International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2301

(08/2013)

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

Next Generation Networks – Enhancements to NGN

Network intelligence capability enhancement – Requirements and capabilities

Recommendation ITU-T Y.2301

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
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.2301

Network intelligence capability enhancement – Requirements and capabilities

Summary

Recommendation ITU-T Y.2301 specifies the requirements and capabilities of network intelligence capability enhancement (NICE), an enhancement for NGNs supporting some intelligence capabilities for the provisioning of services according to the requirements of users and application providers.

NICE capabilities aim to support the following features: 1) awareness features: user, application and network awareness with content and context analysis; 2) on-demand provision features: user self-assignment of service subscription and network resources, and user on-demand service of quality assurance; 3) optimization features: traffic management based on intelligent traffic scheduling; 4) openness features: invocation of the above features by third-party application providers; 5) cooperation features: network coordination between policy control capabilities of different access networks.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2301	2013-08-13	13

Keywords

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

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.2301

Network intelligence capability enhancement – Requirements and capabilities

1 Scope

This Recommendation specifies the requirements and capabilities for the network intelligence capability enhancement (NICE), which enhances NGNs in supporting some intelligence capabilities for the provisioning of services according to the requirements of users and application providers.

The requirements are provided from a high-level perspective. Functional requirements for the different capabilities of NICE are outside of 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.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[ITU-T Y.2111] Recommendation ITU-T Y.2111 (2011), *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.2701] Recommendation ITU-T Y.2701 (2007), *Security 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 are classified as "data" (e.g., text, encoded values, multimedia description language introduced by [b-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 media stream [ITU-T Y.2012]: A media stream can consist of audio, video, or data, or a combination of any of them. Media stream data conveys user or application data (i.e., a payload) but not control data.

3.1.11 network virtualization [b-ITU-T Y.3011]: A technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collections of multiple virtual networks can simultaneously coexist over the shared networks. This includes the aggregation of multiple resources in a provider and appearing as a single resource.

3.1.12 NGN [b-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.

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

3.1.14 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.

3.1.15 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

This Recommendation defines the following term:

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

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
BRAS	Broadband Remote Access Server
DPI	Deep Packet Inspection
DSL	Digital Subscriber Loop
DSLAM	Digital Subscriber Line Access Multiplexer
HD	High Definition
ID	Identity
IdM	Identity Management
IM	Instant Messaging
NGN	Next Generation Network
NICE	Network Intelligence Capability Enhancement
OS	Operating System
P2P	Peer-to-Peer
QoS	Quality of Service
RACF	Resource and Admission Control Functions
RAN	Radio Access Network
SR	Service Router
SUP	Service User Profile
TCP	Transmission Control Protocol
UE	User Equipment
URL	Universal Resource Locator
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network

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 Recommendation 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 this Recommendation.

6 Introduction and requirements of NICE

6.1 Overview of NICE

6.1.1 Network development trends

Emerging and future telecommunication services, together with the introduction of disruptive technologies (e.g., mobile Internet and cloud computing) and new business models, are leading to new requirements for networks, such as high bandwidth, enhanced mobility, real-time interactivity, high quality and enhanced security, etc.

With the arrival of the mobile Internet era, operators are facing increased threats of becoming "pipeline providers". In the past, networks were an operator's core competitive advantage, but nowadays user information, management and service capabilities are the new competitive factors. Meanwhile, with 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" or disparity between traffic and revenues is becoming wider.

These network development trends require operators to identify the implications of user and service requirements at the network level, and to increase the network efficiency and value through intelligent resource scheduling and network traffic management.

From the perspective of the next generation network (NGN), the capabilities provided by NGNs need then to be enhanced while taking into account these emerging requirements. This is a key direction of the evolution of NGNs.

6.1.2 NICE and its features

This Recommendation focuses on some specific enhancements to NGN which are termed globally as "network intelligence capability enhancement" (NICE).

As defined in clause 3, NICE is an enhancement for NGNs which support some intelligence capabilities for the provisioning of services according to the requirements of users and application providers. These intelligence 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.

NICE is required to support the following features:

1) awareness features: user, application and network awareness with content and context analysis;
2) on-demand provision features: user self-assignment of service subscription and network resources, user on-demand service of quality assurance;
3) optimization features: traffic management based on intelligent traffic scheduling;
4) openness features: invocation of the above features by third-party application providers;
5) cooperation features: network coordination between policy control capabilities of different access networks.

Appendix I provides some informative use cases related to these features.

Appendix II provides some information concerning business roles in a NICE environment.

6.2 Requirements of NICE

6.2.1 Requirements of awareness

NICE is required to support awareness features that include the following aspects:

- network resource awareness, such as link bandwidth, bandwidth utilization, cost of routes and other available resource information;
- user location awareness, such as the geographical location of the user, the logical location of the user (i.e., location of the user in terms of NICE provider's network), etc.;
- user profile awareness.

