International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3512

(08/2014)

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

Cloud Computing

Cloud computing – Functional requirements of Network as a Service

Recommendation ITU-T Y.3512

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.3512

Cloud computing – Functional requirements of Network as a Service

Summary

Recommendation ITU-T Y.3512 describes the concept of Network as a Service (NaaS) and its functional requirements. It provides typical use cases of NaaS and specifies the functional requirements of three aspects, ranging from NaaS application, NaaS platform and NaaS connectivity which are based on the corresponding uses cases and cloud capabilities types.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3512	2014-08-29	13	11.1002/1000/12285

Keywords

Cloud computing, Network as a Service, NaaS, NaaS application, NaaS connectivity, NaaS platform.

---

* 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.3512

Cloud computing – Functional requirements of Network as a Service

1 Scope

This Recommendation provides use cases and functional requirements of Network as a Service (NaaS), one of the representative cloud service categories. This Recommendation covers the following:

– High-level concept of NaaS;

– Functional requirements of NaaS;

– Typical NaaS use cases.

This Recommendation provides use cases and functional requirements of NaaS application, NaaS platform and NaaS connectivity.

NOTE – General requirements of NaaS can be found in [ITU-T Y.3501].

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 X.1601] Recommendation ITU-T X.1601 (2014), *Security framework for cloud computing*.

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

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and Vocabulary*.

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2013), *Cloud computing framework and high-level requirements*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application capabilities type [ITU-T Y.3500]: Cloud capabilities type in which the cloud service customer can use the cloud service provider's applications.

3.1.2 cloud capabilities type [ITU-T Y.3500]: Classification of the functionality provided by a cloud service to the cloud service customer, based on resource used.

NOTE – The cloud capabilities types are application capabilities type, infrastructure capabilities type and platform capabilities type.

3.1.3 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.4 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.5 cloud service category [ITU-T Y.3500]: Group of cloud services that possess some common set of qualities.

NOTE – A cloud service category can include capabilities from one or more cloud capabilities types.

3.1.6 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.7 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.8 cloud service user [ITU-T Y.3500]: Natural person, or entity on their behalf, associated with a cloud service customer that uses cloud services.

3.1.9 Communications as a Service (CaaS) [ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is real time interaction and collaboration.

NOTE – CaaS can provide both application capabilities type and platform capabilities type.

3.1.10 infrastructure capabilities type [ITU-T Y.3500]: Cloud capabilities type in which the cloud service customer can provision and use processing, storage and networking resources.

3.1.11 logically isolated network partition [ITU-T Y.3011]: A network that is composed of multiple virtual resources which is isolated from other LINPs.

NOTE – Term "logically isolated", which is the counter concept of "physically isolated", means mutual exclusiveness of the subjects (e.g., network partition, in this case), while the original subjects may be physically united/shared within the common physical constraints.

3.1.12 Network as a Service (NaaS) [ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

NOTE – NaaS can provide any of the three cloud capabilities types.

3.1.13 platform capabilities type [ITU-T Y.3500]: Cloud capabilities type in which the cloud service customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the cloud service provider.

3.1.14 tenant [ITU-T Y.3500]: Group of cloud service users sharing access to a set of physical and virtual resources.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 service chain: An ordered set of functions that is used to enforce differentiated traffic handling policies for a traffic flow.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BGP Border Gateway Protocol

BoD	Bandwidth on Demand
BSS	Business Support System
CaaS	Communications as a Service
CDN	Content Delivery Network
CPE	Customer Premises Equipment
CSC	Cloud Service Customer
CSP	Cloud Service Provider
CSU	Cloud Service User
DNS	Domain Name System
DPI	Deep Packet Inspection
EPC	Evolved Packet Core
GW	Gateway
HQ	Headquarter
IaaS	Infrastructure as a Service
IDE	Integrated Development Environment
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPS	Intrusion Protection System
IPsec	IP security
L2	Layer 2
L3	Layer 3
LAN	Local Area Network
LINP	Logically Isolated Network Partition
MAC	Medium Access Control
MEF	Metro Ethernet Forum
MEN	Metro Ethernet Network
MPLS	Multi-Protocol Label Switching
NaaS	Network as a Service
NNI	Network-to-Network Interface
NOS	Network Operating System
OSS	Operations Support System
QoE	Quality of Experience
QoS	Quality of Service
P2P	Peer-to-Peer
PaaS	Platform as a Service
PoP	Point of Presence
SaaS	Software as a Service

SAL	Software Abstraction Layer
SDN	Software Defined Networking
SLA	Service Level Agreement
SSL	Secure Socket Layer
UNI	User-to-Network Interface
vCDN	virtual Content Delivery Network
vDPI	virtual Deep Packet Inspection
vEPC	virtualised Evolved Packet Core
vFW	virtual Firewall
vRouter	virtual Router
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
VoIP	Voice over IP
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network

5 Conventions

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

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

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

In the body of this Recommendation and its annexes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative is to be interpreted as having no normative intent.

6 General description

6.1 Networking challenges in cloud computing

There are several challenges to build an efficient and reliable network application and infrastructure to provide cloud services. Having both compute, storage and network capabilities may face the following challenges:

- Coordination of compute and storage virtualization with network capabilities

  Compute and storage performance challenges in cloud computing systems are successfully solved using virtualization as a core technique. Server virtualization introduced virtual

machines' (VMs) dynamic and static migration, which imposes demands on the networking environments. Network is expected to provide suitable and flexible support for highly variable cloud applications, when they run inside complex and diverse system architecture. In such system it is possible to provide the compute and storage resources, but it is also expected to dynamically provide the necessary networking support required to assure overall system performance, reliability and quality of service (QoS) demands.

- Harmonized control of heterogeneous network technologies

  Due to the increasing geographical distribution of cloud computing systems several network technologies can be utilised to assure end-to-end connectivity. It is expected that support of efficient control mechanisms for heterogeneous network technologies be provided.

- On-demand reconfiguration

  Cloud computing system allows for dynamic computing and storage resources reconfiguration or migration to meet the changing requirements. It is desirable that networks provide on-demand reconfiguration to satisfy the requirements of cloud services, e.g., change of bandwidth, modification of network topology or addition of new network elements.

6.2 High-level concept of NaaS

As defined in [ITU-T Y.3500], Network as a Service (NaaS) is a category of cloud services in which the capability provided to the cloud service customer (CSC) is transport connectivity and related network capabilities in order to solve the challenges mentioned above. NaaS services are divided into NaaS application service, NaaS platform service and NaaS connectivity service. In particular, NaaS connectivity service is an "infrastructure capabilities type" service limited to networking resources.

The high-level concept of NaaS using the layering framework defined in [ITU-T Y.3502] is illustrated on Figure 6-1.

NaaS can provide any of the three cloud capabilities identified in [ITU-T Y.3500] as follows:

- **NaaS application**: application capabilities type of service where NaaS CSC can use network applications provided by NaaS cloud service provider (CSP). These network applications are considered and used as a virtual network functions provided by NaaS CSP. This includes any network function for either fixed or mobile or both core and access as well as for control and forwarding planes network elements. Examples of NaaS applications include virtual router, virtual content delivery network (vCDN), virtualised evolved packet core (vEPC) and virtual firewall (vFW).

  In this category, CSP offers a set of interfaces for network functionalities.

- **NaaS platform**: platform capabilities type of service where NaaS CSC can use the network platform provided by NaaS CSP. The NaaS platform offers one or more software execution environments and one or more programming languages to deploy, manage and run customer-created or customer-acquired network applications. Such network applications can be created or acquired by CSC as self-implemented network services. Network applications can implement various network functionalities or services, e.g., router, firewall, load balancer, as well as groups of network functionalities. Groups of network applications and functionalities can form an integrated network solution.

  In this category, CSP offers a programmable environment for network functionalities that can be employed by cloud service customer or cloud service partner software.

