International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2303

(01/2015)

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

Next Generation Networks – Enhancements to NGN

Network intelligence capability enhancement – Awareness functional architecture

Recommendation ITU-T Y.2303

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

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

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	**Y.2300–Y.2399**
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999

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

Recommendation ITU-T Y.2303

Network intelligence capability enhancement – Awareness functional architecture

Summary

Recommendation ITU-T Y.2303 defines the awareness functional architecture of network intelligence capability enhancement (NICE). Content and context awareness is an important feature of NICE. This includes: network resource awareness, customer location awareness, profile awareness of users and services, user access network awareness and user terminal parameters awareness. This Recommendation defines the functional architecture of the content and context awareness architecture of NICE, including the definition of service scenarios, functional entities, reference points, service procedures and interconnection between different awareness entities.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.2303	2015-01-13	13	11.1002/1000/12422

Keywords

Awareness, next generation network, NICE, NICE provider.

---

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

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.2303

Network intelligence capability enhancement – Awareness functional architecture

1 Scope

This Recommendation defines the functional architecture of the content and context awareness architecture of network intelligence capability enhancement (NICE), which includes the definition of service scenarios, functional entities and sub-functional entities, reference points, service procedures and interconnection between different awareness entities.

The Recommendation builds on [ITU-T Y.2301] and [ITU-T Y.2302].

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

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

[ITU-T Y.2301] Recommendation ITU-T Y.2301 (2013), *Network Intelligence Capability Enhancement – Requirements and Capabilities*.

[ITU-T Y.2302] Recommendation ITU-T Y.2302 (2014), *Functional Architecture for Network Intelligence Capability Enhancement (NICE).*

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 are classified as "data" (e.g., text, encoded values, multimedia description language introduced by 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 context awareness [b-ITU-T Y.2201]: A capability to determine or influence a next action in telecommunication or process by referring to the status of relevant entities, which form a coherent environment as a context.

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

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

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

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

3.1.9 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

None.

4 Abbreviations and acronyms

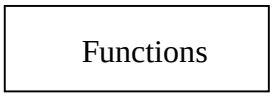
This Recommendation uses the following abbreviations and acronyms:

3G	Third Generation
CA-FE	Content and context Analysis Functional Entity
CD-FE	Content and context Detection Functional Entity
DSL	Digital Subscriber Loop
ID	Identity
IM	Instant Messaging
NGN	Next Generation Network
NICE	Network Intelligence Capability Enhancement
OS	Operating System
P2P	Peer-to-Peer
QoS	Quality of Service
SFE	Sub-Functional Entity
URL	Universal Resource Locator
VoIP	Voice over IP
WiFi	Wireless Fidelity

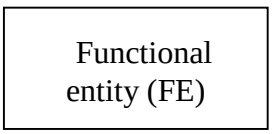
5 Conventions

In this Recommendation:

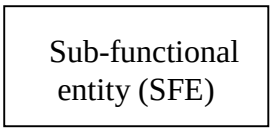
Functions: In the context, "functions" are defined as a collection of functionalities. It is represented with the following symbol:



Functional entity: In the context, a "functional entity (FE)" is defined as a set of one or more functions, and several functional entities constitute the "functions." It is represented with the following symbol:



Sub-functional entity: In the context, a sub-functional entity (SFE) is defined as a sub-function. The scope is smaller than a functional entity and several sub-functional entities constitute a "functional entity." It is represented with the following symbol:



6 Scenarios of the content and context awareness functions in NICE

The content and context awareness functions of NICE support the following scenarios:

- For network resource awareness, the content and context analysis functional entity (CA-FE) interacts with the management functions of transport stratum and wireless access network to gather the bandwidth utilization, cost of routes and other available resources information.
- For user traffic awareness, the content and context analysis functional entity (CA-FE) interacts with the content and context detection functional entity (CD-FE) to get the user's service and traffic flow information.
- For user profile information awareness, the CA-FE interacts with the user profile FE and the open environment FE.
- For user terminal parameters awareness, the CA-FE interacts with user terminal to obtain the terminal type, OS type, access network information, etc.
- The content and context analysis FE needs to interwork with the policy control FE to provide control policies, such as the status of access network. The content and context analysis FE supports the functions of analysis of the data of user, network, etc. The CA-FE also supports openness of the information of user and network to 3rd party, such as provide the user's recent web visiting information to advertisement provider.
- Applications can access the CA-FE either through application support functions or policy control FE. In both cases, applications can configure the analysis policy of the CA-FE in order to collect application-related contents on demand rather than receive the complete information extracted by the CA-FE.

