International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series Y

Supplement 17

(02/2012)

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

ITU-T Y.2200-series – Functional model of a service overlay network framework which uses the next generation network

ITU-T Y-series Recommendations – Supplement 17

ITU-T
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
Numbering, naming and addressing	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.

Supplement 17 to ITU-T Y-series Recommendations

ITU-T Y.2200-series – Functional model of a service overlay network framework which uses the next generation network

Summary

Supplement 17 to ITU-T Y.2200-series Recommendations provides a functional model of a service overlay network (SON) which uses NGNs. It identifies SON service capability functions and also provides a number of operating scenarios which may be used to provide enhanced NGN applications.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y Suppl. 17	2012-02-17	13

Keywords

NGN, service overlay network, SON.

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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

Introduction

A service overlay network (SON) is a virtual or logical service network which possesses a number of specific functions, lies on top of and utilizes existing transport networks and provides support for various types of services beyond those normally offered by the transport network.

SONs are designed to provide and dynamically utilize application features in accordance with users' demands. The application features are provided via the use of a composition function, which can be used to develop user service capabilities in SONs in response to user's needs.

Supplement 17 to ITU-T Y-series Recommendations

ITU-T Y.2200-series – Functional model of a service overlay network framework which uses the next generation network

1 Scope

This Supplement defines a functional framework and service features for service overlay networks (SONs) which use the next generation network (NGN). It also provides a number of SON service scenarios.

2 References

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

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 application [b-ITU-T Y.2261]: A structured set of capabilities, which provide value-added functionality supported by one or more services, which may be supported by an API interface.

3.1.2 application network interface (ANI) [ITU-T Y.2012]: Interface which provides a channel for interactions and exchanges between applications and NGN elements. The ANI offers capabilities and resources needed for realization of applications.

3.1.3 functional architecture [ITU-T Y.2012]: A set of functional entities and the reference points between them used to describe the structure of an NGN. These functional entities are separated by reference points, and thus, they define the distribution of functions.

3.1.4 mobility [b-ITU-T Q.1706]: The ability for the user or other mobile entities to communicate and access services irrespective of changes of the location or technical environment.

3.1.5 multicast [b-ITU-T X.603]: A data delivery scheme where the same data unit is transmitted from a single source to multiple destinations in a single invocation of service.

3.1.6 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 supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

3.1.7 NGN service stratum [b-ITU-T Y.2011]: That part of the NGN which provides the user functions that transfer service-related data and the functions that control and manage service resources and network services to enable user services and applications.

3.1.8 NGN transport stratum [b-ITU-T Y.2011]: That part of the NGN which provides the user functions that transfer data and the functions that control and manage transport resources to carry such data between terminating entities.

3.1.9 nomadism [b-ITU-T Q.1706]: The ability of the users to change their network access point on moving. When changing the network access point, the user's service session is completely stopped and then started again, i.e., there is no service continuity or hand-over used. It is assumed that normal usage pattern is that users shut down their service session before attaching to a different access point.

3.1.10 overlay network [b-ITU-T Y-Sup.10]: A network of nodes and logical links that is built on top of the underlying, e.g., transport, network with the purpose of providing a network service that is not available in the underlying network.

3.1.11 peer-to-peer (P2P) [b-ITU-T Y.2206]: A system is considered to be P2P if the nodes of the system share their resources in order to provide the service the system supports. The nodes in the system both provide services to other nodes and request services from other nodes.

3.1.12 quality of experience (QoE) [b-ITU-T P.10 Amd.2]: The overall acceptability of an application or service, as perceived subjectively by the end-user. Quality of experience includes the complete end-to-end system effects (client, terminal, network, services infrastructure, etc.). Overall acceptability may be influenced by user expectations and context.

3.1.13 service composition [b-ITU-T Y.2234]: Service composition is the capability of creating new services from other existing services.

3.1.14 service node interface (SNI) [ITU-T Y.2012]: Interface which provides a channel for interactions and exchanges between a NGN and other service providers.

3.1.15 session [b-ITU-T Y.2091]: A temporary telecommunications relationship among a group of objects in the service stratum that is assigned to collectively fulfil a task for a period of time. A session has a state that may change during its lifetime.

3.1.16 third-party service provider [ITU-T M.3050.1]: The third-party service provider provides services to the enterprise for integration or bundling as an offer from the enterprise to the customer. Third-party service providers are part of an enterprise's seamless offer. In contrast, a complementary service provider is visible in the offer to the enterprise's customer, including having customer interaction.

3.1.17 topology [ITU-T Y.2012]: Information that indicates the structure of a network. It contains the network address and routing information.

3.1.18 user network interface (UNI) [b-ITU-T G.8012]: An interface that is used for the interconnection of customer equipment with a network element of the transport network.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 service overlay network (SON): A virtual or logical service network deployed to facilitate the creation and deployment of enhanced service-specific functions with applications.

3.2.2 session mobility: The capability that allows a user to transfer an ongoing communication session from one device to another device.

Note that session mobility includes the process of transferring an active session to another terminal or another interface.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AIPF Application Interface Provisioning Function

AKA Authentication and Key Agreement

ANI Application Network Interface

API Application Programming Interface

AV Authentication Vector

CPN Customer Premises Network

DHT Distributed Hash Table

IaaS Infrastructure as a Service

ID Identification

IdM Identity Management

IPTV Internet Protocol Television

NGN Next Generation Network

P2P Peer-to-Peer

PaaS Platform as a Service

QoE Quality of Experience

QoS Quality of Service

SaaS Software as a Service

SNI Service Node Interface

SON Service Overlay Network

UNI User Network Interface

XaaS Everything as a Service

5 Conventions

None.

6 Overview of service overlay networks (SONs)

6.1 Introduction to SON

A service overlay network (SON) uses a logical service networking structure to support diverse application features. SONs can be thought of as being connected logically, regardless of the underlying networks. Additionally, SONs, which use the NGN, support composition functions that are used to provide customer-oriented service features and their associated applications.

With the rapid advancement of computing technology, it is possible to aggregate information and computing resources which are available from clients or peers and utilize these to provide services more effectively. Figure 6-1 shows the general model of a SON that uses the NGN. In this diagram, SON comprises SON functional elements.

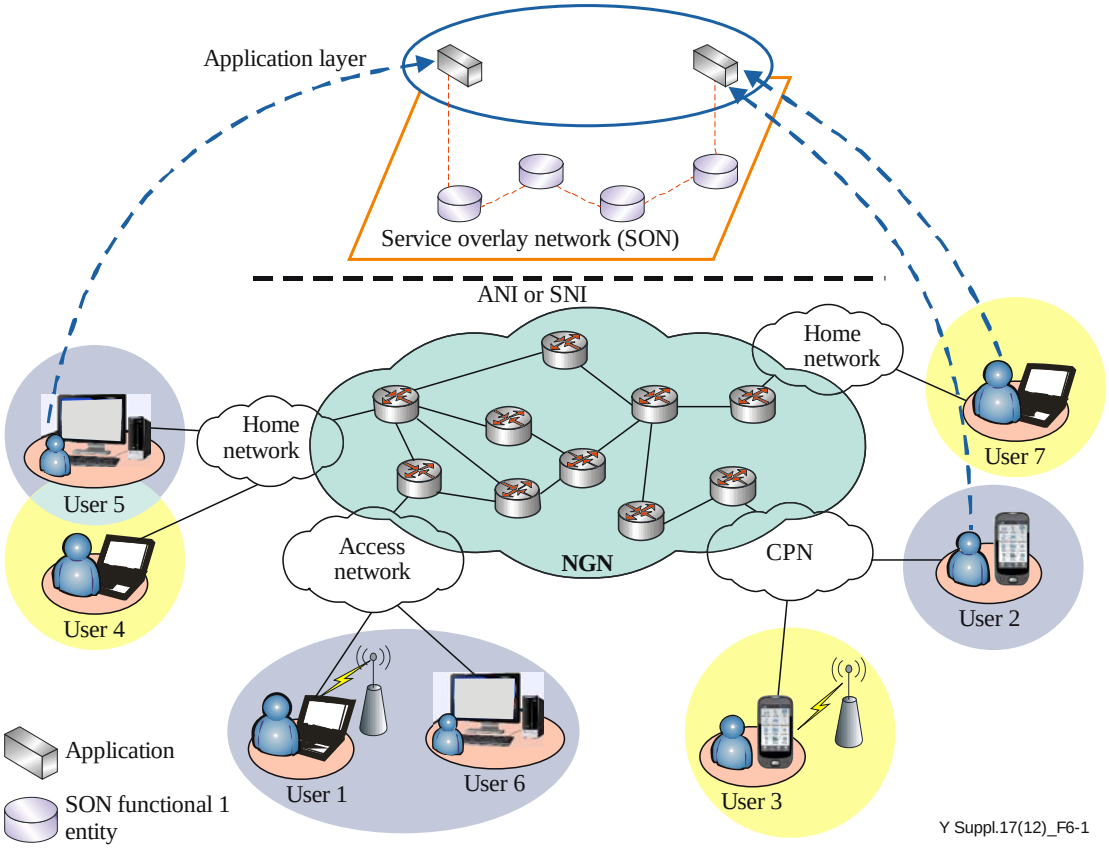

Figure 6-1 – General model of a SON using the NGN

6.1.1 SON relationship with NGN

SON aims to provide easy and quick deployment of service-specific logical networking functions, which can be used to complement the services that can be provided by transport networks. SON need not be constrained by the same technical and political hurdles that may have to be addressed by service providers. SON will also provide active service capabilities that can be used to establish services, modify established services easily, and provide improved and new emerging services.