- **NaaS connectivity**: infrastructure capabilities type of service where NaaS CSC can provision and use networking connectivity resources provided by NaaS CSP. This includes for example flexible and extended virtual private network (VPN), bandwidth on demand (BoD), etc. NaaS can provide basic networking functionalities such as connectivity, using whatever physical, logical or virtual networking capabilities the CSP chooses to offer. There is often a desire to

offer more than IP networking. For example, a CSC may wish for elastic, on-demand control of optical networks, or even for access to dark fibre using photonic switching.

In this category, CSP offers network connections between two or more endpoints, which may include additional network functionalities.

NOTE 1 – The creation, control, management and removal of NaaS connectivity is performed as a cloud service.

NOTE 2 – NaaS typically provides "bearer" connectivity of raw data without regard to the type of data carried between endpoints. Services that are specific to a type of carried data, such as telephony, voice over IP (VoIP), video conferencing, and instant messaging, are typically categorised as Communications as a Service (CaaS).

NOTE 3 – The endpoints of NaaS connectivity can reside either within the NaaS service interface itself, in another cloud service, in a non-cloud service or at a traditional network endpoint.

NaaS services can be utilized by both cloud and non-cloud services.

Network capabilities can be delivered through any combination of the three types of cloud capabilities. In particular, network capabilities could support cloud computing in aspects of interconnection of the CSP and the CSC, topology and route related functionality to share topologies, discovery related functionality to perform other services needed by inter-cloud related activities as well as other functionalities related to monitoring, protection, verification, etc.

Network functionality can be provided as a composite NaaS service where the NaaS service consists of more than one network functionality services. Hierarchically nested NaaS composite services can also be provided. Composite NaaS services could apply for different NaaS capabilities types provided to CSC according to the performance objectives expressed in the service level agreement (SLA).

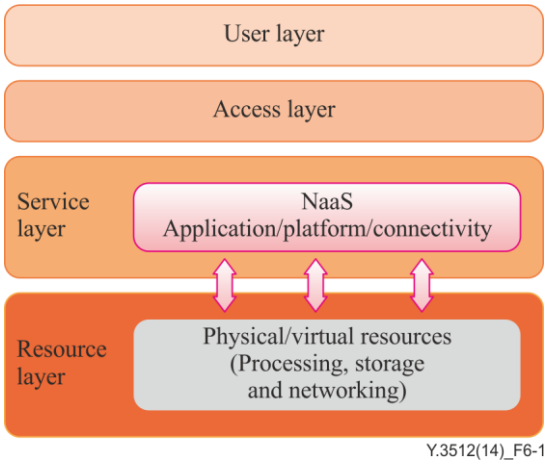


Figure 6-1 – High-level concept of NaaS

Appendix II provides NaaS use cases in which the three cloud capabilities types (i.e., application, platform and infrastructure capabilities) are provided to the CSC.

Appendix III provides considerations on the CSP's network related activities.

NOTE 4 – Regarding the network connectivity, one important difference between Infrastructure as a Service (IaaS) and NaaS is that IaaS is a cloud service category that is offered in only one flavour of cloud capability type, and that is infrastructure capabilities type [ITU-T Y.3500]. However, NaaS is a cloud service category that can be offered in all three cloud capabilities types.

7 Functional requirements of NaaS application

This clause provides requirements of NaaS application derived from the use cases described in Appendix II.

7.1 Performance

– NaaS application performance is recommended to be manageable to satisfy the CSC's needs.

– It is recommended that NaaS CSP monitors the utilization and delivery performance of NaaS application.

– NaaS application is recommended to be provided to the CSC according to the performance objectives expressed in the SLA.

7.2 Operation and management

– The operation of NaaS application is required to be manageable and deterministic in accordance with the CSP operational policies.

– It is recommended that each NaaS application be managed by NaaS CSP efficiently and automatically, complying with the CSP's common framework of service management and service operation management.

– It is recommended the NaaS CSP provide the CSC with an efficient management solution of provisioned NaaS applications allowing to integrate the management of the provisioned NaaS applications into the CSC's network operation environment.

7.3 Service chain

– It is recommended that NaaS CSP provides mechanisms allowing for the chaining of NaaS applications, e.g., the required NaaS applications components and associated order.

7.4 Multiple IP addresses

– It is recommended that NaaS application support multiple IP addresses on a network interface when it delivers network appliance functions (such as firewalls, load balancers).

NOTE – This requirement is also applicable to NaaS platform and NaaS connectivity.

8 Functional requirements of NaaS platform

This clause provides requirements of NaaS platform derived from the use cases described in Appendix II.

8.1 Programmable NaaS platform

– It is recommended that NaaS CSP supports deployment of network applications on NaaS platform by both the CSP and the CSC.

– It is recommended that NaaS platform provides hardware or software modules specialized for network function acceleration.

– It is recommended that NaaS platform assures and indicates performance available to the CSC's applications which are running on it.

– It is recommended that NaaS platform service provides a modular software framework to select and integrate networking functions, security functions and third party applications.

– It is recommended that NaaS CSP provides platform support for the CSC to manage (e.g., install, upgrade or uninstall) CSC owned modules.

– It is recommended that NaaS platform provides network enablers for the CSC to initiate (e.g., design, build, manage) and operate the flexible, scalable, functionally expandable networks.

– It is recommended that NaaS platform provides a unified control and management function over distributed NaaS platforms for the CSC to change, move, or remove network enablers between NaaS platforms.

8.2 Dynamic and flexible network services composition and steering

– It is recommended that NaaS CSP steers the CSC's traffic via service chain which is dynamically and flexibly composed by customized sequences of NaaS applications on the NaaS platform according to the CSC's specific service logic.

8.3 Isolation of service chains for tenants

– NaaS CSP can optionally support isolation of service chains for tenants, combining different network services, implemented on the NaaS platform.

8.4 Flexible scaling of NaaS platform

– It is recommended that NaaS CSP assures flexible scaling of the resources assigned to the NaaS platform to achieve performance objectives of the network services and applications implemented on the Naas platform.

NOTE – This requirement is to meet the changes in services or applications utilization caused by e.g., growth of traffic, change in number of users, adding new services, implementing new applications.

8.5 Integration of software applications

– It is recommended that NaaS CSP supports integration of software applications deployed on the NaaS platform by either the CSP or the CSC, or both, to allow building of the combined solutions.

9 Functional requirements of NaaS connectivity

This clause provides requirements of NaaS connectivity derived from the use cases described in Appendix II.

9.1 Common control mechanism for NaaS connectivity

– It is recommended that the NaaS connectivity control mechanism provided by the NaaS CSP supports the negotiation of connectivity parameters (such as interface characteristics, connection endpoints, IP version support, QoS, L3/L2VPN type, connectivity extension approach (e.g., clause 10 of [b-IETF RFC 4364], routing information (e.g., border gateway protocol (BGP) route target).

– It is recommended that NaaS CSP provides a common NaaS connectivity control mechanism allowing identified NaaS connectivity to be provided in a secure and QoS guaranteed manner.

– It is recommended that the NaaS connectivity control mechanism is able to cope with potentially different CSC identification schemes used on the NaaS CSP side and on the connected endpoint.

– NaaS CSP can optionally provide isolated connectivity for the network tenants.

9.2 Unified SLA for multiple optimized networks

– It is recommended that NaaS CSP provides network connectivity services using unified SLA for CSC's management of multiple optimized networks in order to simplify and unify the control and management of networks.

NOTE – This mechanism allows the CSP to create and add new features to their networks to provide high quality services which can meet CSC's differentiated requirements.

– It is recommended that composite NaaS services policy should be expressed in the SLA.

NOTE 1 – NaaS service can be a composite service, where the service consists of more than one NaaS service.

