International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3322

(09/2016)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Future networks

Functional architecture for NICE implementation making use of software-defined networking technologies

Recommendation ITU-T Y.3322

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

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
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.3322

Functional architecture for NICE implementation making use of software-defined networking technologies

Summary

Recommendation ITU-T Y.3322 specifies the architecture and implementations of software-defined network intelligence capability enhancement (S-NICE). S-NICE is a specific implementation of network intelligence capability enhancement (NICE) making use of software-defined networking (SDN) concepts and technologies. This Recommendation defines the functional architecture of S-NICE, describes the enhancement functions based on NICE, the reference points among different functions and some typical implementation flows.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3322	2016-09-29	13	11.1002/1000/13018

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

Recommendation ITU-T Y.3322

Functional architecture for NICE implementation making use of software-defined networking technologies

1 Scope

This Recommendation provides the functional architecture of software-defined network intelligence capability enhancement (S-NICE), S-NICE is a specific implementation of network intelligence capability enhancement (NICE) [ITU-T Y.2301] making use of software-defined networking (SDN) technologies. This Recommendation defines the functional architecture of NICE implementation making use of SDN technologies, describes the enhancement functions based on NICE, the reference points among different functions and some typical implementation flows.

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*.

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

[ITU-T Y.3321] Recommendation ITU-T Y.3321 (2015), *Requirements and capability framework for NICE implementation making use of software-defined networking technologies*.

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

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

3.1.3 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.

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

3.1.5 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.

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

3.1.7 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.

3.1.8 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.

3.1.9 virtualized network [ITU-T Y.3321]: 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 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

CPE Customer Premises Equipment

FE Functional Entity

NGN Next Generation Network

NICE Network Intelligence Capability Enhancement

QoS Quality of Service

SDN Software-defined Networking

S-NICE Software-defined NICE

5 Conventions

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

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

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

In the body of this Recommendation and its annexes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited

from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Overview for S-NICE

S-NICE is a specific implementation of NICE making use of software-defined networking (SDN) technologies. In S-NICE, the functional entities such as service control functional entity (FE), content and context analysis FE, policy control FE, traffic scheduling FE need to be redesigned and implemented based on the SDN technologies.

S-NICE supports the major functions of SDN technologies including 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. By adopting SDN technologies, highly scalable and flexible control as well as programmable and automatic interaction between network and applications can be supported in S-NICE.

In S-NICE, the control plane functions are centralized in the S-NICE controller, which maintains a global view of the data plane including network status and traffic information. As a result, the data plane appears to the S-NICE controller as an abstracted logical network/resource. Meanwhile, the functional entities in data plane only need to accept and execute the instructions from the centralized S-NICE controller.

7 Functional architecture for S-NICE

7.1 Overall functional architecture of S-NICE

7.1.1 Relationship between architectures of NICE and S-NICE

Figure 7-1 shows the relationship between NICE architecture and S-NICE architecture.

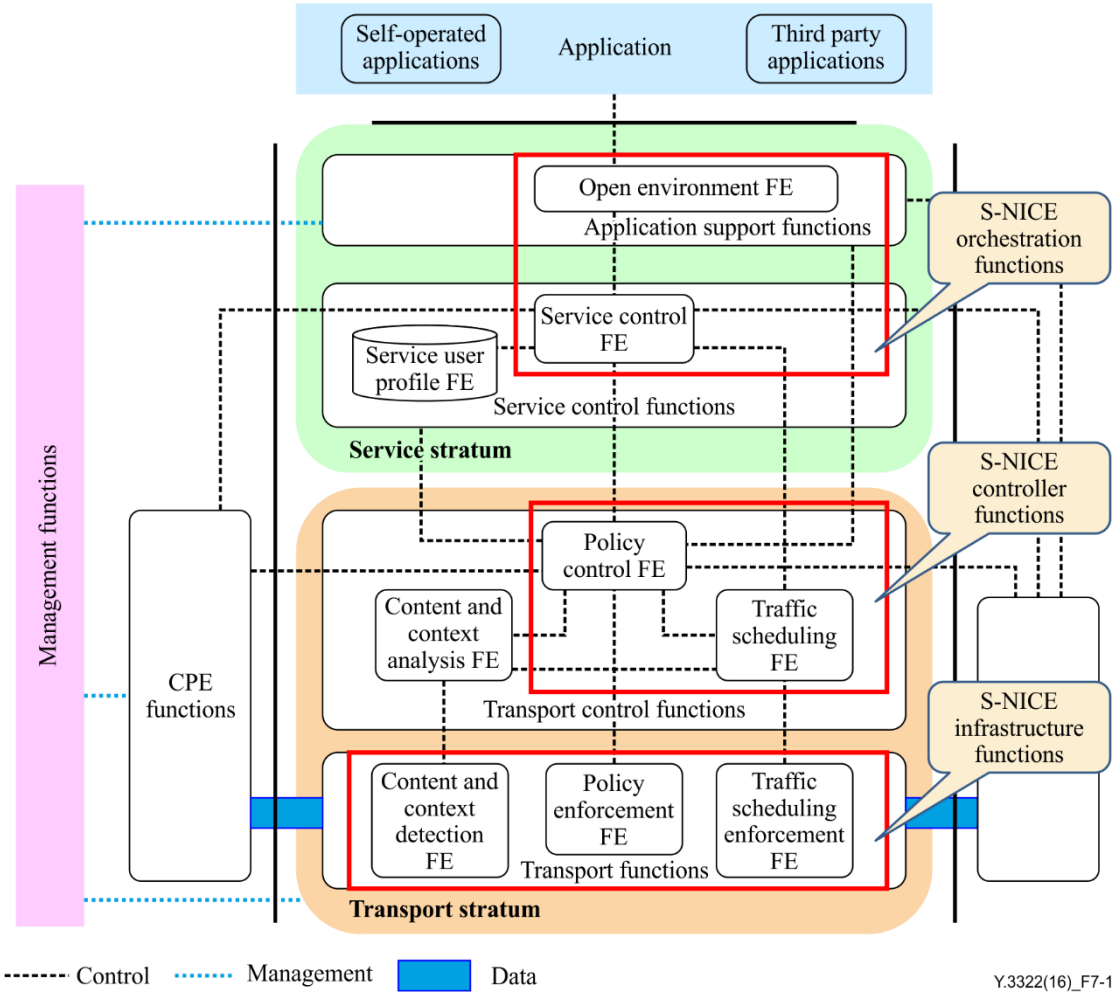

Figure 7-1 – Relationship between architectures of NICE and S-NICE

In S-NICE architecture, there are three main functions: S-NICE orchestration functions, S-NICE controller functions and S-NICE infrastructure functions.

