International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

F.750

(02/2005)

SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES

Audiovisual services

Metadata framework

ITU-T Recommendation F.750

ITU-T F-SERIES RECOMMENDATIONS

NON-TELEPHONE TELECOMMUNICATION SERVICES

TELEGRAPH SERVICE	
Operating methods for the international public telegram service	F.1–F.19
The gentex network	F.20–F.29
Message switching	F.30–F.39
The international telemessage service	F.40–F.58
The international telex service	F.59–F.89
Statistics and publications on international telegraph services	F.90–F.99
Scheduled and leased communication services	F.100–F.104
Phototelegraph service	F.105–F.109
MOBILE SERVICE	
Mobile services and multidestination satellite services	F.110–F.159
TELEMATIC SERVICES	
Public facsimile service	F.160–F.199
Teletex service	F.200–F.299
Videotex service	F.300–F.349
General provisions for telematic services	F.350–F.399
MESSAGE HANDLING SERVICES	F.400–F.499
DIRECTORY SERVICES	F.500–F.549
DOCUMENT COMMUNICATION	
Document communication	F.550–F.579
Programming communication interfaces	F.580–F.599
DATA TRANSMISSION SERVICES	F.600–F.699
AUDIOVISUAL SERVICES	**F.700–F.799**
ISDN SERVICES	F.800–F.849
UNIVERSAL PERSONAL TELECOMMUNICATION	F.850–F.899
HUMAN FACTORS	F.900–F.999

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

ITU-T Recommendation F.750

Metadata framework

Summary

A metadata framework architecture with two layers structure is defined. The metadata gateway provides an integrated metadata retrieval capability across various metadata descriptions, and the policy-based service platform provides specific functions common to content delivery. This Recommendation provides a reference architecture of a metadata model for both content description and network control.

Source

ITU-T Recommendation F.750 was approved on 13 February 2005 by ITU-T Study Group 16 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation F.750

Metadata framework

1 Scope

This Recommendation defines an ITU-T metadata framework architecture for policy-based content delivery over networks. Content includes multimedia Web content and digital broadcast programmes provided by real-time streaming, on-demand streaming, and downloading. In broadband ubiquitous networks, this architecture enables content adaptation to the usage environment and content-aware QoS control, which are provided as network services by the use of policies, rules and network-related metadata. The proposed metadata framework architecture is structured in two layers: a metadata gateway and a policy-based service platform each of which provides open APIs to the next higher layer. The metadata gateway provides an integrated metadata retrieval capability across various metadata descriptions and the policy-based service platform provides specific functions common to content delivery such as compatible content discovery, session control, QoS control, authentication and charging. As implementation examples of the metadata framework architecture, policy-based QoS control and CDN management are addressed.

2 References

2.1 Normative 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.

References: None.

2.2 Non-normative references

[1] IETF RFC 2327 (1998), *SDP: Session Description Protocol*.

[2] ETSI TS 102 822-3-1 (2004), *Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime Phase 1"); Part 3: Metadata; Sub-part 1: Metadata schemas*.

[3] ISO/IEC JTC1/SC29/WG11 2002, *N4980 MPEG-7 Overview (version 8)*.

[4] W3C Recommendation (2004), *Composite Capabilities/Preference Profiles (CC/PP), Structure and Vocabularies*.

[5] IETF RFC 2778 (2000), *A Model for Presence and Instant Messaging*.

[6] IETF RFC 2779 (2000), *Instant Messaging/Presence Protocol Requirements*.

[7] ISO/IEC 21000-7(2004), *Information technology – Multimedia framework (MPEG-21) – Part 7: Digital Item Adaptation*.

[8] IETF RFC 1213 (1991), *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*.

[9] PAM Forum, *http://www.parlay.org/about/pam/index.asp*.

[10] ITU-T Recommendation H.350 (2003), *Directory services architecture for multimedia conferencing.*

[11] IETF RFC 3564 (2003), *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering.*

[12] IETF RFC 3466 (2003), *A Model for Content Internetworking (CDI).*

[13] ETSI TS 102 822-4 (2004), *Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime Phase 1"); Part 4: Content referencing.*

3 Definitions

This Recommendation defines the following terms:

3.1 content delivery network (CDN): A network optimized for delivering digital content.

3.2 differentiated service code point (DSCP): A 6-bit bit-pattern replacing the three IP-Precedence bits and other ToS (Type of Service) bits for differentiated services.

3.3 label switch paths (LSP): Virtual paths between pairs of edges prepared in MPLS.

3.4 metadata: "Metadata" in this Recommendation refers to the attributes of not only the content but also the network.

3.5 resource description framework (RDF): A general framework for describing a Web site's metadata, or the information about the information on the site.

4 Abbreviations

This Recommendation uses the following abbreviations:

3GPP	3rd Generation Partnership Project
API	Application Programming Interface
APL	Application Programming Language
CC	Call Control
CC/PP	Composite Capabilities/Preference Profiles
CDN	Content Delivery Network
CID	Content Identification
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
HTTP	HyperText Transfer Protocol
IMPP	Instant Messaging and Presence Protocol
LSP	Label Switch Paths
MIB	Management Information Base
MPLS	Multi Protocol Label Switching
OWL	Web Ontology Language
PAM	Presence and Availability Management
PBCDNM	Policy-based CDN Management

PC	Personal Computer
PDA	Personal Digital Assistant
QoS	Quality of Service
RDB	Relational Database
RDF	Resource Description Framework
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
ToS	Type of Service
UI	User Interaction
UNI	User-Network Interface
W3C	World Wide Web Consortium
WSDL	Web Services Description Language
XML	eXtensible Markup Language
XQL	XML Query Language

5 Advanced content delivery service architecture

5.1 Advanced content delivery

Owing to rapid progress in broadband and wireless Internet access technologies, various kinds of digital content are being delivered to diverse terminal devices (PDAs, PCs, cellular phones, etc.) that are connected by diverse access methods (DSL, wireless, optical-fibre, etc.). Furthermore, digital broadcasting will soon arrive in such an environment. Figure 1 shows content delivery in a ubiquitous environment.

In such a configuration, it is desirable that the network automatically detects the user's usage environment and adapts the content delivery to allow convenient viewing. It is also desirable that the network recognizes the user's preferences for delivery method and quality and adapts to them. To achieve such advanced content delivery, the network requires context understanding and content adaptation. Figure 2 shows a mechanism for advanced content delivery by the network. Conditions on the content side, user side, and network side are described in metadata. When a user requests content, the network gathers relevant metadata to understand the conditions. Then, for those conditions, it optimizes content delivery according to pre-defined policies.

This Recommendation provides a standardized framework for achieving this mechanism.