  NOTE – Profile information includes, but is not limited to, user identity, user account number, etc.
- Access network awareness, such as access network technology (e.g., cable access, 3rd generation radio access network (3G RAN) access, digital subscriber loop (DSL) access, optical access, wireless fidelity (WiFi) access), access network bandwidth, etc.;
- user terminal parameters awareness, such as terminal manufacturer, terminal type, terminal operating system (OS), etc.;
- application data awareness, according to national and regional laws, regulations and policies. This may include awareness of application data type (such as still image, graphic, video and data), application data statistics and an application's user preferences.

6.2.2 Requirements of on-demand provision

NICE is required to support on-demand provision features that include the following aspects:

- user self-assignment for service subscription;
- user self-assignment for access bandwidth;
- user self-assignment for quality of service (QoS) level of access network;
- intelligent adjustment of bandwidth or QoS level according to the user profile;
- intelligent adjustment of bandwidth or QoS level according to the terminal parameters;
- resource self-assignment and QoS guarantee for specific services of application providers.

6.2.3 Requirements of cooperation

NICE is required to support cooperation features that include the following aspects:

- a user uses a single account number to connect to different access networks;
- a user obtains the required QoS level or quality of experience when he/she connects to different access networks;
- a user obtains the required QoS level or quality of experience when he/she uses different terminals.

6.2.4 Requirements of optimization

NICE is required to support optimization features that include the following aspects:

- traffic analysis based on user profile and application type;
- traffic scheduling optimization via traffic localization;
- traffic scheduling optimization via route selection based policy;
- traffic scheduling optimization via delivery node selection;
- traffic scheduling optimization according to network status;

NOTE – A given traffic transport route needs to be changed in order to improve the user experience when a link in the route is overloaded.

- traffic scheduling optimization via network virtualization;
- transport protocol optimization, e.g., transport control protocol (TCP) optimization in wireless environments.

6.2.5 Requirements of openness

NICE is required to support openness features that include the following aspects:

- invocation by a third-party application provider of user, application, and network awareness features;
- invocation by a third-party application provider of resource assignment features;
- invocation by a third-party application provider of network virtualization features;
- support of standard application programming interfaces (APIs) to invoke awareness and resource assignment features by a third-party application provider.

7 Capability framework of NICE

7.1 Capability framework overview of NICE

NICE builds upon NGN capabilities, including the basic ones described in [ITU-T Y.2201] and the capabilities for NGN service integration and delivery environment described in [ITU-T Y.2240].

Figure 1 provides an overview of the NICE capability framework.

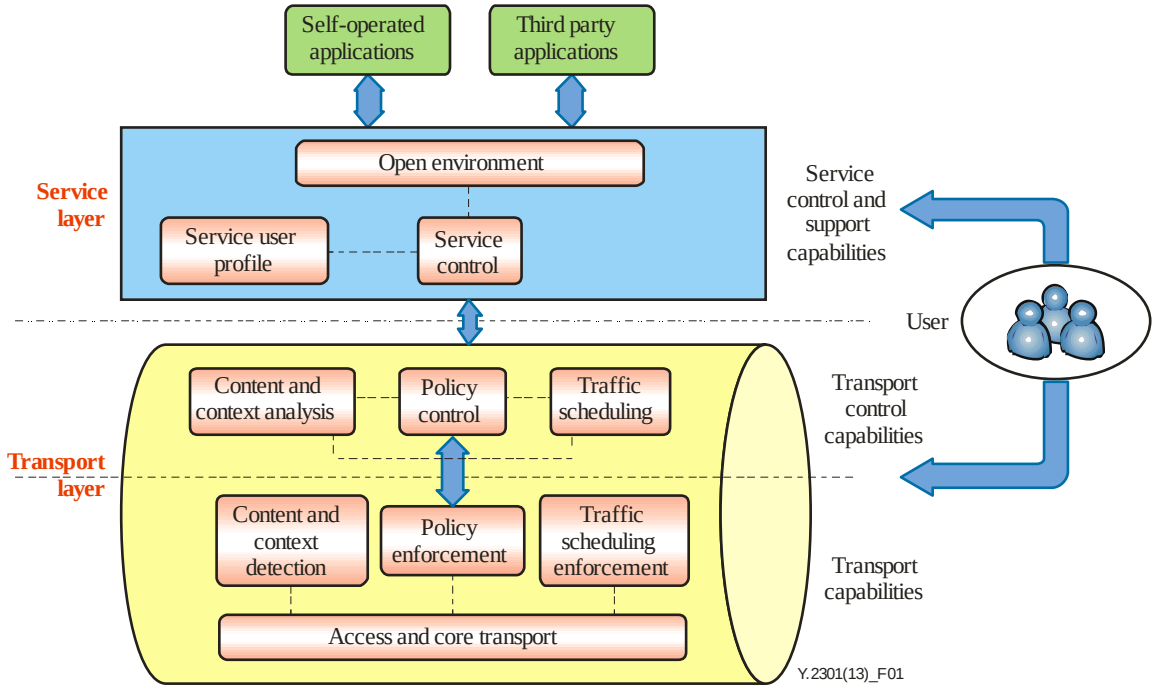

Figure 1 – Overview of the NICE capability framework

The service layer provides service control and support capabilities, consisting of service user profile, service control and open environment capabilities.