In service stratum, S-NICE orchestration functions include the open environment FE, the service control FE of NICE architecture, and have some enhancements by taking advantage of SDN concept and technologies to provide "dynamic" resource control, registration, authentication and authorization functions at the service level, upon the request of applications.

In transport stratum, S-NICE controller functions include the policy control FE, the traffic scheduling FE of NICE architecture, and have some enhancements by taking advantage of SDN concept and technologies to provide the capabilities (such as network topology collection and management, virtualized network information abstraction) and translate these policies and rules into straightforward instructions.

S-NICE infrastructure functions include of the content and context detection FE, the policy enforcement FE, the traffic scheduling enforcement FE of NICE architecture, and have some enhancements by taking advantage of SDN concept and technologies that accept the straightforward instructions from S-NICE controller functions and perform these actions accordingly.

7.1.2 Overall functional architecture of S-NICE

Figure 7-2 shows the overall functional architecture of S-NICE.

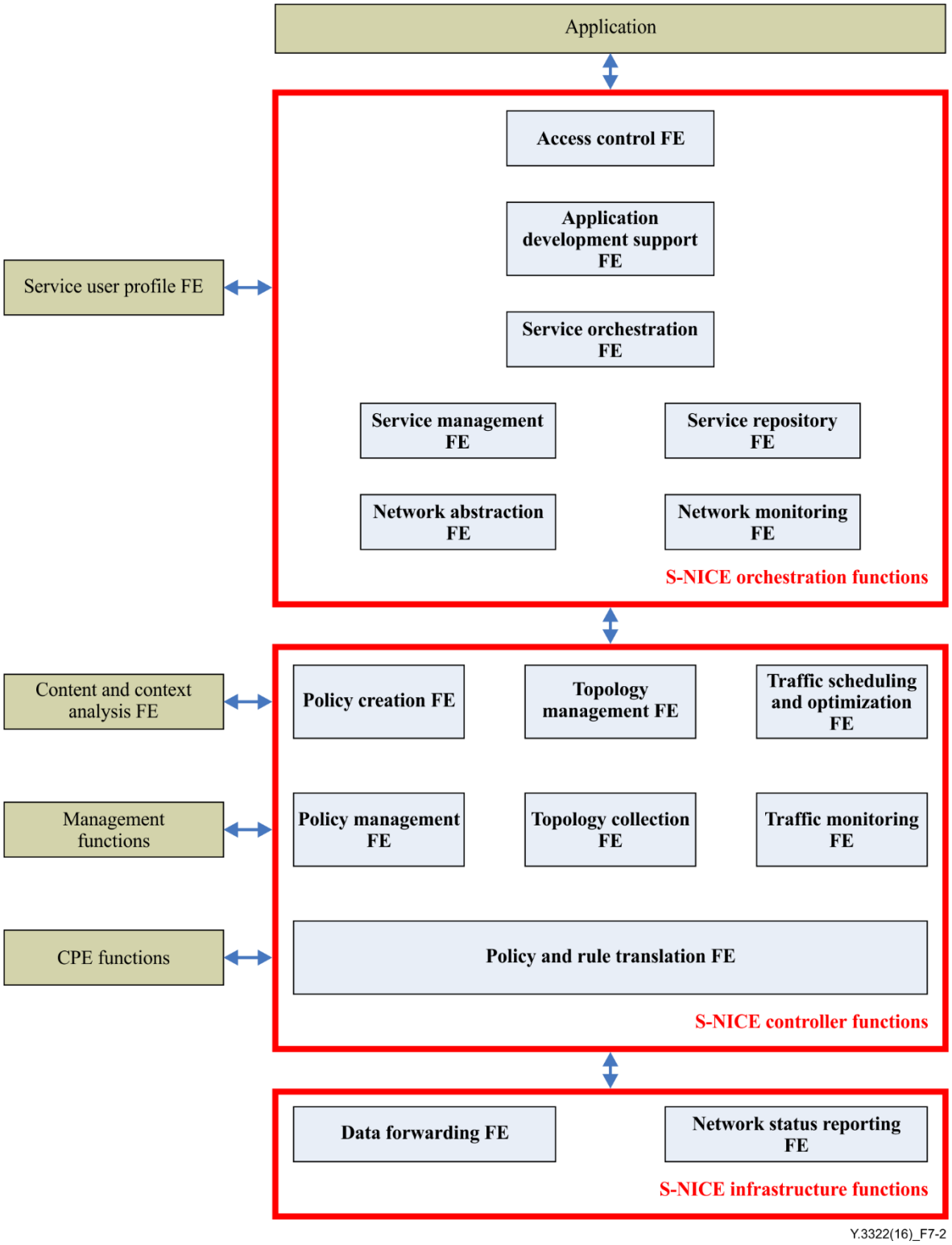

Figure 7-2 – Overall functional architecture of S-NICE

S-NICE connects with the service user profile FE, the content and context analysis FE, the management functions, the customer premises equipment (CPE) functions, the application to collect the network/routing/user information and receive service requests from the application.

It includes three main functions:

1) S-NICE orchestration functions;

2) S-NICE controller functions;

3) S-NICE infrastructure functions.

Following is the detailed description for each function.

7.2 Detailed functional architectures of S-NICE orchestration functions

Figure 7-3 shows the detailed functional architecture of S-NICE orchestration functions.

