International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3321

(06/2015)

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

Future networks

# Requirements and capability framework for NICE implementation making use of software-defined networking technologies

Recommendation ITU-T Y.3321

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.3321

## Requirements and capability framework for NICE implementation making use of software-defined networking technologies


### Summary

Recommendation ITU-T Y.3321 specifies the requirements and capability framework of S-NICE (Software-defined Network Intelligence Capability Enhancement).

NICE (see Recommendation ITU-T Y.2301) is an enhanced next generation network (NGN) (i.e., an evolved version of NGN) supporting extended or additional intelligent capabilities for provisioning of services according to requirements of users and application providers. S-NICE is a specific implementation of NICE, making use of software-defined networking technologies, and its key objective is the identification of the NICE implementation requirements when relevant NICE features are supported by software-defined networking technologies.



### History

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---|---|---|---|---|
| 1.0 | ITU-T Y.3321 | 2015-06-13 | 13 | 11.1002/1000/12523 |

### Keywords

Network intelligence capability enhancement, NICE, SDN, software defined networking.


* 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


| | | Page |
|---|---|---|
| 1 | Scope | 1 |
| 2 | References | 1 |
| 3 | Definitions | 1 |
| 3.1 | Terms defined elsewhere | 1 |
| 3.2 | Terms defined in this Recommendation | 2 |
| 4 | Abbreviations and acronyms | 3 |
| 5 | Conventions | 3 |
| 6 | Requirements of software-defined NICE | 3 |
| 6.1 | Introduction to S-NICE | 3 |
| 6.2 | Requirements of service control | 4 |
| 6.3 | Requirements of open environment | 4 |
| 6.4 | Requirements of content and context analysis | 4 |
| 6.5 | Requirements of policy control | 5 |
| 6.6 | Requirements of traffic scheduling | 5 |
| 6.7 | Requirements of access and core transport | 6 |
| 6.8 | Requirements for support of virtualized network and virtualized network functions | 6 |
| 7 | The capability framework for software-defined NICE | 6 |
| 7.1 | Overview of the capability framework | 6 |
| 7.2 | The S-NICE orchestration capabilities at the service layer | 7 |
| 7.3 | The S-NICE controller capabilities at the transport layer | 8 |
| 7.4 | The S-NICE infrastructure capabilities at the transport layer | 9 |
| 8 | Security considerations | 9 |
| Appendix I – Differences between NICE capabilities and S-NICE capabilities | | 11 |
| Bibliography | | 15 |

# Recommendation ITU-T Y.3321

# Requirements and capability framework for NICE implementation making use of software-defined networking technologies

## 1 Scope

This Recommendation provides the requirements and capability framework for software-defined network intelligence capability enhancement (S-NICE). S-NICE is a specific implementation of NICE [ITU-T Y.2301] making use of software-defined networking technologies. NICE being an evolved version of NGN, S-NICE supports the intelligent features (five major features) of NICE and makes usage of software-defined networking technologies. This Recommendation specifies the requirements and capabilities of S-NICE at the next generation network (NGN) service and network stratum.

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

## 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** [b-ITU-T Y.2012]: A general reference to a provider that offers applications to the customers making use of the service capabilities provided by the NGN.

**3.1.3 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]).

**3.1.4 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.

**3.1.5 context awareness** [b-ITU-T Y.2201]: The 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.

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

**3.1.7 identity management (IdM)** [b-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.

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

**3.1.9 media stream** [b-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.

**3.1.10 network intelligence capability enhancement (NICE)** [ITU-T Y.2301]: An enhanced NGN 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 next generation network (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.

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

**3.1.13 software-defined networking (SDN)** [b-ITU-T Y.3300]: A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

**3.1.14 user** [b-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 terms:

**3.2.1 S-NICE controller capabilities**: Capabilities providing a means to control the S-NICE infrastructure capabilities (such as data transport and processing on per flow basis) requested by applications.

**3.2.2 S-NICE infrastructure capabilities**: Capabilities which are controlled by the S-NICE controller capabilities to perform actions according to applications' requirements.

**3.2.3 S-NICE orchestration capabilities**: Capabilities which coordinate with applications and S-NICE controller capabilities to provide software-defined control and management of network resources and users, as well as service creation and provisioning.

