International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2302

(08/2014)

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

Next Generation Networks – Enhancements to NGN

Network intelligence capability enhancement – Functional architecture

Recommendation ITU-T Y.2302

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
Enhancements to NGN	**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.2302

Network intelligence capability enhancement – Functional architecture

Summary

Recommendation ITU-T Y.2302 specifies the functional architecture for network intelligence capability enhancement (NICE). NICE, which is based on next generation network (NGN) technology, contains a set of enhanced capabilities to intelligently provide services according to the requirements of users and application providers. It enables operators to assign specific network resources according to these requirements and dynamically adjust them based on several factors, such as multi-dimensional awareness, traffic optimization and cooperation between different access networks. NICE supports interfaces for users and applications enabling on-demand resource and service provision.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T Y.2302	2014-08-29	13	11.1002/1000/12281

Keywords

Network intelligence capability enhancement, next generation network, NGN, NICE, NICE provider.

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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/.

Table of Contents

Recommendation ITU-T Y.2302

Network intelligence capability enhancement – Functional architecture

1 Scope

This Recommendation specifies the functional architecture for network intelligence capability enhancement (NICE). NICE (see [ITU-T Y.2301]), which is based on next generation network (NGN) technology, contains a set of enhanced capabilities to intelligently provide services according to the requirements of users and application providers. It enables operators to assign specific network resources according to these requirements and dynamically adjust them based on several factors, such as multi-dimensional awareness, traffic optimization and cooperation between different access networks. It supports interfaces for users and applications enabling on-demand resource and service provision.

This Recommendation defines the functional architecture of NICE, which includes the definition of functional entities, the reference points between different functional entities, the service procedures and security considerations.

Note that network management functionality is outside the scope of this Recommendation.

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 Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN.*

[ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[ITU-T Y.2111] Recommendation ITU-T Y.2111 (2008), *Resource and admission control functions in next generation networks*.

[ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN.*

[ITU-T Y.2240] Recommendation ITU-T Y.2240 (2011), *Requirements and capabilities for next generation network service integration and delivery environment.*

[ITU-T Y.2301] Recommendation ITU-T Y.2301 (2013), *Network intelligence capability enhancement – Requirements and capabilities*.

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

[ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1.*

[ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application [b-ITU-T Y.101]: A structured set of capabilities, which provide value-added functionality supported by one or more services.

3.1.2 application provider [ITU-T Y.2012]: A general reference to a provider that offers applications to the customers making use of the services capabilities provided by the NGN.

3.1.3 charging [b-ITU-T Q.825]: The set of functions needed to determine the price assigned to the service utilization.

3.1.4 content [b-ITU-T H.780]: A combination of audio, still image, graphic, video, or data.

NOTE – A variety of formats is classified as the "data" (e.g., text, encoded values, multimedia description language introduced by ITU-T H.760).

3.1.5 context [b-ITU-T Y.2002]: The information that can be used to characterize the environment of a user.

NOTE – Context information may include where the user is, what resources (devices, access points, noise level, bandwidth, etc.) are near the user, at what time the user is moving, interaction history between person and objects, etc. According to specific applications, context information can be updated.

3.1.6 context awareness [ITU-T Y.2201]: A capability to determine or influence a next action in telecommunication or process by referring to the status of relevant entities, which form a coherent environment as a context.

3.1.7 identity [ITU-T Y.2720]: Information about an entity that is sufficient to identify that entity in a particular context.

3.1.8 identity management [ITU-T Y.2720]: Set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:

- assurance of identity information (e.g., identifiers, credentials, attributes),
- assurance of the identity of an entity (e.g., users/subscribers, groups, user devices, organizations, network and service providers, network elements and objects, and virtual objects), and
- enabling business and security applications.

3.1.9 media [ITU-T Y.2012]: One or more of audio, video, or data.

3.1.10 network intelligence capability enhancement (NICE) [ITU-T Y.2301]: An enhancement for NGNs supporting some intelligent capabilities for the provisioning of services according to requirements of users and application providers. These intelligent capabilities (termed as "NICE capabilities") enable operators to assign and dynamically adjust specific network resources based on the requirements, as well as support interfaces for users and applications enabling on-demand resource and service provision.

3.1.11 NGN [ITU-T Y.2001]: A packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

3.1.12 service [b-ITU-T Y.2091]: A set of functions and facilities offered to a user by a provider.

3.1.13 service provider [b-ITU-T M.1400]: A general reference to an operator that provides telecommunication services to customers and other users either on a tariff or contract basis. A service provider may or may not operate a network. A service provider may or may not be a customer of another service provider.

3.1.14 user [ITU-T Y.2201]: A user includes end user [b-ITU-T Y.2091], person, subscriber, system, equipment, terminal (e.g., FAX, PC), (functional) entity, process, application, provider, or corporate network.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
ANI	Application Network Interface
ASF	Application Support Function
BSS	Business Support System
CA-FE	Content and context Analysis Functional Entity
CD-FE	Content and context Detection Functional Entity
ID	Identity
IDMF	Identity Management Function
IDP	Identity Provider
IP	Internet Protocol
IM	Instant Messaging
NGN	Next Generation Network
NICE	Network Intelligence Capability Enhancement
NNI	Network to Network Interface
OE-FE	Open Environment Functional Entity
PC-FE	Policy Control Functional Entity
PE-FE	Policy Enforcement Functional Entity
PCC	Policy and Charging Control
P2P	Peer-to-Peer
QoS	Quality of Service
RACF	Resource and Admission Control Function
SCF	Service Control Function