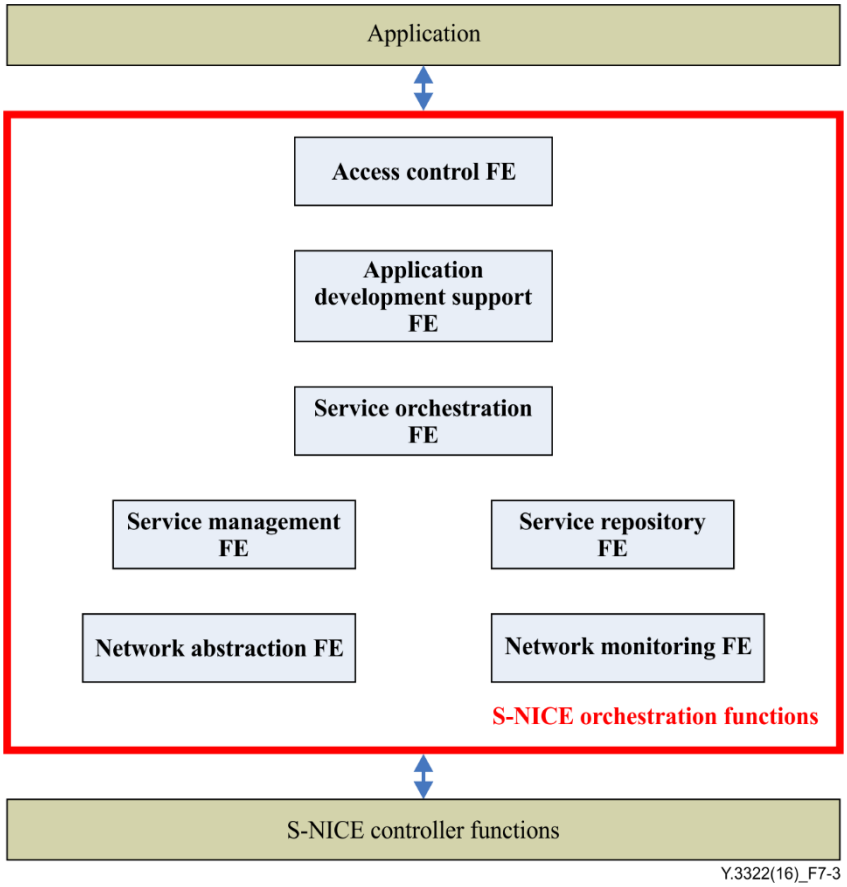

Figure 7-3 – Detailed functional architectures of S-NICE orchestration functions

S-NICE orchestration functions consist of the following functional entities:

– Access control FE;
– Application development support FE;
– Service orchestration FE;
– Service management FE;
– Service repository FE;
– Network abstraction FE;
– Network monitoring FE.

In general, S-NICE orchestration functions provide open environment to the third party applications and self-operated applications and support "on demand" configuration in order to provide "dynamic" resource control, registration, authentication and authorization capabilities at the service level upon the request of applications.

S-NICE orchestration functions connect with S-NICE controller functions, which may include multiple S-NICE controllers, and provide the capabilities (such as route selection, network monitoring) to the third party and self-operated applications. Moreover, S-NICE orchestration functions monitor the whole network status and notify the applications if applicable.

S-NICE orchestration functions provide information provision to applications, such as provision of network topology, route path setting and delivery node selection.

S-NICE orchestration functions also provide conflict management and negotiation mechanism to maintain policy consistency among different S-NICE controllers.

7.2.1 Access control FE

The access control FE provides the functions including application programming interface (API) translation, authentication and authorization, request and response relaying.

1) API translation

The access control FE parses the requests as received from different applications to perform different actions include request authentication, authorization and resource invoking.

2) Authentication and authorization

The access control FE interacts with other functional entities (such as the service user profile FE) to achieve end-user, application and service related identity information for authentication and authorization.

The request is authenticated to identify the application identity securely and further authorized (e.g., the request needs to consume protected resource controlled by the resource provider which has the right of granting application to access the resource) according to the approval of the resource provider and service level agreements (SLAs).

3) Request and response relaying

The access control FE forwards the request and response between applications and target resource.

7.2.2 Service management FE

The service management FE provides service discovery, service registration and service governance functionalities, the service management FE also maintains a catalogue of the registered service interacting with the service repository FE.

The service management FE processes the service registration request from service providers. The service information is stored in service catalogue. When one service needs to be registered or unregistered, the service management FE adds or removes subscription of the service from the local catalogue as well as notifies the service repository FE accordingly.

During service registration process, the service management FE sends service interface description and service routing related information to the service repository FE, which stores the information for further application development purpose.

The registered services are orchestrated by the service orchestration FE before providing them to the users and applications.

The service management FE supports to utilize the abstracted network resource of the underlying physical or virtualized infrastructure to perform service creation.

7.2.3 Service orchestration FE

The service orchestration FE receives requests from users and applications through the access control FE, and orchestrates the services to provide "dynamic" resource control upon the requests of users and applications.

The service orchestration FE generates a composited service logic that combines existing services. The composited service logic describes interactions among multiple services by exchanging messages, branching logics, and invocation sequences.

The service orchestration FE generates a set of requests according to the requirements of the users and applications, and sends these requests to the service management FE.

For example, one user asks for a bandwidth guaranteed connection for a specific application. First, the service orchestration FE translates this requirement into two requests accordingly. Then the service orchestration FE initials a request to establish a dedicate tunnel from the user terminal to the end server and sends this request to the service management FE. After that, the service orchestration FE creates another request to configure the parameters of the established tunnel with guaranteed bandwidth and sends this request to the service management FE again.

7.2.4 Application development support FE

The application development support FE enables application developers to develop applications using services exposed by S-NICE.

Application developers can access this FE to develop applications using online and/or offline design tools. The design tools facilitate application development and provide functions such as drag and drop, automatic code generation, etc. When developing an application, the application development support FE interacts with the service orchestration FE to achieve the development interface information of the services used in the application.

Developers can also develop composite services by the application development support FE. Composite services are stored in the service orchestration FE to be accessible as a resource for other applications.

The application development support FE can include the developer community as an optional functionality which supports a developer forum to discuss and exchange developers' ideas, and supports collection and exposure of customer feedback and ratings about applications, ratings about services and tools, and provides self-service functions. Furthermore, the developer community provides an entrance for developers of S-NICE (e.g., supporting functions of developer registration). In addition, developers can download some development documents via it to assist their development.

7.2.5 Service repository FE

The service repository FE provides functionalities for the storage of registered services and related interfaces for invoking. Application developer uses services interface to create applications.

The service repository FE interacts with the service management FE to get the interface description information. The service repository FE also provides service version management mechanism to keep synchronization of service information registered at the service management FE.

When a service is registered to the resource registry, the service information related to application development such as service interface description information is stored in the service repository. The service can be invoked by the service orchestration FE and the application development support FE.

7.2.6 Network abstraction FE

The network abstraction FE abstracts and exploits the network and traffic information from the network monitoring FE with pre-defined rules, e.g., based on time, location, or access network.

Then the network abstraction FE provides the general view of network and traffic conditions and ways to invoke the network and traffic capabilities. The capabilities include network performance optimization, access network choosing, potential network issue identification, network change impaction, etc.

After abstraction, the capabilities can be registered to the service management FE as new services, with the new services, the service management FE supports to utilize the abstracted network resource of the underlying physical or virtualized infrastructure.

