

LINEAR AND NONLINEAR VIDEO AND TV APPLICATIONS

LINEAR AND NONLINEAR VIDEO AND TV APPLICATIONS

Using IPv6 and IPv6 Multicast

Daniel Minoli



A JOHN WILEY & SONS, INC., PUBLICATION

Copyright © 2012 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Minoli, Daniel, 1952-

Linear and nonlinear video and TV applications: using IPv6 and IPv6 multicast / Daniel Minoli.

p. cm.

Includes bibliographical references.

ISBN 978-1-118-18658-9 (hardback)

1. Internet television. 2. Digital video. 3. Multicasting (Computer networks) I. Title.
TK5105.887.M58 2012
621.388'07-dc23

2011049650

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

For Anna

CONTENTS

Preface	xi
1 Evolving Viewing Paradigms	1
1.1 Overview of the Evolving Environment	1
1.2 New Content Sources and Sinks	14
1.3 Technology Trends (Snapshot)	23
1.4 Revenue-Generation Trends	29
1.5 General Infrastructure Implications for Service Providers	29
1.6 Scope of the Investigation	36
References	37
Appendix 1A Background Statistics and Forecast	40
1A.1 2009 Viewing Habits Nielsen's Data	40
1A.2 2011 Viewing Habits Nielsen's Data	43
2 An Overview of IPv6	45
2.1 Overview and Motivations	45
2.2 Address Capabilities	50
2.2.1 IPv4 Addressing and Issues	50
2.2.2 IPv6 Address Space	51
2.3 IPv6 Protocol Overview	56
2.4 Header Compression Schemes	66
2.5 Quality of Service (QoS) in IPv6	70
2.6 Migration Strategies to IPv6	71
2.6.1 Technical Approaches	71
2.6.2 Residential Broadband Services in an IPv6 Environment	75
2.6.3 Deployment Opportunities	76
References	80
Appendix 2A IPv6 RFCs	81
3 An Overview of IP Multicast and Multicast Principles	95
3.1 Multicast Environment	95
3.2 Basic Multicast Concepts and Protocols	98
3.3 IP Multicast Addresses	103

3.4 Internet Group Management Protocol (IGMP)	107
References	114
4 IPv6 Multicast Approaches	115
4.1 Overview	115
4.2 IPv6 Multicast Addresses	116
4.3 Media Access Control (MAC) Layer Addresses Aspects	118
4.4 Signaling	119
4.5 Routing	119
4.6 Rendezvous Point (RP) Approaches	121
4.7 Multicast Listener Discovery (MLD)	123
4.7.1 Overview of MLDv1	123
4.7.2 Message Format	124
4.7.3 Protocol Description	126
4.7.4 State Transition for Nodes	128
4.7.5 State Transition for Routers	130
4.7.6 Overview of MLDv2	132
4.7.7 Source Filtering	137
References	138
5 Evolving Traditional and Nontraditional TV Services	139
5.1 Basic Services	139
5.1.1 Distributed Content Service	140
5.1.2 Interactive Services	141
5.1.3 Public Interest Services	142
5.2 Advanced Services	142
5.2.1 Linear TV with Trick Mode	143
5.2.2 Personal Video Recorder (PVR) Services	143
5.2.3 Advertising Services	144
5.2.4 Audience Measurement Information	145
5.2.5 Interactive Services Requiring High Security	145
Reference	146
6 IPTV Systems and Technologies	147
6.1 Overview and Stakeholder Universe	148
6.1.1 Definitions	148
6.1.2 Services under Consideration	150
6.1.3 IPTV Stakeholder Universe	156
6.1.4 Market Scope	157
6.1.5 Multicast Mechanisms	159
6.2 IPTV Architectures and Architectural Requirements	160
6.3 QoE and QoS	166
6.3.1 QoE Aspects	166
6.3.2 QoS Aspects	173

6.4	Service Security and Content Protection	176
6.5	IPTV Networks	176
6.5.1	IPTV Multicast Frameworks	183
6.5.2	Control and Signaling Aspects	186
6.5.3	Content Delivery	187
6.6	End Systems and Interoperability Aspects	188
6.6.1	IPTV Terminal Devices	188
6.6.2	Home Network	199
6.6.3	Audience Information	202
6.7	Middleware, Application, and Content Platforms	204
6.7.1	IPTV Metadata	204
6.7.2	IPTV Middleware Architecture	206
6.7.3	Content Provisioning	208
6.7.4	Service Discovery	208
6.7.5	Service Navigation	210
6.7.6	Electronic Program Guide	212
6.7.7	User Profiles	213
6.7.8	Protocol Support Machinery for Middleware, Application, and Content Platforms	214
6.8	IPTV Standards: A Comprehensive Process	217
6.8.1	ITU-T	218
6.8.2	ATIS IPTV Interoperability Forum (IIF)	220
6.8.3	Commercial Products and Interworking	226
	References	227
	Appendix 6A Next-Generation Networks (NGN) and IP Multimedia Subsystem (IMS)	229
6A.1	NGN	229
6A.2	IMS	230
	Appendix 6B IPTV Protocols Used by IPTV Terminal Devices	232
6B.1	Network Attachment: E9	232
6B.2	Service Discovery at Various Interface Points	234
6B.3	Service Navigation: E0	235
6B.4	Service Consumption	236
6B.5	Download Services	237
6B.6	Other Relevant Protocols	238
7	Technologies for Internet-Based TV	240
7.1	Streaming	240
7.1.1	Real-Time Transport Protocol/Real-Time Streaming Protocol (RTP/RTSP)	243
7.1.2	Apple HTTP Live Streaming	248
7.1.3	HTTP Flash Progressive Download	252

7.2 Content Delivery Networks	252
7.3 P2P Networks	256
7.4 Cloud Computing	257
7.5 Core Internet Technologies	260
7.5.1 Very High-Capacity Backbone Networks, Transmission	260
7.5.2 Very High-Capacity Backbone Networks, Routing	268
7.5.3 Terrestrial Trends in Access Networks	269
7.6 Storage Technologies to Support IBTV	282
7.7 Service Provider Strategies for NTTV	294
7.7.1 Overview	294
7.7.2 Discussion	296
References	298
Appendix 7A A Perspective on the Future	299
7A.1 Global Internet Highlights	300
7A.2 Global Video Highlights	300
7A.3 Global Mobile Highlights	301
7A.4 Regional Highlights	301
8 Nontraditional Video Display and Content Sources	308
8.1 NTTV Trends	308
8.2 NTTV Display Units	309
8.3 NTTV Content Sources	311
8.3.1 Hulu	316
8.3.2 Apple	316
8.3.3 Boxee	316
8.3.4 Clicker	319
8.3.5 Revision3 Internet Television	319
8.3.6 Next New Networks	321
8.3.7 UltraViolet	321
8.3.8 Netflix	322
References	323
Glossary	324
Index	390
About the Author	407

PREFACE

Today anyone with a broadband Internet connection can see live or near-live TV from over 2,250 channels from over 140 countries, and the list is growing monthly. Tonight I can watch the nightly news from Luxembourg at [http://www.rtl.lu](http://www rtl lu) or the whole “Doc Martin” series on [http://www.Hulu.com](http://www Hulu com) from a boat marooned in the Chesapeake Bay or select from thousands of other programming choices.

New technologies, new viewing paradigms, and new content distribution approaches are about to take the TV/video services industry by storm. Five emerging trends related to the next-generation delivery of entertainment-quality video are observable, which can be capitalized upon by progressive service providers, telcos, cable operators, and ISPs. These trends are: (1) the (gradual) worldwide deployment of IP Version 6 (IPv6); (2) the (gradual) deployment of streaming and IPTV services; (3) the gradual migration of consumer viewing habits from watching linear (real-time) programming to nonlinear (on-demand/stored/time-shifted) programming (whether from a local or networked Digital Video Recorder [DVR]); (4) the greater interest and reliance on web-produced video content; and (5) the plethora of screens upon which video can be consumed: the TV screen, the personal computer screen, the tablet screen (Kindle/iPad, and so on), game consoles, and the cell/smartphone screen.

Indeed, in the developed world, at the consumer end, not only do the viewers have a variety of output devices to display video content, but also their viewing habits are changing. Nielsen found that time shifting usage with DVRs (also called “nonlinear viewing” or “Television On-Demand” by some) was up 40 percent year-over-year in recent years, with U.S. consumers playing back more than 8 hours per month (against a total TV screen-based viewing of 153 hours a month). The term “TiVo it” has entered the vocabulary just like the term “google it.” Online video watching is beginning to grow as consumers upgrade their PCs to support increased video handling and as broadband connectivity to homes becomes more pervasive. In 2009 in the United States, home consumers enjoyed over 29 hours per month of Internet-based video. Nielsen also found that mobile video viewing has grown at a rate of over 50% per year in recent years. A transition from broadcast to multicast, and even to low-density narrowcast—these last two either in linear or time-shifted/on-demand—is afoot.

Over the next few years, these changes are expected to have tidal impacts on the infrastructure used to deliver content, from broadcast TV to IP-based networks operating over fiber, to satellite delivery, to 3G/4G wireless networks,

to server-based, on-demand content distribution systems. Major sectors of the video distribution industry worry if the greater reliance on DVRs and Internet-based video streaming by consumers means an erosion or shifting of advertisement revenues. Infrastructure providers need to be keenly aware of the impact that these evolving viewer paradigms will have on their networks and even their revenue stream. An understanding of where the technology is going may empower providers to position themselves, in fact, to take advantage of these new trends.

This book is aimed at exploring these evolving trends and offering practical suggestions for how these technologies can be implemented in the service provider networks to support cost-effective delivery of entertainment, especially considering the shifts in viewing habits, and suggestions for how new revenue-generating services can be brought to the market. Chapter 1 discusses some of the evolving video consumption habits and the possible network implications. The chapters that follow cover enabling technologies. Chapter 2 provides an overview of IPv6. Chapter 3 discusses IP multicast and multicast principles, while Chapter 4 focuses on IPv6 multicast approaches and challenges. Chapter 5 describes evolving video services that are of interest to consumers, especially for service-provider environments. Chapter 6 is an overview of IPTV, which is considered to be the platform of choice for service provider-based, packetized video delivery, although it is not the only platform for IP-based video delivery. Chapter 7 looks indeed at the other platforms, such as streaming, Content Delivery Networks, Peer-to-Peer systems, cloud computing, and Internet backbones and access networks. Chapter 7 also looks at the implications of these technologies and the evolving viewing habits in terms of the kind of network evolution that may be required to optimally support end-of-decade video services. Finally, Chapter 8 describes some of the new content sources. Note, however, that the examples of commercial services and service providers identified in Chapter 8 and at various points throughout this text are intended only to depict what we believe to be persistent technical/usage trends. Some of these services, products, or providers may disappear; some providers may sunset initiatives or offerings over time; yet others will emerge. Thus, we believe that the general trends discussed here, as a whole, will persist and prevail.

This is believed to be the first book on IPv6 multicasting and/or IPv6 multicasting with applications to linear and nonlinear video distribution. This work will be of interest to planners, CTOs, and engineers at broadcast TV operations, Cable TV operations, satellite operations, Internet and ISP providers, telcos, and wireless providers, both domestically and in the rest of the world. Also, it will be of interest to set-top box developers, storage vendors, content developers, content distribution outfits, and content aggregators. This compilation is not intended to be exhaustive. Rather, it is a summary survey of generally available materials synthesized to punctuate evolving industry trends and the need for service providers to enhance their infrastructure and networks as required.

1 Evolving Viewing Paradigms

1.1 OVERVIEW OF THE EVOLVING ENVIRONMENT

Many industry observers share the view that “*The television sector is facing a challenging and an unprecedented period of transformation... Television [is] at Crossroads.*”¹ A number of forces are expected to reshape the video distribution and consumption environments during this decade. Major drivers for this evolution include (1) new viewing habits, such as time shifting for nonlinear and on-demand content consumption, (2) new distribution channels (effectively, new content providers, especially Internet-based, along with new transport mechanism, such as streaming), (3) new technologies, and, (4) standardization of Internet Protocol (IP)-based delivery, especially in conjunction multicast-based IP Television (IPTV) networks and/or with web-based content downloading (streaming) and social networks.

New viewer paradigms are evolving related to consumption of entertainment video and TV programming that can be summarized as “anywhere, anything, anytime, any platform”; namely, “from any source, any content, in any (encoded) form, at any time, on any user-chosen device, consumed at any location.” Many new TV sets that now have Ethernet networking connections built directly into the set and require no additional equipment or set-top boxes (STBs) for directly accessing the Internet; also, many high-end TVs already come with the ability to conduct video calls. In the view of some industry observers, these viewer habits, technologies, and approaches will play a part in eventually supplanting broadcast and cable television with Internet programming and distribution. While these predictions may not come to such a full dénouement in the immediate short or medium term, say, mid-decade, it is worth, nonetheless, to consider what the potential implications are for all stakeholders for the end-of-the-decade and beyond.

In this work, we refer to this new paradigm as Nontraditional TV (NTTV). New viewer approaches include, but are not limited to the following:

¹Speakers at the Future TV 2009 trade show, Paris, November 9 and 10, 2009.

2 EVOLVING VIEWING PARADIGMS

- Watching entertainment/news using the Internet (such as a TV show, a movie, or a short clip).
- Watching a multicast (rather than broadcast) entertainment/news program.
- Watching a video on-demand (VoD) program (such as a movie or pay-per-view event; VoD is also known as content on-demand [CoD]).
- Watching time-shifted TV (TSTV):
 - utilizing home-based hardware; or
 - utilizing network-based hardware.
- Watching entertainment/news with a mobile smartphone, a PDA (personal digital assistant), a videogame console (e.g., the Microsoft Xbox 360 and Sony PlayStation 3), a tablet screen (e.g., Amazon Kindle Fire/Apple iPad/B&N Nook), or a device in a car or boat.
- Watching user-generated content (UGC), particularly utilizing social networks.

In this work, time shifted implies the capture of (what was) a live-TV program, either by a customer device or a user-programmable network-resident device, for playback within a relatively short time (up to a few days). Time shifting does not include, in our definition, VoD downloads of a commercially packaged video clip from a Cable TV provider or from an Internet site. Some other related definitions are in order as follows:

- *Internet television* (also known as Internet TV, online TV) is a television service distributed via the Internet by streaming, as exemplified by services such as Hulu (for U.S. content) and BBC iPlayer (for U.K. content). The content is typically commercially produced TV material, but the “transmission/distribution” channel is the Internet; the “transmission/distribution” also includes network-resident storage (supported by video servers). Internet TV content is delivered over the open Internet as the term implies (not over a dedicated IP network). Content providers can reach consumers directly, regardless of the carrier or carriers providing the Internet backbone connectivity or Internet access. Video content is accessible from any Internet-ready computer device and is accessible around the world—a consumer does use STBs, although increasingly TV sets and STBs have direct Internet connections themselves. Video content is now increasingly available on the Internet. In the past, Internet TV has suffered from low quality; this limitation is now being progressively overcome due to greater bandwidth availability in the Internet core and in the consumer’s access. Some approaches also use peer-to-peer (P2P) protocols.
- *Web television* (Web TV, also known as web video) is a genre of digital entertainment distinct from traditional television: in Web TV, the content is created specifically for first viewing on the Internet (via broadband access and/or on mobile networks.) Web television shows, or Web series,

are original episodic shorts (2–9 minutes per episode at press time, although longer episodes may appear in the future). Some notable series include *Dr. Horrible's Sing-Along Blog*, *The Guild*, and *Prom Queen*. Web television networks included the following at press time (however, some of these also post TV-originated material): The WB.com,² MySpace, YouTube, Blip.tv, and Crackle.

- *Time-shifted TV* is a service or capability that allows the consumer to watch a TV program originally as a broadcast-, cable-, satellite-, or IPTV-transmission, that has been time shifted. The time shift service has two flavors. In a basic flavor, the user can preplan the recording of a scheduled TV program (using a local user-owned device, a local cable-provided device, or a remote network-based device); the user can watch the program any time later while still being able to pause, rewind, and resume the playout. Some systems allow the user to skip commercial advertisements during playback. In a more advanced flavor, the service allows a user to halt a scheduled content service in real time and allows the user to continue watching the program later, by providing buffering for pause, rewind, and resume functions. Some refer to time-shifted TV as “catch-up TV,” being that it allows consumers to watch a broadcaster’s program at their own convenience.
- *IPTV* is a framework and architecture that when instantiated in an actual network supports efficient distribution of (targeted) multimedia services, such as television/video/audio/text/graphics/data. The content is delivered over IP-based networks (these being IP Version 4 (IPv4) based and/or IP Version 6 (IPv6) based, instead of being traditional cable-based) that are tightly managed to support the required level of quality of service/quality of experience (QoS/QoE), security, interactivity, and reliability. Its services are provided to customers via a subscription mechanism very similar to traditional Cable TV service.

Collectively, we refer to the first two approaches listed above as Internet-Based TV (IBTV). See Table 1.1 for related concepts (table compiled from various industry sources). Internet-based devices that support IBTV viewing are becoming more popular, ranging from hybrid Internet-ready STBs and digital video recorders (DVRs), to home theater PCs (HTPCs) (that obviously are Internet-ready), to Internet-ready TV sets. These devices enable the kind of transition that is discussed in this text. An HTPC is a converged device that combines a personal computer with a software application that supports video playback; the HTPC unit is typically colocated with a home entertainment system.

²Companies named in this text are simply illustrative examples of entities that may offer technologies and services under discussion at a point in the text; named companies are generally not the only suppliers that may provide such services, and mention of a company and/or service does not imply that such entities or capabilities are recommended herewith or considered in any way better than others.

TABLE 1.1 Various Evolving TV Technologies, Services, and Approaches (Partial List)

Technology/Service	Description
Broadcast TV	One-way transmission of TV signals from one point to two or more other points.
Connected TV	TV sets with built-in Ethernet/WiFi/Internet capabilities.
Converged services	The integration of Internet, multimedia, e-mail, presence, instant messaging, mobile commerce (m-commerce), and/or services with voice service.
Internet-based TV (IBTV)	Video distribution approaches such as Web television, Internet television, and/or User-Generated Video (UGV).
Internet Protocol (IP) TV (IPTV)	Multimedia services, such as television/video/audio/text/graphics/ data, delivered over IP-based networks that are tightly managed to support the required level of Quality of Service/ Quality of Experience (QoS/QoE), security, interactivity, and reliability. Access is usually provided via a subscription service very similar to traditional Cable TV service, except for the transport network, that is IP-based (IPv4 and/or IPv6). Content is supplied to a set-top box to be watched on a TV set.
Internet television (also known as Internet TV, and/ or Online TV)	IPTV is a method of delivering video using an IP network (as an alternative to cable or satellite, but increasingly in conjunction to these systems). IPTV utilizes a closed, tightly-managed network (a “walled garden”), operated by a telecom provider, often as part of a “triple-play” bundled package (TV, Internet, and voice) [SJO200801].
Linear TV	A television service distributed via the Internet, as exemplified by services such as Hulu (for U.S. content) and BBC iPlayer (for U.K. content). The content is typically commercially produced TV material, but the “transmission/distribution” channel is the Internet; the transmission/distribution’ also includes network-resident storage (supported by video servers).
Nontraditional TV (NTTV)	A television service in which a continuous stream flows in real time from the service provider to the terminal device and where the user cannot control the temporal order in which contents are viewed. Typically found in Broadcast TV environments.
Over-The-Top (OTT) streaming devices	New viewer approaches include (but not limited to) the following: watching entertainment/news using the Internet (such as a TV show, a movie, or a short clip); watching a multicast (rather than broadcast) entertainment/news program; watching a Video On Demand (VoD) program (such as a movie or pay-per-view event); watching time-shifted TV (TSTV); watching entertainment/news with a mobile smartphone, a PDA (personal digital assistant), a videogame console, a tablet, or a device in a car or boat; and/or watching user-generated content, particularly utilizing social networks.
Package	(Also known as OTT set-tops) devices employed by viewers to watch shows or programs via multimedia and open public networks (particularly, the Internet). OTTs enable smart TVs, set-top boxes, PCs, tablets, smart phones, and game consoles to receive and process streaming video. Newer TV sets may have this functionality built in.
	A collection of content components that in some combination (either all or a subset) together provide an end-user experience and are intended to be used together.

TABLE 1.1 (*Continued*)

Technology/Service	Description
Pay Per View (PPV)	A TV service where a particular program event (e.g., a yachting race) can be bought separately from any package or subscription. The transmission of the program event is made at the same time to everyone who has ordered it.
Personal mobility	Capability to support mobility for those scenarios where the end-user changes the terminal device used for network access at different locations. The ability of a user to access telecommunication services (including video content) at any terminal on the basis of a personal identifier, and the capability of the network to provide those services delineated in the user's service profile.
Retransmission broadcast service	A service in which content is provided from various broadcasting environments, including, but not limited to, terrestrial, satellite, and cable, and retransmitted into IP network simultaneously or otherwise.
Time shifting	A function that allows playback of content after its initial transmission.
Time-shift TV (TSTV)	A service or capability that allows the consumer to watch a TV program that has been time shifted. The time shift service has two flavors. In a basic flavor, the user can preplan the recording of a scheduled TV program (using a local user-owned device, a local cable-provided device, or a remote network-based device); the user can watch the program any time later, while still being able to pause, rewind, and resume the playout. In a more advanced flavor, the service allows a user to halt a scheduled content service in real time and allows the user to continue watching the program later, by providing buffering for pause, rewind, and resume functions. There may also be advanced playout controls, for example, skipping to chapters, bookmarks, jump to time, and so on [OIP200801].
Trick mode functionality	The ability to pause, rewind, or forward stored content. A TV with trick mode is a TV service with trick mode functionality.
User-generated video (UGV)	Video content created by the user community and distributed over the web with social networks, YouTube, and so on.
VoD	(Also known as Content On-Demand—CoD) A service in which the subscriber can view commercially-produced video content whenever desired. The operating assumption is that the content is stored on the provider's VoD server. The subscriber accesses the movie from a library directory; the interface may include a search engine that accesses the movie description and rating. Subscribers typically have the ability to pause, play, rewind, fast forward the content, or even stop viewing it and return to it at a later time.
VoD trick modes	Download and streaming VoD systems provide the user with a large subset of content display control functionality, including pause, fast forward, fast rewind, slow forward, slow rewind, jump to previous/future frame, and so on. These functions are usually referred to as "trick modes."
Web television (also known as web video)	A genre of digital entertainment where the content is created specifically for first-viewing on the Internet (via broadband access and/or on mobile networks.) Web television shows, or Web series, are original episodic shorts (2–9 minutes per episode), but which may become full-fledged 30–60 minute clips in the future.

6 EVOLVING VIEWING PARADIGMS

On the other hand, new Internet-ready TV sets bypass the PC altogether and access the Internet directly; these sets support the concept of “connected TV (CTV)” [FUT201101]; CTVs are also known in some circles as “Smart TVs.” About 25% of flat panels sold in 2011 had WiFi/Internet capabilities, and about 50% of total flat-panel televisions shipped in 2015 (about 140 million units) was expected to have Internet connectivity. By the end of 2015, more than 500 million Internet-connected TVs will be in homes. TV manufacturers are (apparently) “betting” on the expansion of direct-to-consumer offerings from content producers and outfits such as, but not limited to, Netflix®. It should be noted that the adoption of CTV is not just taking place in developed regions, but also in emerging markets that have good broadband services [MEL20101]. Netflix, Amazon, and Apple are (reportedly) “banking” on the idea that the Internet in general, and cloud computing services in particular, are going to be a game changer for home entertainment, and that the TV screen can be seen as a “big iPad.”³ As an illustrative example of evolving approaches, it was announced recently that Caros Slim, a noted Mexican entrepreneur, is reportedly financing an Internet TV network, Ora.TV, that is expected to include an interview show with Larry King; Ora.TV will feature on-demand content and will produce a set of programs that, by design, will transcend traditional formats.

Table 1.2 depicts the TV population in North America in 2010; some observations about global trends are also included.

A line of investigation such as discussed in this text:

... is justified because the depth of change to the fundamental approaches being taken to providing multimedia telecommunications services ... [ITU200901].

Traditional linear TV has been around for a long time. Linear TV is a television service in which a continuous video stream flows in real time from the service provider to the terminal device and where the user cannot control the temporal order in which contents are viewed [ITU200801]. DVRs enable the process of TV time shifting; equipment of interest includes the personal video recorder (PVR) and the network personal video recorder (nPVR) (this last device also known as remote storage DVR [RS-DVR]). An nPVR is an end user-controlled device that records, stores, and plays back multimedia content (a PVR is also known as personal digital recorder [PDR]). An nPVR supports the same functionality as a PVR except that the recording device is located at the service provider’s edge node (e.g., in the STB), or in the provider’s network.

Approximately 30% of the TV viewing population was making use of time shifting at press time, although the number of hours per month watching such

³The examples of commercial services and service providers identified at various points thought-out this text are intended only to depict what we believe to be persistent technical/usage trends. Some of these service, providers, or products may disappear—yet other will emerge. Hence, we believe that the general trends discussed here, as a whole, will persist and prevail.

TABLE 1.2 TV Customer Profile in North America (2010)

Category	North America Population	Subpopulation	Notes	Prospects
Total households with TVs	116 M			Stable
Cable households	60 M (52%)	Comcast, cablevision, Time Warner, Cox, Charter cover 80% of market	Stable in North America. ROW: no major anticipated growth next few years	Stable in North America. ROW: no major anticipated growth next few years
DTH households	34 M (29%)	Dish Network and Direct TV	Stable in North America. ROW: no major anticipated growth next few years	Stable in North America. ROW: some growth next few years
Fiber/IPTV/telco households	7 M (6%)	AT&T U-verse and Verizon FIOS	Stable in North America. ROW: some growth next few years	Stable in North America. ROW: some growth next few years
Terrestrial	15 M (13%)			Worldwide growth next few years
Broadband only				

programming was still relatively small. However, these trends are expected to continue to progress until a certain quiescent point is reached. As of press time, according to Nielsen, in the United States, people spent approximately 159 hours a month consuming entertainment and news from TV and Internet sources; about 15 hours were on NTTV (10 hours : 46 minutes for TSTV and 4 hours : 43 minutes on Internet sources).⁴ Real-time linear broadcast will likely never go away in total because people also want to (continue) to enjoy a disengaged noninteractive experience, but the amount of NTTV time will definitely increase in the future. Nielsen research (see Appendix 1A) shows that between 2008 and 2011, the amount of time spend on TSTV has been growing at a compound annual growth rate (CAGR) of 20–30% a year and the amount of time spent on Internet-delivered content has had a CAGR of 30–40% a year. Some describe “TV viewers’ stampede to online as a ‘wildfire’,” and observers articulate the fact that the cable TV industry “is feeling the pressure” [LOW200901].

If one accepted that certain assumptions about the growth rates of NTTV habits continue to hold, by 2017, the traditional TV viewing time will decrease from 145 hours in 2009 to 125 hours in 2017, while NTTV will grow to 57 hours (22 on TSTV and 35 on Internet sources). See Figure 1.1 for a graphical view of these trends; Appendix 1A provides some primary data and projections.

In addition, a lot of content is now available online, both in the stored form (e.g., YouTube, Reuters, CNN, Hulu, and Netflix), as well as real time (e.g.,

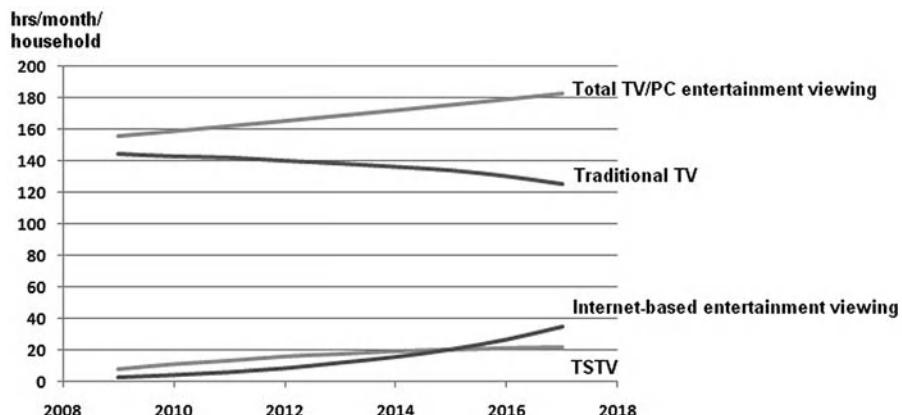


FIGURE 1.1 Apparent transition in viewing habits over time (estimated based on assumptions).

⁴Nielsen data covers the total population in the U.S. over age 2, namely 297 million Americans. Note that that this equates to about 47.3 billion hours per month in the U.S. spent on home-based video entertainment, or 557 billion hours a year.

MSNBC, CNN International, France 24, and BBC World News). Astonishingly, the website [wwiTV.com](#) listed (and linked to) over 2250 TV streaming sites at press time from 143 countries around the world—visiting the site is quite an experience. An estimated 11% of U.S. consumers ages 13–31 view streamed or downloaded video via a console at least once a month [FUT201101]. Observations such as this one may be worth pondering:

... Incumbent cable and satellite pay-TV operators face increasing competition from both IPTV operators, such as Verizon FiOS, and all the other new entrants into the market. Their greatest fear is “cord-cutting”—that subscribers will cancel their subscriptions because video via connected TV is a good enough and often cheaper alternative. One response in the USA is the TV Everywhere initiative. This aims to provide an improved service to subscribers by offering television and VoD via the whole range of viewing devices: not only TV, but also PC, smartphone and iPad . . . Internet connectivity fundamentally changes the nature of television by giving viewers access to video-on-demand, Web video and new online services, such as social networking. The last of these, using Facebook and Twitter with TV, has radical implications for the future of television viewing and the business of TV . . . [FUT201101].

The long-term outlook for DVDs and Blu-ray discs is questionable. Industry observers have noted that there are few bright spots in the DVD retail environment: the TV series box set; however, according to these observers, streamed-TV usage is growing, and it is no longer a service dominated by movies: 50–60% of streamed viewing is now for TV episodes [THO201101]. Along those lines, the following observations are important to the concepts addressed in this text:

Countries with more than 60 percent home broadband penetration include the majority of Western Europe, the USA and Canada, Australia and New Zealand. In Asian countries, such as Japan, South Korea and Singapore, penetration is 100 percent. Through broadband, many consumers are already viewing Internet video at home via PCs, laptops and smartphones. Many watch TV and simultaneously use Internet services, such as social networking. The time has now come for the television set too to go online and bring home audiences increased video choice, combined with new interactive services. Consumer electronics manufacturers, game console firms, tech companies and pay-TV operators are competing to connect home TV sets to the Internet. Each has powerful commercial imperatives for doing so [FUT201101].

The biggest threat to revenue growth [for traditional providers] will be online (or “over-the-top”) viewing, which allows users to stream programming delivered over the Internet via sites like Hulu and YouTube, and to aggregate programming via services such as Boxee [HEY201001].

Many U.S. TV networks and broadcasters (among others) now have their own websites that provide sponsored content. The Internet is being touted as the “future of home entertainment.” Press time observations describing the environment include ones such as this [AXO200901]:

Web television has matured significantly in 2009; we've seen the introduction of the "Streamy Awards⁵" . . . and the launch of more internet TV-related startups than we can count. TV-over-IP (IPTV) is starting to hit television sets thanks to set-top-boxes, TVs, and disc players with built-in streaming capabilities, and like print media before it, traditional broadcast television is beginning to grapple with the inevitability of an Internet-driven future . . .

Other changes include, but are not limited to the following [SVE201101]:

. . . In the future, believing that the TV is talking to you might not be a sign of insanity. You may be getting a Skype video call. Comcast Corp . . . plans to bring Skype calls to TV sets later this year [2011]. Subscribers will then be able to rent a kit from Comcast that includes a webcam and an adapter that plugs into the TV. A new cable box remote will include a keyboard on the back, for typing chat messages . . .

A political campaign consultant states that advertisement campaign expenditures may now be equally allocated to online ads as to TV ads [AVL201101]:

The rules of the game are shifting because convergence is finally occurring. "It matters less and less every year what screen you watch ads on . . . I'm just as likely to watch CNN on an iPad as a TV screen."

Related to Web TV, at press time, YouTube announced the creation of 100 new online YouTube channels with original programming. The company reportedly spent months working with Hollywood agencies and has secured deals with a number of celebrities. Most of these channels were expected to launch in 2012, creating about 25 hours of new programming per day. The company will reportedly share ad revenue with the content creators, giving 55% of revenue to the content creators, who it calls "partners," keeping 45% for itself. The goal is to make available professionally generated content created just for the web, just for the YouTube platform. These new channels are valuable because they are not just limited to users' laptops. With the rise of Internet-connected TVs, with interfaces such as Google TV, consumers will be able to seamlessly watch this content on their flatscreens [BOO201101].

A number of major providers make available digital (video) content for purchase over the Internet, including, among others, Apple's iTunes Store, Amazon, Netflix, and Wal-Mart; this is in addition to sites that have free (but legal) content. Observers note that consumers are finding appealing entertainment and information choices on the Internet—and have already set up data networks for their PCs and laptops that can also help move that content to their TV sets. Internet-ready TVs go a step further. For example, Netflix Inc. announced a deal with Korea's LG Electronics Inc. to make a Netflix online-video service available on a new line of high-definition TV sets from LG; the online service offers 12,000 movie and television titles [WIN200901]. Netflix had over 24 million subscribers in the United States and Canada at

⁵The International Academy of Web Television was founded in 2008 with the charter to organize and support the community of web television creators, actors, and producers. It sponsors the Streamy Awards.

press time for its online streaming service; its ability to stream Disney, Sony, and Starz movies aided its growth in recent years.⁶ Other providers are also entering the video streaming market. For example, Wal-Mart Stores Inc., the world's largest retailer, recently located its Vudu video streaming and rental service on the Walmart.com website to optimize exposure and consumer access. Vudu (a Wal-Mart division) streams films and shows to computers, certain televisions, Blu-ray DVD players, and Sony Corp's Playstation 3 [WOH201101]. Apple's iTunes Store is an online digital media store that supports digital content distribution (see Figure 1.2 for a snapshot of the storefront). The Store (site) started its service in 2003. It reportedly has over a quarter-of-a-million digital items for download, including music, TV shows, movies, podcasts, and audio books. Cloud technology is now used for content management. Around press time, Apple announced that Digital Rights Management (DRM) had been removed from 80% of the entire music catalog in the United States; however, television shows and movies are still protected under the DRM (Apple's DRM system is called FairPlay.)

While time shifting is catching on, some note that there are even more dramatic viewing habit shifts among the young. Specifically, the tendency for the young to not be happy to watch a single video stream at once, and, instead create mash-up desktops of video, audio, text messaging, and social media, all at the same time. Others may also want to watch a video mosaic, say of 2×2 , 2×3 , 3×4 , or other combination of video windows on a single (large) or multiple (wall) screens.

Although current generation of Internet-based services may in some instances (still) imply the use of small screens and the “buffering” latency phenomenon, these issues are basically driven by bandwidth availability along various portion of the Internet path or the video server; this predicament is like to improve over time, with the increasing deployment of high-capacity fiber in the (Internet) backbone and in the access network. Dense wavelength division multiplexing (DWDM) technology is propelling this transition forward. Customer connections in the 10–16 Mbps now available in many parts of the United States (and other developed parts of the world) should prove reasonably adequate as a starting point for the services envisioned;

⁶It should be noted, however, that in 2011, Netflix raised its prices for DVD delivery by mail, apparently because the company miscalculated how many people still want to receive DVDs by mail each month, a more expensive service to provide compared with its streamed Internet videos. According to observers, Netflix has been trying to lure subscribers away from its DVDs by offering cheaper plans that include movies and TV episodes delivered over its Internet streaming service. In 2010, the company began offering a streaming-only plan for \$8; yet Netflix customers were not flocking to Internet video as quickly as some analysts said the company expected. DVDs feature newer titles and the latest theatrical releases that are not available through the company's streaming service. Under the new plan, customers who want to rent DVDs by mail and watch video on the Internet will need to pay at least \$16 per month. The price hike serves multiple purposes: it may likely push more people into the streaming service, which in turn will help the firm lower its postal expenses. The company states that its future is not in the DVDs; its future is in the business of premium pay television delivered over the Internet [CUT201101]. Other pricing arrangements may be announced and/or tried in the future.

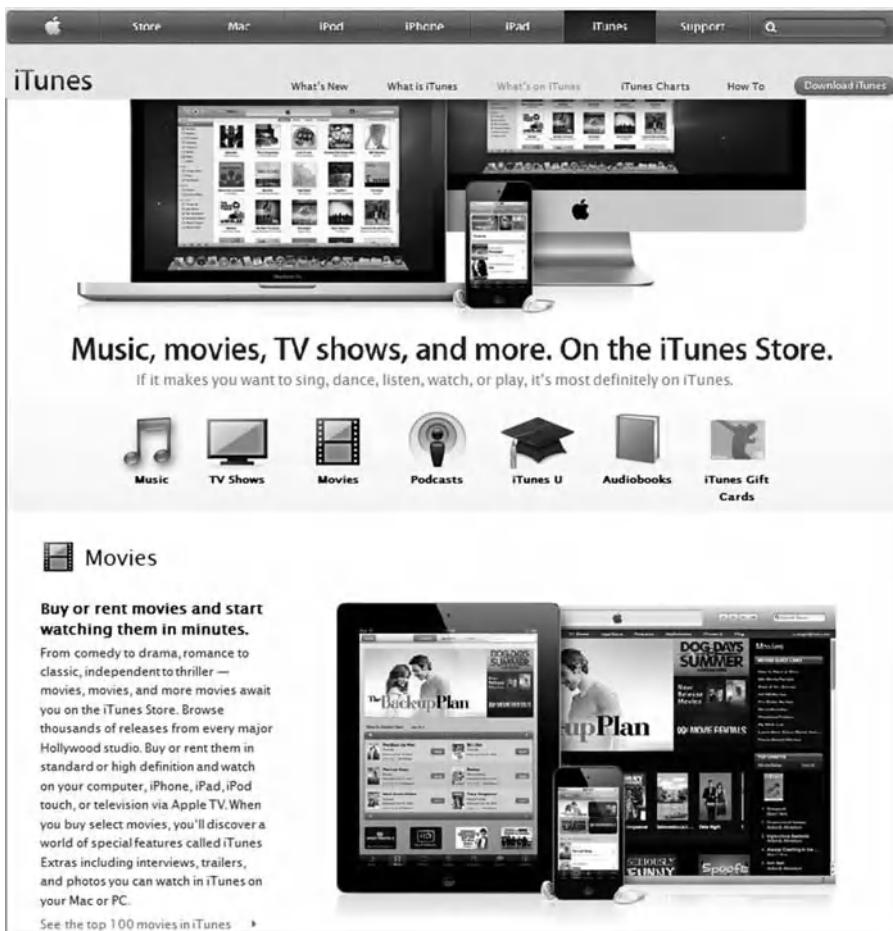


FIGURE 1.2 A snapshot of the Apple's iTunes Store storefront.

access rates of 100 Mbps, and even 1 Gbps may be available to some consumers by 2012–2013. Watching a streaming movie requiring 0.5–2.5 Mbps flow (depending on video quality) over a 16 Mbps Internet connection is not such a technical feat at this point in time (however, performance also depends on the remote server); high definition TV (HDTV) flows require around 5 Mbps.

Video rental methods are discussed next. Internet video-on-demand (iVoD) is a class of transactional digital rental methods that includes electronic sell-thru (EST) and download-to-own (DTO), but when such rental is downloaded via the Internet (rather than being done over a Cable TV network or an IPTV network). See Table 1.3 for a definition of terms. The transactional online movie market is rapidly outstripping the traditional DVD retail market. Observers called 2010 a watershed year in many respects for transactional online movies internationally; they saw it as a year characterized by the

TABLE 1.3 Transactional Digital Rental Methods

Internet Video On Demand (iVoD)	(Some also call this Interactive VoD) Transactional digital rental methods, specifically when such rental is downloaded via the Internet (rather than being done over a Cable TV network or an IPTV network.) <i>Note:</i> The term has not totally congealed in the industry. Some define iVoD as a capability that enhances traditional VoD services by providing trick modes; others define iVoD as a system that uses a consumer's home broadband connection to deliver video content directly to the TV set.
Electronic sell-thru (EST)	(Also known as Digital Retail) A method of media distribution where consumers pay a one-time fee to download a digital media file for storage on a hard drive on a computer or other system. Typically the content may become unusable after a certain period and may not be viewable using competing platforms. EST covers a gamut of digital media products, including TV content, video content, music, gaming, and mobile applications. The delivery mechanism may be the Internet or other networks (e.g., Cable TV network or an IPTV network, or a 4G wireless network.) <i>Note:</i> Some exclude delivery over the Internet in the definition of EST; we include it.
Download-to-own (DTO)	A method similar to electronic sell-thru (EST) but where the consumer may permanently own and/or be able to use the content. Some observers suggest that the increasing popularity of VoD <i>rental services</i> can be linked to the gradual erosion of support for download-to-own (DTO), or digital retail business. It believes that the majority of services operating in global markets offer titles on a rental basis due to limited availability of download-to-own titles whose fundamental business model offers no compelling case in terms of convenience or service to drive a mass-market adoption [OHA201101]. The delivery mechanism may be the Internet or other networks (e.g., Cable TV network or an IPTV network, or a 4G wireless network.) <i>Note:</i> Some exclude delivery over the Internet in the definition of DTO; we include it.

continued expansion of key services,⁷ especially outside of the United States, tapping pent-up early adopter demand for online movies (by way of contrast, analysts predict that annual store-based rental revenue will continue their almost inexorable decline) [OHA201102]. iVoD (VoD rental services with film and/or video downloaded using the Internet) is expected to grow rapidly with the increasing penetration of broadband and newer computers and/or CTVs

⁷Market research showed a 93% year on year rise in total online movie revenues in 2010 for markets outside of the United States to \$243 million. The top five international countries in terms of market size—the United Kingdom, South Korea, Germany, France, and Canada—accounted for just over three quarters of total revenues. Driving growth was a combination of the continued

with larger hard drives.⁸ Until recently, the limited playback options of movie downloads, low quality, and the effort of getting movies transferred from the desktop PC to watch them on flat panel TV screens has made movie downloads somewhat impractical for home theatre use; but the situation is changing driven by the mass availability of new Internet-ready CTVs, STBs, and services from firms such as Apple, Netflix, Amazon, Microsoft, Rovi, Sony Computer Entertainment and Wal-Mart [OHA201101].

As noted, IPTV is the well-developed formal framework and architecture for the delivery of (entertainment-quality) video programming over an IP-based network. This technology is expected to be used to deliver somewhat traditional TV services, but the technology can also be used for NTTV and for TSTV in particular. Telecom carriers are looking to compete with Cable TV companies by deploying IP video services, such as IPTV, over their networks. IPTV provides all the advantages of traditional “linear” TV in terms of service quality, combined with the many advantages the Internet offers in terms of choice and interactivity; but it should not be confused with web streaming, because images are not delivered over the Internet, but rather to homes through a “managed network.” This means TV programs do not have to compete with other traffic on the public Internet, which could negatively impact the viewing experience [ITU201001]. IPTV is a step along the transition continuum discussed in this text; other technologies and approaches are also explored.

1.2 NEW CONTENT SOURCES AND SINKS

The viewing changes discussed above, even if the projected migration to NTTV turns out to be less severe than noted in the previous paragraphs, are expected to have considerable impacts on the infrastructure utilized by providers to deliver content, for the infrastructure ranging from broadcast TV, to IP-based networks operating over fiber, to satellite delivery, to 3G/4G wireless networks, and to server-based on-demand content distribution systems.

Figure 1.3 depicts the evolving “from anywhere to anywhere, anytime” home entertainment-consumption environment that is the subject of this text. Content providers and subtending distribution channels include the following:

rollout of Apple’s iTunes, which launched in six new markets, and the first full year of operation in some regions of not only iTunes but also Microsoft’s Zune Video Marketplace and the Sony PlayStation Network. The market research firm IHS Screen Digest predicted that by 2015, the overall business of online movies will generate \$786 million, with just over half (54.3%) through traditional VoD and 45.7% from the rapidly growing Internet-based VoD [OHA201102].

⁸A press time report by Global Industry Analysts (GIA) predicted that by 2017, the global World Online Movies market will be worth \$4.44 billion [OHA201101]; others predict a market of \$1 billion in 2015 (excluding North America) [OHA201102].

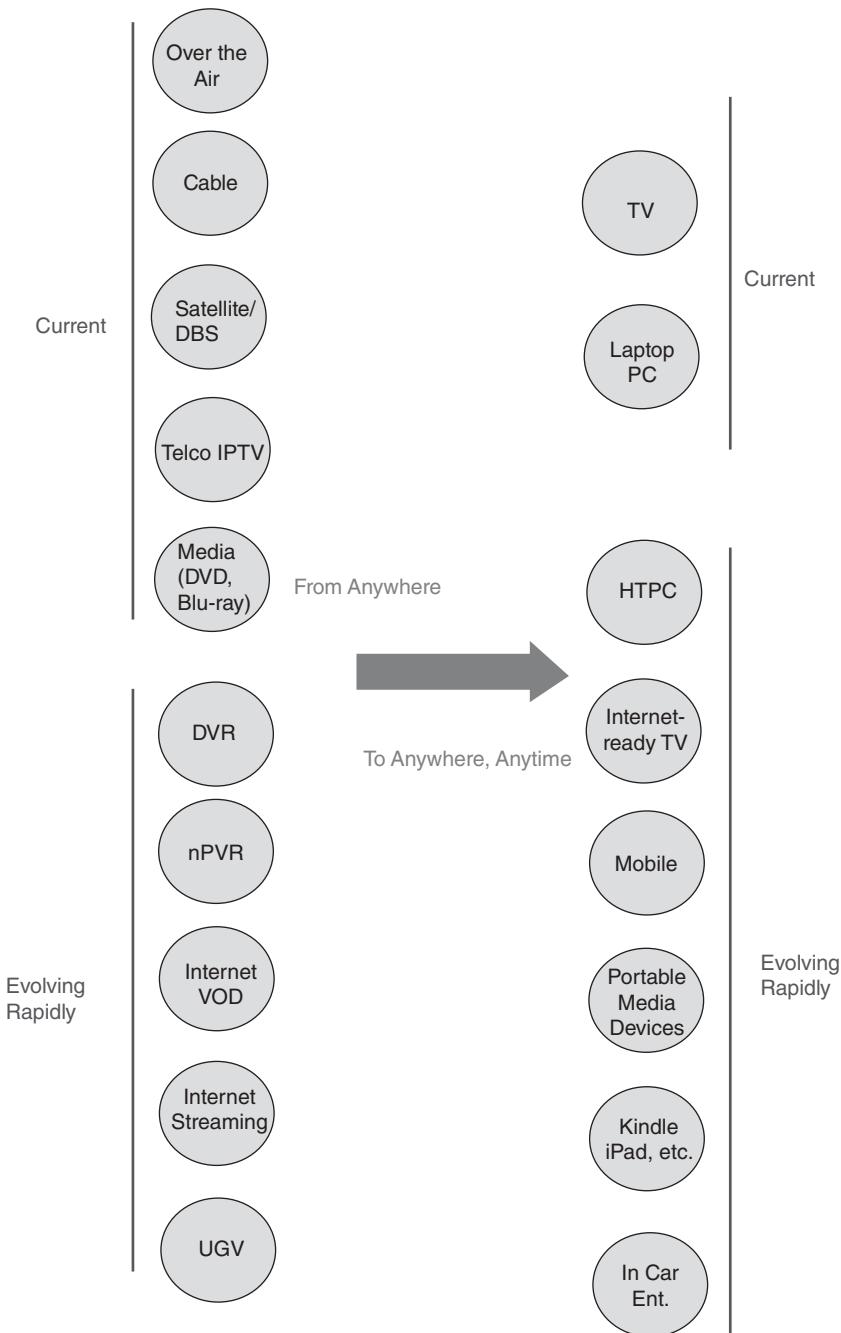


FIGURE 1.3 The evolving “from anywhere to anywhere, anytime” environment.

Traditional Content Providers/Transporters

- Over-the-air broadcasters
- Cable TV providers, also providing VoD
- Satellite backbone providers, satellite direct broadcast (DBS) providers (this also known as direct-to-home [DTH]) with satellites operation in the geosynchronous orbit
- Telecommunications carriers offering IPTV services
- Stored media sources (digital video disc [DVD] and Blu-ray Disc [BD])

Rapidly Evolving Content Providers

- DVR (consumer owned), such as TiVo-based services
- Network-based DVR, also known as nPVR—which can be seen as a form of Cloud Computing, but for video applications
- Internet-based VoD
- Internet-based streaming (real time, downloadable/commercial, network-resident such as YouTube, Hulu, and social networks, among other services. This includes all forms of IBTV.). This approach may use over-the-top (OTT) streaming devices (also known as OTT set-tops).
- User-generated video (UGV) (also called UGC)

Display devices include the following:

Traditional Display Devices (Screens)

- TV screens
- PCs and laptops

Rapidly Evolving Display Devices (Screens)

- Internet-ready TVs (also known as Connected TV)
- HTPCs
- Portable media devices, such as Kindle/iPad-like tablet devices
- Video game consoles
- Smartphones
- In-car entertainment devices

Industry observers note that data and media are being untethered from specific devices or networks. Advanced mobile devices deliver a combination of functions previously available only from multiple tools [NIE201001]. To illustrate the availability of new devices, note that in 2011 Microsoft announced that owners of the Xbox 360 gaming console would be able to start watch TV shows and other content through their gaming consoles, although most of that will not be free; content was expected to be available in more than 20 countries

[ORT201101]. Microsoft has sold 55 million Xbox 360 consoles worldwide since they were introduced in 2005. Microsoft was partnering with services, including Bravo, Comcast, HBO GO, Verizon FiOS, and Syfy in the United States, BBC in the United Kingdom, Telefónica in Spain, Rogers On Demand in Canada, Televisa in Mexico, ZDF in Germany, and MediaSet in Italy, to bring on-demand and live television content to the Xbox. Consumers will still need a subscription to Comcast or other pay TV services; additionally, some live TV channels were expected to be available. The Xbox does not replace the STBs currently used to access TV programming, but it can be used for households where members want to be able to access TV content in different rooms of the house without having to use a second STB.

Figure 1.4 illustrates the traditional TV/entertainment video distribution environment that was in place in the 2005–2010 timeframe (also accompanied by a transition from analog distribution to digital distribution for the over-the-air and cable TV sources). Each of the lines in this diagram represents detailed technical interface specifications that have evolved over the years, specific to each interface.

Figure 1.5 depicts new consumer devices that are being used to capture and display traditional TV/entertainment video. Again, each of the lines in this diagram represents detailed technical interface specifications that have evolved recently or are now emerging, specific to each interface. It should be noted that the larger content-consumption pool can actually be beneficial to the current (traditional) content providers. We mentioned earlier the HTPC; the HTPC software interface incorporates a user interface design (video scalar capability) allowing the video to comfortably be viewed at typical TV viewing distances. Commercially available HTPCs almost invariably support a “TV-out option” using a HDMI, DVI, DisplayPort, component video, VGA (for some LCD televisions), S-Video, or composite video output. A remote control device is typically supported; keyboards are also often included. Some models include DVR functionality. A HTPC can be purchased with the requisite hardware and software needed to add television programming to the PC, or can be assembled from discrete components (e.g. with software based HTPC setups). Internet-ready CTV sets offer other novel opportunities and may be more likely to succeed in the market than HTPCs. The sheer quantity of interfaces and sinks should reinforce the technical and business opportunities for providers and technology developers.

Figure 1.6 shows some new sources of video content for traditional viewing devices, along with the implicit technical interfaces required to support these sources. These sources can represent a threat to both the distribution networks of the traditional content providers, as well as to the advertisers that (ultimately) support content creation. There is also a trend related to UGV. These sources support NTTV paradigms in general and TSTV in particular. There is a large global infrastructure in support of the traditional TV content distribution model, and these “new” sources are likely to drive a rearchitecting of this infrastructure during the course of this decade. This figure illustrates

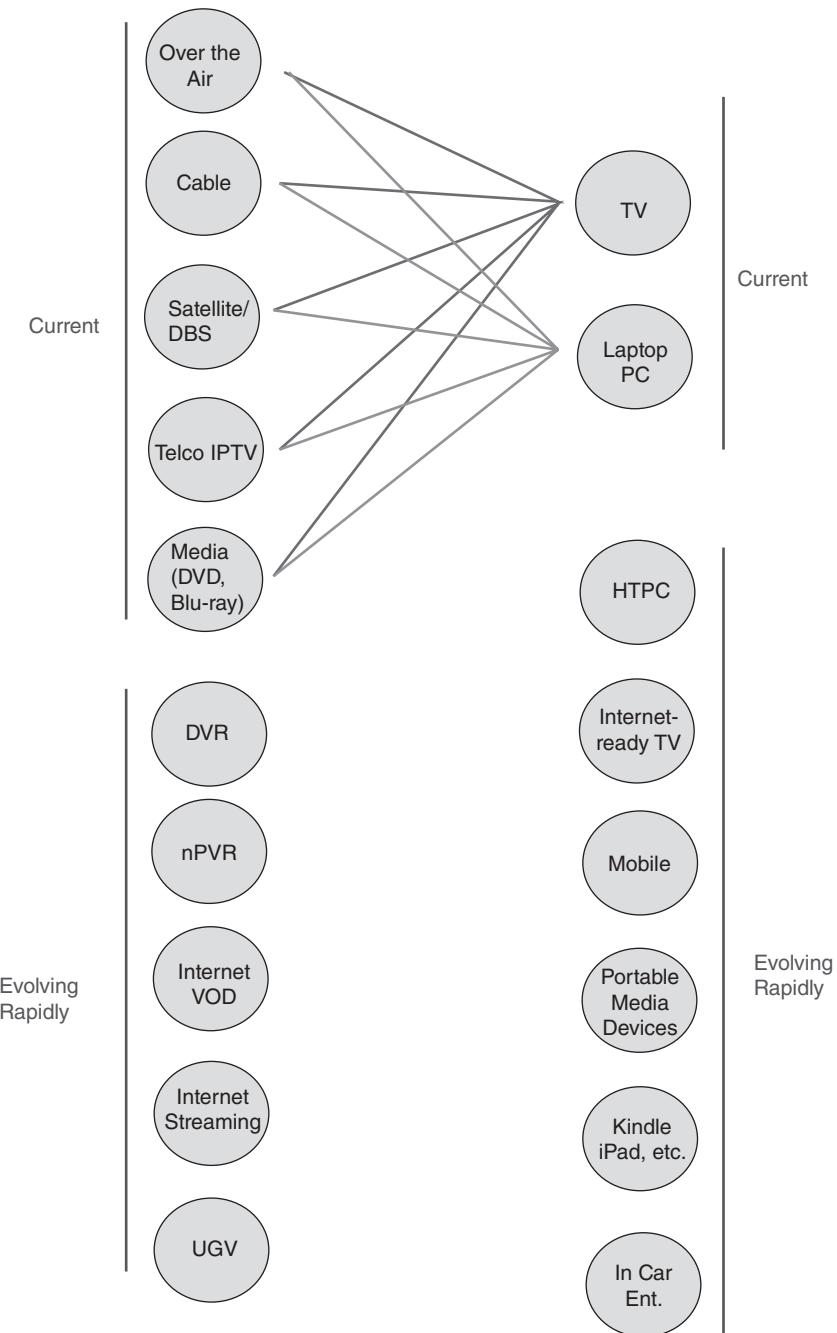


FIGURE 1.4 Traditional TV/entertainment video distribution.

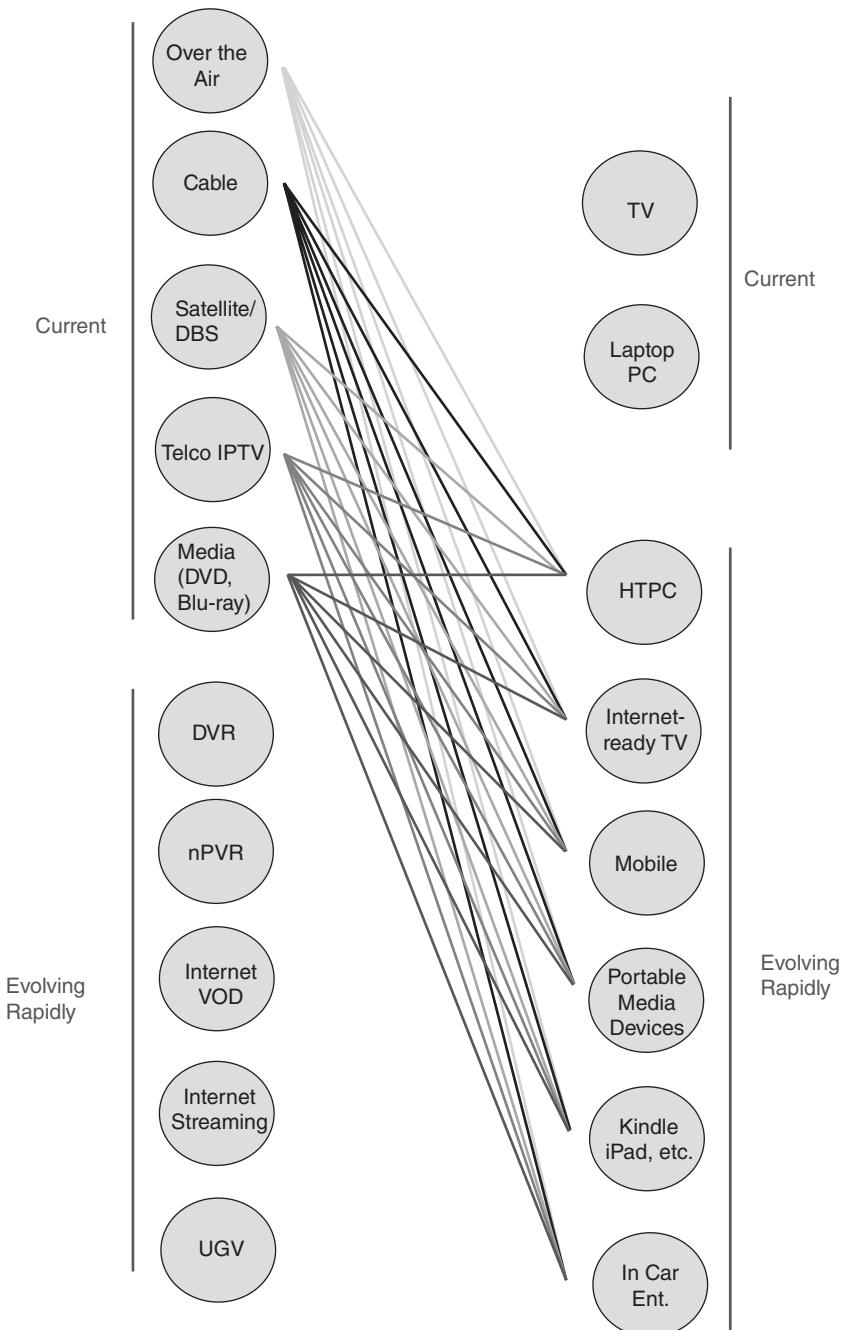


FIGURE 1.5 New consumer devices for traditional TV/entertainment video distribution.

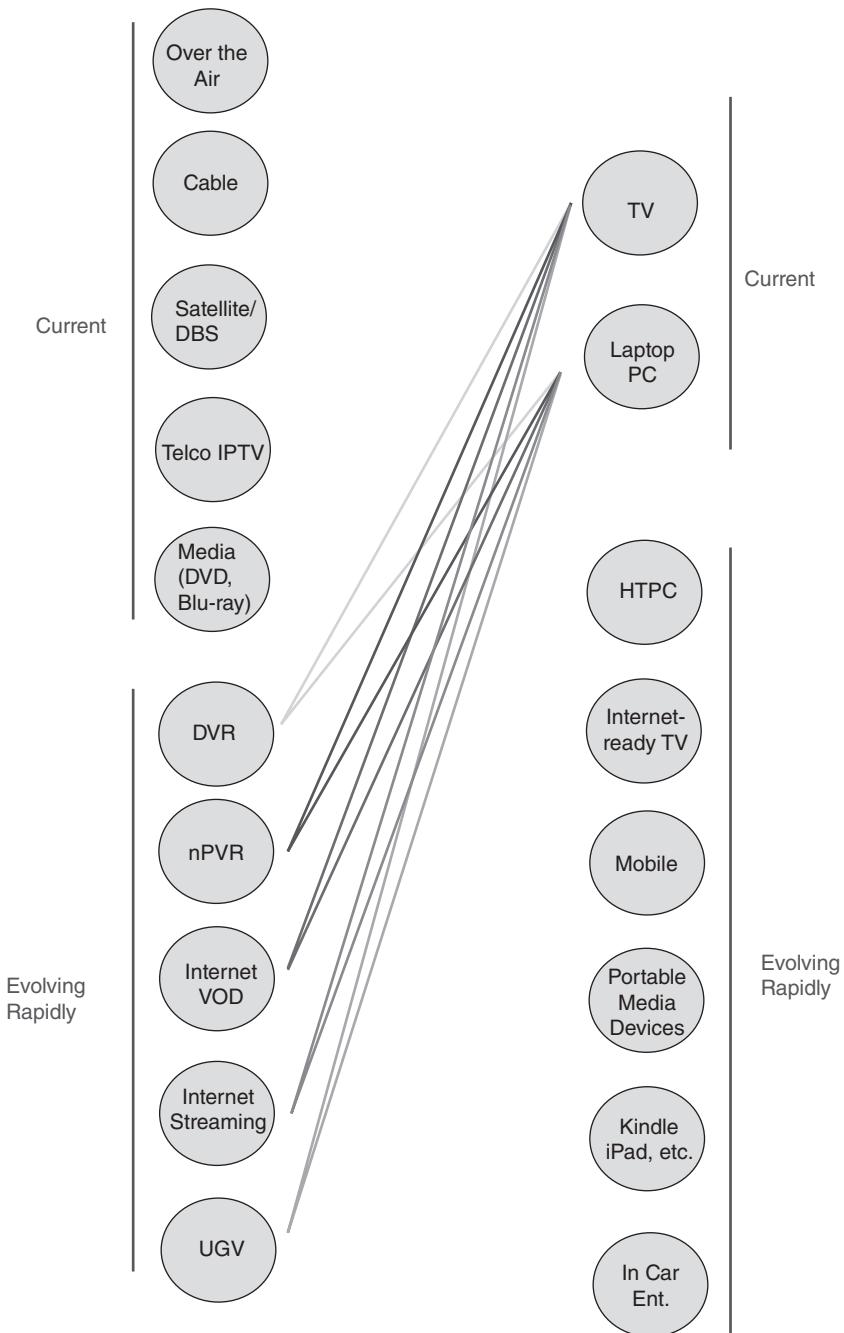


FIGURE 1.6 New sources of video content for traditional viewing devices.

where the most severe and disruptive changes to the incumbent service/content/distribution providers is likely to occur.

Figure 1.7 depicts new sources of video content for newer viewing devices. This set of evolving interfaces are perhaps the most distinct from the others identified so far; however, since the infrastructure supporting these interfaces is in a development stage, the overall impact on incumbent providers is somewhat limited. Nonetheless, the sheer quantity of interfaces and sinks should reinforce the technical and business opportunities for providers and technology developers.

Ultimately, one can view content delivery as being a *push mode* or a *pull mode*.

- Traditional broadcast TV can be seen as a *push mode* technology: the broadcaster pushes the content out, although the receiver can filter it, namely he/she can choose what subset of the pushed content is viewed at any point in time. The number of channels broadcast (both over the air and by cable TV providers) is by the hundreds.
- IPTV can be seen as a *basic pull mode* technology: the receiver selects the multicast group he/she wants to join and thus select/pull/receive content. The number of multicast groups/channels is the thousands.
- Internet/web TV can be seen as a *pure pull mode* technology: the receiver selects the file he/she wants to download (from a site such as YouTube), and, thus, select/pull/receive the content. The number of downloadable files is the tens or hundreds of thousands, and the number of combinations (sequences) of different content arrangements is $n!$, where n is the number of available files.^{9,10} The viewer can compose his/her own sequenced entertainment (some may even call it “his/her own production”).

Note: Stirling’s approximation to $n!$ is

$$n! \approx n^n e^{-n} \sqrt{2\pi n}.$$

For example,

n	$n!$	$n^n e^{-n} \sqrt{2\pi n}$	Error (%)
10	3628800	3598696	0.83
100	9×10^{157}	9×10^{157}	0.083

⁹For example, someone liking tango music/dances could identify, say, 20 clips on YouTube (or some other service), place these URLs in a PC file, and “play them once in a while” either in the linear sequence A, B, C, D, and so on first identified, or in any combination thereof: B, A, C, D; or C, A, D, B, and so on, and so on.

¹⁰Actually, one could play the same clip multiple times. In this case, the number of combinations is n^n , which is, in fact, larger than $n!$

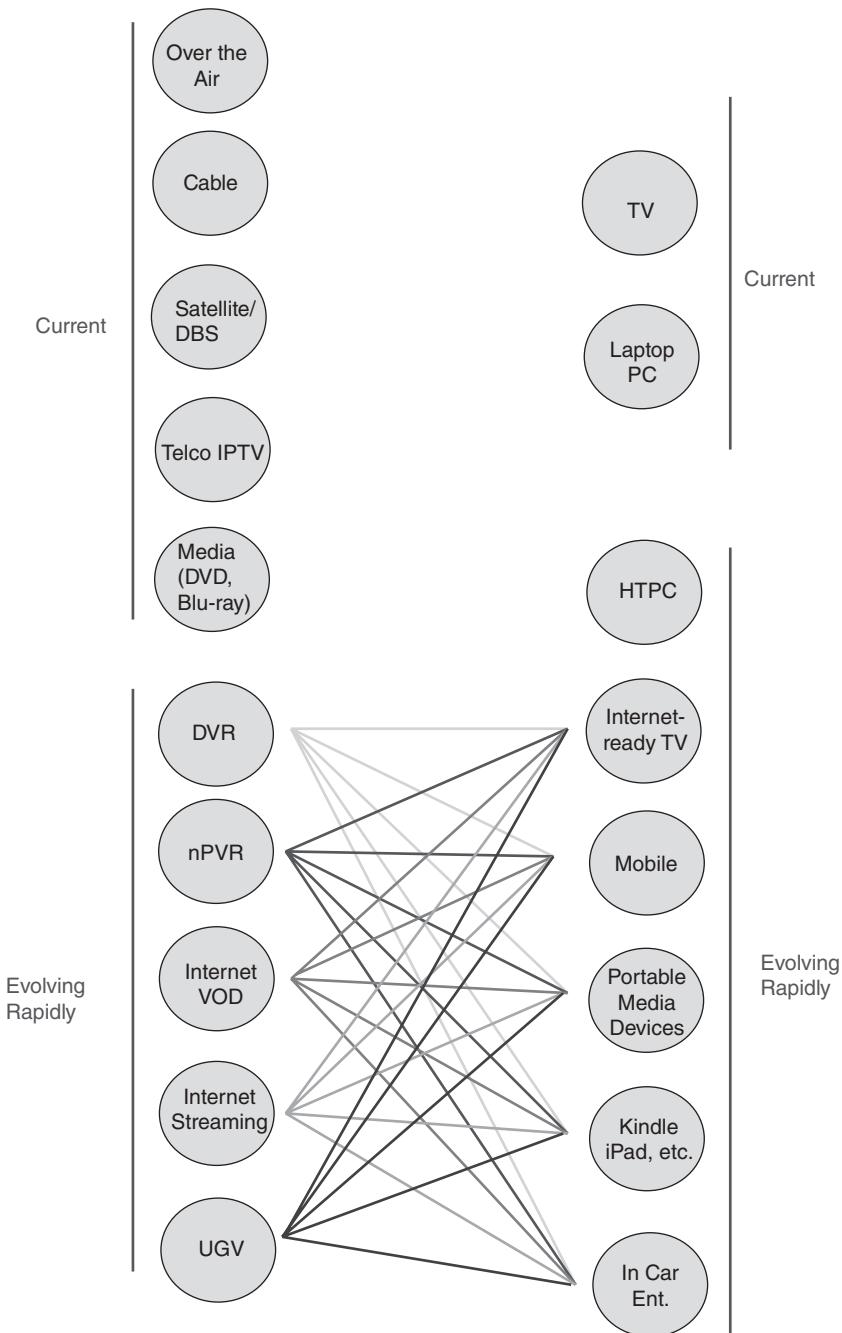


FIGURE 1.7 New sources of video content for newer viewing devices.

Some argue that with a much larger variety of content available in the Internet TV/Web TV content, even the traditional ways of using multicast and broadcast (essentially a single stream everyone watches at the same time) become less relevant. However, in this text, we hold to the principle that multicast is and continues to be a viable mechanism for content distribution for a basic pull-mode paradigm (i.e., for linear TV–VoD may continue to relay on unicast.)

1.3 TECHNOLOGY TRENDS (SNAPSHOT)

As implied in earlier sections, the basic elements of the service under discussion are (1) the content and techniques and technologies to store it; (2) the platforms and networks for distribution and reception of the content; and, (3) the customers, and their changing consumption habits. Some of the major video distribution technological drivers of the decade are seen as including IPTV, HDTV, 3-Dimensional TV (3DTV), inexpensive storage, Widgets, Fiber To The Home (FTTH), super-high-speed Internet backbones, and DVB-T2/DVB-C2/DVB-S2. Synergistic integration of the Internet and TV has been sought for the past 15 years, so far with limited success for a variety of reasons, including limited Internet access bandwidth. However, this process now appears to be picking up momentum, driven by the increased availability of bandwidth and the commercial desire to bring new services to the viewing public. Some of these technological trends are highlighted below.

The key underlying technology for NTTV is IP. Hence, our emphasis and focus of the book on IP in general, and IPv6 in particular.

New technologies and approaches include DVR systems (whether based in the home or in the network) and new IBTV streaming services, such as iTunes (iCloud), YouTube, Microsoft's Xbox, Netflix, Amazon's Video on Demand, Hulu, and Vuze. Some firms are being described as "*Reinventing TV Online*" [AXO200901]. New TV models that come to the market with software, known as widgets, that makes it easy to access Web content on TV sets using the remote control device rather than a computer keyboard. Observers state that [WIN200901]

You are going to see very broad adoption of this open technology by the best brands in the TV industry—not just for specialty products but deeply penetrated in their product lines. . . . Of course, similarly optimistic statements have been made by industry executives since the mid-1990s, when efforts to combine Internet technology with TV sets first emerged. The current economic climate could be another stumbling block, deterring consumers from upgrading their existing TV sets. Still, the topic remains a hot one in high-tech circles because of the potential impact on existing business models in the entertainment industry. Instead of the often expensive packages of video content from cable and satellite providers, the Internet could theoretically deliver a much wider array of entertainment and information choices—many of them free . . .

Observers further note that [THO201101]

Consumer spend on DVDs is in terminal decline, and the lack of mainstream consumer interest in Blu-ray as a format means the trend has not been halted, let alone reversed. Yes, in most markets, physical sales still dominate the paid video content market, but retail prices—and sales—are heading in one direction—down. In countries like the UK, there are few shops now even selling DVDs, while Amazon, the primary online retailer, has plans to convert us all to digital rather than physical content... in the absence of a legitimate alternative, consumers continue to access digital TV and movie content illegally. Yet, as Netflix has demonstrated in the U.S., when consumers are offered a legal, convenient alternative, many are happy to pay for it. In Europe we do not have that choice, and will not have until the likes of Fox actively encourage and accelerate the development of legal digital distribution services. As we have seen with the music industry, if you invest too much in squeezing the last drop out of a declining format, without investing enough in creating the digital alternative, you risk being stranded, rendered irrelevant by consumers' changing tastes.

Consumer surveys show that traditional TV will need to reinvent itself to satisfy their viewers' demands, including interactivity, Internet presence/distribution, and new programming. The range of entertainment options—including YouTube clips, online games, and pirated movies and TV shows—is luring eyeballs away from traditional television. Audiences increasingly look for niches, for example TNT, Bravo, and so on. As audiences continue to fragment, the ability to secure advertisers gets harder [GRO200901]. These trends speak to multicasting approaches (rather than broadcast) and/or on-demand sites. With regard to UGV, everyday, 100 million users watch videos on YouTube; this adds up to 3 billion watched videos each month (9 billion minutes, if each video is 3 minutes long, on the average—150 million hours¹¹).

DVRs were being enhanced at press time to include Internet access, to create what one can call Internet-ready DVR. Table 1.4 defines some of the ancillary technologies that can be used to support time shifting [ITU200701]. For example, a press time announcement indicated that TiVo¹² subscribers were now able to display Internet content, music, and movies onto their television sets more easily with new hybrid devices (called TiVo Premiere); other DVR manufacturers, such as Boxee and Roku, already offered that hybrid feature.¹³ TiVo has an intuitive interface, allowing the user to search both

¹¹Note, however, that this is $150/45,000 = 0.33\%$ of the total viewing time, even if one assumed that all the YouTube watching is from the United States, which it is not.

¹²TiVo was founded in 1997 and developed the first commercially available DVR. Its brand name became virtually synonymous with digital recorders and became a commonly used digital-age verb, much like “Google” and “blog.” TiVo had about 2.7 million subscribers in 2009 (that is down from more than 3.4 million subscriptions in 2008).

¹³The Boxee Box (a \$200 device) lets users search and store Web content and either play it on TV or share it on social-networking sites. Roku has also rolled out a digital video player (a \$100 device) that integrates television, Web content, and a video library.

traditional cable channels and online content. It is stated that TiVo reportedly “*hopes the devices will help the pioneering DVR company shore up a slipping subscriber base by catching up with how digital-era consumers increasingly seek out entertainment*” [GRO201001]. The new boxes combine access to digital cable television, movies, videos on the Web and music, including a Pandora online music service.¹⁴ The TiVo Premiere (initially selling for \$299), had 320 GiB of storage and recorded up to 45 hours of high definition programming or 400 hours of standard-definition fare; the TiVo Premiere XL (initially retailing at \$499), had a terabyte of storage and is capable of recording up to 150 hours in high definition (HD) or 1350 hours of standard definition (SD). A new search function lets users browse for shows from premium cable channels and offer a new interface for broadband sources, such as Netflix, Blockbuster On Demand, and Amazon. It is been marketed by the firm with the following description “*It's the one box that can give you access to almost anything you want, whenever you want it.*” The italicized phrase above is important because it shows that vendors, providers, and infrastructure companies cannot stand still: if they do not keep up with the developments in technology, they may lose ground. Developers of hybrid (Internet-enabled) DVRs, hybrid (Internet-enabled) TV, and hybrid (Internet-enabled) STBs see these developments in these terms [GRO201001]:

It's truly a game-changer . . . We're . . . bringing the creativity of the Web onto your TV screen.

TABLE 1.4 Technologies that Can Be Used to Support Time Shifting (Partial List)

Technology	Description
Personal video recorder (PVR)	An end user-controlled device that records, stores, and plays back multimedia content. PVR is also known as personal digital recorder (PDR). Also called digital video recorders (DVR).
Network personal video recorder (nPVR)	Same as PVR except that the recording device is located at the service provider premises.
Client PVR (cPVR)	An instance of PVR, where the end-user terminal device contains the recording capability that can be solicited and operated by end-users to record and store video, audio, and other associated data locally for subsequent playback.
Distributed PVR (dPVR)	Multiple instances of PVR, where a combination of cPVRs and nPVRs can be used to record and store video, audio, and other associated data for subsequent playback. A Home Network containing multiple cPVRs may use dPVRs in order to distribute storage of video, audio, and other data.

¹⁴The time may not be far off where the Pandora concept is applied to selection of video content (shorts).

Besides using a PC connected to a TV, or a CTV, Over-The-Top (OTT) streaming devices (also known as OTT set-tops) can be employed by viewers to watch their shows or programs via multimedia and open public networks (particularly, the Internet). OTT enable TVs, Smart TVs, STBs, PCs, tablets, and game consoles to receive and process streaming video. In recent years, OTT content from premium service providers, such as Netflix and Hulu, has become popular in the U.S. market. Apple TV¹⁵ dominated the market for media-streaming devices: Apple TV (both the first and second-generation models) had about 55% of the media streamer market based on the number of units sold during 2010 (about 3.5 million media streaming devices were sold in 2010¹⁶). Some observers argue that several issues have contributed toward the success of these devices: they are compact, cost-effective, focus purely on streaming OTT content, and forgo large amounts of storage space to instead relying instead on flash memory [SCR201101]. Other observers have a different perspective since a press time report found that about four times as many respondents said that they watched video content on a TV via a PC, rather than from an OTT set-top (the survey of users found that 41% of those that view streaming video content on the TV use a PC, while 11% utilized a video streamer/OTT box); these observers conclude that the dedicated media streaming STB might not be around in a few years since it does not make sense when there are so many other devices in the home that do the same function (many other devices offer the same services—Netflix, Hulu, YouTube, and Vudu, among others—that the dedicated streaming devices do) [HAC201101].

Other new distribution techniques are also emerging. For example, super-distribution is a paradigm for distributing digital products such videos, music, books, and software, where the products are made publicly available and distributed (although in encrypted form) rather than being sold in brick-and-mortar store or online outlets.

Naturally, networks are at the base of all sorts of content distribution. As one example in the area of network access, Google announced in early 2010 that it was planning to launch 1 Gbps consumer Internet trials using Gigabit Ethernet technology. Google stated that it was planning to become a fixed-line carrier by building out an experimental fiber-optic network; Google was not expecting to be selling services directly to consumers, but instead was planning to be offering the network on an open access basis to multiple service providers with the network managed in an “open, nondiscriminatory and transparent way.” The network was expected to cover only a limited geographic area; the baseline goal was for 50,000 people, but the firm published a potential reach

¹⁵Apple TV is a digital media receiver developed and sold by Apple; in 2010, the company announced a second-generation version of the Apple TV that can stream rented content from iTunes and video from computers or iOS devices.

¹⁶In 2010, Apple TV shipped 1.95 million units, or about 55%; Roku was second with the sales of 450,000 units, or about 13%. TiVo only sold 175,000 units, or about 5%. Some also include Logitech’s Google TV, products from Iomega, Boxee, Western Digital, Sony, and Seagate, in this category; these vendors sold under 100,000 units [HAC201101].

figure of 500,000 people. The network was intended to spur innovation and was expected to be based in the high-tech regions (e.g., Silicon Valley headquarters). This trial was expected to add to pressure on carriers such as AT&T and Verizon to deploy faster networks; some of the older Passive Optical Network (PON) FTTH technologies being deployed by carriers do not provide very high-end speeds. Another objective was to use the deployment to test new ways to build out fiber networks, learning lessons that will be shared with other carriers around the world. Google notes that the project aims to see what application developers can do with the gigabit access speeds to create next-generation applications, for example, collaborative 3D lectures and under five-minute downloads of high definition films.

Yet another trend is user-generated content and the distribution of such content using social networks. For example, Twitter¹⁷ and Facebook streams of the 2009 Emmys points, in the view of some, to the increasing irrelevance of staggered broadcast slots for the U.S. East and West coast: those on Pacific time now have to actively avoid social media or risk seeing spoilers [CAS200901]. As another social media example, in 2011, Google announced Google+, which is supporting Google's push into the social media. Standardization of IP-based delivery, especially in conjunction with social networks, is seen critical by industry observers. A quote such as the following provides a perspective on this new trend [DAW200901]:

... Big shifts will pivot around how we connect to other people and "how we share the content of our lives with others." It's all about the social use of technology ... Social networks will move towards being meshed or interconnected. They say private and public data will blur together and an advanced version of the social networks of your choice will be your browser of entry point. This is not the death of the traditional broadcaster but the role of terrestrial broadcasting of television will significantly decrease as the internet grows as a distribution system. Twitter set up the idea of sharing everything as we go; the next phase will be documented via sharing video ... IPTV¹⁸ [will] become a reality in most people's living rooms. One of the inexorable shifts in moving image viewing will be in distribution channels. Given the existing investment in broadcasting infrastructure this is not going to disappear in a hurry. But an increasing proportion of video content will be delivered over IP. Much or all of the content currently available on free-to-air will be available over IP, meaning it can be consumed across multiple devices and many situations. Managing that transition is perhaps the most prominent strategic issue of the next five years for TV channels ...

In early 2010, Google and Intel teamed with Sony to develop a platform called Google TV to bring the Web into the living room through a new generation

¹⁷Twitter is a free service that lets a person keep in touch with people through the exchange of quick, frequent answers to the question: What's happening?

¹⁸The use of the term IPTV in this context is likely to mean all IP-based TV distribution system, including streaming and IPTV proper.

of televisions and STBs. These capabilities are an example of NTTV. Google TV is a TV platform that provides a new experience by combining TV, the Web, and apps, as well as providing a way to search across them all. Google TV seeks to unite all program searches under its own User Interface (UI). Google TV aims at providing an electronic programming guide (EPG) that harmonizes content from the Internet with a user's pay TV or free-to-air offering. Google TV provides a more direct hands-on experience of Internet TV than services based on OTT mechanisms, enabling access to the open web from the TV, and offering its user interface as the central hub for all TV content, whether linear, on-demand, or OTT-based [SCR201101]. Google TV was jointly developed by Google, Intel, Sony, and Logitech. With Google TV, Google and Sony envision technology that will make it as easy for TV users to navigate Web applications, such as the Twitter social network and the Picasa photo site, as it is to change the channel. Some existing televisions and STBs offer access to Web content, but the choice of sites has generally been limited. Google intends to open its TV platform, which is based on its Android operating system for smartphones, to software developers. The company hopes the move will spur the same outpouring of creativity that consumers have seen in applications for cell phones. Google was planning to deliver a toolkit to outside programmers in early 2010, and products based on the software were planned for later in the year [BIL201001]. Google TV integrates Google's Android operating system and Google Chrome browser to create an interactive television overlay on top of existing Internet television and WebTV sites. There are two ways to get Google TV:

- on a standalone TV; and
- with a separate box, a digital media adapter (DMA), to use with current HDTV devices.

The Logitech Revue DMA, Sony TVs and Blu-Ray Disc players were the initial Google TV products available for retail. The DMA Revue was priced at \$199 at press time. Dish Networks, who partnered with Google TV to use the search capability across its pay TV EPG metadata, has been offering the box at a flat \$179 since launch to Dish subscribers.

New possible services available with some NTTV approaches also include the following:

- T-information (television information) (news, weather, traffic and advertisement and so on);
- T-commerce (television commerce) (banking, stock, shopping, and so on); and
- T-communication (television communication) (e-mail, instant messaging, Short Message Service (SMS), channel chatting, Voice over IP (VoIP), Web, multiple video conference and video phone, and so on).

Consumers may not appreciate the banners, crawls, and logos that clutter their TV screens, but they may be about to see a lot more of it. For example, in 2011, Comcast, Time Warner, Cox Communications, and other U.S. cable and satellite providers were planning to be introducing technologies that let them reach viewers with interactive pop-up ads. Cable companies have created a consortium called Canoe Ventures, which is retrofitting millions of digital cable boxes with software that lets advertisers send on-screen pitches. Bravo, USA, History, and about a dozen other U.S. channels have signed up for the service. Rovi, a U.S. provider of on-screen program guides, has developed its own T-commerce technology and signed up major networks, including NBC and Fox. Samsung, Sony, and other television makers reportedly plan to offer similar services on Web-connected TVs. Satellite operators Dish Network and DirectTV were planning to create their own systems. Ultimately, users may get targeted pitches tailored to their viewing habits. Adopting T-commerce could create new commercial opportunities for cable companies. T-commerce efforts to date, however, have not been a huge financial successes. For example, TiVo boxes deliver interactive pop-ups, although so far they have been used mostly as a way for viewers to request brochures or other information; British Sky Broadcasting has had T-commerce for a decade, also with limited success [EDW201101]. The expectations were that given the scale of the new initiative, it will be more successful.

1.4 REVENUE-GENERATION TRENDS

The new content distribution approaches discussed in the earlier sections also alter the revenue-generation model for content deliverers. Worldwide revenue derived by service providers and cable companies for IPTV, cable video, and satellite video services is forecast to grow to \$234 billion in 2013; therefore, this industry segment is substantive [HEY201001]. Figure 1.8 illustrates an evolving NTTV network. Such networks can support new revenues for the service providers. Except in the case where the consumer purchases the video or movie outright, advertisement is the major vehicle for revenue creation. Table 1.5 depicts some typical (new) approaches, some of which were already hinted in the previous sections [REE201001].

1.5 GENERAL INFRASTRUCTURE IMPLICATIONS FOR SERVICE PROVIDERS

The key question of interest to many planners and researchers is “What will be the TV/content distribution model of the next 10–20 years?” The answer depends on the region of the world. In those developed and high-density, metropolitan locations where fiberoptic and broadband Internet services are readily available, (for example, in the East Coast and West Coast areas of the U.S.) there will be a gradual shift to IBTV/NTTV and/or also IPTV, with an erosion of the Cable TV delivery of TV-packaged content in favor of content

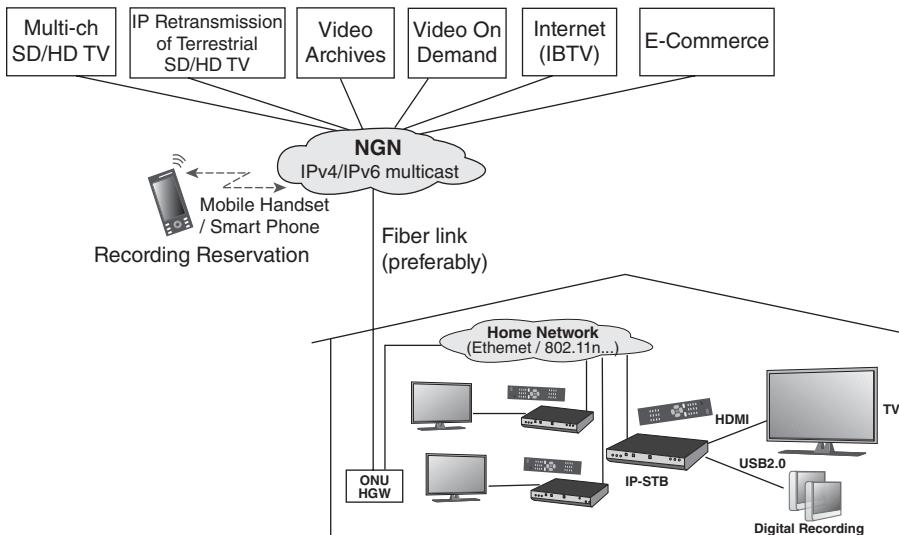


FIGURE 1.8 Example of network providing advanced video services.

provided via Internet service providers (ISPs) in the former case (IBTV/NTTV) and telephony carriers in the latter case (IPTV). In the central states of the U.S., DTH will continue to be important. Europe has had a strong DTH tradition for the past 20 years, and the Cable TV side has been underdeveloped. Hence, DTH will continue to be a strong factor in both Western and Eastern Europe, with IBTV/NTTV and IPTV in the wings. In the rest of the world (Brazil, Russia, India, China, and Africa), DTH will continue to be a strong factor for many years with IBTV/NTTV and IPTV in the wings, but further out in the future.

The infrastructure used to deliver content will have to be tuned to the evolving user-driven requirements. At the macro level, additional in-the-network storage and Internet streaming capabilities will be needed (additional in-home storage may also develop). Increased use of terrestrial IP-over-fiber connectivity will inevitably occur. Global IP traffic is expected to increase fourfold between 2011 and 2016, growing at more than 30% per year, with a large proportion of that expansion will be in the emerging markets [SOR201101]. Packet video delivery is now taking place over fiber (and wireless) infrastructure that use IP Version 4 (IPv4) streams. The expectation is that by the mid-decade and beyond, infrastructure based on IPv6 in general, and IPv6 Multicast in particular, will be the desired canonical approach to video distribution for NTTV, especially to support the migration from broadcast to multicast (and/or narrowcast) and from linear to nonlinear video consumption paradigms. Multicast supports communication between a single sender and multiple simultaneous receivers. Content is streamed to a number distribution servers, usually operated by a network or service provider; these servers, in turn, stream the

TABLE 1.5 Video Ads and Approaches for IBTV

Approach	Description
Ad overlays	A small, semitransparent overlay across the screen (usually on the bottom, but can be anywhere) of an online video, similar to what one often sees during TV shows. These ads usually show up 15 seconds into the videos they are on, and last for 10 seconds.
In-banner video ads	Approach that leverages the banner space to deliver a video experience as opposed to another static or rich media format. The format relies on the existence of display ad inventory on the page for its delivery.
In-page video ads	Approach where ads are delivered as a standalone video ad and do not generally have other content associated with them. This format is typically home page or channel-based and depends on real estate within the page dedicated for the video player.
In-stream video ads	Approach where ads are played before, during, or after the streaming video content that the consumer has requested. These ads cannot typically be stopped from being played (particularly with pre-roll). This format is frequently used to monetize the video content that the publisher is delivering. In-stream ads can be played inside short- or long-form video and rely on video content for their delivery. There are four different types of video content where in-stream may play: UGC, Syndicated, Sourced, and Journalistic.
In-text video ads	Approach where ads are delivered from highlighted words and phrases within the text of web content. The ads are user-activated and delivered only when a user chooses to move their mouse over a relevant word or phrase.
Monetized video	Online videos that generate revenue by themselves. This is usually accomplished by advertisements in and around the video content, but can also be accomplished by charging users to watch, download, or subscribe to the videos.
Nonlinear video ads	An ad product that runs parallel to the video content such that the user still has the option of viewing the content. Common nonlinear ad products include overlays that are shown directly over the content video itself, and product placements that are ads placed within the video content itself. Nonlinear video ads can be delivered as text, graphical banners or buttons, or as video overlays.
Overlay ad	A banner ad that appears in the bottom 20% of the video window. Click action initiates a linear video spot or takes the user to a website. Sold to advertisers on a Cost Per Thousand Impressions (CPM) basis and/or Cost Per Click (CPC) basis.
Pay per click (PPC)	Online advertising payment model in which payment is based on qualifying click-throughs. The content publishers get paid a set rate for every click on the advertiser's material.
Skin ads	Advertisements that appear in a video player skin, that is, the graphics surrounding where a video plays.

content forward to users. Multicast is ideal for linear video distribution but is not by itself ideal for VoD; hence, a service provider should plan to support (IPv6) multicast for linear TV and (IPv6) unicast for nonlinear TV (including VoD). Peer-to-peer technology may also be used; some researchers in fact argue that IPv6 protocol can provide an excellent environment for P2P-based applications (a press time study found that 61% of IPv6 traffic is P2P-related—but IPv6 traffic is still just 0.03% of total Internet traffic [MOY201101]). P2P concepts are not the focus of this book and are only briefly surveyed.

We are not implying here that the various NTTV linear/nonlinear services (VoD/CoD, TSTV, IPTV, UGV, Connected TV, and so on) can only be achieved using IPv6 Multicast. In fact, these services are already being delivered today over IPv4/IPv4 multicast infrastructures. The point of this treatise is that deployment of IPv6 will eventually overcome IPv4 under any number of metrics (number of users, number of sites, amount of traffic, and so on), and, therefore, it is important to be ready for that infrastructure deployment, both in terms of “migrating to it,” but much more importantly and profitably so, “how to take strategic advantage of the new technology and gain market share and/or enter new markets.”

Impacted and/or interested industry players include the following:

- Content providers
- Application providers
- Content aggregators
- Service providers
- Network providers
- Consumers (subscriber, viewer, and so on)
- Standards developers
- Regulators

True innovation is required by providers to survive this major shift and not stagnate; such innovation must be bold to deal with the potentially business-risky consequences of an unflexible continuance of the status quo. Naturally, service providers do not want to obsolete their networks and infrastructure over night, but prefer to evolve them to support the new commercial requirements. Such evolution must be well planned, well thought out, and well executed.

HD services (based on MPEG-4) will require about three to four times the bandwidth of SD services (based on MPEG-2). Emerging Ultra HDTV provides 16× the resolution of HDTV ($7,680 \times 4,320$ pixels), but needs a bandwidth of 100–200 Mbps. If 3DTV takes off, it may increase the bandwidth requirement by 25–50%. However, there are new compression technologies, such as fractals and wavelets, that if perfected and become cost-effective, will decrease the bandwidth requirement by an *order of magnitude or more*. While this is very advantageous to IP-based service providers, it will be a major future challenge to bandwidth-only providers.

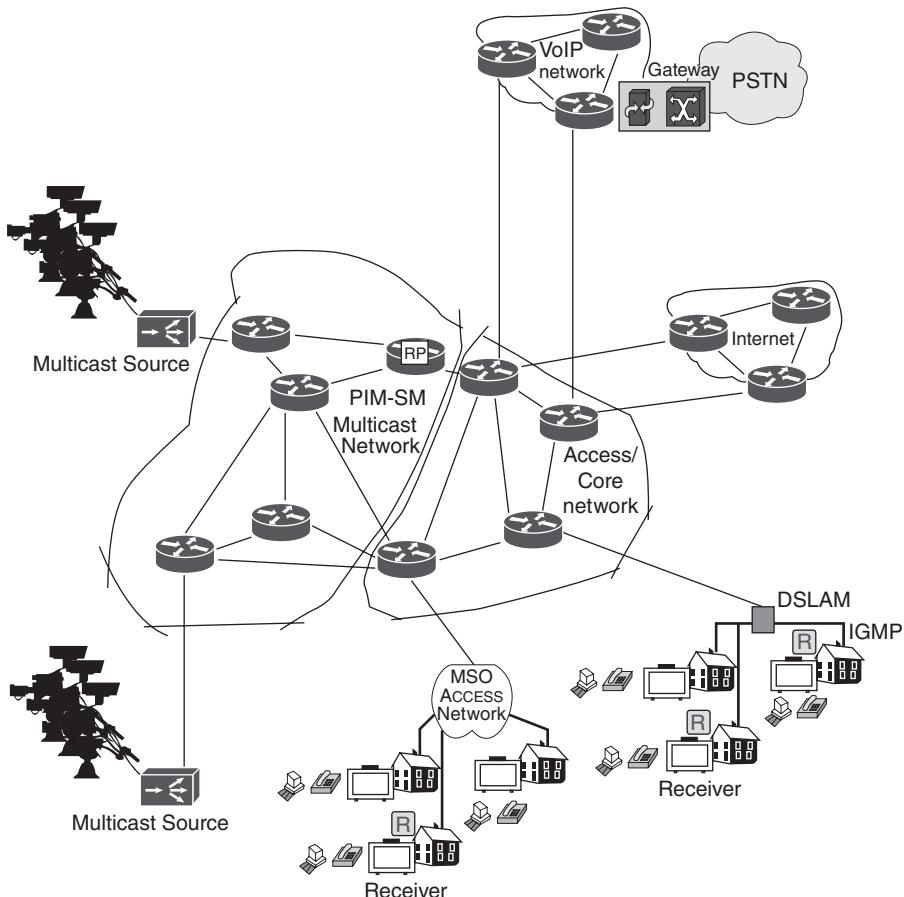


FIGURE 1.9 Illustrative example of triple play IPTV-based multicast network.

Providers also need to consider “triple-play” architectures to support video, Internet, and voice services, although the latter may not necessarily be the big “money maker” (we do not focus on wireless cellular and other mobility services in this text.) Figure 1.9 provides a simplified illustrative example of a “triple play” network; currently such network may be IPv4 based, but the evolution is toward an IPv6-based environment (for all services, or at least a subset thereof.)

It is also clear that satellite providers will have to support a service that encompasses a migration to a hybrid-based delivery mechanism that makes strategic use of both satellite- and fiber-based transmission resources [MIN199101], [MIN199201], [MIN199401], [MIN199501], [MIN199801], [MIN200201], [MIN200202], [MIN200301], [MIN200701], [MIN200801], [MIN200901], [MIN201001], [MIN201101]. Increased support of Internet services, for example, by using Medium Earth Orbit (MEO) assets that

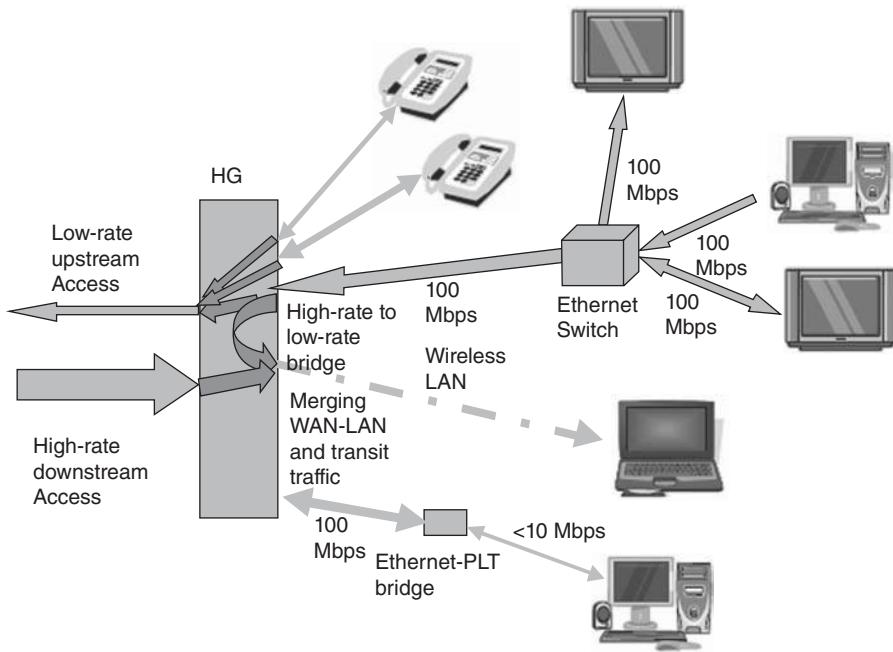


FIGURE 1.10 The evolving home network, as described in the home gateway initiatives.

significantly reduce the roundtrip latency (such as the O3b Networks model), will be advantageous in this context. For example, O3b Networks, a venture of Google and others, is building a new satellite-based, global Internet backbone for telecommunications operators (telcos) and ISPs in emerging markets. O3b's satellites will be placed into orbit approximately 5000 mi from earth, four times closer than geostationary satellites, speeding up Internet connections through its inherent low latency [SOR201101].

The in-home network is also becoming fairly sophisticated, as noted in Figure 1.10, as recognized by the Home Gateway Initiative [HGI200601]. Service providers, network providers, and content providers need to be cognizant of the evolution occurring in the home environment; for example, the direct connecting of TV sets to the Internet, and the implications thereof.

While there is an expectation of transition in viewer habits with ensuing impacts on the delivery infrastructure, one should keep in mind, at the same time, that the current decade has seen and may continue to see some economic difficulties. It follows that, perhaps, not much new infrastructure might be deployed to compete against existing infrastructure in the next 2–3 years. For example, U.S. Cable TV companies may not immediately deploy a lot of new fiber routes, implying that they may continue to use satellite distribution to headends dispersed nationwide instead of migrating rapidly to terrestrial dis-

tribution, at least until the second half of the 2010 decade. The same may occur in reference to the developing world: companies may not deploy a lot of new WiMAX towers to provide local distribution of TV signals, implying that that consumer will continue to use DTH satellite services instead of migrating to terrestrial distribution (as rapidly). While free TV channels are putting their content online with increasing regularity, pay TV channels are more reserved. To date, many pay TV channels have rather limited online video offerings. Thus, while the majority of the key content continues to remain available only on pay TV, the operators (Cable, satellite, IPTV) will hold the customer base; observers are forecasting that by 2015, there will be an additional 150 million pay TV homes globally [SCR201101]. Nonetheless, the expectation is that fiber deployments to support IP, IP Multicast, IPTV services, streaming, and NTTV will continue to make inroads and be dominant by the decade's end or soon thereafter, at least in the industrialized nations of the world, with the exception perhaps of the BRICA countries (Brazil, Russia, India, China, and Africa).

While the theme of this text is the evolving and increasing consumption of IP-based video, delivered either via terrestrial IPTV-based systems or via the Internet in some areas of the world, one needs to note that the consumer landscape can be segmented into the following areas: urban, suburban, exurban, rural, undeveloped. Each of these market segments makes optimal use of different technologies, or at least is at a different deployment cycle and lags behind the other by a number of years (see Figure 1.11) Hence, there will continue to be a key role for satellite-based DTH systems for many years to come and for large shares of the global population, especially outside North America and Europe. Both IPTV and IBTV require, to a large degree, the deployment of FTTH in order to consistently provide the kind of bandwidth required for this delivery mechanism. As a side note, a press time report from Eurostat, the EU's statistical agency, showed that almost a quarter of the European Union's 500 million people have never used the Internet, and there is a widening division between the web-savvy north of Europe and the poorer

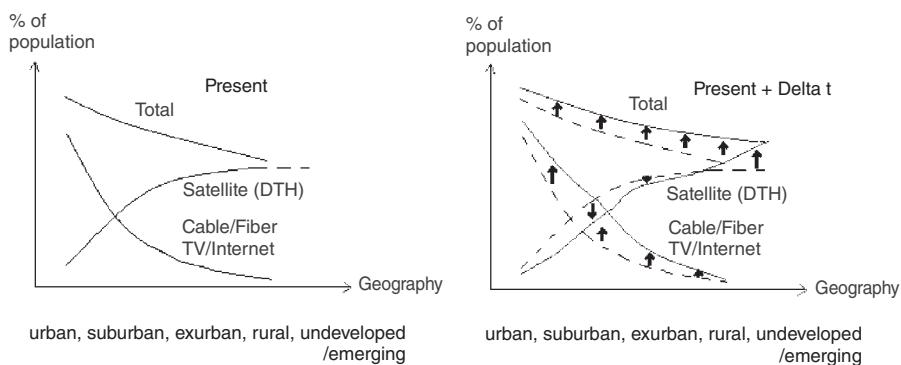


FIGURE 1.11 Various geographic markets and applicability of various technologies.

south and east. More than half the population of Romania and just under half of those in Bulgaria, Greece, Cyprus, and Portugal do not have Internet access at home. Besides highlighting geographic disparities across one of the world's most-developed regions, the figures underline the lack of opportunity people in poorer communities have to take part in advances such as the Internet that have delivered lower cost goods and service to millions of people. The report noted that 24% of 16–74 year olds across the 27 countries in the European Union have never accessed the Internet. Although overall Internet access has risen in the past 5 years, the range is still wide, with just 45% of the population connected in Bulgaria compared with 94% in the Netherlands; others in the top tier include Luxembourg, Sweden, and Denmark, all with access rates of 90% or above. At the bottom end of the scale, 54% of those in Romania have never used the Internet, whether via home access, at an Internet café, or over a smart phone. Those countries with the lowest usage rates also tend to be those with the least number of fixed-line broadband connections [DAV201101]. These observations reinforce the fair-balance point above that while there is increasing consumption of IP-based video, delivered either via terrestrial IPTV-based systems or via the Internet, there will continue to be a key, even critical, role for satellite-based DTH systems for many years to come and for large shares of the global population.

1.6 SCOPE OF THE INVESTIGATION

We just noted that the infrastructure used to deliver content will have to be aligned to the evolving user-driven requirements. Infrastructure providers need to be keenly aware of the impact that these evolving viewer paradigms will have on their networks and even their revenue stream. These changes may impact broadcast TV companies, telephone companies (telcos) delivering IPTV-based services over fiber, satellite providers, and 3G/4G wireless network providers.

The themes discussed earlier in this chapter are amplified in the rest of the text. This work looks at the underlying technologies that support time shifting, broadband delivery, storage, and multicasting. The focus is on IP-based distribution, including IP multicast in general and IP multicast in an IPv6 environment in particular. It should be noted, however, that it is not the intention of this text to exhaustively address and analyze all new possible video and multimedia consumption trends now evolving, and the provider/infrastructure implications should such trends become ubiquitous, but rather to look at the major evolving trends and possible provider and network strategies. One should expect that the viewer trends in 2022 will be different from those of 2012; hence, what is of interest are the fundamental principles that enable one to build a flexible infrastructure that can easily accommodate future new services and delivery mechanisms—such fundamental approaches entail IPTV with IPv4/IPv6 multicast; here we focus on IPv6.

Following an introductory overview of the industry and trends, Chapter 2 provides a primer of IPv6. Chapter 3 discusses at IP multicast, while Chapter 4 focuses on IPv6 multicast approaches and challenges. Chapter 5 describes evolving video services that are of interest to consumers, especially for service-provider environments. Chapter 6 is an overview of IPTV, which is increasingly being considered to be the platform of choice for service-provider-based packetized video delivery. In addition to architectural considerations, some of the newly published ITU-T IPTV standards, including ITU-T H.701 (Error-Recovery), ITU-T H.721 (IPTV Terminal), ITU-T H.740 (Application Event Handling), ITU-T H.750 (Metadata), ITU-T H.761 (Ginga-NCL), ITU-T H.762 (LIME) and ITU-T H.770 (Service Discovery) are discussed. IPTV is indeed not the only platform for IP-based video delivery; hence, Chapter 7 looks indeed at those other platforms, such as streaming, Content Delivery Networks (CDNs), Peer-to-Peer (P2P) systems, cloud computing, and Internet backbones and access networks; the chapter also looks at the implications of these technologies and the evolving viewing habits in terms of the kind of network evolution that may be required to optimally support end-of-decade video services. Finally, Chapter 8 describes some of the new content sources (some of these services and/or providers may disappear over time and others will emerge, but we believe that the general trends discussed here, as a whole, will persist and prevail.)

REFERENCES

- [AVL201101] J. Avlon, “The end of TV campaign ads?” *The Daily Beast*, Online Magazine, Oct 27, 2011, <http://www.thedailybeast.com>
- [AXO200901] S. Axon, “8 companies that are reinventing TV online,” *Mashable*, The Social Media Guide, Online Magazine, December 2009.
- [BIL201001] N. Bilton, “Google teams up with Intel, Sony on TV project,” *The New York Times*, March 18, 2010.
- [BOO201101] J. Boorstin, “YouTube ready to announce original content channels,” *CNBC*, 28 October 2011.
- [CAS200901] P. Cash, “Neil Patrick Harris mocks the Internet at the Emmys 2009,” *Mashable*, The Social Media Guide, Online Magazine, December 2009.
- [CUT201101] C. Cutter, M. Liedtke, “Behind the increase: Why did Netflix raise prices?” *AP*, July 14, 2011.
- [DAV201101] C. Davenport, “More than 100 million EU citizens have never surfed web,” *Reuters/Alex Grimm (Germany)*, December 6, 2011.
- [DAW200901] R. Dawson, “The future of social networks and television distribution channels,” *Sunday Telegraph*, September 15, 2009.
- [EDW201101] C. Edwards, “Coming soon to your screen: T-Commerce,” *Cable*, March 3, 2011.
- [FUT201101] Futurescape Staff, *How Connected Televisoon Transforms The Business OF TV—A white paper based on the Futurescape strategy report Social TV*, Futurescape Ltd, 2011. <http://www.futurescape.tv>

- [GRO200901] R. Grover and T. Lowry, “How network TV will reinvent itself, special report: The future of TV,” *BusinessWeek* (online), April 22, 2009.
- [GRO201001] D. Gross, “TiVo adds web, music, movies with premiere,” *CNN Online*, March 2, 2010.
- [HAC201101] M. Hachman, “Apple dominates shockingly small video streamer market,” *PC*, <http://www.PCMag.com>, May 20, 2011.
- [HEY201001] J. Heynen, “IPTV and video equipment and service markets hampered by slowing subscriber growth,” *Infonetics Research*, January 5, Press Release, 2010, Campbell, CA.
- [HGI200601] Home Gateway Initiatives, *Home Gateway Technical Requirements, Release 1*, 2006.
- [ITU200701] International Telecommunication Union (ITU-T), “ITU announces first global set of standards for IPTV Specifications will fuel market for next-generation services”, Press Release, December 18, 2007, International Telecommunication Union, Telecommunication Standardization Bureau, Place des Nations, CH-1211 Geneva 20.
- [ITU200801] M. Johnson, “ITU-T IPTV focus group proceedings” ITU-T, 2008. International Telecommunication Union, Telecommunication Standardization Bureau, Place des Nations, CH-1211 Geneva 20.
- [ITU200901] International Telecommunication Union (ITU-T), “IPTV global standards initiative (IPTV-GSI)—IPTV-GSI terms of reference,” August 13, 2009. International Telecommunication Union, Telecommunication Standardization Bureau, Place des Nations, CH-1211 Geneva 20.
- [ITU201001] International Telecommunication Union (ITU-T), “ITU Interop event highlights IPTV interoperability—Future of television will rest on stable global standards, say experts,” July 27, 2010. International Telecommunication Union, Telecommunication Standardization Bureau, Place des Nations, CH-1211 Geneva 20.
- [LOW200901] T. Lowry, “Cable TV: Pushing to become more web-like,” *BusinessWeek* (online), April 16, 2009.
- [MEL20101] J. Melloy, “Half of TVs to have internet connectivity by 2015,” *CNBC*, 5 July 2011.
- [MIN199101] D. Minoli, *Telecommunication Technologies Handbook*, 1st Edition, Artech House, 1991.
- [MIN199201] D. Minoli, *Enterprise Networking: Fractional T1 to SONET, Frame Relay to BISDN*, Artech House, 1992.
- [MIN199401] D. Minoli, *Distributed Multimedia Through Broadband Communication Services (coauthored)*, Artech House, 1994.
- [MIN199501] D. Minoli, *Video Dialtone Technology: Digital Video over ADSL, HFC, FTTC, and ATM*, McGraw-Hill, 1995.
- [MIN199801] D. Minoli, *Network Layer Switched Services (coauthored)*, Wiley, 1998.
- [MIN200201] D. Minoli, *Ethernet-based Metro Area Networks—Planning and Designing the Provider Network (coauthored)*, McGraw-Hill, 2002.
- [MIN200202] D. Minoli, *Next-generation SONET-based Metro Area Networks—Planning and Designing the Provider Network*, McGraw-Hill, 2002.
- [MIN200301] D. Minoli, *Telecommunication Technologies Handbook*, 2nd Edition, Artech House, 2003.

- [MIN200701] D. Minoli, *Network Infrastructure and Architecture—Designing High-Availability Networks* (coauthored), Wiley, 2007.
- [MIN200801] D. Minoli, *IP Multicast with Applications to IPTV and Mobile DVB-H*, Wiley, 2008.
- [MIN200901] D. Minoli, *Satellite Systems Engineering in an IPv6 Environment*, Francis and Taylor, 2009.
- [MIN201001] D. Minoli, *3D Television (3DTV) Content Capture, Encoding, and Transmission*, Wiley, 2010.
- [MIN201101] D. Minoli, *3D Television (3DTV) Technology, Systems, and Deployment*, Taylor and Francis, 2011.
- [MOY201101] J. Moya, “STUDY: P2P is 61 percent of IPv6 Traffic, 8 percent of IPv4,” April 22, 2011, online blog, <http://www.zeropaid.com>
- [NIE200901] Nielsen Company, Television, Internet and Mobile Usage in the U.S., A2/M2 Three Screen Report, 1st Quarter, 2009. The Nielsen Company. <http://www.nielsen.com>
- [NIE201001] Nielsen, “On-line observations about Telecom” 2010. <http://www.nielsen.com>
- [NIE201101] Nielsen Company, *The Cross-Platform Report Quarter 1, 2011*, August 30, 2011, The Nielsen Company. <http://www.nielsen.com>
- [OHA201101] J. O’Halloran, “Online film market to be worth \$4.44bn by 2017,” Rapid TV News (online magazine), April 26, 2011. <http://www.rapidtvnews.com>
- [OHA201102] J. O’Halloran, “Apple, Sony and Microsoft spur non-US online video growth,” RapidTV News (online magazine), July 12, 2011. <http://www.rapidtvnews.com>
- [OIP200801] Open IPTV Forum (OIPF), “Services and functions for release 2 [V1.0]-[2008-10-20],” 2008, Open IPTV Forum, 650 Route des Lucioles—Sophia Antipolis, Valbonne, France.
- [ORT201101] B. Ortutay, “Microsoft brings TV to Xbox 360,” Associated Press, 2011.
- [REE201001] ReelSEO.com, “Online video dictionary—glossary of online video terms, the online video marketer’s guide,” 2010.
- [SCR201101] Screen Digest Staff, “Screen Digest” June 2011, Issue number 477, <http://www.ScreenDigest.com>, Screen Digest Limited, Lymehouse Studios, 30-31 Lyme Street, London, NW1 0EE.
- [SJO200801] D. Sjöberg, “Content Delivery Networks: Ensuring quality of experience in streaming media applications”, TeliaSonera International Carrier, CDN White Paper, August 14, 2008.
- [SOR201101] L. Sorrentino, “O3b networks set to virtually double fleet capacity as financing is secured to build four more satellites,” O3b Networks Press release, November 10, 2011, St. John, Jersey, Channel Islands.
- [SVE201101] P. Svensson, “Comcast to sell Skype box for video calls,” CNBC (online), 13 June 2011.
- [THO201101] N. Thomas, “Streamed TV is growing, but the studios are still banking on discs,” Informa Telecoms & Media, October 5 2011, <http://www.informatm.com>
- [WIN200901] N. Wingfield, D. Clark, “Internet-ready TVs usher web into living room,” Wall Street Journal Online. January 5, 2009.
- [WOH201101] J. Wohl, “Walmart puts vudu on its main site to drive use,” Reuters, July 26, 2011.

APPENDIX 1A BACKGROUND STATISTICS AND FORECAST

This appendix provides some primary data and projections. Useful recent time trend data is garnered from The Nielsen Company. We include both the data we had originally gathered when first conceiving of this project (2009), as well as the latest data at actual writing time (2011).

1A.1 2009 Viewing Habits Nielsen's Data

The 2009 data is from the *Television, Internet and Mobile Usage in the U.S., A2/M2 Three Screen Report, 1st Quarter 2009*, published by Nielsen [NIE200901]. Table 1A.1 provides actual data for recent viewing habits in the United States, which forms the basis for the projections we develop below. Figure 1A.1 provides a perspective in terms of the number of content consumers. Also, see additional data at the end of this appendix.

TABLE 1A.1 Actual 2009 Data for Recent TV Viewing Habits: Hours Spent Watching

Monthly Time Spent in Hours:Minutes Per User 2+

	1Q09	1Q08	% Diff Yr to Yr (1Q09 to 1Q08)	Absolute Diff Yr to Yr (1Q09 to 1Q08)
Watching TV in the home ^a	153:27	150:38	1.9	2:49
Watching time-shifted TV ^a	8:13	5:52	40.1	2:21
Using the internet ^b	29:15	27:57	4.6	1:17
Watching video on internet ^b	3:00	1:57	53.2	1:02
Mobile subscribers watching video on a mobile phone ^c	3:37	n/a	n/a	n/a

^a TV in the Home includes Live viewing plus any playback viewing within 7 days. Time-shifted TV is playback primarily on a DVR, but including playback services like Start Over as well as playback from a DVD recorder.

^b Internet figures are from home and work. Hours : minutes for Internet and video use are based on the universe of persons who used the Internet/watched online video. All Internet figures are monthly averages over the course of the quarter.

^c The average monthly unique users of mobile phones and mobile video in 1Q 2009 and 4Q 2008, based on Nielsen Mobile surveys and CTIA projection of U.S. wireless subscriptions. Video user projection, time spent, and composition data based on survey analysis of past 30 day use during the period. The mobile video audience figures in this report for 1Q 2009 and 4Q 2008 include mobile phone users who access mobile video through any means (including mobile Web, subscription-based, downloads, and applications). Projection of all subscribers is based on persons 2+. Projection of mobile video viewers, and all other mobile video estimates, based on subscribers 13+.

Source: The Nielsen Company.

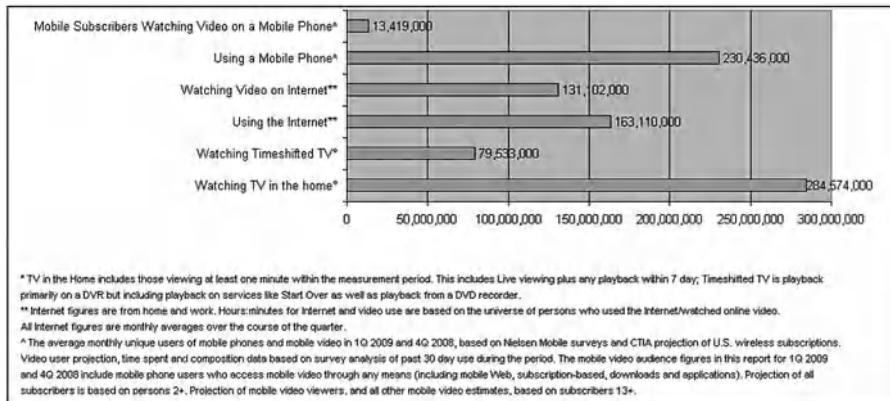


FIGURE 1A.1 Actual 2009 data for recent tv viewing habits: Number of people watching.