NOTE 2 – This requirement is also applicable to the NaaS application and the NaaS platform.

9.3 Leveraging transport networks dynamically

– It is recommended that NaaS CSP leverages transport networks dynamically from multiple choices of physical and virtual networks for the purpose of providing network connectivity services, such as recovery, BoD, QoS guarantee, etc.

NOTE – The transport networks can be heterogeneous in terms of technology and administrative domain.

9.4 Unified network control mechanism

– It is recommended that NaaS CSP provides a unified control mechanism for the end-to-end NaaS connectivity given to a CSC.

NOTE – NaaS connectivity could be provided either by multiple heterogeneous networks or by a network employing one or more NaaS platforms or applications, which perform(s) network functions.

9.5 Elastic network reconfiguration

– It is recommended for the CSP to provide the elastic network reconfiguration in order to match the computing and storage elasticity and to maintain service continuity.

9.6 Seamless and end-to-end solution of bandwidth allocation

– It is recommended that NaaS CSP provides seamless and end-to-end solution of bandwidth allocation independent of network technology and architecture.

9.7 Symmetric or asymmetric capacity

– It is recommended that NaaS CSP provides symmetric or asymmetric network link capacity based on the CSC's demand.

9.8 Optimized and fine-grained traffic engineering

– It is recommended that NaaS CSP provides the CSC with fine-grained view on usage of network resources.

– It is recommended that NaaS CSP collects near real time utilization metrics and topology data from its own network equipment.

– It is recommended that NaaS CSP controls the network resource allocation by reconfiguring network profiles as well as properties (e.g., topology, bandwidth) in response to dynamically changing traffic demands.

– NaaS CSP can optionally provide centralized traffic management to achieve optimized traffic engineering.

9.9 Coexistence with legacy network services and functions

– It is recommended that NaaS CSP avoids or mitigates possible performance and flexibility impacts when introducing new network connectivity services.

– It is recommended that NaaS CSP supports coexistence of new network connectivity services with legacy systems.

9.10 Centralized control view and abstraction view of resources

– NaaS CSP can optionally support logically centralized management and control view of the network resources.

– NaaS CSP can optionally provide to the CSC an abstraction view of the underlying network resources.

9.11 CSC limited control of services

– It is recommended that NaaS CSP provides to the CSC appropriate services control in order to respond to the time-sensitive performance requirements, including bandwidth quantities, maximum latencies and other QoS parameters.

9.12 Logically isolated network partition

– NaaS CSP can optionally implement logically isolated network partition (LINP).

NOTE – LINP is described in [ITU-T Y.3011]. See clause 3.1.14.

9.13 Overlay network mechanism

– NaaS connectivity can optionally support virtual overlay networks on top of the physical underlay network.

9.14 Overlapped private IP addresses

– It is recommended that NaaS CSP allows different CSCs to use their own private IP addresses even when the subnet addresses are overlapped.

9.15 Interworking among different VPN solutions

– It is recommended that NaaS CSP supports interworking among different VPN technologies.

9.16 VPN connection in mobile environment

– It is recommended that NaaS CSP supports VPN connectivity in mobile environment.

9.17 Connection to NaaS CSP's network through public Internet

– It is recommended that NaaS CSP allows the CSC to connect to the NaaS CSP through the public Internet.

10 Security considerations

Security aspects for consideration within cloud computing environments, including NaaS, are addressed by security challenges for the CSPs, as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet security challenges.

Appendix I

Development methodology of NaaS functional requirements and architecture

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

Considering the standardization methodology and conventional study sequence, the abstractions of functional entities and their mutual interactions are based on the functional requirements and the corresponding use cases analysis, which form a standardization body together. Therefore, it is required to progress NaaS functional requirements and architecture according to the following steps and priorities.

Step 1: Use cases and functional requirements of NaaS which are included in Appendix II and clauses 7-9, respectively, of this Recommendation. Note that all the functional requirements are derived from the corresponding use cases.

Step 2: Functional architecture of NaaS should be based on this Recommendation.

Additionally, the general requirements of NaaS are described in [ITU-T Y.3501].

Appendix II

Use cases of NaaS

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

This appendix includes three types of NaaS use cases: NaaS application related use cases, NaaS platform related use cases and NaaS connectivity related use cases. Each type of NaaS use case is further divided into general and detailed use cases.

II.1 Use case template

The use cases developed in Appendix II should adopt the following unified format for consistent readability and convenient material organization.

Title	Title of the use case
Description	Scenario description of the use case
Roles	Roles involved in the use case
Figure (optional)	Figure to explain the use case, but is not mandatory
Pre-conditions (optional)	The necessary pre-conditions that should be achieved before starting the use case.
Post-conditions (optional)	The post-condition that will be carried out after the termination of current use case.
Derived requirements	Requirements derived from the use cases, whose detailed descriptions are presented in the dedicated clauses.

II.2 NaaS applications related use cases

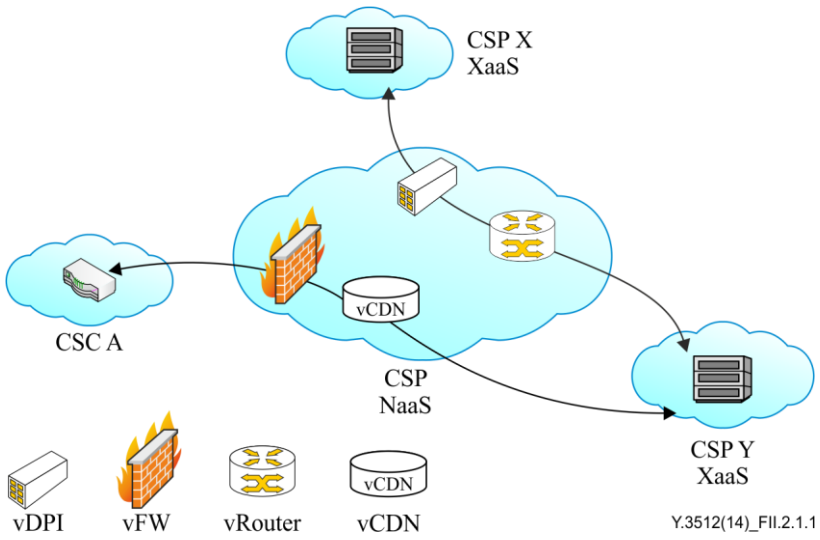
This clause provides description of use cases related where NaaS CSC can provision and use network applications.

NOTE – In the following clauses, XaaS represents any categories of cloud services such as Software as a Service (SaaS), Platform as a Service (PaaS), IaaS, CaaS, etc.