SC-FE	Service Control Functional Entity
SIP	Session Initiation Protocol
SUP-FE	Service User Profile Functional Entity
TRC-FE	Transport Resource Control Functional Entity
TRE-FE	Transport Resource Enforcement Functional Entity
TS-FE	Traffic Scheduling Functional Entity
TSE-FE	Traffic Scheduling Enforcement Functional Entity
UNI	User-Network Interface
URL	Universal Resource Locator
WiFi	Wireless Fidelity
xDSL	x Digital Subscriber Line

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview of NICE

6.1 Rationale behind the development of NICE

Future telecom services will face challenges due to innovations in technologies and applications. For instance, the emergence of mobile Internet, cloud computing applications and their new business models have resulted in new requirements for networks, such as high bandwidth pipes, increased mobility, real-time interactivity, higher quality, increased security, etc. Emerging services such as multi-screen service also require coordination between different networks, especially between mobile and fixed networks.

With the commencement of the mobile Internet era, operators are increasingly facing the threat of becoming "pipeline providers". In the past, the network was an operator's source of core competitiveness advantage, nowadays however user information and management and service capabilities are the new competitive factors. At the same time, due to the growing success of new Internet applications such as high-bandwidth video applications and peer-to-peer (P2P) applications, operators are facing huge pressure to expand network capacity. The scissors difference between traffic and revenues growth becomes wider.

These network development trends require that operators identify the implications for users and of service requirements at the network level. Operators need to increase the efficiency and value of their networks through intelligent resource scheduling and network traffic management. Therefore, the

NGN capabilities need to be enhanced. This enhanced NGN is referred to as network intelligence capability enhancement (NICE).

6.2 Enhanced capabilities of NICE

As defined in [ITU-T Y.2301], NICE is an enhanced NGN which supports some intelligent capabilities for the provisioning of services according to the requirements of users and application providers. These intelligent capabilities (termed as "NICE capabilities") enable operators to assign and dynamically adjust specific network resources based on the requirements, as well as enabling them to support interfaces for users and applications enabling on-demand resource and service provision.

NICE supports the followings capabilities:

1) Awareness capabilities: user, application and network awareness with content and context analysis.

2) On-demand provision capabilities: user self-assignment of service subscription and network resources, user on-demand service of quality assurance.

3) Optimization capabilities: traffic management based on intelligent traffic scheduling.

4) Openness capabilities: invocation of the above features by 3rd party application providers.

5) Cooperation capabilities: network coordination between policy control capabilities of different access networks.

7 Architecture enhancements to NGN

The NICE architecture is an enhancement of the NGN architecture [ITU-T Y.2012].

Concerning the service stratum, the following required enhancements are identified:

- The application support functions need to be enhanced to take information as input from the content and context analysis functional entity, policy control functional entity and traffic scheduling functional entity. Application support functions must then adapt the interface and provide it to both self-operated applications and third party applications. Then self-operated applications and the third party applications can invoke the network resource conveniently for quality of service (QoS) guarantees, network status awareness, suitable content cache, delivery node selection, route optimization, etc.
- The service user profile functional entity (SUP-FE) requires access to user subscription and user location information (e.g., access network related information and physical and logical location). SUP-FE is responsible for storing user profiles and presence status data [ITU-T Y.2012]. The storage and update of these data are handled by the user profile management functions of SUP-FE. They can optionally be used for support of commonly used authentication, authorization and accounting (AAA) and security schemes. With the deployment of an identity management (IdM) function, SUP-FE is enhanced to increase confidence in identity information of entities and thus enhance business and security applications and services.
- The service control functional entity needs to be enhanced to support applications' request transferring to functional entities in the transport stratum. The service control functional entity acts as a connection between NICE functional entities in the transport stratum (e.g., the policy control functional entity) and application support functions. The service control functional entity provides the interfaces to allow the applications to access NICE functions in the transport stratum. The service control functional entity also receives and transfers information such as the information allowing the identification of application data for policy control and traffic scheduling, information allowing the identification of applications and

users and transport stratum events (e.g., notifications of QoS modifications) reported by the transport stratum to the service stratum.

Concerning the transport stratum, the following required enhancements are identified:

- Transport control functions need to be enhanced to support the content and context analysis functional entity. The content and context analysis functional entity retrieves the awareness related information and deeply analyses the information. The content and context analysis functional entity provides analysis results related to user traffic and network status to the policy control functional entity and traffic scheduling functional entity.
- Transport control functions need to be enhanced to support the policy control functional entity which supports coordination between different access networks, for instance via cooperation with policy and charging control (PCC) for 3GPP access networks. The policy control functional entity receives bandwidth and QoS assignment requirements from users and 3rd party or self-operated applications.
- Transport control functions need to be enhanced to support the traffic scheduling functional entity. The traffic scheduling functional entity receives 3rd party or self-operated applications' traffic scheduling requests and is enhanced to support traffic optimization based on traffic scheduling rules. Traffic scheduling rules include traffic localization, delivery node selection, network status awareness, intelligent route adjustment, network resource allocation, etc.
- Besides access network functions, edge functions, core transport functions and gateway functions [ITU-T Y.2012], the transport stratum needs to be enhanced to support the content and context detection functional entity, the policy enforcement functional entity and the traffic scheduling enforcement functional entity.

8 Functional architecture of NICE

8.1 Overview

The functional architecture of NICE includes a service stratum and transport stratum in alignment with the NGN functional architecture. The service stratum consists of application support functions and service control functions. The transport stratum consists of transport control functions and transport functions and this architecture enables the separation of network control and data transport, as shown in Figure 1.

