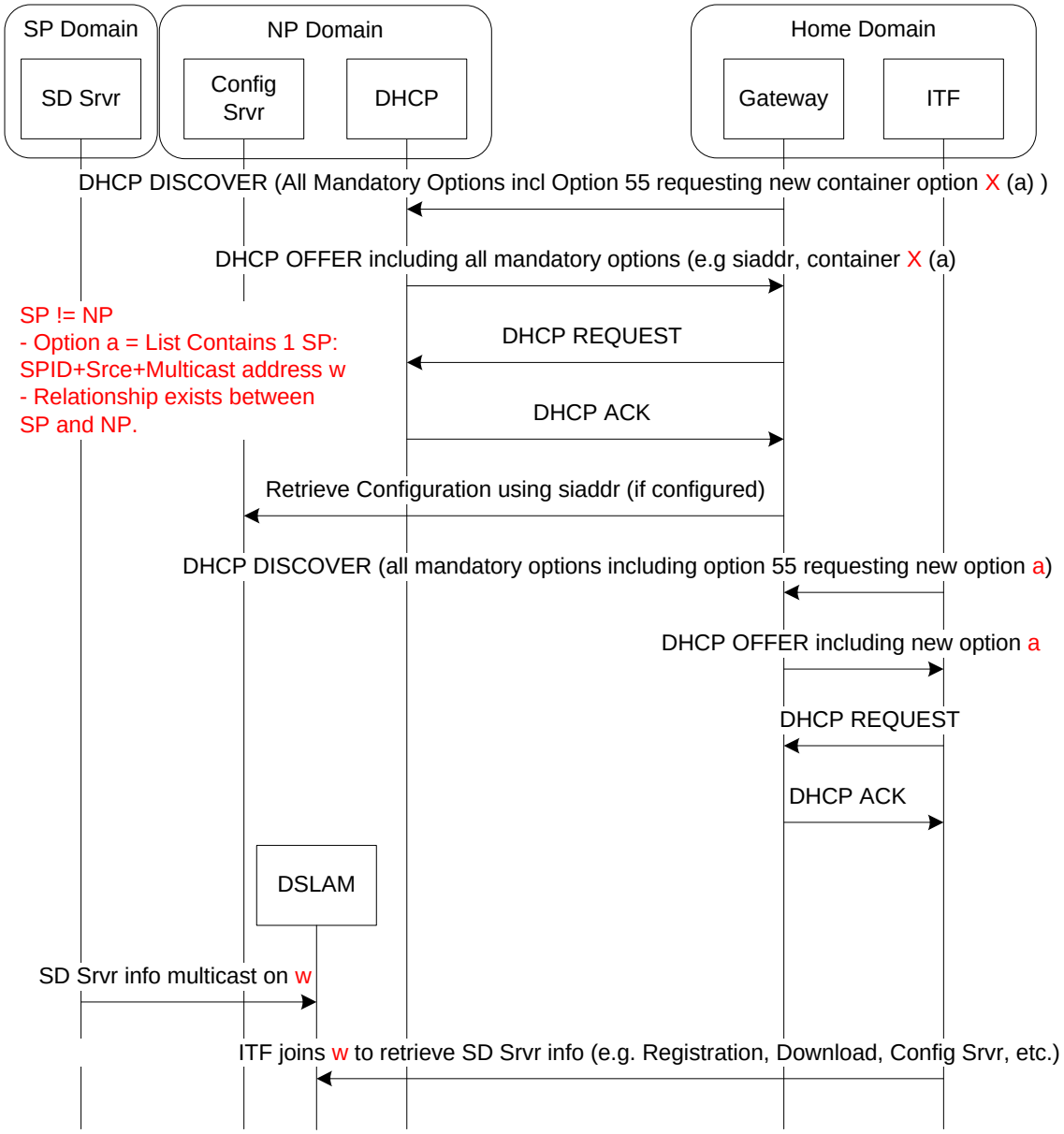

Figure C.3: Possible Functional Entities (FEs) in a DNG

The following flow illustrates how the container option is passed through to the DNG to be delivered to the ITF device. Multiple SPs are assumed in this scenario and that the ITF is preconfigured with its SP information.