II.2.1 General use cases

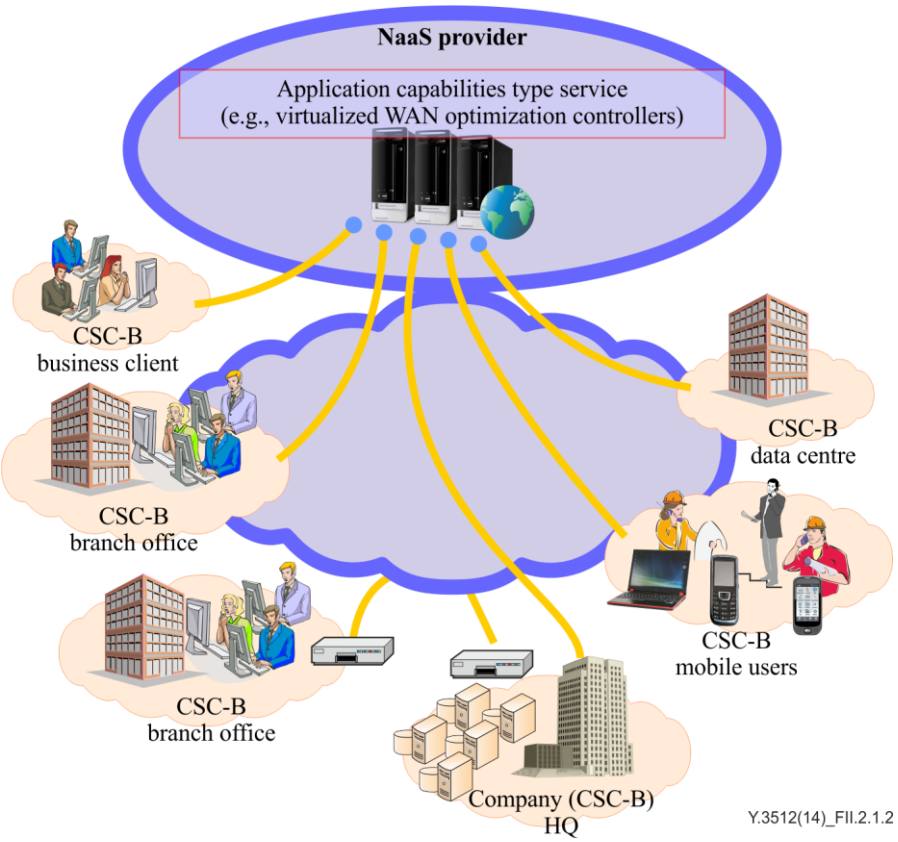
II.2.1.1 General NaaS application use case

Name	General NaaS application use case
Description	A XaaS CSC or XaaS CSP uses the network applications (e.g., virtual DPI (vDPI), vFW, vCDN) provided by NaaS CSP. These network applications can be chained by NaaS CSP.
Roles	CSC, CSP

Figure	 NOTE – Virtual router (vRouter) can also be applicable to NaaS connectivity.
Pre-conditions (optional)	– There is connectivity between XaaS CSC A and XaaS CSP Y. – There is connectivity between XaaS CSP X and XaaS CSP Y. – Either the XaaS CSP or the CSC requests a network application (vFW, vCDN, vDPI, vRouter etc.) to be chained with the connectivity.
Post-conditions (optional)	– NaaS CSP offers network applications for the XaaS CSC/CSP over existing network connectivity.
Derived requirements	– On-demand virtual network application – Scalable network application – Chain of network applications – QoS-guaranteed applications – Secure network applications – Resilient network applications – Multiple IP addresses (refer to clause 7.4) NOTE – The first six requirements belong to general requirements of NaaS which are provided in [ITU-T Y.3501].

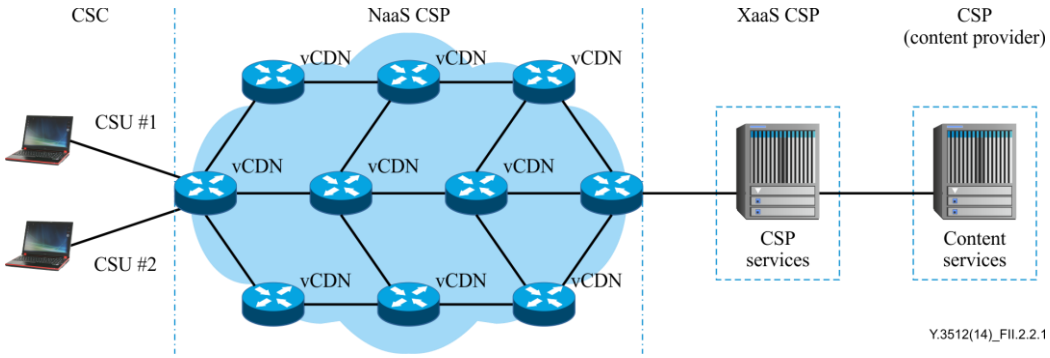
II.2.1.2 NaaS application use case for application provision

Title	NaaS application use case for application provision
Description	Assume that company CSC-B looks for NaaS application services to benefit from key characteristics of the cloud computing services. As an example, the company wants to accelerate network traffic saturated with business applications. Wide area network (WAN) optimization is very crucial for the success of its business applications. CSC-B wants usage-based deployment of WAN optimizations and flexible feature support on-demand. Traditional WAN optimization appliance devices cannot fulfil those requirements, in particular, in terms of total cost of ownership and deployment elasticity. NaaS CSP needs to provide virtual WAN acceleration solution to CSC-B, coping with its dynamic business needs.
Roles	CSP, CSC

Figure (optional)	
Pre-conditions (optional)	CSC-B needs to accelerate network traffic saturated with business applications.
Post-conditions (optional)	CSC-B used virtual WAN acceleration solution provided by NaaS CSP to satisfy the dynamic business needs.
Derived requirements	– On-demand self-service – Multi-tenancy – Resource pooling – Rapid elasticity and scalability – Measured service – Performance assurance and monitoring – Co-existence and compatibility with CSC's legacy network equipment – Interoperability support for management and orchestration – Security and resilience – Performance (refer to clause 7.1) – Operation and management (refer to clause 7.2) NOTE – The first nine requirements belong to general requirements of NaaS which are provided in [ITU-T Y.3501].

II.2.2 Detailed use cases

II.2.2.1 NaaS platform use case for cloud CDN

Title	NaaS platform use case for cloud content delivery network (CDN)
Description	Content provider acting as CSC stores the content in the data centre and monitors the usage of the content. When the usage of the content reaches certain level of popularity or if according to some predictions content provider expects a growth of popularity in a defined period of time, e.g., video transmission of a sport event, content provider creates a virtual CDN to temporarily move the content from the data centre to the network (vCDN). XaaS CSP receives the content from the content provider (which can itself create a distribution service). Content is delivered to the cloud service users (CSUs) from XaaS CSP data centre using the network of NaaS CSP. The XaaS CSP offers the possibilities to store the content and to monitor usage parameters. XaaS CSP in cooperation with the NaaS CSP can duplicate the content in the network nodes, building a virtual CDN service. Basically XaaS CSP supports CDN functions, thus CDN is in some way "emulated" by the XaaS CSP, which cooperates with the NaaS CSP.
Roles	CSU, CSC, CSP
Figure (optional)	
Pre-conditions (optional)	– Content provider acting as CSC stores the content in XaaS CSP data centres. – Content provider acting as CSC monitors the use of content.
Post-conditions (optional)	– XaaS CSP offers the virtual CDN service using network resources of the NaaS CSP. – Content provider acting as CSC decides to move content from the data centre to the virtual CDN for a defined period of time.
Derived requirements	– Performance (refer to clause 7.1) – Operation and management (refer to clause 7.2) – Service chain (refer to clause 7.3)

II.3 NaaS platform related use cases

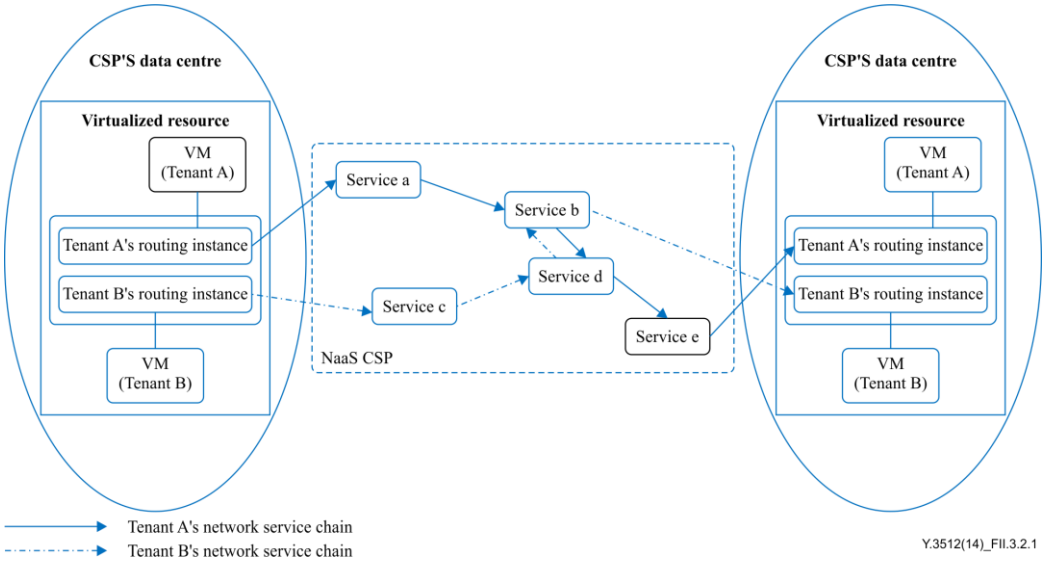
II.3.1 General use cases

None.

