International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Y

Supplement 16

(02/2012)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT GENERATION NETWORKS

ITU-T Y.1900-series – Supplement on guidelines on deployment of IP multicast for IPTV content delivery

ITU-T Y-series Recommendations – Supplement 16

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Smart ubiquitous networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
Future networks	Y.3000–Y.3099

For further details, please refer to the list of ITU-T Recommendations.

Supplement 16 to ITU-T Y-series Recommendations

ITU-T Y.1900-series – Supplement on guidelines on deployment of IP multicast for IPTV content delivery

Summary

Supplement 16 to ITU-T Y-series Recommendations describes the technical guidelines for the deployment of IP multicast technologies for IPTV content delivery. The deployment guidelines identify the technical issues and considerations regarding the capabilities of IP multicast from the perspective of supporting the IPTV services.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y Suppl. 16	2012-02-17	13

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 16 to ITU-T Y-series Recommendations

ITU-T Y.1900-series – Supplement on guidelines on deployment of IP multicast for IPTV content delivery

1 Scope

This supplement describes the technical guidelines for the deployment of IP multicast technologies for IPTV content delivery. The deployment guidelines identify the technical issues and considerations regarding the capabilities of IP multicast from the perspective of supporting the IPTV services.

This supplement can be used for IPTV content delivery using the network multicast-based content delivery model defined in [ITU-T Y.2019] and [ITU-T Y.1902].

Note that this supplement mainly focuses on the IP version 4 multicast support.

2 References

[ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions.*

[ITU-T M.1400] Recommendation ITU-T M.1400 (2006), *Designations for interconnections among operators' networks.*

[ITU-T Y.1901] Recommendation ITU-T Y.1901 (2009), *Requirements for the support of IPTV services.*

[ITU-T Y.1902] Recommendation ITU-T Y.1902 (2011), *Framework for multicast-based IPTV content delivery.*

[ITU-T Y.1910] Recommendation ITU-T Y.1910 (2008), *IPTV functional architecture.*

[ITU-T Y.2019] Recommendation ITU-T Y.2019 (2010), *Content delivery functional architecture in NGN.*

[IETF RFC 1112] IETF RFC 1112 (1989), *Host Extensions for IP Multicasting.*

[IETF RFC 1584] IETF RFC 1584 (1994), *Multicast Extensions to OSPF*.

[IETF RFC 1918] IETF RFC 1918 (1996), *Address Allocation for Private Internets.*

[IETF RFC 2201] IETF RFC 2201 (1997), *Core Based Trees (CBT) Multicast Routing Architecture.*

[IETF RFC 2236] IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2.*

[IETF RFC 2475] IETF RFC 2475 (1998), *An Architecture for Differentiated Services.*

[IETF RFC 2710] IETF RFC 2710 (1999), *Multicast Listener Discovery (MLD) for IPv6.*

[IETF RFC 2858] IETF RFC 2858 (2000), *Multiprotocol Extensions for BGP-4.*

[IETF RFC 3376] IETF RFC 3376 (2002), *Internet Group Management Protocol, Version 3.*

[IETF RFC 3618] IETF RFC 3618 (2003), *Multicast Source Discovery Protocol (MSDP).*

[IETF RFC 3810] IETF RFC 3810 (2004), *Multicast Listener Discovery Version 2 (MLDv2) for Ipv6.*

[IETF RFC 3973] IETF RFC 3973 (2005), *Protocol Independent Multicast – Dense Mode (PIM-DM): Protocol Specification (Revised).*

[IETF RFC 4541] IETF RFC 4541 (2006), *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches.*

[IETF RFC 4601] IETF RFC 4601 (2006), *Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification (Revised).*

[IETF RFC 4604] IETF RFC 4604 (2006), *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source Specific Multicast.*

[IETF RFC 4605] IETF RFC 4605 (2006), *Internet Group Management Protocol (IGMP)/Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying").*

3 Definitions

3.1 Terms defined elsewhere

This supplement uses the following terms defined elsewhere:

3.1.1 broadcast [ITU-T M.60]: One-way transmission from one point to two or more other points.

3.1.2 content provider [ITU-T Y.1910]: The entity that owns or is licensed to sell content or content assets.

3.1.3 delivery [ITU-T Y.1910]: In context of IPTV architecture, "delivery" is defined as sending contents to an end-user.

3.1.4 distribution [ITU-T Y.1910]: In context of IPTV architecture, "distribution" is defined as sending the content to appropriate intermediate locations to enable subsequent delivery.

3.1.5 electronic program guide (EPG) [ITU-T Y.1901]: A structured set of data, intended to provide information on available content that may be accessed by end users.

3.1.6 end user [ITU-T Y.1901]: The actual user of the products or services**.**

3.1.7 linear television (linear TV) [ITU-T Y.1910]: 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.

3.1.8 service provider [ITU-T M.1400]: A general reference to an operator that provides telecommunication services to customers and other users either on a tariff or contract basis. A service provider can optionally operate a network. A service provider can optionally be a customer of another service provider.

3.2 Term defined in this supplement

This supplement defines the following term:

3.2.1 IPTV multicast interoperability: The capability to provide stable multicast-based delivery of IPTV content amongst different IPTV service providers.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms.

AS	Autonomous System
ASM	Any Source Multicast
BGP	Border Gateway Protocol
BSR	Bootstrap Router
CBT	Core Based Trees
CIDR	Classless Inter Domain Routing
CPE	Customer Premises Equipment
DNS	Domain Name Service
DoS	Denial of Service
DVMRP	Distance Vector Multicast Routing Protocol
ECMP	Equal Cost Multiple Path
EPG	Electronic Program Guide
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
ISP	Internet Service Provider
ISSU	In-Service Software Upgrade
MAC	Media Access Control
MBGP	Multicast Border Gateway Protocol
MD5	Message Digest 5
MLD	Multicast Listener Discovery
MOSPF	Multicast Open Shortest Path First
MSDP	Multicast Source Discovery Protocol
NP	Network Provider
OSPF	Open Shortest Path First
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast – Dense Mode
PIM-SM	Protocol Independent Multicast – Sparse Mode
PoP	Points of Presence
QoE	Quality of Experience
QoS	Quality of Service
RP	Rendezvous Point
RPF	Reverse Path Forwarding
SP	Service Provider
SSM	Source-Specific Multicast

TCP Transport Control Protocol

UDP User Datagram Protocol

URI Uniform Resource Identifier

VLAN Virtual Local Area Network

5 Conventions

None.

6 Overview

As an essential content distribution methodology for support of IPTV services, IP multicast is required to distribute a large amount of multimedia content to a number of end users simultaneously. Since IP multicast has highly complex capabilities, and is designed for a general purpose, there should be some guidelines on the development or deployment of IPTV services when using IP multicast for content distribution.

This supplement describes some technical issues that should be considered in the deployment of IPTV services when using IP multicast for content distribution. By describing several solutions to these issues, this supplement provides technical guidelines for the deployment of IP multicast-based content distribution for the IPTV services.

The capabilities of IP multicast can be categorized into four parts: data delivery, group management, QoS control, and security. Each category of general IP multicast capabilities is briefly described and its technical issues are summarized in clause 7. The detailed deployment guidelines for these issues are presented in clauses 8, 9, 10, and 11.