**3.2.4 virtualized network**: In this Recommendation, a network that makes use of virtualization technologies. It enables the abstraction of network resources such as creation of logically isolated virtual networks over a single physical network, and aggregation of multiple network resources as a single network resource.

**3.2.5 virtualized network function**: In this Recommendation, a network function whose functional software is decoupled from hardware, and runs on virtual machine(s).

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

IdM Identity Management

IoT Internet of Things

NGN Next Generation Network

NICE Network Intelligence Capability Enhancement

OAM Operation, Administration and Maintenance

QoS Quality of Service

RACF Resource and Admission Control Functions

S-NICE Software-defined NICE

SDN Software-defined Networking

SUP Service User Profile

## 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.

## 6 Requirements of software-defined NICE

### 6.1 Introduction to S-NICE

Software-defined NICE (S-NICE) is a specific implementation of NICE [ITU-T Y.2301] making use of software-defined networking (SDN) concept and technologies. NICE is an evolved version of NGN. S-NICE supports the intelligent features (five major features) of NICE and is enhanced by taking advantage of SDN concept and technologies. Some capabilities of NICE are considered in S-NICE with different implementation approaches and enhancements.

In S-NICE, the capabilities of NICE such as the service control capability, the policy control capability, and the traffic scheduling capability, can be redesigned and deployed based on SDN concept and technologies.

Major features supported by SDN technologies include the decoupling of control and data planes, the logical centralization of network intelligence and status, and the abstraction of the underlying network infrastructure for the applications. S-NICE adopts the major features of SDN technologies to provide highly scalable and flexible control as well as programmable and automatic interaction between network and applications.

In S-NICE, except for the content and context analysis capability, the transport control layer capabilities are centralized as controller capabilities (the so-called S-NICE controller capabilities), which maintain a global view of the underlying S-NICE infrastructure. As a result, the S-NICE infrastructure appears to the S-NICE controller capabilities as abstracted logical networks.

In S-NICE, the transport layer capabilities are regarded as infrastructure capabilities (the so-called S-NICE infrastructure capabilities), which no longer need to understand and process various protocol standards as in traditional NGNs or NICEs but merely accept instructions from the centralized S-NICE controller capabilities.

S-NICE also uses SDN related protocols to identify network traffic based on pre-defined match rules that can be statically or dynamically programmed by the S-NICE controller capabilities. Since SDN technologies allow the control elements of a network to be programmed, S-NICE provides extremely small granular control of the network to enable the network response to real-time changes for applications and users.

Appendix I provides a summary of both NICE and S-NICE capabilities and shows their differences.

### 6.2 Requirements of service control

In NICE, the service control capability is required to receive and transfer the application requests concerning policy control and traffic scheduling to the transport layer or to receive and transfer transport related information to the service layer. In addition, the service control capability is also required to provide resource control, registration, authentication, and authorization capabilities at the service level.

In S-NICE, the service control capability is one of the S-NICE orchestration capabilities, and it is required to support "on demand" configuration in order to provide "dynamic" resource control, registration, authentication, and authorization capabilities at the service level, upon request of applications. For example, if a user asks for high quality of service (QoS) level during an ongoing service session of an application when the user feels unsatisfied of the delivered QoS, then the service control capability of S-NICE selects the appropriate S-NICE controller capabilities to adjust the network resources in order to fulfil the user's requirement immediately.

### 6.3 Requirements of open environment

In NICE, the open environment capability supports the invocation by developers and applications of NICE capabilities, such as the policy control capability and the traffic scheduling capability, via standard application programming interfaces (APIs).

In S-NICE, the open environment capability is one of the S-NICE orchestration capabilities, and it is required to enable developers and applications to take full advantage of the S-NICE controller capabilities, such as virtualized network information abstraction, S-NICE controller(s) selection, and status monitoring. It is also required to support openness of content and context analysis information to developers and applications. Moreover, it is required to provide APIs to developers and applications for openness of S-NICE controller capabilities.

### 6.4 Requirements of content and context analysis

In NICE, the content and context analysis capability receives the awareness related information from the content and context detection capability and deeply analyses this information. The content and context analysis capability supports processing and storage of content and context information and distributes user traffic analysis results and network status analysis results to the requestor of content and context information, such as the policy control capability and the traffic scheduling capability. Moreover, the interaction between the NICE content and context detection capability and the NICE content and context analysis capability is based on management configuration.