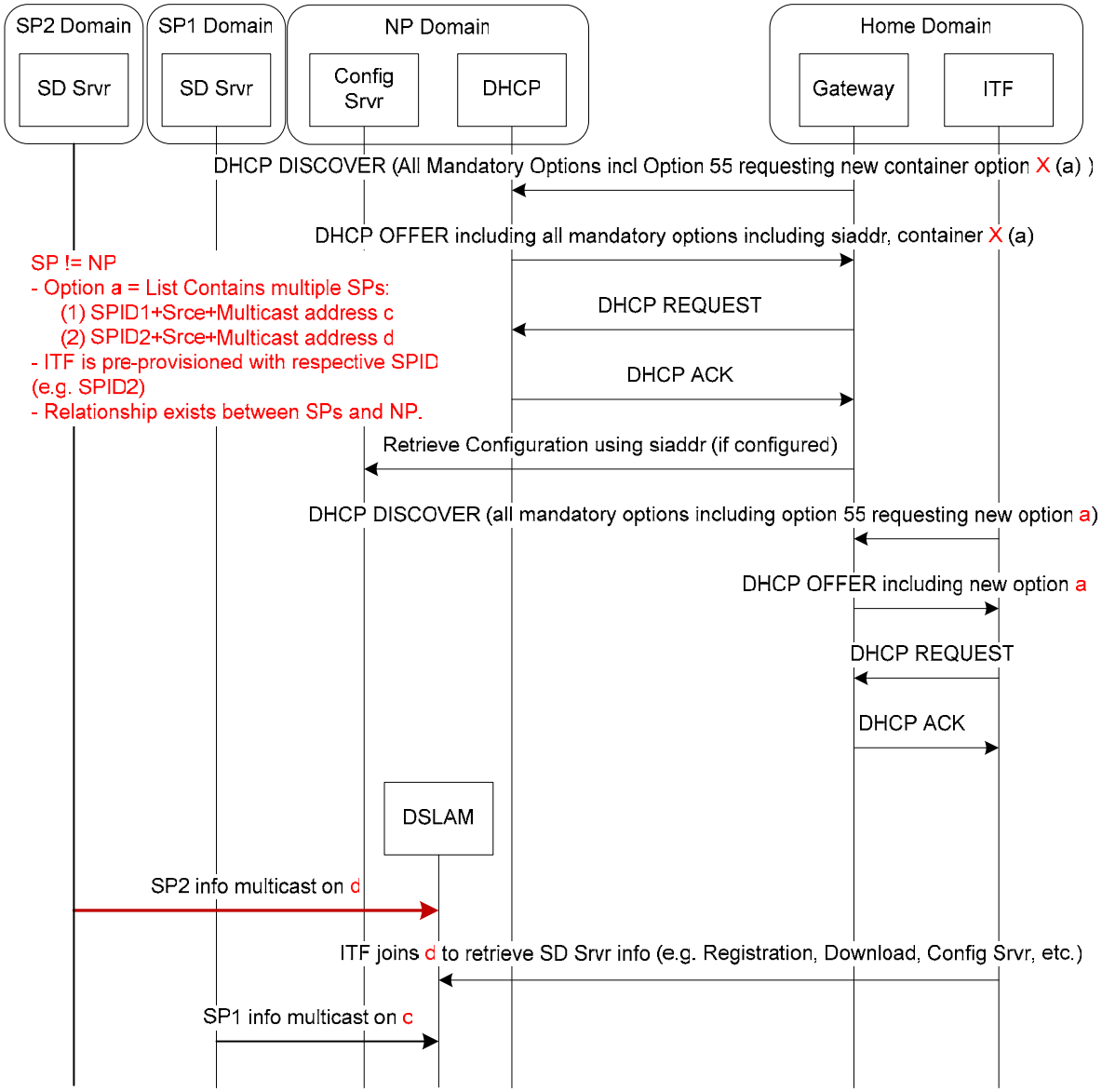

Figure C.4: Possible Functional Entities (FEs) in a DNG

Appendix D
(informative)

D DEVICE & USER AUTHENTICATION

A *device* can be authenticated by verifying against a database embedded parameters -- such as MAC address, device ID, certificate, xDSL access port, etc. A *user* can be authenticated by verifying against database credentials provided by the user -- such as a certificate or a password. For example, the NACF contains a database with information on xDSL access port associated with a subscription, and the UPSF will hold information on a subscriber profile against which authentication is performed. Authentication is typically performed during registration, attachment, or accessing some privileges.

D.1 Authentication Types Definition

D.1.1 Access Level Authentication

This involves mutual authentication of devices in customer premises and access network. Elements of NACF in the network take part in authenticating the device and providing it with access privileges. This procedure will help an operator to prevent access to unauthorized devices that can lie behind an authorized DNG.

D.1.2 Service Level Authentication

This involves authentication of a device or a user attached to a device for specific IPTV services. This level of authentication can be used by an operator to provide service differentiation.

D.1.3 Implicit Authentication

Implicit authentication performs the authentication of device by virtue of its network attachment. It relies on physical identity or logical identity associated with layer 2 connectivity. The authentication process does not always involve explicit signaling between device and the NACF.

D.1.4 Explicit Authentication

Explicit authentication requires explicit signaling and verification of an identity to be authenticated. The identity can be associated with a device or user thus explicit authentication allows for authentication of a device or a user. Explicit authentication can result in access level authentication or service level authentication or both.

D.2 DNG Authentication

Implicit authentication of DNG would allow authentication of DNG-based online ID of access segment it is attached to; or, in the case of a xDSL network, the port id on the xDSL access equipment to which it is attached.

Explicit authentication of DNG will involve signaling of some unique parameters associated with a physical DNG -- such as DNG MAC, DNG ID, DNG Certificate -- to elements of NACF involved in

authentication. For example Extensible Authentication Protocol (EAP) can be used with encapsulation provided by 802.1x or PANA.

D.3 ITF Device Authentication

Explicit authentication of ITF device will involve signaling of some unique parameters associated with a physical ITF device -- such as ITF device MAC, ITF device ID, or ITF device certificate -- to the authentication server.

D.4 ITF User Authentication

User authentication to an ITF is local to the device and could be performed through a password, etc., and stored and verified locally.

D.4.1 Using Provider NGN Authentication

If the authentication mechanism uses provider domain authentication infrastructure, then the authentication mechanism could use the approach defined by RFC 2904.

For the IPTV case, three broad participants can be identified: 1) User; 2) Authentication infrastructure (which in its simplest form would be an Authentication server); and 3) IPTV Application Server (AS). The interaction among the participants varies according to three possible messaging sequences:

1) *Authentication Agent Sequence:* The Provider Authentication Server functions as an agent between user and the AS. The user first sends a request to the Authentication server. The Authentication server authenticates user and forwards the authorization to the IPTV AS. This step can also carry configuration information to the IPTV AS. The IPTV AS sends ACK after setting up the requested configurations. The Authentication server replies to the user notifying them of AS readiness.
2) *Pull Mechanism Sequence:* The user sends a request to the IPTV AS which then forwards it to the Authentication server for verification. The Authentication server checks user identity and policy settings and sends an ACK to the IPTV AS. The IPTV AS sets up the configuration according to the policy request and notifies the user of readiness.
3) *Push Mechanism Sequence:* The user gets a ticket or certificate from the Provider's Authentication Server verifying that it is permitted for the user to have access to the service (1,2). The user includes the ticket in the request (3) to the IPTV AS. The AS uses the ticket to verify that the request is approved by the Service Provider's Authentication Server. In the push mechanism, the communication between the Authentication Server and the AS is relayed through the user rather than directly between themselves.