7.2.7 Network monitoring FE

The network monitoring FE gathers all the network related information from S-NICE controller functions and management functions, and provides the information to the network abstraction FE after summary.

The network information includes network type, network topology, network available bandwidth and utilization rate, busy hour and area of network, network alarm information, network historical data, etc.

The traffic information includes traffic localization scheme, traffic delivery network node selection, network load status (idle or overload), intelligent routing adjustment, virtualized network resource allocation.

7.3 Detailed functional architectures of S-NICE controller functions

Figure 7-4 shows the detailed functional architecture of S-NICE controller functions.

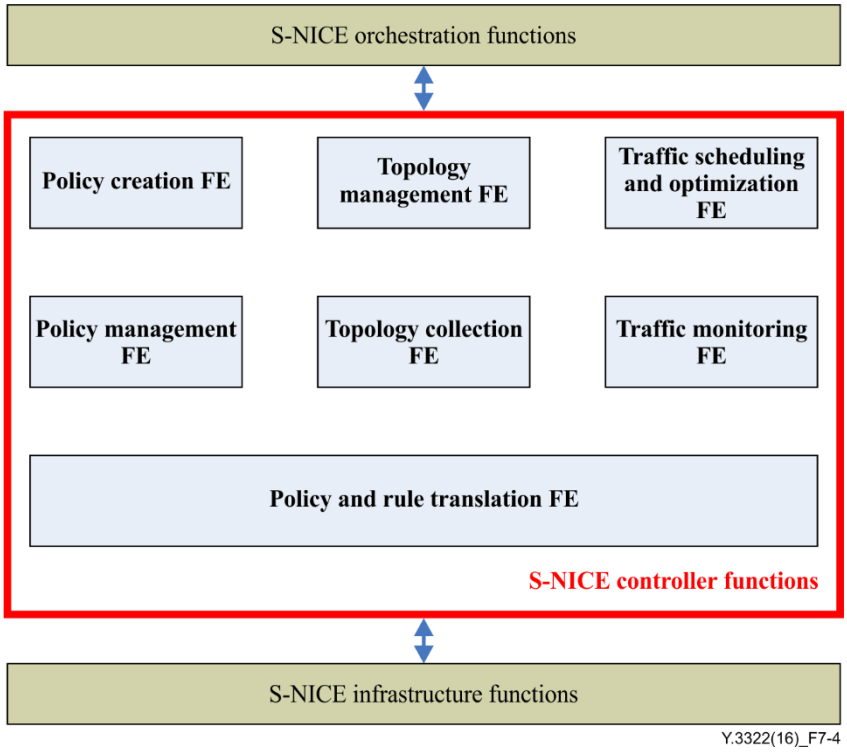

Figure 7-4 – Detailed functional architectures of S-NICE controller functions

S-NICE controller functions consist of the following functional entities:

– Policy creation FE;
– Policy management FE;
– Topology management FE;
– Topology collection FE;
– Traffic scheduling and optimization FE;
– Traffic monitoring FE;
– Policy and rule translation FE.

In general, S-NICE controller functions provide the policy control function and the traffic scheduling function of NICE. By using SDN concept and technologies, the policy decisions and the traffic scheduling rules transferred to S-NICE infrastructure functions are straight forward instructions.

S-NICE controller functions provide policy control and network resource management based on S-NICE infrastructure information.

S-NICE controller functions provide policy control function based on S-NICE infrastructure information, application requirements of S-NICE orchestration functions and analysis result from the content and context analysis FE.

S-NICE controller functions provide traffic scheduling function based on application requirements provided by S-NICE orchestration functions, and analysis results from the content and context analysis FE.

S-NICE controller functions can cooperate between physical networks and virtualized networks.

7.3.1 Policy creation FE

The policy creation FE receives service requests from S-NICE orchestration functions and topology information from the topology management FE. Based on the "dynamic" resource control requirements from users and applications, the content and context analysis results from the content and context analysis FE, and the topology and traffic information from the topology management FE, the policy creation FE creates a set of policy rules, and sends these policy rules to the policy management FE.

7.3.2 Policy management FE

The policy management FE provides policy registration, policy storage and policy governance functionalities, the policy management FE also maintains a catalogue of the registered policy rules interacting with the policy and rule translation FE.

The policy management FE processes the policy rules registration requests from the policy creation FE. When one policy rule needs to be registered or unregistered, the policy management FE adds or removes the policy rule from the local catalogue. Then the policy management FE sends registered policy rules in the local catalogue to the policy and rule translation FE for further processing.

7.3.3 Topology management FE

The topology management FE receives global topology information from the topology collection FE and provides maintenance functionality with the global topology. The topology management FE provides the global topology information to the traffic scheduling and optimization FE, and also obtains traffic optimization results (e.g., routing path selection) from the traffic scheduling and optimization FE.

By combining the global topology information and the traffic optimization results (e.g., routing path selection), the topology management FE provides a global topology with detailed traffic load information to the policy creation FE and the S-NICE orchestration functions.

7.3.4 Topology collection FE

The topology collection FE collects topology information from the policy and rule translation FE, and the topology collection FE processes all the topology information and generates the global topology information based on every network node's status and each link's status. The topology collection FE sends the global topology information to the topology management FE for further processing.

7.3.5 Traffic scheduling and optimization FE

The traffic scheduling and optimization FE receives global topology information from the topology management FE, and the real time traffic load information from the traffic monitoring FE. The traffic scheduling and optimization FE also receives service requests from S-NICE orchestration functions. By using all the information together, the traffic scheduling and optimization FE computes the

optimized routing path and traffic scheduling results, and provides the traffic optimization results to the topology management FE.

7.3.6 Traffic monitoring FE

The traffic monitoring FE monitors the real time traffic load information by receiving information from the policy and rule translation FE. The traffic monitoring FE sends all traffic load information to the traffic scheduling and optimization FE for further processing.

7.3.7 Policy and rule translation FE

The policy and rule translation FE connects directly with the S-NICE infrastructure functions, and receives real time traffic load information and topology information from the S-NICE infrastructure functions.

The policy and rule translation FE provides topology information to the topology collection FE, as well as real time traffic load information to the traffic monitoring FE. The policy and rule translation FE receives policy rules from the policy management FE and performs policy rules translation in order to decompose complex policy rules into straightforward instructions, and sends these instructions to the S-NICE infrastructure functions.

7.4 Detailed functional architectures of S-NICE infrastructure functions

Figure 7-5 shows the detailed functional architecture of S-NICE infrastructure functions.