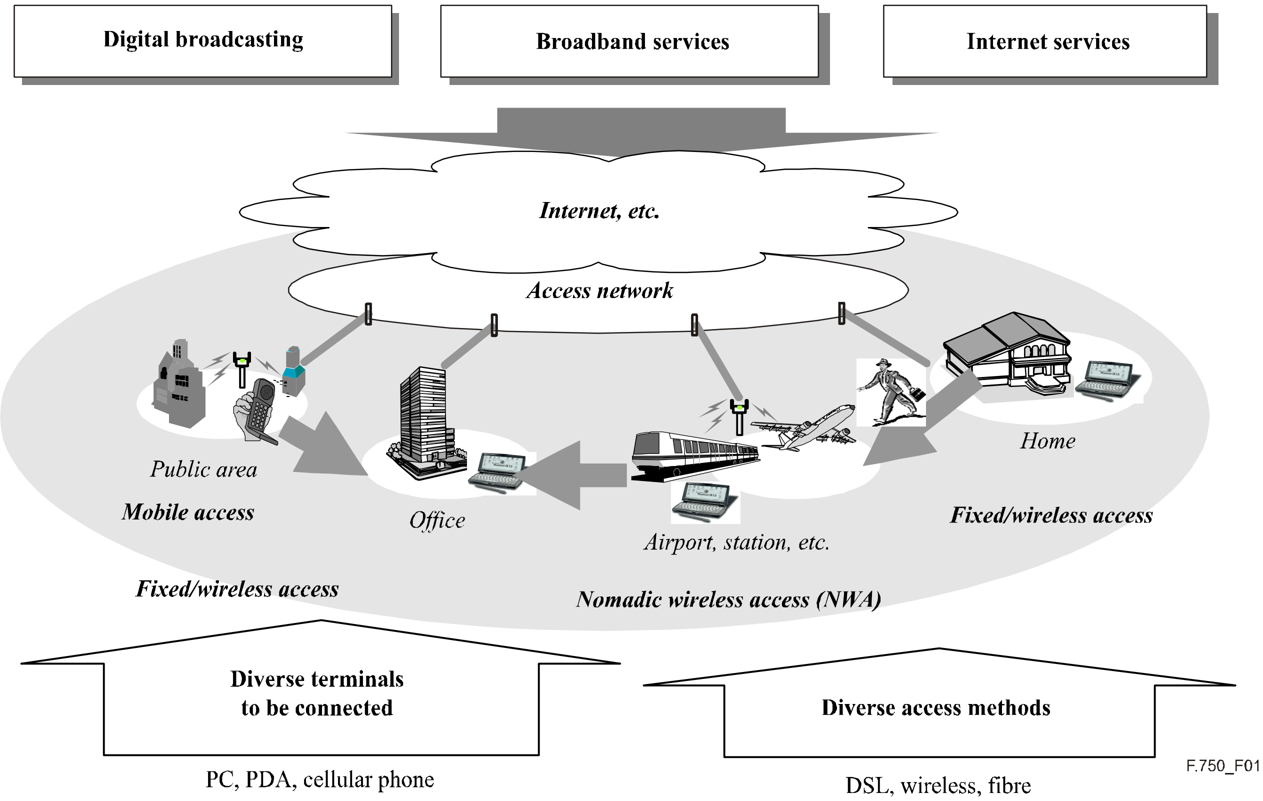


Figure 1/F.750 – Content delivery in ubiquitous environment

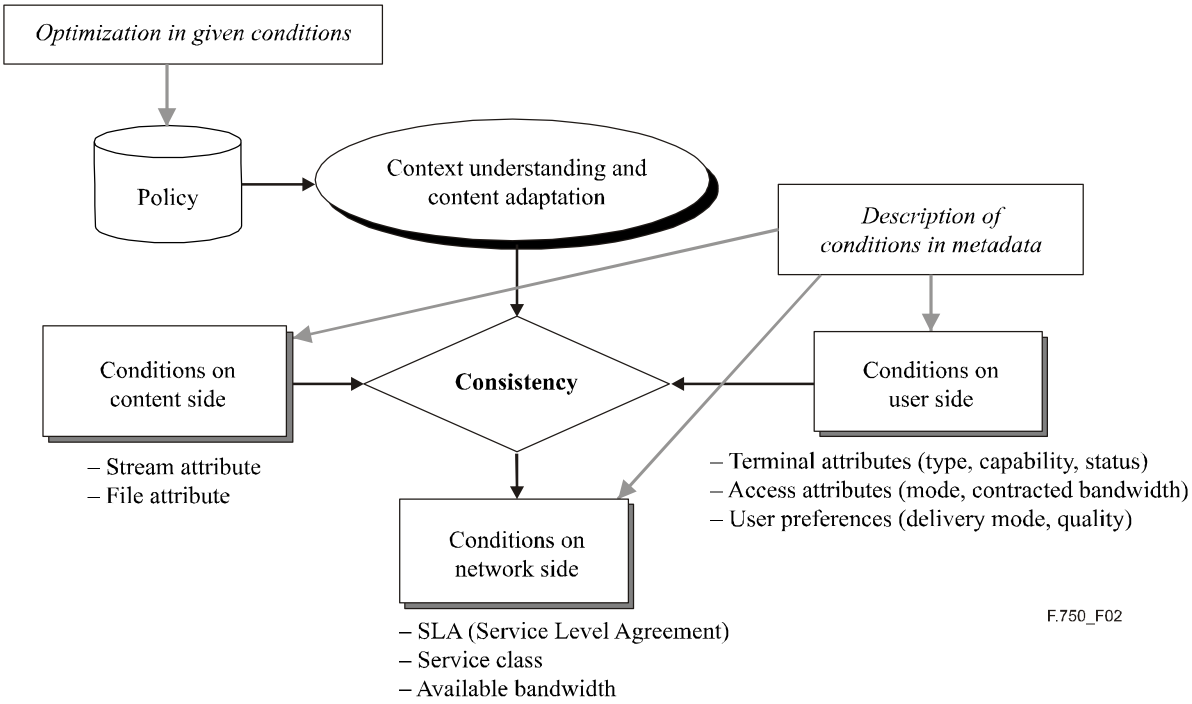

Optimization in given conditions
Policy
Context understanding and content adaptation
Description of conditions in metadata
Conditions on content side
Consistency
Conditions on user side
– Stream attribute
– File attribute
– Terminal attributes (type, capability, status)
– Access attributes (mode, contracted bandwidth)
– User preferences (delivery mode, quality)
Conditions on network side
– SLA (Service Level Agreement)
– Service class
– Available bandwidth
F.750_F02

Figure 2/F.750 – Mechanism for advanced content delivery

5.2 Network-related metadata

Originally, metadata is defined for efficient content retrieval and for building up clear rules in secondary use of content across different providers and/or organizations. This metadata describes attribution, usage rules, and target user profiles of content for the consumer.

In addition to such metadata for customer and/or content provider use, this Recommendation defines a new kind of metadata for network use, which will facilitate advanced content delivery. Called "network-related metadata", it specifies various conditions for content delivery over networks such as terminal device characteristics, access network characteristics, and user preferences.

Several standardization bodies have already defined various attribute types of information for network services that are equivalent to network-related metadata:

a) *Content delivery metadata*
   - i) Session Description Protocol (SDP) (IETF) [1];
   - ii) Instance description metadata (TV-Anytime Forum) [2];
   - iii) Multimedia description (MPEG-7) [3].

b) *User description metadata*
   - i) Composite Capability and Preference Profiles (CC/PP) (W3C) [4];
   - ii) Consumer metadata (TV-Anytime Forum) [2];
   - iii) User interaction (MPEG-7) [3];
   - iv) Presence information (IETF) [5], [6];
   - v) Usage environment (MPEG-21) [7].

c) *Terminal description metadata*
   - i) Composite Capability and Preference Profiles (CC/PP) (W3C) [4];
   - ii) Usage environment (MPEG-21) [7].

d) *Network description metadata*
   - i) Service Level Agreement (SLA);
   - ii) Management Information Base (MIB-II) (IETF) [8].

Except for SLA and MIB-II, these types of information are described by XML (or RDF) and some are interoperable. By using this information, 3GPP specifies CC/PP-based content adaptation service for cell phones, and IETF specifies SIP (Session Initiation Protocol) that establishes dynamic sessions to a target user by using presence information.

As these types of metadata are defined by different organizations for different application domains, metadata translation and/or matching is needed to share metadata for specific services. The objective in defining this metadata framework is not to invent new metadata, but to extract existing metadata relevant to communication and make it interoperable.

In a similar way to content-related metadata, network-related metadata should be interoperable within the same provider and/or across different providers. The requirements of metadata are that the total structure is clearly defined in terms of language, scheme, elements, and vocabulary and is interoperable at some levels of the metadata structure shown in Figure 3.