7 IP multicast capabilities and issues related to IPTV content delivery

7.1 Multicast data delivery

This capability deals with the delivery of data to multicast group members. The essential function of multicast data delivery is data forwarding according to the group membership of end users.

There are two models for data delivery capability: any source multicast (ASM) and source-specific multicast (SSM). In ASM, the multicast chann§el is specified by the multicast group addresses only, regardless of the multicast senders (*, G). ASM is appropriate for the many-to-many delivery model (with multiple sources and multiple receivers in a session). Note, however, that the ASM model has high complexity in terms of management of group membership, globally unique addresses, and rendezvous points (RPs). In contrast, SSM uses a combination of the multicast sender's address and the multicast group address for a multicast channel (S, G); hence the easier management of group membership and address in SSM. Note, however, that SSM has a limitation with regard to the many-to-many delivery model. Since multicast-based IPTV content delivery is based on one-to-many delivery model (with one source and multiple receivers), SSM is more appropriate for support IPTV services.

Multicast data is forwarded along a multicast routing tree built by the network elements using a multicast routing protocol. Among multicast routing protocol standards, protocol independent multicast – sparse mode (PIM-SM) [IETF RFC 4601] is typically used. Although based on the ASM model, PIM-SM is widely used by network providers (NPs) for its easy deployment and maintenance.

Another issue to be considered is IPTV multicast interoperability among different IPTV service providers. To support IPTV multicast interoperability, routing policies such as the topological location of network elements and Multicast Border Gateway Protocol (MBGP) configurations require further consideration.

7.2 Multicast group management

This capability deals with the membership management of a group involved in a multicast-based service. Its main functionalities include group or group member identification, group advertisement and discovery, group monitoring and membership management.

The group identifier in multicast is the IP multicast address of the group. Note, however, that the IP multicast address is not easily manageable, and that the space of these addresses is limited. To increase the manageability of group address management for the support of IPTV services, binding IP multicast addresses with domain names is being attempted.

Group membership determines which terminal can receive the multicast data. Internet Group Management Protocol (IGMP) [IETF RFC 2236] is widely used for group membership management. Note, however, that IGMP has some technical issues to be considered when used for IPTV content delivery, one of which is the problem of exposure of membership update messages since IGMP is based on periodic membership update.

IPTV service providers need to control the access of end users to the multicast delivery of IPTV content. Note, however, that the existing multicast group management protocol standards (e.g., IGMP and Multicast Listener Discovery (MLD) [IETF RFC 2710]) do not specify user authorization or authentication mechanisms.

7.3 QoS control

This capability deals with QoS control support for multicast-based services. It defines the target QoS level of a multicast connection.

Since IPTV content is multimedia data with a large volume, IPTV services are more likely to be threatened by QoS deficiency. There are two types of QoS for IPTV multicast: end-to-end QoS and topological QoS.

For end-to-end QoS, multicast traffic management or routing policies need to be considered because IP multicast does not have a mechanism for congestion control or resource reservation.

For topological QoS, the topological design for the multicast delivery of IPTV content should be considered through the appropriate positioning of RPs and traffic balancing among topological domains.

High availability is one of the key deployment considerations for QoS control.

7.4 Security

This capability deals with security support for multicast-based services. It provides user authentication and authorization, data confidentiality support and data integrity support.

Security is the most crucial issue in multicast network deployment. Thus, very strict security considerations are a must throughout the multicast network to minimize service interruption caused by security loopholes. RPs and PIM routers are the main network elements whose security support needs careful consideration in IPTV multicast.

Supporting the interoperability of different service providers also requires considering the protection of the IP multicast network of a service provider against incoming multicast traffic or control messages from different service providers.

8 Deployment guidelines for data delivery

The physical implementation of IPTV multicast transport can be realized by network elements with multipoint configurations.

8.1 IP multicast models for IPTV

Two different service models for IP multicast are currently supported: any source multicast (ASM) and source-specific multicast (SSM). To provide IPTV content delivery, both service models can be used and deployed at the same time because ASM and SSM use different address spaces.

ASM generally deploys IGMPv2 [IETF RFC 2236] or IGMPv3 [IETF RFC 3376] (MLDv1 [IETF RFC 2710]/MLDv2 [IETF RFC 3810]) without source information and PIM-sparse mode in combination with the Multicast Source Discovery Protocol (MSDP) [IETF RFC 3618], whereas SSM deploys IGMPv3/MLDv2 with source information and PIM-source-specific multicast as routing protocol.

8.1.1 Any source multicast

As the classic variant, any source multicast (ASM) uses a model wherein all decisions are made based on the multicast group address (G) only. Multicast receivers (i.e., terminal devices) are able to join and leave multicast groups to receive IPTV content. The terminal devices do not have knowledge of the multicast senders (i.e., content sources) within the network. Assuming that two content sources are sending IPTV content to the same IP multicast group address (G), when a terminal device joins (G), it receives the content from both content sources. Figure 8-1 presents an example of an ASM model.

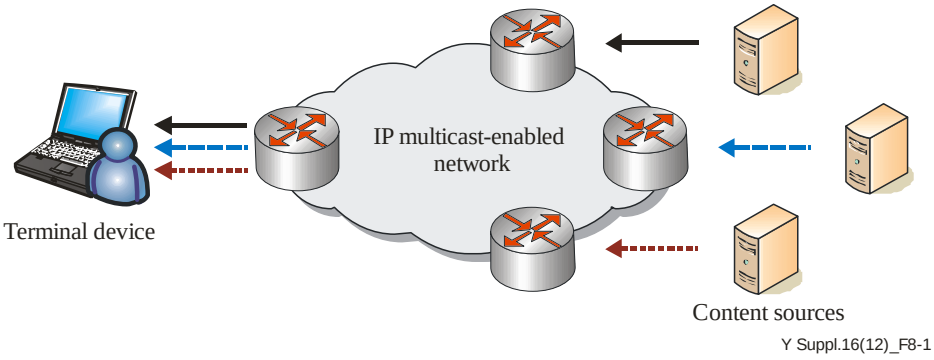

Figure 8-1 – Example of an any source multicast model

This model has some significant drawbacks with regard to IPTV services as follows:

– Addressing:

  Due to the fact that only the IP multicast address is used, it is not possible to distinguish different senders at the network level. Hence it is needed to provide functions that manage the use of IP multicast addresses. However, this may slow down the IPTV service deployment because it is required through obtaining a free (unused) IP multicast address to set up a new IPTV channel or to change the existing IPTV channel.

– Security:

  In the ASM model, it is easy to disrupt the existing IPTV channels by simply sending traffic to the same group address. To avoid such kind of attacks, complex filter mechanisms are needed at the ingress and/or egress points of the network (and possibly at the customer's premises to avoid unwanted and disruptive IP multicast traffic).

– Redundancy:

  At the network level, any source multicast (ASM) usually deploys protocol independent multicast-sparse mode (PIM-SM) with a centralized rendezvous point (RP) representing a single point of failure. Overcoming this problem necessitates redundant RPs and relevant protocols.

– Complexity:

  Taking above items 1, 2, and 3 into account (as well as some other drawbacks), the use of any source multicast (ASM) can be said to be highly complex. To reduce the complexity and to overcome the problems with ASM, a new model "source specific multicast" can be used instead.