The transport layer provides transport control capabilities and transport capabilities.

The transport control capabilities consist of content and context analysis, policy control and traffic scheduling capabilities.

The transport capabilities consist of access and core transport, content and context detection, policy enforcement and traffic scheduling enforcement capabilities.

Via the interaction with the service control and support capabilities, the transport control capabilities can provide network status and application data-related information to applications, and can collect resource requirements from applications.

7.2 Relationships between requirements and capabilities of NICE

The relationships between the requirements and capabilities of NICE are as follows:

- open environment capabilities support the requirements of openness;
- content and context analysis and content and context detection capabilities support the requirements of awareness;
- policy control and traffic scheduling capabilities support the requirements of on-demand provision;
- traffic scheduling and traffic scheduling enforcement capabilities support the requirements of optimization;
- policy control and policy enforcement capabilities support the requirements of cooperation.

7.3 Layering and interactions between capabilities

7.3.1 Service layer

Open environment capabilities allow the interconnection of third-party applications and self-operated applications with transport control capabilities. Service control capabilities interconnect with service user profile (SUP) and transport control capabilities.

Open environment receives a NICE capability request from third-party applications or self-operated applications and transfers the request to transport control capabilities.

Service control enforces service registration, service authentication and service resource assignment. Service control may also send a NICE capability request to transport control capabilities with the necessary user and service information obtained from the SUP.

7.3.2 Transport layer

Content and context analysis interconnects with policy control, traffic scheduling and content and context detection capabilities.

Policy control interconnects with service control and open environment capabilities in the service layer and with policy enforcement capabilities in the transport layer.

Traffic scheduling interconnects with service control and open environment capabilities in the service layer and with traffic scheduling enforcement capabilities in the transport layer.

Content and context detection, policy enforcement and traffic scheduling enforcement also interconnect with access and core transport capabilities.

As far as content and context analysis is concerned:

- content and context analysis retrieves the awareness-related information from content and context detection capabilities and the SUP, then deeply analyses the information.

  NOTE – Deep packet inspection (DPI) [b-ITU-T Y.2770] is one of the possible technical methods for content and context detection, while it is not the mandatory one.

  Content and context analysis provides analysis results related to user traffic and network status to policy control and traffic scheduling capabilities.

As far as policy control is concerned:

- policy control receives third-party or self-operated application's bandwidth and QoS assignment requirements from service control and open environment capabilities. Policy control may also receive bandwidth and QoS assignment requests from users;
- policy control sends policy deployment requests to policy enforcement capabilities.

As far as traffic scheduling is concerned:

- traffic scheduling receives third-party or a self-operated application's traffic scheduling requests from service control and open environment capabilities;
- traffic scheduling sends traffic scheduling requests to traffic scheduling enforcement capabilities.

8 Service layer capabilities

8.1 Service user profile

The SUP requires access to user subscription and user location information (e.g., access network-related information, physical and logical location). The SUP 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 the SUP.

SUP requirements for NICE are aligned with the functional requirements of SUP-FE in an NGN [ITU-T Y.2012].

The SUP for NICE is also required to support identity management (IdM) [ITU-T Y.2720] as an enhancement to increase confidence in identity information of entities and enhance business and security applications and services. SUP requirements to support IdM are 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;
- support of entity location and presence information;
- support of discovery and exchange of identity information;
- identity lifecycle management;
- enablement of business and security applications;
- support of data model and schemas to facilitate interoperability of SUP-related information (e.g., identity information exchange) within a NICE provider;
- access control to identity information in order to guarantee identity information security and privacy.

8.2 Service control

Service control is required to receive and transfer the application requests concerning policy control and traffic scheduling to the transport layer or transport-related information to the service layer.

Service control requirements for NICE are aligned with the functional requirements of service control functions (SCF) in NGNs [ITU-T Y.2012] with the following additional requirements in terms of received and transferred information:

- information allowing the identification of application data for policy control and traffic scheduling;
- information allowing the identification of applications and users;

- transport layer events (e.g., notifications of QoS modifications) reported by the transport layer to the service layer.

8.3 Open environment

Open environment requirements are aligned with the requirements of openness identified in [ITU-T Y.2240], in particular with the following requirements specific to the exposure of NICE capabilities:

- open access to a service creation environment [ITU-T Y.2240], including to a wide range of tools and technologies, enabling developers and third-party applications to create rich applications taking full advantage of NICE capabilities, such as policy control and traffic scheduling capabilities;
- support for self-operated applications' invocation of NICE capabilities.

  NOTE – Self-operated applications are not prevented from communicating directly with other NICE capabilities.

9 Transport layer capabilities

9.1 Transport control capabilities

9.1.1 Content and context analysis

Content and context analysis receives the content and context information from the content and context detection capabilities and deeply analyses this information.

Content and context analysis supports processing of this information with other information obtained from SUP capabilities (e.g., user profiles and presence status data), as well as storage of the post-processing content and context information.