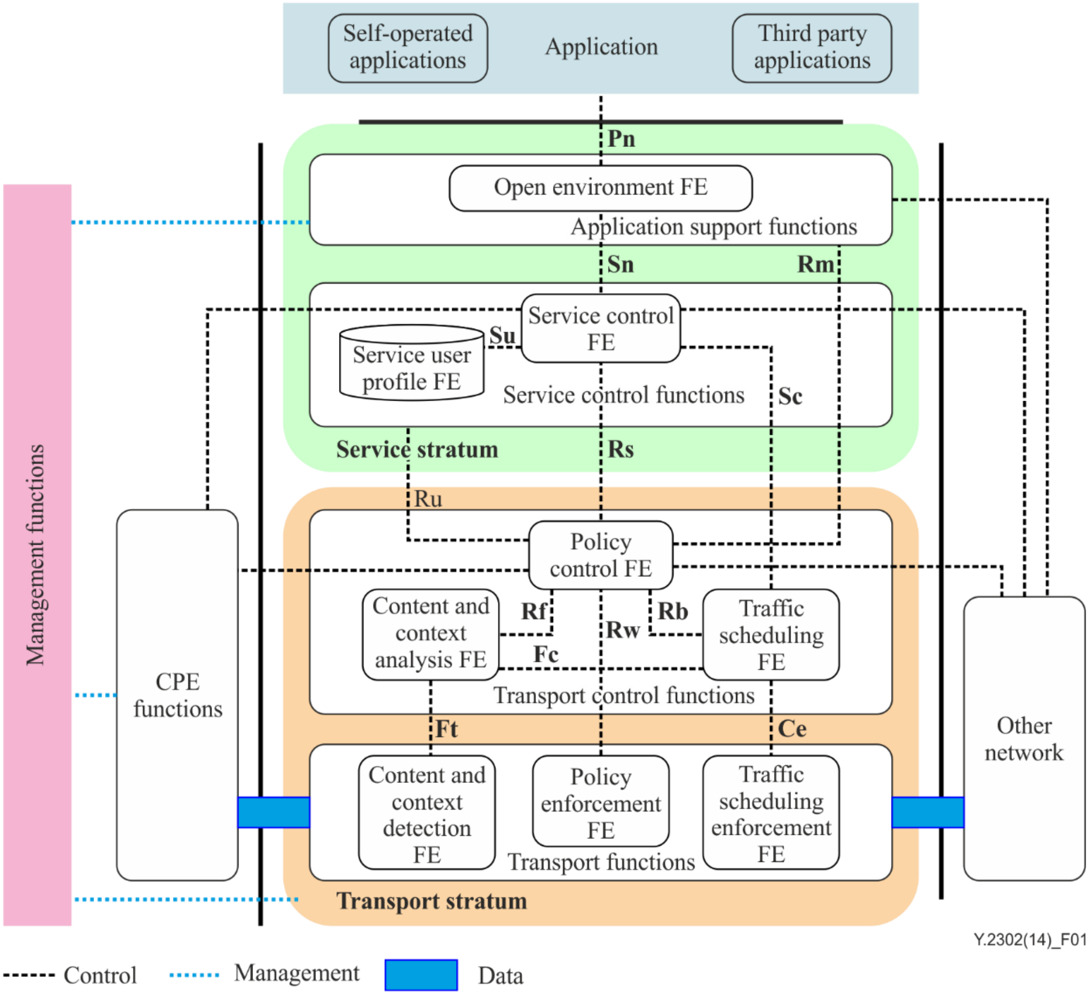

Figure 1 – Functional architecture of NICE

Figure 1 describes the functional architecture of NICE with functions, related functional entities and relevant interfaces and reference points.

In the service stratum, there are application support functions (ASF) and service control functions (SCF). For supporting self-operated applications and 3rd party applications, the application support functions include an open environment functional entity to provide secure access and capability openness. Service control functions include a service control functional entity (SC-FE) and a service user profile functional entity (SUP-FE).

In the transport stratum, there are transport control functions and transport functions. Transport control functions include a policy control functional entity (PC-FE), a content and context analysis functional entity (CA-FE) and a traffic scheduling functional entity (TS-FE). In addition to access network functions, edge functions, core transport functions and gateway functions [ITU-T Y.2012], transport functions include a content and context detection functional entity (CD-FE), a policy enforcement functional entity (PE-FE) and a traffic scheduling enforcement functional entity (TSE-FE).

8.2 Application support functions

8.2.1 Open environment functional entity (OE-FE)

In order to provide an interface to self-operated applications and third party applications, the open environment functional entity (OE-FE) has the following functions:

- The OE-FE provides exposure of new resources to the applications in a secure and controlled way.
- The OE-FE provides an enhanced service creation environment for new resources including standardized description of resources and service logic, a static and dynamic service orchestration function, online and offline design tools and an easy to operate testing environment.
- The OE-FE provides an enhanced service execution environment for new resources, including a mechanism for resource registration, discovery and routing and a mechanism for application provisioning, addressing and routing.
- The OE-FE provides an enhanced service delivery management environment for new resources, particularly for new security assurance and charging models.
- The OE-FE provides an enhanced brokering function and adaptor function for new resources. The resource brokering function interacts between applications and the new resources for the downward invocation of resources and the upward triggering of applications and also executes policies related to resources and applications.

8.3 Service control functions

8.3.1 Service user profile functional entity (SUP-FE)

The service user profile functional entity (SUP-FE) in NICE is aligned with the SUP-FE in NGN [ITU-T Y.2012] and includes some functional enhancements.

In NICE architecture, the SUP-FE can be constructed in a hierarchical structure which supports a network to network interface (NNI) by name mapping.

