International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.1920

(07/2012)

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

Internet protocol aspects – IPTV over NGN

Guidelines for the use of traffic management mechanisms in support of IPTV services

Recommendation ITU-T Y.1920

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
Packet-based 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.3499
CLOUD COMPUTING	Y.3500–Y.3999

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

Recommendation ITU-T Y.1920

Guidelines for the use of traffic management mechanisms in support of IPTV services

Summary

Recommendation ITU-T Y.1920 describes a set of traffic management mechanisms which are aimed to facilitate the efficient support of IPTV services over the network infrastructure and provides guidelines on the use of the traffic management mechanisms in various IPTV services such as VoD and Live TV.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.1920	2012-07-29	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 Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation 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 Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation 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 Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. 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/.

© ITU 2013

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Recommendation ITU-T Y.1920

Guidelines for the use of traffic management mechanisms in support of IPTV services

1 Scope

This Recommendation defines functional requirements which are derived from the high-level requirements of traffic mechanisms in [ITU-T Y.1901]. Based on them, a set of traffic management mechanisms at the transport stratum in support of IPTV services are described from the perspectives of control plane, data plane and management plane. Guidelines on how such mechanisms can be used to effectively meet the functional requirements are also provided in detail.

The network supporting IPTV services will span a number of network domains which may be designed, deployed and operated by different providers and which may differ in their traffic management capabilities. Therefore, it is expected that the network provider(s) will implement a set of these mechanisms described in this Recommendation by following the guidelines to ensure that IPTV service objectives are satisfied efficiently. Furthermore, the traffic management mechanisms also depend on the specific network architectures used for IPTV services as defined in [ITU-T Y.1910].

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.1081] Recommendation ITU-T G.1081 (2008), *Performance monitoring points for IPTV*.

[ITU-T Y.1291] Recommendation ITU-T Y.1291 (2004), *An architectural framework for support of Quality of Service in packet networks*.

[ITU-T Y.1541] Recommendation ITU-T Y.1541 (2006), *Network performance objectives for IP-based services*.

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

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

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

3 Definitions

3.1 Term defined elsewhere

None.

3.2 Term defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AF	Assured Forwarding
BA	Behaviour Aggregate
BE	Best Effort
BRAS	Broadband Remote Access Server
BTV	Broadcast TV
CAC	Connection Admission Control
CLS	Controlled Load Service
CoS	Class of Service
CS	Class Selector
DF	Default Forwarding
DNGF	Delivery Network Gateway Functions
DSCP	Differentiated Services Code Point
DSLAM	Digital Subscriber Line Access Multiplexer
EF	Expedited Forwarding
GS	Guaranteed Service
HG	Home Gateway
IGMP	Internet Group Management Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
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
IPTV	Internet Protocol Television
LAN	Local Area Network
MAC	Media Access Control
MF	Multi-Field
MPEG	Moving Picture Experts Group
NAL	Network Adaptation Layer
NVoD	Near Video on Demand
OSPF	Open Shortest Path First

PHB	Per-hop Behaviour
PVR	Private Video Recorder
QoS	Quality of Service
RACF	Resource Admission Control Function
RSVP	Resource Reservation Protocol
SLA	Service Level Agreement
ToS	Type of Service
VLAN	Virtual LAN
VoD	Video on Demand
VoIP	Voice over IP
VTC	Video Teleconference
WAN	Wide Area Network
WLAN	Wireless LAN

5 Conventions

In this Recommendation, functional requirements are identified using the following convention:

– Functional requirement number xx in clause n.m is of the form FR n.m-xx.

6 Requirements

6.1 High-level requirements

Clause 6.2.2 of [ITU-T Y.1901] specifies the high-level traffic management requirements for IPTV services. For the convenience of the reader, the traffic management related mandatory requirements are listed below:

R 6.2.2-01: The IPTV architecture is required to support traffic management mechanisms for the differential treatment of IPTV traffic.

R 6.2.2-02: The IPTV architecture is required to support the ability to configure quality of service (QoS) rules at the delivery network gateway functions (DNGF) that govern traffic mapping (upstream or downstream) for the different IPTV services.

R 6.2.2-03: The IPTV architecture is required to support a mechanism for assigning IPTV traffic priorities.

R 6.2.2-04: The IPTV architecture is required to support the relevant mechanisms for IPTV traffic identification, classification and marking, policing and conditioning, scheduling and discarding.

6.2 Functional requirements

This clause describes the functional requirements, derived from high-level requirements, on three different planes: control plane, management plane and data plane.

6.2.1 Control plane functional requirements

FR 6.2.1-01: The traffic management mechanisms are required to support admission control capability.

FR 6.2.1-02: The traffic management mechanisms are required to support the capability of controlling network congestion and improve network utilization by selecting an appropriate path.

FR 6.2.1-03: The traffic management mechanisms are required to support exchanging the network traffic information with the network management systems.

6.2.2 Management plane functional requirements

FR 6.2.2-01: The traffic management mechanisms are required to enable policy control and management capabilities.

FR 6.2.2-02: The traffic management mechanisms are required to support capability of obtaining performance information for IPTV QoS assurance.

FR 6.2.2-03: The traffic management mechanisms are required to support service level agreement (SLA) capability in IPTV.

6.2.3 Data plane functional requirements

FR 6.2.3-01: The traffic management mechanisms are required to enable the differentiation of traffic to provide the expected delivery of IPTV services with corresponding level of quality and reliability.

FR 6.2.3-02: The traffic management mechanisms are required to support traffic marking capability to associate packets with different priorities.

FR 6.2.3-03: The traffic management mechanisms are required to support buffer management capability to deal with received packets.

FR 6.2.3-04: The traffic management mechanisms are required to support traffic queuing and traffic scheduling capability.

FR 6.2.3-05: The traffic management mechanisms are required to support traffic policing and traffic shaping capabilities for rate control.

FR 6.2.3-06: The traffic management mechanisms are required to support congestion management capability.

6.3 Mapping among high-level requirements, functional requirements and mechanisms

Table 1 – Mapping table among requirements, mechanisms and sections

High-level requirement	Related functional requirements	Related mechanisms	Related clause
R 6.2.2-01	FR 6.2.3-01	traffic classification	7.2 data plane
	FR 6.2.3-02	packet marking	
	FR 6.2.3-03	buffer management	
	FR 6.2.3-04	queuing and scheduling	
	FR 6.2.3-05	traffic policing and shaping	
R 6.2.2-02	FR 6.2.1-01	admission control	7.1 control plane
	FR 6.2.1-02	QoS routing	
	FR 6.2.1-03	resource control	
	FR 6.2.2-01	policy	7.3 management plane
	FR 6.2.2-03	service level agreement	

Table 1 – Mapping table among requirements, mechanisms and sections

High-level requirement	Related functional requirements	Related mechanisms	Related clause
R 6.2.2-03	FR 6.2.2-01	policy	7.3 management plane
	FR 6.2.2-02	performance measurement	
	FR 6.2.2-03	service level agreement	
R 6.2.2-04	FR 6.2.1-01	admission control	7.1 control plane
	FR 6.2.3-01	traffic classification	7.2 data plane
	FR 6.2.3-02	packet marking	
	FR 6.2.3-04	queuing and scheduling	
	FR 6.2.3-05	traffic policing and shaping	
	FR 6.2.3-06	congestion avoidance	

7 Traffic management mechanisms for control plane, data plane and management plane

IPTV traffic management mechanisms are typically used for dealing with IPTV service traffic directly as well as other user traffic. Traffic management systems enable delivery of IPTV services with required level of quality and reliability, and can be deployed with other network mechanisms as a comprehensive QoS solution.