7 Functional architecture of the content and context awareness in NICE

7.1 Overview of the content and context awareness functional architecture in NICE

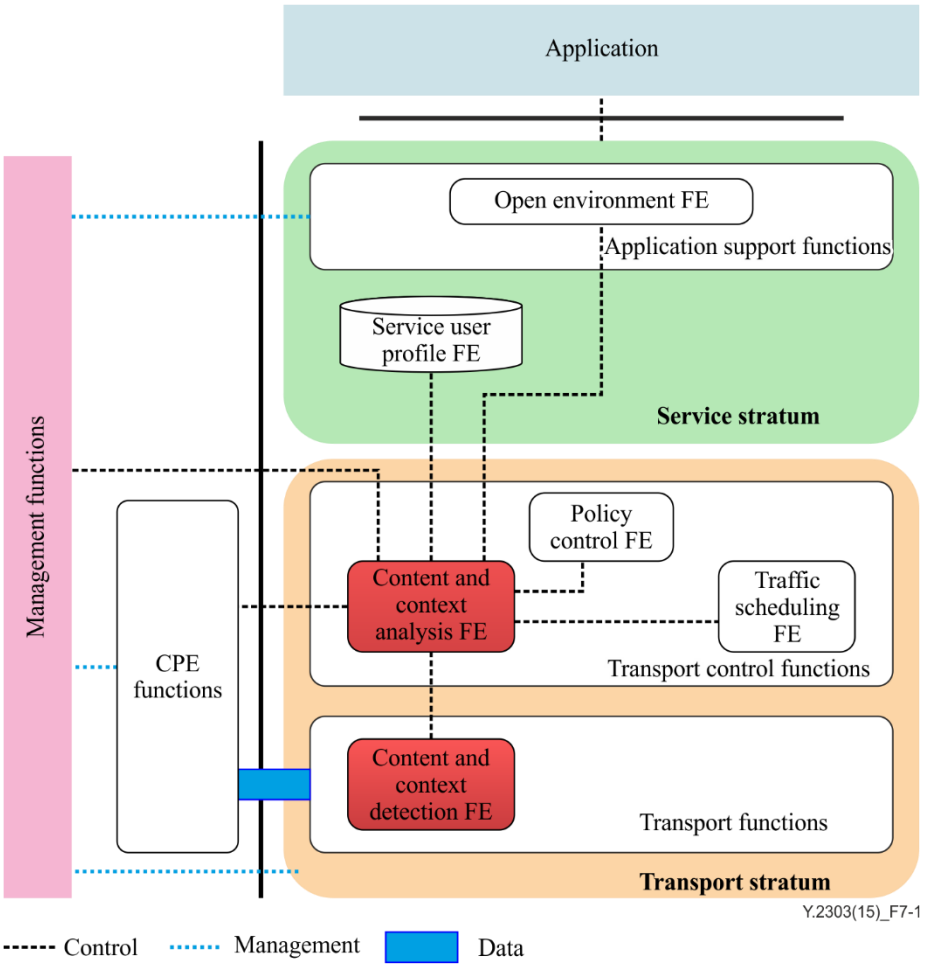


Figure 7-1 – Overview of the content and context awareness functional architecture in NICE

Figure 7-1 shows the overview of the content and context awareness functional architecture in NICE.

In NICE architecture, the CA-FE and the CD-FE are two main FEs that play the role of awareness functions. These two FEs interact with other FEs and functions in NICE, such as the policy control FE, the traffic scheduling FE, and the open environment FE to provide awareness analysis data or results.

Beyond NICE architecture, the awareness functions also reside in the NGNs, e.g., the CPE functions, the management functions, the service user profile FE, etc. These FEs and functions interact with the CA-FE and the CD-FE as awareness resource data inputs.