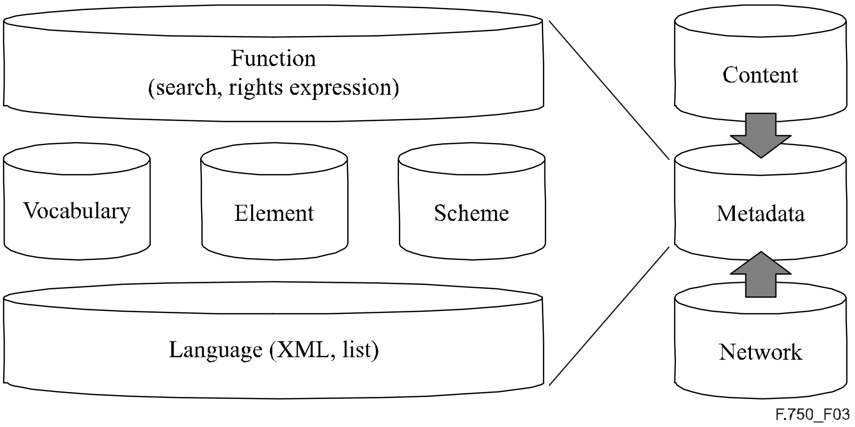
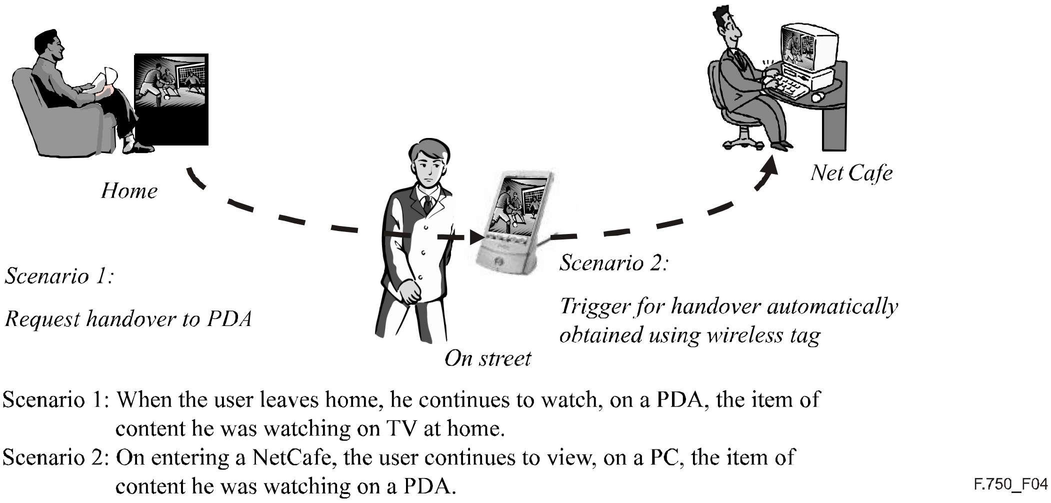


Figure 3/F.750 – Metadata structure

5.3 Role and application of metadata in network

Figure 4 shows, as an example, a potential usage scenario of a metadata-based network service in terms of seamless content handover. This service allows easy handover of programmes between a wide range of terminals irrespective of the specific viewing site, terminal capability, or ownership, so that the user can continue to watch a programme even when he or she changes viewing terminal. In this example, the user can continue to watch the same TV programme that he was watching at home even if he is out on the street using his PDA, or in a NetCafe using a PC available there.



Scenario 1: When the user leaves home, he continues to watch, on a PDA, the item of content he was watching on TV at home.
Scenario 2: On entering a NetCafe, the user continues to view, on a PC, the item of content he was watching on a PDA.

Figure 4/F.750 – Potential usage scenarios

In order to provide this service, the network must automatically detect the user's usage environment and adapt the content delivery to allow continued viewing. Users need not identify the item of content or the interruption point in the new terminal to which the content delivery is handed over.

To meet these requirements, various conditions related to content delivery over the network should be clearly described in metadata. Network metadata provides such descriptions so that the network can understand the context. Optimization of content delivery under given conditions is the scope of policy control. When there are contradictory conditions or when it is impossible to meet conditions simultaneously, resolving policies and policy enforcing schemes for network devices need to be provided. Policy-based control using metadata can provide advanced content delivery services.

Besides seamless content handover, a metadata-based network service can provide a variety of context-aware content delivery services.

6 Metadata framework

This Recommendation describes a metadata framework to achieve advanced content delivery. The architecture of the metadata framework is shown in Figure 5. It is structured in two layers: namely, a metadata gateway and a service platform. The metadata gateway provides integrated metadata retrieval across different domains, and the policy-based service platform provides specific functions common to content delivery such as context-aware address resolution, QoS control, authentication and charging.

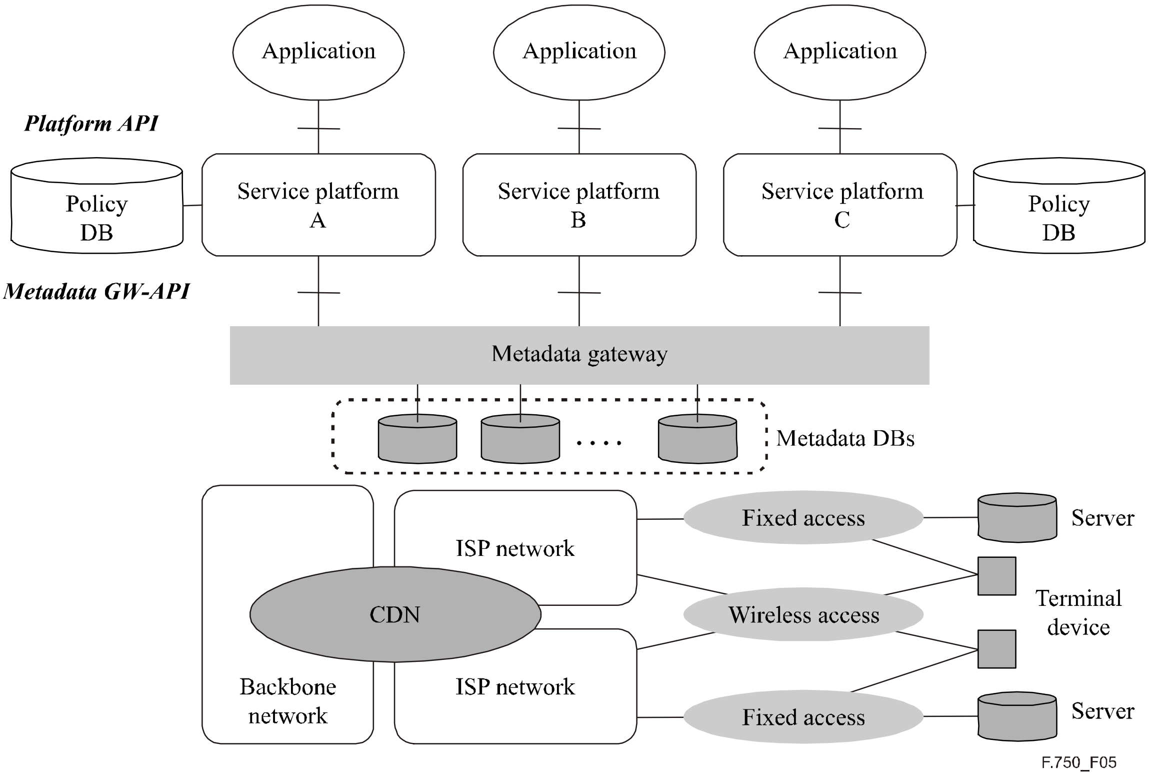


Figure 5/F.750 – Metadata framework architecture

When a user requests content, the metadata framework gathers relevant network-related metadata to understand the conditions. Then, for these conditions, it optimizes content delivery by using pre-defined policies. More specifically, the metadata gateway gathers relevant metadata and performs translations between different metadata descriptions when needed. On top of the metadata gateway, the service platform functions perform policy-based control functions such as QoS control, session control, authentication control, and charging control, to support content delivery applications. For this purpose, the service platform API and metadata gateway API are defined as open interfaces.