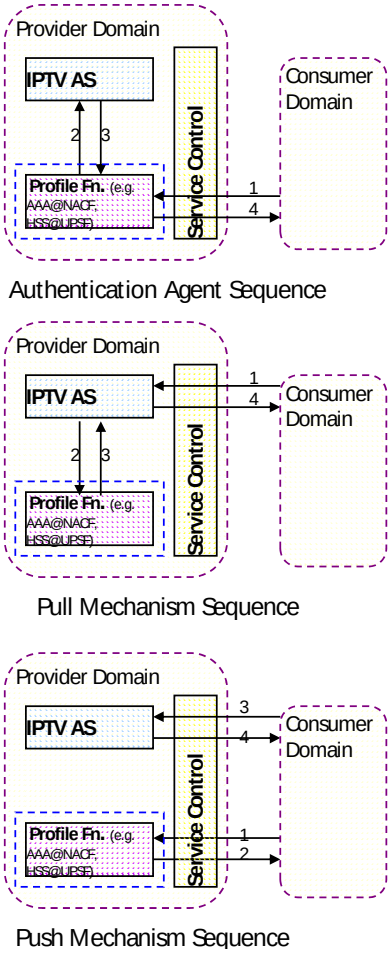

Figure D.1 : Provider Authentication for all Three Modes

The profile functions represented in the above figure are generic representations of NGN profile functions including the 'T-user Profile' at NACF and the 'Service User Profile Function' in the Session Control Function (SCF) as represented in Figure 7 of ATIS-0800007, *IPTV High Level Architecture*.

The Generic User Profile (GUP) can be seen as a data federation solution where data (user profiles) decentralized in databases can be accessed via a single point of access. An operator can choose to provide single sign-on by a GUP mechanism.

D.4.2 Using Application Server Integrated Authentication

An operator can choose not to use an authentication infrastructure in their NGN, instead performing explicit IPTV service authentication using the mechanism that is integrated with the IPTV application server. In this case, the user or ITF device credentials are transported to the AS for verification.

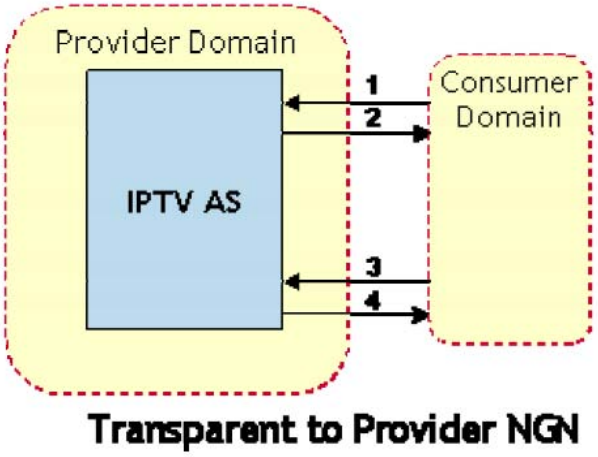

Figure D.2: AS-Integrated Authentication

Appendix E
(informative)

E SIGN-ON DURING DHCP-BASED ATTACHMENT

Sections 3.2 and 6.2 describe DHCP-based network attachment for DNGs and ITFs respectively. DHCP Option 82, if used, authenticates only the line to which the consumer is attached.

In a case where there are multiple ITFs, each ITF can be serviced by the IPTV SP with a different policy. Moreover, in a service model with multiple SPs, it is possible that certain ITFs have to be specifically identified by an SP and knowing the identity of the line (e.g., xDSL line) to the Consumer Domain is not sufficient. Authentication can occur during the network attachment phase where a minimum authentication requires a challenge-response type exchange to occur.

Here a subscriber is required to provide authentication credentials which are passed on to the AAA server. The AAA server will choose a service level based on the pre-determined policies matching the user credentials. For transport level authentication the AAA server is an Authentication and Authorization Functional entity within NACF.

Figure E.1 shows examples of the various protocol combinations that could be used for consumer domain device or user authentication.

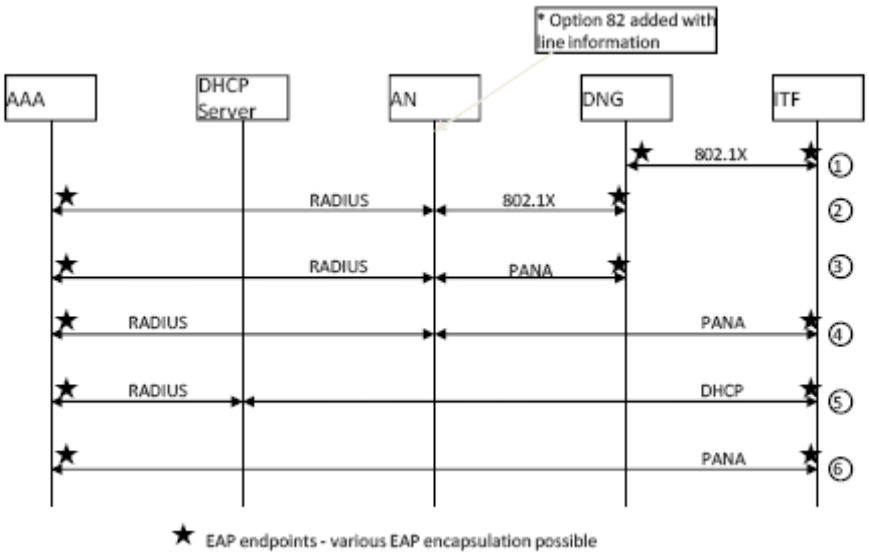

Figure E.1 : Authentication Options

The simplest form of authentication is line authentication that could be performed using 802.1X (1 in figure E.1). The limitation of 802.1X is that it cannot traverse bridges or routers and cannot be used to authenticate multiple devices attached to a line.

Cases 2 and 3 in Figure E.1 show a routed DNG being authenticated via 802.1X and PANA.