Content and context analysis distributes the analysis results related to content and context information to the requester(s), such as policy control and traffic scheduling capabilities. Content and context information can be distributed in real time and/or on-demand according to the requirements.

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

Content and context analysis is also required to support the following additional requirements:

- providing user traffic analysis results based on predefined rules and information provided by content and context detection capabilities (e.g., user profile information, user location information and user terminal parameters);
- providing information related to user's application data, such as application data type (such as audio, still image, graphic, video and data), application data statistics, application's user preferences;
- providing network status analysis results based on predefined rules and information provided by content and context detection capabilities (e.g., network resource information and access network-related information).

9.1.2 Policy control

Policy control receives analysis results regarding content and context information from content and context analysis capabilities while it also receives application requests related to bandwidth and the QoS assignment from service control and open environment capabilities.

Policy control also makes policy information decisions and updates, and sends the results of these policy decisions and updates to policy enforcement capabilities.

Policy control also makes decisions regarding network resource and admission control, supporting unified policy database and consistent policy definitions, and a variety of access and core networks within a general resource control framework.

Policy control requirements for NICE are aligned with the functional requirements of resource and admission control functions (RACF) [ITU-T Y.2111], with the following additional requirements concerning transport resource allocation and the management of QoS policies (within the network and at the network boundaries), based on users' and application providers' requirements:

- support of intelligent assignment of bandwidth and QoS level according to on-demand requirements from users via a user self-service portal.

  NOTE – The self-service portal allows the interaction of users with the NICE provider for on-demand service provision, but it is not part of the NICE capabilities.
- Support of intelligent assignment and adjustment of bandwidth and QoS level according to requirements from a third-party application provider or possibly, a NICE provider via open environment capabilities;
- support of intelligent adjustment of bandwidth and QoS level according to the content and context analysis results (e.g., user traffic and network status analysis results).

9.1.3 Traffic scheduling

Traffic scheduling receives an application's traffic delivery requests from service control and open environment capabilities and receives analysis results from content and context analysis capabilities. It then makes decisions based on these results and generates traffic scheduling rules.

Traffic scheduling requirements are aligned with the requirements of NGN [ITU-T Y.2201] with the following additional requirements in terms of the generation of traffic scheduling rules:

- traffic scheduling rules (for intra-NICE provider's network and inter-NICE provider's network) based on traffic localization;
- traffic scheduling rules based on the selection of the traffic delivery network node;
- traffic scheduling rules according to network status;

  NOTE – For example, a route needs to be changed in order to improve the user experience when a network link in the route is overloaded.
- traffic scheduling rules according to intelligent routing based on route selection policy;
- traffic scheduling rules according to network virtualization.

9.2 Transport capabilities

9.2.1 Content and context detection

Content and context detection collects transport-related information.

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

Content and context detection extracts the following transport-related information:

- user location information, including user 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, according to national and regional laws, regulations and policies;
- 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.

9.2.2 Policy enforcement

Policy enforcement applies the policy control's policy decisions via the interaction with transport capabilities.

Policy enforcement supports end-to-end traffic management across access and core transport networks of varying technologies to ensure that the requirements from users and applications can be satisfied.

Policy enforcement requirements for NICE are aligned with the functional requirements of RACF [ITU-T Y.2111] and with the following additional requirements:

- enforcement of on-demand bandwidth and QoS levels in order to satisfy on-demand requirements from users and application providers;
- enforcement of bandwidth and QoS levels based on content and context analysis results.

9.2.3 Traffic scheduling enforcement

Traffic scheduling enforcement receives traffic scheduling rules and decisions from traffic scheduling capabilities and fulfils these rules and decisions via the interaction with transport capabilities.

Traffic scheduling enforcement requirements are aligned with the requirements of NGN [ITU-T Y.2201] with the following additional requirements:

- Enforcement of traffic scheduling based on traffic localization schemes.

  NOTE 1 – P2P contents may be stored locally to decrease outgoing traffic and the peers for storage selected based on the localization principle.

- Enforcement of traffic scheduling based on optimal selection of delivery nodes.

  NOTE 2 – Other nodes can be selected to satisfy the requirements when a current delivery node has insufficient computational and storage resources.

- Enforcement of traffic scheduling based on intelligent route selection and adjustment based on routing policies.

  NOTE 3 – Route selection and adjustment may occur, for example, when a default link is overloaded or when resources are virtualized and allocated to different applications according to related requirements.

- Enforcement of traffic scheduling based on resource allocation using network virtualization.

9.2.4 Access and core transport capabilities

Access and core transport capabilities provide the connectivity for the components of the NICE provider's infrastructure. These capabilities provide support for application data delivery, as well as control and management information delivery.

Access and core transport requirements for NICE are aligned with the transport requirements of NGN [ITU-T Y.2012], with the additional following optional requirement:

- Support of cache and media stream delivery functions in transport nodes.

  NOTE – For example, transport nodes may integrate cache functions to support content localization: media streams may be stored in the cache of the NICE provider's network nodes so that transport nodes outside the NICE provider's network may not be selected based on the localization principle.