Observations included in the cited 2009 Nielsen report include the following:

- (fact) Television is still the dominant choice for Americans who watch video. Almost 99% of the video watched in the United States is still done on television.
- (fact) Traditional TV usage in the United States remains at an all-time high at approximately 153 hours a month. Of all demographics, adults age 18–24 show signs of using DVRs and online video about the same amount of time—they time shift television 5 hours, 47 minutes per month, and video on the Internet 5 hours, 3 minutes each month.
- (fact) Teens age 13–17 continue to be avid viewers of mobile video; they report viewing an average of 6.5 hours of video on their mobile phones each month.
- (trend) Time shifting usage with DVRs is up 40% from 2008, with Americans playing back 8 hours, 13 minutes per month.
- (trend) With broadband levels increasing in the United States, online video audiences will continue to grow as consumers begin to upgrade their PCs to support increased video consumption. Growth also hinges on how broadband channels promote themselves. As sites continue to aggressively market themselves, they will increase the levels of growth by creating demand.
- (trend) Mobile video viewing has grown a significant 52% in Q1 2009 from the previous year, up to over 13 million Americans. The most watched categories on mobile phones are comedy and weather.

These data are used to build a forecast of future trends. In Table 1A.2, some of the growth rates suggested by the study are used to project forward, but these rates are moderated substantially over time (e.g., while the growth rate for TSTV was 40% in 2009, we reduce that number to 5% by 2017). We take the overall growth rate of the aggregate all-TV home viewing hours to be 2%

TABLE 1A.2 Forecast for Transitions in Viewing Habits over Time (Parametric Forecast)

	2009	2010	2011	2012	2013	2014	2015	2016	2017
Aggregate all-TV home viewing growth rate (%)		2.0	2.0	2.0	2.0	2.0	2.0	2.0	2.0
Aggregate all-Internet home viewing growth rate (%)		4.0	4.0	4.0	4.0	4.0	4.0	4.0	4.0
Total TV (calculated) (hour.)	156.0*	159.1	162.3	165.5	168.9	172.2	175.7	179.2	182.8
Total internet (calculated) (hour.)	30.0*	31.2	32.4	33.7	35.1	36.5	38.0	39.5	41.1
Super total: All TV viewing and all internet usage (hour.)	186.0*	190.3	194.8	199.3	204.0	208.7	213.6	218.7	223.8
Time shifted TV growth rate (%)		40.0	20.0	20.0	10.0	10.0	5.0	5.0	2.5
Internet TV growth rate (%)		50.0	40.0	40.0	40.0	30.0	30.0	30.0	30.0
Traditional TV home viewing (hour.)	145.0*	143.4	142.6	140.6	138.8	136.7	134.3	130.6	125.5
Time shifted/on demand home viewing TV (hour.)	8.0*	11.2	13.4	16.1	17.7	19.5	20.5	21.5	22.1
Internet-downloaded home viewing programming (hour.)	3.0*	4.5	6.3	8.8	12.3	16.1	20.9	27.1	35.3
Total TV viewing (all forms)	156.0*	159.1	162.3	165.5	168.9	172.2	175.7	179.2	182.8

*Actual data

a year, because people cannot continue to increase their entertainment time at infinitum—people also have to do productive work and attend to other family or related responsibilities. For the same reason, we take the aggregate all-Internet home viewing hours to be 4%. Figure 1A.2 depicts some of these trends graphically.

1A.2 2011 Viewing Habits Nielsen's Data

The 2011 data is from *The Cross-Platform Report Quarter 1, 2011* report published by Nielsen [NIE201101] Table 1A.3 provides the latest observations. Table 1A.4 compares 1Q2008 with 1Q2011; the increases for NTTV are conspicuous, supporting the fundamental theme of the text.

TABLE 1A.3 2011 Nielsen Company data on U.S. Watching Habits

	Q1 11	Q1 10	% Diff Yr to Yr	Hours : Minutes Diff Yr to Yr
Watching TV in the home	158:47	158:25	0.2	0:22
Watching time-shifted TV (all TV homes)	10:46	9:36	12.2	1:10
DVR playback (only in homes with DVRs)	26:14	25:48	1.7	0:26
Using the internet on a computer	25:33	25:54	-1.4	-0:21
Watching video on internet	4:33	3:23	34.5	1:10
Mobile subscribers watching video on a mobile phone	4:20	3:37	20.0	0:43

Note: Monthly hours of content consumption, per person in the United States over the age of 2.

TABLE 1A.4 2008–2011 Comparison of U.S. Watching Habits

Activities ↓	Timeframe →	Q1 11	Q1 08	Delta	Total Percentage Increase	CAGR (%)
Watching TV in the home		158:47	150:38	8:09	5.41	1.77
Watching time-shifted TV (all TV homes)		10:46	5:52	4:54	83.52	22.40
Using the Internet on a computer		25: 33	27:57	-2:24	-8.59	-2.90
Watching video on Internet		4: 33	1:57	2:36	133.33	32.50

Coding for time spent on activity: H : m.

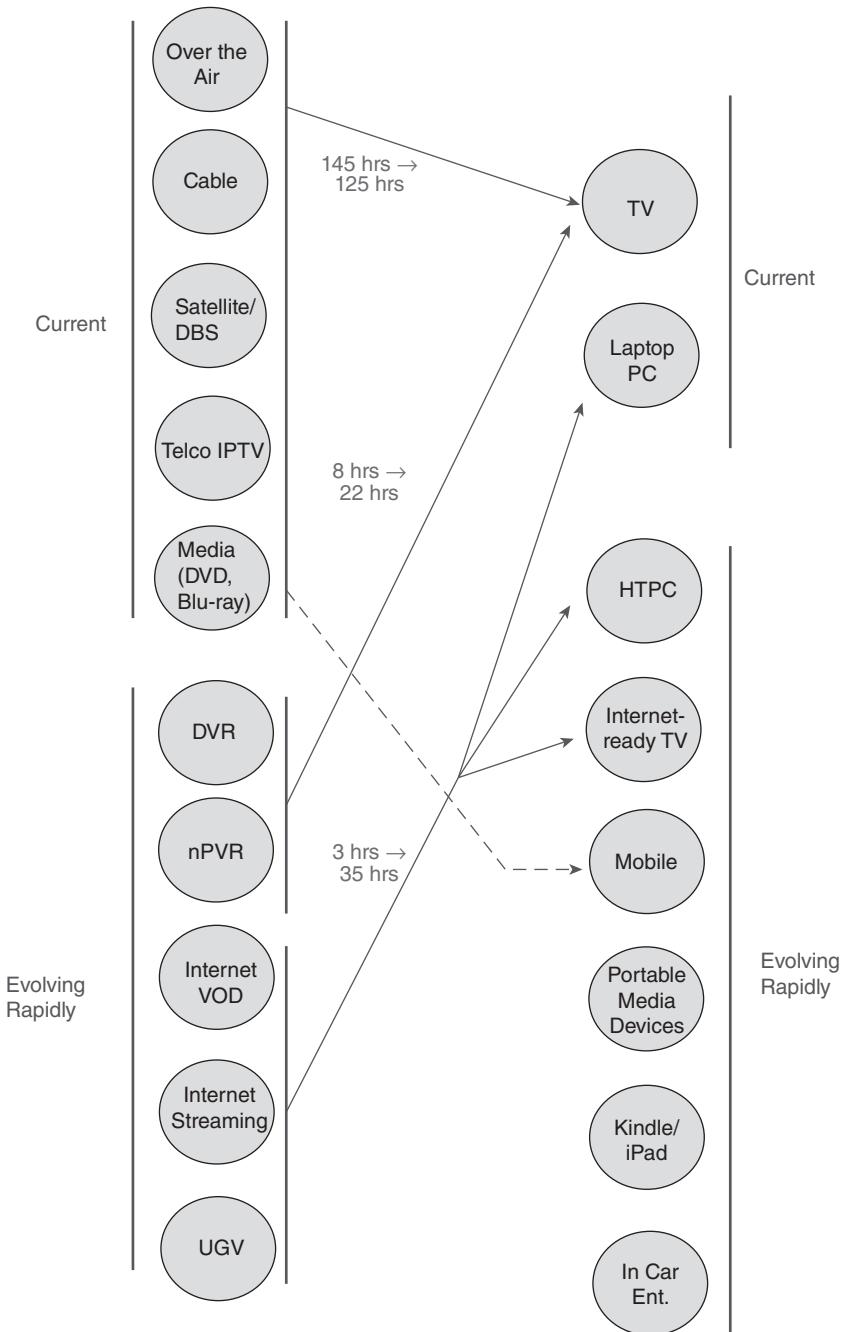


FIGURE 1A.2 Another view of shifts in viewing habits.

2 An Overview of IPv6

2.1 OVERVIEW AND MOTIVATIONS

Internet Protocol Version 6 (IPv6) is a newer version of the network layer protocol that is designed to coexist with IPv4 and eventually replace it. IPv6 provides improved internetworking capabilities compared with what is presently available with IPv4. The current IPv4 version of the Internet Protocol has been in use for 30 years but it exhibits some challenges in supporting emerging demands for address space cardinality, high-density mobility, multi-media, and strong security. IPv6 offers the potential of achieving scalability, reachability, end-to-end interworking, Quality of Service (QoS), and commercial-grade robustness that is needed for contemporary and emerging web services, data services, and IP-based IPTV/IBTV/NTTV content distribution. The innovation and growth of the Internet is now predicated on deployment of IPv6. As already stated, we are not implying in this text that IPv6 is strictly and uniquely required to support IP-based IPTV/IBTV/NTTV, linear video, Video/Content On demand (VoD/CoD), and/or streaming video, just that it provides an ideal, future-proof, scalable mechanism for such services, whether in a terrestrial mode or in a satellite-based mode [MIN200801], [MIN200902].

IP was designed in the late 1970s–early 1980s for the purpose of connecting computers that were in separate geographic locations. Starting in the early 1990s, developers realized that the communication needs of the twenty-first century needed a protocol with some new features and capabilities, while at the same time retaining the useful features of the existing protocol. IPv6 was initially developed in the early 1990s because of the anticipated need for more end system addresses based on anticipated Internet growth, encompassing mobile phone deployment, smart home appliances, and billions of new users in developing countries (e.g., BRIC countries: Brazil, Russia, India, and China). Technologies and applications, such as Voice Over IP (VoIP), “always-on access” (e.g., cable modems), broadband and/or Ethernet-to-the-home, converged networks, and evolving ubiquitous computing applications will be driving this need even more in the next few years [MIN200601].

IPv6 is now being slowly deployed worldwide: there is documented institutional and commercial interest and activity in Europe and Asia, and there is also evolving interest in the United States. The expectation is that in the next few years' deployment, this new protocol will occur worldwide. For example, the U.S. Department of Defense (DoD) announced that from October 1, 2003, all new developments and procurements needed to be IPv6-capable; the DoD's goal was to complete the transition to IPv6 for all intra- and inter-networking across the agency by 2008, which was accomplished. The U.S. Government Accountability Office (GAO) has recommended that all agencies become proactive in planning a coherent transition to IPv6. The current expectation is that IPv4 will continue to exist for the foreseeable future, while IPv6 will be used for new broadscale applications. The two protocols are not directly interworkable, but tunneling and dual-stack techniques allow coexistence and coworking.

While the basic function of the network layer internetworking protocol is to move information across networks, IPv6 has more capabilities built into its foundation than IPv4. Link-level communication does not generally require a node identifier (address) since the device is intrinsically identified with the link level address; however, communication over a group of links (a network) does require unique node identifiers (addresses). The IP address is an identifier that is applied to each device connected to an IP network. In this setup, different entities taking part in the network (servers, routers, user computers, etc.) communicate among each other using their IP address, as an entity identifier. The current IPv4 naming scheme was developed in the 1970s and had capacity for about 4.3 billion addresses, which were grouped into 255 blocks of 16 million addresses each. In Version 4 of the IP protocol, addresses consist of four octets. With IPv4, the 32-bit address can be represented as **AdrClass|netID|hostID**. The network portion can contain either a network ID or a network ID and a subnet. Every network and every host or device has a unique address, by definition. For ease of human conversation, IP protocol addresses are represented as separated by periods, for example: 166.74.110.83, where the decimal numbers are a short hand (and corresponds) to the binary code described by the byte in question (an 8 bit number takes a value in the 0–255 range). Since the IPv4 address has 32 bits, there are nominally 2^{32} different IP addresses (as noted, approximately 4.3 billion nodes, if all combinations are used).

IPv4 has proven, by means of its long life, to be a flexible and powerful networking mechanism. However, IPv4 is starting to exhibit limitations, some accentuated by the need for an increase of the IP address space, driven, for example, by new populations of users in countries such as China and India; by new technologies with “always connected devices” (e.g., cable modems, networked PDAs, and 3G/4G mobile smartphones); and by new services, such as global rollout of VoIP, IPTV, and social networking. A Regional Internet Registry (RIR) manages the allocation and registration of Internet resources, such as IPv4 addresses, IPv6 addresses, and Autonomous System (AS) Numbers, in

TABLE 2.1 Projected RIR Unallocated Address Pool Exhaustion (as of April 2011)

RIR	Assigned Addresses (/8s)	Remaining Addresses (/8s)
AFRINIC	8.3793	4.6168
APNIC	53.7907	1.2093
ARIN	77.9127	6.0130
LACNIC	15.6426	4.3574
RIPE NCC	45.0651	3.9349

RIR, Regional Internet Registry; AfriNIC, African Network Information Centre; ARIN, American Registry for Internet Numbers; APNIC, Asia-Pacific Network Information Centre; LACNIC, Latin America and Caribbean Network Information Centre (LACNIC); RIPE NCC, Réseaux IP Européens Network Coordination Centre (the RIR for Europe, the Middle East and parts of Central Asia).

a specific region of the world. As of February 1, 2011 only 1% of all possible IPv4 addresses were left unassigned. This has led to a predicament known as *IPv4 Run-Out*. The entire address space was expected to be more or less exhausted by September 2011, according to the IPv4 Address Report (see Table 2.1) [RAS201101], [IPV201101]. The IPv4 address allocation is based on the following hierarchy:

Internet Assigned Numbers Authority (IANA) → Regional Internet Registries (RIRs) → Internet Service Providers (ISPs) → the Public (including businesses).

Thus, a key desirable capability is the increase in address space such that it is able to cover all elements of the universe set under consideration. For example, all computing devices could have a public IP address, so that they can be uniquely tracked¹; today, for example, inventory management of dispersed IT assets cannot be achieved with IP mechanisms alone. With IPv6, one can use the network to verify that such equipment is deployed in place and active; even non-IT equipment in the field can be tracked by having an IP address permanently assigned to it. IPv6 creates a new IP address format, such that the number of IP addresses will not exhaust for several decades or longer, even though an entire new crop of devices are expected to connect to Internet over the coming years. IPv6 also adds improvements in areas, such as routing and network configuration. IPv6 has extensive automatic configuration (auto-configuration) mechanisms and reduces the IT burden, making configuration essentially “plug and play.” Specifically, new devices that connect to intranet or Internet will be “plug-and-play” devices. With IPv6, one is not required to

¹Note that this has some potential negative security issues as attackers could be able to own a machine and then exactly know how to go back to that same machine again. Therefore, reliable security mechanisms need to be put understood and put in place in IPv6 environments.

configure dynamic nonpublished local IP addresses, the gateway address, the subnet mask, or any other parameters. The equipment automatically obtains all requisite configuration data when it connects to the network. Auto-configuration implies that a Dynamic Host Configuration Protocol (DHCP) server is not needed and/or does not have to be configured [MIN200802], [MIN200901], [MIN200902].

IPv6 was originally defined in RFC 1883 that was then obsolete by RFC 2460, “Internet Protocol, Version 6 (IPv6) Specification”, S. Deering, R. Hinden (December 1998).² A large body of additional RFCs has emerged in recent years to add capabilities and refine the concept (see Appendix 2A.)

The advantages of IPv6 can be summarized as follows:

- *Scalability and Expanded Addressing Capabilities:* IPv6 has 128-bit addresses versus 32-bit IPv4 addresses. With IPv4, the theoretical number of available IP addresses is $2^{32} \sim 10^{10}$. IPv6 offers a 2^{128} space. Hence, the number of available unique node addressees is $2^{128} \sim 10^{39}$. IPv6 has more than 340 undecillion ($340,282,366,920,938,463,463,374,607,431,768,211,456$) addresses, grouped into blocks of 18 quintillion addresses.
- *“Plug-and-Play”:* IPv6 includes a “plug-and-play” mechanism that facilitates the connection of equipment to the network. The requisite configuration is automatic; it is a server-less mechanism.
- IPv6 makes it easy for nodes to have multiple IPv6 addresses on the same network interface. This can create the opportunity for users to establish overlay or Communities of Interest (COI) networks on top of other physical IPv6 networks. Department, groups, or other users and resources can belong to one or more COIs, where each can have its own specific security policy [JUN200801].
- *Security:* IPv6 includes security in its specifications, such as payload encryption and authentication of the source of the communication. End-to-end security, with built-in, strong IP-layer encryption and authentication (embedded security support with mandatory IPsec implementation) is supported. It follows that IPv6 network architectures can easily adapt to an end-to-end security model where the end hosts have the responsibility of providing the security services necessary to protect any data traffic between them; this results in greater flexibility for creating policy-based trust domains that are based on varying parameters, including node address and application [KAE200601].
- In IPv6, creating a VPN is easier and more standard than in IPv4, because of the (authentication header [AH] and encapsulating security protocol

²The “Version 5” reference was employed for another use—an experimental real-time streaming protocol—and to avoid any confusion, it was decided not to use this nomenclature.

[ESP]) Extension Headers. The performance penalty is lower for the VPN implemented in IPv6 compared with those built in IPv4 [LIO199801].

- *Optimized Protocol:* IPv6 embodies IPv4 best practices but removes unused or obsolete IPv4 characteristics. This results in a better-optimized Internet protocol. Also, merging two IPv4 networks with overlapping addresses (say, if two organizations merge) is complex; it will be much easier to merge networks with IPv6.
- *Real-Time Applications:* To provide better support for real time traffic (e.g., VoIP, IPTV), IPv6 includes “labeled flows” in its specifications. By means of this mechanism routers can recognize the end-to-end flow to which transmitted packets belong. This is similar to the service offered by MultiProtocol Label Switching (MPLS), but it is intrinsic with the IP mechanism rather than an add-on. Also, it preceded this MPLS feature by a number of years.
- *Mobility:* IPv6 includes more efficient and robust mobility mechanisms (enhanced support for Mobile IP and Mobile Computing Devices). Mobile IPv6³ as defined in RFC 3775 is now starting to be deployed [JOH200401], [MIN201201].
- Streamlined header format and flow identification.
- *Extensibility:* IPv6 has been designed to be extensible and offers support for new options and extensions.

ISPs and carriers have been preparing for IP-address exhaustion for a number of years, and there are transition plans in place. The expectation is that IPv6 can make IP devices less expensive, more powerful, and even consume less power; the power issue is not only important for environmental reasons, but also improves operability (e.g., longer battery life in portable devices, such as mobile phones and iPads).

³RFC 3775 notes that without specific support for mobility in IPv6, packets destined to a mobile node would not be able to reach it while the mobile node is away from its home link. In order to continue communication in spite of its movement, a mobile node could change its IP address each time it moves to a new link, but the mobile node would then not be able to maintain transport and higher-layer connections when it changes location. Mobility support in IPv6 is particularly important, as mobile computers are likely to account for a majority or at least a substantial fraction of the population of the Internet during the lifetime of IPv6. The Mobile IPv6 protocol defined in RFC 3775 allows nodes to remain reachable while moving around in the IPv6 Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current location. IPv6 packets addressed to a mobile node's home address are transparently routed to its care-of address. The protocol enables IPv6 nodes to cache the binding of a mobile node's home address with its care-of address, and to then send any packets destined for the mobile node directly to it at this care-of address. To support this operation, Mobile IPv6 defines a new IPv6 protocol and a new destination option. All IPv6 nodes, whether mobile or stationary, can communicate with mobile nodes. Refer to [MIN201201] for a complete discussion of this topic.

2.2 ADDRESS CAPABILITIES

2.2.1 IPv4 Addressing and Issues

IPv4 addresses can be from an officially assigned public range or from an internal intranet private (but not globally-unique) block. As noted, IPv4 theoretically allows up to 2^{32} addresses, based on a four-octet address space. Hence, there are 4,294,967,296 unique values, which can be considered as a sequence of 256 “/8s,” where each “/8” corresponds to 16,777,216 unique address values. Public, globally unique addresses are assigned by IANA. IP addresses are addresses of network nodes at layer 3; each device on a network (whether the Internet or an intranet) must have a unique address. In IPv4, it is a 32-bit (4-byte) binary address used to identify a host’s network ID. It is represented by the nomenclature a.b.c.d (each of a, b, c and d being from 1 to 255 (0 has a special meaning). Examples are 167.168.169.170, 232.233.229.209, and 200.100.200.100.

The problem is that during the 1980s many public, registered addresses were allocated to firms and organizations without any consistent control. As a result, some organizations have more addresses than they actually need, giving rise to the present dearth of available “registerable” Layer 3 addresses. Furthermore, not all IP addresses can be used due to the fragmentation described above.

One approach to the issue would be a renumbering and a reallocation of the IPv4 addressing space. However, this is not as simple as it appears since it requires worldwide coordination efforts. Moreover, it would still be limited for the human population and the quantity of devices that will be connected to Internet in the medium-term future. At this juncture, and as a temporary and pragmatic approach to alleviate the dearth of addresses, Network Address Translation (NAT) mechanisms are employed by organizations and even home users. This mechanism consists of using only a small set of public IPv4 addresses for an entire network to access to Internet. The myriad of internal devices are assigned IP addresses from a specifically designated range of Class A or Class C address that are locally unique but are duplicatively used and reused within various organizations. In some cases (e.g., residential Internet access use via DSL or Cable), the legal IP address is only provided to a user on a time-lease basis, rather than permanently.

Internal intranet addresses may be in the ranges 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. In the internal intranet private address case, a NAT function is employed to map the internal addresses to an external public address when the private-to-public network boundary is crossed. This, however, imposes a number of limitations, particularly since the number of registered public addresses available to a company is almost invariably much smaller (as small as 1) than the number of internal devices requiring an address. A number of protocols cannot (easily) travel through a NAT device and hence the use of NAT implies that many applications (e.g., VoIP) cannot be used effectively.

in all instances. As a consequence, these applications can only be used in intranets. Examples include:

- Multimedia applications, such as videoconferencing, VoIP, or video on demand/IPTV, do not work smoothly through NAT devices. Multimedia applications make use of real-time transport protocol (RTP) and real time control protocol (RTCP). These in turn use the User Datagram Protocol (UDP) with dynamic allocation of ports, and NAT does not directly support this environment.
- IPsec is used extensively for data authentication, integrity, and confidentiality. However, when NAT is used, IPsec operation is impacted, since NAT changes the address in the IP header.
- Multicast, although possible in theory, requires complex configuration in a NAT environment and hence, in practice, is not utilized as often as could be the case.

The need for obligatory use of NAT disappears with IPv6.

2.2.2 IPv6 Address Space

The IPv6 addressing architecture is described in RFC 4291 February 2006 [HIN200601]. One of the major modifications in the addressing scheme in IPv6 is a change to the basic types of addresses and how they are utilized. *Unicast* addresses are utilized for a majority of traditional (enterprise) communications, as was the case in IPv4. However, *Broadcast* as a specific addressing type has been eliminated; in its place, support for *multicast* addressing has been expanded and made a required part of the protocol. A new type of addressing called *anycast* has also been implemented. In addition, there are a number of special IPv6 addresses. Figure 2.1 compares the two address formats. Figure 2.2 provides a pictorial comparison of these three transmission (and address) modes. Logically, one can interpret the types of transmissions as follows⁴:

- Unicast transmission: “send to this one specific address”
- Multicast transmission: “send to every member of this specific group”
- Anycast transmission: “send to any one member of this specific group.” Typically (motivated by efficiency goals), the transmission occurs to the closest (in routing terms) member of the group. Generally, one interprets anycast to mean “send to the closest member of this specific group.”

The format of IPv6 addressing is described in RFC 2373. As noted, an IPv6 address consists of 128 bits, rather than 32 bits as with IPv4 addresses; the number of bits correlates to the address space, as follows:

⁴Broadcast, by contrast, means “send this information/content to the entire universe of users in the address space.”

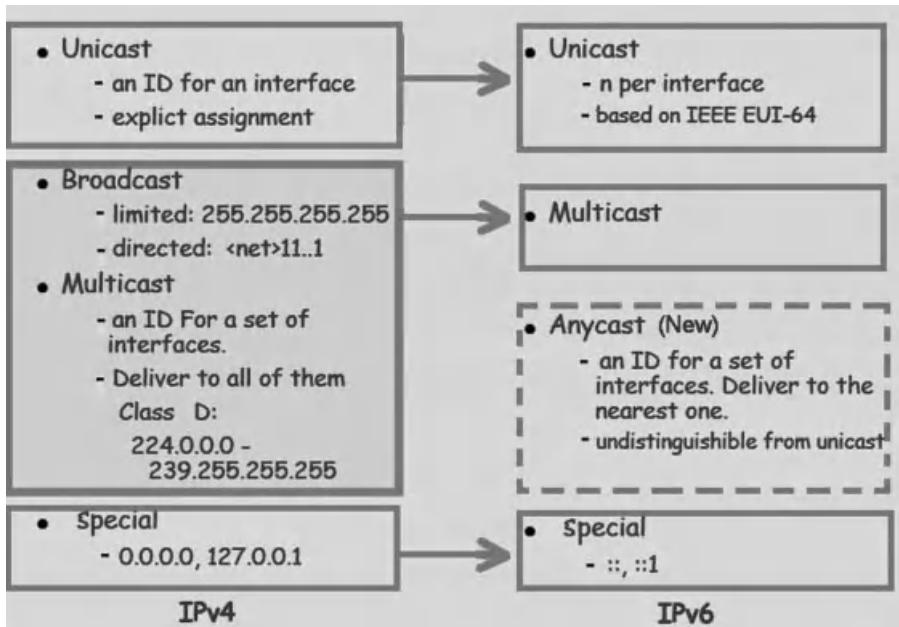


FIGURE 2.1 Address comparison between IPv4 and IPv6.

IP Version	Size of Address Space
IPv6	128 bits, which allows for 2^{128} or 340,282,366,920,938,463,463,374,607, 431,768,211,456 (3.4×10^{38}) possible addresses.
IPv4	32 bits, which allows for 2^{32} or 4,294,967,296 possible addresses.

The relatively large size of the IPv6 address is designed to be subdivided into hierarchical routing domains that reflect the topology of the modern-day Internet. The use of 128 bits provides multiple levels of hierarchy and flexibility in designing hierarchical addressing and routing. The IPv4-based Internet currently lacks this flexibility [MSD200401].

The IPv6 address is represented as eight groups of 16 bits each, separated by the “:” character. Each 16 bit group is represented by 4 hexadecimal digits, that is, each digit has a value between 0 and f (0,1, 2, . . . a, b, c, d, e, f with a = 10, b = 11, and so on to f = 15). What follows is an IPv6 address example

3223:0ba0:01e0:d001:0000:0000:d0f0:0010.

An abbreviated format exists to designate IPv6 addresses when all endings are 0. For example

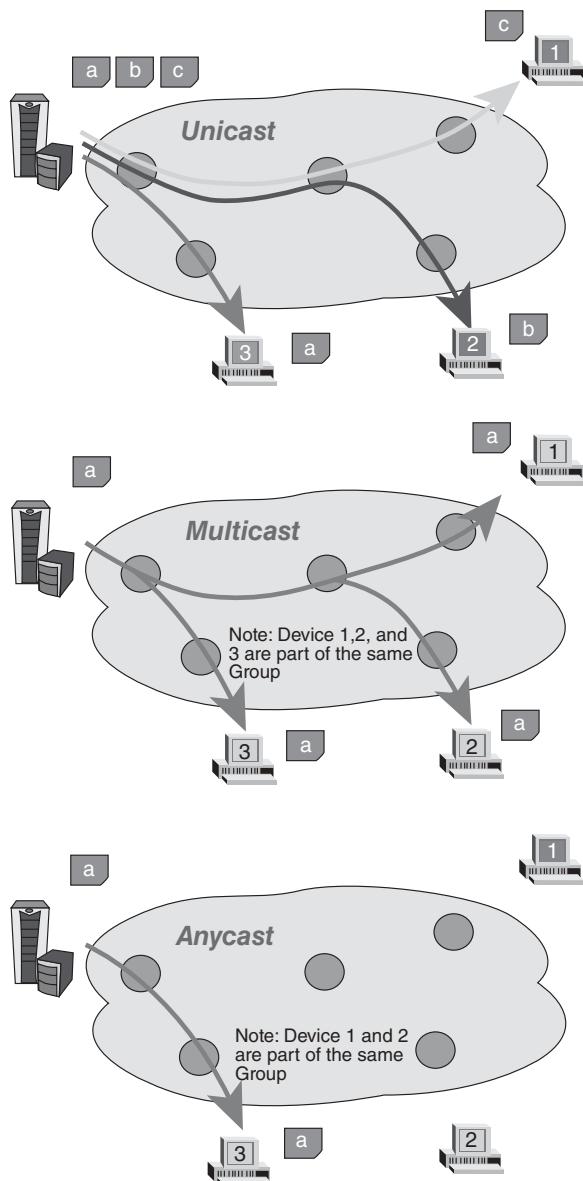


FIGURE 2.2 Comparison of transmissions to IPv6 nodes.

3223:0ba0::

is the abbreviated form of the following address:

3223:0ba0:0000:0000:0000:0000:0000

Similarly, only one 0 is written, removing 0s in the left side, and four 0s in the middle of the address. For example, the address

3223:ba0:0:0:0:1234

is the abbreviated form of the following address

3223:0ba0:0000:0000:0000:0000:1234

There is also a method to designate groups of IP addresses or subnetworks that is based on specifying the number of bits that designate the subnetwork, beginning from left to right, using remaining bits to designate single devices inside the network. For example, the notation

3223:0ba0:01a0::/48

indicates that the part of the IP address used to represent the subnetwork has 48 bits. Since each hexadecimal digit has 4 bits, this points out that the part used to represent the subnetwork is formed by 12 digits, that is: "3223:0ba0:01a0." The remaining digits of the IP address would be used to represent nodes inside the network.

As noted, anycast addresses are a new type of address defined in IPv6 (as originally defined in RFC 1546.) The purpose of the anycast address functionality is to enable capabilities that were difficult to implement in IPv4 environments. Datagrams sent to the anycast address are automatically delivered to the device in the network that is the easiest to reach. Anycast addresses can be used to define a group of devices, any one of which can support a service request from the user sent to a single specific IP address. One example is situations where one needs a service that can be provided by a set of different (dispersed) servers, but where one does not specifically care which one provides it; a specific example here may be an Internet or video (streaming) cache. Another example of anycast addressing is a router arrangement that allows datagrams to be transmitted to whichever router in a group of equivalent routers is closest to the point of transmission; a specific example here may be to allow load sharing between routers. It should be noted that there is no special anycast addressing format: anycast addresses are the same as unicast addresses from an address format perspective. In practicality, an anycast address is defined and created in a self-declarative manner when a unicast address is assigned to more than one device interface.

Special IPv6 addresses, as follows (see Table 2.2 for additional details [BLA200801]):

TABLE 2.2 A Set of IPv6 Addresses of Particular Note

Node-Scoped Unicast	::1/128 is the loopback address (per RFC 4291). ::/128 is the unspecified address (per RFC 4291).
IPv4-Mapped Addresses	Addresses within this block should not appear on the public Internet. ::FFFF:0:0/96 are the IPv4-mapped addresses (per RFC 4291). Addresses within this block should not appear on the public Internet.
IPv4-Compatible Addresses	::ipv4-address/96 are the IPv4-compatible addresses (per RFC4291). These addresses are deprecated and should not appear on the public Internet.
Link-Scoped Unicast	FE80::/10 are the link-local unicast (per RFC 4291) addresses. Addresses within this block should not appear on the public Internet.
Unique-Local	FC00::/7 are the unique-local addresses (per RFC 4193). Addresses within this block should not appear by default on the public Internet.
Documentation Prefix	The 2001:db8::/32 are the documentation addresses (per RFC 3849). They are used for documentation purposes such as user manuals, RFCs, and so on Addresses within this block should not appear on the public Internet.
6to4	2002::/16 are the 6to4 addresses (per RFC 3056). The 6to4 addresses may be advertised when the site is running a 6to4 relay or offering a 6to4 transit service. However, the provider of this service should be aware of the implications of running such service (per RFC 3964), that include some specific filtering rules for 6to4. IPv4 addresses disallowed in 6to4 prefixes are listed in (per RFC 3964).
Teredo	2001::/32 are the Teredo addresses (per RFC 4380). The Teredo addresses may be advertised when the site is running a Teredo relay or offering a Teredo transit service.
6bone	5F00::/8 were the addresses of the first instance of the 6bone experimental network (per RFC 1897). 3FFE::/16 were the addresses of the second instance of the 6bone experimental network (per RFC 2471). Both 5F00::/8 and 3FFE::/16 were returned to IANA (per RFC 3701). These addresses are subject to future allocation, similar to current unallocated address space. Addresses within this block should not appear on the public Internet until they are reallocated.
ORCHID	2001:10::/28 are ORCHID addresses (per RFC 4843). These addresses are used as identifiers and are not routable at the IP layer. Addresses within this block should not appear on the public Internet.
Default Route	::/0 is the default unicast route address.
IANA Special Purpose IPv6 Address Block	An IANA registry (iana-ipv6-special-registry) is set (per RFC 4773) for Special Purpose IPv6 address blocks assignments used for experiments and other purposes. Addresses within this registry should be reviewed for Internet routing considerations.
Multicast	FF00::/8 are multicast addresses (per RFC 4291). They have a 4 bits scope in the address field where only some values are of global scope (per RFC 4291). Only addresses with global scope in this block may appear on the public Internet. Multicast routes must not appear in unicast routing tables.

- Auto-return or loopback virtual address. This address is specified in IPv4 as the 127.0.0.1 address. In IPv6, this address is represented as ::1.
- Not specified address (::). This address is not allocated to any node since it is used to indicate absence of address.
- IPv6 over IPv4 dynamic/automatic tunnel addresses. These addresses are designated as IPv4-compatible IPv6 addresses and allow the sending of IPv6 traffic over IPv4 networks in a transparent manner. They are represented as, for example, ::156.55.23.5.
- IPv4 over IPv6 addresses automatic representation. These addresses allow for IPv4-only nodes to still work in IPv6 networks. They are designated as “mapped from IPv4 to IPv6 addresses” and are represented as ::FFFF; for example ::FFFF.156.55.43.3.

2.3 IPv6 PROTOCOL OVERVIEW

Table 2.3 shows the core protocols that comprise IPv6 (see Appendix 2A for a more complete list). IPv6 basic protocol capabilities include the following:

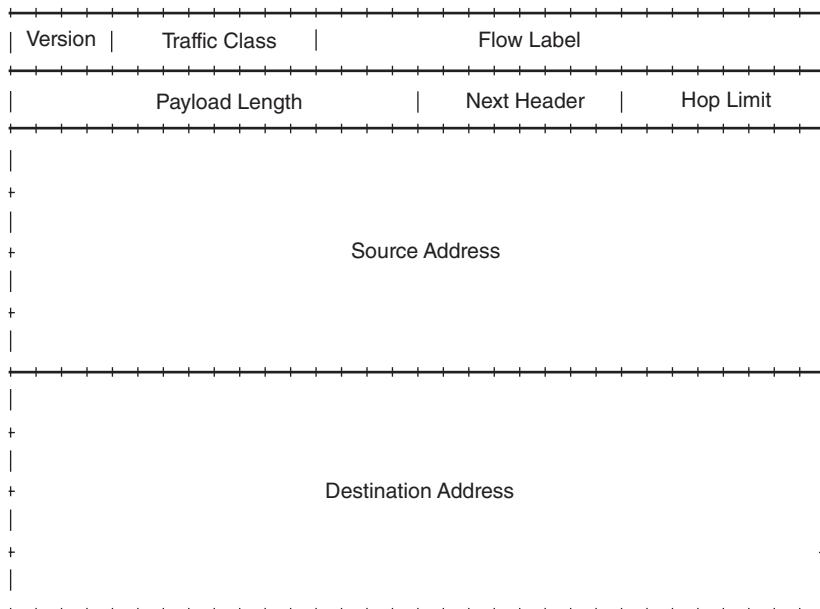
- Addressing
- Anycast
- Flow Labels
- ICMPv6
- Neighbor Discovery

Like IPv4, IPv6 is a connectionless datagram protocol used primarily for addressing and routing packets between hosts. Connectionless means that a session is not established before exchanging data. “Unreliable” means that delivery is not guaranteed. IPv6 always makes a best-effort attempt to deliver a packet. An IPv6 packet might be lost, delivered out of sequence, duplicated, or delayed. IPv6 *per se* does not attempt to recover from these types of errors. The acknowledgment of packets delivered and the recovery of lost packets is done by a higher-layer protocol, such as transmission control protocol (TCP) [MSD200401]. From a packet forwarding perspective, IPv6 operates in a similar, nearly identical manner to IPv4.

An IPv6 packet, also known as an IPv6 datagram, consists of an IPv6 header and an IPv6 payload, as shown Figure 2.3. The IPv6 header consists of two parts: the IPv6 base header and optional extension headers. See Figure 2.4. Functionally, the optional extension headers and upper-layer protocols, for example, TCP, are considered part of the IPv6 payload. Table 2.4 shows the fields in the IPv6 base header. IPv4 headers and IPv6 headers are not directly interoperable: hosts and/or routers must use an implementation of both IPv4 and IPv6 in order to recognize and process both header formats (see Figure 2.5). This gives rise to a number of complexities in the migration process

TABLE 2.3 Key IPv6 Protocols

Protocol (Current Version)	Description
Internet Protocol Version 6 (IPv6): RFC 2460 Updated by RFC 5095, RFC 5722, RFC 5871	IPv6 is a connectionless datagram protocol used for routing packets between hosts.
Internet Control Message Protocol for IPv6 (ICMPv6): RFC 4443 Updated by RFC 4884	A mechanism that enables hosts and routers that use IPv6 communication to report errors and send status messages.
Multicast Listener Discovery (MLD): RFC 2710 Updated by RFC 3590, RFC 3810	A mechanism that enables one to manage subnet multicast membership for IPv6. MLD uses a series of three ICMPv6 messages. MLD replaces the Internet Group Management Protocol (IGMP) v3 that is employed for IPv4.
Neighbor Discovery (ND): RFC 4861 Updated by RFC 5942	A mechanism that is used to manage node-to-node communication on a link. ND uses a series of five ICMPv6 messages. ND replaces Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and the ICMPv4 Redirect message. ND is implemented using the Neighbor Discovery Protocol (NDP).

**FIGURE 2.3** IPv6 packet.

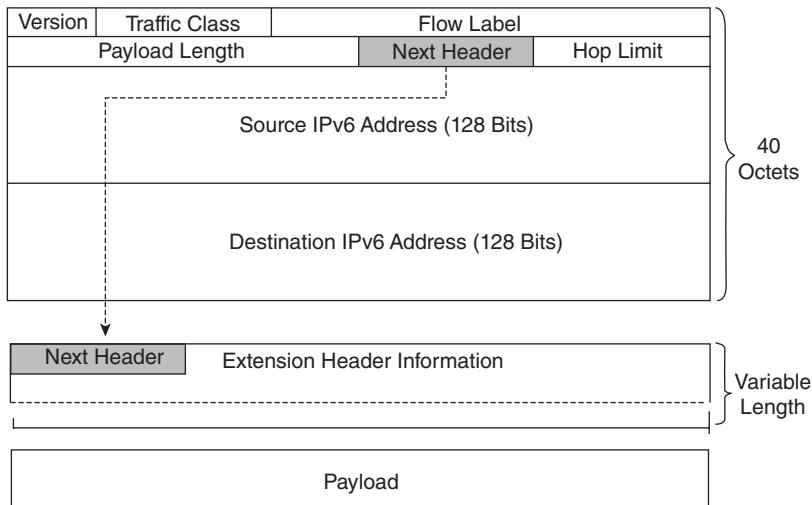


FIGURE 2.4 IPv6 Extension headers. IPv6 extension headers are optional headers that may follow the basic IPv6 header. An IPv6 PDU may include zero, one, or multiple extension headers. When multiple extension headers are used, they form a chained list of headers identified by the Next Header field of the previous header.

between the IPv4 and the IPv6 environments. The IP header in IPv6 has been streamlined and defined to be of a fixed length (40 bytes). In IPv6, header fields from the IPv4 header have been removed, renamed, or moved to the new optional IPv6 Extension Headers. The header length field is no longer needed since the IPv6 Header is now a fixed length entity. The IPv4 “Type of Service” is equivalent to the IPv6 “Traffic class” field. The “Total Length” field has been replaced with the “Payload Length” field. Since IPv6 only allows for fragmentation to be performed by the IPv6 source and destination nodes, and not individual routers, the IPv4 segment control fields (Identification, Flags, and Fragment Offset fields) have been moved to similar fields within the Fragment Extension Header. The functionality provided by the “Time to Live (TTL)⁵” field has been replaced with the “Hop Limit” field. The “Protocol” field has been replaced with the “Next Header Type” field. The “Header Checksum” field was removed, that has the main advantage of not having each relay spend time processing the checksum. The “Options” field is no longer part of the header as it was in IPv4. Options are specified in the optional IPv6 Extension Headers. The removal of the options field from the header enables more efficient routing; only the information that is needed by a router needs to be processed [HER200201].

⁵TTL has been used in many attacks and Intrusion Detection System (IDS) tricks in IPv4.

TABLE 2.4 IPv6 Base Header

IPv6 Header Field	Length (bits)	Function
Version	4	Identifies the version of the protocol. For IPv6, the version is 6.
Traffic Class	8	Intended for originating nodes and forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets.
Flow Label	20	(Sometimes referred to as Flow ID) Defines how traffic is handled and identified. A flow is a sequence of packets sent either to a unicast or a multicast destination. This field identifies packets that require special handling by the IPv6 node. The following list shows the ways the field is handled if a host or router does not support flow label field functions: If the packet is being sent, the field is set to zero. If the packet is being received, the field is ignored.
Payload Length	16	Identifies the length, in octets, of the payload. This field is a 16-bit unsigned integer. The payload includes the optional extension headers, as well as the upper-layer protocols, for example, TCP.
Next Header	8	Identifies the header immediately following the IPv6 header. The following shows examples of the next header: 00 = Hop-by-Hop options 01 = ICMPv4 04 = IP in IP (encapsulation) 06 = TCP 17 = UDP 43 = Routing 44 = Fragment 50 = Encapsulating security payload 51 = Authentication 58 = ICMPv6
Hop Limit	8	Identifies the number of network segments, also known as links or subnets, on which the packet is allowed to travel before being discarded by a router. The Hop Limit is set by the sending host and is used to prevent packets from endlessly circulating on an IPv6 internetwork. When forwarding an IPv6 packet, IPv6 routers must decrease the Hop Limit by 1, and must discard the IPv6 packet when the Hop Limit is 0.
Source Address	128	Identifies the IPv6 address of the original source of the IPv6 packet.
Destination Address	128	Identifies the IPv6 address of intermediate or final destination of the IPv6 packet.

IPv4 Header				IPv6 Header					
Version	IHL	Type of Service	Total Length		Version (4-bit)	Version (4-bit)	Notes		
Identification		Flags	Fragment Offset	Header length (4-bit)	—	Removed in IPv6, the basic IPv6 header has fixed length of 40 octets	IPv6 header contains a new value		
Time to Live	Protocol		Header Checksum	Type of service (8-bit)	Traffic class (8-bit)	Same function for both headers.			
Source Address		Destination Address		—	Flow label (20-bit)	New field added to tag a flow for IPv6 packets.			
Options		Padding		Total PDU length (16-bit)	Payload length (16-bit)	Same function for both headers.			
IPv4 Header				Identification (16-bit)	—	Removed in IPv6 because fragmentation is no longer done by intermediate routers in the networks, but by the source node that originates the packet.			
				Flags (3-bit)	—	Removed in IPv6 because fragmentation is no longer done by intermediate routers in the networks, but by the source node that originates the packet.			
				Fragment offset (13-bit)	—	Removed in IPv6 because fragmentation is no longer done by intermediate routers in the networks, but by the source node that originates the packet.			
				Time to live (8-bit)	Hop limit (8-bit)	Same function for both headers.			
				Protocol number (8-bit)	Next header (8-bit)	Same function for both headers.			
				Header checksum (16-bit)	—	Removed in IPv6; upper-layer protocols handle checksums			
				Source address (32-bit)	Source address (128-bit)	Same function, but Source address is expanded in IPv6.			
				Destination address (32-bit)	Destination address (128-bit)	Same function, but Destination address is expanded in IPv6.			
				Options (variable)	—	Removed in IPv6. Options handled differently.			
				Padding (variable)	—	Removed in IPv6. Options handled differently.			
				—	Extension headers	New way in IPv6 to handle Options field, security			

IPv6 Header

IPv4 Header				IPv6 Header					
Version	IHL	Type of Service	Total Length		Version (4-bit)	Version (4-bit)	Notes		
Identification		Flags	Fragment Offset	Header length (4-bit)	—	Removed in IPv6, the basic IPv6 header has fixed length of 40 octets			
Time to Live	Protocol		Header Checksum	Type of service (8-bit)	Traffic class (8-bit)	Same function for both headers.			
Source Address		Destination Address		—	Flow label (20-bit)	New field added to tag a flow for IPv6 packets.			
Destination Address		Options		Total PDU length (16-bit)	Payload length (16-bit)	Same function for both headers.			
IPv4 Header				Identification (16-bit)	—	Removed in IPv6 because fragmentation is no longer done by intermediate routers in the networks, but by the source node that originates the packet.			
				Flags (3-bit)	—	Removed in IPv6 because fragmentation is no longer done by intermediate routers in the networks, but by the source node that originates the packet.			
				Fragment offset (13-bit)	—	Removed in IPv6 because fragmentation is no longer done by intermediate routers in the networks, but by the source node that originates the packet.			
				Time to live (8-bit)	Hop limit (8-bit)	Same function for both headers.			
				Protocol number (8-bit)	Next header (8-bit)	Same function for both headers.			
				Header checksum (16-bit)	—	Removed in IPv6; upper-layer protocols handle checksums			
				Source address (32-bit)	Source address (128-bit)	Same function, but Source address is expanded in IPv6.			
				Destination address (32-bit)	Destination address (128-bit)	Same function, but Destination address is expanded in IPv6.			
				Options (variable)	—	Removed in IPv6. Options handled differently.			
				Padding (variable)	—	Removed in IPv6. Options handled differently.			
				—	Extension headers	New way in IPv6 to handle Options field, security			

FIGURE 2.5 Comparison of IPv4 and IPv6 headers.

One area requiring consideration, however, is the length of the IPv6 protocol data unit (PDU): the 40-octet header can be a problem for real-time IP applications, such as VoIP and IPTV. Header compression becomes critical for many applications, as noted in Section 2.4. Also, there will be some bandwidth inefficiency in general that could be an issue in limited-bandwidth environments or applications (e.g., wireless networks and sensor networks.)

Stateless address autoconfiguration (described in RFC 4862) defines how an IPv6 node generates addresses without the use of a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server [THO200701]. “Autoconfiguration” is a new characteristic of the IPv6 protocol that facilitates network management and system setup tasks by users. This characteristic is often called “plug-and-play” or “connect-and-work.” Autoconfiguration facilitates initialization of user devices: after connecting a device to an IPv6 network, one or several IPv6 globally unique addresses are automatically allocated. Note, however, that an IPv6 address must be configured on a router’s interface for the interface to forward IPv6 traffic. Configuring a global IPv6 address on a router’s interface automatically configures a link-local address and activates IPv6 for that interface.

DHCP allows systems to obtain an IPv4 address and other required information (e.g., default router or Domain Name System [DNS] server); a similar protocol, DHCPv6, has been published for IPv6. DHCP and DHCPv6 are known as stateful protocols because they maintain tables on (specialized) servers. However, IPv6 also has a new stateless autoconfiguration protocol that has no equivalent in IPv4. The stateless autoconfiguration protocol does not require a server component because there is no state to maintain (a DHCP server may typically run in a router or firewall). Every IPv6 system (other than routers) is able to build its own unicast global address [DON200401]. “Stateless” autoconfiguration is also described as “serverless.” The acronym SLAAC is also used; it expands to *stateless address autoconfiguration*. SLAAC was originally defined in RFC 2462. With SLAAC, the presence of configuration servers to supply profile information is not required.

The host generates its own address using a combination of the information that it possesses (in its interface or network card) and the information that is supplied by the router. As noted in RFC 4941, nodes use IPv6 stateless address autoconfiguration to generate addresses using a combination of locally available information and information advertised by routers. Addresses are formed by combining network prefixes with an interface identifier. On an interface that contains an embedded IEEE Identifier, the interface identifier is typically derived from it. On other interface types, the interface identifier is generated through other means, for example, via random number generation [NAR200701]. Some types of network interfaces come with an embedded IEEE Identifier (i.e., a link-layer Media Access Control [MAC] address), and in those cases, stateless address autoconfiguration uses the IEEE identifier to generate a 64-bit interface identifier [HIN200601]. By design, the interface identifier is likely to be globally unique when generated in this fashion. The interface identifier

is in turn appended to a prefix to form a 128-bit IPv6 address. Not all nodes and interfaces contain IEEE identifiers. In such cases, an interface identifier is generated through some other means (e.g., at random), and the resultant interface identifier may not be globally unique and may also change over time. Routers determine the prefix that identifies networks associated to the link under discussion. The “interface identifier” identifies an interface within a subnetwork and is often, and by default, generated from the MAC address of the network card. The IPv6 address is built combining the 64 bits of the interface identifier with the prefixes that routers determine as belonging to the subnetwork. If there is no router, the interface identifier is self-sufficient to allow the PC to generate a “link-local” address. The “link-local” address is sufficient to allow the communication between several nodes connected to the same link (the same local network).

In summary, all nodes combine interface identifiers (whether derived from an IEEE identifier or generated through some other technique) with the reserved link-local prefix to generate link-local addresses for their attached interfaces. Additional addresses can then be created by combining prefixes advertised in Router Advertisements via Neighbor Discovery (defined in RFC 4861 [NAR200702]) with the interface identifier.

Note: As seen addresses generated using stateless address autoconfiguration contain an embedded interface identifier that remains constant over time. Whenever a fixed identifier is used in multiple contexts, a security exposure could theoretically result. A correlation can be performed by an attacker who is in the path between the node in question and the peer(s) to which it is communicating, and who can view the IPv6 addresses present in the datagrams. Because the identifier is embedded within the IPv6 address, which is a fundamental requirement of communication, it cannot be easily hidden. Solutions to this issue have been proposed by generating interface identifiers that vary over time [NAR200701].

IPv6 addresses are “leased” to an interface for a fixed established time (including an infinite time.) When this “lifetime” expires, the link between the interface and the address is invalidated and the address can be reallocated to other interfaces. For the suitable management of addresses’ expiration time, an address goes through two states (stages) while is affiliated to an interface [IPV200501]:

1. At first, an address is in a “preferred” state, so its use in any communication is not restricted.
2. After that, an address becomes “deprecated,” indicating that its affiliation with the current interface will (soon) be invalidated.

When it is in a “deprecated” state, the use of the address is discouraged, although it is not forbidden. However, when possible, any new communication

(e.g., the opening of a new TCP connection) must use a “preferred” address. A “deprecated” address should only be used by applications that have already used it before and in cases where it is difficult to change this address to another address without causing a service interruption.

To ensure that allocated addresses (granted either by manual mechanisms or by autoconfiguration) are unique in a specific link, the *link duplicated addresses detection algorithm* is used. The address to which the duplicated address detection algorithm is being applied to is designated (until the end of this algorithmic session) as an “attempt address.” In this case, it does not matter that such address has been allocated to an interface and received packets are discarded.

Next, we describe how an IPv6 address is formed. The lowest 64 bits of the address identify a specific interface, and these bits are designated as “interface identifier.” The highest 64 bits of the address identify the “path” or the “prefix” of the network or router in one of the links to which such interface is connected. The IPv6 address is formed by combining the prefix with the interface identifier.

It is possible for a host or device to have IPv6 and IPv4 addresses simultaneously. Most of the systems that currently support IPv6 allow the simultaneous use of both protocols. In this way, it is possible to support communication with IPv4-only-networks, as well as IPv6-only-networks and the use of the applications developed for both protocols [IPV200501].

Is it possible to transmit IPv6 traffic over IPv4 networks via tunneling methods? This approach consists of “wrapping” the IPv6 traffic as IPv4 payload data: IPv6 traffic is sent “encapsulated” into IPv4 traffic, and at the receiving end, this traffic is parsed as IPv6 traffic. Transition mechanisms are methods used for the coexistence of IPv4 and/or IPv6 devices and networks. For example, an “IPv6-in-IPv4 tunnel” is a transition mechanism that allows IPv6 devices to communicate through an IPv4 network. The mechanism consists of creating the IPv6 packets in a normal way and encapsulating them in an IPv4 packet. The reverse process is undertaken in the destination machine that deencapsulates the IPv6 packet.

There is a significant difference between the procedures to allocate IPv4 addresses that focus on the parsimonious use of addresses (since addresses are a scarce resource and should be managed with caution) and the procedures to allocate IPv6 addresses that focus on flexibility. Internet Service Providers (ISPs) deploying IPv6 systems follow the RIRs’ policies relating to how to assign IPv6 addressing space among their clients. RIRs are recommending ISPs and operators allocate to each IPv6 client a /48 subnetwork; this allows clients to manage their own subnetworks without using NAT. (The implication is that the *obligatory* need for NAT for intranet-based devices disappears in IPv6).

In order to allow its maximum scalability, the IPv6 protocol uses an approach based on a basic header, with minimum information. This differentiates it from

IPv4 where different options are included in addition to the basic header. IPv6 uses a header “concatenation” mechanism to support supplementary capabilities. The advantages of this approach include the following:

- The size of the basic header is always the same, and is well known. The basic header has been simplified compared with IPv4, since only eight fields are used instead of 12. The basic IPv6 header has a fixed size; hence, its processing by nodes and routers is more straightforward. Also, the header’s structure aligns to 64 bits, so that new and future processors (64 bits minimum) can process it in a more efficient way.
- Routers placed between a source point and a destination point (i.e., the route that a specific packet has to pass through), do not need to process or understand any “following headers.” In other words, in general, interior (core) points of the network (routers) only have to process the basic header, while in IPv4, all headers must be processed. This flow mechanism is similar to the operation in MPLS, yet precedes it by several years.
- There is no limit to the number of options that the headers can support (the IPv6 basic header is 40 octets in length, while in IPv4 the header varies from 20 to 60 octets, depending on the options used).

In IPv6, interior/core routers do not perform packets fragmentation, but the fragmentation is performed end-to-end. That is, source and destination nodes perform, by means of the IPv6 stack, the fragmentation of a packet and the reassembly, respectively. The fragmentation process consists of dividing the source packet into smaller packets or fragments [IPV200501].

The IPv6 specification defines a number of Extension Headers [HER200201] (also see Table 2.5 [DES200301]):

- *Routing Header*: Similar to the source routing options in IPv4. The header is used to mandate a specific routing.
- *Authentication Header (AH)*: A security header that provides authentication and integrity.
- *Encapsulating Security Payload (ESP) Header*: A security header that provides authentication and encryption.
- *Fragmentation Header*: The Fragmentation Header is similar to the fragmentation options in IPv4.
- *Destination Options Header*: Header that contains a set of options to be processed only by the final destination node. Mobile IPv6 is an example of an environment that uses such a header.
- *Hop-by-Hop Options Header*: A set of options needed by routers to perform certain management or debugging functions.

TABLE 2.5 IPv6 Extension Headers

Header (protocol ID)	Description
Hop-by-Hop Options header (protocol 0)	The Hop-by-Hop Options header is used for Jumbogram packets and the Router Alert. An example of applying the Hop-by-Hop Options header is Resource Reservation Protocol (RSVP). This field is read and processed by every node and router along the delivery path.
Destination Options header (protocol 60)	This header carries optional information that is specifically targeted to a packet's destination address. The Mobile IPv6 protocol specification makes use of the Destination Options header to exchange registration messages between mobile nodes and the home agent. Mobile IP is a protocol allowing mobile nodes to keep permanent IP addresses even if they change point of attachment.
Routing header (protocol 43)	This header can be used by an IPv6 source node to force a packet to pass through specific routers on the way to its destination. A list of intermediary routers may be specified within the Routing header when the Routing Type field is set to 0.
Fragment header (protocol 44)	In IPv6, the Path MTU Discovery (PMTUD) mechanism is recommended to all IPv6 nodes. When an IPv6 node does not support PMTUD and it must send a packet larger than the greatest MTU along the delivery path, the Fragment header is used. When this happens, the node fragments the packets and sends each fragment using Fragment headers; then the destination node reassembles the original packet by concatenating all the fragments.
Authentication header (AH) (protocol 51)	This header is used in IPsec to provide authentication, data integrity, and replay protection. It also ensures protection of some fields of the basic IPv6 header. This header is identical in both IPv4 and IPv6.
Encapsulating Security Payload (ESP) header (protocol 50)	This header is also used in IPsec to provide authentication, data integrity, replay protection, and confidentiality of the IPv6 packet. Similar to the authentication header, this header is identical in both IPv4 and IPv6.

As noted, IPsec provides network-level security where the application data is encapsulated within the IPv6 packet. IPsec utilizes the AH and/or ESP Header to provide security (the AH and ESP Header may be used separately or in combination). IPsec, with ESP, offers integrity and data origin authentication, confidentiality, and optional (at the discretion of the receiver) anti-replay features (using confidentiality without integrity is discouraged by the RFCs); in addition, ESP provides limited traffic flow confidentiality. Both the AH and ESP header may be employed as follows [HER200201]:

- “*Tunnel mode*”: The protocol is applied to the entire IP packet. This method is needed to ensure security over the entire packet, where a new IPv6 header and an AH or ESP header are wrapped around the original IP packet.
- “*Transport mode*”: The protocol is just applied to the transport layer (i.e., TCP, UDP, ICMP) in the form of an IPv6 header, AH or ESP Header, followed by the transport protocol data (header, data) (see Figure 2.6).

It should be noted that although the basic IPv6 standards have long been stable, considerable work continues in the IETF, particularly to resolve the issue of highly scalable multihoming support for IPv6 sites, and to resolve the problem of IP layer interworking between IPv6-only and IPv4-only hosts. IPv6/IPv4 interworking at the application layers is handled within the original dual-stack model of IPv6 deployment: either one end of an application session will have dual-stack connectivity, or a dual-stack intermediary such as an Hypertext Transfer Protocol (HTTP) proxy or Simple Mail Transfer Protocol (SMTP) server will interface to both IPv4-only and IPv6-only hosts or applications [CAR201001].

2.4 HEADER COMPRESSION SCHEMES

Implementation of IPv6 gives rise to concerns related to expanded packet headers, especially for video and wireless (low bandwidth channel) applications. As noted in earlier sections the packet header size doubled from 20 bytes in IPv4 to at least 40 bytes in IPv6. The use of network-layer encryption mechanism nearly doubles IP operational overhead. Header Compression (HC) is, therefore, of interest. Currently, the use of HC in commercial networks is generally rare, but wireless and video applications (especially in an IPv6 environment) may well drive future deployment of the technology.

HC algorithms can reduce the performance and throughput impact of expanded IPv6 packet headers and protocol-imposed overhead. Consider the illustrative case where packets with constant 20 byte payloads are transmitted using a 40-byte IPv6 Header. Consider a 1 Mbps link. Then during a 1 second period, about 666 Kb transmitted over the link is IPv6 overhead, and only about 333 Kb transmitted over the link is actual user data. This implies that 66% of data transmitted is overhead. Now consider the case where the same packet of payload is sent with a 2-byte Compressed Header. Now over a 1 second period, about 90 Kb transmitted is IPv6 overhead, and about 910 Kb transmitted is actual user data. This implies that only 9% of data transmitted is overhead. This example shows that HC can theoretically decrease header overhead by 95%. Overhead is defined as “IP header bytes” divided by “total bytes transmitted.” Naturally, the overhead for larger packets will be less as a total percentage. Studies show that although the average packet length of packets traveling over the Internet is around 350–400 bytes, a considerable

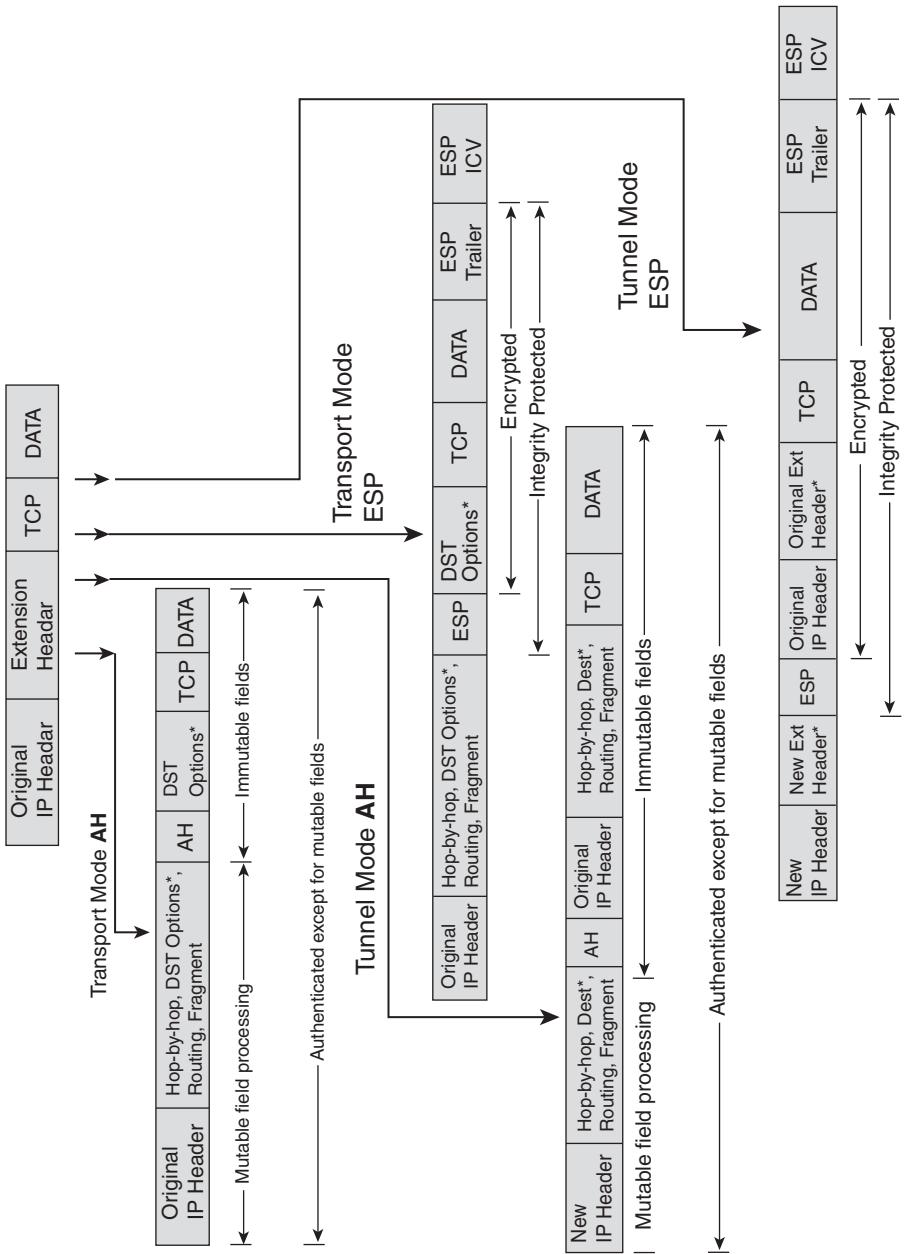


FIGURE 2.6 IPsec modes and types.

portion of the Internet traffic is short (say, 40 bytes or less) [ERT200401]. Depending on the encapsulation protocol, video packets can also be small. For example, under the DVB standard (e.g., DVB-T, DVB-C, DVB-S, and DVB-S2), basic packets have a length of 204 bytes. This implies a significant percentage of overhead is incurred without HC. (For illustration, a 40 byte IPv6 header on a DVB packet would result in an overhead of $40/244 = 16.39\%$; if one assumes that header size is reduced to 2 bytes per packet, the overhead is $2/206 = 0.97\%$.)

There is additional protocol overhead. Applications using data carried within RTP will, in addition to link-layer framing, have an IPv4 header (20 octets), a UDP header (8 octets), and an RTP header (12 octets), for a total of 40 octets. With IPv6, the IPv6 header is 40 octets for a total of 60 octets. Applications transferring data using TCP have 20 octets for the transport header, for a total size of 40 octets for IPv4 and 60 octets for IPv6 [JOH200701].

Usually, HC techniques are applied to a link, on a per-hop basis. Application of hop-by-hop header compression techniques to network backbones is relatively rare because to achieve compression over the network, multiple compression-decompression cycles are required. This represents a scalability and resource issues on core network nodes. Developments in the IETF in the past five years provide a framework for applying header compression over multiple hops to backbone networks. For example, work has been done header compression techniques to MPLS backbones and mobile ad hoc networks (MANETs) (where tradeoffs need to be made between computational processing, power requirements, and bandwidth savings.)

Traditionally compression is applied to Layer 3 (IP) and several Layer 4 protocol headers; for example, RTP/UDP/IPv6 headers can be compressed from 60 bytes to 2–4 bytes. See Figure 2.7. HC algorithms can also reduce the additional overhead introduced by network-layer encryption mechanisms

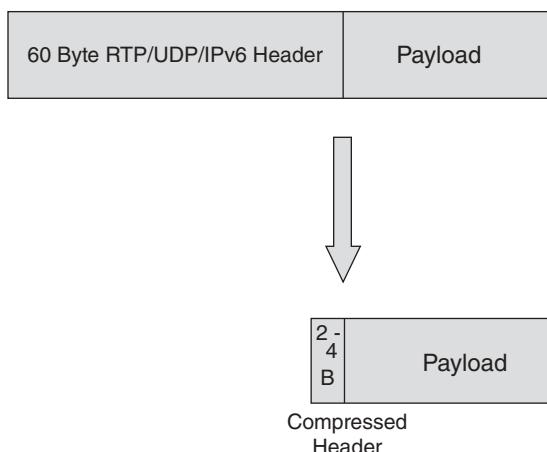


FIGURE 2.7 HC for IPv6.

(e.g., IPsec). Compression algorithms that address encryption/decryption have the ability to: (1) compress inner headers before encryption, and (2) compress outer ESP/IP headers after encryption. Two compression protocols emerged from the IETF in recent years:

1. Internet protocol header compression (IPHC), a scheme designed for low-bit error rate links (compression profiles were originally defined in RFC 2507 and RFC 2508, and further discussed in RFC 4995, 4996, and 4497); it provides compression of TCP/IP, UDP/IP, RTP/UDP/IP, and ESP/IP header; “enhanced” compression of RTP/UDP/IP (ECRTP) headers is defined in RFC 3545.
2. Robust header compression (ROHC) is a scheme designed for wireless links that provides greater compression compared with IPHC at the cost of greater implementation complexity (compression profiles were originally defined in RFC 3095 and RFC 3096 with further developments in other RFCs [JOH200701], [PEL200701], [FIN200701]); this is more suitable for high BER, long RTT links, and supports compression of ESP/IP, UDP/IP, and RTP/UDP/IP headers.

Compression is applied over a link between a source node (i.e., compressor), and a destination node (i.e., decompressor). HC algorithms make use of protocol interpacket header field redundancies to improve overall efficiency. Both compressor and decompressor store header fields of each packet stream, and associate each stream with a context identifier (CID). Upon reception of a packet with an associated context, the compressor removes the IPv6 header fields from packet header and appends a CID. Upon reception of a packet with a CID, the decompressor inserts IPv6 header fields back into the packet header and transmits the packet [ERT200401]. IPHC and ROHC are both specified in Release 4 and Release 5 of the 3rd Generation Partnership Project (3GPP). The Cisco Systems router Internetwork Operating System (IOS) provides IPHC implementation.

Point-to-Point Protocol (PPP) (defined in RFC 1661) provides (1) a method for encapsulating datagrams over serial links; (2) a Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection; and (3) a family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols. In order to establish communications over a point-to-point link, each end of the PPP link must first send LCP packets to configure and test the data link. After the link has been established and optional facilities have been negotiated as needed by the LCP, PPP must send NCP packets to choose and configure one or more network-layer protocols. Once each of the chosen network-layer protocols has been configured, datagrams from each network-layer protocol can be sent over the link. The link will remain configured for communications until explicit LCP or NCP packets close the link down, or until some external event occurs (power failure at the other end, carrier drop, etc.) [VAR200801].

In RFC 5072, the NCP for establishing and configuring IPv6 over PPP, called IPV6CP, is defined. In RFC 5172, the compression parameter for use in IPv6 datagram compression is defined. The Configuration Option described in this just-cited RFC provides a way to negotiate the use of a specific IPv6 packet compression protocol. The IPv6 Compression Protocol Configuration Option is used to indicate the ability to receive compressed packets. IPv6-Compression-Protocol field values have been assigned in for IPHC (0061), and for ROHC (0003).

2.5 QUALITY OF SERVICE (QoS) IN IPv6

Obviously, streaming audio and video requires low latency and high throughput. QoS is supported in IPv6. The IPv6 header has two QoS-related fields:

- 20-bit Flow label, usable in IntServ-based environments. In IntServ environments, performance guarantees to traffic and resource reservations are provided on per-flow basis. A guaranteed and controlled load service capability is supported. IntServ approaches have scalability issues;
- 8-bit Traffic Class indicator usable in DiffServ-based environments. DiffServ environments are more common. The traffic class field may be used to set specific precedence or Differentiated Services Code Point (DSCP) values. These values are used in the exact same way as in IPv4. Performance guarantees are provided to traffic aggregates rather than to flows. DiffServ classifies all the network traffic into classes. Two distinct types (per hop behaviors) are supported:
 - *Expedited Forwarding (EF)*: Aims at providing QoS for the class by minimizing jitter and is generally focused on providing stricter guarantees;
 - *Assured Forwarding (AF)*: Inserts at most four classes with at most three levels of packets dropping categories.

There are no signaling protocol for resource allocation (admission control) and QoS mechanisms control. The following priority levels are typical, but variances are possible:

- Level 0—No specify priority
- Level 1—Background traffic (news)
- Level 2—Unattended data transfer (email)
- Level 3—Reserved
- Level 4—Attended bulk transfer (FTP)
- Level 5—Reserved
- Level 6—Interactive traffic (Telnet and Windowing)
- Level 7—Control traffic (routing, network management)

2.6 MIGRATION STRATEGIES TO IPv6

2.6.1 Technical Approaches

While the infrastructure is in place for IPv4 and IPv6 systems to run in parallel, widespread adoption of IPv6 has been slow because the two systems are not directly compatible (IPv6 and IPv4 protocols can coexist, but they cannot inter-communicate directly), and there has been so far rather limited economic incentive for providers and end-user firms to introduce the technology [RAS201101]. Therefore, migration to IPv6 environments is expected to be fairly complex. However, with the growth in the number of users and the IPv4 address exhaustion, large-scale deployment will invariably happen in the near future. Initially, internetworking between the two environments will be critical [MIN200802]. Existing IPv4-end points and/or nodes will need to run dual stack nodes or convert to IPv6 systems. Fortunately, the new protocol supports an IPv4-compatible IPv6 address that is an IPv6 address employing embedded IPv4 addresses. Tunneling, which we already described in passing, will play a major role in the beginning. There are a number of requirements that are typically applicable to an organization wishing to introduce an IPv6 service [6NE200501]:

- The existing IPv4 service should not be adversely disrupted (e.g., as it might be by router loading of encapsulating IPv6 in IPv4 for tunnels).
- The IPv6 service should perform as well as the IPv4 service (e.g., at the IPv4 line rate, and with similar network characteristics).
- The service must be manageable and be able to be monitored (thus tools should be available for IPv6 as they are for IPv4).
- The security of the network should not be compromised, due to the additional protocol itself or a weakness of any transition mechanism used.
- An IPv6 address allocation plan must be drawn up.

Well-known interworking mechanisms include the following, as described in RFC 2893:

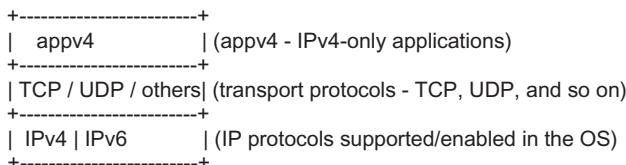
- *Dual IP Layer (Also Known as Dual Stack)*: A technique for providing complete support for both Internet protocols—IPv4 and IPv6—in hosts and routers.
- *Configured Tunneling of IPv6 over IPv4*: Point-to-point tunnels made by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures.
- *Automatic Tunneling of IPv6 over IPv4*: A mechanism for using IPv4-compatible addresses to automatically tunnel IPv6 packets over IPv4 networks.

Tunneling techniques include the following approaches, as described in RFC 2893:

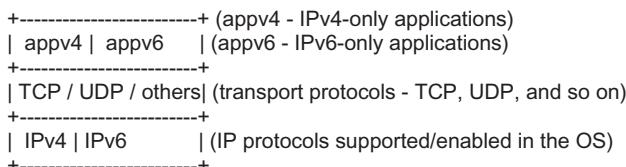
- *IPv6-over-IPv4 Tunneling*: The technique of encapsulating IPv6 packets within IPv4 so that they can be carried across IPv4 routing infrastructures.
- *Configured Tunneling*: IPv6-over-IPv4 tunneling where the IPv4 tunnel end point address is determined by configuration information on the encapsulating node. The tunnels can be either unidirectional or bidirectional. Bidirectional configured tunnels behave as virtual point-to-point links.
- *Automatic Tunneling*: IPv6-over-IPv4 tunneling where the IPv4 tunnel end point address is determined from the IPv4 address embedded in the IPv4-compatible destination address of the IPv6 packet being tunneled.
- *IPv4 Multicast Tunneling*: IPv6-over-IPv4 tunneling where the IPv4 tunnel end point address is determined using Neighbor Discovery. Unlike configured tunnelling, this does not require any address configuration, and unlike automatic tunnelling, it does not require the use of IPv4-compatible addresses. However, the mechanism assumes that the IPv4 infrastructure supports IPv4 multicast.

Applications (and the lower-layer protocol stack) need to be properly equipped. Some example interoperability techniques include dual stacks and tunneling—IPv6-in-IPv4 (e.g., 6-to-4, 6rd, and protocol 41), IPv4-in-IPv6, IPv6-in-UDP (Teredo, TSP). There are four cases, as described in RFC 4038:

Case 1: IPv4-only applications in a dual-stack node. IPv6 protocol is introduced in a node, but applications are not yet ported to support IPv6. The protocol stack is as follows:

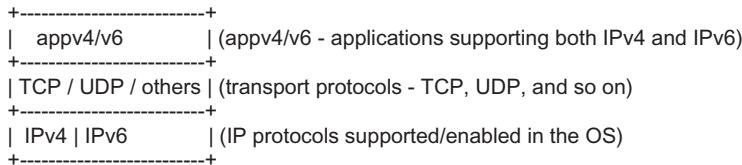


Case 2: IPv4-only applications and IPv6-only applications in a dual-stack node. Applications are ported for IPv6 only. Therefore there are two similar applications, one for each protocol version (e.g., ping and ping6). The protocol stack is as follows:



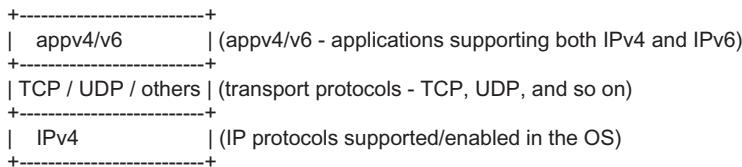
Case 3: Applications supporting both IPv4 and IPv6 in a dual stack node.

Applications are ported for both IPv4 and IPv6 support. Therefore, the existing IPv4 applications can be removed. The protocol stack is as follows:



Case 4: Applications supporting both IPv4 and IPv6 in an IPv4-only node.

Applications are ported for both IPv4 and IPv6 support, but the same applications may also have to work when IPv6 is not being used (e.g., disabled from the OS). The protocol stack is as follows:



The first two cases are not interesting in the longer term; only a few applications are inherently IPv4 or IPv6 specific and should work with both protocols without having to care about which one is being used.

It should be noted that the transition from a pure IPv4 network to a network where IPv4 and IPv6 co-exist brings a number of extra security considerations that need to be taken into account when deploying IPv6 and operating the dual-protocol network and the associated transition mechanisms [DAV200701], [MIN200901].

Figure 2.8 depicts some basic scenarios of carrier-based IPv6 support. Case (a) and (b) represent traditional environments where the carrier link supports either a clear channel that is used to connect, say, two IPv4 routers, or is IP-aware. (In each case, the “cloud” on the left could also be the IPv4 Internet or the IPv6 Internet.)

In Case (c), the carrier link is used to connect as a transparent link two IPv6 routers; the carrier link is not (does not need to be) aware that it is transferring IPv6 PDUs. In Case (d), the carrier system is IPv4-aware, so the use of that environment to support IPv6 requires IPv6 to operate in a tunneled-mode over the non-IPv6 cloud, which is a capability of IPv6.

In Case (e), the carrier infrastructure needs to provide a gateway function between the IPv4 and the IPv6 world (this could entail repacking the IP PDUs from the v4 format to the v6 format). Case (f) is the ideal long-term scenario where the “world has converted to IPv6” and “so did the carrier network.”

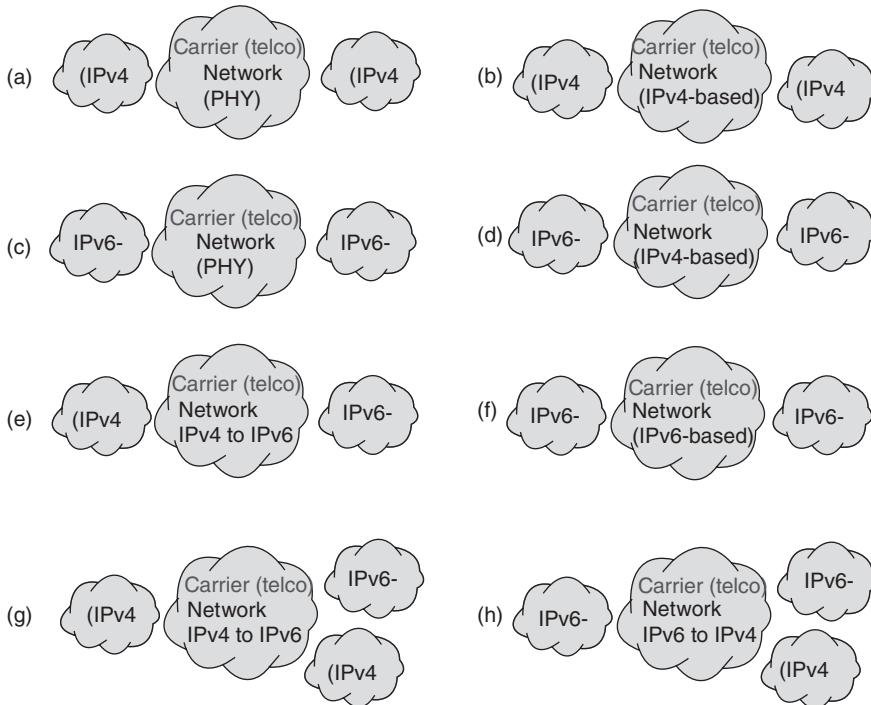


FIGURE 2.8 Support of IPv6 in carrier networks.

In Case (g), the carrier IP-aware network provides a conversion function to support both IPv4 (as a baseline) and IPv6 (as a “new technology”) handoffs. Possibly, a dual-stack mechanism is utilized. In Case (h), the carrier IPv6-aware network provides a support function for IPv6 (as a baseline), and also a conversion function to support legacy IPv4 islands.

Some user organizations have expressed concerns about security in an IPv6 environment, fundamentally because of tunneling and firewall issues. The interested reader should consult [MIN200901] for an extensive discussion of this topic and for tools and techniques to address the issues. Even network/security administrators that operate in a pure IPv4 environment need to be aware of IPv6-related security issues. In a standard IPv4 environment where IPv6 is not explicitly supported, any form of IPv6-based tunneling traffic must be considered abnormal, malicious traffic. For example, unconstrained 6to4-based traffic should be blocked (as noted elsewhere 6to4 is a transitional mechanism intended for individual independent nodes to connect IPv6 over the greater Internet.) Most commercial-grade IPv4 firewalls block IP protocol 41, the 6to4 and tunnel protocol, unless it has been explicitly enabled [WAR200401].

2.6.2 Residential Broadband Services in an IPv6 Environment

One of the challenges related to the deployment of IPv6 is how to continue to support IPv4 services in residential broadband environments at the same time as the users migrate to a mixed IPv4 and IPv6 operational model. IPTV/IBTV/NTTV users may want to use IPv6 to access video services. This is especially critical as IPv6 is technically incompatible with IPv4; this forces the introduction of some new concepts that change the present operation of broadband networks and has ramifications on how IPv6 can be offered to residential subscribers. Three approaches can be used, as covered in [HEN201101] on which this discussion is based:

1. IPv6 support in telco environments using Point-to-Point Protocol over Ethernet (PPPoX) and/or Asynchronous Transfer Mode (ATM) as defined in TR-187 of the Broadband Forum.
2. IPv6 support using PPPoX in conjunction with the Bridged Residential Gateway.
3. IPv6 support using IP over Ethernet (IPoE) as defined in the Broadband Forum specification TR-177.

Approach 1: The introduction of IPv6 using PPPoX/Layer 2 Tunneling Protocol (L2TP) has no implications on the access and aggregation network elements. PPP session authentication for IPv6 is identical to IPv4, using Password Authentication Protocol/Challenge Handshake Authentication Protocol (PAP/CHAP) or option 82. IPv4 and IPv6 authentication can be done in a single authentication phase to RADIUS (Remote Authentication Dial-In User Service). Since PPPoX IPv6 Control Protocol (CP) is only defining the Link Local Address (LLA), global IPv6 addresses are typically assigned using DHCP or SLAAC. To support an IPv6-routed Residential Gateway (RG) using the PPP termination and aggregation/L2TP Network Server (PTA/LNS) model, the following mechanisms are required between the RG and the Broadband Network Gateway/Broadband Remote Access Server (BNG/BRAS) to ensure IPv6 connectivity:

- PPPoX IPv6 Control Protocol (CP) is used for LLA assignment.
- DHCPv6 Prefix Delegation (IA-PD—Identity Association for Prefix Delegation) is used to obtain a prefix for LAN address assignment.
- Stateless DHCPv6 is used to obtain additional configuration parameters.
- When the numbered RG model is deployed, stateful DHCPv6 (Identity Association for Non-temporary Addresses [IA-NA]) is used to obtain an RG management IPv6 address; in case of an unnumbered RG model, this is not required.
- Route advertisements are required to assign the default gateway assignment.

Approach 2: The utilization of the Bridged Residential Gateway requires the following:

- PPPoX IPv6CP is used for LLA assignment;
- SLAAC is used for the host to obtain a Global-Unicast IPv6 address;
- stateless DHCP is used to obtain additional configuration parameters; and
- route advertisements are used to assign the default gateway assignment.

Therefore, to support IPv6 in a telco environment, PPPoX for IPv6 imposes no different requirements on $N:1$ Virtual Local Area Network (VLAN) or $1:1$ VLAN architectures or on a bridged gateway model, compared with IPv4. However, PPPoX for IPv6 will always impact the BNG/BRAS, CPE, and home gateway using a routed gateway model.

Approach 3: The implications for introducing IPv6 IPoE mainly depend on the VLAN model used ($1:1$ or $N:1$) and the operational model of the home gateway (bridged or routed). The impact of IPv6 support for IPoE in a Bridged Residential Gateway model depends on whether DHCP or SLAAC is used to the end device. When deploying DHCP, the key difference from the Routed RG IPoE model arises from the fact that there is no DHCP PD address required, and only an IA address is assigned to the host. Care must be taken to ensure communication between IPv6 devices in the home remains local and is not sent through the BNG.

2.6.3 Deployment Opportunities

There was a lack of ubiquitous IPv6 utilization as of early 2012; this is partly due to the fact that the number of IPv6 nodes is rather low. However, IPv6 rollout has started to get traction. The approaching exhaustion of IPv4 address space will bring about a situation where ISPs are faced with a choice between one or more of three major alternatives [CAR201001]:

1. Squeeze the use of IPv4 addresses even harder than today, using smaller and smaller address blocks per enterprise customer, and possibly trading address blocks with other ISPs.
2. Install multiple layers of NAT or share IPv4 addresses by other methods, such as address-plus-port mapping.
3. Deploy IPv6 and operate IPv4-IPv6 coexistence and interworking mechanisms.

RFC 5514 (April 2009) proposed to vastly increase the number of IPv6 hosts by transforming all Social Networking platforms into IPv6 networks. This would immediately add millions of IPv6 hosts to the existing IPv6 Internet.

Hosts (PCs and servers) and network infrastructure (routers, switches) are generally IPv6-ready at this time, but organizations may need to upgrade their overall end-to-end environment. Service providers, such as Google, have

already rolled out an IPv6 site for customers already on that system. In fact, Google, Facebook, Yahoo!, Akamai, and Limelight Networks are among some of the larger companies that planned a one-day test run of IPv6 addresses as part of World IPv6 Day, on June 8, 2011, to encourage the transition to the new namespace. These organizations were planning to offer their content over IPv6 for a 24-hour “test flight” with the goal of the Test Flight Day is to motivate organizations across the industry—Internet service providers, hardware makers, operating system vendors and web companies—to prepare their services for IPv6 to ensure a successful transition as IPv4 addresses run out. Internet users did not need to do anything different on World IPv6 Day. Web services, Internet service providers, and operating system (OS) manufacturers were planning to be updating their systems to ensure Internet users receive uninterrupted service. In rare cases, users may still experience connectivity issues when visiting participating Websites. Users were able to visit an IPv6 test site to check if their connectivity was impacted. Organizations that wanted to bring their company’s website online using IPv6 during the World IPv6 Day needed to make it IPv6 accessible using dual stack technology and provide a AAAA record for the site. Of course, IPv4 websites continued to be accessible over IPv4 during the event.

According to the Internet Society (ISOC), the World IPv6 Day saw more than 1000 major website operators switch over to IPv6-compatible main pages in the most extensive live run of the next-generation addressing protocol so far. The day turned out to be a technological success. Around two-thirds of the participants were reportedly so pleased with the results they left IPv6 enabled going forward. Nonetheless, just 0.16% of Facebook users were IPv6 natives and 0.04% were using 6to4 tunnelling capabilities, delivering around 1 million IPv6 visitors over the course of the day.

In DNS, host names are mapped to IPv6 addresses by AAAA (also known as Quad A) resource records (RR). The IETF specifies the use AAAA RR for forward mapping and Pointer Records (PTR) RRs for reverse mapping. The IPv6 AAAA RR approach is described in RFC 3596. The forward DNS entry for an IPv6 entry is entered using AAAA. It can be entered using the full IPv6 address or by using the shorthand :: notation. Pointer records are the opposite of AAAA RRs and are used in Reverse Map zone files to map an IPv6 address to a host name.

Tier 1 telecommunication firms have been upgrading their infrastructure over the past few years in anticipation of the eventual transition. The same has occurred for content providers. For example, Comcast has begun assigning IPv6 addresses to its cable modem customers in a “native dual stack” configuration as of early 2011; under this configuration, customers have both IPv4 and IPv6 addresses and can access content and services over both systems. Comcast’s first 25 IPv6-enabled customers went live January 11, 2011 in the Littleton, Colorado. Time Warner Cable has already signed up commercial customers on IPv6 and was planning to begin residential IPv6 trials in early 2011. Time Warner Cable is also expected to adopt a dual-stack approach similar to that

of Comcast. Domain infrastructure company VeriSign will also provide business services to assist companies with the transition in 2011 [RAS201101].

Having ISPs deploy IPv6 to customers' sites, in addition to IPv4 and without extra charge, is a way to break the existing impasse that has delayed IPv6 deployment: ISPs wait for customer demand before deploying IPv6; customers do not demand IPv6 as long as application vendors announce that their products work on existing infrastructures (that are based on IPv4 with NATs); application vendors focus their investments on NAT traversal compatibility as long as ISPs do not deploy IPv6. However, most ISPs are not willing to add IPv6 to their current offerings at no charge unless incurred investment and operational costs are small. For this, ISPs that provide router customer premise equipment (CPE) to their customers have the most favorable conditions: they can upgrade their router CPEs and can operate gateways between their IPv4 infrastructures and the global IPv6 Internet to support IPv6 encapsulation in IPv4. They then need no additional routing plans than those that already exist on these IPv4 infrastructures. Encapsulation using 6to4 methods, as specified in RFC 3056, is nearly sufficient for this: (1) it is simple; (2) it is supported on many platforms, including PC-compatible appliances; (3) open-source portable code is available; and (4) its stateless nature ensures good scalability. There is, however, a limitation of 6to4 that prevents ISPs from using it to offer full IPv6 unicast connectivity to their customers. While an ISP that deploys 6to4 can guarantee that IPv6 packets outgoing from its customer sites will reach the IPv6 Internet, and also can guarantee that packets coming from other 6to4 sites will reach its customer sites, it cannot guarantee that packets from native IPv6 sites will reach them. The problem is that a packet coming from a native IPv6 address needs to traverse (somewhere on its way) a 6to4 relay router to do the required IPv6/IPv4 encapsulation. There is no guarantee that routes toward such a relay exist from everywhere, nor is there a guarantee that all such relays do forward packets toward the IPv4 Internet. Also, if an ISP operates one or several 6to4 relay routers and opens IPv6 routes toward them in the IPv6 Internet, for the 6to4 prefix 2002::/16, it may receive in these relays packets destined to an unknown number of other 6to4 ISPs. If it does not forward these packets, it creates a “black hole” in which packets may be systematically lost, breaking some of the IPv6 connectivity. If it does forward them, it can no longer dimension its 6to4 relay routers in proportion to the traffic of its own customers; QoS, at least for customers of other 6to4 ISPs, will then not be guaranteed [DES201001]. To address these issues, RFC 5569, *6rd—IPv6 Rapid Deployment*, also known simply as *6rd*, proposes to slightly modify 6to4 so that:

1. Packets coming from the global Internet that enter *6rd* gateways of an ISP are only packets destined to customer sites of this ISP.
2. All IPv6 packets destined to *6rd* customer sites of an ISP, and coming from anywhere else on the IPv6 Internet, traverse a *6rd* gateway of this ISP.

The principle of the RFC 5569 proposal is that to build on 6to4 and suppress its limitation, it is sufficient that:

1. 6to4 functions are modified to replace the standard 6to4 prefix 2002::/16 by an IPv6 prefix that belongs to the ISP-assigned address space, and to replace the 6to4 anycast address by another anycast address chosen by the ISP.
2. The ISP operates one or several 6rd gateways (upgraded 6to4 routers) at its border between its IPv4 infrastructure and the IPv6 Internet.
3. CPEs support IPv6 on their customer-site side and support 6rd (upgraded 6to4 function) on their provider side.

There is no guarantee that this proposal will be broadly accepted, but it represents one press-time approach for IPv6 deployment. Table 2.6 lists some key recent RFCs dealing with IPv6 deployment (see Appendix 2A for a more comprehensive list).

TABLE 2.6 Some Recent RFC Dealing with IPv6 Deployment

RFC 4029 (March 2005)	Discusses scenarios for introducing IPv6 into ISP networks, as the problem was viewed some years ago. Its end goal is simply a dual-stack ISP backbone. Today's view is that this is insufficient, as it does not allow for interworking between IPv6-only and legacy (IPv4-only) hosts. Indeed, the end goal today might be an IPv6-only ISP backbone, with some form of legacy IPv4 support.
RFC 4779 (January 2007)	Discusses deployment in broadband access networks, such as Cable Television, Asymmetric Digital Subscriber Line (ADSL), and wireless.
RFC 5181 (May 2008)	RFCs deal with IEEE 802.16 access networks.
RFC 5121 (February 2008)	Discusses how MPLS-based ISPs may use the IPv6 Provider Edge Router (6PE) mechanism.
RFC 5692 (October 2009)	Covers IPv6 security issues, especially those that are specific to transition and IPv4-IPv6 coexistence scenarios.
RFC 4798 (February 2007)	Discusses “Local Network Protection”: how the internal structure of an IPv6 site network can be protected. This affects how well an ISP’s customers are protected after they deploy IPv6.
RFC 4942 (September 2007)	Describes a possible sequence of events for IPv6 adoption in the Internet as a whole, with direct implications for ISPs. Its main point, perhaps, is that by the year 2012, it will be appropriate to regard IPv4 networks as the legacy solution.
RFC 4864 (May 2007)	
RFC 5211 (July 2008)	

REFERENCES

- [6NE200501] 6NET, “D2.2.4:Final IPv4 to IPv6 transition cookbook for organizational/ISP (NREN) and backbone networks,” Version: 1.0 (4th February 2005), Project Number: IST-2001-32603, CEC Deliverable Number: 32603/UOS/DS/2.2.4/A1.
- [BLA200801] M. Blanchet, “Special-use IPv6 addresses,” draft-ietf-v6ops-rfc3330-for-ipv6-04.txt, January 15, 2008.
- [CAR201001] B. Carpenter, S. Jiang, “Emerging service provider scenarios for IPv6 deployment,” RFC 6036, October 2010.
- [DAV200701] E. Davies, S. Krishnan, P. Savola, “IPv6 transition/co-existence security considerations,” RFC 4942, September 2007.
- [DES200301] R. Desmeules, *Cisco Self-Study: Implementing Cisco IPv6 Networks (IPv6)*, Cisco Press, 2003, Jun 6.
- [DES201001] R. Despres, “6rd—IPv6 rapid deployment,” RFC 5569, January 2010.
- [DON200401] F. Donzé, “IPv6 autoconfiguration,” *The Internet Protocol Journal*, 7(2), 2004. Published Online, <http://www.cisco.com>
- [ERT200401] E. Ertekin, C. Christou, “IPv6 header compression,” North American IPv6 Summit, June 2004.
- [FIN200701] R. Finking, G. Pelletier, “Formal notation for ROBust header compression (ROHC-FN),” RFC 4997, July 2007.
- [HEN201101] W. Henderickx, “Making the move to IPv6,” Alcatel-Lucent White Paper, September 20, 2011.
- [HER200201] P. Hermann-Seton, “Security features in IPv6,” SANS Institute 2002, As part of the Information Security Reading Room.
- [HIN200601] R. Hinden, S. Deering, “IP Version 6 addressing architecture,” RFC 4291, February 2006.
- [IPV200501] IPv6 Portal 2005. <http://www.ipv6tf.org>
- [IPV201101] G. Huston, “The IPv4 Address Report,” 2011. Online resource, <http://www.potaroo.net>
- [JOH200401] D. Johnson, C. Perkins, and J. Arkko, “Mobility support in IPv6,” RFC 3775, June 2004.
- [JOH200701] L.-E. Jonsson, G. Pelletier, K. Sandlund, “The ROBust header compression (ROHC) framework,” RFC 4995, July 2007.
- [JUN200801] Juniper Networks Staff, “An IPv6 security guide for U.S. government agencies—Executive summary,” The IPv6 World Report Series, Volume 4 February 2008, Juniper Networks, 1194 North Mathilda Avenue, Sunnyvale, CA 94089 USA.
- [KAE200601] M. Kaeo, D. Green, J. Bound, Y. Pouffary, “IPv6 security technology paper,” North American IPv6 Task Force (NAv6TF) Technology Report, July 22, 2006.
- [LIO199801] A. Lioy, Security features of IPv6. Chapter 8, in *Internetworking IPv6 with Cisco Routers*, ed. Silvano Gai McGraw-Hill, 1998; also available at: www.ip6.com/us/book/Chap8.pdf
- [MIN200601] D. Minoli, *Voice Over IPv6—Architecting the Next-generation VoIP*, Elsevier, New York, 2006.
- [MIN200801] D. Minoli, *IP Multicast with Applications to IPTV and Mobile DVB-H*, Wiley, New York, 2008.

- [MIN200802] D. Minoli, J. Amoss, *Handbook of IPv4 to IPv6 Transition Methodologies For Institutional & Corporate Networks*, Auerbach/CRC, New York, 2008.
- [MIN200901] D. Minoli, J. Kouns, *Security in an IPv6 Environment*, Taylor and Francis, 2009.
- [MIN200902] D. Minoli, *Satellite Systems Engineering in an IPv6 Environment*, Francis and Taylor, 2009.
- [MIN201201] D. Minoli, *Mobile Video with Mobile IPv6*, Wiley, New York, 2012.
- [MSD200401] Microsoft Staff, “Microsoft Corporation, MSDN library, Internet protocol,” 2004, <http://msdn.microsoft.com>
- [NAR200701] T. Narten, R. Draves, S. Krishnan, “Privacy extensions for stateless address autoconfiguration in IPv6,” RFC 4941, September 2007.
- [NAR200702] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, “Neighbor discovery for IP Version 6 (IPv6),” RFC 4861, September 2007.
- [PEL200701] G. Pelletier, K. Sandlund, L.-E. Jonsson, M. West, “RObust header compression (ROHC): A profile for TCP/IP (ROHC-TCP),” RFC 4996, July 2007.
- [RAS201101] F. Y. Rashid, “IPv4 address exhaustion not instant cause for concern with IPv6 in wings, eweek,” 2011-02-01.
- [THO200701] S. Thomson, T. Narten, and T. Jinmei, “IPv6 stateless address autoconfiguration,” RFC 4862, September 2007.
- [VAR200801] S. Varada, ed. “IPv6 datagram compression,” RFC 5172, March 2008.
- [WAR200401] M. H. Warfield, “Security implications of IPv6,” 16th Annual FIRST Conference on Computer Security Incident Handling, June 13–18, 2004—Budapest, Hungary.

APPENDIX 2A IPv6 RFCs

RFC 1809 (Informational)	Using the Flow Label Field in IPv6	1995-06
RFC 1881 (Informational)	IPv6 Address Allocation Management	1995-12
RFC 1883 (Proposed Standard) Obsoleted by RFC 2460	Internet Protocol, Version 6 (IPv6) Specification	1995-12
RFC 1885 (Proposed Standard) Obsoleted by RFC 2463	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)	1995-12
RFC 1887 (Informational)	An Architecture for IPv6 Unicast Address Allocation	1995-12
RFC 1888 (Historic) Obsoleted by RFC 4048 Updated by RFC 4548	OSI NSAPs and IPv6	1996-08
RFC 1897 (Experimental) Obsoleted by RFC 2471	IPv6 Testing Address Allocation	1996-01
RFC 1924 (Informational)	A Compact Representation of IPv6 Addresses	1996-04
RFC 1933 (Proposed Standard) Obsoleted by RFC 2893	Transition Mechanisms for IPv6 Hosts and Routers	1996-04
RFC 1970 (Proposed Standard) Obsoleted by RFC 2461	Neighbor Discovery for IP Version 6 (IPv6)	1996-08

RFC 1971 (Proposed Standard) Obsoleted by RFC 2462	IPv6 Stateless Address Autoconfiguration	1996-08
RFC 1972 (Proposed Standard) Obsoleted by RFC 2464	A Method for the Transmission of IPv6 Packets over Ethernet Networks	1996-08
RFC 2019 (Proposed Standard) Obsoleted by RFC 2467	Transmission of IPv6 Packets Over FDDI	1996-10
RFC 2023 (Proposed Standard) Obsoleted by RFC 2472	IP Version 6 over PPP	1996-10
RFC 2030 (Informational) Obsoleted by RFC 4330	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI	1996-10
Errata		
RFC 2073 (Proposed Standard) Obsoleted by RFC 2374	An IPv6 Provider-Based Unicast Address Format	1997-01
RFC 2080 (Proposed Standard)	RIPng for IPv6	1997-01
RFC 2133 (Informational) Obsoleted by RFC 2553	Basic Socket Interface Extensions for IPv6	1997-04
RFC 2147 (Proposed Standard) Obsoleted by RFC 2675	TCP and UDP over IPv6 Jumbograms	1997-05
RFC 2185 (Informational)	Routing Aspects of IPv6 Transition	1997-09
RFC 2292 (Informational) Obsoleted by RFC 3542	Advanced Sockets API for IPv6	1998-02
RFC 2374 (Historic) Obsoleted by RFC 3587	An IPv6 Aggregatable Global Unicast Address Format	1998-07
RFC 2375 (Informational)	IPv6 Multicast Address Assignments	1998-07
RFC 2428 (Proposed Standard)	FTP Extensions for IPv6 and NATs	1998-09
RFC 2452 (Proposed Standard) Obsoleted by RFC 4022	IP Version 6 Management Information Base for the Transmission Control Protocol	1998-12
RFC 2454 (Historic) Obsoleted by RFC 4113	IP Version 6 Management Information Base for the User Datagram Protocol	1998-12
RFC 2460 (Draft Standard) Updated by RFC 5095, RFC 5722, RFC 5871	Internet Protocol, Version 6 (IPv6) Specification	1998-12
Errata		
RFC 2461 (Draft Standard) Obsoleted by RFC 4861 Updated by RFC 4311	Neighbor Discovery for IP Version 6 (IPv6)	1998-12
RFC 2462 (Draft Standard) Obsoleted by RFC 4862	IPv6 Stateless Address Autoconfiguration	1998-12
Errata		
RFC 2463 (Draft Standard) Obsoleted by RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	1998-12
RFC 2464 (Proposed Standard) Updated by RFC 6085 Errata	Transmission of IPv6 Packets over Ethernet Networks	1998-12

RFC 2465 (Proposed Standard) Obsoleted by RFC 4293	Management Information Base for IP Version 6: Textual Conventions and General Group	1998-12
RFC 2466 (Proposed Standard) Obsoleted by RFC 4293	Management Information Base for IP Version 6: ICMPv6 Group	1998-12
RFC 2467 (Proposed Standard)	Transmission of IPv6 Packets over FDDI Networks	1998-12
RFC 2470 (Proposed Standard)	Transmission of IPv6 Packets over Token Ring Networks	1998-12
RFC 2471 (Historic) Obsoleted by RFC 3701	IPv6 Testing Address Allocation	1998-12
RFC 2472 (Proposed Standard) Obsoleted by RFC 5072, RFC 5172	IP Version 6 over PPP	1998-12
RFC 2473 (Proposed Standard)	Generic Packet Tunneling in IPv6 Specification	1998-12
RFC 2474 (Proposed Standard) Updated by RFC 3168, RFC 3260	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	1998-12
RFC 2491 (Proposed Standard)	IPv6 over Non-Broadcast Multiple Access (NBMA) networks	1999-01
RFC 2492 (Proposed Standard) Errata	IPv6 over ATM Networks	1999-01
RFC 2497 (Proposed Standard)	Transmission of IPv6 Packets over ARCnet Networks	1999-01
RFC 2507 (Proposed Standard)	IP Header Compression	1999-02
RFC 2526 (Proposed Standard)	Reserved IPv6 Subnet Anycast Addresses	1999-03
RFC 2529 (Proposed Standard)	Transmission of IPv6 over IPv4 Domains without Explicit Tunnels	1999-03
RFC 2545 (Proposed Standard)	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	1999-03
RFC 2553 (Informational) Obsoleted by RFC 3493 Updated by RFC 3152	Basic Socket Interface Extensions for IPv6	1999-03
RFC 2590 (Proposed Standard)	Transmission of IPv6 Packets over Frame Relay Networks Specification	1999-05
RFC 2675 (Proposed Standard) Errata	IPv6 Jumbograms	1999-08
RFC 2710 (Proposed Standard) Updated by RFC 3590, RFC 3810	Multicast Listener Discovery (MLD) for IPv6	1999-10
RFC 2711 (Proposed Standard)	IPv6 Router Alert Option	1999-10
RFC 2732 (Proposed Standard) Obsoleted by RFC 3986 Errata	Format for Literal IPv6 Addresses in URL's	1999-12

(Continued)

RFC 2740 (Proposed Standard) Obsoleted by RFC 5340 Errata	OSPF for IPv6	1999-12
RFC 2874 (Experimental) Updated by RFC 3152, RFC 3226, RFC 3363, RFC 3364	DNS Extensions to Support IPv6 Address Aggregation and Renumbering	2000-07
RFC 2893 (Proposed Standard) Obsoleted by RFC 4213	Transition Mechanisms for IPv6 Hosts and Routers	2000-08
RFC 2894 (Proposed Standard)	Router Renumbering for IPv6	2000-08
RFC 2928 (Informational)	Initial IPv6 Sub-TLA ID Assignments	2000-09
RFC 3041 (Proposed Standard) Obsoleted by RFC 4941 Errata	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	2001-01
RFC 3053 (Informational)	IPv6 Tunnel Broker	2001-01
RFC 3056 (Proposed Standard) Errata	Connection of IPv6 Domains via IPv4 Clouds	2001-02
RFC 3089 (Informational)	A SOCKS-based IPv6/IPv4 Gateway Mechanism	2001-04
RFC 3111 (Proposed Standard)	Service Location Protocol Modifications for IPv6	2001-05
RFC 3122 (Proposed Standard)	Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification	2001-06
RFC 3142 (Informational)	An IPv6-to-IPv4 Transport Relay Translator	2001-06
RFC 3146 (Proposed Standard)	Transmission of IPv6 Packets over IEEE 1394 Networks	2001-10
RFC 3162 (Proposed Standard) Errata	RADIUS and IPv6	2001-08
RFC 3175 (Proposed Standard) Updated by RFC 5350	Aggregation of RSVP for IPv4 and IPv6 Reservations	2001-09
RFC 3177 (Informational) Obsoleted by RFC 6177	IAB/IESG Recommendations on IPv6 Address Allocations to Sites	2001-09
RFC 3178 (Informational)	IPv6 Multihoming Support at Site Exit Routers	2001-10
RFC 3226 (Proposed Standard) Updated by RFC 4033, RFC 4034, RFC 4035 Errata	DNSSEC and IPv6 A6 aware server/ resolver message size requirements	2001-12
RFC 3266 (Proposed Standard) Obsoleted by RFC 4566 Errata	Support for IPv6 in Session Description Protocol (SDP)	2002-06
RFC 3306 (Proposed Standard) Updated by RFC 3956, RFC 4489	Unicast-Prefix-based IPv6 Multicast Addresses	2002-08
RFC 3307 (Proposed Standard)	Allocation Guidelines for IPv6 Multicast Addresses	2002-08

RFC 3314 (Informational) Errata	Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards	2002-09
RFC 3315 (Proposed Standard) Updated by RFC 4361, RFC 5494, RFC 6221 Errata	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	2003-07
RFC 3316 (Informational)	Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts	2003-04
RFC 3363 (Informational)	Representing Internet Protocol Version 6 (IPv6) Addresses in the Domain Name System (DNS)	2002-08
RFC 3364 (Informational) Errata	Tradeoffs in Domain Name System (DNS) Support for Internet Protocol Version 6 (IPv6)	2002-08
RFC 3484 (Proposed Standard)	Default Address Selection for Internet Protocol Version 6 (IPv6)	2003-02
RFC 3493 (Informational)	Basic Socket Interface Extensions for IPv6	2003-02
RFC 3513 (Proposed Standard) Obsoleted by RFC 4291	Internet Protocol Version 6 (IPv6) Addressing Architecture	2003-04
RFC 3531 (Informational)	A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block	2003-04
RFC 3542 (Informational) Errata	Advanced Sockets Application Program Interface (API) for IPv6	2003-05
RFC 3572 (Informational)	Internet Protocol Version 6 over MAPOS (Multiple Access Protocol Over SONET/SDH)	2003-07
RFC 3582 (Informational)	Goals for IPv6 Site-Multihoming Architectures	2003-08
RFC 3587 (Informational)	IPv6 Global Unicast Address Format	2003-08
RFC 3595 (Proposed Standard)	Textual Conventions for IPv6 Flow Label	2003-09
RFC 3627 (Informational) Errata	Use of /127 Prefix Length Between Routers Considered Harmful	2003-09
RFC 3633 (Proposed Standard) Errata	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) Version 6	2003-12
RFC 3646 (Proposed Standard)	DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	2003-12
RFC 3697 (Proposed Standard) RFC 3701 (Informational)	IPv6 Flow Label Specification 6bone (IPv6 Testing Address Allocation) Phaseout	2004-03 2004-03

(Continued)

RFC 3736 (Proposed Standard)	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6	2004-04
RFC 3750 (Informational)	Unmanaged Networks IPv6 Transition Scenarios	2004-04
RFC 3756 (Informational) Errata	IPv6 Neighbor Discovery (ND) Trust Models and Threats	2004-05
RFC 3769 (Informational)	Requirements for IPv6 Prefix Delegation	2004-06
RFC 3775 (Proposed Standard)	Mobility Support in IPv6	2004-06
RFC 3776 (Proposed Standard)	Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	2004-06
Updated by RFC 4877		
RFC 3810 (Proposed Standard) Updated by RFC 4604	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	2004-06
RFC 3831 (Proposed Standard) Obsoleted by RFC 4338	Transmission of IPv6 Packets over Fibre Channel	2004-07
RFC 3849 (Informational)	IPv6 Address Prefix Reserved for Documentation	2004-07
RFC 3879 (Proposed Standard)	Deprecating Site Local Addresses	2004-09
RFC 3898 (Proposed Standard)	Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	2004-10
RFC 3901 (Best Current Practice)	DNS IPv6 Transport Operational Guidelines	2004-09
RFC 3904 (Informational)	Evaluation of IPv6 Transition Mechanisms for Unmanaged Networks	2004-09
RFC 3919 (Informational)	Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS)	2004-10
RFC 3956 (Proposed Standard)	Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address	2004-11
RFC 4007 (Proposed Standard)	IPv6 Scoped Address Architecture	2005-03
RFC 4022 (Proposed Standard)	Management Information Base for the Transmission Control Protocol (TCP)	2005-03
RFC 4029 (Informational) Errata	Scenarios and Analysis for Introducing IPv6 into ISP Networks	2005-03
RFC 4038 (Informational)	Application Aspects of IPv6 Transition	2005-03
RFC 4057 (Informational) Errata	IPv6 Enterprise Network Scenarios	2005-06
RFC 4068 (Experimental) Obsoleted by RFC 5268	Fast Handovers for Mobile IPv6	2005-07
RFC 4074 (Informational)	Common Misbehavior Against DNS Queries for IPv6 Addresses	2005-05

RFC 4076 (Informational)	Renumbering Requirements for Stateless Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	2005-05
RFC 4087 (Proposed Standard)	IP Tunnel MIB	2005-06
RFC 4113 (Proposed Standard)	Management Information Base for the User Datagram Protocol (UDP)	2005-06
Errata		
RFC 4135 (Informational)	Goals of Detecting Network Attachment in IPv6	2005-08
RFC 4140 (Experimental)	Hierarchical Mobile IPv6 Mobility Management (HMIPv6)	2005-08
Obsoleted by RFC 5380		
Errata		
RFC 4147 (Informational)	Proposed Changes to the Format of the IANA IPv6 Registry	2005-08
Errata		
RFC 4177 (Informational)	Architectural Approaches to Multi-homing for IPv6	2005-09
RFC 4191 (Proposed Standard)	Default Router Preferences and More-Specific Routes	2005-11
Errata		
RFC 4192 (Informational)	Procedures for Renumbering an IPv6 Network without a Flag Day	2005-09
RFC 4193 (Proposed Standard)	Unique Local IPv6 Unicast Addresses	2005-10
RFC 4213 (Proposed Standard)	Basic Transition Mechanisms for IPv6 Hosts and Routers	2005-10
Errata		
RFC 4215 (Informational)	Analysis on IPv6 Transition in Third Generation Partnership Project (3GPP) Networks	2005-10
RFC 4218 (Informational)	Threats Relating to IPv6 Multihoming Solutions	2005-10
RFC 4219 (Informational)	Things Multihoming in IPv6 (MULTI6) Developers Should Think About	2005-10
RFC 4241 (Informational)	A Model of IPv6/IPv4 Dual Stack Internet Access Service	2005-12
Errata		
RFC 4242 (Proposed Standard)	Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	2005-11
RFC 4260 (Informational)	Mobile IPv6 Fast Handovers for 802.11 Networks	2005-11
RFC 4283 (Proposed Standard)	Mobile Node Identifier Option for Mobile IPv6 (MIPv6)	2005-11
Errata		
RFC 4285 (Informational)	Authentication Protocol for Mobile IPv6	2006-01
Errata		
RFC 4291 (Draft Standard)	IP Version 6 Addressing Architecture	2006-02
Updated by RFC 5952, RFC 6052		
Errata		
RFC 4292 (Proposed Standard)	IP Forwarding Table MIB	2006-04

(Continued)

RFC 4293 (Proposed Standard) Errata	Management Information Base for the Internet Protocol (IP)	2006-04
RFC 4294 (Informational) Updated by RFC 5095 Errata	IPv6 Node Requirements	2006-04
RFC 4295 (Proposed Standard) Errata	Mobile IPv6 Management Information Base	2006-04
RFC 4311 (Proposed Standard) RFC 4330 (Informational) Obsoleted by RFC 5905 Errata	IPv6 Host-to-Router Load Sharing Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI	2005-11 2006-01
RFC 4338 (Proposed Standard) Updated by RFC 5494	Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel	2006-01
RFC 4339 (Informational) Errata	IPv6 Host Configuration of DNS Server Information Approaches	2006-02
RFC 4380 (Proposed Standard) Updated by RFC 5991, RFC 6081 Errata	Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)	2006-02
RFC 4389 (Experimental) Errata	Neighbor Discovery Proxies (ND Proxy)	2006-04
RFC 4429 (Proposed Standard) Errata	Optimistic Duplicate Address Detection (DAD) for IPv6	2006-04
RFC 4443 (Draft Standard) Updated by RFC 4884 Errata	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	2006-03
RFC 4449 (Proposed Standard) Errata	Securing Mobile IPv6 Route Optimization Using a Static Shared Key	2006-06
RFC 4472 (Informational)	Operational Considerations and Issues with IPv6 DNS	2006-04
RFC 4477 (Informational)	Dynamic Host Configuration Protocol (DHCP): IPv4 and IPv6 Dual-Stack Issues	2006-05
RFC 4487 (Informational)	Mobile IPv6 and Firewalls: Problem Statement	2006-05
RFC 4489 (Proposed Standard)	A Method for Generating Link- Scoped IPv6 Multicast Addresses	2006-04
RFC 4554 (Informational)	Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks	2006-06
RFC 4580 (Proposed Standard)	Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Subscriber-ID Option	2006-06
RFC 4584 (Informational) Errata	Extension to Sockets API for Mobile IPv6	2006-07
RFC 4620 (Experimental) RFC 4640 (Informational) Errata	IPv6 Node Information Queries Problem Statement for bootstrapping Mobile IPv6 (MIPv6)	2006-08 2006-09

RFC 4649 (Proposed Standard)	Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option	2006-08
RFC 4651 (Informational)	A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization	2007-02
RFC 4659 (Proposed Standard)	BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN	2006-09
RFC 4668 (Proposed Standard) Errata	RADIUS Authentication Client MIB for IPv6	2006-08
RFC 4669 (Proposed Standard) Errata	RADIUS Authentication Server MIB for IPv6	2006-08
RFC 4670 (Informational) Errata	RADIUS Accounting Client MIB for IPv6	2006-08
RFC 4671 (Informational) Errata	RADIUS Accounting Server MIB for IPv6	2006-08
RFC 4692 (Informational)	Considerations on the IPv6 Host Density Metric	2006-10
RFC 4704 (Proposed Standard)	The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option	2006-10
RFC 4727 (Proposed Standard)	Experimental Values In IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers	2006-11
RFC 4773 (Informational)	Administration of the IANA Special Purpose IPv6 Address Block	2006-12
RFC 4779 (Informational) Errata	ISP IPv6 Deployment Scenarios in Broadband Access Networks	2007-01
RFC 4798 (Proposed Standard)	Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)	2007-02
RFC 4818 (Proposed Standard)	RADIUS Delegated-IPv6-Prefix Attribute	2007-04
RFC 4843 (Experimental)	An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID)	2007-04
RFC 4852 (Informational) Errata	IPv6 Enterprise Network Analysis— IP Layer 3 Focus	2007-04
RFC 4861 (Draft Standard) Updated by RFC 5942 Errata	Neighbor Discovery for IP Version 6 (IPv6)	2007-09
RFC 4862 (Draft Standard)	IPv6 Stateless Address Autoconfiguration	2007-09
RFC 4864 (Informational)	Local Network Protection for IPv6	2007-05
RFC 4866 (Proposed Standard) Errata	Enhanced Route Optimization for Mobile IPv6	2007-05

(Continued)

RFC 4877 (Proposed Standard) Errata	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture	2007-04
RFC 4882 (Informational)	IP Address Location Privacy and Mobile IPv6: Problem Statement	2007-05
RFC 4891 (Informational)	Using IPsec to Secure IPv6-in-IPv4 Tunnels	2007-05
RFC 4919 (Informational) Errata	IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals	2007-08
RFC 4941 (Draft Standard) Errata	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	2007-09
RFC 4942 (Informational)	IPv6 Transition/Co-existence Security Considerations	2007-09
RFC 4943 (Informational)	IPv6 Neighbor Discovery On-Link Assumption Considered Harmful	2007-09
RFC 4944 (Proposed Standard)	Transmission of IPv6 Packets over IEEE 802.15.4 Networks	2007-09
RFC 4968 (Informational) Errata	Analysis of IPv6 Link Models for 802.16 Based Networks	2007-08
RFC 5006 (Experimental) Obsoleted by RFC 6106	IPv6 Router Advertisement Option for DNS Configuration	2007-09
RFC 5014 (Informational)	IPv6 Socket API for Source Address Selection	2007-09
RFC 5026 (Proposed Standard)	Mobile IPv6 Bootstrapping in Split Scenario	2007-10
RFC 5072 (Draft Standard)	IP Version 6 over PPP	2007-09
RFC 5075 (Proposed Standard) Obsoleted by RFC 5175 Errata	IPv6 Router Advertisement Flags Option	2007-11
RFC 5094 (Proposed Standard)	Mobile IPv6 Vendor Specific Option	2007-12
RFC 5095 (Proposed Standard)	Deprecation of Type 0 Routing Headers in IPv6	2007-12
RFC 5096 (Proposed Standard)	Mobile IPv6 Experimental Messages	2007-12
RFC 5118 (Informational) Errata	Session Initiation Protocol (SIP) Torture Test Messages for Internet Protocol Version 6 (IPv6)	2008-02
RFC 5121 (Proposed Standard) Errata	Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks	2008-02
RFC 5149 (Informational)	Service Selection for Mobile IPv6	2008-02
RFC 5156 (Informational)	Special-Use IPv6 Addresses	2008-04
RFC 5157 (Informational)	IPv6 Implications for Network Scanning	2008-03
RFC 5172 (Proposed Standard)	Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol	2008-03

RFC 5175 (Proposed Standard)	IPv6 Router Advertisement Flags Option	2008-03
RFC 5180 (Informational)	IPv6 Benchmarking Methodology for Network Interconnect Devices	2008-05
Errata		
RFC 5181 (Informational)	IPv6 Deployment Scenarios in 802.16 Networks	2008-05
RFC 5213 (Proposed Standard)	Proxy Mobile IPv6	2008-08
RFC 5268 (Proposed Standard)	Mobile IPv6 Fast Handovers	2008-06
Obsoleted by RFC 5568		
RFC 5269 (Proposed Standard)	Distributing a Symmetric Fast Mobile IPv6 (FMIPv6) Handover Key Using SEcure Neighbor Discovery (SEND)	2008-06
RFC 5270 (Informational)	Mobile IPv6 Fast Handovers over IEEE 802.16e Networks	2008-06
RFC 5271 (Informational)	Mobile IPv6 Fast Handovers for 3G CDMA Networks	2008-06
RFC 5308 (Proposed Standard)	Routing IPv6 with IS-IS	2008-10
RFC 5340 (Proposed Standard)	OSPF for IPv6	2008-07
Errata		
RFC 5350 (Proposed Standard)	IANA Considerations for the IPv4 and IPv6 Router Alert Options	2008-09
RFC 5375 (Informational)	IPv6 Unicast Address Assignment Considerations	2008-12
RFC 5380 (Proposed Standard)	Hierarchical Mobile IPv6 (HMIPv6) Mobility Management	2008-10
RFC 5419 (Informational)	Why the Authentication Data Suboption is Needed for Mobile IPv6 (MIPv6)	2009-01
RFC 5447 (Proposed Standard)	Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction	2009-02
Errata		
RFC 5453 (Proposed Standard)	Reserved IPv6 Interface Identifiers	2009-02
RFC 5514 (Experimental)	IPv6 over Social Networks	2009-04
Errata		
RFC 5533 (Proposed Standard)	Shim6: Level 3 Multihoming Shim Protocol for IPv6	2009-06
RFC 5534 (Proposed Standard)	Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming	2009-06
RFC 5549 (Proposed Standard)	Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop	2009-05
RFC 5555 (Proposed Standard)	Mobile IPv6 Support for Dual Stack Hosts and Routers	2009-06
Errata		
RFC 5568 (Proposed Standard)	Mobile IPv6 Fast Handovers	2009-07
Errata		

(Continued)

RFC 5569 (Informational) Errata	IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)	2010-01
RFC 5570 (Informational) Errata	Common Architecture Label IPv6 Security Option (CALIPSO)	2009-07
RFC 5572 (Experimental) Errata	IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)	2010-02
RFC 5637 (Informational)	Authentication, Authorization, and Accounting (AAA) Goals for Mobile IPv6	2009-09
RFC 5701 (Proposed Standard)	IPv6 Address Specific BGP Extended Community Attribute	2009-11
RFC 5722 (Proposed Standard)	Handling of Overlapping IPv6 Fragments	2009-12
RFC 5726 (Experimental)	Mobile IPv6 Location Privacy Solutions	2010-02
RFC 5739 (Experimental) Errata	IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2)	2010-02
RFC 5757 (Informational)	Multicast Mobility in Mobile IP Version 6 (MIPv6): Problem Statement and Brief Survey	2010-02
RFC 5778 (Proposed Standard)	Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction	2010-02
RFC 5779 (Proposed Standard)	Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server	2010-02
RFC 5798 (Proposed Standard)	Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6	2010-03
RFC 5844 (Proposed Standard) RFC 5845 (Proposed Standard)	IPv4 Support for Proxy Mobile IPv6 Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6	2010-05 2010-06
RFC 5846 (Proposed Standard) RFC 5847 (Proposed Standard) Errata	Binding Revocation for IPv6 Mobility Heartbeat Mechanism for Proxy Mobile IPv6	2010-06 2010-06
RFC 5855 (Best Current Practice)	Nameservers for IPv4 and IPv6 Reverse Zones	2010-05
RFC 5871 (Proposed Standard)	IANA Allocation Guidelines for the IPv6 Routing Header	2010-05
RFC 5881 (Proposed Standard) Errata	Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)	2010-06
RFC 5902 (Informational)	IAB Thoughts on IPv6 Network Address Translation	2010-07
RFC 5942 (Proposed Standard)	IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes	2010-07

RFC 5949 (Proposed Standard)	Fast Handovers for Proxy Mobile IPv6	2010-09
RFC 5952 (Proposed Standard)	A Recommendation for IPv6 Address Text Representation	2010-08
Errata		
RFC 5954 (Proposed Standard)	Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261	2010-08
Errata		
RFC 5963 (Informational)	IPv6 Deployment in Internet Exchange Points (IXPs)	2010-08
RFC 5969 (Proposed Standard)	IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)—Protocol Specification	2010-08
RFC 6018 (Informational)	IPv4 and IPv6 Greynets	2010-09
RFC 6036 (Informational)	Emerging Service Provider Scenarios for IPv6 Deployment	2010-10
Errata		
RFC 6052 (Proposed Standard)	IPv6 Addressing of IPv4/IPv6 Translators	2010-10
RFC 6058 (Experimental)	Transient Binding for Proxy Mobile IPv6	2011-03
RFC 6059 (Proposed Standard)	Simple Procedures for Detecting Network Attachment in IPv6	2010-11
RFC 6085 (Proposed Standard)	Address Mapping of IPv6 Multicast Packets on Ethernet	2011-01
RFC 6089 (Proposed Standard)	Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support	2011-01
RFC 6092 (Informational)	Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service	2011-01
RFC 6097 (Informational)	Local Mobility Anchor (LMA) Discovery for Proxy Mobile IPv6	2011-02
RFC 6104 (Informational)	Rogue IPv6 Router Advertisement Problem Statement	2011-02
RFC 6105 (Informational)	IPv6 Router Advertisement Guard	2011-02
RFC 6106 (Proposed Standard)	IPv6 Router Advertisement Options for DNS Configuration	2010-11
RFC 6119 (Proposed Standard)	IPv6 Traffic Engineering in IS-IS	2011-02
RFC 6144 (Informational)	Framework for IPv4/IPv6 Translation	2011-04
RFC 6146 (Proposed Standard)	Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers	2011-04
RFC 6147 (Proposed Standard)	DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers	2011-04
RFC 6156 (Proposed Standard)	Traversal Using Relays around NAT (TURN) Extension for IPv6	2011-04
RFC 6157 (Proposed Standard)	IPv6 Transition in the Session Initiation Protocol (SIP)	2011-04

(Continued)

RFC 6164 (Proposed Standard)	Using 127-Bit IPv6 Prefixes on Inter-Router Links	2011-04
RFC 6177 (Best Current Practice)	IPv6 Address Assignment to End Sites	2011-03
RFC 6204 (Informational)	Basic Requirements for IPv6 Customer Edge Routers	2011-04
RFC 6214 (Informational)	Adaptation of RFC 1149 for IPv6	2011-04
RFC 6219 (Informational)	The China Education and Research Network (CERNET) IVI Translation Design and Deployment for the IPv4/IPv6 Coexistence and Transition	2011-05
RFC 6224 (Informational)	Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains	2011-04

3

An Overview of IP Multicast and Multicast Principles

This chapter provides a short overview of multicast principles and IP Multicast in the IPv4 environment to set the stage for the discussion on IPv6 multicast to follow. The reader interested in a more extensive treatment of this topic (from this author) may refer to reference [MIN200801]. Chapter 4 specifically looks at multicast in an IPv6 environment.