This clause provides an overview of the basic traffic management mechanisms that are commonly deployed in a managed network. A provider may choose to deploy a subset of these mechanisms depending on the performance objectives of applications supported by the network.

The traffic management framework contains mechanisms dealing with the user traffic directly, the pathways through which user traffic travels, and the operation, administration and management aspects of the network. As depicted in Figure 1, its building blocks are organized into three planes: control plane, data plane and management plane.

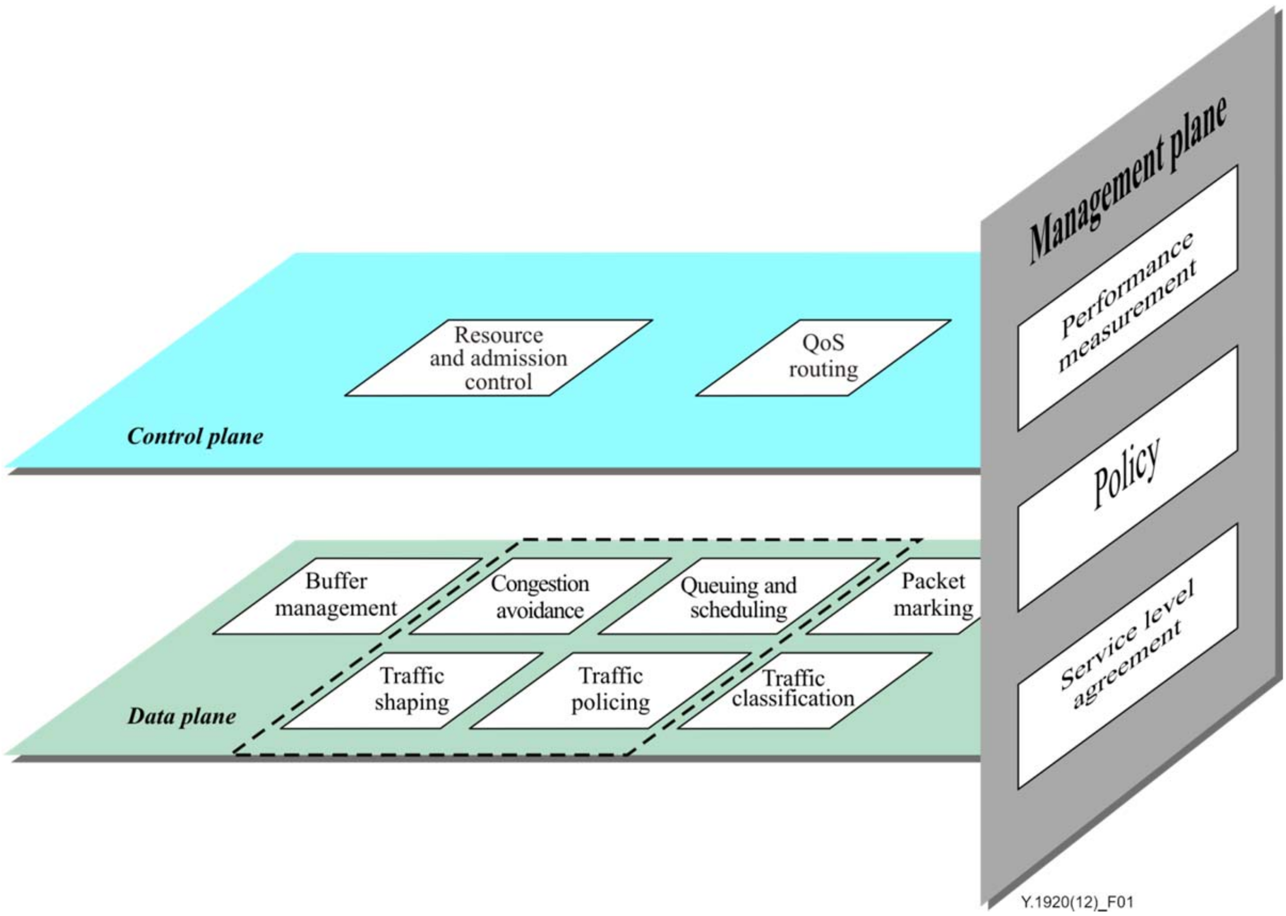

Figure 1 – Traffic management framework for QoS support

7.1 Control plane

7.1.1 Resource and admission control

The traffic management systems are recommended to be capable of supporting resource and admission control functions performed in a centralized or distributed way for the IPTV service, including traffic generated by end-users over the access and core network.

The role of the resource and admission control is to control the traffic to be admitted into the network, i.e., accept or reject IPTV services request based on the traffic demand and the current utilization of network resources. Normally the admission criteria are policy driven [b-IETF RFC 2753]. Whether traffic is admitted depends on an *a priori* SLA. In addition, the decision can depend on whether adequate network resources are available so that newly admitted traffic does not overload the network and degrade service for on-going traffic. For a service provider, the goal is to admit as much traffic as possible without degrading the quality of service of traffic flows already in progress. To achieve that, the network resource manager may be configured in the control layer to collect network information by means of data transmission between the network resource controller and the network nodes (e.g., digital subscriber line access multiplexer (DSLAM), broadband remote access server (BRAS), switches, routers, gateways) and provide them to the network management system. Meanwhile, resource and admission control meets requirements for IPTV multicast/unicast services as negotiated in the SLA. Specifically, the desired IPTV services reliability and/or availability can be requested as a priority level for resource and admission control. Resource and admission control mechanisms can efficiently support QoS assurance for IPTV services on a managed network. IPTV services supported by resource and admission control will meet unicast and multicast service demand for subscribers. Unicast resource and admission control ensures IPTV unicast services, such as video on demand (VoD) and time shifted TV. Multicast resource and admission control satisfies multicast services, such as broadcast TV (BTV) and near video on demand (NVoD). The policy of multicast admission control is triggered through subscribers joining multicast groups via IP multicast protocols (e.g., Internet group management protocol (IGMP) or multicast listener discovery protocol (MLD)).

There are two resource and admission controls for IPTV services: provider-based and subscription-based.

7.1.1.1 Provider-based resource and admission control for IPTV services

Provider-based resource and admission control uses the exchange of signalling between user equipment and provider.

As an example, a service provider may apply resource and admission control to IPTV services. The request for IPTV services involves the exchange of signalling between user equipment (e.g., set-top box) and the service provider video server. The service provider may reject the IPTV services request based on network resources, user status, or the current use of a specific program across all subscribers. Criteria such as user standing and the current use of a given program are related to policies set by the service provider and do not change very frequently.

As another example, a network provider may apply resource and admission control to IPTV services. Request for IPTV services involves exchanging of signalling between user equipment and network provider, e.g., by means of equipment that maintains subscriber privileges in a local database and may receive IPTV services request. Based on subscriber privileges, equipment may reject this request or forward it to network side transparently and then allow media stream to be transferred from network side to subscriber.

The effect of an IPTV services request on the network resources is dynamic and it varies based on the program requested. For instance, requesting high definition content will impose more demand on the network compared to the demand generated when standard definition content is requested.

7.1.1.2 Subscription-based resource and admission control for IPTV services

Currently, linear TV service is provided on a subscription basis through cable or satellite. Once subscribed, the linear TV service will continue without interruption unless subscription is terminated by either the provider or the end-user. This behaviour must also be allowed for IPTV services, i.e., linear TV service must continue to be on subscription basis. A service provider ensures that the network is properly engineered to accommodate the number of subscribers that match its business model.