8.1.2 Source-specific multicast

Source-specific multicast (SSM) overcomes the problems associated with any source multicast (ASM). The main difference between the two models lies in the use of the source address of the multicast sender. Unlike ASM, SSM enables distinguishing between one sender (S1) and another sender (S2) sending to the same IP multicast address (G). Receivers specify not only group address (G) but also the address of the sender (S); thus resulting in an IP multicast channel (S,G). Since the unicast address within a network uniquely identifies a terminal device, the combination of (S,G) is unique as well. A receiver joining (S1, G) does not receive traffic from another system sending to the same IP multicast address.

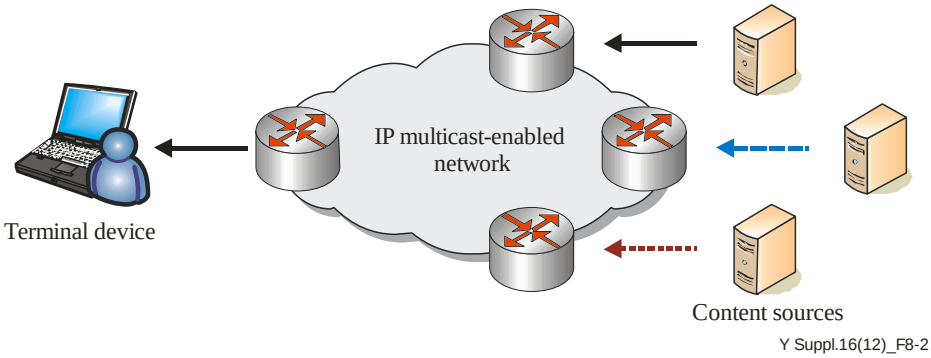

Figure 8-2 – Source-specific multicast

Source-specific multicast solves the following problems:

– Addressing:

  It is no longer necessary to coordinate centrally the use of IP multicast addresses. Any sender can send to any existing IP multicast group. The network and receivers are able to specify a particular sender using an IP multicast group. IP multicast channels (S,G) are handled and routed individually by the network and the terminal devices as well.

– Security:

  Denial of service (DoS) attacks, which are launched by simply sending to a multicast group that is already in use, are no longer possible since individual senders can be distinguished.

– Complexity:

  Source specific multicast reduces the overall complexity within IPTV. It solves several issues related to security and addressing as well as foregoes the need for centralized rendezvous points.

SSM is also optimized for one-to-many deployment scenarios that are typically used within IPTV. ASM and SSM can be used in parallel (deploying different address ranges) if necessary. The use of SSM eases the deployment of IPTV and reduces complexity, allowing for more flexible IPTV services. IETF has assigned the default address space 232/8 for use with source-specific multicast.

8.2 Multicast routing protocols

To enable the network elements to route the IP multicast packets of IPTV content, the network elements are required to support multicast routing protocols, e.g., Distance Vector Multicast Routing Protocol (DVMRP) [IETF RFC 1075], Multicast Open Shortest Path First (MOSPF) [IETF RFC 1584], Protocol Independent Multicast – Sparse Mode (PIM-SM) [IETF RFC 4601], Protocol Independent Multicast – Dense Mode (PIM-DM) [IETF RFC 3973], and Core Based Trees (CBT) [IETF RFC 2201]. In this supplement, the deployment guidelines based on PIM-SM are described.

PIM-SM is used for multicast data distribution among IP multicast-enabled network elements. The network elements build multicast routing trees spanning from multicast sources to destinations. Along these multicast routing trees, multicast packets are replicated by the network elements and forwarded to the child network elements.

Within the access networks, the Internet Group Membership Protocol (IGMP) is used for the management and maintenance of multicast receivers (i.e., group members). Using IGMP, an end terminal belonging to a multicast group continuously reports its membership to the edge network element to have the multicast data forwarded.

A rendezvous point (RP) is a temporary contact point connecting multicast sources and receivers. Upon receiving a multicast group join from a multicast receiver, the network elements derive a shared multicast routing tree rooted by RP. The multicast data from the source are delivered to RP, which in turn further replicates and forwards them to the child network elements. If multicast traffic via RP gets larger than a threshold value, RP triggers the network elements near the multicast receivers to join source multicast routing trees rooted by the multicast source.

If a large number of multicast channels are used, or multicast traffic needs to traverse across different domains of service providers, a Multicast Source Discovery Protocol (MSDP) [IETF RFC 3618] is required to support more than one RPs. MSDP is used for RP to exchange the information on multicast sources, e.g., (source, group) address-pair and Source Active (SA), with the other RPs.

If the information on a multicast source is already known, multicast receivers do not need to use RP; instead, they can use SSM with which multicast data are delivered along the shortest forwarding paths from the source. Note that SSM requires IGMP version 3 [IETF RFC 3376]. Details on SSM are described in the following clause.

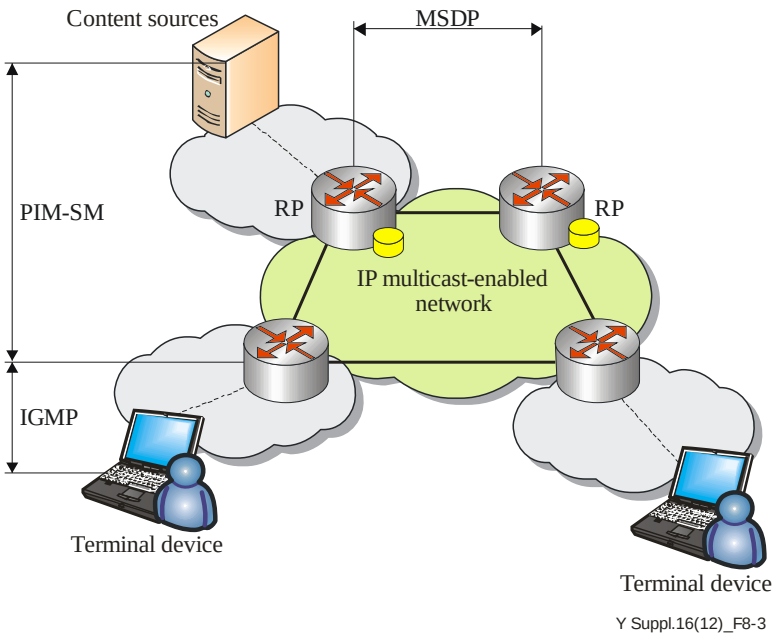

Figure 8-3 – Overview of the PIM-SM-based IP multicast-enabled network

8.3 Routing policy for IPTV multicast interoperability

The IPTV service provider should provide capabilities for exchanging IPTV service information between different IPTV service providers for interoperability. For IPTV multicast interoperability in particular, the fundamental IPTV service information for each IPTV service provider (SP) should be announced to each SP. The purpose of IPTV service information exchange is to share the IPTV source information received from all IPTV service providers in the multicast-based IPTV service environment.

The IPTV service information for IPTV multicast interoperability can include the IPTV content provider information, source IP address block, multicast group information, service start and end times, QoS/QoE information, traffic rate, and video encoding rate.

Each IPTV service provider (SP) may have its own multicast address policy. The policy of IPTV SP's internal multicast address may not match the inter-service provider address policy.