3.1 MULTICAST ENVIRONMENT

The concept of multicast is simple (as already noted in Chapter 2): *Multicast transmission implies “send this information/content to every member of this specific group”*—broadcast, by contrast, means “send this information/content to the entire universe of users in the address space”. Traditional TV distribution (over the air) followed a broadcast paradigm: everybody (in a region) gets the same programming. Cable TV relaxed this model somewhat where there would be, say half-a-dozen different subscription packages; however, all subscribers in the system to a given subscription package get the same programming. Clearly, for bandwidth-constrained networks (which, in the end, include most terrestrial networks), there is a strong (one could say, mandatory) desire not to send multiple copies of the same message for users in the same group at the origination point of the content, but rather, rather to send a single copy, which is then replicated as needed at the far end of the network, as close as possible to the intended group recipients.

There are classes of applications, including evolving NTTV applications in general and IBTV in particular, that require distribution of information to a defined (but possibly dynamic) set of users. In traditional IP networks, a packet is typically sent by a source to a single destination (unicast); alternatively, the packet can be sent to all devices on the network (broadcast). There are business and multimedia (entertainment) applications that require a multicast transmission mechanism to enable bandwidth-efficient communication between groups of devices where information is transmitted to a single multicast address and received by any device that wishes to obtain such

information. Examples of applications requiring one-to-many or many-to-many communications include, but are not limited to: digital entertainment video and audio distribution, multi-site corporate videoconferencing, broad-distribution financial data, cloud computing, stock quotes and news bulletins distribution, database replication, software distribution, and content caching (e.g., website content caching). In traditional IP networks, it is not possible to generate a *single transmission* of data when this data is destined for a (large) group of remote devices. IP Multicast, an extension to IP, is required to efficiently support these communications needs; as the term implies, IP Multicast has been developed to support efficient communication between a source and multiple remote destinations. See Figure 3.1 for a pictorial example. IP Multicast protocols and underlying technologies enable distribution of data, voice, and video streams to a large group of users, ranging from hundreds, to thousands, to millions of users. For example, social media networks can make effective use of this technology. IP Multicast technology enjoys intrinsic scalability that is critical for these types of applications. Multicast applications include, among others, datacasting (e.g., for distribution of real-time financial data), entertainment digital television over an IP network (commercial-grade IPTV), Internet radio, multipoint video conferencing, distance learning, streaming media applications, distributed video gaming, and corporate communications.

An important feature of IP Multicast is its ability to allow receiver-initiated attachment (joins) to information streams. Another important feature is the ability to support optimal pruning such that the distribution of the content is streamlined by pushing content replication as close to the receiver as possible. These features enable bandwidth-efficient use of underlying network infrastructure. As an example in the IPTV arena, with the current trend toward the delivery of high-definition TV (HDTV) signals, each requiring in the 10–12 Mbps range, and the consumers' desire for a large number of channels (200–300 being typical), there has to be an efficient mechanism of delivering a signal of 1–2 Gbps in aggregate to a large number of remote users. If a source had to deliver 1 Gbps of signal to, say, 1 million receivers by transmitting all of this bandwidth across the core network, it would require a petabit-per-second network fabric; this is not currently possible. On the other hand, if the source could send the 1 Gbps of traffic to (say) 50 remote distribution points (e.g., headends), each of which then makes use of a local distribution network to reach 20,000 subscribers, the core network only needs to support 50 Gbps; this is possible with proper design. For these kinds of reasons, IP Multicast is seen as a bandwidth-conserving technology that optimizes traffic management by simultaneously delivering a stream of information to a large population of recipients, including corporate enterprise users and residential customers.

IP Multicast, defined originally in Request for Comments (RFC) 988 (1986), and then further refined in RFC 1054 (1988), RFC 1112 (1989), RFC 2236 (1977), RFC 3376 (2002), and RFC 4604 (2006), among others, is the basic mechanism for these emerging NTTV applications, especially when large-scale deployment is contemplated. Given its long history, the technology is stable and relatively well understood, particularly for architecturally-simple (yet

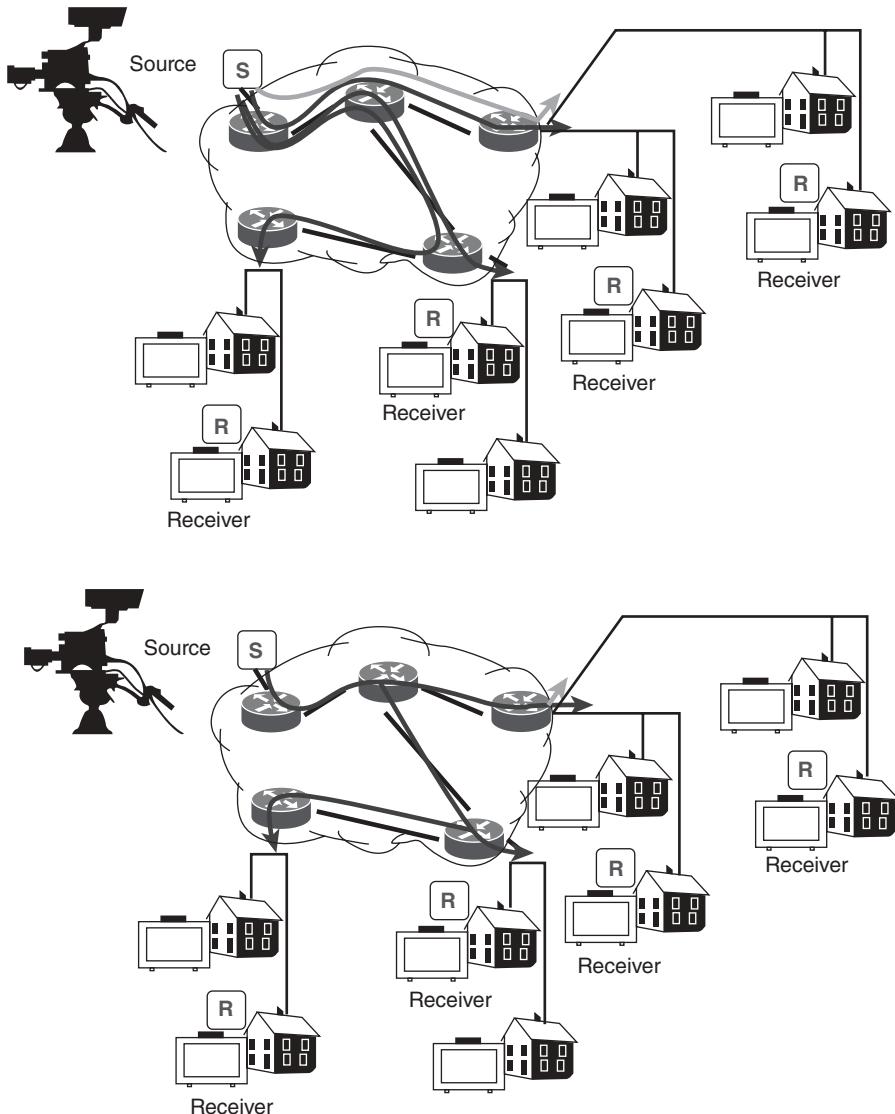


FIGURE 3.1 Bandwidth advantage of IP multicast. Top: Traditional IP. Bottom: IP Multicast. S = Source; R = Receiver.

large) networks. Enhancements to IP Multicast have actually occurred in the recent past, including the issuing of Internet Group Management Protocol, Version 3 (October 2002), the issuing of *Multicast Listener Discovery Version 2 for IPv6* (June 2004), the issuing of Source-Specific Multicast for IP (August 2006), and the publication of new considerations for Internet Group Management Protocol and Multicast Listener Discovery Snooping Switches (May 2006).

3.2 BASIC MULTICAST CONCEPTS AND PROTOCOLS

Multicast communication is based on the construct of a group of receivers (hosts) that have an interest in receiving a particular stream of information. There are no physical or geographical constraints, or boundaries to belong to a group, as long as the hosts have (broadband) network connectivity. The connectivity of the receivers can be heterogeneous in nature, in terms of bandwidth and connecting infrastructure (e.g., receivers connected over the Internet), or homogenous (e.g., IPTV users). Hosts that wish to receive data intended for a particular group join the group using a group management protocol: hosts/receivers must become explicit members of the group to receive the data stream, but such membership may be ephemeral and/or dynamic. Groups of IP hosts that have joined the group and wish to receive traffic sent to this specific group are identified by multicast addresses, as discussed below. Multicast transmission involves several mechanisms, as we briefly discuss next.

- *Addressing for Payload:* To communicate with a group of receivers (hosts) one needs a Layer 3 address; also, there must be a mechanism of mapping the Layer 3 address onto Layer 2 multicast addresses of the underlying local area network (LAN); Ethernet multicast addresses have a hex “01” in the first byte of the 6-octet destination address. The Internet Assigned Numbers Authority (IANA) manages the assignment of IP addresses at Layer 3, and it has assigned the (original) Class D address space to be used for IP Multicast. A Class D address consists of 1110 as the higher order bits in the first octet, followed by a 28-bit group address. A 1110-0000 address in the first byte starts at 224 in the dotted decimal notation; a typical address might be 224.10.10.1, and so on. All IP Multicast-group addresses belong to the range 224.0.0.0–239.255.255.255. The mapping of IP Multicast addresses to Ethernet addresses takes the lower 23 bits of the Class D address and maps them into a block of Ethernet addresses that have been allocated for multicast. Addresses are discussed in Section 3.3.
- *Dynamic Host Registration:* There must be a mechanism that informs the network that a host (receiver) is a member of a particular group (otherwise, the network would have to flood rather than multicast the transmissions for each group.) For IP networks, the Internet Group Multicast Protocol (IGMP) serves this purpose.
- *Multicast Payload Forwarding:* Typical IP multicast applications make use of User Datagram Protocol (UDP) at the Transport Layer and IP at the Network Layer. UDP is a “best effort delivery” protocol with no guarantee of delivery; it also lacks the congestion management mechanism (such as those utilized in Transmission Control Protocol [TCP]). Real-time applications such as commercial live video distribution do not (and cannot) make use of a retransmission mechanism (such as the one utilized in TCP). In some cases, portions of the network may be simplex (such as a satellite link), practically precluding end-to-end retransmission.

Hence, the risk exists for audio and video broadcasts to suffer content degradation due to packet loss. To minimize lost packets, one must provision adequate bandwidth and/or keep the distribution networks simple and with as few hops as possible. IP QoS (*difftserv*), the Real-Time Transport Protocol (RTP), and 802.1p at Layer 2 are often utilized to manage QoS. (To minimize in-packet bit corruption Forward Error Correction (FEC) mechanisms may be used.)

- *Multicast Routing:* A multicast network requires a mechanism to build distribution trees that define a unique forwarding path between the subnet of the content source and each subnet containing members of the multicast group, specifically, receivers. A principle utilized in the construction of distribution trees is to guarantee that at most, one copy of each packet is forwarded on each branch of the tree. This is implemented by ascertaining that there is sufficient real-time topological information at the multicast router of the source host for constructing a spanning tree rooted at said multicast router (or other appropriate router) and providing connectivity to the local multicast routers of each receiving host. A multicast router forwards multicast packets to two types of devices: downstream dependent routers and receiver (hosts) that are members of a particular multicast group.

A number of multicast-related protocols have emerged in recent years (see Table 3.1). Multicast routing protocols belong to one of two categories: Dense Mode (DM) protocols and Sparse Mode (SM) protocols.

- DM protocols are designed on the assumption that the majority of routers in the network will need to distribute multicast traffic for each multicast group. DM protocols build distribution trees by initially flooding the

TABLE 3.1 Basic Multicast Protocols (IPv4) (Partial List)

Protocol	Purpose
Internet Group Management Protocol (IGMP)	Client (receiver, set-top box [STB], PC) to Router signaling
Protocol Independent Multicast (PIM) Distance Vector Multicast Routing Protocol (DVMRP) Core Based Tree (CBT) Multicast OSPF (MOSPF)	Router to Router topology (multicast route) management
Multiprotocol BGP (MBGP) Multicast Source Discovery Protocol (MSDP)	Large-Scale Router to Router routing functionality
Multicast Address Dynamic Client Allocation Protocol (MADCAP) Multicast Address Set Claim Protocol (MASC)	Multicast Address Allocation

entire network and then pruning out the (presumably small number of) paths without active receivers. DM protocols are used in LAN environments, where bandwidth considerations are less important, but can also be used in wide area networks (WANs) in special cases (e.g., where the backbone is a one-hop broadcast medium, such as a satellite beam with wide geographic illumination, e.g., in some IPTV applications).

- SM protocols are designed on the assumption that only few routers in the network will need to distribute multicast traffic for each multicast group. SM protocols start out with an empty distribution tree and add drop-off branches only upon explicit requests from receivers to join the distribution. SM protocols are generally used in WAN environments, where bandwidth considerations are important.

For IP Multicast, there are several multicast routing protocols that can be employed to acquire real-time topological and membership information for active groups. Routing protocols that may be utilized include: the Protocol-Independent Multicast (PIM), the Distance Vector Multicast Routing Protocol (DVMRP), the Multicast extensions to OSPF (MOSPF), and Core-Based Trees (CBT). PIM is currently the most widely used protocol. Multicast routing protocols build distribution trees by examining routing forwarding table that contains unicast reachability information. PIM and CBT use the unicast forwarding table of the router, while other protocols use their specific unicast reachability routing tables.

PIM Version 2 (PIMv2) is a protocol that provides intradomain multicast forwarding for all underlying unicast routing protocols (e.g., Open Shortest Path First [OSPF] or Border Gateway Protocol [BGP]), independent from the intrinsic unicast protocol. Two modes exist: PIM Sparse Mode (PIM SM) and PIM Dense Mode (PIM DM):

- PIM Dense Mode (defined in RFC 3973, January 2005) is a multicast routing protocol that uses the underlying unicast routing information base to flood multicast datagrams to all multicast routers. Prune messages are used to prevent future messages from propagating to routers without group membership information [ADA200501]. PIM-DM attempts to send multicast data to all potential receivers (flooding) and relies upon their self-pruning (removal from group) to achieve distribution. In PIM-DM, multicast traffic is initially flooded to all segments of the network. Routers that have no downstream neighbors or directly connected receivers prune back the unwanted traffic. PIM-DM assumes most receivers (hosts, PCs, TV viewers, and cellular phone handsets) wish to receive the multicast; therefore, the protocol forwards the multicast datagrams everywhere, and then routers prune the distribution tree where it is not needed. PIM is now being utilized for IPTV applications; typically, Dense Mode is used in the backbone; however, Sparse Mode could also be utilized in some applications or portions of the overall network.

- In Sparse Mode PIM, only network segments with active receivers that have explicitly requested multicast data are forwarded the traffic. PIM SM relies on an explicit joining request before attempting to send multicast data to receivers of a multicast group. In a PIM-SM network, sources must send their traffic to a rendezvous point (RP); this traffic is in turn forwarded to receivers on a shared distribution tree. Sparse Mode works by routers sending PIM Join messages, to start the multicast feed being sent across links. The assumption in Sparse Mode is that relatively few users need the multicast information; therefore, PIM-SM starts with no flooding of multicast. In short order, router-to-router PIM Join messages cause the multicast streams to be forwarded across links to where it is needed. This is the current standard for ISPs supporting Internet multicast [WEL200101].

An RP (described in RFC 2362) acts as the meeting place for sources and receivers of multicast data. A RP is required only in networks running Protocol Independent Multicast Sparse Mode, and it is needed only to start new sessions with sources and receivers. In a PIM-SM network, sources send their traffic to the RP; this traffic is in turn forwarded to receivers downstream on a shared distribution tree. A designated router (DR) is the router on a subnet that is selected to control multicast routes for the members on its directly attached subnet. The receiver sends an IGMP Join message (see below) to this designated multicast router.¹ IP multicast traffic transmitted from the multicast source is distributed over the tree, via the designated router, to the receiver's subnet. When the designated router of the receiver learns about the source, it sends a PIM Join message directly to the source's router, creating a source-based distribution tree, from the source to the receiver. This source tree does not include the RP unless the RP is located within the shortest path between the source and receiver.

IGMP (Versions 1, 2, and 3) is the protocol used by IPv4 hosts to communicate multicast group membership information to neighboring multicast routers. IGMP is used to dynamically register individual hosts/receivers on a particular local subnet (e.g., LAN) to a multicast group. IGMP Version 1 defined the basic mechanism; it supports a membership query (MQ) message and a membership report (MR) message. Most implementations at press time employed IGMP Version 2; Version 2 adds Leave Group (LG) messages. Version 3 adds source awareness, allowing the inclusion or exclusion of sources. IGMP allows group membership lists to be dynamically maintained. The host (user) sends an IGMP “report,” or join, to the router to be included in the group. Periodically, the router sends a “query” to learn which hosts (users) are still part of a group. If a host wishes to continue its group membership, it

¹This is different from the router-to-router PIM Join message just described; this message is from receiver to its gateway multicast router.

responds to the query with a “report.” If the host does not send a “report,” the router prunes the group list to delete this host; this eliminates unnecessary network transmissions. With IGMPv2, a host may send a “leave group” message to alert the router that it is no longer participating in a multicast group; this allows the router to prune the group list to delete this host before the next query is scheduled, thereby minimizing the time period during which unneeded transmissions are forwarded to the network.

Multicast Listener Discovery Protocol Version 2 (MLDv2), described in RFC 3810, June 2004, is the protocol used in IPv6 to enable a host (e.g., a set-top box) to inform its neighboring routers of its desire to receive IPv6 multicast transmissions; MLDv2 is covered in Chapter 4.

Other basic multicast protocols/mechanisms include the following:

- Internet Group Management Protocol Snooping is a method by which a switch can constrain Multicast packets to only those ports that have requested the stream.
- STUB multicast routing is a mechanism that allows IGMP messages to be forwarded through a non-PIM enabled router toward a PIM-enabled router.
- PIM Source-Specific Multicast (SSM) is a form of multicast where a receiver must specify both the network-layer address of the source and the multicast destination address in order to receive the multicast information. IGMPv3 is used to support SSM, as discussed in Section 3.4.
- Multicast Source Discovery Protocol (MSDP) is a protocol that allows multiple PIM Sparse Mode domains to share information about active sources. The protocol announces active sources to MSDP peers.
- Multiprotocol Border Gateway Protocol (MP-BGP) is a protocol that defines multiprotocol extensions to BGP, the unicast interdomain protocol that supports multicast-specific routing information. MP-BGP augments BGP to enable multicast routing policy and connect multicast topologies within and between BGP autonomous systems. It carries multiple instances of routes for unicast routing, as well as multicast routing.
- Pragmatic General Multicast (PGM) is a reliable multicast transport protocol for applications that require ordered, duplicate-free multicast data delivery. The protocol guarantees that a receiver in a multicast group receives all data packets from direct transmissions or via retransmissions of lost packets. PGM can detect unrecoverable data packet loss.
- Router-Port Group Management Protocol (RGMP) is a protocol that constrains IP multicast on switches that have only routers attached.

Figures 3.2 and 3.3 illustrate where some of these concepts and protocols apply in the context of a typical multicast network.

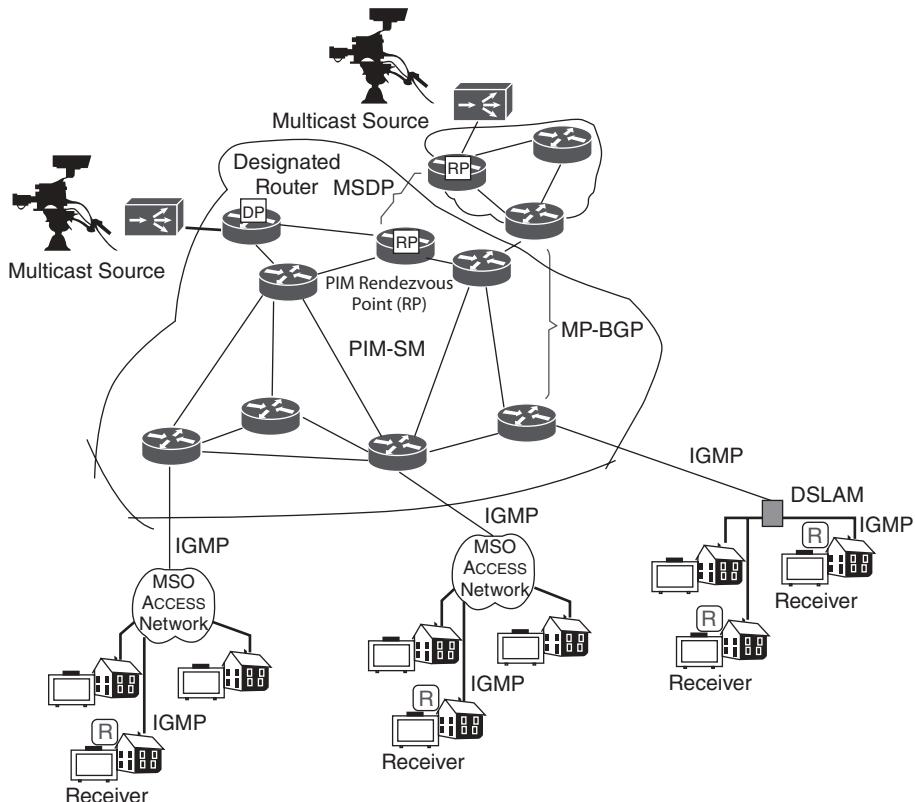


FIGURE 3.2 Typical IP multicast network as applied to video distribution.

3.3 IP MULTICAST ADDRESSES

Multicast addresses define, in effect, the group of hosts that participate in the shared reception of the content intended for that group. One can think of this by analogy with a local TV station or local radio station. When a user “tunes” the TV to, say, Channel 2 (WCBS TV in New York City), the user joins the set of viewers (receivers) that receive the content produced and distributed by WCBS TV. When a user then changes channel and “tunes” the TV to, say, Channel 4 (WNBC TV in New York City), the user joins the set of viewers (receivers) that receive the content produced and distributed by WNBC TV. In IP Multicast, the analogous activity is accomplished by using IP Multicast addresses. The various content providers stream IP packets that have their own source address and a multicast address as the destination address. For example, WCBS TV in New York City could generate programming with the address 239.10.10.1; WNBC TV in New York City could generate programming with the address 239.10.10.2. And so on.

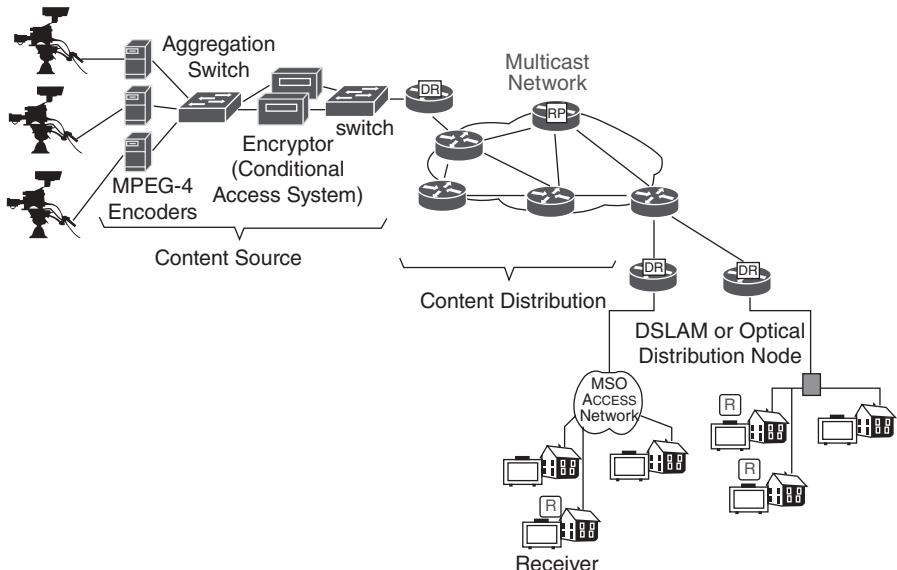
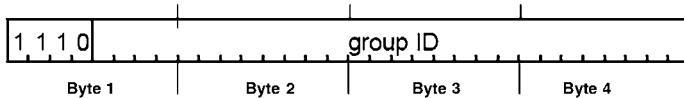


FIGURE 3.3 IPTV application of IP multicast showing some content aggregation elements.

IP Multicast Addresses

Class D IP addresses



in "dotted decimal" notation: 224.0.0.0 – 239.255.255.255

Administrative categories:

- (1) “well-known” multicast addresses (assigned by IANA)
- (2) “transient” multicast addresses, assigned and reclaimed dynamically by organization

FIGURE 3.4 IP multicast address.

RFC 1112 specifies the extensions required of a host implementation of IP to support multicasting [DEE198901]. The Internet Assigned Numbers Authority (IANA) controls the assignment of IP Multicast Addresses. IANA has allocated what has been known as the Class D address space to be utilized for IP Multicast. IP Multicast-group addresses are in the range 224.0.0.0 through 239.255.255.255. See Figure 3.4. For each multicast address, there exists a set

of zero or more hosts (receivers) that look for packets transmitted to that address. This set of devices is called a host group. A source (host) that sends packets to a specific group does not need to be a member of the group, and the host typically does not even know the current members in the group [PAR200601]. The source address for multicast IP packets is always the unicast source address.

There are two types of host groups [PAR200601]:

- *Permanent Host Groups:* Applications that are part of this type of group have an IP address permanently assigned by the IANA. A permanent group continues to exist even if it has no members. Membership in this type of host group is not permanent: a host (receiver) can join or leave the group as desired. An application can use DNS to obtain the IP address assigned to a permanent host group using the domain mcast.net.
- *Transient Host Groups:* Any group that is not permanent as just described is by definition transient. The group is available for dynamic assignment as needed. Transient groups cease to exist when the number of members drops to zero.

Some IP multicast addresses have been reserved for specific functions: addresses in the 224.0.0.0 through 224.0.0.255 are reserved to be used by network protocols on a local network segment. Network protocols make use of these addresses for automatic router discovery and to communicate routing information (e.g., OSPF uses 224.0.0.5 and 224.0.0.6 to exchange link state information). IP packets with these addresses are not forwarded by a router; they remain local on a particular LAN segment (they have a time-to-live (TTL) parameter set to 1; even if the TTL is different from 1, they still are not forwarded by the router). These addresses are also known as Link Local Addresses.

The statically assigned link-local scope is 224.0.0.0/24. The list of IP addresses assigned to permanent host groups is included in RFC 3232 [RAY200201]. Some well-known Link-Local Addresses include the following:

- 224.0.0.1: All Systems on this subnet
- 224.0.0.2: All Routers on this subnet
- 224.0.0.4: DVMRP Routers
- 224.0.0.5: OSPF Routers
- 224.0.0.6: OSPF Designated Routers
- 224.0.0.12: DHCP Server/Relay Agent
- 224.0.0.13 All PIM Routers
- 224.0.0.22 All IGMPv3-capable multicast routers
- 224.0.0.102 HSRP
- 224.0.0.253 Teredo

The range of addresses from 224.0.1.0 through 238.255.255.255 are known as Globally Scoped Addresses. These addresses are used to transmit multicast information across the Internet and between organizations. Some of these addresses have been reserved for specific uses such as Network Time Protocol (NTP) (224.0.1.1).

Examples of as Globally Scoped Addresses ranges include:

- 224.1.0.0-224.1.255.255 ST Multicast Groups
- 224.2.0.0-224.2.127.253 Multimedia Conference Calls
- 224.2.127.254 SAPv1 Announcements
- 224.2.128.0-224.2.255.255 SAP Dynamic Assignments
- 224.252.0.0-224.255.255.255 DIS transient groups
- 232.0.0.0-232.255.255.255 VMTCP transient groups

At a more granular level, examples of Globally Scoped Addresses include:

- 224.0.12.000-224.0.12.063 Microsoft and MSNBC
- 224.0.13.000-224.0.13.255 WorldCom Broadcast Services
- 224.0.15.000-224.0.15.255 Agilent Technologies
- 224.0.16.000-224.0.16.255 XingNet
- 224.0.17.000-224.0.17.031 Mercantile & Commodity Exchange
- 224.0.18.000-224.0.18.255 Dow Jones
- 224.0.19.000-224.0.19.063 Walt Disney Company
- 224.0.253.000-224.0.253.255 KPN Broadcast Services
- 224.0.254.000-224.0.254.255 Intelsat IPTV

Some of these Globally Scoped Addresses have been assigned recently, for example (partial list):

- 224.0.25.0-224.0.28.255 CME Market Data: assigned March 22, 2007
- 224.0.254.000-224.0.254.255 Intelsat IPTV: assigned March 31, 2006
- 224.0.23.52 Amex Market Data: assigned August 11, 2006
- London Stock Exchange: assigned March 31, 2006

Note that the range of addresses from 239.0.0.0 through 239.255.255.255 are called Limited Scope Addresses (also known as Administratively Scoped Addresses). RFC 2365 defines these addresses to be limited to a local group or organization [MEY199801]. Routers are required to be configured with packet filters to prevent multicast traffic in this address range from flowing outside of an Autonomous System (AS); these are similar to the 10.x.x.x or 192.x.x.x ranges for traditional intranets. Within an AS the Limited Scope address space can be subdivided so that local multicast boundaries can be defined. This also allow for address reuse between these subdomains.

3.4 INTERNET GROUP MANAGEMENT PROTOCOL (IGMP)

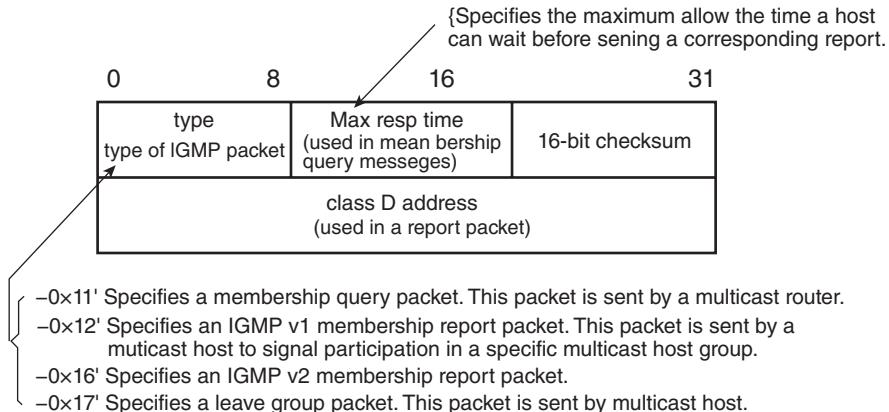
This section covers the important multicast topic of dynamic host registration. In a multicast environment, group membership information is exchanged between a receiver (host) and the nearest multicast router. IGMP is used by host receivers to join or leave a multicast host group. Hosts establish group memberships by sending IGMP messages to their local multicast router. Multicast-enabled routers monitor for IGMP messages to maintain forwarding tables for the various interfaces on the router. Multicast-enabled routers periodically send out queries to discover which groups are active or inactive on a given subnet.

IGMP is used by IPv4-based receivers to report their IP multicast group memberships to neighboring multicast routers: it defines the signaling communication occurring between receiving hosts and their local multicast router. IGMP Version 2, now widely deployed, is defined by RFC 2236 (November 1997). The latest version at press time was Version 3, defined in RFC 3376 (IGMPv3, October 2002); RFC 3376 subsumes and obsoletes RFC 2236 (IGMPv2). IGMPv3 supports receivers that explicitly signal sources from which they wish to receive traffic. Specifically, IGMPv3 is employed by hosts to signal channel access in SSM. For SSM to work, IGMPv3 must be available in last hop routers and receiver host operating system network stacks, and be used by the applications running on those receiver hosts. Benefits of SSM include optimized access bandwidth utilization (receivers are able to request traffic only from explicitly known sources, relieving the typically congested access link from unnecessary traffic) and improved security (eliminates denial of service attacks from unknown sources). Note that all routers on a subnet must be configured for the same version of IGMP.

In Version 1 (defined in RFC 1112), there are two types of IGMP messages: MQ and MR. In a Version 1 implementation, receivers interested in joining a particular multicast group generate MRs that contain references to that multicast address (group). The router in turn builds a forwarding table entry and routinely forwards the multicast packets to the interface(s) that support the subnet where registered hosts reside. The router periodically sends out an IGMP MQ to verify that at least one host on the subnet is still interested in receiving traffic directed to that group. When there is no reply to three consecutive IGMP MQs, the router times-out the group and stop forwarding traffic directed toward that group.

The basic IGMP Version 2 (defined in RFC 2236) message types are: MQ, MR,² and leave group (LG). MQs can be generic (general MQ) or specific (group-specific MQ). In the discussion below, the querier is the sender of a Query message—the querier is a multicast router. IGMP Version 2 works in a similar fashion as Version 1 but with the addition of the LG message. With

²There is Version 1 Membership Report and Version 2 Membership Report.

**FIGURE 3.5** IGMP V2 message format.

the LG mechanism, receivers/hosts can explicitly communicate their intention to depart from the group to the local multicast router. The use of LGs reduces the traffic on subnets, especially if there is a lot of join/change/leave activity. Upon receiving an LG message, the router issues a group-specific query to determine if there are any remaining hosts on that subnet that are in need of receiving the traffic. If there are no replies, the router times out the group and stops forwarding the traffic.

The IGMP messages for IGMP Version 2 are shown in Figure 3.5. The message is comprised of an 8-octet structure. During transmission, IGMP messages are encapsulated in IP datagrams; to indicate that an IGMP packet is being carried, the IP header contains a protocol number of 2. An IGMP V2 PDU consists of a 20-byte IP header and 8 bytes of IGMP.

The *Type* field identifies the type of IGMP packet.

- An MQ packet has a Type of 0 × “11.” This message is sent by a multicast-enabled router. A MQ packet is sent by a multicast router either to learn which groups have members on an attached network (also known as General Query), or to learn if a particular group has any members on an attached network (also known as Group-Specific Query).
- An IGMPv1 MR packet has a Type of 0 × “12.” This message is sent by a multicast receiver (host) to indicate a request for participation in a specific multicast receiver (host) group.
- An IGMPv2 MR packet has a Type of 0 × “16”.
- A leave group, LG, packet has a Type of 0 × “17.” This message is sent by a multicast receiver (host) to indicate a request for disassociation from a group.

The *Max response time* field is employed in MQ messages, and it specifies the maximum time a host can wait before sending a corresponding report. This parameter allows routers to optimize the leave latency, the time between the last receiver (host) leaves a group and the time the routing protocol is notified that there are no more active members in that group. The Maximum response time is measured in tenths of a second.

The *Checksum* field contains a 16-bit checksum for the message. The Checksum is the 16-bit one's complement of the one's complement sum of the whole IGMP message (the entire IP payload). For computing the checksum, the Checksum field is set to zero.

The *Class D Addreqss* field contains a valid multicast group address and is used in a report packet.

As noted above, in the recent past, the IGMPv2 message format has been extended in IGMP Version 3 (IGMPv3). Version 3 allows receivers to subscribe to or exclude a specific *set* of sources within a multicast group, rather than just an individual source (this is called, as already discussed, Source Specific Multicast.) With this feature, IGMPv3 adds support for “source filtering,” that is, the ability for a system to report interest in receiving packets sent to a particular multicast address *only* from specific source addresses, or from *all but* specific source addresses. That information may be used by multicast routing protocols to avoid delivering multicast packets from specific sources to (sub)networks where there are no interested receivers [CAI200201].

“Source filtering,” enables a multicast receiver (host) to signal to a multicast-enabled router that groups the host wants to receive multicast traffic from (i.e., signal membership to a multicast host group), and from which source(s) this traffic is expected. This membership information allows a multicast-enabled router to forward traffic only from those sources from which receivers requested the traffic. “Source Filtering” supports an atomic leave/join; this helps recovery from lost “leave” messages and simplifies some of the error recovery scenarios. This capability also halves the message traffic, as now only a single message is needed to “leave” one stream and “join” another. Receivers signal membership to a multicast host group in the following two modes [CIS200701]:

- *INCLUDE Mode:* In this mode, the receiver announces membership to a host group and provides a list of IP addresses (the INCLUDE list) from which it wishes to receive traffic.
- *EXCLUDE Mode:* In this mode, the receiver announces membership to a host group and provides a list of IP addresses (the EXCLUDE list) from which it does not wish to receive traffic. This indicates that the host wants to receive traffic only from other sources whose IP addresses are not listed in the EXCLUDE list.

To support this capability, the MQ packet (Type of $0 \times "11"$) has been changed; in addition, a new packet type of $0 \times "22"$ has been added. Note that all

IGMPv3 implementations must still support packet types $0 \times "12"$, $0 \times "16"$, and $0 \times "17"$.

In IGMPv3, there are three variants of the Query message:

1. A “General Query” is sent by a multicast router to learn the complete multicast reception state of the neighboring interfaces (i.e., the interfaces attached to the network on which the Query is transmitted). In a General Query, both the Group Address field and the Number of Sources (N) field are zero (see below).
2. A “Group-Specific Query” is sent by a multicast router to learn the reception state, with respect to a *single* multicast address, of the neighboring interfaces. In a Group-Specific Query, the Group Address field contains the multicast address of interest, and the Number of Sources (N) field contains zero (see below).
3. A “Group-and-Source-Specific Query” is sent by a multicast router to learn if any neighboring interface desires reception of packets sent to a specified multicast address, from any of a specified list of sources. In a Group-and-Source-Specific Query, the Group Address field contains the multicast address of interest, and the Source Address fields contain the source address(es) of interest.

The IGMPv3 MQ packet $0 \times "11"$ message includes a field that specifies the number of sources being covered by the request along with a list of Class D addresses. See Figure 3.6.

The *Type* field remains unchanged.

The *Max response code* field is has been modified and distinguishes between a maximum response *code* and a maximum response *time*. The Max Resp Code field specifies the maximum time allowed before sending a responding report. The actual time allowed, called the Max Resp Time, is represented in units of

0		8		16		31					
0×11 [Type]		Max. Resp. Code		Checksum							
Group Address											
Resv	S	QRV	QQIC		Number of Sources						
Source Address [1]											
Source Address [2]											
⋮											
Source Address [N]											

FIGURE 3.6 IGMPv3 membership query message.

1/10 second and is derived from the Max Resp Code. Here is how that is done: when the maximum response code is less than 128, the value of the maximum response time equates to the value of the maximum response code. When the maximum response code is greater than 128, the maximum response time is calculated as follows:

If $\text{Max Resp Code} \geq 128$, Max Resp Code represents a floating-point value where the coding is:

0	1	2	3	4	5	6	7
+-----+-----+							
1	exp		mant				
+-----+-----+							

mant = mantissa

exp = exponent

$$\text{Max Resp Time} = (\text{mant} | 0 \times 10) \ll (\text{exp} + 3)$$

($|$ is the Boolean OR function; e.g., $0010 | 10000 = 10010$); (note that the *exp* calculation uses a binary representation of decimal 3, namely 11). “ \ll ” is the bitwise left shift operator. It defines the shift the bits of a number to the left by a certain number of places and zero is used for filling.

For example: $2147483646 \ll 1$ leads to the following: the 32-bit binary representation of 2147483646 is 100000000000000000000000000010. If its leftmost bit is removed and a zero is filled at the rightmost position, the result is 0000000000000000000000000000100, which is equal to 4 in decimal representation. Consider the example of $18 \ll 6$: the 11-bit binary representation is 00000010010. If its leftmost six bits are removed and a six zeros are filled at the rightmost positions, the result is 1001000000 or decimal 1152. Now we are ready to apply the formula.

As an example, assume that the value of maximum response code is decimal 178. The bit string representation of this is 10110010. From this, the fields of the maximum response code are:

- Byte 0 = 1
- *exp* = 011
- *mant* = 0010

The subsequent calculations are:

- $(\text{mant} | 0 \times 10) = (0010 | 10000) = 10010$
- $\text{exp} + 11 = 011 + 11 = 110$ (basically, $3 + 3 = 6$ in base 10, or 110 in base 2)

Now,

- $10010 \ll 110 = 10010 \ll 110 = 1001000000$
- Binary 1001000000 = Decimal 1152

Therefore, when the maximum response code is decimal 178, the maximum response time is 1152 tenths of a second.

Small values of Max Resp Time allow IGMPv3 routers to tune the “leave latency” (the time between the moment the last host leaves a group and the moment the routing protocol is notified that there are no more members). Larger values allow the tuning of the burstiness of IGMP traffic on a network.

The *Checksum* field contains a 16-bit checksum, and remains unchanged from Version 2.

The *Group Address* field contains the Class D address, and is the same as Version 2. The Group Address field is set to zero when sending a General Query, and set to the IP multicast address being queried when sending a Group-Specific Query or Group-and-Source-Specific Query.

The *Resv* field is reserved, and is set to zero on transmission and is ignored on reception.

The *S Flag* field is used as follows: When set to 1, this field indicates that any receiving multicast routers should suppress the normal timer updates normally performed upon receiving a query.

The *QRV* field (Querier’s Robustness Variable) carries a parameter that is used in tuning timer values for expected packet loss. The higher the value of the QRV, the more tolerant the environment is for lost packets. One needs to keep in mind, however, that increasing the QRV also increases the delay in detecting a problem. If nonzero, the QRV field contains the (Robustness Variable) value used by the querier (i.e., the sender of the Query, a multicast router). If the querier’s (Robustness Variable) exceeds 7, the maximum value of the QRV field, the QRV is set to zero. Routers adopt the QRV value from the most recently received Query as their own (Robustness Variable) value, unless that most recently received QRV was zero, in which case the receivers use the default (Robustness Variable) value.

The *QQIC* field (Querier’s Query Interval Code) carries a value specifying the query interval, in seconds, used by the originator of this query. In other words, QQIC specifies the (Query Interval) used by the querier. The actual interval, called the Querier’s Query Interval (QQI), is represented in units of seconds and is derived from the Querier’s Query Interval Code. Multicast routers that are not the current querier adopt the QQI value from the most recently received Query as their own (Query Interval) value, unless that most recently received QQI was zero, in which case the receiving routers use the default (Query Interval) value. The calculations to convert this code into the actual interval time are the same used for the maximum response code discussed above.

Number of Sources field indicates how many source addresses are contained within the Query message. This number is zero in a General Query or a Group-Specific Query, and non-zero in a Group-and-Source-Specific Query. This number is limited by the Maximum Transfer Unit (MTU) of the network over which the Query is transmitted. For example, on an Ethernet with an MTU of 1500 octets, the IP header, including the Router Alert option, consumes 24

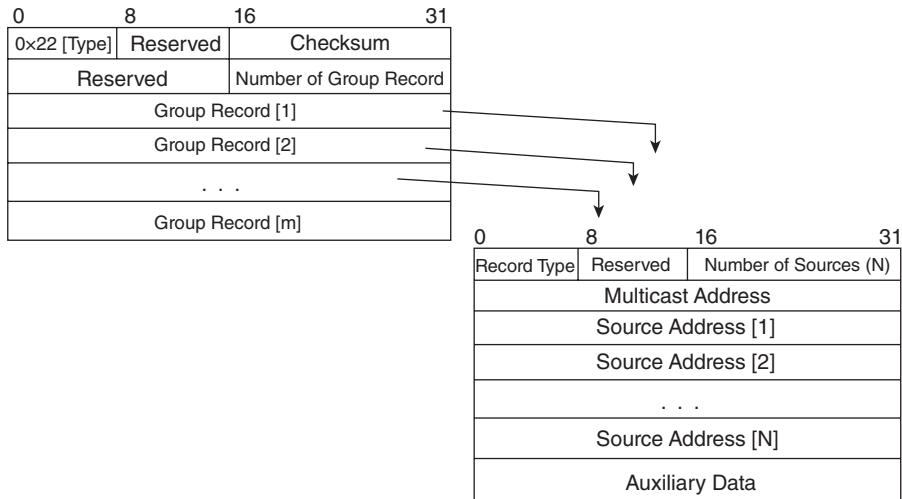


FIGURE 3.7 Membership report message.

octets, and the IGMP fields up to including the Number of Sources (N) field consume 12 octets, leaving 1464 octets for source addresses; this limits the number of source addresses to 366 ($1464/4$).

Source Addresses: This list of fields identifies N IP unicast addresses, where the value N corresponds to the Number of Sources field.

As noted earlier, IGMPv3 adds a new type of $0 \times "22"$ to support the IGMPv3 MR; see Figure 3.7 for the format of v3 Reports. MRs are sent by IP systems to report (to neighboring routers) the current multicast reception state, or changes in the multicast reception state, of their interfaces. Notice how each Group Record is assembled in the MR message.

The *Record Type* field indicates whether the group record type is a *current-state*, *filter-mode-change*, or *source-list-change* record. *Current-state* records (MODE_IS_INCLUDE, MODE_IS_EXCLUDE) are records sent by a system in response to a query received on an interface and report the current reception of that interface. *Filter-mode-change* records (CHANGE_TO_INCLUDE_MODE, CHANGE_TO_EXCLUDE_MODE) are records sent by a system when an interface's state changes for a particular multicast address. *Source-list-change* records (ALLOW_NEW_SOURCES, BLOCK_OLD_SOURCES) are records sent by a system when an interface wishes to alter the list of source addresses without altering its state.

IGMPv3 Reports are sent with an IP destination address of 224.0.0.22, to which all IGMPv3-capable multicast routers listen. A system that is operating in Version 1 or Version 2 compatibility modes sends Version 1 or Version 2 Reports to the multicast group specified in the Group Address field of the Report. In addition, a system must accept and process any Version 1 or Version

2 Report whose IP Destination Address field contains *any* of the addresses (unicast or multicast) assigned to the interface on which the Report arrives [CAI200201].

Note: Because of its higher complexity, IGMPv3 is not universally supported by all the receiver hosts or the receiver applications as of press time; IGMPv2 is more common, especially in IPTV applications.³

REFERENCES

- [ADA200501] A. Adams, J. Nicholas, W. Siadak, “Protocol independent multicast—Dense mode (PIM-DM): Protocol specification (revised),” RFC 3973, January 2005.
- [CAI200201] B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan, “Internet Group Management Protocol, Version 3,” RFC 3376, October 2002.
- [CIS200701] Cisco Systems, Internet Protocol (IP) Multicast Technology Overview and White Papers, Cisco Systems, Inc., 170 West Tasman Dr., San Jose, CA 95134, USA.
- [DEE198901] S. E. Deering, “Host extensions for IP multicasting,” RFC 1112, August 1989.
- [MEY199801] D. Meyer, “Administratively scoped IP multicast,” RFC 2365, University of Oregon, July 1998.
- [MIN200801] D. Minoli, *IP Multicast with Applications to IPTV and Mobile DVB-H*, Wiley, 2008.
- [PAR200601] L. Parziale, W. Liu, et al, *TCP/IP Tutorial and Technical Overview*, IBM Press, 2006, ISBN 0738494682, IBM Form Number GG24-3376-07. Redbook Abstract.
- [RAY200201] J. Reynolds, ed. “Assigned numbers: RFC 1700 is replaced by an on-line database,” RFC 3232, January 2002. Obsoletes RFC 1700, (Status: Informational).
- [WEL200101] P. J. Welcher, “The protocols of IP multicast,” 2001 NetCraftsmen White Paper, Chesapeake NetCraftsmen, LLC., 1290 Bay Dale Drive—Suite #312, Arnold, MD 21012. <http://www.netcraftsmen.net/welcher/papers/multicast01.html>

³Some vendors have developed a IGMP Version 3 lite (IGMPv3lite).

4 IPv6 Multicast Approaches

This chapter discusses multicast operations in Internet Protocol Version 6 (IPv6) environments. The capability is supported via an *IPv6 Multicast Address* and via a *user signaling protocol*, specifically the Multicast Listener Discovery (MLDv2) protocol.

4.1 OVERVIEW

The multicast environment consists of transmitters (senders) and receivers. Just as was the case in the IPv4 case, an IPv6 multicast group is a group of receivers that wish to receive a specific data stream that is transmitted using IPv6 packets at the network layer. This group has no physical or geographical specificity: receivers can be located anywhere on the underlying (public or private) network. IPv6-based devices that wish to receive specific traffic are known as group members, and packets delivered to group members are identified by a single multicast group address. The network can deliver information to a large (unlimited) number of receivers, by transmitting only one copy of the multicast information on each subnet. Multicast packets are delivered to a group using best-effort methods, just as is the case for IPv6 unicast packets.

Receivers that wish to receive data intended for a particular group must join the group by signaling their local router. This signaling is achieved with the MLD protocol. Routers utilize the MLD protocol to learn whether members of a group are present on their directly attached subnets. Devices join multicast groups by sending MLD report messages. Membership in a multicast group is dynamic: devices can join and leave at will. A device can be a member of more than one multicast group at a time.

Properly configured/authorized IPv6 hosts, regardless of whether they are a member of a group, can send to a group. However, only the members of a group receive the message. A multicast address is assigned for the receivers in a multicast group. Senders (transmitters) utilize that address as the destination address of a packet intended to reach all members of the group.

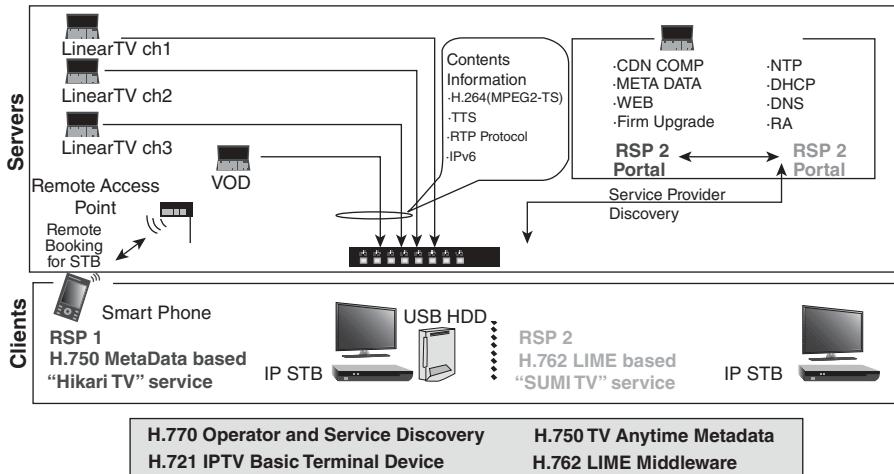


FIGURE 4.1 The 3rd ITU-T IPTV Interop Event and Showcase, December 14–17, 2010 in Pune, India, makes use of IPv6 Multicast.

This chapter provides an overview of MLD, based on RFC 2170, *Multicast Listener Discovery (MLD) for IPv6* [DEE199901], and RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*. MLDv2 is backward-compatible with MLDv1 (described in RFC 2710). Hosts that support only MLDv1 can interoperate with a router running MLDv2. Mixed LANs with both MLDv1 and MLDv2 hosts can also be supported. The focus in this chapter is on MLDv1. Next-generation video services as supported by the evolving IPTV technology is already making use of IPv6 (in addition, of course, to IPv4): the 3rd ITU-T IPTV Interop Event and Showcase held in, Pune, India, on December 14–17, 2010, made use of IPv6 Multicast, as shown in Figure 4.1 [NIS201101] (also see Chapter 6). Table 4.1 identifies key RFCs that describe the operational aspects of IPv6 Multicast.

4.2 IPV6 MULTICAST ADDRESSES

Figure 4.2 depicts the IPv6 Multicast Address. In IPv6, multicast addresses begin with the format prefix 1111 1111 (FF in hex). The format prefix is followed by two fields, each 4 bits long: *Flags* and *Scope*. The Flags field T indicates whether the address was permanent or transient. A permanent multicast address has a lifetime parameter equal to 0; a temporary multicast address has a lifetime parameter equal to 1. RFC 3306 added a P (prefix) flag; this flag allows part of the group address to include the source networks Unicast prefix, which creates a globally unique Group Address. The R flag is used to indicate that Rendezvous Point (RP) address is embedded in the group address; with Embedded RP, the flags R, P, T are set to 1. The Scope is a subset of the network. The remaining 112 bits of the IPv6 address are the Group ID.

TABLE 4.1 Key RFCs that Describe the Operational Aspects of IPv6 Multicast

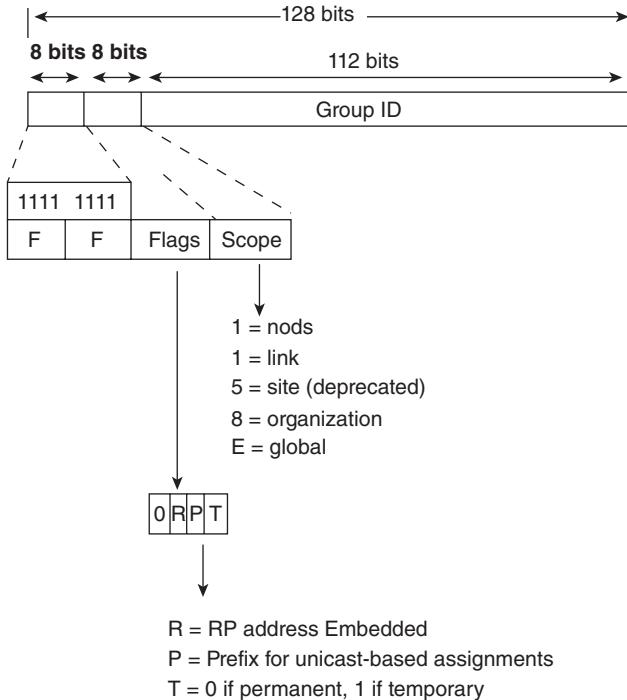
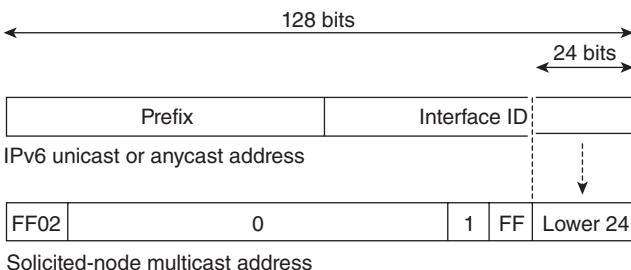
RFC 2375 (Informational)	IPv6 Multicast Address Assignments	1998-07
RFC 2710 (Proposed Standard) Updated by RFC 3590, RFC 3810	Multicast Listener Discovery (MLD) for IPv6	1999-10
RFC 3306 (Proposed Standard) Updated by RFC 3956, RFC 4489	Unicast-Prefix-based IPv6 Multicast Addresses	2002-08
RFC 3307 (Proposed Standard)	Allocation Guidelines for IPv6 Multicast Addresses	2002-08
RFC 3810 (Proposed Standard) Updated by RFC 4604	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	2004-06
RFC 3956 (Proposed Standard)	Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address	2004-11
RFC 4489 (Proposed Standard)	A Method for Generating Link-Spaced IPv6 Multicast Addresses Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast	2006-04
RFC 4604		2008-08
RFC 5757 (Informational)	Multicast Mobility in Mobile IP Version 6 (MIPv6): Problem Statement and Brief Survey	2010-02
RFC 6085 (Proposed Standard)	Address Mapping of IPv6 Multicast Packets on Ethernet	2011-01
RFC 6224 (Informational)	Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains	2011-04

As part of the operational requirements, IPv6 nodes (hosts and routers) are required to join (receive packets destined for) the following multicast groups:

- All-nodes multicast group FF02:0:0:0:0:0:1 (scope is link-local).
- Solicited-node multicast group FF02:0:0:0:0:1:FF00:0000/104 for each of its assigned unicast and anycast addresses. IPv6 nodes must join the associated solicited-node multicast group for every unicast and anycast address to which it is assigned. The IPv6 solicited-node multicast address has the prefix FF02:0:0:0:0:1:FF00:0000/104 concatenated with the 24 low-order bits of a corresponding IPv6 unicast or anycast address, as illustrated in Figure 4.3.

IPv6 routers must also join the following multicast group:

- All-routers multicast group FF02:0:0:0:0:0:2 (scope is link-local).

**FIGURE 4.2** IPv6 multicast addressing.**FIGURE 4.3** Solicited-node multicast address format.

4.3 MEDIA ACCESS CONTROL (MAC) LAYER ADDRESSES ASPECTS

MAC layer addresses consist of 24 bits for the Organizational Unit Identifier (OUI) and 24 bits for serial number of the Ethernet Network Interface Card (NIC). For a multicast environment, the MAC address format uses a special OUI.

The OUI for IPv4 Multicast is 00:00:5E, with the Least Significant Bit Most Significant Octet set and with only half of this address space allocated to IP Multicast; the implication of the fact that only 23 bits are available for the

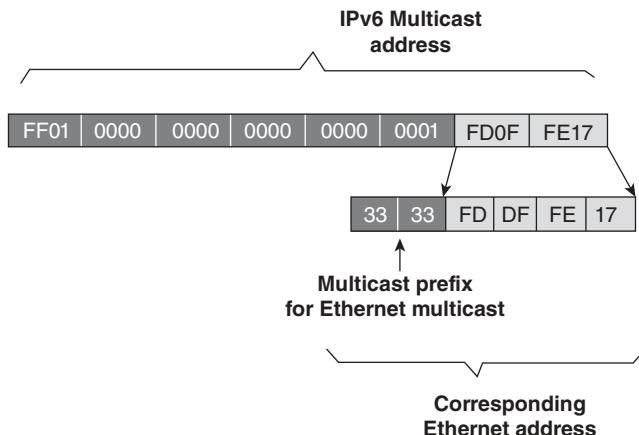


FIGURE 4.4 IPv6 multicast address mapping to derive an Ethernet address.

group address means a potential address overlap at Layer 2. A different OUI format is used for IPv6 Multicast: the leading two octets are set to hex 33-33, and the remaining 4 octets are available for address mapping from the last 32 bits of the 128 bit IPv6 Multicast address. See Figure 4.4 for an example.

4.4 SIGNALING

Just as is the case in IPv4, IPv6 hosts (receivers) must signal a gateway router with their desire to receive data from a specific group. IPv6 Multicast does not use the IGMP but rather MLD. MLD Version 1 is similar to IGMPv2, and MLDv2 is similar to IGMPv3. See Figure 4.5. MLD is used by IPv6 routers to discover the presence of multicast listeners (i.e., nodes that want to receive multicast packets, including IPTV receivers and other video devices) on their directly attached links, and to discover which multicast addresses are of interest to those neighboring nodes. This topic is discussed in more detail in Section 4.5.

4.5 ROUTING

Protocol Independent Multicast (PIM) Sparse Mode (PIM-SM) is utilized between routers to enable them to support intradomain multicast routing, namely, to track which multicast packets to forward to each other and to their directly connected subnets or LANs. PIM works independently of the unicast routing protocol (such as Routing Information Protocol [RIP], Enhanced Interior Gateway Routing Protocol [EIGRP], etc.) to perform “send” or “receive” multicast route updates, and it operates in a manner generally similar to how other protocols handle this function. Specifically, PIM-SM utilizes unicast routing to provide reverse-path information for multicast tree building.

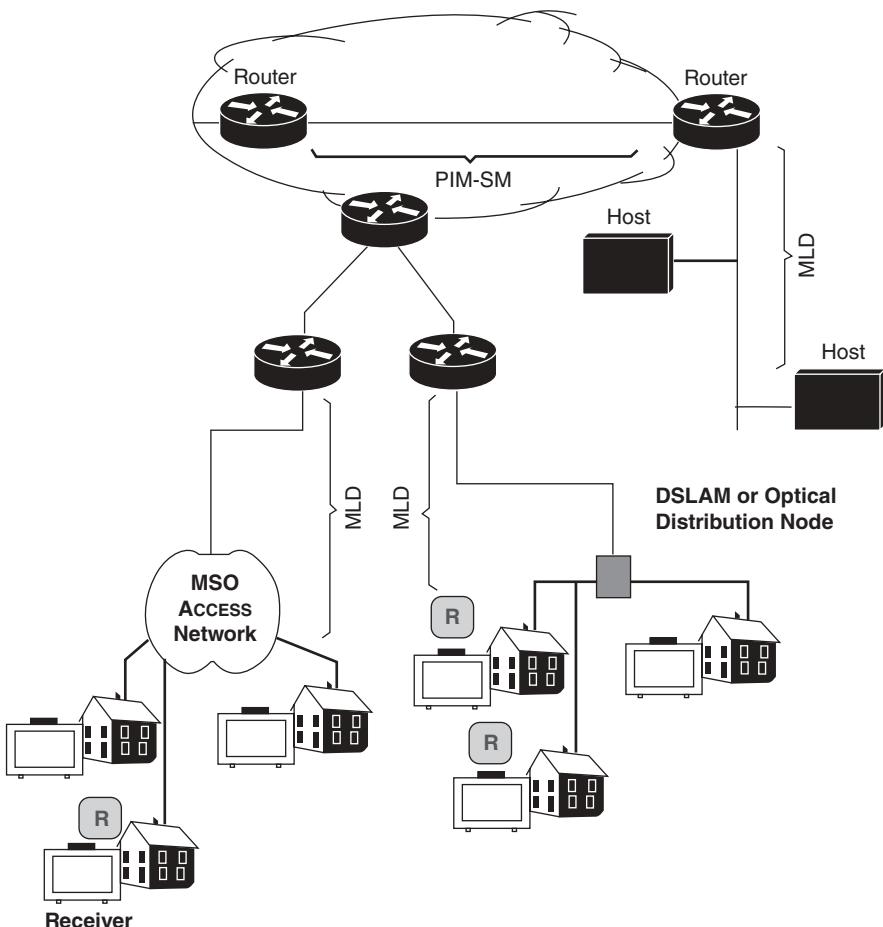


FIGURE 4.5 Role of MLD and PIM-SM.

As hinted in Chapter 3, PIM-SM is employed in a multicast network when relatively few routers are involved in each multicast; these routers do not forward multicast packets for a group, unless there is an explicit request for the content. PIM-SM distributes information about active sources by forwarding data packets on the shared tree. A shared tree is a routing tree that supports one or more multicast groups. Shared trees require the use of a rendezvous point (RP). The RP tree is constructed to connect all receivers to the RP. In PIM-SM, group members for a group G join the shared RP tree for a particular group; this tree is represented by $(*, G)$ multicast route entries along the shortest path branches between the RP and the group members.

Requests are accomplished via PIM joins that are sent hop by hop toward the root node of the tree. The root node of a tree in PIM-SM is the RP in the

case of a shared tree or the first-hop router that is directly connected to the multicast source in the case of a shortest path tree (SPT). The RP keeps track of multicast groups, and the hosts that send multicast packets are registered with the RP by that host's first-hop router. As a PIM join travels up the tree, routers along the path set up a multicast forwarding state so that the requested multicast traffic will be forwarded back down the tree. When multicast traffic is no longer needed, a router sends a PIM prune up the tree toward the root node to prune (or remove) the unnecessary traffic. As this PIM prune travels hop by hop up the tree, each router updates its forwarding state appropriately. Ultimately, the forwarding state associated with a multicast group or source is removed. A multicast data sender sends data destined for a multicast group. The designated router (DR) of the sender is responsible for sending PIM register and PIM join and prune messages toward the RP to inform it about active sources and host group membership. The DR, then, takes those data packets, unicast encapsulates them, and sends them directly to the RP (the process of encapsulating data packets to the RP is called registering, and the encapsulation packets are called PIM register packets). The RP receives these encapsulated data packets, deencapsulates them, and forwards them onto the shared tree. The packets then follow the $(*, G)$ multicast tree state in the routers on the RP tree, being replicated wherever the RP tree branches, and eventually reaching all the receivers for that multicast group [CIS201101].

If there are multiple PIM-SM routers on a LAN, a unique DR must be elected to avoid duplicating multicast traffic for connected hosts. PIM-SM uses a selection process to select a designated router when there is more than one router on a LAN segment. Typically, the PIM router with the highest IPv6 address is selected to become the DR for the LAN. See Figure 4.6 for a graphical example. In the diagram, only the leftmost router operates as the DR and sends joins to the RP to construct the shared tree for Group A—clearly if both routers were permitted to send $(*, G)$ joins to the RP, parallel paths would be created and the end devices would receive duplicate multicast traffic. If the active DR should fail, PIM-SM has a capability to detect the failure of the DR and elect a failover DR.

4.6 RENDEZVOUS POINT (RP) APPROACHES

As just seen, PIM-SM sources must send their traffic to a RP; this traffic is in turn forwarded to receivers on a shared distribution tree. PIM routers in a domain must be able to map each multicast group to the correct RP address. In IPv6, there is a Bootstrap Router (BSR) protocol for and also a static configuration mechanism for an RP (Embedded RP).

The BSR protocol for PIM-SM provides a dynamic, adaptive mechanism to distribute group-to-RP mapping information rapidly throughout a domain. With the IPv6 BSR feature, if an RP becomes unreachable, it will be detected; in turn, the mapping tables are modified so that the unreachable RP is no

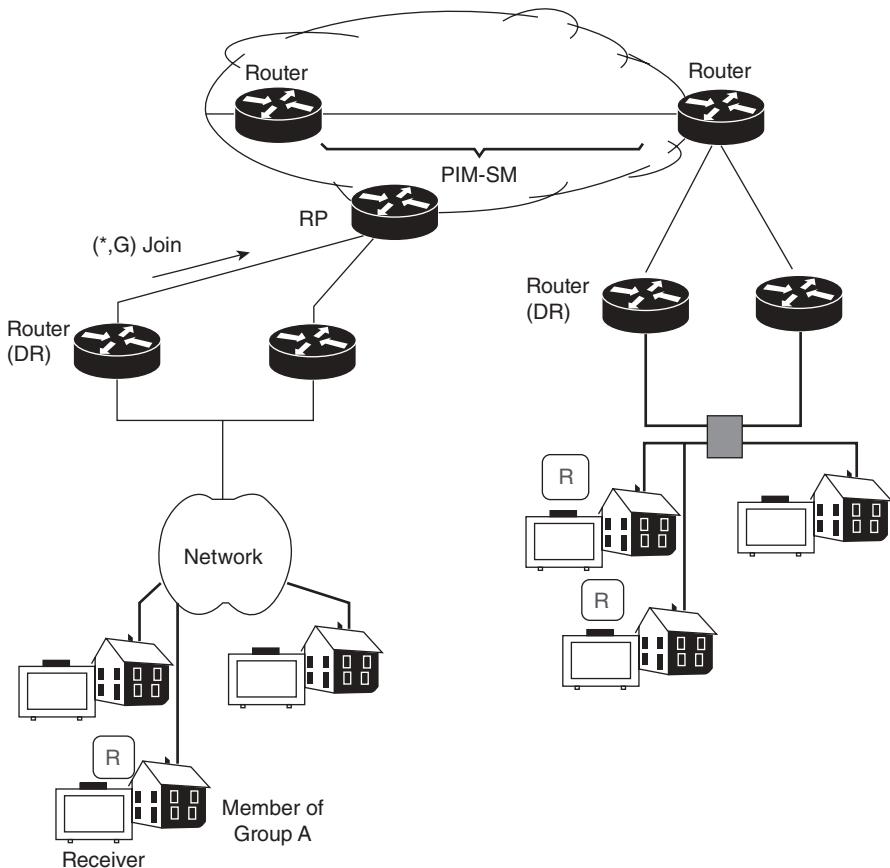


FIGURE 4.6 Pictorial view of designated router for multiaccess segments.

longer used, and the new tables will be rapidly distributed throughout the domain [CIS201101].

Embedded RP support allows the router to learn RP information using the multicast group destination address instead of the statically configured RP. Embedded RP is a an approach that can be utilized for those applications that cannot leverage SSM and that require a PIM SM model to interoperate across multiple domains. For routers that are the RP, the router must be statically configured as the RP. The router searches for embedded RP group addresses in MLD reports or PIM messages and data packets. Upon finding such an address, the router learns the RP for the group from the address. It then uses this learned RP for all protocol activity for the group. For routers that are the RP, the router that is advertised as an embedded RP must be configured as the RP [CIS201101]. Embedded RP uses the R flag discussed above: when the

flags R, P, T are set to 1, this indicates that the RP address is embedded in the group address.

4.7 MULTICAST LISTENER DISCOVERY (MLD)

This section provides a detailed view of MLD. Just as is the case in IPv4, IPv6 hosts (receivers) signal a router with their desire to receive data from a specific group. IPv6 Multicast does not use the IGMP but rather the MLD protocol. MLD used by an IPv6 router to discover the presence of multicast listeners on directly attached links and to discover which multicast addresses are of interest to those neighboring nodes. MLDv1 is similar to Internet Group Management Protocol Version 2 (IGMPv2), and MLDv2 is similar to IGMPv3. MLDv2 adds the ability for a node to report interest in listening to packets with a particular multicast address only from specific source addresses or from all sources except for specific source addresses, this being similar to Source-Specific Multicast (SSM). Recall that SSM is a form of multicast where a receiver must specify both the network-layer address of the source and the multicast destination address in order to receive the multicast datagrams of interest.

4.7.1 Overview of MLDv1

MLD¹ (RFC 2710, RFC 3550, RFC 3810, and RFC 4604) specifies the protocol used by an IPv6 router to discover the presence of multicast listeners (i.e., nodes wishing to receive multicast packets) on its directly attached links, and to discover which multicast addresses are of interest to those neighboring nodes. MLD enables IPv6 routers to discover the presence of multicast listeners. This information is then provided to the multicast routing protocol being used by the router in order to ensure that multicast packets are delivered to all links where there are interested receivers. MLD is derived from Version 2 of IPv4's IGMPv2. One important difference is that MLD uses ICMPv6 message types (IP Protocol 58) rather than IGMP message types (IP Protocol 2).

MLD is an asymmetric protocol, specifying different behaviors for multicast listeners and for routers. For those multicast addresses to which a router itself is listening, the router performs both parts of the protocol, the “multicast router part” and the “multicast address listener part,” including responding to its own messages. If a router has more than one interface to the same link, it needs to perform the router part of MLD over only one of those interfaces. Listeners, on the other hand, must perform the listener part of MLD on all interfaces from which an application or upper-layer protocol has requested reception of multicast packets.

¹The discussion this section is based on and summarized from RFC 2710 [DEE199901].

Note that a multicast router may itself be a listener of one or more multicast addresses; in this case, it performs both the “multicast router part” and the “multicast address listener part” of the protocol to collect the multicast listener information needed by its multicast routing protocol on the one hand, and to inform itself and other neighboring multicast routers of its listening state on the other hand.

In the discussion below,

- A querier is a network device, such as a router, that sends query messages to discover which network devices are members of a given multicast group.
- A host is a receiver, including routers, that sends report messages to inform the querier of a host membership.

A set of queriers and hosts that receive multicast data streams from the same source is called a multicast group. Queriers and hosts utilize MLD reports to join and leave multicast groups and to begin receiving group traffic. MLD provides a mechanism to automatically control the flow of multicast traffic throughout the network with the use of special multicast queriers and hosts.

4.7.2 Message Format

MLD is a subprotocol of ICMPv6, namely, MLD message types are a subset of the set of ICMPv6 messages, and MLD messages are identified in IPv6 packets by a preceding Next Header value of 58. All MLD messages are sent with a link-local IPv6 Source Address, an IPv6 Hop Limit of 1, and an IPv6 Router Alert option in a Hop-by-Hop Options header. (The Router Alert option is necessary to cause routers to examine MLD messages sent to multicast addresses in which the routers themselves have no interest.)

MLD messages have the following depicted in Figure 4.7 and discussed below.

There are three *types* of MLD messages:

- *Type 1*: Multicast Listener Query (Type = decimal 130), also known as “Query.” There are two subtypes of Multicast Listener Query messages (differentiated by the contents of the Multicast Address field):
 - General Query, used to learn which multicast addresses have listeners on an attached link.
 - Multicast Address-Specific Query, used to learn if a particular multicast address has any listeners on an attached link.
- *Type 2*: Multicast Listener Report (Type = decimal 131), also known as “Report.”
- *Type 3*: Multicast Listener Done (Type = decimal 132), also known as “Done.”

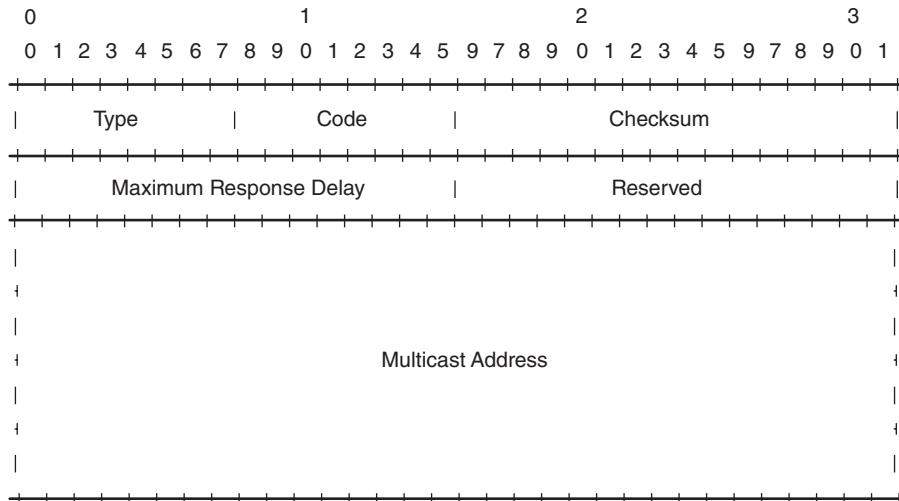


FIGURE 4.7 MLD messages format.

The *Type* is initialized to zero by the sender; ignored by receivers.

The *Checksum* is the standard ICMPv6 checksum, covering the entire MLD message plus a “pseudo-header” of IPv6 header fields.

The *Maximum Response Delay* field is meaningful only in Query messages, and specifies the maximum allowed delay before sending a responding Report, in units of milliseconds. In all other messages, it is set to zero by the sender and ignored by receivers.

Varying this value allows the routers to tune the “leave latency” (the time between the moment the last node on a link ceases listening to a particular multicast address and moment the routing protocol is notified that there are no longer any listeners for that address). It also allows tuning of the burstiness of MLD traffic on a link.

The *reserved* field is initialized to zero by the sender; ignored by receivers.

In a Query message, the *Multicast Address* field is set to zero when sending a General Query, and set to a specific IPv6 multicast address when sending a Multicast-Address-Specific Query. In a Report or Done message, the Multicast Address field holds a specific IPv6 multicast address to which the message sender is listening or is ceasing to listen, respectively.

The length of a received MLD message is computed by taking the IPv6 Payload Length value and subtracting the length of any IPv6 extension headers present between the IPv6 header and the MLD message. If that length is greater than 24 octets, that indicates that there are other fields present beyond the fields described above, perhaps belonging to a future backwards-compatible version of MLD. An implementation of the version of MLD specified in this document must not send an MLD message longer than 24 octets and must ignore anything past the first 24 octets of a received MLD message. In all cases,

the MLD checksum must be computed over the entire MLD message, not just the first 24 octets.

4.7.3 Protocol Description

Routers use MLD to learn which multicast addresses have listeners on each of their attached links. Each router keeps a list, for each attached link, of which multicast addresses have listeners on that link, and a timer associated with each of those addresses. Note that the router needs to learn only that the listeners for a given multicast address are present on a link; it does not need to learn the identity (e.g., unicast address) of those listeners or even how many listeners are present.

For each attached link, a router selects one of its link-local unicast addresses on that link to be used as the IPv6 Source Address in all MLD packets it transmits on that link.

For each interface over which the router is operating the MLD protocol, the router must configure that interface to listen to all link-layer multicast address that can be generated by IPv6 multicasts. For example, an Ethernet-attached router must set its Ethernet address reception filter to accept all Ethernet multicast addresses that start with the hexadecimal value 3333; in the case of an Ethernet interface that does not support the filtering of such a range of multicast address, it must be configured to accept ALL Ethernet multicast addresses in order to meet the requirements of MLD.

With respect to each of its attached links, a router may assume one of two roles: Querier or Non-Querier. There is normally only one Querier per link. All routers start up as a Querier on each of their attached links. If a router hears a Query message whose IPv6 Source Address is numerically less than its own selected address for that link, it must become a Non-Querier on that link. If the timer (Other Querier Present Interval) passes without receiving, from a particular attached link, any Queries from a router with an address less than its own, a router resumes the role of Querier on that link.

A Querier for a link periodically sends (with timer [Query Interval]) a General Query on that link to solicit reports of all multicast addresses of interest on that link. On startup, a router should send as many General Queries as specified by (Startup Query Count), spaced closely together (based on the [Startup Query Interval] timer) on all attached links in order to quickly and reliably discover the presence of multicast listeners on those links.

General Queries are sent to the link-scope all-nodes multicast address (FF02::1), with a Multicast Address field of 0, and a Maximum Response Delay defined by the timer (Query Response Interval).

When a node receives a General Query, it sets a delay timer for each multicast address to which it is listening on the interface from which it received the Query, excluding the link-scope all-nodes address and any multicast addresses of scope 0 (reserved) or 1 (node-local). Each timer is set to a different random value, using the highest clock granularity available on the node, selected from the range (0, Maximum Response Delay) with Maximum

Response Delay as specified in the Query packet. If a timer for any address is already running, it is reset to the new random value only if the requested Maximum Response Delay is less than the remaining value of the running timer. If the Query packet specifies a Maximum Response Delay of zero, each timer is effectively set to zero, and the action specified below for timer expiration is performed immediately.

When a node receives a Multicast Address-Specific Query, if it is listening to the queried Multicast Address on the interface from which the Query was received, it sets a delay timer for that address to a random value selected from the range (0, Maximum Response Delay), as above. If a timer for the address is already running, it is reset to the new random value only if the requested Maximum Response Delay is less than the remaining value of the running timer. If the Query packet specifies a Maximum Response Delay of zero, the timer is effectively set to zero, and the action specified below for timer expiration is performed immediately.

If a node's timer for a particular multicast address on a particular interface expires, the node transmits a Report to that address via that interface; the address being reported is carried in both the IPv6 Destination Address field and the MLD Multicast Address field of the Report packet. The IPv6 Hop Limit of 1 (as well as the presence of a link-local IPv6 Source Address) prevents the packet from traveling beyond the link to which the reporting interface is attached.

If a node receives another node's Report from an interface for a multicast address while it has a timer running for that same address on that interface, it stops its timer and does not send a Report for that address, thus suppressing duplicate reports on the link.

When a router receives a Report from a link, if the reported address is not already present in the router's list of multicast address having listeners on that link, the reported address is added to the list, its timer is set to (Multicast Listener Interval), and its appearance is made known to the router's multicast routing component. If a Report is received for a multicast address that is already present in the router's list, the timer for that address is reset to (Multicast Listener Interval). If an address's timer expires, it is assumed that there are no longer any listeners for that address present on the link, so it is deleted from the list, and its disappearance is made known to the multicast routing component.

When a node starts listening to a multicast address on an interface, it should immediately transmit an unsolicited Report for that address on that interface, in case it is the first listener on the link. To cover the possibility of the initial Report being lost or damaged, it is recommended that it be repeated once or twice after short delays (Unsolicited Report Interval). (A simple way to accomplish this is to send the initial Report and then act as if a Multicast-Address-Specific Query was received for that address, and set a timer appropriately.)

When a node ceases to listen to a multicast address on an interface, it should send a single Done message to the link-scope all-routers multicast address (FF02::2), carrying in its Multicast Address field the address to which it is

ceasing to listen. If the node's most recent Report message was suppressed by hearing another Report message, it may send nothing, as it is highly likely that there is another listener for that address still present on the same link. If this optimization is implemented, it must be able to be turned off but should default to on.

When a router in Querier state receives a Done message from a link, if the Multicast Address identified in the message is present in the Querier's list of addresses having listeners on that link, the Querier sends (Last Listener Query Count) Multicast-Address-Specific Queries, one every (Last Listener Query Interval) to that multicast address. These Multicast Address-Specific Queries have their Maximum Response Delay set to (Last Listener Query Interval). If no Reports for the address are received from the link after the response delay of the last query has passed, the routers on the link assume that the address no longer has any listeners there; the address is therefore deleted from the list, and its disappearance is made known to the multicast routing component. This process is continued to its resolution (i.e. until a Report is received or the last Multicast-Address-Specific Query is sent with no response) despite any transition from Querier to Non-Querier on this link.

Routers in Non-Querier state must ignore Done messages.

When a router in Non-Querier state receives a Multicast Address-Specific Query, if its timer value for the identified multicast address is greater than (Last Listener Query Count) times the Maximum Response Delay specified in the message, it sets the address's timer to that latter value.

4.7.4 State Transition for Nodes

Node behavior is more formally specified by the state transition diagram below. A node may be in one of three possible states with respect to any single IPv6 multicast address on any single interface:

- “Non-Listener” state, when the node is not listening to the address on the interface (i.e., no upper-layer protocol or application has requested reception of packets to that multicast address). This is the initial state for all multicast addresses on all interfaces; it requires no storage in the node.
- “Delaying Listener” state, when the node is listening to the address on the interface and has a report delay timer running for that address.
- “Idle Listener” state, when the node is listening to the address on the interface and does not have a report delay timer running for that address.

There are five significant events that can cause MLD state transitions:

- “start listening” occurs when the node starts listening to the address on the interface. It may occur only in the Non-Listener state.
- “stop listening” occurs when the node stops listening to the address on the interface. It may occur only in the Delaying Listener and Idle Listener states.

- “query received” occurs when the node receives either a valid General Query message, or a valid Multicast Address-Specific Query message. To be valid, the Query message must come from a link-local IPv6 Source Address, be at least 24 octets long, and have a correct MLD checksum. The Multicast Address field in the MLD message must contain either zero (a General Query) or a valid multicast address (a Multicast-Address-Specific Query). A General Query applies to all multicast addresses on the interface from which the Query is received. A Multicast-Address-Specific Query applies to a single multicast address on the interface from which the Query is received. Queries are ignored for addresses in the Non-Listener state.
- “report received” occurs when the node receives a valid MLD Report message. To be valid, the Report message must come from a link-local IPv6 Source Address, be at least 24 octets long, and have a correct MLD checksum. A Report applies only to the address identified in the Multicast Address field of the Report, on the interface from which the Report is received. It is ignored in the Non-Listener or Idle Listener state.
- “timer expired” occurs when the report delay timer for the address on the interface expires. It may occur only in the Delaying Listener state.

All other events, such as receiving invalid MLD messages or MLD message types other than Query or Report, are ignored in all states.

There are seven possible actions that may be taken in response to the above events:

- “send report” for the address on the interface. The Report message is sent to the address being reported.
- “send done” for the address on the interface. If the flag saying we were the last node to report is cleared, this action may be skipped. The Done message is sent to the link-scope all-routers address (FF02::2).
- “set flag” that we were the last node to send a report for this address.
- “clear flag” since we were not the last node to send a report for this address.
- “start timer” for the address on the interface, using a delay value chosen uniformly from the interval (0, Maximum Response Delay), where Maximum Response Delay is specified in the Query. If this is an unsolicited Report, the timer is set to a delay value chosen uniformly from the interval (0, [Unsolicited Report Interval]).
- “reset timer” for the address on the interface to a new value, using a delay value chosen uniformly from the interval (0, Maximum Response Delay), as described in “start timer.”
- “stop timer” for the address on the interface.

The link-scope all-nodes address (FF02::1) is handled as a special case. The node starts in Idle Listener state for that address on every interface, never transitions to another state, and never sends a Report or Done for that address.

MLD messages are never sent for multicast addresses whose scope is 0 (reserved) or 1 (node-local).

MLD messages are sent for multicast addresses whose scope is 2 (link-local), including Solicited-Node multicast addresses, except for the link-scope, all-nodes address (FF02::1).

4.7.5 State Transition for Routers

A router may be in one of two possible states with respect to any single attached link:

- “Querier,” when this router is designated to transmit MLD Queries on this link.
- “Non-Querier,” when there is another router designated to transmit MLD Queries on this link.

The following three events can cause the router to change states:

- “query timer expired” occurs when the timer set for query transmission expires. This event is significant only when in the Querier state.
- “query received from a router with a lower IP address” occurs when a valid MLD Query is received from a router on the same link with a lower IPv6 Source Address. To be valid, the Query message must come from a link-local IPv6 Source Address, be at least 24 octets long, and have a correct MLD checksum.
- “other querier present timer expired” occurs when the timer set to note the presence of another querier with a lower IP address on the link expires. This event is significant only when in the Non-Querier state.

There are three actions that may be taken in response to the above events:

- “start general query timer” for the attached link to (Query Interval).
- “start other querier present timer” for the attached link to (Other Querier Present Interval).
- “send general query” on the attached link. The General Query is sent to the link-scope all-nodes address (FF02::1), and has a Maximum Response Delay of (Query Response Interval).

A router starts in the Initial state on all attached links, and immediately transitions to Querier state. In addition, to keep track of which multicast addresses have listeners, a router may be in one of three possible states with respect to any single IPv6 multicast address on any single attached link:

- “No Listeners Present” state, when there are no nodes on the link that have sent a Report for this multicast address. This is the initial state for all multicast addresses on the router; it requires no storage in the router.
- “Listeners Present” state, when there is a node on the link that has sent a Report for this multicast address.

- “Checking Listeners” state, when the router has received a Done message but has not yet heard a Report for the identified address.

There are five significant events that can cause router state transitions:

- “report received” occurs when the router receives a Report for the address from the link. To be valid, the Report message must come from a link-local IPv6 Source Address, be at least 24 octets long, and have a correct MLD checksum.
- “done received” occurs when the router receives a Done message for the address from the link. To be valid, the Done message must come from a link-local IPv6 Source Address, be at least 24 octets long, and have a correct MLD checksum. This event is significant only in the “Listerners Present” state and when the router is a Querier.
- “multicast address-specific query received” occurs when a router receives a Multicast Address-Specific Query for the address from the link. To be valid, the Query message must come from a link-local IPv6 Source Address, be at least 24 octets long, and have a correct MLD checksum. This event is significant only in the “Listeners Present” state and when the router is a Non-Querier.
- “timer expired” occurs when the timer set for a multicast address expires. This event is significant only in the “Listeners Present” or “Checking Listeners” state.
- “retransmit timer expired” occurs when the timer set to retransmit a Multicast-Address-Specific Query expires. This event is significant only in the “Checking Listeners” state.

There are seven possible actions that may be taken in response to the above events:

- “start timer” for the address on the link—also resets the timer to its initial value (Multicast Listener Interval) if the timer is currently running.
- “start timer*” for the address on the link—this alternate action sets the timer to the minimum of its current value and either (Last Listener Query Interval) \times (Last Listener Query Count) if this router is a Querier, or the Maximum Response Delay in the Query message \times (Last Listener Query Count) if this router is a non-Querier.
- “start retransmit timer” for the address on the link (Last Listener Query Interval).
- “clear retransmit timer” for the address on the link.
- “send multicast address-specific query” for the address on the link. The Multicast-Address-Specific Query is sent to the address being queried, and has a Maximum Response Delay of (Last Listener Query Interval).
- “notify routing +” internally notify the multicast routing protocol that there are listeners to this address on this link.

- “notify routing –” internally notify the multicast routing protocol that there are no longer any listeners to this address on this link.

The state diagrams that follow apply per group per link (one for routers in Querier state and one for routers in Non-Querier state). The transition between Querier and Non-Querier state on a link is handled specially. All groups on that link in “No Listeners Present” or “Listeners Present” states switch state transition diagrams when the Querier/Non-Querier state transition occurs. However, any groups in “Checking Listeners” state continue with the same state transition diagram until the “Checking Listeners” state is exited. For example, a router that starts as a Querier, receives a Done message for a group and then receives a Query from a router with a lower address (causing a transition to the Non-Querier state) continues to send multicast address-specific queries for the group in question until it either receives a Report or its timer expires, at which time it starts performing the actions of a Non-Querier for this group.

The state transition diagram for a router in Non-Querier state is similar, but non-Queriers do not send any messages and are only driven by message reception.

4.7.6 Overview of MLDv2

The MLDv2 protocol, when compared with MLDv1, adds support for “source filtering,” that is, the ability for a node to report interest in listening to packets *only* from specific source addresses, as required to support Source-Specific Multicast defined in RFC 3569, or from *all but* specific source addresses, sent to a particular multicast address. MLDv2 is designed to be interoperable with MLDv1. RFC 3810 (June 2004) updates RFC 2710. Below is a brief summary MLDv2 based directly on the RFC. Developers and interested parties should consult the RFC outright.

Protocol Overview As noted already, MLD is an asymmetric protocol; it specifies separate behaviors for multicast address listeners (i.e., hosts or routers that listen to multicast packets) and multicast routers. The purpose of MLD is to enable each multicast router to learn, for each of its directly attached links, which multicast addresses and which sources have interested listeners on that link. The information gathered by MLD is provided to whichever multicast routing protocol is used by the router in order to ensure that multicast packets are delivered to all links where there are listeners interested in such packets.

Multicast routers only need to know that *at least one* node on an attached link is listening to packets for a particular multicast address, from a particular source; a multicast router is not required to *individually* keep track of the interests of each neighboring node.

A multicast router performs the *router part* of the MLDv2 protocol on each of its directly attached links. If a multicast router has more than one interface

connected to the same link, it only needs to operate the protocol on one of those interfaces. The router behavior depends on whether there are several multicast routers on the same subnet or not. If that is the case, a querier election mechanism is used to elect a single multicast router to be in Querier state. This router is called the Querier. All multicast routers on the subnet listen to the messages sent by multicast address listeners, and maintain the same multicast listening information state, so that they can take over the querier role, should the present Querier fail. Nevertheless, only the Querier sends periodical or triggered query messages on the subnet.

A multicast address listener performs the *listener part* of the MLDv2 protocol on all interfaces on which multicast reception is supported, even if more than one of those interfaces are connected to the same link.

Building Multicast Listening State on Multicast Address Listeners Upper-layer protocols and applications that run on a multicast address listener node use specific service interface calls to ask the IP layer to enable or disable reception of packets sent to specific multicast addresses. The node keeps Multicast Address Listening state for each socket on which the service interface calls have been invoked. In addition to this per-socket multicast listening state, a node must also maintain or compute multicast listening state for each of its interfaces. Conceptually, that state consists of a set of records, with each record containing an IPv6 multicast address, a filter mode, and a source list. The filter mode may be either INCLUDE or EXCLUDE. In INCLUDE mode, reception of packets sent to the specified multicast address is enabled *only* from the source addresses listed in the source list. In EXCLUDE mode, reception of packets sent to the given multicast address is enabled from all source addresses *except* those listed in the source list.

At most, one record per multicast address exists for a given interface. This per-interface state is derived from the per-socket state, but may differ from it when different sockets have differing filter modes and/or source lists for the same multicast address and interface. After a multicast packet has been accepted from an interface by the IP layer, its subsequent delivery to the application connected to a particular socket depends on the multicast listening state of that socket (and possibly also on other conditions, such as what transport-layer port the socket is bound to). Note that MLDv2 messages are not subject to source filtering and must always be processed by hosts and routers.

Exchanging Messages between the Querier and the Listening Nodes There are three types of MLDv2 query messages: General Queries, Multicast Address-Specific Queries, and Multicast Address and Source Specific Queries. The Querier periodically sends General Queries to learn multicast address listener information from an attached link. These queries are used to build and refresh the Multicast Address Listener state inside all multicast routers on the link.

Nodes respond to these queries by reporting their per-interface Multicast Address Listening state through Current State Report messages sent to a specific multicast address all MLDv2 routers on the link listen to. On the other hand, if the listening state of a node changes, the node immediately reports these changes through a State Change Report message. The State Change Report contains either Filter Mode Change records, Source List Change records, or records of both types.

Both router and listener state changes are mainly triggered by the expiration of a specific timer, or the reception of an MLD message (listener state change can be also triggered by the invocation of a service interface call). Therefore, to enhance protocol robustness, in spite of the possible unreliability of message exchanges, messages are retransmitted several times. Furthermore, timers are set so as to take into account the possible message losses, and to wait for retransmissions.

Periodical General Queries and Current State Reports do not apply this rule in order not to overload the link; it is assumed that in general, these messages do not generate state changes, their main purpose being to refresh existing state. Thus, even if one such message is lost, the corresponding state will be refreshed during the next reporting period.

As opposed to Current State Reports, State Change Reports are retransmitted several times, in order to avoid them being missed by one or more multicast routers. The number of retransmissions depends on the so-called Robustness Variable. This variable allows tuning the protocol according to the expected packet loss on a link. If a link is expected to be lossy (e.g., a wireless connection), the value of the Robustness Variable may be increased. MLD is robust to (Robustness Variable)-1 packet losses. The RFC recommends a default value of 2 for the Robustness Variable.

If more changes to the same per-interface state entry occur before all the retransmissions of the State Change Report for the first change have completed, each additional change triggers the immediate transmission of a new State Change Report. Retransmissions of the new State Change Report will be scheduled as well in order to ensure that each instance of state change is transmitted at least (Robustness Variable) times.

If a node on a link expresses, through a State Change Report, its desire to no longer listen to a particular multicast address (or source), the Querier must query for other listeners of the multicast address (or source) before deleting the multicast address (or source) from its Multicast Address Listener state and stopping the corresponding traffic. Thus, the Querier sends a Multicast Address-Specific Query to verify whether there are nodes still listening to a specified multicast address or not. Similarly, the Querier sends a Multicast Address and Source Specific Query to verify whether, for a specified multicast address, there are nodes still listening to a specific set of sources, or not.

Both Multicast Address Specific Queries and Multicast Address and Source Specific Queries are only sent in response to State Change Reports, never in response to Current State Reports. This distinction between the two types of

reports is needed to avoid the router treating all Multicast Listener Reports as potential changes in state. By doing so, the fast leave mechanism of MLDv2 might not be effective if a State Change Report is lost, and only the following Current State Report is received by the router. Nevertheless, it avoids an increased processing at the router and it reduces the MLD traffic on the link.

Nodes respond to the above queries through Current State Reports, that contain their per-interface Multicast Address Listening state only for the multicast addresses (or sources) being queried.

As stated earlier, in order to ensure protocol robustness, all the queries, except the periodical General Queries, are retransmitted several times within a given time interval. The number of retransmissions depends on the Robustness Variable. If, while scheduling new queries, there are pending queries to be retransmitted for the same multicast address, the new queries and the pending queries have to be merged. In addition, host reports received for a multicast address with pending queries may affect the contents of those queries.

Protocol robustness is also enhanced through the use of the S flag (Suppress Router-Side Processing). As described above, when a Multicast Address Specific or a Multicast Address and Source Specific Query is sent by the Querier, a number of retransmissions of the query are scheduled. In the original (first) query, the S flag is clear. When the Querier sends this query, it lowers the timers for the concerned multicast address (or source) to a given value; similarly, any non-querier multicast router that receives the query lowers its timers in the same way. Nevertheless, while waiting for the next scheduled queries to be sent, the Querier may receive a report that updates the timers. The scheduled queries still have to be sent in order to ensure that a non-querier router keeps its state synchronized with the current Querier (the non-querier router might have missed the first query). Nevertheless, the timers should not be lowered again, as a valid answer was already received. Therefore, in subsequent queries, the Querier sets the S flag.

Building Multicast Address Listener State on Multicast Routers Multicast routers that implement MLDv2 (whether they are in Querier state or not) keep state per multicast address per attached link. This multicast address listener state consists of a Filter Mode, a Filter Timer, and a Source List, with a timer associated to each source from the list. The Filter Mode is used to summarize the total listening state of a multicast address to a minimum set, such that all nodes' listening states are respected. The Filter Mode may change in response to the reception of particular types of report messages, or when certain timer conditions occur.

A router is in INCLUDE mode for a specific multicast address on a given interface if all the listeners on the link interested in that address are in INCLUDE mode. The router state is represented through the notation INCLUDE (A), where A is a list of sources, called the "Include List." The Include List is the set of sources that one or more listeners on the link have

requested to receive. All the sources from the Include List will be forwarded by the router. Any other source that is not in the Include List will be blocked by the router.

A source can be added to the current Include List if a listener in INCLUDE mode sends a Current State or a State Change Report that includes that source. Each source from the Include List is associated with a source timer that is updated whenever a listener in INCLUDE mode sends a report that confirms its interest in that specific source. If the timer of a source from the Include List expires, the source is deleted from the Include List.

Besides this “soft leave” mechanism, there is also a “fast leave” scheme in MLDv2; it is also based on the use of source timers. When a node in INCLUDE mode expresses its desire to stop listening to a specific source, all the multicast routers on the link lower their timers for that source to a given value. The Querier then sends a Multicast Address and Source Specific Query, to verify whether there are other listeners for that source on the link or not. If a report that includes this source is received before the timer expiration, all the multicast routers on the link update the source timer. If not, the source is deleted from the Include List.

A router is in EXCLUDE mode for a specific multicast address on a given interface if there is at least one listener in EXCLUDE mode for that address on the link. When the first report is received from such a listener, the router sets the Filter Timer that corresponds to that address. This timer is reset each time an EXCLUDE mode listener confirms its listening state through a Current State Report. The timer is also updated when a listener, formerly in INCLUDE mode, announces its filter mode change through a State Change Report message. If the Filter Timer expires, it means that there are no more listeners in EXCLUDE mode on the link. In this case, the router switches back to INCLUDE mode for that multicast address.

When the router is in EXCLUDE mode, the router state is represented by the notation EXCLUDE (X,Y), where X is called the “Requested List” and Y is called the “Exclude List.” All sources, except those from the Exclude List, will be forwarded by the router. The Requested List has no effect on forwarding. Nevertheless, the router has to maintain the Requested List for two reasons:

1. To keep track of sources that listeners in INCLUDE mode listen to. This is necessary to assure a seamless transition of the router to INCLUDE mode, when there is no listener in EXCLUDE mode left. This transition should not interrupt the flow of traffic to listeners in INCLUDE mode for that multicast address. Therefore, at the time of the transition, the Requested List should contain the set of sources that nodes in INCLUDE mode have explicitly requested.

When the router switches to INCLUDE mode, the sources in the Requested List are moved to the Include List, and the Exclude List is deleted. Before switching, the Requested List can contain an inexact

guess of the sources listeners in INCLUDE mode listen to—might be too large or too small. These inexactitudes are due to the fact that the Requested List is also used for fast blocking purposes, as described below. If such a fast blocking is required, some sources may be deleted from the Requested List in order to reduce router state. Nevertheless, in each such case, the Filter Timer is updated as well. Therefore, listeners in INCLUDE mode will have enough time before an eventual switching to reconfirm their interest in the eliminated source(s) and rebuild the Requested List accordingly. The protocol ensures that when a switch to INCLUDE mode occurs, the Requested List will be accurate.

2. To allow the fast blocking of previously unblocked sources. If the router receives a report that contains such a request, the concerned sources are added to the Requested List. Their timers are set to a given small value, and a Multicast Address and Source Specific Query is sent by the Querier, to check whether there are nodes on the link still interested in those sources, or not. If no node announces its interest in receiving those specific source, the timers of those sources expire. Then, the sources are moved from the Requested List to the Exclude List. From then on, the sources will be blocked by the router.

4.7.7 Source Filtering

What follows is a brief discussion of Source Filtering based on RFC 4604. The term “Source Filtering GMP (SFGMP)” is used to refer jointly to the IGMPv3 and MLDv2 group management protocols. The use of source-specific multicast is facilitated by small changes to the SFGMP protocols on both hosts and routers. SSM defines general requirements that must be followed by systems that implement the SSM service model; this document defines the concrete application of those requirements to systems that implement IGMPv3 and MLDv2. In doing so, RFC 4604 defines modifications to the host and router portions of IGMPv3 and MLDv2 for use with SSM, and presents a number of clarifications to their behavior when used with SSM addresses. RFC 4604 updates the IGMPv3 and MLDv2 specifications.

One should note that SSM can be used by any host that supports source filtering APIs and whose operating system supports the appropriate SFGMP. The SFGMP modifications described in RFC 4604 make SSM work better on an SSM-aware host (but they are not strict prerequisites for the use of SSM.)

The 232/8 IPv4 address range is currently allocated for SSM by IANA. In IPv6, the FF3x::/32 range (where “x” is a valid IPv6 multicast scope value) is reserved for SSM semantics, although today SSM allocations are restricted to FF3x::/96.

A host that knows the SSM address range and is capable of applying SSM semantics to it is described as an “SSM-aware” host. A host or router may be configured to apply SSM semantics to addresses other than those in the IANA-allocated range. The GMP module on a host or router should have a

configuration option to set the SSM address range(s). If this configuration option exists, it must default to the IANA-allocated SSM range.

If the host IP module of an SSM-aware host receives a nonsource-specific request to receive multicast traffic sent to an SSM destination address, it should return an error to the application. On a non-SSM-aware host, an application that uses the wrong API (e.g., “join(G),” “IPMulticastListen(G,EXCL UDE(S1))” for IGMPv3, or “IPv6MulticastListen(G,EXCLUDE(S2))” for MLDv2) to request the delivery of packets sent to an SSM address will not receive the requested service, because an SSM-aware router (following the rules of this document) will refuse to process the request, and the application will receive no indication other than a failure to receive the requested traffic.

RFC 4604 documents the behavior of an SSM-aware host with respect to sending and receiving the following GMP message types:

- IGMPv1/v2 and MLDv1 Reports
- IGMPv3 and MLDv2 Reports
- IGMPv1 Queries, IGMPv2 and MLDv1 General Queries
- IGMPv2 Leave and MLDv1 Done
- IGMPv2 and MLDv1 Group-Specific Query
- IGMPv3 and MLDv2 Group-Specific Query
- IGMPv3 and MLDv2 Group- and Source-Specific Query

REFERENCES

- [CIS201101] Cisco Systems, “Implementing IPv6 Multicast, White Papers” Cisco Systems, Inc., 170 West Tasman Dr., San Jose, CA 95134, USA, March 25, 2011.
- [DEE199901] W. Deering, B. Fenner, “Haberman, Multicast Listener Discovery (MLD) for IPv6,” RFC 2710, October 1999, Updated by: RFC 3590, RFC 3810. Copyright (C) The Internet Society (1999). All Rights Reserved. This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works.
- [NIS201101] H. Nishimoto, “ITU-T IPTV-GSI, Workshop on Harmonization of Web and IPTV Technologies,” Overview of ITU-T H.721 Recommendation for IPTV Terminal Device, Rio de Janeiro, Brazil, July 21, 2011.

5 Evolving Traditional and Nontraditional TV Services

We have made note in Chapter 1 that consumers are increasingly interested in Nontraditional TV (NTTV) services, which include time-shifted TV (TSTV) and Internet-based TV (IBTV). A broadcast service is generally known as a *linear TV service*, and an on-demand service is also known as a *nonlinear TV service*. These services can be delivered over cable systems, satellite systems, various access vehicles to the Internet, and Internet Protocol TV (IPTV) systems.

This chapter reviews the basic TV/video services, both existing and evolving, that are of purported interest to consumers, while the chapters that follow focus on the requisite infrastructure. This discussion is based on the framework presented in ITU H.720, “*Overview of IPTV terminal devices and end-systems*” [ITU200801]. Distributed video content services include broadcast services, on-demand services, time-shifting and place-shifting services, supplementary content, and advertising services. Interactive services include information services, entertainment services, commerce services, interactive advertising, portal services, learning services, medical services, and monitoring services. Others services include public interest services, presence services, session mobility services, and hosting services. The discussion below takes a service provider perspective, but such provider perspective is based on documented consumer trends and on the desire on the part of the providers to meet consumer demand. The gamut of services and capabilities discussed in this chapter is not exhaustive, but is representative.

5.1 BASIC SERVICES

Of the many video services that have evolved and are evolving, the following are generally considered to be the most basic services for a provider, including an IPTV provider: broadcast services, on-demand services, portal services, and public interest services. These are discussed next.

5.1.1 Distributed Content Service

Linear TV Linear TV is a broadcast TV service that is the same as the classic form of television services provided by terrestrial, cable, and direct-to-the-home satellite broadcasting operators, where the program content is transmitted to a large universe of potential users according to a defined schedule controlled by the operator (not by the recipient), and is intended for real-time display by the end user. The service provides a continuous stream of (digital) video emanating from the content provider and received by the terminal device located in the end-user network. Linear TV includes (but is not limited to) the following approaches:

- *Audio and Video*: Audio and video (audiovisual) signals are broadcast and distributed to the downlink without end-user control of the content flow (e.g., without trick mode).
- *Audio Only*: Audio signals are broadcast and distributed to the downlink without end-user control of the content flow (e.g., without trick mode).
- *Linear TV with Audio, Video, and Data*: These audiovisual services are combined with interactive data for related or supplementary information of audiovisual programs using bidirectional links. The end user can watch the downlink audiovisual stream and can simultaneously access more detailed or value-added information via the uplink.

A terminal device (for example, an IPTV terminal device [IPTV TD]) is part of end-use equipment that supports end-user function(s) associated with (1) receiving and responding to network control channel messages regarding session setup, maintenance, and tear-down, and (2) receiving the content of an IP transport from the network and rendering the content on the display unit. A set-top box (STB) is an example of a terminal device. This equipment may be a standalone element, or it may be integrated in other home video equipment, for example, integrated inside a TV panel.

Service Navigation Service Navigation (SN) is mechanism for presenting information that allows the end-user to discover, select, and consume services; without service navigation, it is difficult, if not impossible, to obtain services. A typical means of service navigation is by way of a service navigation application; this is a user interface application that is intended to provide information on available services, including content that may be accessed by end-users for service navigation. Examples of service navigation applications include Electronic Program Guide (EPG), Interactive Program Guide (IPG), Electronic Content Guide (ECG), and Electronic Service Guide (ESG). While service navigation is “useful” for Linear TV, it is indispensable for other forms of evolving video services.

An EPG contains information about future programs; it generally includes the title and genre of the program, a short description of the episode, the start

time, the duration, and other data. The time horizon is 1–2 weeks. ECGs typically describe the content of local storage, including relevant information, such as title and genre of the program, the duration, and other data. An IPG typically allows the user to (1) browse listings by program title, channel or theme; (2) scan current and future programs on other channels without leaving the current program; (3) purchase Pay Per View (PPV) events; (4) start recording a program; (5) set parental controls; (6) set up a “favorites” channel list; and (7) undertake other related tasks.

Formally, an ESG is a capability used to signal the services that are available, how they can be received, and what they contain. Service discovery and purchase of services is based on information transmitted in the ESG. For each service and program, the ESG contains all the necessary information for making a purchase and for the device to find services and programs. Practitioners consider ESG as more general form of an EPG, namely, ESG encompasses more abstract concepts of “Service and Content” beyond just a TV channel. For example, in addition to TV channels, and ESG can describe a radio channel, a Video On Demand (VoD) service (also known as Content On Demand [CoD]), a data services (e.g., stock quotes and news items). As a special case, an EPG is an ESG, where services are TV channels, contents are TV programs, and bundles are bouquets of channels. The ESG enables the user to select and acquire content. The EPG can be used to purchase a Service Bundle (a group of services composed respectively offered by a single party). ESGs are also used in mobile environments.