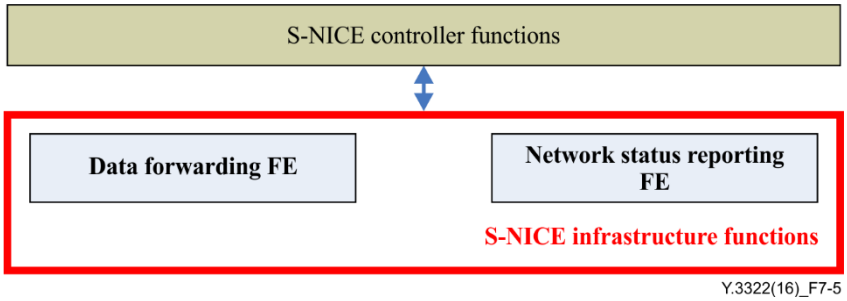

Figure 7-5 – Detailed functional architecture of S-NICE infrastructure functions

S-NICE infrastructure functions consist of the following functional entities:

– Data forwarding FE;

– Network status reporting FE.

In general, S-NICE infrastructure functions implement the actions decided by S-NICE controller functions. S-NICE infrastructure functions provide the capabilities such as forwarding, quality of service (QoS) adjustment and performance monitoring.

S-NICE infrastructure functions provide the infrastructure information (e.g., network topology information, flow information, service routing information) to the relevant S-NICE controller functions and the content and context analysis functions based on requests.

S-NICE infrastructure functions receive policy decisions from S-NICE controller functions and enforce these policy decisions (e.g., forwarding and processing packet).

S-NICE infrastructure functions receive traffic scheduling rules from S-NICE controller functions and enforce these traffic scheduling rules (e.g., transport node selection and path selection).

S-NICE infrastructure functions also support isolation and virtualization of different parts of the network.

7.4.1 Data forwarding FE

The data forwarding FE receives instructions from the policy and rule translation FE, and executes these instructions by forwarding and processing data. By adopting the technology of SDN, the data forwarding FE of S-NICE infrastructure functions no long needs to compute the route path but merely enforces instructions received from the S-NICE controller functions.

7.4.2 Network status reporting FE

The network status reporting FE receives requests from the S-NICE controller functions, and according to the requests it reports network information to the S-NICE controller functions including modifications of network nodes, resource utilization rate of each node, modifications of network links, physical or virtual capacity of each link, and the real time traffic load of each link, etc. The network status reporting FE is applicable for both physical networks and virtual networks.

8 Reference points of S-NICE

8.1 Internal reference points of S-NICE orchestration functions

Figure 8-1 and the following content provides the descriptions of the internal reference points of S-NICE orchestration functions:

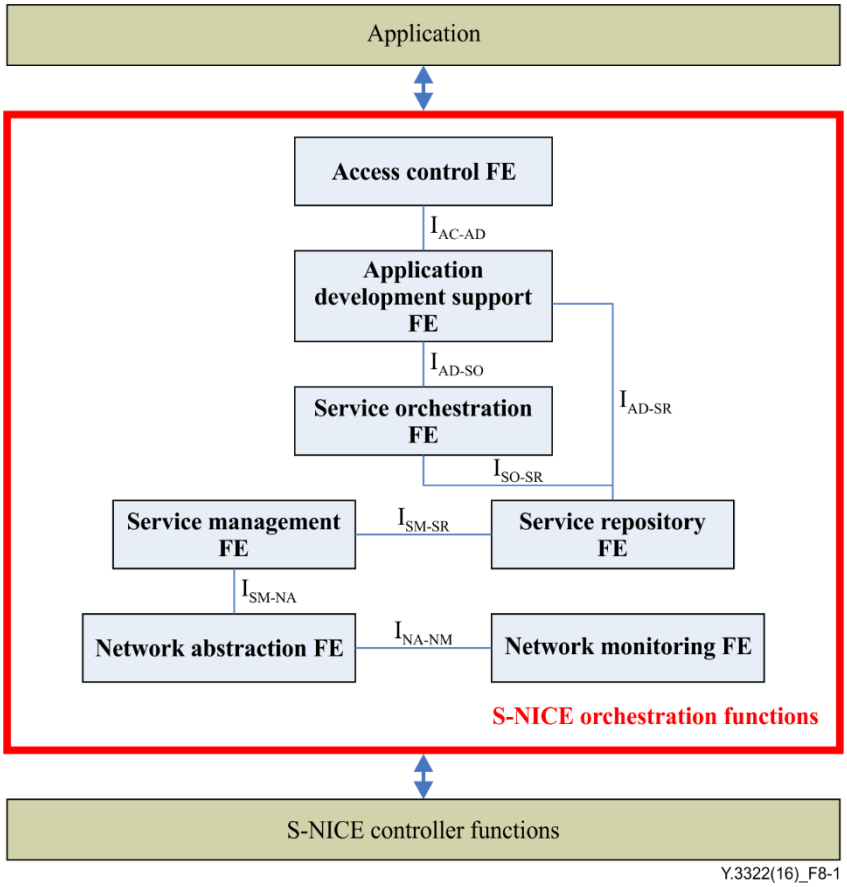

Figure 8-1 – Internal reference points of S-NICE orchestration functions

I_{AC-AD} the reference point between the access control FE and the application development support FE.

After authentication and authorization, the developers can access the development environment provided by S-NICE with this reference point.

I_{AD-SO} the reference point between the application development support FE and the service orchestration FE.

The application developer can store their application as resource in the service orchestration FE through this reference point, also can achieve the resource kept in the service orchestration FE for their own use.

I_{AD-SR} the reference point between the application development support FE and the service repository FE.

The application development support FE can achieve development interface information of the services through this reference point.

I_{SO-SR} the reference point between the service orchestration FE and the service repository FE.

The service orchestration FE can achieve development interface information of the services through this reference point for new service composting.

I_{SM-SR} the reference point between the service management FE and the service repository FE.

The service repository FE can achieve service description information from the service management FE through this reference point.

I_{SM-NA} the reference point between the service management FE and the network abstraction FE.

The service management FE supports to utilize the abstracted network resource of the underlying physical or virtualized infrastructure with this reference point.

I_{NA-NM} the reference point between the network abstraction FE and the network monitoring FE.

The network monitoring FE gathers all the network related information and provides the information to the network abstraction FE after summary with this reference point.