In S-NICE, the content and context analysis capability is required to provide user traffic analysis results and network status analysis results to the S-NICE controller capabilities and the S-NICE orchestration capabilities. The analysis results include not only user traffic, users' service preferences and network status, but also abstracted information of physical and logical transport networks. Based

on the analysis results, the S-NICE controller capabilities and the S-NICE orchestration capabilities configure, manage, secure, and optimize the network resources.

In S-NICE, the transfer of all the detected information from the content and context detection capability to the content and context analysis capability, and the transfer of detection rules from the content and context analysis capability to the content and context detection capability are required to support SDN related protocols.

### 6.5 Requirements of policy control

In NICE, the policy control capability receives analysis results regarding user, traffic, and network information from the content and context analysis capability while it also receives the application's bandwidth and QoS assignment requirements from the service control capability and the service user profile (SUP) capability. The policy control capability makes policy information decisions and updates, and then sends the results of these policy decisions and updates to the policy enforcement capability. The policy control capability also makes decisions regarding network resource and admission control, supports unified policy database and consistent policies definitions, and supports a variety of access and core networks within a general resource control framework.

In NICE, the policy enforcement capability is based on pre-defined rules and receives policy control requirements from the policy control capability.

In S-NICE, the policy control capability is one of the S-NICE controller capabilities. The control policies are not only concerning access control, bandwidth management, and QoS level, but also security, reliability, energy usage, network monitoring and statistics, etc. The policy control capability is also required to support additional service layer APIs in order to allow on-demand resource allocation and self-service provisioning to application providers and users. The policy control capability is enhanced in S-NICE, so that the policy decisions transferred to the policy enforcement capability of S-NICE are straightforward instructions.

In S-NICE, the policy enforcement capability no longer needs to understand and process various protocol standards as in traditional NGNs or NICEs, but merely accepts instructions from the policy control capability of S-NICE and performs actions such as packet forwarding and packet dropping. The transfer of the policy control decisions between the policy control capability and the policy enforcement capability is required to support SDN related protocols.

### 6.6 Requirements of traffic scheduling

In NICE, the traffic scheduling capability receives the application's traffic delivery requirements from the service control capability and analysis results from the content and context analysis capability. Then, it establishes traffic scheduling rules based on these results. The traffic scheduling capability of NICE includes route and delivery node selection or adjustment based on traffic localization, network status, etc.

In NICE, the traffic scheduling enforcement capability is based on pre-defined rules, and receives traffic scheduling rules from the traffic scheduling capability.

In S-NICE, the traffic scheduling capability is one of the S-NICE controller capabilities. It includes traffic engineering based on multicast routing optimization, processor and storage optimization, etc. The traffic scheduling capability is also required to support additional service layer APIs to allow on-demand resource allocation and self-service provisioning to application providers and users. The traffic scheduling capability is enhanced in S-NICE, so that the traffic scheduling rules transferred to the traffic scheduling enforcement capability of S-NICE are straightforward instructions.

In S-NICE, the traffic scheduling enforcement capability no longer needs to understand and process various protocol standards as in traditional NGNs or NICEs, but merely accepts instructions from the traffic scheduling capability of S-NICE and performs actions such as input and output port selection and route selection. The transfer of the traffic scheduling rules between the traffic scheduling

capability and the traffic scheduling enforcement capability is required to support SDN related protocols.

### 6.7 Requirements of access and core transport

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

The access and core transport capabilities requirements of S-NICE are aligned with the requirements of NICE [ITU-T Y.2301], and have some enhancements. In S-NICE, the access and core transport capabilities are part of the S-NICE infrastructure capabilities, and they are required to perform the decisions made by the S-NICE controller capabilities. In addition, the access and core transport capabilities are required to support SDN related protocols.

### 6.8 Requirements for support of virtualized network and virtualized network functions

S-NICE is required to support virtualized network and virtualized network functions, which decouple network function software from hardware, in order to provide various capabilities including fast network function deployment, abstraction of transport, computing and storage resources, dynamic virtual and physical resource management, automatic fault detection and recovery, and on-demand system scalability.