10 Security considerations

The security requirements of NICE are aligned with the security requirements of NGN [ITU-T Y.2201], [ITU-T Y.2701] and [ITU-T Y.2240] and with the following additional requirements:

- enhanced security of network availability and accessibility, upon demand by users;
- protection against unauthorized use of information generated by content and context analysis;
- enhanced security for protection against a third-party's unauthorized use of network resources and unauthorized access to traffic flows.

Appendix I

Use cases of NICE features

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

I.1 Use case of cooperation feature: unified user profile and charging case between fixed and mobile network

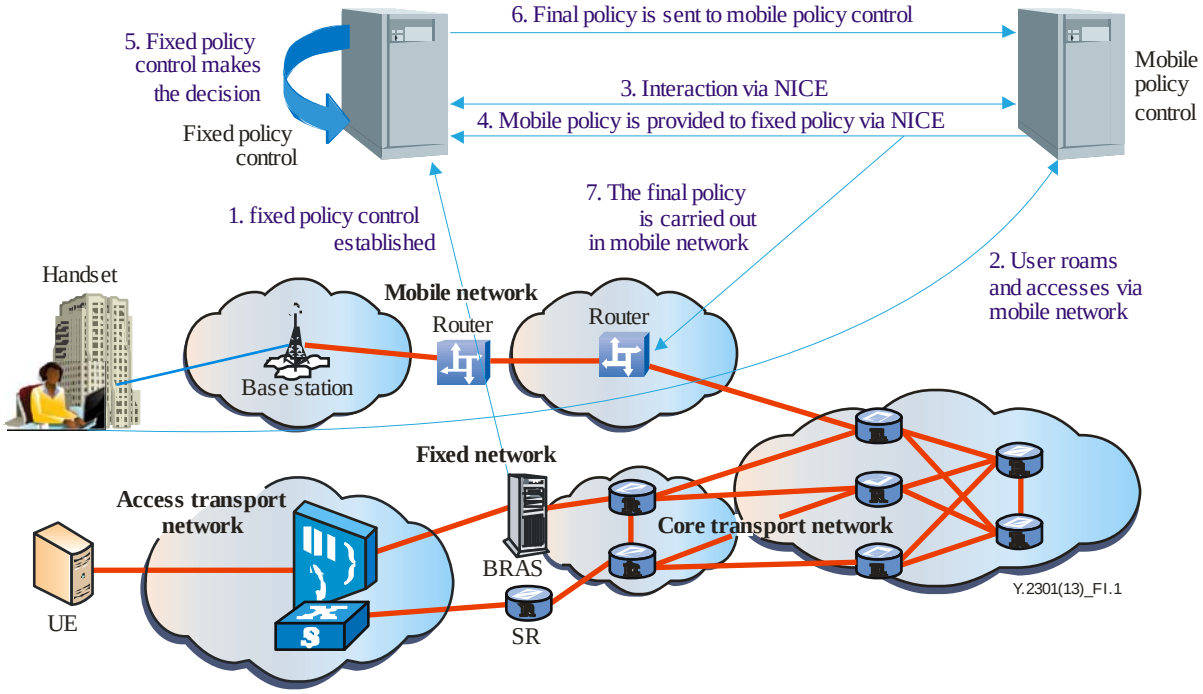

Figure I.1 – Fixed-mobile network cooperation

In traditional networks (e.g., NGN without NICE capabilities), when a user switches the network connection between the mobile network and the fixed network (including WLAN), policies (including charging rules, services, bandwidth, etc.) may change causing severe inconvenience.

With NICE capabilities, when the user roams between the mobile and fixed network, the same policies apply all the time; the procedure is as follows:

1. fixed policy control is established when a user accesses a fixed network;
2. the user roams and accesses the mobile network;
3. interaction via NICE capabilities is established between the fixed policy control and mobile policy control;
4. mobile policy control is established and the mobile policy is provided to the fixed policy control via NICE capabilities;
5. fixed policy control makes decisions according to current mobile network resource information;
6. fixed policy control sends the final policy to mobile policy control;
7. mobile policy control carries out the final policy and the user gets access while the policies (charging rules, services, bandwidth, etc.) remain unchanged.

I.2 Use case of on-demand provision feature: user self-service access bandwidth assignment