In a multiple ITF in a Consumer domain (4, 5, and 6 in Figure E.1) and multiple SP environments, it is important that an ITF is authenticated before an IP address is assigned to it. In certain network setups, it is possible that the IP address to be assigned will depend on the identity credentials provided by the

user. Moreover, each SP can use a different authentication method. Therefore, the mechanism used needs to be flexible enough to accommodate these features.

Extensible Authentication Protocol (EAP) supports multiple authentication methods and runs over a data link layer such as PPP or IEEE 802.1x, PANA, RADIUS, or DIAMETER. ITU-T Recommendation X.1034 provides guidelines for EAP based authentication. ITU-T Recommendation X.1113 provides guidelines on user authentication mechanism to enable secure home network services.

PANA (Protocol for Carrying Authentication for Network Access) is a link-layer agnostic network access authentication protocol that can carry EAP across layer 3 networks (e.g., from client to the RADIUS AAA server) transparent to DHCP. PANA is not involved in the auto-configuration process. PANA needs interaction with DHCP to enforce authentication result at layer 3.

Both EAP over DHCP and over PANA allows for multiple authentications per access line. Both allow authentications of the type subscriber per-DNG for the routed DNG case and subscriber per-device in the bridged DNG case. PANA is agnostic of IPv4 or IPv6 but EAP over DHCP currently is limited to IPv4.

E.1 References:

[1] ITU-T Recommendation Y.2014, *Network attachment control functions in Next Generation Networks*, 2008.[14]

[2] ITU-T Q.3201, *EAP-based security signalling protocol architecture for network attachments*, 2007.[14]

[3] ITU-T Recommendation X.1034, *Guideline on Extensible Authentication Protocol based Authentication and Key Management in a Data Communication Network*, 2008. [14]

[4] ITU-T Recommendation X.1113, *Guideline on user authentication mechanisms for home network services*, 2007. [14]

[5] IETF RFC 3748, *Extensible Authentication Protocol (EAP)*, 2004.[4]

[6] IETF RFC 4058, *Protocol for Carrying Authentication for Network Access (PANA) Requirements*, 2005. [4]

[14] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

Appendix F
(informative)

F GBA ARCHITECTURE & SINGLE SIGN-ON OVERVIEW

For IMS-based services, which is based on SIP signaling, the IMS security architecture handles security aspects for service access. 3GPP AKA using a shared secret in the ISIM and SUP establishes a security relation between the UE and the certain nodes in the IMS architecture (e.g., P-CSCF, S-CSCF) during the initial registration, so that subsequent message exchanges can be guaranteed to be only from authorized users and confidentiality and integrity protected.

However, a number of services in IMS-based IPTV require interactions between the UE and an AS in the network using HTTP, or other protocols such as RTSP. This can span IMS-based services, such as presence, messaging, and conferencing, or IPTV services such as retrieving an EPG. In all cases, there is no prior security relationship between the UE and the AS which provides the service, and which can be used to secure the interactions between them.

While this is described for IMS-based IPTV services, it can also be applied to non-IMS-based IPTV services as long as the Application Servers trust the IMS authentication credentials for users.

The 3GPP Generic Authentication Architecture based on TS 33.220 and TS 33.222 provides a suitable framework for securing the access between the UE and an AS, and for ensuring that only authorized users are allowed to access the various services. It does so, by bootstrapping the security relationship between the UE and a trusted node in the network to derive a common master key (secret), which can be shared between the UE and Application Servers for secure access to various services.

Figure F.1 illustrates the steps that occur during the bootstrapping procedure. It uses the push mechanism sequence as described in section D.4.1.

Initially when the UE decides to access a service such as IPTV server over the Ua interface (using HTTP, for example) it needs to acquire a key to share with the AS for securing its communications. For that purpose, the UE authenticates itself with a trusted entity in the network, the Bootstrap Server Function (BSF), over the Ub interface using 3GPP AKA (Ua and Ub are reference points defined in TS 33.220).

Once successfully authenticated with the BSF, the UE uses the integrity and protection key that it generates locally to generate the key to be used as a master key for the keys to be shared with the IPTV AS. The BSF performs the same procedure and generates the same master key.

Later on, when the UE attempts to activate the service, mutual authentication is required with the IPTV AS. By establishing a TLS with the IPTV AS, the IPTV AS is first authenticated using a server certificate. Once TLS setup is completed, HTTP digest can than be used to authenticate the user, with the UE using the shared key with the IPTV AS as the password in HTTP digest. At the same time, the IPTV AS uses Diameter or HTTP to fetch the appropriate key from the BSF node. Once mutual authentication is successfully concluded by the IPTV AS, it can verify if the user is authorized for the service. Obviously that step is skipped if the mutual authentication cannot be established.

Service authorization is based on the service access information in the user profile which is received from the BSF simultaneously while fetching the key.