S-NICE is required to support the coexistence of virtualized network functions and non-virtualized network functions by virtualizing some network functions while still having some other non-virtualized functions in the same network. S-NICE is also required to support the coexistence of a virtualized network and a non-virtualized network by deploying a new complete virtualized network which can be used for specific services and devices (e.g., Internet of Things (IoT) applications and devices) or for traffic exceeding the capacity of the non-virtualized network while still having the non-virtualized one.

## 7 The capability framework for software-defined NICE

### 7.1 Overview of the capability framework

S-NICE capabilities are aligned with, and enhance, the NICE capabilities as described in [ITU-T Y.2301].

Making use of SDN concept and technologies, the S-NICE capability framework differs from the NICE capability framework. Figure 1 provides the capability framework overview of S-NICE.

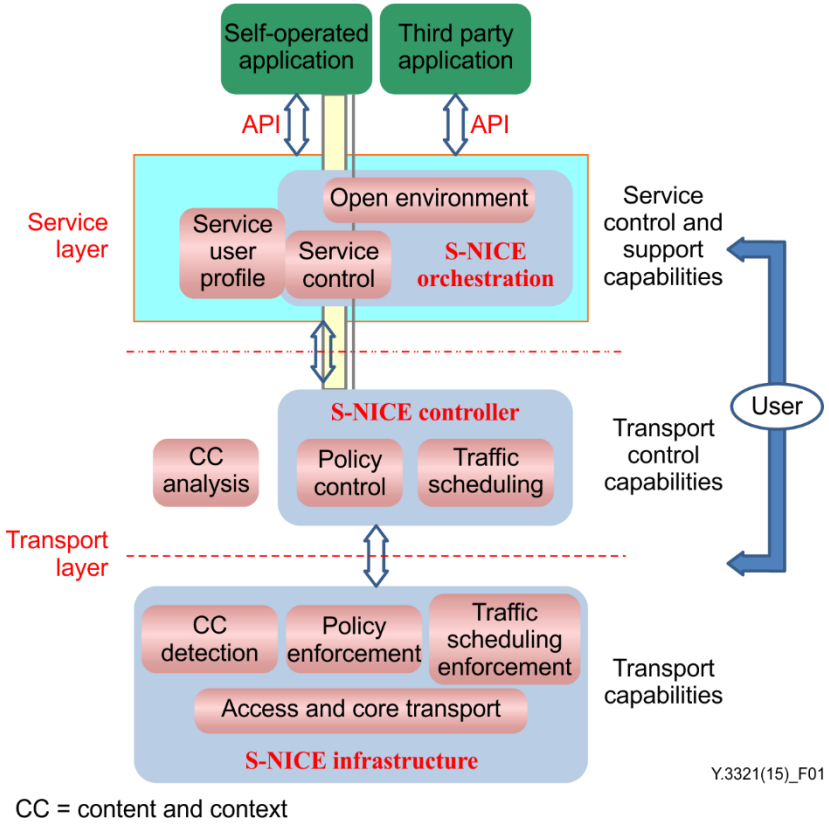


**Figure 1 – Capability framework overview of S-NICE**

At the service layer, the S-NICE orchestration capabilities consist of the service control capability and the open environment capability, and interact with the SUP capability.

The transport layer has S-NICE controller capabilities (named "S-NICE controller", for brevity, in Figure 1), which consist of the policy control capability and the traffic scheduling capability of S-NICE. The transport layer also has S-NICE infrastructure capabilities which support the access and core transport capability with the requirements to support SDN related protocols. Meanwhile, the S-NICE infrastructure capabilities support the content and context detection capability, the policy enforcement capability, and the traffic scheduling enforcement capability of S-NICE.

Although the separation of network control and transport applies in both NICE and S-NICE, S-NICE extends this concept further by taking advantage of SDN technologies. The interaction mechanisms and interfaces of S-NICE are different from those of NICE. In S-NICE, the interfaces between applications and the S-NICE orchestration capabilities, the interfaces between S-NICE controller capabilities and the S-NICE infrastructure capabilities, and the interfaces between the S-NICE orchestration capabilities and the S-NICE controller capabilities are required to use SDN related protocols while in NICE this usage is not required.

## 7.2 The S-NICE orchestration capabilities at the service layer

In NICE, the NICE provider interconnects with third-party applications as well as self-operated applications via the open environment capability and the service control capability.