There are scenarios where multiple set-top boxes may exist in a single home and reception of multiple video streams may be restricted due to the access bandwidth. For such cases the service provider may need to limit the number of streams admitted for a single subscriber. There are also times that a subscriber may request video streams that are denied due to insufficient bandwidth as per SLA.

7.1.2 QoS routing

The text in this clause is based on clause 7.2 of [ITU-T Y.1291] with modifications. This mechanism is used to control network congestion and improve network utilization by selecting an appropriate path. The path selected is most likely not the traditional shortest path. Depending on the specifics and the number of QoS metrics involved, computation required for path selection can become prohibitively expensive as the network size grows. Hence practical QoS routing schemes consider mainly cases for a single QoS metric (e.g., bandwidth or delay) or for dual QoS metrics (e.g., cost-delay, cost-bandwidth, and bandwidth-delay). To further reduce the complexity of path computation, various routing strategies can be utilized. Based on how the state information is maintained and how the search of feasible paths is carried out, different strategies such as source routing, hierarchical routing, and distributed routing can be used. Also based on QoS granularity and model expansibility, different mechanisms such as IntServ, DiffServ and IntServ over DiffServ (refer to [b-IETF RFC 2998]) can be used. In an IntServ over DiffServ in which the network is divided into several QoS domains, the QoS domain is divided into a QoS domain connected to the source terminal, a QoS domain connected to the destination terminal and other intermediate QoS domains. Each QoS comprises a plurality of QoS edge routers and a plurality of QoS core routers. A QoS server adopts its own resource allocation scheme so that end-to-end QoS can be achieved based on resources allocated in a single QoS domain or multiple QoS domains. In addition, depending on how multiple QoS metrics are handled, mechanisms, such as metric ordering and sequential filtering can be used, which may trade global optimality with reduced computational complexity [b-IETF RFC 2386].

The path selection process involves the knowledge of the flow's QoS requirements and characteristics and (frequently changing) information on the availability of network resources (expressed in terms of standard metrics such as available bandwidth and delay). The knowledge is typically obtained and distributed with the aid of signalling protocols. For example, the resource reservation protocol (RSVP) [b-IETF RFC 2205] can be used for conveying a flow's requirements and characteristics and open shortest path first (OSPF) extensions as defined in [b-IETF RFC 2676] for resource availability. Compared to shortest-path routing, which selects optimal routes based on a relatively constant metric (i.e., hop count or cost), QoS routing tends to entail more frequent and complex path computation and more signalling traffic.

It is important to note that QoS routing provides a means to determine only a path that can likely accommodate the requested performance. To guarantee performance on a selected path, QoS routing needs to be used in conjunction with resource reservation to reserve necessary network resources along the path.

QoS routing can also be generalized to apply to traffic engineering. (Concerning slowly-changing traffic patterns over a long time scale and a coarse granularity of traffic flows, traffic engineering encompasses traffic management, capacity management, traffic measurement and modelling, network modelling, and performance analysis.) To this end, routing selection often takes into account a variety of constraints such as traffic attributes, network constraints, and policy constraints [b-IETF RFC 3272]. Such generalized QoS routing is also called constraint-based routing.

7.2 Data plane

Traffic management in data plane is a set of generic network mechanisms for controlling the network service response to a service request, which can be specific to a network element, or for signalling between network elements, or for controlling and administering traffic across a network, mainly including bandwidth allocation, packet classification/marking, congestion management, congestion avoidance, traffic policing, traffic shaping, etc.

The basic processing sequence is shown in Figure 2. It describes the traffic processing procedure of transport functions in the data plane, mainly including traffic classification, traffic conditioning, traffic schedule and queues, etc. The detailed procedure for traffic processing is described in clause 7.2.

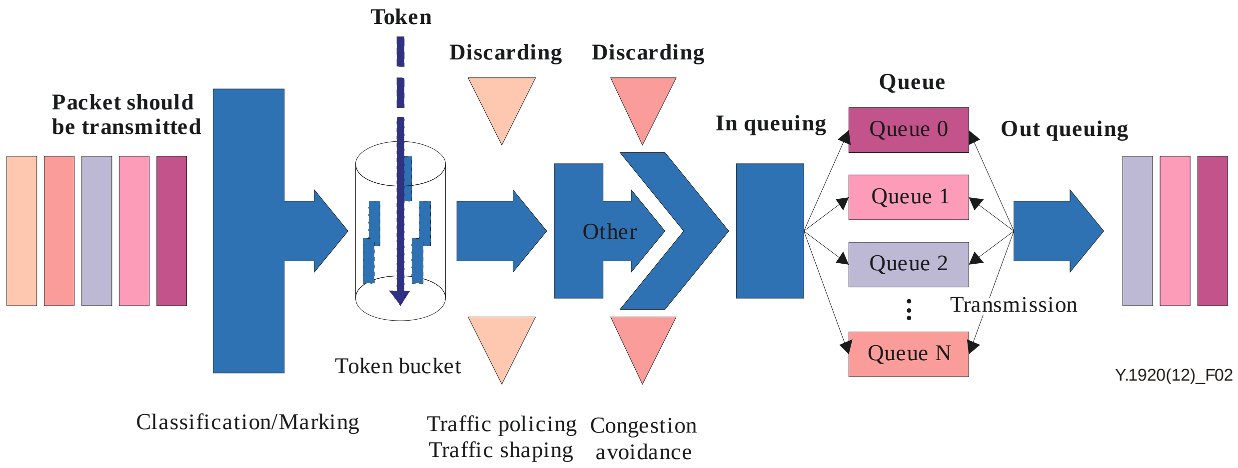

Figure 2 – The basic processing sequence of traffic

7.2.1 Traffic classification

In traffic management, packet classifiers are used to select packets in a traffic stream based on the content of some portion of the packet header. The behaviour aggregate (BA) classifier classifies packets based on the differentiated services (DS) code point only. The multi-field (MF) classifier selects packets based on the value of a combination of one or more header fields, such as source address, destination address, DS field, protocol ID, source port and destination port numbers and other information such as incoming interface. It is recommended to follow the guidelines specified in [b-IETF RFC 4594].

7.2.2 Traffic conditioning

A traffic conditioner which refers to [b-IETF RFC 2475] is an entity that performs traffic conditioning functions where meter, marker, shaper and dropper are optional. A traffic stream is selected by a classifier, which steers the packets to a logical instance of a traffic conditioner. A meter is used (where appropriate) to measure the traffic stream against a user profile. The state of the meter with respect to a particular packet (e.g., whether it is in- or out-of-profile) may be used to affect a marking, dropping or shaping action.

During traffic conditioning, the following are required in access network for supporting multimedia services such as IPTV services:

- QoS provisioning per subscriber and per service;
- traffic classification based on multiple header fields (e.g., 5-tuple or 6-tuple);
- minimum bandwidth guarantee;
- traffic shaping/policing;
- advanced packet queuing and scheduling;
- packet marking IP differentiated services code point (DSCP), Ethernet priorities [b-IEEE 802.1q], etc.);
- congestion avoidance.

7.2.3 Buffer management

Queue or buffer management deals with which packets, awaiting transmission, to store or drop. An important goal of buffer management is to minimize the steady-state buffer size while not underutilizing the link, as well as avoiding the monopolization of the available buffer space by a single flow [b-IETF RFC 2309]. Schemes for buffer management differ mainly in the allocation of the buffer space and the criteria for dropping packets.