7.2 Detailed functional architecture of the content and context awareness

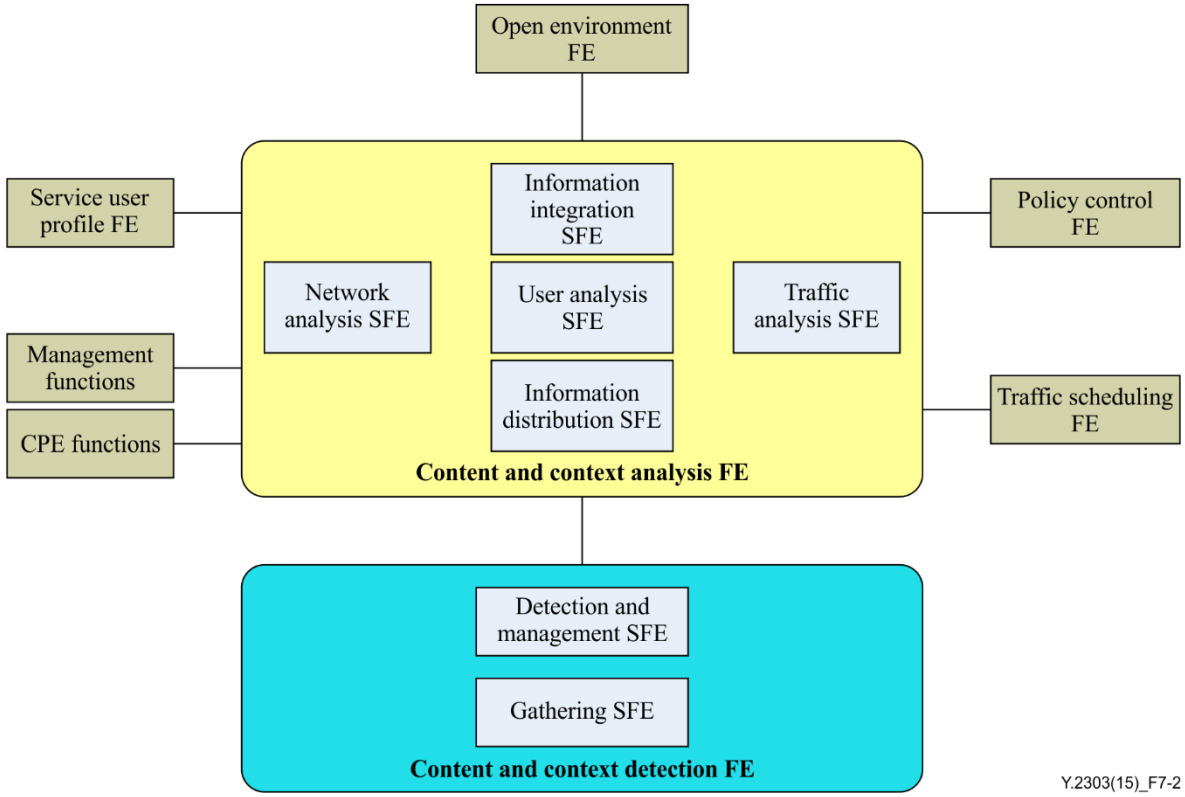


Figure 7-2 – Detailed functional architecture of the content and context awareness FE

Figure 7-2 shows the detailed functional architecture of the content and context awareness functional entity.

1) The content and context analysis FE (CA-FE) receives the awareness information from the content and context detection FE (CD-FE). CA-FE performs processing and storage of content and context information. CA-FE distributes user traffic analysis results and network status analysis results to the requestor of content and context information, such as the policy control FE and the traffic scheduling FE. Content and context information can be distributed in real time or on demand according to requirements.

   CA-FE includes the following sub-functional entities:

   – information integration SFE
   – network analysis SFE
   – user analysis SFE
   – traffic analysis SFE
   – information distribution SFE

2) The CD-FE collects transport-related information and provides the information to CA-FE.

   CD-FE includes the following sub-functional entities:

   – gathering SFE
   – detection and management SFE

7.2.1 Network analysis SFE

The network analysis SFE gathers all the network-related information (such as network topology, network status, bandwidth utilization, etc.) and analyses this information in a systematic way. It then

provides the general view of network condition and detailed analysis results, which can be used for network performance optimization, network access choosing, etc.

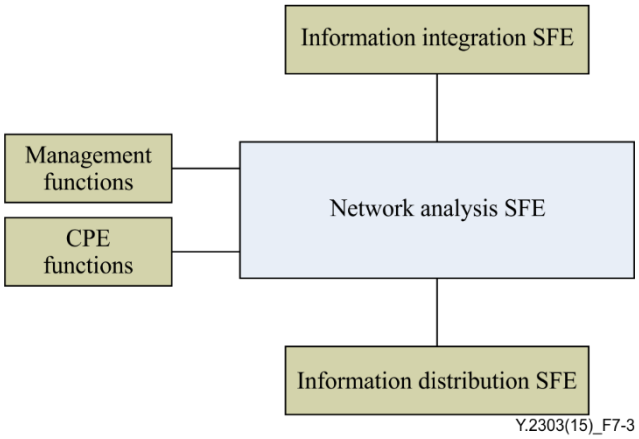


Figure 7-3 – Network analysis SFE functional view

The network analysis SFE interacts with the information distribution SFE to collect network information, which includes, but is not limited to:

– access network type (cable, fibre, DSL, 3G, WiFi, etc.)