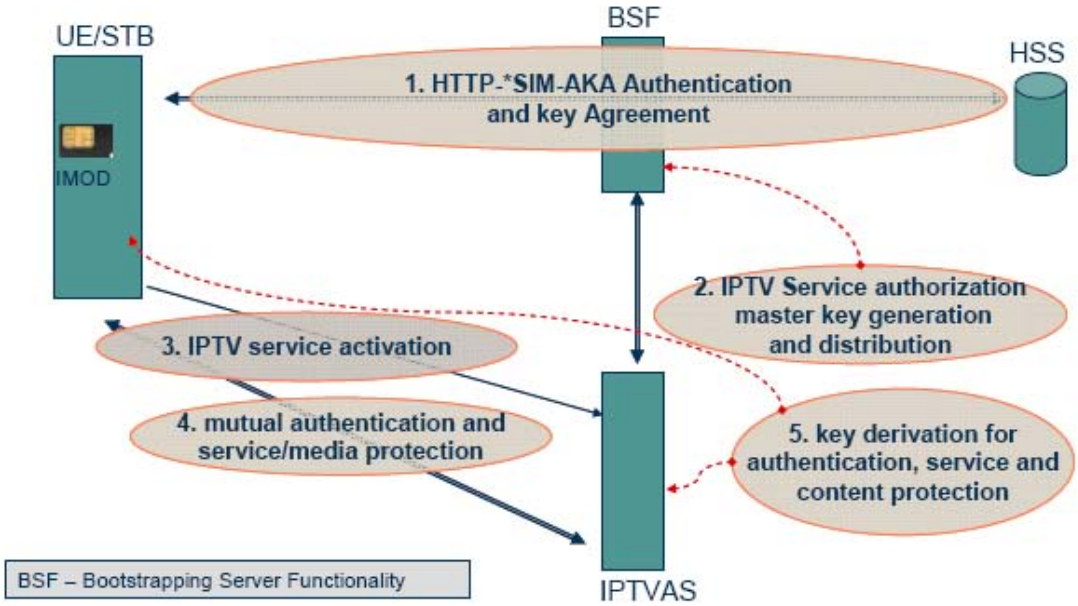

Figure F.1 : Bootstrapping Procedure

Appendix G
(informative)

G DETAILED IMS EXAMPLE

This section provides detail around one potential way of utilizing IMS to provide IPTV services. The example here would allow not only Phase I deliverables ("Linear TV"), but also is easily extensible into future applications such as Video on Demand.

The video service in this example is being modeled as a terminating service. In certain message flows below, the IMS Core is represented as a single object. This simplifies the flows and allows a focus on the client and AS components.

In the example flows that follow, the IPTV service is displayed alongside an "other service" which the example ITF is capable of providing. This is meant to highlight the operation of IPTV within the broader context of IMS and is not meant to imply any kind of extra requirements on the ITF. The "other service" is illustrative only and is outside the scope of IPTV.

G.1 Application Server Registration with IMS

There is no formal application server registration sequence in IMS. Instead, the HSS is provisioned with the public service identity (PSI) of the application server (AS). The PSI enables the I-CSCF to forward SIP requests to the appropriate AS. Because the video service is a terminating service, the IMS can use the role of the I-CSCF to forward requests to the AS using the PSI.

The HSS is configured with the filter criteria necessary to route the SIP SUBSCRIBE messages to the correct AS given that both the IPTV AS and ASes providing other network services utilize this mechanism for service data.

G.2 Subscriber provisioning on IMS

The subscriber is provisioned into the HSS. The subscriber's record in the HSS further indicates that the subscriber is subscribed to the PSI of the video application.

G.3 Subscriber SIP Registration

During subscriber registration, several key activities take place:

- The subscriber identity, or address of record, becomes associated with a particular device or contact address.
- The subscriber is authenticated by the IMS using IMS procedures as per 23.228 and 24.229.
- The IMS forwards a registration to the Application Servers. At this time, the IP Video AS will create state for the video subscriber. Note that because the AS has a trusted relationship with the IMS and all SIP messages traverse IMS before arriving at the AS, the AS can assume the subscriber is appropriately authenticated for all SIP signaling.

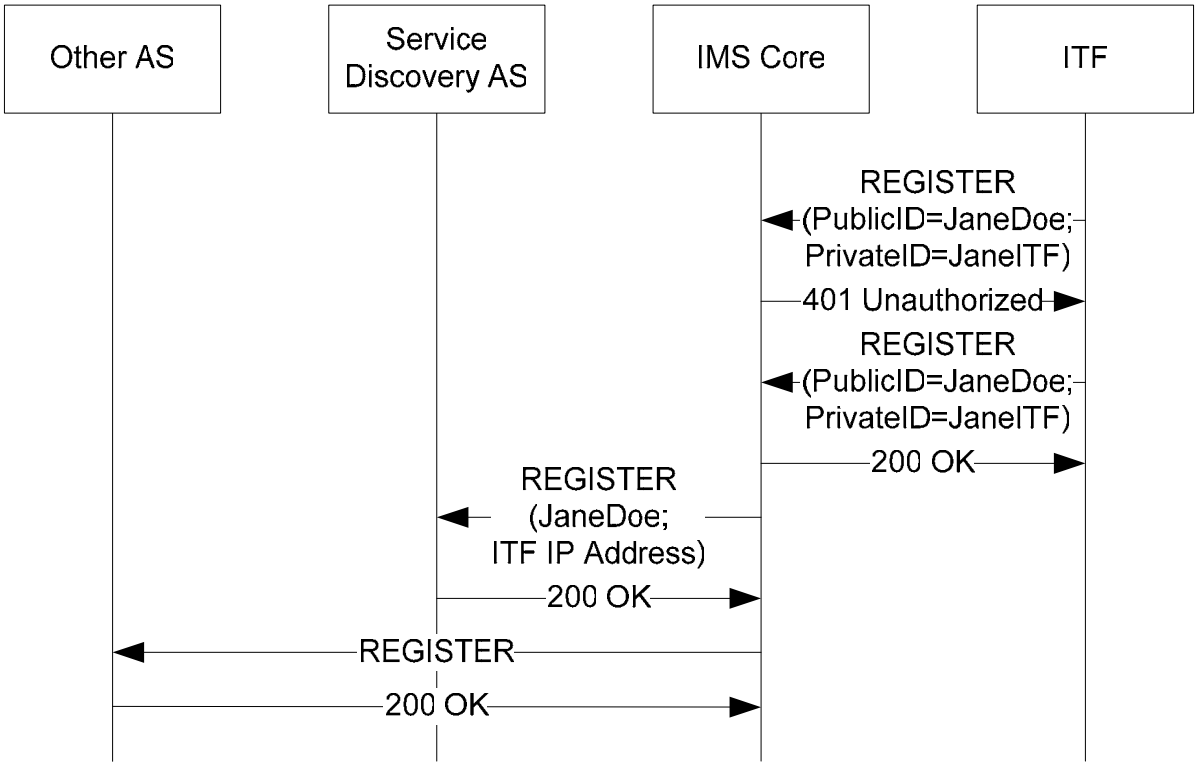

Figure G.1 : IPTV Client Registration

G.4 Content Catalogue Retrieval

As detailed in section 9.4.1, the SIP notification framework is used to request the ITF Service Data. In this specific example, the content catalogue will be obtained using this approach. This assumes IMS based authentication has already occurred and that the ITF/user has rights to the IPTV service.