A common criterion for dropping packets is the buffer reaching its maximum size. Packets are dropped when the buffer is full. Determining which packet to drop depends on the drop disciplines, for example:

- "Tail drop" drops newly arriving packets. This is the most common strategy since it is easy to implement.
- "Front drop": A buffer space for newly arriving packets is made available by dropping the packet at the front of the queue, provided that the length of the newly arriving packet is less than or equal to the dropped packet.
- "Random drop": A buffer space for the newly arriving packet is made available by randomly choosing a packet to drop from the queue, provided that the length of the newly arriving packet is less than or equal to the dropped packet.

7.2.4 Traffic queuing and scheduling

This mechanism controls which packets to select for transmission on an outgoing link. Incoming traffic is held in a queuing system, which is made of, typically, multiple queues and a scheduler. Governing the queuing system is the queuing and scheduling discipline it employs. There are several key approaches such as first-in-first-out and round-robin, which have been defined in [ITU-T Y.1291].

7.3 Management plane

7.3.1 Performance measurement

The performance of complete IPTV service delivery to an end user can be monitored by service provider/network provider at the performance monitoring points [ITU-T G.1081]. Monitored performance characteristics, across a single domain or multiple domains, can be integrated with existing or new operations support systems (OSSs) and/or network management systems (NMSs) for IPTV service and network elements to meet the appropriate performance objectives.

7.3.2 SLA

A SLA in IPTV service typically represents the agreement between an end user and one or more providers of IPTV service that specifies the level of availability, service delivery, performance, operation, billing compensations or other attributes of the IPTV service. It may include the parameters and their values that define the IPTV service offered to an end user by a network. Overall, [b-ITU-T E.860] defines a general SLA framework for a multi-vendor service.

7.3.3 Policy

A policy is typically a set of rules which represents the provider's equipment operation and management criteria for resource usage and access. It can be specific to the needs of objective statements identified in SLA(s). The service and/or network provider can implement mechanisms in the control plane to manage its IPTV service based on policies. Policy-based admission control functionality, such as the resource admission control function (RACF) [b-ITU-T Y.2111], is recommended to be deployed by the IPTV service provider and/or network provider over the IP network for ensuring stable IPTV service provisioning and management.

8 Guidelines to use IPTV traffic management mechanisms

This clause consists of two parts: mapping of traffic management mechanisms into the corresponding functions in IPTV functional architecture and usage guidelines of such mechanisms for IPTV services.

8.1 Mapping of traffic management mechanisms to functions in IPTV functional architecture

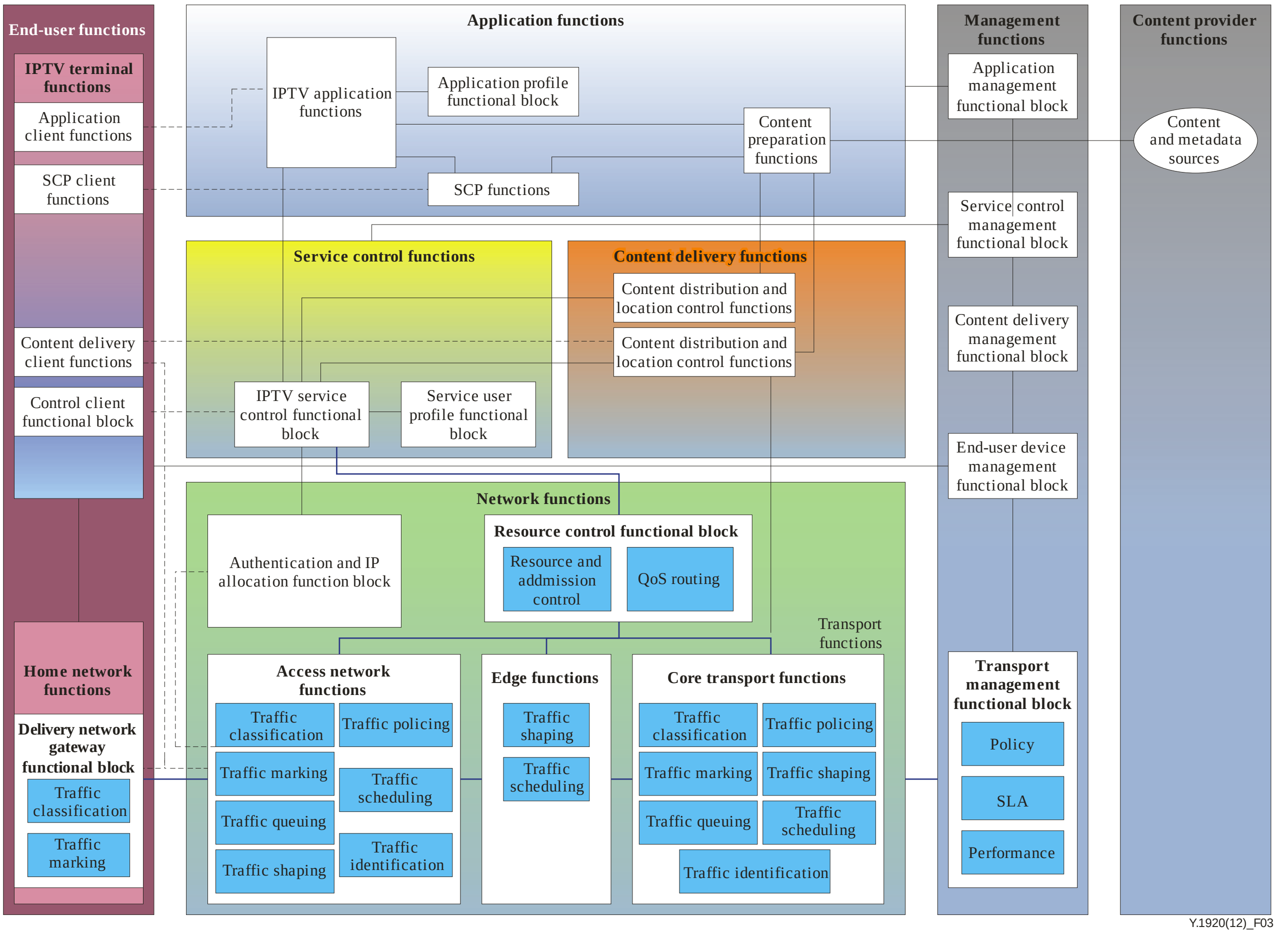

Figure 3 – Traffic management in IPTV architecture

[ITU-T Y.1910] defines an overview of IPTV architecture intended to support IPTV services. In order to provide guidance on the use of traffic management mechanisms, it is necessary to implement these mechanisms in the functions of IPTV architecture. Figure 3 illustrates how the traffic management mechanisms are involved in IPTV architecture. The blue building blocks in Figure 3 indicate the traffic management mechanisms suggested to be implemented in the corresponding functions. The bold and solid lines in the figure represent direct relationships between functions, functional blocks, or functions and functional blocks.

The mechanisms from data plane in this Recommendation are recommended to be mainly implemented in home network functions located in the home network and transport functions, which include access network functions, edge network functions and core network functions. Home network function and transport function verify transport resource availability and exchange with the control plane to enforce policy decision from control plane and handle traffic priority and so on. In the home network, traffic classification and marking mechanisms are implemented for differentiation at the service level. In the access network, traffic classification and marking mechanisms are used to isolate flows at a customer level. Traffic queuing, shaping, policing and scheduling are implemented to enable controlling traffic flow in different queues with different priorities. In the edge function, upstream traffic flows are aggregated to get traffic shaping and scheduling control. In the core network, traffic identification mechanisms can be used for upstream flows. For downstream flows, traffic classification and traffic marking mechanisms are used to differentiate different services. Traffic queuing, shaping, policing and scheduling are recommended to control traffic flow in different queues with different priorities in the core network.