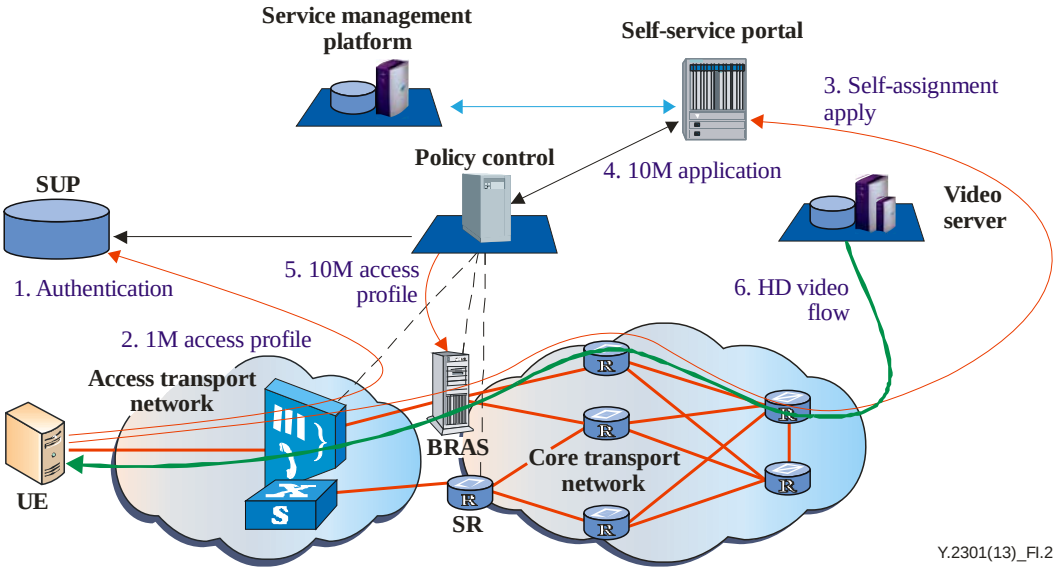

Figure I.2 – User self-service access bandwidth assignment

A user subscribes to a fixed broadband network with 1 Mbit/s data rate. His/her user profile is authenticated in the SUP. The user would like to have a high definition (HD) video on-demand service which requires 10 Mbit/s data rate. In the current situation, the user has to subscribe to a new service pack which requires manual operation and takes a lot of time.

With NICE capabilities, the user can log onto a self-service portal and apply for a higher bandwidth automatically without further manual care.

The self-service procedure instructions are as follows:

1. a user accesses a NICE network and is authenticated by the SUP;
2. SUP sends the user profile of 1 Mbit/s access bandwidth to the access network gateway, e.g., broadband remote access server (BRAS), service router (SR);
3. the user wants to have an HD video service and requires a bandwidth increase to 10 Mbit/s through a self-service portal;
4. the 10 Mbit/s bandwidth requirement is transferred to the policy control server;
5. the policy control server processes the user's bandwidth increase requirement and sends the new user profile of 10 Mbit/s to the access network gateway;
6. the user bandwidth is raised by the access network gateway, then HD video on-demand traffic is delivered to the user from the video server.

I.3 Use case of awareness feature: guaranteed user experience of applications based on content and context analysis

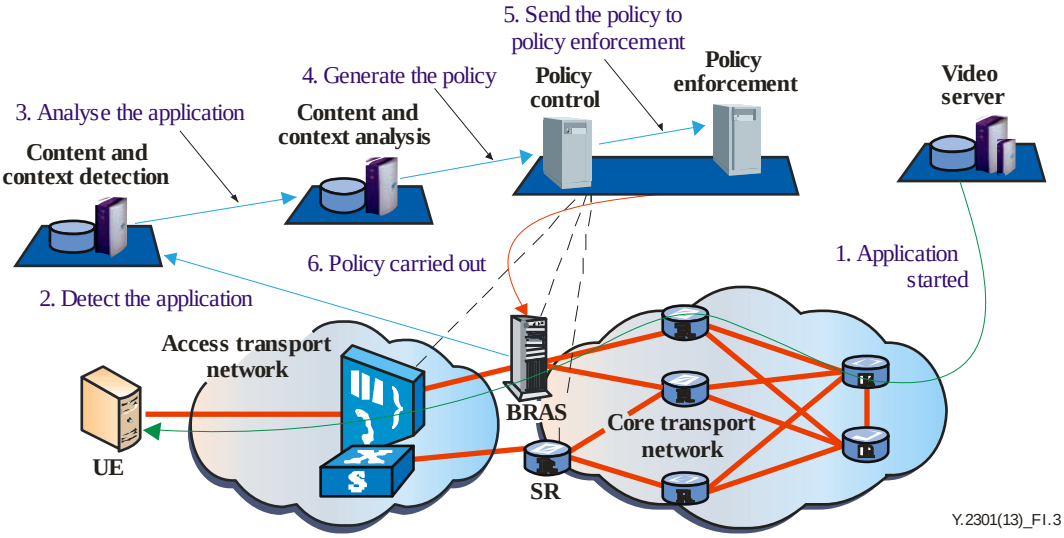

Figure I.3 – Guaranteed user experience of a video application

A user is surfing the web and downloading large files. The user decides to watch a video from an Internet video website. Without NICE capabilities, the video traffic is interfered with by other traffic at the same time. The experience of watching the video is severely affected.

With NICE capabilities, content and context detection detects the video application and sends the information to content and context analysis. The analysis results, including application data-related information, terminal parameters, etc., are sent to policy control. Based on the analysis results, policy control generates the policy to guarantee the video's bandwidth and QoS level, and sends the policy to policy enforcement. Then policy is carried out to make sure the user has a satisfactory experience of the video application.