In an authorization scenario, the SUP-FE can deliver a user's authorization grant token from a content provider (CP) to a service provider (SP) with Oauth protocol application network interface (ANI).

In NICE architecture, the SUP-FE supports identity management (IdM) [ITU-T Y.2720] as an enhancement to increase confidence in the identity information of entities and enhance business and security applications and services. The SUP-FE supports IdM as follows:

- assurance of the identity of an entity (e.g., users, user groups, user devices, network and service providers, network elements and objects and virtual objects).
- support of entity mobility, entity location and presence information, discovery and exchange of identity information.
- identity lifecycle management.
- enablement of business and security applications.
- support of data models and schemas to facilitate interoperability of SUP related information (e.g., identity information exchange) within a NICE provider.

8.3.2 Service control functional entity (SC-FE)

In NICE architecture, the service control functional entity (SC-FE) has an enhancement on the routing and protocol transmission function to support the policy control functional entity and the traffic scheduling functional entity. The service control functional entity interconnects with these two functional entities, transmits the protocol transparently to the ASF and allows the ASF to invoke these functions.

The SC-FE also receives and transfers the following information:

- information allowing the identification of application data for policy control and traffic scheduling.
- information allowing the identification of applications and users.
- transport stratum events (e.g., notifications of QoS modifications) reported by the transport stratum to the service stratum.

8.4 Transport control functions

8.4.1 Policy control functional entity (PC-FE)

The policy control functional entity (PC-FE) receives results from the content and context analysis functional entity regarding user, traffic and network information while it also receives application bandwidth and QoS assignment requirements from the service control functional entity (SC-FE) and the open environment functional entity (OE-FE).

The PC-FE makes decisions regarding network resource and admission control. It supports a unified policy database and consistent policies definitions as well as a variety of access and core networks within a general resource control framework.

The PC-FE outputs decisions to the policy enforcement functional entity (PE-FE).

The PC-FE is aligned with the functional requirements of the resource and admission control function (RACF) [ITU-T Y.2111], and includes the following additional functions concerning transport resource allocation and management of QoS policies (within the network and at the network boundaries), based on the requirements of users and application providers:

- intelligent bandwidth and QoS level assignment according to the output from user self-service functions. Self-service functions are the interfaces for users requesting on-demand service provision from NICE functions;
- intelligent bandwidth and QoS level assignment and adjustment according to specific requirements from a third party application provider or NICE provider through application support functions;
- intelligent bandwidth and QoS level adjustment according to the output of the content and context analysis functional entity (CA-FE).

8.4.2 Content and context analysis functional entity (CA-FE)

The content and context analysis functional entity (CA-FE) receives the extracted information from the content and context detection functional entity (CD-FE).

The CA-FE performs processing and storage of content and context information.

The CA-FE distributes user traffic analysis results and network status analysis results to the requestor of content and context information such as the policy control functional entity and the traffic scheduling functional entity. Content and context information can be distributed in real time or/and on-demand according to requirements.

Context analysis functions are aligned with the context awareness requirements of NGN (clause 7.3 of [ITU-T Y.2201]).

The CA-FE also provides the following information:

- The CA-FE provides user traffic analysis results based on predefined rules and information provided by the content and context detection functional entity, such as user profile information, user traffic information and user terminal parameters.

- The CA-FE provides network status analysis results based on predefined rules and information provided by the content and context detection functional entity, such as network resource information and access network related information.
- The CA-FE provides information related to user application data, such as application data type (e.g., audio, image, graphic, video, data, etc.), application data statistics and application user preferences.

8.4.3 Traffic scheduling functional entity (TS-FE)

In NICE architecture, the traffic scheduling functional entity (TS-FE) receives application traffic delivery requests from the service control functional entity and application support functions and also receives analysis results from the content and context analysis functional entity. The TS-FE supports the establishment of traffic scheduling rules based on these results.

The TS-FE is aligned with the functions of the transport resource control functional entity (TRC-FE) of NGN [ITU-T Y.2111] and includes the following additional requirements in terms of generation of traffic scheduling rules:

- traffic scheduling rules (for intra-NICE provider networks and inter-NICE provider networks) based on traffic localization;
- traffic scheduling rules based on selection of the traffic delivery network node;
- traffic scheduling rules according to network status;
- traffic scheduling rules according to intelligent routing based on route selection policy.

8.5 Transport functions

In NICE architecture, in addition to access network functions, edge functions, core transport functions and gateway functions [ITU-T Y.2012], transport functions include the content and context detection functional entity (CD-FE), the policy enforcement functional entity (PE-FE) and the traffic scheduling enforcement functional entity (TSE-FE).

8.5.1 Policy enforcement functional entity (PE-FE)

The policy enforcement functional entity (PE-FE) receives policy decisions and updates from the PC-FE and then enforces different QoS and resource allocation policies based on different traffic.

The PE-FE performs end-to-end traffic management across different networks of varying technologies provided by multiple operators to ensure the requirements for users or applications can be accomplished.

The PE-FE is aligned with the functional requirements of the resource and admission control function (RACF) [ITU-T Y.2111], with the following additional requirements:

- In order to satisfy on-demand requirements from users and application providers, the PE-FE performs on-demand bandwidth and QoS management.
- The PE-FE performs bandwidth and QoS management based on PC-FE outputs.

8.5.2 Content and context detection functional entity (CD-FE)

The content and context detection functional entity (CD-FE) collects transport related information and provides the information to the CA-FE.

The context detection functions are aligned with the context awareness requirements of NGN (clause 7.3 of [ITU-T Y.2201]).