8.2 Internal reference points of S-NICE controller functions

Figure 8-2 and the following content provides the descriptions of the internal reference points of S-NICE controller functions:

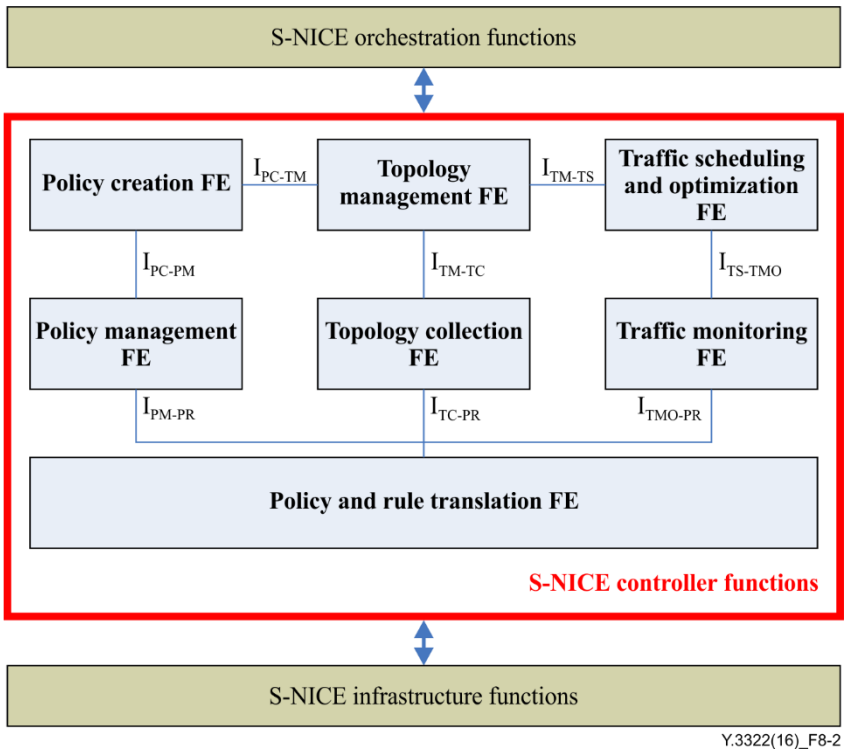

Figure 8-2 – Internal reference points of S-NICE controller functions

I_{PC-PM} the reference point between the policy creation FE and the policy management FE.

The policy creation FE sends the policy rules to the policy management FE with this reference point.

I_{PM-PR} the reference point between the policy management FE and the policy and rule translation FE.

The policy management FE sends registered policy rules in the local catalogue to the policy and rule translation FE for further processing with this reference point.

I_{PC-TM} the reference point between the policy creation FE and the topology management FE.

The policy creation FE receives topology information from the topology management FE with this reference point.

I_{TM-TC} the reference point between the topology management FE and the topology collection FE.

The topology collection FE sends the global topology information to the topology management FE for further processing with this reference point.

I_{TC-PR} the reference point between the topology collection FE and the policy and rule translation FE.

The topology collection FE collects topology information from the policy and rule translation FE with this reference point.

I_{TM-TS} the reference point between the topology management FE and the traffic scheduling and optimization FE.

With this reference point, the topology management FE provides the global topology information to the traffic scheduling and optimization FE, and obtains traffic optimization results from the traffic scheduling and optimization FE.

I_{TS-TMO} the reference point between the traffic scheduling and optimization FE and the traffic monitoring FE.

The traffic scheduling and optimization FE retrieves the real time traffic load information from the traffic monitoring FE with this reference point.

I_{TMO-PR} the reference point between the traffic monitoring FE and the policy and rule translation FE.

The traffic monitoring FE monitors the real time traffic load information by receiving information from the policy and rule translation FE with this reference point.

8.3 Internal reference points of S-NICE infrastructure functions

Figure 8-3 and the following content provides the descriptions of the internal reference points of S-NICE infrastructure functions:

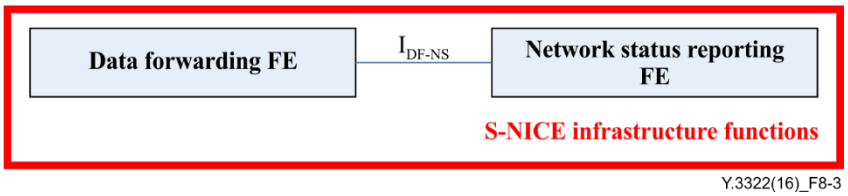

Figure 8-3 – Internal reference points of S-NICE infrastructure functions

I_{DF-NS} the reference point between the data forwarding FE and the network status reporting FE.

The network status reporting FE retrieves the traffic information (such as data processing information) from the data forwarding FE with this reference point.

8.4 Internal reference points among functions of S-NICE

Figure 8-4 and the following content provides the descriptions of the internal reference points among functions of S-NICE:

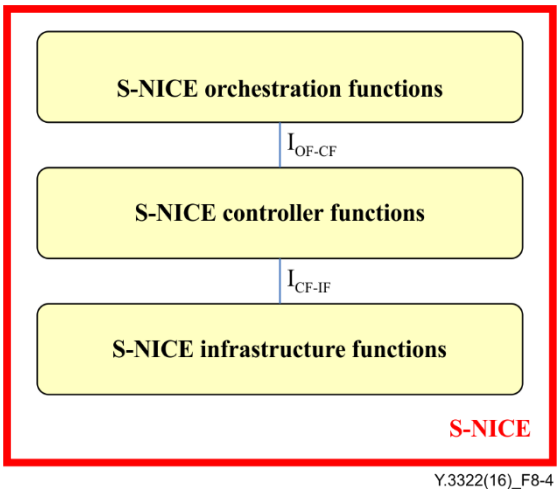

Figure 8-4 – Internal reference points of S-NICE

I_{OF-CF} the reference point between S-NICE orchestration functions and S-NICE controller functions.

With this reference point, S-NICE orchestration functions invoke the capabilities of S-NICE controller functions according to the request from the applications.

I_{CF-IF} the reference point between S-NICE controller functions and S-NICE infrastructure functions.

With this reference point, S-NICE controller functions retrieve the network and traffic information from S-NICE infrastructure functions.

S-NICE controller functions also send instructions to S-NICE infrastructure functions for executing with this reference point.