8.3.1 Topology requirements

The multicast traffic exchange point could be located at any point of the network. Routers could be connected directly or indirectly using the tunnel mechanism. Note, however, that SPs must avoid the single point of failure.

– Centralized vs. distributed
  - Centralized multicast exchange point: SPs establish multicast peering at a centralized point.
  - Distributed multicast exchange point: Multicast traffic is transmitted at the closest regional point of presences (PoP) to maximize resource utilization.

– Multi-homing vs. single-homing
  - Multi-homing: In this topology, a customer Internet service provider (ISP) peers with a single-backbone ISP or two-backbone ISPs for failure redundancy and traffic load balancing. One of the many cautions in this topology is that the customer ISP should advertise only its local autonomous system (AS) information without transiting another ISP's multicast traffic.

8.3.2 MBGP policy

The following should be considered as peering policy wherein Multiprotocol Border Gateway Protocol (MBGP) [IETF RFC 2858] is used for the multicast routing protocol between IPTV service providers:

– Advertising summarized prefixes:

  Increasing the routing table size is cumbersome in inter-ISP environments. A summarization technique such as classless inter domain routing (CIDR) can be used to control the growth of the routing tables.

– Route filtering policy:

  Filtering the following destinations or addresses is recommended: default routing information, private addresses defined in [IETF RFC 1918], all multicast groups (224/4), and ISP's unicast prefix range from peer ISP.

– AS path filtering:

  One ISP can permit only routes sourced from the peering ISP and deny routes from its customer AS. In this scenario, the AS path filtering technique is conveniently used to filter out unwanted routes of AS.

– Maximum prefix limit:

  MBGP routers can receive more routes than they can take. This results in an MBGP problem, which could disrupt multicast service delivery. With the maximum prefix limit feature, it is possible to protect a router against this situation. This feature allows controlling how many prefixes can be received from a neighbour.

– Message Digest 5 **(**MD5) authentication between MBGP peers:

  MD5 authentication can be used between two MBGP peers. With this, each segment sent on the TCP connection between peers is verified to protect against denial of service attacks.

In the IPTV multicast interoperability environment, IPTV service providers should provide the QoS monitoring function to handle the IPTV services quality measurement including the QoS management function for consistently high–quality IPTV service.

9 Deployment guidelines for group management

9.1 IPTV multicast address management

According to rules of the Internet Assigned Numbers Authority (IANA), several hundred millions of IPv4 and IPv6 multicast addresses can be used in the Internet. As one of the important resources, these multicast addresses should be managed effectively.

9.1.1 IP multicast address transition

When deploying linear TV services, service providers often use one multicast group address representing an IPTV channel. Unlike the unicast addresses, multicast addresses are not distributed depending on different countries, areas, and service providers all over the world. Therefore, during the operation of the linear TV service, the corresponding relationship between the IPTV channel and multicast address can be overlapping or conflicting among different service providers or different network providers.

Figure 9-1 shows service provider A and service provider B wanting to interconnect their IPTV services; and service provider B initiating a local IPTV service within network providers C and D where the service providers should interconnect for content delivery. With regard to these IPTV multicast traffic crossing multiple network provider domains, IP multicast address transition needs to be deployed at the edge of each network provider domain to check the multicast service traffic

from other domains. If it is detected that the multicast address of the IPTV content from the other domain is conflicting with the multicast address allocated in the local domain, the multicast address of IPTV content coming from other domains should be changed before entering the local domain.

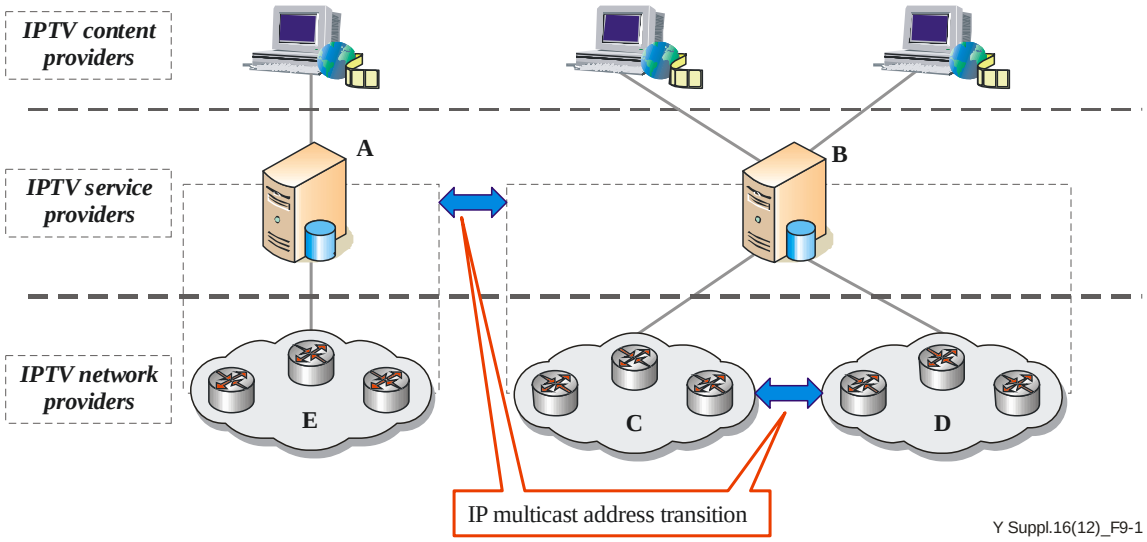

Figure 9-1 – IPTV multicast address transition

9.1.2 Control of users' multicast addresses

As the demand on multi-user applications (such as distance learning, online games, and video conference) increases, multicast services can autonomously use the multicast addresses in the network provider's domain. To avoid impact on the IPTV services from the other multicast services, IPTV service providers can deploy the multicast service controller to manage the uniform distribution of multicast addresses.

For multicast application without a registration, however, service providers will restrict the usage of these multicast addresses at the access point of the network provider domain. The procedures for applying for multicast service and multicast address are shown in Figure 9-2.

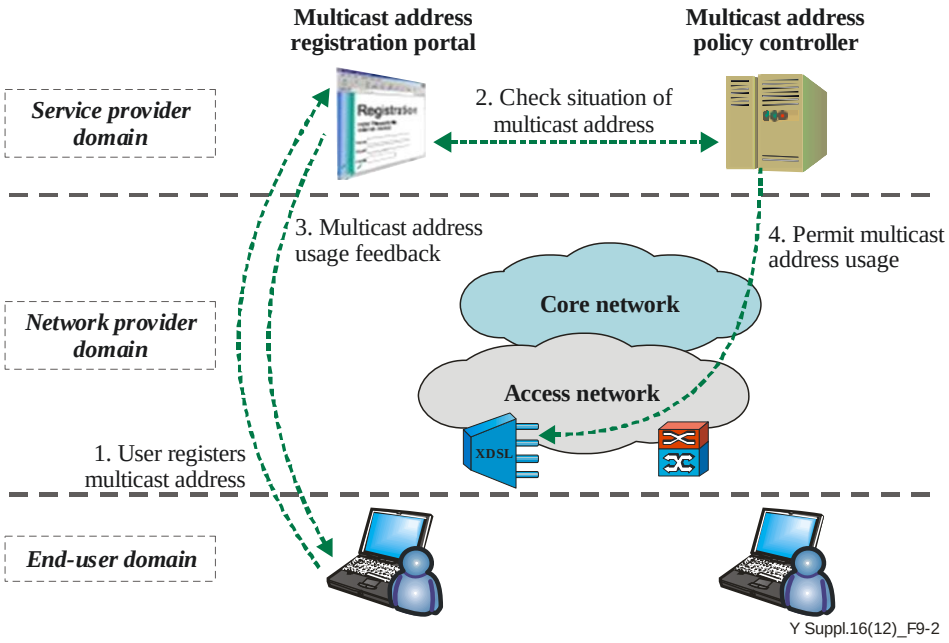

Figure 9-2 – Control procedure for multicast address

The interactions shown in Figure 9-2 are as follows:

1) To carry out services based on the multicast address, users should arrange the inquiry and registration on the portal of the SP-provided multicast address and service control platform.