The CD-FE extracts information related to the following aspects according to national and regional laws, regulations and policies:

- user location information, including physical location and logical location;

- user application data information, including application data type (such as audio, still image, graphic, video and data) and application data statistics;
- user terminal parameters, such as terminal manufacturer, terminal type, terminal OS, etc.;
- network resource information, such as link bandwidth, bandwidth utilization, user data rate and other available resource parameters;
- access network related information, such as access technology and access bandwidth.

8.5.3 Traffic scheduling enforcement functional entity (TSE-FE)

The traffic scheduling enforcement functional entity (TSE-FE) receives traffic scheduling rules and decisions from the TS-FE and enforces these rules and decisions. TSE-FE supports traffic scheduling rules deployed in network devices, such as routers, switches and access control systems.

The TSE-FE is aligned with the functions of the transport resource enforcement functional entity (TRE-FE) of NGN [ITU-T Y.2111], with the following additional aspects:

- traffic scheduling based on traffic localization schemes.

  NOTE – P2P contents may be stored locally to decrease outgoing traffic and the peers for storage are selected based on the localization principle.
- traffic scheduling based on optimal selection of delivery nodes.

  NOTE – Other nodes can be selected to satisfy the requirements when a current delivery node has insufficient computation and storage resources.
- traffic scheduling based on intelligent route selection and adjustment based on routing policies.

  NOTE – Route selection and adjustment may occur, for example, when a default link is overloaded.

9 Procedures supported in NICE

Clauses 9.1 to 9.4 describe some procedures supported in NICE.

9.1 Procedure for on-demand provision

In NICE architecture, the policy control functional entity of the transport stratum plays the role of capability engine that controls the policy enforcement functional entity and on-demand provision applications or 3rd party applications can invoke this capability engine for policy updates or event reports through the service stratum.

The procedure illustrated in Figure 2 invokes a particular resource such as policy control capability. This procedure involves the interaction between an on-demand provision application (which can be a self-operated application or 3rd party application), application support functions, service control functional entity, policy control functional entity and policy enforcement functional entity.

In the following service flows, the on-demand provision application requests more bandwidth for QoS guarantees by sending a policy change request.

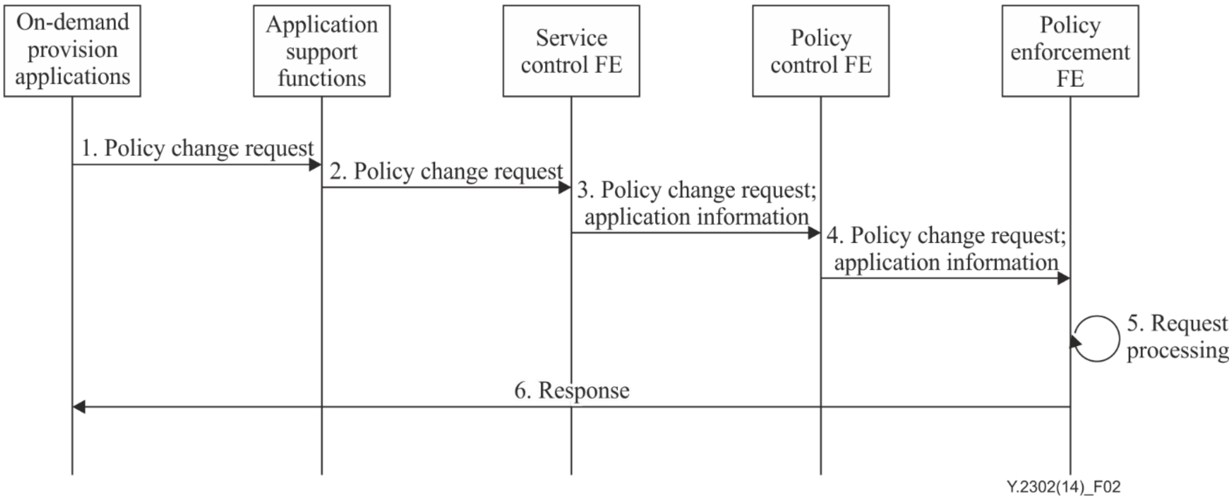
On-demand provision applications
Application support functions
Service control FE
Policy control FE
Policy enforcement FE
1. Policy change request
2. Policy change request
3. Policy change request; application information
4. Policy change request; application information
5. Request processing
6. Response
Y.2302(14)_F02

Figure 2 – Policy change request and response

1. An on-demand provision application sends a policy change request to the application support functions;
2. The application support functions transfer this request to the service control functional entity;
3. The service control functional entity transfers this request and the application information (IP filter, application ID, etc.) to the policy control functional entity;
4. The policy control functional entity analyses the request according to factors such as network status and application QoS level, then decides if the policy should be changed or not;
5. If yes, policy enforcement functional entity processes the request;
6. The policy enforcement functional entity sends a policy change report back as response.

9.2 Procedure for cooperation between fixed and mobile networks

This procedure describes the service flow of policy control cooperation between fixed and mobile networks. This service flow includes interactions between the policy control and enforcement of fixed and mobile networks and the application. The following service flow, illustrated in Figure 3, describes the detailed procedure for visiting applications through converged policy control.