SONs are expected to support control and management functions that can be used to deliver diverse application features in accordance with a user's request. SONs will also incorporate and support service-processing functions to harmonize and integrate application-related entities. The processing functions will allow enhancement of application service features, e.g., allowing creation and use of application-aware functions.

SON will provide the following:

- user-driven service networking: SON will accept and act upon user requests to create a specific logical service-oriented networking function to deliver user-driven service capabilities for a particular customer, a particular customer group or members of a group.
- context-aware service: SON will allow the provisioning of context-aware services by responding and adapting to the changes in the computing environment. For example, SON-supported context-aware services may react when the location of the user, or the capabilities of the device used, changes.
- service composition: SON will allow two or more service entities to compose and create new application features through the overlay networked service components.
- service personalization: SON will provide the means for retrieving the optimal variant of content (as a response to content requests) based primarily on (i) subscriber profiles including service preferences and end-device capabilities; (ii) content profiles; and (iii)

content provider policies. Examples of personalized services include virus scanning, content adaptation based on subscriber bandwidth and device capability, request and content filtering and localization services.

6.2 SON functional positioning

Service will be provided by SONs using one of the two functional positions of SON shown in Figure 6-2. Each SON deployment model uses the NGN and will have an interface as discussed below.

a) SON associated with an application network interface (ANI): This deployment model will be used when SON interfaces with the NGN using the ANI.

b) SON associated with a service node interface (SNI): This deployment model (used to interface the NGN using the SNI) will be used when SON relies on a service provider to provide certain functions and access the NGN via the SNI. In this deployment model, SON features will be provided via the SNI to users. This deployment configuration may include use of the existing Internet.

As shown in Figure 6-2, SON function is positioned at the application level, and it is associated with the service stratum of the NGN via the ANI interface or, when third party service providers are utilized, via the SNI.

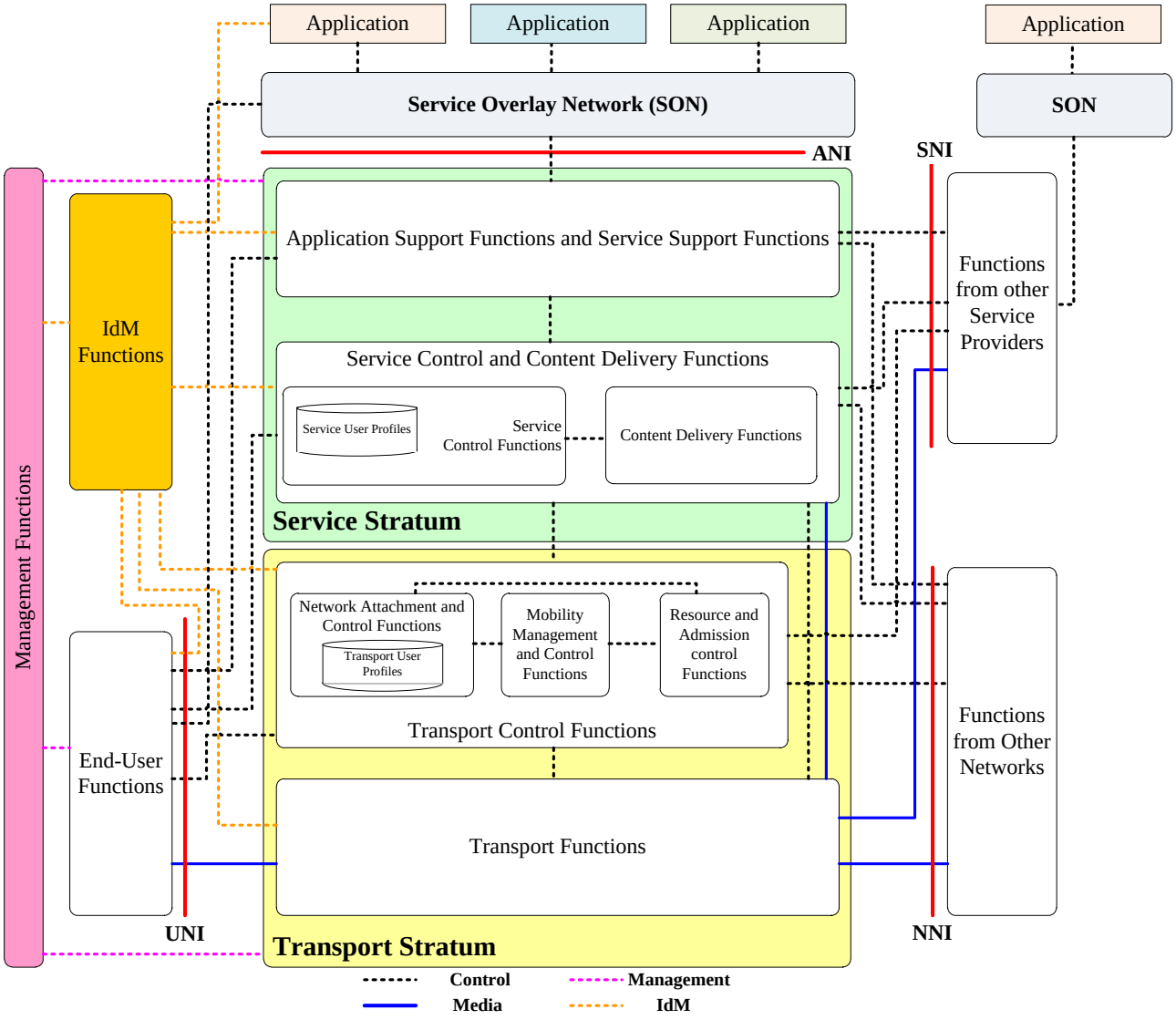

Figure 6-2 – Functional positioning of SON

7 SON functional framework

7.1 SON functional model

As indicated in clause 6.2, the functional model of SON is consistent with [ITU-T Y.2012] in that the advanced application capabilities are created using a SON to NGN interface, as shown in Figure 6-2.

SON includes five major functional groups, as shown in Figure 7-1, and these are as follows:

- SON control function;
- SON service composition function;
- SON management function;
- application interface and provisioning function;
- ANI interworking function.

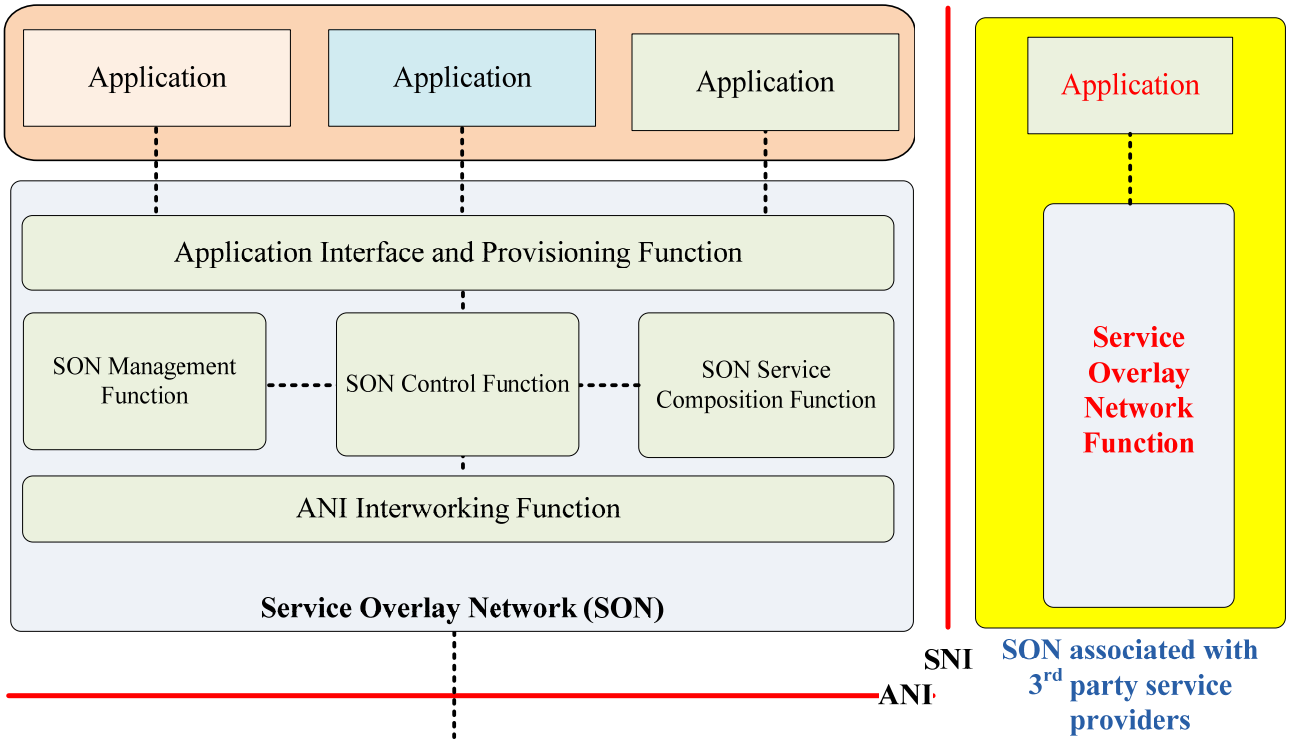

Figure 7-1 – SON functional model

SON functional elements are associated with other functional elements in single-tier or hierarchical peer-to-peer (P2P) configurations in distributed environments. The application interface provisioning function of SONs provides the functions to interact between SON functional elements and applications to add enhanced service capabilities.