The format of the content catalogue can vary from client to client. In this example, the catalogue is an XML document and is identified by a URI delivered within the body of the SIP Notify. The content catalogue includes a list of commercial assets which the subscriber is authorized to view and which are able to be played on the subscriber's currently active device. An identifier for each commercial asset is included in the catalogue. This identifier is the URI which is used for the address of the SIP Invite message which the ITF would use to later set up the video session.

Note that this example allows the usage of the SIP notification framework for delivery of client service packages from other Application Servers. This is existing behavior of the IMS and the presence of IPTV video services needs to remain transparent to it. The HSS filter criteria can be sufficiently defined such that the Subscribe messages are routed to the correct app servers based upon the event package name.

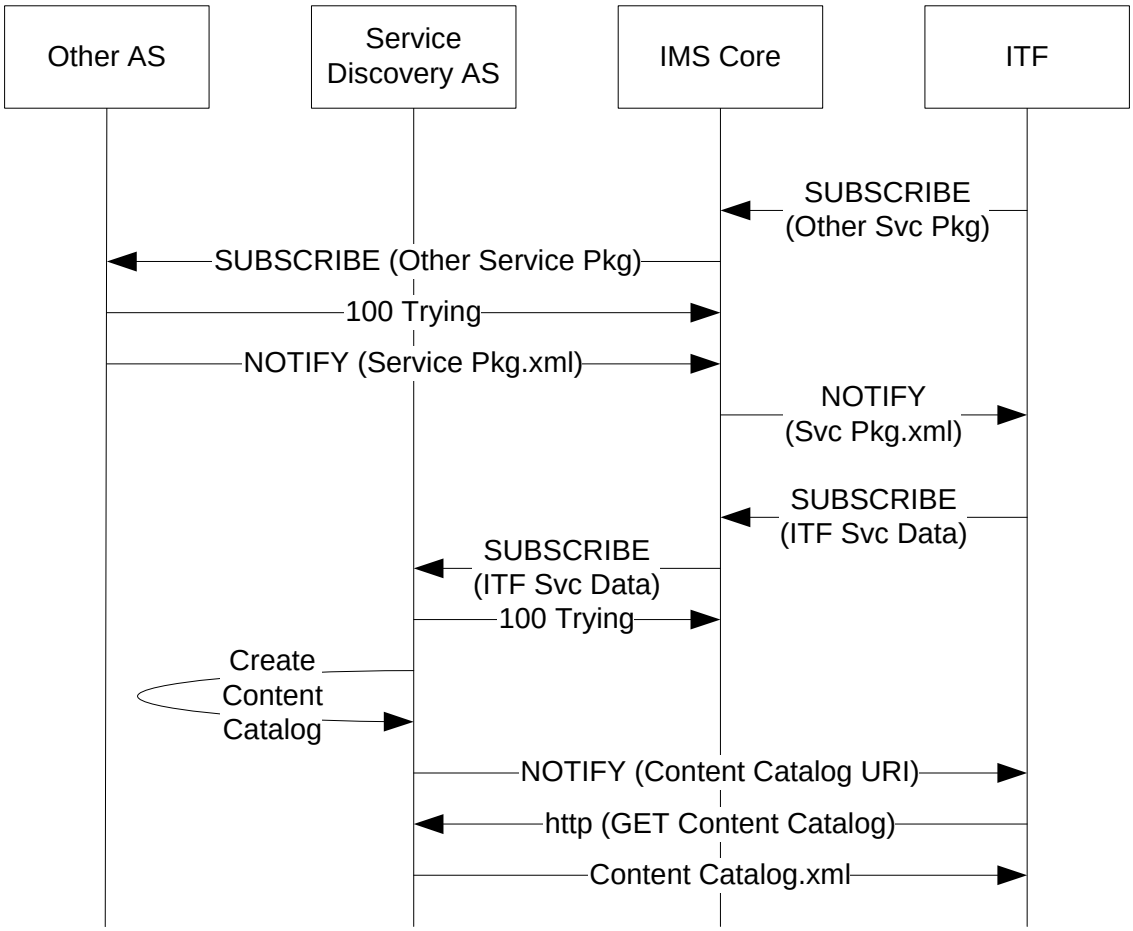

Figure G.2: IPTV Thin Client Content Catalog Retrieval

Appendix H
(informative)

H POTENTIAL OPTIMIZATIONS FOR SUBSCRIBE/NOTIFY SIGNALING EVENT PACKAGE

There are areas of potential optimization brought about by examination of the initialization process. These areas need to be studied more closely once essential network architecture and functions in IPTV phase 1 are well-established and shown to be meeting the requirements of the IPTV service.

Of note is the need to send one SUBSCRIBE for each data type that the ITF wishes to receive. There are several different possibilities that could reduce the amount of messaging required in the network to achieve this end.

To reduce this subscription messaging, an "accumulator function" can be of great use, such that the ITF sends a single SUBSCRIBE and the IPTV AS then acts as a Back-to-Back User Agent (B2BUA). The IPTV AS would provide whatever data it had immediate access to, and SUBSCRIBE itself on behalf of the ITF to other network entities that would have the rest. This function needs to be well-defined in the scope of IMS and SIP, as this kind of optimization is not unique to IPTV or the ITF. The work done on presence in the IETF can be of great use here.

How to communicate multiple data types in a single subscribe needs to also be examined. Two possibilities include special construction rules for the SIP header or the use of XML message bodies to carry that information.

Appendix I
(informative)

I ITF SERVICES DISCOVERY & SELECTION BY A THICK CLIENT USING A MULTICAST-BASED PUSH MECHANISM

When using the multicast push mechanism, typically a hierarchical configuration of the multicast signaling flows to be consumed by the ITF is used, as shown in the figure below.