2) The self-service system checks the situation of this multicast address from the multicast address policy controller.

3) If this multicast address is available, users will be told that they are allowed to use it.

4) At the same time, the multicast address policy controller sends policies to the access point to allow access to the multicast services.

9.1.3 IPTV channel domain name management function for IPTV service providers

The function of IPTV channel domain name management is optional for IPTV service providers to represent their multicast IPTV channels with a constant identifier (i.e., domain names) rather than multicast IP addresses. With this function, IPTV service providers register the domain names of their multicast channels with the help of Domain Name Service (DNS) providers and bind multicast IP addresses with these domain names dynamically.

The procedures for providing IPTV channels with domain names are as follows:

– multicast resources (i.e., multicast IP addresses) for IPTV services are managed by network operators;

– network operators allocate to IPTV service providers multicast IP addresses with which IPTV service providers can carry their multicast channels into the service;

– there are DNS service providers maintaining DNS servers and providing DNS services (domain name registration, domain name query) to the public;

– with the domain name registration service provided by DNS service providers, IPTV service providers manage the domain names of their multicast channels. The following actions can be used:

  • Channel registration: Register the domain name of an IPTV channel with a multicast IP address obtained from network operators;

  • Channel deregistration: Deregister the domain name of an IPTV channel and withdraw the multicast IP address assigned to this channel;

  • Channel rearrangement: Modify the domain name registration of IPTV channels;

– IPTV service providers represent their multicast channels with domain names when they release the Uniform Resource Identifier (URI) information of these channels (such as in the Electronic Program Guide (EPG));

– multicast IPTV channel servers get the address information of the channel by DNS query before broadcasting IPTV contents to the multicast address;

– end users access the multicast IPTV channels by their domain names.

Aside from the obvious advantages of representing multicast IPTV channels with domain names, this solution is advantageous to IPTV service providers in the following two aspects:

– the solution allows IPTV service providers to represent multicast IPTV channels with domain names even when network operators do not deploy the IPTV multicast address/domain name management function;

– the solution provides an efficient way for IPTV service providers to manage dynamically their multicast resources (multicast IP addresses) obtained from network operators. Rearranging multicast addresses among their multicast IPTV channels has little impact on other aspects.

9.1.4 IPTV multicast address allocation

If interoperable multicast channels are supported, the IPv4 multicast addresses for the IPTV service should be in the range of [IETF RFC 3180], and the IPv6 multicast addresses, in the range of [IETF RFC 3307].

The IPTV service can optionally use the IPv4 multicast addresses in the range of [IETF RFC 3138] or [IETF RFC 2365] based on an agreement between peering IPTV service providers.

If source specific multicast (SSM) is used for IPTV multicast content delivery, the IP multicast addresses should be in the range of [IETF RFC 4607].

9.2 IGMP policy

9.2.1 Different versions of IGMP and MLD

IGMP and MLD are used by terminal devices to join or leave the multicast groups or channels of IP version 4 and IP version 6, respectively.

They are used between an IP multicast capable end system (e.g., IPTV terminal device) and an IP multicast capable router. IGMP and MLD are available in different versions.

The following indicates the main characteristics of each IGMP and MLD version:

– IGMPv1 [IETF RFC 1112]: IGMPv1 is the initial version of IGMP. Since IGMPv1 does not support a "Leave Message", IGMPv1 was not widely implemented but was replaced by IGMPv2/IGMPv3. IGMPv1 supports only the ASM model.

– IGMPv2 [IETF RFC 2236]/MLDv1 [IETF RFC 2710]: IGMPv2 added the capability of the terminal device leaving a multicast group by sending "Leave Messages" to the next node. IGMPv2/MLDv1 supports only the ASM model; both protocols are widely deployed today.

– IGMPv3 [IETF RFC 3376]/MLDv2 [IETF RFC 3810]: The main difference lies in the support of filter mechanisms (exclude/include filter) to support source specific multicast (SSM). IGMPv3/MLDv2 supports the ASM and SSM service models.

9.2.2 Transparent IGMP snooping

IGMP snooping optimizes the distribution of multicast within a layer-2 bridging domain where no IGMP capable router is placed, so multicast traffic is only sent on bridge ports where there are known active receivers and/or multicast routers. The IGMP snooping functionality resides on the bridging devices that connect IGMP hosts to IGMP routers and consists of two main components. The first function is the IGMP snooping control section that does the following:

1) Monitors IGMP messages (and other multicast router messages optionally, such as PIM or DVMRP hello packets) to determine the port location of the multicast routers and active receivers within a bridging domain.

2) Builds per port, per VLAN multicast forwarding tables.

3) Maintains basic IGMP membership state on non-router ports to determine when a forwarding entry should be removed.

The second function is the data forwarding section that does the following:

1) Forwards packets in the 224.0.0.0/24 range, which are not IGMP messages on all ports.

2) Forwards multicast packets with destination IP address outside 224.0.0.0/24, which are not IGMP according to per VLAN, per port multicast forwarding tables.

This basic mode of operation is often referred to as "transparent IGMP snooping"; it neither absorbs nor alters nor generates IGMP messages when performing the aforesaid functions.

9.2.3 IGMP proxy

IGMP proxy is a function to reduce the number of IGMP/MLD messages in a network and to enable a device to communicate with a multicast-enabled router without using an IP multicast routing protocol.

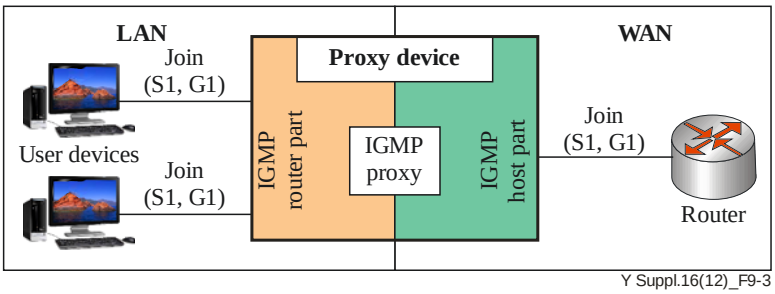

Figure 9-3 – Functional model of IGMP proxy

If more than one upstream interface is available (e.g., different VLANs) the following rules apply:

– "Simple Mode" – only one upstream interface for IGMP/multicast:

  If only one upstream interface needs to support multicast and IGMP, it should be possible to select the proxy interface via static configuration or dynamic mechanism such as a multicast default route using DHCP option 121 (classless static route option).