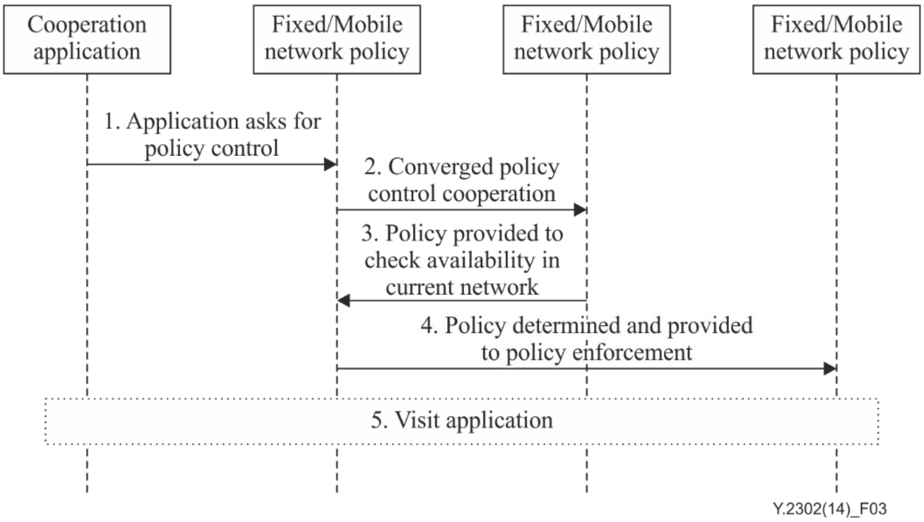
Cooperation application
Fixed/Mobile network policy
Fixed/Mobile network policy
Fixed/Mobile network policy
1. Application asks for policy control
2. Converged policy control cooperation
3. Policy provided to check availability in current network
4. Policy determined and provided to policy enforcement
5. Visit application
Y.2302(14)_F03

Figure 3 – Procedure for visiting application policy control

1. A user visits an application while accessing via a fixed/mobile network which is not the subscribed network.

2. Converged policy control is established between the network that the user is currently accessing and the network to which the user is subscribed.
3. The policy of the user's subscribed network is checked by the current network's policy control and modified accordingly.
4. The policy is determined and sent to the policy enforcement functional entity.
5. The policy enforcement functional entity carries out the policy and the user visits the application.

9.3 Procedure for awareness and optimization

In NICE architecture, the content and context detection functional entity (CD-FE) extracts information from the transport stratum, including network resource, user profile information etc., and transfers the extracted information to the content and context analysis functional entity. Then the analysis results are provided to the traffic scheduling functional entity for route scheduling.

The service flow illustrated in Figure 4 describes the procedure to schedule the route for a special application based on content and context analysis of this application. This procedure involves interaction of the content and context detection functional entity, the content and context analysis functional entity, the traffic scheduling functional entity and the traffic scheduling enforcement functional entity.

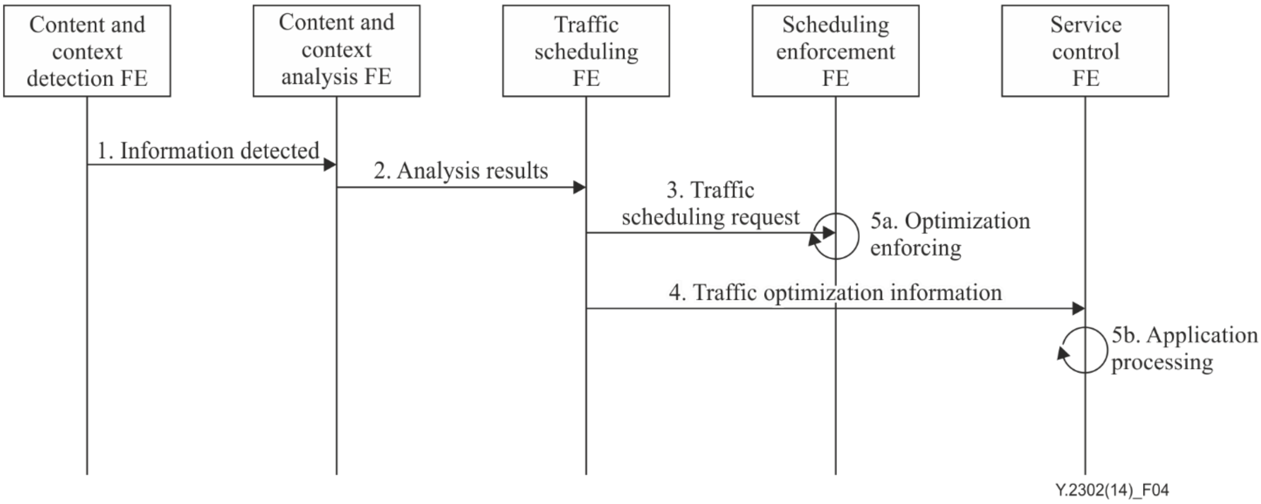
Content and context detection FE
Content and context analysis FE
Traffic scheduling FE
Scheduling enforcement FE
Service control FE
1. Information detected
2. Analysis results
3. Traffic scheduling request
5a. Optimization enforcing
4. Traffic optimization information
5b. Application processing
Y.2302(14)_F04

Figure 4 – Application route scheduling based on content and context analysis

1. The content and context detection functional entity (CD-FE) extracts network resource information, user profile information and user terminal parameters, and provides the information to the content and context analysis functional entity (CA-FE).
2. The CA-FE distinguishes and marks traffic flows based on predefined rules. The CA-FE provides analysis results to the traffic scheduling functional entity (TS-FE) according to predefined rules and information provided by the CD-FE.
3. The TS-FE provides scheduling rules to the traffic scheduling enforcement functional entity (TSE-FE) based on the content and context analysis results and scheduling rules.
4. The TS-FE also provides scheduling rules to the service control functional entity (SC-FE).
5. The TSE-FE executes traffic localization, route selection or delivery node selection rules or the SC-FE executes application scheduling rules to optimize the application experience.