The following example illustrates one possible flow classification:

- *Global Area flow (reachable by all ITFs within the SP network)*: This multicast flow carries information of interest to all ITFs in the network (e.g., Registration/RCMS hostname, software/image directory information, etc.). One Global Area flow is defined for the whole network by the SP.

- *Regional Area flow (reachable by ITFs within a given regional area)*: A Regional Area is a logical grouping of ITFs defined by the SP and can consist of multiple Sub-areas (defined below). The Regional Area multicast flow carries information of interest to ITFs assigned to that given Regional Area (e.g., System Information). Multiple Regional Areas can be defined by the SP as shown in the figure below.

- *Sub-Area flow (reachable by ITFs within a given Sub-Area)*: A Sub-Area is a logical grouping of ITFs defined by the SP. The Sub-Area multicast flow carries asynchronous and critical information (e.g., EAS, update messages) of interest to ITFs assigned to a given Sub-Area. Because of the type of data that are conveyed on this flow, the ITF never leaves it. Multiple Sub-Area flows can be defined by the SP as shown in the figure below.

  NOTE -- Conditional Access (CA) information can be provided through a unicast or multicast flow to the ITF. If multicast is used, it is sent on the flow that the ITF always listens to.

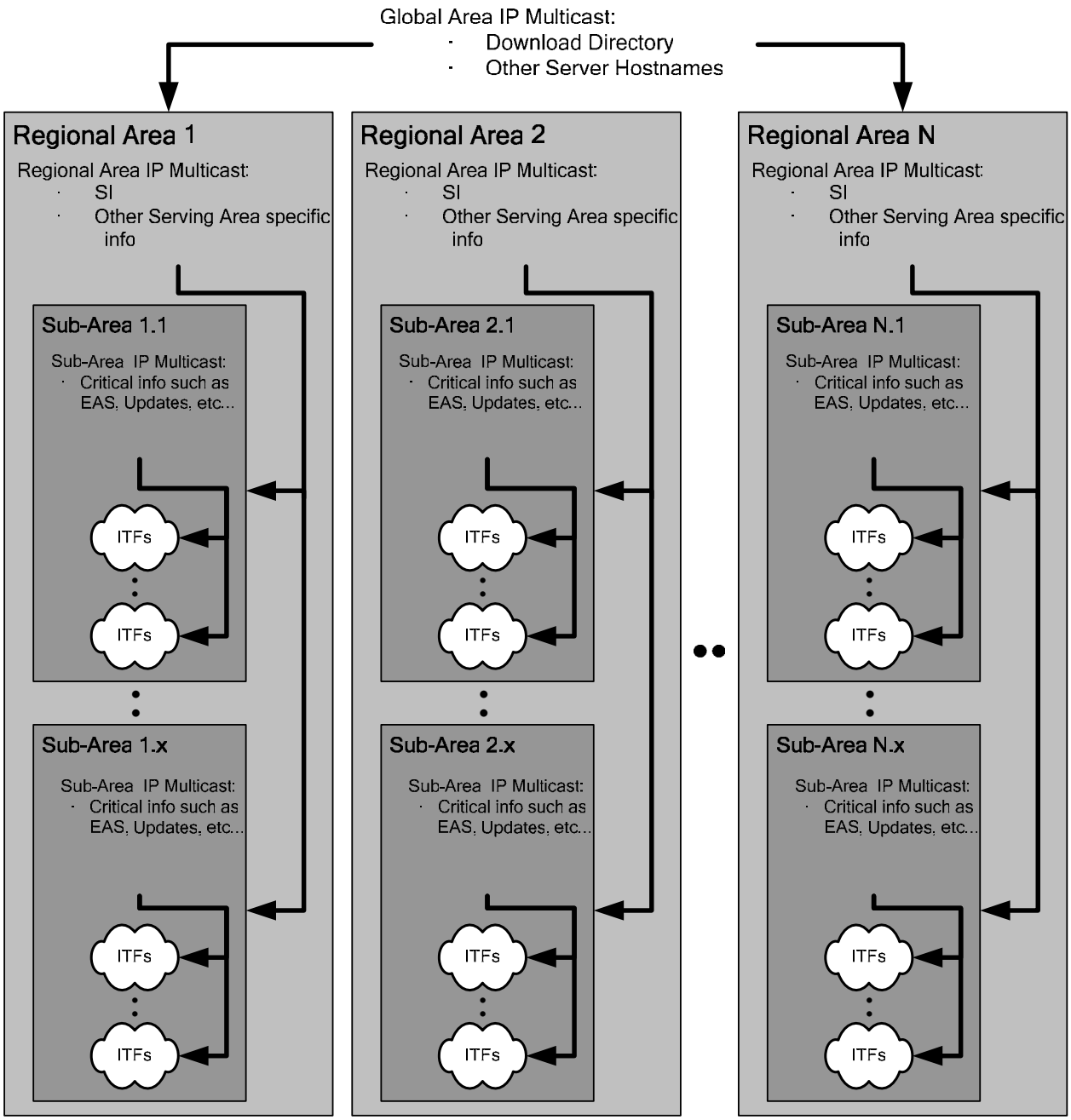

Figure I.1 : Signaling Flows Hierarchical Classification

Assuming the flow classification above, the following steps summarize the ITF initialization process (which includes Network Attachment, SP Discovery/ Attachment and Service Discovery & Selection), including how it signs on with the IPTV Application sever in order to receive the necessary signaling information that prepares it to access the IPTV services available on the network:

1. The ITF attaches to the network per section 6 in this document.
2. The ITF discovers its Service Provider using one of the alternatives (1 through 5) discussed in section 7 of this document.