Content On Demand Content on demand enables an end user to select, acquire, and display video from a library of content stored on a remote or local server.

5.1.2 Interactive Services

As noted in Chapter 1, new video display systems terminal have the ability to communicate with a remote interactive content server using Internet-based protocols, such as Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS). Examples of interactive services are information services, learning services, and entertainment services. Client-side interactive services include video and traditional Internet web access. Interactive services may also include service provider-specific customer services, such as subscription, PPV, among others.

Information Services Information services support various types of content, such as news, weather and traffic forecasts, transportation, local community, among others.

Learning Services Learning services are instructional services for delivering educational content to students who are physically located in different geographic areas in a real-time and/or nonreal-time manner.

Entertainment Services Entertainment services are designed to provide content such as games, karaoke, lottery, blogs, and photo albums for the purpose of providing end user's entertainment.

5.1.3 Public Interest Services

Some examples of community and accessibility services that may be required by the local customer-base or regulations include the ones listed next.

Emergency Alert System (EAS) Next-generation video services, including IPTV, may be required to be compliant with regulatory requirements for emergency alerts. The terminal notifies the user of an incoming emergency alert notification (EAN) message both visually and audibly, or according to the user's preferences and capabilities, if specified.

Closed Captions, Subtitles, Audio Description, and Sign Language Interpretation These features may be provided along with the above-mentioned basic services.

- *Closed Captions and Subtitles:* These services provide a real-time on-screen transcript of dialogue. Subtitles may be in different languages for the purposes of language translation. Captions for hearing-impaired people are in the same language.
- *Audio Description:* Primarily intended to assist end-users who are unable to see the video content clearly. This service provides a commentary describing the visual events pertinent to the content.
- *Sign Language Interpretation:* This service provides supplementary video, usually smaller in image size to that of the main video content, showing an interpreter who uses hand gestures and facial expressions to convey the main audio content to sign language and lip readers.

5.2 ADVANCED SERVICES

More advanced features of a full-fledged next-generation video services provide some or all of the following services:

- linear TV with trick mode;
- personal video recorder (PVR) services;
 - client PVR (cPVR);
 - network PVR (nPVR); and
 - distributed PVR (dPVR);
- advertising services;
- audience measurement information;

- interactive services requiring high security; and
- personal broadcast.

5.2.1 Linear TV with Trick Mode

Linear TV with trick mode enables the end-user to pause linear TV. For the ability to skip content and for other capabilities (e.g., instant replay), the use of a PVR is required. A PVR provides the capability of an end user-controlled electronic device that records linear TV and stores it in a digital storage facility, either in standalone STBs or in the network. This capability can support “time-shifting,” “trick modes.” Next-generation video services terminal devices (including IPTV systems) should have the following capabilities:

- provide an interface for the user to access the contents without time limitations, including pause, rewind, fast forward, and so on;
- provide an interface for the user to enable or disable the service of TV with trick mode; and
- provide an interface to set the expiration time.

5.2.2 Personal Video Recorder (PVR) Services

STBs and IPTV TDs are increasingly capable of supporting PVR, enabling end users to retrieve and playback content at will. An intuitive graphical user interface (GUI) is usually supported. PVR services can include the following capabilities:

- schedule recordings;
- display a list of stored programs/content and a list of upcoming recordings;
- rank recordings according to priority;
- playback/erase stored programs/content; and
- copy stored programs/content to removable or external local storage devices.

Such services are required to ensure that copyright enforcement mechanisms are preserved. Relevant security issues should be taken into account. Advanced PVRs support personal channel services at the PVR. In such services, the PVR generates the end user’s own preview schedule customized according to his/her preferences.

Client PVR (cPVR) In the case of client PVR, the STB or IPTV terminal contains (or is directly connected to) a storage buffer, such as a hard disk drive, removable media, or solid state memory (e.g., flash RAM). The end-user can interact with the GUI in order to schedule, modify, playback, erase, and locate recordings.

Network PVR (nPVR) There are cases where it is not appropriate to save the content locally. One example is where the IPTV terminal is a PDA with limited size of hard drive, in which case a network PVR is more appropriate. The design is such that the end user is not ostensibly able to recognize any difference between using cPVR or nPVR. The PVR service should function identically, the only difference being the location of the storage device.

Distributed PVR (dPVR) In the distributed PVR case, all content is stored within the home network on multiple cPVRs or on a combination of multiple nPVRs and cPVRs, with interaction being done in order to schedule, modify, playback, erase, and record. The home network is the collection of elements that process, manage, transport, and store information, thus enabling the connection and integration of multiple computing, control, monitoring, communication and entertainment devices in the home. For examples, an IPTV TD could store an end user's content on a nPVR when the cPVR's disk, which is mainly used, is full. The end user should not be able to perceive the difference between the cPVR, nPVR, or dPVR. The PVR service should function identically, with the only difference being the location or distribution of the storage device(s).

See Figure 5.1 for a graphical illustration. In this example, the “primary IPTV-TD” implements the PVR service. The content may be stored in the primary IPTV-TD or other device in combination with one or more cPVRs (connected to the home network) or nPVRs (network storage in the IPTV network), or may be stored in one or more cPVRs or nPVRs entirely, without storing anything in the primary IPTV-Terminal Device (the STB).

5.2.3 Advertising Services

Traditional advertising consists of broadcasting commercial advertising or public promotion of goods, services, and companies. End users located in a

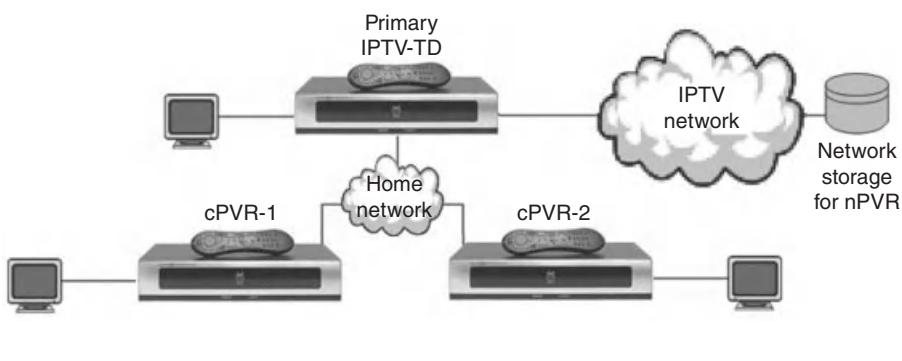


FIGURE 5.1 Distributed PVR. IPTV-TD, IPTV Terminal Device (e.g., STB).

certain region will receive the same advertisements, which are usually inserted in audiovisual programs. STBs are now typically capable of supporting new advertising services. Some of these services are listed next.

Targeted Advertising Targeted advertising can be defined as automatically matching and delivering relevant content to the end users according to certain campaign objectives. Targeted advertising usually takes advantage of the end user's profile, including user preferences, residence, usage history, personal characteristics (e.g., accessibility), and usage environments (terminals, networks and natural environmental characteristics, and so on). Advanced PVR can have a capability for selective playback and recording of advertisement content according to the end user's preferences and other attributes.

On-Demand Advertising On-demand advertising delivers directory information of business so that the end-user can select and navigate through additional information or get additional services and benefits, such as coupons. This type of advertisement is also called an “interactive advertisement.”

5.2.4 Audience Measurement Information

Audience measurement information is used for the end user's convenience when watching video (IPTV) content. For example, advertisement services can refer to this information to provide appropriate advertisement. The information consists of the channel numbers before and after a channel change, time of the change and user information (e.g., a unique identifier). With the end-user's permission, information can be collected by the STB, and the IPTV network can be used to upload the collected information to the relevant server-side applications.

5.2.5 Interactive Services Requiring High Security

Interactive services requiring tight security enable end-users to send various types of requests and receive feedback with high security and reliability. Examples of interactive services requiring high security are commerce and medical services.

Commerce Services Commerce services enable the end user to purchase goods and use financial services, such as banking, stocks, shopping, ticketing, auctions, among others.

Medical Services Medical services provide connections between doctors and patients who are in different geographic areas. Doctors can perform health monitoring, remote diagnosis, remote consultation, remote medical examinations, medical education, among others.

Personal Broadcast Personal broadcast services provide the end-user with a way to advertise personal content (possibly including scheduling information) so that other end users can access such content. This service makes the IPTV end user a content provider. For a personal IPTV broadcast scenario, the IPTV TD can play a role as the content source or the delivery function. Some portion of the following capabilities is needed within the IPTV TD or other device in order to support a service, such as:

- Audiovisual capturing/encoding.
- Supporting protocols for transmission of content (e.g., RTP/RTCP).
- Security aspects associated with broadcasting of customer-generated content.

REFERENCE

[ITU200801] International Telecommunication Union, H.720. “Overview of IPTV terminal devices and end-systems,” (also known as ex H.IPTV-TDES.0), October 2008. ITU-T Study Group 16. International Telecommunication Union, Telecommunication Standardization Bureau, Place des Nations, CH-1211 Geneva 20.

6 IPTV Systems and Technologies

This chapter provides a short overview of Internet Protocol TV (IPTV). IPTV systems enable service providers to offer basic and value-added services such as traditional (linear) TV, nonlinear TV, video/content on demand (VoD/CoD), Nontraditional TV (NTTV), and interactive TV over IP-based managed (e.g., single-provider) networks; some of these services were described in Chapter 5. IP Multicast is the basis for IPTV: currently, IPv4 is used extensively; however, as time progresses and as the population of users and/or the number multicast groups grows, IPv6 will increasingly become the transport engine for IPTV. While there also are other approaches that can be utilized to deliver the linear and nonlinear TV services discussed in this book (e.g., peer-to-peer technology may also be used), IPTV is a key standardized technology that is available for use, especially by large (wireline and wireless) telecom providers that have significant IP assets in their networks.

Issues related to requirements, architecture, and interoperability are discussed in the chapter. Interoperability, and, therefore, open standards, is important to the successful, large-scale deployment of the technology. Hence, in addition to architectural considerations, some of the newly published International Telecommunications Union, Telecommunication Standardization Bureau (ITU-T) IPTV standards, including ITU-T H.701 (Error Recovery), ITU-T H.721 (IPTV Terminal), ITU-T H.740 (Application Event Handling), ITU-T H.750 (Metadata), ITU-T H.761 (Ginga-NCL), ITU-T H.762 (Light-weight Interactive Multimedia Framework for IPTV Services [LIME]), and ITU-T H.770 (Service Discovery) are assessed. Some discussion related to Quality of Service (QoS), performance, service security, content protection, and middleware is included. The reader should be able to see the applicability of IPv6 Multicast at various points in this discussion; a number of evolving ITU-T standards (including H.721), in fact, support IPv6 Multicast. As noted in Chapter 1, multicast is ideal for linear video distribution but is not by itself ideal for VoD; hence, a service provider should plan to support (IPv6) multicast for linear TV and (IPv6) unicast for nonlinear TV (including VoD).

Distribution of entertainment-quality video over packet networks is not a totally new technology. Considerable amount of work was undertaken by the (U.S.) Regional Bell Operating Companies in the early-to-mid 1990s to provide

such video services over Asynchronous Transfer Mode (ATM) networks [MIN199501]. While the transport fabric has now been changed from connection-oriented ATM to connectionless IP because of cost considerations, many of the fundamental elements of the systems under study in the 1990s have carried forward into the IPTV systems of the current day.

6.1 OVERVIEW AND STAKEHOLDER UNIVERSE

6.1.1 Definitions

The following background observations on evolving video services were recently made by the ITU-T [ITU200801]:

The focus of much of ITU-T's ongoing standards-making activities on Next-Generation Networks (NGNs) is essential to meet the needs of the information-driven society. In the context of NGN we see the attractive promise of IPTV to generate multiple revenue streams over the same core network. Indeed, IPTV is one of the most highly visible applications to emerge as part of work on the NGN, because it is aimed at consumer entertainment markets. IPTV underlies "multiple play", whereby service providers can offer bundled voice, video on-demand, TV, high-speed Internet and other entertainment and communication services over the same basic network. This creates a compelling business case that is one of the principal drivers for accelerated deployment of NGNs.

This author previously defined IPTV as "approaches, technologies, and protocols to deliver commercial-grade Standard Definition (SD) and High Definition (HD) entertainment-quality real-time linear and on-demand video content over IP-based networks, while meeting all prerequisite QoS, Quality of Experience (QoE), Conditional Access (CA) (for security), Blackout Management (for sporting events), Emergency Alert System (AES), Closed Captions, Parental Controls, Nielsen Rating collection, Secondary Audio channel, Picture-in-Picture, and Electronic Program Guide (EPG) data requirements of the content providers and/or regulatory entities" [MIN200801]. The ITU-T defines IPTV as "Multimedia services such as television/video/audio/text/graphics/data delivered over IP-based networks managed to support the required level of QoS/QoE, security, interactivity and reliability" [ITU200801]. The Alliances for Telecommunications Industry Solutions (ATIS) IPTV Interoperability Forum (IIF) describes IPTV as follows [IIF200801]: "... a collection of video and related services primarily delivered to consumers for entertainment purposes. These services may include live broadcast video, CoD, and interactive TV (iTV) services. In contrast to video over the public Internet, with IPTV deployments, network security and performance are closely managed to help ensure a superior entertainment experience, resulting in a compelling business environment for content providers, advertisers, and customers alike. These services are delivered across an access-agnostic,

packet-switched network that employs the IP protocol to transport the audio and video signals.”

As just noted, IPTV is not to be confused with the simple delivery of video over an IP network and/or streaming, which have been possible for well over two decades and is typical of IBTV: IPTV supports all business, billing, provisioning, and content protection requirements that are associated with fee-based commercial video distribution. Typically, IPTV makes use of Moving Pictures Expert Group 4 (MPEG-4) encoding with the goal of giving the consumer the ability to select from 200 to 300 SD channels and 40 to 80 HD channels or more.¹ Service is expected to be comparable with that received over Cable TV or Direct Broadcast Satellite (DBS). Viewers need to be able to switch channels within 1 second or less. Also, the need exists to simultaneously support multiple active set-top boxes (STBs), each simultaneously processing distinct programming (say 2–4 streams) within a single domicile. Make note that various forms of NTTV and IBTV may utilize IP technology for content delivery; however, IPTV is a specific “carrier-grade” architecture intended to support “broadcast quality” delivery of real-time and VoD/CoD² content, along with other value-added services. Such a managed IP network can also be seen as a dedicated Content Delivery Network (CDN), although the latter usually also included distributed cache servers (which may or may not be present in a “pure” IPTV environment.)

The list that follows represents an IPTV concept classification that can be utilized to highlight the key areas of technical focus required for commercial deployment of the technology (which we follow in this chapter):

Architecture and Requirements

- IPTV services
- IPTV architecture

QoS and Performance Aspects

- Quality of experience requirements for IPTV
- Traffic management mechanisms for the support of IPTV services
- Application layer reliability error recovery mechanisms for IPTV
- Performance monitoring for IPTV

Service Security and Content Protection

- IPTV security aspects

¹This mix of channels will change over time in favor of HD-based content.

²Some define CoD as delivery of an offering, packaged in a media format, anywhere, anytime via a network; variants include audio on demand and video on demand.

IPTV Networks

IPTV multicast frameworks
IPTV network control aspects

End Systems and Interoperability Aspects

Aspects of IPTV end system—terminal device
Aspects of home network supporting IPTV services

Middleware, Application, and Content Platforms

IPTV middleware, application, and content platforms
IPTV middleware
IPTV metadata
Standards for IPTV multimedia application platforms

6.1.2 Services under Consideration

Basic services to be supported by any IPTV system include the following:

1. Linear TV service (a television service in which a continuous stream flows in real time from the service provider to the terminal device and where the user cannot control the temporal order in which contents are viewed).
 - (a) Multicast delivery
 - (b) Programs on temporal order
 - (c) Includes IP retransmission of Terrestrial and Satellite Broadcasting
2. Time Shifted TV (TSTV)/VoD Service (a service in which the end user can, on demand, store [for TSTV] or access prestored [for VoD] content, and then select and view a video content; the end user can control the temporal order in which the video content is viewed, namely, the end user has the ability to start the viewing, pause, fast forward, rewind, variable playback speed).
 - (a) Unicast delivery (when using network-based DVR/nPVR and/or VoD).
 - (b) For TSTV, the contents is stored/served by end-user's choice; the user has choice on (1) recoding time of Linear TV; (2) Linear TV content; (3) playback time; and (4) tricks (controls).
 - (c) For VoD, the contents is served by end user's choice; the user has choice on (1) content choice (from a library); (2) playback time; and (3) tricks (controls).

A more complete set of proposed IPTV services includes the following (some of these were also discussed in Chapter 5):

- Linear/Broadcast TV (audio, video, and data)
- Linear Broadcast TV with Trick Modes
- TSTV
- Pay Per View (PPV)
- Video/TV/Content On Demand (VoD/CoD)
 - Near VoD/broadcasting
 - Real VoD
- Download-based video content distribution services (Push VoD)
- Content download service
- PVR service (network or client-based)
- Interactive TV (iTV)
- Consumer Originated content (video, audio, and applications)
- Consumer Originated broadcast TV (e.g., consumer-to-consumer hosting)
- User-specific advertising
- Third-party content services
- Linear Broadcast Audio
- MoD (Music On Demand) including audio book
- T-learning (television learning) (education for children, elementary, middle and high school student, languages and estate, and so on)
- 3DTV
- Multi-angle TV service
- Games
- T-information (television information) (news, weather, traffic and advertisement, etc.)
- T-commerce (television commerce) (security, banking, stock, shopping, auction and ordered delivery, and so on)
- T-communication (television communication) (e-mail, instant messaging, SMS, channel chatting, Voice over IP (VoIP), Web access, multiple video conference and video phone, etc.)
- T-entertainment (television entertainment) (photo album, games, karaoke and blog, etc.)
- Presence service
- Communications messaging
- Service Information (EPG: Electronic Program Guide, ECG: Electronic Content Guide, etc.)
- Portal services
- Hybrid services

The services at the top of this list are more fundamental to the commercial IPTV portfolio, at least for the initial set of deployments. Building on this generic list Table 6.1 provides a description of the commercially practical

TABLE 6.1 IPTV Services as Defined by the Open IPTV Forum

Service	Description
Scheduled Content Service (also known as broadcast or linear TV service)	An audio and video content service where the play-out schedule is fixed. The content is delivered to the user for immediate consumption or recording. Service and Content protection mechanisms may be applied to the content.
Content On Demand (CoD) also known as Video On Demand and including Content Download)	A service where a user can select individual content items they want to watch from a list of available content. Play-out of the content is started at the user's request. Content can be streamed from network-based storage for immediate consumption, or played out from the local storage of the IPTV Terminal Function (ITF) device after user or service provider initiated download to the ITF device. CoD service encompasses basic playout controls as well as additional capabilities (e.g., skipping to chapters, bookmarks, and jump to time). For download CoD services (e.g., Push CoD and Deferred Download CoD), there typically is a mechanism for the synchronization of content and its associated rights between a CoD service and the local ITF storage.
Personal Video Recorder (PVR) service	A service that enables a user to record scheduled content program events using local or network-based storage. The recorded items can be played back under the control of the user. The PVR service encompasses basic playout controls, as well as additional capabilities (e.g., skipping to chapters, bookmarks, and jump to time). In addition, an authorized user will be able to perform PVR scheduling and content management operations using devices such as mobile phones, PDAs, and so on, that are associated with the IPTV subscription. It will also be possible for a user to have these operations performed by the service provider on his/her behalf.
Time shift	A service that allows a user to halt a scheduled content service and continue watching the program later, by providing buffering for pause, rewind, and resume. One can supports time shift using local IPTV ITF storage. There is also support of network storage for the time shift service, and extends basic playout controls with additional capabilities (e.g., skipping to chapters, bookmarks, and jump to time).

TABLE 6.1 (*Continued*)

Service	Description
Content Guide	An information service tailored to user preferences that provides a searchable list of Scheduled Content Service and CoD items. The presentation to the user can be created from metadata available on local equipment or received over the network in a form equivalent to web pages. The basic capabilities of the Content Guide are often complemented to enable the user to access information about his recorded content (e.g., availability locally or on the network, and the length of availability) through the Content Guide. The Content Guide can also be enhanced with search capabilities, so as to allow a user to search by content, genre, actor, and so on. In addition, the Service Provider will be able to use the Content Guide to alert the user of the availability of new services.
Notification service	A service that enables a user to be informed of delivered messages, including emergency alert notifications, and events. This service also enables a user to set reminders and be informed of scheduled content program events. Reminder notifications will be displayed on the customer equipment at the preconfigured time before the program event starts. There typically is support for emergency notifications. Users will also be able to receive notification (e.g., the start of a program) on devices associated with their subscription (e.g., mobile phones) when outside the home network. Notifications can be prioritized appropriately by the service provider, and, if needed, their delivery guaranteed. Notifications can be filtered based on user preferences or targeted to specific or groups of users by the service provider.
Integration with communication services	A service that provides IPTV users with access to person-to-person communication services. Aspects of such communication services may be integrated with the IPTV service, providing a richer experience to both. Examples of communication services include presentation of Caller ID, textual messaging, chatting and presence, integration of IPTV with voice and video telephony, that is, the establishment and management of voice and video telephony, the ability to deliver different components of the media stream to different devices, and additional enhancements to presence and chat/messaging.

(Continued)

TABLE 6.1 (*Continued*)

Service	Description
Web access	A service that allows IPTV users to navigate and display information provided in the World Wide Web in a manner dependent upon the presentation capabilities of the display equipment. It may include mechanisms to filter web content based on criteria set by an authorized user (e.g., a parent for children in a household).
Information service	Portal for presenting tailored information to the IPTV user with or without relation to the content.
Interactive applications	Interactive applications are those that allow user interaction via the IPTV ITF device or other user devices. Both network-based applications that interact with the ITF device using web technologies, as well as local applications in the home network are supported. The applications can be both related and unrelated to the content. Applications might interact with the IPTV services using standardized APIs. Applications might be authenticated to prevent misuse and the service provider might charge for applications.
Parental control including remote control	This service limits access by minors to certain content and services based on parental ratings and spending limits. Parents should be capable of using remote devices to check the usage and grant access to requested items.
Home networking	The ITF device provides access to Digital Living Network Alliance (DLNA ^a) content stored on other devices in the home, as well as offering IPTV content to DLNA devices.
Remote access	A service that provides access to the home via a remote device (e.g., a mobile phone), enabling a user to, for example, schedule recordings or access content stored within the home.
Support of hybrid services	The ITF device may provide access to TV services delivered over traditional broadcast networks (satellite, cable, or terrestrial broadcast) in addition to, or as a substitute for, IPTV services. For example, an application (e.g., a presence application) to receive status information (e.g., watched content) from the broadcast stream, or receive a notification of the availability of an interactive application via the broadcast stream, may be supported.

TABLE 6.1 (Continued)

Service	Description
Personalized channel service	A service that provides a variation of a scheduled content service where the program line up is modified on a per user basis according to the user's preferences, viewing habits, or service provider recommendations. This will be reflected in the user's Content Guide.
Digital media purchase	Digital media relates to content items, such as ring tones and video clips, that can be purchased by users.
Content sharing	Content sharing allows a user, when allowed by DRM policies, to share content with other users.

^a Digital Living Network Alliance (DLNA) is, according to their materials, a cross-industry organization of leading consumer electronics, computing industry, and mobile device companies. They focus on wired and wireless network of interoperable Consumer Electronics (CE), personal computers (PC), and mobile devices in the home and on the road, enabling a seamless environment for sharing and growing new digital media and content services. DLNA is focused on delivering interoperability guidelines based on open industry standards to complete the cross-industry digital convergence. DLNA has published a common set of industry design guidelines that allow manufacturers to participate in a growing marketplace of networked devices, leading to more innovation, simplicity, and value for consumers. The DLNA Networked Device Interoperability Guidelines are use case driven and specify the interoperable building blocks that are available to build platforms and software infrastructure. These guidelines also focus on interoperability between the devices for personal media uses involving imaging, audio, and video. In the DLNA digital home, it will be common for consumers to:

- easily acquire, store and access digital music from almost anywhere in the home;
- effortlessly manage, view, print and share digital photos;
- carry favorite content anywhere to enjoy while on the road; and
- enjoy distributed, multi-user content recording and playback.

services generally available at press time, as defined by the Open IPTV Forum (OIPF) [OIP200801].

Proposed IPTV business/commercial models include the ones listed below, but other models and/or combinations of these may be possible:

- *Free*: A viewer can watch IPTV service or use it without paying for it (this is not the typical arrangement.)
- *Subscription*: A viewer pays an amount of money regularly in order to watch or use IPTV service (this is the typical arrangement.)
- *Pay Per View (PPV)/Pay Per Use (PPU)*: A viewer can purchase each service, content, or application to be seen on TV at any time and pay for the only item he/she buys. That is, each service or content can be purchased using an on-screen guide, an automated telephone system, or through a live customer service representative (this is typical of VoD/CoD.)

- *A La Carte*: A viewer can buy whichever channels and contents he/she wants, and pay a price for each.
- *Package*: A viewer can select and use a set of products, such as VoD (including channel) and T-entertainment (including for example game, karaoke, and so forth), that are already organized (“packaged”) by the service provider. Then, pay for the set of products that he or she chooses.
- *Cash-Back Point*: A cash-back point is prepaid e-money or ticket for IPTV service. With these cash-back points, the user can pay the service fee in IPTV service domain as with real-money. Users can acquire the cash-back points by buying it with real money or accumulating bonus cash-back point that accrues in a particular rate when they use the IPTV service.

6.1.3 IPTV Stakeholder Universe

The overall end-to-end-system supporting IPTV services is typically comprised of a number of domains that may be designed, deployed, and operated by different providers. There are at least four communities of interest (see Figure 6.1):

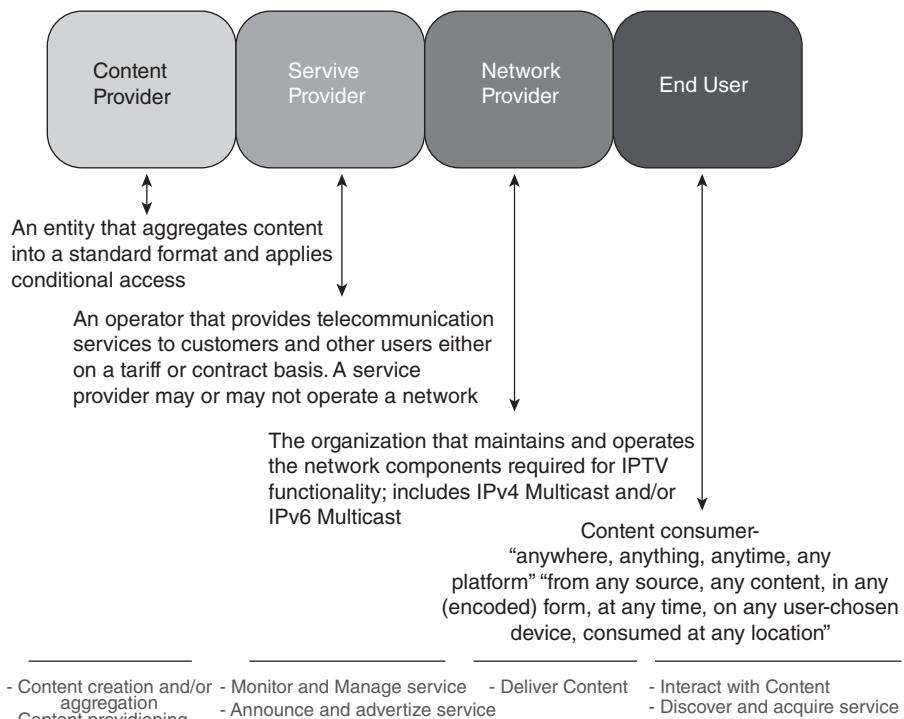


FIGURE 6.1 Main functional domains that are involved in the provision of an IPTV services.

- *Content Provider/Aggregator (CP)*: An entity that may produce content and/or aggregate content from multiple sources for general distribution. Typically (but not always), the entity adds CA: to protect content rights, the content provider encrypts the content before delivery to Service Provider.
- *Service Provider (SP)*: An operator that provides telecommunication services to customers and other users either on a tariff or contract basis. A service provider may or may not operate a network.
- *Network Provider (NP)*: The organization that maintains and operates the network components required for IPTV functionality. A network provider can optionally also act as service provider.
- *Content Receivers*: End users, consumers of content.

Figure 6.2 depicts an example of logical implementation of the architecture.

6.1.4 Market Scope

IPTV has been around for some time (at least since 2003) but up to the present it has not been the immediate commercial success that planners had originally hoped.³ IPTV reached about 50 million worldwide at the end of 2010 [CAM201101]. As we saw in Chapter 1, the 2010 U.S. IPTV population was about 7 million households; while the IPTV penetration held at around 5% share of total television households, the penetration was expected to reach 13% in 2013 with about 15 million households by then [HEY201001]. Figure 6.3 shows the worldwide deployment of new STBs in recent years, based on system technology [SCR201101]. Up to 2014, shipments of IPTV STBs are expected to remain flat around the 16 million units per year worldwide, and then increase to 18 million in 2015; growth is anticipated in China, and to a far lesser extent Latin America and Eastern Europe.

Beside general economic weakness, the other key reasons for this lack of full market impetus relate to the fact that so far, one has seen the deployment of closed, vendor-proprietary systems, with the ensuing consequence that the efficiencies of scale and the benefits of competition have not yet materialized; however, continued and accelerated commercial deployment is expected throughout the decade of the 2010s, as standards become available. Given the set of distinct service providers involved in IPTV video delivery, each fulfilling a different role, it follows that service and equipment interoperability are critical; in order to achieve such interoperability, it is important to have open standards that can facilitate end-to-end service delivery. Standards are key to the wide-scale deployment of IPTV because standards impact (in a beneficial way) the cost of products, the breath of market offerings, and the timeline for

³Worldwide penetration at press time is about half of what was originally forecast around 2006.

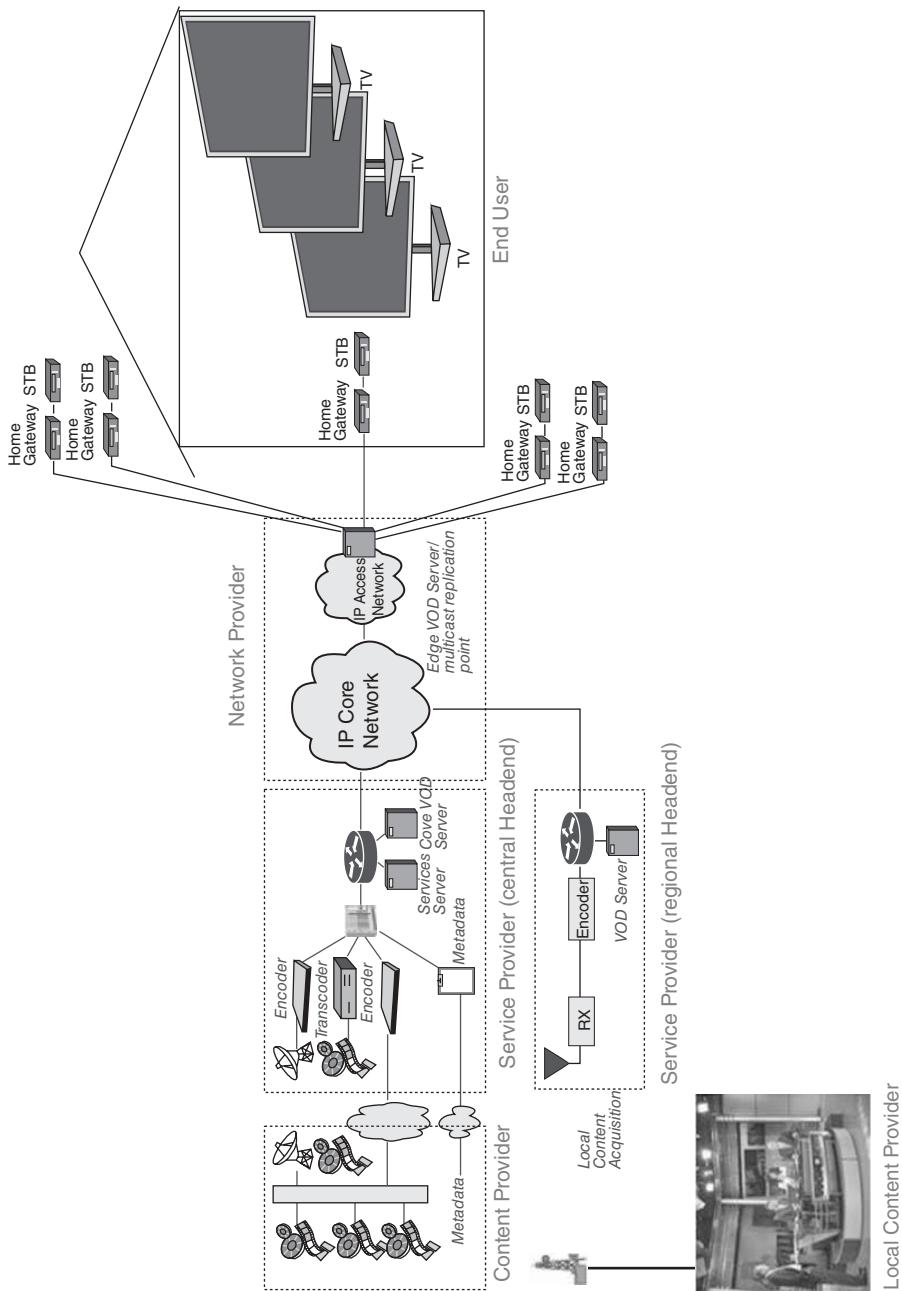


FIGURE 6.2 Example of IPTV implementation.

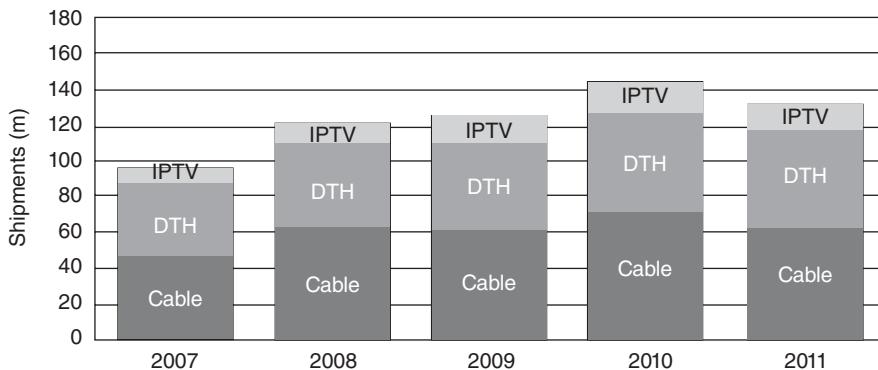


FIGURE 6.3 STB market worldwide.

service introduction by broadcasters, Internet Service Providers (ISPs), telecoms service providers, and/or content providers.

6.1.5 Multicast Mechanisms

IP multicast is routinely used for IPTV services. To provide the IPTV service, the NP must install multicast-capable routers in its IP network. As it might be expected, service delivery (specifically, QoS and QoE) depends on the design parameters of the IP multicast network. Each member registers on IP multicast groups by exchanging Internet Group Management Protocol (IGMP) and/or Multicast Listener Discovery (MLD) messages with its designated access router; the IP multicast router constructs the requisite IP multicast tree by exchanging multicast routing protocol messages; finally, data from source flow according to the multicast tree from source to each receivers.

Figure 6.4 depicts the IP multicast mechanism as applied to the IPTV service [ITU200801]. Here, the CP entrusts the SP to multicast content media (Step 1); the SP thus prepares the content media for multicasting to the announce group (Step 2). The consumer (IPTV client) exchanges signaling with SP's IPTV control function for the purpose of initiating IPTV service (Step 3). The NP is in charge of replicating and delivering content media to each receiver; the responsibility of the network transport function of the NP is (1) to configure an optimized multicast tree, and then (2) to forward replicated data along the configured multicast tree. The network provided by NP consists of access, edge, and core subnetworks. To secure multicast delivery service, it is required for IPTV client to subscribe to a specific multicast group: the IPTV client uses a network/resource management function to subscribe the multicast group (Step 4); the IPTV client can join a specific multicast group by using IGMP and/or MLD. The IPTV client's subscription to a group is accomplished after successful network authentication with the NP; thereafter, the IPTV client is attached to the specific multicast tree. In the case of the NP,

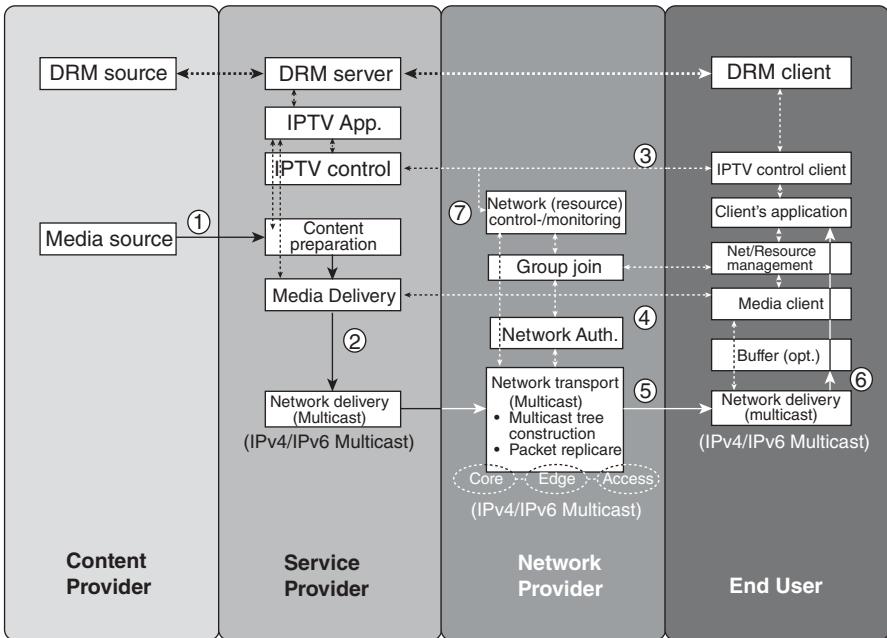


FIGURE 6.4 High-level information flow for IPTV service using IP multicast.
DRM = Digital Rights Management.

the most optimized multicast tree from the SP to the consumers is configured by exchanging appropriate routing protocol information. After the optimized multicast tree is configured, the content media from the SP can be delivered to IPTV client, employing multicast forwarding capabilities provided by the NP (Step 5). Finally, the content media reaches the IPTV client's network transport function and is thus delivered to IPTV client application. To improve video quality (to deal with jitter or delay), the IPTV client may utilize appropriately sized buffers between the network transport and the client's application (Step 6). In cases where QoS monitoring is necessary, the SP may gather information by asking the end-user IPTV client for a QoS report, or by soliciting the NP for network statistics (Step 7).

6.2 IPTV ARCHITECTURES AND ARCHITECTURAL REQUIREMENTS

There are many possible architectures to support IPTV services; however, given the four communities of interest depicted in Figure 6.1, it is important to have a defined reference architecture that can be utilized to develop interworking systems and products. In order to be able to develop an IPTV functional architecture, architecture requirements have to be identified. Macro

level architecture/system requirements to support end-user services include, but are not limited to, the following:

- QoS requirements (for end user performance expectations and associated metrics for audio/video quality and control functionality);
- QoE requirements (QoE requirements for video, audio, text, graphics, control functions, and metadata must all be defined from an end-user perspective; these also need to be agnostic of the various architectures and transport protocols);
- Security requirements (security and protection aspects of IPTV content, services, networks, terminal devices, and subscriber);
- Middleware requirements (including requirements for applications, content formats, and their uses—middleware facilitates effective and interoperable use of an IPTV system for presenting and interacting with IPTV services); and
- Network requirements: the functional architecture must support NGN and non-NGN transport networks, as well as operation modes with or without IP Multimedia Subsystem (IMS).

Some more basic functional requirements that are expected to be supported by any IPTV architecture include, but are not limited to, the following [ATI200601], [ITU200601], [ITU200801]:

- The architecture must make use of the Internet suite of protocols and standards, including IPv4 initially, and IPv6 as a long-term evolution.
- The architecture must have the ability to support various content resolutions, including resolutions adequate for HD, SD, and 3DTV for the delivery of Linear TV content, as well as for VoD content. It must support mechanisms for the receipt of content from different sources, for example, satellite, dedicated IP connections, and other sources. If retransmission broadcast service is supported, the architecture should support geographical regionalization of content.
- The architecture must provide content and segment data integrity.
- The architecture must support CA mechanisms, for example, simulcrypt (simulcrypt is a mechanism that facilitates using several service protection systems simultaneously). The exchange of information related to access conditions (e.g., ID information for Digital Rights Management [DRM]) must be supported.
- The architecture must support content and content metadata storage and distribution.
- The architecture is required to support secure delivery of content protection and content management metadata, including usage rights metadata.

- The architecture must be able to maintain accurate time-based control for synchronization, for example, lip-sync with video, pause and resume, and random access.
- The architecture must allow the end user to move between a free-to-air (FTA) and PPV environments.
- The architecture must support access to EPG.
- The architecture must encompass functional components that present an open interface for the third-party applications to use the capabilities and resources of the IPTV network.
- The architecture must have the capability of allowing content to be seen only by the appropriate audience (controls may be triggered by the service provider and/or the user—both modes should be supported). This includes Parental Control (a mechanism for deciding the suitability of particular content for a minor on his/her age).
- The architecture should support multiple-languages audio, multiple-language subtitles, multiple-languages captioning, multiple-language supplementary video, and multiple-language descriptive audio.
- The architecture should support interactive services, such as educational and entertainment applications (e.g., games), communications services (such as mail, chat, and messaging), and information services (such as stock and weather services.)
- The architecture must allow the delivery of IPTV services over different access networks (e.g., cable, fiberoptic/Passive Optical Networks [PON] access, Digital Subscriber Line [xDSL] access, wireless, satellite). It must support a mechanism that allows for service-based transport QoS to be managed across multiple network domains.
- The architecture must allow the delivery of IPTV services to as many different IPTV terminal devices (IPTV TDs) as possible, preferably all (e.g., mobile phone, PDA, and STB).
- The architecture must support mechanisms to support PPV services and On-Demand services. The service provider must be able to authenticate the end-user to authorize the purchase of products, ordering VoD, or watching particular programs by using the appropriate controls.
- The architecture must support networked personal video recorder (nPVR).
- The architecture must enable the service provider to be able to push content onto the end-user IPTV TD (whether the content is requested or not by the end-user).
- The architecture must support the time-shift TV functionality (the ability to play a content that has been broadcast in the past).
- The architecture must support recording of files and playback of video and audio content residing either in the network or at the IPTV TD.

- The architecture must support advertisement insertion.
- The architecture must support mechanisms to block transmission of content to specified geographical areas whenever blackout requirements are applicable (e.g., for sporting events.)
- The IPTV TD is required to support the decoding of at least one video and one audio format.
- The architecture must support seamless transition from one codec to another codec in the same channel within the limits of Digital Broadcasting networks, for example, scheduled daily transitions between SD and HD).
- The IPTV TD must be able to furnish media-providing entities their usage environments description, for example, type of service, type of terminal, type of transmission medium, user preferences, and available QoS Level.
- The service provider should be able to upgrade the end-user device remotely.
- The architecture must support user registration.
- The architecture must support mechanisms for accounting and charging purposes related to IPTV services usage; it must support IPTV services charging through various payment methods (such as prepay, postpay, advice of charge, and third-party charging). It must have mechanisms for the collection of data for accounting and reporting purposes, partner settlements, and reconciliation of end-user usage—such as service subscriptions, purchases, and transactions.
- Traffic management mechanisms are needed. These traffic management mechanisms are aimed at facilitating efficient support of IPTV services over the network infrastructure. Traffic management mechanisms for the home, access, and core networks are required.

Building on these and other requirements, ITU-T Y.1901, “*Requirements for Support of IPTV Services*” and ITU-T Y.1910, “*IPTV Functional Architecture*,” along with various other IPTV-related ITU-T Recommendations, constitute an initial set of IPTV standards enabling equipment vendors, along the entire system chain, to roll out standardized IPTV products [ITU200902].

The high-level requirements for IPTV services are described in ITU-T Y.1901: it specifies requirements concerning service offering, QoS/QoE, service and content protection, middleware, content management, and network and end-system aspects. Some typical requirements loosely include the ones listed above, among others. Y.1901 is the basis for other ITU-T IPTV recommendations; these other recommendations provide technical specifications that satisfy the conditions listed in Y.1901 [ITU200902].

ITU-T Y.1910, “*IPTV Architecture*,” provides recommendations on IPTV architectures. The ITU has been looking at three IPTV Architecture Models, as noted earlier, also with the idea of enabling future migration:

- Non-NGN IPTV. Effectively, a traditional but single-institution IP-based network.
- NGN without IMS IPTV. IP services obtainable in NGNs provide definable QoS capabilities and adequate levels of network/content security.
- NGN with IMS IPTV. IMS is a 3GPP/3GPP2 (Third-Generation Partnership Project/Third-Generation Partnership Project 2⁴) initiative to define an all IP-based wireless network as an evolution from historically distinct voice, data, signaling, and control network elements). IMS provides service controls utilizing the Session Initiation Protocol (SIP).

See Appendix 6A for a brief description of these network architectures. Y.1910 describes the architecture at a level of abstraction based on the reference model shown in Figure 6.5 (also see Figure 6.6 for additional details). The following function groups are discussed in the recommendation [YAM200901]:

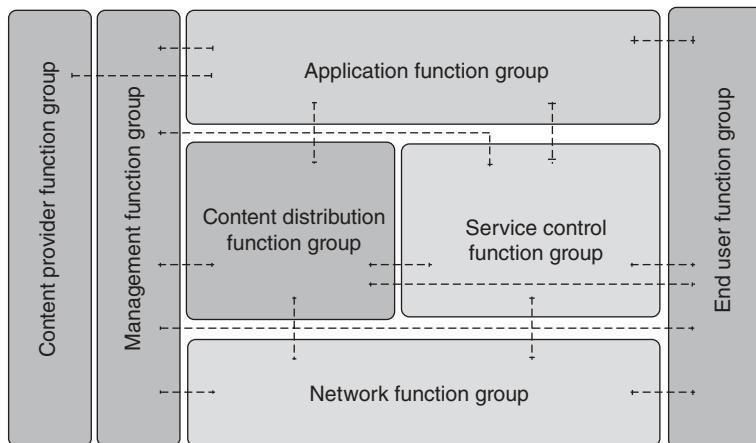


FIGURE 6.5 IPTV functional model.

⁴The Third Generation Partnership Project 2 (3GPP2) is a collaborative third-generation (3G) telecommunications specifications-setting project comprising North American and Asian interests, developing global specifications for ANSI/TIA/EIA-41 Cellular Radiotélécommunication Inter-system Operations network evolution to 3G; it is also a global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41. 3GPP2 grew out of the ITU's International Mobile Telecommunications "IMT-2000" initiative, covering high-speed, broadband, and IP-based mobile systems featuring network-to-network interconnection, feature/service transparency, global roaming and seamless services independent of location. IMT-2000 aimed at bringing high-quality mobile multimedia telecommunications to a worldwide mass market by achieving the goals of increasing the speed and ease of wireless communications, responding to the problems faced by the increased demand to pass data via telecommunications, and providing "anytime, anywhere" services [3GP201101].

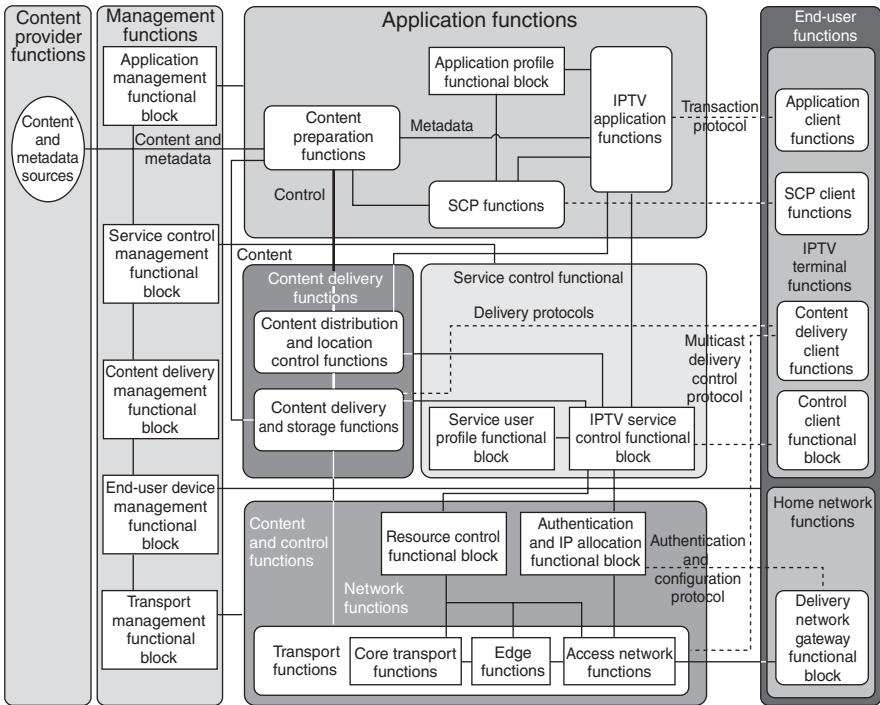


FIGURE 6.6 IPTV functional model, details.

- **End-User Function Group:** This function group is intended to provide functions to serve users that are comprised of IPTV terminal functions, such as a Set-top Box and a home network function.
- **Application Function Group:** This function group provides application functions for using IPTV services. Program guides for selecting or purchasing content, as well as guides for VoD content, are included in this function group. Additionally, protection functions for the services and content are expected to be provided.
- **Service Control Function Group:** This function group assigns networks and service resources according to requests from terminals in order to provide the services of IPTV in an adequate manner.
- **Content Distribution Function Group:** This is a set of functions that handles the physical distribution of the content to the terminals of end users (content consumers). Multicasting methods are used to support specific groups of receivers, and unicasting methods are used for the distribution of VoD material. Whenever distribution functions are provided by multiple servers, capabilities for selecting the most suitable server for a user, depending on the positional information of the user and load conditions of the servers, are provided by this functional group.

- *Network Function Group*: This function group provides the underlying resource of a managed IP network. These functions also promulgate IP addresses and allocate the bandwidth necessary for video distributions.
- *Management Function Group*: This function group monitors the status of the assets that are used to support the end-user functions, application functions, service control functions, content distribution functions, and network functions.
- *Content Provider Function Group*: This function group comprised of functions that provide content and metadata.

6.3 QOE AND QoS

6.3.1 QoE Aspects

IPTV architectures in general, and actual implementations in particular, must enable the delivery of IPTV services with a defined QoE for the end user. The IPTV QoE is much stronger than what has traditionally been achieved with basic Internet streaming services, although significant progress has also been made in recent years in that space also. QoE is defined in ITU-T P.10/G.100 as the overall acceptability of an application or service, as perceived subjectively by the end-user. QoE includes the complete end-to-end-system effects (client, terminal, network, services infrastructure, etc.), and may be influenced by user expectations and context. Hence, QoE is measured subjectively by the end-user and may differ from one user to another; however, it is often estimated using objective measurements. Information loss and delay contribute to the ultimate QoE; fortunately, information loss and delay are objective service performance measures. QoE requirements for video and audio may be defined by subjective QoE scales, such as the Mean Opinion Score (MOS) and/or Double Stimulus Continuous Quality Scale (DSCQS). Objective measures, along with human components that may include emotions, linguistic background, attitude, motivation, and so on, determine the overall acceptability of the service by the end user. Figure 6.7 identifies (some) elements contributing to QoE; these can be classified as (1) those related to QoS and (2) those that can be classified as human factors.

Some examples of QoE are as follows. One goal is to support transmission of video or data with sufficient quality for sign language perception, including lip reading; this requires the transmission of a sufficient number of frames per second and sufficient spatial resolution to reproduce details of the signing person's hands, face, lips, eyes, and body. Audio/Video Synchronization goals are generally as follows: audio–lead–video: 15 ms maximum; audio–lag–video: 45 ms maximum. Note that inconsistent loudness levels between channels can negatively impact QoE. Also, the IPTV system is expected to support an appropriate QoE when uploading content to the service provider's network and when changing channels.

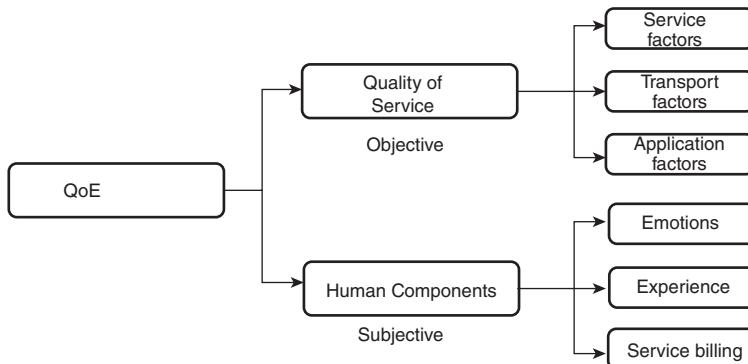


FIGURE 6.7 Some elements contributing to QoE.

As implied above, in addition to QoE (and, in fact, to support QoE), the IPTV architecture is expected to provide consistent QoS for the duration of the service interaction. QoS is defined in ITU-T E.800 as the collective effect of performance that determines the degree of satisfaction of a user of the service. In telecommunication networks, QoS is usually a measure of performance of the network itself. QoS mechanisms include any mechanism that contributes to improvement of the overall performance of the system, and, hence, contributes to improving the end-user experience. QoS mechanisms can be implemented at different levels. For example, at the network level, it includes traffic management mechanisms, such as buffering and scheduling employed to differentiate between traffic belonging to different applications. Key metrics for network transport include packet loss, packet latency, and jitter. It is generally understood that bounded end-to-end delay and jitter values are not drastically problematic because STBs provide dejitter buffers (the de-jitter buffer size is engineered to match network and video element performance—typical STB de-jitter buffers can store 100–500 ms of SDTV video, hence, network jitter must be within these limits). Other QoS mechanisms include but are not limited to loss concealment and application Forward Error Correction (FEC). QoS performance parameters can be used to assess analytically a number of performance goals. As is the case for QoS mechanisms, QoS parameters can be defined for different layers. At the network (IP) layer, those parameters usually include information loss rate and information delay and delay variation. QoS is further discussed in the next subsection.

One of the main components of QoE for video and audio is the process of digitization and compression of video and audio source materials, and the various settings and parameters utilized. Clearly, since video compression schemes such as MPEG are lossy and an identical copy of the original cannot be recovered, there are potentially negative impacts on video picture quality, and, therefore, on the viewer's QoE. The issue, however, has less to do with the compression scheme and more with the data rate that the provider is

willing to live with. Generally, SD material encoded with MPEG-4 generates 2.5–3 Mbps, and HD material generates 8–12 Mbps.

MPEG encoding algorithms aim at exploiting redundancy between pictures to achieve video compression. A simple interframe coder would operate as follows: after starting with an intra-coded picture, the subsequent pictures are described in terms of how they differ from the previous picture, by computing differences between frames, produced by subtracting every pixel in one picture from the same pixel in the next. The “difference picture” is then processed using a Digital Cosine Transform. At the far end, the decoder adds these differences to the previous picture to produce the new next picture. However, simple interframe coding becomes problematic when there is major movement of objects between pictures. The solution is to use motion compensation. Here at the coding stage, successive pictures are compared and the motion of an area from one picture to the next is measured to produce motion vectors. The picture is partitioned into rectangular areas within a frame called macroblocks, each of which can be assigned its own motion vector.

The major factors influencing video QoE at the application layer due to compression are [ITU200801]:

- Quality of the source material itself
- The baseline quality (excluding any network impairments) of the codec standard used:
 - There are a range of video codecs available, but typically television applications will use one of the following: MPEG-2, MPEG-4 AVC (also known as MPEG-4 Part 10 or H.264), SMPTE VC-1 (previously known as VC-9, the standardized version of Windows Media™ 9), and AVS.
- Resolution
- Bit rate
- Application layer video encoding—Constant Bit Rate (CBR) or Variable Bit Rate (VBR) at the encoder output
 - Video encoding is a naturally variable bit rate, but to simplify network engineering for telco delivery systems, the video encoders are set to provide a constant bit rate (as averaged over some specified time period on the order of seconds).
 - VBR streams such as those used in DVD encoding have constant quality since the bit rate is allowed to vary to accommodate varying complexity of the source material.
 - CBR streams have variable quality since there may be times when the bit rate is insufficient to accommodate the video complexity, but CBR streams enable more straightforward traffic engineering and system design.
- Group of Pictures (GOP) structure—a GOP is a sequence of picture frames. Longer GOPs require lower bandwidth but there are a number

of QoE-impacting issues, including a greater coding delay, lower video quality, and error propagation. A GOP sequence begins with an I (intra-coded) picture as an anchor; this picture, and all pictures before the next I picture, comprise the GOP. Within the GOP there are a number of forward predicted (P) pictures. The first P picture is decoded using the I picture as a basis, using motion compensation and adding difference data; the next and subsequent P pictures are decoded using the previous P picture as a reference. The balance of the pictures in the GOP are known as bidirectional (B) pictures. B pictures are decoded using vectors and difference data from I or P pictures immediately before or afterwards. Note that a bidirectional system needs memory at the encoder and the decoder to allow pictures to be reordered.

- Shorter GOPs improve quality in terms of performance of random accessibility and error recovery, but reduce the maximum compression ratio.
- Longer GOPs improve the compression ratio, but increase channel change time and the amount of damage a lost packet will cause.
- Dynamic GOPs can be used to better handle scene changes and other effects, but are not always implemented on STBs. In addition, dynamic GOPs can impact the variability of zapping latency and may complicate mechanisms to increase zapping speed considerably.
- Motion vector search range
- Rate control
- Preprocessing (such as noise reduction)
- Tandem encoding and rate shaping (e.g., digital turnaround)

Table 6.2 depicts typical IPTV data rates. Note that the industry is now settling on MPEG-4, since as can be seen in the table, the data rate for the (same quality video) is lower than that for MPEG-2. The source material for SD services is typically NTSC or PAL/SECAM with 4:3 aspect ratio. The Maximum Viewable Resolution (Horizontal × Vertical) is as follows: 720 pixels × 480 lines (NTSC) or 720 pixels × 576 lines (PAL). Frame rate is typically as follows: 29.97 fps (NTSC) or 25 fps (PAL/SECAM) (23.97/24 fps may also be used for film-based materials). The content included two interlaced fields per frame. The source material for SD services is typically ATSC or DVB, 16:9 aspect ratio. The following resolution and frame rate combinations are common:

- 720p60 (example: SMPTE 296M) or 720p50 (DVB)
 - Horizontal × Vertical: 1280 pixels × 720 lines
 - 50, 59.94, 60 progressive scan frames per second
- 1080i60 (example: SMPTE 274M) or 1080i50 (DVB)
 - Horizontal × Vertical: 1920 pixels × 1080 lines
 - 29.97 (59.94i), 30 (60i) interlaced frames per second, two fields per frame

TABLE 6.2 Typical IPTV Data Rates

Recommended Minimum Application Layer Performance for Standard Definition (SD) Broadcast Program Sources	<i>Video Codec Standard</i>	<i>Minimum Bit Rate (Video Only)</i>	<i>Preprocessing Enabled</i>
	MPEG-2—Main profile at Main level (MP@ML)	2.5 Mbps CBR	Yes (if available)
	MPEG-4 AVC (Main profile at Level 3.0)	1.75 Mbps CBR	Yes (if available)
	SMPTE VC-1 AVS	1.75 Mbps CBR	Yes (if available)
Recommended Minimum Audio Application Layer Performance for Standard Definition (SD) Sources	<i>Audio Codec Standard</i>	<i>Number of Channels</i>	<i>Minimum Bit Rate (Kbps)</i>
	MPEG Layer II	Mono or stereo	128 for stereo
	Dolby Digital (AC-3)	5.1 if available, else left/right stereo pair	384 for 5.1/128 for stereo
	AAC	Stereo	96 for stereo
Recommended Minimum Application Layer Performance for Standard Definition (SD) VoD and Premium Program Sources	<i>Video Codec Standard</i>	<i>Minimum Bit Rate (Video Only)</i>	<i>Preprocessing Enabled</i>
	MPEG-2—Main profile at Main level (MP@ML)	3.18 Mbps CBR	Yes (if available)
	MPEG-4 AVC (Main profile at Level 3)	2.1 Mbps CBR	Yes (if available)
	SMPTE VC-1 AVS	2.1 Mbps CBR	Yes (if available)
Recommended Minimum Application Layer Performance for High Definition (HD) Broadcast Program Sources	<i>Video Codec Standard</i>	<i>Minimum Bit Rate (Video Only)</i>	<i>Preprocessing Enabled</i>
	MPEG-2—Main profile at Main level (MP@ML)	2.1 Mbit/s CBR	Yes (if available)
	MPEG-4 AVC (Main profile at Level 4)	10 Mbps CBR	Yes (if available)
	SMPTE VC-1 AVS	10 Mbps CBR	Yes (if available)
Recommended Minimum Audio Application Layer Performance for High Definition (HD) Sources	<i>Audio Codec Standard</i>	<i>Number of Channels</i>	<i>Minimum Bit Rate (Kbps)</i>
	MPEG Layer II	Mono or stereo	128 for stereo
	Dolby Digital (AC-3)	5.1 if available, else left/right stereo pair	384 for 5.1 /128 for stereo
	AAC	Stereo	96 for stereo
Recommended Minimum Application Layer Performance for High Definition (HD) VoD and Premium Program Sources	<i>Video Codec Standard</i>	<i>Minimum Bit Rate (Video Only)</i>	<i>Preprocessing Enabled</i>
	MPEG-2—Main profile at Main level (MP@ML)	19 Mbps CBR	Yes (if available)
	MPEG-4 AVC (Main profile at Level 3)	12 Mbps CBR	Yes (if available)
	SMPTE VC-1 AVS	12 Mbps CBR	Yes (if available)

Video streams are highly sensitive to information loss. QoE impact depends on a number of factors:

- Impact is dependent on type of data lost: for example, lost data from I and P frames produce impairments that are different from loss of B frame packet because of temporal error propagation.
- Impact is dependent on codec used.
- Impact is dependent on transport stream packetization used.
- Impact is dependent on loss distance and loss profile. Loss distance is a measure of the spacing between consecutive network packet loss or error events; a loss period is the duration of a loss or error event.
- Impact is dependent decoder concealment algorithms.

Packet loss objectives are stated in terms of loss period and loss distance. Ideally the maximum loss period would correspond to one IP packet. The loss period should be less than 16 ms. Packet Loss Ratio (PLR) should be of the order of 10^{-7} (SD) to 10^{-8} (HD). See Table 6.3.

QoE also applies to VoD applications. VoD trick mode provides VCR-like features in VoD services; this service provides the trick ability to handle pause, play, rewind, fast forward, and stop entries for these control features. Typically, when a subscriber wishes to access some video content through STB, the subscriber accesses the video content from the EPG; the EPG supports the contents-search engine to help access of content information. Each control function (video selection, play, pause, rewind, fast-forward, and stop) has its own behavior and associated user satisfaction. For example, QoE metrics for a VoD transaction may include the following:

- *Video Selection Process Delay*: Timing period from the time when the subject is selected to the time when content is displayed.
- *Play Delay*: Timing period from the time when the Play entry was selected to the time the content is displayed.
- *Stop Delay*: Timing period from the time when the Stop play video entry was selected to the time the content is stopped playing as indicated by video content display.
- *Rewind Delay*: Timing period from the time when the Rewind video entry was selected to the time the rewind action is executed as indicated on display device.
- *Pause Delay*: Timing period from the time when the Pause video entry was selected to the time the pause action is executed as indicated on display device.
- *FFW (Fast Forward) Delay*: Timing period from the time when the FFW video entry was selected to the time the FFW action is executed as indicated on display device.

TABLE 6.3 Minimum Transport Layer Parameters for Satisfactory QoE

	Transport Stream Bit Rate (Mbps)	Latency	Jitter	Duration of a Single Error	Corresponding Loss Period in IP Packets	Loss Distance	Corresponding Average IP Video Stream Packet Loss Rate
Recommended Minimum Transport Layer Parameters for Satisfactory QoE for MPEG-4 AVC, VC-1, or AVS encoded SDTV Services	1.75	<200 ms	<50 ms	≤16 ms	4 IP packets	1 error event per hour	≤6.68 × 10 ⁻⁶
Recommended Minimum Transport Layer Parameters for Satisfactory QoE for MPEG-4 AVC, VC-1, or AVS encoded HDTV Services	2.0	<200 ms	<50 ms	≤16 ms	5 IP packets	1 error event per hour	≤7.31 × 10 ⁻⁶
Recommended Minimum Transport Layer Parameters for Satisfactory QoE for MPEG-4 AVC, VC-1, or AVS encoded HDTV Services	2.5	<200 ms	<50 ms	≤16 ms	5 IP packets	1 error event per hour	≤5.85 × 10 ⁻⁶
Recommended Minimum Transport Layer Parameters for Satisfactory QoE for MPEG-4 AVC, VC-1, or AVS encoded HDTV Services	3.0	<200 ms	<50 ms	≤16 ms	6 IP packets	1 error event per hour	≤5.85 × 10 ⁻⁶
Recommended Minimum Transport Layer Parameters for Satisfactory QoE for MPEG-4 AVC, VC-1, or AVS encoded HDTV Services	8	<200 ms	<50 ms	≤16 ms	14 IP packets	1 error event per 4 hours	≤1.28 × 10 ⁻⁶
Recommended Minimum Transport Layer Parameters for Satisfactory QoE for MPEG-4 AVC, VC-1, or AVS encoded HDTV Services	10	<200 ms	<50 ms	≤16 ms	17 IP packets	1 error event per 4 hours	≤1.24 × 10 ⁻⁶
Recommended Minimum Transport Layer Parameters for Satisfactory QoE for MPEG-4 AVC, VC-1, or AVS encoded HDTV Services	12	<200 ms	<50 ms	≤16 ms	20 IP packets	1 error event per 4 hours	≤1.22 × 10 ⁻⁶

6.3.2 QoS Aspects

DiffServ-based QoS, as described in IETF RFC 2475 and elsewhere, is typically supported by the IP networks that are used to deliver IPTV content. To maintain QoS, the IPTV architecture must support a mechanism for assigning traffic priorities and must have mechanisms for IPTV traffic identification, classification and marking, policing and conditioning, scheduling, and discarding. The IPTV architecture must also support mechanisms for dynamic IPTV traffic load balancing; load balancing enables the NP to dynamically accommodate traffic flows based on the network load and congestion conditions at any given time in order to deliver the set of IPTV services to the end users with the requisite level of quality. Specifically, networks that support IPTV are required to support the IP QoS-classed and -associated performance requirements specified in ITU-T Y.1541. Y.1541, “*Network performance objectives for IP-based services*,” recommends the election of specific QoS classes based on application requirements (see Table 6.4). Table 6.5 provides suggestions (shown with the checkmark) of the mapping of service components to QoS classes. QoS in IPv6 was discussed in Chapter 2.

There are two QoS mechanisms that are used in IP networks: (1) priority (or class-based) QoS and (2) parameterized QoS. These are briefly discussed next.

With the priority-based QoS technique, intermediate routing entities between the source and the destination of an IPTV data stream determine how to handle an IP packet from the IPTV data stream according to the priority field in the header of that IP packet. The priority field has been set to a certain value (“marking” or “classification”) by the source; the IP Services Code Points (DSCPs) are used to implement the service markings in the *diffserv* approach just described. With this technique, higher priority IP packets will get “better” treatment during transit to the destination; thus, the application-level streams (e.g., a content stream) will get better overall QoS than other streams that have been assigned lower priority. In many video applications, QoS consideration of traffic *to* the user is more important than traffic *from* the user (although the traffic rates are generally substantially different, and, so, the onus on the network is not always significant even if the upstream traffic is treated with equal priority⁵).

There are two intrinsic issues in using the DSCPs. The first issue is that DSCP markings need to be trusted, although they can be abused or spoofed (a mechanism to establish trust with end devices is needed, if one wants to address this concern.) The second issue is that all traffic of the same type has the same marking, while, on the other hand, one may have the need for the ability to differentiate on a service basis (for example, SD vs. HD service; VoD service vs. linear TV service, etc.). When using DSCPs, then, it would be

⁵In applications such as VoIP or gaming, QoS treatment for upstream traffic is also important.

TABLE 6.4 IP network QoS Class Definitions and Network Performance Objectives/Applications

QoS Class	IPTD	IPDV	IPLR	IPER	IPRR	Applications (Examples)
0	100 ms	50 ms	1×10^{-3}	1×10^{-4}	—	Real-time, jitter sensitive, low delay, highly interactive
1	400 ms	50 ms	1×10^{-3}	1×10^{-4}	—	Real-time, jitter sensitive, medium delay, interactive
2	100 ms	Undefined	1×10^{-3}	1×10^{-4}	—	Transaction data, low delay, highly interactive
3	400 ms	Undefined	1×10^{-3}	1×10^{-4}	—	Transaction data, medium delay, interactive
4	1 s	Undefined	1×10^{-3}	1×10^{-4}	—	Low loss
5	Undefined	Undefined	—	—	—	Best effort
6	100 ms	50 ms	1×10^{-5}	1×10^{-6}	1×10^{-6}	High bit rate, strictly low loss, low delay, highly interactive
7	400 ms	50 ms	1×10^{-5}	1×10^{-6}	1×10^{-6}	High bit rate, strictly low loss, medium delay, interactive

IPDV, IP packet delay variation; IPER, IP packet error ratio; IPLR, IP packet loss ratio; IPRR, IP packet reordering ratio; IPTD, IP packet transfer delay.

TABLE 6.5 Mapping of key IPTV Service Components to Y.1541 QoS Classes

IPTV Service Components	Example IPTV Services	Y.1541 QoS Class					
		5	4	3	2	1	0
Streaming of live TV content	Linear TV including Pay per View and Multi-view						
Streaming of video content	VoD, Network PVR, time-shift TV						
Streaming of audio content	Music On Demand						
Streaming control	VoD, Network PVR, time-shift TV						
Download of video content	Push VoD, Near VoD						
Upload of video content	User-generated content						
Download of data	Content guides, pictures, applications download						
Access to web pages	Portals, information services						
Streaming of live speech	Voice call, audio conference						
Streaming of live low resolution video content	Video telephony, videoconference						
Interactive message exchange	Chatting						
Message exchange	Messaging, Email						
Payment Transactions	VoD rental						

^a Consumer television quality can be achieved using the standard Y.1541 QoS classes 0 and 1 together with the DVB-IP AL-FEC mechanism, low to modest overhead, and the enhanced decoder (e.g., ETSI TS102034 Annex E).

desirable for the traffic classification scheme (also known as classification rule) to be able to classify a service rather than a traffic type. If the classification is done by the content provider or by the service provider, that may be achieved by direct knowledge of what the stream carries. If the classification is done by a downstream network provider, then each packet can be classified by inspecting one or more of its header fields; this, however, may be resource intensive. Once this classification is done, the packet queuing, scheduling, and dropping treatments are clearly determined based upon the service classification. In spite of these issues and nuances, for reasons of simplicity and scalability, QoS in IPTV environments is, in practice, traffic class-based, that is, the QoS treatment is the same for all flows belonging to the same class.

In the parameterized QoS technique, the QoS requirements of an IPTV data stream (e.g., bandwidth, delay, and jitter) are specified and requested to the network before the first IP packet is sent. The parameterized QoS technique may provide guaranteed quality of service as requested for IPTV services, but this approach has not yet been widely used in this context.

6.4 SERVICE SECURITY AND CONTENT PROTECTION

IPTV security spans the following domains: (1) Service Security, (2) Network Security, (3) Terminal Security, and (4) Subscriber Security. The security threats can, therefore, be classified into the following types: content security threats, service security threats, network security threats, terminal device security threats, and subscriber security threats. See Table 6.6 for a partial list of threats.

Table 6.7 identifies some of the basic capabilities supported and/or needed in each of these categories [ITU200801].

6.5 IPTV NETWORKS

Multicast routing and forwarding capabilities are widely employed in IPTV; IPTV service delivery over telecommunications networks makes use of multicast mechanisms because IP multicast communication improves the efficiency of data transmission and make efficient use of network bandwidth resources when delivering broadcast content. Figure 6.8 compares multicast with unicast transmission; the advantages of using multicast are relatively self-evident. A perspective on multicast capabilities is provided next, followed by a discussion of network control and content control. In passing, we make note that IPv6 Multicast-based IPTV networks have already been deployed, as seen in Table 6.8 [NIS201101], which describes some parameters for systems deployed in Japan in the recent past.

TABLE 6.6 Security Threats in IPTV Environments (Partial List)

	IPTV Asset	Risk	Severity	Threat Source	Likelihood
Content assets, risks, and threats	Compressed, plaintext content asset	Unauthorized copy obtained from network, network device or end-system	High if the work is within the release window or deemed highly valuable by the provider. Otherwise medium to low	Cracker Professional Insider	High
	Compressed, encrypted content asset	Unauthorized access	Low if end user does not distribute, or if content is traceable to the end user, moderate to high otherwise	End user	High
Any content asset		Denial of service attack	None, unless the key is obtained, high otherwise	Cracker Professional Insider	Low

(Continued)

TABLE 6.6 (Continued)

Service assets, risks, and threats	IPTV Asset	Risk	Severity	Likelihood
	Domain Name Server	Denial of service attack	Medium	Cracker Professional Insider
		Unauthorized access	High	Consumer Low
				Cracker High
				Professional Medium
				Insider Low
				Consumer Low
				Cracker High
				Professional Medium
				Insider Low
				Consumer Low
				Cracker High
				Professional Medium
				Insider Low
				Consumer Low
				Cracker High
				Professional Low
				Insider Low
				Consumer Low
				Cracker High
				Professional Low
				Insider Low
				Consumer Low

Network assets, risks, and threats	Network bandwidth	Denial of service attack	Medium	Cracker Professional Insider	High Medium Low
	Unauthorized access or use	High		Consumer Cracker Professional Insider	Low Low Medium High
	Unauthorized access	High		Consumer Cracker Professional Insider	Low Low High Low
	Unauthorized modification	High		Consumer Cracker Professional Insider	Low Low High Medium
Network Messages	Replay	High		Consumer Cracker Professional Insider	High High Low Medium
	Denial of service attack	High		Consumer Cracker Professional Insider	Low Low High Medium
	Unauthorized use	High		Consumer Cracker Professional Insider	Low Low High Medium
	System hosts			Consumer	Low Low

(Continued)

TABLE 6.6 (Continued)

	IPTV Asset	Risk	Severity	Threat Source	Likelihood
Terminal device assets, risks, and threats	Locality	Fixed-location device that is outside residence is given service	Medium	Cracker Professional Insider	Low Low Low
		Mobile device owned by nonsubscriber is given service	Medium	Consumer Cracker Professional Insider	Medium Low Low Low
Processor and Disk	Infection by malicious software	High	Medium	Consumer Cracker	Medium Low unless executables downloaded from the network

TABLE 6.7 Security Mechanisms Supported in IPTV

Security Domain	Basic (Requisite) Mechanisms and Capabilities
Service security	<p>Mechanisms for authorization and authentication of the end user.</p> <p>Mechanisms for secure delivery of entitlements to the IPTV terminal devices (IPTV TDs)</p> <p>Mechanisms to enable content confidentiality; also, the ability to support multiple scrambling algorithms.</p> <p>Mechanisms to signal the IPTV TD to utilize a specified scrambling algorithm based on a standardized framework.</p> <p>Ability to use standard key management systems</p> <p>Mechanisms to support content usage control (e.g., replay entitlements); also mechanism to support different modes of replay entitlements, for example, limit on number of plays, time limit on plays, and restriction of fast forward or rewind.</p> <p>Mechanisms for transmitting signaling messages securely between the Service and Content Protection (SCP) server and the IPTV TD SCP client. Note: The SCP Client obtains or receives rights and keys, using this information to control content decryption and usage rules.</p> <p>Mechanisms to allow for the confidentiality of signaling messages between the SCP server and the IPTV TD SCP client.</p> <p>Mechanisms to allow for the authenticity of signaling messages between the SCP server and the IPTV TD SCP client. There is a need to maintain integrity of signaling messages between the SCP server and the IPTV TD SCP client.</p> <p>Capabilities to turn on and off content tracing function (e.g., based on time, an event, content, or channel).</p> <p>If the IPTV architecture employs a Key Management System, then such system needs to be designed for scalability, reliability, and interoperability. If the IPTV architecture employs a Key Management System, then a hierarchical key management scheme is desirable to support scalability.</p> <p>The ability to support a “blackout mechanism”: a mechanism for limiting viewing-rights of certain programs to certain groups of subscribers (e.g., block viewing by residents of a specific area—for example, this can optionally be useful for sporting events).</p>
Network security	<p>System must be hardened against attacks on multicast capabilities.</p> <p>Capability for preventing Denial of Service (DoS) attacks to network.</p> <p>Support the provision of security measures to block illegal or unwanted traffic.</p> <p>Mechanisms to prevent network topology and its resources become visible to unauthorized entities.</p> <p>Mechanisms to protect the home network from malicious or unauthorized access (e.g., have firewall capabilities, with multiple levels of security and appropriate application level gateways.)</p>

(Continued)

TABLE 6.7 (Continued)

Security Domain	Basic (Requisite) Mechanisms and Capabilities
Terminal security	<p>Methods to authenticate IPTV TDs.</p> <p>Secure means for performing security-critical processes in IPTV TD, such as key management and media serialization, to abort playback of content in the event of a security-related malfunction, detection of tampering, or other indication of misuse.</p> <p>Ability to provide physical protection of sensitive security-enabling processes and components involved in the processing transmission and storage of valued content in IPTV TD in case no logical protection (such as encryption or serialization watermarks) is present. These processes include descrambling and media serialization (content tracing).</p>
Subscriber security	<p>Mechanisms to allow a subscriber to set an access control mechanism (e.g., a password) in order to restrict access to content and/or services.</p> <p>Mechanisms for parental rating, that is, facilities for rating programs according to content.</p> <p>Mechanisms to allow a subscriber to request extensions (e.g., more plays and more play-time) to digital rights associated with specific content instances.</p> <p>Mechanisms to allow an IPTV TD SCP component to authenticate the SCP servers.</p>

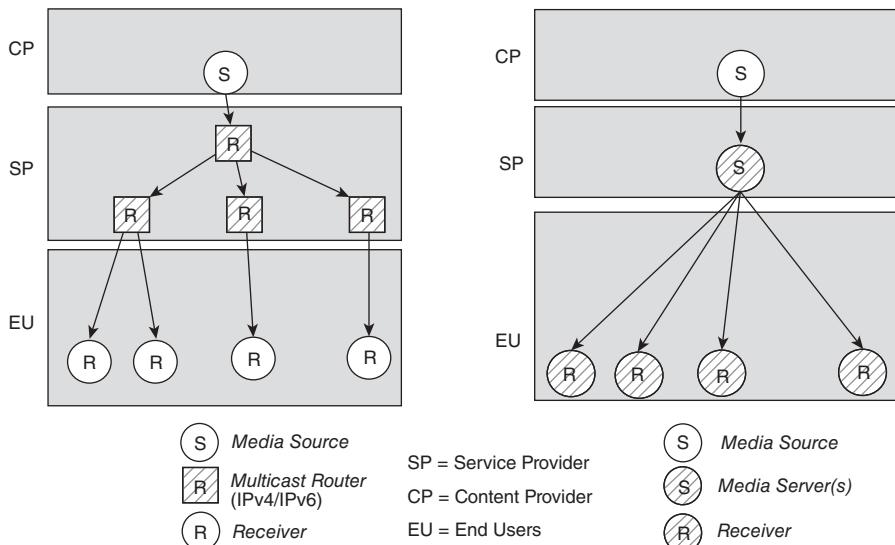
**FIGURE 6.8** Comparing multicast with unicast. Left: Data distribution scheme with native IP multicast. Right: Data distribution scheme with replicated unicast.

TABLE 6.8 Use of IPv6 Multicast in Evolving IPTV Networks

Group	NTT		KDDI		Softback
Servicer	NTT-COM/ OCN-Theater	Plala/ 4thMEDIA	OnDemand TV	Hikari Plus TV	BBTV
Network	IPv6 FTTH	IPv6 FTTH	IPv6 FTTH	IPv4 FTTH/ DSL	IPv4 FTTH/ DSL
Codec	MPEG-2TS	MPEG-2PS 6 Mbps	MPEG-2	MPEG-2	MPEG-2
Service	Multicast TV	61 ch	61 ch	35 ch	43 ch
VOD	6000 titles		12,000 titles	5000 titles	5000 titles
Karaoke	✓		✓	✓	✓
Game	✓		✓	✓	✓

6.5.1 IPTV Multicast Frameworks

The following multicast-based functionality is of interest in IPTV systems:

- End-User Functions
- Application Functions
- Service Control Functions
- Content Delivery Functions
- Network Transport Functions
- Content Provider Functions

These functions are defined next (the discussion below is summarized from reference [ITU200801]).

End-User Functions for IPTV Multicast The multicast end-user functions include those functions normally provided by the IPTV Terminal and the end-user Network. The multicast end-user functions are responsible for collecting control commands from the user, and interacting with the multicast application functions to join and leave from IPTV multicast groups. Multicast end-users can request the multicast service information. After receiving this information, they can join the multicast group specifying some QoS requirements (typically from a pre-defined set of choices). Then, the user receives multicast data through multicast network transport functions.

Application Functions for IPTV Multicast The multicast application functions interact with end-user functions to join and leave of IPTV multicast services. These functions support basic multicast control functionality, such as IPTV multicast channel change, pause, resume, and so on. Application functions for IPTV multicast include the “IPTV Application block,” the “DRM Rights & Key Management block,” the “Application Profile Functions block,” and the “Content Preparation block,” discussed next.

1. *IPTV Application Block*: This block supports Linear TV application functions to perform session management, service authorization, presentation of the content metadata, and execution of the service logic of the Linear TV service.
2. *DRM Rights & Key Management (Multicast Key Management) Block*: This block controls the protection of the content and is responsible for the management of the content rights and the keys used to encrypt and decrypt contents. It acquires the content rights (or content license, originated from the Content Provider) from the Content Preparation function, generates and distributes this security information (rights object or keys) to the DRM Client; it may also provide the keys to Content Encryption.
3. *Application Profile Functions Block*: This block stores the profiles for the IPTV Applications. Application Profile may be located either within Service User Profile Functions or within IPTV applications, depending on implementation.
4. *Content Preparation Block*: This block is used to aggregate content, to manage contents, to process metadata, and to encrypt contents. It may be used to convert the content that is delivered by the content owner into the required delivery format.

Service Control Functions for IPTV Multicast The Multicast Service Control Functions for IPTV multicast provides the functions of requesting and releasing the network and service resources that are required to support the IPTV multicast services. These functions include the “IPTV Service Control Functions block,” and the “Service User Profile Function block,” discussed next.

1. *IPTV Service Control Functional Block*: This block provides functions of handling service initiation and/or termination requests, performing service access control, and establishing and maintaining the network and system resources required to support the required IPTV Terminal functionality. For example, it can request the Content Delivery Functions to allocate multicast media server capacity and to request the Network Transport Functions to reserve Network bandwidth for the multicast media stream.
2. *Service User Profile Function Block*: This block can be used for storing user profiles, subscriber-related location data, and presence status data in the service stratum. The service user profile functional block performs basic data management and maintenance functions. The service user profile functional block has responsibility of responses to queries for user profiles.

Content Delivery Functions for IPTV Multicast Multicast content delivery functions provide the distributed content servers for the IPTV multicast ser-

vices. Multicast contents, which are prepared in the application functions, are delivered to the End-Users via the Network Transport Functions through the Content Delivery Functions. During multicast service, Application Functions send contents to Content Delivery Functions. In order to support the efficient multicast services, contents may be stored and/or cached in the Content Delivery Functions. These functions include the “Content Distribution & Location Functions block” and the “Content Delivery & Storage Functions block,” discussed next.

1. *Content Distribution & Location Functions Block:* This block controls the Delivery & Storage Functions to optimize content distribution and selection, and deliver content to the end user.
2. *Content Delivery & Storage Functions Block:* This block distributes, caches, stores, and delivers the content to the end-user. These functions handle the media control messages and the Pause and Fast Forward activities.

Network Transport Functions for IPTV Multicast The “Network Transport Functions” provide multicast connectivity with transport functions for all multicast users. The multicast transport functions can support multicast tree construction, multicast traffic replication, and multicast member identification functionalities. Then, multicast traffic is forwarded along multicast delivery path. The Network Transport Functions include the “Authentication and IP allocation Functions block,” the “Resource Control Functions block,” the “Multicast Control Point Functions block,” the “Multicast Replication Functions block,” and the “Access Network Functions block,” discussed next.

1. *Authentication and IP Allocation Functional Block:* This block provides the capability of authenticating the Delivery Network Gate Functions, connecting the Network Transport and Control Functions, and allocating IP address to the terminal device.
2. *Resource Control Functional Block:* This block provides the capability of controlling network resources in the Access and Transport networks to allow appropriate resources to be provided to the Content Streams.
3. *Multicast Control Point Functions Block:* This block provides the capability of selecting individual Multicast stream that is to be delivered, over the access network, to the IPTV Devices. The request for a Multicast Stream may need to be authorized before it is accepted. This is one of the Transport Network functions.
4. *Multicast Replication Functions Block:* The functions replicate multicast stream to all the Multicast Control Points that need to receive it.
5. *Access Network Functions Block:* This block for IPTV multicast is for further study.

Content Provider Functions for IPTV Multicast Content can come from a number of different sources, for example, IP networks, DTH satellite decoders, and so on; because of this, the physical interfaces and signals formats may be different from each of the sources. These functions may include content ratifying, which means it needs to ratify content licence, content access prioritization, and parental control level; it can provide distributed storage servers for large volumes of video and audio contents.

6.5.2 Control and Signaling Aspects

Replication of video streams is one of the fundamental functions for multicast. The IPTV architecture generally supports static configuration of the IP multicast distribution tree, but to reduce traffic proliferation, it can also support dynamic IP multicast protocol. Therefore, multicast technology and its control functions are important to the delivery of IPTV service. IPTV multicast network control is required to support the multicast control function and multicast replication function that provide IPTV multicast services for users.

The multicast control function builds a privilege table for multicast users according to the multicast group address: when users receive IPTV multicast services, the multicast network control deals with IPTV multicast services according to users' multicast privilege. The multicast replication function forwards multicast media content to users that have the privilege of IPTV multicast services: The IPTV multicast network control will forward the IPTV service contents to a user only if the user has the multicast privilege. Selection of applicable rendezvous points (RPs) within the IPTV network is important because such selection can impact the bandwidth utilization and traffic management complexity. Some basic control functions include: Traffic Management (TM) and Connection Admission Control (CAC).

Traffic Management Traffic management is a set of generic network mechanisms for controlling the network service response to a service request. The mechanisms can be specific to a network element, but more generally, these mechanisms are used for signaling between network elements or for controlling and administering traffic across a network. Functions include bandwidth allocation, admission control, packet classification/marketing, congestion management, congestion avoidance, traffic policing, and traffic shaping (also see Figure 6.9.)

Multicast Connection Admission Control An IPTV network supports transportation of multicast traffic; such network must also support multicast admission control policy for QoS management of IPTV services. The multicast admission control system based on users' admission control policy allocates and reserves resources, and also controls IPTV multicast transportation for subscribers. The multicast replication function forwards the IPTV multicast stream to subscribers according to their successful resources allocation in the network control system.

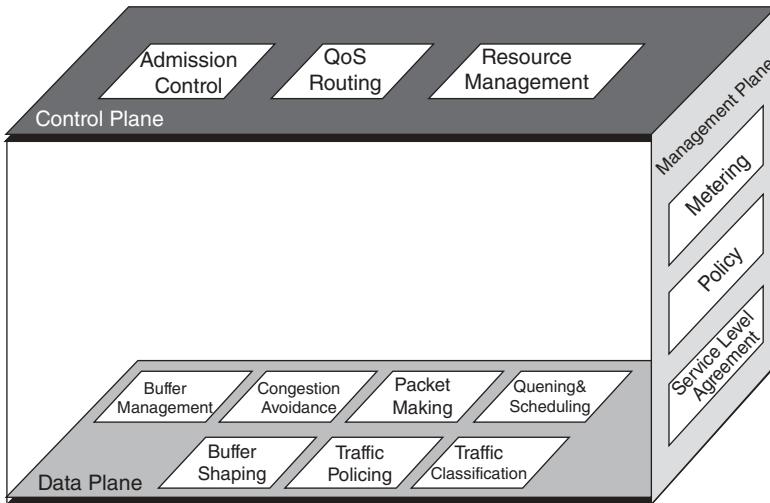


FIGURE 6.9 Control planes.

Other Control Functions Other control functions include the following:

- Multicast IP Address Management
- Multicast User Management
- Multicast Session Identifier Management
- Source-Specific Multicast

6.5.3 Content Delivery

Control of Linear TV includes but is not limited to the followings:

- *Channel Access Control*: This capability of Linear TV aims at supporting access right statuses of the entitlement to each of the broadcast channels for each user, such as “fully allowed,” “preview allowed,” and “not allowed.”
- *Channel Preview Capability*: This capability of Linear TV aims at supporting preview control functions of the Linear TV channel, such as Maximum duration for each preview, Maximum times of previews, Black-out duration after each preview, Reset period of channel preview, Recognition Time of channel preview, and so on.
- *Call Detail Record*: This capability is used to report the entitlement status of the channel being access, and to record the channel access activities of each customer are generated automatically.
- *Priority of Linear and Other Traffic*: Linear TV in IPTV supports capabilities for classifying channel priorities, such as based on bandwidth and multicast resource reserved for programs, and so on.

- Channel audience rating statistics could be obtained by policy server based on end-user multicast behavior information collected from access nodes and used to determine and provision subscriber channels priority in the access node for channels difference disposal. The end-user multicast behavior information can optional include program item number, start viewing time, and stop viewing time. In order to guarantee Linear TV's quality and service provisioning, Linear TV traffic should receive higher priority than other traffic and not be impacted from other data traffic during the viewing session.
- Parental controls have been typically included in digital television services, video games, and other systems, allowing parents to monitor or limit what their children can see or do. For the IPTV architecture, parental control mechanism can be used to restrict IPTV contents that children can receive. Policy control and management for parental control is used to support the network capability to store and forward the requested IPTV services and its rating to specified terminals (for example, monitoring terminal for parent) based on preconfigured control policy and user profiles.

6.6 END SYSTEMS AND INTEROPERABILITY ASPECTS

Figure 6.10 provides an overview of the protocol (standards) apparatus needed to support the IPTV end-system. A number of these protocols are discussed next.

6.6.1 IPTV Terminal Devices

IPTV TDs are described in the H.720 series of ITU-T recommendations. H.720 “*Overview of IPTV Terminal Devices and End-Systems*” and H.721 “*IPTV Terminal Devices: Basic Model*” have been officially published as of press time, while H.IPTV-TDES.3 “*IPTV Terminal Device: Full-fledged Model*” and H.IPTV-TDES.4 “*IPTV Terminal Device: Mobile Model*” were under study. Recommendation ITU-T H.770 “*Mechanisms for service discovery and selection for IPTV*” describes the mechanisms for service provider discovery, service discovery, and selection. Linear TV and VoD services are addressed with metadata that describes programming and delivery protocols details.

H.720 provides a general description and an overview of the architecture and functional components of an IPTV TD, and it provides a high-level description of the functionality necessary to support IPTV services. H.720 describes the basic architecture of IPTV TDs' functions based on ITU-T Y.1910 which, as noted, defines the overall IPTV architecture. Figure 6.11 depicts the architecture overview described in H.720 while Figure 6.12 fills in many details. H.720 provides the following: (1) definitions of a TD and of an end-system; (2) the location of TDs and end-systems within the overall

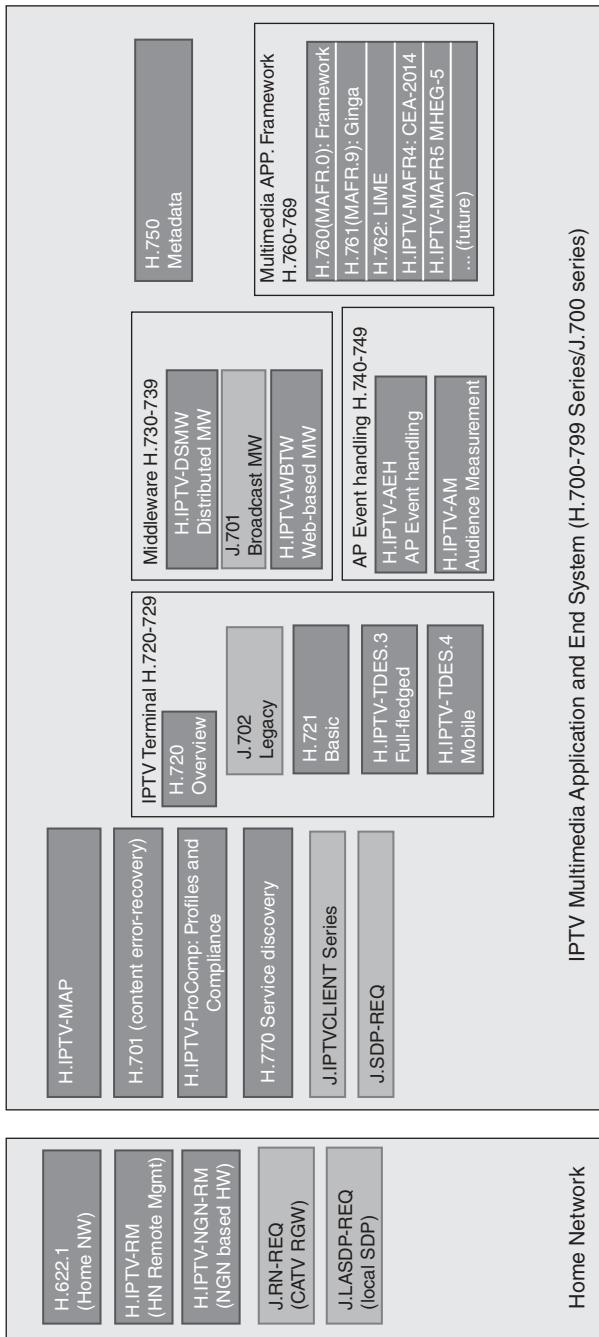


FIGURE 6.10 Recommendations for end-systems.

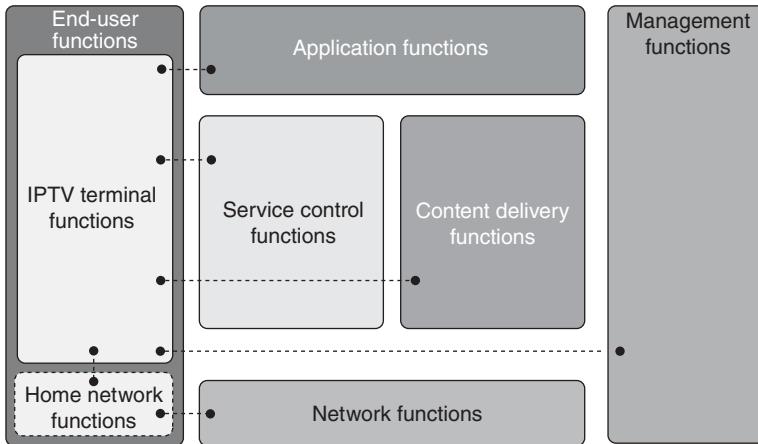


FIGURE 6.11 IPTV terminal device architectural overview.

architecture of IPTV; (3) examples of IPTV services; (4) an abstract description of the terminal device architecture; and, (5) identification of other ITU Recommendations that discuss IPTV TDs.

H.721 specifies the functions to be supported by IPTV TDs that are connected to the managed network, as depicted in Table 6.9. Table 6.10 expands on Table 6.9 and provides additional information on these function blocks. H.721 describes and specifies the functionalities of the IPTV TDs for IPTV basic services defined in ITU-T H.720, over a dedicated CDN that takes into consideration such conditions on content delivery, such as QoS requirements. The expected types of terminal devices are STBs and digital TV sets with embedded IPTV capabilities. The specification is targeted at IPTV TDs capable of receiving linear TV service and VoD service. Basic additional data content, such as text and graphics, can also be used.

The key target devices are IP-STBs and TV sets with an embedded IPTV function. Included services are Linear TV, VoD, Service navigation, and public Internet services. Conformance testing specifications (HSTP.CONF-H721) has also been approved and tested by the ITU-T. Multiple H.721 compliant terminal devices have been already implemented and deployed in the market [NIS201101].

There are “Target Services” and “Scopes” described in Recommendation H.721. Table 6.11 (and Figure 6.13) depicts the various end-system features and capabilities that have been under consideration. Target services and Scopes of H.721 Recommendation include Linear TV and VoD services on managed networks, and are intended to be supported either via a STB or in embedded-IPTV receivers. In particular, H.721 describes the Basic Model of the IPTV terminal; this design is targeted at resource-limited devices such as TV sets, STB, and TV sets with built-in IPTV capabilities. Supported services include the following among others (see Figure 6.14):

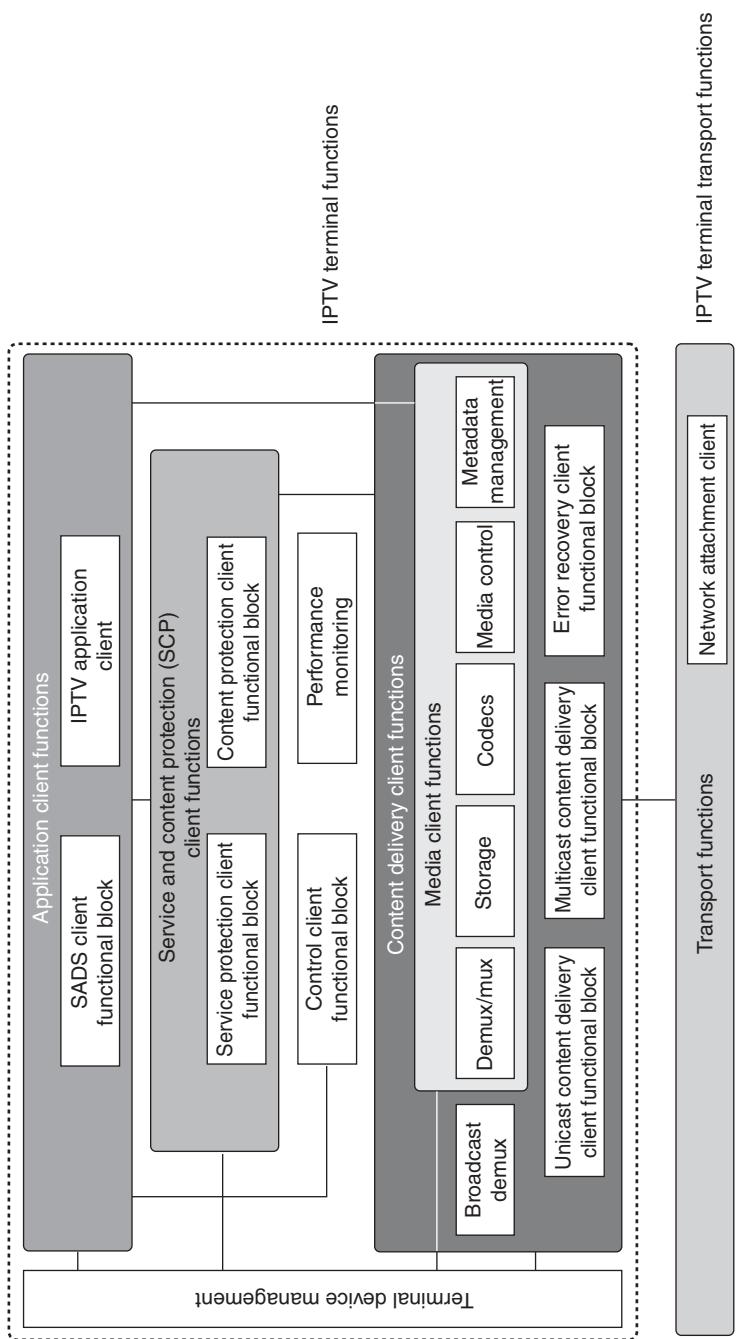


FIGURE 6.12 Functional architecture block diagram of IPTV terminal device.

TABLE 6.9 Functions of Each Terminal Component

Functional Block	Function	Protocols
Terminal transport functions	Network communication interface Communication processing Network attachment processing	RTP, UDP, HTTP/TLS, TCP, IP, and IGMP/MLD DHCP and DNS
Content delivery client functions	Multicast content delivery client function block Unicast content delivery client functional block Error recovery client functional block	IGMPv2 and MLDv2 RTP and RTSP; HTTP for VoD contents selection FEC-based error recovery (H.701)
Media client functions	Playback and trick mode functionalities for VoD Demux/mux functional block Codec functional block (Decoding) Storage functional block Metadata management	Playback, Fast-Forward, Rewind, Pause, Stop, Chapter, and so on MPEG-2 TS/TTS and clock synchronization Video: MPEG-2 (ITU-T H.262) and MPEG-4/AVC (ITU-T H.264) Audio: MPEG-2AAC, MPEG-1 L2, MPEG-4 HE-AAC, and AC-3 Storing ID of services, password, License key Caching, Searching, Parental control
SCP (service and content protection) client functions	Service protection client functions Content protection client functions	<ul style="list-style-type: none"> Secure communication channel Authentication with SCP server CRL update and management Content key acquisition Extraction of the descrambling key from Entitlement Control Message (ECM)
IPTV application client functions	IPTV application client functions Service and application discovery and selection (SADS client functions)	<ul style="list-style-type: none"> Handling HTML/BML Metadata to replay control EPG/ECG Service provider discovery Service discovery Service selection (compliant with H.770)
Other functions	Control client functions Terminal device management Physical interface	<ul style="list-style-type: none"> Rest button, Remote controller RGB, DVI, Digital Audio, HDMI

TABLE 6.10 Description of the Function Blocks (Details)

Key Function	Description	Subfunctions
IPTV terminal transport functions	Functions responsible for handling the IP-based connection between the Delivery Network Gateway (DNG) and the IPTV terminal device (IPTV TD), or between the IPTV network and the IPTV TD.	The network attachment client functional entity manages IP connectivity and obtains IP addresses and configurations for the IPTV TD in the process of network attachment.
Content delivery client functions	Functions that receive and control the delivery of the content from the content delivery and storage functions. After receiving the content, the content delivery client functions can optionally use the service and content protection (SCP) client functions to decrypt and decode the content, and can also optionally support playback control.	<p>Broadcast demux: The hybrid IPTV TD supports both IP content reception and non-IP content reception for terrestrial, cable, or satellite broadcast services. The broadcast demux functional entity is responsible for demultiplexing in non-IP content reception.</p> <p>Multicast content delivery client functional block: The multicast content delivery client functional block receives the content from the multicast delivery functional block within the content delivery and storage functions. This functional block communicates with the multicast control point functional block for the selection of the multicast stream. Multicast protocols, such as IGMP for IPv4, or MLD for IPv6, are handled by this functional block.</p> <p>Unicast content delivery client functional block: The unicast content delivery client functional block receives the content from the unicast delivery functional block within the content delivery and storage functions. This functional block communicates with the content delivery control functional block within the content delivery and storage functions for the control of the unicast stream. For example, RTP and HTTP for unicast content on demand are supported in this functional block.</p> <p>Error recovery client functional block: The error recovery client functional block is responsible for improving the QoS/QoE provided by the network. Retransmission, forward error correction (FEC), and hybrid combinations of both techniques are well-known mechanisms for error recovery.</p>

(Continued)

TABLE 6.10 (Continued)

Key Function	Description	Subfunctions
	<p>Media client functions: Function for the content reception, and content delivery; has content processing functionalities, such as transcoding. It follows that client functions are located in content delivery client functions.</p> <p>Media control: The media control functional entity controls video and audio components, and other components such as demultiplexing, encoding, metadata handling, content storing, and play/reproduction of content including streaming data. The PVR controller is involved in this functional entity.</p> <p>Video: The IPTV TD is expected to support commonly used video formats.</p> <p>Audio: The IPTV TD is expected to support commonly used audio formats.</p> <p>Other data formats: The IPTV TD is expected to support other commonly used multimedia data formats, such as text (i.e., closed caption) and graphics.</p> <p><i>Media Control—Demux/mux Function:</i> The Demux/mux functional entity is responsible for the following functions:</p> <ul style="list-style-type: none"> • Demultiplexing of video, audio and data streams. • Optional remultiplexing functionality to combine video, audio and/or data streams, for potential distribution over the home network. • Embedding of content tracing information if required by the content provider and not done previously or elsewhere <p><i>Media Control—Codecs:</i> The codecs functional entity is responsible for:</p> <ul style="list-style-type: none"> • Decoding the compressed video and audio streams. • Decoding textual data, that is, closed caption. • Decoding other multimedia content, for example, graphics. 	

Media Control—Storage: The storage functional entity is responsible for the caching and storage of content and other application data. The storage function may be implemented internally or externally (i.e., by means of the TD-PD interface).

Media control—Metadata Management: The metadata management functional entity processes and manages the metadata provided within the IPTV TD. For example, the IPTV TD is expected to retrieve metadata from the service provider and temporarily store it as cache. Thus, the management of the cached metadata is an important aspect of metadata management. Another example is interaction with the service provider and/or with metadata locally cached in the IPTV TD to provide the search capability based on metadata. Still another example is the controlling of viewing based on metadata, for example, parental guidance and control.

Content protection client functional block: The IPTV TD is responsible for enforcing content usage rules ascribed to rights information (also known as content protection metadata). This functional block interprets content rights and keys obtained from the server-side right and key management function then acts on the interpretation to control how the content is processed and exposed to the end user, either through integrated presentation devices (such as a display or audio rendering system) or through physical interconnects to external devices.

Service protection client functional block: For managed services involving protected content, it is typically the case that the end user (who may be the subscriber) and the IPTV TD must be authenticated, and, subsequent to successful authentication, authorized to access service(s) and the content contained therein.

(Continued)

The SCP client functions include the following functions:

- Handling of authentication mechanisms including key exchange and processing
- Creation of content tracing information to be bound to the content, if required by the content provider.
- Embedding of content tracing information, or enforcing subsequent embedding of content tracing information, if required by the content provider.
- Processing of SCP entitlement issues.
- Descrambling of input stream(s).

Service and content protection (SCP) client functions

TABLE 6.10 (*Continued*)

Key Function	Description	Subfunctions
Application client functions	<p>The application client functions in IPTV services are responsible for the following functions:</p> <p><i>Basic functions:</i> Applications include the software components capable of enabling functional and observable behavior, such as the GUI, SNA (Service Navigation Application), VoD controls, SCP applications, and other service-related applications.</p> <p><i>Management functions:</i> Some applications are responsible for basic management of the IPTV TD, such as power management and event management.</p> <p><i>Service supporting functions:</i> Some applications are responsible for supporting services, including, but not limited to, plug-in applications, browser applications, and media player applications.</p>	<p>IPTV application client: The IPTV application client functions consist of the following service-specific functional blocks.</p> <p>On-demand client functional block: This functional block interacts with the server-side relevant one to perform session management, service authorization, presentation of the content metadata, and execution of the service logic for the on-demand applications.</p> <p>Linear TV client functional block: This functional block interacts with the server-side relevant one to perform session management, service authorization, presentation of the content metadata, and execution of the service logic for the linear TV applications.</p> <p>Other client functional blocks: These functional blocks interact with the server-side relevant one for the delivery and presentation of additional IPTV services and their content, for example, games and distant learning.</p> <p>Service and Application Discovery and Selection (SADS) client functional block: The SADS client functional block provides for the end user's discovery and selection of IPTV services and applications. This functional block facilitates common services, cooperating with the IPTV application client.</p>

Connection and session management	<p>Connection and session management is responsible for the following functions (this functionality is not depicted in the figure →however, individual functions are satisfied by one or more functional blocks/entities depicted in the figure):</p> <ul style="list-style-type: none"> • Authentication, communication and management of the connection to the IPTV server through the IPTV network (the control client functional block allows the IPTV TD to initiate service requests to the IPTV service control functional block in order to prepare for the connection to the content delivery functions). • Managing the protocols necessary to stream and control the flow of media and other content arriving at the IPTV TD (the unicast content delivery client functional block, multicast content delivery client functional block and IPTV application client functions could have responsibilities for content reception and control of real-time streaming). 	<p>The terminal device management functional entity provides the following functions:</p> <ul style="list-style-type: none"> • Configuration management of IPTV TDs. • Monitoring and control of the IPTV TD functionality. 	<p>The performance monitoring functional entity provides various QoE data, such as audiovisual quality and IPTV service attributes.</p>
--	--	---	---

TABLE 6.11 Recommendations for End-Systems: Services for Each Terminal Device Model

Terminal Device Model	Service
Basic model (H.721) “Basic Services”	Linear TV, VoD, and portal service
Full-fledged model (TDES.3) “Basic Services” + “Advanced Services”	Push VoD, video phone, advertisement, PVR, Audience measurement, and Personal Broadcasting
Mobile model (TDES.4) “Basic Services” + Mobile oriented Services”	Linear TV and VoD for mobile, interactive services, and advertisement based on user location

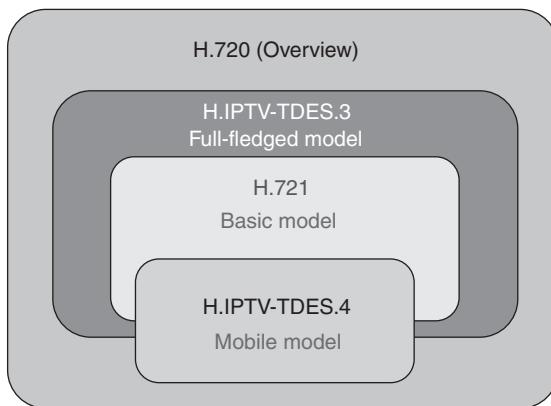


FIGURE 6.13 Scope and relationship of H.72X recommendations.

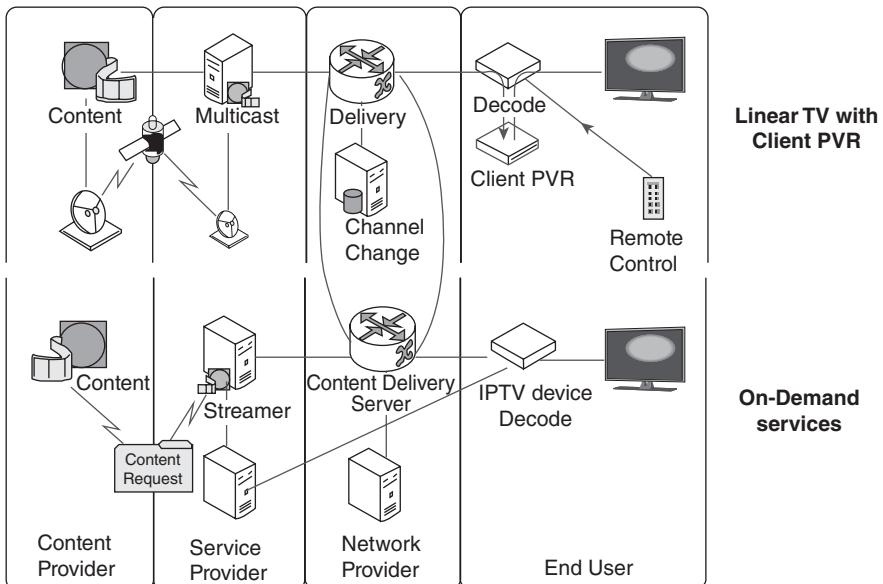


FIGURE 6.14 H.721-supported services—a logical view.

- Linear TV service via Multicast delivery where programs are provided on temporal order; this service also includes IP retransmission of terrestrial and satellite broadcasting.
- Time-shifted TV and/or VoD Service via unicast delivery. In TSTV, the content is stored/served by end user's choice (selects time and content of Linear TV). In VoD the content is served by end-user's choice.

Interactive services are also supported in the Basic Model of the IPTV TD. Furthermore, in addition to the basic video capabilities, service navigation functions (e.g., Remote Controller, EPG, Portal services), public interest services (e.g., Emergency Broadcast, Subtitle, Sign language), and interactive services, are also supported by the Basic Model.

As mentioned, IPTV TDs also need to support key basic functionality, such as network attachment, service discovery, service navigation, security, privacy, and quality and performance monitoring. These capabilities are described in Recommendation ITU-T H.770. The IPTV TD attachment and initialization process is the process by which the IPTV TD is configured to attach to the network to discover the service provider and discover the services offered in an IPTV system. When the IPTV TD attaches to the network, it has to be aware of where to get the description of the IPTV service providers available to it (possibly one or more than one). Such information is accessed via entities called *service provider description entry points*. Service provider discovery is the process by which an IPTV TD becomes aware of the available IPTV service providers, learns the location of their service discovery servers, and learns the means for attaching to each service discovery server. As a result, by contacting the discovered service discovery server(s), an IPTV TD can perform the subsequent service discovery and service attachment procedures. Service navigation is a process of presenting information that allows the end user to discover, select, and consume services. There are many security and privacy concerns and requirements that are addressed and supported by the IPTV TD: an IPTV TD is a source of private information, and some of the private information that requires protection within an IPTV TD includes viewing history, return/interaction channel usage, audience rating information, history of interactive operations, personal profiles and preferences, and identification.

In conclusion, Figure 6.15 shows a diagram of the typical protocol stack for IPTV TDs (inspired by reference [ITU201101]). As it can be inferred from this figure, the protocol mechanism used by the STB and/or IPTV home client is fairly complex.

6.6.2 Home Network

Homes have become more sophisticated in terms of devices, connectivity, and desired services. Many homes have wired or wireless Ethernet infrastructures, as well as in-house coaxial distribution systems. IPTV frameworks recognize

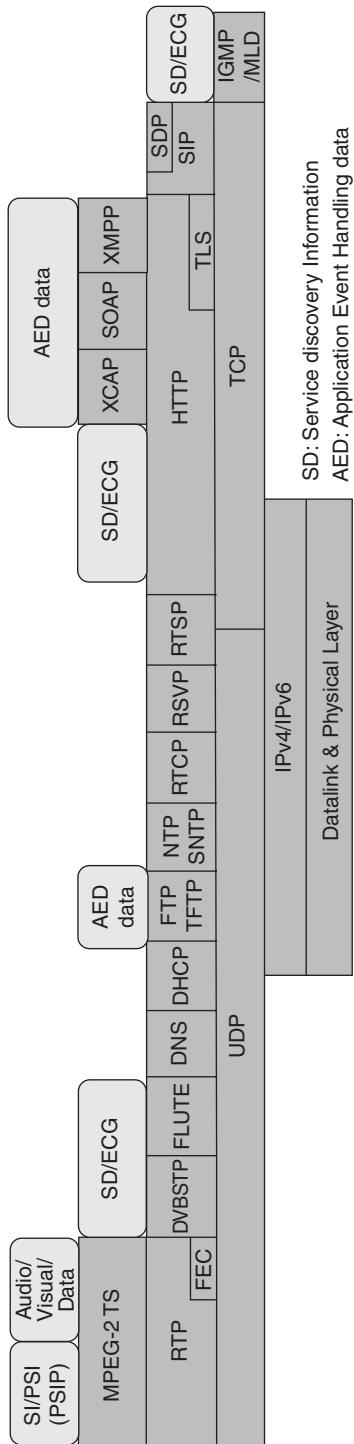


FIGURE 6.15 Major protocols supporting IPTV terminal devices.

the need for home networking. The following terminology is used in the context of the Home Network (HN):

- **Delivery Network Gateway Functions (DNGF):** Set of functions that mediate between the network and service provider domains and the IPTV Terminal Function (ITF). Note: A device implementing the DNGF is commonly referred to as the Residential Gateway (RG) or as the Delivery Network Gateway (DNG).
- **Delivery Network Gateway (DN):** A device implementing the DNGF. Note: There are other terms used for the same device, including Home Access, Home Gateway, and RG.
- **IPTV Terminal Function (ITF):** The functionality that is responsible for processing the content conveyed by the IP transport.