6.1 Metadata gateway

To make network-related metadata universally usable, we need a gateway function for retrieving required metadata and providing the application interface. This capability is provided by the metadata gateway. It is desired that network-related metadata such as content delivery attributes, user and terminal attributes and network attributes are stored in a metadata database and managed by a directory. The directory needs to include rules for selecting metadata that meet required conditions and evaluation criteria that determine the order in which candidate metadata should be provided.

Furthermore, to enable metadata defined in a specific domain be usable in other domains, a function is required that absorbs the difference in metadata descriptions and translates description schema. This capability is also needed in the metadata gateway.

To provide the above-mentioned capabilities, the use of PAM-API defined by the Presence, Availability and Management Forum (PAM Forum) [9] is envisaged. The PAM Forum defines an open interface for application development that integrates and/or associates various communication services by enabling the use of presence and/or availability information about networks through open APIs.

PAM-API provides operations for identity (equivalent to user) or group identity, agent (equivalent to device), agent assignment, agent presence, and identity presence, as well as preference control, event notification and access control. Security protection is another significant feature of PAM-API.

The metadata gateway architecture based on PAM-API is shown in Figure 6. It is composed of two parts. The platform part gathers and manages network-related metadata including presence and/or availability information. On top of the platform part, the application part provides various functions by manipulating metadata and/or integrating metadata from different domains through PAM-API.

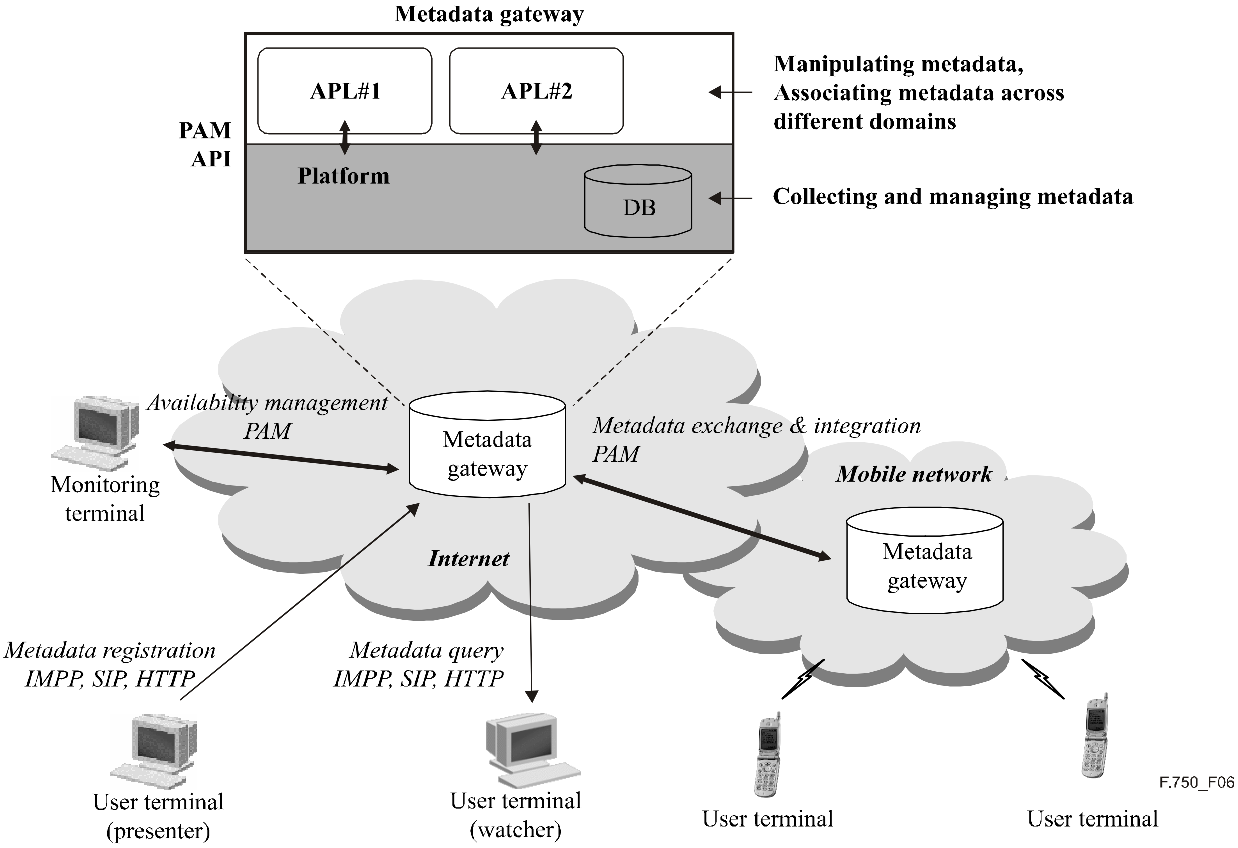

Metadata gateway
APL#1
APL#2
PAM API
Platform
DB
Manipulating metadata, Associating metadata across different domains
Collecting and managing metadata
Availability management PAM
Monitoring terminal
Metadata gateway
Metadata exchange & integration PAM
Mobile network
Metadata gateway
Internet
Metadata registration IMPP, SIP, HTTP
Metadata query IMPP, SIP, HTTP
User terminal (presenter)
User terminal (watcher)
User terminal
User terminal
F.750_F06

Figure 6/F.750 – Functions of metadata gateway

For the platform part, this metadata framework defines the following four metadata gateway functions:

a) *Metadata disclosure control*

When notified metadata does not meet the application user's requirements in terms of item and/or format, this function requests the metadata provider to disclose new metadata items and/or metadata formats. It also reports candidate metadata that meet given conditions.

b) *Metadata storing and gathering*

This stores static and/or dynamic metadata information. It enables metadata information to be manipulated and acquired according to given filtering conditions.

c) *Metadata transformation and sharing*

This automatically transforms given metadata items of given subjects into given formats.

d) *Metadata distributed management*

Based on the intentions of metadata providers, this function enables distributed management of metadata information according to its characteristics, usages, and objectives within servers and/or terminal devices. Furthermore, it enables dynamic changes in the location of stored metadata.

Figure 7 shows a possible architecture for the metadata transformation and sharing function achieved by the metadata gateway. Integrated retrieval across different metadata is achieved by transformation rules stored in a repository in this example. The use of semantic transformation by using an ontology would also be possible.