SON cooperates with the end-user functions to provide additional enhancement, flexibility and efficiency in applications.

Consistent with the SON functional model shown in Figure 7-1, Figure 7-2 shows the information flows that would result from a service request. Both request and response flows between SON functional elements and other entities are shown in Figure 7-2.

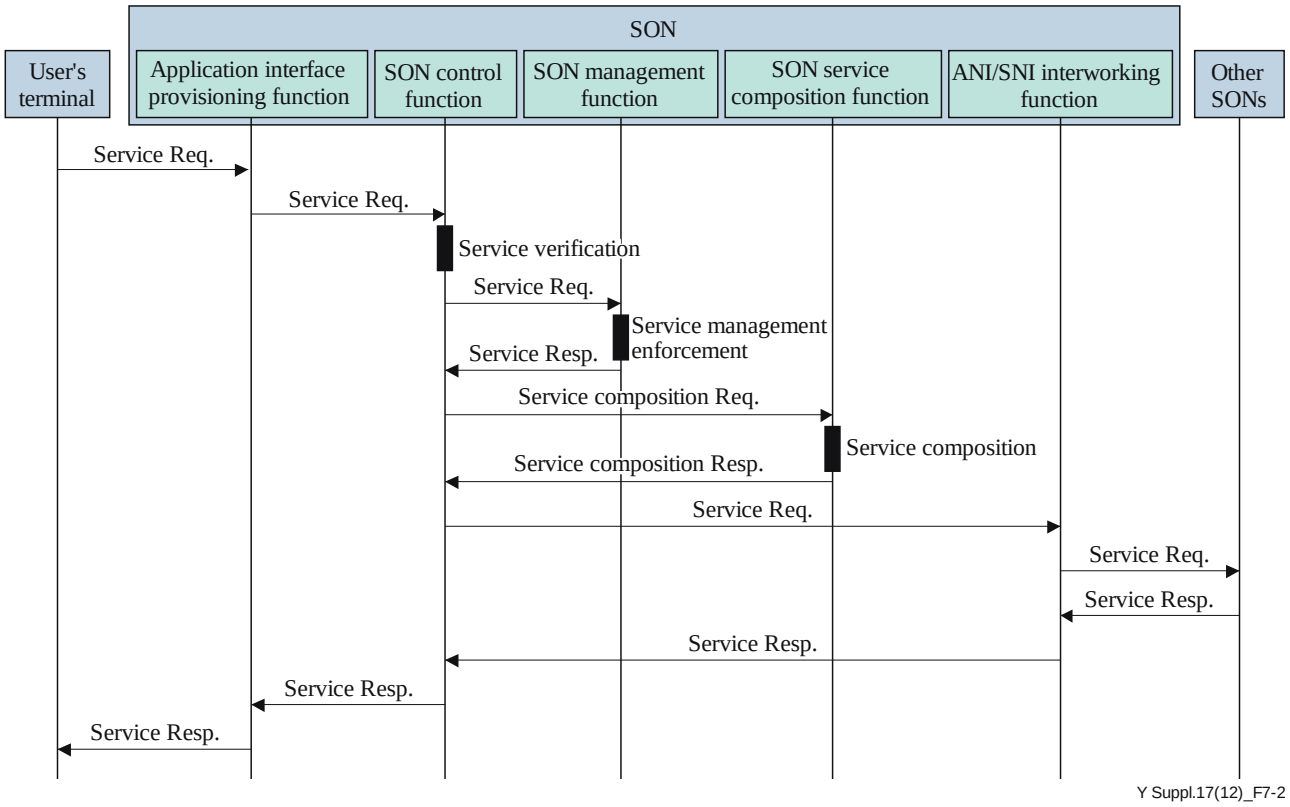

Figure 7-2 – SON control data flow

1) A user requests an additional or new service feature to be added to an application, and the user's terminal sends control data to the nearest SON in order to receive the appropriate service.
2) The application interface provisioning function receives the data request from the user and delivers it to the SON control function.
3) The SON control function verifies the requested service and requests a management policy from the SON management function.
4) The SON management function enforces the appropriate management policy on the information from the SON control function and then replies.
5) If the service is not composed before the request, the SON control function requests the service composition function to perform a service composition according to the response from the SON management function.
6) The service composition function composes a service overlay network using the information received from the SON control function and the SON management function.
7) Data produced by the service composition function is then sent to other SONs as required, requesting that they cooperate in the composition of the service overlay network.
8) The replies from other SONs are then integrated in the SON control function and an appropriate response is returned to the originating application on the end-user terminal.

In a distributed SON environment as shown in Figure 7-3, each SON functional element interacts with other SON functional elements to find the most suitable capabilities in response to the user's requests.

If one functional element of distributed SON supports the application capabilities that are needed by other users attached to a remote SON functional element, the functional element nearest to where the customer request was initiated starts to search for the requested application capability through

the use of a search mechanism. Then, the user request will ultimately be forwarded to the appropriate SON functional element to make use of its service capability.

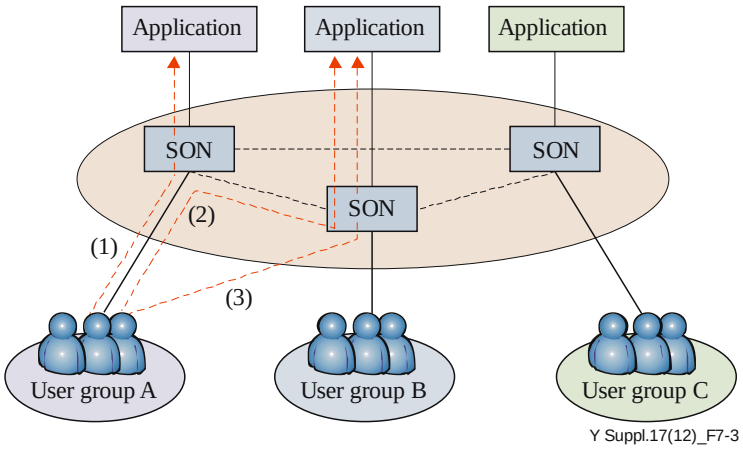

Figure 7-3 – Distributed SON scenario

7.2 SON functional description

7.2.1 Application interface provisioning function

The application interface provisioning function (AIPF) provides a means to interact with applications supported by SON. An AIPF delivers the required information to the SON control function to create or compose proper service features for the application. The SON control function also uses the AIPF to exchange service information with an application.

7.2.2 SON control function

The SON control function supports registration, release, authentication and authorization of users and/or applications in accordance with users' requests. In order to support additional application capabilities, the SON control function also provides interaction with the SON composition function, the SON management function and the ANI/SNI interworking function, as well as with the application interface provisioning function.

7.2.3 SON composition function

The SON composition function composes several interlinked service components that have the ability to become part of the service solutions, no matter how complex the solution is. A newly composed service developed by the SON composition function is inherited by service orientation.

NOTE – Service orientation refers to a process which combines multiple services in SON.

The SON composition function takes the following elements into consideration, in accordance with service requests from the users:

- required QoS level of the service;
- adaptability of the requested service;
- required security level of the service;
- user behaviour;
- user preference;
- emergency conditions.

7.2.4 SON management function

The SON management function provides the ability to manage the composed service overlay network in order to provide services using NGN environments. Sessions and required authentications are also managed should there be requests for modifications of services. The SON management function provides:

- service-driven session topology management;
- per-flow, per-session, per-service-class QoS management;
- accounting management;
- security management.

7.2.5 ANI/SNI interworking function

The ANI/SNI interworking function provides adaptation of service information and interaction between applications in SONs and the application support functions and service support functions in the NGN via the ANI, and in the case where other service providers are involved via the SNI. It is recommended that SONs support standardized APIs to expose capabilities to applications.

The ANI/SNI interworking function provides a channel for interactions and exchanges between the NGN and applications supported by SONs through an ANI. ANI/SNI interworking functions invoke applicable capabilities and resources needed for applications. This function also provides a channel for interactions and exchanges between the NGN and other service providers through the SNI in order for SONs to support control of service level interaction.

8 SON service features

SON provides service abstractions to support intelligent and customer-oriented capabilities of application services.

Some or all of the functional entities may be used as part of the composition process to provide service features dynamically according to user demands or the required application features. SON service features may also be created via cooperation among the SON functional elements.

8.1 Service control

The SON service control function is required to provide:

- means for users to specify SON membership;
- accommodation of user-defined SON access schemes;
- provision of standards-based interfaces (independent of a user's device supplier);
- means to support QoS/QoE requirements as defined by the user, or as negotiated/renegotiated by the user (i.e., negotiated between the user and the service provider);
- means to meet a user's security requirements (e.g., in terms of having the option to select different levels of security);
- SON members with secure dynamic access;
- appropriate SON management services in terms of configuration, QoS/QoE, security, fault, performance, accounting, mobility and multicast support;
- accommodation for a given SON or multiple SONs.