Figure 6.16 depicts schematically the home environment supported by IPTV. The interfaces identified in the diagram are precisely defined in various standards. In Figure 6.11, the *primary domain* deals with IPTV-related IP traffic between the access network and the IPTV TD including audio and/or video streams. Traffic in the primary domain is associated with traffic to/from the access network. The devices and traffic related to the primary domain are required to be configured to be reachable to and/or from the access network, directly or indirectly (e.g., via NAT). Since this domain is expected to work as

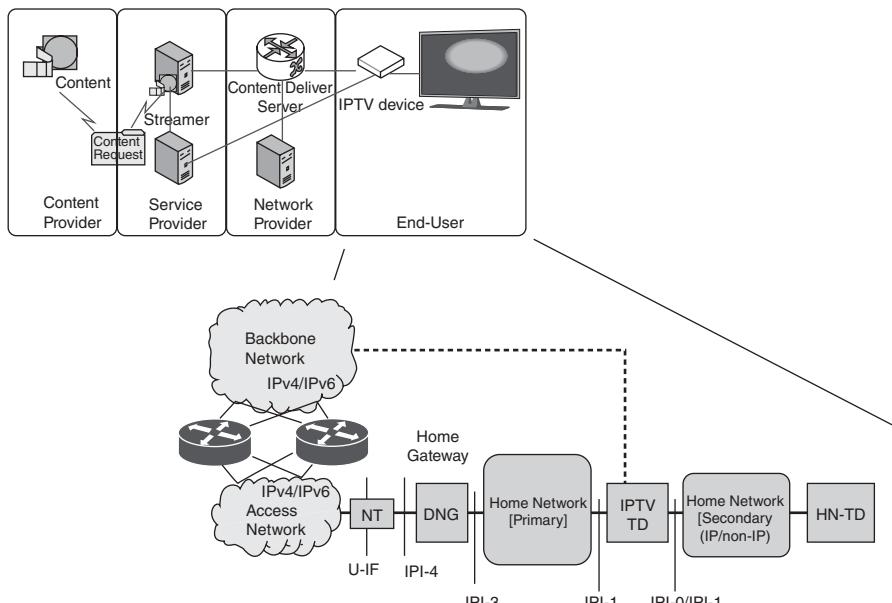


FIGURE 6.16 Home environment.

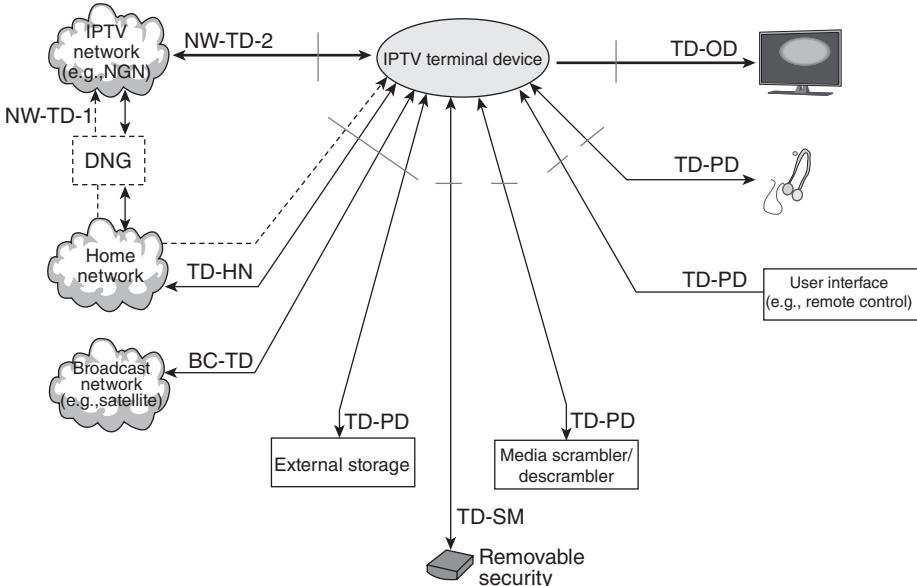


FIGURE 6.17 Examples of IPTV terminal device interfaces.

an extension of the access network, technical coordination, such as QoS mapping, with the access network is needed. The *secondary domain* deals with IPTV-related traffic between the IPTV TD and the home network terminal device (HN-TD). The devices and traffic belonging to the secondary domain do not need to be configured to be reachable to and/or from the access network [ITU200601]. The secondary domain may typically be comprised of two parts, an IP-based part and a non-IP part.

The IPTV TD must support a number of interfaces. Figure 6.17 depicts a possible subset of these interfaces (also see Table 6.12).

6.6.3 Audience Information

Utilization of audience information that can be collected with IPTV systems, for example utilization information for IP broadcasting and VoD services, will enable service providers to deliver, in due course, new revenue-enhancing business services. Two such services include audience rating services and advertisement services that match user characteristics. Appropriate functionality will be necessary for collecting audience information from terminals, home gateways (home gateways are inaccessible to users), and also from network elements [YAM200901]. Technical approaches that can be employed for the utilization of audience information are described in the following documents:

TABLE 6.12 Description of Interfaces

Interface	Description
BC (Broadcast)-TD interface	This interface is between non-IPTV broadcasting network, such as satellite and terrestrial network, and the IPTV terminal device (IPTV TD)
Network terminal device (NW-TD) interface	NW-TD-1: NW-TD-1 represents a connection by which the IPTV TD connects to the IPTV network via the DNG, including TD-HN. NW-TD-2: NW-TD-2 represents a direct connection between the IPTV network and the IPTV TD. This interface is between an IPTV TD or DNG and the IPTV network. This interface could facilitate content and metadata transfer via wireless network (e.g., 3G/WiFi/WiMAX) by multicast or unicast operation.
TD-HN interface	TD-HN is an interface that provides a connection to the home network. TD-HN is used for the connection between the IPTV TD and other in-home devices, such as an external PVR
TD-OD and TD-PD interfaces	TD-PD interface: This interface is between a peripheral device (e.g., USB adapter or mobile telephone headset) and the IPTV TD. It allows the transfer of information through a non-IP-based connection (e.g., Bluetooth and infrared communication) <ul style="list-style-type: none">• <i>User Input Interface:</i> A user input interface is a combination of software and hardware components through which a user can interact with the user input functional entity. It can manifest itself in such forms as a remote control or a keyboard.• <i>Input Interface:</i> The input interface is responsible for the interaction between user devices and the appropriate applications in the IPTV TD. TD-OD interface: This interface is between an output device (e.g., display, home theatre system, and external PVR) and IPTV TD, and facilitates the transfer of audio and video signals from the IPTV TD to the output device.
TD-SM interface	TD-SM is the terminal device-security module interface. It is the interface between the IPTV TD and an optional removable security function, such as an IC card.

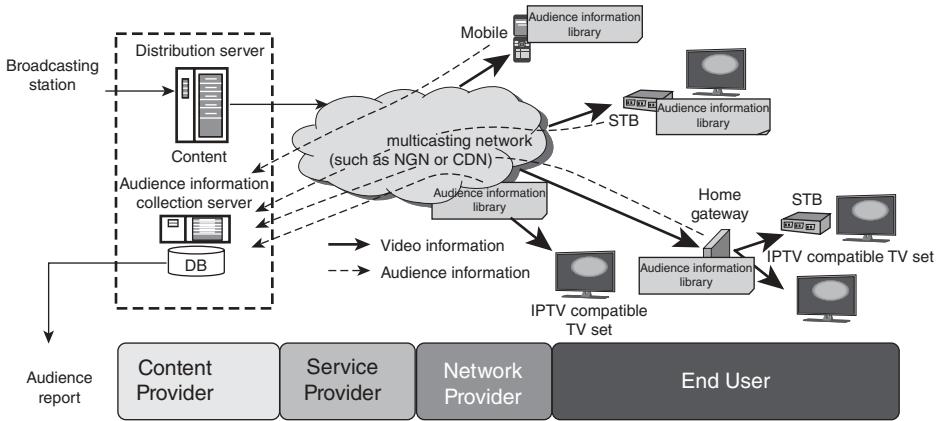


FIGURE 6.18 IPTV information flows, including audience information.

- ITU Y.1901, a recommendation for requirements as noted earlier;
- ITU H.750 “*High-level specification of metadata for IPTV services*,” a recommendation for metadata; and
- ITU H.720 “*Overview of IPTV terminal devices and end-systems*,” a recommendation providing a general statement for terminals.

Figure 6.18 provides a graphical view of the environment. Note that because audience information is personal information, approval will be necessary from users prior to realizing the actual services.

6.7 MIDDLEWARE, APPLICATION, AND CONTENT PLATFORMS

In order to accelerate the deployment of IPTV, standards are also needed for middleware, applications, and content platforms. *Middleware* is a layer of software between applications and resources that allows functionality-supporting entities running on one or more devices in an IPTV system to interact across a network. *Metadata* are structured, encoded data that describe characteristics of information-bearing entities to aid in the identification, discovery, assessment, and management of said entities. *Content provisioning* is the activity of providing TV channels, programs, movies, music, and other contents between content providers and service providers. Figure 6.19 depicts graphically the scope of these capabilities.

6.7.1 IPTV Metadata

Middleware and metadata are used to support content provisioning, service discovery and navigation, channel identification, and location resolution.

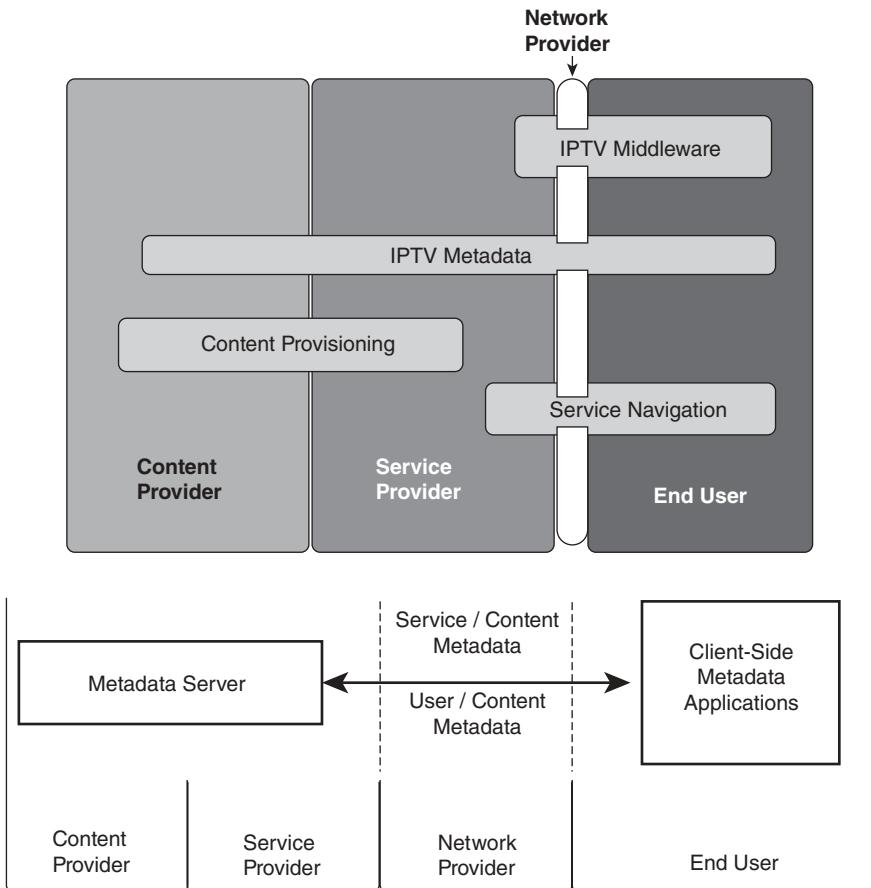


FIGURE 6.19 Scope of Middleware and metadata capabilities. Top: General scope. Bottom: Metadata distribution.

Metadata can vary in details from (1) simply identifying the content package title or information to support a service navigation interface, to (2) more elaborate structures providing a complete index of different scenes in a movie; it can also (3) provide business rules detailing how the content package may be displayed, copied, or sold. Metadata is typically generated by CPs or SPs to describe services and content. Metadata types, in the context of IPTV include the following [OIP200901]:

- *Linear TV Metadata:* Metadata that is associated with the content items provided in the Scheduled Content Service. In the Scheduled Content Service, the content playout time is determined by the service provider.
- *CoD Metadata:* Metadata describing the attributes of content items available to the user on an on-demand basis. The CoD Metadata is typically

organized as a catalog that may be presented in different perspectives, such as alphabetical listing or grouped by genre.

- *Interactive Services Metadata:* Metadata describing interactive applications that may be available to the user.
- *Stored Content Metadata:* Metadata describing scheduled content items that have been recorded by the user and are available for playback either from network storage or local storage.
- *File Delivery Metadata:* Metadata describing a file delivery session over the unidirectional network.

The Metadata Server is the entity responsible for aggregating metadata sets produced by CPs or SPs, as well as metadata sets generated or registered by metadata clients to describe end-user preference or context. These metadata sets are maintained in the database managed by the Metadata Server. The metadata maintained in the Metadata Server's database is accessed by, delivered to, or contributed from metadata clients through metadata delivery and exchange protocols. These clients are typically categorized as Web-based navigation servers maintained by the Service Provider or client-side applications running on the IPTV client. The Web servers provide web pages to the IPTV client through logical interfaces between the SP and end-user domain. These pages are consumed by Web browsers to aid end users in obtaining their preferred content. Metadata directly consumed by a client-side metadata application is used for providing the network-transparent user interface for navigation, for example, a content overview listing integrated with local content storage management. The Metadata Server also stores and manages end user profiles or context metadata required to support content or service adaptation [ITU200801]. There are several approaches to metadata delivery, such as unicast or multicast, subscribe-notify, query-response, or a mixture of those modes. Specifically:

- push or pull mode of delivery (e.g., using Simple Object Access Protocol [SOAP]);
- unicast or multicast, ensuring reliability or not; and
- query-response; metadata bi-directional transport, and so on.

Metadata transport containers carrying ESG metadata instances are transported in File Delivery over Unidirectional Transport (FLUTE) dynamic file delivery carousel sessions as described for file delivery in ETSI TS 102 472.

6.7.2 IPTV Middleware Architecture

The IPTV middleware supports a variety of functionalities (e.g., EPG, PVR, and gaming) provided by the IPTV architecture to the IPTV TDs. Figure 6.20 provides an overview of the IPTV middleware architecture. The IPTV middleware architecture components are described next [ITU200801].

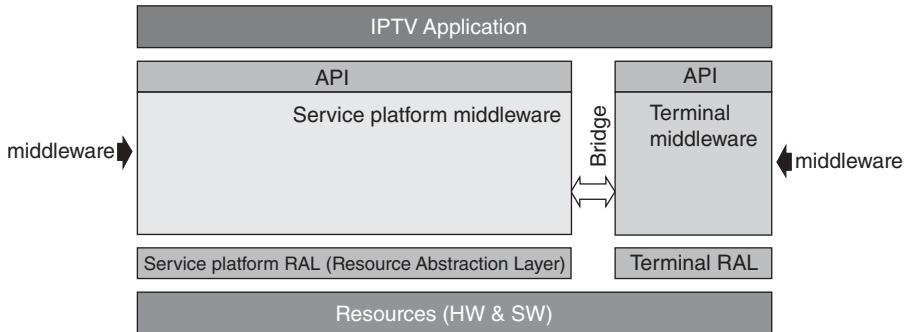


FIGURE 6.20 IPTV middleware architecture.

1. *IPTV Application Layer*: The application layer is the layer where operators and third parties provide services and applications. These services and applications include EPG applications, VoD, linear TV streams, PVR, games, Internet applications, as well as other value-added services.
2. *Application Programming Interface (API) layer*: A set of interfaces for service providers or manufacturers to build specific applications and be presented on a granular basis for a variety of purposes.
3. *IPTV Middleware*: The IPTV middleware is divided into a service platform middleware and a terminal middleware linked through a Bridge. The IPTV middleware invokes the lower layer resources (e.g., network interfaces) to control them, and provides APIs for upper layers. The IPTV middleware also provides some specific functions, including:
 - Resource management function, a functional module to manage system resources in IPTV TDs and servers.
 - Application management function, a functional module to manage the life cycle of the applications and interaction operations between them.
 - Optionally, the terminal middleware implements a multimedia application platform and a presentation engine.
4. *Resource Abstraction Layer (RAL)*: The RAL is employed to make the middleware independent of lower software and hardware layers. The resources abstracted in RAL include:
 - software resources, such as drivers and Operating System (OS); and
 - hardware resources, such as computing devices, CPU, storage devices, firmware (e.g., codec), rendering devices (e.g., display and speaker), and I/O (input/output) devices.

The IPTV TD has a fairly extensive middleware support. As seen in Figure 6.21, the IPTV TD runs a number of middleware components, which we discuss in the subsections that follow. The RAL enables the IPTV terminal middleware software to be hardware agnostic. A RAL exists for each specific hardware/

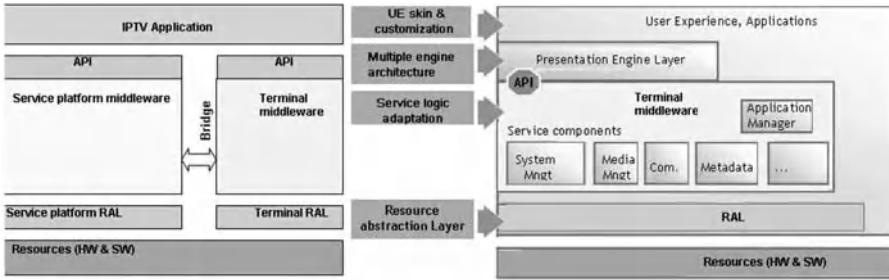


FIGURE 6.21 IPTV terminal middleware architecture: overview (left-hand side of picture).

OS combination to provide the necessary interface to the lower layers (e.g., RAM, network access, hard drive, USB port, and so on). The Service logic adaptation layer is comprised of various service components; these components offer functionalities common to all middleware implementations (e.g., service selection and presentation, service information management, PVR, and security system). The presentation engine layer may include various engines along with a set of high-level services. This layer is built on top of the service logic adaptation layer (in some implementation this layer may not exist). The user experience and application layer provide direct interface with the user. The applications themselves are either downloaded or resident.

6.7.3 Content Provisioning

Content providers typically supply audiovisual channels, contents, and metadata together or separately. In the case of broadcast retransmission, broadcast service platforms, such as terrestrial, cable, or satellite digital broadcasting, can provide audiovisual channels, metadata, and contents for interactive services to IPTV Service platforms for retransmission. For content provisioning, a set of interfaces between content/metadata providers and service providers must be defined including the following (see Figure 6.22):

- contract exchange (not to be standardized);
- content and metadata provisioning interface; and
- consumption reporting.

6.7.4 Service Discovery

Related to service discovery, one should keep in mind that there are a number of IPTV configurations to be considered, such as:

- configuration with only one IPTV service provider on the network; and
- configuration with multiple IPTV service providers on the network with or without preconfigured specific IPTV service provider.

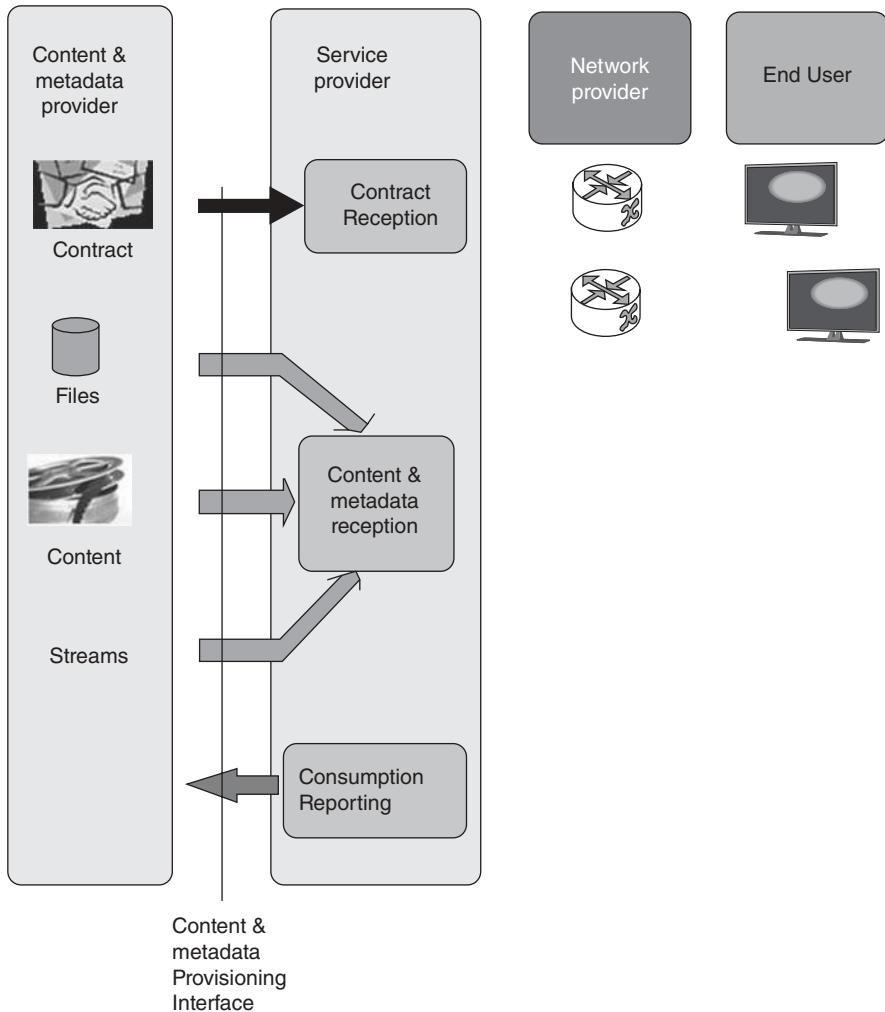


FIGURE 6.22 Relations between content providers and service providers.

Generally, however, a commercial environment supports a single IPTV service provider per network per administrative area. In the case where there is only one IPTV service provider on the network, or when there is a preconfigured service provider, the steps involved in the service discovery are as follows:

- *Step 1:* Discovery of IPTV service provider entry point.
- *Step 2:* Acquisition of the description of the IPTV services offered by the service provider and IPTV Service Selection.

In the case where there are several service providers and there is no pre-configured service provider, the steps involved in the service discovery entail interrogation of an “IPTV Service Provider Description Provider,” as follows:

Step 1: Discovery of the “IPTV Service Provider Description Provider” entry point.

Step 2: Acquisition of the description of the IPTV service providers and IPTV service provider selection.

Step 3: Acquisition of the description of the IPTV services provided by the selected service provider and IPTV service selection.

The starting entry point might be:

- An IPTV service provider description provider entry point (when there are several IPTV service providers on the network and no specific service provider entry point is defined in the terminal device configuration data).
- An IPTV service provider entry point (when there is only one IPTV service provider on the network or when a specific service provider entry point is defined in the terminal device configuration data). The IPTV service provider maybe running a web-based solution, a metadata-based one or a mixture of them.

Figure 6.23 depicts two examples showing how descriptions of available IPTV service providers can be acquired by terminal devices, when the entry point is an IPTV service provider description provider entry point; the first example makes use of HTTP or S-HTTP protocols, and the second example makes use of the IGMP protocol.

6.7.5 Service Navigation

Service Navigation (SN) is the process of presenting information that allows the end user to discover, select, and consume services. SN is critical to IPTV because there is, increasingly, a variety services on IPTV platforms. SN is generally realized via a service navigation interface that provides information on available services and content; examples of SN interfaces include EPG, Interactive Program Guide (IPG), Electronic Content Guide (ECG), and Electronic Service Guide (ESG). SN is supported by three abstract functional entities: metadata, navigation logic, and presentation (see Figure 6.24).

- Data
 - Metadata, structured, encoded data.
- Service Navigation Logic
 - Service navigation logic: a means to characterize the process in which service navigation is conducted through service navigation interface;

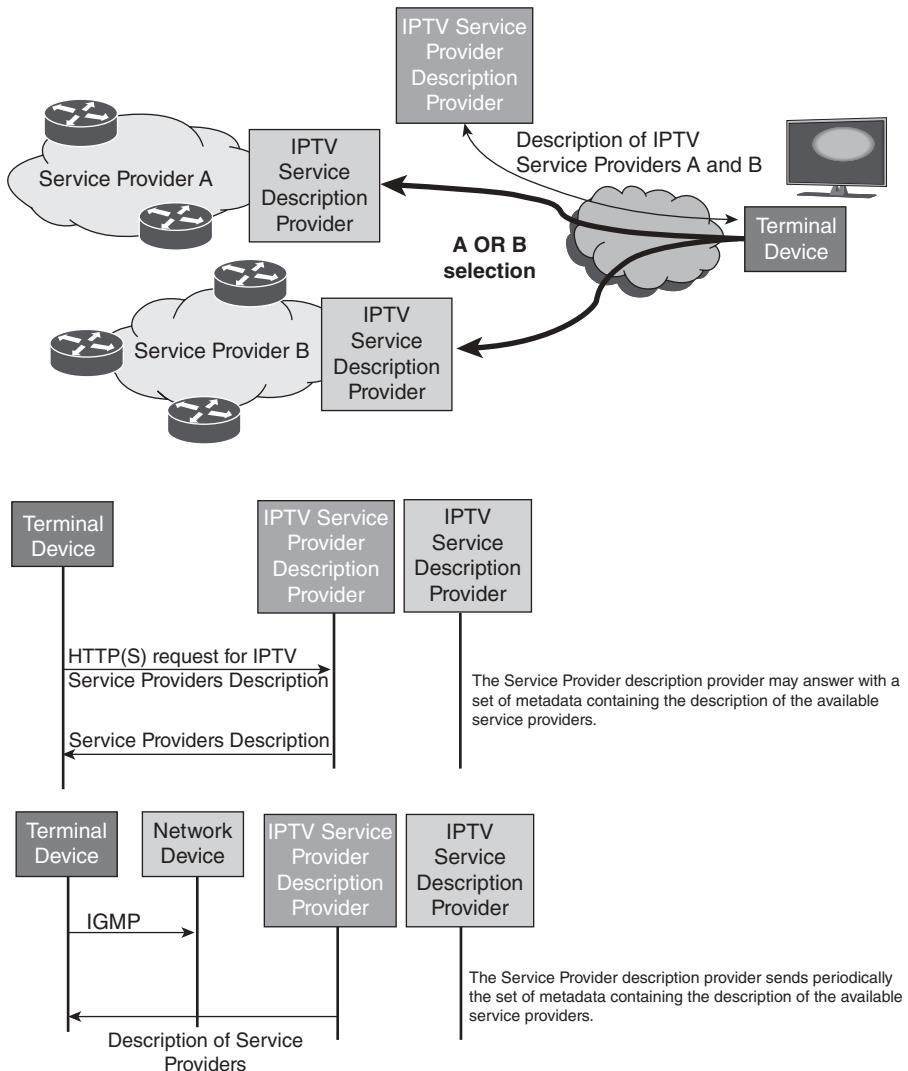
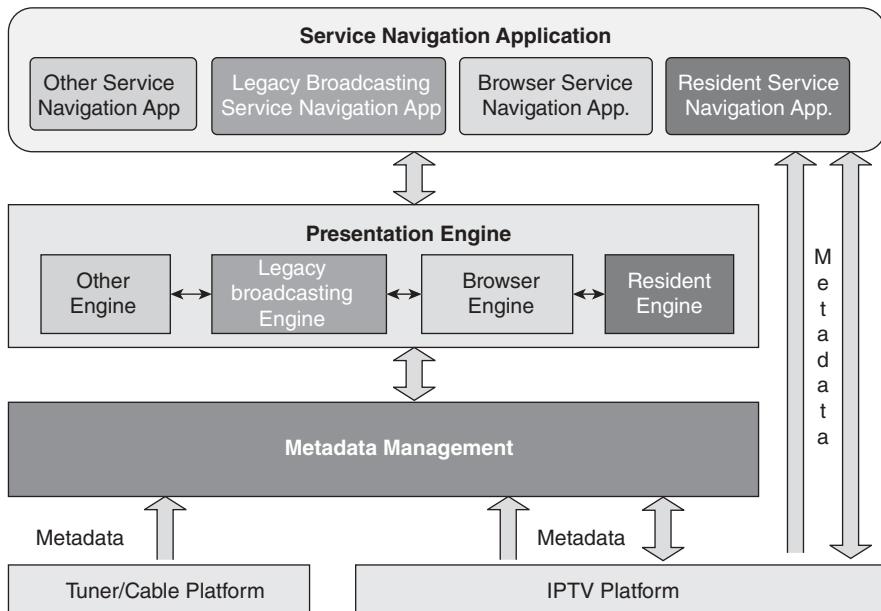


FIGURE 6.23 Request mechanism to get description of service providers. Top: Generic environment. Middle: HTTP or S-HTTP request to get the description of the available IPTV service providers. Bottom: IGMP join request to receive the description of the available IPTV service providers.

**FIGURE 6.24** SN system architecture.

- Service Navigation Logic Description: the description of the navigation logic in a clearly defined language;
- Navigation Logic Execution: the execution of the navigation logic described by the navigation logic description.
- Presentation
 - (Navigation) Presentation: the operation of rendering content in a form perceptible to a human being.
 - Presentation Description: the description, in a clearly defined language, of how the navigation logic is to be presented and displayed, for example, layout, design, and style, through service navigation interface.
 - Presentation Execution: the actual presentation and displaying of the service navigation logic through the service navigation interface according to the presentation description.

6.7.6 Electronic Program Guide

The EPG allows the customer to retrieve the program/content information as required, at any time; it supports retrieval capabilities, including fast search, semantic search, and quick selection. EPG information should be selectable by various methods, including keyword-based search and/or menu-driven selection for program. EPG can have customized capabilities, including on-demand feeding, transforming, filtering, and gathering functions. EPG should

typically support PVR applications (recording and storing). Using EPG information, the EPG application should support a recording operation for a selected program at client side as reservation basis and/or time-shift basis. It can also support multiple-recording operation, enabling one to simultaneously record the distinct programs that are selected by the user.

6.7.7 User Profiles

The IPTV standards support mechanisms for an IPTV service provider to collect information about user consumption of content and services over a period of time, for example: watched programs on broadcast TV channels, consumed CoD assets, and frequently used integrated IPTV and NGN services. The IPTV service provider can then use this information for IPTV content and service recommendations. Knowledge about users and their services is considered to be a key competitive advantage by service providers and Internet-based application providers [ALC201001].

The discussion in this subsection follows the concepts described by the ITU in reference [ITU200801]. Table 6.13 shows the characteristics basic profiles (user perspectives). In profile 1, users may recognize the IPTV service as terrestrial/cable/satellite digital TV service providing CoD service. In profile 2, users may recognize the IPTV service as internet service enabled TV. Users access web applications and Internet content with IPTV end devices. A complete set of IPTV service that satisfies all the requirements are provided in profile 3.

End devices are classified into five profiles based on their service capabilities, as shown in Table 6.14. End devices will be implemented with different profiles; therefore, compatibility between different profiles is required.

TABLE 6.13 Profiles on User Perspectives

	Profile 1	Profile 2	Profile 3
	TV/CoD over IP Network	Internet service-enabled TV	Complete IPTV on NGN
Service category	Linear/broadcast TV Content on demand	Web services Interactive data services	Telephony services Converged service
Content diversity	SP provisioned content	3rd-Party Content Internet content User-created content	Mobile IPTV service
Interactivity	Content selection/ view (Play/pause)	Various content manipulation (search, save, copy, transfer, etc.) Internet services	Telephony

TABLE 6.14 End Device Profile

	Profile 1			Profile 2	Profile 3
	Minimal 1	Minimal 2	Basic	Enhanced	Full
Channel	X		X	X	X
CoD		X	X	X	X
Interactive data and /or storage				X	X
Telephony					X

Table 6.15 lists the deliverable services for each profile, while Table 6.16 summarizes the target environment and required functionalities for each profile.

6.7.8 Protocol Support Machinery for Middleware, Application, and Content Platforms

Given the scope of functionality, a number of standards are needed and have emerged in recent years, as already highlighted to support middleware functions, including, but not limited to, H.740, H.750, H.760, H.761, and H.762.

- Recommendation ITU-T H.740—“*Application Event Handling for IPTV services*” enables enhanced two-way communication in IPTV environments by providing a framework of application event handling in IPTV services. For example, the framework supports interactive services, such as voting and e-commerce; it also supports emergency alerts and audience monitoring. The standard prescribes behavior for an IPTV terminal when receiving these instructions from either a broadcaster or a user. An application event is described as a specific user interaction or occurrence related with multimedia content. One of the characteristics of the new standard is that it provides privacy protection, with differing degrees of security [ITU200903].
- Recommendation H.750—“*High-level specification of metadata for IPTV services*” (also originally known as H.IPTV-MD) defines metadata required for EPG; it stipulates the elements of metadata necessary to realize various EPG services.
- Recommendation H.760—“*Multimedia Application Framework*” provides a basic framework for multimedia features; specifically, it defines a suite of multimedia applications that adds multimedia interactivity to IPTV content. As noted in earlier sections, IPTV not only supports streaming of video with defined QoS/QoE, but it is also supports bidirectional IP services and data streaming (see Figure 6.25.)

TABLE 6.15 Services for Each Profile

1st Level	2nd Level	Profile 1	Profile 2	Profile 3
Content	Channel	Linear/ broadcast TV and audio Broadcast ADV	Trick mode PPV NPVR Multi-angle PVR Content sharing User-created channel 3rd-party channel	Mobile IPTV Targeted ads
	On demand	Real/near content on demand	Push content on demand User-created content 3rd-party content	Mobile IPTV
	Content navigation	EPG Content advisory	IPG IPTV/Internet portal	
Interactive data			Internet access E-mail Chat Presence Interactive ad T-information (news, weather, transportation, and government) T-entertainment (games) T-commerce (banking, shopping, and ticketing)	Location-based services
Telephony based				SMS Caller ID Voice call/ conference Video call/ conference Converged service

TABLE 6.16 Target Environment and Required Functionalities

	Profile 1	Profile 2	Profile 3
Target end device	STB without storage	PC/STB with storage	PC/STB/mobile device with storage
Target network infrastructure	Wired IP network	Wired/wireless IP network	NGN, including mobile network
Target network QoS model	Best-effort or <i>Diffserv</i>	SLA-based QoS control	NGN QoS control
Security aspects	Content security(select/view only)	Content security (various manipulations)	Network security
QoS/performance aspects	Service security Dedicated/ Provisioned QoS	End device security Dynamic QoS	Dynamic QoS on NGN QoE/Performance monitoring
Middleware aspects	Content metadata	Content delivery/licensing metadata Content provisioning	User metadata
End system aspects	A/V format Terminal management	Remote management Home networking	
Network control aspects	Identification Stream control Transport packet format	Content distribution Session control	Multicast network control

- Recommendation H.761 “*Ginga-NCL for IPTV*” (also originally known as H.IPTV-MAFR.9) is based on the Ginga middleware component that has been used for digital broadcasting in Brazil. It is based on XML and is used as a facilitation language for other multimedia frameworks.
- Recommendation ITU-T H.762 “*Lightweight interactive multimedia framework for IPTV services (LIME)*” specifies a subset of html and javascript for use in IPTV terminals. LIME is strictly profiled so that it can be used on resource-limited devices, such as basic TV sets. LIME can support interactivity via widgets and portals, as well as AJAX-like applications on IPTV.* LIME can be used with basic services, such as VoD, linear (channel) service (over IP), and EPG (electronic/extended program guide). The expected main user interface is a remote controller [ITU200903].

ITU’s suite of IPTV standards, such as ITU-T H.761 (Ginga-NCL) and H.762 (LIME), enable value-added providers to develop innovative IPTV applications (e.g., enabling a product purchase by the end user).

*AJAX (Asynchronous JavaScript and XML) is a set of web development tools utilized to create asynchronous client-side web applications.

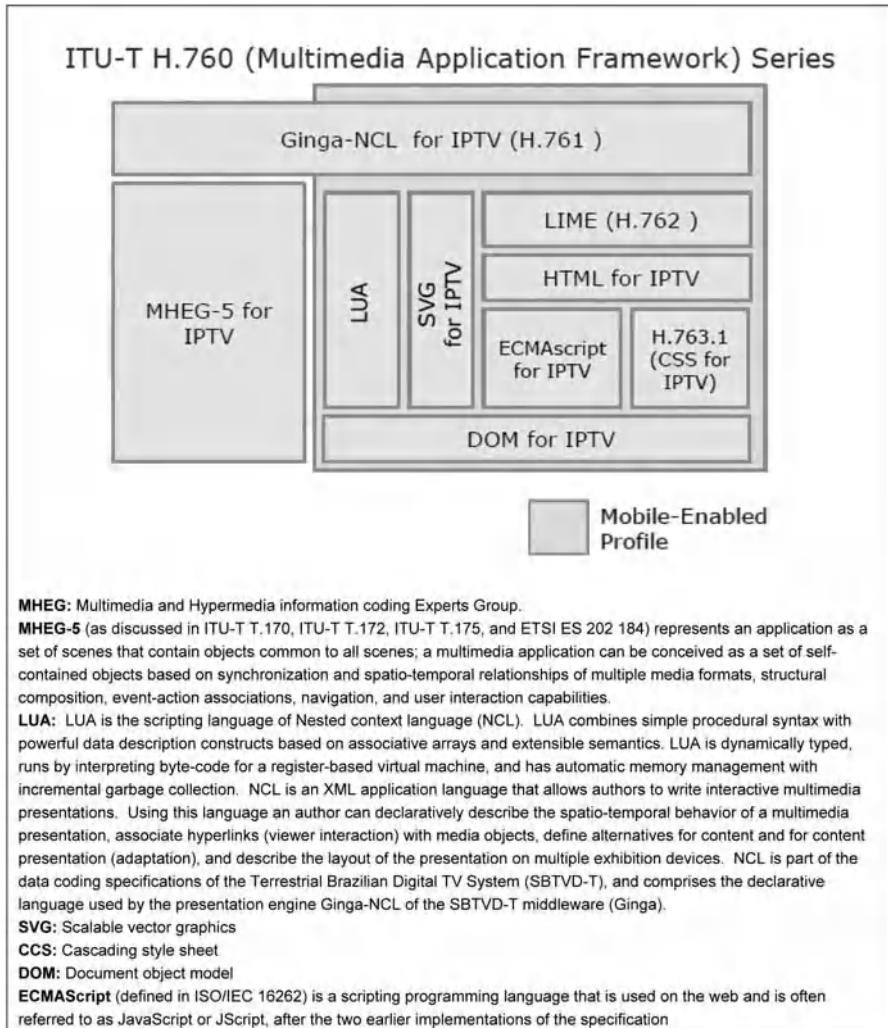


FIGURE 6.25 H.760.

6.8 IPTV STANDARDS: A COMPREHENSIVE PROCESS

We have discussed evolving recommendations in previous sections; here we provide a higher-level perspective. As already hinted earlier, and as it is generally accepted, standards have a significant effect on (1) the cost of products; on (2) the wide plethora of market offerings or lack thereof; on (3) the providers' interoperability; on (4) the barriers to service entry (by broadcasters, ISPs, telecoms service providers, or content providers) by lowering such barriers; and, on (5) limiting the phenomenon of “concept failure” due to limited industry support. Practitioners agreed that stable global standards are the key to

broad commercial deployment of IPTV, avoiding costly and confusing: “format wars” and reduced choice for consumers. Proprietary solutions may offer fast deployment in the short term, but in the medium and longer term, buyers will be subject to vendor lock-in, with the risk of costly future upgrades and reduced content and hardware choice. Industry consortia-based “standards” are mostly region-specific with little or no implementation [ITU201001]. Global standards provide for high service quality and lower cost.

6.8.1 ITU-T

The ITU’s Telecommunication Standardization Bureau articulates the drive for standards as follows [ITU200701]:

Standards are crucial for IPTV to reach its market potential and global audience. They are necessary in order to give service providers—whether traditional broadcasters, ISPs, cable operators or telecoms service providers—control over their platforms and their offerings. Standards . . . will encourage innovation, help mask the complexity of services, guarantee quality of service, ensure interoperability and, ultimately, help players remain competitive.

As implied by the earlier discussion, standardized video and audio coding in services delivered over IP are of fundamental importance. The use of H.264/AVC (Advanced Video Coding) video, VC 1 video,⁶ Application Visualization System (AVS) video,⁷ High-Efficiency Advanced Audio Coding Version 2 (HE AAC v2) audio, Extended Adaptive Multi-Rate Wideband⁸ (Extended AMR WB, also known as AMR WB+) audio, and AC-3 and Enhanced AC-3 audio⁹ is typical in the IPTV space. However, there is a lot more protocol- and

⁶VC-1 is the common name of the SMPTE 421M video codec standard. VC-1 was initially developed as a proprietary video format by Microsoft; in 2006, it was released as a formal SMPTE video standard. Currently, it is a widely used standard found in Blu-ray Discs, Windows Media, Slingbox and Microsoft’s Silverlight framework.

⁷Application Visualization System is a high-quality digital video format developed and maintained by Application Visualization System Inc. and is based on the DVI (Digital Video Interactive) technology. AVS is mostly utilized as a post-production tool to edit and process video files.

⁸AMR-WB+ is a 3GPP standard that supports mixed speech and audio content, providing high-quality sound across multiple content types, even at low and very low bit rates. AMR-WB+ provides high-quality music, speech-over-music, and speech-between-music, making it ideal to low-bit-rate mixed-content audio applications, such as multimedia streaming, mobile TV/radio broadcasts, podcasting, 3GPP Packet-switched Streaming Service (PSS), Multimedia Messaging Services (MMS), Multimedia Broadcast/Multimedia Service (MBMS), IP Multimedia Subsystem (IMS) Messaging Service, and other applications. AMR-WB+ extends the AMR-WB wideband speech codec standard by combining ACELP speech coding technology with advanced audio coding technology.

⁹Dolby Digital (AC-3) (also known as Audio Compression Version 3) is Dolby’s third generation audio coding algorithm. It is a perceptual coding algorithm that allows the use of lower data rates with a minimum of perceived degradation of sound quality. The signal contains up to six discrete channels of sound, but the common usage involves five channels for normal-range speakers. The AC3 audio standard is now being replaced with AAC, although AC3 audio will continue to be used for some time due to its wide deployment.

infrastructure-standardization work needed for the reliable delivery of IPTV services. Detailed standards are necessary for IPTV deployment to give service providers the means to offer the wide range of services expected in IPTV.

IPTV-related standards have been developed by a number of Standards Development Organizations, including the ITU-T, the ATIS, the IIF, the Digital Video Broadcasting (DVB), the Telecoms and Internet-Converged Services and Protocols for Advanced Networks (TISPAN) of the European Telecommunications Standards Institute (ETSI), and the Home Gateway Initiative (HGI).

The ITU-T¹⁰ formed an IPTV Focus Group (FG IPTV) in 2006 to ascertain what IPTV standardization activities would be kicked off and be of benefit to the stakeholder community. The follow-on phase of ITU's IPTV work—called the IPTV-GSI (for Global Standards Initiative)—intended to focus on speedy deployment of ITU-T Recommendations (standards) based on the output of the Focus Group as well as the detailed protocols necessary for global service deployment.

- Focus Group on IPTV (FG IPTV) (2006–2007) Responding to market demands for standard. First set of draft on Architecture, QoS, Security, End Systems, and Multimedia Application.
- IPTV Global Standardization Initiative (GSI) (2008–Present) Building on the work of Focus Group, Coordinating all ITU-T's IPTV-related activities. Comprising ITU-T Recommendations approved by six Study Groups (SGs 9, 11, 12, 13, 16, and 17).

The focus of the activity is to develop Series H; Series H is known as “*Audiovisual and Multimedia Systems: Infrastructure of Audiovisual Services—Communication Procedures*.” The press-time status of ITU standardization effort was as follows [CAM201101]:

- “Basic IPTV Service” Recommendations ready for TV services, VoD, and interactivity. Critical recommendations that have been developed (or existed) include the following (as discussed earlier at various points) (also see Appendix 6B):
 - Architecture, Network, and General Requirements: Y.1910 and Y.1901
 - Quality of Service and Experience: G.1080 series
 - Multimedia and Interactive Application: H.264 and H.760 series, including H.761 (NCL Ginga) and H.762 (LIME)
 - Metadata and Service Discovery: H.701 (Error Recovery), H.740 (Event Handling and Audience Measurement), H.750, and H.770

¹⁰General areas of standardization focus by the ITU-T include Next-Generation Networks (NGN), broadband access, multimedia services, emergency telecommunications, home networking, IP issues, optical networking, network management, ICT security issues, and fixed/mobile convergence.

- Home-networking: H.622.1, H.721 (IPTV Terminal Device)
- Security: X.1191
- Advanced features actively discussed
 - Audience measurement
 - Digital signage
 - 3DTV
 - Internet-sourced contents
 - Service over multiple devices
 - Widgets
- Conformance and Interoperability
 - Purpose of interoperability events (2010, 2011, etc.), where IPTV equipment/software conformance and interoperability have been tested
 - Conformance specifications
 - Implementation Guidelines—ongoing work

Tables 6.17 and 6.18 identify evolving interoperability IPTV standards that have been (or are being) developed; Table 6.17 focuses on ITU-T, while Table 6.18 identifies the broader suite of required standards (neither of these two tables are intended to be exhaustive.)

6.8.2 ATIS IPTV Interoperability Forum (IIF)

To address IPTV standardization, ATIS established the IIF. The IIF defines industry requirements, the overall industry reference architecture, and critical standards to support various aspects of IPTV delivery, including DRM and QoS. Since its establishment in July 2005, the ATIS IIF has produced a number of key requirements and framework documents to serve as the foundation for further development of IPTV specifications and standards [IIF200801]. Table 6.19 enumerates the various committees that were active at press time. Table 6.20 identifies some key recommendations being developed (at press time) by ATIS. In 2011, IIF released the standard “*IPTV Content on Demand Service*,” which specifies functions and interfaces for the delivery of an IPTV CoD service in a managed IP network. The CoD standard represented a key milestone for the IIF’s Phase 2 work, which is focused on interactive services, including CoD. The standard specifies asset preparation, efficient content distribution to service provider servers based on CDN principles, IMS, and non-IMS CoD session management for high QoE, and content delivery to users based on RTP/RTSP or HTTP streaming [IPT201101]. A CDN is a network that contains and is optimized to deliver content. It replicates content from the origin server to cache servers (also called replica servers), spread across the globe. Content requests are directed to the cache server closest to the user, and that server delivers the requested content [SJO200801]. The IIF’s Phase 3 aims at expanding the IPTV service offering to include support for Internet Sourced Content, adaptive streaming, and IPv6.

TABLE 6.17 Evolving Interoperability IPTV Standards (Key ITU-T Recommendations)

Category	Standard	Title/Topic
Architecture and services	Y.1901	IPTV Services Requirements
	Y.1910	IPTV Architecture
	Y.Sup5	ITU-T Y.1900 Series—Supplement on IPTV Service Use Cases
	Y.Sup7	NGN Release 2 Scope
	Y.2007	NGN Capability Set 2
	Q.3010	Authentication protocol
	G.1080	Quality of Experience Requirements for IPTV Services
	G.1081	Performance Monitoring Points for IPTV
	Y.1544	Multicast IP Performance Parameters
	G.1082	Measurement-based Methods for Improving the Robustness of IPTV Performance
Service quality and QoS/QoE models	X.1191	Functional Requirements and Architecture for IPTV Security Aspects
Security and content protection	H.701	Content Delivery Error Recovery for IPTV Services
	H.740	Application event handling for IPTV services
	H.750	High-Level Specification of Metadata for IPTV Services
	H.760	Overview of Multimedia Application Frameworks for IPTV
	H.761	Nested Context Language (NCL) and Ginga-NCL for IPTV Services
	H.762	LIME
	H.763.1	Cascading style sheets for IPTV services
	J.701	Broadcast-Centric IPTV Terminal Middleware
	J.700	IPTV Service Requirements and Framework for Secondary Distribution
	H.622.1	Architecture and Functional Requirements for Home Networks Supporting IPTV Services
Home networks	H.264	IPTV video
	H.720	Overview of IPTV Terminal Devices and End Systems
	H.721	IPTV Terminal Device, Basic Model
	H.770	Mechanisms for services discovery up to consumption for IPTV
	J.702	Enablement of Current Terminal Devices for the Support of IPTV Services
End systems		

TABLE 6.18 Evolving Interoperability IPTV Standards, Including IETF/Internet and Other Protocols (Partial List)

Standard	Description
ITU-T Y.1901	Recommendation ITU-T Y.1901 (2008), <i>IPTV services requirements</i>
ITU-T Y.1910	Recommendation ITU-T Y.1910 (2008), <i>IPTV architecture</i>
ITU-T H.610	Recommendation H.610 (2007), <i>Full service VDSL—System architecture and customer premises equipment.</i>
ITU-T H.701	Recommendation ITU-T H.720 (2008), <i>Content delivery error recovery for IPTV services</i>
ITU-T H.720	Recommendation ITU-T H.720 (2008), <i>Overview of IPTV terminal devices and end-systems</i>
ITU-T H.721	Recommendation ITU-T H.721 (2009), <i>IPTV terminal devices, Basic Model</i>
ITU-T H.740	Recommendation ITU-T H.740 (2010), <i>Application event handling for IPTV services</i>
ITU-T H.750	Recommendation ITU-T H.750 (2008) <i>High-level specification of metadata for IPTV services</i>
ITU-T H.770	Recommendation ITU-T H.770 (2009), <i>Mechanisms for service discovery up to consumption for IPTV</i>
ITU-T X.1191	Recommendation ITU-T X.1191 (2009), <i>Functional requirements and architecture for IPTV security aspects</i>
ITU-T Q.3402	Recommendation Q.3402 (2008), <i>NGN UNI signaling profile (Protocol Set 1)</i>
ITU-T Q.3040	Recommendation Q.3040 (2010), <i>IPTV Signaling Control Plane Architecture</i>
ITU-T X.1301	Recommendation X.1303(2007), <i>Common alerting protocol (CAP 1.1)</i>
ATIS-0800013	ATIS standard ATIS-0800013 (2008), <i>Media Formats and Protocols for IPTV services</i>
ATIS-0800017	ATIS standard ATIS-0800017 (2008), <i>Network Attachment and Initialization of Devices and Client Discovery of IPTV Services</i>
ATIS-0800042	ATIS standard ATIS-0800042 (2010), <i>IPTV Content on Demand Service</i>
ETSI TS 102 034	ETSI TS 102 034 v1.3.1 (2007), <i>Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks.</i>
ETSI TS 102 539	ETSI TS 1-2 539 V1.2.1 (2008), <i>Digital Video Broadcasting (DVB); Carriage of Broadband Content Guide (BCG) information over Internet Protocol (IP)</i>
ETSI TS 183 063	ETSI TS 183 063 V2.1.0 (2008), <i>Telecommunications and Internet converged Services and Protocols for Advances Networking (TISPAN); IMS-based IPTV stage 3 specification</i>

TABLE 6.18 (Continued)

Standard	Description
BBFF TR069	Broadband Forum TR-069 (2007), <i>CPE WAN Management Protocol</i>
IETF RFC 768	IETF RFC 768 (1980), <i>User Datagram Protocol (UDP)</i>
IETF RFC 959	IETF RFC 959 (1985), <i>File Transfer Protocol (FTP)</i>
IETF RFC 1350	IETF RFC1350 (1992), <i>The TFTP Protocol (Revision 2)</i>
IETF RFC 2131	IETF RFC 2131(1997), <i>Dynamic Host Configuration Protocol</i>
IETF RFC 2236	IETF RFC 2236 (1997), <i>Internet Group Management Protocol, Version 2</i>
IETF RFC 2250	IETF RFC 2250 (1998), <i>RTP Payload Format for MPEG1/MPEG2 Video</i>
IETF RFC 2326	IETF RFC 2326 (1998), <i>Real Time Streaming Protocol (RTSP)</i>
IETF RFC 2616	IETF RFC 2616 (1999), <i>Hypertext Transfer Protocol—HTTP/1.1</i>
IETF RFC 2782	IETF RFC 2782 (2000), <i>A DNS RR for specifying the location of services (DNS SRV)</i>
IETF RFC 2818	IETF RFC 2818 (2000), <i>HTTP over TLS</i>
IETF RFC 3261	IETF RFC 3261 (2002), <i>SIP: Session Initiation Protocol</i>
IETF RFC 3376	IETF RFC 3376 (2002), <i>Internet Group Management Protocol, Version 3</i>
IETF RFC 3550	IETF RFC 3550 (2003), <i>RTP: A Transport Protocol for Real-Time Applications</i>
IETF RFC 3810	IETF RFC 3810 (2004), <i>Multicast Listener Discovery Version 2 (MLDv2) for IPv6</i>
IETF RFC3920	IETF RFC3920 (2004), <i>Extensible Messaging and Presence Protocol (XMPP): Core</i>
IETF RFC3921	IETF RFC3921 (2004), <i>Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence</i>
IETF RFC3926	IETF RFC3926 (2004), <i>FLUTE—File Delivery over Unidirectional Transport</i>
IETF RFC4330	IETF RFC 4330 (2006), <i>Simple Network Time Protocol (SNTP) Version4 for IPv4, IPv6 and OSI</i>
IETF RFC4301	IETF RFC4301 (2005), <i>Security Architecture for the Internet Protocol</i>
IETF RFC 4825	IETF RFC 4825 (2007), <i>The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)</i>
W3C XML	World Wide Web Consortium (W3C) Recommendation XML1.0 (2008), <i>Extensible Markup Language (XML) 1.0, Fifth Edition</i>
W3C SOAP	World Wide Web Consortium (W3C) <i>Recommendation SOAP 1.2 (2007), Simple Object Access Protocol (SOAP)</i>
ETSI TS 181 016 V2.0.0 (2007-11)	<i>Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service Layer Requirements to integrate NGN services and IPTV</i>

(Continued)

TABLE 6.18 (Continued)

Standard	Description
ETSI TS 181 014 V2.0.0 (2007-11)	<i>Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements for network transport capabilities to support IPTV services.</i>
ETSI TS 182 028 V2.0.0 (2008-01)	<i>Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; Dedicated subsystem for IPTV functions</i>
ETSI TS 182 027 V2.0.0 (2008-02)	<i>Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; IPTV functions supported by the IMS subsystem</i>
ETSI TS 183 063 V2.0.10 (2008-04) DTS/TISPAN-03127-NGN-R2	<i>Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IMS based IPTV Stage 3 specification—Approved as 17TD022r1</i>
ETSI TS 183 064 V0.1.1 (2008-06) DTS/TISPAN-03137-NGN-R2	<i>Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Dedicated IPTV subsystem stage 3 specification (Pending TB approval)</i>

TABLE 6.19 ATIS IIF Committees

Committee	Role
Architecture (ARCH) Committee	The ARCH Committee develops IPTV architecture requirements, specifications, protocols, and other documents required to enable deployment of a standardized, interoperable, access-agnostic IPTV service.
IPTV Security Solutions (ISS) Committee	The ISS Committee develops security standards with emphasis on a security requirements framework and an integrated toolkit of security functions that can be utilized for an interoperable solution for enabling IPTV services.
Metadata and Transaction Delivery (MTD) Committee	The MTD Committee develops standards that define metadata elements, the representation of metadata elements, and the content of application level transactions where the MTD Committee is the primary developer of metadata standards in support of all ATIS IIF Committees.
Quality of Service Metrics (QoSM) Committee	The QoSM Committee develops standards that define metrics, models, and approaches for measurement and reporting of QoS and QoE for IPTV services.
Testing & Interoperability (T&I) Committee	The T&I Committee develops the necessary test scripting and test planning for the interoperability of ATIS IIF standards and addresses IPTV interoperability issues, providing recommended courses of action for mitigation of the identified issues.

TABLE 6.20 ATIS IIF Standards and Specifications Under Development at Press Time

Standard/Specification	Description
IPTV Linear Broadcast Service	Describes the service capabilities associated with the delivery of the Linear/Broadcast TV service to the end user.
IPTV Multicast Network Service Specification	Describes a simple IP multicast service that the network provider can offer for use as a basis for a linear/broadcast TV service. The specification will focus on the service requirements from the perspective of the IPTV service provider rather than detail-specific implementation mechanisms within the network operator domain.
Media Protocols Specification for IPTV	Defines the media protocols for IPTV service, including the protocols used for actual audio and video media delivery over IP. Reliability techniques applied at the IP layer and above will also be considered, including QoS marking, Forward Error Correction at the application or transport layer, and retransmission.
Content Acquisition Latency	Examines the question of the latency of acquiring a content stream and the methods of reducing said latency. Technical Report on IPTV Advertising explores the range of IPTV advertising services and lists high-level requirements for IPTV-related advertising.
IPTV QoE Model Requirements and Model Definition	Supports the estimation of end-to-end quality, incorporating all the factors that would impact the user experience in real time. These would include media transmission path quality metrics, video codec and loss concealment, and factors that affect playback control.
Categorized Listing of Fault Codes for IPTV	Defines a standard set of fault codes that cause the improper functioning of an IPTV service or component. The type of fault is a vital input to service assurance, test, fault and performance operations, and systems.
Test Plan for Evaluation of Quality Models for IPTV Services	Describes subjective and objective test plans appropriate for the formal evaluation of objective video quality prediction algorithms.
Application Level Interfaces (API) Interoperability Specification for IPTV	Addresses the need for interoperable DRM Application Programming Interfaces.

(Continued)

TABLE 6.20 (Continued)

Standard/Specification	Description
Security Robustness Rules	Facilitates interoperability and encourages product innovation while maintaining standardized procedures, interfaces, and platforms with respect to secure transmission and storage of materials.
Distribution of IPTV Content in the Subscriber's Authorized Service Domain	Identifies requirements for interoperability of the system and components necessary to share protected content in the IPTV/DRM security environment. Managing the Trust Hierarchy Standardizes the management mechanisms that establish trust within a Trust Hierarchy including, for example, revocation of certificates, additions of new Certificate Authorities, and specifications of rules for handling various aspects of the operation of the Trust Hierarchy.
Consumer Domain Configuration Metadata Requirements Specification for IPTV	Establishes requirements for metadata associated with configuration of consumer domain devices—specifically the Delivery network Gateway (DNG) and the IPTV Terminal Function (ITF)—during network attachment, initialization, configuration and remote management.
IPTV Metadata Consumer Requirements Specification	Establishes basic consumer (subscriber and user) profile and preferences metadata requirements for an IPTV Consumer Metadata Specification/Standard.

6.8.3 Commercial Products and Interworking

Beginning in 2010, the ITU-T has started a series of conformance and interoperability test events for ITU-T H.700 series of IPTV products, known as Interop Event. Table 6.21 lists the initial Events. These events seek to test and demonstrate product interoperability of ITU-T IPTV standards, including ITU-T H.701 (Error Recovery), ITU-T H.721 (IPTV Terminal), ITU-T H.740 (Application Event Handling), ITU-T H.750 (Metadata), ITU-T H.761 (Ginga-NCL), ITU-T H.762 (LIME), and ITU-T H.770 (Service Discovery).

As a proof of the success of the standardization effort, many companies are now selling TV and STB products based on ITU-T's IPTV Terminal Standard ITU-T H.721, with products already available in countries, including Brazil, China, Japan, Republic of Korea, France, and elsewhere. The customer can purchase a TV or PC at a retail shop, connect to network, and receive an IPTV service. Cisco, Mitsubishi, NEC, NTT, OKI, Panasonic, Sumitomo, TVStorm, among others, have already built and tested products conforming to ITU-T Recommendations. In China and Japan, services based on ITU-T IPTV stan-

TABLE 6.21 IPTV Interoperability Events Sponsored by the ITU-T

Interop Event	Date/Location	Participants
The 1st Interop event	From July 20–23, 2010 in Geneva (ITU HQ)	Various Carriers and media companies
The 2nd Interop event	From September 23–27, 2010 in Singapore (Fusionopolice)	Cisco, Mitsubishi, NEC, NTT, OKI, PUC-Rio, Sumitomo, TVStorm, and V One Multimedia
The 3rd Interop event and showcase	December 14–17, 2010 in Pune (Sinhgad Polytechnic)	New participants: Tech Mahindra
The 4th Interop event and showcase	From July 18–22, 2011 in Rio de Janeiro	IOT participants: OKI, PUC-Rio, Sumitomo, and TOTVS
New test case: H.761 (Ginga NCL) and H.762 (LIME)		Showcase participants: Mitsubishi, OKI, PUC-Rio, Sumitomo, TOTVS, and ZTE

dards are being deployed and already reaches several million subscribers [ITU201001], [NIS201101], [CAM201101]. A test service was being conducted in Singapore at press time, and there was interest in setting up test beds in India and Canada.

REFERENCES

- [3GP201101] 3GPP2, “The Third Generation Partnership Project 2 (3GPP2),” <http://www.3gpp2.org>.
- [ALC201001] Alcatel Lucent, “IMS Integrated IPTV with Multi-Screen Foundation Delivering content with enriched communication across different end-user devices,” Technology Whitepaper, 2010.
- [ATI200601] ATIS, “*IPTV Architecture Requirements* ATIS standard ATIS-0800002,” 2006.
- [CAM201101] S. Campos, “ITU IPTV standards—the key for the successful development of IPTV,” ITU-T SG 16 “Multimedia,” 4th Annual Vietnam Telecoms International Summit, June 1–2, 2011.
- [HEY201001] J. Heynen, “IPTV and video equipment and service markets hampered by slowing subscriber growth,” Infonetics Research, Press Release, January 5, 2010, Campbell, CA.
- [IIF200801] Alliance for Telecommunications Industry Solutions, “IPTV Interoperability Forum, ATIS,” November 2008, 1200 G Street NW, Suite 500, Washington, DC 20005, <http://www.atis.org>.
- [IPT201101] Staff, “IPTV News, ATIS releases two new IPTV standards” March 10, 2011, Online Magazine. <http://www.ipv-news.com>.

- [ITU200601] ITU, “WG 1 (Requirement and Architecture of IP TV) meeting report, FG IPTV-MR-0001,” 1st FG IPTV meeting: Geneva, 10–14 July 2006, International Telecommunication Union, Telecommunication Standardization Bureau, Place des Nations, CH-1211 Geneva 20.
- [ITU200602] ITU-T, “ITU-T Newslog—NGN functional architecture described in key recommendation,” October 02, 2006.
- [ITU200603] International Telecommunication Union, “ITU-T Recommendation Y. 2012” (09/2006)—Functional requirements and architecture of the NGN release 1.
- [ITU200701] International Telecommunication Union, “ITU announces first global set of standards for IPTV Specifications will fuel market for next-generation services,” Press Release, December 18, 2007, Telecommunication Standardization Bureau, Place des Nations, CH-1211 Geneva 20.
- [ITU200801] M. Johnson, “ITU-T IPTV Focus Group Proceedings, ITU-T,” 2008. Telecommunication Standardization Bureau, Place des Nations, CH-1211 Geneva 20.
- [ITU200901] International Telecommunication Union, “ITU-T Recommendation Y. 1901” (01/2009)—Requirements for the support of IPTV services, clause 3.2.15.
- [ITU200902] International Telecommunication Union, “New IPTV Standard supports Global Rollout,” February 3, 2009. International Telecommunication Union, Telecommunication Standardization Bureau, Place des Nations, CH-1211 Geneva 20.
- [ITU200903] International Telecommunication Union, “New standards bring interactivity to IPTV,” November 2009. International Telecommunication Union, Telecommunication Standardization Bureau, Place des Nations, CH-1211 Geneva 20.
- [ITU201001] International Telecommunication Union, “ITU Interop Event Highlights IPTV Interoperability—Future of television will rest on stable global standards, say experts,” July 27, 2010. International Telecommunication Union, Telecommunication Standardization Bureau, Place des Nations, CH-1211 Geneva 20.
- [ITU201101] ITU-T Technical Paper, “HSTP-IPTV-PITD Delivery and control protocols handled by IPTV terminal devices,” Series H: Audiovisual And Multimedia Systems: Infrastructure of audiovisual services—Communication procedures, Telecommunication Standardization Sector Of ITU, 25 March 2011.
- [MIN199501] D. Minoli, *Video Dialtone Technology: Digital Video over ADSL, HFC, FTTC, and ATM*, McGraw-Hill, 1995.
- [MIN200801] D. Minoli, *IP Multicast with Applications to IPTV and Mobile DVB-H*, Wiley, 2008.
- [MOR200601] N. Morita, “Functional architecture model of NGN,” ITU-T Workshop on Next Generation Networks, Hanoi, Vietnam, 15–16 May 2006.
- [NIS201101] H. Nishimoto, “ITU-T IPTV-GSI, Workshop on Harmonization of Web and IPTV Technologies, Overview of ITU-T H.721 Recommendation for IPTV Terminal Device,” Rio de Janeiro, Brazil, July 21, 2011.
- [OIP200801] Open IPTV Forum (OIPF), “Services and Functions for Release 2 [V1.0]-[2008-10-20],” 2008, Open IPTV Forum, 650 Route des Lucioles—Sophia Antipolis, Valbonne, France.
- [OIP200901] Open IPTV Forum (OIPF), “Content Metadata, Release 1 Specification [V1.1]-[2009-10-08],” 2009, Open IPTV Forum, 650 Route des Lucioles—Sophia Antipolis, Valbonne, France.
- [SCR201101] Screen Digest, “European Broadband Cable 2011 Report,” June 2011, Issue number 477, August 2011, www.ScreenDigest.com, Screen Digest Limited, Lymehouse Studios, 30-31 Lyme Street, London, NW1 0EE.

[SJO200801] D. Sjöberg, “Content Delivery Networks: Ensuring quality of experience in streaming media applications,” TeliaSonera International Carrier, CDN White Paper, August 14, 2008.

[YAM200901] H. Yamamoto, “Standardization Trends of Internet Protocol Television (IPTV) and Activities Undertaken by OKI,” *Oki Technical Review*, Special Issue on Networks, October 2009/Issue 215, Vol. 76, No.2, pages 86 ff.

APPENDIX 6A NEXT-GENERATION NETWORKS (NGN) AND IP MULTIMEDIA SUBSYSTEM (IMS)

This appendix provides a short description of NGN and IMS. The interested reader may consult ITU-T documentation for additional details.

6A.1 NGN

In ITU-T’s parlance, NGN is a packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. The NGN architecture supports the delivery of services, such as multimedia services, conversational services, and content delivery services (e.g., video streaming and broadcasting); it also supports generalized mobility to allow consistent and ubiquitous provision of services to users. Recommendation Y.2012 *Functional requirements and architecture of the NGN Release 1* describes the functional architecture of the NGN [ITU200603]. NGN functional architecture incorporates the following principles (also see Figure 6A.1) [ITU200602]:

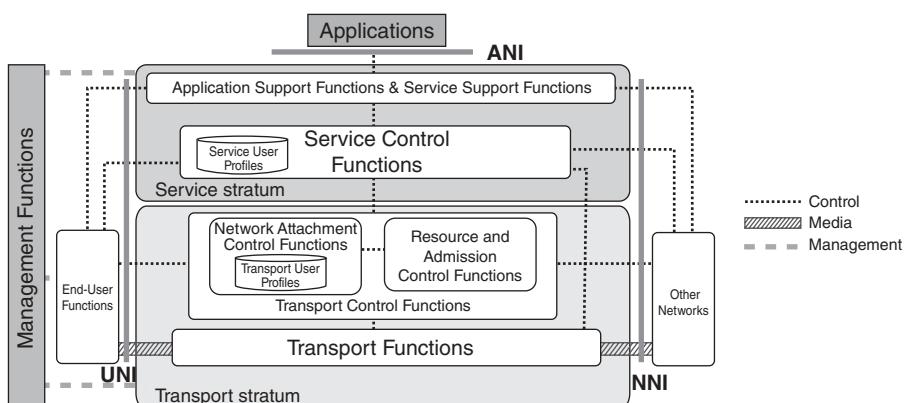


FIGURE 6A.1 NGN architecture.

- *Support for Multiple Access Technologies:* The NGN functional architecture offers the configuration flexibility needed to support multiple access technologies.
- *Distributed Control:* This will enable adaptation to the distributed processing nature of packet-based networks and support location transparency for distributed computing.
- *Open Control:* The network control interface is open to support service creation, service updating, and incorporation of service logic provision by third parties.
- *Independent Service Provisioning:* The service provisioning process is separated from transport network operation by using the above-mentioned distributed, open control mechanism. This is intended to promote a competitive environment for NGN development in order to speed up the provision of diversified NGN services.
- *Support for Services in a Converged Network:* This is needed to generate flexible, easy-to-use multimedia services, by tapping the technical potential of the converged, fixed-mobile functional architecture of the NGN.
- *Enhanced Security and Protection:* This is the basic principle of an open architecture. It is imperative to protect the network infrastructure by providing mechanisms for security and survivability in the relevant layers.
- *Functional Entities Incorporate the Following Principles:*
 - Functional entities may not be distributed over multiple physical units, but may have multiple instances.
 - Functional entities have no direct relationship with the layered architecture. However, similar entities may be located in different logical layers.

6A.2 IMS

IMS is a subsystem providing call processing and a variety of multimedia services in an IP-based packet-switching domain [MOR200601] (see Figure 6A.2)

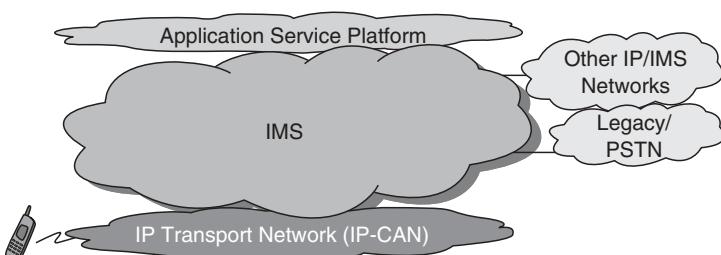


FIGURE 6A.2 IMS environment.

- Provides voice, video, presence, messaging, conferencing, and other services
- Complies with IETF standardized session control (SIP); profiling
- Independent of the access network
- The application service platform itself is outside the scope of IMS

NGNs can be based on IMS capabilities. Here, the architecture centers on SIP proxy-equivalent Call Session Control Functions (CSCFs). The architecture employs a separation model that decouples media processing elements and their controlling elements. Links to transmission systems is through a well-defined Gq interface, as illustrated in Figure 6A.3.

An example of a basic capability is the ability to support Roaming, as illustrated in Figure 6A.4. In IMS nomenclature, the SIP proxy function is called the CSCF. IMS defines a mobile destination (roaming destination) SIP server (proxy CSCF) in addition to the subscribing SIP server (serving CSCF) to

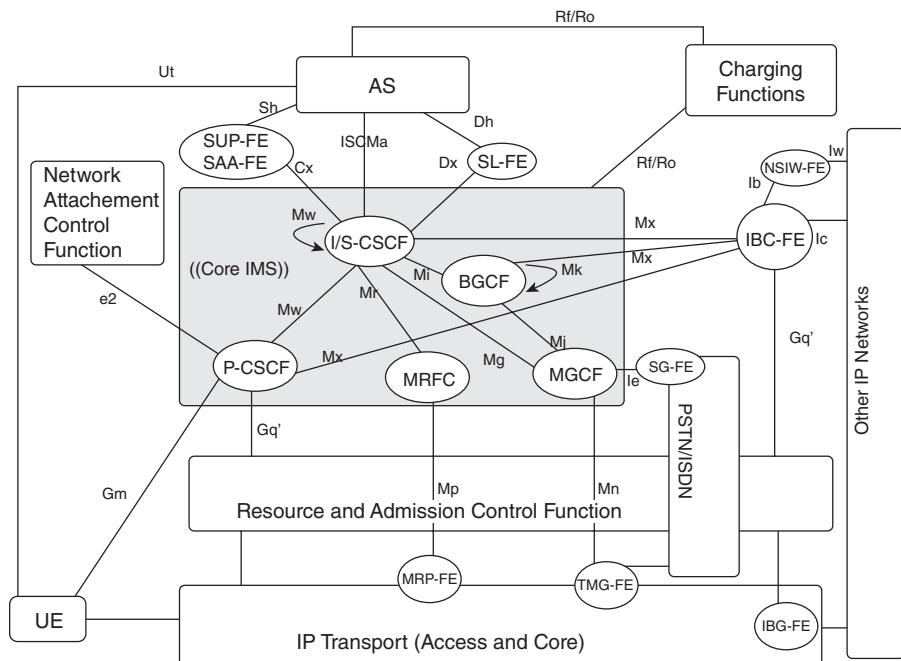


FIGURE 6A.3 NGNs based on IMS capabilities. AS, application server; BGCF, breakout gateway control function; CSCF, serving CSCF; HSS, home subscriber server; IP-CAN, IP-connectivity control interface; MGCF, media gateway control function; MGW, media gateway; MRFC, multimedia resource function controller; MRFP, multimedia resource function processor; P-CSCF, proxy CSCF; SLF, subscription locator function.

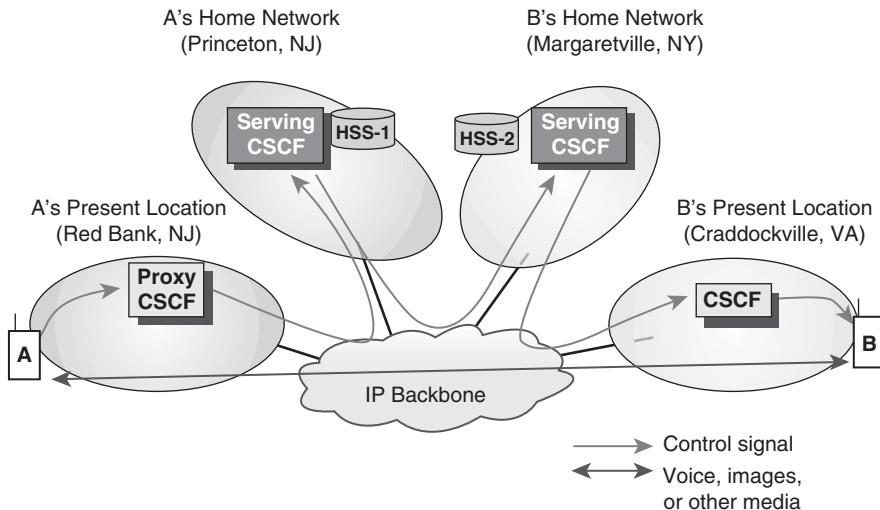


FIGURE 6A.4 Roaming support.

allow authentication and QoS control by the mobile-destination network. IMS presumes that the serving CSCF cannot be accessed directly (a walled garden) [MOR200601]. In IMS, a CSCF is assigned to a user each time the user is registered (at power up). SIP signals from another network are first sent to the interrogating CSCF and then forwarded to the assigned CSCF. The interrogating CSCF has a topology hiding internetwork gateway function that can be deployed on the exit side as well. Fixed-network NGN discussions are permitting the deployment of a border gateway control function, which is different type of SIP proxy from an interrogating CSCF.

APPENDIX 6B IPTV PROTOCOLS USED BY IPTV TERMINAL DEVICES

This discussion, loosely based on/summarized from the ITU-T Technical Paper, “HSTP-IPTV-PITD Delivery and Control Protocols” [ITU201101] identifies protocols used by IPTV terminal devices; these protocols are utilized for functions ranging from the initialization of an IPTV terminal device, up to consumption of IPTV services by such device. Figure 6B.1 depicts functional reference points utilized in the discussion. The motivation for including protocols is driven by the fact that standardization positively impacts costs, functionality, and commercial rollout timetables.

6B.1 Network Attachment: E9

Preconfigured IPTV terminal devices may be employed in some instances with service discovery information; however, automated methods generally

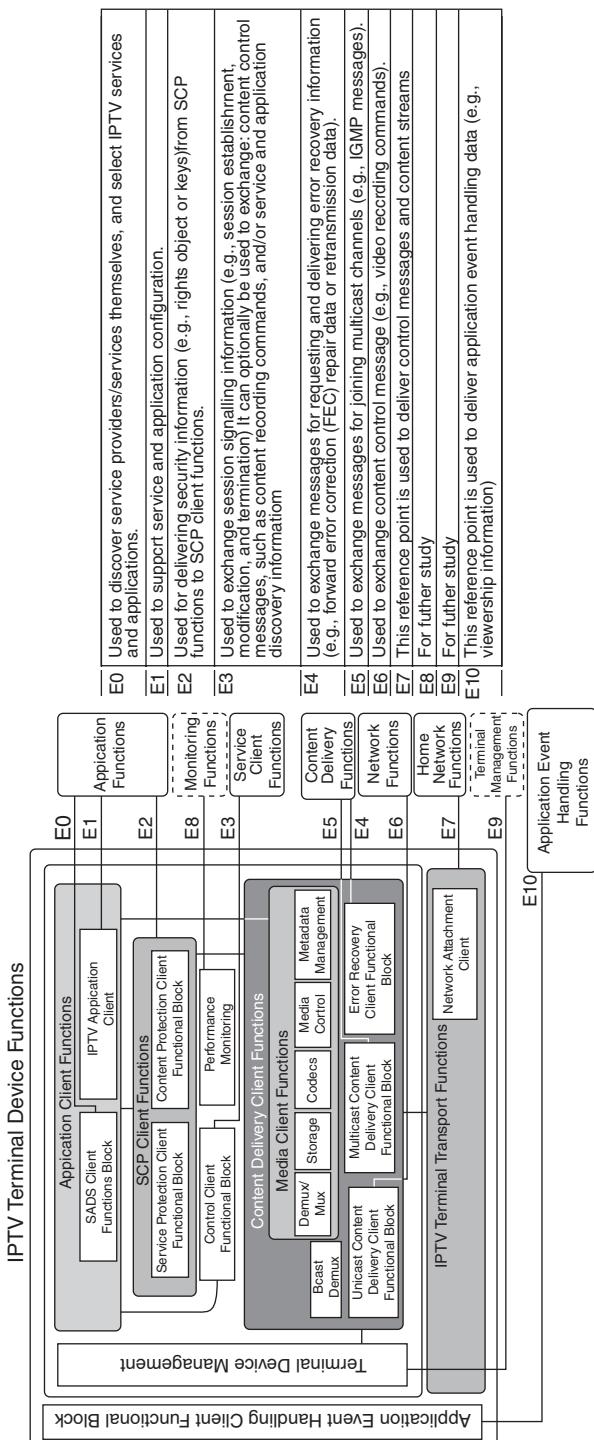


FIGURE 6B.1 Reference points on protocols of IPTV terminal devices.

work better. The followings are protocols for handling entry data of service discovery:

- DHCP-based methods:
 - DHCP (IETF RFC 2131): By using “Container Option,” service discovery information can be delivered when IPTV terminal device acquires network information such as its own IP address from a DHCP server.
 - Download methods (aka Pull mode).
 - IPTV terminal device may download information using unicast based procedure such as TFTP (IETF RFC 1350), HTTP.
- TR-069 protocol (Broadband Forum) based method:
 - Remote management system can provide addressing information of service providers with TR-069 protocol (BBF TR069).
- Multicast delivery method (aka Push mode):
 - SI delivery using IGMP/MLD and/or DVBSTP is the popular way to deliver service discovery information.
 - FLUTE multicast stream can deliver service information files to IPTV devices (ETSI TS 102 472).
- DNS Service Records (SRV)-based method. The result of DNS SRV (IETF 2782) lookup can provide available IPTV service servers within the specified Domain Name.

6B.2 Service Discovery at Various Interface Points

Service Discovery contains two processes: service provider discovery and service discovery. The former process used service provider information, the later uses detailed service offer information.

Service Provider Information Delivery Protocol(s): E0, E3, E5 Available transport mechanisms for the delivery of the descriptions of IPTV service providers over IP networks are as follows:

- HTTP Version 1.1 (IETF RFC 2616) for “Service Provider Information” delivery over unicast (“pull mode”)
- HTTP over TLS (IETF RFC 2818) for “Service Provider Information” delivery over unicast with secure manner (“pull mode”)
- IGMP Version 2 (IETF RFC 2236) for “Service Provider Information” delivery over IPv4 multicast (“push mode”)
- IGMP Version 3 (IETF RFC 3376) for “Service Provider Information” delivery over IPv4 multicast (“push mode”)
- MLD Version 2 (IETF RFC 3810) for “Service Provider Information” delivery over IPv6 multicast (“push mode”)

- DVBSTP (ETSI TS 102 034): a light protocol specified by DVB, used for delivery over multicast (push mode)
- FLUTE (ETSI TS 102 472) for “Service Provider Information” delivery over IPv4/IPv6 multicast (push mode)
- SIP (IETF RFC 3261) for “Service Provider Information” delivery over SIP (“push mode” or “pull mode”)
- TR-069 (BBF TR069) for “Service Provider Information” delivery

Detailed Service Offer Information Delivery Protocol: E0, E5, E6 Available transport mechanisms for delivery of the descriptions of IPTV services offered by an IPTV service provider are as follows:

- HTTP 1.1 (IETF RFC 2616) for “Detailed Service Offer” delivery over unicast (“pull mode”)
- HTTP over TLS (to be confirmed for the use of HTTPS)
- IGMP Version 2 (IETF RFC 2236) for “Detailed Service Offer” delivery over IPv4 multicast (“push mode”)
- IGMP Version 3 (IETF RFC 3376) for “Detailed Service Offer” delivery over IPv4 multicast (“push mode”)
- MLD Version 2 (IETF RFC 3810) for “Detailed Service Offer” delivery over IPv6 multicast (“push mode”)
- DVBSTP (ETSI TS 102 534): a light protocol specified by DVB, used for delivery over multicast (“push mode”)
- FLUTE (ETSI TS 102 472) for “Detailed Service Offer” delivery over IPv4/IPv6 multicast (push mode)
- SIP (IETF RFC 3261) for “Detailed Service Offer” delivery over SIP (“push mode” or “pull mode”)
- TR-069 (BBF TR069) for “Detailed Service Offer” delivery

6B.3 Service Navigation: E0

Following query mechanism is optionally used to access ECG/EPG/IPG information.

- SOAP (W3C SOAP) over HTTP. This is a possible approach for acquiring and retrieving service discovery information using remote procedure call (RPC)
- XCAP (IETF RFC4825) over HTTP XCAP (lightweight protocol based on HTTP for real-time aspects) over HTTP is another method for direct manipulation of elements and attributes within service discovery information.

6B.4 Service Consumption

This section describes protocols depending on IPTV services (e.g., Linear TV and VoD).

Linear TV Service Delivery Protocol: E5 Linear TV services (characterized as the equivalent of the traditional broadcast like TV and radio) are streamed continuously over IP multicast. The element “Service Location” in the “Detailed Service offer” records gives all the information required to access Linear TV services. IPTV terminal devices can receive or stop the reception of Linear TV services simply by issuing the appropriate multicast control messages. Linear TV services may be encoded as MPEG-2 Transport Streams (TS), encapsulated either in RTP or directly in UDP. Relevant standards are as follows:

- MPEG-2 TS (ETSI TS 101 154) Implementation guidelines for the use of Video and Audio Coding in Broadcasting Applications based on the MPEG-2 Transport Stream.
- UDP (IETF RFC 768) simply for delivery of data.
- RTP payload format (IETF RFC 2250) specifies a data format for MPEG-1/MPEG-2 Video.
- RTP (IETF RFC 3550) specifies a transport protocol for real-time applications.
- Full service VDSL (ITU-T H.610) specifies system architecture and customer premises equipment for VDSL.

Linear TV Service Control Protocol: E5 Relevant standards are as follows:

- IGMP Version 2 (IETF RFC 2236) for Linear TV delivery over multicast (“push mode”)
- IGMP Version 3 (IETF RFC 3376) for Linear TV delivery over multicast (“push mode”)
- MLD Version 2 (IETF RFC 3810) for Linear TV delivery over multicast (“push mode”)

VoD Service Delivery Protocol: E6 VoD services are encoded as MPEG-2 Transport Streams encapsulated either in RTP or directly in UDP. Relevant standards are as follows:

- MPEG-2 TS (ETSI TS 101 154) Implementation guidelines for the use of Video and Audio Coding in Broadcasting Applications based on the MPEG-2 Transport Stream
- UDP (IETF RFC 768) for simply content delivery
- RTP payload format (IETF RFC 2250) specifies a RTP payload format for MPEG-1/MPEG-2 Video

- RTP (IETF RFC 3550, ATIS-0800042) specifies a transport protocol for real-time applications
- Full service VDSL (ITU-T H.610) specifies system architecture and customer premises equipment

VoD Service Control Protocol: E6 IPTV terminal devices can receive or stop the reception of VoD services simply by issuing the appropriate control messages. Relevant standards are as follows:

- RTSP (IETF RFC 2326) (ATIS-0800042) for handling real-time data streaming

6B.5 Download Services

Content download services allow for the download of contents to local storages of the IPTV terminal devices. The content download services may support two different download modes:

- Push download mode that is defined as distribution of contents where the distribution decision is taken by the service providers, without explicit requests from the users.
- Pull download mode provides download services at explicit request of users.

This implies the supports of both multicast and unicast download. Download of a file from a single server and download of the files in chunks from multiple servers are supported. A reception reporting procedure allows the IPTV terminal devices to report the successful download of content.

Download Service Delivery Protocol: E5, E6 Relevant standards are as follows:

- FTP (IETF RFC 959) for delivery over unicast
- FLUTE (IETF RFC 3926) for acquiring data over multicast. This protocol may be combined with a file repair mechanisms
- HTTP/1.1 (IETF RFC 2616, ATIS-0800042) for delivery over unicast
- HTTPS (IETF RFC 2818, ATIS-0800042) for data delivering over HTTP in a secure manner

Download Service Control Protocol: E5, E6 Relevant standards are as follows:

- FTP (IETF RFC 959) for controlling delivery over unicast
- HTTP/1.1 (IETF RFC 2616, ATIS-0800042) for controlling delivery over unicast

6B.6 Other Relevant Protocols

Well-known protocols for supporting IPTV services are noted here.

Time Synchronization It is useful to synchronize automatically all timers of IPTV terminal devices connecting an IP network. Following well-known protocol provides such functionality. Relevant standards are as follows:

- (IETF RFC 4330) Simple network time protocol (SNTP)

Security/Privacy IPTV terminal devices are required to support secure communication depending on types of IPTV services (e.g., e-commerce). Relevant standards are as follows:

- HTTPS (IETF RFC 2818) for data delivering over HTTP in a secure manner

Performance Monitoring at E6 IPTV terminal devices can periodically send performance monitoring reports to a network side management functionality by issuing the appropriate RTSP or RTCP messages (via Interface E6). Relevant standards are as follows:

- RTSP (IETF RFC 2326) for reporting the status of IPTV terminal devices
- RTCP XR (IETF RFC 3611) for reporting a set of status relevant to QoS

Application Event Handling

General Notification Delivery Methods: E10

Relevant standards of transport mechanisms for the delivery of application event data and metadata over an IP network are as follows:

- HTTP Version 1.1 (IETF RFC 2616) for application event or metadata delivery over unicast
- HTTP over TLS (IETF RFC 2818) for application event or metadata delivery over unicast in a secure manner
- TFTP (IETF RFC1350) for application event or metadata delivery over unicast
- FLUTE (IETF RFC 3926) for application event or metadata delivery over multicast

The transports mechanisms for the delivery are not limited in the above lists.

Emergency Telecommunications (ET) ET includes any emergency-related service that requires special handling from networks or specific service orga-

nizations relative to other services. This includes government-authorized emergency services and public safety services.

Common Alerting Protocol: The Common Alerting Protocol (CAP) (ITU-T X.1303) is an XML (W3C XML)-based data format for exchanging public warnings and emergencies between alerting technologies. CAP allows a warning message to be consistently disseminated simultaneously over many different warning systems to many applications. Detailed relation between CAP and an emergency alert service as an event handling application is consulted in (ITU-T H.740).

Delivery Methods over E10: Relevant standards of transport mechanisms for the delivery of emergency alert data over IP are as follows:

- RTP (IETF RFC 3350)/UDP (IETF RFC 768) for ET event or meta-data delivery over unicast.

The transports mechanisms for the delivery are not limited in the above descriptions.

Event Gathering Over E10 There is a need for an interface for aggregation of events from the IPTV terminal devices. One example of such an event gathering is audience measurement. Relevant standards of transport mechanisms for gathering data from IPTV terminal devices are as follows:

- SOAP(W3C SOAP) over HTTP/HTTPS
- TFTP (IETF RFC1350) for delivery of data if the event data is file-based format;
- XMPP (IETF RFC3920)(IETF RFC3921) for delivery of data when it transmits small messages in real time, rather than storing files into batches, such as TFTP;
- UDP over IPsec (IETF RFC4301) for delivery of event data in a secure manner.

The transports mechanisms for the gathering are not limited in the above.

7 Technologies for Internet-Based TV

Because of the fundamental importance of the Internet in the evolving framework of next-generation TV, this chapter surveys some key technical and architectural aspects of state-of-the-art technologies related to the Internet; these include streaming (also known as streaming media), Content Delivery Networks (CDNs), Peer-to-Peer (P2P) systems, cloud computing, and Internet backbones and access networks. The sections that follow explore these technologies at some level of detail.

To support Internet-Based TV (IBTV), one needs very high capacity backbone networks (transmission and routing), high-speed access networks, high capacity (virtualized) storage systems, and Internet-ready TVs and/or set-top boxes (STBs). These technologies, in the aggregate, support the widespread deployment of IBTV services; indeed, observers note that from a volume-of-traffic perspective packet-based data communications are being replaced by video and rich media traversing the evolving provider networks. These themes are discussed in this chapter. Note, however, it is not the intent of this chapter to exhaustively cover all pertinent and/or underlying Internet technologies that support IBTV, but to survey a basic subset of such technologies.

7.1 STREAMING

Streaming is the process of receiving and (dis)playing a multimedia file while it is still downloading; it allows a user view content (video, but also just sound in some cases) as it is being downloaded using a World Wide Web browser plug-in or other STB/over-the-top (OTT) capabilities. Naturally, such a system (network connection, content/web server, storage, etc.) needs to support an adequate level of Quality of Service/Quality of Experience (QoS/QoE). Video streaming architectures can be classified as (1) server to single client unicast, (2) server multicasting to several clients, (3) P2P unicast distribution, where each peer forwards packets to another peer, and, (4) P2P multicasting, where each peer forwards packets to several other peers [D32200701].

Streaming protocols are commands, processes, and procedures that can be used to select, set up, and start the playing, as well as the pausing, recording, and tear down of streaming sessions. We already discussed the importance of standardized protocols in previous chapters. H.264-based MPEG-4 is the video format of choice for video publishers and distributors, such as Netflix®, MLB, and iTunes among others; these content providers require secure streaming protocols to deliver or stream their video assets to the video player. Other streaming services provide open-access streaming. Encoded video is typically delivered or streamed using one of several possible streaming formats/protocols such as: HTTP Live Streaming, HTTP Dynamic Streaming, and Smooth Streaming.¹ Players implemented in HTML5, Flash, and Silverlight receive these streams and play them out for the viewer [PHI201101]. From a deployment perspective, the most commonly used video delivery protocols at press time were as follows: Real-Time Transport Protocol/Real-Time Streaming Protocol (RTP/RTSP) streaming protocols, Apple HTTP Live Streaming (HTTP Adaptive Streaming running on the Apple iPhone/iPad), and HTTP Flash progressive download. Table 7.1 provides a short list of key nonvendor-specific streaming protocols.

One commercial example of video streaming is Netflix and the Netflix Video Streaming Protocol. Netflix is an online movie rental service offering flat-fee subscription plans for DVD and Blu-ray disc rental-by-mail and video streaming. Netflix claims a growing catalog of over 100,000 titles and over 25 million subscribers; titles include not only movies, but many television series, documentaries, and anime. Netflix's video streaming service accounts for more than 20% of downstream Internet traffic during peak times in the United States, according to a study based on data collected from more than 200 cable, DSL, and mobile service providers in the summer of 2010 [BRE201101]. The quality of the video streams that Netflix delivers is equal to, and in some cases even surpasses, that found on DVD video, but the user's available bandwidth and the processing power of their computer affect the quality of the video stream as well. Netflix's minimum streaming bandwidth requires 564 Kbps, which provides a pixel resolution of approximately 512×288 ; the best possible quality video requires up to 5 Mbps and provides a resolution of 720 lines of vertical resolution.

As another example of commercial video streaming, in 2011, Amazon unveiled its Amazon Prime unlimited video streaming service, an offering that competes with Netflix. The viewer can use Amazon's new unlimited streaming service to watch more than 5000 movies and TV shows on a Mac or Windows PC, as well as select set-top boxes and Internet-connected TVs (CTVs). Amazon Prime's video streaming is free with an annual \$79 Prime membership fee [PAU201101].

¹HTTP Live Streaming is backed by Apple, Smooth Streaming is backed by Microsoft, and HTTP Dynamic Streaming is backed by Adobe; they all use MPEG-4 H.264 for video encoding.

TABLE 7.1 Key Nonproprietary Protocols Used in Streaming Applications (Partial List)

Protocol	Description
Hypertext Transfer Protocol (HTTP)	An application-level, stateless, object-oriented protocol for distributed, collaborative, hypermedia information systems.
Real-Time Streaming Protocol (RTSP)	An IETF protocol that is used for continuous (streaming) of audio and video sessions. It provides the control for playing, stopping, media position control (e.g., fast forward) via bidirectional communication sessions. An application-level protocol for control of the delivery of data with real-time properties. It embodies an extensible framework to enable controlled, on-demand delivery of real-time audio and video data; it uses Transmission Control Protocol (TCP) or/or the User Data Protocol (UDP), depending on function.
Real-Time Transport Protocol (RTP)	An IETF protocol (a set of commands and processes) that is used to add timing and sequence information to each packet to allow the reassembly of packets to reproduce real time audio and video information. It is a UDP-based packet format and set of conventions that provides end-to-end network connectivity functions suitable for applications transmitting real-time data, such as audio, video, and so on , over multicast or unicast network services.
Real-Time Transport Control Protocol (RTCP)	(Also known as RTP Control Protocol) Control protocol that works in conjunction with RTP to control performance and for diagnostic purposes. RTCP control packets are periodically transmitted by each participant in an RTP session to all other participants.
Session Description Protocol (SDP)	A media description specification used for describing multimedia sessions for the purposes of session announcement, session invitation, and session initiation.

Up to now, Internet service provided by Cable TV companies in the United States generally offer higher throughput than service provided by traditional telephone companies, but this could change in the future. Fortunately, many streaming mechanisms, including HTTP Live Streaming, Smooth Streaming, and HTTP Dynamic Streaming, are based on Adaptive Bit Rate Streaming mechanisms; this allows the stream to adapt the video experience to the quality of the network and the device's processing capability. The video stream can increase or decrease the bit rate and resolution of the video in real time so that it is always streaming the best possible quality the available network connection can support. This flexibility is particularly important for wireless/smartphone applications.

7.1.1 Real-Time Transport Protocol/Real-Time Streaming Protocol (RTP/RTSP)

RTSP (described in RFC 2326 in 1998) is an application-level protocol that provides a robust mechanism for streaming multimedia applications utilizing unicast and/or multicast delivery techniques. Being a recognized standard, it provides interoperability between clients and servers from distinct vendors. RTSP establishes and controls either a single or several time-synchronized streams of continuous media, such as audio and video. It does not typically deliver the continuous streams itself, although interleaving of the continuous media stream with the control stream is possible. Effectively, RTSP acts as a “network remote control” for multimedia servers. RFC 4567 (July 2006) proposed extensions for Session Description Protocol (SDP) and RTSP to address security considerations; the goal was to define a security profile for the protection of real-time applications running over RTP.

RTP (described in RFC 1889 and in RFC 3550) provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video. These services include payload type identification, sequence numbering, timestamping, and delivery monitoring. Applications typically run RTP on top of User Data Protocol (UDP) to make use of its multiplexing and checksum services; both protocols contribute parts of the transport protocol functionality. RTP may also be used with other suitable underlying network or transport protocols. RTP supports data transfer to multiple destinations using multicast distribution if provided by the underlying network [SCH200301].

Real-Time Transport Control Protocol (RTCP) (also described in RFC 3550) is based on the periodic transmission of control packets to all participants in the session, using the same distribution mechanism as the data packets. The underlying protocol provides multiplexing of the data and control packets, for example, using separate port numbers with UDP. The primary function of RTCP is to provide feedback on the quality of the data distribution; this is an integral part of the RTP’s role as a transport protocol and is related to the flow and congestion control functions of other transport protocols. See Figure 7.1 for a pictorial view.

As an ensemble, a video streaming system includes the basic functionality of creating, delivering, and displaying the video content; the main elements of a complete video streaming system include the encoding station, the video server, the delivery network infrastructure, and the playback client. The video server supports the delivery of video to clients using the appropriate network transport protocols; it is comprised of a hardware platform that is optimally configured for the delivery of real-time video. At the end-user station, the video player client receives and buffers the video stream and displays it in the appropriate size window for the screen in question.

Streaming media can be accessed as follows:

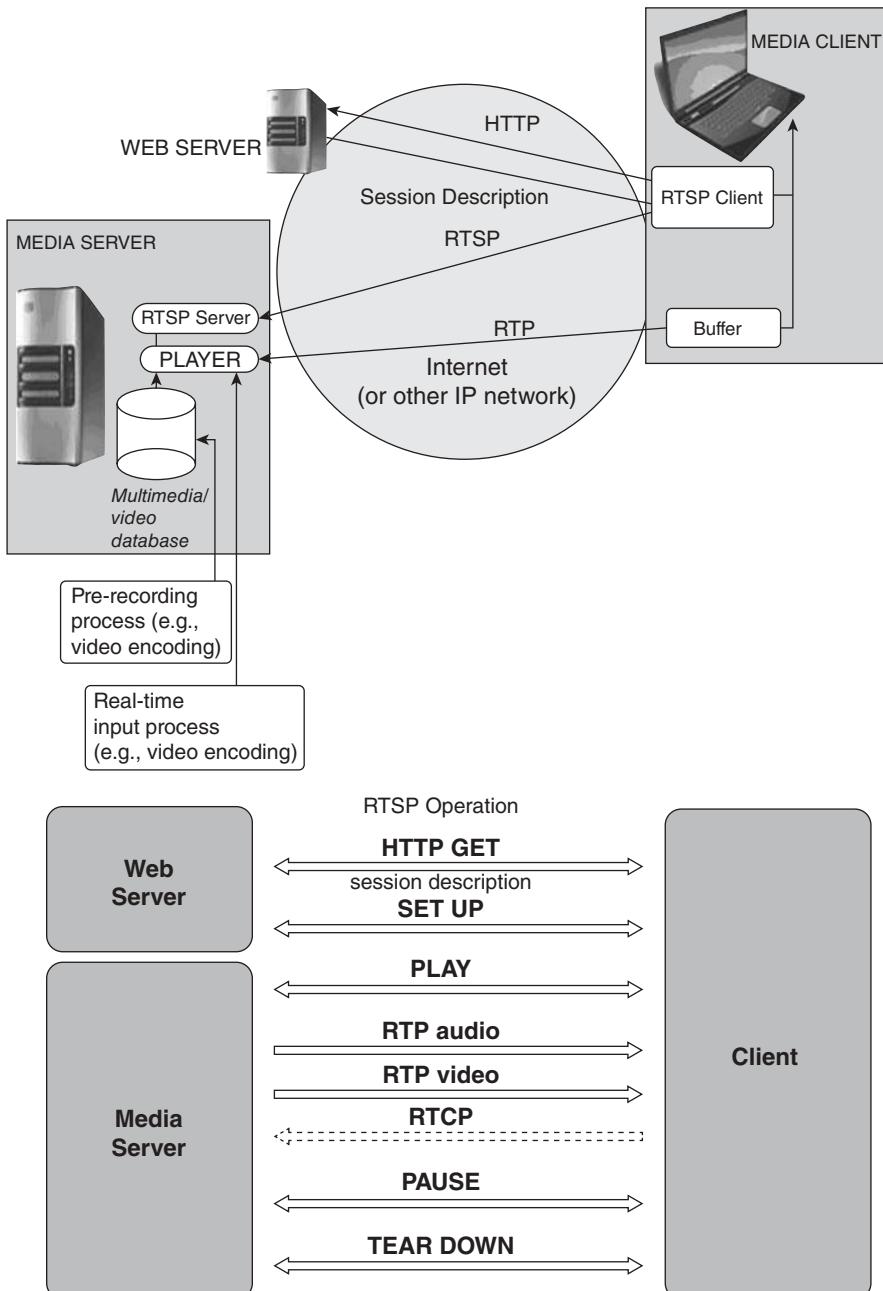


FIGURE 7.1 Simplified protocols interaction to support streaming.

- *On-Demand*: A clip is available to a specific end user whenever he/she wants it. The user has “trick modes” (that is can fast-forward, rewind, or pause the clip). This type of video content (clip) is prerecorded. Unicast-ing methods are employed.
- *Linear (Live)*: A user can gain access to the action that is happening in real time. Note that a user does not have “trick modes” (i.e., cannot not fast-forward or rewind through the clip). Content can be delivered using unicasting or multicasting.

A brief overview RTSP is provided below based on concepts from RFC 2326 [SCH199801]. The set of (video) streams to be controlled is defined by a presenta-tion description. There is no notion of an RTSP connection; instead, a server maintains a session labeled by an identifier. An RTSP session is not tied to a transport-level connection, such as a Transmission Control Protocol (TCP) connection. During an RTSP session, an RTSP client may open and close many reliable transport connections to the server to issue RTSP requests. Alternatively, it may use a connectionless transport protocol, such as UDP. The streams controlled by RTSP may use RTP, but the operation of RTSP does not depend on the transport mechanism used to carry continuous media. It also may interact with HTTP in that the initial contact with streaming content is often to be made through a web page. RTSP has some overlap in functionality with HTTP. The media streams are left unspecified by RTSP; it only specifies the control. The streams could be RTP streams, or any other form of media transmission; it is up to the client and server software to maintain the mapping between the control channel and the media streams. The protocol supports the following operations:

- *Retrieval of Media from Media Server*: The client can request a presenta-tion description via HTTP or some other method. If the presentation is being multicast, the presentation description contains the multicast addresses and ports to be used for the continuous media. If the presenta-tion is to be sent only to the client via unicast, the client provides the destination for security reasons.
- *Invitation of a Media Server to a Conference*: A media server can be “invited” to join an existing conference, either to play back media into the presentation or to record all or a subset of the media in a presentation. This mode is useful for distributed teaching applications. Several parties in the conference may take turns “pushing the remote control buttons.”
- *Addition of Media to an Existing Presentation*: Particularly for live presenta-tions, it is useful if the server can inform the client about additional media becoming available.

Several modes of operation can be distinguished:

- *Unicast*: The media is transmitted to the source of the RTSP request, with the port number chosen by the client. Alternatively, the media is transmit-ted on the same reliable stream as RTSP.

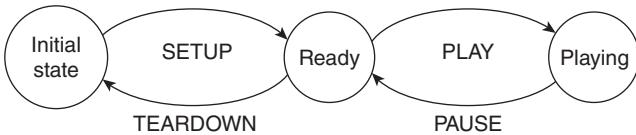


FIGURE 7.2 Basic RTSP state machine.

- *Multicast, Server Chooses Address:* The media server picks the multicast address and port. This is the typical case for a live or near-media on-demand transmission.
- *Multicast, Client Chooses Address:* If the server is to participate in an existing multicast conference, the multicast address, port, and encryption key are given by the conference description.

RTSP maintains a certain amount of process state; Figure 7.2 depicts a basic state machine that illustrates the minimal state.

The following functions (called “methods” in the RTSP context) play a central role in defining the allocation and usage of stream resources on the server: SETUP, PLAY, RECORD, PAUSE, and TEARDOWN.

- *Setup:* Causes the server to allocate resources for a stream and start an RTSP session.
- *Play and Record:* Starts data transmission on a stream allocated via SETUP.
- *Pause:* Temporarily halts a stream without freeing server resources.
- *Teardown:* Frees resources associated with the stream. The RTSP session ceases to exist on the server.

See Table 7.2 for a more complete list of functions.

The RTSP Operation is as follows. To send a control request, the client constructs a line consisting of the method, the request URL, and the protocol version number. Then, the client includes a general header, a request header, and possibly an entity header. The control request is sent to the server, which, if possible, executes the request. The control requests and responses may be sent over either TCP or UDP; because the order of the requests matters, the requests are sequenced, so if any requests are lost, they must be retransmitted. The server then returns a response containing a status line, general response, and entity headers; the status line contains the protocol version, the numeric status code, and a textual description. RTSP works by first requesting a presentation to be started by a server, receiving in return a session identifier which it then uses in all subsequent controls. Eventually, the client can request the teardown of session, which releases the associated resources. The session identifier represents the shared state between the client and server [CAL200201].

TABLE 7.2 RTSP Methods

Method	Description	Direction
Options	Get available methods. An OPTIONS request may be issued at any time, for example, if the client is about to try a nonstandard request. It does not influence server state.	C → S, S → C
Describe	The DESCRIBE method retrieves the description of a presentation or media object identified by the request URL from a server.	C → S
Announce	Get description of media object. The ANNOUNCE method serves two purposes: (1) When sent from client to server, ANNOUNCE posts the description of presentation or media object identified by the request URL to a server. (2) When sent from server to client, ANNOUNCE updates the session description in real-time.	C → S, S → C
Setup	The SETUP request for a Uniform Resource Identifier (URI) specifies the transport mechanism to be used for the streamed media. A client can issue a SETUP request for a stream that is already playing to change transport parameters, which a server may allow.	C → S
Play	Start playback, reposition. The PLAY method tells the server to start sending data via the mechanism specified in SETUP.	C → S
Record	Start recording. This method initiates recording a range of media data according to the presentation description. The timestamp reflects start and end time (UTC).	C → S
Redirect	Redirect client to new server. A redirect request informs the client that it must connect to another server location. It contains the mandatory header Location, which indicates that the client should issue requests for that URL (Uniform Resource Locator.)	S → C
Pause	Halt delivery, but keep state. The PAUSE request causes the stream delivery to be interrupted (halted) temporarily.	C → S
Get_parameter	The GET_PARAMETER request retrieves the value of a parameter of a presentation or stream specified in the URI.	C → S, S → C
Set_parameter	Device or encoding control. This method requests to set the value of a parameter for a presentation or stream specified by the URI.	C → S, S → C
Teardown	Remove state. The TEARDOWN request stops the stream delivery for the given URI, freeing the resources associated with it.	C → S

Note: C, Client; S, Server.

7.1.2 Apple HTTP Live Streaming

Apple HTTP Live Streaming (HLS) allows the streaming audio or video to iPhone, iPod touch, iPad, or Apple TV; it supports streaming live events without special server software and the distribution of Video On Demand (VoD) with encryption and authentication. HLS is a mechanism to send audio and video over HTTP from a web server to client software on the desktop or to iOS-based devices. It is possible that in the future HLS may expand beyond just iOS devices. Android, Google's mobile OS, is now capable of playing HLS video thanks to a company called Nextreaming, which has built a HLS player SDK for the Android platform. Furthermore, HLS is no longer a just a mobile video mechanism. Roku, which makes set-top streaming players, now supports HLS. Perhaps, most importantly, several major video publishers, such as ABC, Netflix, and Hulu, are taking advantage of HLS in their iPad Apps [PHI201101].

HTTP Live Streaming² allows one to send audio and video over HTTP from an ordinary web server for playback on iOS-based devices—including iPhone, iPad, iPod touch, and Apple TV—and on desktop computers (Mac OS X). HTTP Live Streaming supports both live broadcasts and prerecorded content (VoD). HTTP Live Streaming supports multiple alternate streams at different bit rates, and the client software can switch streams intelligently as network bandwidth changes. HTTP Live Streaming also provides for media encryption and user authentication over HTTPS, allowing publishers to protect their work. An example of a simple HTTP streaming configuration is shown in Figure 7.3. All devices running iOS 3.0 and later include built-in client software for HTTP Live Streaming. The Safari browser can play HTTP streams within a webpage on iPad and desktop computers, and Safari launches a full-screen media player for HTTP streams on iOS devices with small screens, such as iPhone and iPod touch. Apple TV 2 (and later) includes an HTTP Live Streaming client. Many existing streaming services require specialized servers to distribute content to end users. These servers require specialized skills to set up and maintain, and in a large-scale deployment this can be costly. HTTP Live Streaming avoids this by using standard HTTP to deliver the media. Additionally, HTTP Live Streaming is designed to work seamlessly in conjunction with media distribution networks for large-scale operations. The HTTP Live Streaming specification is also an IETF Internet-Draft [PAN201101].

HTTP Live Streaming sends audio and video as a series of small files, typically of about 10-second duration, called media segment files. An index file, or playlist, gives the clients the URLs of the media segment files. The playlist can be periodically refreshed to accommodate live broadcasts, where media segment files are constantly being produced. One can embed a link to the playlist in a webpage or send it to an app.

²This information in the next few paragraphs is summarized and synthesized from Apple sources [APP201101].

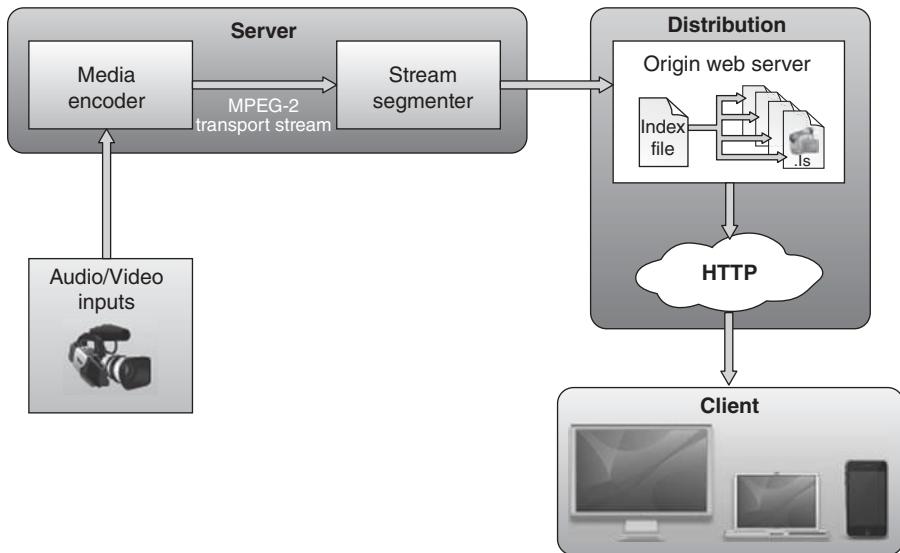


FIGURE 7.3 Apple HTTP live streaming environment.

For VoD from prerecorded media, Apple provides a free tool to make media segment files and playlists from MPEG-4 video or QuickTime movies with H.264 video compression, or from audio files with Advanced Audio Coding³ (AAC) or MP3 compression. The playlists and media segment files can be used for VoD or streaming radio. For live streams, Apple provides a free tool to make media segment files and playlists from live MPEG-2 transport streams carrying H.264 video, AAC audio, or MP3 audio. There are a number of hardware and software encoders that can create MPEG-2 transport streams (TS) carrying MPEG-4 video and AAC audio in real time. Either of these tools can be utilized to encrypt the media and generate decryption keys. One can use a single key for all the streams, a different key for each stream, or a series of randomly generated keys that change at intervals during a stream. Keys are further protected by the requirement for an initialization vector, which can also be set to change periodically.

Conceptually, HTTP Live Streaming consists of three parts: the server component, the distribution component, and the client software.

- The *server component* is responsible for taking input streams of media and encoding them digitally, encapsulating them in a format suitable for delivery, and preparing the encapsulated media for distribution.

³AAC is a standardized, lossy compression and encoding scheme for digital audio intended to be the successor of the MP3 format.

- The *distribution component* consists of standard web servers. They are responsible for accepting client requests and delivering prepared media and associated resources to the client. For large-scale distribution, edge networks or other CDNs can also be used.
- The *client software* is responsible for determining the appropriate media to request, downloading those resources, and then reassembling them so that the media can be presented to the user in a continuous stream. Client software is included on iOS 3.0 (and later) and computers with Safari 4.0 (or later) installed.

In a typical configuration, a hardware encoder takes audio-video input, encodes it as H.264 video and AAC audio, and outputs it in an MPEG-2 TS, which is then broken into a series of short media files by a software stream segmenter. These files are placed on a web server. The segmenter also creates and maintains an index file containing a list of the media files. The URL of the index file is published on the web server; client software reads the index, then requests the listed media files in order and displays them without any pauses or gaps between segments.

A noted, input can be live or from a prerecorded source. It is typically encoded as MPEG-4 (H.264 video and AAC audio) and packaged in an MPEG-2 TS by off-the-shelf hardware. MPEG-2 TSs should not be confused with MPEG-2 video compression. The TS is a packaging format that can be used with a number of different compression formats; audio-only content can be either MPEG-2 transport or MPEG elementary audio streams, either in AAC format with Audio Data Transport Stream (ADTS) headers or in MP3 format. The MPEG-2 TS is then broken into segments and saved as a series of one or more .ts media files; this is typically accomplished using a software tool, such as the Apple Stream Segmenter. Audio-only streams can be a series of MPEG elementary audio files formatted as either AAC with ADTS headers or as MP3. The segmenter also creates an index file. The index file is an .M3U8 playlist. The index file contains a list of media files; the index file also contains metadata. See Table 7.3 for additional information. The URL of the index file is accessed by clients, which then request the indexed files in sequence.

The protocol specification does not limit the encoder selection. However, the current Apple implementation should interoperate with encoders that produce MPEG-2 TSs containing H.264 video and AAC audio (HE-AAC or AAC-LC). Encoders that are capable of broadcasting the output stream over UDP should also be compatible with the current implementation of the Apple-provided segmenter software. Although the protocol specification does not limit the video and audio formats, the current Apple implementation supports the following formats:

- Video: H.264 Baseline Level 3.0, Baseline Level 3.1, and Main Level 3.1.
- Audio:

TABLE 7.3 File format for Apple HTTP Live Streaming

File format	Description
.ts	A .ts file contains an MPEG-2 Transport Stream (TS). This is a file format that encapsulates a series of encoded media samples—typically audio and video. The file format supports a variety of compression formats, including MP3 audio, AAC audio, H.264 video, and so on.
.M3U8	An .M3U8 file is an extensible playlist file format. It is an m3u playlist containing UTF-8 encoded text. The m3u file format is a de facto standard playlist format suitable for carrying lists of media file URLs. This is the format used as the index file for HTTP Live Streaming.

- HE-AAC or AAC-LC up to 48 kHz, stereo audio
- MP3 (MPEG-1 Audio Layer 3) 8–48 kHz, stereo audio

For live sessions, as new media files are created and made available, the index file is updated; the new index file lists the new media files. Older media files can be removed from the index and discarded, presenting a moving window into a continuous stream—this type of session is suitable for continuous broadcasts. Alternatively, the index can simply add new media files to the existing list—this type of session can be easily converted to VoD after the event completes.

For VoD sessions, media files are available, representing the entire duration of the presentation. The index file is static and contains a complete list of all files created since the beginning of the presentation. This kind of session allows the client full access to the entire program.

It is possible to create a live broadcast of an event that is instantly available for VoD. VoD can also be used to deliver “canned” media. HTTP Live Streaming offers advantages over progressive download for VoD, such as support for media encryption and dynamic switching between streams of different data rates in response to changing connection speeds. (QuickTime also supports multiple data-rate movies using progressive download, but QuickTime movies do not support dynamically switching between data rates in mid-movie.)

HLS also provides the publisher with the opportunity of seamless in-stream ad insertion. Injecting the “ad stream” into the “content stream” is a new concept several major broadcasters, such as Canadian Broadcaster Global TV, have adopted. The traditional delivery mechanism for pre- or mid-roll video ads is to perform a (disruptive) video player switch: while watching a video, the stream goes blank while another player is presented, and a spinner or buffer is shown until the video ad stream is cued up and ready for playback. Then when the ad is finished, the player is closed and the feature content player is opened and a spinner presented until the feature content is cued up

and ready for playback. With HLS, there is the opportunity to do all the video content switching in the stream rather than within the video player [PHI201101].

7.1.3 HTTP Flash Progressive Download

Progressive downloading is the simplest and least expensive way to display Flash video on a web page. Although it is not as powerful and flexible as true streaming, it simulates streaming reasonably well. To add a progressive download video to a web page, one needs two files: an FLV video file and an SWF file to play the video.

- *SWF*: The standard Flash file format used in web pages and other delivery media.
- *FLV*: A special file type used for Flash video. This file type is not played back directly—it must be embedded in (or linked from) an SWF file.

The idea is to use a “container” SWF file from which to play the FLV file. The most common approach is to use an SWF file which functions as a media player with video screen and playback controls. Once the FLV video files are ready, one needs a Flash media player to play them on a web page. This is a Flash SWF file that includes components such as a video playback screen and controls [WAV201101]. There are two ways to obtain a Flash media player:

- Create a player using the *Macromedia Flash* authoring program
- Download a video player and customize it to play the video files (there are a number of Flash video players available on the Internet.)