8.5 External reference points of S-NICE

Figure 8-5 and the following content provides the descriptions of the external reference points:

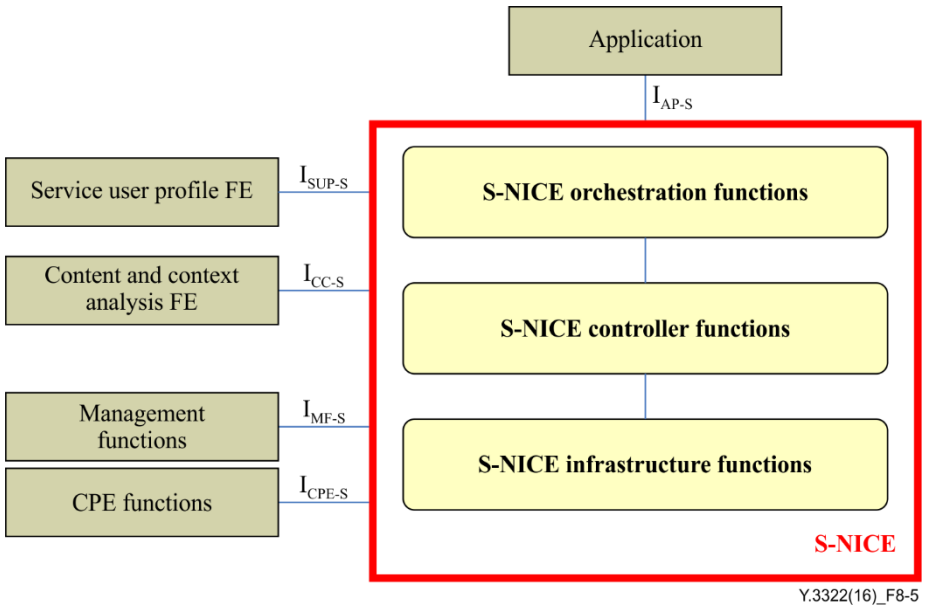

Figure 8-5 – External reference points of S-NICE

I_{SUP-S} the reference point between S-NICE and the service user profile FE.

With this reference point, S-NICE achieves user's profile information (such as mobile device management (MDN)/international mobile subscriber identity (IMSI)/other identity, service information) from the service user profile FE.

I_{AP-S} the reference point between S-NICE and the application.

With this reference point, S-NICE receives service requests from the application, such as resource guarantee, traffic scheduling request, etc.

I_{CC-S} the reference point between S-NICE and the content and context analysis FE.

The content and context analysis FE receives original information from the S-NICE infrastructure functions, and provides the analysis capability and results to S-NICE. With this reference point, S-NICE configures the analysis policy of the content and context analysis FE, in order to collect application related contents on demand.

I_{MF-S} the reference point between S-NICE and the management functions.

With this reference point, S-NICE interacts with the management functions to provide network management related information to the management functions, such as network traffic information, network alarm information and network topology information.

I_{CPE-S} the reference point between S-NICE and the CPE functions.

With this reference point, S-NICE interacts with the CPE functions to collect CPE information, such as access network type, network available bandwidth and related application information.

9 Security considerations

The security requirements of S-NICE are aligned with the security requirements of NICE [ITU-T Y.2301] and [ITU-T Y.2302]. Furthermore, S-NICE provides:

– Enhanced protection of the S-NICE controller functions, because the logically centralized controller could be a single point of failure, or a target of malicious attacks;

– Secure mechanisms of S-NICE orchestration functions to against unauthorized network configurations (e.g., routing path establishment) upon demand by third party services or applications;

– Network isolation of S-NICE infrastructure functions 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 of S-NICE infrastructure functions to monitor abnormal situations, to detect and defend from attacks and to recover network components and their status.

Appendix I

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

I.1 Implementation flows of on-demand provision

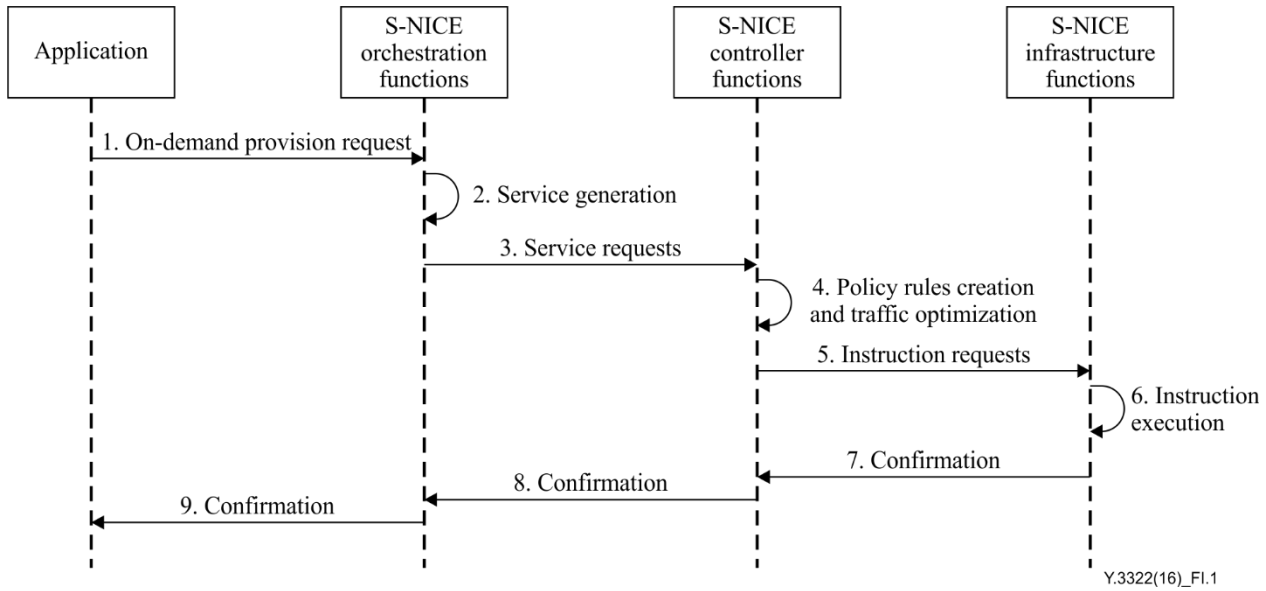

Figure I.1 – Implementation flows of on-demand provision

Figure I.1 shows the implementation flows of on-demand provision:

– 1: The application sends an on-demand provision request to the S-NICE orchestration functions;

– 2: According to the provision request, the S-NICE orchestration functions generate service requests;

– 3: The S-NICE orchestration functions send service requests to the S-NICE controller functions;

– 4: The S-NICE controller functions create policy rules based on the service request and the traffic optimization result;

– 5: The S-NICE controller functions translate the policy rules into instruction requests and send them to the S-NICE infrastructure functions;

– 6: The S-NICE infrastructure functions execute all the instructions;

– 7-9: After all instructions have been executed, the confirmation message is sent back to the application.