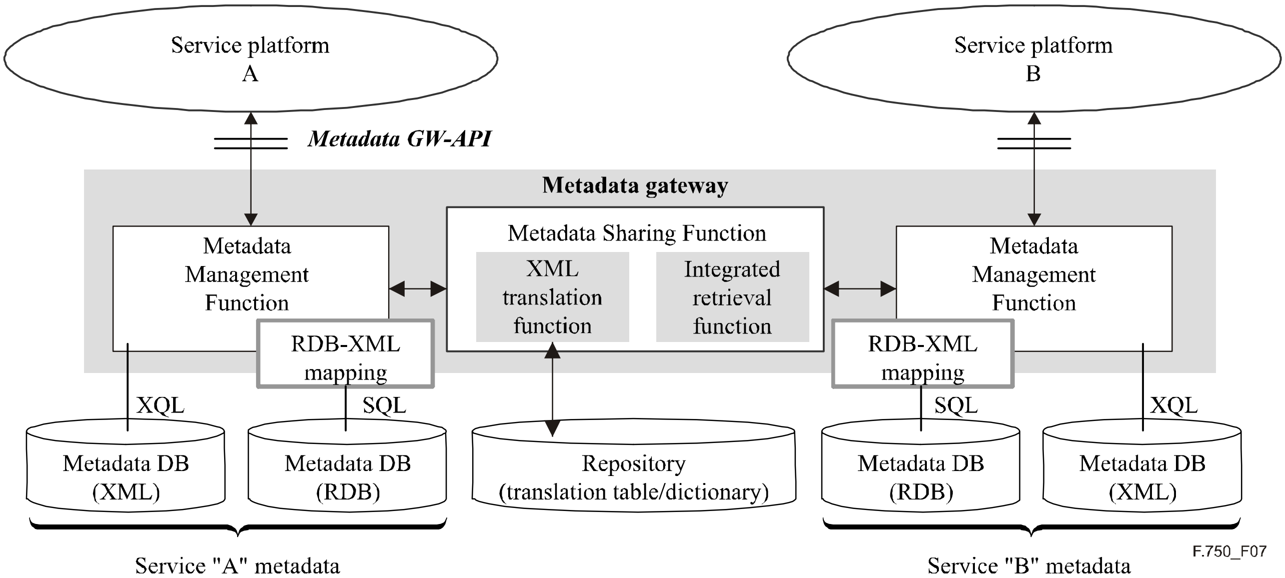


Figure 7/F.750 – Metadata gateway architecture

To achieve common expression of metadata among different industry standard schemas, integration of attribute types, reference rules, and name definitions are needed. Figure 8 shows a possible mapping between various industry standard metadata and directory object classes. To harmonize metadata across domains, firstly an ontology language such as OWL needs to describe the relationship between metadata elements that are mutually referred to, and then these elements are mapped to the same attribute type in the directory database.

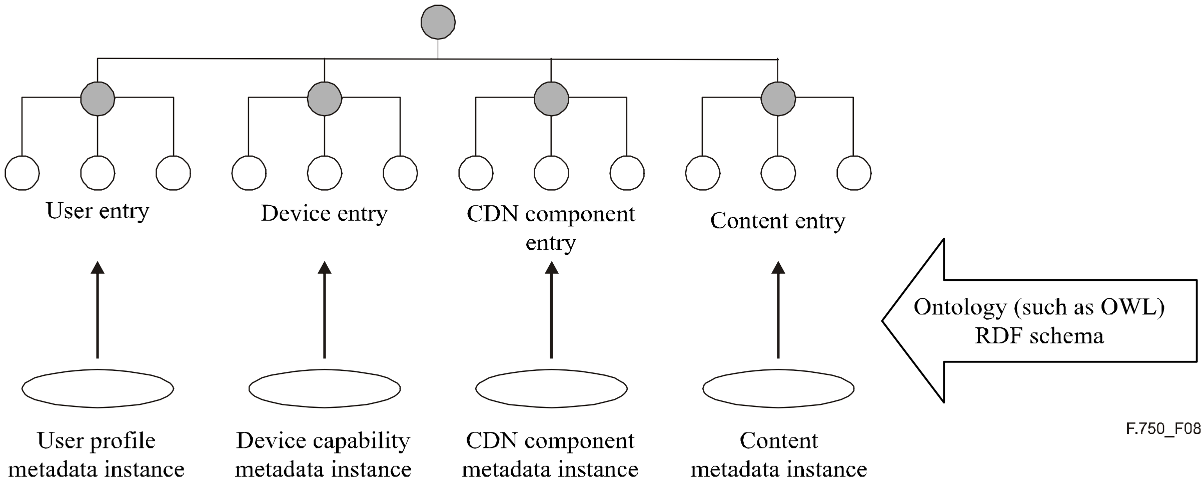

User entry
Device entry
CDN component entry
Content entry
Ontology (such as OWL) RDF schema
User profile metadata instance
Device capability metadata instance
CDN component metadata instance
Content metadata instance
F.750_F08

Figure 8/F.750 – Mapping from metadata to directory object classes

6.2 Service platform using metadata

Utilizing network-related metadata, the service platform supports advanced content delivery by providing common functions through their application interfaces. The following platform functions are envisaged:

a) *Address resolution function*

When a user retrieves and selects content logically, this function resolves the location of a physical content instance that meets the user's preference and usage environment as described by metadata.

b) *Quality of service (QoS) control function*

This function controls network QoS based on the content delivery configuration and user preference as described by metadata.

c) *Session control function*

This function establishes a connection from a server to a given user. It further enables simultaneous use of multiple terminals and/or seamless handover between terminals.

d) *Secure delivery function*

This function prevents malicious access to the content delivery service by using user, terminal, and content authentication. Furthermore, it associates the user with upper-layer services by using single-sign-on authentication.

e) *Charging function*

This function gathers relevant charging information needed to charge for a particular service and achieves bundled charging. It also enables associated charging of multiple services.

These platform functions provide their services to application via an API called the network service API.

6.2.1 Service platform based on the Parlay-API

The Parlay-API specifies open interfaces of network functions for applications over IP-based networks and/or mobile systems [10]. Parlay v4.0/3GPP OSA Release 5/ETSI ES 202 915 defines fourteen APIs including framework, call control (CC), user interaction (UI), mobility (user status/location), terminal capability, policy control, content-based charging, and presence and availability management (PAM). The framework provides access control to APIs as well as API instance creation, API retrieval, fault management, event notification and domain authentication, etc. PAM-API is a part of the Parlay-API.

Since the Parlay-API allows flexible combination of network functions for application development, it is a realistic solution for a metadata framework that associates metadata and network functions. Parlay-API should be included in the service platform of the ITU-T metadata framework.

6.2.2 Service platform based on Web service (SOAP)

W3C specified SOAP 1.2 as a W3C Recommendation for a framework of exchanging XML structured data between peers. Web services are associated by sharing data described in WSDL (Web Services Description Language). As these are language specifications, actual services need to be defined independently. If Parlay-based terminologies are defined, then a metadata framework could be built by using the Web service description. Parlay-X pursues aims for interoperability with Web services. This needs further study.

Details about platform functions are also a subject for further study. Some details are discussed in the appendices. A QoS control function and address resolution function are included in Appendices I and II, respectively.

Appendix I

Policy-based QoS control using metadata

This appendix addresses a scheme for policy-based QoS control in multimedia content delivery over a network, as an implementation example of the metadata framework.

To utilize network QoS control functions effectively, user requirements need to be described and associated with network QoS control functions. In a policy-based QoS control scheme, user requirements and the usage environment are described in metadata, and policy control associates these requirements with network QoS capability. This scheme is provided as a guideline.

As user requirements for content delivery are high-level and abstract, they need to be translated into an appropriate application QoS class and then mapped into an appropriate network QoS class, according to some rules. Once the mapping has been done, admission control needs to decide whether or not the selected network QoS class should be admitted considering relevant conditions such as the characteristics of transferred data and capability and/or environment of end-systems. The policy-based QoS control scheme performs admission control under the conditions described by metadata, according to predefined policies.

A set of application QoS classes is defined in ITU-T Rec. G.1010 "End-user multimedia QoS categories". Various service level agreements (SLAs) define another type of application QoS classes. For network QoS , IETF DiffServ and ITU-T Rec. Y.1541 "Network performance objectives for IP-based services" are envisaged. ITU-T Rec. Y.1541 defines network QoS classes with UNI-to-UNI performance objectives. The policy-based QoS control scheme uses these definitions and provides mapping rules and mechanisms between these hierarchical QoS class definitions.

Furthermore, although termination points of data flow are located at a server or terminal, edge-nodes cannot recognize these termination points in the current network configurations. The policy-based QoS control scheme introduces flag information within the packet header that is commonly used by end-systems (server, terminal) and edge-nodes to segregate the admitted flow.

I.1 Model of policy-based QoS control using metadata

In the IP-based network, network QoS control is implemented by, for example, differentiated packet forwarding behaviour according to the assigned network QoS class. Since the network QoS class is defined on a UNI-to-UNI basis, QoS requirements for servers/terminals connected to edge-nodes are further categorized in QoS classes depending on the characteristics of transferred data as well as on the capabilities and/or environment of the end-system (server/terminal). In the policy-based QoS control scheme, QoS classes that the end-system provides to the user are defined as application QoS classes. Transferred data characteristics and end-system capabilities and/or environment are described by metadata.