The limitations of progressive downloading are as follows [WAV201101]:

- It cannot be used for live events—only stored video files.
- It is less efficient than true streaming.
- It cannot automatically adjust for the end user’s connection speed.
- It is not secure—the video file is saved on the end user’s computer.
- The end user cannot jump ahead to a later part of the video until it has downloaded.

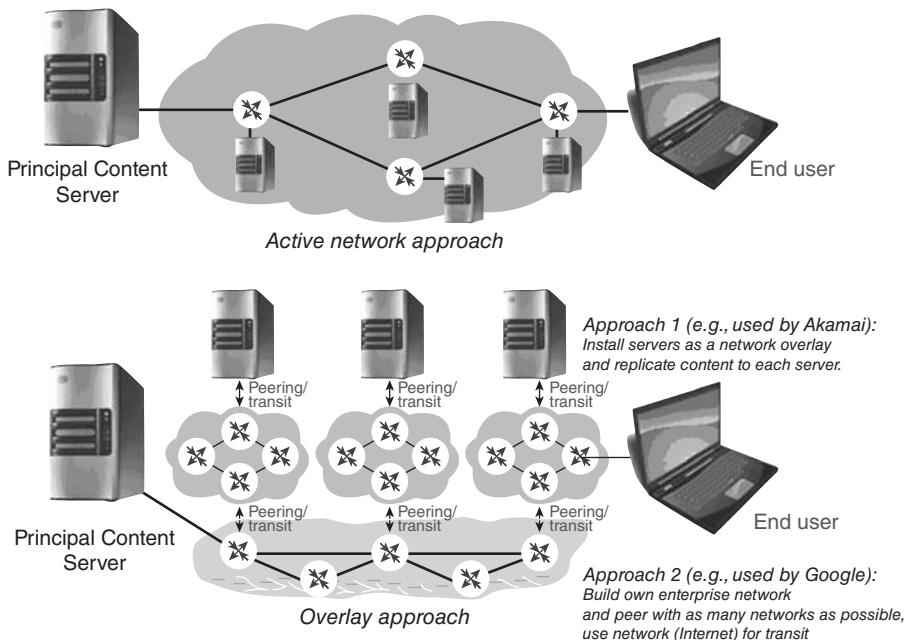
Note: Adobe announced in 2012 that it was abandoning the Flash Player on mobile browsers in favor of HTML5.

7.2 CONTENT DELIVERY NETWORKS

A CDN is a system of cooperative computers networked together that interact transparently via caching servers to deliver content to users from a principal content-origin server, over a core network (such as the Internet) and one or more access networks. When a user logs into a streaming network, including a CDN, he or she is automatically provided content from the nearest available

TABLE 7.4 Key CDN Functions

Function	Description
Request	Capability to direct users' requests to appropriate edge servers. Also, interacts with the distribution infrastructure to keep up-to-date information about the content stored in caches.
Distribution	Transfer of content from the origin server to edge servers and ensures consistency of content in caches.
Delivery	Delivery of copies of content to users utilizing a set of edge servers (also called surrogates) that store content locally for near-user distribution.
Management	Management of network components, retention of logs of user accesses and recording of servers usage data for traffic reporting, statistical analysis, and billing.

**FIGURE 7.4** CDN approaches.

server on the core network and/or the Internet. The main functions of a CDN are identified in Table 7.4.

Classic methods of building CDNs are (1) the *overlay approach* and (2) the *active network approach* (also see Figure 7.4) [SJO200801].

- **Overlay Approach:** Application-specific caches and servers throughout the network distribute specific content types, such as static web pages, streaming media, or live television. Core network components, such as routers and switches, play no active part in content delivery, other than

providing basic network connectivity. Generally, these CDNs are not affiliated with a particular Internet service provider (ISP). CDN providers team up with as many ISPs as possible and collocate their cache servers with ISP's points of presence (POPs) or entry points into ISP backbones. Most CDN providers use this approach, although a CDN of this type requires the deployment and maintenance of thousands of servers, which leads to high capital and operational expenses.

- *Active Network Approach:* Core network elements (routers in particular) play an active part in content delivery: in addition to forwarding packets, they also run other software to identify application types and forward content requests based on predefined policies. Requests are redirected to local cache servers or to servers optimized to serve specific content types. ISPs (telcos, IP carriers) operate such content delivery services over their own networks. ISPs with extensive networks of their own (e.g., Tier 1 carriers) have a cost advantage because they do not have to buy transit bandwidth from other ISPs (Tier 1 networks can typically reach every other network on the Internet without purchasing IP transit from other providers).

Note: Some CDN providers use both the active network and the overlay approaches.

As illustrative examples, Figures 7.5–7.7 depict use of satellite distribution technology (point-to-point and/or point-to-multipoint) to support caching, although terrestrial distribution is more common.

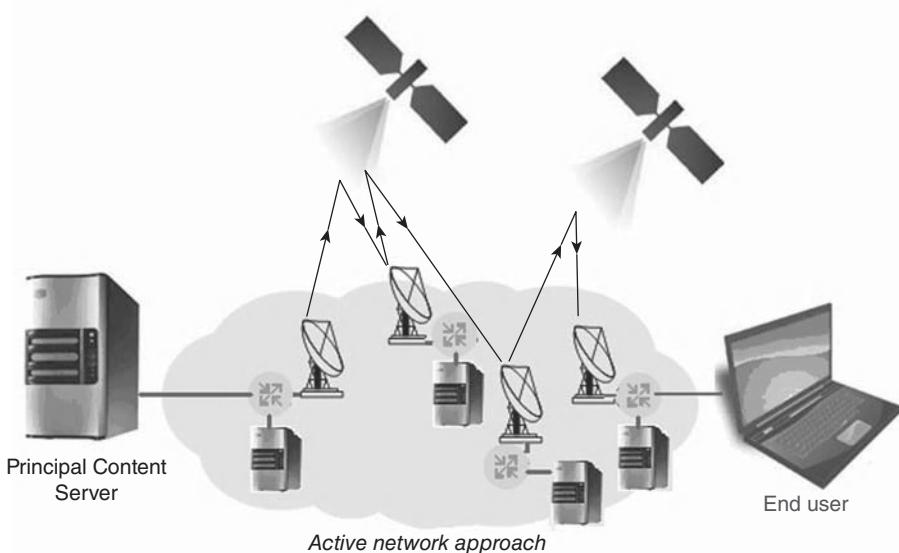


FIGURE 7.5 CDN approaches, satellite distribution, active approach.

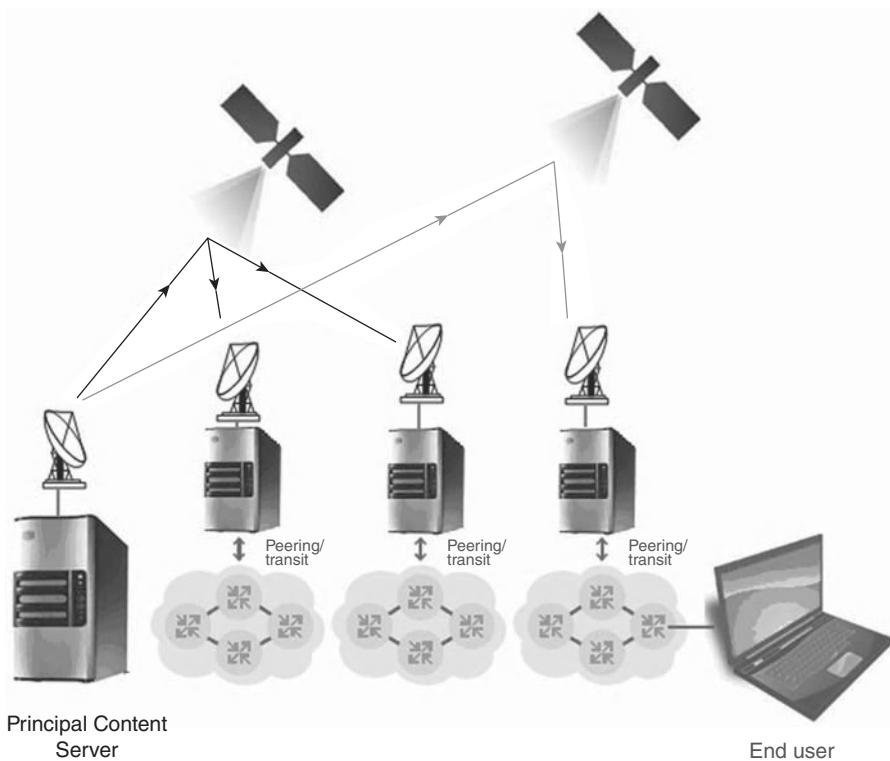


FIGURE 7.6 CDN approaches, satellite distribution, overlay approach.

The most widely used methods to distribute content to cache servers are: (1) pull-based caching, and (2) push replication (in practice, commercial CDNs combine pull-based and push-based approaches)

- In pull-based caching, when a cache server receives a request for content, it checks whether it has that content. If it has that content, it serves it; if not, it requests it from the content-origin server and saves it for future use (note: the cache server does not have a copy of a particular piece of content until it receives the first request for it). With these implementations, the cache server does not have a requirement to have copies of the full content in the content-origin server, but only of those portions that are in demand by users in the server's vicinity. This approach reduces the work the origin server has to do, since content is served primarily from the cache server.
- In push replication, the content-origin server pushes out content beforehand to all replica servers. Communication occurs only when there is an update to the content.

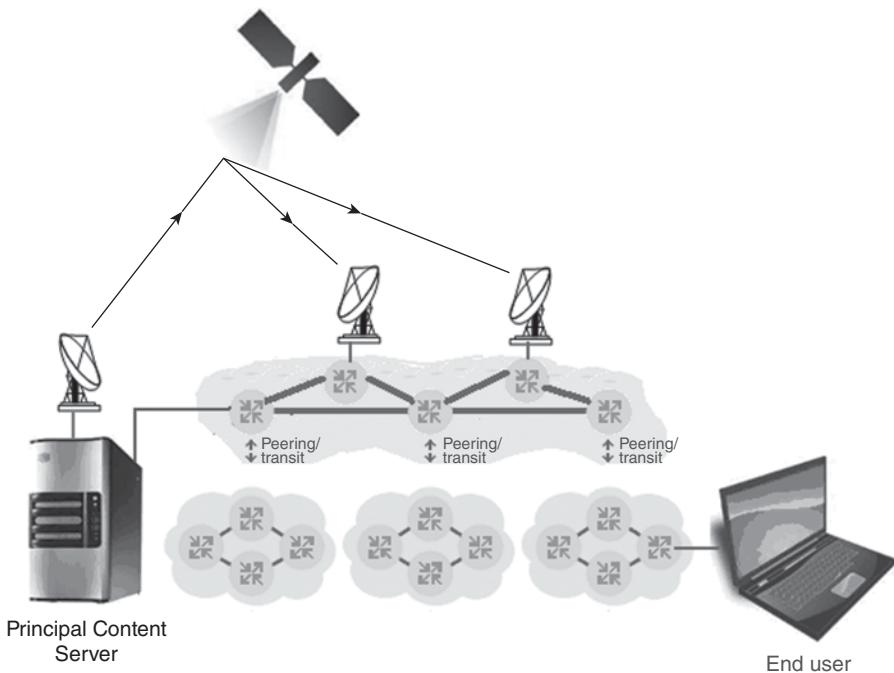


FIGURE 7.7 CDN approaches, satellite distribution, other overlay approach.

7.3 P2P NETWORKS

A P2P network is a distributed system in which all nodes have identical responsibilities and all communication is symmetric. P2P applications rely by design on the interaction between end nodes: every participating node acts as both as a server and a client, and these nodes have significant or total independence of the original content server. The idea behind P2P is to (1) bring communication to the edges of the network to avoid overloading central servers, and (2) make use of the large number of underutilized computers and Internet connections in people's homes and offices; this approach embodies, in a way, the concept of grid computing [MIN200501]. The P2P environment is created by turning every user into a rebroadcaster. The content stream is segmented into small parts, and each part is distributed to one user's computer. The participating computers request missing parts from each other and exchange parts to rebuild the whole content. Users can view the content, for example, a movie, as if it were sent directly from the content provider [SJO200801]. See Figure 7.8. A number of organizations have launched P2P-based services. In principle, P2P systems are scalable to large populations (in the millions), are reliable, and can deliver streaming video at lower costs; however, at the practical level performance, reliability, QoE/QoS, and security issues continue to be challenges.

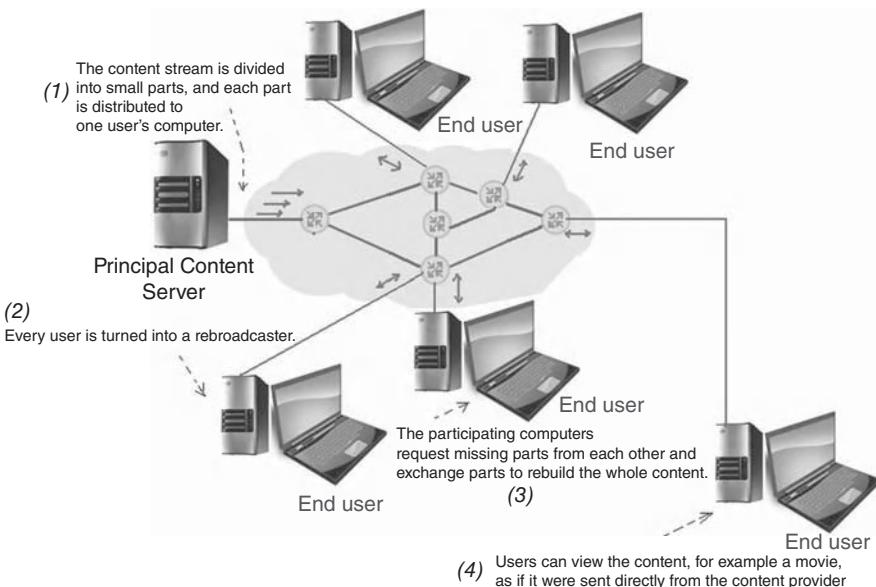


FIGURE 7.8 P2P approaches.

In conjunction with a P2P network arrangement, content providers can continue using their existing streaming servers. Users are required to install a small streaming client the first time they visit the content provider's website. Naturally, the performance of the system will depend on performance factors of the end-user population; in addition, as noted, security is a critical concern. Furthermore, ISPs have (unsuccessfully) attempted to block, delay, or deprioritize P2P traffic because P2P has become a strong consumer of bandwidth demand (it has been estimated that 20% of today's Internet traffic is P2P applications). Evolving methods, however, allow the network optimize the delivery route of large files, making transfers faster and less expensive.

7.4 CLOUD COMPUTING

Cloud computing (also previously known as grid computing or utility computing) entails network-based infrastructure that enables relocating computation and/or data storage offsite to a(n external) service provider in a location-transparent manner; some implementations entail relocating computation and/or data storage offsite to an internal centralized facility but still owned by the organization in question (this is called a “private cloud”) [MIN200501], [MIN200801]. The motivation for using public clouds is generally for cost reductions compared with owning a dedicated infrastructure. Cloud infrastructures provide (in principle) massively scalable architectures to support

computing, storage, and application services. Google, Yahoo, Amazon, and others have built large infrastructures that implement cloud architectures to support their applications, including digital content distribution. Inexpensive computing capacity, inexpensive storage, and software virtualization are some of the enabling technologies for cloud computing. Cloud computing started out with institutional applications (e.g., in the grid computing paradigm [MIN200501]), then moved on to the enterprise environment (e.g., in corporate environments [MIN200801]), and, finally, in the general population where it could usher in the concept of thin clients on a global scale (according to some, the idea of a standalone personal computer with a big processor is going the way of the VCR [FLO201101].) A press time Office of Management and Budget report noted that 25 U.S. government agencies identified close to 100 applications that would move to the cloud by 2012 (agencies such as the Department of Homeland Security and the Justice Department were planning to move services, such as e-mail, to the cloud).

Cloud computing is now generally classified three areas [CRE200901]:

- *SaaS (Software-as-a-Service)*: WAN-enabled application services (e.g., Google Apps, Salesforce.com, and WebEx).
- *PaaS (Platform-as-a-Service)*: Foundational elements to develop new applications (e.g., Coghead and Google Application Engine).
- *IaaS (Infrastructure-as-a-Service)*: Providing computational and storage infrastructure in a centralized, location-transparent service (e.g., Amazon).

Proponents make various claims of the advantages of cloud computing in the context of the enterprise requirement for CapEx (capital expense) to build infrastructure for peak service demand, combined with the in-house OpEx (operational expense) needed to maintain the infrastructure, by arguing that running application services on a cloud is advantageous because:

- Sharing the resources and purchasing power of very large-scale multitenant data centers provides an economic advantage. For example, a study demonstrated that a company's current internal cost to provide a gigabyte of managed storage is \$3.75 per month, while Amazon charges 10–15 cents per month.
- Operations can reduce system administration resources by avoiding the need for internally-purchased and maintained servers. Studies have shown that prior to virtualization, server utilization is typically between 5% and 15%. With virtualization in widespread use, server utilization is up to 80%. In one case, with server consolidation a data center floor space that was around 35,000 to 1000 ft².

Our inclusion of the cloud concept is less from the perspective of advantages to the enterprise (e.g., see [MIN200801], among other references), but more

from a technology perspective for distributed storage of video and multimedia content (e.g., data warehouse functionality). A short list of examples of content/video applications include the following:

- Amazon's Kindle tablet, an electronic book reader that relies on cloud computing. Amazon also offers a more general storage service that charges \$50 for 50 GB.
- Mogulus streams 120,000 live TV channels over the Internet and owns no hardware except for the laptops it uses. It handled all of the election coverage for most of the large media sites using IaaS capabilities [CRE200901]
- Apple's iCloud allows consumers to store music, video, photos, and documents on the Web, one of several emerging "cloud" computing offerings that are diminishing the need for a computer. Apple has reportedly secured deals with several music companies so that customers can access songs on the cloud without having to upload their library. Apple allows a maximum of five gigabytes, but does not count songs, apps, photos and iBooks toward that limit [FLO201101]. iCloud is a free service initially intended to sync user content and push it to various devices via the cloud. It is integrated with apps, ensuring automatic updates, and it will keep folders automatically updated. Contacts, calendar, and mail are now cloud-centric features, with new messages and updates pushed to associated devices. In addition to productivity features, such as email, iCloud will also serve as an online repository/syncing tool for users' documents, photos, and music, although initially iCloud did not allow one to stream music one bought, just freely redownload it. For individuals with lots of music not purchased via iTunes, a new service, iTunes Match, will allow access to those songs via Apple's cloud for \$25 per year. Google's music platform (along with Amazon's offering) requires that users upload their music to Google's servers; by contrast, Apple will scan users' hard drives for music and use that information to create a personalized music directory in iCloud—without needing to upload songs from the local drive [KOL201101].
- An evolution into video is expected. The trade press was reporting that Apple was reportedly finalizing deals to put iTunes movies in the cloud, allowing iPhone and iPad owners to stream the video content just as they can now access iTunes in the Cloud music. The service would be available in 2012, with Apple's system an alternative approach to the Ultraviolet digital locker—Ultraviolet offers a digital copy of a purchased DVD or Blu-ray, available for streaming to Digital Rights Management (DRM)-compatible devices [DAV201101].
- In 2010, The DECE (Digital Entertainment Content Ecosystem) announced its plans for a cross-platform DRM that would allow digital content like movies to be stored in a cloud and then played on whichever

hardware supports the system, without providers having to worry about copyright theft. The technology, given the name UltraViolet, has been backed by Warner Brothers, Sony, Microsoft, and Netflix; however, there were notable exceptions, including Apple and Disney. UltraViolet is a free, online personal library that gives the user greater flexibility with how and where they watch the movies and TV shows that they purchase. Once a movie or TV show has been added to the user's UltraViolet Library, the user will have options to stream it over the Internet, download it for offline viewing, or play it back on a disc. The user will have greater freedom to choose where he/she want to watch—whether it is on a mobile device, computer, television, game console, and so on. UltraViolet locks content not to individual devices or platforms, but to the user; the user is then able to access content—which will initially include TV episodes and movies, but should eventually also support music—on any UltraViolet-compliant device, whether these are a portable media players (PMPs), a PC, or a set-top box. When new content is bought, the retail account is linked to their UltraViolet account and the rights to view it will be spread to any registered hardware [DAV201001]. See Figure 7.9 [ULT201101]. UltraViolet was expected to launch its own content with series such as *Green Lantern* and *Horrible Bosses*.

7.5 CORE INTERNET TECHNOLOGIES

The rest of this chapter focuses on (some key) underlying Internet technologies that come into play to support IBTV.

7.5.1 Very High-Capacity Backbone Networks, Transmission

Internet services depend on carrier-provided core connectivity to enable users to reach websites, likely hosted in large data center hosting sites. A collection of routers, usually arranged in a tiered architecture, makes use of backbone fiber-optic links to provide high-speed IP connectivity between the various hosting, cashing, and streaming elements that comprise the Internet. Generally Internet providers (for both backbone and access) make use of simple very high-capacity transmission links that interconnect very high throughput routers. However, they may occasionally make use of higher-layer (layer 2/3) services, such as wide-area Ethernet services, and/or MultiProtocol Label Switching (MPLS). Figure 7.10 depicts a basic IP/core network. Figure 7.11 shows how such basic core network relies on underlying transport facilities.

Internet-based video generates large amount of traffic that needs to be supported across the infrastructure. For example, it has been estimated that YouTube generated approximately 45 Pb per month of traffic at the end of 2008; at a 50% growth rate a year, the 2012 figure would be 227 Pb of traffic per month. comScore estimates that in the United States, 14 billion online

WHAT IS ULTRAVIOLET?

OVERVIEW	TOTAL FREEDOM	MORE CHOICES	BETTER VALUE
			
<p>Your Library at your fingertips It's easy and convenient to access your UltraViolet Digital Library.</p> <p>Your entire movie and TV show collection is available whenever you want. You can log into your Library from the websites and apps of UltraViolet-participating companies.</p> <p>And with "remember me" setting, your Library is always just a click away — whether you're going out to shop or sitting down to watch.</p>	<p>Disc, stream or download Purchasing UltraViolet content gives you flexibility to watch the way you want:</p> <ul style="list-style-type: none"> Stream to any internet-connected device, including cable/satellite set-top boxes Download for offline viewing, including full HD copies Get a disc included even when you buy online - either download or streaming 	<p>How do you want to watch? At home or on the go, UltraViolet lets you watch where you want</p> <ul style="list-style-type: none"> TVs Computers Tablets Game consoles Set top boxes Blu-ray players Internet TVs Smartphones 	

UltraViolet Digital Library
Your online library of movies and TV shows that lets you watch how, where and when you want



Multiple Devices
Watch on the devices YOU want, with even more choices coming soon

Streaming
You can watch your UltraViolet titles over the Internet

Downloads
Get copies for your devices so you can watch when there's no Internet

Disc
Included with select Blu-rays and DVDs. Disc copy available as an option with digital purchases

Multiple Account Members
Up to 6 family or household Members can use a single UltraViolet Library

FIGURE 7.9 Ultraviolet concept/cloud.

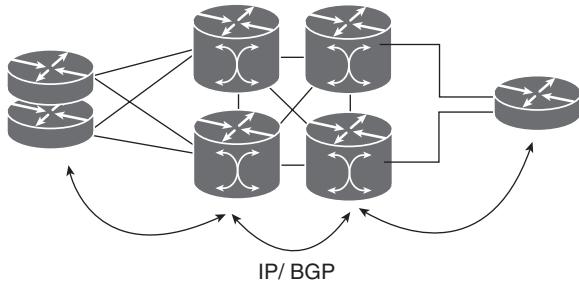


FIGURE 7.10 Illustrative basic IP/core network.

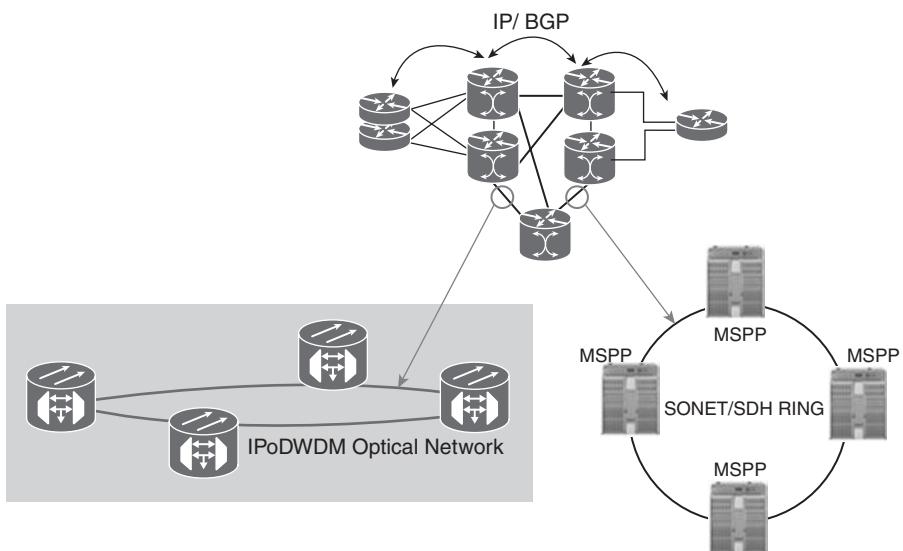


FIGURE 7.11 Core network making use of underlying transport facilities.

video streams were initiated in December 2008 [CIS200801]. If each stream generated 10 Mb of traffic, the total for the United States would be 140 Pb for the month of December 2008; at a 50% growth rate a year, the 2012 figure would be 700 Pb of traffic per month. At the end of 2008, there were approximately 10 million Xbox consoles in North America capable of downloading video. If 30% of those consoles downloaded 5 hours of content per month, that would generate approximately 30 Pb per month; at a 50% growth rate a year, the 2012 figure would be 152 Pb of traffic per month. In the aggregate, in the past several years, U.S. broadband services (as a geographic example) have grown about 40% annually; in the next several years, global Internet traffic is expected to maintain a similar, if not higher, growth rate [WEL201001]. In 2013, global IP traffic is expected to exceed 55 Eb per month ($\text{exa} = 10^{18}$); see Table 7.5 [CIS200801] (see Appendix 7A for additional information.)

TABLE 7.5 Growth of IP Traffic: Global IP Traffic, 2008–2013
IP Traffic, 2008–2013

	2008	2009	2010	2011	2012	2013	CAGR 2008–2013 (%)
By type (PB per month)							
Total IP traffic	10,160	14,743	21,367	30,811	42,165	55,560	40
Internet—Denotes all IP traffic that crosses an Internet backbone	8126	11,627	16,591	23,682	31,695	40,401	38
Non-Internet IP—Includes corporate IP WAN traffic, IP transport of TV/VoD	2001	3031	4569	6647	9394	12,975	45
Mobile data	33	85	207	482	1076	2184	131
By segment (PB per month)							
Consumer—Includes fixed IP traffic generated by households, university populations, and Internet cafés)	7023	10,399	15,354	22,606	31,067	40,543	42
Business—Includes fixed IP WAN or Internet traffic generated by businesses and governments	3103	4258	5805	7,722	10,022	12,833	32
Mobile—Includes mobile data and Internet traffic generated by handsets, notebook cards, and mobile broadband gateways	33	85	207	482	1076	2184	131
By geography (PB per month)							
North America	2578	3666	5309	7797	10,498	13,431	39
Western Europe	2593	3623	4995	7126	9707	12,593	37
Asia Pacific	3661	5503	8089	11,503	15,877	21,177	42
Japan	644	950	1355	1919	2490	3107	37
Latin America	308	503	800	1196	1,690	2360	50
Central Eastern Europe	280	421	665	1021	1441	2042	49
Middle East and Africa	110	165	264	408	606	877	51

Source: Cisco VNI, 2009.

These large volumes of traffic require very high-speed links and routers. Traditionally, high-speed links reached into the 10 Gbps area; higher speeds are now emerging. Data center and commercial network operators cite the need for 100 GbE connectivity and WAN transport to support the increasing Internet traffic growth during this decade. According to these operators, the bandwidth requirements of core networking applications has been growing and continues to double every 18 months. This growth is expected to require Terabit Ethernet by 2015, according to industry observers [JDA201001]. Cloud computing data centers already need multi-terabit capacity for support of blade servers using 10GbE interfaces. In response to these needs, early adopters (carriers) were deploying 100 Gbps transport in their networks in 2010, and next-stage adopters are expected to do so in 2011–2012.

Layer 1/Transport Networks As noted, carriers have already been trialing 100 Gbps core networks in the past few years. For example, Verizon deployed the first 100 Gbps production network in December 2009 on a 900-km route between Paris, France and Frankfurt, Germany; other routes were planned to be turned-up in 2010. Work is also starting on extensions to higher speeds. Requirements for data centers are driving needs to 1 Tbps; on the terrestrial networking side, a number of technical barriers to 1 Tbps are motivating researchers to aim at a 400 Gbps rate as a next step. A simple and historical extrapolation shows that 400GbE/1TbE may appear in or around 2017 [ROE201001].

The industry is also seeing a need for convergence of LAN/WAN protocols at these higher speeds, as we discuss briefly below. Responding to this demand, the IEEE 802.3 Working Group (WG) and the International Telecommunications Union (ITU) Study Group (SG) 15 reached milestones in standards development of specifications for supporting 40/100GbE interfaces and transmission across an Optical Transport Network (OTN) infrastructure, which is a new-generation transport infrastructure compared with traditional Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) systems [AND201001]. Figure 7.12 depicts a traditional SONET/SDH environment, while Figure 7.13 depicts an evolving OTN environment.

The traditional Digital Hierarchy for digital terrestrial networks was based on SONET/SDH and includes the following rates:

OC-48/STM-16	2.4 Gbps
OC-192/STM-64	9.8 Gbps
OC-768/STM-256	40 Gbps

New data rates have been advanced by OTN. The OTN frame consists of 4-byte row \times 4080-byte columns; the frame is called Optical Channel Transport Unit-k (OTUk). One then gets:

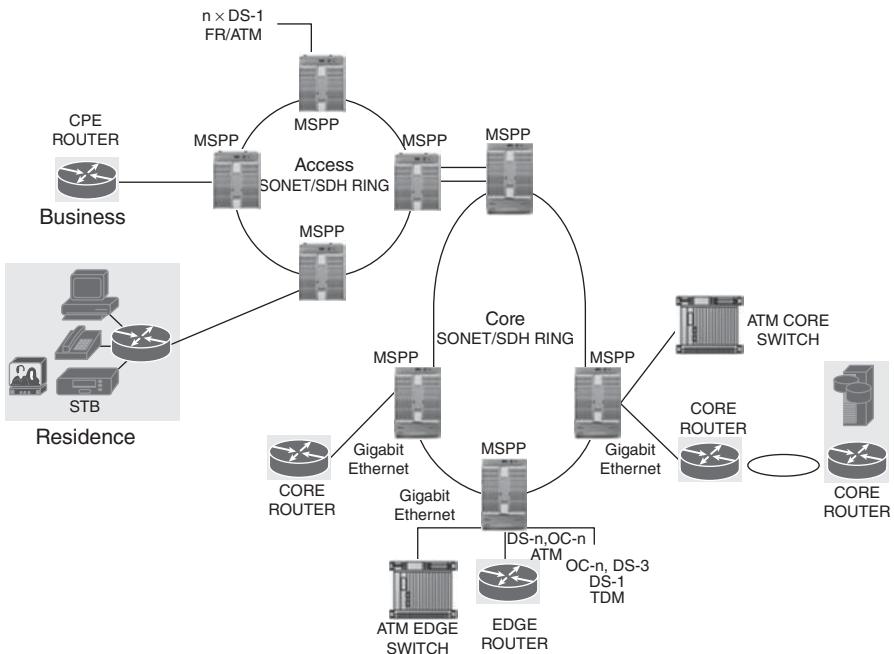


FIGURE 7.12 Traditional SONET/SDH network (typical for carriers).

OTU1	2.67 Gbps
OTU2	10.71 Gbps
OTU3	43.02 Gbps
OTU4	111.81 Gbps

The ITU-T G.709 recommendation defines standard interfaces and rates based on the SONET/SDH rates. Table 7.6 lists the ITU G.709 line rates and their corresponding SONET/SDH interfaces. When taking into consideration the additional G.709 overhead and FEC information, the resulting interfaces operate at line rates approximately 7% higher than the corresponding SONET/SDH rates.

Starting in 2004, extensive work was undertaken to achieve a 10GbE (10 Gigabit Ethernet) mapping into OTU2. Initially, the IEEE specified 10GbE-WAN (9.95328 Gbps) to comply with SONET/SDH OC-192/STM-64; however, the market pushed the 10GbE interface as a more cost-effective solution, resulting in the dominance of the 10GbE spec as the router/switch interface. That simply means that the carrier/user handoff is 10GbE, with the carrier proving a 10GbE-ready access multiplexer on the customer site and then mapping the signal to a SONET/OTN interface. A direct LAN/WAN interface

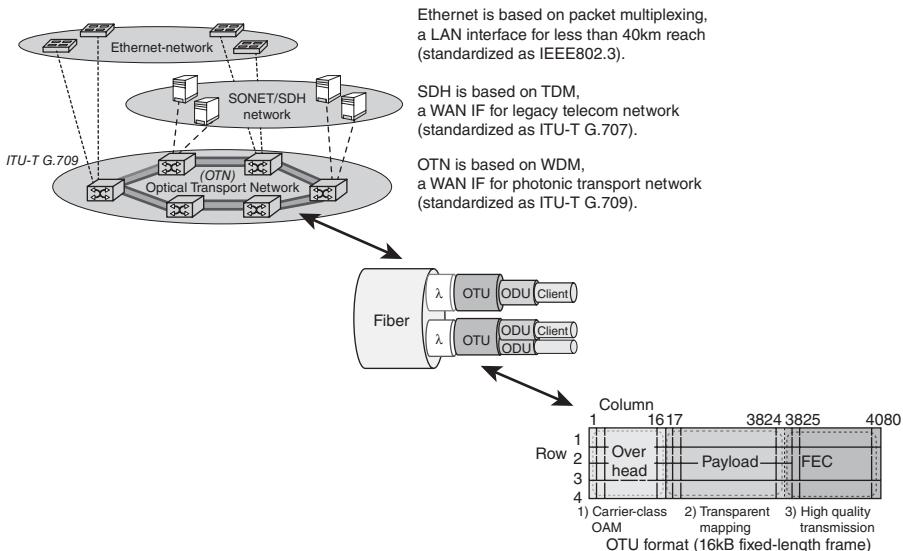


FIGURE 7.13 New-generation optical networks now being deployed by early adopters. ODU, optical-channel data unit; OUT, optical channel transport unit.

TABLE 7.6 ITU SONET/SDH versus OTN Rates

G.709 Interface	Line Rate (Gbps)	Corresponding SONET/SDH Rate	Line Rate (Gbps)
OTU1	2.666	OC-48/STM-16	2.488
OTU2	10.709	OC-192/STM-64	9.953
OTU3	43.018	OC-768/STM-256	39.813

that maps Ethernet directly to the OTN is desirable and is being sought. ITU-T SG15 is now actively discussing and rapidly advancing the mapping of 1GbE/10GbE/40GbE/100GbE into the OTN digital frame format.

For operation at 40 and 100 Gbps Ethernet, the specification IEEE Std 802.3ba-2010 “*IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks-Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 4: Media Access Control Parameters, Physical Layers and Management Parameters for 40 Gbps and 100 Gbps Operation*” was approved at the June 2010 IEEE Standards Board meeting. This amendment to IEEE Std 802.3-2008 includes changes to IEEE Std 802.3-2008 and adds Clause 80 through Clause 88, Annex 83A through Annex 83C, Annex 85A, and Annex 86A. This amendment includes IEEE 802.3 Media Access Control (MAC) parameters, Physical Layer specifications, and management parameters for the

transfer of IEEE 802.3 format frames at 40 and 100 Gbps. The standard includes a number of Physical Layer (PHY) specifications, some of which utilize Dense Wavelength Division Multiplexing (DWDM) techniques to support transmission of four lanes at 25 Gbps each at a distance of 40 km on a pair of singlemode fibers (SMF). While early adopters (carriers) contemplate the initial deployments of systems supporting 100 Gbps to provide relief to congested core networks, others are already looking at the development of next-generation electrical/optical signaling technologies (e.g., single lane) that are expected to (1) drive reduced costs, and (2) facilitate the development of terabit Ethernet systems. The IEEE is working with the Optical Interworking Forum (OIF) and the ITU to ascertain that 40/100 Gbps Ethernet can be supported seamlessly in carriers' environments.

The paradigm of circuit switched networks has changed to packet switched networks due to the exponential (or at least geometric) increase in IP-centric traffic created by applications, such as IPTV, VoIP, social networks, and other-based IP applications, including 3G/4G wireless services, as noted by many, including [ROE201001]. IP-based services have increased the demand on network capacity both in the access and metro/regional networks, as well as in the core/backbone network. IP has become the transmission protocol of choice. Internet traffic is expected to grow at a fast pace because of bandwidth-hungry services, such as video services (including user-generated video, HDTV video, and high-quality 3DTV video), large-scale data storage and mirroring, increased social networking, and other services taking advantage of broadband communications.

Layer 2/3 Networks We mentioned the possible use of higher-layer services in some applications. These might be used in CDNs, cloud computing environments, and enterprise networks. Some of these network services include: emerging Ethernet-based WAN connectivity (also called Carrier Ethernet Services), MPLS services, MPLS Virtual Private Network (VPN), Ethernet over MPLS (EoMPLS), Layer 3 Protocol Independent Multicast-Source Specific Multicast (PIM-SSM), high-throughput IP, IP over dense wavelength-division multiplexing (IPoDWDM), Hierarchical Virtual Private LAN Service (H-VPLS), and IEEE 802.1ad.

Carrier Ethernet connectivity services have been defined by the Metro Ethernet Forum (MEF), as follows:

- *E-Line* is a service based on a point-to-point Ethernet Virtual Connection. Two E-Line services are defined:
 - Ethernet Private Line (EPL): A simple and basic point-to-point service that provides low frame delay, low frame delay variation, and low frame loss ratio. A Committed Information Rate (CIR) is supported. No service multiplexing is allowed, and no Class of Service (CoS) is supported.

- Ethernet Virtual Private Line (EVPL): A point-to-point service wherein service multiplexing (namely where multiple Ethernet Virtual Connections) is allowed. The individual Ethernet Virtual Circuits can be defined with a set of Bandwidth Profiles and Layer 2 Control Protocol Processing methods as defined by the MEF.
- *E-LAN* is a service based on a multipoint-to-multipoint Ethernet Virtual Connection. Service multiplexing (more than one Ethernet Virtual Circuit at the same User-Network Interface [UNI]) is permitted, as is the rich set of performance assurances defined by the MEF, such as CIR with an associated Committed Burst Size (CBS) and Excess Information Rate (EIR).
- *E-Tree* is a point-to-multipoint ELAN service in which the spoke “leaves” can communicate with the hub or “root” location but not with each other.

Figure 7.14 depicts a typical MPLS network. MPLS VPN service is specified by IETF RFC 2547bis. It allows service providers to offer a virtual IP network to customers that rides on top of their MPLS network infrastructure; customers can connect to the MPLS VPN using a variety of access services.

With the exception of IPoDWDM, these services tend to support edge/access networks rather than core networks; however, they are used for core connectivity in some instances (specifically, these services may be found in core network of telco carriers, but less so in the core of pure Internet backbones).

7.5.2 Very High-Capacity Backbone Networks, Routing

High throughput routers are basic constituent elements of Internet core networks. Figures 7.15–7.17 illustrate basic router architectures. To provide an illustrative example, Cisco Systems introduced in the recent past a high-end core router, the Cisco Carrier Routing System 3 (CRS-3). CRS-3 is targeted

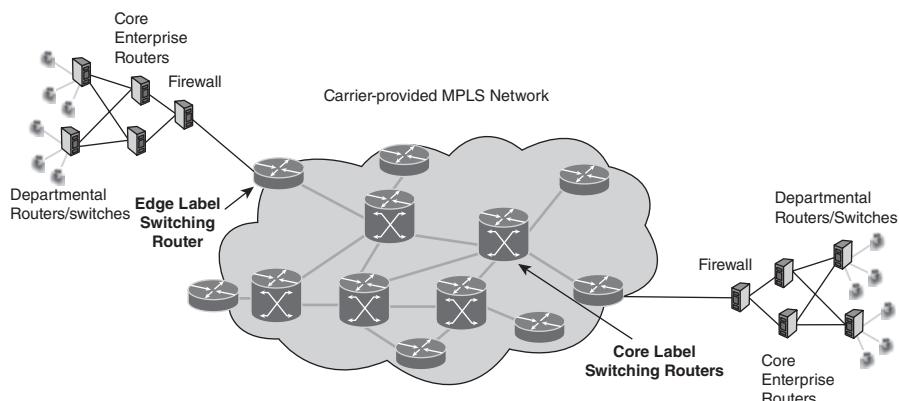


FIGURE 7.14 Logical view of a typical MPLS network environment.

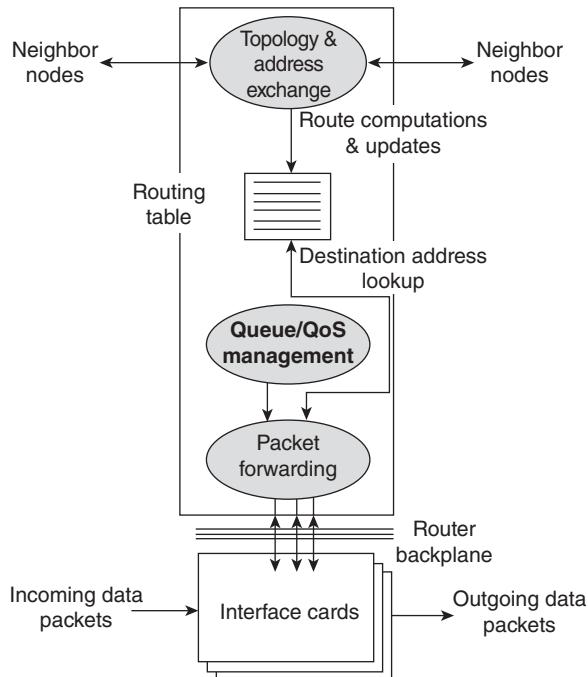


FIGURE 7.15 Basic router internals.

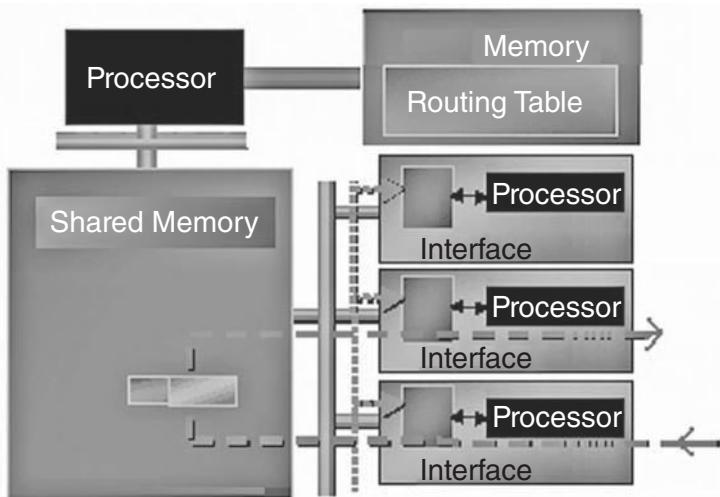
to support services such as Internet video. Cisco stated that “the product could deliver every movie ever made in just four minutes . . . it has 12 times the capacity of existing products” [CAR201001]. The Cisco CRS scales easily from numerous single-chassis form factors to a large multi-chassis system, supporting aggregate switch capacities of up to 322 Tbps. Table 7.7 provides some performance data for select Cisco routers.

7.5.3 Terrestrial Trends in Access Networks

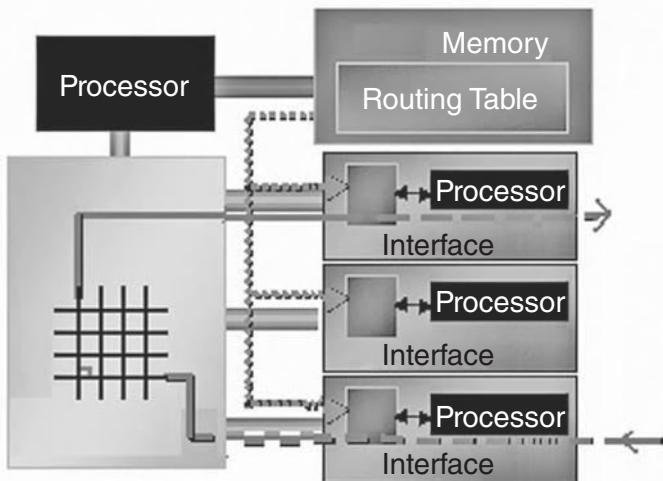
There are several local-distribution network architectures, depending in large measure who architect and manages (owns) the network:

- Telco metropolitan networks (usually found in IPTV applications)
- Cable TV fiber networks (usually found in Cable TV applications, but also supporting broadband Internet access)
- Broadband Internet access based on Digital Subscriber Line technology (of various kinds), or provided by other fiber/cable means

Telco metropolitan networks, such as those used for IPTV, are typically high-quality routed networks with very tightly controlled latency, jitter, and packet



Shared Memory Distributed Processors Architecture



Crossbar Architecture

FIGURE 7.16 Basic router internals (another view).

loss. The local distribution network is typically comprised of a metropolitan core tier and an access (consumer distribution) tier. See Figure 7.18. Figure 7.19 depicts one view of an access/service aggregation network. In the metropolitan core tier, IPTV is generally transmitted using the telco's private "carrier-grade" IP network (streaming and other IBTV services are supported

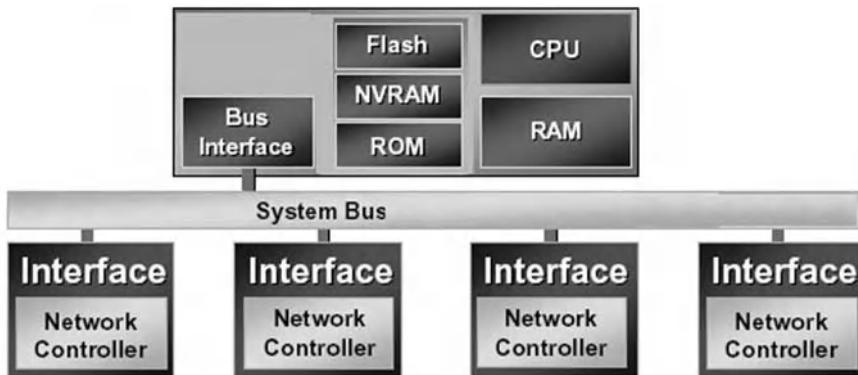


FIGURE 7.17 Typical router hardware.

TABLE 7.7 Performance Data for Select Cisco Routers

Model	Aggregate Switching Capacity
Cisco CRS-1 4-Slot Single-Shelf System	320 Gbps
Cisco CRS-1 8-Slot Single-Shelf System	640 Gbps
Cisco CRS-1 16-Slot Single-Shelf System	1.2 Tbps
Cisco CRS-1 Multishelf System	92 Tbps
Cisco CRS-3 4-Slot Single-Shelf System	1.12 Tbps
Cisco CRS-3 8-Slot Single-Shelf System	2.24 Tbps
Cisco CRS-3 16-Slot Single-Shelf System	4.48 Tbps
Cisco CRS-3 Multishelf System	322 Tbps

by public networks connected to the Internet backbone, as shown in Figure 7.20). The network engine can be pure IP-based, MPLS-based (layer “2.5”), metro Ethernet-based (layer 2), or optical SONET/OTN based (layer 1), or a combination thereof. A (private) wireless network, such as WiMAX, can also be used. The backbone network supports IP Multicast, very typically Protocol Independent Multicast Dense Mode (PIM-DM) or PIM Sparse-Dense. It is important to keep the telco-level IP network (the metropolitan core tier) streamlined with as few routed hops as possible, and with plenty of bandwidth between links and with high-power nodal routers in order to meet the QoS requirements of IPTV. Otherwise, pixilation, tiling, waterfall effects, and even blank screens will be an issue. It is important to properly size all Layer 2 and Layer 3 devices in the network.

For both the IPTV access, as well as for the broadband Internet access, the consumer distribution tier provided by the traditional carriers is generally (but not always) DSL-based at this time (e.g., VDSL or ADSL2+); other technologies, such as PON (Passive Optical Network), may also be used as time goes by, as we discuss later (see Table 7.8). A bandwidth in the 20–50 Mbps is generally desirable for delivery of video/IPTV services, although rates of 5–16 Mbps have been common in the recent past. For example, the simultaneous viewing

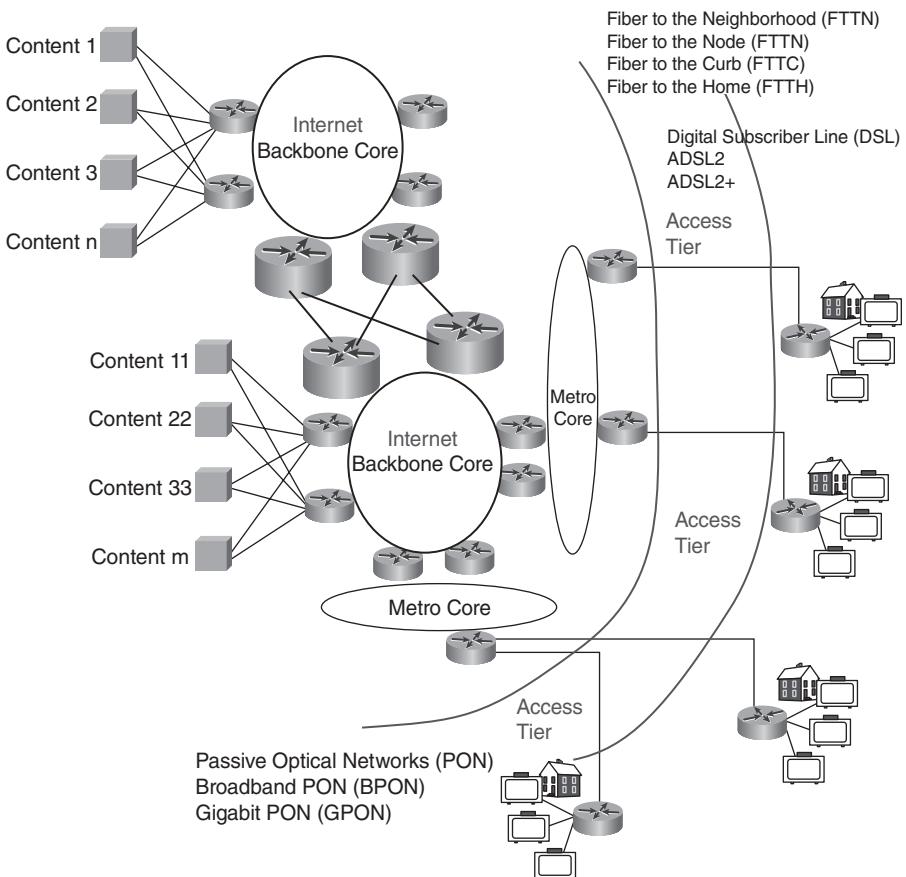


FIGURE 7.18 IPTV distribution networks.

of an HD channel along with two SD channels would require about 17 Mbps; Internet access would require additional bandwidth. Therefore, the 20 Mbps is seen as a lower bound on the bandwidth. In the United States, Verizon is implementing Fibre to the Premises (FTTP) technologies, delivering fiber to the subscriber's domicile; this supports high bandwidth, but it requires significant investments; AT&T is implementing Fibre to the Curb (FTTC) in some markets, using existing copper for only the last 1/10 of a mile, and Fibre to the Node (FTTN), in other markets, terminating the fiber run within a few thousand feet of the subscriber. These approaches lower the up-front cost but limit the total bandwidth.

As noted, IPTV as delivered by the telephone carriers may use PON technology, as a FTTH implementation technology, or perhaps Very High Bit Rate DSL 2 (VDSL2). However, if loop investments are made by these carriers, likely it will be in favor of FTTH. VDSL2 may find a use in multidwelling units (MDUs), as we note below.

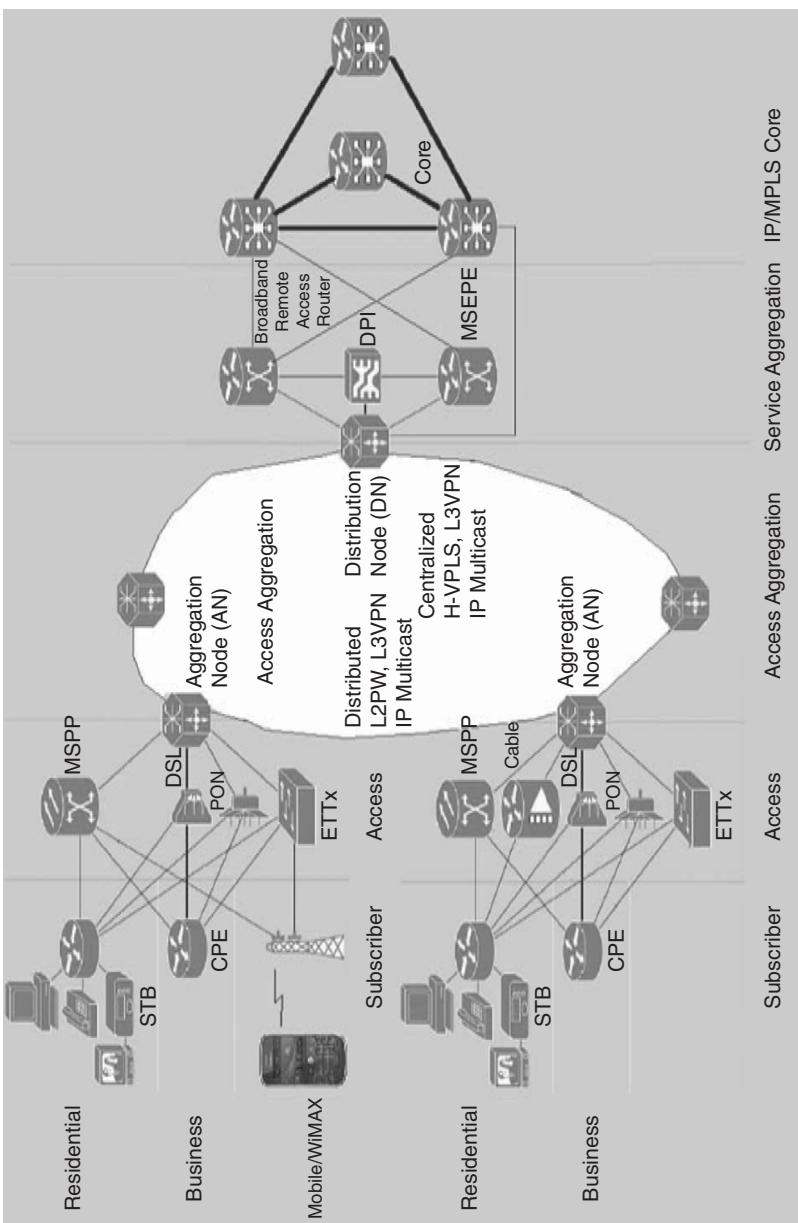


FIGURE 7.19 A view of access/service aggregation. Modeled after Cisco's views.

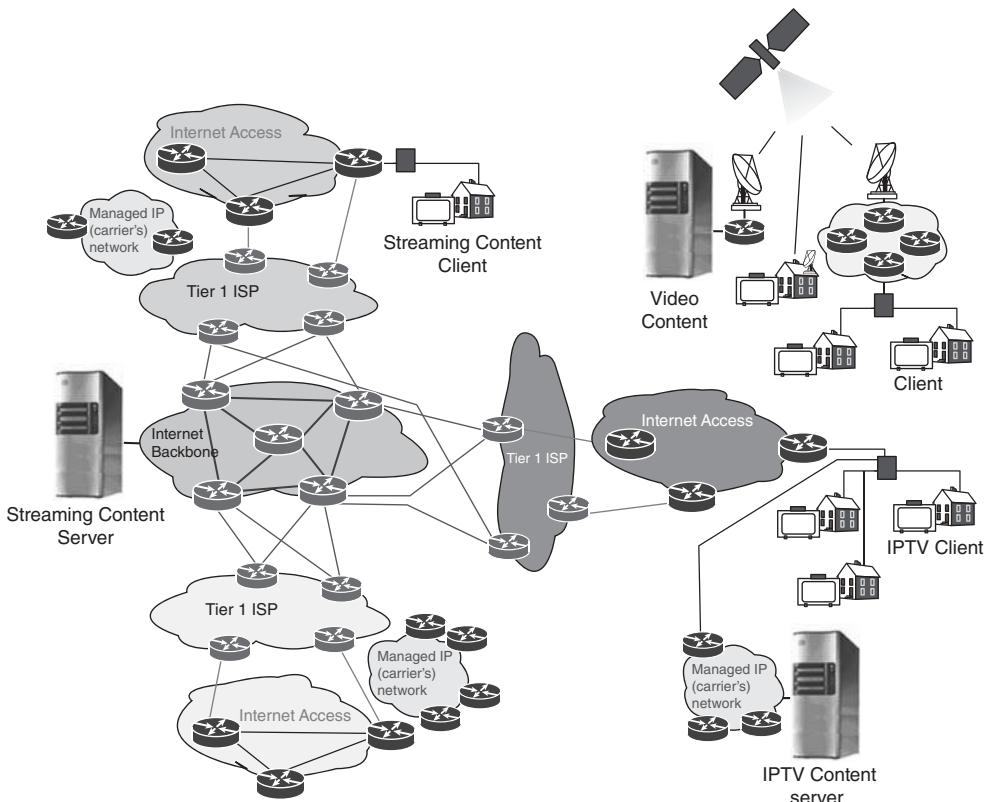
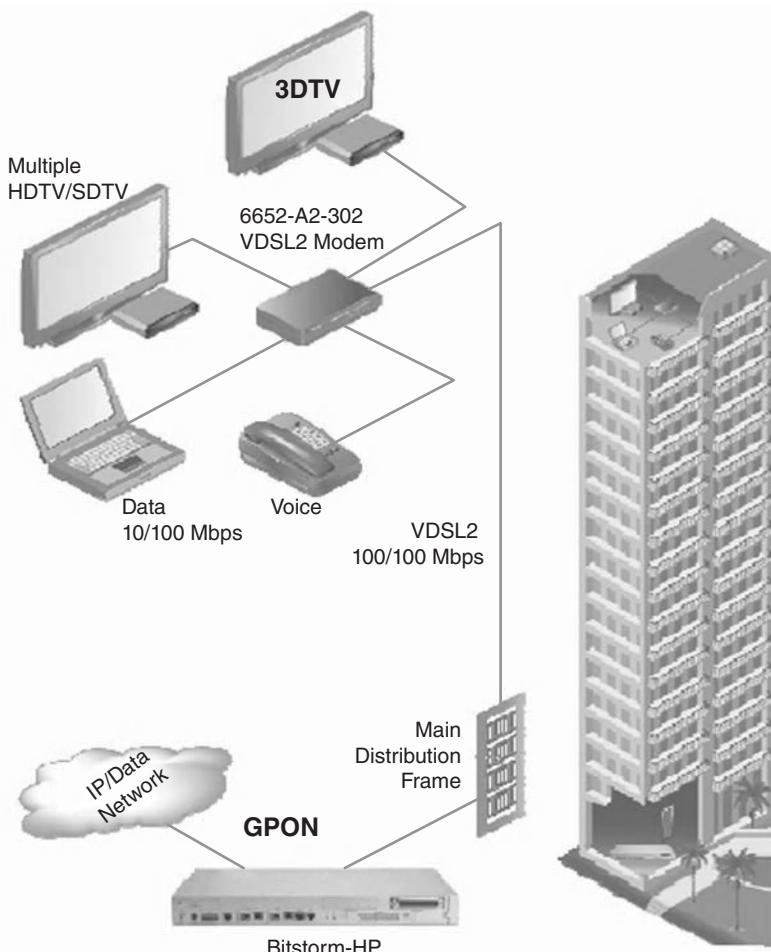


FIGURE 7.20 Internet-based, managed IP network based-, and satellite-based Video Distribution.

The VDSL2 standard ITU G.993.2 is an enhancement to G.993.1 (VDSL). It uses about 30 MHz of spectrum (vs. 12 MHz in VDSL) and thus allows more data to be sent at higher speeds and over longer distances. VDSL2 utilizes up to 30 MHz of bandwidth to provide speeds of 100 Mbps both downstream and upstream within 1000 ft. Data rates in excess of 25 Mbps are available for distances up to 4000 ft. See Figure 7.21; Figure 7.22 depicts, for illustrative purposes, test results for Zhone's VDSL2 products [ZHO200901]. VDSL2 technology can handle, say, three simultaneous HDTV streams (studies show that the average U.S. home now has 3.1 televisions). Of course, there is the issue that many homes in the United States are too far from the Central Office. The VDSL2 standard defines a set of profiles (see Table 7.9) that can be used in different VDSL deployment architectures; ITU G.992.3 extends the North American frequency range from 12 to 30 MHz. For example, carriers, such as Verizon Communications, may use VDSL2 for risers in multi-dwelling units (MDUs) to bring fiber-to-the-home service in these buildings.

TABLE 7.8 Consumer Distribution Tier

Approach for the consumer distribution tier	Description
“Classical”	Digital Subscriber Line (DSL) delivers digital data over a copper connection, typically using the existing local loop. There are multiple DSL variants, with ADSL2 and ADSL2+ being the most prevalent. DSL is distance-sensitive and provides limited bandwidth. As a result, DSL often cannot be used alone and fiber must be deployed to connect to a DSLAM located in an outside plant cabinet.
Under deployment	<ul style="list-style-type: none">• <i>Fibre to the Neighborhood (FTTN)</i>: Fibre is extended to each neighborhood where broadband services, including IPTV service, is to be supported. A small-size DSLAM in each neighborhood supports a few dozen subscribers.• <i>Fibre to the Curb (FTTC)</i>: Fibre is extended to within (typically) less than 1/10th of a mile from the subscriber site. Each fiber typically supports one to three subscribers.• <i>Fibre to the Premises/Home/Subscriber/Business (FTTP, FTTH, FTTS, and FTTB)</i>: Fibre reaches the subscriber site directly. This approach delivers the highest throughput but it is the most expensive solution.
New/future	<ul style="list-style-type: none">• Passive Optical Networks (PON) technology can be used to deliver service using end-to-end fiber. A single fiber emanates from the Central Office, and a passive splitter in the outside plant splits the signal to support multiple subscribers. Broadband PON (BPON) supports up to 32 subscribers per port, while Gigabit PON (GPON) supports up to 128 subscribers per port. Higher-capacity systems are also under development.• Fixed wireless WiMAX. Note that WiMAX supports only 17 Mbps of shared bandwidth over a 2.5-mi radius (and less at higher distances), and is, therefore rather limited.
Cable operators	Hybrid Fibre Coax (HFC) is the traditional technology used by cable operators. Fibre is used for the first section, from the headend to the subscriber’s neighborhood. The link is then converted to coax for the remainder of the connection, terminating at the subscriber premises.
Satellite operators	High power Direct Broadcast Satellite (DBS) service, also known as Direct To Home (DTH). Important in non-metro areas of U.S.; also important in Europe; critical for the developing world (for example in BRICA countries).



Zhone's VDSL2 products shown for illustrative purposes

FIGURE 7.21 VDSL2 aggregate channel capacity as a function of the link length. Zhone's VDSL2 products shown for illustrative purposes.

Verizon has been using relatively inexpensive optical network terminals (ONTs) (also called optical network units [ONUs]⁴) for single family units (SFUs) (using BPON initially, but now also seeing GPON deployment). Using this arrangement it is not excessively expensive to bring the fiber service to the living unit of a SFU. However, tenants of MDUs are more expensive to service because of the cost in pulling the fiber up the risers. Here is where DSL technologies still have some play: on the link between the basement and the apartment unit: VDSL1 is used with BPON, and VDSL2 is used with GPON.

⁴ONU is IEEE terminology and ONT is ITU-T terminology.

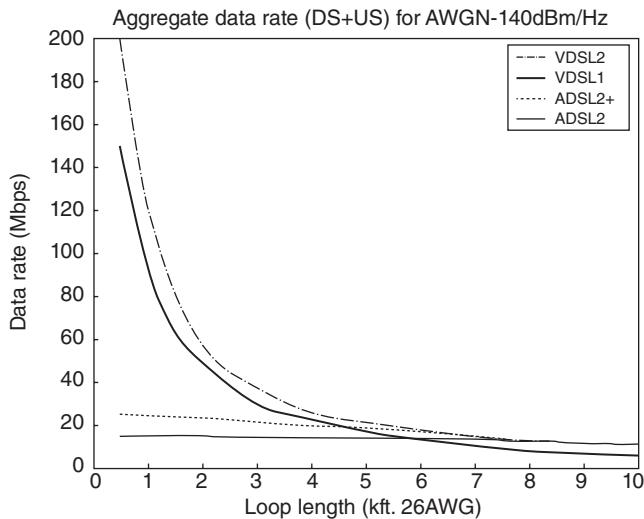


FIGURE 7.22 Actual VDSL2 downstream/upstream line rates, based on profiles.

TABLE 7.9 VDSL2 Profiles

Regional Relevance	North America						Europe	Asia
Profiles	8a	8b	8c	8d	12a	12b	17a	30a
Bandwidth MHz	8.5	8.5	8.5	8.5	12	12	17.7	30
Bandwidth KHz	4.312	4.312	4.312	4.312	4.312	4.312	4.312	8.625
Maximum Throughput (Mbps, downstream)	50				68		100	200

The carrier will set the locations of the MDUs so that the furthest tenant is around 500 ft; this achieves speeds of around 35 Mbps downstream, and 10 Mbps upstream on VDSL1 and BPON. On GPON/VDSL2, the carrier expects to achieve 75 Mbps downstream. See Figure 7.23.

PON is the leading FTTH technology⁵ (see Figure 7.24). This approach differs from most of the telecommunications networks in place today by featuring “passive” operation. Active networks such as DSL, VDSL, and cable TV have active components in the network backbone equipment, in the central office, in the neighborhood network infrastructure, and in the customer premises equipment. PONs only employ passive light transmission components in the neighborhood infrastructure; active components are only located in the central office and the customer premises equipment. The elimination of active components means that the access network consists of one bidirectional light source and a number of passive splitters that divide the data stream into the individual links to each customer. At the central office, the termination point

⁵This section is summarized on material from reference [PCM200901].

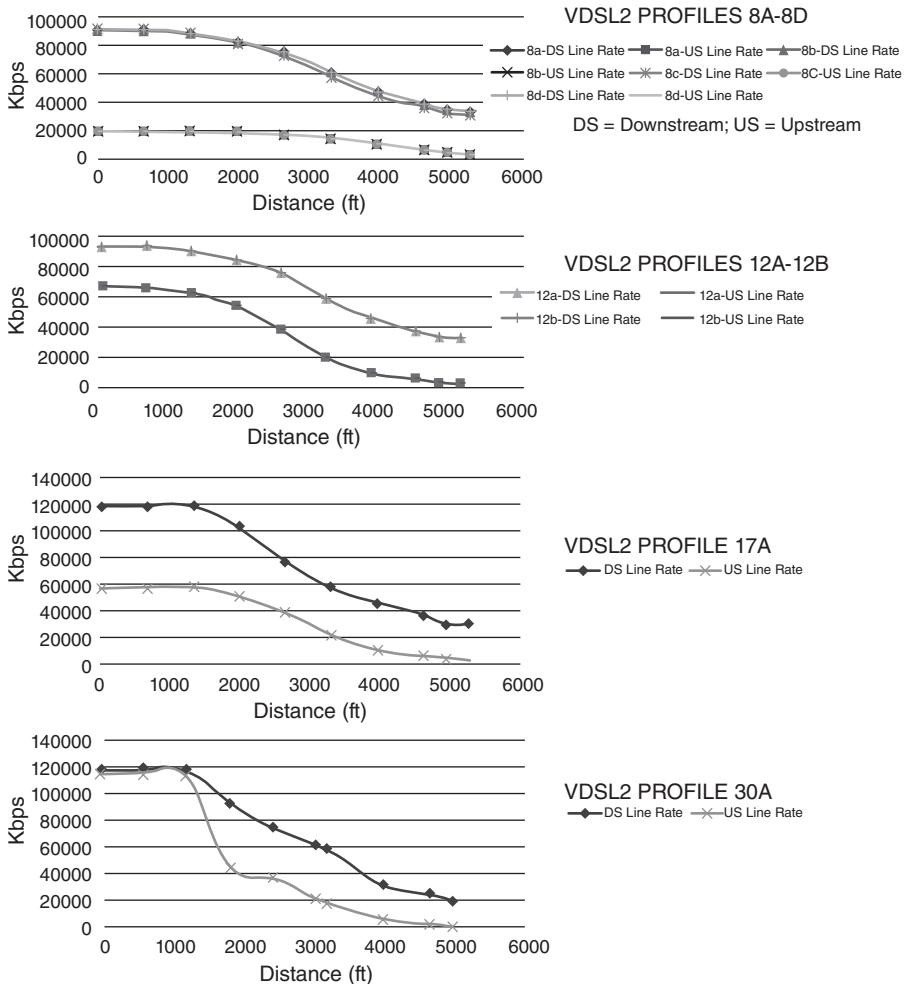


FIGURE 7.23 MDU use of VDSL2.

is in the PON's optical line terminal (OLT) equipment. Between the OLT and the customer's ONT/ONUs, one finds the PON; the PON is comprised of fiber links and passive splitters and couplers.

The industry has seen several generations of PON systems. BPON,⁶ GPON, EPON/GE-PON/1G-EPON, GPON, and 10G-EPON represent various flavors of PON technology. One important distinction between the standards is operational speed: BPON is relatively low speed with 155 Mbps upstream/622 Mbps downstream operation; EPON/GE-PON supports 1.0 Gbps symmetrical operation; GPON supports 2.5/1.25 Gbps asymmetrical operation. Another key distinction is the protocol support for transport of data packets between access

⁶BPON is also known as Asynchronous Transfer Mode (ATM) PON (APON)).

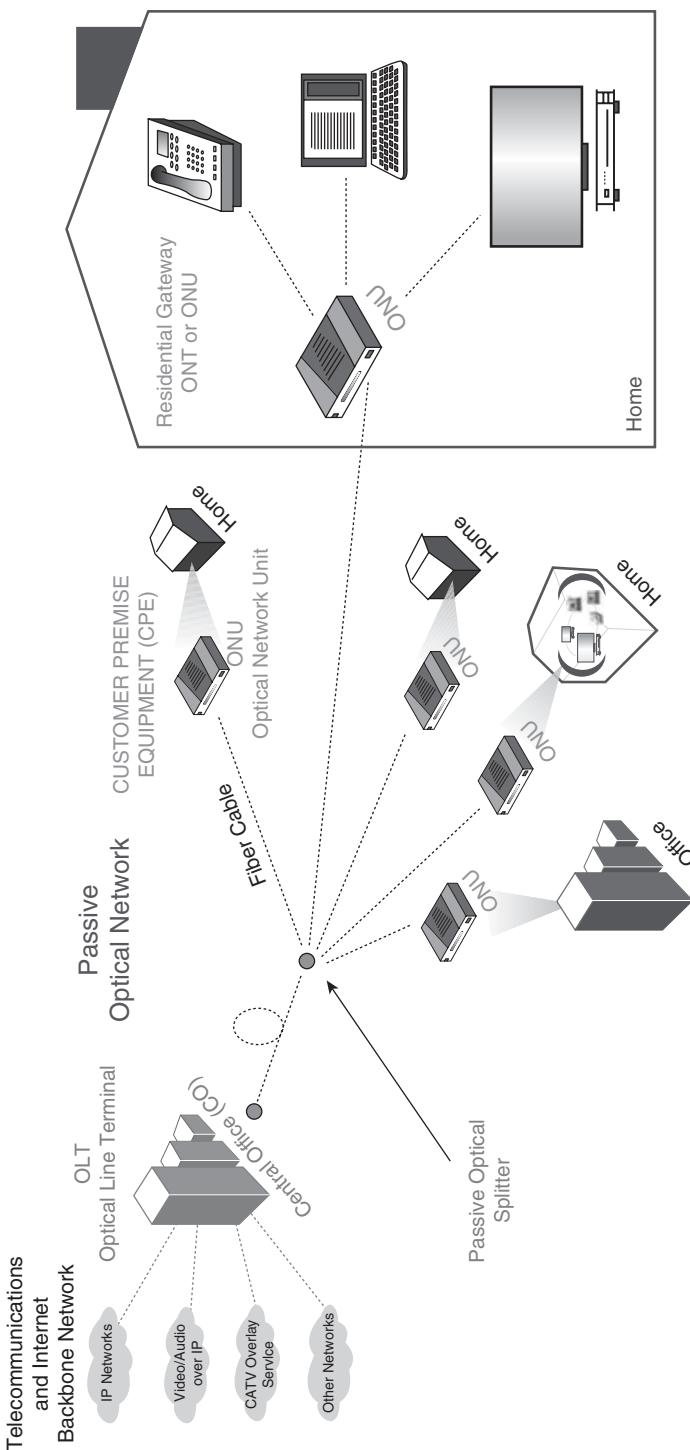


FIGURE 7.24 PON.

network equipment: BPON is based on ATM technology, GE-PON uses native Ethernet, and GPON supports ATM, Ethernet, and WDM using a superset multiprotocol layer. Table 7.10 compares the technologies.

BPON is the oldest PON standard, defined in the mid-1990s. While there is an installed base of BPON, most of the new market focus and actual field deployment is now on the 1 Gbps EPON/GE-PON and the 2.5 Gbps ITU-T GPON.

GE-PON (also known as 1G-EPON) and EPON are different names for the same specification, which is defined by the IEEE 802.3ah Ethernet in the First Mile standard ratified in 2004. This is the current standardized high-volume solution for gigabit PON technologies. BPON suffers from the very aggressive optical timing of ATM and the high complexity of the ATM transport layer. ATM-based FTTH solutions face a number of problems posed by (1) the provisioning process (requires ATM-based central office equipment); (2) the complexity (in timing requirements and protocol complexity); and (3) the cost of components. This cost is exacerbated by the relatively small market for traditional ATM equipment used in the backbone telecommunications network.

GPON was being standardized as the ITU-T G.984 recommendation (see Table 7.11) and is receiving interest in North America and elsewhere. GPON devices have been announced, but there is no large-volume deployment as yet. GPON supports a multiple protocols through translation to the native Generic Encapsulation Method (GEM) transport layer that through emulation provides support for ATM, Ethernet, and WDM protocols. This added complexity and lack of standard low-cost 2.5/1.25 Gbps optical components has delayed industry development of low-cost, high-volume GPON devices. GE-PON or Ethernet in the First Mile has been ratified as the IEEE 802.3ah EFM standard and is already widely deployed in Asia. It uses Ethernet as its native protocol and simplifies timing and lowers costs by using symmetrical 1 Gbps data streams using standard 1 Gbps Ethernet optical components. Similar to other Ethernet equipment found in the extended network, Ethernet-based FTTH equipment is much lower in cost relative to ATM-based equipment, and the streamlined protocol support for an extended Ethernet protocol simplifies development.

At the same time, PON systems supporting 10 Gbps are being readied for deployment to support the need for increased bandwidth to the user. The ITU-T G.988 Recommendation of the 10G GPON (XG-PON) series was approved SG15 meeting held in Switzerland in 2010.⁷ Clearly 10G PON

⁷Since 2008, the research of 10G GPON standards has been supported and promoted by all carrier members, such as AT&T, NTT, France Telecom, Telecom Italia, Portugal Telecom, Deutsche Telecom, Telefonica, Verizon, British Telecom, China Telecom, China Mobile, and China Unicom and leading equipment vendors, chip vendors, and optical module vendors. Carriers, such as Verizon, France Telecom, Telecom Italia, Telefonica, and China Mobile, have actively conducted tests and pilot runs on the 10G GPON technology. Leading equipment vendors, including Huawei, Alcatel-Lucent, and Ericsson, have rolled off their 10G GPON prototypes. Optical module vendors, such as Neophotonics, Source Photonics, and Hisense, also introduced standard-compliant 10G GPON optical modules, and chip manufacturers, such as Vitesse, PMC-Sierra, and Broadcom, are developing 10G GPON-supporting chips [JUN201001].

TABLE 7.10 PON Comparison

Attributes	Technology		
	BPON (APON)	GE-PON (EPON)	GPON
Speed—upstream/ downstream	155/622 Mbps	1.0/1.0 Gbps	1.25/2.5 Gbps
Native protocol	ATM	Ethernet	GEM
Complexity	High	Low	High
Cost	High	Low	Undetermined
Standards body	ITU-T	IEEE	ITU-T
Standard complete	Yes, 1995	Yes, 2004	No
Volume deployment	Yes, in 100,000s	Yes, in 1,000,000s	No
Primary deployment area	North America	Asia	Not applicable

TABLE 7.11 G-PON ITU-T Recommendations

Recommendation	Description
G.984.1, Gigabit-Capable Passive Optical Networks (G-PON)—General characteristics	This Recommendation provides examples of services, User Network Interfaces (UNI), and Service Node Interfaces (SNI) that are required by network operators. In addition, it shows the principal deployment configuration. Wherever possible, this Recommendation maintains characteristics from the ITU-T G.982 and G.983.x series Recommendations in order to promote backward compatibility with existing Optical Distribution Networks (ODN) that comply with these Recommendations.
G.984.2, G-PON—Physical Media Dependent (PMD) layer specification	This Recommendation specifies the physical layer requirements and specifications for the Physical Media Dependent (PMD) layer. It covers systems with nominal line rates of 1244.160 and 2488.320 Mbps in the downstream direction and 155.520, 622.080, 1244.160, and 2488.320 Mbps in the upstream direction. Both symmetrical and asymmetrical (upstream/downstream) G-PON systems are described.
G.984.3, G-PON—Transmission Convergence Layer Specification	This Recommendation specifies the frame format, media access control method, ranging method, OAM functionality, and security in G-PON networks.

provides a ten-fold speed improvement over EPON/GE-PON/1G-EPON, and a fourfold increase over GPON. Future work is expected to include improvements to the XG-PON series (e.g., amendments to describe 5 Gbps upstream.) 10G GPON can be smoothly evolved from GPON or even EPON. A specification known as 10G-EPON (10 Gbps Ethernet PON) developed by the IEEE 802.3av Task Force was also recently approved. Both 1G-EPON and 10G-EPON (as well as GPON) dynamically time-share a single transmission channel among multiple ONUs. In the upstream direction, multiple ONUs take turns transmitting in their preallocated time slots. The upstream transmission occurs in burst mode, since ONUs must only enable their lasers to transmit a burst of data and disable immediately after that. In the downstream direction, the signal from a single transmitter at the OLT is passively split to reach every ONU. The OLT transmitter operates in continuous mode. Being part of the IEEE 802.3 family of standards, all EPON systems use Ethernet framing; thus subscriber data exchanged between ONUs and OLT is encapsulated in the Ethernet frame, adding 25 octets of overhead [ROY201101].

7.6 STORAGE TECHNOLOGIES TO SUPPORT IBTV

Storage technologies are important to Nontraditional TV (NTTV) services, including Internet television, time-shifted TV, VoD, and IPTV, because these services require large amounts of storage and/or content cashing. A typical SD movie may be in the range of 6 GB, and an HD may need in the range of 12–20 GB. A library of 1000 movies would need 6–20 TB. Storage may be viewed as the storage media itself and the local in-data-center network to access the content for distribution to a requesting user.

At press time, about half of the storage deployed is networked; by 2015, the amount of networked storage will increase to 70%, according to industry observers. Fibre Channel (FC) has a 60–80% market share (depending on various market sources). The industry is moving to a unified fabric, namely the combining of FC and Internet Small Computer System Interface (iSCSI) on the Ethernet (there will be only one type of switch and one type of adapter; cabling, which represents 25–30% of the data center cost, is also streamlined) [RAD201001]. Table 7.12 identifies some key concepts and technologies related to storage, while Table 7.13 depicts some typical applications and tradeoffs.

Storage arrays are expected to continue to follow Moore's law for the next few years. 10Gbps Ethernet and 8 Gbps FC are currently the standard interfaces for enterprise arrays. Storage arrays will continue to consist primarily of hard disk drives (HDDs) for the next few years, although the size and form factor may vary, but ultimately the storage will be ultrahigh-density arrays packing large numbers of drives into small footprints. Solid

TABLE 7.12 Key Concepts and Technologies Related to Storage

Cloud computing—storage	The latest term to describe a grid/utility computing service. Such service is provided in the network. From the perspective of the user, the service is virtualized. In turn, the service provider will most likely use virtualization technologies (virtualized computing, virtualized storage, etc.) to provide the service to the user.
Array	Two or more hard disks that read and write the same data. In a RAID (Redundant Array of Inexpensive Disks) (also known as Redundant Array of Independent Disks) storage system, the operating system treats the array as if it were a single hard disk.
Fibre Channel (FC)	The dominant storage networking protocol used in the enterprise data center and for (multimedia) content storage. A high speed storage/networking interface that offers a high performance, large transfer capacity, long cabling distance, system configuration flexibility and scalability, and simplified cabling. The current operating speed is 8 Gbps; the expectation is that a16 Gbps rate will be achievable by mid-decade (by comparison, 10 Gbps Ethernet is expected to move up to a 40 Gbps or even 100 Gbps rates over the same period).
Fibre Channel Arbitrated Loop (FCAL)	A Fibre Channel (FC) implementation where users are attached to a network via a one-way ring (loop) cabling scheme
Fibre Channel over Ethernet (FCoE)	A method for encapsulation of FC frames over Ethernet networks. This allows FC to use 10 Gigabit Ethernet for transport. A content-management site may have several FC fabrics, IP networks dedicated to Network-Attached Storage (NAS), a LAN to link hosts and clients to that storage, and a WAN. FCoE is a technology that makes it possible to link these previously disparate networks, promising simpler administration, less complexity, and lower costs. The success of FCoE depends on a number of factors, including widely available/cost-effective 10 GigE components, and the implementation of the Data Center Ethernet (DCE) (also known as Converged Enhanced Ethernet [CEE]) standard [CAS201001].

(Continued)

TABLE 7.12 (Continued)

Fibre Channel over IP (FCIP)	A protocol for transmitting FC data over an IP network. It allows the encapsulation/tunneling of FC packets and transport via Transmission Control Protocol/Internet Protocol (TCP/IP) networks (gateways are used to interconnect FC Storage Area Networks (SANs) to the IP network and to set up connections between SANs). FCIP uses IP-based network services to provide the connectivity between the SAN islands over LANs, Metropolitan Area Networks (MANs), or WANs. It enables applications developed to run over FC SANs to be supported under IP, enabling organizations to leverage their current IP infrastructure and management resources to interconnect and extend FC SANs. FCIP relies on TCP for congestion control and management and upon both TCP and FC for data error and data loss recovery. FCIP treats all classes of FC frames the same as datagrams.
Fibre Channel SCSI	This refers to products with FC physical and protocol layers using the SCSI command set. The FC interface is completely different from parallel SCSI in that it is a serial interface, meaning command and data information is transmitted on one signal stream organized into packets. The fibre may be either a copper coaxial cable or a fiber optic cable. The signal on the first implementation of Fibre Channel uses a 1 GHz rate, thereby achieving 100 MBps over the cable. The Fibre Channel also implements increased software control of configuration and pushes the total device on the bus to 126 IDs, as opposed to only 8 or 16 on a parallel bus [SUN201001].
Hierarchical Storage Management (HSM)	A storage system in which new, frequently used data is stored on the fastest, most accessible (and generally more expensive) media (e.g., RAID) and older, less frequently used data is stored on slower (less expensive) media (e.g., tape) [SUN201001].
Internet FCP (iFCP)	A protocol that converts FC frames into TCP enabling native FC devices to be connected via an IP network. iFCP is a gateway-to-gateway protocol allows the replacement of FC fabric components, allowing attachment of existing FC-enabled storage products to an IP network. Encapsulation protocols for IP storage solutions where the lower-layer FC transport is replaced with TCP/IP and Gigabit Ethernet. The protocol enables existing FC storage devices or SANs to attach to an IP network. The operation is as follows: FC devices, such as disk arrays, connect to an iFCP gateway or switch. Each FC session is terminated at the local gateway and converted to a TCP/IP session via iFCP. A second gateway or switch receives the iFCP session and initiates a FC session. In iFCP, TCP/IP switching and routing elements complement and enhance, or replace, FC SAN fabric components.

Internet Small Computer System Interface (iSCSI)

A protocol that serializes Small Computer System Interface (SCSI) commands and converts them to Transmission Control Protocol/Internet Protocol (TCP/IP). Encapsulation protocols for IP storage solutions for the support of Direct Attached Storage (DAS) (specifically SCSI-3 commands) over IP network infrastructures (at the physical layer, iSCSI supports a Gigabit Ethernet interface so that systems supporting iSCSI interfaces can be directly connected to standard Gigabit Ethernet switches and/or IP routers; the iSCSI protocol sits above the physical and data-link layers). iSCSI is a protocol for a new generation of storage end-nodes that natively use TCP/IP and replaces FCP with a pure TCP/IP implementation. iSCSI has broad industry support.

Using IP and Gigabit Ethernet to build SANs. Traditional SANs were developed using the FC transport, because it provided gigabit speeds compared with 10 and 100 Mbps Ethernet used to build messaging networks at that time. FC equipment has been costly, and interoperability between different vendors' switches was not completely standardized. Since Gigabit Ethernet and IP have become commonplace, IP storage enables familiar network protocols to be used, and IP allows SANs to be extended throughout the world. Variants include:

- Internet FCP (iFCP)
 - Metro Fibre Channel Protocol (mFCP) is another proposal for handling “IP storage.” It is identical to iFCP, except that Transmission Control Protocol (TCP) is replaced by User Datagram Protocol (UDP).
 - Internet Small Computer System Interface (iSCSI)
 - Fibre Channel Over Internet Protocol (FCIP)
- A disk array storage system that is attached directly to a network rather than to the network server (i.e., host attached). It functions as a server in a client/server relationship, has a processor, an operating system or micro-kernel, and processes file I/O protocols such as SMB and NFS [SUN201001]. An emerging storage approach similar to file-based storage except it makes greater use of metadata. It trades the efficiency and performance of block-based storage for easier management and more automation. Object metadata will let content providers and enterprises manage the storage more effectively and apply policies based on the data content, regulatory requirements, ownership of the data, or based on other principles. The metadata can also be used to dynamically store data at the most appropriate service levels [RAD201001].

Network-Attached Storage (NAS)

Object storage

(Continued)

TABLE 7.12 (*Continued*)

Storage	Infrastructure (typically in the form of appliances) that is used for the permanent or semi-permanent online retention of structured (e.g., databases) and unstructured (e.g., business/e-mail files) corporate information. Typically includes (1) a controller that manages incoming and outgoing communications as well as the data steering onto the physical storage medium (e.g., RAIDs (redundant arrays of independent disks, semiconductor memory, etc); and, (2) the physical storage medium itself. The communications mechanism could be a network interface (such as Gigabit Ethernet), a channel interface (such as Small Computer System Interface [SCSI]), or a SAN Interface (i.e., FC).
Storage appliance	A storage platform designed to perform a specific task, such as NAS, routers, virtualization, etc.
Storage virtualization	Software (sub)systems (typically middleware) that abstract the physical and logical storage assets from the host systems.
Tiered storage	A process for the assignment of different categories of data to different types of storage media. The purpose is to reduce total storage cost and optimize accessibility. Organizations are reportedly finding cost savings and improved data management with a tiered storage approach. In practice, the assignment of data to particular media tends to be an evolutionary and complex activity. Storage categories may be based on a variety of design/architectural factors, including levels of protection required for the application or organization, performance requirements, and frequency of use. Software exists for automatically managing the process based on a company-defined policy. Tiered storage generally introduces more vendors into the environment and interoperability is important. As an example of tiered storage is as follows: Tier 1 data (e.g., mission-critical files) could be effectively stored high-quality Directly Attached Storage (DAS) (but relatively expensive) media, such as double-parity RAIDs (redundant arrays of independent disks). Tier 2 data (e.g., quarterly financial records) could be stored on media affiliated with a SAN; this media tends to be less expensive than DAS drives, but there may be network latencies associated with the access. Tier 3 data (e.g., e-mail backup files) could be stored on recordable compact discs (CD-Rs) or tapes. (Clearly there could be more than three tiers, but the management of the multiple tiers than becomes fairly complex.) Another example (in the medical field) is as follows: Real-time medical imaging information may be temporarily stored on DAS disks as a Tier 1, say for a couple of weeks. Recent medical images and patient data may be kept on FC drives (Tier 2) for about a year. After that, less-frequently accessed images and patient records are stored on AT Attachment (ATA) drives (tier-3) for 18 months or more. Tier 4 consists of a tape library for archiving.

Virtual infrastructure

An infrastructure where there is a dynamic mapping of physical resources to functional service requests, such that the entity requiring service is oblivious to the specific nature of the actual hardware supporting the underlying service.

Virtualization

The abstraction of server, storage, and network resources in order to make them available dynamically for sharing by IT services, both internal to and external to an organization. In combination with other server, storage, and networking capabilities, virtualization offers customers the opportunity to build more efficient IT infrastructures. Virtualization is seen by some as a step on the road to utility computing. An approach that allows several operating systems to run simultaneously on one (large) computer (e.g., IBM's z/VMM operating system lets multiple instances of Linux coexist on the same mainframe computer). It is the practice of making resources from diverse devices accessible to a user as if they were a single, larger, homogenous, appear-to-be-locally-available resource. Virtualization depends on being able to dynamically shift resources across platforms to match computing demands with available resources: the computing environment can become dynamic, enabling autonomic shifting applications between servers to match demand.

Web cache

A Web cache fills requests from the Web server, stores the requested information locally, and sends the information to the client. The next time the Web cache gets a request for the same information, it simply returns the locally cached data instead of searching over the Internet, thus, reducing Internet traffic and response time [SUN201001].

Web Services (WSs)

Web Services provide standard infrastructure for data exchange between two different distributed applications.

TABLE 7.13 Typical Storage Applications by Storage Approach and Tradeoffs

Storage Approach	Applications	Advantages	Limitations
Direct-Attached Storage (DAS)	<ul style="list-style-type: none"> Data and application sharing Data backup/archiving 	<ul style="list-style-type: none"> Simplicity and Low initial cost Ease of management 	<ul style="list-style-type: none"> Storage for each server must be administered separately Inconvenient for data transfer in network environments Relatively high cost Management complexity
Fibre Channel (FC)	<ul style="list-style-type: none"> High data rate content Supports SANs Cache storage Mission-critical applications Distributed content/databases Cache storage/offsite storage Mission-critical applications Data backup/archiving 	<ul style="list-style-type: none"> Used to transmit data between devices at Gbps speeds Flexible in terms of distance Used to transmit data between devices using IP More flexible in terms of distance than Fibre Channel (but not as fast) Fast file access for multiple clients Ease of data sharing High storage capacity Redundancy Ease of drive mirroring High speed High storage capacity High data availability High reliability Security Fault tolerance 	<ul style="list-style-type: none"> May not be as effective as Fibre Channel for large content transfers Management complexity Less convenient than SAN for moving large amounts of data Recovery is difficult in some instances
Internet Small Computer System Interface (iSCSI)			
Network-Attached Storage (NAS)			
Redundant Array of Inexpensive Disks (RAID)	<ul style="list-style-type: none"> Internet/content service providers applications 		
Storage Area Network (SAN)	<ul style="list-style-type: none"> High data rate content Mission-critical applications 	<ul style="list-style-type: none"> Optimal for handling large files High reliability/fault tolerance Scalability 	<ul style="list-style-type: none"> Relatively high cost Management complexity

State Drives (SSD) will not take over for the foreseeable future. Vendors currently incorporate SSD in arrays and will continue to do so, but SSD will be reserved for critical applications requiring very high throughput [RAD201001].

Given the ever-growing volumes of data, more intelligence will be needed in storage systems. According to observers the Storage Area Network (SAN) is taking over much of the intelligence that used to be in the server. In the near future, storage controllers will have sufficient processing power to run, for example, database apps [RAD201001]. A SAN is a special-purpose network that interconnects data storage devices with servers that process requests for such data from a larger network of users. A SAN is a subnetwork of the overall network of an enterprise or content provider. General-purpose networks, such as LANs, enable communication between servers; a SAN uses multiple paths to connect servers and storage systems. A SAN is usually located in close proximity to other computing resources but can have remote elements for backup and archival storage, using wide area network (WAN) carrier technologies services, such as high-capacity SONET/SDH links. A FC network provides connectivity among heterogeneous devices and supports multiple interconnect topologies. The network can be connected to a variety of storage systems, for example, Redundant Array of Inexpensive Disks (RAID) arrays, tape devices, and backup libraries. FC technology supports simultaneous use transport protocols such as IP, SCSI, and iSCSI.

Storage devices and the local networks needed to access them are closely related. The FC roadmap has enabled enterprises and content providers to upgrade over the years from 1 to 2 Gbps, then to 4 to 8 and 16 Gbps in the near future. New technologies, such as Fibre Channel over Ethernet (FCoE), provide another upgrade path. FCoE leverages an enhanced version of the 10 Gbps Ethernet standard referred to as Converged Enhanced Ethernet (CEE) (the changes are mostly related to eliminating dropped packets and relieving congestion). The roadmap for FCoE mirrors Ethernet; this means the next leap is four times the throughput (up to 40 Gbps), which will quickly surpass the FC roadmap [LIB201001].

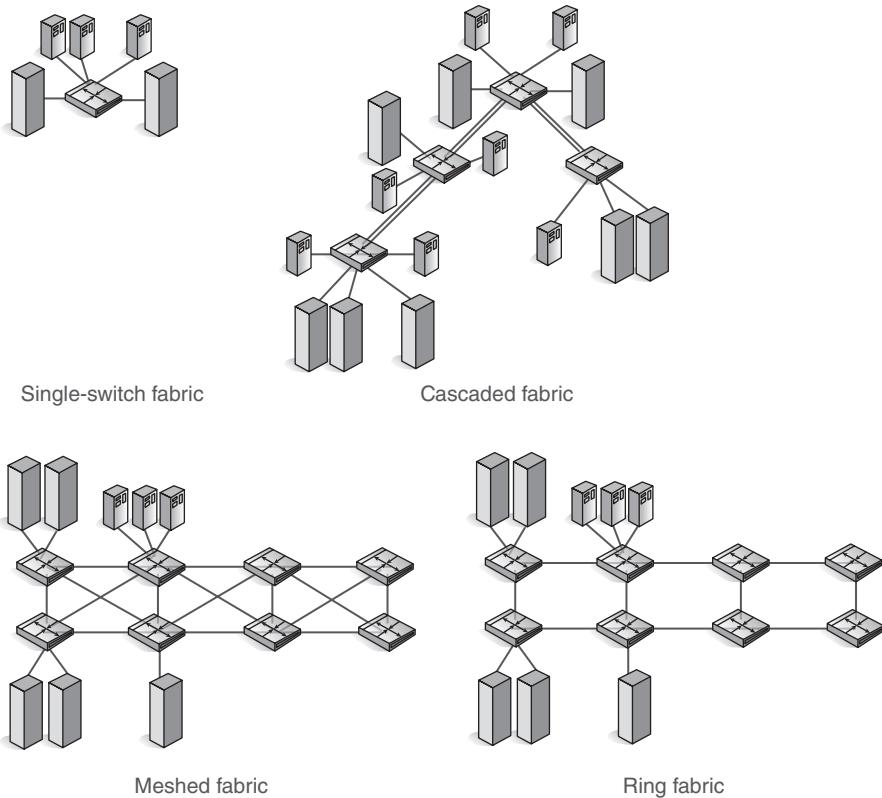
The Ethernet Alliance reportedly sees 2012 as the year when costs are low enough for the market to see widespread adoption of 10 GbE. Generally, when a standard is written, it takes about 10 years before it reaches widespread volume adoption. The earliest 10 GbE components were built around optical fiber, but copper cable-based products soon followed. In most data centers, copper is the standard transport for data and storage networks because it is relatively cheap and easy to install. 10GBASE-T, approved in 2006, has gained some degree of popularity. It uses unshielded (or shielded) twisted-pair cables, and will work at up to 100 m; companies may opt to use already installed Cat 6 cabling, but the distance will be effectively halved. Connectors for 10GBASE-T are RJ-45-style connectors rated at 650 MHz [CIG201001].

A SAN consists of the following hardware and software components [HPS200901]:

- *Switches*: An FC switch creates the fabric of the SAN. A SAN fabric topology defines the arrangement of FC switches in a fabric. By interconnecting switches, one can create scalable SANs with thousands of port connections. A fabric is a single switch or a set of switches connected to form a network. Fabric services manage device names and addresses, timestamps, and other functionality for the switches. A set of switches can be connected as a single fabric, an interconnected network of independent fabrics, or partitioned into multiple logical fabrics. FC supports a maximum of 239 switches in a single fabric. A switch is identified by its function in a SAN:
 - *Core (or Director)*: Provides ISLs for any-to-any connectivity
 - *Edge (or Fabric or SAN)*: Provides user ports for connecting servers and storage systems
- *Routers, Bridges, and Gateways*: Router functionality provides high levels of scalability, dynamic device sharing, and FC network fault isolation. Routers, bridges, and gateways extend the SAN over long distances and enable integration of multi-protocol technologies.
- *Storage Devices*: An SAN can integrate multiple storage system types, such as disk arrays and tape libraries, to allocate storage efficiently.
- *Servers and Host Bus Adapters (HBAs)*: HBAs connect the server to the SAN. HBA drivers provide an intelligent interface to the switches and minimize CPU overhead.
- *Cabling and Cable Connectors*: Fiber optic cables provide the physical connections between SAN components.
- *SAN Management Applications*: Applications manage and monitor components and ensure optimal SAN operation.

A number of fabric topologies are possible, as follows.

- *Single-Switch Fabric*: A single-switch fabric consists of a FC switch, server, and storage system (Figure 7.25, left top). For example, one can connect two single-switch fabrics to create a cascaded fabric. Or, one can connect three or more single-switch fabrics to create a ring fabric or a core-edge fabric.
- *Cascaded Fabric*: A cascaded fabric is a set of interconnected switches, arranged in a tree format, that have one or more of Interswitch links (ISLs) (Figure 7.25, right top). One can connect one switch to one or more switches using a single ISL to each, or connect a pair of ISLs between two switches. One should have a minimum of two ISL connections on each switch to provide fabric path redundancy. One should consider using a cascaded fabric topology if one requires multiple groups of devices with localized intraswitch access.
- *Meshed Fabric*: A meshed fabric is a group of interconnected switches using multiple ISLs for fabric resiliency (Figure 7.25, left bottom). If one ISL fails, the switch automatically reroutes data through an alternate path

**FIGURE 7.25** FC fabrics.

in the fabric. If the alternate path includes other switches, the data must pass through those switches to reach its destination. As one adds switches, ISLs are connected to two or more adjacent switches to maintain mesh connectivity, ensuring path redundancy throughout the fabric. The additional ISL connectivity provides communicating devices with more paths through the fabric. This reduces the chance that, as one adds switches, one will exceed the maximum hop count.

- **Ring Fabric:** A ring fabric is a ring of interconnected switches (Figure 7.25, right bottom). The ring fabric provides a similar level of fabric resiliency as the meshed fabric and ensures full fabric connectivity with a minimum of two paths for each switch.
- **Core-Edge Fabric:** Practitioners recommend using a core-edge fabric wherever possible. A core-edge fabric has one or more FC switches (called core switches) that connect to edge switches in the fabric (Figure 7.26). The core switches provide high bandwidth and redundant connectivity to the edge switches. The edge switches provide user ports for servers and

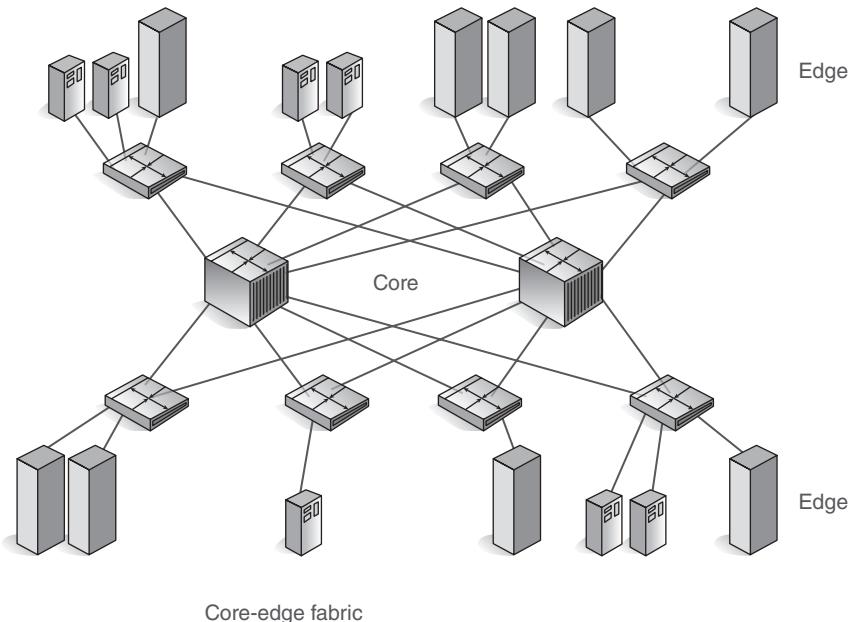


FIGURE 7.26 FC core-edge fabric.

storage. One can also connect centralized storage (disk or tape) to the core switches if centralized access is required. The core-edge fabric is optimal for:

- Many-to-many connectivity environments that require high performance
- Unknown or changing I/O traffic patterns
- SAN-wide storage pooling

To choose a SAN fabric topology, one must determine which data access type is appropriate for a given environment. Table 7.14 lists the data access performance ratings for each SAN fabric topology [HPS200901].

An integration technology now emerging, FCoE allows one to converge Ethernet and FC technology at the server, providing cable, adapter, and switch consolidation. Converged Network Adapters (CNAs) are utilized to support this convergence. Typical two-port 10GbE CNAs, together with a converged 10GbE Switch Module, provide Converged Ethernet solutions that offers native Ethernet and FC connectivity, maximum bandwidth and performance, and simplicity in a converged environment. Figure 7.27 depicts the arrangement pictorially.

Cloud data storage (also called Storage-as-a-Service [SaaS]—do not confuse this acronym with the Software-as-a-Storage service defined earlier) is beginning to see some deployment; however, it is still a relatively new concept

TABLE 7.14 Data Access Performance Ratings for Various SAN Fabrics

SAN Topology	Data Access Performance			
	Local (One-to-One).	Centralized (Many-to-One)	Data Access between Multiple, Dispersed Servers and One Centrally Located Storage System	Distributed (Many-to-Many) Data Access between Multiple, Dispersed, and Storage Systems
Single-switch fabric	Highest	Highest	Highest	Highest
Cascaded fabric	Highest	Not recommended	Not recommended	Not recommended
Meshed fabric	Medium	Medium	Medium	High
Ring fabric	Medium	Highest	Medium	Not recommended
Core-edge fabric (15:1, 7:1)	Medium	High	High	High
Core-edge fabric (3:1, 1:1)	High	Highest	Highest	Highest

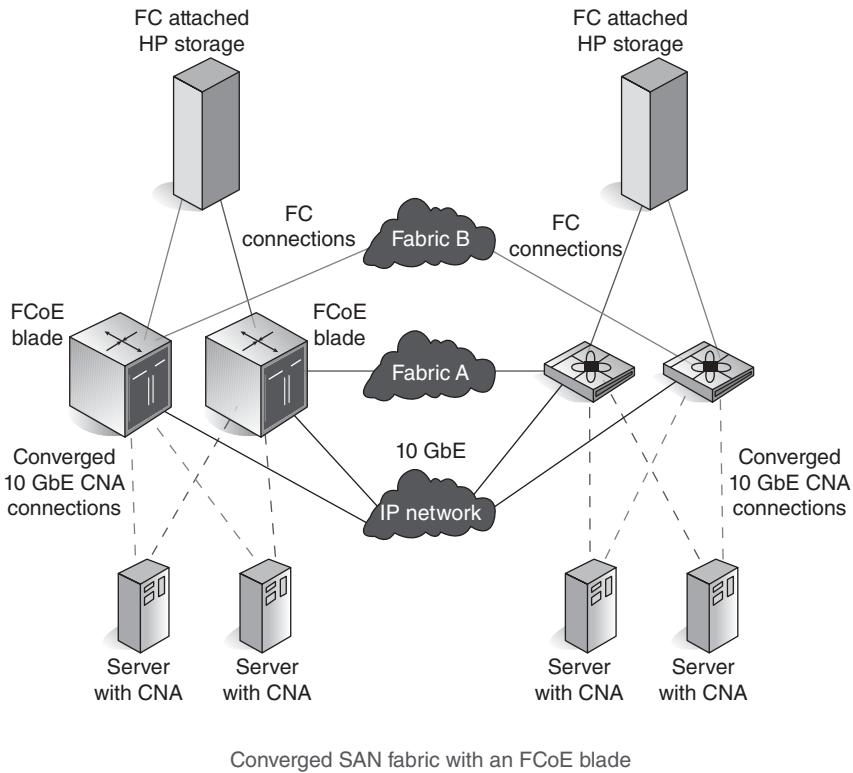


FIGURE 7.27 FC over Ethernet (FCoE) example.

[COO201001]. At press time, cloud data storage was available from vendors such as, but not limited, to Amazon S3, Iron Mountain Inc., and Nirvanix Inc. To mitigate control problems, one should have a contract with a tight service-level agreement (SLA). Latency is a critical issue with cloud storage. Like any other remote application, cloud storage requires proper WAN bandwidth: enough capacity to transmit files back and forth between location and the storage service provider. The bandwidth needed to support an environment depends on the amount of storage traffic the system generates.

7.7 SERVICE PROVIDER STRATEGIES FOR NTTV

7.7.1 Overview

In this section we provide a brief view to what might be network evolution to support evolving video services; it is not intended to exhaustive in any way.

The basic assumption is that TV and new on-demand programming and interactive video services will increasingly be delivered to the consumer

through IP in a number of developed countries, especially in urban areas (also as described in Appendix 7A.). Large traffic growth is expected to result from a steady increase in demand for VoD and HD content delivered over both IPTV multicast and VoD unicast connections. To support this ongoing trend, the evolving carrier-grade IP network requires scaling video transport from 1 to 10 Gbps at line rate, and being positioned to support 100 Gbps and beyond, while greatly increasing the total number of multicast groups and broadcast TV channels [CIS200702]. This transition will necessitate important network upgrades, some of which are listed below (service providers are not necessarily expected to implement all of these, but should implement a meaningful, appropriate subset).

- Be prepared to deploy IPv6 technology in the network.
- Be prepared to upgrade and scale the core network to high speed routing, switching, and transport.
 - Build Carrier-Class IP next-generation networks (the IP/MPLS infrastructure must be able to meet the same carrier-class requirement at both node and network level as it has been traditionally the case for SONET and other carrier services).
 - Deploy OTN technologies at the optical layer. Initially IPoDWDM may be adequate, but a standardized architecture, as offered by OTN, is desirable in the long term.
 - Transition network to Ethernet-based systems.
- Be prepared to upgrade the access network to high speed (e.g., using PON and/or other hybrid fiber/cable technologies).
- Deploy network-resident caches and storage to place frequently-used content close to the user.
- Enhance that portion of the network that supports the high-speed backbone for Internet transit and also enhance the customer-facing Internet access network and services.
- Embrace IP services and move away from Time Division Multiplexing (TDM) technologies. While services previously offered on TDM architectures have strict performance requirements, newer IP technologies (including but certainly not limited to pseudowire⁸) can provide comparable QoS.
- Move to a switched environment (such as IPTV principles) such that the access speed can be (say) $4 \times 10 = 40$ Mbps (to support four simultaneous actively selected HD channels) instead of having to be (say) $100 \times 10 = 1$ Gbps (to support 100 channels, which are then switched at the STB-level)

⁸Pseudowires allow one to encapsulate and transport TDM, Frame Relay, and ATM traffic over MPLS. Its deployment is and will continue to be limited, as applications migrate to use the IP layer directly.

- Deploy nPVR technology to support TSTV
- Deploy cloud-based technology to support network storage and to support video streaming
- Satellite providers should deploy hybrid networks that combine wireless and appropriate terrestrial distribution. Hybrid DTH/Internet access systems will be useful architectures, especially for the BRICA countries (Brazil, Russia, India, China, and Africa). Also, the use of low-orbit satellites may be useful.

7.7.2 Discussion

For traditional carriers, a variety of architectures, system (switching, transmission, and routing) technologies, and platforms must be upgraded meet the NTTV and other user requirements, as several previously distinct networks are converged into one. With IP as the common denominator, service-specific and feature-specific platforms will form the multicapable edge, converging around a common IP/optical core. Each different application and technology will place its own unique set of requirements on the IP infrastructure, as noted in a Cisco whitepaper [CIS200701]:

- *Application Convergence:* Carriers can integrate new IP data, voice, and video applications over a single broadband infrastructure for increased profitability. Application convergence opens the doors to “all-media services,” such as IBTV/IPTV services that entail not just voice, video, or data, but an integration of all three. This and other innovative value-added services can be delivered over any broadband connection.
- *Service Convergence:* IP makes a service available to end users across any access network. For example, a service available in the office can be available over a wireless LAN, a broadband connection, or a cellular network. A streamed TV program should be available on the home TV, the home PC, the tablet, and the smartphone or other portable media devices (e.g., portable media players [PMPs]). All these access networks can transfer the service and the state of connection transparently as the user roams, using the most efficient and cost-effective means possible.
- *Network Convergence:* Creating a converged network is a goal that many carriers are already pursuing through their efforts to eliminate multiple service-specific networks or to reduce multiple layers within a network. A “many services, one network” model in which a single network can support all existing and new services will dramatically reduce the total cost of ownership for service providers.

Table 7.15 summarizes some IP possible technologies for evolving carrier networks, as advocated by Cisco Systems [CIS200702].

TABLE 7.15 IP Technologies for Evolving Carrier Networks

Service	Recommended Transport Protocols	Transport Function
Residential high-speed Internet	EoMPLS or IEEE 802.1ad	Backhaul Internet traffic from the access network to the Broadband Remote Access Router for Authentication, Authorization, and Accounting (AAA), and service control. Provide QoS, tiered, quota-based, and usage-based Internet access.
Residential VoIP	EoMPLS or Layer 3 IP Routing over MPLS FRR	Connect signaling traffic to softswitch and RTP traffic to Internet or core IP network. Provide QoS.
Residential IPTV	Layer 3 PIM SSM over MPLS FRR	Broadcast TV service with massive scalability, fast recovery from failures, and excellent QoE.
Residential video on demand	Layer 3 IP Routing over MPLS FRR	Video on demand service with massive scalability, fast recovery from failures, and excellent QoE.
Business Ethernet Private Line (EPL)	EoMPLS or IEEE 802.1ad	Transport of Ethernet circuit at full data rate with no statistical multiplexing. This requires QoS.
Business Ethernet Virtual Private Line (EVPL)	EoMPLS or IEEE 802.1ad	Transport of Ethernet Virtual Connection with CIR/EIR and statistical multiplexing gain.
Business MPLS VPN	MPLS or IEEE 802.1ad	Transport of subscriber Ethernet Virtual Connection to MSE router that is the provider edge of the MPLS VPN service. CIR/EIR guarantees bandwidth.
Business E-LAN	H-VPLS or IEEE 802.1ad	Multipoint virtual LAN service for business customers. CIR/EIR guarantees bandwidth.
Mobile backhaul	EoMPLS or IEEE 802.1ad	Pseudowire backhaul for 3G, WiMAX, and Wi-Fi networks.
Wholesale residential high-speed internet	EoMPLS or IEEE 802.1ad	Pseudowire backhaul from the access network to the retail service provider.
Wholesale IPTV and Vod	RFC 2547bis MPLS VPN with multicast	Private IP network with multicast that interconnects the retail service provider with the access network.
Wholesale business services	EoMPLS or IEEE 802.1ad	Provide transport from the business customer to the retail service provider with EIR/CIR bandwidth guarantees.

REFERENCES

- [AND201001] J. Anderson, M. Traverso, “Optical transceivers for 100 gigabit Ethernet and its transport,” IEEE Communications Magazine, March 2010, pages S35 ff.
- [APP201101] Apple, “HTTP live streaming overview,” Mac Dev Center, MacOS X Developer Library, November 2011.
- [BRE201101] Breaking Point Systems, “Netflix video streaming protocol,” White Paper, 2011, 3900 North Capital of Texas Highway Austin, TX 78746.
- [CAL200201] Calsoftlabs, “Basic streaming technology and RTSP protocol,” Calsoft-labs Whitepaper, 39465 Paseo Padre Parkway, Suite 2900, Fremont, CA 94538. 2002.
- [CAR201001] S. Carew et al., “Cisco introduces faster router,” Reuters, New York, Tue March 9, 2010.
- [CAS201001] R. Castagna, “Essential guide to storage networking,” Storage Media Group/SearchStorage.com Whitepaper, March 2010.
- [CIG201001] C. Cignoli, “Timetable for 10GigE,” Essential Guide To Storage Networking, Storage Media Group/SearchStorage.com Whitepaper, March 2010.
- [CIS200701] Cisco, “Building the carrier-class IP next-generation network,” Whitepaper, 2007, Cisco Systems, Inc. 170 West Tasman Dr. San Jose, CA 95134 USA.
- [CIS200702] Cisco, “IP NGN carrier Ethernet design: Powering the connected life in the zettabyte era,” Cisco Whitepaper, 2007, Cisco Systems, Inc., 170 West Tasman Dr., San Jose, CA 95134, USA.
- [CIS200801] Staff, Cisco Whitepaper “Cisco visual networking index: Forecast and methodology, 2008–2013,” (June 9, 2009).
- [COO201001] R. Cook, “Cloud data storage services for smaller businesses: The pros and cons,” 04.19.2010, *SearchSMBStorage.com*, c/o TechTarget, 117 Kendrick Street, Needham, MA 02494.
- [CRE200901] M. Creeger, “Cloud computing: An overview—a summary of important cloud-computing issues distilled from ACM CTO Roundtables,” Queue vol. 7, no. 5, June 1, 2009, ACM Digital Library.
- [D32200701] Murat Tekalp, Editor, “D32.2, Technical Report #2 on 3D telecommunication issues,” Project Number: 511568, Project Acronym: 3DTV, Title: Integrated Three-Dimensional Television—Capture, Transmission and Display, February 20, 2007.
- [DAV201001] C. Davies, “DECE UltraViolet cross-platform DRM ‘digital locker’ unveiled; Apple conspicuously absent,” Slashgear (online Magazine), July 20th 2010.
- [DAV201101] C. Davies, “Apple iCloud streaming Movie storage deal imminent tip insiders,” October 13, 2011, Slashgear (online magazine).
- [FLO201101] E. Flock, H. Tsukayama, “iCloud, cloud computing services promise to change the way we use computers,” Washington Post/Bloomberg, June 6, 2011.
- [HPS200901] Staff, “HP StorageWorks, SAN design reference guide,” Fifty-third edition, February 16, 2009. Hewlett-Packard Development Company, L.P.
- [JDA201001] J. D’Ambrosia, “100 gigabit ethernet and beyond,” IEEE Communications Magazine, March 2010, pages S6 ff.
- [JUN201001] J. Junmu, “ITU-T SG15 chairperson talks on 10G GPON: Industry ready for a boom, C114 (online magazine),” August 17, 2010, 4F Room 421 No.822 Yishan Rd, ShangHai China(200233).