The mechanisms from control plane in this Recommendation are recommended to be mainly implemented in resource control functional block of network functions. Resource and admission control located in the resource control functional block can be triggered by requests from the IPTV service control block and then interact with transport functions to check user status and network resources for controlling service traffic to be admitted or not. It also performs bandwidth reservation and allocation control, traffic classification, marking, policing, etc. QoS routing mechanisms located in the resource control functional block are able to interact with other functions to obtain the necessary routing information, compute paths and then send the results back to transport functions.

The mechanisms specified in management plane are required to be implemented in the transport management functional block of the management functions to provide overall system status monitoring and configuration.

8.2 Guidelines for the use of traffic management mechanisms for IPTV services

IPTV services as listed in [b-ITU-T Y-Sup.5] usually consist of several service applications which can have different QoS requirements regarding the transport of related data. For example, real-time telephony applications consume relatively low sustained bandwidth (a typical voice connection is less than 100 kbit/s), they have stringent jitter and latency requirements. Video requires a high-level of sustained bandwidth per channel (a few hundred kbit/s to several Mbit/s), however some latency is tolerable. Online gaming and financial applications typically require relatively small amounts of extremely time-sensitive data. [ITU-T Y.1541] defines performance classes and Appendix I provides a guideline on potential mappings of various IPTV services into performance classes.

Performance classes of various IPTV services represent the network service class subscribed by the end user device (e.g., CPE). And they should be carried along with the QoS resource information from the control plane to the transport functions across the core network, access network and home network in the data plane. Within the access, core and home network, it is recommended that three important abilities be required in a network designed to meet service-specific requirements modulated with subscriber-specific SLAs, including:

- checking conformance (i.e., policing);
- making discard decisions (i.e., resource and admission control, buffer management);
- regulating traffic flow in various queues (i.e., traffic scheduling).

The following appendices illustrate the use of different traffic management mechanisms. Appendix II provides an example guideline on how to implement traffic management mechanisms for the core network, access network and home network. Appendix III gives an illustration on the use of the admission control mechanism for VoD service in an IP multimedia subsystem (IMS)-based IPTV service scenario as defined in [ITU-T Y.1910]. Appendix IV gives implementation guidelines for management plane mechanisms.

In addition, to ensure better-quality IPTV services and meet QoS requirements of various service applications, it is recommended to provide cross-plane interaction between different planes in the IPTV network. Taking the multicast resource management as an example, IPTV network supports multicast traffic and multicast admission control for QoS of IPTV services. The multicast admission control system allocates and reserves resource and controls IPTV multicast transportation based on users' admission control policy for subscribers. The multicast replication point forwards the IPTV multicast stream to subscribers according to their successful resources allocation in the network control system. In such a case, IPTV traffic management systems are recommended as an option to interact with policy-based management functions to install the management decisions relative to multicast, and use RACF [b-ITU-T Y.2111] for multicast resource management. Appendix V provides additional discussion of cross-layer interaction between different planes for IPTV services.

Note that, due to the diversity of IPTV services and performance class requirements, the mapping from traffic management mechanisms to IPTV service and performance classes could be variable and complex. Any additional traffic management usage cases beyond the above guidelines are for further study.

9 Security considerations

The major security requirements for the traffic management function are:

- protection of the information exchange within three planes and with other functions;
- protection of the information contained in all function entities involved in traffic management;
- ensuring the availability of the traffic management function;
- preventing illegitimate access;
- maintaining the confidentiality of end-user information.

For any additional security requirements, this Recommendation aligns with the security requirements in [ITU-T Y.2701].

Appendix I

Discussion on ITU-T Y.1541 performance classes for IPTV

(This appendix does not form an integral part of this Recommendation.)

[ITU-T Y.1541] defines eight network classes for IP-based service performance. While the classes from 0 to 5 are defined as a set of normative QoS classes, the classes 6 and 7 are defined as a set of provisional QoS classes. These classes cover a wide range of services including real-time telephony, multimedia applications and interactive data transfer. Each class defined in [ITU-T Y.1541] is characterized by a set of performance parameters bounded by agreed upon parameter values. The class performance parameters of [ITU-T Y.1541] are:

- IP packet transfer delay (IPTD)
- IP packet delay variation (IPDV)
- IP packet loss ratio (IPLR)
- IP packet error ratio (IPER)

In order to classify any given service as compatible with a given performance class, it is necessary to carry out a supporting analysis that demonstrates the compliance of the observed performance parameters within the bounds specified for the desired class. The analysis for the desired service needs to consider proper evaluation time intervals, the reference path of the desired service and packet sizes. To provide guidance on traffic management for any given IPTV service component, a summary of [ITU-T Y.1541] performance class definitions, performance objectives and guidance for applicability is discussed below.

Table I.1 summarizes all pertinent information from [ITU-T Y.1541] as given in Tables1, 2 and 3 of [ITU-T Y.1541].

Table I.1 – ITU-T Y.1541 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, highly interactive (VoIP, VTC)
1	400 ms	50 ms	1×10^{-3}	1×10^{-4}	–	Real-time, jitter sensitive, highly interactive (VoIP, VTC)
2	100 ms	U	1×10^{-3}	1×10^{-4}	–	Transaction data, highly interactive (signalling)
3	400 ms	U	1×10^{-3}	1×10^{-4}	–	Transaction data, interactive
4	1 s	U	1×10^{-3}	1×10^{-4}	–	Low loss only (short transactions, bulk data, video streaming)
5	U	U	U	U	–	Traditional applications of default IP networks
6	100 ms	50 ms	1×10^{-5}	1×10^{-6}	1×10^{-6}	
7	400 ms	50 ms	1×10^{-5}	1×10^{-6}	1×10^{-6}	
NOTE 1 – U = undefined NOTE 2 – QoS classes 6 and 7 are defined as a set of provisional classes.						

Table I.2 provides an illustrative example of potential ITU-T Y.1541 performance class mappings for a variety of IPTV service applications. As indicated in clause 8, the precise mappings require extensive and detailed examination based on component characteristics (e.g., packet size) and network conditions (reference model). Such mappings are for further study.

Table I.2 – Illustrative example of potential mapping of IPTV service components to ITU-T Y.1541 QoS classes

IPTV service	Service applications	Example IPTV services	ITU-T Y.1541 QoS class							
			5	4	3	2	1	0	7	6
Streaming	Live TV content	Linear TV including pay per view and multi-view						✓1		✓
	Video content	VoD, network PVR, time-shift TV					✓1		✓	
	Audio content	Music on Demand					✓			
	Content control	VoD, network PVR, time-shift TV				✓				
	Live speech	Voice call, audio conference						✓		
	Live low-resolution video content	Video telephony, video conference						✓		
Download	Video content	Push VoD, near VoD		✓						
	Data	Content guides, pictures, applications download	✓							
Upload	Video content	User generated content		✓						
Message exchange	Interactive	Chatting			✓					
	Non-interactive	Messaging, email	✓							
Middleware/ application	Portal	Web services, information services			✓					
	Payment transactions	VoD rental			✓					
NOTE – Consumer television quality can be achieved using ITU-T Y.1541 QoS classes 0 and 1 together with the DVB-IP AL-FEC mechanism, and the enhanced decoder according to [b-ETSI TS 102034], clause E.5.1.2.										

NOTE 1 – QoS classes 6 and 7 are defined as a set of provisional classes.