Firstly, user and/or application requirements are described in metadata. Secondly, these are translated into an application QoS class. Thirdly, they are mapped to a network QoS class. Translation and mapping are achieved by policy control. These relationships are shown in Figure I.1.

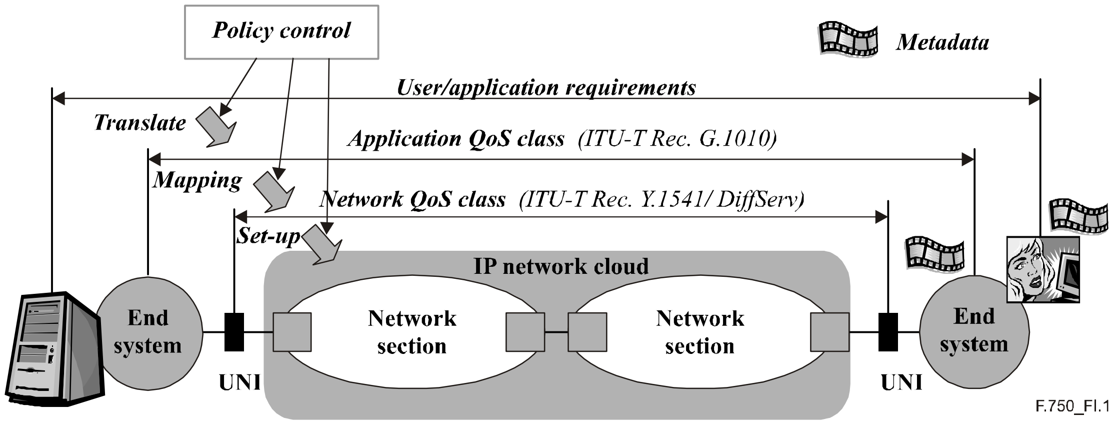


Figure I.1/F.750 – Hierarchical model of policy-based QoS control

Functional components that are required in the policy-based QoS control using metadata are shown in Figure I.2. They consist of the following five components:

1) User and/or application requirement metadata;
2) Rules and mechanisms that map given metadata to an appropriate application QoS class;
3) Mechanism for querying the policy server about the admission of a selected application QoS class;
4) Network resource management database to provide information about network status, and an admission control mechanism equipped with set-up information notification;
5) Mechanism to configure set-up information via the network API.

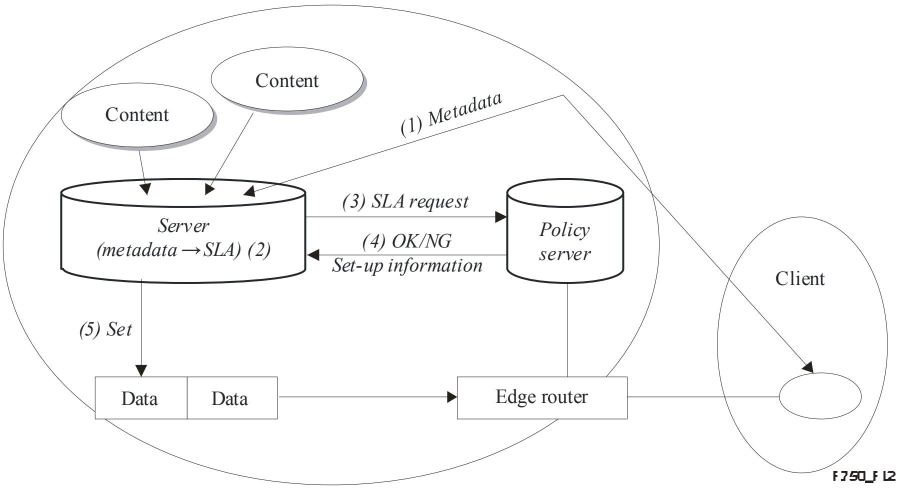


Figure I.2/F.750 – Architectural model of policy-based QoS control using metadata

I.1.1 Metadata mapping

To describe user and/or application requirements, international standard metadata defined by MPEG, TV-Anytime and others could be used. As for content metadata, TV-Anytime content instance metadata that includes information about content delivery conditions such as data format, size, and delivery configuration (streaming or downloading), could be used as user requirements. As for the terminal profile, CC/PP defined by W3C could be used, which would enable the server to select a content instance or adjust the transmission bandwidth. Further information that is required in QoS control includes terminal type (PC, PDA, or cell-phone) and/or contracted bandwidth. These attributes are defined by MPEG21 DIA (Digital Item Adaptation) as usage environment metadata or by CC/PP.

The metadata framework is used for sharing metadata coming from different organizations.

I.1.2 Mapping rules and mechanisms

The domain manager provides policy rules for translating user and/or application requirements to a particular application QoS class or SLA, by using metadata. One prerequisite is that at least one SLA is contracted. The application QoS class is specified by ITU-T Rec. G.1010 "End-user multimedia QoS categories". Parameters for determining service categories include delay, jitter, and information loss. It is recommended that the application QoS class should be categorized by a combination of these parameters and the allowable range in terms of delay, loss rate, etc. ITU-T Rec. G.1010 further categorizes audio, video, and data by their data characteristics and usage situations, to define assured delay and error rate; thus, it can be a basis for defining SLAs for content delivery over a network.

For example, real-time streaming needed by broadcast content delivery could be classified into one-way video, and a download service could be classified into bulk data as recommended by ITU-T Rec. G.1010. For "one-way video service class", the delay is specified to be less than 150 ms and the maximum delay is 400 ms and admitted information loss is specified to be less than 1 %. The delay for "bulk data", is specified to be less than 15 s, and information loss is zero. These specifications are useful for defining SLAs between different organizations.

I.1.3 Mechanism for querying the policy server

In this component, the server asks the policy server about the admission of a data transmission by using the application QoS or SLA, which was selected by the mapping rules. The query information includes application QoS class or SLA, and content delivery attributes (required bandwidth, content size, etc.). The policy server provides the admission control function. It decides to grant or reject a request, after consulting a network resource management database. If the request is granted, the policy server sends back configuration information for setting a flag that indicates permitted data. Since the policy server and edge router can register the IP address and port number of the application server, the data stream from the permitted application server is differentiable from other data streams. If other terminals set the configuration information and send data, the edge router can refuse to forward the data.

I.1.4 Network configuration information

Network configuration information, such as DSCP, is provided by IETF to make guidelines for using Diffserv. For example, "one-way video" for broadcast should be set to AF31, AF32, AF33, or CS4 and "bulk data" should be set to AF11, AF12, AF13, or CS. These guidelines are stored in the policy server database and sent as a reply for configuration information to the application server.

I.1.5 Setting configuration information

Currently, even if the application server and policy server negotiate to reserve a connection for the application layer, there is no way to differentiate negotiated data from other data; hence, other data may be allowed to use the reserved connection. This means that the negotiated result is not reflected in network resource utilization. In this implementation example model, the application server gets configuration information from the policy server at the time of negotiation and puts it in packets as a flag by means of the network API provided by the operating system. As a result, the policy server and edge router can distinguish packets of a negotiated server from other packets. This kind of flag could be implemented in the DS field of IP packets and flow label defined by IPv6.

I.2 Implementation of QoS control

Diffserv, MPLS, Wide Area Ethernet, and others could implement network QoS control. Diffserv differentiates defined service classes by using DSCP as a flag. MPLS prepares virtual paths between pairs of edges, which are called Label Switched Paths (LSPs). If an edge router recognizes a flow, then succeeding packets that belong to the flow are transmitted over the same LSP, which achieves service segregation and QoS control. IETF published an RFC about LSP switching algorithms using Diffserv DSCP (RFC 3564). When MPLS is used for QoS control, security technology such as intrusion detection, forensics, firewalls, honey pots, etc., should be deployed to make MPLS networks more secure. Wide Area Ethernet can set the IEEE 802.1p priority bit in the Ethernet frame to achieve multiple priority paths that have different priority levels. Since each IP-based network QoS is implemented as a multi-priority virtual path, it is easy to map service classes.