In S-NICE, the open environment capability and the service control capability of NICE are both provided by the S-NICE orchestration capabilities. In addition, the S-NICE orchestration capabilities are required to provide interfaces to the S-NICE controller capabilities which are located in the transport control layer.

The S-NICE orchestration capabilities are required to connect with all the S-NICE controllers and offer access to all the controllers' capabilities for third-party and self-operated applications.

NOTE – The notion of S-NICE controller will be introduced in clause 7.3.

The S-NICE orchestration capabilities also allow applications to not have to deal with each S-NICE controller one by one, they can be aware of and access the capabilities of all S-NICE controllers. Moreover, the orchestration capabilities are required to monitor the network and notify the applications when applicable.

The orchestration capabilities are required to support, but are not limited to, the following features:

- access to open environment for applications including content and context analysis openness, policy control openness, and traffic engineering openness;
- virtualized network information provision to applications, such as provision of virtual network topology, route path setting and delivery node selection [ITU-T Y.2301];
- monitoring of S-NICE controllers' status;
- selection of the S-NICE controller capabilities;
- service creation and provisioning based on applications' requirements;
- orchestration of the S-NICE controller capabilities based on applications' requirements;
- orchestration of the S-NICE controller capabilities based on virtualized network and physical network status;
- conflict management and negotiation to maintain policy consistency among different capabilities of a S-NICE controller, among different S-NICE controllers, and between S- NICE controller capabilities and S-NICE infrastructure capabilities.

### 7.3 The S-NICE controller capabilities at the transport layer

The S-NICE controller capabilities are required to provide the transport control capabilities such as the policy control capability and the traffic scheduling capability. Because the policy control capability and the traffic scheduling capability are enhanced in S-NICE so that the policy decisions and the traffic scheduling rules transferred to the S-NICE infrastructure capabilities are straightforward instructions, the S-NICE infrastructure capabilities no longer need to understand and process various protocol standards as in traditional NGNs or NICEs, but merely accept instructions from the centralized S-NICE controller capabilities.

NOTE 1 – From an implementation point of view, the policy control capability and the traffic scheduling capability of S-NICE are implemented within a single S-NICE controller, and because of the limitation of geographical reasons and processing capabilities, multiple S-NICE controllers may be required to control different network regions.

The S-NICE controller capabilities are required to connect with the S-NICE orchestration capabilities and the S-NICE infrastructure capabilities by using SDN related protocols. The S-NICE controller capabilities are required to control the S-NICE infrastructure capabilities in order to meet the applications' requirements.

The S-NICE controller capabilities are required to support, but are not limited to, the following features:

- connection with the S-NICE orchestration capabilities and with the S-NICE infrastructure capabilities;
- policy control and network resource management based on infrastructure information;

NOTE 2 – The S-NICE controller capabilities can obtain information from network links and nodes to compute network topology information. The S-NICE controller capabilities can also obtain resource usage information and statistics from the network management system and the content and context analysis capability;

- policy control based on application requirements provided by the S-NICE orchestration capabilities, information from network resource management, and analysis results from the content and context analysis capability;

- traffic scheduling based on information provided by network resource management, application requirements provided by the S-NICE orchestration capabilities, and analysis results from the content and context analysis capability;
- receiving results of content and context analysis of infrastructure and applications, and performing policy control and traffic scheduling based on these results. The S-NICE controller capabilities are required to be aware of physical and virtual network topology, traffic flows and information of the infrastructure;
- cooperation with the network management system to provide operation, administration and maintenance (OAM) and alarm information;

NOTE 3 – The S-NICE controller capabilities can provide additional support for the provisioning of OAM and alarm information, however functional overlapping between S-NICE controller capabilities and the network management system needs to be avoided.

- cooperation between physical network and virtualized network;
- connection with other S-NICE controller capabilities;
- monitoring of physical network and virtualized network.

### 7.4 The S-NICE infrastructure capabilities at the transport layer

The S-NICE infrastructure capabilities implement the actions decided by the S-NICE controller capabilities. The S-NICE infrastructure capabilities include the policy enforcement capability, the traffic scheduling enforcement capability, the content and context detection capability, and the access and core transport capability of S-NICE.