– "Extended Mode" – different upstream interfaces for IGMP/multicast:

  More than one upstream interface needs to support multicast and IGMP (e.g., different service VLANs). In this scenario, the multicast group's multicast channels need to be configured on the corresponding interfaces, e.g., 239/8 on interface #1 and 232/8 on interface #2. The proxy needs to separate the address spaces, e.g., IGMP report on interface #1 must not include information on multicast groups/channels on interface #2. The device must support a mechanism to configure (assign) the multicast groups/channels to the corresponding upstream interfaces. This can be done using static configuration (pre-configured device, using a GUI, etc.) or dynamic mechanism.

– "Forking Mode":

  In this mode, IGMP reports are sent to more than one upstream interface. Queries will be answered on all upstream interfaces configured for "Forking Mode"; reports include information on all multicast groups/channels to which Customer Premises Equipment (CPE) is subscribed. Part of the responsibility of the receivers of the membership reports is to take action on the received reports. In a standard scenario, only one of the receivers will forward multicast traffic to avoid duplicate traffic. Other network components can act on the membership reports (e.g., change filters or QoS settings) without forwarding the traffic (see Figure 9-4).

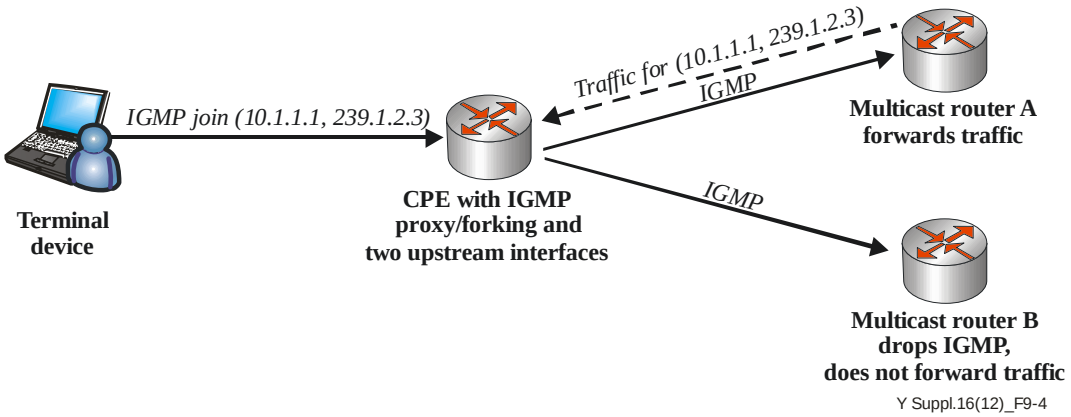

Figure 9-4 – IGMP Proxy in forking mode

9.2.4 Fast leave/immediate leave

This is a function associated with IGMP snooping or IGMP routing wherein the switch or router stops sending the multicast stream immediately upon receiving an IGMP leave for the last member on this requesting interface, i.e., without sending one or more group-specific queries and waiting for its timeout.

9.3 IPTV multicast user management

Since the current multicast group management protocols (e.g., IGMP and MLD) do not consider multicast user authentication and authorization, further development of those functions is requested to support IPTV services efficiently.

The multicast user authentication function controls the authority of users to receive multicast flows. By authenticating multicast users, the network can distinguish legal multicast users from the illegal ones and subsequently distribute the multicast traffic to the legitimate receivers. The following procedures should be considered:

– when a user initiates a multicast "join" request to join a certain multicast group with an account, the duplication point should not accept the request but make the user join the group at once and must send the request to the authentication point;

– the authentication point queries the account information database and returns the result to the multicast duplication point. The value of the user's multicast property in the account should be set by the service layer system;

– according to the authentication result returned from the authentication point, the Multicast duplication Point should decide whether to allow the user to join the group or not. If the user is allowed to join the group, the duplication will add it to the distribution table. Otherwise, it will reject the user's request to join the group.

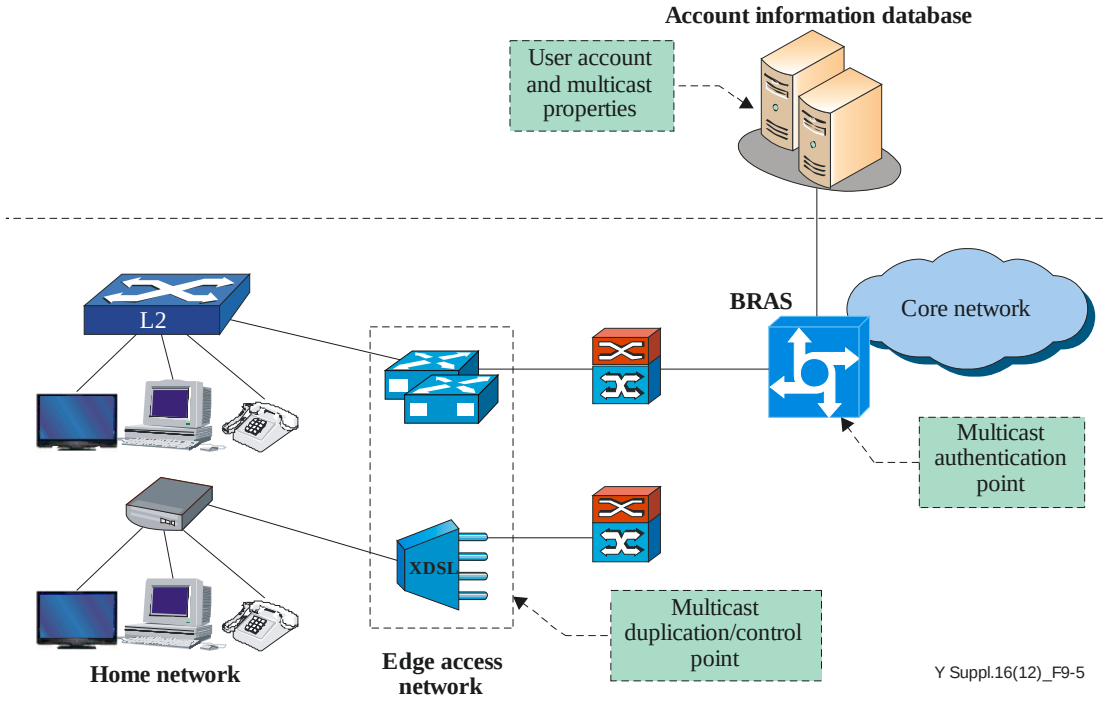

Figure 9-5 – Example of network architecture and functional components for multicast user management

10 Deployment guidelines for QoS control

10.1 Types of IPTV multicast QoS

There are two types of QoS for IPTV multicast.

The first one is end-to-end QoS experienced by end users during the delivery of IPTV service traffic to IPTV end users. This kind of QoS can be guaranteed or maintained by resource reservation mechanisms or congestion control mechanisms. The IPTV network provider can guarantee QoS by using a resource pre-reservation mechanism. The pre-reservation mechanism is more efficient than the dynamic resource reservation mechanism since the latter needs to manage dynamic membership with many receivers. Moreover, the pre-reservation mechanism is simple to use in controlling and maintaining multicast resources.