II.3.2 Detailed use cases

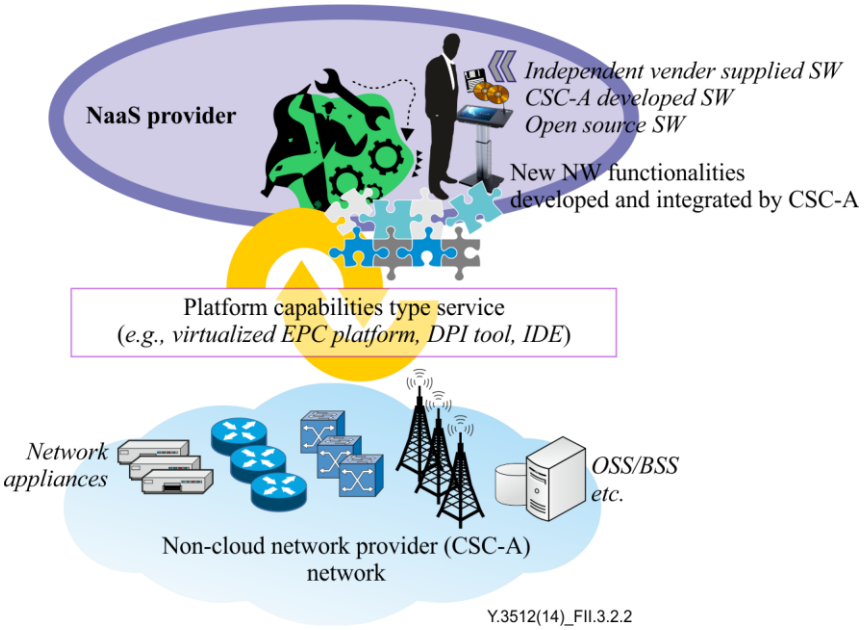
II.3.2.1 NaaS platform use case for service chain

Title	NaaS platform use case for service chain
Description	With CSC's tenants increasing requirements on the service diversity and complexity, CSP needs to deliver integrated network application services, such as deep packet inspection (DPI), intrusion detection, intrusion prevention, load balance, firewall, etc. Traditionally, the set of services are provided using dedicated physical network elements, which have limited network capacity and functionalities, complex configuration and update, and lengthy provision period. The situation, when the output of one service is used as input for the other service is called service chain. In traditional network the set-up of services chain, e.g., chain composed of intrusion protection

	system (IPS), load balancer and DPI, needs dedicated configuration and is not flexible in case of e.g., growth of traffic, adding/removing services to/from the chain. For the better service flexibility, it is recommended for NaaS CSP to provide programmable NaaS platform, on which NaaS applications such as vRouter, vCDN, vEPC, etc. can be deployed, in order to steer the CSC's traffic via customized NaaS applications sequence.
Roles	CSC (Tenant A, Tenant B), CSP
Figure (optional)	
Pre-conditions (optional)	– CSP can deliver dedicated physical network appliances solutions for services, such as DPI, intrusion detection, intrusion prevention, load balance, firewall, etc.
Post-conditions (optional)	– CSP can provide composed either virtual or physical network services or both, or services chains dynamically and flexibly according to the CSC's specific service logic in a shorter deployment, configuration, and update intervals, compared with dedicated physical network appliances solution.
Derived requirements	– Programmable NaaS platform (refer to clause 8.1) – Dynamic and flexible network services composition and steering (refer to clause 8.2) – Isolation of service chains for tenants (refer to clause 8.3)

II.3.2.2 NaaS platform use case for platform provision

Title	NaaS platform use case for platform provision
Description	CSC-A is a network operator. CSC-A wants to build advanced traffic analysis system and multi-dimensional reporting using dynamically scaling DPI functionalities, opportunistic services at low risk, and in short time of implementation, multi-tenant CDN, etc., in mobile networks. However, classical proprietary hardware-based network appliances inhibit the rapid roll out of new converged network functionalities and revenue earning services. They neither scale on-demand nor are flexible enough. CSC-A has the possibility to cope with its business innovation needs by developing necessary features and services using NaaS platform. Innovating using NaaS platform allows it to utilize CSP network services and combine them with the functionalities developed by CSC-A. All functionalities can be integrated by CSC-A on the basis of NaaS platform to build enhanced network services e.g., virtualized evolved packet core (EPC), software-based DPI platform, integrated development environments (IDEs). The capacity of NaaS platform needs to scale elastically according to the utilization of enhanced network services to secure the required performance. Solutions to support

	integration of the CSP network services with the CSC-A's developed software are also needed.
Roles	CSP, CSC
Figure (optional)	
Pre-conditions (optional)	CSC-A needs to build enhanced network services using dedicated hardware equipment for each functionality and manage the whole network.
Post-conditions (optional)	CSC-A used NaaS platform to combine CSP network services with self-developed functionalities and integrate them into enhanced network services.
Derived requirement	– Flexible scaling of NaaS platform (refer to clause 8.4) – Integration of software applications (refer to clause 8.5)

II.4 NaaS connectivity related use cases

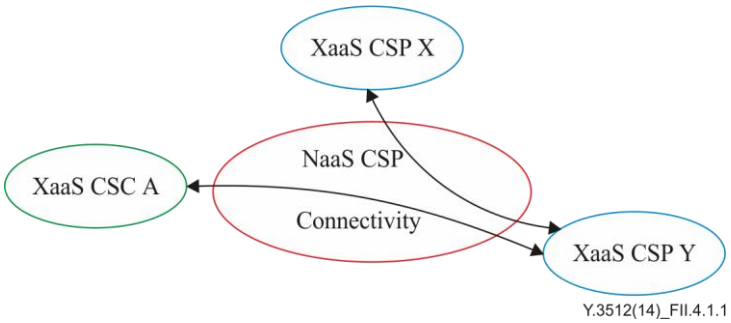
This clause provides description of use cases where NaaS CSC can provision and use network connectivity.

II.4.1 General use cases

II.4.1.1 General NaaS connectivity use case

NOTE – The following use case is based on a use case provided in [ITU-T Y.3501].

Name	General NaaS connectivity use case
Description	A NaaS CSP sets up, maintains and releases the network connectivity between CSCs and between the CSP and the CSC as a cloud service. This can include on-demand and semi-permanent connectivity.
Roles	CSC, CSP

Figure	
Pre-conditions (optional)	– There is no connectivity between XaaS CSC A and XaaS CSP Y. – There is no connectivity between XaaS CSP X and XaaS CSP Y. – Either XaaS CSC A or XaaS CSP Y requests the connectivity between them with their end-point identifiers and associated characteristics (referring to QoS and security aspects) for the connectivity. – Either XaaS CSP X or XaaS CSP Y requests the connectivity between them with their end-point identifiers and associated characteristics (referring to QoS and security aspects) for the connectivity.
Post-conditions (optional)	– XaaS CSC A and XaaS CSP Y can communicate with each other. – XaaS CSP X and XaaS CSP Y can communicate with each other.
Requirements	– On-demand network configuration – Heterogeneous networks compatibility – QoS-guaranteed connectivity – Secured connectivity – Common control mechanism for NaaS connectivity (refer to clause 9.1) NOTE – The first 4 requirements belong to general requirements of NaaS which are provided in [ITU-T Y.3501].