– network topology

– network available bandwidth and utilization rate.

The network analysis SFE interacts with the management functions to collect network information, which includes, but is not limited to:

– busy hour and area of network

– network alarm information

– network historical data.

The network analysis SFE also interacts with the CPE functions to collect network information, which includes but is not limited to:

– access network type (cable, fibre, DSL, etc.)

– network available bandwidth and utilization rate.

The network analysis SFE exploits this information from different dimensions with pre-defined rules, e.g., based on time, location, or access network. It then provides the general view of network condition and detailed analysis results. The results can be used for network performance optimization, access network choosing, potential network issue identification, network change impaction, etc.

As the information integration SFE is the information centre, the network analysis SFE transports the network analysis results to the information integration SFE for further data mining.

7.2.2 User analysis SFE

The user analysis SFE gathers all the user related information (such as user profile information, user traffic information and user terminal information) and analyses this information according to pre-defined rules. The results of this data mining can be used for improving user experience, targeted advertising marketing, etc.

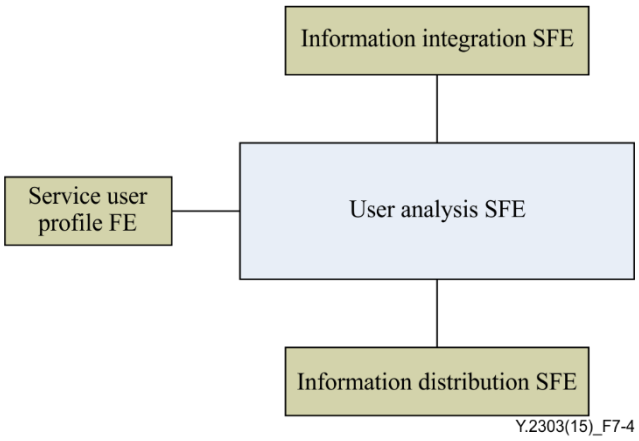


Figure 7-4 – User analysis SFE functional view

The user analysis SFE interacts with the service user profile FE to collect profile information, which include but are not limited to:

– user ID

– user location information (geographical and logical location)

– service profile, including the ordering relationship.

The user analysis SFE interacts with the information distribution SFE to collect other user information, which includes, but not limited to user:

– ID

– terminal information (terminal manufacturer, terminal type, terminal OS, etc.)

– access network

– QoS information (upload/download bandwidth, priority, etc.)

– service information (the application operated, the uniform/universal resource locators (URLs) visited, etc.).

The user analysis SFE exploits this information according to pre-defined data mining rules. For example, it finds out users' service preferences by calculating the visiting times of specific URLs while users are surfing the web, or introduces new products to users when their location or access network changes.

As the information integration SFE is the information centre, the user analysis SFE transports the user analysis results to the information integration SFE for further data mining.

7.2.3 Traffic analysis SFE

The traffic analysis SFE gathers all the traffic related information (such as traffic localization scheme, traffic delivery network node selection, routing adjustment, etc.) and analyses this information according to pre-defined rules. The data mining results can be used for user routing selection, network resource reallocation, etc.

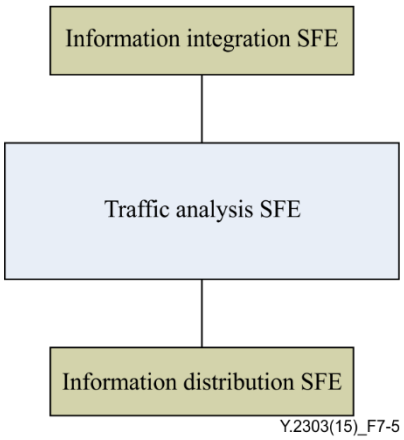


Figure 7-5 – Traffic analysis SFE functional view

The traffic analysis SFE interacts with the information distribution SFE to collect the traffic information, which includes but is not limited to:

– traffic localization scheme

– traffic delivery network node selection

– current network status (idle, normal or overload)

– routing adjustment

– network resource allocation

The traffic analysis SFE exploits the information according to pre-defined rules. For example, it plans a new routing path for the user to prevent network overload.

As the information integration SFE is the information centre, the traffic analysis SFE transports the traffic analysis results to the information integration SFE for further data mining.

7.2.4 Information integration SFE

The information integration SFE is the information centre, and it gathers information from the network analysis SFE, the user analysis SFE and the traffic analysis SFE for further data mining.