NOTE 2 – It is recognized that under network congestion conditions, some traffic may not achieve the objectives of their assigned class. This may be managed by:

a) Recommending appropriate traffic management methods specified in this Recommendation to increase the likelihood of meeting ITU-T Y.1541 class objectives.

b) Specifying an appropriate percentage of time when the objectives of the desired class will be met, and possibly specifying another class that would be applicable during the remaining percentage of time. The determination of the percentage of time spent in the specified classes is for further study.

Appendix II

Traffic management for core network, access network and home network

(This appendix does not form an integral part of this Recommendation.)

II.1 Traffic management for the core network

II.1.1 Traffic management mechanisms for the core network

This clause describes an overview of the IP traffic management mechanisms including integrated services and differentiated service.

IP networks allow both reservation and differentiated models for QoS support and traffic management. The IP reservation model is that based on the IP integrated services (IntServ) and allows the use of resource reservation protocol (RSVP) signalling protocol for bandwidth reservation. Two service classes are defined in the context of IP IntServ:

- Guaranteed service (GS) defines a service type where all packets belonging to the same session are delivered within a deterministic delay bound. Routers along the path of the session must employ appropriate scheduling algorithm and reserve resources to ensure that the delay bound is always satisfied.
- The controlled load service (CLS) provides a service equivalent to a "lightly" loaded best effort network.

IP networks are also capable of supporting a differentiated model with the IP differentiated service (DiffServ). The IP differentiated model defines a set of edge functions and a number of per-hop behaviour (PHB). Edge functions are those related to classification, metering, marking, dropping and shaping. A PHB defines an externally observable treatment applied at a network node to a DiffServ behaviour aggregate. A number of PHBs are defined by the IETF in the context of IP DiffServ:

- Expedited forwarding (EF): The intent of the EF behaviour is to provide the building block for the creation of low loss, low delay, and low delay variation services. The EF PHB definition mandates that the EF packets should ideally be served at a rate R or faster and bounds the deviation of the actual departure time for each packet by the relationship [b-IETF RFC 3246]:

$$d_j \le f_j + E_a$$

$$f_j = \max\left[a_j, \min\left[d_{j-1}, f_{j-1}\right]\right] + \frac{\ell_j}{R}$$

  Where d_j is the actual departure time of the j-th packet, f_j is the target departure time of the j-th packet, and E_a is an error term bounding the deviation of the actual departure time from the target departure time. E_a is a function of the nodal scheduler implementation. ℓ_j is the length of the j-th packet. The above relationship paves the way for the specification of a delay bound as long as the aggregate EF traffic adheres to some traffic pattern (e.g., as specified by a token bucket).
- Assured forwarding (AF): The AF PHB group defines four AF classes. For each class three discard precedence levels are defined (AF*ij*, i=1, 2, 3 or 4 and j=1, 2 or 3). No priority order is defined among the four AF classes. [b-IETF RFC 2597] requires that each node in the networks to allocate certain amount of forwarding resources for each AF class to assure forwarding of the IP packets. However, no delay or loss bounds are defined.

- Class selector (CS): The CS PHB group is defined for DiffServ to be backward compatible with legacy routers that support the type of service (ToS) bits in the IP packet header. CS PHB group defines eight forward treatments where packets belonging to CSi are served before packets marked with CSj as long as $i > j$. It effectively defines a straight priority discipline with CS1 being reserved for the default forwarding (DF) used for the traditional IP best effort (BE) service.

IP DiffServ is scalable compared to IP IntServ since it does not require per flow reservation, scheduling and buffering. In IP DiffServ flow information is available at the network edge while nodal behaviour is applied on an aggregate basis.

IP DiffServ paradigm does not include the definition of service classes. However service classes could be realized by proper specification of edge rules and consistent application of PHB by the different nodes in the network.

II.1.2 IP traffic management approach applicable to IPTV service in core network

The core IP network transporting IPTV services is expected to be well-engineered and shared between a number of applications including data and voice support. Since IP DiffServ allows the core IP network to scale to a large number of flows, it is also expected that the network will be equipped with DiffServ capabilities in terms of scheduling implementation that supports all or some of the DiffServ PHBs. It can be shown that if the EF traffic arriving at an interface is bounded by a token bucket with parameters (B, R) then the delay of any packet departing the interface is bounded by:

$$D \leq \frac{B}{R} + E_a$$

where:

R (in bytes per second) is the token bucket rate

B (in bytes) is the token bucket size

E_a typically represents the value of non-rate dependent delay which may be specified by the combination of fixed minimum delay and variable delay. The specific definition for IP traffic control and congestion control algorithms including token bucket can be found in Annex A of [b-ITU-T Y.1221].

IPTV services that require stringent loss and delay constraints may be supported using EF PHB. The use of PHB will ensure that IPTV packets are transported within a certain delay bound with almost no loss as long as the aggregate burst of the offered EF traffic is within some bound. The EF PHB must be configured with enough resources to satisfy the delay requirements of video packets. Since performance of video application is sensitive to packet loss, sufficient buffer needs to be allocated to ensure that it accommodates a burst size equal to B.

It is also possible to support IPTV services using AF PHB group as long as the AF class or classes designated for IPTV services are configured with the amount of resources needed to assure the service QoS parameters. Unlike the EF PHB, there is no delay constraint associated with the definition of the AF PHB. However, use of the AF offers the added benefit of selectively discarding video packets based on their relative importance. This will require the relative importance of video information to be inherited by the IP layer.

An IP node supporting the CS PHB group implies that an absolute priority scheduler is in place. IPTV services shall be supported at a priority level high enough to maintain its quality assurances. Starvation of classes supporting IPTV services must always be avoided.

II.2 Traffic management for the access network

II.2.1 Traffic management mechanisms for the access network

Access networks should have the means to control the following functions for traffic management:

- per-packet/flow and per-class basis connection admission control (CAC)
- per-user and per-service QoS provisioning
- per-packet/flow mapping between IP DSCP markings and Ethernet priorities [b-IEEE 802.1q]

II.2.2 Traffic management approach applicable to IPTV services in the access network

Generic mechanisms are required for traffic management of upstream and downstream directions in an access network.

a) Upstream

To support quality of service in access networks including broadcasting traffic, network nodes should have the following requirements in the upstream direction:

- Guarantee of minimum bandwidth
- Guarantee of bandwidth quality per service (e.g., VoIP, video conference, and IPTV)

To address the above 2 requirements, the following functions are recommended to be supported:

- 5-tuple based classification and policing
- Priority queuing
- Traffic shaping

b) Downstream

To support QoS in access networks including broadcasting traffic, network nodes are recommended to guarantee availability of minimum bandwidth per service in the downstream direction.

To support the above, access networks are recommended to have the following functions in downstream:

- Per-packet/flow and per-class basis CAC for broadcast channels
- Traffic shaping/policing per subscriber
- Support of class of service (CoS) based DSCP
  – 5-tuple classification
  – DSCP marking
- Mapping between IP DSCP markings and Ethernet priorities [b-IEEE 802.1q]

II.3 Traffic management for home network

This clause describes home network environment and the need for traffic management for IPTV services. A possible architecture for the home network is shown in [b-HGI].