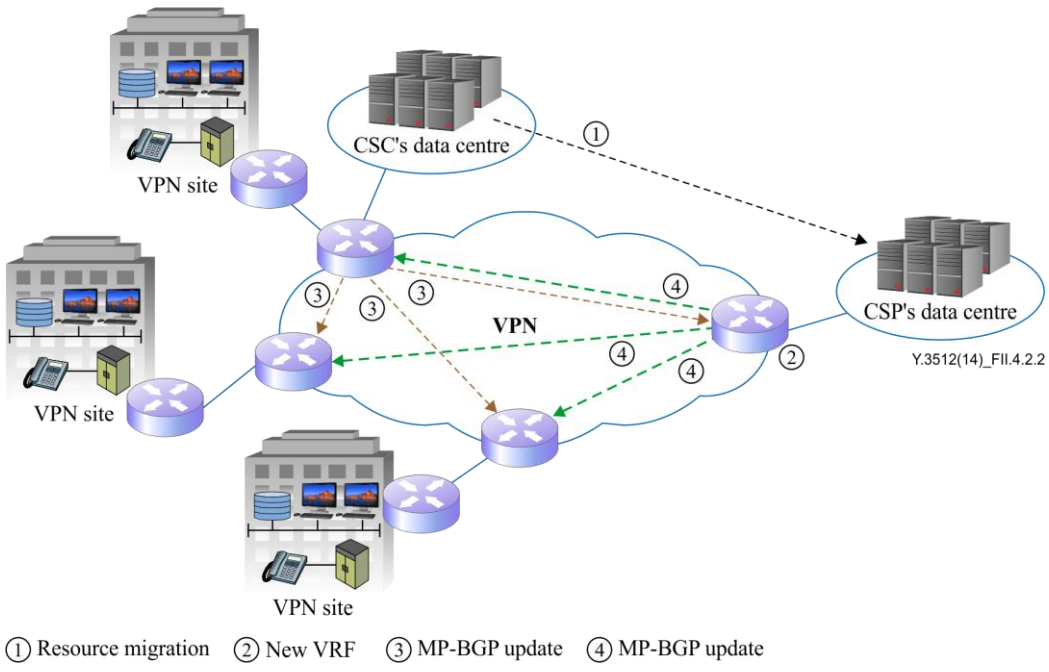
II.4.2 Detailed use cases

II.4.2.1 NaaS connectivity use case for dynamic transport network

Title	NaaS connectivity use case for dynamic transport network
Description	CSC demands a geographically distributed connectivity service and dynamic traffic capacity which can accommodate cloud bursting (e.g., VM migration or the transfer of large data files across data centres which sit in different places) which brings a surge of traffic passing through the backbone of the CSP. IP and transport networks of the CSP are separately managed and therefore cannot provide the common control mechanism for dynamic bandwidth adjustment. In order to guarantee the service continuity and consistent SLA to the CSC, such CSP would have to offer over-provisioning of links, most of which being not used effectively and thus causing resource waste. The CSP is recommended to cope with the surge of transit traffic which traverses its backbone without making use of traditional over-provisioning approaches of the networking resources.
Roles	CSC, CSP
Figure (optional)	
Pre-conditions (optional)	

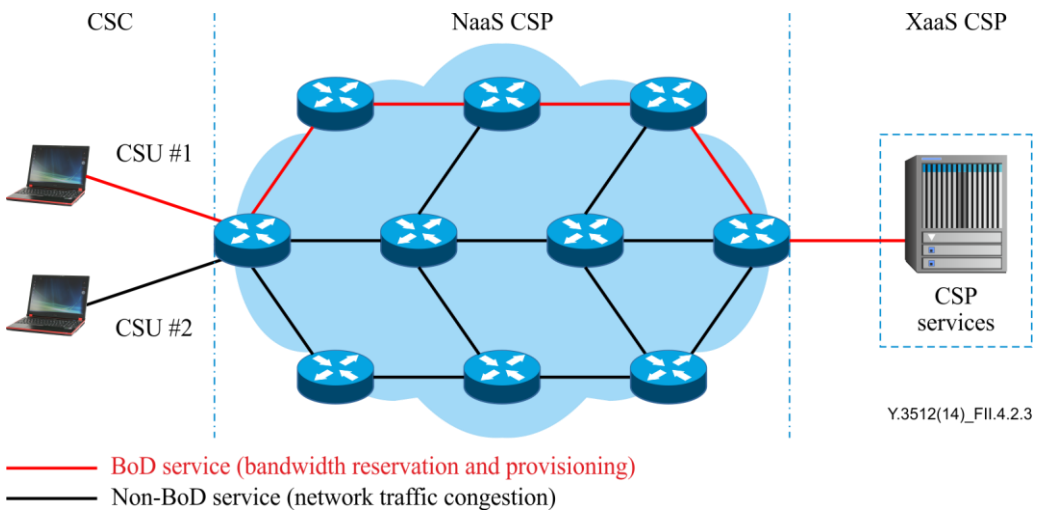
Post-conditions (optional)	
Derived requirements	– Unified SLA for multiple optimized networks (refer to clause 9.2) – Leveraging transport networks dynamically (refer to clause 9.3) – Unified network control mechanism (refer to clause 9.4)

II.4.2.2 NaaS connectivity use case for flexible and extended VPN

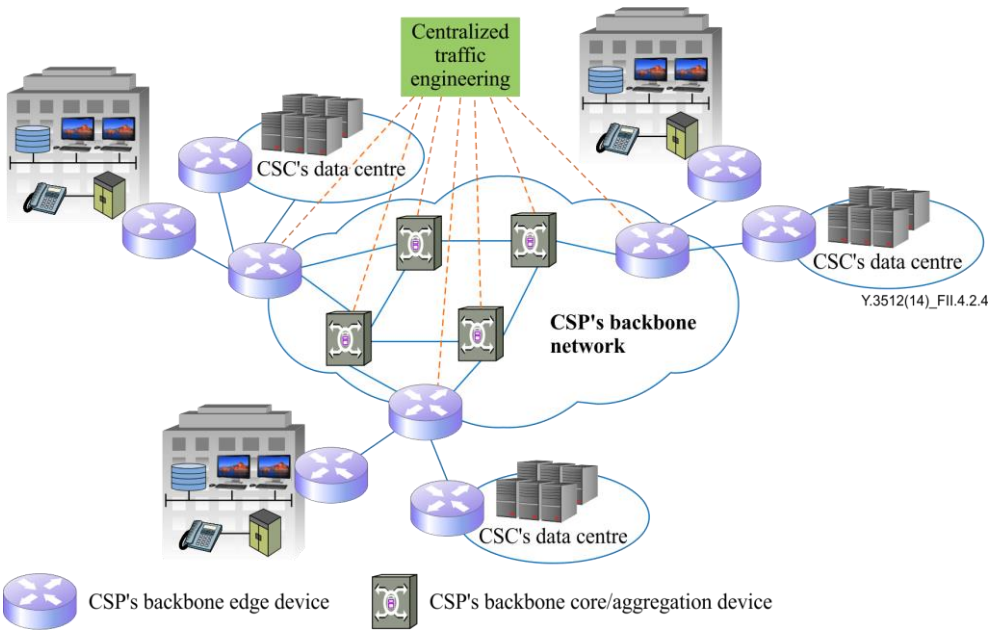
Title	NaaS connectivity use case for flexible and extended VPN
Description	The different VPN sites are connected via BGP/MPLS IPVPN. The processing resources and the corresponding subnet are migrated from the CSC's data centre to the CSP's data centre, which is not yet involved in the VPN as a VPN site. In order to add this new site in the existing VPN, there is a need to provision a new subnet in the CSP's data centre and to set up a new virtual routing and forwarding (VRF) in its edge router. The migration of the corresponding subnet from the CSC's data centre to the CSP's data centre and the subnet removal from the CSC's data centre needs to be announced to the remaining edge routers. The concrete procedure is shown in the following figure. 1. Processing resources and the corresponding subnet migrate from the CSC's data centre to the CSP's data centre. 2. New VRF is configured in the edge router of the CSP's data centre. 3. The removal of the CSC's subnet is announced through MP-BGP update to all VPN sites. 4. CSP's new subnet is announced through MP-BGP update to all VPN sites. Service continuity needs to be ensured during the whole migration and reconfiguration procedure. However, the existing VPN is a black box from the CSC's perspective, and as such it can't be provisioned and reconfigured by the CSC. In addition, the current VPN technology cannot support the dynamic addition and reduction of the VPN sites and bandwidth capacity.
Roles	CSC, CSP
Figure (optional)	
Pre-conditions (optional)	