8.2 Service composition

The service composition is a coordinated aggregate of services that delegate actions requested by the end user or service provider for the target service. For example, the service composition will create a new service via the addition of service features provided by SON elements to the existing service.

The SON service composition function is required to provide:

- support to aggregate suitable functions;
- support for the delegation actions so as to provide available services to the end user;
- support to allow service transformations when users move from one service environment to another.

8.3 Application-aware provisioning

As indicated in clause 7.2, SON manages information that is related to services and applications. SON has the capability of using information to verify and check the need to perform adaptation, in order to adapt the manner in which applications and services are provided.

The application-aware provisioning function performed in SONs is expected to:

- provide support services which can identify applications with specific application characteristics;
- provide scalability to avoid placing an upper limit on the kind of centralized control or managing functions that can be offered;
- assist in the control and/or management of services to be adapted to applications;
- classify provided media types;
- support dedicated quality of experience (QoE) parameters;
- support real-time and non-real-time services;
- provide security to prevent unauthorized access (from malicious nodes) and ensure user privacy before the service is provided to the destination.

8.4 QoS-aware provisioning

SON supports services that are requested by users by applying the appropriate QoS levels by profiling QoS requirements for each service. QoS profiles should be justified for each service according to the required QoS level. This will require the QoS-aware provisioning function to consider and react to: service environments, transport capability, QoS profile, user profile and service policy, to maintain a certain level of QoS service. All QoS profiles are to be defined by SON or delivered to SON from terminal functions in advance of the provisioning of service. The QoS-aware provisioning function performed in SONs is expected to:

- support a service to be adapted to application or service environments that require a certain level of QoS;
- gather QoS information according to the service type;
- create QoS profiles with the gathered QoS information.

QoS profiles are managed by the SON management function, which enables the service composition function to create QoS-enabled service networking. The composition results in the application support functions and service support functions via the ANI/SNI in the NGN.

The following functions are used to support QoS-aware provisioning:

- control function to keep the service level QoS;
- management function to profile and adapt the service level QoS.

Terminal devices will inform SON of the specific application and service specific requirements and profiles of QoS. A QoS-aware provisioning scenario is introduced in Appendix I.

8.5 Context-aware provisioning

The context-aware provisioning function adapts services as a result of the knowledge of the available resources near the users. The context-aware provisioning function provides the ability to acknowledge and understand the various aspects of the current service environmental status and to interact with the user in a more intelligent way. Context awareness is performed either explicitly or implicitly.

The application-aware provisioning function performed in SONs is expected to:

- gather service and user context information;
- provide services to the user according to the context information;
- differentiate between various situations, in an explicit and implicit way;
- operate and organize tailored services to the users.

8.6 Service mobility

SON provides capabilities to support service mobility by managing application and user profile adaptation to provide service consistency. SON also manages context and status information to converge profiles using the appropriate attributes. The SON service mobility management function is expected to support:

- user and application profile adaptation;
- session and service information management;
- nomadism for personal service mobility;
- support for registration, location update and user profile management to enable service mobility in SONs;
- service exchange subscriptions, identification and authentication management;
- user privacy;
- service continuity, where applicable.

8.7 Security management

SON will provide security services to identified users through collaboration among security service environments, user profile, service provider's policy and user's security information. A distinguished user will be given a secured service environment provided he/she is using the SON security management function.

The security management function performed in SONs is expected to support mechanisms for:

- controlling user access to SONs via the access control mechanisms (identification, authentication and authorization of (fixed or mobile) users accessing SONs);
- ensuring the privacy of service information being transported by SONs;
- securing key distribution;
- securing an efficient QoE negotiation;
- securing the security policies which satisfy users' and/or providers' security requirements (e.g., to adjust the configuration of SON users or SON groups, to reflect trust relationships).

Additionally, the SON security management function requires the following two mechanisms in order to support the security-aware provisioning capability:

- security-aware provisioning control;
- security-aware provisioning optimization.

The security-aware provisioning control function performs the control function according to the user's required security level. The security-aware provisioning optimization function is a capability which provides an ability to classify the optimal security level required by the users, and makes security plans for users by arranging the security functions required to support the service requested by the users. A SON security-aware provisioning scenario is introduced in Appendix II.

9 SON-based service scenarios

9.1 IPTV service scenario using SONs

SON can support, control and manage IPTV application services for users. SON is operated in an organized and coherent way by the third party service provider or by the network provider to provide customer-oriented IPTV services. SON controls and manages the service flows for user-centric service provisioning in IPTV.

The SON session control function for IPTV keeps track of session configuration for the IPTV service. In order to provide IPTV service enhancements, the SON session control function supports context-aware and community-based applications. The session control function also provides service mobility and service personalization.

The SON session control function for IPTV includes:

- topology information management;
- session mobility;
- session security.

The SON service control function is expected to support the following:

- IPTV service community creation/federations;
- user-centric service control functions;
- service personalization functions.

9.2 Community-based service scenario using SONs

In this scenario, NGN users join the community service that is built on SONs according to applications and user's requirements. Once a community is created, users in the community service will share applications in accordance with the defined SON community service capability to create community groups, e.g., security, QoS and other features suitable for the community service.

Figure 9-1 shows a scenario where community service is provided using SON. It illustrates how users can organize new community groups for their own purpose by using SON, and then how SON applies the control policy for QoS and security levels to each community group.

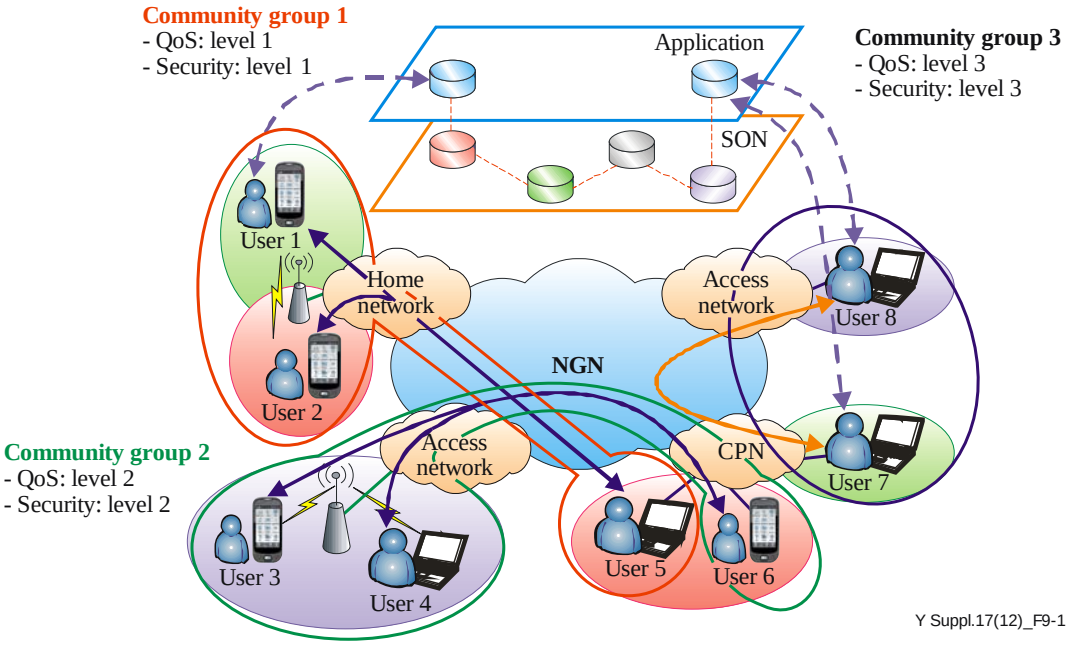

Figure 9-1 – A scenario illustrating the use of a community service with QoS and security functions using SON

In Figure 9-1, users can organize communities on SON, as needed, via the use of applications. During the establishment of the community group, the owner of the community group decides the required level of QoS and security support needed and requests that it be provided. SON provides the session configuration function according to QoS parameters and the security for each community group that is created.

A scenario that shows how QoS is supported in SON is provided in Appendix I, while a second scenario that shows how security is supported in SON is provided in Appendix II.

9.3 Virtual home network service using SON

SON, which operates in a distributed environment, interacts with other SONs to create a virtual home network environment among the members in different home network locations. The virtual home community is composed through interactions with SONs to share services in the physical home networks.

9.4 Cloud computing service provisioning using SON

A cloud computing service provider is requested to provide an entirely new level of service and efficiency from its delivery platform, to enable resources ubiquity and configurability with minimal management effort or service interaction for a rapid provisioning of service capabilities. SONs will enable end users to consume cloud-computing capabilities without any concerns about where, how, and by whom the computation is performed and where storage is provided.

For the provisioning of a complete end-user application, the SON control function delivers the results through service level agreement (SLA) negotiation, security configuration, adaptation, provisioning and integration of cloud computing services to the users. When the SON control function invokes a complex or advanced service function related to a cloud computing service, an enhanced set of service features will be provided directly to the user's terminal. SON can also provide collaboration functions with the cloud computing service environment to support user-centric computing capabilities and intelligent service functions.