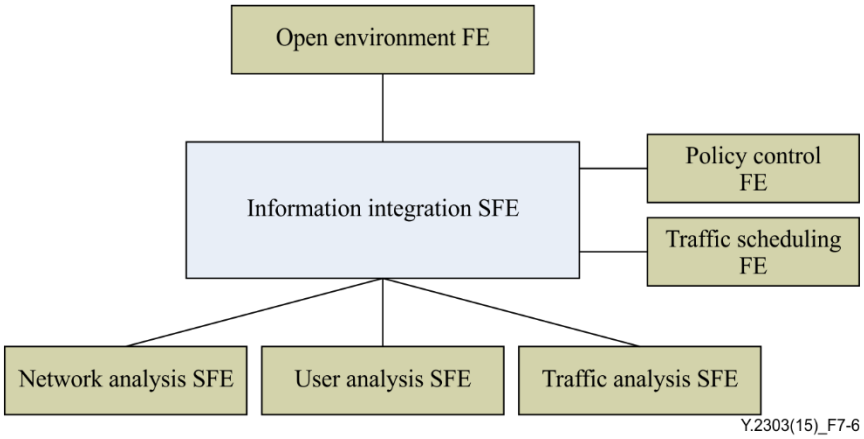


Figure 7-6 – Information integration SFE functional view

The information integration SFE plays the role of comprehensive analysis centre of multiple information inputs, finds the relationship among the network condition, the user option and the current traffic status and provides aggregate analysis results to other FEs.

For example, when a user visits a video website, the information integration SFE can find out if the video content is stored locally or not, according to the user's location information and the traffic localization scheme. Then the traffic scheduling FE can take the advantage of the results to set a rule for the user's routing selection.

In the same way, the policy control FE receives analysis results from the information integration SFE, then it makes policy decisions and updates such as intelligent assignment of bandwidth and QoS level according to the analysis results.

The information integration SFE also interacts with the open environment FE, mainly to open the analysis capability and results to the applications.

7.2.5 Gathering SFE

The gathering SFE collects the content and context related information and sends it to the detection and management SFE.

7.2.6 Detection and management SFE

The detection and management SFE receives the policy from the CA-FE or from the policy control FE. The policy is based on the carrier's service policy and network traffic and resources.

The detection and management SFE compares the particular packet headers and payloads with the target packet flows and a set of rules to identify the application and traffic. The detection and management SFE detects the packet from Layer 2-Layer 7 to identify the different kinds of applications, such as P2P downloading, P2P streaming, http application, IM, VoIP. It can also identify the IPv4 and IPv6 traffic.

Based on the policy for different kinds of applications, the detection and management SFE manages the traffic concerning different applications, such as:

– Limit the bandwidth of some applications (e.g., P2P download);

– Identify different kinds of VoIP applications with different policies, e.g., providing QoS guarantee for VoIP applications of the carrier itself or the 3rd party collaborating with the carrier.

8 Reference points of the content and context awareness architecture in NICE

The reference points of the content and context awareness architecture are classified in:

– internal reference points, related to interactions between awareness architecture SFEs

– external reference points, related to interactions between awareness architecture SFEs and external FEs, and between awareness architecture SFEs and external functions.