The guaranteed experience procedure instructions are as follows:

1. a user starts a certain application that requires good experience;
2. content and context detection detects the application and sends the application information to content and context analysis;
3. content and context analysis extracts the user's and application's information, then sends it to policy control;
4. based on the analysis results, policy control generates the policy to guarantee the bandwidth and QoS of the application;
5. policy control sends the policy to policy enforcement;
6. policy enforcement carries out the policy.

I.4 Use case of optimization feature: P2P traffic optimization

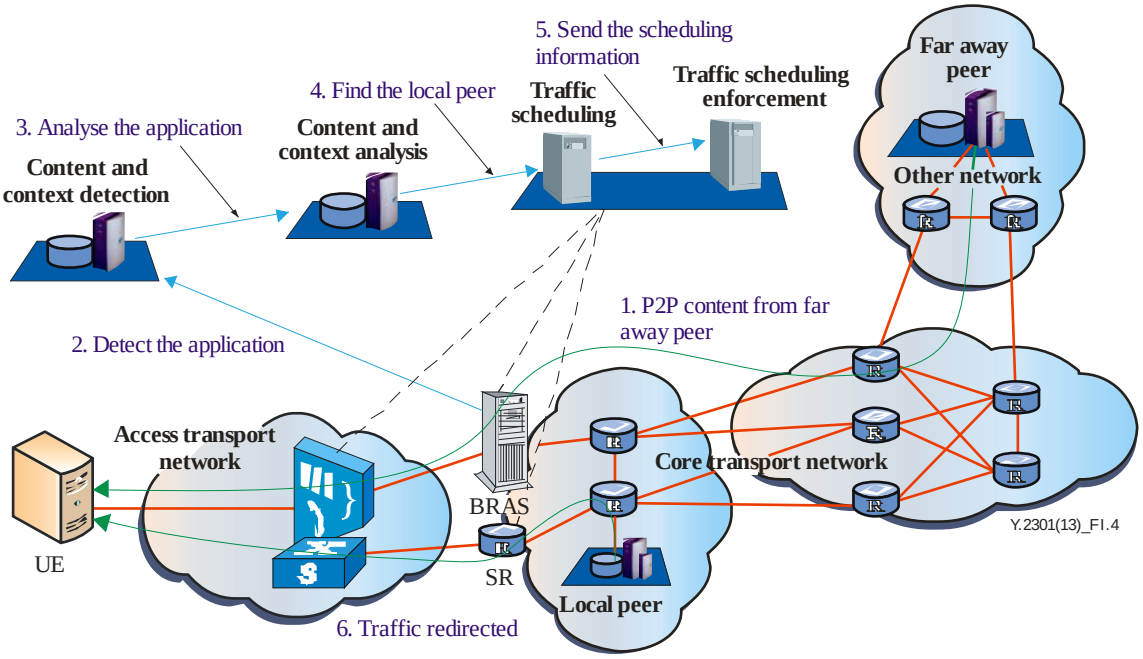

Figure I.4 – P2P traffic optimization

P2P traffic is huge in either fixed or mobile broadband networks. When a user tries to visit some P2P content via a third-party application, the third-party application searches for the content in the network.

Without NICE capabilities, the application may locate the content from peers outside the NICE provider's network, far away from the user, causing a lot of traffic in the core transport network, as well as deteriorating the user's experience.

With NICE capabilities, content and context detection sends the P2P application-related information to content and context analysis. Content and context analysis sends the analysis results to traffic scheduling. Traffic scheduling provides information to traffic scheduling enforcement about the local peer inside the NICE provider's network containing the desired P2P content for the user. Then traffic scheduling enforcement carries out the traffic scheduling and redirects the traffic, significantly decreasing the core transport network traffic, as well as improving the user experience.

P2P traffic optimization procedure instruction is shown as follows:

1. a user starts a P2P application and retrieves the content from the far away peer outside the NICE provider's network;
2. content and context detection detects the application and sends the application information to content and context analysis;
3. content and context analysis extracts the user's and traffic's information and sends it to traffic scheduling;
4. based on analysis results, traffic scheduling processes the information to find the local P2P peer node inside the NICE provider's network;
5. traffic scheduling sends the scheduling information to traffic scheduling enforcement;
6. traffic scheduling enforcement redirects the P2P traffic to the local P2P peer node according to traffic localization rules.