SON functions can be used to create a service platform to support additional service features in cloud computing services, e.g., application-aware, context-aware and user-centric features over the NGN. The scenarios related to cloud computing services cooperating with SONs are addressed in Appendices IV and V.

Appendix I

QoS-aware provisioning in SONs

SON determines the QoS profile based on user-terminal-provided information and requested services. In order to provide a dynamic service control via the SON, SON composes a QoS-aware service based on the user's request, using the existing resource information and the QoS profile of the service. As shown in Figure I.1, SON receives the user's service request and composes a QoS-aware service in response to the request. SON enforces QoS information on the NGN via the ANI.

An example of the service procedure is as follows:

1) The user requests a service from SON.
2) SON verifies the request and applies the appropriate QoS level based on the QoS profile.
3) SON composes the service for the request and enforces the QoS level on the NGN.
4) SON delivers the request to the service provider with the composed service information via the ANI.
5) The service provider delivers the service to the user according to the QoS level composed by SON.

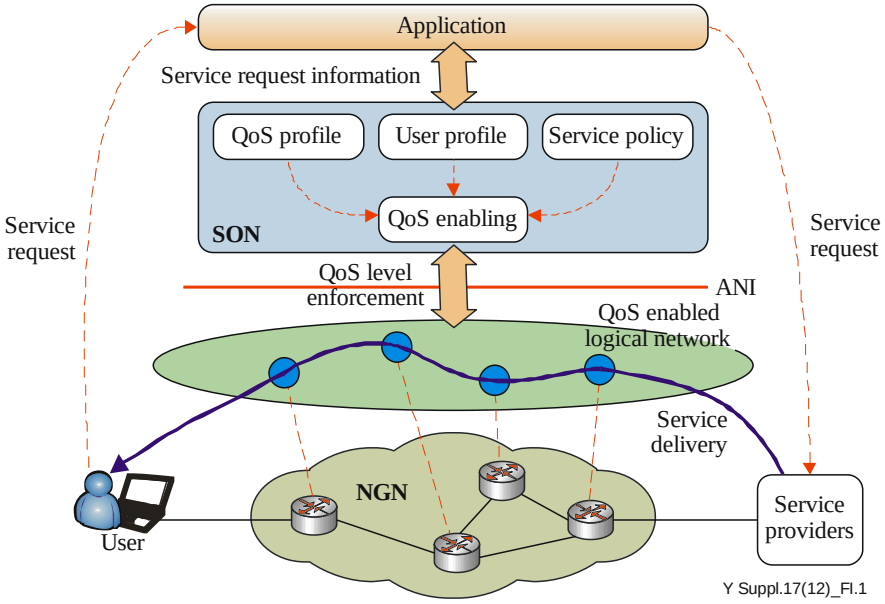

Figure I.1 – Example scenario for SON QoS-aware provisioning

Appendix II

Security-aware provisioning in SONs

Mutual authentication between SON and the NGN is used to provide authentication vectors that are computed based on the pre-shared root key. This appendix indicates how an authentication mechanism based on authentication and key agreement (AKA) can be used to provide mutual authentication for the users in a P2P-based security-aware SON, which uses the services of the NGN.

II.1 Security-aware SON scenario for authentication

This SON security-aware scenario for authentication uses the following procedure:

1) A P2P connection is constructed by all the core nodes based on distributed hash table (DHT) routing.
2) The core nodes in the DHT ring may be out of service because of overloading or other reasons.
3) Users' authentication data (such as user ID and root key K, etc.) can be stored on any core node.
4) User node A's authentication data can be stored on several core nodes at the same time (such as core node B, D and E).
5) Each core node can store connection information in the SON simultaneously.
6) SON monitors each and every core node for security purposes.
7) Each core node has the capability to determine on which core node a user's authentication data are stored, based on the user's information.
8) The user node will choose a core node (e.g., core node A) according to the specific policy to support a security-aware SON.

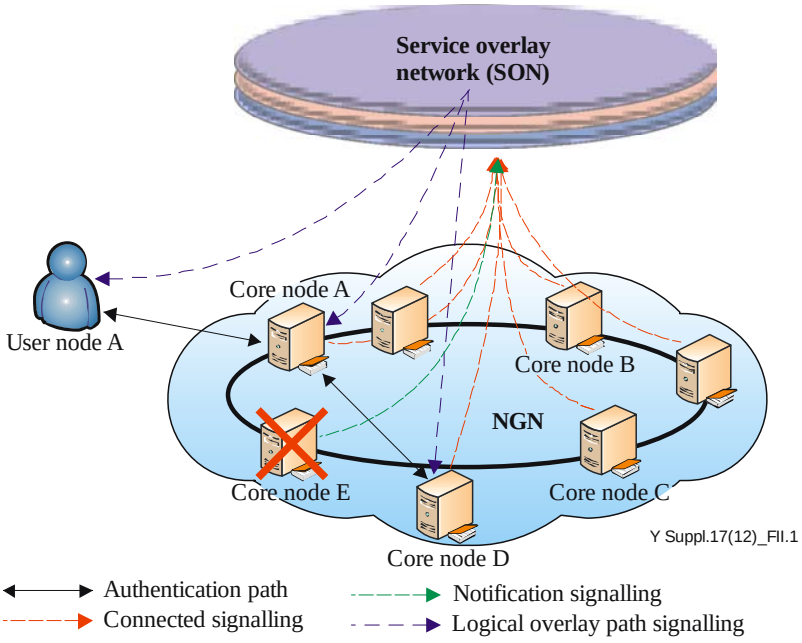

Figure II.1 – Security-aware SON scenario for authentication

II.2 Basic concept of security-aware SON for the authentication mechanism

In this scenario, when a user node needs to access the NGN, mutual authentication between the user node and NGN is executed; this method is based on AKA, which is specified in [b-3GPP TS 33.102]. As shown in Figure II.1, when user node A sends a request to SON (through core node A) to access the NGN, SON checks if user node A's authentication data are stored in SON. If it is confirmed that the data are stored there, SON will provide support to generate authentication vectors (AVs) from core node A and authentication is then executed between user node A and core node A.

If user node A's authentication data are not stored in SON, SON will search for the core node which has user node A's authentication data in the DHT routing ring (i.e., core node E in this case) and will detect whether it can provide AVs for user A. If core node E works properly, SON will check the core node status (i.e., security, connection, etc.) to generate the AVs from core node E and then send the AVs to core node A. Once this is done, authentication can be executed between core node A and user node A.

If core node E has no ability to provide AVs, the security-aware SON can notify the current connection status of the core node and will select a new core node to obtain authentication data for user node A. If core nodes cannot provide AVs for user node A, a notification will be sent to user node A from SON to announce authentication failure.

II.3 Flow diagram of security-aware provisioning in the security management function

The SON control data flows shown in Figure 7-2 do not consider security-aware services. Figure II.2 shows security-aware provisioning flows when a security management function is used to provide a security-aware service. A security-aware provisioning flow can be initiated after a service request between the application interface provisioning function and the SON control function has been sent and received.