Post-conditions (optional)	
Derived requirements	– Elastic network reconfiguration (refer to clause 9.5)

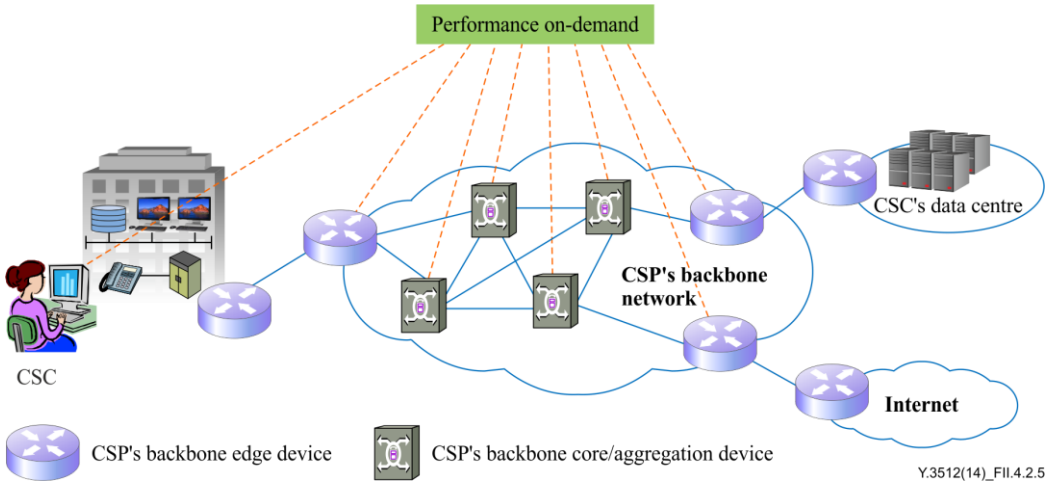
II.4.2.3 NaaS connectivity use case for BoD service

Title	NaaS connectivity use case for BoD service
Description	In this scenario CSU access to cloud computing service offered by XaaS CSP is considered (e.g., virtual desktop infrastructure (VDI), video streaming). CSU accesses the service from a fixed location e.g., using a company local area network (LAN) or from mobile location e.g., mobile terminal. The XaaS CSP serves the services on the basis of own data centres and has no impact on the performance of particular connectivity between end users and the data centre where the service is hosted. From the perspective of CSU, quality of experience (QoE) of the service is dependent on a combination of data centre and network performance. The XaaS CSP is able to guarantee certain service quality limited to its own data centre. This quality could be downgraded on network performance on the connection between CSC and particular data centre. The XaaS CSP acting alone is not able to impact network performance without interaction with NaaS CSP. As a solution to guarantee end-to-end service quality, bandwidth reservations can be applied in the network between the CSU and the data centre. This allows the guarantee of certain network performance and can be a basis for end-to-end SLA contract for the service between a CSU and the XaaS CSP. To fulfil these needs, XaaS CSP interacts with NaaS CSP. NaaS CSP can be any actor that has the ability to offer connectivity between XaaS CSP and the CSC, to which CSU belongs.
Roles	CSU, CSC, CSP
Figure (optional)	
Pre-conditions (optional)	– XaaS CSP has no impact on connectivity parameters between the service and the CSU.
Post-conditions (optional)	– XaaS CSP offers end-to-end service quality or SLA to the CSC, on the basis of cooperation with NaaS CSP.
Derived requirements	– Seamless and end-to-end solution of bandwidth allocation (refer to clause 9.6) – Symmetric or asymmetric capacity (refer to clause 9.7)

II.4.2.4 NaaS connectivity use case for optimized traffic engineering

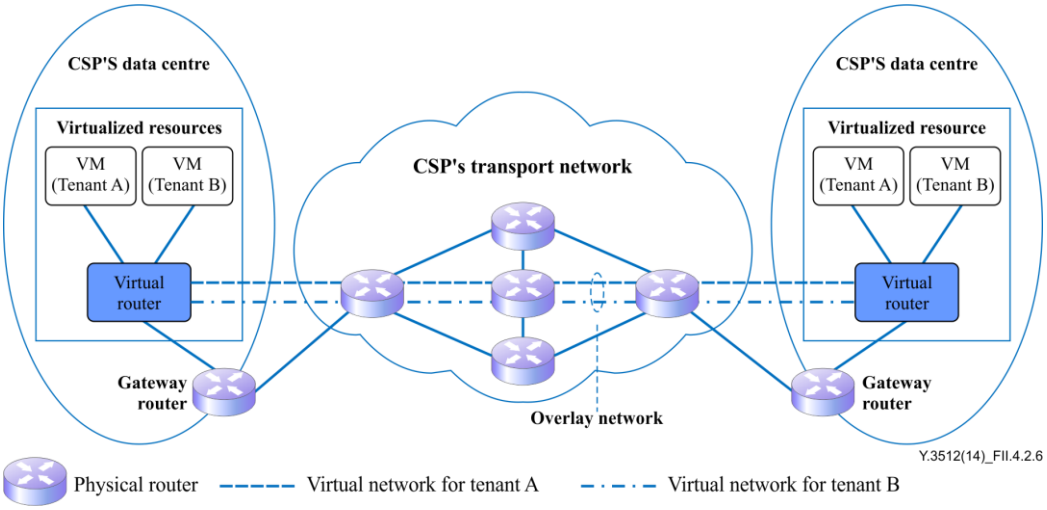
Title	NaaS connectivity use case for optimized traffic engineering
Description	The CSP provides network connectivity services to a CSC in order for the CSC to inter-connect its own multiple geographically distributed data centres. With the increase of cloud services deployed over the CSC's data centres, more and more traffic, e.g., for data mirroring, redundancy, database synchronization, VM migration, active-active storage replication, is traversing the CSP's backbone network due to the CSC's increasing distributed services. Currently, CSP typically provides the CSC with static connectivity services resulting in either over-provisioned, under-utilized service capacity or under-provisioned, capacity-capped services. In order to make a more efficient use of its connectivity resources, a solution for the CSP is to support a central decision-making function for the backbone traffic engineering. At the minimum, such solution has to coexist with other legacy network solutions used by the CSP for the support of other services.
Roles	CSC, CSP
Figure (optional)	
Pre-conditions (optional)	
Post-conditions (optional)	
Derived requirements	– Optimized and fine-grained traffic engineering (refer to clause 9.8) – Coexistence with legacy network services and functions (refer to clause 9.9) – Centralized control view and abstraction view of resources (refer to clause 9.10)