9.4 Procedure for openness

Similar to clause 9.1, Figure 5 and the procedure that follows describe how third party applications invoke the capability of the policy control functional entity (PC-FE) for guarantying QoS.

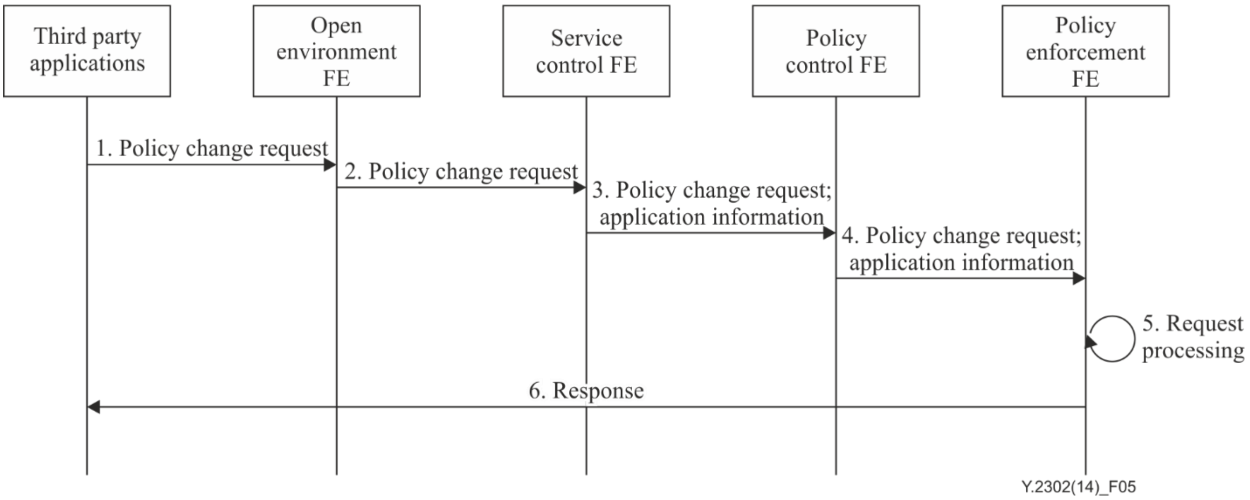

Figure 5 – QoS guarantee invoked for third party applications

1. Third party applications send a policy change request to the open environment functional entity (OE-FE);
2. The OE-FE adapts the protocol and transfers this request to the service control functional entity (SC-FE);
3. The SC-FE transfers this request and the application information (IP filter, application ID, etc.) to the policy control functional entity (PC-FE);
4. The PC-FE analyses the request according to factors such as network status or application QOS level, then decides if the policy should be changed or not;
5. If the policy is to be changed, the policy enforcement functional entity (PE-FE) processes the request;
6. The PE-FE sends a change report back as response.

10 Reference points

10.1 Pn reference point

Pn is the reference point between the open environment functional entity (OE-FE) and the applications.

With this reference point, the application developers can access the development and test environment provided by the OE-FE.

In addition with this reference point, the applications can send resource and capability requests with authentication and authorization information to the OE-FE.

10.2 Sn reference point

Sn is the reference point between open environment functional entity (OE-FE) and service control functional entity (SC-FE).

With this reference point, the OE-FE can transfer formatted resource and capability requests, such as application bandwidth and QoS assignment requirement, to the SC-FE.

In addition with this reference point, the response and notification information, such as the resource invocation result or network current status, can be sent from the SC-FE to the OE-FE.

10.3 Rm reference point

Rm is the reference point between the open environment functional entity (OE-FE) and the policy control functional entity (PC-FE).

With this reference point, the OE-FE sends policy requests, such as bandwidth adjustment or QoS level update, to the PC-FE, then receives the response or invokes a result and sends it back to third party applications.

10.4 Ru reference point

Ru is the reference point between the service user profile functional entity (SUP-FE) and the policy control functional entity (PC-FE).

With this reference point, the PC-FE utilizes the user's identity message (in NICE architecture, charge rate/content authorization information is required to be included).

The Ru reference point is required to correspond with I-TCn in [ITU-T Y.2012]. In NICE architecture, the transport user profile functional entity (TUP-FE) is merged into the SUP-FE; the PC-FE is required to support user priority according to the SUP-FE.

10.5 Rs reference point

Rs is the reference point between the service control functional entity (SC-FE) and the policy control functional entity (PC-FE).

The Rs reference point is aligned with the Rs reference point specified in RACF [ITU-T Y.2111] which allows application bandwidth and QoS assignment requirements to be exchanged between PC-FE and SC-FE. Either push or pull mode may be used.

The Rs reference point allows the PC-FE to send release of resource confirmation and results to the SC-FE.

Besides the capabilities described in RACF [ITU-T Y.2111], the Rs reference point allows the PC-FE to assign bandwidth and QoS level according to the output of application support functions which reflects the requirements from third party or self- operated applications.

10.6 Sc reference point

Sc is the reference point between the service control functional entity (SC-FE) and the transport scheduling functional entity (TS-FE).

The Sc reference point allows traffic distribution requirements to be exchanged between the TS-FE and the SC-FE. Either push or pull mode may be used.

The Sc reference point allows the TS-FE to send scheduling of resource confirmation and results to the SC-FE.

10.7 Rw reference point

Rw is the reference point between the policy control functional entity (PC-FE) and the policy enforcement functional entity (PE-FE).

The Rw reference point is aligned with the Rw reference point of RACF [ITU-T Y.2111] which allows the final admission decisions to be installed (either pushed or pulled) to the PE-FE from the PC-FE. This reference point is required to be able to support both fixed and mobile networks.