8.1 Internal reference points

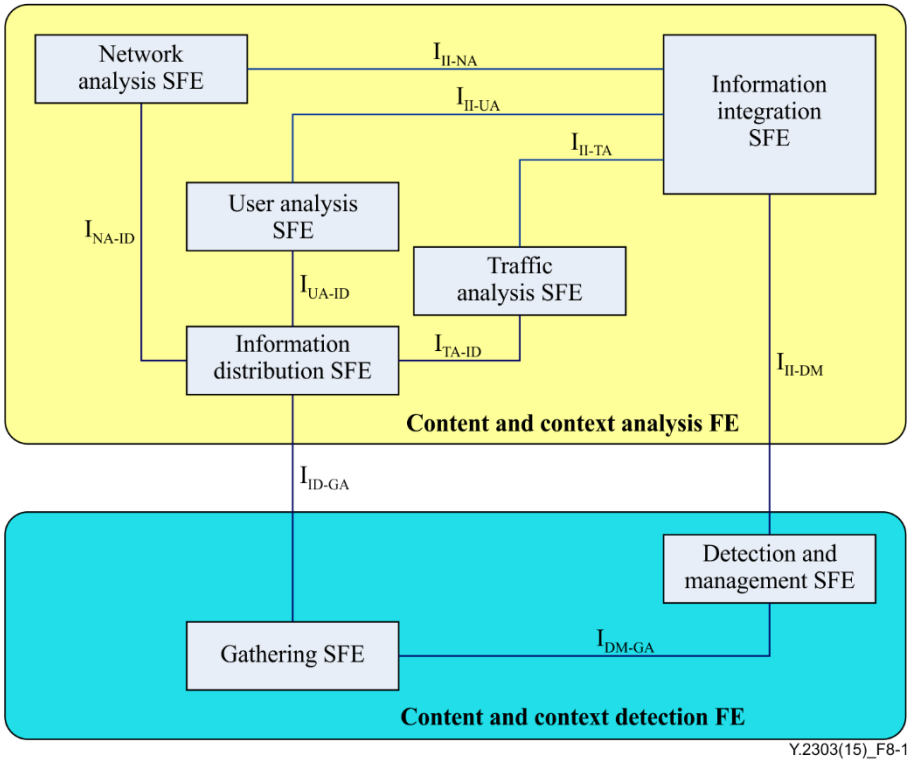


Figure 8-1 – Internal reference points

The following content provides the description of the internal reference points:

I_{II-NA} The reference point between the information integration SFE and the network analysis SFE.

The information integration SFE achieves network analysis results through this reference point.

I_{II-UA} The reference point between the information integration SFE and the user analysis SFE.

The information integration SFE achieves user analysis results through this reference point.

I_{II-TA} The reference point between the information integration SFE and the traffic analysis SFE.

The information integration SFE achieves traffic analysis results through this reference point.

I_{NA-ID} The reference point between the network analysis SFE and the information distribution SFE.

The network analysis SFE achieves network information (such as network topology, network status, bandwidth utilization) through this reference point.

I_{UA-ID} The reference point between the user analysis SFE and the information distribution SFE.

The user analysis SFE achieves user information (such as user profile information, user traffic information and user terminal information) through this reference point.

I_{TA-ID} The reference point between the traffic analysis SFE and the information distribution SFE.

The user traffic SFE achieves traffic information (such as traffic localization scheme, traffic delivery network node selection, routing adjustment) through this reference point.

I_{DM-GA} The reference point between the detection and management SFE and the gathering SFE.

The detection and management SFE achieves all raw information including network, user and traffic information through this reference point.

I_{II-DM} The reference point between the information integration SFE and the detection and management SFE.

The detection and management SFE gets the policy to be executed according to analysis results through this reference point.

I_{ID-GA} The reference point between the information distribution SFE and the gathering SFE.

The information distribution SFE achieves all raw information including network, user and traffic information through this reference point.

8.2 External reference points

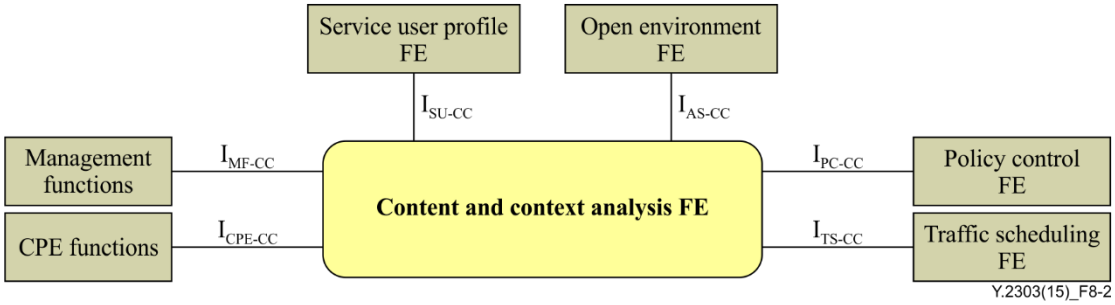


Figure 8-2 – External reference points

The following content provides descriptions of the external reference points:

I_{SU-CC} The reference point between the CA-FE and the service user profile FE.

With this reference point, the CA-FE achieves user's profile information (such as MDN/IMSI/other identity, service information) for further analysis.

I_{AS-CC} The reference point between the CA-FE and the open environment FE.

With this reference point, the CA-FE provides the original information, analysis capability and results to the open environment FE, and finally open to the applications. With this reference point, open environment FE configures the analysis policy of the CA-FE, in order to collect application related contents on demand.

I_{PC-CC} The reference point between the CA-FE and the policy control FE.

This reference point allows the CA-FE to distribute analysis results to the policy control FE. The distribution is performed in either push or pull mode. It also allows the policy control FE to configure the analysis policy of the CA-FE, in order to collect application related contents on demand.