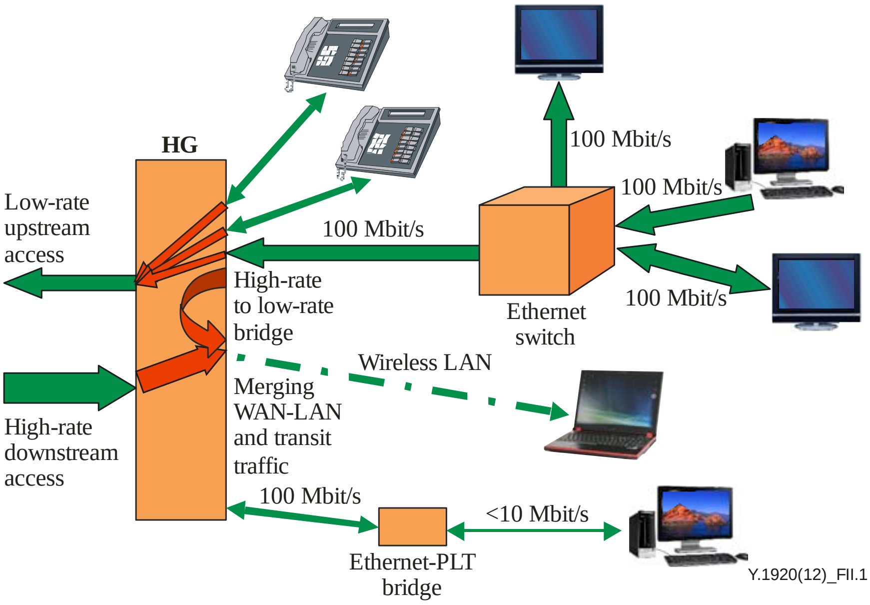

Figure II.1 – Home network architecture

As shown in Figure II.1, the home network employs multiple local area network (LAN) technologies. Prominent among these technologies are the wireless LAN (WLAN) based on [b-IEEE 802.11] and wire-line Ethernet and bridges based on [b-IEEE 802.3] and [b-IEEE 802.1d]. The home gateway (HG) is the interface of the home network to provide access network. HG receives and sends packets from and to the wide area network (WAN). It also supports transit (LAN-to-LAN) traffic. The main function of the HG is the classification of the packets as they traverse the HG to and from the WAN and setting the appropriate priority level using the IP DSCP or the Ethernet user priority bits. Possible classification criteria include type of LAN, media access control (MAC) addressing and virtual LAN (VLAN) tag. HG requirements include the support of multiple queues managed using strict priority or weighted round robin at the WAN egress ports. It requires the support buffer management mechanisms.

Home Ethernet switches may support the existence of the user priority bits (also known as p-bits). User priority bits define up to eight priority levels that can be used to identify traffic classes such as voice, video, best effort, etc.

The current IEEE 802.11 standards support rates up to 54 Mbit/s. Emerging IEEE 802.11 standards are expected to support rates up to 600 Mbit/s based on [b-IEEE 802.11n]. Traffic management is supported on a WLAN using [b-IEEE 802.11e] which defines four access categories that effectively supports four priority levels.

Appendix III

Admission control example for IMS based architecture

(This appendix does not form an integral part of this Recommendation.)

Figure III.1 shows an example of admission control for on-demand service in an IPTV service scenario using the IP Multimedia Subsystem (IMS)-based architecture as defined in [ITU-T Y.1910].

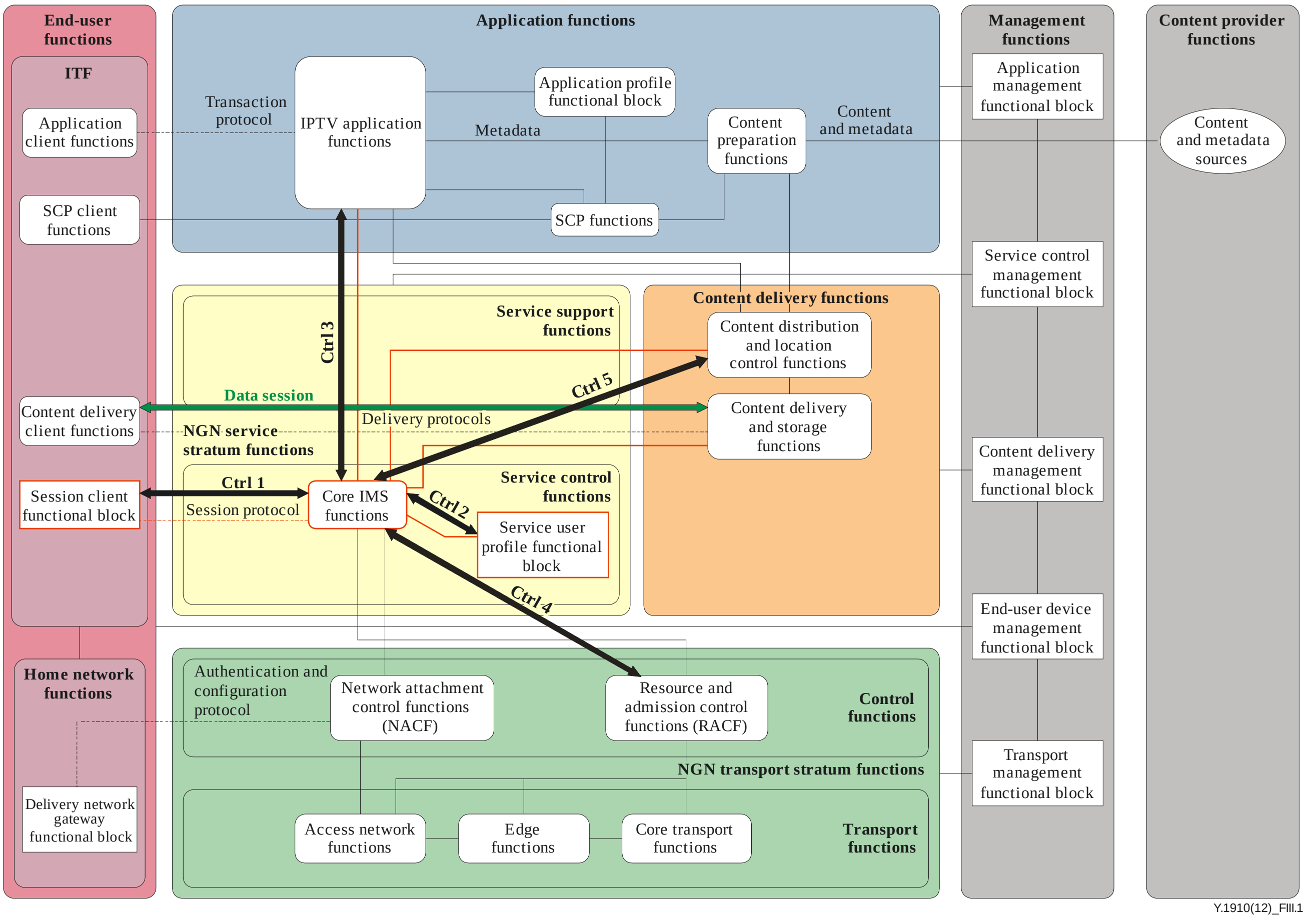

Figure III.1 – Admission control example for IMS based architecture

The admission sequence involves the generation of the request by the session client of the IPTV terminal function using a session level protocol (Ctrl 1 flow in Figure III.1). The request is received by the core IMS. The core IMS checks with the service user profile (Ctrl 2 flow in Figure III.1) and IPTV application (Ctrl 3 in Figure III.1) if the user is allowed to access the specific service and content and checks with the resource and admission control function (Ctrl 4 flow in Figure III.1) if the required resources are available. Based on this information the incoming request may be accepted or rejected and the result of the admission process is reported back to the session client (Ctrl 1 flow in Figure III.1). In case the request is accepted the content delivery control function is notified (Ctrl 5 flow in Figure III.1) and the session is established between the media client IPTV terminal and the content delivery and storage function (data session flow in Figure III.1).