- [KOL201101] N. Kolakowski, “Cloud computing: Apple’s iCloud offers Amazon, Google competition,” Eweek (online magazine), June 7, 2011.
- [LIB201001] B. Laliberte, “Storage networking outlook,” Essential Guide To Storage Networking, Storage Media Group/SearchStorage.com Whitepaper, March 2010.
- [MIN200501] D. Minoli, *A Networking-Approach to Grid Computing*. Wiley, 2005, New York.
- [MIN200801] D. Minoli, *Enterprise Architecture A thru Z: Frameworks, Business Process Modeling, SOA, and Infrastructure Technology*. CRC Press, 2008, Auerbach, Taylor and Francis, New York.
- [PAN201101] R. Pantos, Ed. “HTTP live streaming, internet-draft draft-pantos-http-live-streaming-07,” September 30, 2011.
- [PAU201101] I. Paul, “Amazon prime vs. netflix: Video streaming feature showdown,” PCWorld, Feburary 23, 2011.
- [PCM200901] PCM, “FTTH fiber to the home overview,” PCM-Sierra, Mission Towers, 3975 Freedom Circle, Santa Clara, CA 95054, USA, 2009 Whitepaper.
- [PHI201101] G. Philpott, “Adaptive bit rate video streaming: Why delivery will matter more than codec,” Mashable (online Magazine), January 25, 2011.
- [RAD201001] A. Radding, “SAN of the future,” Essential Guide To Storage Networking, Storage Media Group/SearchStorage.com Whitepaper, March 2010.
- [ROE201001] J. Roese, et al., “Optical transport network evolving with 100 gigabit ethernet,” IEEE Communications Magazine, March 2010, pages S28 ff.
- [ROY201101] R. Roy, G. Kramer, et al., “Performance of 10G-EPON,” IEEE Communications Magazine, November 2011, pages 78 ff.
- [SCH199801] H. Schulzrinne, A. Rao, R. Lanphier, “Real time streaming protocol (RTSP),” April 1998, IETF Request for Comments (RFC) 2326.
- [SCH200301] H. Schulzrinne, S. Casner, et al., “RTP: A transport protocol for real-time applications,” IETF Request for Comments (RFC) 3550, July 2003.
- [SJO200801] D. Sjöberg, “Content delivery networks: Ensuring quality of experience in streaming media applications TeliaSonera International Carrier,” CDN white paper, August 14, 2008.
- [SUN201001] SunStar, “Storage glossary of terms,” 900 West Hyde Park Blvd. Inglewood, CA 90302. 2010.
- [ULT201101] UltraViolet Web Site, <http://www.uvnu.com>, November 2011.
- [WAV201101] Wavelength Media, “Flash video: Progressive download, on-line tutorial,” MediaCollege.com. PO Box 128,Te Awamutu, New Zealand. 2011.
- [WEL201001] G. Wellbrock, T. J. Xia, “The road to 100G deployment,” IEEE Communications Magazine, March 2010, pages S14 ff.
- [ZHO200901] Zhone Technologies, “Zhone VDSL2 technology,” November 2009, Zhone Technologies, Inc., @ Zhone Way, 7001 Oakport Street, Oakland, CA 94621, USA.

APPENDIX 7A A PERSPECTIVE ON THE FUTURE

The following material is based on a Cisco white paper entitled: “*Cisco Visual Networking Index: Forecast and Methodology, 2008–2013*” (June 9, 2009),

which provides a perspective on the critical nature of IP (and the Internet) in support of visual-based communications, including video and television.

7A.1 Global Internet Highlights

- *Annual global IP traffic will exceed two-thirds of a zettabyte (667 EB) in 2013.* The 2008 forecast anticipated a run rate of 522 EB per year in 2012. The economic downturn has only slightly tempered traffic growth, and this year's forecast predicts 510 EB per year in 2012, growing to 667 EB per year or 56 EB per month in 2013.
- *Global IP traffic will quintuple from 2008 to 2013.* Overall, IP traffic will grow at a compound annual growth rate (CAGR) of 40%.
- *In 2013, the Internet will be nearly four times larger than it is in 2009.* By year-end 2013, the equivalent of 10 billion DVDs will cross the Internet each month.
- *Peer-to-peer (P2P) is growing in volume, but declining as a percentage of overall IP traffic.* P2P file-sharing networks are now carrying 3.3 EB per month and will continue to grow at a moderate pace with a CAGR of 18% from 2008 to 2013. Other means of file sharing, such as one-click file hosting, will grow rapidly at a CAGR of 58% and will reach 3.2 EB per month in 2013. Despite this growth, P2P as a percentage of consumer Internet traffic will drop to 20% of consumer Internet traffic by 2013, down from 50% at the end of 2008.

7A.2 Global Video Highlights

- *Internet video is now approximately one-third of all consumer Internet traffic,* not including the amount of video exchanged through P2P file sharing.
- *The sum of all forms of video (TV, video On Demand, Internet, and P2P) will account for over 91% of global consumer traffic by 2013.* Internet video alone will account for over 60% of all consumer Internet traffic in 2013.
- *In 2013, Internet video will be nearly 700 times the U.S. Internet backbone in 2000.* It would take well over half a million years to watch all the online video that will cross the network each month in 2013. Internet video will generate over 18 EB per month in 2013.
- *Video communications traffic growth is accelerating.* Though still a small fraction of overall Internet traffic, video over instant messaging and video calling are experiencing high growth. Video communications traffic will increase tenfold from 2008 to 2013.
- *Real-time video is growing in importance.* By 2013, Internet TV will be over 4% of consumer Internet traffic, and ambient video will be 8% of

consumer Internet traffic. Live TV has gained substantial ground in the past few years: globally, P2P TV is now slightly over 7% of overall P2P traffic at over 200 PB per month.

- *Video On Demand (VoD) traffic will double every two years through 2013.* Consumer IPTV and CATV traffic will grow at a 53% CAGR between 2008 and 2013, compared to a CAGR of 40% for consumer Internet traffic.

7A.3 Global Mobile Highlights

- *Globally, mobile data traffic will double every year through 2013, increasing 66× between 2008 and 2013.* Mobile data traffic will grow at a CAGR of 131% between 2008 and 2013, reaching over 2 EB per month by 2013.
- *Almost 64% of the world's mobile data traffic will be video by 2013.* Mobile video will grow at a CAGR of 150% between 2008 and 2013.
- *Mobile broadband handsets with higher than 3G speeds and laptop air-cards will drive over 80% of global mobile traffic by 2013.* A single high-end phone (such as an iPhone or Blackberry) generates more data traffic than 30 basic-feature cell phones. A laptop aircard generates more data traffic than 450 basic-feature cell phones.

7A.4 Regional Highlights

- *IP traffic is growing fastest in the Middle East and Africa,* followed closely by Latin America. Traffic in Middle East and Africa will grow at a CAGR of 51%.
- *IP traffic in North America will reach 13 EB per month by 2013 at a CAGR of 39%.* Monthly Internet traffic in North America will generate 2.4 billion DVDs worth of traffic, or 10 EB per month.
- *IP traffic in Western Europe will reach 12.5 EB per month by 2013 at a CAGR of 37%.* Monthly Internet traffic in Western Europe will generate 2.2 billion DVDs worth of traffic, or 9 EB per month.
- *IP traffic in Asia Pacific will reach 21 EB per month by 2013 at a CAGR of 42%.* Monthly Internet traffic in Asia Pacific will generate 4.1 billion DVDs worth of traffic, or 16.5 EB per month.
- *IP traffic in Japan will reach 3 EB per month by 2013 at a CAGR of 37%.* Monthly Internet traffic in Japan will generate half a billion DVDs worth of traffic, or 2 EB per month.
- *IP traffic in Latin America will reach 2 EB per month by 2013 at a rate of 50%.* Monthly Internet traffic in Latin America will generate 410 million DVDs worth of traffic, or 1.7 EB per month.
- *IP traffic in Central and Eastern Europe will reach 2 EB per month by 2013 at a rate of 49%.* Monthly Internet traffic in Central and Eastern

Europe will generate 340 million DVDs worth of traffic, or 1.4 EB per month.

- *IP traffic in the Middle East and Africa will reach 1 exabyte per month by 2013 at a rate of 51%.* Monthly Internet traffic in the Middle East and Africa will generate 140 million DVDs worth of traffic, or 550 PB per month.

Some details follow.

As shown in Table 7A.1, global consumer IP traffic is expected to surpass 40 Eb per month in 2013. The majority of today's consumer IP traffic is Internet traffic, but consumer IPTV and VoD traffic will grow more rapidly than Internet at a CAGR of 53%.

"Non-Internet IP Video" refers to IP traffic generated by traditional commercial TV services. This traffic remains within the footprint of a single service provider, so it is not considered Internet traffic (for Internet video delivered to the set-top box see "Internet Video to TV" in the Table 7A.2)

Consumer Internet Traffic encompasses any IP traffic that crosses the Internet and is not confined to a single service provider's network. P2P traffic, still the largest share of Internet traffic today, will decrease as a percentage of overall Internet traffic. Internet video streaming and downloads are beginning to take a larger share of bandwidth, and will grow to over 60% of all consumer Internet traffic in 2013. See Table 7A.3.

TABLE 7A.1 Global Consumer IP Traffic, 2008–2013
 Consumer IP Traffic, 2008–2013

	2008	2009	2010	2011	2012	2013	CAGR 2008–2013 (%)
By type (PB per month)							
—Internet	6020	8755	12,726	18,601	25,168	32,129	40
Denotes all IP traffic that crosses an Internet backbone (see more details in Table 7A.3)							
—Non-Internet IP	1004	1644	2628	4006	5,899	8415	53
Here includes IP traffic generated by traditional commercial TV services; IP transport of TV/VoD (see more details in Table 7A.2)							
By geography (PB per month)							
North America	1,522	2,306	3,522	5,466	7,472	9,563	44
Western Europe	1,965	2,682	3,706	5,351	7,354	9,561	37
Asia Pacific	2,730	4,131	6,097	8,679	11,939	15,661	42
Japan	378	593	880	1,301	1,707	2,129	41
Latin America	202	336	551	840	1,187	1,629	52
Central Eastern Europe	180	283	480	780	1,122	1,602	55
Middle East and Africa	45	69	118	190	285	398	55
Total (PB per month)	7,023	10,399	15,354	22,606	31,067	40,543	42
Consumer IP traffic							

Source: Cisco VNI, 2009.

TABLE 7A.2 Global Consumer Non-Internet IP Traffic, 2008–2013

Consumer Non-Internet IP Traffic, 2008–2013	2008	2009	2010	2011	2012	2013	CAGR 2008–2013 (%)
By subsegment (PB per month)							
Cable MPEG-2 VoD	804	1326	2155	3332	4957	7155	55
Cable MPEG-4 VoD	6	12	20	31	51	77	66
IPTV VoD	193	307	453	643	892	1182	44
By geography (PB per month)							
North America	243	424	715	1109	1633	2350	57
Western Europe	343	506	717	1018	1513	2111	44
Asia Pacific	243	424	715	1109	1633	2350	57
Japan	110	172	266	396	536	715	45
Latin America	38	66	114	185	267	385	59
Central Eastern Europe	18	40	83	162	279	449	91
Middle East and Africa	8	12	19	27	39	55	47
Total (PB per month)	1004	1644	2628	4006	5899	8415	53
Non-Internet IP video traffic							

Source: Cisco VNI, 2009.

TABLE 7A.3 Global Consumer Internet Traffic, 2008–2013

Consumer Internet Traffic, 2008–2013	2008	2009	2010	2011	2012	2013	CAGR 2008–2013 (%)
By sub-segment (PB per month)							
—Web/Email	1239	1595	2040	2610	3377	3965	26
Includes web, email, instant messaging, and other data traffic (excluding file sharing)							
Note that “data” may include the download of video files that are not captured by the “Internet video to PC” forecast. It includes traffic generated by all individual Internet users. An Internet user is defined as someone who accesses the Internet through a desktop or laptop at home, school, Internet café, or other location outside the context of a business.	3345	4083	5022	6248	7722	9629	24
—File Sharing (P2P)							
Includes peer-to-peer traffic from all recognized P2P systems, such as BitTorrent, eDonkey, and web-based file sharing. Note that a large portion of P2P traffic is due to the exchange of video files, hence a total view of the impact of video on the network should count P2P video traffic (estimated to be approximately 70–80% of P2P in 2009) in addition to the traffic counted in the “Internet Video to PC” and “Internet Video to TV” categories. Note: The P2P category is limited to traditional file exchange, and does not include commercial video-streaming applications that are delivered through P2P, such as PPStream or PPLive							

(Continued)

TABLE 7A.3 (Continued)

Consumer Internet Traffic, 2008–2013

						CAGR 2008–2013 (%)
	2008	2009	2010	2011	2012	2013
—Internet Gaming Includes casual online gaming, networked console gaming, and multiplayer virtual world gaming	47	87	135	166	217	239
—Internet Voice Includes traffic from retail VoIP services and PC-based VoIP, but excludes wholesale VoIP transport	103	129	152	174	183	190
—Internet Video Communications Includes PC-based video calling, webcam viewing, and web-based video monitoring—expected to experience substantial long-term growth in the 2013–2018 timeframe	36	57	94	160	239	354
—Internet Video to PC Online video that is downloaded or streamed for viewing on a PC screen, free or pay TV or VoD viewed on a PC, excludes P2P video file downloads (it is distinct from Internet-delivery of video to a TV screen through a set-top box or equivalent device). Much of the video viewed on PC is short-form content, and a large part of it is made up of free clips, episodes, and other content offered by traditional content producers, such as movie studios and television networks	1112	2431	4268	6906	9630	12,442

—Internet Video to TV Free or pay TV or VOD delivered via Internet but viewed on a TV screen using a set-top box or media device; examples of devices now available include Microsoft's Xbox 360 and the Roku digital video player, through which users can download film and television content.	29	149	381	1004	1711	2594	146%
—Ambient Video Nannycams, petcams, home security cams, and other persistent video streams	110	224	634	1332	2089	2715	90
By geography (PB per month)							
North America	1279	1881	2807	4357	5839	7213	41
Western Europe	1622	2177	2989	4333	5841	7450	36
Asia Pacific	2487	3707	5382	7570	10,306	13,311	40
Japan	268	421	614	905	1,172	1,415	39
Latin America	165	270	437	655	921	1243	50
Central Eastern Europe	163	242	397	619	843	1153	48
Middle East and Africa	37	57	100	162	246	343	56
Total (PB per month)	6020	8755	12,726	18,601	25,168	32,129	40
Consumer Internet traffic							

Source: Cisco VNI, 2009.

8 Nontraditional Video Display and Content Sources

This chapter provides a short overview of Nontraditional TV (NTTV) trends, display units, and content sources. The examples of commercial services and service providers identified at various points throughout this text are intended only to depict what we believe to be persistent technical/usage trends. Some of these service/providers may sunset some of these initiatives or offerings over time; some providers or products may disappear—other will emerge. But we believe that the general trends discussed here, as a whole, will persist and prevail. These services are currently provided with IPv4; however, we are of the opinion that over the next few years, on IPv6 and/or IPv6, multicasting with applications to linear and nonlinear video distribution will become pervasive.

8.1 NTTV TRENDS

According to market research company Futurescape, by 2014, 54% of flat-panel TVs shipped globally (148.3 million units) in 2014 will have Internet connectivity and services. By this same date, 57 million U.S. broadband households will be viewing full-length online video on TV, and by 2015, more than 43 million U.S. homes will have at least one Connected TV (CTV) by 2015; this represents about 37% of the United States' current 116 million TV households. It was also forecast that European households with a connected TV will grow from less than 4 million in 2009 to 47 million in 2014 [FUT201101]. At press time, countries with large broadband penetration include Japan, South Korea, Singapore, the majority of Western Europe, the United States and Canada, Australia, and New Zealand.

Below is a representative list of press time industry activities that highlights the theme of this book [FUT201101].

- Sony: Partnering with Google TV for Web-on-TV service.
- Toshiba: Using Yahoo Connected TV (which has deals with seven of the top 10 TV manufacturers) for TV apps.
- Apple TV: Streaming media player for Apple iTunes store.

- Liberty Global cable and satellite TV (18 million subscribers in Europe, Chile, and Australia): Next-generation set-top box will access Web content and incorporate social networking, 2011 rollout starts with Netherlands, Germany, and Austria.
- DISH Network satellite TV (14 million subscribers in the United States): Offering discounted set-top box for subscribers to access Google TV services.
- Verizon FiOS IPTV (3.2 million subscribers in the United States): Integrates Facebook and Twitter apps with television viewing.
- Microsoft Xbox Live and Sony PS3 deliver movies, other video content, and some interactive services.
- Dell: Living room media center PCs, such as the Dell Inspiron Zino HD desktop.
- Broadcasters in the United States are also considering to deploy Mobile TV, as they roll out the new mobile television standard ATSC-M/H, which allows TV stations to put their live broadcasts on mobile devices with relatively little investment [HAR201001].

8.2 NTTV DISPLAY UNITS

We noted in Chapter 1 that a multitude of display devices are now employed for video consumption. In addition to traditional TV sets and PCs, users are now starting to employ Connected TVs (also known as Smart TVs). Figure 8.1 depicts the evolution of Internet access on a TV screen over time, culminating with the use of Smart TVs. TV manufacturers see Internet connectivity as a feature that can differentiate them competitors' products. Figure 8.2 depicts an example of a Smart TV. Furthermore, consumers are using portable media devices, smartphones, PDAs (personal digital assistant), videogame consoles (e.g., the Microsoft Xbox 360 and Sony PlayStation 3), tablets screen (e.g., Amazon Kindle/Apple iPad), and/or a device in a car or boat.

Questions such as these are now being posed:

What will the viewer see first when they switch on their television? An interface and content from the manufacturer? Or a pay-TV operator? Or a new entrant, such as Apple TV or Google TV?

Initial connected TV products were either closed/apps based or open/browser based. The closed apps-based approach presents viewers with only preselected content and services via an apps menu; it is easy to use, but precludes viewers from having access to the Internet per se. Apple TV and Yahoo Connected TV follows this approach (sometimes called a “walled garden”), at least initially. The open browser-based approach incorporates not only apps, but also a Web browser, which gives viewers full Internet access; this makes the interface somewhat more complicated. Google TV uses this model.

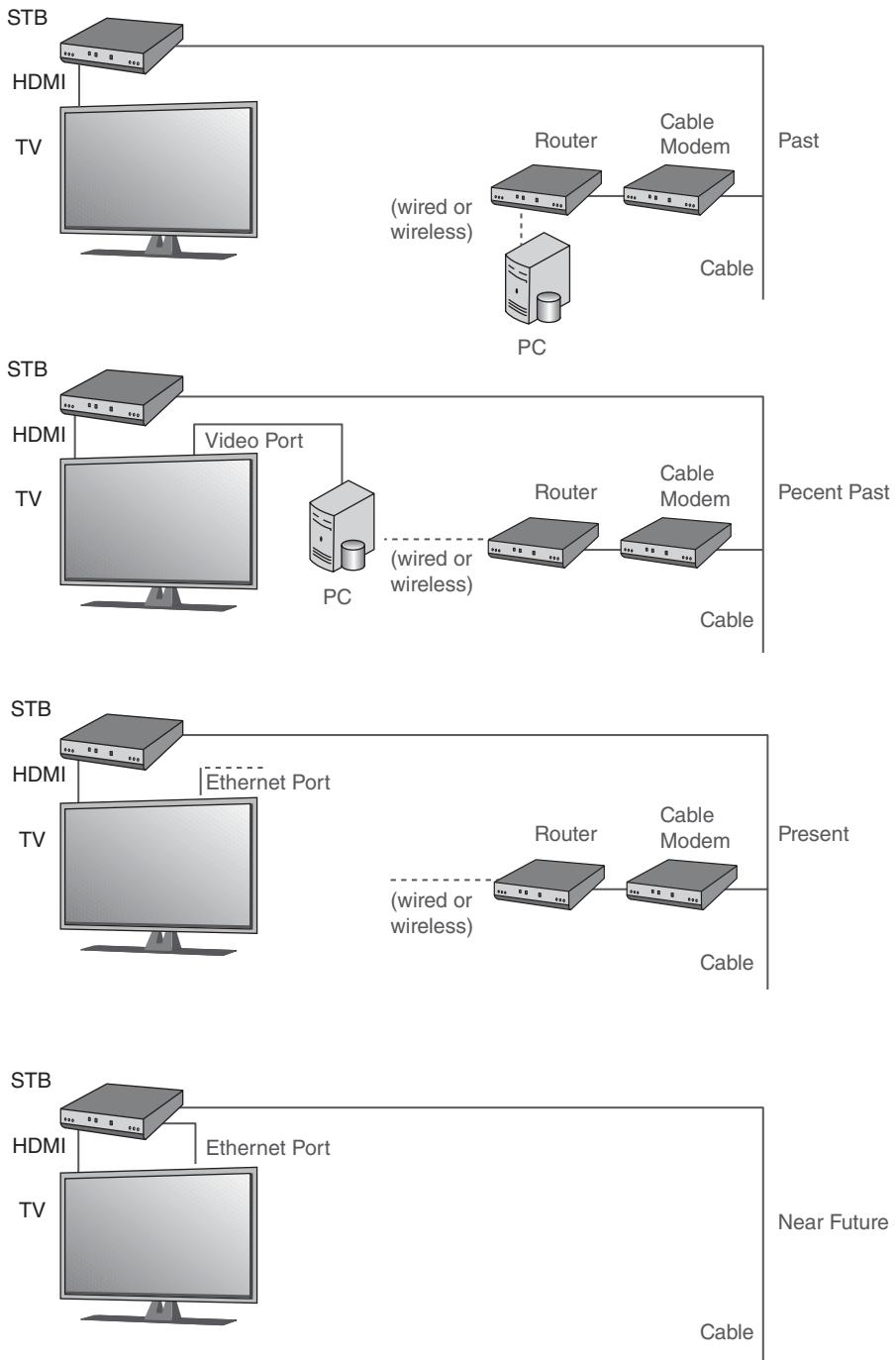


FIGURE 8.1 Evolution of TV sets to a Smart TV environment.



FIGURE 8.2 Example of Smart TV (LG).

8.3 NTTV CONTENT SOURCES

Also as we noted in Chapter 1, there is now a multitude of content sources including local over-the-air stations, Cable TVs operators, satellite providers with Direct to Home (DTH) systems, IPTV operators, and Internet streaming services. The website wwiTv.com listed (and linked to) over 2250 TV streaming sites at press time (see Figure 8.3 and Table 8.1). The content is now available online includes both the stored form (e.g., YouTube, Reuters, CNN, Hulu, and Netflix), as well as real-time material (e.g., MSNBC, CNN International, France 24, and BBC World News). It should be noted, however, that in some instances, streaming video uploads still leave something to be desired (see Figure 8.4 for an anecdote) in terms of waiting for the server to either accept a connection or push out the content (especially when many users want to get simultaneous access to a given site), and/or in terms of network performance.

What follows provides a partial survey of *Internet television* and *Web television* providers. This survey is a small sample of Internet-based content distribution/management/access providers that are illustrative of some of the trends in next-generation TV. Internet TV is television service distributed via the Internet, as exemplified by services such as Hulu (for U.S. content, but also other content) and BBC iPlayer (for U.K. content, but also other content). *Web television* provides content that is created specifically for first-viewing on the Internet (via broadband access and/or on mobile networks). Figure 8.5 identifies some of the key providers, some of which are discussed in more details below.



WWITV: World Wide Internet TV

Your Portal to watch live and on demand online TV broadcasts.

This site is designed to enable users of personal computers and other consumer electronic devices to easily find and access streaming media content over the Internet.

4093	Users online
381	<u>Emmanuel TV</u> (9.31%)
374	<u>Movies</u> (9.14%)
147	<u>Kontra Channel</u> (3.59%)
138	<u>MSNBC</u> (3.37%)
122	<u>Hellenic TV 2</u> (2.98%)
74	<u>Mega TV</u> (1.81%)
58	<u>Skai</u> (1.42%)
57	<u>CNN International</u> (1.39%)
54	<u>France 24 (French)</u> (1.32%)
54	<u>Al Jazeera (english)</u> (1.32%)
53	<u>BBC World News</u> (1.29%)
50	<u>RTR Planeta</u> (1.22%)
43	<u>Extra channel 3</u> (1.05%)
41	<u>Sky News</u> (1%)
38	<u>CNBC Stream 2</u> (0.93%)
37	<u>Saudi 1 - KSA1</u> (0.9%)
36	<u>Saudi 2 - KSA2</u> (0.88%)
35	<u>Al Jazeera (Arabic)</u> (0.86%)

2251 online TV stations listed.

Updated: 7-11-2011 14:32:25 GMT+1

FIGURE 8.3 WWITV portal.

TABLE 8.1 Example of Online TV Services from German Sources Listed at the WWiTv Portal

Streaming Channel	Data rate (bps)	Description
3Sat	1591K	General TV channel
Alex Berlin	331K	Community access TV
ARD Tagesschau	325K	The most popular German news program on-demand
ARD Tagesschau	On site	Recorded news
Bayerischer Rundfunk	On site	Regional TV from München
BR Alpha	On site	Educational programs from the Bayerischen Rundfunk from München
Buergerschaft HH	On site	Hamburger Parliament (sometimes online)
Campus TV	330K	TV from the Technischen Fachhochschule Wildau
Center TV Duesseldorf	528K	Local TV from Düsseldorf
Center TV Ruhrgebiet	300K	Regional TV
CP TV	200K	IT channel
DAF TV	300K	Financial news
Deluxe Music	on site	Music television for adults. 24-hour music pur. 1980s, 1990s, smooth jazz, soul, and more
Der Schmuckkanal	On site	Offers jewelry
DGF TV	On site	Health TV
DHD 24 TV	400K	Interactive TV channel
DW TV Arabia	366K	Every hour, on the hour—the JOURNAL with the latest news, European markets data, the In-Depth segment and the weather report
DW TV ASIA+	366K	Every hour, on the hour—the JOURNAL with the latest news, European markets data, the In-Depth segment and the weather report.
DW TV Europe	366K	Every hour, on the hour—the JOURNAL with the latest news, European markets data, the In-Depth segment and the weather report
Elbekanal	On site	Regional TV from Schönebeck
Elsterwelle	On site	Local TV from Lausitz
Family TV	200K	General Internet TV channel
FashionGuide TV	500K	Fashion channel
Flott TV	330K	Local TV from Guenzburg
Franken Fernsehen	On site	Located in Nürnberg
Global Tunes	200K	View from inside the studio
Hamburg 1	On site	Recorded news

(Continued)

TABLE 8.1 (*Continued*)

Streaming Channel	Data rate (bps)	Description
Hamm TV	On site	Local TV from Hamm
Hope channel Deutsch	273K	Christian television network
Hope TV Europe	264K	Christian television network
HR Fernsehen	On site	Regional TV from Hessen
HSE 24 Digital	On site	Offers a broad range of products
IT news	500K	News for IT specialists
JATV	On site	Archived clips, reports, and comedy
Jena TV	On site	Local TV from Jena
Juwelo	448K	Shopping TV
Kanal 1	391K	Regional TV channel from Stollberg
KSTA	On site	Local TV from Koeln
Kultur MD	On site	Regional TV channel from Magdeburg
KWTV	232K	Regional TV from Wildau/Königs Wusterhausen
Landtag BW	On site	The State Parliament of Baden- Wuerttemberg (not always online)
Lausitz TV	On site	Local TV from Lausitz
LTV	On site	Regional TV from Ludwigsburg
Massive Mag	500K	Action, Sport and Lifestyle TV
MDR	On site	Regional TV from Leipzig
Medizin TV (Schmerz)	491K	Health TV
Merkurtz TV	On site	Local TV from München
n tv	On site	News TV
N24	On site	News TV with recorded streams
NDR (Hamburg)	500K	Regional TV
NDR (Mecklenbug Vorpommern)	500K	Regional TV
NOA4	700K	Norderstedt on Air 4. Local TV channel
NRW TV	On site	TV from Dortmund for Nordrhein- Westfalen
Oberlausitz TV	On site	Local TV from Oberlausitz (Ostsachsen)
Oeins	400K	Local TV from Oldenburg
Offener Kanal Magdeburg	200K	Community access TV
Offener Kanal Mainz	2091K	Community access TV
Offener Kanal Trier	350K	Community access TV
Phoenix	1591K	News from Bonn, documentaries, and debates. Transmission sometimes interrupted
Primetime TV	291K	
QVC	On site	(Home Shopping) Offers a broad range of products

TABLE 8.1 (*Continued*)

Streaming Channel	Data rate (bps)	Description
RAN1	On site	Regional TV from Anhalt
RBB	On site	Regional TV from Berlin Brandenburg
RFH	On site	Local TV from Halberstadt
Rhein Sieg TV	On site	Regional TV from Siegburg
Rheinmain TV	314K	Local TV from Bad Homburg
RTL Hessen	on site	Local TV from Hessen
RTL Muenchen TV	300K	Regional TV from München
Sonneberger TV	On site	Regional TV from Sonneberg
Sonnenklartv	On site	Travel shopping TV
Spiegel TV	On site	A lot of archived news, reports and previews
Sporttime TV	On site	Sport TV channel with on-demand news
SR Online	On site	Regional TV from Saarbrücken
Streetclip TV	1100K	Music and culture channel
SWR Mediathek	On site	Public broadcaster with recorded programs
TRP 1	300K	Regional television from Niederbayern (Passau)
TV Aktuell	500K	Regional television from Regensburg
TV Berlin	On site	Local TV from Berlin
TV Coburg	On site	Local TV from Coburg
TV Emscher Lippe	On site	Regional TV from Herten
TV Halle	900K	Local TV from Halle
TV Kiel	300K	Community access TV
TV Mittelrhein	On site	Regional TV aus Koblenz
TV Suedbaden	400K	Regional Television from Freiburg
VRF Vogtland	199K	Regional TV from Vogtland
WDR	On site	The main news programs of the Westdeutscher Rundfunk are shown live
Wetter	400K	Recorded and live weather forecast
WM TV	On site	Regional TV for Münsterland/Münster
WMZ TV	141K	Regional TV for Senftenberg, Lauchhammer and Frankfurt (Oder)
Worm TV	173K	Electronic music
WWTV	On site	Local TV from Wied
ZDF Heute 100sec	On site	Recorded news and special reports
ZDF Mediathek	On site	Recorded sports items available on website
ZDF Mediathek Live	On site	Sports items available on website



FIGURE 8.4 Loading . . . Still waiting for server and/or network performance to hit critical performance.

8.3.1 Hulu

The Hulu website (see Figure 8.6) is popular site for users seeking network television programming on the web. The site is a joint venture of NBC, FOX, and ABC and provides professionally developed content from these networks. Hulu also makes available some programming that originates on the web. The sites displays some advertising content, but in a limited fashion at this time. The creation of Hulu is seen as an antipiracy strategy: TV studios have come to realize that it may be better have viewers get the content directly from the studios with a low level of advertising than from BitTorrent and RapidShare pirates with no advertising at all.

8.3.2 Apple

Apple's iTunes (see Figure 8.7) is the largest online distribution platform for professional quality videos. The consumer can rent HD movies; buy HD movies or shows, and get iTunes Extras. Apple TV uses a set-top box connected to the Internet; in turn, the set-top box is connected to the TV over an HDMI cable, and one can use the service as if it were just a Cable TV setup. The content can also be watched on the iPhone or iPod. However, the cost per view is not trivial at \$2.99 per episode (in HD) at press time; a monthly plan for an all-access pass is reportedly under consideration.

8.3.3 Boxee

The Boxee website (see Figure 8.8) provides software for Windows, Mac, and Linux HTPCs (also for the Apple TV Set-top Box). Microsoft Windows (XP,



FIGURE 8.5 Major content providers at press time (partial list).



FIGURE 8.6 Hulu.



FIGURE 8.7 Apple iTunes.



FIGURE 8.8 Boxee.

Vista, 7), Mac OS X, Apple TV, Ubuntu 32-bit, and 64-bit Linux platforms are supported. After loading the software, the user can connect the PC to TV set using an S-Video cable (most PCs and digital televisions are equipped with an S-Video port), or VGA 15-pin cable, a DVI cable, a DVI-to-HDMI cable, or other arrangements. The software provides an interface for watching content created by others (Boxee does not produce video content, and it does not distribute content on the web). Using Boxee's media center, one can browse Internet-based videos. Viewing can be achieved several feet away from the screen; the software also supports a remote control device. Boxee also offers social networking features where the viewer can rate the content and recommend content to others.

8.3.4 Clicker

Clicker is a web-focused TV guide (see Figure 8.9). It indexes 400,000 episodes from 7000 TV shows, with the number of episodes and shows increasing over time. Clicker lists professionally produced content from channels, such as Hulu, Netflix, and Amazon, and other sources. The database is organized by network, genre, and other tags. Clicker also provides tools for browsing shows.

8.3.5 Revision3 Internet Television

The Revision3 network (see Figure 8.10) produces, distributes, and markets shows for niche audiences. The website creates and produces all-original



FIGURE 8.9 Clicker.



FIGURE 8.10 Revision3 Internet television.

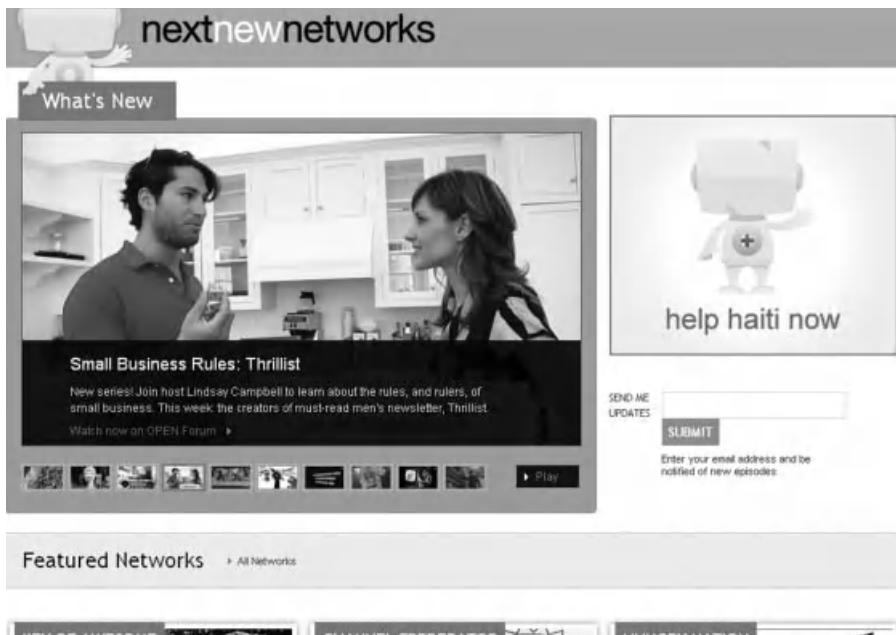


FIGURE 8.11 Next new networks.

episodic community-driven programs. The business model is to produce shows for niche audiences that mainstream television does not serve.

8.3.6 Next New Networks

Next New Networks (see Figure 8.11) operates a number of websites that each push out videos on specific themes. These sites generate regularly scheduled programming. The firm is an independent producer of online television networks. Next New Networks creates, packages, brands, markets, and syndicates some of the Web's most popular regularly scheduled and episodic programming. Since its inception in March 2007, the company has launched 16 networks, and its programming has been viewed more than 400 million times. The sites employ a superdistribution strategy—that is, they send their content to as many outlets as possible, including BitTorrent, YouTube, iTunes, and others. They maintain relationships with the leading destinations for online content.

8.3.7 UltraViolet

UltraViolet (<http://www.uvvu.com>) (see Figure 8.12) is a free, online personal library that gives the user flexibility with how and where he/she watch the



FIGURE 8.12 UltraViolet.

movies and TV shows that one purchases. Once a movie or TV show has been added to the user's UltraViolet Library, the user will have options to stream it over the Internet, download it for offline viewing, or play it back on a disc. Because UltraViolet offers so many viewing choices, the user has the freedom to choose where he/she want to watch—whether it is on a mobile device, computer, television, game console, and so on. Every time the user buys an UltraViolet-enabled movie or TV show, the user can add a digital “proof of purchase” to the user's UltraViolet Digital Library. By doing this, UltraViolet Retailers, Streaming Services, and UltraViolet-capable devices and apps can confirm the rights to the movie or TV show and enable the user to watch.

8.3.8 Netflix

Netflix allows subscribers to watch unlimited movies and TV episodes streaming over the Internet to the user's TV via an Xbox 360, PS3, Wii, or any other device that streams from Netflix, including PCs, Macs, and laptops for a fee of \$7.99 a month. Netflix (Figure 8.13) had over 24 million subscribers in the United States and Canada at press time for its online streaming service; its ability to stream Disney, Sony, and Starz movies aided its growth in recent years. Starz Play service choices are incremental to the continually growing Netflix library available to watch instantly. Starz Play includes approximately 1000 movies, Original Series, and other entertainment. These choices include new releases from major Hollywood studios, such as Walt Disney Pictures, Sony Pictures Entertainment, Overture Films, Revolution Studios, Miramax Films, Touchstone Pictures, Hollywood Pictures, Pixar, TriStar, Screen Gems, Sony Classics, and Warren Miller Films. Select first-run theatrical films from



FIGURE 8.13 Netflix.

The Weinstein Company, IFC, and Yari Film Group are also available. Starz Play also supplies access to a streaming version of the live Starz TV channel on all unlimited plans at no additional cost.

REFERENCES

- [FUT201101] Staff, "How connected televison transforms the business of TV—A white paper based on the Futurescape strategy report social TV," Futurescape Ltd., 2011, <http://www.futurescape.tv>.
- [HAR201001] N. Hartvig, "Changing channels: Who will switch on to mobile TV?" CNN, February 25, 2010.

GLOSSARY

(*,*,RP) route entry In PIM-SM, $(*,*,\text{RP})$ refers to any source and any multicast group that maps to the RP included in the entry. The routers along the shortest path branches between a domain's RP(s) and its PIM Multicast Border Router (PMBR) maintain $(*,*,\text{RP})$ state and use this state to determine how to deliver packets toward the PMBRs should data packets arrive, but there is not a longer match [EST199801].

(*,G) route entry In PIM-SM, group members join the shared RP-Tree for a particular group. This tree is represented by $(*,\text{G})$ multicast route entries along the shortest path branches between the RP and the group members [EST199801]. The $*$ wildcard means “all sources”.

(S,G) Pair Source S and destination group G associated with an IP packet.

(S,G) route entry In PIM-SM, (S,G) is a source-specific route entry. It may be created in response to data packets, Join/Prune messages, or Asserts. The (S,G) state in routers creates a source-rooted, shortest path (or reverse shortest path) distribution tree. $(\text{S},\text{G})\text{RPT}$ bit entries are source-specific entries on the shared RP-Tree; these entries are used to prune particular sources off of the shared tree [EST199801].

1080p video format A high definition video format with a resolution of 1920×1080 pixels. The “p” stands for progressive scan, which means that each video frame is transmitted as a whole in a single sweep. 1080p TVs display video at 60 frames per second. The video on most high-definition discs (Blu-Ray and HD DVD) is encoded at the film’s native rate of 24 frames per second, or *1080p24*. For compatibility with most current 1080p TVs, high-definition players internally convert the 1080p24 video to 1080p60. Newer TVs have the ability to accept a 1080p24 signal directly [KIN200901].

120 Hz refresh rate The digital display technologies (LCD, plasma, DLP, LCoS, etc.) that have replaced picture tubes are progressive scan by nature, displaying 60 video frames per second—often referred to as “60 Hz.” HDTVs with 120 Hz refresh rate employ video processing to double the standard rate to 120 frames per second by inserting either additional video frames or black frames. Note: 240 Hz refresh rate reduces LCD motion blur

even more; systems operating at 240 Hz creates and inserts three new video frames for every original frame [KIN200901].

2D Two dimensional. An image or object with only two dimensions, such as width and height, but no depth.

2D+Delta A single image along with data that represents the difference between that image view and a second eye image view along with other additional metadata. The delta data could be spatial temporal stereo disparity, temporal predictive or bidirectional motion compensation. Used in 3DTV.

3D (three dimensions) Having or appearing to have width, height, and depth (three-dimensional). Accepts and/or produces uncompressed video signals that convey 3D.

3D DVD A DVD movie recorded in 3D.

3D ready Contains 3D decoder/transcoder and may accept and/or produce uncompressed video signals that convey 3D.

6over4 An IPv6 transition technology that provides IPv6 unicast and multicast connectivity through an IPv4 infrastructure with multicast support using the IPv4 network as a logical multicast link.

6over4link-local address An IPv6 address of the form—FE80:WWXX:YYZZ—where WWXX:YYZZ is the hexadecimal representation of w.x.y.z, a public or private IPv4 address assigned to the 6over4 device interface.

6over4 unicast address An IPv6 address of the form—64-bit prefix:0:0:WWXX:YYZZ—where WWXX:YYZZ is the hexadecimal representation of w.x.y.z, a public or private IPv4 address assigned to the 6over4 device interface.

6to4 An IPv6 transition technology that provides unicast connectivity between IPv6 networks and devices through an IPv4 infrastructure. 6to4 uses a public IPv4 address to build a global IPv6 prefix.

6to4 address A global IPv6 address of the form—2002:WWXX:YYZZ:SLA_ID:interface ID—where WWXX:YYZZ is the hexadecimal representation of w.x.y.z, a public IPv4 address assigned to a 6to4 router's IPv4 interface, and SLA_ID is the Site-Level Aggregation Identifier (SLA ID). The address space 2002::/16 is assigned to 6to4 addresses.

6to4 host An IPv6 device that is configured with at least one 6to4 address (a global address with a 2002::/16 prefix). 6to4 devices do not require manual configuration, and they create 6to4 addresses by means of standard auto-configuration mechanisms.

6to4 relay router An IPv6/IPv4 router that forwards traffic between 6to4 routers and IPv6 Internet devices.

6to4 router A router that participates in the 6to4 transition technology, providing unicast connectivity between IPv6 networks and devices through an IPv4 infrastructure.

A la carte VoD VoD where one pays for each item viewed (similar to Pay Per View). Typically the subscriber has one day to view the content [NOR200601].

Access control The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

Accessibility The property of being accessible and useable upon demand by an authorized entity.

Accessibility feature An additional content component that is intended to assist people hindered in their ability to perceive an aspect of the main content. Examples: captions for the hard of hearing, subtitles in various languages, sign language interpretation video, and descriptive audio [ITU200801].

Acquisition The activity related to obtaining content by the end user.

Ad overlays A small, semitransparent overlay across the screen (usually on the bottom, but can be anywhere) of an online video, similar to what one often sees during TV shows. These ads usually show up 15 seconds into the videos they are on, and last for 10 seconds [REE201001].

Adaptation field An optional variable-length extension field of the fixed-length Transport Stream (TS) Packet header, intended to convey clock references and timing and synchronization information, as well as stuffing over an MPEG-2 multiplex [CLA200301].

Address Network layer identifier assigned to an interface or set of interfaces that can be used as source or destination field in IP datagrams. An IP layer identifier for an interface or a set of interfaces.

The IPv6 128-bit address is divided along 16-bit boundaries. Each 16-bit block is then converted to a 4-digit hexadecimal number, separated by colons. The resulting representation is called colon hexadecimal. This is in contrast to the 32-bit IPv4 address represented in dotted-decimal format, divided along 8-bit boundaries, and then converted to its decimal equivalent, separated by periods [MSD200401].

The following example shows a 128-bit IPv6 address in binary form:

The following example shows this same address divided along 16-bit boundaries:

0010000111011010 0000000011010011 0000000000000000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010

The following example shows each 16-bit block in the address converted to hexadecimal and delimited with colons.

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

IPv6 representation can be further simplified by removing the leading zeros within each 16-bit block. However, each block must have at least a single digit. The following example shows the address without the leading zeros:

21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

Address autoconfiguration The automatic configuration process for IPv6 addresses on an interface; specifically, the process for configuring IP addresses for interfaces in the absence of a stateful address configuration server, such as Dynamic Host Configuration Protocol Version 6 (DHCPv6).

Address maximum valid time Time period during which a unicast address, obtained by means of stateless autoconfiguration mechanism, is valid.

Address resolution Procedure used by a node for determining the link layer address of other nodes on a link. In an IPv6 context, the process by which a node resolves a neighboring node's IPv6 address to its link-layer address. In IPv4, the procedure is accomplished via the ARP protocol. In IPv6, the procedure is accomplished via Neighbor Advertisement and Neighbor Solicitation ICMPv6 messages.

Advanced encryption standard (AES) Cryptographic algorithm; NIST-approved standard. It was chosen by NIST because it is considered to be both faster and smaller than its competitors [CON200701].

Advanced streaming format (ASF) A file format for files used to stores audio and video information; ASF is specially-designed/optimized for use over IP networks such as the Internet.

Advanced Television Systems Committee (ATSC) A set of framework and associated standards for the transmission of video, audio, and data, using the ISO MPEG-2 standard [CLA200301].

AFC Adaptation Field Control.

Aggregatable global unicast address Also known as global addresses, these addresses are identified by means of the 3-bit format prefix 001 (2000::/3). IPv6 global addresses are equivalent to IPv4 public addresses, and they are routable in the IPv6 Internet.

Anycast address A unicast address that is assigned to several interfaces and is used for the delivery of IP datagrams to one of the several interfaces. With an appropriate route, datagrams addressed to an anycast address will be delivered to a single interface—the nearest one.

Apple TV A digital media receiver developed and sold by Apple; in 2010, the company announced a second-generation version of the Apple TV that can stream rented content from iTunes and video from computers or iOS devices.

Array Two or more hard disks that read and write the same data. In a Redundant Array of Inexpensive Disks (RAID) storage system, the operating system treats the array as if it were a single hard disk.

Aspect ratio The ratio of width to height for an image or screen. The North American NTSC television standard uses the squarish 4:3 (1.33:1) ratio. HDTVs use the wider 16:9 ratio (1.78:1) to better display widescreen material like high definition broadcasts and DVDs [KIN200901].

Asymmetric encryption algorithm Same as public key algorithm.

Asymmetric encryption Type of encryption in which encryption keys are different from decryption keys, and one key is computationally difficult to determine from the other. Uses an asymmetric algorithm [CON200701].

Asynchronous video delivery The delivery of a video file that has been previously recorded and stored. Nonlive video transmission.

Attempt address Unicast address where uniqueness is no longer checked.

Audio description This service provides a commentary describing the visual events pertinent to the content and augments the dialog in the content.

Audio Video Interleave (AVI) The most common format for audio/video data on the PC; developed by Microsoft AVI a special case of the RIFF (Resource Interchange File Format).

Authentication The process of proving the genuineness of an entity (such as a smart card) by means of a cryptographic procedure. Authentication entails using a fixed procedure to determine whether someone is actually the person he or she claims to be [CON200701].

Authentication, authorization, and accounting (AAA) Authentication refers to the confirmation that a user who is requesting services is a valid user of the network services requested. Authorization refers to the granting of specific types of service (including “no service”) to a user, based on their authentication, what services they are requesting, and the current system state. Accounting refers to the tracking of the consumption of network resources by users. This information may be used for management, planning, billing, or other purposes [CIS200702].

Authorization An authorization provides access (or legal power) to some protected service. In a Conditional Access (CA) system, the authorization gives access to encrypted services (channels, movies, etc.) [CON200701].

Automatic IPv6 Tunnel Automatic creation of tunnels, generally through the use of various IPv6 address formats that contain the IPv4 tunnel endpoints.

Autonomous system (AS) A network domain that belongs to the same administrative authority.

Autostereoscopic 3D displays that do not require glasses to see the stereoscopic image. Multiview autostereoscopic displays based on parallax barrier or lenticules.

Bandwidth The amount of information that can be sent through a connection. In digital settings it is measured in bits per second. Full-motion full-screen video requires 2.5–12 Mbps depending on compression (e.g., MPEG-2 and MPEG-4) and format (SD or HD).

Bootstrap router (BSR) In PIM-SM, a BSR is a dynamically elected router within a PIM domain. It is responsible for constructing the RP-Set and originating Bootstrap messages [EST199801]. A router with multiple potential RPs; the BSRs provide mechanisms that identify RPs for various multicast groups [ROD200701].

Brand awareness Research studies aimed at associating ad effectiveness to measure the impact of online advertising on key branding metrics.

Broadband video commercial A video ad as a commercial that may appear before, during, and or after a variety of content, including streaming video, animation, gaming, and music video content in a player environment. These commercials are generally :15 and :30 video ads that run before, between, and after a video clip is shown. In 2008, the IAB Digital Video Committee renamed Broadband Video Commercials as “In-Stream Video” ads that are either “Linear” or “Nonlinear” core video products [REE201001].

Broadcast environment Environment where one system communicates to all systems.

Broadcast interface In Core-Based Tree (CBT) multicasting, any interface that supports multicast transmission [BAL199701].

Broadcast TV One-way transmission of TV signals from one point to two or more other points.

Broadcasting satellite service (BSS) A satellite service that (for ITU Region 2 segments covering the majority of the Americas) operates at 17.3–17.8 GHz for the uplink and 12.2–12.7 GHz for the downlink. High power geostationary satellites are utilized.

Buffering The temporary storing data before playing it back. A buffer is a temporary holding area in memory for data; buffers can be on the inputs or outputs side of a data-carrying link.

Bug In this context, an embedded graphic icon or logo used to brand a video program or player; clicking on it will take the user to a website [REE201001].

Bump in the Application (BIA) An IPv6 transition mechanism that performs the IPv4 to IPv6 translation in the end host. The mechanism works at a layer above IP, translating between IPv4 and IPv6 socket API calls [IPV200501].

Bump in the Stack (BIS) An IPv6 transition mechanism that performs the IPv4 to IPv6 translation in the end host. The mechanism works at the IP level. BIS employs the SIIT algorithm.

Bumper ad Refers to a linear video ad with clickable call-to-action; format is usually shorter than full linear ads (e.g., 3–10 seconds) and call-to-action usually can load another video or can bring up a new site while pausing the content [REE201001].

CableCARD A device that consumers can plug into their DCR TV sets that permits for the descrambling of digital programming. The card works in place of a traditional STB [CON200701].

Candidate BSR (CBSR) In PIM-SM, it is a router that can potentially play the role of a BSR, provided it wins an automated BSR election process [ROD200701], [EST199801].

Candidate RP (C-RP) In PIM-SM, a C-RP is a router configured to send periodic C-RP advertisement messages to the BSR, and act as an RP when

it receives Join/Prune or Register messages for the advertised group prefix [EST199801].

Captions Text that appears over a video that labels a scene, identifies a location or person, or narrates dialogue onscreen. Captions can be either open or closed. Open captioning is displayed anytime the video is played; closed captioning is not seen unless it is called up by the receiving equipment (e.g., subtitles that can be turned on for different languages) [REE201001].

Center-based trees Same as Core-based trees.

Certificate A digital certificate consists of three things: (1) The public key portion of the certificate holder's public and private key pair. (2) Information that identifies the holder of the certificate (the owner of the corresponding private key). (3) The digital signature of a trusted entity attesting to the validity of the certificate (i.e., that the key and the certificate information truly go together) [CON200701].

Channel Content formatted as a selectable set of data and transported as part of a data stream.

Channel changing The act of changing from one channel to another.

Channel zapping The act of fast changing from one channel to another.

Cisco Group Management Protocol (CGMP) A Cisco-developed group management protocol that limits the forwarding of IP multicast packets to only those ports associated with IP multicast clients. These clients automatically join and leave groups that receive IP multicast traffic, and the switch dynamically changes its forwarding behavior according to these requests.

Clickable video Online video that is completely interactive. Viewers can move the cursor over the various objects/people/places in the video and click them to obtain additional information, or interact in some other way, for example, making purchase transactions [REE201001].

Click-through The action of following a hyperlink within an advertisement or editorial website or another page or frame within the website content to another.

Cloud computing The latest term to describe a grid/utility computing service. Such service is provided in the network. From the perspective of the user, the service is virtualized. In turn, the service provider will most likely use virtualization technologies (virtualized computing, virtualized storage, etc.) to provide the service to the user.

Codec (COmpressor/ DECompressor)—The system (hardware, software, or combination of both) used to compress/decompress an audio and/or video file for storage or transmission. Codecs convert data between uncompressed and compressed formats, thereby reducing the bandwidth a clip consumes.

Colon Hexadecimal Notation The notation used to represent IPv6 addresses. The 128-bit address is divided in eight blocks of 16 bits. Each block is rep-

resented as a hexadecimal number and is separated from the next block by means of a colon (:). Inside each block, left zeros placed are removed. An example of an IPv6 unicast address represented in hexadecimal notation is 3FFE:FFFF:2A1D:48C:2AA:3CFF:FE21:81F9.

Companion ad Both Linear and Nonlinear Video ad products have the option of pairing their core video ad product with what is commonly referred to as companion ads. Commonly text, display ads, rich media, or skins that wrap around the video experience, can run alongside either or both the video or ad content. The primary purpose of the Companion Ad product is to offer sustained visibility of the sponsor throughout the video content experience. Companion Ads may offer click-through interactivity and rich media experiences, such as expansion of the ad for further engagement opportunities [REE201001].

Compatibility addresses IPv6 addresses used when IPv6 traffic is sent through an IPv4 infrastructure. Some examples are: IPv4 compatible addresses, 6to4 addresses, and ISATAP addresses.

Compressed video signal A stream of compacted data representing an uncompressed video signal. A compressed video signal is an encoded version of an uncompressed video signal. A compressed video signal must be decoded to an uncompressed video signal in order to be edited or displayed. Compressed video formats vary according to the encoding methods used. A compressed video signal format may be converted to another using a “transcoder.”

Compressing zeros Some IPv6 addresses expressed in colon hexadecimal contain long sequences of zeros. A contiguous sequence of 16-bit blocks set to 0 in the colon-hexadecimal format can be compressed to :: (known as double colon). The following shows examples of compressing zeros [MSD200401]:

The link-local address of FE80:0:0:0:2AA:FF:FE9A:4CA2 can be compressed to FE80::2AA:FF:FE9A:4CA2.

The multicast address of FF02:0:0:0:0:0:2 can be compressed to FF02::2.

Zero compression can only be used to compress a single contiguous series of 16-bit blocks expressed in colon-hexadecimal notation.

Conditional access (CA) Encryption mechanisms (especially rotating keys) used in IPTV or Cable TV to support Digital Rights Management, that is, protect content from being accessed by individuals that have not paid for it. A component of a Service and Content Protection system, the purpose of which is to prevent unauthorized (unentitled) access to a service or to content [ITU200801], [CLA200301].

Conditional Access Table (CAT) MPEG Signaling Table that defines type of scrambling used and Program ID (PID) values of transport streams that contain the conditional access management and entitlement information (EMM). The CAT is sent with the well-known PID value of 0x001 [FAI200101].

Conditional-access system (CAS) In a DVB context, Conditional Access (CA) is a security technology used to control the access to broadcast content (including video and audio, interactive services, etc.) through the transmission of encrypted signals and the programmable regulation of their decryption by a system such as smart cards [CON200701]. A component of a Service and Content Protection system, the purpose of which is to prevent unauthorized (unentitled) access to a service or to content [ITU200801].

Confidentiality The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Connected TV (CTV) An Internet-ready TV set that has direct broadband access to the Internet.

Consumer video hosting Online video hosting and sharing sites (typically usable free of charge) that allow their users to upload videos for viewing by private and public audiences.

Content Delivery Network (CDN) A network that contains and is optimized to deliver content. Content cashing (possibly at multiple locations) and streaming mechanisms are typically supported. Network-supported priorities are also typically included in order to optimally distribute various type of traffic with stated QoS goals. A CDN replicates content from the origin server to cache servers (also called replica servers), spread across the globe. Content requests are directed to the cache server closest to the user, and that server delivers the requested content [SJO200801].

Content Delivery Networks Content providers that deliver video streaming to users worldwide.

Content On Demand (CoD) A generic term for on-demand television (VoD); services other than video may also be included.

Content protection Ensuring that an end user can only use the content they have already acquired in accordance with the rights that they have been granted by the rights holder [ITU200801].

Content provider An entity that acts as the agent for or is the prime distributor of the content.

Content tracing A process to enable the identification of the (arbitrary) origin of content, and/or the responsible party (e.g., the end user), to facilitate subsequent investigation in the event of unauthorized content copying or distribution [ITU200801].

Contextual ads Existing contextual ad engines deliver text and image ads to non-video content pages. Ads are matched to keywords extracted from content. Advertisers can leverage existing keyword-based paid search campaigns and gain access to a larger audience. Third-party publishers receive a share of the revenue collected from the advertisers [REE201001].

Control Word (CW) (aka Code Word) The key used to encrypt the payload in a transport stream.

Converged services The integration of Internet, multimedia, e-mail, presence, instant messaging, m-commerce, and so on, services with voice service.

Core router (or just “core”) In core-based tree (CBT) multicasting, a “core router” is a router that acts as a “meeting point” between a sender and group receivers. The term “rendezvous point (RP)” is used equivalently in some contexts. A core router need not be configured to know it is a core router [BAL199701].

Core-based tree (aka center-based trees) A bidirectional shared tree where the routing state is “bidirectional,” namely, packets can flow both down the tree away from the core and up the tree towards the core, depending on the location of the source in the network, and the tree is “shared” by all sources to the group. Core-based forwarding trees have a single node, for example, a router, known as the core of the tree, from which branches emanate. These branches are made up of other routers, so-called noncore routers, which form the shortest path between a member-host’s directly attached router and the core. A router at the end of a branch is known as a leaf router on the tree. The core need not be topologically centered between the nodes on the tree, since multicasts vary in nature, and, correspondingly, so can the form of a core-based tree [BAL199301].

Core-based tree (CBT) multicasting A multicast routing architecture that builds a single delivery tree per group that is shared by all of the group’s senders and receivers. Most multicast algorithms build one multicast tree per sender (subnetwork), the tree being rooted at the sender’s subnetwork. The primary advantage of the shared tree approach is that it typically offers more favorable scaling characteristics than all other multicast algorithms. The CBT protocol is a network layer multicast routing protocol that builds and maintains a shared delivery tree for a multicast group. The sending and receiving of multicast data by hosts on a subnetwork conforms to the traditional IP multicast service model [BAL199702].

Correspondent node Refers to a node that is communicating with a node that is using Mobile IP.

Cost Per Action (CPA) (also known as Cost Per Interaction) A pricing model that allows marketers to be charged by their publishers only when an agreed upon action is taken by their potential customer, such as a sale or registration.

Cost Per Click (CPC) An advertiser’s estimation of how much it costs for each click on a given advertisement. Number is obtained by dividing the cost of an ad or marketing endeavor by the number of clicks on that ad or endeavor generated.

Cost Per Thousand Impressions (CPM) A pricing model for online advertising based on impressions or views where the advertiser pays the publisher a predetermined rate for every 1000 impressions.

Cue point User-defined points in the playback of a video when an event is designated to occur. In online video one can use cue points to trigger custom, synchronized functionality, such as animations, synchronized ad units, or closed captions [REE201001].

Data Encryption Standard (DES) A 64-bit block cipher, symmetric algorithm also known as Data Encryption Algorithm (DEA) by ANSI and DEA-1 by ISO. Widely used for over two decades, adopted in 1976 as FIPS 46 [CON200701].

Data Origin Authentication The corroboration that the source of data received is as claimed.

Datagram Another name for an IP-level packet.

Decoding The decompression of an encoded file for playback or use.

Decoding Time Stamp (DTS) Time stamps are inserted close to the material to which they refer (normally in the PES packet header). They indicate the exact moment where a video frame or an audio frame has to be decoded or presented to the user respectively. These rely on reference time stamps for operation [FAI200101].

Default route The route with a ::/0 prefix. The default route is the route used to obtain the next destination address when there are no other matching routes.

Default routers list A list of routers that can be used as a default router. The list is populated based on Router Advertisement messages received that have a non-null router lifetime.

Delivery Network Gateway Functions (DNGF) Set of functions that mediate between the network and service provider domains and the IPTV Terminal Function (ITF). A device implementing the DNGF is commonly referred to as the Residential Gateway (RG) or Delivery Network Gateway (DNG) [ITU200801].

Denial of Service (DoS) The prevention of authorized access to resources or the delaying of time-critical operations.

Dense Mode (DM) protocols Multicast routing protocols designed on the assumption that the majority of routers in the network will need to distribute multicast traffic for each multicast group. DM protocols build distribution trees by initially flooding the entire network and then pruning out the (presumably small number of) paths without active receivers. The DM protocols are used in Local Area Network environments, where bandwidth considerations are less important, but can also be used in Wide Area Networks in special cases (e.g., where the backbone is a one-hop broadcast medium, such as a satellite beam with wide geographic illumination, e.g., in some IPTV applications.)

Designated Router (DR) In PIM-SM, the router on a subnet that is selected to control multicast routes for the members on its directly attached subnet. When more than one PIM-capable router is located on a subnet, the selected DR is the router with the highest IP address [ROD200701]. The DR sets up multicast route entries and sends corresponding Join/Prune and Register messages on behalf of directly connected receivers and sources, respectively. The DR may or may not be the same router as the IGMP Querier. The DR

may or may not be the long-term, last-hop router for the group; a router on the LAN that has a lower metric route to the data source, or to the group's RP, may take over the role of sending Join/Prune messages [EST199801].

Destination cache Table supported by each IPv6 node that maps each destination address (or address range) to the next hop address to which the datagram has to be sent. It also stores the associated path MTU.

Destinations for online content; online destination Website that provides TV-related content that become popular. Well-known, branded sites.

Digital Rights Management (DRM) The methodology used to control user access to licensed information. Conditional Access (CA) encryption mechanisms used in IPTV or Cable TV is an example of DRM. A synonym for Service and Content Protection or Content. A system that enables secure distribution of digital content and that prevents unauthorized access to and illegal and perfect copying of same [CON200701].

Digital signature Data appended to or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, for example, by the recipient.

Digital Storage Management Command and Control (DSM-CC) An MPEG extension that allows for the control of MPEG streaming. It supports trick-mode features. A format for transmission of data and control information in an MPEG-2 Private Section, defined by the ISO MPEG-2 standard [FAI200501], [CLA200301].

Digital Subscriber Line (DSL) A phone-company technology that exploits unused frequencies on copper telephone lines to transmit traffic typically at multi-megabit speeds. DSL can allow voice and high-speed data to be sent simultaneously over the same line. Because the service is "always available", end users do not need to dial in or wait for call setup. Asymmetrical variations include: ADSL, G-lite ADSL (or simply G-lite), VDSL (ITU G.993.1) and VDSL2 (ITU G.993.2). The standard forms of ADSL (ITU G.992.3, G.992.5, and ANSI T1.413-Issue 2) are all built upon the same technical foundation, Discrete Multi Tone (DMT). The suite of ADSL standards facilitates interoperability between all standard forms of ADSL [DSL200701].

Digital Subscriber Line Access Multiplexer (DSLAM) Telephone carrier equipment typically residing at the Central Office that terminates multiple DSL lines (usually 96, 192, or 384) and multiplexes the combined output to an ATM, MPLS, or IP uplink. The uplink is typically an OC-3 (155 Mbps) or an OC-12 (622 Mbps).

Digital Television (DTV) (also sometimes known as advanced TV–ATV) Refers to all formats of digital television, including high definition television (HDTV), and standard definition television (SDTV). DTV supports the

transmission, reception and display of digital signals on a digital TV set. The digital signals can be broadcast over the air or transmitted by a cable or satellite system. Traditional broadcasters choose which formats to broadcast. In the home, the decoder (located inside the TV or in a set-top box) receives the signal and drives the digital TV set.

Digital Video Broadcast-Handheld (DVB-H) Properly a protocol. More broadly, approaches and technologies to deliver commercial-grade medium-quality real-time linear and on-demand video content to handheld, battery-powered devices, such as mobile telephones and PDAs. IP multicast is typically employed.

Digital Video Broadcasting (DVB) (aka ETSI-DVB). A set of framework and associated standards published by the European Telecommunications Standards Institute (ETSI) for the transmission of video, audio, and data, using the ISO MPEG-2 standard [CLA200301]. Organization defined transmission standards for digital broadcasting systems using cable (DVB-C), satellite (DVB-S), terrestrial (DVB-T) and handheld (DVB-H) devices. See <http://www.dvb.org> [CON200701].

Digital Video Recorders (DVRs) Devices (perhaps built into the STB) that provide the ability to “time-shift” television viewing. DVRs use a hard disk to record the content. As such, they can record hundreds of hours of content, and subscribers can directly access any recording without “fast forwarding” through other programs. DVRs are integrated into the IPTV system. From the operator’s electronic program guide (EPG), the subscriber simply scrolls to the content to be recorded and hits a “record” button [NOR200601].

Direct To Home (DTH) A term used to describe the overall system of signal video transmissions from an uplink station to a satellite for distribution to home satellite dishes/receivers. Such satellite/service is also known as Direct Broadcast Satellite (DBS). Generally encompasses the Ku-BSS band and/or Ka-bands, but occasionally also the Ku-FSS band. In the Americas (for ITU Region 2 segments covering the majority of the Americas), the following frequency band allocations are used:

- Ku-BSS: 17.3–17.8 GHz uplink and 12.2 to 12.7 GHz downlink
- Ku-FSS: 14.0–14.5 GHz uplink and 11.7 to 12.2 GHz downlink
- Ka-bands: 27.5 GHz and 31 GHz uplink and 18.3–18.8 GHz and another 500 MHz band at 19.7 to 20.2 GHz downlink.

Display An electronic device that presents information in visual form, that is, produces an electronic image—such as CRTs, LCDs, plasma displays, electroluminescent displays, field emission displays, and so on. Also known as a “sink” that renders an image.

Distance Vector Multicast Routing Protocol (DVMRP) A routing protocol, originally defined in RFC 1075, to support internetwork multicasting. DVMRP combines many of the features of RIP with the Truncated Reverse

Path Broadcasting (TRPB) algorithm. DVMRP is an “interior gateway protocol”; suitable for use within an autonomous system, but not between different autonomous systems. The multicast forwarding algorithm requires the building of trees based on routing information. This tree building needs more state information than RIP was designed to provide, so DVMRP is much more complicated in some places than RIP [WAI198801]. DVMRP is based in the RIP protocol.

Distance Vector Routing Protocol A routing protocol in which a router periodically informs its neighbors of topology changes. This is in contrast to link state routing protocols, which require a router to inform all the nodes in a network of topology changes [IPV200501].

Domain Name System (DNS) A hierarchical storage system and its associated protocol to store and retrieve information about names and IP addresses.

Double colon Notation used in compressing continuous series of 0 blocks in IPv6 addresses. For example, the FF02:0:0:0:0:0:2 multicast address is expressed as FF02::2.

Download-to-own (DTO) A method similar to electronic sell-thru (EST) but where the consumer may permanently own and/or be able to use the content. Some observers suggest that the increasing popularity of VoD *rental services* can be linked to the gradual erosion of support for DTO, or digital retail business. It believes that the majority of services operating in global markets offer titles on a rental basis due to limited availability of download-to-own titles whose fundamental business model offers no compelling case in terms of convenience or service to drive a mass-market adoption [OHA201101]. The delivery mechanism may be the Internet or other networks (e.g., Cable TV network or an IPTV network, or a 4G wireless network.) Note: Some exclude delivery over the Internet in the definition of DTO; we include it.

Downstream interface (or router) In CBT, A “downstream” interface (or router) is one which is on the path away from the group’s core router with respect to this interface (or router) [BAL199701] . All interfaces that are not the upstream interface, including the router itself [ADA200501].

Dual Stack Architecture A node architecture in which two complete protocols stack implementations exist, one for IPv4 and one for IPv6, each with its own implementation of the transport layer (TCP and UDP).

DVB Project A market-led consortium of public and private sector organizations in the television industry. Its aim is to establish the framework for the introduction of MPEG-2 based digital television services. Now comprising over 200 organizations from more than 25 countries around the world, DVB fosters market-led systems, which meet the real needs, and economic circumstances, of the consumer electronics and the broadcast industry [DVB201101].

DVB-C2 A Cable TV transmission standard. “Frame structure channel coding and modulation for a second generation digital transmission system for cable systems (DVB-C2)” was published in April 2011 (DVB EN 302 769 V1.2.1). The original DVB-C specification was developed in 1994 and provides a toolbox of QAM modulation schemes from 16-QAM to 256-QAM for television and radio broadcasting services, as well as for data transmission. At the moment, this standard is deployed worldwide in cable systems, ranging from the larger CATV networks down to smaller SMATV systems. Demand for more and more advanced services, however, is constantly growing, and cable operators are seeking ways to offer products like HDTV and VoD on a commercial scale within a relatively short timeframe, together with the required accompanying interactive services. Hybrid Fibre Coax (HFC) networks are therefore being optimized, providing enhanced performance and thus allowing even higher modulation schemes than DVB-C is offering today. A DVB-TM Study Mission addressing this challenge showed that recent technological developments in the areas of signal processing, channel coding, and modulation well provide the means to significantly increase the transmission capacity of cable networks, and to allow for the broad introduction of advanced digital TV services via cable. The process initiated in DVB to capture a set of Commercial Requirements, and to solicit technical contributions, led to the development of the DVB-C2 specification that will be capable of serving the cable industry for at least the upcoming 10–12 years [DVB201101].

DVB-S2 A satellite transmission standard. “Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications” was published in August 2009 (EN 302 307 V1.2.1). It is an extension of DVB-S “Framing structure, channel coding and modulation for 11/12 GHz satellite services,” originally published in 1997. The DVB-S standard specifies QPSK modulation and concatenated convolutional and Reed–Solomon channel coding, and is now used by most satellite operators worldwide for television and data broadcasting services. DVB-S2 defines a “second-generation” modulation and channel coding system, DVB-S2 is a single, very flexible standard, covering a variety of applications by satellite, as described below. It is characterized by [DVB201101]:

- a flexible input stream adapter, suitable for operation with single and multiple input streams of various formats (packetized or continuous);
- a powerful FEC system based on LDPC (Low-Density Parity Check) codes concatenated with BCH codes, allowing Quasi-Error-Free operation at about 0.7–1 dB from the Shannon limit, depending on the transmission mode (AWGN channel, modulation constrained Shannon limit);
- a wide range of code rates (from 1/4 up to 9/10); 4 constellations, ranging in spectrum efficiency from 2 to 5 bit/s/Hz, optimized for operation over non-linear transponders;

- a set of three spectrum shapes with roll-off factors 0.35, 0.25, and 0.20; and
- Adaptive Coding and Modulation (ACM) functionality, optimizing channel coding and modulation on a frame-by-frame basis.

DVB-T2 A DTT (Digital Terrestrial Television) transmission standard. DVB-T is the most widely deployed system worldwide, with over 60 countries that have adopted or deployed the DVB-T standard and more than 200 million receivers deployed. DVB-T2 offers an increased efficiency of 30–50% in its use of spectrum compared with DVB-T. The DVB Project fully expects DVB-T and DVB-T2 services to coexist side-by-side for some time to come [DVB201101].

Dynamic Host Configuration Protocol (DHCP) A configuration protocol that provides IP addresses and other configuration parameters when connected to an IP network.

Dynamic Host Registration A mechanism that informs the network that a host (receiver) is a member of a particular group (otherwise, the network would have to flood rather than multicast the transmissions for each group). For IP networks, the Internet Group Multicast Protocol (IGMP) serves this purpose.

Effective Cost Per Thousand Impressions (eCPM) A performance measure for various ad units used by a sponsor. The measure calculated by dividing total earnings by total number of impressions in thousands. eCPM = Total Earnings/Impressions.

Electronic Content Guide (ECG) A mechanism similar to the Electronic Program Guide (EPG) but that typically describes the content of local storage, including relevant information, such as title and genre of the program, the duration, and other data.

Electronic Program Guide (EPG) A listing of all available TV programs typically covering a few days (1–2 weeks) that displays on a TV screen. A structured set of data, intended to provide information on available content that may be accessed by end users. The EPG contains information about future programs; it generally includes title and genre of the program, a short description of the episode, the start time, the duration, and other data.

Electronic sell-thru (EST) (also known as Digital retail) A method of media distribution where consumers pay a one-time fee to download a digital media file for storage on a hard drive on a computer or other system. Typically the content may become unusable after a certain period and may not be viewable using competing platforms. EST covers a gamut of digital media products, including TV content, video content, music, gaming, and mobile applications. The delivery mechanism may be the Internet or other networks (e.g., Cable TV network or an IPTV network, or a 4G wireless network). Note: Some exclude delivery over the Internet in the definition of EST; we include it.

Electronic Service Guide (ESG) A capability used to signal the services that are available, how they can be received, and what they contain. Service discovery and purchase of services is based on information transmitted in the ESG. For each service and program, the ESG contains all the necessary information for making a purchase and for the device to find services and programs. Practitioners consider ESG as a more general form of an EPG, namely ESG encompasses more abstract concepts of “Service and Content” beyond just a TV channels.

Elementary Stream (ES) A DVB / MPEG-2, raw bit-stream consisting of digitized video or audio.

Embed In this context, refers to taking video from an online video provider and locating it elsewhere on the Internet (websites, social networking sites, etc.).

Emergency Alert System (EAS) In the United States, the government mandates that operators support the Emergency Alert System. Each operator must listen for any alerts and translate these encoded messages for presenting to viewers. An EAS receiver provides this function [NOR200601].

Encapsulating Security Payload An IPv6 extension header that provides data source authentication, data integrity and confidentiality.

Encapsulator A network device that receives PDUs (Ethernet frames or IP datagrams) and formats these for output as a transport stream of TS Packets [CLA200301].

Encoder A device that converts an audio or video signal to a specific streaming format, for example, MPEG-4 (or MPEG-2). The conversion typically includes compression and generation on an IP packet.

Encoding Converting a file into a compressed format.

Encryption The process of making a message unintelligible for all who do not have the proper key.

Entitlement Access criteria authorizations.

Entitlement Control Messages (ECMs) A Conditional Access message that contains the key for decrypting transmitted programs. It is transmitted with the Entitlement Management Message. Private conditional access information that specifies authorization levels or the services of specific decoders. Encrypted message that contains access criteria and control words (CWs). The ECM is decrypted and checked against the access criteria in order to provide authorization. If authorization is granted, the CW will be released [CON200701].

Entitlement Management Messages (EMMs) A satellite Conditional Access specifies customer entitlements. Entitlements are transmitted with the Entitlement Control Message. Encrypted messages are sent to the smart card or STB to authorize it for certain access criteria. The EMM contains the actual authorization data (i.e., entitlements) [CON200701].

Ethernet over an MPLS (EoMPLS) Transport of native Ethernet over an MPLS Pseudowire.

EUI-64 address 64-bit link layer address that is used as the basis to generate interface identifiers in IPv6.

European Telecommunications Standards Institute (ETSI) An independent, nonprofit organization whose mission is to produce telecommunications standards for today and for the future.

Event trackers Mechanisms used for tracking click-throughs, companion banner interactions, and video session duration.

Excess Information Rate (EIR) The maximum rate that a Carrier Ethernet subscriber can burst to assuming that on average they do not exceed the CIR [CIS200702].

Extended Unique Identifier (EUI) Link layer address defined by the Institute of Electrical and Electronic Engineers (IEEE).

Extension headers Headers placed between the IPv6 header and higher level protocols headers to provide additional functionalities to IPv6.

Fibre Channel (FC) The dominant storage networking protocol used in the enterprise data center and for (multimedia) content storage. A high speed storage/networking interface that offers a high performance, large transfer capacity, long cabling distance, system configuration flexibility and scalability, and simplified cabling. The current operating speed is 8 Gbps; the expectation is that a 16 Gbps rate will be achievable by mid decade (by comparison, 10 Gbps Ethernet is expected to move up to a 40 Gbps or even 100 Gbps rates over the same period).

Fibre Channel Arbitrated Loop (FCAL) A Fibre Channel implementation where users are attached to a network via a one-way ring (loop) cabling scheme.

Fibre Channel over Ethernet (FCoE) A method for encapsulation of Fibre Channel (FC) frames over full duplex IEEE 802.3 networks. This allows the FC to use 10 Gbit Ethernet for transport. The goal is to provide I/O consolidation over Ethernet, reducing network complexity in the Datacenter or content site. A content-management site may have several FC fabrics, IP networks dedicated to Network-Attached Storage, a LAN to link hosts and clients to that storage, and, a WAN. Fibre Channel over Ethernet (FCoE) is a technology that makes it possible to link these previously disparate networks, promising simpler administration, less complexity, and lower costs. The success of FCoE depends on a number of factors, including widely available/cost-effective 10 GigE components, and the implementation of the Data Center Ethernet (also known as Converged Enhanced Ethernet) standard [CAS201001].

The FCoE standardization activity started in April 2007 inside the FC-BB-5 working group of T11. In June 2009, the FC-BB-5 working group of T11 completed the development of the draft standard and unanimously approved it as the final standard. Also, in June 2009, the plenary session of T11 approved forwarding the FC-BB-5 standard to INCITS for publication as an ANSI standard [FCO201101].

Fibre Channel over IP (FCIP) A protocol for transmitting Fibre Channel (FC) data over an IP network. It allows the encapsulation/tunneling of FC packets and transport via Transmission Control Protocol/Internet Protocol (TCP/IP) networks (gateways are used to interconnect FC Storage Area Networks (SANs) to the IP network and to set up connections between SANs. FCIP uses IP-based network services to provide the connectivity between the SAN islands over Local Area Networks (LANs), Metropolitan Area Networks (MANs), or Wide Area Networks. It enables applications developed to run over FC SANs to be supported under IP, enabling organizations to leverage their current IP infrastructure and management resources to interconnect and extend FC SANs. FCIP relies on TCP for congestion control and management and upon both TCP and FC for data error and data loss recovery. FCIP treats all classes of FC frames the same as datagrams.

Fibre Channel SCSI This refers to products with FC physical and protocol layers using the SCSI command set. The FC interface is completely different from parallel SCSI in that it is a serial interface, meaning command and data information is transmitted on one signal stream organized into packets. The fiber may be either a copper coaxial cable or a fiber optic cable. The signal on the first implementation of fibre channel uses a 1 GHz rate, thereby achieving 100 Mbps over the cable. Fibre channel also implements increased software control of configuration and pushes the total device on the bus to 126 IDs, as opposed to only 8 or 16 on a parallel bus [SUN201001].

File formats Container file formats for various platforms. The more common formats include:

- .avi (Audio Video Interleave)—A multimedia container file format developed by Microsoft to allow synchronous audio-with-video playback.
- .flv—Flash video file format; used to deliver video over the Internet.
- .mov—A video publishing file format developed by Apple for use with their QuickTime video players.
- .wmv (Windows Media Video)—An audio and video file encoded for use with Windows Media Player.

Fixed Satellite Service (FSS) A satellite service that (for ITU Region 2 segments covering the majority of the Americas) operates at 14.0–14.5 GHz for the uplink, and 11.7–12.2 GHz for the downlink. Geostationary satellites are utilized. The service is utilized by television stations/ broadcast networks/ Cable TV systems to distribute signals to affiliates across a wide geographic region, as well as for other traditional telecommunications (voice and data communications) applications. Typical video applications include content distribution from a content-generation center (e.g., studios) to local cable headends. FSS satellites have also been used for Direct-To-Home (DTH) applications, although DBS services at the ku-BSS frequencies (such as those used by DirecTV and Dish Network) are specifically intended for those applications. The term “fixed” is used to imply that the sending station

is fixed and the receiving stations are generally (but not always) fixed. This is in contrast to the Mobile Satellite services (MSS), which refers to communications satellites intended for use with mobile and portable wireless devices/telephones. MSS-supporting services can be delivered using geostationary (GEO), medium earth orbit (MEO), or low earth orbit (LEO) satellites.

Flow A series of IP datagrams exchanged between a source and a destination.

Format Prefix Variable number of high order bits of an IPv6 address that defines an IPv6 address type.

Forward Direction The dominant direction of data transfer over a network path. Data transfer in the forward direction is called “forward transfer”. Packets traveling in the forward direction follow the forward path through the IP network [CLA200301].

Forward Error Correction (FEC) FEC is a family of well-known simplex error correction techniques that add “coding” bits to the information bits at the transmit end (encoder) that enables the decoder to determine which bits are in error and correct them (up to a limit), for example, R 5/4 FEC means 1 coding bit is added for every 4 information bits; the more coding bits, the “stronger” the code (requires less transmit power or link quality to get the same performance), but more coding bits mean more bandwidth required. Because satellite transmission can attenuate the signal by up to 200 db, FEC is critical. High coding: R 1/2; low coding: R 7/8. Typical satellite FEC is either Convolutional/Viterbi with Reed-Solomon or Turbo coding. Typical Turbo codes provide about a 2 dB advantage over conventional codes. “Viterbi” soft-decision decoding has been the norm (<4.4 dB gain). “Turbo coding” advanced recently (<6.3 dB gain). “Low Density Parity Check” (LDPC) newest (<7.8 dB gain).

Fragment A portion of a message sent by a host in an IPv6 datagram. Fragments contain a fragmentation header to allow reassembly at the destination.

Fragmentation Process in which the source device divides a message into some number of smaller messages, termed fragments.

Fragmentation header An IPv6 extension header that contains information that allows the receiving node to reassemble fragments into the original message.

Frame rate The rate at which frames are displayed. The frame rate for movies on film is 24 frames per second (24 fps). Standard NTSC video has a frame rate of 30 fps (actually 60 fields per second). The frame rate of a progressive-scan video format is twice that of an interlaced-scan format. For example, interlaced formats like 480i and 1080i deliver 30 complete frames per second; progressive formats like 480p, 720p, and 1080p provide 60 [KIN200901].

Free On-Demand VoD VoD where access and content is free, as stimulus to buy the overall service.

Full Rate Asymmetrical DSL (ADSL) Access technology that offers differing upload and download speeds and can be configured to deliver up to 6 megabits of data per second (6000 Kbps) from the network to the customer that is up to 120 times faster than dial-up service and 100 times faster than ISDN. ADSL enables voice and high-speed data to be sent simultaneously over the existing telephone line. This type of DSL is the most predominant in commercial use for business and residential customers around the world. Good for general Internet access and for applications where downstream speed is most important, such as video-on-demand. ITU-T Recommendation G.992.1 and ANSI Standard T1.413-1998 specify full rate ADSL. ITU Recommendation G.992.3 specifies ADSL2 that provides advanced diagnostics, power saving functions, PSD shaping, and slightly better performance than G.992.1. ITU Recommendation G.992.5 specifies ADSL2Plus that provides the benefits of ADSL2Plus twice the bandwidth so that bit rates as high as 20 Mbps downstream can be achieved on relatively short lines [DSL200701].

Full screen views The number of impressions where the video was played in full screen mode.

Fully qualified domain name (FQDN) FQDN gives the full location of a resource within the whole DNS name space. When interpreting the FQDN, one starts at the root and then follows the sequence of domain labels from right to left, going top to bottom within the name space tree. A FQDN includes the top-level domain. For example, <http://www.cnn.com> is a fully qualified domain name. www is the host, cnn is the second-level domain and com is the top level domain. This is in contrast to a partially qualified domain name (PQDN), which does not give the full path to the domain. One can only use a PQDN within the context of a particular parent domain.

G-lite ADSL (or simply G-lite) A standard that was specifically developed to meet the plug-and-play requirements of the consumer market segment. G-lite is a medium bandwidth version of ADSL that allows Internet access at up to 30 times the speed of the fastest 56K analog modems—up to 1.5 Mbps downstream and up to 500 Kbps upstream. G-lite is an International Telecommunications Union (ITU) standard, globally standardized interoperable ADSL system per ITU G.992.2. G-lite has seen comparatively little use, but it did introduce the valuable concept of splitterless installation [DSL200701].

GARP Multicast Registration Protocol (GMRP) A Layer 2 network protocol defined in the IEEE 802.1D specification. It provides multicast pruning and dynamic group membership for multicast. Typically used in Layer 2 switches. A switch can exchange multicast group information with other GMRP switches, prune unnecessary broadcast traffic, and dynamically create and manage multicast groups.

GLOB Addressing RFC 2770 recommended that the 233.0.0.0/8 address range be reserved for statically defined addresses by organizations that

already have an AS number reserved. The AS number of the domain is embedded into the second and third octets of the 233.0.0.0/8 range. GLOP is a mechanism that allocates multicast addresses to ASs (GLOP is neither an acronym nor an abbreviation.)

Global Address See aggregatable global unicast address.

Group Identifier Last 112 bits (for predefined multicast addresses) or last 32 bits (for new multicast addresses) of an IPv6 multicast address used to identify a multicast group.

Group of Pictures (GOP) A GOP is a group of successive pictures within a MPEG-coded film and/or video stream. Each MPEG-coded film and/or video stream consists of successive GOPs. From the MPEG pictures contained in it, the visible frames are generated.

HDSL (high data rate DSL) A DSL variety created in the late 1980s delivers symmetric service at speeds up to 2.3 Mbps in both directions. Available at 1.5 or 2.3 Mbps, this symmetric fixed rate application does not provide standard telephone service over the same line and is already standardized through ETSI and ITU (International Telecommunications Union). Seen as an economical replacement for T1 or E1, it uses one, two, or three twisted copper pairs [DSL200701].

HDSL2: (2nd-generation HDSL) A variant of DSL that delivers 1.5 Mbps service each way, supporting voice, data, and video using either ATM (Asynchronous Transfer Mode), private-line service, or frame relay over a single copper pair. The ATIS standard (T1.418) for this symmetric service gives a fixed 1.5 Mbps rate both up and downstream. HDSL2 does not provide standard voice telephone service on the same wire pair. HDSL2 differs from HDSL in that HDSL2 uses one pair of wires to convey 1.5 Mbps, whereas ANSI HDSL uses two wire pairs [DSL200701].

HDSL4 A high data rate DSL that is virtually the same as HDSL2 except it achieves about 30% greater distance than HDSL or HDSL2 by using two pairs of wire (thus, four conductors), whereas HDSL2 uses one pair of wires [DSL200701].

Hierarchical Storage Management (HSM) A storage system in which new, frequently used data is stored on the fastest, most accessible (and generally more expensive) media (e.g., RAID), and older, less frequently used data is stored on slower (less expensive) media (e.g., tape) [SUN201001].

High Definition (HD) DTV video that is of higher resolution than standard definition.

Higher-Level Checksum A checksum based on the IPv6 pseudo-header, used in ICMPv6, TCP, and UDP.

Higher-Level Protocol Protocol that uses IPv6 as transport and is carried as a payload in IPv6, such as ICMPv6, TCP, and UDP.

Hit (also known as Web Request) A request for a single file from a web server.

Home Network (HN) A communication system designed for the residential environment, in which two or more devices exchange information.

Home Theater PCs (HTPCs) PC-based hardware and software for interfacing and integrating televisions and home computers.

Homes passed Number of domiciles that are “passed” by cable plant. Alternatively, the number of homes in a defined geographic area within the footprint of satellite transmission.

Hop-By-Hop Option Header An IPv6 extension header that contains options that must be processed by all intermediate routers as well as final router.

Host Any node that is not a router.

Host-To-Host Tunnel An IPv6 over IPv4 tunnel where end points are hosts.

Host-To-Router Tunnel An IPv6 over IPv4 tunnel in which the tunnel begins at a host and ends at an IPv6/IPv4 router.

Hot spot In this context, an ad unit that is sold within the video content experience. A click action starts a linear video commercial or navigates the user to a specified website.

HTTP streaming The default higher-layers protocol for streaming audio and video over the Internet. It involves the simultaneous download and viewing/listening of the file through HTTP [REE201001].

Hybrid terminal device An IPTV terminal device that can also receive content from different types of transmission systems (e.g., satellite and cable) [ITU200801].

Hyperlinked video (also known as clickable video) A video in which specific objects are made selectable by some form of user interface, and the user’s interactions with these objects modify the presentation of the video.

Hypertext Transfer Protocol (HTTP) An application-level, stateless, object-oriented protocol for distributed, collaborative, hypermedia information systems.

ICMPv6 See Internet Control Message Protocol for IPv6.

IEEE 802.1ad IEEE 802.1ad (Provider Bridges) is an amendment to IEEE standard IEEE 802.1Q-1998, intended to develop an architecture and bridge protocols to provide separate instances of the MAC services to multiple independent users of a Bridged Local Area Network in a manner that does not require cooperation among the users, and requires a minimum of cooperation between the users and the provider of the MAC service. This is a standard version of the Q-in-Q protocol used by Cisco for Carrier Ethernet Service [CIS200702].

IEEE 802.1ah Provider Backbone Bridges (PBB) is being formalized by IEEE 802.1ah standards. It allows for layering the Ethernet network into customer and provider domains with complete isolation among their MAC addresses. It defines a B-DA and B-SA to indicate the backbone source and

destination address. It also defines B-VID (backbone VLAN ID) and I-SID (Service Instance VLAN ID).

IEEE 802.1Q IEEE 802.1Q was a project in the IEEE 802 standards process to develop a mechanism to allow multiple bridged networks to transparently share the same physical network link without leakage of information between networks (i.e., trunking). IEEE 802.1Q is also the name of the standard issued by this process, and, in common usage, the name of the encapsulation protocol used to implement this mechanism over Ethernet networks. IEEE 802.1Q also defines the meaning of a virtual LAN or VLAN with respect to the specific conceptual model underpinning bridging at the MAC layer and to the IEEE 802.1D spanning tree protocol. This protocol allows for individual VLANs to communicate with one another with the use of a Layer 3 (network) router [CIS200702].

IGMP Snooping A method by which a switch can constrain multicast packets to only those ports that have requested the stream.

IGMP Snooping Switches Local Area Network switches that do not adhere to the conceptual model that provides the strict separation of functionality between different communications layers in the ISO model, and instead utilize information in the upper level protocol headers as factors to be considered in processing at the lower levels. This is analogous to the manner in which a router can act as a firewall by looking into the transport protocol's header before allowing a packet to be forwarded to its destination address. In the case of IP multicast traffic, an IGMP snooping switch provides the benefit of conserving bandwidth on those segments of the network where no node has expressed interest in receiving packets addressed to the group address. This is in contrast to normal switch behavior where multicast traffic is typically forwarded on all interfaces [CHR200601].

In-banner video ads Approach that leverages the banner space to deliver a video experience as opposed to another static or rich media format. The format relies on the existence of display ad inventory on the page for its delivery [REE201001].

Incoming interface (iif) In PIM-SM, the iif of a multicast route entry indicates the interface from which multicast data packets are accepted for forwarding. The iif is initialized when the entry is created [EST199801].

In-page video ads An approach where ads are delivered as a standalone video ad and do not generally have other content associated with them. This format is typically home page or channel-based and depends on real estate within the page dedicated for the video player [REE201001].

In-stream video ads Approach where ads are played before, during, or after the streaming video content that the consumer has requested. These ads cannot typically be stopped from being played (particularly with preroll). This format is frequently used to monetize the video content that the publisher is delivering. In-stream ads can be played inside short or long form video and rely on video content for their delivery. There are four different

types of video content where in-stream may play, UGC (User Generated Content/Video), Syndicated, Sourced and Journalistic [REE201001].

Integrated Services Digital Network DSL (ISDL) A form of DSL that supports symmetric data rates of up to 144 Kbps using existing phone lines. It is unique in that it has the ability to deliver services through a DLC (Digital Loop Carrier: a remote device often placed in newer neighborhoods to simplify the distribution of cable and wiring from the phone company). While DLCs provide a means of simplifying the delivery of traditional voice services to newer neighborhoods, they also provide a unique challenge in delivering DSL into those same neighborhoods. ISDL addresses this market along with ADSL and G.lite as they are implemented directly into those DLCs. ISDL differs from its relative ISDN (integrated services digital network) in that it is an “always-available” service, but capable of using the same terminal adapter, or modem, used for ISDN [DSL200701].

Integrity The property that data has not been altered or destroyed in an unauthorized manner.

Interactive Program Guide (IPG) A mechanism similar to the Electronic Program Guide (EPG) that typically allows the user to browse listings by program title, channel or theme; scan current and future programs on other channels without leaving the current program; purchase Pay Per View events; start recording a program; set parental controls; set up a “favorites” channel list; and undertake other related tasks.

Interface A node’s attachment to a link. A representation of a physical or logical link of a node to a link. An example of a physical interface is a network interface. An example of a logical interface is a tunnel interface.

Interface Identifier Last 64 bits of a unicast or anycast IPv6 address.

Internet-Based TV (IBTV) Video distribution approaches, such as Web television, Internet television, and/or User-Generated Video (UGV).

Internet Control Message Protocol For IPv6 (ICMPv6) Protocol for Internet Control Messages for IPv6. A protocol that provides error messages for the routing and delivery of IPv6 datagrams and information messages for diagnostics, neighbor discovery, multicast receiver discovery, and IPv6 mobility.

Internet FCP (iFCP) A protocol that converts Fibre Channel (FC) frames into Transmission Control Protocol (TCP) enabling native Fibre Channel devices to be connected via an IP network. iFCP is a gateway-to-gateway protocol allows the replacement of FC fabric components, allowing attachment of existing FC enabled storage products to an IP network. Encapsulation protocols for IP storage solutions where the lower-layer FC transport is replaced with TCP/IP and Gigabit Ethernet. The protocol enables existing FC storage devices or Storage Area Network (SAN) to attach to an IP network. The operation is as follows: FC devices, such as disk arrays, connect to an iFCP gateway or switch. Each FC session is terminated at the local gateway and converted to a TCP/IP session via iFCP. A second gateway or

switch receives the iFCP session and initiates a FC session. In iFCP, TCP/IP switching and routing elements complement and enhance, or replace, FC SAN fabric components.

Internet Group Management Protocol (IGMP) The protocol used by IP Version 4 (IPv4) hosts to communicate multicast group membership states to multicast routers. IGMP is used to dynamically register individual hosts/receivers on a particular local subnet to a multicast group. IGMP Version 1 defined the basic mechanism. It supports a Membership Query, MQ, message and Membership Report, MR, message. Most implementations at press time employed IGMP Version 2; Version 2 adds Leave Group, LG, messages. Version 3 adds source awareness allowing the inclusion or exclusion of sources. IGMP allows group membership lists to be dynamically maintained. The host (user) sends an IGMP “report”, or join, to the router to be included in the group. Periodically, the router sends a “query” to learn which hosts (users) are still part of a group. If a host wishes to continue its group membership, it responds to the query with a “report.” If the host does not send a “report,” the router prunes the group list to delete this host; this eliminates unnecessary network transmissions. With IGMP V2, a host may send a “leave group” message to alert the router that it is no longer participating in a multicast group; this allows the router to prune the group list to delete this host before the next query is scheduled, thereby minimizing the time period during which unneeded transmissions are forwarded to the network.

Internet Protocol Television (IPTV) A system for the delivery of (high quality) video programming using video streams encoded/multiplexed with MPEG-2 or MPEG-4 Transport Streams (TSs) and then encapsulated in IP packets. IPTV-based content is distributed by a service provider, typically a telephone company (but not always) and can be free or fee-based. IPTV can carry live TV content or stored video content. IPTV uses multicasting implemented with Internet Group Management Protocol (IGMP) (typically Version 2) for live television broadcasts and Real Time Streaming Protocol for on-demand programs.

Multimedia services such as television/video/audio/text/graphics/data delivered over IP-based networks that are tightly managed to support the required level of Quality of Service/Quality of Experience (QoS/QoE), security, interactivity, and reliability [ITU200801]. Access is usually provided via a subscription service very similar to traditional Cable TV service, except for the transport network, which is IP-based (IPv4 and/or IPv6.)

Approaches, technologies, protocols to deliver commercial-grade Standard Definition (SD) and High Definition (HD) entertainment-quality real-time linear and on-demand video content over IP-based networks, while meeting all prerequisite QoS, QoE, Conditional Access (security), Blackout Management (for sporting events), Emergency Alert System, Closed Captions, Parental Controls, Nielsen Rating collection, Secondary Audio

channel, Picture-in-Picture, and guide data requirements of the content providers and/or regulatory entities. Typically, IPTV makes use of Moving Pictures Expert Group 4 (MPEG-4) encoding to deliver 200–300 SD channels and 20–30 HD channels; viewers need to be able to switch channels within 2 seconds or less; also, the need exists to support multiset-top boxes/multiprogramming (say 2-4) within a single domicile. Not to be confused with simple delivery of video over an IP network, which has been possible for over two decades; IPTV supports all business, billing, provisioning, content protection requirements that are associated with commercial video distribution. Service needs to be comparable with that received over Cable TV or Direct Broadcast Satellite. IP multicast is typically employed. Multimedia services, such as television/video/ audio/text/graphics/data, delivered over IP-based networks managed to support the required level of QoS/QoE, security, interactivity, and reliability [ITU200801].

Internet Small Computer System Interface (iSCSI) A protocol that serializes SCSI commands and converts them to Transmission Control Protocol/Internet Protocol (TCP/IP). Encapsulation protocols for IP storage solutions for the support of Direct Attached Storage (DAS) (specifically SCSI-3 commands) over IP network infrastructures (at the physical layer, iSCSI supports a Gigabit Ethernet interface so that systems supporting iSCSI interfaces can be directly connected to standard Gigabit Ethernet switches and/or IP routers; the iSCSI protocol sits above the physical and data-link layers). iSCSI is a protocol for a new generation of storage end-nodes that natively use TCP/IP and replaces FCP with a pure TCP/IP implementation. iSCSI has broad industry support.

Internet television (also known as Internet TV, Online TV) A television service distributed via the Internet, as exemplified by services such as Hulu (for U.S. content, mostly) and BBC iPlayer (for U.K content, mostly). The content is typically commercially produced TV material, but the “transmission/distribution” channel is the Internet; the transmission/distribution’ also includes network-resident storage (supported by video servers).

Internet television, Internet-Based TV (IBTV) (Also known as Internet TV and Online TV) A system for the delivery of video programming where the content is typically distributed through an Internet website. Users can select from a library of shows online and select the show they want. A television service distributed via the Internet, as exemplified by services such as Hulu (for U.S. content) and BBC iPlayer (for U.K content). The content is typically commercially produced TV material, but the “transmission/distribution” channel is Internet; the transmission/distribution’ also include network-resident storage (video servers).

Internet video on demand (iVoD) (Some also call this Interactive VoD) Transactional digital rental methods, specifically when such rental is downloaded via the Internet (rather than being done over a Cable TV network or an IPTV network.)

Note: The term has not totally congealed in the industry. Some define iVoD as a capability that enhances traditional VoD services by providing trick modes; others define iVoD as a system that uses a consumer's home broadband connection to deliver video content directly to the TV set.

Interstitial program A short program that is shown between events (e.g., between two movies) or embedded during presentation of an event (e.g., advertisement) [ITU200801].

Interworking mechanisms for IPv6 and IPv4 Well-known interworking mechanisms include [GIL200001]:

- *Dual Stack*: A technique for providing complete support for both protocols—IPv4 and IPv6—in hosts and routers.
- *Configured Tunneling of IPv6 over IPv4*: Manually configured point-to-point tunnels for encapsulating IPv6 packets within IPv4 headers to carry them over an IPv4 routing infrastructures.
- *Automatic Tunneling of IPv6 over IPv4*: Mechanisms for automatically tunneling IPv6 packets over IPv4 networks.
- *Translation*: Refers to the direct conversion of protocol0s.

In-text video ads Approach where ads are delivered from highlighted words and phrases within the text of web content. The ads are user-activated and delivered only when a user chooses to move their mouse over a relevant word or phrase [REE201001].

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) An IPv6 transition technology that provides IPv6 unicast connectivity between devices placed in an IPv4 intranetwork. ISATAP obtains an interface identifier from the IPv4 address (public or private) assigned to the device. This identifier is used for the establishment of automatic tunnels through the IPv4 infrastructure [IPV200501].

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Address An IPv6 address of the form—64-bit prefix:0:5EFE:w.x.y.z—where w.x.y.z is a public or private IPv4 address allocated to an ISATAP device.

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Device A device to which an ISATAP address is assigned to.

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Name The name “ISATAP” is resolved by computers with Windows XP or Windows Server 2003 operating system to automatically discover the ISATAP router address for initial configuration.

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Router An IPv6/IPv4 router that answers ISATAP node requests and routes traffic to and from ISATAP nodes.

Invitation unit A small still or animated graphic overlaid directly onto video content. Typically used as a less-intrusive initial enticement. When the

viewer clicks or interacts with the invitation graphic, they expand into the ad's full expression (e.g., an auto-play video or an interactive session.)

IP Multimedia Subsystem (IMS) IMS is a 3GPP/3GPP2 initiative to define an all IP-based wireless network as an evolution from historically distinct voice, data, signaling, and control network elements.

IP over Ethernet (IPoE) IP over Ethernet is used in DSL and PON access networks in place of PPPoE.

IP storage Using IP and Gigabit Ethernet to build Storage Area Networks (SANs). Traditional SANs were developed using the Fibre Channel (FC) transport, because it provided gigabit speeds compared to 10 and 100 Mbps Ethernet used to build messaging networks at that time. FC equipment has been costly, and interoperability between different vendors' switches was not completely standardized. Since Gigabit Ethernet and IP have become commonplace, IP storage enables familiar network protocols to be used, and IP allows SANs to be extended throughout the world. Variants include:

- Internet FCP (iFCP)
- Metro Fibre Channel Protocol (mFCP)
- Internet Small Computer System Interface (iSCSI)
- Fibre Channel Over Internet Protocol (FCIP)

IP6.arpa The DNS domain created for the IPv6 reverse resolution (RFC 3596). The reverse resolution has the purpose of “reverse mapping” of IPv6 addresses to DNS names.

IPoDWDM Optical Network Carriage of IP packets directly over the optical layer provided by a Dense wavelength Division Multiplexing optical system.

IPTV Terminal Device (TD) A terminal device that has ITF (IPTV Terminal Function) functionality, for example, a set-top box (STB).

IPTV terminal function (ITF) The functionality that is responsible for processing the content conveyed by the IP transport. The functionality within the home network that is responsible for terminating the IP signal, and converting the content into a renderable (i.e., enabling to be seen and/or heard) format [ITU201101].

IPv4 node A node that implements IPv4; it can send and receive IPv4 packets. It can be an IPv4 only node or a dual IPv4/IPv6 node.

IPv4-compatible IPv6 address A 0:0:0:0:0:w.x.y.z or ::w.x.y.z address, where w.x.y.z is the decimal representation of a public IPv4 address. For example, ::131:107:89:42 is an IPv4-compatible address. IPv6 transition mechanisms no longer use IPv4-compatible address scheme.

IPv4-mapped IPv6 address A 0:0:0:0:FFFF:w.x.y.z (or ::FFFF:w.x.y.z) address, where w.x.y.z is the IPv4 address of an IPv4-only node. Mapped IPv4 addresses are used to represent an IPv4-only host.

IPv6 in IPv4 See IPv6 over IPv4 tunnel.

IPv6 Node Node that implements IPv6; it can send and receive IPv6 packets. An IPv6 node can be an IPv6 only node or a dual IPv6/IPv4 node.

IPv6 over IPv4 tunnel Encapsulating IPv6 packets into an IPv4 datagram and transporting the datagram over an IPv4 infrastructure. In the IPv4 header, the protocol field value is 41.

IPv6 prefixes The initial bits of an IP address. The number of bits is represented via the prefix-length notation. Prefixes for IPv6 routes and subnet identifiers are expressed in the same way as Classless Interdomain Routing (CIDR) notation for IPv4. For example, 21DA:D3::/48 is a route prefix, and 21DA:D3:0:2F3B::/64 is a subnet prefix. IPv4 implementations commonly use a dotted decimal representation of the network prefix known as the subnet mask. A subnet mask is not used in IPv6. Only the prefix-length notation is used [MSD200401].

IPv6 Routing Table Set of routes used to determine the next node address and interface when forwarding IPv6 traffic.

IPv6/IPv4 node A node that has both IPv4 and IPv6 implementations.

Join list In PIM-SM, the Join list is one of two lists of addresses that is included in a Join/Prune message; each address refers to a source or RP. It indicates those sources or RPs to which downstream receiver(s) wish to join [EST199801].

Key A digital code used to encrypt, sign, decrypt, and verify messages and files. A sequence of symbols that controls the operations of encipherment and decipherment.

Key Management Generation, distribution, storage, replacement, and destruction of keys.

Key pair A public key and its complementary private key. In public-key systems, each user has at least one key pair.

Keyframe A position on a video timeline when an event occurs.

Last-hop router In PIM-SM, the last-hop router is the last router to receive multicast data packets before they are delivered to directly connected member hosts. In general, the last-hop router is the DR for the LAN. However, under various conditions described in this document, a parallel router connected to the same LAN may take over as the last-hop router in place of the DR [EST199801]. It is generally the same as the DR and is responsible for forwarding packets to its directly connected members. There are some special conditions where this last hop router is not the DR [ROD200701].

Layer 2 Layer 2 of the protocol stack. This typically refers to the set of Ethernet protocols that operate below the IP layer of the protocol stack.

Layer 2 Tunneling Protocol (L2TP) Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs).

Layer 3 Layer 3 of the Open Systems Interconnection (OSI) protocol stack. This refers to the Internet protocol used for routing in the Internet.

Lifetime In Preferred State Time during which a unicast address, obtained by means of stateless autoconfiguration mechanism, stays in the preferred state. This time is specified by the preferred lifetime field in Routers Advertisement message prefix information option.

Limited Scope Addresses (also known as Administratively Scoped Addresses)

The range of addresses from 239.0.0.0 through 239.255.255.255. RFC 2365 defines these addresses to be limited to a local group or organization. Routers are required to be configured with packet filters to prevent multi-cast traffic in this address range from flowing outside of an Autonomous System (AS).

Linear programming Real-time TV content, including national channels, local channels, sports channels, and premium channels.

Linear TV A television service in which a continuous stream flows in real time from the service provider to the terminal device and where the user cannot control the temporal order in which contents are viewed [ITU200801]. Typically found in Broadcast TV environments.

Linear Video Ads Ads experienced in-stream presented before, between, or after the video content is consumed by the user. With linear video ads, the ad takes over the full view of the video.

Link A communication facility or medium over which nodes can communicate at the link layer, that is, the layer immediately below IPv6. Examples include: Ethernet environments (simple or bridged); PPP links; X.25 Packet Switching, Frame Relay, and Cell Relay/Asynchronous Transfer Mode (ATM); or IPv4.

Link-local addresses IP multicast addresses that have been reserved for specific functions. Addresses in the 224.0.0.0 through 224.0.0.255 are reserved to be used by network protocols on a local network segment. Network protocols make use of these addresses for automatic router discovery and to communicate routing information (e.g., OSPF uses 224.0.0.5 and 224.0.0.6 to exchange link state information). IP packets with these addresses are not forwarded by a router; they remain local on a particular LAN segment (they have a time-to-live (TTL) parameter set to 1; even if the TTL is different from 1, they still are not forwarded by the router).

Link State Routing Protocol A routing protocol in which a router informs all the nodes in a network of topology changes. Information exchanged consists of prefixes of networks connected to the router and their associated cost. This is in contrast to distance vector routing protocols that exchange routing table information but only with neighboring nodes.

Link-Layer Identifier A link-layer identifier for an interface. Examples include IEEE 802 addresses for Ethernet or Token Ring network interfaces and E.164 addresses for ISDN links.

Link-local address An IPv6 address having a link-only scope, indicated by the prefix (FE80::/10), that can be used to reach neighboring nodes attached to the same link. Every interface has a link-local address.

Liquid crystal display (LCD) Liquid Crystal Display technology is one of the methods used to create flat-panel TVs. Light is not created by the liquid crystals; a “backlight” behind the panel shines light through the display. The display consists of two polarizing transparent panels and a liquid crystal solution sandwiched in between. An electric current passed through the liquid causes the crystals to align so that light cannot pass through them. Each crystal acts like a shutter, either allowing light to pass through or blocking the light. The pattern of transparent and dark crystals forms the image [KIN200901].

Liquid crystal on silicon (LCoS) A projection TV technology based on LCD. With LCoS, light is reflected from a mirror behind the LCD panel rather than passing through the panel. The control circuitry that switches the pixels on and off is embedded further down in the chip so it does not block the light, which improves brightness and contrast. This multilayered microdisplay design can be used in rear-projection TVs and projectors [KIN200901].

Local address An IPv6 unicast address that is not reachable on IPv6 Internet. Local addresses include “link-local” and “site-local” addresses. (However, site-local addresses have been deprecated).

Local Interface Internal interface that allows a node to send packets to itself.

Long-Term Evolution (LTE) (aka 4G) LTE is a project name and an “all IP” standard for mobile traffic that will increase the broadband capabilities beyond current 3G mobile technologies.

Loopback Address The IPv6 address—`0:0:0:0:0:1` or `::1`—assigned to the local interface.

MAC Medium Access and Control of the Ethernet IEEE 802 standard of Protocols [CLA200301].

MAC Address A link layer address for local area network technologies such as Ethernet and Token Ring. It is also referred to as a physical address, hardware address, or network adapter address.

MAC Header The link layer header of the IEEE 802.3 standard or Ethernet v2. It consists of a 6B destination address, 6B source address, and 2B type field (see also NPA, LLC) [FAI200501].

Machine (Host) A node that cannot send datagrams not created by itself. A machine (host) is both the source and destination of IPv6 traffic and will discard traffic that is not specifically addressed to it.

Masquerade The pretense by an entity to be a different entity.

Maximum Transmission Unit MTU MTU refers to the size (in bytes) of the largest packet that a given layer of a communications protocol can pass onwards. Maximum transmission units are defined at the link layer (frame maximum size) and at the network or Internet layer (maximum IPv6 packet size).

Maximum-Level Aggregation Identifier (aka Top-Level Aggregation Identifier—TLA ID). 13-bit field inside the global unicast address reserved for large organizations or ISP by the IANA, hence, it identifies the address

range that they have delegated. The TLA scheme has been obsoleted by RFC 3587.

M-commerce (mobile commerce) (also known as next-generation e-commerce)

The buying and selling of goods and services through wireless handheld devices, such as smartphones, traditional cellular telephone, and personal digital assistants (PDAs). M-commerce enables users to access the Internet without needing to find a place to plug in.

Media Access Control (MAC) A sublayer of the link layer of local area networks defined by the Institute of Electrical and Electronic Engineers. Its functionalities include the creation of frames and the management of medium sharing and access.

Medium Earth Orbit (MEO) satellite A satellite with an earth orbit within the range from a few hundred miles to a few thousand miles above the earth's surface. MEO satellites orbit higher than low earth orbit (LEO) satellites, but lower than geostationary (GEO) satellites.

Member In PIM-SM it is the host that is to receive multicast transmissions. The protocol documentation also refers to a member as a “receiver” [ROD200701].

Metadata Metadata is descriptive data associated with a content asset package or file. It may vary in depth from merely identifying the content package title or information to populate an Electronic Program Guide (EPG) to provide a complete index of different scenes in a movie or providing business rules detailing how the content package may be displayed, copied, or sold. Separate uses for metadata have originated from the studios, distribution networks (Cable and Satellite), down to the CPE (STBs and PVRs) [ITU200801].

Metro Fibre Channel Protocol (mFCP) A proposal for handling “IP storage”. It is identical to iFCP, except that Transmission Control Protocol (TCP) is replaced by User Datagram Protocol (UDP).

Middleware A layer of software between applications and resources, which consists of a set of service enablers that allow multiple functionalities running on one or more devices in an IPTV system to interact across a network [ITU200801].

Mid-roll A linear video spot that appears in the middle of the video content.

Mobility The ability for the end user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment.

Monetized Video Online videos that generate revenue by themselves. This is usually accomplished by advertisements in and around the video content, but can also be accomplished by charging users to watch, download, or subscribe to the videos [REE201001].

Motion Picture Expert Group (MPEG) A family of standards used for coding audiovisual information (e.g., movies, video, and music) in a digitally

compressed format. There are three major MPEG standards: MPEG-1, MPEG-2, and the newer MPEG-4.

MPEG-2/MPEG-4 (Motion Picture Experts Group-2/4) A set of multiplexing/encoding standards specified by the Motion Picture Experts Group (MPEG), and standardized by the International Organization for Standardization (ISO/IEC 113818-1), and ITU-T (H.220). Both MPG-2 and MPEG-4 are important for IPTV, but the recent trend is in favor of MPEG-4.

MPEG-7 An ISO/IEC standard for description and search of audio and visual content.

MPLS VPN A Layer 3 virtual IP network specified by RFC 2547bis. It used a combination of BGP routing and MPLS forwarding to create a virtual IP network on top of a service provider's physical IP network. MPLS VPN services are replacing Frame Relay and ATM services [CIS200702].

Multicast A methodology and supporting mechanisms, technologies, and standards for distribution of information (including video content) over the Internet. Multicast allows a server to inject a single copy of a given content into the Internet and many receivers (computers, smart phones, Internet-ready TV sets, etc.), but not the entire universe of receivers as would be the case in broadcast, to receive and play the same stream simultaneously.

Multicast Address An address that identifies several interfaces and is used to deliver data from one source to several destinations. That is, an identifier for a set of interfaces typically belonging to different nodes. By means of the multicast routing topology, packets to a multicast address will be delivered to all interfaces identified by that address.

An identifier for a group of nodes. An IP multicast address or group address, as defined in "Host Extensions for IP Multicasting", STD 5, RFC 1112, August 1989, and in "IP Version 6 Addressing Architecture", RFC 2373, July 1998. The Internet Assigned Numbers Authority (IANA) controls the assignment of IP Multicast Addresses. IANA has allocated what has been known as the Class D address space to be utilized for IP Multicast. IP Multicast-group addresses are in the range 224.0.0.0 through 239.255.255.255.

Multicast Address Dynamic Client Allocation Protocol (MADCAP) A protocol defined in RFC 2730 that allows hosts to request multicast addresses from multicast address allocation servers. This protocol is part of the IETF Multicast Address Allocation Architecture [HAN199901].

Multicast Address Set Claim Protocol (MASC) Protocol defined in RFC 2909 that can be used for interdomain multicast address set allocation. MASC is used by a node (typically a router) to claim and allocate one or more address prefixes to that node's domain. While a domain does not necessarily need to allocate an address set for hosts in that domain to be able to allocate group addresses, allocating an address set to the domain does ensure that interdomain group-specific distribution trees will be locally rooted, and that traffic will be sent outside the domain only when and where external receivers exist [RAD200001].

Multicast Environment Environment where one system communicates to a select group of other systems.

Multicast Group Set of interfaces listening to a specific multicast address.

Multicast IPv4 Tunnel See 6over4.

Multicast Listener Discovery Protocol (MLDv2) MLDv2 is a multicast listener discovery protocol that is used by an IPv6 router to discover the presence of multicast listeners on directly attached links, and to discover which multicast addresses are of interest to those neighboring nodes. MLDv2 is designed to be interoperable with MLDv1. MLDv2 adds the ability for a node to report interest in listening to packets with a particular multicast address only from specific source addresses or from all sources except for specific source addresses [VID200401].

The Internet Group Management Protocol (IGMP) (RFC1112, IGMPv2, IGMPv3) allows an IPv4 host to communicate IP multicast group membership information to its neighboring routers; IGMPv3 provides the ability for a host to selectively request or filter traffic from individual sources within a multicast group. MLD defined in RFC 2710 (MLDv2) offers similar functionality for IPv6 hosts. MLDv2 provides the analogous “source filtering” functionality of IGMPv3 for IPv6 [HOL200601].

Multicast OSPF (MOSPF) Protocol defined in RFC 1584 that provides enhancements to OSPF Version 2 to support IP multicast routing. With MOSPF, an IP multicast packet is routed based both on the packet’s source and its multicast destination (commonly referred to as source/destination routing). As it is routed, the multicast packet follows a shortest path to each multicast destination. During packet forwarding, any commonality of paths is exploited; when multiple hosts belong to a single multicast group, a multicast packet will be replicated only when the paths to the separate hosts diverge.

OSPF, a link-state routing protocol, provides a database describing the Autonomous System’s topology. A new OSPF link state advertisement has been added, describing the location of multicast destinations. A multicast packet’s path is then calculated by building a pruned shortest-path tree rooted at the packet’s IP source. These trees are built on demand, and the results of the calculation are cached for use by subsequent packets [MOY199401].

Multicast Payload Forwarding Communication mechanism to forward payload. Almost invariably this is IP-based at the network layer. Typical IP Multicast applications make use of User Datagram Protocol (UDP) at the Transport Layer; however, Transmission Control Protocol (TCP) can also be used in same applications.

Multicast Routing A mechanism to build distribution trees that define a unique forwarding path between the subnet of the content source and each subnet containing members of the multicast group, specifically, receivers.

Multicast Routing Information Base (MRIB) This is the multicast topology table, which is typically derived from the unicast routing table, or from routing protocols such as Multiprotocol Border Gateway Protocol (MP-BGP) that carry multicast-specific topology information [ADA200501].

Multicast Scope A range of multicast addresses configured so that traffic sent to these addresses is limited to some subset of the internetwork. Defined in “Administratively Scoped IP Multicast”, BCP 23, RFC 2365, July 1998.

Multicast Source Discovery Protocol (MSDP) A protocol that allows multiple PIM Sparse Mode domains to share information about active sources. The protocol announces active sources to MSDP peers. It is a BGP-like protocol that allows a rendezvous point (RP) to forward source and multicast group information to other RPs (e.g., to support redundant RPs or multidomain applications where each ISP can each have its own RP(s) [WEL200101]).

Multi-channel audio Audio signal with more than two channels.

MultiCrypt The specification of a Common Interface which, when installed in the set-top-box or television, permits the user to switch manually between Conditional Access (CA) systems. Thus, when the viewer is presented with a CA system that is not installed in his box, he/she simply switches cards [DVB201101]. A mechanism that enables the reception of programs encrypted according to various encryption systems by means of a Common Interface (CI) [ITU200801].