3. The ITF joins its SP multicast Global stream to retrieve some IPTV Application server attachment information (shown as step 1 in the figure below).
4. The ITF sends a Sign-on request to the IPTV Application server (shown as step 2 in the figure below) which includes information about itself (e.g., MAC address, model/version #, capabilities, etc.).
5. Based on unique information provided by the ITF to the IPTV Application server, the IPTV Application server provides to the ITF a list of multicast flows needed by the ITF in order to proceed with Service Discovery and Service Attachment. This is shown as step 3 in the figure below and includes:
    a. The ITF's associated Regional Area flow information (Regional Area ID, source IP address and destination multicast address of Regional Area flow).
    b. The ITF's associated Sub-Area flow information (Sub-Area ID, source IP address and destination multicast address of Sub-Area flow).
    c. Other multicast flows (e.g., EPG) information (including their associated source IP address and destination multicast address), as defined by the operator, that the ITF needs as part of its Service Discovery and Service Attachment in order to offer service.
6. Upon successful sign-on with the IPTV Application server, the ITF joins the multicast flows (in any order) as described in the subsequent steps.
7. The ITF joins its Regional Area flow in order to collect its SI information and other regional area-specific information. This is shown as step 4 in the figure below.
8. The ITF joins its Sub-Area flow in order to collect critical information (e.g., EAS, notification messages, etc.). This is shown as step 5 in the figure below. Because of the type of data transported on the Sub-Area flow, once the ITF joins this multicast stream, it never leaves it unless it is rebooted. It needs to continuously join this stream in order to receive any EAS message and monitor any change notification concerning the other multicast flows (i.e., Global, Regional Area, and/or other streams as defined per the SP).

    When a notification message is received on the Sub-Area flow, the ITF joins the multicast group which the notification refers to in order to receive the appropriate changes while remaining a member of the Sub-Area flow.
9. The ITF joins other appropriate flows (e.g., EPG). This is shown as step 6 in the figure below).

The ITF is now ready to join any media/content flow selected by the user. The ITF device Services Discovery and Selection flow initialization using the multicast-based push mechanism is illustrated in the figure below. Note that the Network Attachment and SP discovery steps are not represented there. It is assumed that they have already been performed by the ITF.

Preconditions: All multicast flows required by the ITF are being streamed on the network. These are shown as steps "0" in the Figure below.

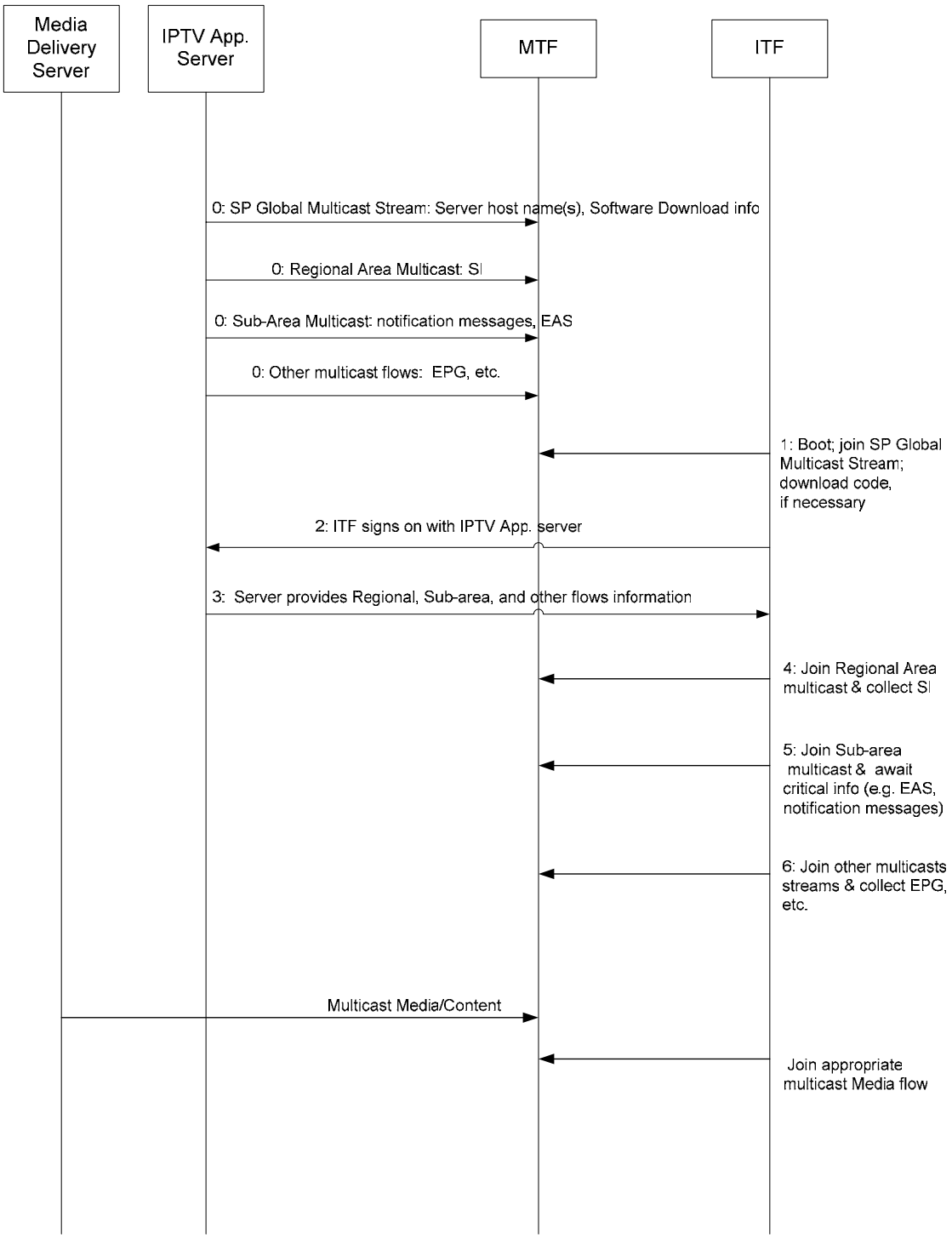

Figure I.2: ITF Services Discovery and Selection Flow