Appendix IV

An example of guidelines for management plane mechanisms

(This appendix does not form an integral part of this Recommendation.)

IV.1 Management plane

In order to support video traffic, the network should provide consistent carrier grade quality service across the network. Current networks seldom deliver the required OAM functionalities in management plane thus forcing IPTV operators to deploy very complex solutions to monitor the IPTV signals. Typically, monitoring the quality is done by decoding all the IPTV signals and showing them on screens on various locations in the network. So it is recommended that a set of management functions for NGN should be designed to support the enforcement of the QoS mechanisms.

IV.2 Performance measurement and management

IPTV service providers need mechanisms to assess the performance requirements of the end-users before providing IPTV services. They must be able to provide a consistent and expected level of performance. Metric is important for ensuring the performance of NGN transport control functionality which is an integral part of a business process commonly referred to as service assurance (SA). Some of the responsibilities of SA include:

- proactive and reactive maintenance to ensure that services provided to customers are continuously available and performing to service level agreements (SLA), if applicable, or QoS performance levels;
- continuous resource status and performance monitoring to proactively detect possible failures;
- collection of performance data;
- analysis of performance data to identify potential problems and resolve them without impact to the end-user;
- if applicable, managing SLAs and report service performance to the end-user;
- receiving trouble reports from the end-user and informing it of the trouble status and ensuring the end-user of restoration and repair. In other words, SA supports the following applications:
  - network planning and engineering;
  - service installation and provisioning; and
  - management of the customer's service by supporting fault and accounting management processes.

The detailed mechanisms for metrics measurement can be found in [b-ITU-T Y.2173].

IV.3 SLA

Mechanisms are required to measure the diverse aspects of SLA which include:

- defect free forwarding (The service is considered to be available and the other aspects of performance measurement listed below have meaning, or the service is unavailable and other aspects of performance measurement do not have meaning);
- latency;

- amount of time required for traffic to transit the network;
- packet loss;
- jitter – measurement of latency variation.

Such measurements can be made independent of the user traffic or via a hybrid of user traffic measurement and OAM probing. At least one mechanism is required to measure the number of OAM packets. In addition, the ability to measure the qualitative aspects of user traffic such as jitter, delay, latency and loss must be available in order to determine whether or not the traffic for a specific user traffic are travelling within the operator-specified tolerances.

IV.4 Policy management

Policies are a set of rules typically for administering, managing and controlling access to network resources. They can be specific to the needs of the service provider or reflect the agreement between the end-user and service provider, which may include reliability and availability requirements over a period of time and other QoS requirements. Policies are used to implement mechanism for service provider includes but not limited to:

- routing policies (e.g., directing packet flow to a destination port without a routing table);
- packet filtering policies (e.g., marking or dropping packets based on a classifier policy);
- packet logging policies (e.g., allowing users to log specified packet flows);
- security related policies.

The detailed mechanism for policy management can be found in [b-ITU-T Y.2111].

Appendix V

Cross-layer interaction for IPTV services

(This appendix does not form an integral part of this Recommendation.)

Figure V.1 shows a generic layer architecture for offering of video services (not limited to the examples shown). At the application layer, video codec generates video elementary streams as a result of the encoding process. Service layer is responsible for packaging video streams into services such as broadcast video, VoD, etc. The function of the transport layer is to transport video streams from source to the destination through different network segments.

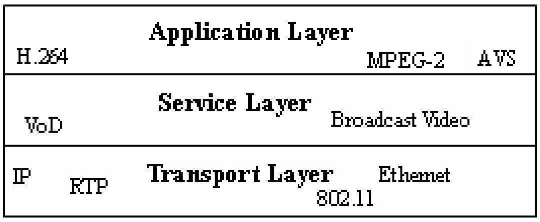

Figure V.1 – Layer architecture for video transport

Cross-layer interaction is the ability of one layer adapting its performance based on information received from other layers. For instance, in a wireless transport environment, it may be beneficial for the application to adjust its rate based on the status of the rates that can be supported by the transport layer. Cross layer interaction may be implemented in a top-down or down-top fashion.

The use of application layer priority to optimize transport layer performance is of particular interest. Video codecs generate video elementary streams with different priorities based on the picture type (i.e., I, P or B). Type I pictures are essential for the codec operation and should always be given transport priority over the P and B frames. MPEG-2/AVS transport stream and ITU-T H.264/AVS network adaptation layer (NAL) generate transport video stream packets with relative priority indication (one bit transport priority in the MPEG-2/AVS transport stream packet and 2 bits NAL Reference ID(NRI) in ITU-T H.264/AVS).

Bibliography

[b-ITU-T E.860] Recommendation ITU-T E.860 (2002), *Framework of a service level agreement*.

[b-ITU-T Y.1221] Recommendation ITU-T Y.1221 (2002), *Traffic control and congestion control in IP based networks*.

[b-ITU-T Y.2111] Recommendation ITU-T Y.2111 (2008), *Resource and admission control functions in Next Generation Networks*.

[b-ITU-T Y.2173] Recommendation ITU-T Y.2173 (2008), *Management of performance measurement for NGN*.

[b-ITU-T Y-Sup.5] ITU-T Y-series Recommendations – Supplement 5 (2008), *ITU-T Y.1900-series – Supplement on IPTV service use cases*.

[b-ETSI TS 102034] ETSI TS 102034 v1.3.1 (2007), *Digital Video Broadband (DVB) Transport of MPEG-2 TS Based DVB Service over IP Based Networks*.

[b-IEEE 802.1d] IEEE 802.1D (2004), *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridge*.

[b-IEEE 802.1q] IEEE 802.1Q (2005), *IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*.

[b-IEEE 802.3] IEEE 802.3 (2005), *IEEE Standard for Local and Metropolitan Area Networks – Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*.

[b-IEEE 802.11] IEEE 802.11 (2007), *IEEE Standard for Local and Metropolitan Area Networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.

[b-IEEE 802.11e] IEEE 802.11e (2005), *IEEE Standard for Local and Metropolitan Area Networks – Specific requirements Part 11: Wireless LAN MAC and PHY specifications: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements*.

[b-IEEE 802.11n] IEEE 802.11n (D3.00) *Draft, IEEE Standard for Local and Metropolitan Area Networks – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)*.

[b-IETF RFC 2205] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*.

[b-IETF RFC 2309] IETF RFC 2309 (1998), *Recommendations on Queue Management and Congestion Avoidance in the Internet*.

[b-IETF RFC 2386] IETF RFC 2386 (1998), *A Framework for QoS-based Routing in the Internet*.

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

[b-IETF RFC 2597] IETF RFC 2597 (1999), *Assured Forwarding PHB Group*.

[b-IETF RFC 2676] IETF RFC 2676 (1999), *QoS Routing Mechanisms and OSPF Extensions*.

[b-IETF RFC 2753] IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control*.

[b-IETF RFC 2998] IETF RFC 2998 (2000), *A Framework for Integrated Services Operation over DiffServ Networks*.

[b-IETF RFC 3246] IETF RFC 3246 (2002), *An Expedited Forwarding PHB (Per-Hop Behavior)*.

[b-IETF RFC 3272] IETF RFC 3272 (2002), *Overview and Principles of Internet Traffic Engineering*.

[b-IETF RFC 4594] IETF RFC 4594 (2006), *Configuration Guidelines for DiffServ Service Classes*.

[b-HGI] Home Gateway Initiatives (2006), *Home Gateway Technical Requirements: Release 1*.

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, 2013