Appendix II

Policy-based CDN management using metadata

The outstanding feature of the content delivery network (CDN) is the separation of the content pre-caching function and the content delivery function. A content request from a user is redirected to a surrogate (CDN edge node) close to where the actual content is delivered, which improves performance, scalability and availability.

Address resolution plays a key role in CDN management. It helps to find a suitable content instance that meets not only the user's preference about content, but also the usage environment such as client device capabilities and access network characteristics.

This Recommendation defines a CDN management optimization by use of the metadata framework. In particular, it optimizes the address resolution API managed by policy control taking into account various conditions described by shared metadata across different domains. Currently, metadata is defined by different organizations in different schemas for specific application domains. To adapt content to network environment and user profile, metadata must be shared across different domains. Policy-based CDN management provides metadata translation and matching across different domains and a policy scheme in terms of expression and control for CDN optimization.

II.1 Directory database as metadata retrieval infrastructure

The benefits of a database are characterized by its standard retrieval language and repeatability of retrieval, propagation and tracking in renewal, availability, and robustness. For common expression among different industry standard schemas, integration of attribute types, reference rules, and name definitions are needed. For this purpose, mapping between various industry standard metadata and directory object classes as shown in Figure 8 in 6.1 is used.

To harmonize metadata across domains, firstly an ontology language such as OWL needs to describe the relationship between metadata elements that are mutually referred to, and then these elements are mapped to the same attribute type in the directory database. A policy-based CDN management model (PBCDNM) using such a directory method is shown in Figure II.1.

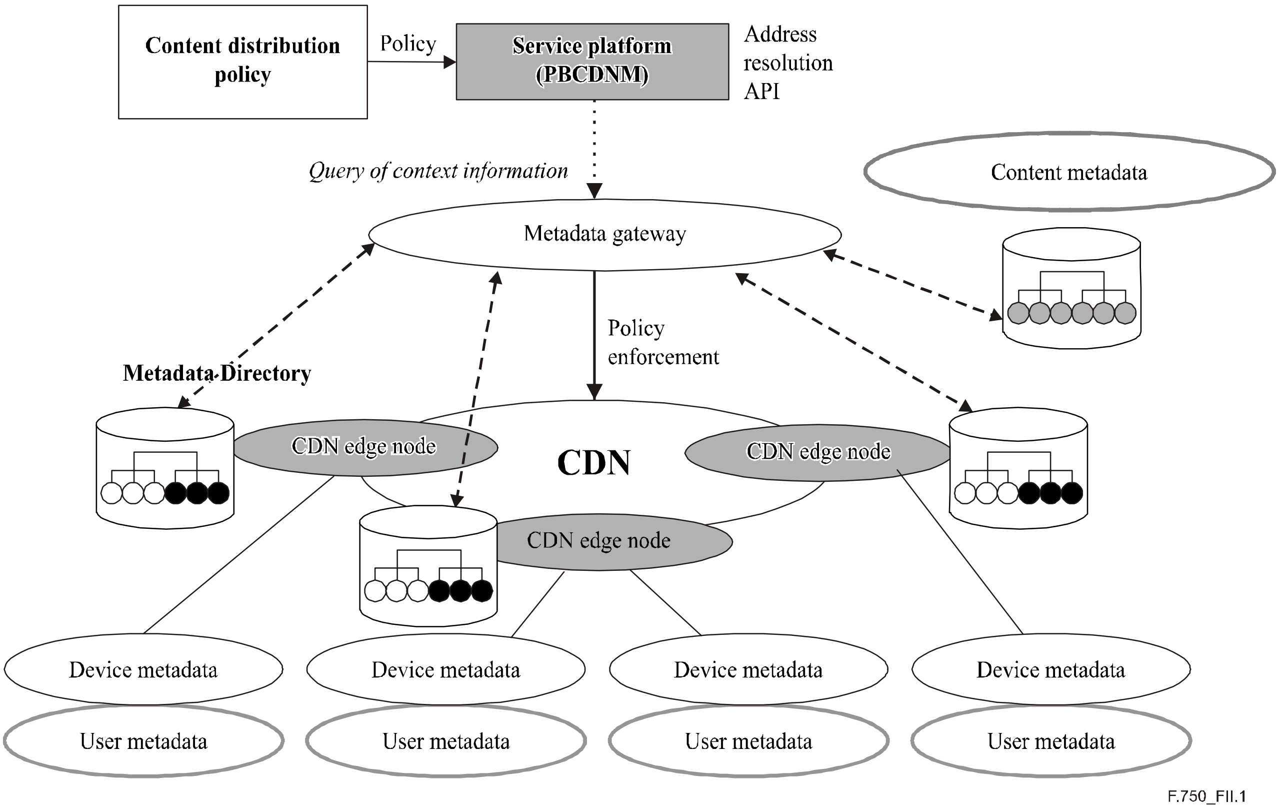


Figure II.1/F.750 – Policy-based CDN management

II.2 Metadata for CDN optimization

The essentials of CDN technology are server pre-caching control that optimizes content instance allocation among surrogates, and redirection control that finds content instances of requested content having attributes that match to usage environment and selects the optimum surrogate, which stores such instances by address resolution.

In pre-caching control, cost efficiency is a goal. The cost of a surrogate server depends on its capacity and delivery capability available to target users and target devices. The following metadata are envisaged:

– Content delivery attributes;

– Surrogate delivery capability attributes and storage capability attributes for streaming and downloading;

– Delivery environment attributes of the access network between surrogate and client;

– Client device storage and rendering capability attributes (terminal profile);

– User profile;

– User preference attributes (statistics on content access between surrogate and client).

As for content delivery attributes, TV-Anytime Forum (TVA) content instance description metadata (Programme Location: Audio/VideoCodingParameter (FileFormat, BitRate, etc.)) could be used. For the terminal profile, CC/PP (composite capability and preference profiles) could be used as it includes terminal hardware, software, and browser platform attributes. For the user profile, TVA targeting metadata (intended audience) could be used.

For user preference attributes, statistical information, analysed by content viewing history and by access requests between surrogate and client, is required, where TVA content description metadata, (Programme (Group) Information: Title, Genre, CreditList, Keyword, ParentalGuideline, Language), and TVA instance description metadata, could be used.

These sets of attributes are also used as context information for address resolution to achieve redirection control. Address resolution is performed to identify the location of a content instance by examining device capabilities, and available bandwidth in the access network between the surrogate and client to carry the content instance data. Among metadata listed above, content delivery attributes (TVA instance description metadata), access network delivery environment attributes, and terminal profile (CC/PP) could be used for this purpose.

II.3 Policy descriptions in CDN management

This clause provides the policy description in CDN management for the optimization of pre-cache control and redirection control, based on the metadata as described in the previous clause.

Broadcast and/or multimedia content are assigned unique names or identifiers independent of their locations on a network. Association between these identifiers and the location information of actual content instances is provided by the address resolution system. The role of policy-based CDN management (PBCDNM) is to resolve the location of requested content that matches client device capability, access network characteristics, and user preferences as described in metadata. As a result, a content request from a user is redirected to a surrogate that stores the content instance adapted to the usage environment.

II.3.1 Optimization of pre-caching control

To optimize pre-caching, surrogates need to store frequently accessed categories of content to improve the hit rate. The optimum pre-cache policy could be determined by analyzing surrogate user preferences and the statistics of content access frequency. For this purpose, metadata access frequency statistics stored at a client device need to be categorized according to metadata attributes. A surrogate stores access frequency statistics to a particular metadata attribute such as "Genre" in its directory entries.

Figure II.2 shows an example, where two client devices store user preference metadata in their usage environment metadata entries, and a surrogate stores statistics of user preference metadata of client devices that frequently access the surrogate. The User-1 device classifies the ratio of Genre-A content and Genre-B content to be 4 to 3. Surrogate-1 stores Genre-A as a genre preference.