The Rw reference point allows the PC-FE to push decisions to the PE-FE and also allows the PE-FE to request decisions.

10.8 Rf reference point

Rf is the reference point between the policy control functional entity (PC-FE) and the content and context analysis functional entity (CA-FE).

The Rf reference point allows the CA-FE to distribute analysis results to the PC-FE. The distribution is performed in either push or pull mode.

The information distributed with the Rf reference point includes, but is not limited to, the following items:

- User traffic analysis results based on predefined rules and information provided by the CD-FE, such as user profile information, user traffic information and user terminal parameters.
- Information about users' service preferences (e.g., preferred URL while surfing the web).
- Network status analysis results based on predefined rules and information provided by the CD-FE, such as network resource information and access network related information.

10.9 Rb reference point

Rb is the reference point between the policy control functional entity (PC-FE) and the traffic scheduling functional entity (TS-FE).

The Rb reference point allows PC-FE decisions regarding network resources including QoS and bandwidth and admission control to be distributed to the TS-FE. The distribution is performed in either push or pull mode.

10.10 Fc reference point

Fc is the reference point between the content and context analysis functional entity (CA-FE) and the traffic scheduling functional entity (TS-FE).

The Fc reference point allows the CA-FE to distribute analysis results to the TS-FE. The distribution is performed in either push or pull mode.

The information distributed with Fc reference point could be the same as that distributed with the Rf reference point.

10.11 Ft reference point

Ft is the reference point between the content and context analysis functional entity (CA-FE) and content and context detection functional entity (CD-FE).

The reference point Ft allows the following information to be exchanged between the CA-FE and the CD-FE:

- Data information:
  - user profile information from the service user profile functional entity (SUP-FE), including user geographical location, logical location, user ID, service profile etc.;
  - user terminal parameters from traffic transferred through the transport network or from the terminal management system, such as manufacturer, terminal type, terminal OS, etc.;
  - user traffic information from traffic transferred through the transport network, including types of network traffic such as web, P2P, instant message (IM) and e-mail. Concerning web traffic, the CD-FE counts the number of visits to different uniform/universal resource locators (URLs);

  - network resource information from the operation support system (OSS), such as link bandwidth, bandwidth utilization, user data rate and other available resource parameters;
  - access network related information from the OSS, such as the access technology used (cable, fibre, DSL, 3G, WiFi) and available bandwidth.
- Control information:
  - Application/user management strategy.
  - AAA information.
  - Necessary file updates.
  - Device management information.

The reference point Ft also allows security analysis between the CA-FE and the CD-FE. Abnormal data flows are checked through the reference point Ft.

10.12 Ce reference point

Ce is the reference point between the traffic scheduling functional entity (TS-FE) and the traffic scheduling enforcement functional entity (TSE-FE).

The reference point Ce allows traffic scheduling rules exchanged between the TSE-FE and the TS-FE. Either push or pull mode can be used.

All types of traffic scheduling rules are specified as follows:

- Localization rules: The TSE-FE deploys traffic localization rules from Ce.
- Intelligent route rules: The TS-FE selects or adjusts routes intelligently based on the rules from Ce. The TSE-FE deploys network resource allocation. The intelligent route rules include but are not limited to:
  - Messages to keep the the reference point and the channel alive.
  - Messages for the TS-FE to request device information from the TSE-FE, including processing capabilities, transport capabilities, storage capabilities, etc.
  - Messages for the TSE-FE to send device information, flow table information and port information to the TS-FE.
  - Command messages from the TS-FE to the TSE-FE.
- Traffic scheduling rules based on selection of the traffic delivery network node.
- Traffic scheduling rules according to network status.

NOTE – For example, a route needs to be changed when a certain network link in the route is overloaded in order to improve the user experience.

10.13 Su reference point

Su is the reference point between the service user profile functional entity (SUP-FE) and the service control functional entity (SC-FE).

With this reference point, the SC-FE utilizes the user's identity message (in NICE architecture, charge rate/content authorization information is required to be included) for authentication and authorization.

11 Security considerations

NICE is required to contain the security features incorporated in existing networks and allow for secure interconnection with other networks including NICE or non-NICE networks. The security requirements of the NGN are addressed in [ITU-T Y.2701], [ITU-T Y.2201], [ITU T Y.2702], [ITU-T Y.2240] and [ITU-T Y.2111].

Besides the security requirements for NGN, NICE provides:

1) Protection against unauthorized use of data from the CA-FE results.

2) Security checks of abnormal data flow between the CA-FE and the CD-FE.

3) Protection against third party unauthorized use of network resources and unauthorized access to information flows and applications.

4) Security access environment for third party and self-operated applications and compliance with the authentication and authorization requirements according to [ITU-T Y.2240].

5) Encrypted channel between the TS-FE and the TSE-FE. The TS-FE and TSE-FE are required to authenticate each other by exchanging certificates. The certificates must be configurable.

Bibliography

[b-ITU-T H.780]	Recommendation ITU-T H.780 (2012), *Digital signage: Service requirements and IPTV-based architecture*.
[b-ITU-T M.1400]	Recommendation ITU-T M.1400 (2013), *Designations for interconnections among operators' networks*.
[b-ITU-T Q.825]	Recommendation ITU-T Q.825 (1998), *Specification of TMN applications at the Q3 interface: call detail recording*.
[b-ITU-T Y.101]	Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.
[b-ITU-T Y.2002]	Recommendation ITU-T Y.2002 (2009), *Overview of ubiquitous networking and of its support in NGN*.
[b-ITU-T Y.2091]	Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*.

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, 2014