I.2 Implementation flows of resource guarantee based on network awareness

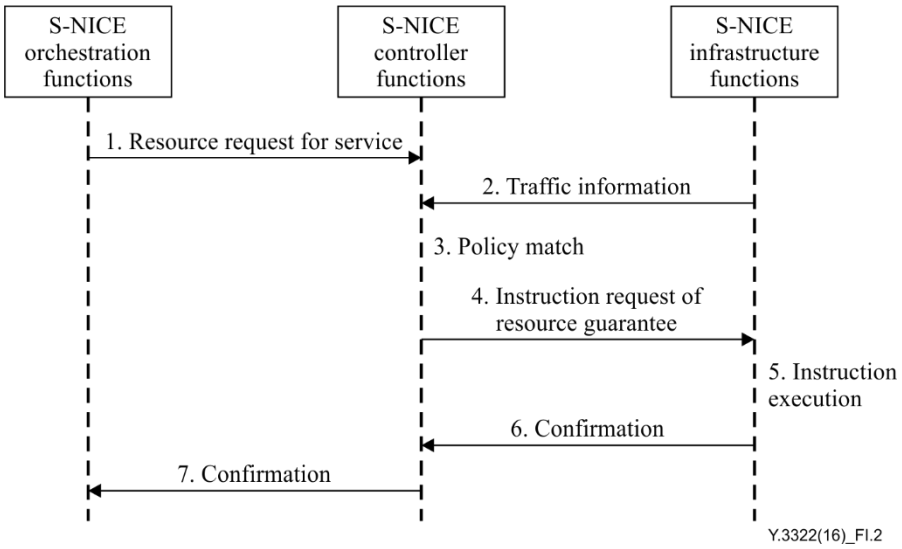

Figure I.2 – Implementation flows of resource guarantee based on network awareness

Figure I.2 shows the implementation flows of resource guarantee based on network awareness:

– 1: The S-NICE orchestration functions send resource request for special service to the S-NICE controller functions;

– 2: The S-NICE infrastructure functions send real time traffic information (such as network congestions) to the S-NICE controller functions;

– 3: According to the resource request, the network awareness traffic information, the S-NICE controller functions decide if one or several resource guarantee policy rules are matched;

– 4: If yes, the S-NICE controller functions translate the policy rules into instruction requests and send them to the S-NICE infrastructure functions;

– 5: The S-NICE infrastructure functions execute all the related instructions;

– 6-7: After all instructions have been executed, the confirmation message is sent back to the S-NICE orchestration functions.

I.3 Implementation flows of traffic scheduling based on network awareness

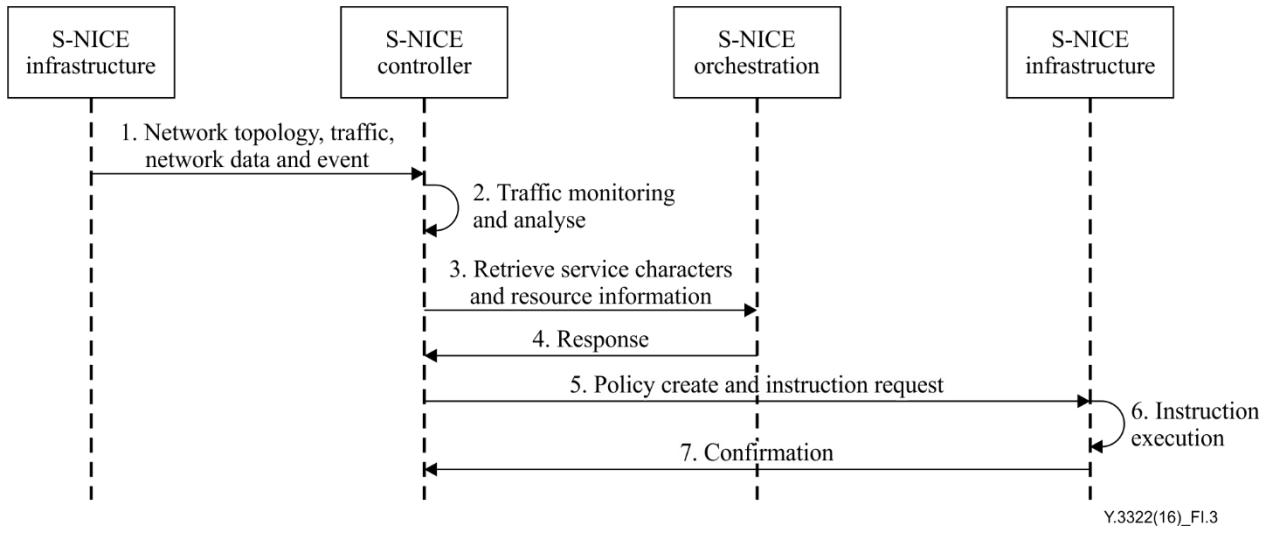

Figure I.3 – Implementation flows of traffic scheduling based on network awareness

Figure I.3 shows the implementation flows of traffic scheduling based on network awareness:

– 1: The S-NICE controller functions retrieve traffic related information from the S-NICE infrastructure functions, including network topology, real time traffic status, etc.;

– 2: The S-NICE controller functions monitor and analyse these traffic information according to the pre-defined rules, then decide if the traffic scheduling request is needed;

– 3-4: If needed, the S-NICE controller functions retrieve service characters (e.g., 5-tuple of service servers) and resource information (e.g., bandwidth, latency) from the S-NICE orchestration functions;

– 5: According to the traffic scheduling request, the service characters and resource information, the S-NICE controller functions decide if one or several traffic scheduling policy rules are matched; if yes, the S-NICE controller functions translate the policy rules into instruction requests and send them to the S-NICE infrastructure functions;

– 6: The S-NICE infrastructure functions execute all the related instructions;

– 7: After all instructions have been executed, the confirmation message is sent back to the S-NICE controller functions.

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.2002] Recommendation ITU-T Y.2002 (2009), *Overview of ubiquitous networking and 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.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN*.

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

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

[b-ONF TR-502] Open Networking Foundation, ONF TR-502 (2014), *SDN architecture*. https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf

[b-ONF TR-516] Open Networking Foundation, ONF TR-516 (2015), *Framework for SDN, Scope and Requirements*. <https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/Framework_for_SDN_-Scope_and_Requirements.pdf>

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, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016