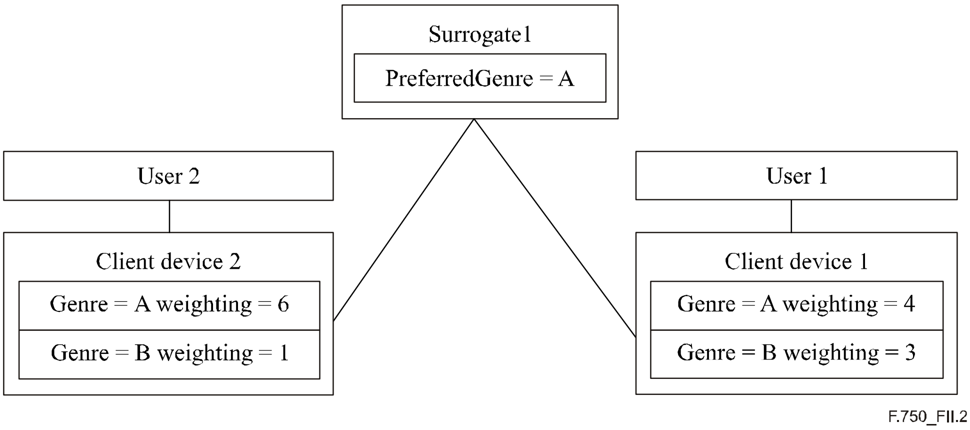


Figure II.2/F.750 – Pre-cache policy

The criteria for judging whether to cache a content instance or not in a given surrogate are stored in a surrogate entry of the directory database as a pre-caching policy. This policy characterizes the performance of the CDN service that a CDN provider provides to content providers. An example of a pre-cache policy is described below:

```
IF (ContentInstance1.genre = Surrogate1.preferredGenre)
  THEN
    IF (ContentInstance1.fileSize < Surrogate1.availableStorageSize)
      THEN
          CacheIt(ContentInstance1)
      ELSE
          ThrowAway(ContentInstance1)
ELSE
          ThrowAway(ContentInstance1)
```

This policy evaluates the possibility of pre-caching content instance1at Surrogate-1. Firstly, it evaluates whether the genre attribute of content1 matches the genre preference of Surrogate-1. If they match, then it evaluates whether the file size of content1 is within the storage size of Surrogate-1. As a result, it decides whether to cache content1 in Surrogate-1 or not.

II.3.2 Optimization of redirection control

A key technology for achieving redirection control is address resolution. The address resolution function redirects the content request to the content instance that matches the usage environment such as terminal capability and access network characteristics.

Suppose that the following network-related metadata is described:

1) Access network characteristics in terms of "assured maximum bit-rate";

2) Terminal capability in terms of implemented "codec-type";

3) Content delivery characteristics in terms of "coding method".

The problem is how to select one instance from two content instances having different bit-rates, which are created from the same original content. The selection policy is described as follows: (see Figure II.3):

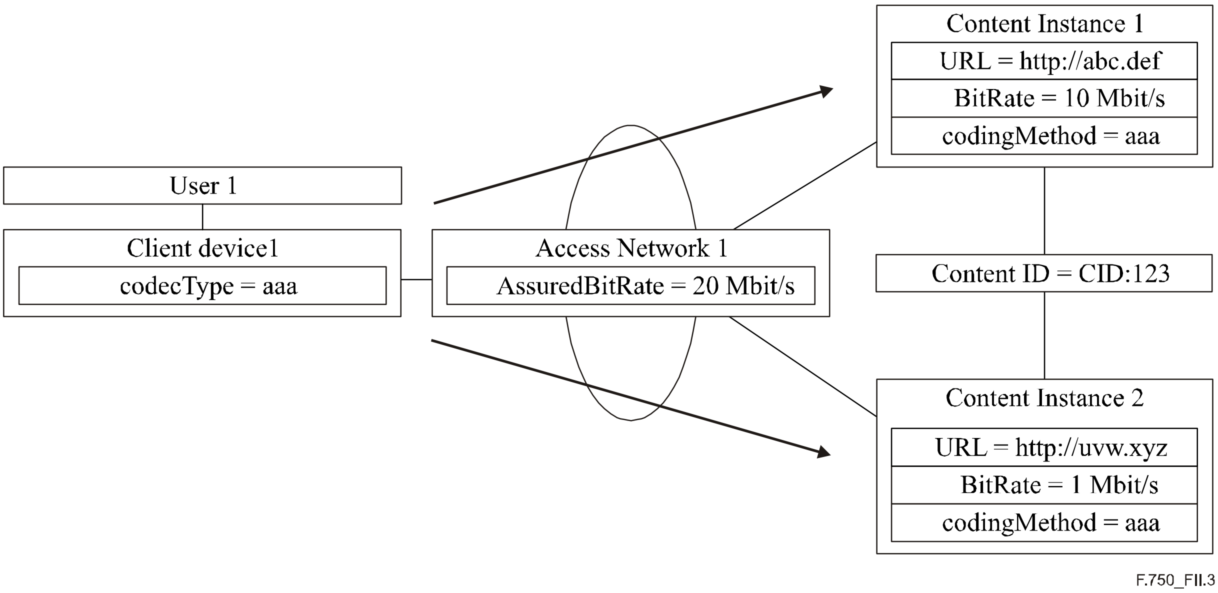


Figure II.3/F.750 – Surrogate selection policy

```
IF((ClientDevice1.codecType=ContentInstance1.codingMethod) AND
        (ClientDevice1.codecType = ContentInstance2.codingMethod))
THEN
  dif1=ClientDevice1.accessNetwork1.assuredBitRate
    – ContentInstance1.bitRate
  dif2=ClientDevice1.accessNetwork1.assuredBitRate
    – ContentInstance2.bitRate
  IF((dif1 > 0) AND (dif2) > 0))
    THEN
       IF (dif1 > dif2)
          resolveTo(ContentInstance2.URL)
    ELSE
          resolveTo(ContentInstance1.URL)
```

This selection policy is stored in the directory database.

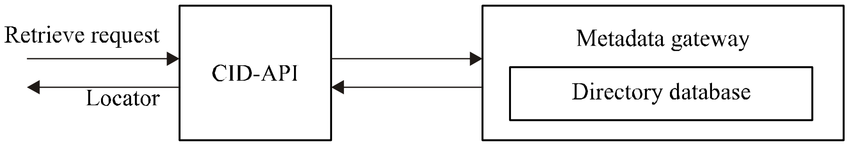
II.4 Interoperability of metadata across different domains

To achieve interoperability between metadata, we need to define mapping and/or translation methods between different metadata in terms of application domains or standardization bodies. In the above example, terminal capability attributes such as "codec-type" may be described by CC/PP, and content delivery attributes such as "coding method" may be described by TV-Anytime content instance metadata.

To achieve interoperation of these types of metadata across different domains, the relationship between metadata elements needs to be described beforehand. For example, it should be pre-described that the codec-type of a client device and coding-method of a content instance have a mutually checkable relationship. Then, these elements need to be mapped into the same attribute type of a directory database and stored. In the above example, two metadata elements are stored as the codec-type attribute of a client device and coding-method attribute of content instance, respectively. Both have the attribute type "enumeration type".

II.5 Service platform API

The service platform API of the address resolution service is defined as follows (see Figure II.4):



F.750_FII.4

Figure II.4/F.750 – Address resolution platform

Content ID (CID) is an identifier of a content item that is independent of location. CID is resolved into a locator that shows the location of the content. By using the CID address resolution API that provides a network-transparent address resolution interface, various application services that need an address resolution system and/or protocol are implemented. The CID address resolution API accesses the directory database via a metadata gateway to obtain device metadata about the client device. Based on this device metadata, it accesses the directory database to obtain a content instance that matches the device characteristics, which resolves the optimum address.

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	Telephone transmission quality, telephone installations, local line networks
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, 2005