The information distributed with this reference point includes but not limited to the following items:

User traffic analysis results based on pre-defined rules and information, such as user profile information, user traffic information and user terminal parameters.

Information about users' service preferences (e.g., preferred URL while surfing the web).

Network status analysis results based on pre-defined rules and information, such as network resource information and access network related information.

I_{TS-CC} The reference point between the CA-FE and the traffic scheduling FE.

This point allows the CA-FE to distribute analysis results to the traffic scheduling FE. The distribution is performed in either push or pull mode.

I_{MF-CC} The reference point between the CA-FE and the management functions.

With this reference point, the CA-FE interacts with the management functions to collect network management related information, such as busy hour and area of network, network alarm information and network topology.

$\mathbf{I}_{\text{CPE-CC}}$ The reference point between the CA-FE and the CPE functions.

With this reference point, the CA-FE interacts with the CPE functions to collect CPE information, such as access network type (cable, fibre, DSL, etc.), network available bandwidth and related application information.

9 Information flow and service procedure of the content and context awareness architecture in NICE

9.1 Procedure of information collection and preliminary analysis

In NICE awareness architecture, the CD-FE extracts information from the transport stratum, including network resources, user information etc., and transfers the awareness information to the CA-FE. Then the CA-FE analyses this information according to pre-defined rules.

The following content describes the procedure details. This procedure involves interaction of the:

– detection and management SFE
– gathering SFE
– information distribution SFE
– management functions
– CPE functions
– service user profile FE
– network analysis SFE
– user analysis SFE
– traffic analysis SFE.

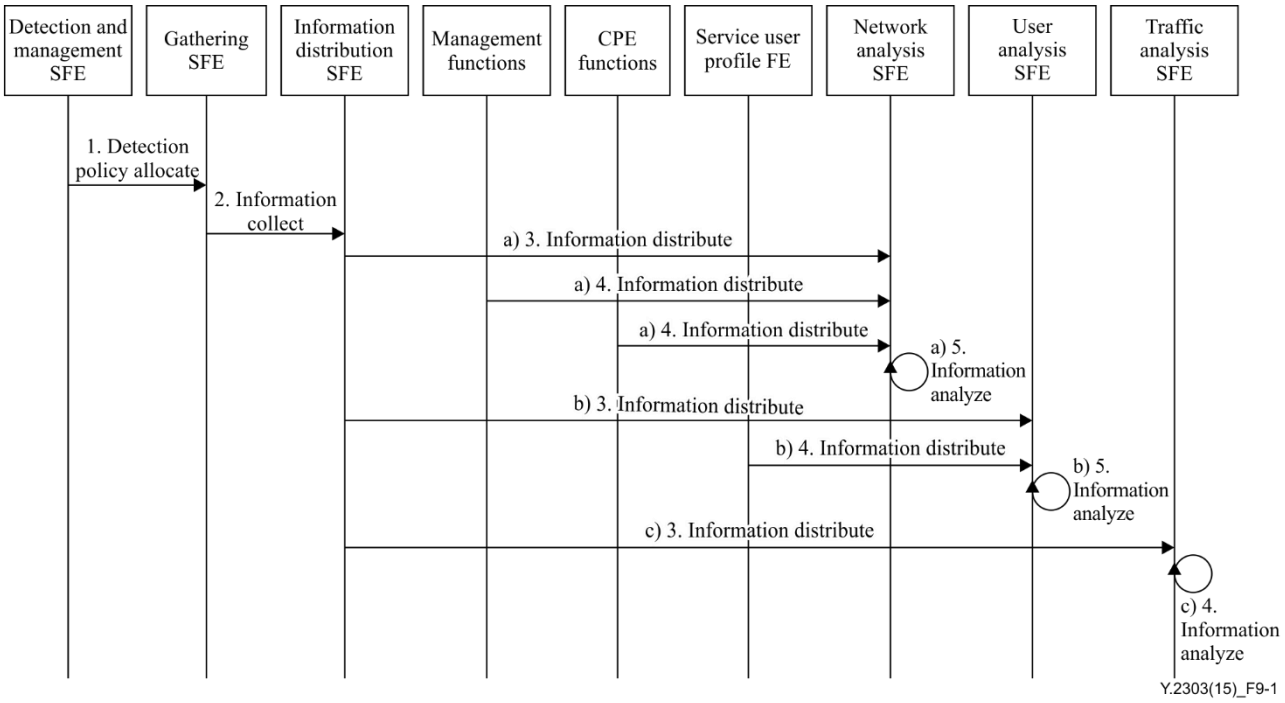


Figure 9-1 – Procedure of information collection and preliminary analysis

1) The detection and management SFE allocates the detection policy to the gathering SFE. The detection policy is based on the carrier's service policy, network traffic and network resources.