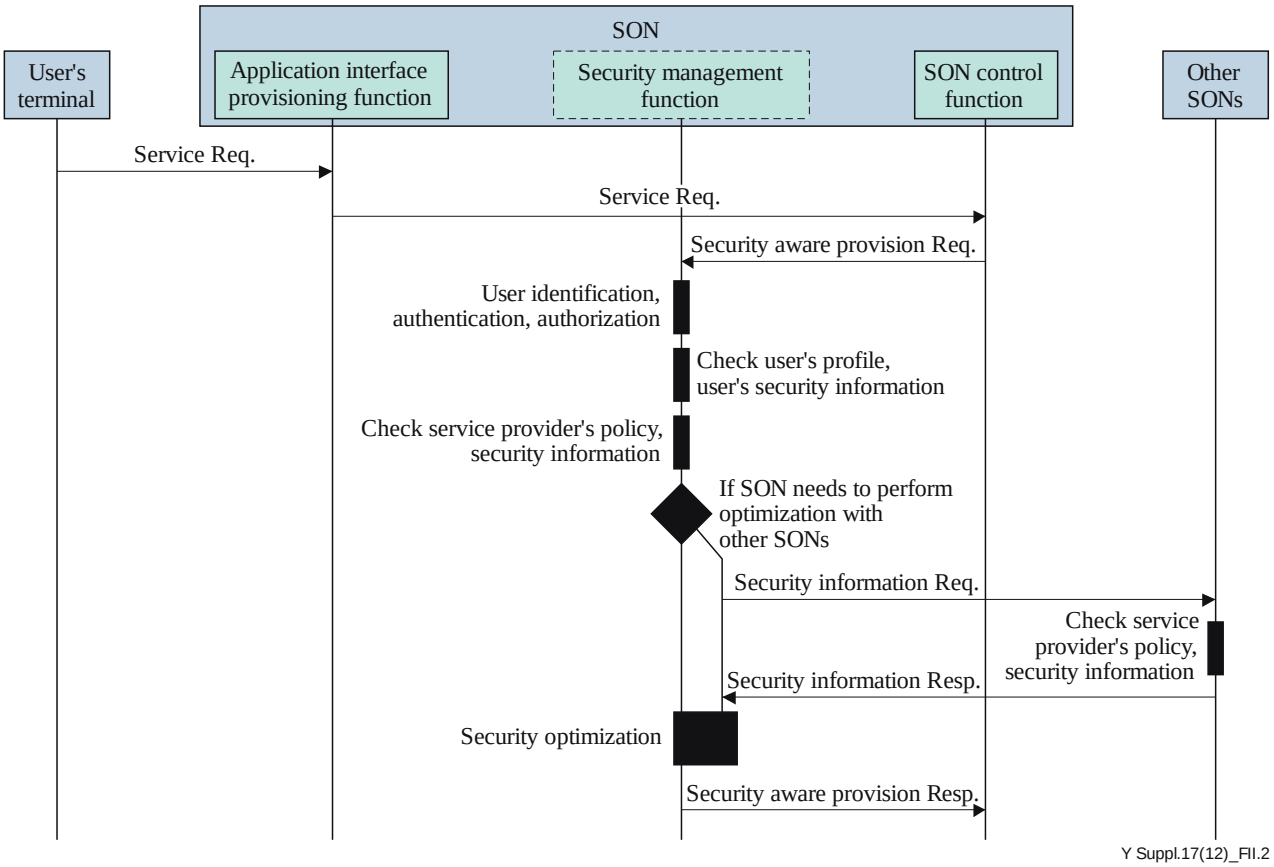

Figure II.2 – Flow diagram showing security-aware provisioning in SONs

The security-aware provisioning procedures are as follows:

1) The application interface provisioning function that receives the service request from the user's terminal sends a service request to the SON control function.

2) The SON control function sends a security-aware provisioning request to the security management function.

3) The security management function verifies the user's identification, authentication and authorization using the user's security information, and then the security management function verifies the security status such as user profile, the user's security information, the service provider's policy and security information.

4) If the security management function needs to perform optimization according, or in response, to a security status change, the security management function sends a security modification request to receive the necessary security information from other SONs.

5) The security management function, using the collected security information, performs the required security optimization function.

6) The security management function sends the information of the security-aware provisioning to the SON control function.

Appendix III

Service scenario for IPTV in SONs

SON can be used to assist IPTV service providers in configuring IPTV sessions in order to support enhanced IPTV services to end users. Typical examples of IPTV-enhanced service capabilities are personalization, context-aware and user-centric services. These features of SON are performed by providing service control functions, as shown Figure III.1.

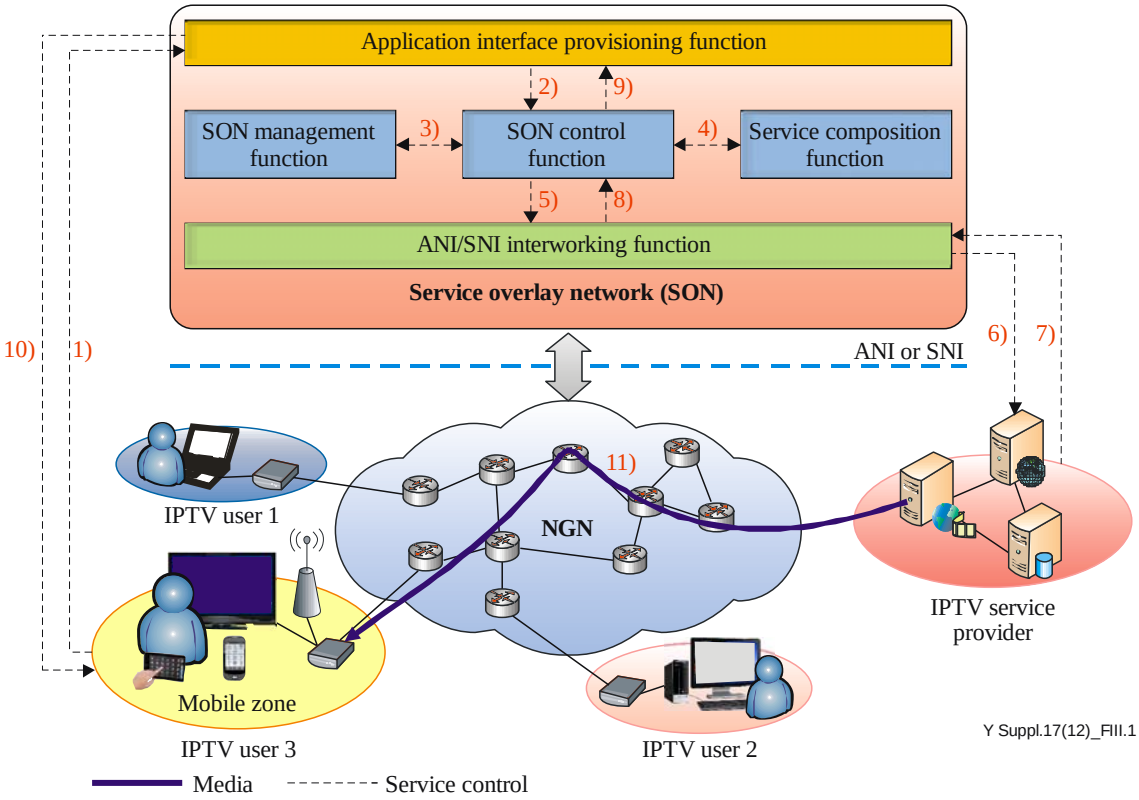

Figure III.1 – SON scenario for provisioning of IPTV services

The information flows associated with the SON IPTV service scenario depicted in Figure III.1 are as follows:

1) IPTV User 3 sends a request for IPTV service to SON.

2) The transmitted request message is then relayed by AIPF and passed on to the SON control function.

3) The SON control function requests the SON management function to authenticate and authorize the user. If the request is confirmed by the SON management function, it replies to the SON control function.

4) Based on the confirmed information from the SON management function, the SON control function requests a service composition function to create or compose a service overlay network. The service overlay network is composed by the service composition function, upon completion of the results sent to the SON control function.

5) The SON control function requests the ANI/SNI interworking function to relay the message, which enables the IPTV service provider to accept it.

6),7) The message sent from the ANI/SNI interworking function is then received by the IPTV service provider which then prepares the IPTV content to be delivered to the end user. Once the preparation has completed, the IPTV service provider notifies the ANI/SNI interworking function.

8),9) The response from the IPTV service provider is converted in such a way that SON can handle it, and the message is passed on to the SON control function. The SON control function stores the information, and then passes it on to the AIPF.

10) AIPF then responds to IPTV User 3.

11) The IPTV service provider delivers the requested IPTV content to IPTV User 3.

Appendix IV

Collaboration scenario between cloud computing services and SONs

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing services offer everything as a service (XaaS) such as software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), etc., by virtualizing the resources. An example of cloud computing architecture is shown in Figure IV.1.

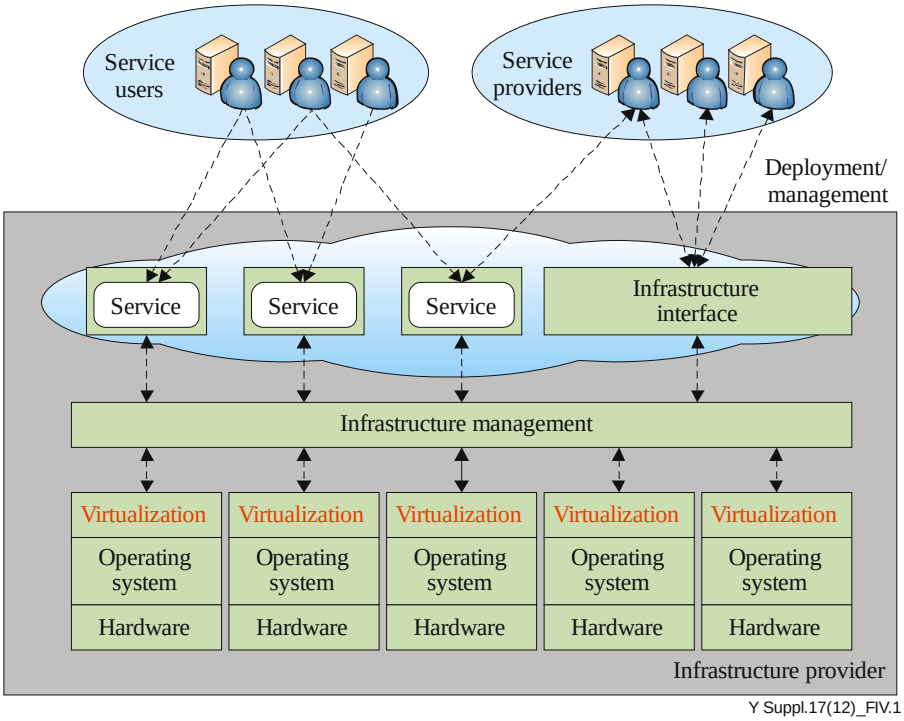

Figure IV.1 – Example of cloud computing architecture

The figure shows that virtualization of the core technology in cloud computing can be used to provide specific services to the user, thereby allowing limited computing power to be used more efficiently. It is very similar to the service provided by SON, which dynamically composes a service overlay network by using the physical resources.