I.5 Use case of openness feature: exposure of NICE capabilities for provision of QoS guaranteed third-party application

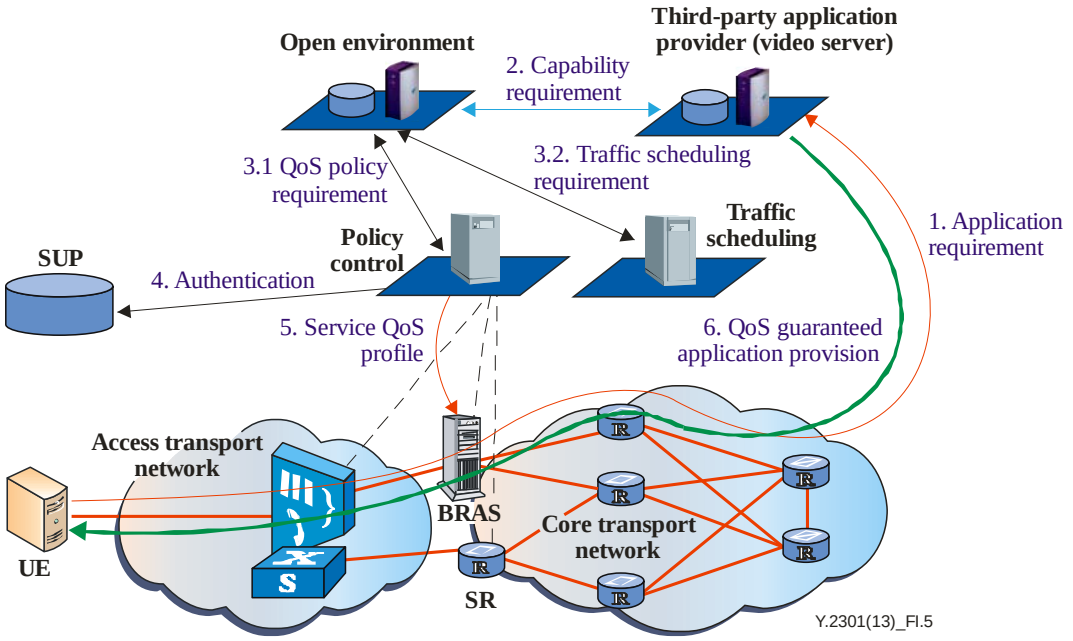

Figure I.5 – Provision of QoS guaranteed third-party application

A third-party application provider (e.g., video application provider) can cooperate with the NICE provider through an open environment, and provide high quality service to its users.

The procedure instruction of the openness of NICE capabilities is as follows:

1. a user of the video application provider visits the website requesting a high quality online video application;
2. the video application provider sends requirements including application information for requirement identification (e.g., application ID, application user ID, quality parameters) to NICE through an open environment;
3. open environment processes and transfers QoS control requirements to policy control (or a traffic scheduling requirement to traffic scheduling);
4. policy control connects the SUP and authenticates if this user has the authentication of high quality network resource allocation. After the user is authenticated, policy control decides which service profile needs to be configured in the access network gateway;
5. policy control sends the service profile to the access network gateway;
6. access network gateway deploys policy enforcement (or traffic scheduling enforcement) capabilities and guarantees the QoS of the user's video application.

Appendix II

Business roles in a NICE environment

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

The following provides some information concerning business roles in a NICE environment.

NOTE – The identified business roles and their relationships as described below do not represent an exclusive representation of all possible relevant roles and relationships which can be involved in a NICE environment.

The identified key business roles in a NICE environment are: the NICE provider, the third-party application provider and the user. Figure II.1 depicts these business roles.

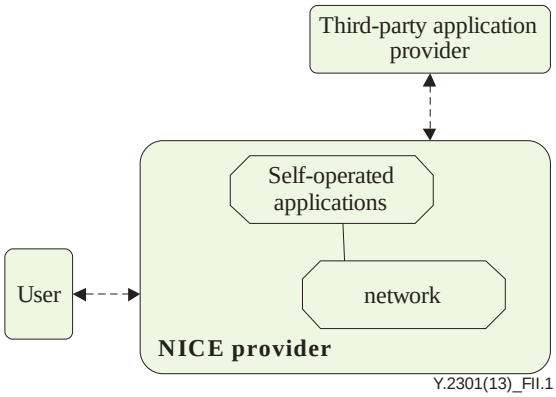

Figure II.1 – Business roles in a NICE environment

The NICE provider is an NGN provider with additional support of the NICE capabilities. The NICE provider supports the provisioning of third-party applications and self-operated applications.

NOTE 1 – The NICE provider supports the invocation by self-operated applications of the awareness, on-demand provision, cooperation and optimization NICE features for the user without a second authentication process because the user has been already authenticated by the NICE provider.

The third-party application provider has a relationship with the NICE provider. The NICE provider offers open interfaces to third-party applications for the invocation of awareness, cooperation and optimization NICE features.

The user has a relationship with the NICE provider. The NICE provider offers on-demand services and network resource provision to users making use of the awareness, cooperation and optimization NICE features.

NOTE 2 – The user may also have a relationship with the third-party application provider, but this relationship is out of the scope of the NICE environment.

Bibliography

[b-ITU-T H.760] Recommendation ITU-T H.760 (2009), *Overview of multimedia application frameworks for IPTV*.

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

[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*.

[b-ITU-T Y.2234] Recommendation ITU-T Y.2234 (2008), *Open service environment capabilities for NGN*.

[b-ITU-T Y.2770] Recommendation ITU-T Y.2770 (2012), *Requirements for deep packet inspection in next generation networks*.

[b-ITU-T Y.3011] Recommendation ITU-T Y.3011 (2012), *Framework of network virtualization for future 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, 2013