The second one is the topological QoS of the multicast-enabled network, which may affect the availability and responsiveness of IPTV services. This kind of QoS can be improved by optimizing multicast network design and minimizing the service interruption time for an internal network failure.

The design of multicast network topology needs to consider how to position Rendezvous Points (RPs). RP positioning is related to the network burden and service response time. RP redundancy should also be considered to minimize service interruption for active RP failure. Multicast traffic is forwarded along the multicast distribution tree generalized by the multicast routing protocol such as PIM. Since the multicast routing protocol runs over interior gateway protocols such as Open Shortest Path First (OSPF), maintaining stable routing is critical in improving multicast service stability. The network device itself is another frequently occurring failure point, thereby necessitating the application of high-availability feature to detour multicast service traffic as quickly as possible.

10.2 End-to-end multicast QoS guarantee policy

10.2.1 Inbound/outbound QoS policy

Many ISPs providing multicast services have partial or full deployment of Diffserv [IETF RFC 2475] implementations in their networks today, either across the entire network or minimally on the edge of the network. In inter-AS environments as well, they should provide a set of QoS policies such as traffic classification, rewriting, and scheduling rules for the reliable transport of multicast traffic.

10.2.2 Policing of multicast and unicast traffic based on contract

ISPs should provide a set of policing mechanisms that could be configured on the inter-AS links to ensure that traffic routed through the links does not exceed the bandwidth negotiated among them.

10.3 QoS-aware topology for IPTV multicast service

10.3.1 Optimal RP positioning and RP redundancy

The location of a rendezvous point (RP) affects not only multicast service delay but also multicast network stability. A rendezvous point (RP) is recommended to support optimal RP positioning, which depends on the service providers' network topology and multicast traffic path that takes into account the following:

– loop-free, delay/jitter-independent, stability guarantee topology;

– optimal position to exchange source active information among multicast service providers.

One of the main reasons for applying multicast is to reduce the backbone traffic produced by redundant customers' request. Thus, it is advantageous to locate an RP near the source instead of locating it somewhere in the middle of the backbone.

A rendezvous point is recommended to support the RP redundancy mechanism; the IPTV network provider should guarantee optimized RP redundancy to improve IPTV service stability in case of RP failure. Likewise, the IPTV network provider should have its RP mechanism designed not only to maximize service stability but also to minimize the service recovery time during RP failure.

Once multicast-based IPTV service providers decide the optimal RP position in their multicast network, they need to consider how to configure RP to maximize service efficiency. There are basically two ways of selecting RP: one is dynamic RP selection, and the other is static RP selection. It is often difficult to determine that one way is superior to the other. Thus, multicast-based IPTV Service Providers should decide which way is the best for their own multicast network. When multicast-based IPTV service providers design their RP, they should consider the following:

– Service recovery time in RP failure: In case of RP failure, service recovery time should be minimized. Normally, static RP recovers quicker compared to dynamic RP.

– Operation issues (configuration and troubleshooting): RP should be designed such that it should not incur too much operational overhead but should be advantageous to troubleshooting. In case of a static RP, all routers running the multicast routing protocol such as PIM-SM must include adequate configuration to designate their RP. Note, however, that the dynamic RP does not require duplicate configuration for all routers. For troubleshooting, a dynamic RP normally requires much more complicated steps to track the problem compared with a static RP, which is relatively much simpler to troubleshoot.

– Feasibility issues (RP selection policy): When selecting the RP in a dynamic manner, one thing to keep in mind is that an identical RP should always be selected for the groups in a network. RP for group "A" should be RP "A"; it cannot be any other RP for that group. However, there could be compatibility issues among multicast routers because they may use different policies for selection of a primary RP among the RP candidates. Thus, it is essential to check if they all work in an expected manner.

Anycast RP has been widely adopted in existing IPTV multicast solutions for service robustness and scalability and to realize load balancing as well. The best working examples of anycast RP in IPTV are anycast RP redundancy and anycast source. The anycast RP mechanism is intended to address the need for better fail-over (or shorter convergence time) and load sharing of source register messages among RPs in a domain.

10.3.2 Load balancing of IPTV multicast

When multicast routers receive a join message, the multicast routing protocol normally sends its join message to one of the multicast interfaces. If some groups have the same source among multiple multicast interfaces, only one of them is selected to send the join message. In an equal cost multiple path (ECMP) environment, all multicast interfaces cannot be used to distribute multicast traffic; instead only a single interface is used. For the load sharing of the traffic, a multicast source should be distributed for different groups.

10.3.3 Multiple multicast trees of IPTV multicast

Multiple multicast trees include many multicast trees, with each tree constructed from the multicast source to the receivers and the multicast data delivered among all the multicast trees.

10.4 High availability

Two most critical quality factors to increase IPTV service stability are channel zapping time and service recovery time for network failure. Although not foolproof, these two factors can minimize defects by improving network availability.

Unlike data services, IPTV services are delay-sensitive and jitter-sensitive. Customers for data services may not recognize an instant network failure, but IPTV customers easily do since IPTV services may pause or may not even display at all. When there is network failure, multicast traffic is recovered after the total routing status is restored. Thus, it is essentially difficult to guarantee nonstop forwarding for multicast traffic. SPs need to optimize the decrease in service recovery time such that routing status recovery time is shortened and multicast traffic is maintained as close as possible to the customer side.

The approaches to support high availability of IPTV services are as follows:

– Static IGMP join:

  Static join can decrease service delay by maintaining multicast traffic to the places close to customers. Not only can the application of static join decrease the service impact of intermediate link and node failure; it also shortens the service delay time. Although static join has many advantages, it consumes network resource especially in an access network. Thus, the feature should be applied within the SPs' environment.

– PIM, IGP, and BGP graceful restart:

  Multicast services are affected the most by network link failures and/or routing protocol neighbour down. There have been graceful restart techniques to avoid temporary service disruption during a link failure and neighbour down. If these techniques are applied along with static join, SPs can improve multicast service stability during temporary outages. One thing to take note of is that the graceful restart feature may give rise to compatibility issues among different network elements, so the network providers should validate if all the network elements inter-work with each other.

– Fully redundant network architecture and topology:

  The network provider should provide fully redundant network architecture and topology such that a single point of failure does not affect the entire network.

– Robust network against DoS attacks:

  The network provider should design the network to be robust such that it can tolerate unexpected DoS attacks.

– In-service software upgrade (ISSU):

  By the in-service software upgrade (ISSU) feature, the multicast service should not be affected even during the maintenance period such as software upgrade.

10.5 Quality measurement of IPTV services

In providing IPTV services over IP multicast for the residential customer or providing the company's internal linear TV services and advertisement services, functions to measure the service quality of IPTV are needed to provide high-quality IPTV services or to provide QoS-guaranteed IPTV services. Even though it is possible to consider from the multi-branch side which embodies IPTV service quality measurement as well as the control facility, there is a need to select the server-client measurement model that is most feasible.

Using the statistics based on the information of the measurement data received from the terminal devices, IPTV service quality measurement and service quality management can be done. The quality measurement information produced by the terminal device is transmitted to the IPTV service quality management server and can be applied as real-time quality measurement data.