Multiple Systems Operator (MSO) Term used to describe cable operators that own more than one franchises.

Multiprotocol Border Gateway Protocol (MP-BGP) (also referred to by the acronym form MBGP) A protocol that defines multiprotocol extensions to the Border Gateway Protocol (BGP), the unicast interdomain protocol that supports multicast-specific routing information. MP-BGP augments BGP to enable multicast routing policy and connect multicast topologies within and between BGP autonomous systems. It carries multiple instances of routes for unicast routing, as well as multicast routing. Protocol that carries routing information about several protocols, including IP multicast (and also IPv6 and MPLS VPN information, among others). In IP multicast, MP-BGP carries a separate copy of unicast routes. MP-BGP helps establish which links the PIM Join messages use, which in turn allows us to control which links the multicast traffic traverses [WEL200101].

Multiprotocol Encapsulation (MPE) A scheme that encapsulates PDUs, forming a DSM-CC Table Section. Each Section is sent in a series of TS Packets using a single TS Logical Channel [FAI200501], [CLA200301].

Multi-room Enabling management and consumption of Conditional Access (CA) protected content on several TV-sets simultaneously, located within the same household. The STBs must be subject to physical or logical

grouping of devices. May or may not utilize a home network solution [CON200701].

Name Resolution Procedure to obtain an IP address from a name.

National Television System Committee (NTSC) format A type of interlaced analog video stream used primarily in North America. It is made up from 525 horizontal lines playing at 30 frames per second (or 60 fields per second).

Near Video On Demand (nVoD) Service similar to PPV. While PPV service starts the movie every 2 hours, nVoD service shows the same movie on several channels, each starting as little as 15 minutes apart. Hence the subscriber has a short wait time until the movie begins [NOR200601]. Systems that deliver programming at a time acceptable to the consumer, although not instantaneous, accomplished by repeating the same programs on several channels simultaneously at frequent intervals, for example, every 15 or 30 minutes [CON200701].

Neighbor Discovery (ND) A set of messages and ICMPv6 processes that fixes the relations between neighbor nodes. Neighbor Discovery replaces ARP, ICMP routes discovery, and ICMP redirection messages used in IPv4. It also provides inaccessible neighbor detection.

Neighbor Discovery Options Options in a Neighbor Discovery message that show link layer addresses, information about prefixes, MTU, routes and configuration information for IPv6 mobility.

Neighbors Nodes connected to the same link.

Neighbors cache A cache supported by each IPv6 node that stores the IP address of its neighbors on the link, its corresponding link layer address and an indication of its accessibility state. Neighbors cache is equivalent to the ARP cache in IPv4.

Network Address Translation-Protocol Translation (NAT-PT) Process performed by a network device on the boundary of an IPv4 and IPv6 network. NAT-PT uses a pool of IPv4 addresses for dynamic assignment to the IPv6 nodes. NAT-PT also allows the multiplexing of multiple sessions on a single IPv4 address via the “port” field.

Network Addresses Translator A device that translates IP addresses and port numbers when forwarding packets between a network with private addresses and the Internet.

Network Point of Attachment (NPA) A 6-byte destination address (resembling an IEEE MAC address) within the MPEG-2 transmission network that is used to identify individual Receivers or groups of Receivers [FAI200501].

Network segment See Subnetwork.

Network-Attached Storage (NAS) A disk array storage system that is attached directly to a network rather than to the network server (i.e., host attached). It functions as a server in a client/server relationship, has a pro-

cessor, an operating system or micro kernel, and processes file I/O protocols such as SMB and NFS [SUN201001].

Network personal video recorder (nPVR) Same as PVR except that the recording device is located at the service provider premises [ITU200801].

Next-Level Aggregation Identifier (NLAID) 24-bit field inside the global unicast aggregatable address that allows the creation of several hierarchical levels of addressing to organize addresses and routing to other ISPs, as well as to identify organization sites. The NLA scheme has been obsoleted by RFC 3587.

NIT (Network Information Table) MPEG Signaling Table that (contains details of the bearer network used to transmit the MPEG multiplex, including the carrier frequency (PID = 10) [FAI200101].

Node A device that implements IP.

Node types Node types in an IPv6 environment include the following [GIL200001]:

- *IPv4-Only Node*: A host or router that implements only IPv4. An IPv4-only node does not understand IPv6. The installed base of IPv4 hosts and routers existing before the transition to IPv6 begins are IPv4-only nodes.
- *IPv6/IPv4 Node*: A host or router that implements both IPv4 and IPv6.
- *IPv6-Only Node*: A host or router that implements IPv6, and does not implement IPv4.
- *IPv6 Node*: Any host or router that implements IPv6. IPv6/IPv4 and IPv6-only nodes are both IPv6 nodes.
- *IPv4 Node*: Any host or router that implements IPv4. IPv6/IPv4 and IPv4-only nodes are both IPv4 nodes.

Nonbroadcast Multiple Access (NBMA) A link layer technology that supports links with more than two nodes, but without allowing the sending of a packet to all nodes on the link (broadcast). Example technologies include: X.25 Packet Switching Service, Frame Relay Service, and Cell Relay Service/ Asynchronous Transfer Mode (ATM).

Nonbroadcast networks A network supporting the attachment of more than two stations, but not supporting the delivery of a single physical datagram to multiple destinations (i.e., not supporting data-link multicast). OSPF describes these networks as nonbroadcast, multiaccess networks. An example of a nonbroadcast network is an X.25 Public Data Network [MOY199401].

Nonlinear Video Ads An ad product that runs parallel to the video content such that the user still has the option of viewing the content. Common nonlinear ad products include overlays that are shown directly over the content video itself, and product placements, which are ads placed within

the video content itself. Nonlinear video ads can be delivered as text, graphical banners or buttons, or as video overlays [REE201001].

Nonmulticast router In the context of Multicast Open Shortest Path First (MOSPF), a router running OSPF Version 2, but not the multicast extensions. These routers do not forward multicast datagrams, but can interoperate with MOSPF routers in the forwarding of unicast packets. Routers running the MOSPF protocol are referred to as either multicast-capable routers or MOSPF routers [MOY199401].

Nontraditional TV (NTTV) New viewer approaches include (but not limited to) the following: watching entertainment/news using the Internet (such as a TV show, a movie, or a short clip); watching a multicast (rather than broadcast) entertainment/news program; watching a Video On Demand program (such as a movie or pay-per-view event); watching time-shifted TV; watching entertainment/news with a mobile smartphone, a personal digital assistant, a videogame console, a tablet, or a device in a car or boat; and/or watching user-generated content, particularly utilizing social networks.

Object Storage An emerging storage approach similar to file-based storage, except it makes greater use of metadata. It trades the efficiency and performance of block-based storage for easier management and more automation. Object metadata will let content providers and enterprises manage the storage more effectively and apply policies based on the data content, regulatory requirements, ownership of the data, or based on other principles. The metadata can also be used to dynamically store data at the most appropriate service levels [RAD201001].

On-demand A type of streaming in which a clip plays from start to finish when a user clicks a link; most clips are streamed this way.

Online video Any form of digital video that is available for use over the internet.

On-tree router In CBT, a router that is part of a CBT distribution tree is known as an “on-tree” router. An on-tree router maintains active state for the group [BAL199701].

OpenCable A CableLabs project with the goal of helping the cable industry deploy interactive services over cable. See <http://www.opencable.com>

Outgoing interface (OIF) list In PIM-SM, each multicast route entry has an oif list containing the outgoing interfaces to which multicast packets should be forwarded [EST199801].

Overlay ad A banner ad that appears in the bottom 20% of the video window. Click action initiates a linear video spot or takes the user to a website. Sold on a CPM and CPC basis.

Over-The-Top (OTT) streaming devices (also known as OTT set-tops) devices employed by viewers to watch shows or programs via multimedia and open public networks (particularly the Internet). OTT enable TVs,

Smart TVs, set-top boxes, PCs, tablets, smartphones, and game consoles to receive and process streaming video.

Over/under format (aka over-and-under) Over/Under 3D format involves using a mirror system to separate the left and right images that are placed one above one another. Special mirrored viewers are made for over/under format. A form of 3D stereo recording (on cine film) or viewing (of prints) in which the left and right images are positioned one above the other rather than side-by-side, and viewed with the aid of prisms or mirrors that deflect the light path to each eye accordingly.

Package A collection of content components that in some combination (either all or a subset) together provide an end-user experience and are intended to be used together [ITU200801].

Packet Protocol Data Unit (PDU) at network layer. In IPv6, a packet that consists of an IPv6 header and an IPv6 payload.

Packet Identifier (PID) A field carried in the header of all MPEG-2 Transport Stream (TS) packets. This is used to identify the TS logical channel to which it belongs [CLA200301]. A 13-bit field carried in the header of TS Packets. This is used to identify the TS Logical Channel to which a TS Packet belongs. The TS Packets forming the parts of a Table Section, PES, or other Payload Unit, must all carry the same PID value. The all ones PID value indicates a Null TS Packet introduced to maintain a constant bit rate of a TS Multiplex. There is no required relationship between the PID values used for TS Logical Channels transmitted using different TS Multiplexes [FAI200501].

Page View (also called Page Impressions) A request to load a single page of a website. A page request can originate from a user clicking on a link on another HTML page pointing to the page in question. Note for comparison that a hit refers to a request for a file from a web server; there may be several hits per page view.

Parallax Apparent change in the position of an object when viewed from different points. The distance between conjugate points. Generally, the differences in a scene when viewed from different points (as, photographically, between the viewfinder and the taking lens of a camera). In stereo, often used to describe the small relative displacements between homologues, more correctly termed deviation [3DA201001].

Parameter Discovery Part of the Neighbors Discovery process that allows nodes to learn configuration parameters, including link MTU, and the default hop limit for outgoing packets.

Parental control An (IPTV) mechanism for deciding the suitability of particular content for a minor on his/her age.

Path Determination Procedure to select the route from the routing table for use in forwarding the datagram.

Path MTU Maximum IPv6 packet size that can be sent without using fragmentation between a source and a destination over an IPv6 network route. The route MTU equates with the smallest link MTU for all links in such route.

Path MTU Discovery Process relating to the use of ICMPv6 “Too Big” message to discover the path MTU.

Path Vector A routing protocols approach that involves the exchange of hop information sequences showing the path to follow in a route. For example, BGP-4 exchanges sequences of numbers of Autonomous Systems (ASs).

Pay Per Click (PPC) Online advertising payment model in which payment is based on qualifying click-throughs. The content publishers get paid a set rate for every click on the advertiser’s material.

Pay Per View (PPV) programming Services that are ordered on-the-fly (or prereserved at some point prior to a broadcast) that requires that the subscriber pay an additional fee to view specific content. As is the case in standard television service, PPV content is broadcast at a set time [NOR200601]. The transmission of the program event is made at the same time to everyone who has ordered it [ITU200801]. A TV service where a particular program event can be bought separately from any package or subscription.

Payload Unit Start Indicator (PUSI) Payload_Unit_Start_Indicator of MPEG-2. A PUSI value of zero indicates that the TS Packet does not carry the start of a new payload. The TS Packet does carry the start of a new payload [CLA200301].

Peer-Entity Authentication The corroboration that a peer entity in an association is the one claimed.

Peer-to-Peer (P2P) network A distributed system in which all nodes have identical responsibilities, and all communication is symmetric. P2P applications rely by design on the interaction between end nodes. The nodes have significant or total independence of central servers. Every participating node acts as both as a server and a client. The idea behind P2P is to (1) bring communication to the edges of the network to avoid overloading central servers and (2) harness the great number of underutilized computers and Internet connections in people’s homes and offices. This is accomplished by turning every user into a rebroadcaster. The content stream is divided into small parts, and each part is distributed to one user’s computer. The participating computers request missing parts from each other and exchange parts to rebuild the whole content. Users can view the content, for example, a movie, as if it were sent directly from the content provider [SJO200801].

Permanent host groups Applications that are part of this type of group have an IP address permanently assigned by the IANA. A permanent group continues to exist even if it has no members. Membership in this type of host group is not permanent: a host (receiver) can join or leave the group as desired. An application can use DNS to obtain the IP address assigned to a permanent host group using the domain mcast.net. The application can determine the permanent group from an address by using a pointer query in the domain 224.in-addr.arpa.

Personal digital recorder (PDR) The same as Personal video recorder (PVR).

Personal mobility Mobility for those scenarios where the end user changes the terminal device used for network access at different locations. The ability of a user to access telecommunication services at any terminal on the basis of a personal identifier and the capability of the network to provide those services delineated in the user's service profile [ITU200801].

Personal video recorder (PVR) An end-user controlled device that records, stores, and plays back multimedia content. PVR is also known as Personal Digital Recorder (PDR) or Digital Video Recorder (DVR).

Phase Alternating Line (PAL) A type of interlaced analog video stream used in the United Kingdom and around the world. It is made up from 625 horizontal lines playing at 25 frames per second (or 50 fields per second).

Phishing Act of acquiring sensitive or personal information such as user-names, date of birth, passwords or credit card details, by masquerading as a trustworthy entity.

PIM Dense Mode (PIM-DM) PIM-DM (RFC 3973, January 2005) is a multicast routing protocol that uses the underlying unicast routing information base to flood multicast datagrams to all multicast routers. Prune messages are used to prevent future messages from propagating to routers without group membership information [ADA200501].

PIM multicast border router (PMBR) In PIM-SM, it is a router that connects the PIM domain to other multicast routing domains. The gateway functions provided by the PMBR address the need to interoperate with other multicast routing protocols [ROD200701].

PIM Source-Specific Multicast (SSM) A multicast protocol where forwarding uses only source-based forwarding trees. IGMPv3 is used to support SSM. SSM mapping is a mapping allows SSM routing to occur without IGMPv3 being present. SSM mapping uses statically configured tables or dynamic Domain Name System discovery of the source address for a SSM channel. PIM-SSM builds trees that are rooted in just one source, offering a more secure and scalable model for a limited amount of applications (mostly broadcasting of content). In SSM, an IP datagram is transmitted by a source S to an SSM destination address G, and receivers can receive this datagram by subscribing to channel (S,G) [CIS200702].

PIM Sparse Mode (PIM-SM) Protocol defined in RFC 2362 that uses a pull mechanism to deliver multicast traffic. Only subnetworks (network segments) that have active receivers that have explicitly requested the information via IGMP joins are forwarded the traffic. PIM-SM makes use of a shared tree to distribute the information to active sources. The PIM-SM protocol shared tree algorithm actually uses a variant of the center-based tree algorithm. PIM-SM makes use of a rendezvous point.

Plaintext Ordinary readable text before being encrypted into ciphertext or after being decrypted.

Plasma Plasma technology is one of the methods used to create flat-panel TVs. The display consists of two transparent glass panels with a thin layer of pixels sandwiched in between. Each pixel is composed of three gas-filled cells or subpixels (one each for the red, green, and blue primary colors). A grid of tiny electrodes applies an electric current to the individual cells, causing the gas to ionize. This ionized gas (plasma) emits a high-frequency UV ray that stimulate the cells' phosphors, causing them to glow, that creates the TV image [KIN200901].

Player controls The controls that operate the features and functions of a hardware or software multimedia player.

Player skin The appearance or look and feel of a multimedia player. Advanced skins may be programmed to increase video player functionality, and may include ads [REE201001].

Playlist Online video content can be classified by content verticals such as news, music, TV shows, movies, sports, games, travel, business, education, and so on.

Point-to-Point Protocol (PPP) Point-to-point network encapsulation method that provides frame delimiters, protocol identification, and integrity services at the bit level.

Point-to-Point Protocol over Ethernet (PPPoE) PPPoE is a network protocol for encapsulating PPP frames in Ethernet frames. It is used mainly with ADSL services. It offers standard PPP features, such as authentication, encryption, and compression.

Pop-up A web page that displays within a new web browser window. Pop-ups are often used for advertisements, but they can be used to display any sort of online content such as video.

Postroll A linear video spot that appears after the video content completes.

P-PPV (Prebooked PPV) PPV services offered in a way that the consumer has to order the service within a given time in advance.

PPT (Pay Per Time) The consumer pays for consuming a media file once within a time limit.

PPV (Pay Per View) Services offered in a way that the consumer will pay for the service on a.

PPV basis PPV services can be offered either as pre-booked (P-PPV) or impulse PPV (I-PPV).

Pragmatic General Multicast (PGM) A reliable multicast transport protocol for applications that require ordered, duplicate-free multicast data delivery. The protocol guarantees that a receiver in a multicast group receives all data packets from direct transmissions or via retransmissions of lost packets. PGM can detect unrecoverable data packet loss.

Prefix The initial bits of an IP address. The number of bits is represented via the prefix-length notation.

Prefix length The number of bits in a prefix.

Prefixes list A collection of prefixes typically used when creating match conditions, for example, for firewall filters.

Prefix-length notation Notation used to represent network prefix length. It uses the “address/prefix length” form, where prefix length indicates the number of bits in the prefix.

Premium VoD VoD where one pays an additional monthly fee for premium content such as recent movies.

Preroll A Linear video spot that appears before the video content plays.

Presentation Time Stamp (PTS) Time stamps are inserted close to the material to which they refer (normally in the PES packet header). They indicate the exact moment where a video frame or an audio frame has to be decoded or presented to the user respectively [FAI200101].

Privacy The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Private key Decryption key is often called private key in public-key systems. A private key is also used for signing a message.

Private section A syntactic structure used for mapping all service information (e.g., an SI table) into Transport Stream (TS) Packets. A table may be divided into a number of sections. All sections of a table must be carried over a single TS logical channel [CLA200301]. A structure constructed in accordance with Table 2-30 of ISO-MPEG-2. The structure may be used to identify private information (i.e., not defined by ISO-MPEG-2) relating to one or more elementary streams, or a specific MPEG-2 program, or the entire Transport Stream. Other Standards bodies, for example, ETSI, ATSC, have defined sets of table structures using the private_section structure. A Private Section is transmitted as a sequence of TS Packets using a TS Logical Channel. A TS Logical Channel may carry sections from more than one set of tables [FAI200501].

Product metadata Metadata related to a media file, including product id, category, protecting services, access modes, usage rights, pricing info, scheduling info, maturity rating, addressing, and so on [CON200701].

Professional Video Hosting Websites that provide online video hosting and sharing for viewing by private and public audiences, similar to consumer video hosting, but at a cost. The video content is of higher quality and the users are given greater control of their videos [REE201001].

Program Television program or multimedia streams.

Program Association Table (PAT) MPEG Signaling Table that lists the PIDs of tables describing each program. The PAT is sent with the well-known PID value of 0x000. [FAI200101].

Program Map Table (PMT) MPEG Signaling Table that defines the set of PIDs associated with a program (e.g., audio and video) [FAI200101].

Program Specific Information (PSI) PSI is used to convey information about services carried in a TS Multiplex. It is carried in one of four specifically identified table section constructs, see also SI Table [FAI200501].

Program stream A PES packet multiplex that carries several elementary streams that were encoded using the same master clock or system time clock.

Progressive download A technique that allows downloading Internet video (or audio) content in such a manner that it can be viewed at the same time that it is being transferred to the user (this does not a streaming server.)

Promotional video Video content aiming to promote a company, brand, product, and so on. Content does not generate direct revenue, but can increase interest in a product and indirectly drive revenue.

Protocol Data Unit (PDU) A unit of information associated with a particular protocol. During transmission the protocol data unit of the N-layer in a protocol suite becomes the payload of the protocol data unit of the N-1 layer.

Protocol Independent Multicast (PIM) A family of multicast routing protocols that can provide one-to-many and many-to-many distribution of data over the Internet. The “protocol-independent” part refers to the fact that PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other traditional routing protocols such as Border Gateway Protocol (BGP) [CIS200702]. A protocol that provides intradomain multicast forwarding for all underlying unicast routing protocols (e.g., Open Shortest Path First [OSPF] or Border Gateway Protocol [BGP]), independent from the intrinsic unicast protocol. Two modes exist: PIM Sparse Mode (PIM SM) and PIM Dense Mode (PIM DM).

Prune list In PIM-SM, the Prune list is the second list of addresses that is included in a Join/Prune message. It indicates those sources or RPs from which downstream receiver(s) wish to prune [EST199801].

Pseudo-header Provisional header that is built to calculate the needed checksum for higher layer protocols. IPv6 uses a new pseudo-header format to calculate UDP, TCP and ICMPv6 checksums.

Pseudo-periodic Event that is repeated at intervals of various lengths. For example, the routes advertisement sent by an IPv6 router is made at intervals that are calculated between a minimum and a maximum [IPV200501].

Pseudowire Emulation of a native service over a Packet Switched Network (PSN). The native service may be ATM, Frame Relay, Ethernet, low-rate TDM, or SONET/SDH, while the PSN may be MPLS, IP (either IPv4 or IPv6), or L2TPv3. The first PW specifications were the Martini draft for ATM PWs, and the TDMoIP draft for transport of E1/T1 over IP. In 2001, the IETF set up the PWE3 Working Group, which was chartered to develop an architecture for service provider edge-to-edge PWs, and service-specific

documents detailing the encapsulation techniques. Other standardization forums, including the ITU and the MFA Forum, are also active in producing standards and implementation agreements for PWs [CIS200702].

Public key Encryption key is often called public key in public-key systems. A public key can also be used for verification of signatures [CON200701].

Public key algorithm An algorithm where the key used for encryption is different from the key used for decryption. Furthermore, the private (decryption) key cannot be calculated from the public (encryption) key [CON200701].

Public key infrastructure (PKI) System that provides public-key encryption and digital signature services.

Public Key Cryptography Standards (PKCS) Set of standards for public-key cryptography from RSA Security Inc. [CON200701].

Pull VoD VoD system that stores content within the operator network. Upon request, the content is streamed to the subscriber. The advantage is that the user can select from a large, centrally stored content library. The disadvantage is that bandwidth must be allocated to each subscriber viewing VoD content [NOR200601].

Pure Streaming The delivery of media content over the internet without needing to first download the media; the content is delivered to the user through a dedicated streaming server.

Push VoD (aka virtual VoD) A system where a selection of movies are broadcast in encrypted format and stored directly on hard disks in the STBs. A consumer can later purchase access to the movies [CON200701].

VoD system that automatically downloads the VoD content to the subscriber's DVR. This download is done during off-peak times or at low priority, eliminating the need for additional bandwidth. The downside is that this makes some of the DVR disk unavailable to the subscriber. As such, this approach is practical only for the latest content that will be viewed by a relatively large number of subscribers [NOR200601]. A TV service where multimedia content is packaged and delivered at the discretion of the service provider to the end user's storage system.

Q-in-Q An enhancement of IEEE 802.1q that allows service providers to create Carrier Ethernet VLANs that will preserve the IEEE 802.1q headers used in the internal enterprise VLAN.

Quadrature Amplitude Modulation (QAM) Modulation technique that has been used in Cable TV broadcasting (as well as in other applications).

Quadrature Phase Shift Keying (QPSK) (aka Quaternary Phase Shift Keying) Modulation technique for satellite broadcasting and other applications.

Quality of Content (QoC) A user's subjective, often unconscious, appraisal of the attractiveness or importance of a piece of content or of a content provider's entire offering. Questions such as these come into play: Is it

entertaining, exciting, educational or helpful? Is it well produced, designed and written? Is it easy to find and access? [SJO200801].

Querier (also known as IGMP Querier) The sender of a Query message—the querier is a multicast router. A multicast router keeps a list of multicast group memberships and a timer for each membership; querier routers periodically send a General MQ, to solicit membership information. Hosts respond to this General MQ to report their membership status for each multicast group.

Random access point A point in the content from where playback can begin.

Rate adaptive DSL (RADSL) A nonstandard version of ADSL. Note that standard ADSL also permits the ADSL modem to adapt speeds of data transfer [DSL200701].

Real-Time Streaming Protocol (RTSP) An IETF protocol that is used for continuous (streaming) of audio and video sessions. It provides the control for playing, stopping, media position control (e.g., fast forward) via bidirectional communication sessions. An application-level protocol for control of the delivery of data with real-time properties. It embodies an extensible framework to enable controlled, on-demand delivery of real-time audio and video data; it uses Transmission Control Protocol or/or the User Data Protocol, depending on function.

Real-Time Transport Control Protocol (RTCP) (also known as RTP Control Protocol) An IETF protocol used for signaling, for example, to identify and coordinate the reporting of streaming flow information (e.g., lost packets). Control protocol that works in conjunction with RTP to control performance and for diagnostic purposes. RTCP control packets are periodically transmitted by each participant in an RTP session to all other participants.

Real-Time Transport Protocol (RTP) An IETF protocol (a set of commands and processes) that is used to add timing and sequence information to each packet to allow the reassembly of packets to reproduce real-time audio and video information. A UDP-based packet format and set of conventions that provides end-to-end network connectivity functions suitable for applications transmitting real-time data, such as audio, video, and so on, over multicast or unicast network services.

RTP provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video. Those services include payload type identification, sequence numbering, time stamping, and delivery monitoring. Applications typically run RTP on top of UDP to make use of its multiplexing and checksum services; both protocols contribute parts of the transport protocol functionality. However, RTP may be used with other suitable underlying network or transport protocols. RTP supports data transfer to multiple destinations using multicast distribution if provided by the underlying network [SCH200301].

Reassembly Procedure to rebuild the original message that had been subject to fragmentation.

Receiver Equipment that processes the signal from a Transport Stream (TS) Multiplex and performs filtering and forwarding of encapsulated PDUs to the network-layer service (or bridging module when operating at the link layer) [FAI200501].

Redirect Procedure included in the Neighbor Discovery mechanisms to inform a host about the IPv6 address of another neighbor that is more appropriate as a next hop destination.

Redundant Array of Inexpensive Disks (RAID) Also known as “Redundant Array of Independent Disks.” It is a storage approach (system) that provides high reliability through redundancy. It combines multiple disk drive components into a logical unit, allowing the data to be distributed across the drives in one of a number of ways called “RAID levels.”

Reference time stamp Time stamp providing the indication of the current time. Reference time stamps are to be found in the PES syntax (ESCR), in the program syntax (SCR), and in the transport packet adaption Program Clock Reference (PCR) field [FAI200101].

Rendezvous point (RP) In Protocol Independent Multicast—Sparse Mode (PIM-SM) each multicast group has a shared-tree via which receivers hear of new sources and new receivers hear of all sources. The RP is the root of this per-group shared tree, called the RP Tree [EST199801]. An RP is the root of a shared multicast distribution tree. Similar to the core router in CBT protocols.

Rendezvous point (RP) operation Protocol Independent Multicast—Sparse Mode (PIM-SM) uses RP, a router with a special function, to support how a multicast source and receiver get connected. When a multicast source wishes to transmit multicast, it just starts sending; it is up to network routers to forward the multicast packets to the RP. In turn, the RP is aware of sources and multicasts in the network.

Replays Refers to the number of times a user requested to see the video ad again (where available).

Repudiation Denial by one of the entities involved in a communication of having participated in all or part of the communication.

Request headers Request headers are used in client requests to communicate information about the client.

Residential Gateway (RG) A logical element that acts as a bridge between the access network and the home network, providing in premise and aggregated security management, provisioning and addressing services for logical elements within a compliant IPTV Network [ITU200801].

Response headers Response headers are used in server responses to communicate information about the server and how it may handle requests.

Retransmission Broadcast Service A service in which content is provided from various broadcasting environments, including, but not limited to, terrestrial, satellite, and cable, and re transmitted into IP network simultaneously or otherwise [ITU200801].

Reverse Direction The direction in which feedback control messages generally flow (e.g., acknowledgments of a forward TCP transfer flow). Data transfer could also happen in this direction (and it is termed “reverse transfer”) [CLA200301].

Reverse Path Forwarding (RPF) In PIM-SM, RPF is used to select the appropriate incoming interface for a multicast route entry. RPF is a multicast forwarding mode in which a data packet is accepted for forwarding only if it is received on an interface used to reach the source in unicast [ADA200501]. The RPF neighbor for an address X is the next-hop router used to forward packets toward X. The RPF interface is the interface to that RPF neighbor. In the common case, this is the next hop used by the unicast routing protocol for sending unicast packets toward X. For example, in cases where unicast and multicast routes are not congruent, it can be different [EST199801].

Rich media Advertisements with which users can interact (as opposed to solely animation) in a web page format. They may appear in ad formats such as banners and buttons, as well as transitionals and various over-the-page units such as floating ads, page take-overs, and tear backs [REE201001].

Rights One or more legal or business entitlements to Use or employ Content, for example, to view, record, and redistribute Content. Referring to the ability to perform a predefined set of utilization functions for a content item; these utilization functions include permissions (e.g., to view/hear, copy, modify, record, excerpt, sample, keep for a certain period, and distribute), restrictions (e.g., play/view/hear for multiple number of times and play/view/hear for certain number of hours), and obligations (e.g., payment and content tracing) that apply to the content and provide the liberty of use as granted to the end user [ITU201001].

Rights Expression The syntactic embodiment of Rights in a concrete form.

Route entry In PIM-SM, a multicast route entry is a state maintained in a router along the distribution tree and is created and updated based on incoming control messages. The route entry may be different from the forwarding entry; the latter is used to forward data packets in real time. Typically, a forwarding entry is not created until data packets arrive, the forwarding entry’s iif and oif list are copied from the route entry, and the forwarding entry may be flushed and recreated at will [EST199801]. A route entry may include such fields as the source address, the group address, the incoming interface from which packets are accepted, the list of outgoing interfaces to which packets are sent, timers, flag bits, and so on.

Router Node that can forward datagrams not specifically addressed to it. In an IPv6 network, a router is also used to send advertisements related to its presence and node configuration information.

Router Advertisement Neighbor Discovery message sent by a router in a pseudo-periodic way or as a Router Solicitation message response. The advertisement includes, at a minimum, a prefix that can be used by the host

to calculate its own unicast IPv6 address following the stateless address configuration procedures.

Router Discovery Neighbor Discovery process that allows a node to discover routers connected to a particular link.

Router's Cache See Destination Cache.

Router-Port Group Management Protocol (RGMP) A protocol that constrains IP multicast on switches that have only routers attached.

Routing Loop Undesirable situation in a network where traffic is relayed over a closed loop and never reaches its destination. The time-to-live field is used to detect such traffic and delete it.

RP-Set In Protocol Independent Multicast—Sparse Mode (PIM-SM), the RP Set is a set of RP addresses constructed by the BSR based on Candidate-RP advertisements received. The RP-Set information is distributed to all PIM routers in the BSR's PIM domain [EST199801].

Satellite Footprint The geographic area of the earth on which a satellite's direct transmissions can be received by a ground-based station or home dish.

Scope For IPv6 addresses, the scope is the portion of the network to which the traffic will be propagated.

Scope ID The scope ID is an identifier for a specific area or scope.

Scope Zone One multicast scope may have several instances, which are known as Scope Zones or zones, for short. For instance, an organization may have multiple sites. Each site might have its own site-local Scope Zone, each of which would be an instance of the site-local Scope. However, a given interface on a given host would only ever be in at most one instance of a given scope. Messages sent by a host in a site-local Scope Zones to an address in the site-local Scope would be limited to the site-local Scope Zone containing the host [HAN199901].

Scrambling Term used as a word for weaker encryption or controlled distortion of an analog signal. The distortion can be removed by possessing and using the descrambling equipment and proper keys [CON200701].

Scrambling algorithm An algorithm used in a scrambling (encryption) or descrambling (decryption) process.

Second generation VDSL (VDSL2) An ITU Recommendation G.993.2 specifies eight profiles that address a range of applications, including up to 100 Mbps symmetric transmission on loops about 100-m long (using a bandwidth of 30 MHz), symmetric bit rates in the 10–30 Mbps range on intermediate length loops (using a bandwidth of 12 MHz), and asymmetric operation with downstream rates in the range of 10–40 Mbps on loops of lengths ranging from 3 to 1 km (using a bandwidth of 8.5 MHz). VDSL2 includes most of the advanced feature from ADSL2. The rate/reach performance of VDSL2 is better than VDSL [DSL200701].

Security label The marking bound to a resource (e.g., a data unit) that names or designates the security attributes of that resource.

Security policy The set of criteria for the provision of security services.

Service Protection Ensuring that an end user can only acquire a service, and, by extension, the content contained therein, that they are entitled to receive.

Session Description Protocol (SDP) A media description specification used for describing multimedia sessions for the purposes of session announcement, session invitation, and session initiation.

Session key A key (normally symmetric) used to encrypt each set of data on a transaction basis. A different session key is used for each communication session. The session key is normally transferred to the receiver using a key exchange mechanism or by encrypting the key under the receiver's public key [CON200701].

Shared tree A tree that uses a single common root placed at some chosen point in the network. This shared root is called a rendezvous point (RP) (also called core or center). All sources in the multicast group use the common shared tree. The notation $(*, G)$ is used to represents the tree. In this case, “*” is a wildcard that means all sources.

Shared tree (also known as the RP tree) In Protocol Independent Multicast—Sparse Mode (PIM-SM), it is a routing tree that supports one or more multicast groups. The RP tree is constructed to connect all receivers to the RP [ROD200701].

Shortest path tree (SPT) In Protocol Independent Multicast—Sparse Mode (PIM-SM) it is the shortest path tree based on the merged shortest paths from all receivers to the multicast source. This is one of the features that distinguishes PIM-SM from CBT. When appropriate, the use of the shortest path tree provides an optimal distribution network that helps to keep the multicast traffic closer to the minimum required to deliver the information to all members. [ROD200701]. In PIM-SM, the SPT is the multicast distribution tree created by the merger of all of the shortest paths that connect receivers to the source (as determined by unicast routing) [EST199801].

SI Table Service Information Table. Any table used to convey information about the service carried in a Transport Stream (TS) Multiplex (e.g., ISO-MPEG). SI tables are carried in MPEG-2 private sections [CLA200301]. A Table may consist of one or more Table Sections; however, all sections of a particular SI Table must be carried over a single TS Logical Channel [FAI200501].

Signaling Tables For a user to receive a particular transport stream, the user must first determine the PID being used, and then filter packets that have a matching PID value. To help the user identify which PID corresponds to which program, a special set of streams, known as Signaling Tables, are transmitted with a description of each program carried within the MPEG-2 Transport Stream [FAI200101].

SimulCrypt A mechanism that facilitates using several service protection systems. A mechanism whereby a single transport stream can contain several Conditional Access Systems (CASs). This enables different CA decoder populations (potentially with different CA systems installed) to receive and correctly decode the same video and audio streams [DVB201101].

Simulcrypt supports the coexistence of two or more CASs operating simultaneously in one system. For example, it can enable existing Cable-CARD options and the evolving Downloadable CAS (DCAS) scenario when legacy receiving devices are already in place. The Simulcrypt specifications resulted from a DVB project. Content security and CASs are typically proprietary systems; while CASs almost invariably use well-known encryption algorithms; the key management, the key distribution, and the handling of entitlement messaging of such system are not published as a matter of course. This represents challenge to the deployment of IPTV devices in a provider's space (e.g., Verizon FiOS in the United States) should such provider desire (or be forced) to deploy STBs from multiple vendors within a cable or IPTV system. While Simulcrypt has not traditionally generated a great deal of interest with the North American MSOs, there have been international CATV deployments of Simulcrypt, and there is evolving interest in the IPTV world. Simulcrypt works by employing a common encryption algorithm for the content streams and further uses a common set of keys (sometimes called control words) for each stream. Each of the two or more CAS must therefore share the control words for each service but can package the control words in a proprietary way for transmission to receiving devices that use that CAS. Control words are typically sent in-band (i.e., in packets that are intermixed with the content stream packets) in Entitlement Control Messages (ECMs). Since one set of ECMs needs to be sent to accommodate each CAS, there is a slight additional overhead that is imposed by Simulcrypt, but because Simulcrypt requires only one copy of the content to be sent, the total overhead is quite minimal (usually on the order of 15–20 Kbps per CAS for the ECMs) [WAS200801].

Single Program Transport Stream (SPTS) An MPEG-2 compliant transport stream that contains a single program. Because it contains only one program, an SPTS is referenced to a single time base. The time base is encoded into the SPTS using MPEG-2 PCRs. An SPTS may contain multiple elementary streams [CON200701].

Site-Level Aggregation Identifier (SLA ID) 16-bit field in the global unicast address that identifies subnetworks. The SLA ID field is used by an individual organization to create its own local addressing hierarchy and to identify subnets.

Site-Local Address Address identified by the 1111 1110 11 (FEC0::/10) prefix. The scope of these addresses is a local site (of an organization).

Site-local addresses are not accessible from other sites, and routers should not direct site-local traffic out of a site. Site-local unicast addresses were deprecated by the IETF in 2003.

Skin A customized graphical appearance (the visual aspect of a graphical user interface [GUI]) applied to certain software and websites for aesthetic reasons or ease of use.

Skin ads Advertisements that appear in a video player skin, that is the graphics surrounding where a video plays.

Smart TV A marketing term for Connected TV; a TV with an Internet-ready connection.

SMIL (Synchronized Multimedia Integration Language) A mark-up language for specifying how and when each clip plays. SMIL files utilize the .smil or .smi extension.

SNDU Subnetwork Data Unit, an IPv4 or IPv6 datagram (or other subnet-work packet, e.g., an arp message or bridged Ethernet frame) [CLA200301]. An encapsulated PDU sent as an MPEG-2 Payload Unit.

Solicited-Node Address IPv6 multicast address used by nodes during the address resolution process. The solicited-node address facilitates efficient querying of network nodes during address resolution. IPv6 uses the Neighbor Solicitation message to perform address resolution. In IPv4, the ARP Request frame is sent to the MAC-level broadcast, disturbing all nodes on the network segment regardless of whether a node is running IPv4. For IPv6, instead of disturbing all IPv6 nodes on the local link by using the local-link scope all-nodes address, the solicited-node multicast address is used as the Neighbor Solicitation message destination. The solicited-node multicast address consists of the prefix FF02::1:FF00:0/104 and the last 24 bits of the IPv6 unicast address that is being resolved [IPV200501].

Source tree A tree that has its root at the multicast source and has branches forming a spanning tree over the network to the receivers. The tree uses the shortest path through the network and hence. A separate shortest path tree (SPT) exists for each individual source sending to each group. The notation of (S,G) is used to describe an SPT, where S is the IP address of the source and G is the multicast group address.

Sourced video Content generated by a third party (typically professional) and will denote the source.

Source-specific multicast (SSM) A form of multicast in which a receiver is required to specify both the network-layer address of the source and the multicast destination address in order to receive the multicast transmission. The 232/8 IPv4 address range is currently allocated for SSM by IANA. In IPv6, the FF3x::/32 range (where “x” is a valid IPv6 multicast scope value) is reserved for SSM semantics, although today SSM allocations are restricted to FF3x::/96 [HOL200601].

Sparse–Dense A Cisco’s alternative to choosing just dense mode or just sparse mode on a router interface. This was necessitated by a change in

the paradigm for forwarding multicast traffic via PIM that became apparent during its development: it turned out that it was more efficient to choose sparse or dense on a per group basis rather than a per router interface basis. Sparse–dense mode facilitates this ability. Network Administrators can also configure “sparse-dense” mode. This configuration option allows individual groups to be run in either sparse or dense mode depending on whether rendezvous point (RP) information is available for that group. If the router learns RP information for a particular group, it will be treated as sparse mode, otherwise that group will be treated as dense [CIS200701].

Sparse Mode (SM) Protocol Independent Multicast (PIM) In Sparse Mode PIM, only network segments with active receivers that have explicitly requested multicast data are forwarded the traffic. PIM SM relies on an explicit joining request before attempting to send multicast data to receivers of a multicast group. In a PIM-SM network, sources must send their traffic to a rendezvous point (RP); this traffic is in turn forwarded to receivers on a shared distribution tree.

Sparse Mode (SM) protocols SM is one mode of operation of a multicast protocol. Protocol Independent Multicast (PIM) SM uses explicit Join/Prune messages and rendezvous points in place of Dense Mode PIM’s and DVMRP’s broadcast and prune mechanism [EST199801]. Multicast routing protocols designed on the assumption that only few routers in the network will need to distribute multicast traffic for each multicast group. SM protocols start out with an empty distribution tree and add drop-off branches only upon explicit requests from receivers to join the distribution. SM protocols are generally used in WAN environments, where bandwidth considerations are important.

Sponsorship Graphics Components that are displayed as very persistent graphics such as with a player surrounding skin. Sponsorship graphics are generally displayed throughout the entirety of the content play. Sometimes the sponsorship graphic remains interactive and will behave like an invitation unit allowing viewers to explore deeper ad units such as the embedded interactive [REE201001].

Spoofing An activity in which a forged (spoofed) source (e.g., a person or computer program) successfully masquerades as a legitimate source by falsifying data and for the purpose of obtaining information and/or obscuring the true source to prevent nonrepudiation for spreading computer viruses.

SSM-aware host A host that knows the Source-specific multicast (SSM) address range and is capable of applying SSM semantics to it [HOL200601].

Standard Definition (SD) The traditional video quality (resolution, aspect ratio) of broadcast television.

Stateless IP/ICMP Translation (SIIT) An IPv6 transition technique that allows IPv4-only hosts to talk to IPv6-only hosts.

Static Routing Utilization of routes configured manually into a router’s routing table.

Static Tunneling Tunneling technique where addresses are manually configured for the tunnel source and destination end points.

STB (set-top box) A device that enables a TV to receive and decode digital/Cable/IPTV television broadcasts.

Storage Infrastructure (typically in the form of appliances) that is used for the permanent or semi-permanent on-line retention of structured (e.g., databases) and unstructured (e.g., business/e-mail files) corporate information. Typically includes (1) a controller that manages incoming and outgoing communications as well as the data steering onto the physical storage medium (e.g., RAIDs [redundant arrays of independent disks], semiconductor memory, etc.); and (2) the physical storage medium itself. The communications mechanism could be a network interface (such as Gigabit Ethernet), a channel interface (such as Small Computer System Interface), or a SAN Interface (i.e., Fibre Channel).

Storage Appliance A storage platform designed to perform a specific task, such as NAS, routers, virtualization, and so on.

Storage Virtualization Software (sub)systems (typically middleware) that abstract the physical and logical storage assets from the host systems.

Stream A flow of a single type of data.

Stream cipher Algorithms that simply produce a keystream to be XORed with the plaintext. The same keystream is reproduced at receiver side for decryption [CON200701].

Streaming An approach where a large media file (audio, video, etc.) is partitioned into smaller pieces so it can be viewed or heard immediately; this forgoes having to wait for the whole file to be downloaded first. The process of playing a file while it is still downloading. Streaming technology, also known as streaming media, lets a user view and hear digitized content—video, sound and animation—as it is being downloaded. Using a World Wide Web browser plug-in, streamed sounds and images can arrive within seconds of a user’s click [CAL200201].

Streaming Media Internet video and/or audio clips that can play directly over the Internet, without needing to be downloaded first onto a computer. Used to view and hear broadcasts, and to interactively play and seek in stored clips [REE201001].

Streaming protocols Commands, processes, and procedures that can be used to select, setup, start the playing, pausing, recording, and tearing down of streaming sessions.

STUB multicast routing A mechanism that allows IGMP messages to be forwarded through a non-PIM enabled router towards a PIM-enabled router.

Stub network A network having only a single OSPF router attached. A network belonging to an OSPF system is either a transit or a stub network, but never both [MOY199401].

Subnet-Router Anycast Address Anycast address that is allocated to router interfaces. Packets sent to the Subnet-Router anycast address will be delivered to one router on the subnet.

Subnetwork One or more links that use the same 64 bit prefix in IPv6.

Subscriber A household or business that legally receives and pays for cable or Pay TV services for its own use (not for retransmission).

Subscription The commercial for-fee acquisition of (protected) services, typically based on a monthly pricing schedule.

Subscription VoD VoD where one pays a monthly fee for access to all content in the standard library.

Superdistribution A paradigm for distributing digital products such videos, music, books, and software, where the products are made publicly available and distributed (although in encrypted form) rather than being sold in brick-and-mortar store or online outlets.

Supplementary content Video, audio, textual, graphical, or other forms of content that can be optionally accessed by the end user and rendered by the terminal.

Symmetric DSL (SDSL) A vendor-proprietary version of symmetric DSL that may include bit-rates to and from the customer ranging of 128 kbps to 2.32 Mbps. SDSL is an umbrella term for a number of supplier-specific implementations over a single copper pair providing variable rates of symmetric service. SDSL uses 2B1Q HDSL run on a single pair with an Ethernet interface to the customer. The industry is expected to quickly move towards the higher performing and standardized G.shdsl technology developed by the ITU with support from T1E1.4 (USA) and ETSI (European Telecommunications Standards Institute) [DSL200701].

Symmetric encryption Type of encryption in which encryption and decryption keys are the same key or can easily be derived from each other. In most cryptographic systems, the decryption key and the encryption keys are identical [CON200701].

Symmetric flavors DSL Symmetrical variations of DSL that include: SDSL, SHDSL, HDSL, HDSL2, and IDSL. The equal speeds make Symmetrical DSLs useful for LAN (local area network) access, video-conferencing, and for locations hosting their own Web sites [DSL200701].

Symmetric High-Speed Digital Subscriber Line (SHDSL) A state-of-the-art, industry standard based on ITU Recommendation G.991.2, also known as G.shdsl (2001). SHDSL achieves 20% better loop-reach than older versions of symmetric DSL, it causes much less crosstalk into other transmission systems in the same cable, and multivendor interoperability is facilitated by the standardization of this technology. SHDSL systems may operate at many bit rates, from 192 Kbps to 5.7 Mbps, thereby maximizing the bit-rate for each customer. G.shdsl specifies operation via one pair of wires, or for operation on longer loops, two pairs of wire may be used. For example, with

two pairs of wire, 1.2 Mbps can be sent over 20,000 ft of 26 AWG wire. SHDSL is best suited to data-only applications that need high upstream bit rates. SHDSL is being deployed primarily for business customers [DSL200701].

Syndicated Video Content sourced from a professional third party; examples may include syndicated television shows, news footage from AP, Reuters, and so on.

Table Section A Payload Unit carrying all or a part of an SI or PSI Table.

Telco Traditional telephone company.

Teredo IPv6 transition technology for use when IPv6/IPv4 hosts are located behind an IPv4 network address translator.

Teredo Client Software on an IPv6/IPv4 host, allowing it to participate in the Teredo transition technology.

Teredo Relay An IPv6 router that can receive traffic from the IPv6 Internet and forward to a Teredo client.

Teredo Server A node that assists in the provision of IPv6 connectivity to Teredo clients.

Terminal Device (TD) A device that typically presents and/or processes the content, such as a personal computer, a computer peripheral, a network appliance, a mobile device, a TV set, a monitor, a VoIP Terminal, or an audiovisual media player [ITU200801].

Terminal Device (TD) protection Ensuring that a terminal device employed by an end user in the reception of a Service can reliably and securely use content while enforcing the rights of use granted for that content, and while physically and electronically protecting the integrity of the terminal device, and the confidentiality of the content and critical security parameters not otherwise protected by encryption or watermarking [ITU200801].

Terminal mobility This is the mobility for those scenarios where the same terminal equipment is roving or is used at different locations. The ability of a terminal to access IPTV services from different locations and while in motion, and the capability of the network to identify and locate that terminal [ITU200801].

Threat A potential violation of security.

Tickers (also known as crawler) A small screen space dedicated to presenting headlines, promotions, and/or other information.

Tiered Storage A process for the assignment of different categories of data to different types of storage media. The purpose is to reduce total storage cost and optimize accessibility. In practice, the assignment of data to particular media tends to be an evolutionary and complex activity. Storage categories may be based on a variety of design/architectural factors, including levels of protection required for the application or organization, performance requirements, and frequency of use. Software exists for automatically

managing the process based on a company-defined policy. Tiered storage generally introduces more vendors into the environment and interoperability is important.

As an example of tiered storage is as follows: Tier 1 data (e.g., mission-critical files) could be effectively stored high-quality Directly Attached Storage (DAS) (but relatively expensive) media, such as double-parity RAIDs (redundant arrays of independent disks). Tier 2 data (e.g., quarterly financial records) could be stored on media affiliated with a storage area network; this media tends to be less expensive than DAS drives, but there may be network latencies associated with the access. Tier 3 data (e.g., e-mail backup files) could be stored on recordable compact discs (CD-Rs) or tapes. (Clearly there could be more than three tiers, but the management of the multiple tiers than becomes fairly complex.)

Another example (in the medical field) is as follows: Real-time medical imaging information may be temporarily stored on DAS disks as a Tier 1, say for a couple of weeks. Recent medical images and patient data may be kept on Fibre Channel (FC) drives (Tier 2) for about a year. After that, less frequently accessed images and patient records are stored on AT Attachment drives (Tier 3) for 18 months or more. Tier 4 consists of a tape library for archiving.

Time shifting A function that allows playback of content after its initial transmission.

Time code An exact time used to identify a specific frame in a clip or production. Measured in hours, minutes, seconds, and frames.

Time-shift TV (TSTV) A service or capability that allows the consumer to watch a TV program that has been time shifted. The time-shift service has two flavors. In a basic flavor, the user can preplan the recording of a scheduled TV program (using a local user-owned device, a local cable-provided device, or a remote network-based device); the user can watch the program any time later, while still being able to pause, rewind, and resume the playout. In a more advanced flavor, the service allows a user to halt a scheduled content service in real time and allows the user to continue watching the program later, by providing buffering for pause, rewind, and resume functions. There may also be advanced playout controls, for example, skipping to chapters, bookmarks, jump to time, and so on [OIP200801].

Time-shifted viewing As enhancements to television service that allows content to be viewed at a time that is more convenient to the subscriber [NOR200601].

Toeing-in The 3D technique of causing the optical axes of twin planar cameras to converge at a distance point equivalent to that of a desired stereo window, such that the borders of the images are coincident at that distance (apart from any keystoneing that results) [3DA201001].

Transient host groups Any group that is not permanent as just described is by definition transient. The group is available for dynamic assignment as

needed. Transient groups cease to exist when the number of members drops to zero.

Transit network A network having two or more OSPF routers attached. These networks can forward data traffic that is neither locally-originated nor locally destined. In OSPF, with the exception of point-to-point networks and virtual links, the neighborhood of each transit network is described by a network links advertisement [MOY199401].

Translation Translation refers to the direct conversion of protocols, for example, between IPv4 and IPv6.

Transport Relay Translator (TRT) Transport Relay Translator partitions the IP layer into two terminated IP legs, one IPv4 and one IPv6. Translation then occurs at the higher layers [IPV200501].

Transport stream (TS) Format for transmission of DVB content. A multiplex of several program streams that are carried in packets. A method of transmission at the MPEG-2 level using TS Packets; it represents level 2 of the ISO/OSI reference model. See also TS logical channel and TS Multiplex [CLA200301].

Transport Stream (TS) Logical Channel A channel identified at the MPEG-2 level; it represents level 2 of the ISO/OSI reference model. All packets sent over a channel carry the same PID value [CLA200301]. Term identifies a channel at the MPEG-2 level. This exists at level 2 of the ISO/OSI reference model. All packets sent over a TS Logical Channel carry the same PID value (this value is unique within a specific TS Multiplex). The term “Stream” is defined in MPEG-2. This describes the content carried by a specific TS Logical Channel. Some PID values are reserved (by MPEG-2) for specific signaling. Other standards (e.g., ATSC and DVB) also reserve specific PID values [FAI200501].

Transport Stream (TS) Multiplex A set of MPEG-2 TS Logical Channels sent over a single lower layer connection. This may be a common physical link (i.e., a transmission at a specified symbol rate, FEC setting, and transmission frequency) or an encapsulation provided by another protocol layer (e.g., Ethernet or RTP over IP). The same TS Logical Channel may be repeated over more than one TS Multiplex (possibly associated with a different PID value), for example, to redistribute the same multicast content to two terrestrial TV transmission cells [FAI200501].

Transport Stream (TS) Packet A fixed-length 188B unit of data sent over an MPEG-2 multiplex (ISO-MPEG); it corresponds to the cells of, for example, ATM networks, and is frequently also referred to as a TS_cell. Each TS Packet carries a 4B header, plus optional overhead, including an adaptation field, encryption details and time stamp information to synchronize a set of Transport Streams [CLA200301].

Tree Information Base (TIB) This is the collection of state maintained by a PIM router and created by receiving PIM messages and IGMP information

from local hosts. The table essentially stores the state of all multicast distribution trees at that router [ADA200501].

Trick mode functionality The ability to pause, rewind, or forward stored content. A TV with trick mode is a TV service with trick mode functionality.

Tunnel In IPv6 transition context, an IPv6 over IPv4 tunnel.

Tunneling techniques Tunneling techniques include the following [GIL200001]:

- *IPv6-over-IPv4 Tunneling*: The technique of encapsulating IPv6 packets within IPv4 so that they can be carried across IPv4 routing infrastructures.
- *Configured Tunneling*: IPv6-over-IPv4 tunneling where the IPv4 tunnel endpoint address is determined by configuration information on the encapsulating node. The tunnels can be either unidirectional or bidirectional. Bidirectional configured tunnels behave as virtual point-to-point links.
- *Automatic Tunneling*: Tunneling where the IPv4 tunnel end point address is automatically determined, generally being embedded in the IPv6 address. Examples include IPv6-compatible addresses and IPv6 6to4 addresses.

TV with trick mode TV service with trick mode functionality.

Twin camera stereo photography Stereo photography using two monoscopic cameras, usually with shutters and other components connected internally or externally using mechanical or electronic means. This photography has advantages that include using common formats and being able to achieve a variable stereo base. Drawbacks include difficulty matching cameras, film and getting normal stereo bases [3DA201001].

Unicast address An address that identifies an IPv6 interface and allows network layer point-to-point communication. It identifies a single interface within the scope of the unicast address type. An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address. The following list shows the types of IPv6 unicast addresses:

- Aggregatable global unicast addresses
- Link-local addresses
- Site-local addresses
- Special addresses, including unspecified and loopback addresses
- Compatibility addresses, including 6to4 addresses

Unicast Environment Environment where one system communicates directly to another system.

Unidirectional link (UDL) A one-way transmission IP over DVB link, for example, a broadcast satellite link.

Unspecified Address 0:0:0:0:0:0:0 or ::—used to show the absence of any address, equivalent to the IPv4 address—0.0.0.0.

Upstream Interface Interface toward the source of the datagram. Also known as the RPF Interface [ADA200501].

Upstream interface (or router) In CBT, an “upstream” interface (or router) is one that is on the path towards the group’s core router with respect to this interface (or router) [BAL199701].

User Privacy Protection Ensuring that information considered to be private (or confidential) by an end user be maintained in confidence, while remaining subject to mandatory disclosure due to legal processes [ITU200801].

User-Generated Video (UGV) Content created by the public at large and directly loaded to a site, such as YouTube, Facebook, MySpace, and so on. Video content created by the user community and distributed over the web with social networks.

Very high bit rate DSL (VDSL) A standard for up to 26 Mbps, over distances up to 50 m on short loops, such as from fiber to the curb. In most cases, VDSL lines will be served from neighborhood cabinets that link to a Central Office via optical fiber. VDSL has been introduced in some market to deliver video services over existing phone lines. VDSL can also be configured in symmetric mode [DSL200701].

Video ad An ad in which the advertising message is delivered through video.

Video ad experience Term used to describe where the source of the video advertising experience is coming from. Ad experiences include, but are not limited to: “in-stream,” “in-banner,” and “in-text”.

Video Application Program Interface (Video API) A documented (software) interface that allows a program to communicate with another program in a standardized manner.

Video bookmarking services Services that allow users to manage bookmarks to multiple videos across the Internet.

Video buffering Activity that occurs when a streaming video player stores portions of a streaming video file to local storage for playback shortly thereafter (usually a few seconds for real-time video, but for a longer period of time for offline downloads of content such as an “online rented movie”).

Video Compression The process through which a video file is reduced in size for storing and streaming either on traditional TV systems, IPTV, or IBTV. Performing a digital compression process on a video signal. Compression techniques are used to enable efficient transmission of video signals.

Video e-commerce Using a video as the means for creating an electronic monetary transaction, for example, through the use of links in/on the video or the video player that take the user to a transaction website or that start the transaction process directly from the player [REE201001].

Video format The file type of a video file. Some of the most well-known formats for digital video include .avi (Microsoft), .mov (Quicktime), .wmv (Windows), and .flv (Flash).

Video On Demand (VoD) (also known as Content On Demand) Services offered by cable companies that allow a user to select specified content;

usually entails a fee, but increasingly some content is available for free. Service that allows the subscriber to view content whenever he/she wants, from a library of stored content. VoD supports a complete set of VCR-like functions, including rewind, pause and fast-forward [NOR200601]. A service in which the subscriber can view video content whenever desired. The operating assumption is that the content is stored on the provider's VoD server. Subscriber accesses the movie from a library directory, which may include search engine that accesses movie description and rating. Subscribers typically have the ability to pause, play, rewind, fast forward the content, or even stop viewing it and return to it at a later time when using this service [ITU200801].

Video player Media player used for the playback of digital videos from media including optical discs (DVD, Blu-ray Disc), and computer files.

Video Publishing and Management Platform A software system used to create, edit, host, play, manage, organize, publish, stream, and distribute online video according to consistent rules. Video publishing and management platforms are frequently used for storing, controlling, versioning, publishing, and distributing video assets of all types. The digital video content managed may include videos, pictures, ads, metadata, and other Web content [REE201001].

Video Search Engine Optimization (Video SEO) The process of maximizing the indexability and ranking of a video within search engines.

Video search engines Services that seek to index video content from multiple sources and allow users to search across all content.

Video size The amount of hard drive storage space a video file takes up. Typically expressed in kilobytes (1000 bytes), megabytes (1000 KB), gigabytes (1000 MB), and terabytes (1000 GB).

Viral videos Video content that has become popular through online sharing via email, forums, blogs and other web sites.

Virtual infrastructure An infrastructure where there is a dynamic mapping of physical resources to functional service requests, such that the entity requiring service is oblivious to the specific nature of the actual hardware supporting the underlying service.

Virtual private LAN service (VPLS) Virtual private LAN service (VPLS) is a way to provide Ethernet-based multipoint-to-multipoint communication over IP/MPLS networks. It allows geographically dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires. The technologies that can be used as pseudowire can be Ethernet over MPLS, L2TPv3, or even GRE. There are two IETF standards describing VPLS establishment. VPLS requires a full mesh of LSPs, which has the n^2 scaling problem. H-VPLS helps solve this problem by dividing the virtual LAN into separate hierarchies [CIS200702].

Virtualization The abstraction of server, storage, and network resources in order to make them available dynamically for sharing by IT services, both

internal to and external to an organization. In combination with other server, storage, and networking capabilities, virtualization offers customers the opportunity to build more efficient IT infrastructures. Virtualization is seen by some as a step on the road to utility computing. An approach that allows several operating systems to run simultaneously on one (large) computer (e.g., IBM's z/VM operating system lets multiple instances of Linux coexist on the same mainframe computer). It is the practice of making resources from diverse devices accessible to a user as if they were a single, larger, homogenous, appear-to-be-locally available resource. Virtualization depends on being able to dynamically shift resources across platforms to match computing demands with available resources: the computing environment can become dynamic, enabling autonomic shifting applications between servers to match demand.

Visits A series of requests to a website from the same uniquely identified visitors with a set timeout. A visit may contain multiple hits and page views.

Vlog—(Video blog) A video-enabled blog; users can post video entries that are presented in reverse chronological order. A typical vlog entry combines an embedded video or video link, along with supporting text and images [REE201001].

VoD Trick Modes Download and streaming VoD systems provide the user with a large subset of VCR functionality, including pause, fast forward, fast rewind, slow forward, slow rewind, jump to previous/future frame, and so on. These functions are usually referred to as “trick modes” [ITU200801].

Watermarking Process that lets one add hidden information in data files to prove the origin of the files.

Web cache A Web cache fills requests from the Web server, stores the requested information locally, and sends the information to the client. The next time the Web cache gets a request for the same information, it simply returns the locally cached data instead of searching over the Internet, thus reducing Internet traffic and response time [SUN201001].

Web Services (WSs) Web Services provide standard infrastructure for data exchange between two different distributed applications.

Web television (Web TV) A genre of digital entertainment distinct from traditional television. The content is created specifically for first viewing on the Internet (via broadband access and/or on mobile networks). Web television shows, or Web series, are episodic shorts (typically 2–9 minutes per episode). Some notable series include *Dr. Horrible's Sing-Along Blog*, *The Guild*, and *Prom Queen*. Web television networks include: The WB.com, MySpace, YouTube, Blip.tv, and Crackle (however, some of these also post TV-originated material). (Press time web television production companies included but are not limited to Next New Networks, Vuguru, Revision3, Deca, Generate LA-NY, and Take180.)

Webcast A noninteractive, live broadcast over the web. An online distribution of audio and/or video to multiple viewers or listeners at the same time.

Widget A stand-alone application that can be embedded into a (third party) website by a(ny) user on a page where they have rights of authorship (for example, a profile on a social media site). A widget is a standardized on-screen representation of a control that may be manipulated by the user. Scroll bars, buttons, and text boxes are all examples of widgets. For example, a “Search Widget” could be added on a personal website by copying and pasting the embed code into the home page (or some similar action on a Facebook profile). Widgets allow users to turn personal content into dynamic web apps. Traditional web widgets provided functions such as advertising banners and link counters.

Wi-Fi Wi-Fi is a brand originally licensed by the Wi-Fi Alliance to describe the underlying technology of wireless local area networks (WLANs) based on the IEEE 802.11 specifications. It was developed to be used for mobile computing devices, such as laptops, in Local Area Networks (LANs), but is now increasingly used for more services, including the Internet and Voice Over IP (VoIP) phone access, gaming, and basic connectivity of consumer electronics such as televisions and DVD players, or digital cameras [CIS200702].

Wildcard (WC) multicast route entry In PIM-SM, wildcard multicast route entries are those entries that may be used to forward packets for any source sending to the specified group. Wildcard bots in the join list of a Join/Prune message represent either a (*,G) or (*,*,RP) join; in the prune list, they represent a (*,G) prune [EST199801].

WiMAX WiMAX is defined as Worldwide Interoperability for Microwave Access by the WiMAX Forum, formed in June 2001 to promote conformance and interoperability of the IEEE 802.16 standard. The WiMAX Forum describes WiMAX as “a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL.”

Zone name A human readable name for a Scope Zone. An ISO 10646 character string with an RFC 1766 language tag. One zone may have several zone names, each in a different language. For instance, a zone for use within IBM’s locations in Switzerland might have the names “IBM Suisse,” “IBM Switzerland,” “IBM Schweiz,” and “IBM Svizzera” with language tags “fr,” “en,” “de,” and “it” [HAN199901].

REFERENCES

- [3DA201001] The 3D@Home Consortium, <http://www.3dathome.org/>.
- [ADA200501] A. Adams, J. Nicholas, W. Siadak, “Protocol Independent Multicast—Dense Mode (PIM-DM): Protocol specification (revised),” RFC 3973, January 2005.
- [BAL199301] T. Ballardie, P. Francis, J. Crowcroft, “Core Based Trees (CBT): An architecture for scalable inter-domain multicast routing,” ACM SIGCOMM’93—Ithaca, NY, 1993.

- [BAL199701] A. Ballardie, “Core Based Trees (CBT Version 2) multicast routing—protocol specification,” RFC 2189, September 1997.
- [BAL199702] A. Ballardie, “Core Based Trees (CBT) multicast routing architecture,” RFC 2201, September 1997.
- [CAL200201] California Software Labs, “Basic streaming technology and RTSP protocol—A technical report,” 2002, California Software Labs, 6800 Koll Center Parkway, Suite 100 Pleasanton CA 94566, USA.
- [CHR200601] M. Christensen, K. Kimball, F. Solensky, “Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) snooping switches,” RFC 4541, May 2006.
- [CIS200701] Cisco Systems, “Internet Protocol (IP) multicast technology overview,” 2007, Cisco Systems, Inc., 170 West Tasman Dr., San Jose, CA 95134, USA.
- [CIS200702] Cisco, “IP NGN carrier ethernet design: Powering the connected Life in the zettabyte era,” Cisco Whitepaper, 2007, Cisco Systems, Inc., 170 West Tasman Dr., San Jose, CA 95134, USA.
- [CLA200301] H. D. Clausen, B. Collini-Nocker, et al., “Simple Encapsulation for transmission of IP datagrams over MPEG-2/DVB networks,” Internet Engineering Task Force, draft-unisal-ipdvb-enc-00.txt, May 2003.
- [CON200701] Conax AS, “Glossary of terms,” Fred Olsensgate 6, NO-0152 Oslo, Norway, 2007.
- [DSL200701] DSL Forum, “DSL forum,” 48377 Fremont Blvd, Suite 117, Fremont, CA 94538, 2007, <http://www.dslforum.org>.
- [DVB201101] DVB, “DVB project materials,” DVB Organization, 2011, <http://www.dvb.org>.
- [EST199801] D. Estrin, D. Farinacci, et al., “Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol specification,” RFC 2362, June 1998.
- [FAI200101] G. Fairhurst, “MPEG-2 digital video, background to digital video,” University of Aberdeen, King’s College, Dept. of Engineering, Aberdeen, AB24 3FX, UK, January 2001, <http://www.erg.abdn.ac.uk/research/future-net/digital-video/mpeg2-trans.html>.
- [FAI200501] G. Fairhurst, M.-J. Montpetit, “Address resolution for IP datagrams over MPEG-2 networks, internet draft draft-ietf-ipdvb-ar-00.txt, IETF ipdvb,” June 2005.
- [FCO201101] FCoE (Fibre Channel over Ethernet) online site. 2011, <http://www.fcoe.com>.
- [GIL200001] R. Gilligan, E. Nordmark, “Transition mechanisms for IPv6 hosts and routers,” RFC 2893, August 2000.
- [HAN199901] S. Hanna, B. Patel, M. Shah, “Multicast Address Dynamic Client Allocation Protocol (MADCAP),” RFC 2730, December 1999.
- [HOL200601] H. Holbrook, B. Cain, B. Haberman, “Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for source-specific multicast,” RFC4604, August 2006.
- [IPV200501] IPv6 Portal, <http://www.ipv6tf.org/meet/faqs.php>.
- [ITU200801] M. Johnson, “ITU-T IPTV Focus Group Proceedings, ITU-T,” 2008.
- [ITU201001] International Telecommunication Union, “ITU Interop Event Highlights IPTV Interoperability—Future of Television Will Rest on Stable Global Standards, Say Experts”, Press Release, July 27, 2010. International Telecommunication Union, Telecommunication Standardization Bureau, Place des Nations, CH-1211 Geneva 20.

- [ITU201101] International Telecommunication Union, ITU-T Technical Paper “HSTP—IPTV-PITD delivery and control protocols handled by IPTV terminal devices,” SERIES H: Audiovisual And Multimedia Systems Infrastructure of audiovisual services—Communication procedures, Telecommunication Standardization Sector Of ITU, March 25, 2011.
- [KIN200901] S. Kindig, “TV and HDTV glossary,” December 2, 2009, Crutchfield, 1 Crutchfield Park, Charlottesville, VA 22911.
- [MOY199401] J. Moy, “Multicast extensions to OSPF,” RFC 1584, March 1994.
- [MSD200401] Microsoft Corporation, “MSDN Library, internet protocol,” 2004, <http://msdn.microsoft.com>.
- [NOR200601] NORTEL, “Position paper: Introduction to IPTV,” 2006, 35 Davis Drive Research Triangle Park, NC 27709, USA.
- [OHA201101] J. O’Halloran, “Online film market to be worth \$4.44bn by 2017,” Rapid TV News (online magazine), April 26, 2011. <http://www.rapidtvnews.com>.
- [OHA201102] J. O’Halloran, “Apple, Sony and Microsoft spur non-U.S. online video growth,” Rapid TV News (online magazine), July 12, 2011. <http://www.rapidtvnews.com>.
- [OIP200801] Open IPTV Forum (OIPF), “Services and functions for release 2 [V1.0]-[2008-10-20],” 2008, Open IPTV Forum, 650 Route des Lucioles—Sophia Antipolis, Valbonne, France.
- [RAD200001] P. Radoslavov, D. Estrin, et al., “The Multicast Address-Set Claim (MASC) protocol,” RFC2909, September 2000.
- [RAD201001] A. Radding, “SAN of the future,” Essential Guide To Storage Networking, Storage Media Group/SearchStorage.com Whitepaper, March 2010.
- [REE201001] ReelSEO.com, “Online video dictionary—Glossary of online video terms, The Online Video Marketer’s Guide,” 2010.
- [ROD200701] M. Rodbell, “Protocol independent multicast—sparse mode, CMP COMMs design,” an EE Times Community, 03 June 2007, <http://www.commsdesign.com/main/9811/9811standards.htm>.
- [SCH200301] H. Schulzrinne, S. Casner, et al., “RTP: A transport protocol for real-time applications,” IETF Request for Comments, July 2003.
- [SJO200801] D. Sjöberg, “Content delivery networks: Ensuring quality of experience in streaming media applications,” TeliaSonera International Carrier, CDN white paper, August 14, 2008.
- [SUN201001] SunStar, “Storage glossary of terms,” 900 West Hyde Park Blvd. Inglewood, CA 90302, 2010.
- [VID200401] R. Vida, L. Costa, Eds. “Multicast listener discovery Version 2 (MLDv2) for IPv6,” RFC 3810, June 2004.
- [WAI198801] D. Waitzman, C. Partridge, S. Deering, “Distance vector multicast routing protocol,” RFC 1075, November 1988.
- [WAS200801] T. Wasilewski, “Simulcrypt: May they live happily ever after,” May 30, 2008, Cisco Blog SP360: Service Provider. Cisco Systems, Inc., 170 West Tasman Dr., San Jose, CA 95134 USA.
- [WEL200101] P. J. Welcher, “The protocols of IP multicast,” NetCraftsmen White Paper, Chesapeake NetCraftsmen, LLC., 1290 Bay Dale Drive—Suite #312, Arnold, MD 21012, 2001, <http://www.netcraftsmen.net/welcher/papers/multicast01.html>.

INDEX

- (*,*RP) route entry 324
- (*G) route entry 324
- AAA 328
- AAAA (also known as Quad A) 77
- AAC audio 249
- Abbreviated form of address 54
- Access Control 326
- Access Network (IPTV) 185
- Access, web pages 175
- Accessibility 326
- Acquisition 326
- Adaptation Field 326
- Addition of media to existing presentation 245
- Address 326
- Address autoconfiguration 327
- Address maximum valid time 327
- Address resolution 327
- Administratively scoped addresses 354
- Ad overlays 31, 326
- ADTS 250
- Advanced encryption standard (AES) 327
- Advanced streaming format (ASF) 327
- Advanced Television Systems Committee (ATSC) 327
- Advertising services 144
- AES 327
- AF 70
- AFC 327
- Aggregatable global unicast address 327
- Aggregate all-Internet home viewing growth rate 42
- Aggregate all-TV home viewing growth rate 42
- AH 48, 64–65
- A la carte VoD 326
- Alliances for Telecommunications Industry Solutions (ATIS) 148
- Amazon Prime 241
- Amazon's Kindle tablet 259
- Amazon's Video on Demand 23
- Android 248
- Annual global IP traffic 300
- Anycast address 327
- Anycast transmission 51, 53
- API 207
- Apple HTTP Live Streaming (HLS) 248–249
- Apple HTTP Live Streaming file format 251
- Apple iTunes 10–12, 316
- Apple's iCloud 259
- Apple TV, TV 2 26, 248, 308, 327
- Application client functions 196
- Application convergence 296
- Application event handling for IPTV 214, 238
- Application function group 165
- Application functions for IPTV multicast 183
- Application profile 184
- Application Programming Interface (API) 207
- Array 327
- AS 46, 328
- ASF 327
- Aspect ratio 327

Linear and Nonlinear Video and TV Applications: Using IPv6 and IPv6 Multicast,
First Edition. Daniel Minoli.

© 2012 John Wiley & Sons, Inc. Published 2012 by John Wiley & Sons, Inc.

- Assured Forwarding (AF) 70
 Asymmetric encryption
 algorithm 327–328
 Asynchronous video delivery 328
 ATIS 148
 ATIS IIF Committees 224
 ATIS IIF standards 225
 ATIS IPTV Interoperability Forum (IIF) 220
 ATSC 327
 Attempt Address 328
 Audience measurement
 information 145, 202
 Audio Data Transport Stream (ADTS) 250
 Audio description 142, 328
 Audio Video Interleave (AVI) 328
 Authentication 185, 328
 Authentication, Authorization, and Accounting (AAA) 328
 Authentication header (AH) 48, 64
 Authorization 328
 Autoconfiguration 47, 61
 Automatic Tunneling of IPv6 over IPv4 71–72, 328
 Autonomous System (AS) numbers 46, 328
 AVI 328
- Bandwidth 328
 Bandwidth advantage of IP
 multicast 97
 Bidirectional (B) pictures 169
 Blu-ray discs 9
 Bootstrap router (BSR) 121, 328
 Boxee 316
 BPON 2, 75, 278, 281
 Brand awareness 329
 BRICA countries (Brazil, Russia, India, China, and Africa) 35
 Broadband Internet access 269
 Broadcast (IP) 51
 Broadband PON (BPON) 275
 Broadband video commercial 329
 Broadcast environment 329
 Broadcasters 9
 Broadcasting satellite service (BSS) 329
 Broadcast interface 329
- Broadcast TV 4, 21, 329
 BSR 121, 328
 BSS 329
 Buffering 329
 Bug 329
 Bumper Ad 329
 Bump in the Application (BIA) 329
 Bump in the Stack (BIS) 329
- CA 148, 161, 331–332
 CableCARD 329
 Cable TV fiber networks 269
 Cable TV providers 16
 CAC 186
 Call Detail Record (CDR) 187
 Call Session Control Functions (CSCFs) 231
 Candidate BSR (CBSR) 329
 Candidate-BSR (C-BSR) 330
 Candidate RP (C-RP) 329–330
 Captions 330
 CAS 148, 161, 331, 332
 Cascaded fabric 290
 Catch-up TV 3
 CBR 168
 CC 142
 CDN 149, 240, 252, 332
 CDN active network approach 253
 CDN approaches, satellite distribution 254–255
 CDN overlay approach 253–254
 CDR 187
 Center-based trees 330
 Certificate 330
 Channel 330
 Channel access control 187
 Channel changing 330
 Channel preview capability 187
 Channel zapping 330
 Cisco Group Management Protocol (CGMP) 330
 Clear flag 129
 Clickable video 330
 Clicker 319
 Click-through 330
 Client PVR (cPVR) 25, 143
 Closed captions (CC) 142
 Cloud computing 257, 330
 Cloud data storage 292

- CoD 141, 147, 152, 332
 Codec 330
 CoD metadata 205
 Colon hexadecimal notation 330–331
 Comcast 77
 Commerce services 145
 Companion Ad 331
 Comparison of IPv4 and IPv6 headers 60
 Compatibility addresses 331
 Compressed video signal 331
 Compressing zeros 331
 Conditional Access (CA) 148, 156, 331–332
 Conditional Access System (CAS) 148, 161, 331–332
 Conditional Access Table (CAT) 331
 Confidentiality 332
 Configured tunneling 72
 Configured tunneling of IPv6 over IPv4 71
 Connected TV (CTV) 4, 6, 16–17, 241, 309, 332
 Connection Admission Control (CAC) 186
 Connection and session management 197
 Connectionless datagram protocol 56
 Constant bit rate (CBR) 168
 Consumer distribution tier 275
 Consumer video hosting 332
 Content assets, risks, and threats 177
 Content delivery 185, 187
 Content delivery client functions 192–193
 Content delivery functions for IPTV Multicast 184
 Content Delivery Network (CDN) 149, 240, 252, 332
 Content distribution 185
 Content distribution function group 165
 Content guide 153
 Content on demand (CoD) 141, 147, 332
 Content preparation 184
 Content protection 332
 Content provider 209, 332
 Content provider functions for IPTV multicast 186
 Content Provider/Aggregator (CP) 157
 Content provisioning 204, 208
 Content receivers 157
 Content tracing 332
 Context identifier (CID) 69
 Contextual ads 332
 Control and signaling 186
 Control word (CW) 332
 Converged services 332
 Core-based tree 333
 Core-based tree (CBT) multicasting 333
 Core-edge fabric 291
 Core network 262
 Core router (or just “core”) 333
 Correspondent Node 333
 Cost Per Action (CPA) 333
 Cost Per Click (CPC) 333
 Cost Per Thousand Impressions (CPM) 333
 CPA 333
 CPC 333
 CPM 333
 cPVR 25, 143
 CTV 4, 6, 16–17, 241, 309, 332
 Cue Point 333
 Current state reports 134
 DAS 288
 Data distribution scheme with native IP multicast 182
 Data distribution scheme with replicated unicast 182
 Data Encryption Standard (DES) 334
 Datagram 334
 Data origin authentication 334
 DBS 16, 149
 DECE (Digital Entertainment Content Ecosystem) 259
 Decoding 334
 Decoding Time Stamp (DTS) 334
 Default route 334
 Default routers list 334
 Delaying listener 128
 Delivery Network Gateway (DNG) 201
 Delivery Network Gateway Functions (DNGF) 201, 334
 Denial of Service (DoS) 334

- Dense-Mode (DM) protocols 334
 Dense wavelength division multiplexing (DWDM) 11
 Designated router (DR) 101, 121, 334–335
 Destination cache 335
 Destination Options Header 64
 Destinations for online content; online destination 335
 DHCP 61, 339
 DiffServ 173
 Digital Cosine Transform (DCT) 168
 Digital Entertainment Content Ecosystem (DECE) 259
 Digital Rights Management (DRM) 161, 335
 Digital signature 335
 Digital Storage Management Command and Control (DSM-CC) 335
 Digital Subscriber Line Access Multiplexer (DSLAM) 335
 Digital Subscriber Line (DSL) 271, 275, 335
 Digital Subscriber Line (xDSL) access 162
 Digital television (DTV) 335–336
 Digital Video Broadcasting (DVB) 336
 Digital Video Broadcast–Handheld (DVB-H) 336
 Digital Video Recorder (DVR) 24, 336
 Direct-Attached Storage (DAS) 288
 Direct Broadcast Satellite (DBS) 16, 149
 Direct to Home (DTH) satellite services 35, 311, 336
 DirectTV 29
 Dish Network 309
 Display 336
 Distance Vector Multicast Routing Protocol (DVMRP) 336–337
 Distance vector routing protocol 337
 Distributed content service 140
 Distributed PVR (dPVR) 25, 144
 DM protocols 334
 DNG 201
 DNGF 201, 334
 Document Object Model (DOM) 217
 Domain Name System (DNS) 337
 DoS 334
 Double colon notation 337
 Double Stimulus Continuous Quality Scale (DSCQS) 166
 Download of data 175
 Download of video content 175
 Download services 237
 Download-to-own (DTO) 12–13, 337
 dPVR 25, 144
 DR 101, 121, 334–335
 DRM Rights 184
 DSLAM 335
 DTH 16, 30, 35, 311, 336
 DTH households 7
 DTO 12–13, 337
 DTV 335–336
 Dual IP layer (also known as dual stack) 71
 Dual-Stack approach 77
 Dual Stack Architecture 337
 DVB 336
 DVB-C2 23, 338
 DVB-H 336
 DVB Project 337
 DVB-S2 23, 338–339
 DVB-T2 23, 339
 DVDs 9, 11, 24
 DVR 24, 336
 DVR playback 24, 43
 DWDM 11
 Dynamic Host Configuration Protocol (DHCP) 339
 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) 61
 Dynamic host registration 98, 339
 ECG 140, 151, 210, 339
 ECMAScript 217
 Effective Cost Per Thousand Impressions (eCPM) 339
 EH 341
 E-LAN 268
 Electronic Content Guide (ECG) 140, 151, 339
 Electronic Program Guide (EPG) 140, 151, 339
 Electronic sell-thru (EST) 12–13, 339
 Electronic Service Guide (ESG) 140, 340
 Elementary stream (ES) 340
 E-Line 267

- Embed 340
- Embedded rendezvous point (RP) 122
- Emergency Alert System (EAS) 142, 148, 340
- Encapsulating Security Payload (ESP) 64–65, 340
- Encapsulator 340
- Encoder 340
- Encryption 340
- End-User Function Group 165
- End-User Functions for IPTV
 - Multicast 183
- Entitlement 340
- Entitlement Control Messages (ECMs) 340
- Entitlement Management Messages (EMMs) 340
- EPG 140, 151, 210, 212, 339
- EPON 278
- ES 340
- ESG 140, 210, 340
- ESP 64–65
- EST 12–13, 339
- Ethernet over an MPLS (EoMPLS) 267, 340
- Ethernet Private Line (EPL) 267
- Ethernet Virtual Private Line (EVPL) 268
- E-Tree 268
- EUI-64 address 341
- European Telecommunications Standards Institute (ETSI) 341
- Event trackers 341
- Excess Information Rate (EIR) 341
- Exchanging messages between querier and listening nodes 133
- Expedited Forwarding (EF) 70
- Extended Unique Identifier (EUI) 341
- Extension headers (EH) 341
- FC cabling and connectors 290
- FCAL 283, 341
- FC core 290
- FC edge (or Fabric or SAN) 290
- FC fabrics 291
- FC HBAs 290
- FCoE 283, 289, 341
- FC routers, bridges, and gateways 290
- FC servers 290
- FC storage devices 290
- FC switches 290
- FFW (Fast Forward) Delay 171
- Fiber/IPTV/telco households 7
- Fiber to the Business (FTTB) 275
- Fiber to the Curb (FTTC) 272, 275
- Fiber to the Home (FTTH) 275, 280
- Fiber to the Neighborhood 275
- Fiber to the Node (FTTN) 272
- Fiber to the Premises (FTTP) 272, 275
- Fiber to the Subscriber (FTTS) 275
- Fibre Channel (FC) 282–283, 288, 341
- Fibre Channel Arbitrated Loop (FCAL) 283, 341
- Fibre Channel over Ethernet (FCoE) 283, 289, 341
- Fibre Channel over IP (FCIP) 284, 342
- Fibre Channel SCSI 284, 342
- File delivery metadata 206
- File format for Apple HTTP live streaming 251
- File formats 342
- Fixed Satellite Service (FSS) 342–343
- Flow 343
- Format prefix 343
- 40GbE 266
- Forward direction 343
- Forward error correction (FEC) 167, 343
- Forward predicted (P) pictures 169
- 400GbE 264
- Fragment 343
- Fragmentation 343
- Fragmentation Header 64, 76, 355
- Frame rate 343
- Free On-Demand VoD 343
- Free-to-air (FTA) 162
- FTTH technologies 27, 275, 277, 280
- Full Rate Asymmetrical DSL (ADSL) 344
- Full screen views 344
- Fully-qualified domain name (FQDN) 344
- Functional architecture of IPTV
 - terminal device 191
- Gaming consoles 16
- GARP Multicast Registration Protocol (GMRP) 344

- General queries 134
- Generic Encapsulation Method (GEM) 280
- GE-PON 278, 280–281
- Gigabit Ethernet technology 26, 266
- Gigabit PON (GPON) 275, 277, 278, 280–281
- Ginga-NCL for IPTV 216
- G-lite ADSL 344
- GLOB addressing 344–345
- Global address 345
- Global consumer IP traffic 303
- Globally scoped addresses 106
- Google TV 26–28
- GPON 275, 277–278, 280–281
- Grid computing 257
- Group identifier 345
- Group of Pictures (GOP) 668, 345
- Growth of IP Traffic 263

- HC for IPv6 68
- HC techniques 68
- HDSL (high data rate DSL) 345
- HDSL2 (2nd generation HDSL) 345
- HDSL4 345
- HE-AAC 250
- Header compression schemes 66
- Hierarchical Storage Management (HSM) 284, 345
- Hierarchical Virtual Private LAN Service (H-VPLS) 267
- High Definition (HD) 170, 345
- Higher level checksum 345
- Higher level protocol 345
- High-level specification of metadata for IPTV services 214
- High-throughput IP 267
- Hit 345
- HLS 248–249, 241, 251
- Home gateway initiative (HGI) 34
- Home Network (HN) 154, 346
- Home network terminal device (HN-TD) 202
- Homes passed 346
- Home theater PCs (HTPCs) 3, 17, 346
- Hop-By-Hop option header 64, 346
- Host 346
- Host-to-host tunnel 346
- Host-to-router tunnel 346

- Hot spot 346
- HTPCs 3, 16–17, 346
- HTTP dynamic streaming 241
- HTTP Flash progressive download 252
- HTTP Live Streaming (HLS) 248–249, 241, 251
- HTTP streaming 346
- Hulu 8, 16, 311, 316
- Hybrid-based delivery mechanism 33
- Hybrid Fiber Coax (HFC) 275
- Hybrid terminal device 346
- Hyperlinked video 346
- Hypertext Transfer Protocol (HTTP) 242, 346

- IaaS (Infrastructure-as-a-Service) 258
- I (intracoded) pictures 169
- IBTV 4, 35, 95, 139, 240, 260
- ICMPv6 message types 123
- ICMPv6 346
- Idle listener 128
- IEEE 802.1 267
- IEEE 802.1ad 346
- IEEE 802.1ah 346–347
- IEEE 802.1q 347
- IGMP 99, 101, 107, 159
- IGMP Join message 101
- IGMP Snooping 347
- IGMP Snooping Switches 347
- IGMP version 3 (IGMPv3) 109, 117
- IGMP v2 message format 108
- IGMPv3 membership query message 110
- IGMPv3 Query message 110
- IIF 220
- IMS 230
- In-banner video ads 31, 347
- Incoming interface (iif) 347
- Information services 141, 154
- In-page video ads 31, 347
- In-stream video ads 31, 347–348
- Integrated Services Digital Network DSL (ISDL) 348
- Integrity 348
- Interactive data 215
- Interactive message exchange 175
- Interactive Program Guide (IPG) 140, 348
- Interactive services metadata 206

- Interactive services 141, 162
 Interface 348
 Interface identifier 62, 348
 Internet access at home 36
 Internet Based TV (IBTV) 348
 Internet Control Message Protocol for IPv6 (ICMPv6) 57, 348
 Internet FCP (iFCP) 284, 348–349
 Internet Group Management Protocol (IGMP) 99, 101, 107, 159, 349
 Internet Group Management Protocol Snooping 102
 Internet Protocol (IP) TV (IPTV) 1, 4, 349, 350
 Internet protocol header compression (IPHC) 69
 Internet Protocol Version 6 (IPv6) 45
 Internet service provider (ISP) 47, 78
 Internet Small Computer System Interface (iSCSI) 285, 288, 350
 Internet suite of protocols 161
 Internet television (also known as Internet TV, Online TV) 4, 350
 Internet television, Internet-based TV (IBTV) 2–4, 42, 311, 350
 Internet-ready TVs 10, 16
 Internet video 300
 Internet video-on-demand (iVoD) 12–13, 350–351
 Interstitial program 351
 Interworking mechanisms for IPv6 and IPv4 351
 In-Text Video Ads 31, 351
 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) 351
 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Address 351
 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Device 351
 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Name 351
 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Router 351
 Invitation of a Media Server to a Conference 245
 Invitation unit 351
 iPad 15–16
 IP address 46
 IPG 210
 IP multicast 95–96
 IP multicast addresses 103–104
 IP Multimedia Subsystem (IMS) 352
 IP network QoS class definitions 174
 IPoDWDM optical network 352
 IP over dense wavelength-division multiplexing (IPoDWDM) 267
 IP over Ethernet (IPoE) 352
 IP-over-fiber connectivity 30
 IP Services Code Points (DSCPs) 173
 IP6.arp 352
 IPsec 65, 67
 IP storage 285, 352
 IP Technologies for Evolving Carrier Networks 297
 IP traffic, growth of 263
 IP traffic in North America 301
 IP traffic in Western Europe 301
 IPTV application client functions 192
 IPTV application Layer 207
 IPTV architecture 149, 160, 163
 IPTV data rates 169, 170
 IPTV distribution networks 272
 IPTV Focus Group (FG IPTV) 219
 IPTV functional architecture 163
 IPTV functional domains 156
 IPTV functional model 164–165
 IPTV HN interfaces 203
 IPTV home network 199
 IPTV Interoperability Events 227
 IPTV Interoperability Forum (IIF) 148, 220
 IPTV market scope 157
 IPTV metadata 204, 226
 IPTV middleware architecture 206–207
 IPTV multicast frameworks 150
 IPTV networks 176
 IPTV protocols 232
 IPTV security (network) 181
 IPTV security (terminal) 182
 IPTV security 149, 176, 181, 221
 IPTV service control 184
 IPTV service discovery 234
 IPTV service navigation 235
 IPTV services 16, 150
 IPTV standards 217, 219–222, 226
 IPTV subscriber security 182
 IPTV terminal device (TD) 162, 163, 188, 207, 352

- IPTV terminal device architecture 190
 IPTV Terminal Device Model 198
 IPTV Terminal Function (ITF) 201, 352
 IPTV terminal transport functions 193
 IPTV user profiles 213
 IPTV 3, 14, 20, 35, 139, 147, 271
 IPTV, reference points on protocols of
 IPTV TD 233
 IP Version 4 (IPv4) 3, 30
 IP Version 6 (IPv6) 3
 IPv4 addressing 50
 IPv4-compatible addresses 55
 IPv4-compatible IPv6 address 352
 IPv4-mapped addresses 55
 IPv4-mapped IPv6 address 352
 IPv4 multicast tunneling 72
 IPv4 node 352
 IPv6 Address 52
 IPv6 address space 51
 IPv6 base headers 59
 IPv6 deployment 76
 IPv6 extension headers 58, 65
 IPv6 in carrier networks 74
 IPv6 in IPv4 352
 IPv6-in-IPv4 tunnel 63
 IPv6/IPv4 encapsulation 78
 IPv6/IPv4 node 353
 IPv6 multicast 30
 IPv6 multicast address mapping 119
 IPv6 multicast addresses 116, 118
 IPv6 multicast in evolving IPTV
 networks 183
 IPv6 node 353
 IPv6 over IPv4 tunnel 353
 IPv6-over-IPv4 tunneling 72
 IPv6 packet 56–57
 IPv6 prefixes 353
 IPv6 protocol overview 56
 IPv6 RFCs 81
 IPv6 routing table 353
 IPv6 security 48
 ITF 201, 352
 ITU IPTV recommendations 189
 ITU-T H.264/AVC (Advanced Video
 Coding) 218, 249
 ITU-T H.701 (Error Recovery) 147
 ITU-T H.720 188, 204
 ITU-T H.721 (IPTV Terminal) 147,
 190, 198, 226
 ITU-T H.740 (Application Event
 Handling) 147, 214
 ITU-T H.750 (Metadata) 147, 214
 ITU-T H.760 214, 217
 ITU-T H.761 (Ginga-NCL) 147, 216,
 226
 ITU-T H.762 (Lightweight Interactive
 Multimedia Framework for IPTV
 Services (LIME)) 147, 216, 226
 ITU-T H.770 (Service Discovery) 147,
 188
 ITU-T Y.1901 204
 iVoD 12–13, 350–351
 Join list 353
 Key 353
 Keyframe 353
 Key management 353
 Key pair 353
 Last-hop router 353
 Layer 1/transport networks 264
 Layer 2 Tunneling Protocol (L2TP) 353
 Layer 2 353
 Layer 2/3 networks 267
 Layer 3 Protocol Independent Multicast–
 Source Specific Multicast () 267
 Layer 3 353
 Learning services 141
 Leave Group (LG) messages 101, 107
 Lifetime in preferred state 354
 Lightweight Interactive Multimedia
 Framework for IPTV services
 (LIME) 216
 Limited scope addresses 354
 Linear/Broadcast TV 151
 Linear (Live) 245
 Linear programming 354
 Linear TV 4, 6, 140, 152, 161, 190, 198,
 236, 354
 Linear TV metadata 205
 Linear TV services 150, 199
 Linear TV with trick mode 142–143
 Linear video ads 354
 Link 354
 Link duplicated addresses detection
 algorithm 63
 Link-layer identifier 354

- Link local addresses 354
 Link state routing protocol 354
 Liquid crystal display (LCD) 355
 Liquid crystal on silicon (LCoS) 355
 Local address 355
 Local interface 355
 Long Term Evolution (LTE) (aka 4G) 355
 Loopback Address 355
 LUA 217
- MAC 355
 MAC address 355
 MAC header 355
 Mac OS X 248
 Machine (Host) 355
 Masquerade 355
 Maximum transmission unit (MTU) 355
 Maximum-level aggregation identifier 355–356
 M-commerce (mobile commerce) 356
 MDUs 274, 276
 Mean Opinion Score (MOS) 166
 Media Access Control (MAC) 61, 356
 Media client functions 192
 Medical services 145
 Medium Earth Orbit (MEO)
 satellite 356
 Member 356
 Membership report message (IGMP) 113
 Meshed fabric 290
 Message exchange 175
 Metadata 356
 Metro Fibre Channel Protocol (mFCP) 356
 MHEG, MHEG-5 217
 Microsoft Xbox live 309
 Middleware 150, 204–205, 214, 356
 Middleware requirements 161
 Mid-roll 356
 Migration strategies to IPv6 71
 Minimum transport layer parameters for satisfactory QoE 172
 MLD 57, 115, 117, 123, 126, 159
 MLD EXCLUDE 136
 MLD INCLUDE 136
 MLD message format 124–125
- MLD state transition for nodes 128
 MLD state transition for routers 130
 MLDv1 116, 123
 MLDv2 116, 132
 Mobile data traffic 301
 Mobile subscribers watching video on a mobile phone 40, 43
 Mobile video 40–41
 Mobility 49, 356
 MoD (Music on Demand) 151
 Monetized video 31, 356
 Motion Picture Expert Group (MPEG) 356–357
 Moving Picture Experts Group 2 (MPEG-2) 32, 357
 Moving Picture Experts Group 4 (MPEG-4) 32, 149, 250
 MPEG encoding algorithms 168
 MPEG-2 Transport Stream (TS) 250, 382
 MPEG-4 32, 149, 250
 MPEG-7 357
 MPLS 64, 168, 260
 MPLS network environment 268
 MPLS Virtual Private Network (VPN) 267
 MPLS VPN 357
 MP3 249
 Multicast 51, 53, 357
 Multicast, client chooses address 246
 Multicast, server chooses address 246
 Multicast address 357
 Multicast Address Dynamic Client Allocation Protocol (MADCAP) 357
 Multicast address field 125
 Multicast address listener state on multicast routers 135
 Multicast Address Set Claim Protocol (MASC) 357
 Multicast address-specific query 127
 Multicast communication 98
 Multicast connection admission control 186
 Multicast control (IPTV) 185
 Multicast environment 358
 Multicast group 358
 Multicast IP address management 187
 Multicast IPv4 Tunnel 358

- Multicast Listener Discovery (MLD)
 - protocol 57, 115, 117, 123, 126, 159, 358
- Multicast Listener Discovery Protocol
 - Version 2 (MLDv2) 102
- Multicast listener done 124
- Multicast listener query 124
- Multicast listener report 124
- Multicast listening state on multicast address listeners 133
- Multicast mechanisms 159
- Multicast Mobility in Mobile IP Version 6 (MIPv6) 117
- Multicast OSPF (MOSPF) 358
- Multicast payload forwarding 98, 358
- Multicast replication (IPTV) 185
- Multicast routing 99, 358
- Multicast Routing Information Base (MRIB) 359
- Multicast scope 359
- Multicast session identifier management 187
- Multicast Source Discovery Protocol (MSDP) 359
- Multicast transmission 51, 95
- Multicast user management 187
- Multi-channel audio 359
- MultiCrypt 359
- Multi-dwelling units (MSUs) 272
- Multimedia and Hypermedia information coding Experts Group (MHEG) 217
- Multimedia Application Framework 214
- Multiple-languages 162
- Multiple Systems Operator (MSO) 359
- Multiprotocol BGP (MBGP) 99
- Multiprotocol Border Gateway Protocol (MP-BGP) 359
- Multiprotocol Encapsulation (MPE) 359
- MultiProtocol Label Switching (MPLS) 64, 168, 260
- Multi-room 359–360
- Name Resolution 360
- NAT 50, 63, 78
- National Television System Committee (NTSC) format 360
- Navigation 212
- Near Video On-Demand (nVoD) 360
- Neighbor Discovery (ND) 57, 62, 72, 360, 371–373
- Neighbors 360
- Neighbors cache 360
- Netflix 6, 8, 10, 311, 322
- Netflix Video Streaming Protocol 241
- Network Address Translation (NAT) 50, 63, 78, 360
- Network Address Translation–Protocol Translation (NAT-PT) 360
- Network assets, risks, and threats 179
- Network-Attached Storage (NAS) 285, 288, 360–361
- Network Control Protocols (NCPs) 69
- Network Convergence 296
- Network personal video recorder (nPVR) 6, 25, 361
- Network Point of Attachment (NPA) 360
- Network provider (NP) 157
- Network PVR (nPVR) 144
- Network requirements 161
- Network segment 360
- Network Transport Functions for IPTV Multicast 185
- Next New Networks 321
- Next-Generation Networks (NGNs) 148
- Next-Level Aggregation Identifier (NLA ID) 361
- NGN architecture 229
- NGN with IMS IPTV 164
- NGN without IMS IPTV 164
- Nielsen Rating collection 148
- NIT (Network Information Table) 361
- Node Types 361
- Node 361
- Non-Broadcast Multiple Access (NBMA) 361
- Nonbroadcast networks 361
- Nonlinear video ads 31, 361
- Non-listener 128
- Non-multicast router 362
- Non-NGN IPTV 164
- Non-Querier 126, 128, 130
- Nontraditional TV (NTTV) 1, 4, 8, 14, 17, 23, 30, 95, 139, 147, 308, 362

- Notification service 153
 nPVR 6, 15–16
 NTSC 169
 NTTV 1, 4, 8, 14, 17, 23, 30, 95, 139,
 147, 308, 362
 NTTV linear/nonlinear services 32
- Object storage 285, 362
 On-demand advertising 145
 On-demand services 198, 245, 362
 1GbE 266
 1G-EPON 278, 280
 100GbE 266
 120 Hz refresh rate 324
 1TbE 264
 1080p video format 324
 Online TV 2
 Online video 362
 On-tree router 362
 OpenCable 362
 Open IPTV Forum (OIPF) 155
 Optical Interworking Forum (OIF) 267
 Optical line terminal (OLT) 278
 Optical network terminals (ONTs) 276
 Optical Transport Network (OTN) 264
 Organizational Unit Identifier
 (OUI) 118
 O3b Networks 34
 OTT 4, 16, 26, 28, 240, 362–363
 Outgoing interface (OIF) list 362
 Overlay ad 31, 362
 Over-The-Top (OTT) streaming
 devices 4, 16, 26, 28, 240, 362–363
 Over/under format 363
- PaaS (Platform-as-a-Service) 258
 Package 363
 Packet 363
 Packet Identifier (PID) 363
 Page View 363
 PAL/SECAM 169
 Parameter Discovery 363
 Parameterized QoS 173
 Parental control 154, 162, 363
 Passive Optical Network (PON) 27,
 162, 275
 Path Determination 363
 Path MTU 363
 Path MTU Discovery 364
- Path Vector 364
 Pause Delay 171
 Payload Unit Start Indicator
 (PUSI) 364
 Payment Transactions 175
 Pay per click (PPC) 31, 364
 Pay per use (PPU) 155
 Pay per view (PPV) 4–5, 141, 155, 364
 Peer-entity authentication 364
 Peer-to-peer (P2P) network 364
 Peer-to-peer (P2P) technology 2, 32,
 240
 Performance monitoring 197, 238
 Permanent host groups 105, 364
 Personal broadcast 146
 Personal digital recorder (PDR) 365
 Personal mobility 365
 Personal video recorder (PVR) 6, 25,
 152, 365
 Personal video recorder (PVR)
 services 142–143, 162
 Phase Alternating Line (PAL) 365
 Phishing 365
 PIM Dense Mode (PIM-DM) 100, 365
 PIM multicast border router
 (PMBR) 365
 PIM Source Specific Multicast
 (SSM) 365
 PIM Sparse Mode (PIM-SM) 365
 PIM Version 2 (PIMv2) 100
 Plaintext 365
 Plasma 366
 Play Delay 171
 Player controls 366
 Player skin 366
 Playlist 366
 Plug-and-Play 48
 Point of Deployment (POD) 366
 Point-To-Point Protocol (PPP) 69, 366
 Point-to-Point Protocol over Ethernet
 (PPPoE) 366
 PON (Passive Optical Network) 271,
 279
 Pop-up 366
 Post-roll 366
 PPC 31, 364
 P-PPV (pre-booked PPV) 366
 PPT (pre-booked PPV) 366
 PPU 155

- PPV 5, 141, 155, 364, 366
- Pragmatic General Multicast (PGM) 366
- Prefix 366
- Prefixes list 367
- Prefix length 367
- Prefix-length notation 367
- Premium VoD 367
- Pre-roll 367
- Presentation Time Stamp (PTS) 367
- Priority of linear and other traffic 187
- Priority (or class-based) QoS 173
- Privacy 367
- Private cloud 257
- Private key 367
- Private section 367
- Product metadata 367
- Professional Video Hosting 367
- Program 367
- Program Association Table (PAT) 367
- Program Map Table (PMT) 367
- Program Specific Information (PSI) 368
- Program stream 368
- Progressive Download 368
- Projected RIR unallocated address pool exhaustion 47
- Promotional video 368
- Protocol data unit (PDU) 368
- Protocol Independent Multicast Dense Mode (PIM-DM) 271
- Protocol Independent Multicast (PIM) 99, 100, 368
- Protocol Independent Multicast Sparse Mode (PIM-SM) 119
- Protocols supporting IPTV terminal devices 200
- Prune list 368
- Pseudo-header 368
- Pseudo-periodic 368
- Pseudowire 368–369
- P2P networks 32, 256
- Public interest services 142
- Public key 369
- Public key algorithm 369
- Public key infrastructure (PKI) 369
- Public-Key Cryptography Standards (PKCS) 369
- Pull-based caching 255
- Pull mode 21
- Pull VoD 369
- Pure streaming 369
- Push mode 21
- Push pull 21, 206
- Push replication 255
- Push VoD 369
- PVR 6, 25, 152
- PVR service 151
- Q-in-Q 369
- QoE 148, 166–167, 171, 221, 240
- QoE requirements 161
- QoS 147, 167, 173, 221, 240
- QoS Classes 175
- QoS requirements 161
- Quadrature Amplitude Modulation (QAM) 369
- Quality of content (QoC) 369–370
- Quality of experience (QoE) 148, 166–167, 171
- Quality of service (QoS) 147, 167, 173, 221
- Quality of service (QoS) in IPv6 70
- Quaternary Phase Shift Keying (QPSK) 370
- Querier 126, 128, 130, 370
- Query received 129
- Random access point 370
- Rapidly Evolving Content Providers 16
- Rapidly evolving display devices 16
- Rate adaptive DSL (RADSL) 370
- Real-time streaming protocol (RTSP) 241–242, 370
- Real-Time Transport Control Protocol (RTCP) 242–243, 370
- Real-Time Transport Protocol (RTP) 241–242, 370
- Reassembly 370
- Receiver 371
- Redirect 371
- Redundant Array of Inexpensive Disks (RAID) 288–289, 371
- Reference time stamp 371
- Regional Internet Registries (RIRs) 47
- Remote storage DVR (RS-DVR) 8
- Rendezvous point (RP) 101, 117, 120–121, 371

- Replays 371
- Report 127
- Report received 129
- Repudiation 371
- Request headers 371
- Request mechanism 211
- Requirements for support of IPTV services 163
- Reset Timer 129
- Residential broadband services in an IPv6 environment 75
- Residential Gateway (RG) 371
- Resource Abstraction Layer (RAL) 207
- Resource control (IPTV) 185
- Resource records (RR) 77
- Response headers 371
- Re-transmission broadcast service 371
- Retrieval of Media from Media Server 245
- Reverse direction 372
- Reverse path forwarding (RPF) 372
- Revision3 internet television 319
- Rewind delay 171
- RFC dealing with IPv6 deployment 79
- Rich media 372
- Rights 372
- Rights expression 372
- Ring fabrics 291
- RIRs 63
- Robust header compression (ROHC) 69
- Route entry 372
- Router 372
- Router advertisement 62, 372–373
- Router discovery 373
- Router internals 269–270
- Router-Port Group Management Protocol (RGMP) 373
- Router’s cache 373
- Routing 119, 268
- Routing header 64
- Routing loop 373
- RPs 186
- RP-Set 373
- RP-tree (also known as shared tree) 374
- RTSP 243, 245
- RTSP methods 247
- RTSP pause 246
- RTSP play and record 246
- RTSP setup 246
- RTSP state machine 246
- RTSP teardown 246
- SaaS (Software-as-a-Service) 258
- SAN 292
- SAN fabrics 293
- SAN management applications 290
- Satellite distribution, CDN approaches 254–255
- Satellite footprint 373
- Scalable vector graphics (SVG) 217
- Scope 373
- Scope ID 373
- Scope Zone 373
- SCP (service and content protection) client functions 192
- Scrambling 373
- Scrambling algorithm 373
- Second generation VDSL (VDSL2) 373
- Secure delivery of content 161
- Security label 374
- Security mechanisms supported in IPTV 149, 176, 181, 221
- Security policy 374
- Security requirements, IPTV 161
- Security threats in IPTV environments (partial list) 177
- Send done 129
- Send report 129
- Service and content protection (SCP) client functions 195
- Service assets, risks, and threats 178
- Service consumption 236
- Service control function group 165
- Service control functions for IPTV multicast 184
- Service convergence 296
- Service discovery 208
- Service navigation logic 210
- Service navigation (SN) 140, 210
- Service protection 374
- Service provider (SP) 157, 209
- Service provider strategies for NTTV 294
- Service user profile 184

- Session Description Protocol (SDP) 242–243, 374
- Session key 374
- Set flag 129
- Set-top boxes (STBs) 1, 14, 28, 140, 149, 167, 190, 226, 240
- (S,G) Pair 324
- (S,G) route entry 324
- Shared tree (also known RP-tree) 374
- Shortest path tree (SPT) 374
- Sign language interpretation 142
- Signaling 119
- Signaling Tables 374
- SimulCrypt 375
- Single Program Transport Stream (SPTS) 375
- Single-switch fabric 290
- SI table 374
- Site-Level Aggregation Identifier (SLA ID) 375
- Site-local address 375–376
- 6bone 55
- 6over4 325
- 6over4 link-local address 325
- 6over4 unicast address 325
- 6to4 55, 325
- 6to4 address 325
- 6to4 host 325
- 6to4 router 325
- size of address space 52
- Skin 376
- Skin ads 31, 376
- Smartphones 16
- Smart TV (also known as connected TV) 310, 376
- Smooth Streaming 241
- SMPTE 169
- SNDU 376
- Social networks 16
- Solicited-node address 376
- Solicited-node multicast address format 118
- SONET/SDN network 265
- Sony 308
- Sourced video 376
- Source filtering 109, 137
- Source tree 376
- Source-specific multicast (SSM) 187, 376
- Sparse Mode PIM 101
- Sparse-Dense 376–377
- Sparse-Mode (SM) Protocol Independent Multicast (PIM) 377
- Sponsorship graphics 377
- Spoofing 377
- SSM-aware host 377
- Standard definition (SD) 170, 377
- Start listening 128
- Start timer 129
- State Change Report 134
- Stateless address autoconfiguration (SLAAC) 61
- Stateless IP/ICMP Translation (SIIT) 377
- Static routing 377
- Static tunneling 378
- STB market worldwide 159
- STB (set-top box) 1, 14, 28, 140, 149, 167, 190, 226, 240, 378
- Stop delay 171
- Stop listening 128
- Stop timer 129
- Storage 378
- Storage appliance 378
- Storage Area Network (SAN) 288–289
- Storage technologies 282
- Storage virtualization 286, 378
- Stored content metadata 206
- Stored media sources 16
- Stream 378
- Stream cipher 378
- Streaming 240, 244, 378
- Streaming control 175
- Streaming media 378
- Streaming of Audio Content 175
- Streaming of live low resolution video content 175
- Streaming of live speech 175
- Streaming of live TV content 175
- Streaming of video content 175
- Streaming protocols 378
- STUB multicast routing 378
- Stub network 378
- Subnet-router anycast address 379
- Subnetwork 379
- Subscriber 379
- Subscription 155, 379
- Subscription VoD 379

- Subtitles 142
- Superdistribution 379
- Supplementary content 379
- Symmetric DSL (SDSL) 379
- Symmetric encryption 379
- Symmetric flavors DSL 379
- Symmetric High-Speed Digital Subscriber Line (SHDSL) 379, 380
- Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) 264
- Syndicated video 380

- Table Section 380
- Targeted advertising 145
- T-commerce 28, 151
- T-communication 28, 151
- Telco 380
- Telco metropolitan networks 269
- 10GbE 266
- 10G-EPON 278, 280
- T-entertainment 151
- Teredo 55, 381
- Teredo client 381
- Teredo relay 381
- Teredo server 381
- Terminal device (TD) 380
- Terminal device (TD) protection 380
- Terminal device assets, risks, and threats 180
- Terminal device management 197
- Terminal mobility 380
- Terminal transport functions 192
- Terrestrial transmission 7
- Third Generation Partnership Project 2 (3GPP2) 164
- 3rd ITU-T IPTV Interop Event and Showcase 116
- Threat 380
- 3-Dimensional TV (3DTV) 23, 151, 220, 325
- Tickers 380
- Tiered storage 286, 380–381
- Timecode 381
- Timer expired 129
- Time-shifted TV (TSTV) 2–5, 32, 41, 43, 139, 151, 199, 381
- Time-shifted viewing 381
- Time shifting 5, 152, 381

- Time synchronization 238
- Time to Live (TTL) 58
- Time Warner Cable 77
- T-information 28, 151
- TiVo 16, 24
- Toshiba 308
- Total households with TVs 7
- Traditional broadcast TV 21
- Traditional content providers/transporters 16
- Traditional TV 24, 41–42
- Traffic management (TM) 186
- Transient host groups 105, 381–382
- Transition in viewing habits 8
- Transit network 382
- Translation 382
- Transmission control protocol (TCP) 246
- Transport mode 66
- Transport Relay Translator (TRT) 382
- Transport stream (TS) 382
- Transport stream (TS) logical channel 382
- Transport stream (TS) multiplex 382
- Transport stream (TS) packet 382
- Tree Information Base (TIB) 382–383
- Trick mode functionality 5, 383
- Triple play IPTV-based multicast network 33
- TSTV 2, 4–5, 8, 14, 17, 32, 41, 139, 150–151
- Tunneling techniques 383
- Tunnel mode 66
- TV with trick mode 383

- UGC 2, 16, 31, 348
- UGV 4, 5, 15–20, 22, 24, 32, 44, 348, 384
- UltraViolet 261, 321
- Unicast 51, 53, 245
- Unicast address 383
- Unicast delivery 150
- Unicast environment 383
- Unicast transmission 51
- Unidirectional link (UDL) 383
- U.S. cable TV 34
- U.S. IPTV population 157
- Unspecified address 383
- Upload of video content 175

- Upstream Interface 384
- User Data Protocol (UDP) 243, 246
- User-generated content (UGC) 2, 4, 16, 27, 31, 384
- User-generated video (UGV) 4–5, 15–20, 22, 24, 32, 44, 348, 384
- User privacy protection 384
- User-specific advertising 151
- Utility computing 257
- Variable bit rate (VBR) 168
- VDSL2 272, 274
- Verizon FiOS IPTV 309
- very high bit rate DSL (VDSL) 384
- Very high bit rate DSL 2 (VDSL2) 272, 274
- Very High-Capacity Backbone Networks, Transmission 260
- Video ad 384
- Video ad experience 384
- Video Application Program Interface (Video API) 384
- Video bookmarking services 384
- Video buffering 384
- Video compression 384
- Video E-commerce 384
- Video format 384, 385
- Video game consoles 16
- Video-on-demand (VoD) 2, 4–5, 9, 12–16, 18–20, 22–23, 32, 44–45, 384–385
- Video player 385
- Video Publishing and Management Platform 385
- Video Search Engine Optimization (Video SEO) 385
- Video search engines 385
- Video selection process delay 171
- Video size 385
- Video watching on Internet 40
- Viewing Habits Nielsen's Data (2009) 40
- Viewing Habits Nielson's Data (2011) 43
- Viral videos 385
- Virtual infrastructure 287, 385
- Virtual private LAN service (VPLS) 385
- Virtualization 287, 385–386
- Visits 386
- Vlog (Video BLog) 386
- VoD 2, 4–5, 9, 12–16, 18–20, 22–23, 32, 44–45, 141, 147, 150, 161, 170, 190, 199, 248, 384–385
- VoD service delivery 150, 236
- VoD trick modes 386
- Watching video on internet 43
- Watermarking 386
- Web cache 287, 386
- Webcast 386
- Web services (WSs) 287, 386
- Web television 2–6, 10, 311
- Web video 2
- Widget 387
- Wi-Fi 387
- Wildcard (WC) multicast route entry 387
- WiMAX 275, 387
- World IPv6 Day 77
- Wrapping IPv6 traffic 63
- wwiTv.com 311
- Xbox 360 gaming console 16
- XG-PON 280
- YouTube 8, 10, 23
- Zone Name 387

ABOUT THE AUTHOR

Among other activities, **Mr. Daniel Minoli** has done extensive work in video engineering, design, and implementation over the years. The results presented in this book are based on foundation work done while at Telcordia (Bellcore), Stevens Institute of Technology, AT&T, and other engineering firms, starting in the early 1990s and continuing to the present. Some of his video work has been documented in books he has authored, including:

1. *Mobile Video with Mobile IPv6* (Wiley, 2012);
2. *3D Television (3DTV) Content Capture, Encoding, and Transmission—Building the Transport Infrastructure for Commercial Services* (Wiley, 2010);
3. *3D Television (3DTV) Technology, Systems, and Deployment—Rolling out the Infrastructure for Next-Generation Entertainment* (Francis and Taylor, 2010);
4. *IP Multicast with Applications to IPTV and Mobile DVB-H* (Wiley/IEEE Press, 2008);
5. *Video Dialtone Technology: Digital Video over ADSL, HFC, FTTC, and ATM* (McGraw-Hill, 1995); and
6. *Distributed Multimedia Through Broadband Communication Services* (co-authored) (Artech House, 1994).

Mr. Minoli has many years of technical hands-on and managerial experience in planning, designing, deploying, and operating IP/IPv6, telecom, wireless, satellite, and video networks, and Data Center systems and subsystems for global Best-In-Class carriers and financial companies. He has worked on advanced network deployment at financial firms, such as AIG, Prudential Securities, Capital One Financial, and service provider firms, such as Network Analysis Corporation, Bell Telephone Laboratories, ITT DTS/Worldcom, Bell Communications Research (now Telcordia), AT&T, Leading Edge Networks Inc., SES, and other institutions. Recently, Mr. Minoli has been responsible for the development and deployment of IPTV systems, terrestrial and mobile

IP-based networking services, and IPv6 services over satellite links. He also played a founding role in the launching of two companies through the high-tech incubator Leading Edge Networks Inc., which he ran in the early 2000s: Global Wireless Services, a provider of secure broadband hotspot mobile Internet and hotspot VoIP services; and, InfoPort Communications Group, an optical and Gigabit Ethernet metropolitan carrier supporting Data Center/SAN/channel extension and cloud network access services. For several years, he has been Session, Tutorial, and now overall Technical Program Chair for the IEEE ENTNET (Enterprise Networking) conference; ENTNET focuses on enterprise networking requirements for large financial firms and other corporate institutions.

Mr. Minoli has also written columns for *ComputerWorld*, *NetworkWorld*, and *Network Computing* (1985–2006). He has taught at New York University (Information Technology Institute), Rutgers University, and Stevens Institute of Technology (1984–2006). Also, he was a Technology Analyst At-Large, for Gartner/DataPro (1985–2001); based on extensive hand-on work at financial firms and carriers, he tracked technologies and wrote CTO/CIO-level technical scans in the area of telephony and data systems, including topics on security, disaster recovery, network management, LANs, WANs (ATM and MPLS), wireless (LAN and public hotspot), VoIP, network design/economics, carrier networks (such as metro Ethernet and CWDM/DWDM), and e-commerce. Over the years, he has advised Venture Capitals for investments of \$150 million in a dozen high-tech companies. He has acted as Expert Witness in a (won) \$11 billion lawsuit regarding a VoIP-based wireless Air-to-Ground radio communication system for airplane in-cabin services and has been engaged as a technical expert in a number of patent infringement proceedings in the digital imaging and VoIP space, supporting premiere legal firms such as Schiff Hardin LLP, Fulbright & Jaworski LLP, Dimock Stratton LLP/ Smart & Biggar LLP, and Baker & McKenzie LLP, among others.