The S-NICE infrastructure capabilities are required to support, but are not limited to, the following features:

- communication with the S-NICE controller capabilities;
- provision of the infrastructure information (e.g., network topology information, flow information, service routing information) to the relevant S-NICE controller capabilities based on requests;

NOTE 1 – Different S-NICE controller capabilities may request different infrastructure information.

- forwarding of traffic on a per flow basis;
- forwarding of traffic while maintaining policy consistency among the S-NICE controller capabilities, the S-NICE infrastructure capabilities and the applications;
- isolation and virtualization of different parts of the network;

NOTE 2 – For example, many access transport networks can be isolated from each other and virtualized as one network.

- reception of policy decisions from the S-NICE controller capabilities and enforcement of these policy decisions (e.g., by packet forwarding and processing);
- reception of traffic scheduling rules from the S-NICE controller capabilities and enforcement of these traffic scheduling rules (e.g., by transport node selection and path selection).

## 8 Security considerations

The security requirements of S-NICE are aligned with the security requirements of NICE [ITU-T Y.2301] with the following additional requirements:

- enhanced security of the SDN controller(s) which incorporates the transport control capabilities, because the logically centralized controller could be a single point of failure, or a target of malicious attacks;

- secure mechanisms to authorize network configurations and operations such as routing path establishment or virtualized network function deployment, upon demand by services or applications;
- mechanisms to provide network isolation for both virtualized and physical network resources, in order to protect the network from malware attacks, even when some components of the network have already been affected;
- appropriate mechanisms to monitor abnormal situations, to detect and defend from attacks and to recover network components and their states for virtualized network and virtualized network functions.

# Appendix I

## Differences between NICE capabilities and S-NICE capabilities

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

The following table shows the differences between NICE capabilities and S-NICE capabilities.

NOTE – The capabilities listed in Table I.1 are respectively derived from [ITU-T Y.2301] and this Recommendation.

**Table I.1 – Differences between NICE capabilities and S-NICE capabilities**

| Capabilities group | | NICE capabilities | S-NICE capabilities |
|---|---|---|---|
| Service layer capabilities | SUP | The SUP capability of NICE is required to support:<br>• SUP-FE in NGN [ITU-T Y.2012];<br>• Identity Management (IdM) [ITU-T Y.2720]. | The SUP capability of S-NICE is aligned with that of NICE. |
| | Service control | The service control capability of NICE is required to support:<br>• Service Control Functions in NGN [ITU-T Y.2012];<br>• receiving and transferring information allowing the identification of application data for policy control and traffic scheduling;<br>• receiving and transferring information allowing the identification of applications and users;<br>• receiving and transferring transport layer events (e.g., notifications of QoS modifications) reported by the transport layer to the service layer. | The service control capability of S-NICE is aligned with that of NICE with support of the following additional requirements:<br>• "on demand" configuration in order to provide "dynamic" resource control, registration, authentication, and authorization. |
| | Open environment | The open environment capability of NICE is required to support:<br>• openness [ITU-T Y.2240];<br>• open access to a service creation environment [ITU-T Y.2240];<br>• self-operated applications' invocation of NICE capabilities. | The open environment capability of S-NICE is aligned with that of NICE with support of the following additional requirements:<br>• openness of content and context analysis information to developers and applications;<br>• openness of virtualized network information abstraction;<br>• openness of S-NICE controller(s) selection and status monitoring. |
| Transport control capabilities | Content and context analysis | The content and context analysis capability of NICE is required to support: | The content and context analysis capability of S-NICE is aligned with that |