2) The gathering SFE collects the user, traffic and network information and sends this information to the information distribution SFE. The information distribution SFE dispenses it to the correlative analysis SFE: a) the network analysis SFE; b) the user analysis SFE; c) the traffic analysis SFE.

a) For the network analysis:

3) The information distribution SFE dispenses network related information to the network analysis SFE.

4) The network analysis SFE also interacts with the management functions and the CPE functions to collect other network information such as network access type, network alarm information, etc.

5) The network analysis SFE exploits the information with pre-defined rules.

b) For the user analysis:

3) The information distribution SFE dispenses user related information to the user analysis SFE.

4) The user analysis SFE also interacts with the service user profile FE to collect the profile information such as user ID, user QoS information, etc.

5) The user analysis SFE exploits the information with pre-defined rules.

c) For the traffic analysis:

3) The information distribution SFE dispenses traffic related information to the traffic analysis SFE.

4) The traffic analysis SFE exploits the information with pre-defined rules.

9.2 Procedure of information integration and utilization

In NICE awareness architecture, the analysis results are integrated and provided to the policy control FE, the traffic scheduling FE and the open environment FE for policy decision, route scheduling and openness to the applications.

The following content describes the procedure details. This procedure involves interaction of network analysis SFE, user analysis SFE, traffic analysis SFE, information integration SFE, policy control FE, traffic scheduling FE and open environment FE.

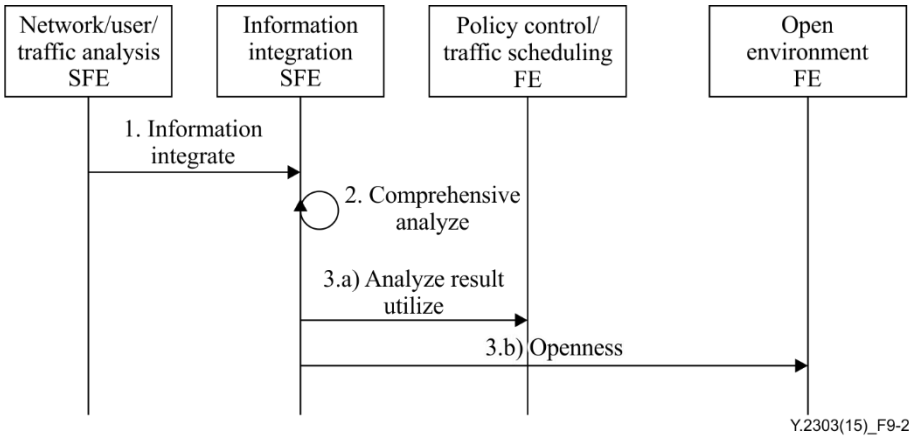


Figure 9-2 – Procedure of information integration and utilization

1) The network analysis SFE, the user analysis SFE and the traffic analysis SFE transport the network analysis results to the information integration SFE for further data mining.

2) The information integration SFE plays the role of comprehensive analysis of multiple information inputs, and finds the relationship among the network condition, the user option and the current traffic status and gives aggregate analysis results.

3a) The information integration SFE provides the analysis results to the policy control FE and the traffic scheduling FE for policy decision, route scheduling.

3b) The information integration SFE also interacts with the open environment FE, opens the analysis capability and results to the applications.

10 Security

The content and context awareness architecture supports the followings security requirements:

1) The content and context awareness architecture fulfils the NICE security requirements according to [ITU-T Y.2301].

2) The content and context awareness architecture provides protection against unauthorized use of awareness data.

3) The content and context awareness architecture provides a secure environment for the NICE user and the NICE provider. It also sets up a trust domain for content and context aware applications.

4) The content and context awareness architecture provides a privacy schema to protect users' personal content information from unauthorized access.

5) The content and context awareness architecture has mechanisms to manage, control and distribute context related information in a secure way according to the NICE provider's privacy policies, and related agreements with NICE users and NICE resource providers supplying context information.

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 M.1400] Recommendation ITU-T M.1400 (2013), *Designations for interconnections among operators' networks*.

[b-ITU-T Q.825] Recommendation ITU-T Q.825 (1998), *Specification of TMN applications at the Q3 interface: call detail recording*.

[b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[b-ITU-T Y.2002] Recommendation ITU-T Y.2002 (2009), *Overview of ubiquitous networking and of its support in NGN*.

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

[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.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*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015