SONs can cooperate with cloud computing entities to provide additional computing capability provisioning with the following characteristics:

- Dynamic provisioning and activation – Configure, start and manage applications based on schedule, policy or priority.
- Application-level fault tolerance – Transparently enable fault tolerance at the application layer, by automatically replicating and propagating state information among multiple computers.
- Horizontal scaling – Dynamically scale applications to meet SLA targets, performance metrics are tracked and triggers can activate additional application instances.
- Centralized command and control – Provides an environment that greatly simplifies the configuration and management of running multiple applications across widely distributed resources.

- Utility business model – Customers pay for the application services as a utility, with little or no upfront commitment; costs and a variety of subscription-based and non-subscription-based charging models may be offered.

Figure IV.2 shows a scenario of cloud computing service using SON.

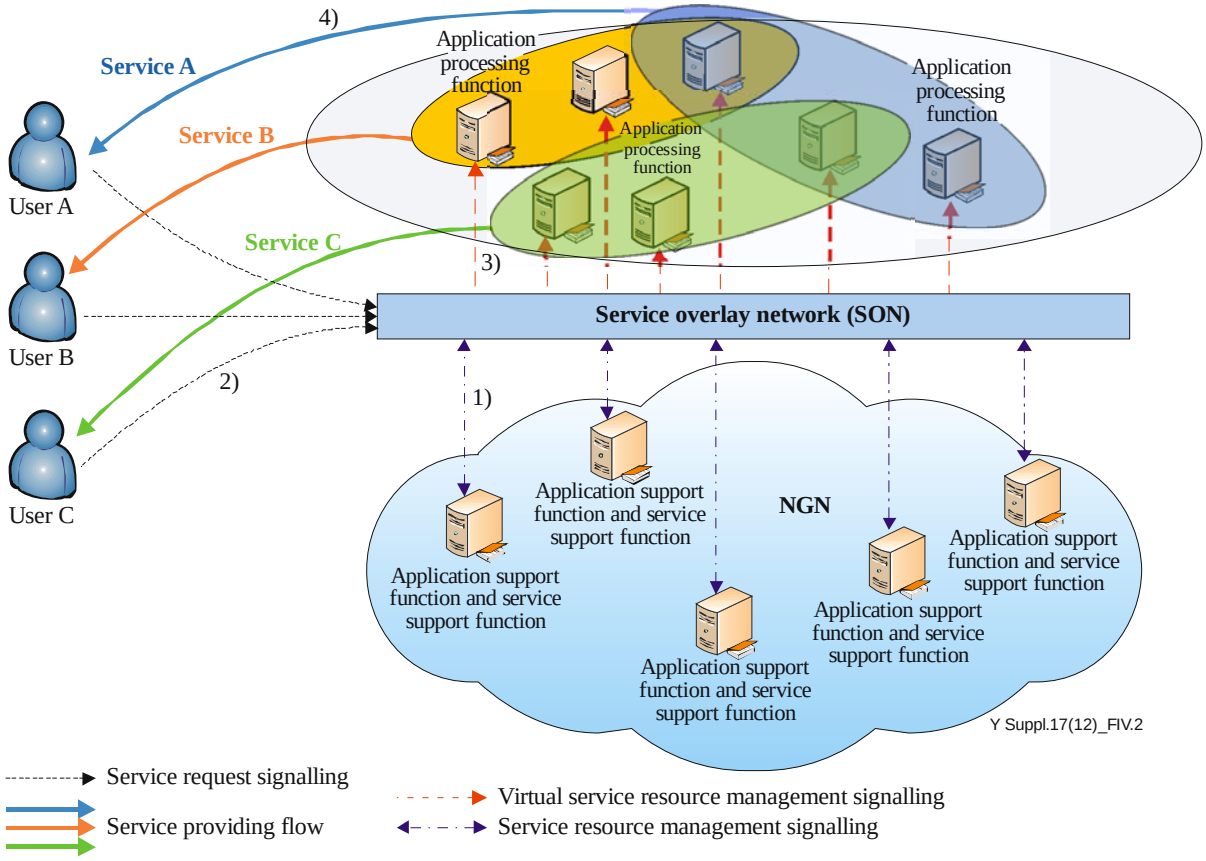

Figure IV.2 – Scenario of cloud computing service using SON

In this scenario, SON provides different cloud computing services by composing a unique service overlay network for each end user. In particular:

1) SON manages actual service resources such as hardware or operating systems to compose service overlay networks.

2) The end users request a cloud computing service from SON for applications.

3) SON creates a service overlay network through the virtualized service resources for the cloud computing service requested by the end user.

4) SON provides the cloud computing service to the end user using the virtualized service resources on the actual service resources that are distributed in the NGN.

Appendix V

Software as a service (SaaS) in cooperation with SONs

Software as a service (SaaS) is a software delivery model in which software and associated data are centrally hosted in the cloud. SaaS is typically accessed by users using a thin client via a web browser. A SaaS provider supports a software management function for companies and individual users.

SON is capable of invoking an entirely new level of service and efficiency and making it available to software vendors. Thus, SON in cooperation with SaaS will provide new business models to be developed and new technologies to be created. Similarly, SaaS in cooperation with SON enables end users to consume service capabilities without any concern about where, how and by whom the computation is performed.

Figure V.1 demonstrates the concept of SaaS in cooperation with SON.

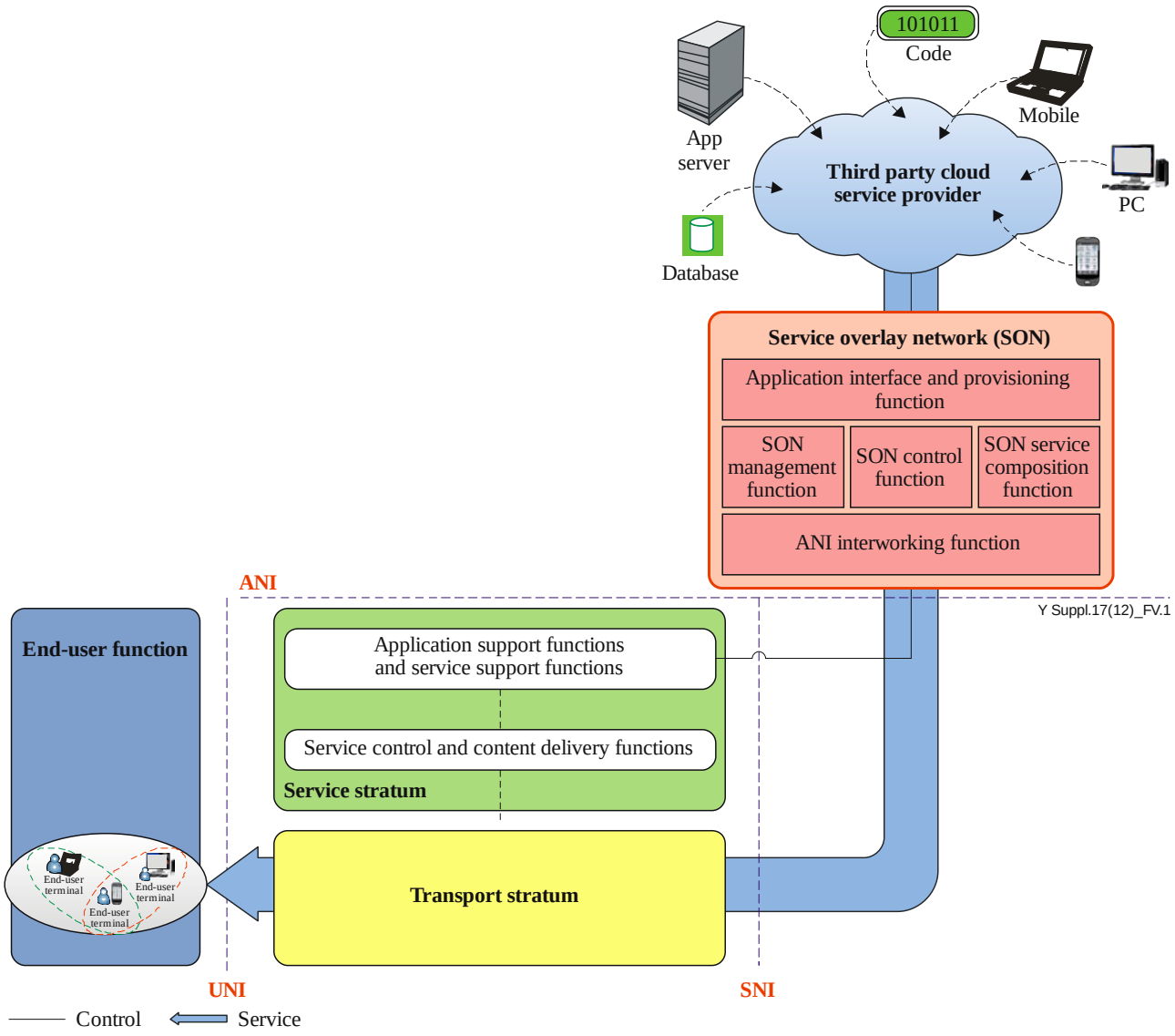

Figure V.1 – Concept of SaaS in cooperation with SON

Figure V.2 shows a functional procedure for a SaaS service scenario that uses SON. SON provides a management function to deliver a service of third party cloud service provider. The software requested through SON is delivered to an end user to perform an application service function as indicated below.