For the quality measurement of IPTV services over IP multicast, a client-server model can be used as an example as shown in the following figure:

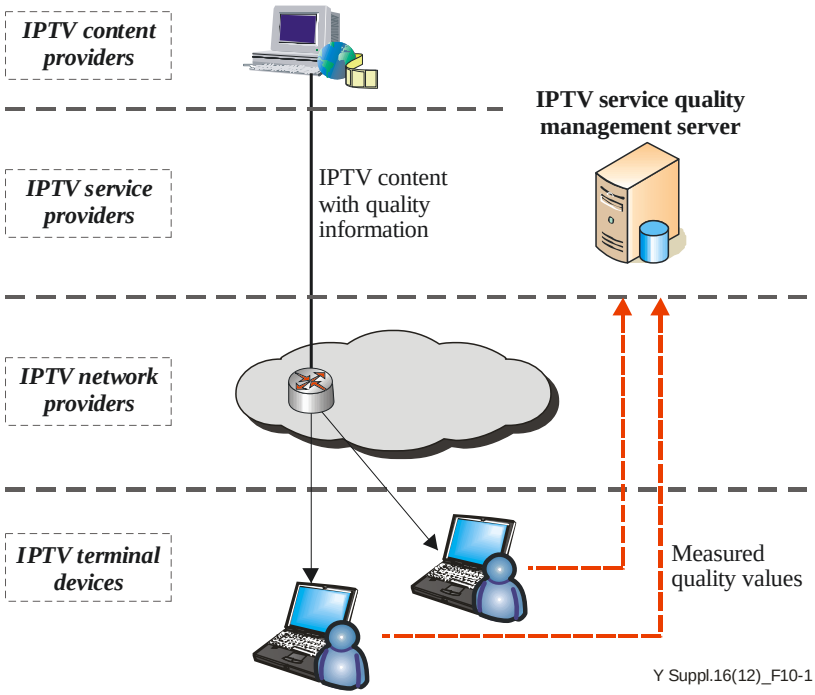

Figure 10-1 – IPTV service quality measurement using a client-server model

In this model, a content source sends the signal information to terminal devices in each media's data frame header. Based on this information, the terminal device measures the service quality and transmits an aggregated result of such measurement data to an IPTV service quality management server.

The measurement data may consist of the following information:

– Multicast group information:

  The multicast group's IP address and port information are delivered from the content source to terminal devices during the linear TV connection time. Such information is used for checking whether the multicast group information is correct or not.

– Terminal device information:

  If terminal devices start to receive linear TV content, the IPTV service quality management server that implements the IPTV service control functions can get information on each terminal device's IP and media access control (MAC) addresses. Such information is used for checking the device's status.

– Video type information:

  When receiving IPTV content, terminal devices get video information such as video size and codec type received from the content source. Such information is used for video quality measurement data.

– Video frame information:

  - By checking the timestamp and sequence number of the media data header, it is possible to get the exact time information on frame reception and remaking;
  - The sequence number is a consecutive one; its unusual increase can be regarded as a case of IPTV service frame loss, so it can be used as a service quality measurement factor;
  - From the decoding procedure of media data, it is possible to obtain the I, P, and B frame information that can be used as service quality measurement information.

– Bitrate information:

  - The bitrate information can also be used for the IPTV service quality measurement factor.
  - Bitrate (bit/sec) = data size/time.

Finally, these IPTV service quality measurement data will be transmitted to the service quality management server periodically. In this case, there is a need to define a transmission protocol and the specific transmission method in each network.

11 Deployment guidelines for security

Providing reliable IPTV service depends heavily on how to build a multicast network that is robust against both expected and unexpected malicious attempts and how to protect service content efficiently.

Consumers are provided by IPTV service providers with either their own content or the content provider's asset throughout the network provider's medium. Thus, the ability to protect both IPTV content providers and end-users' rights is a key factor for successful service deployment.

In the following, this clause identifies issues that need to be considered for IPTV multicast security in the domain of IPTV network provider.

11.1 Rendezvous point security

– RP group range filtering:

  All multicast groups send join messages to the RP in a domain by default. When configuring the RP, there is a need to designate specific group addresses to prevent unwanted groups from sending join messages and consequently ease RP overload.

– PIM register message filtering:

  Every first hop router sends source registration to RP once it receives multicast packet from any source. RP needs to apply the PIM register message filter to prevent unwanted sources from sending by bogus sources.

– MSDP SA filter:

  MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains via MSDP Source Active (SA) messages. MSDP SA messages contain source and group information for RPs in PIM-SM domains and exchange SA messages without filtering them for specific source or group addresses by default. The MSDP SA filter is necessary to prevent bogus (S, G) sending.

  The following should be taken into account for the MSDP filtering policy wherein MBGP is used for multicast routing protocol between IPTV SPs:

  - Domain-local multicast applications
  - Auto-RP groups
  - Administrative scope groups (239/8)
  - Default SSM range (232/8)
  - Loopback addresses (127/8)
  - Private addresses (range of [IETF RFC 1918])

11.2 PIM router security

– Multicast route limit:

  This feature is necessary to limit the impact of denial of service attacks based on the creation of bogus IP multicast routing states.

– BSR message filtering:

  If RP selection is selected in a static manner, bootstrap messages should be blocked to prevent RP from overriding the information. Fault RP information can be inserted and spread into the network by malicious users, resulting in source interception or service failure. If SP's domain does not use bootstrap messages to select RP, blocking bootstrap messages in multicast routers is recommended.

– PIM authentication among neighbours:

  The definition and purpose of this feature are the same as those of IGP/BGP authentication. Blocking PIM neighbourship facing customer interfaces is highly recommended to prevent unwanted information from spreading out.

– TCP/ICMP message filtering:

  Multicast traffic is transported using UDP. Blocking any and all TCP and Internet Control Message Protocol (ICMP) packets destined for all multicast addresses at all multicast routers is recommended.

11.3 Last-mile PIM router security

In the last mile, there is a need to apply filtering to block spoofed customer IP, multicast sources sent from the customer side, and PIM neighbourship with customer facing interface.

11.4 Security policy over multicast exchange peers

IPTV network providers should protect their own multicast-enabled network and IPTV content sources against malicious traffic injection from peering SPs. This function should be implemented in the IPTV multicast interoperability peering point. The following should be considered as the security policy for IPTV multicast interoperability:

– uRPF in exchange peer interface:

  Used for preventing source address spoofing, unicast reverse path forwarding (uRPF) is the ability that allows the router to check if any IP packet received at a router interface arrives on the best return path (return route) to the source address of the packet. If received from one of the best reverse path routes, the packet is forwarded as normal. If there is no reverse path route on the same interface from which the packet was received, however, the packet is dropped.

– PIM authentication:

  The purpose of this feature is authenticating the peer's identity to maintain reliable PIM neighbourship between two ISP's PIM peers.

– Protection against multicast source spoofing:

  There is a need to apply filtering to block spoofed IP addresses and multicast sources sent from peering ISP.

– BSR message filtering:

  Fault RP information can be inserted and spread into the network by malicious users, thereby resulting in source interception or service failure. Blocking bootstrap messages in domain exit points is recommended because there is no need to use bootstrap messages among multicast domains.

12 Security considerations

The security issues of IP multicast deployment for IPTV services are provided in clause 11.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012