**Table I.1 – Differences between NICE capabilities and S-NICE capabilities**

| Capabilities group | | NICE capabilities | S-NICE capabilities |
|---|---|---|---|
| | | • context awareness requirements of NGN (clause 7.3 of [ITU-T Y.2201]);<br>• providing user traffic analysis results;<br>• providing information related to user's application data;<br>• providing network status analysis results. | of NICE with support of the following additional requirements:<br>• providing user traffic analysis results and network status analysis results to the S-NICE controller capabilities and the S-NICE orchestration capabilities;<br>• providing additional analysis results, including abstracted information of physical and logical transport layer networks;<br>• support of SDN related protocols. |
| | Policy control | The policy control capability of NICE is required to support:<br>• functional requirements of RACF [ITU-T Y.2111];<br>• intelligent assignment of bandwidth and QoS level according to:<br>– on-demand requirements from users via a user self-service portal;<br>– requirements from a third-party application provider or, possibly, NICE provider via open environment capabilities;<br>– the content and context analysis results. | The policy control capability of S-NICE is aligned with that of NICE with support of the following additional requirements:<br>• providing control policies concerning security, reliability, energy usage, network monitoring and statistics, etc.;<br>• translating policy decisions into straightforward instructions and transferring these instructions to the policy enforcement capability of S-NICE;<br>• support of SDN related protocols. |
| | Traffic scheduling | The traffic scheduling capability of NICE is required to align with the requirements of NGN [ITU-T Y.2201] with support of the following additional requirements in terms of generation of traffic scheduling rules:<br>• traffic localization;<br>• selection of the traffic delivery network node;<br>• network status;<br>• intelligent routing based on route selection policy;<br>• network virtualization. | The traffic scheduling capability of S-NICE is aligned with that of NICE with support of the following additional requirements:<br>• traffic engineering based on multicast routing optimization, processor and storage optimization, etc.;<br>• translating traffic scheduling rules into straightforward instructions and transferring these instructions to the traffic scheduling enforcement capability of S-NICE;<br>• support of SDN related protocols. |
| Transport capabilities | Content and context detection | The content and context detection capability of NICE is required to extract the following transport-related information:<br>• user location information; | The content and context detection capability of S-NICE is aligned with that of NICE with support of the following additional requirements: |

**Table I.1 – Differences between NICE capabilities and S-NICE capabilities**

| Capabilities group | | NICE capabilities | S-NICE capabilities |
|---|---|---|---|
| | | • user application data information;<br>• application data statistics;<br>• user terminal parameters;<br>• network resource information;<br>• access network related information. | • detecting abstracted information of physical and logical transport layer networks;<br>• support of SDN related protocols. |
| | Policy enforcement | The policy enforcement capability of NICE is required to support:<br>• policy enforcement requirements in [ITU-T Y.2111];<br>• enforcement of on-demand bandwidth and QoS levels in order to satisfy on-demand requirements from users and application providers;<br>• enforcement of bandwidth and QoS levels based on content and context analysis results. | The policy enforcement capability of S-NICE is aligned with that of NICE with support of the following additional requirements:<br>• accepting instructions from the policy control capability of S-NICE and performing actions such as packet forwarding and packet dropping;<br>• support of SDN related protocols. |
| | Traffic scheduling enforcement | The traffic scheduling enforcement capability of NICE is required to support:<br>• enforcement of traffic scheduling based on traffic localization schemes;<br>• enforcement of traffic scheduling based on optimal selection of delivery nodes;<br>• enforcement of traffic scheduling based on intelligent route selection and adjustment based on routing policies;<br>• enforcement of traffic scheduling based on resource allocation using network virtualization. | The traffic scheduling enforcement capability of S-NICE is aligned with that of NICE with support of the following additional requirements:<br>• accepting instructions from the traffic scheduling capability of S-NICE and performing actions such as input and output port selection as well as route selection;<br>• support of SDN related protocols. |

**Table I.1 – Differences between NICE capabilities and S-NICE capabilities**

| Capabilities group | | NICE capabilities | S-NICE capabilities |
|---|---|---|---|
| | Access and core transport capabilities | The access and core transport capabilities of NICE are required to align with the transport requirements of NGN [ITU-T Y.2012], with support of the additional following optional requirement:<br>• cache and media stream delivery functions in transport nodes. | The access and core transport capabilities of S-NICE are aligned with that of NICE with support of the following additional requirements:<br>• support of SDN related protocols. |

# Bibliography


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

[b-ITU-T H.780] Recommendation ITU-T H.780 (2012), *Digital signage: Service requirements and IPTV-based architecture*.

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

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*.

[b-ITU-T Y.2111] Recommendation ITU-T Y.2111 (2011), *Resource and admission control functions in next generation networks*.

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

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

[b-ITU-T Y.2302] Recommendation ITU-T Y.2302 (2014), *Network intelligence capability enhancement – Functional architecture*.

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

[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*.

[b-ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*.

## 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 | Environment and ICTs, climate change, e-waste, energy efficiency; 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, 2015