1) Application services set up a service-provisioning environment on a SON in response to a user request.

2),3) The SON interacts with a second SON to request the delivery of software to the user.

4),5) The software provided by the software vendor is stored in an application and supports components of SON.

The delivered SaaS information is managed by the SON management function, and the service composition function classifies the services based on the characteristics of the service requests such as context-aware, application-aware and QoS-aware services.

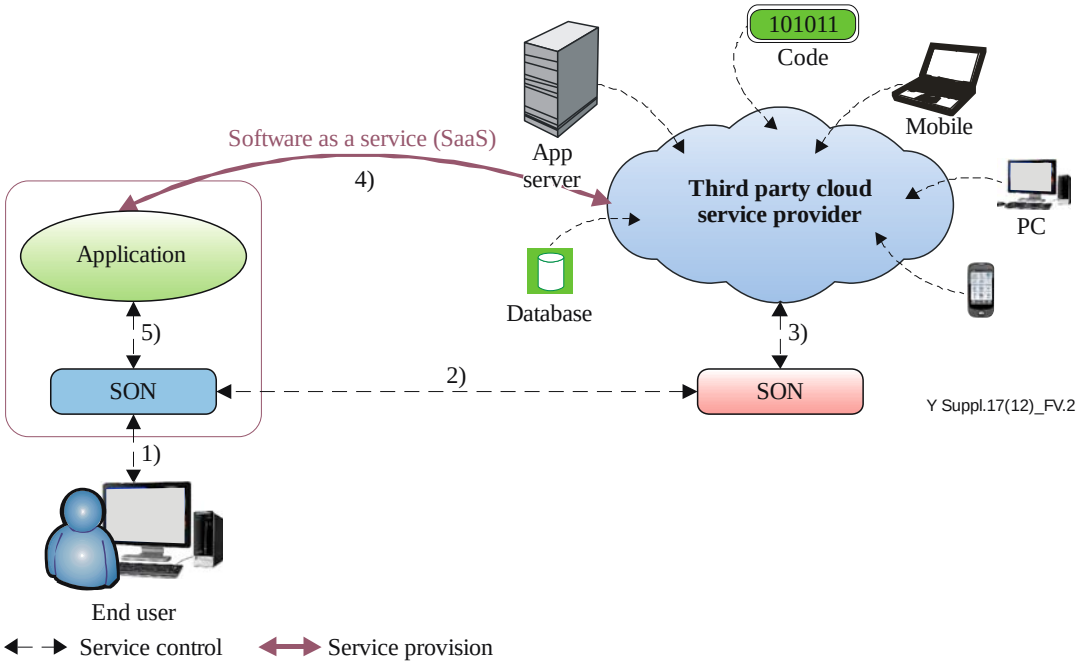

Figure V.2 – SaaS service scenario that cooperates with SON

Appendix VI

Platform as a service (PaaS) using SONs

In a platform as a service (PaaS) cloud environment, software is deployed and executed without requiring the user to think about how the infrastructure is configured.

By using SON, it becomes easier to use application features as explained below. With PaaS, developers can build web applications without installing any software tools on their computer, and then they can deploy the developed web applications without any specialized system administration skills. By using SONs, PaaS provides application platforms that can support additional application features (such as community-based applications, application-aware features and context-aware features) to NGN end users without their being aware of how the features are being provided.

For instance, (A) is a PaaS cloud provider which utilizes itself with SON services. With (A) there is little need to think about servers, operating systems, load balancers and the underlying network of an application; a developer simply pushes software (B) up to (A) in the same manner the developer would "load" a source code into a source code control system. The (A) cloud automation system picks up the software and deploys it on virtual machines fully configured with a (B) application environment that, for example, updates the load balancers and executes all the necessary steps to "just make it work". The need to understand how to configure the entire underlying network is removed – the cloud automation system using SON does that for the developer.

Additionally, a PaaS cloud automation system must have some awareness of the application and data frameworks and the ability to interact with them. For example, when new software is provided to the cloud environment, the PaaS cloud automation system may need to accept and copy that application code to new or existing application framework nodes, and it may need to update a load balancer to ensure that the needed additional application capacity is available online.

Figure VI.1 describes service flows of a PaaS cloud automation system that uses SON.

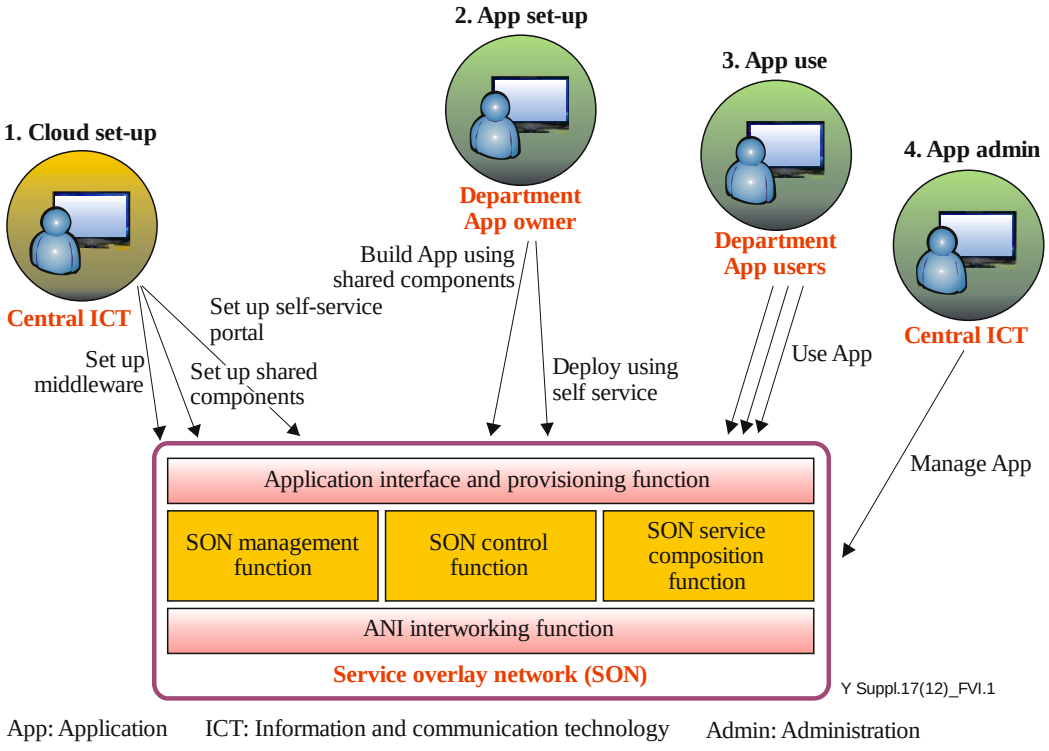

Figure VI.1 – Service flow of a PaaS system that uses SON

In this service flow example, PaaS systems using SONs have a life cycle as follows:

- Cloud set-up: set up middleware, set up shared components, set up a self-service portal through a central information and communication technology (ICT) department.
- Application set-up: build applications using the shared components, and deploy them by using the services available to the ICT department's application owner.
- Application use: use the applications provided by the ICT department's application users.
- Application administration: the central ICT manages the applications.

Bibliography

[b-ITU-T G.8012] Recommendation ITU-T G.8012/Y.1308 (2004), *Ethernet UNI and Ethernet NNI.*

[b-ITU-T I.312] Recommendation ITU-T I.312/Q.1201 (1992), *Principles of intelligent network architecture.*

[b-ITU-T J.200] Recommendation ITU-T J.200 (2010), *Worldwide common core – Application environment for digital interactive television services.*

[b-ITU-T M.3050.1] Recommendation ITU-T M.3050.1 (2007), *Enhanced Telecom Operations Map (eTOM) – The business process framework.*

[b-ITU-T P.10 Amd.2] Recommendation ITU-T P.10/G.100 Amd.2 (2008), *New definitions for inclusion in Recommendation ITU-T P.10/G.100*.

[b-ITU-T Q.1706] Recommendation ITU-T Q.1706/Y.2801 (2006), *Mobility management requirements for NGN*.

[b-ITU-T X.603] Recommendation ITU-T X.603 (2004) | ISO/IEC 16512-1:2005, *Information technology – Relayed multicast protocol: Framework.*

[b-ITU-T Y-Sup.7] ITU-T Y-series Recommendations – Supplement 7 (2008), *ITU-T Y.2000-series – Supplement on NGN release 2 scope*.

[b-ITU-T Y-Sup.10] ITU-T Y-series Recommendations – Supplement 10 (2010), *ITU-T Y.2000-series – Supplement on distributed service network (DSN) use cases.*

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

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *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.2206] Recommendation ITU-T Y.2206 (2010), *Requirements for distributed service networking capabilities.*

[b-ITU-T Y.2234] Recommendation ITU-T Y.2234 (2008), *Open service environment capabilities for 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.2261] Recommendation ITU-T Y.2261 (2006), *PSTN/ISDN evolution to NGN.*

[b-3GPP TS 33.102] Third Generation Partnership Project TS 33.102 (2000), *3G Security; Security architecture*.

[b-IEEE 1093] IEEE 1093-2011, *Standard for the Functional Architecture of Next Generation Service Overlay Networks*
<http://grouper.ieee.org/groups/ngson/>

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2013