II.4.2.5 NaaS connectivity use case for performance on demand

Title	NaaS connectivity use case for performance on demand
Description	CSC requests CSP to provide on-demand network performance (such as bandwidth quantities, maximum latencies and other QoS parameters), which includes dynamic establishment, change and resized capacity of links. However, traditional solution based on human intervention lacks automation capabilities which make it difficult to deliver self-provisioned services and respond to time-sensitive changes in network performance requirements. Additionally, frequent changes sometimes result in congestion and instability because traffic, which comes from multiple sources, shares the same network link. CSP provides CSC the appropriate control in order to request services through a portal and to shield the underlying physical network to the CSC.
Roles	CSC, CSP
Figure (optional)	
Pre-conditions (optional)	
Post-conditions (optional)	
Derived requirements	– Centralized control view and abstraction view of resources (refer to clause 9.10) – CSC limited control of services (refer to clause 9.11)

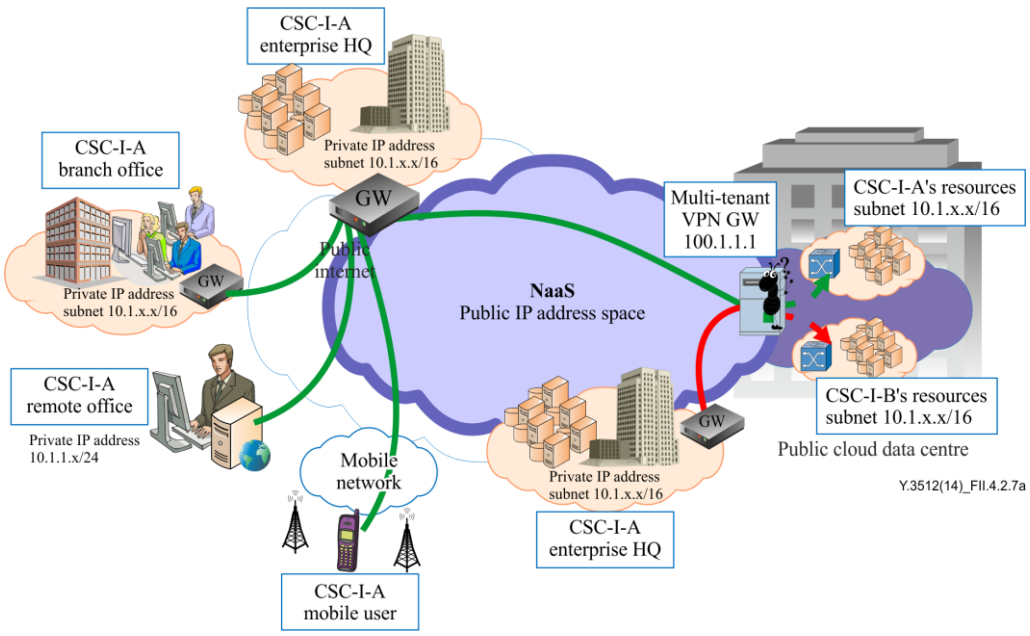
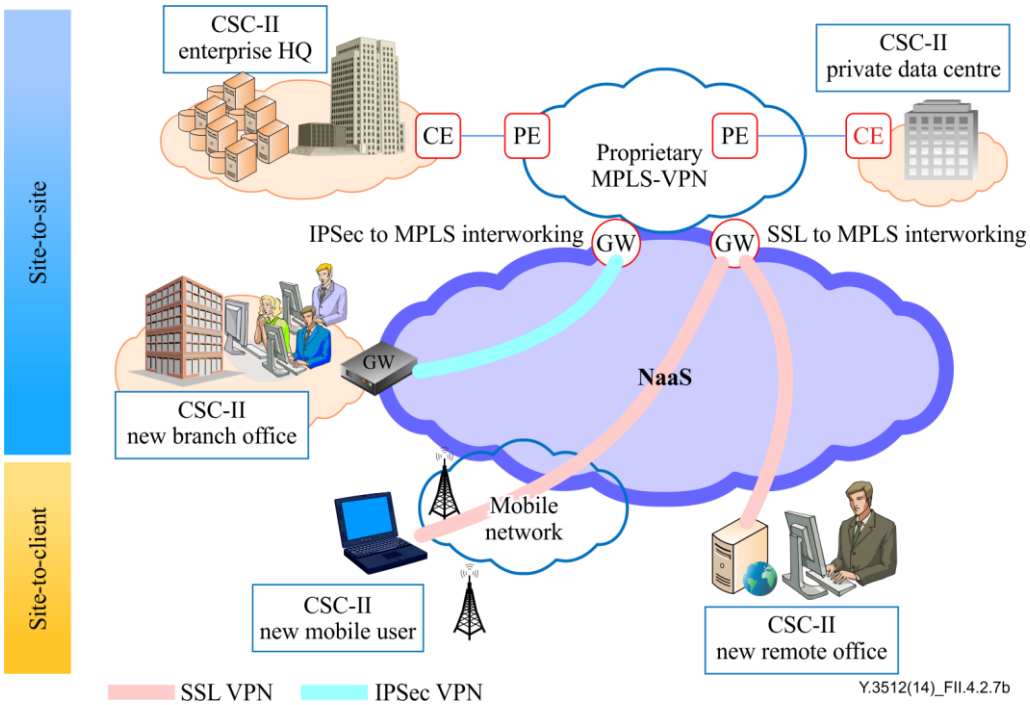
II.4.2.6 NaaS connectivity use case for virtual router

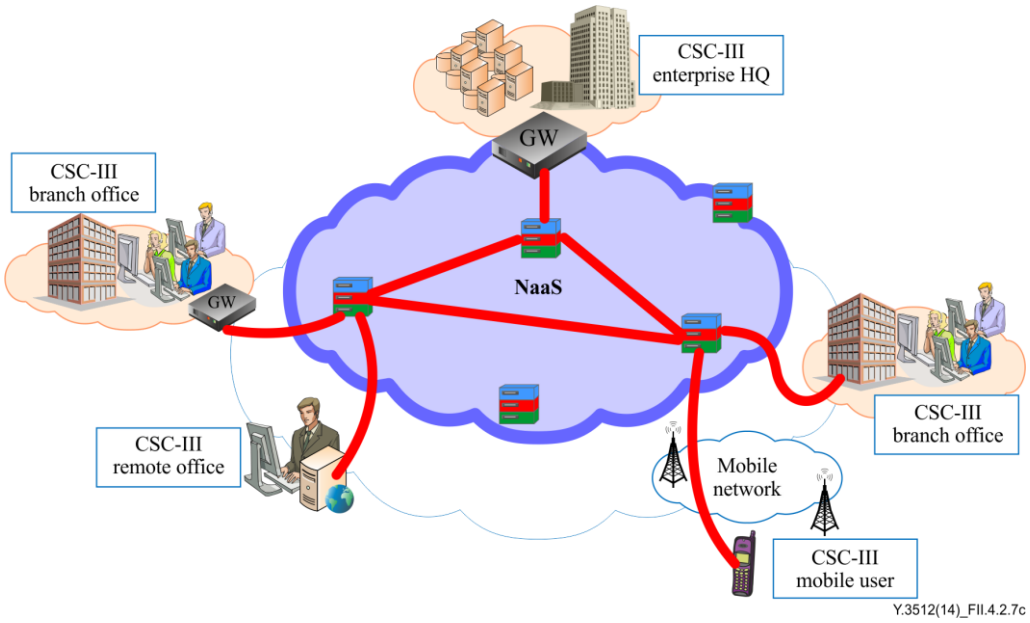
Title	NaaS connectivity use case for virtual router
Description	According to [ITU-T Y.3500], multi-tenancy is a key characteristic of the cloud service, which requires the CSP to provide the CSC either shared physical or virtual resources or both, such that multiple tenants and their resources and data are isolated from and inaccessible to each other. These tenants share the same underlay physical resources, including physical servers, physical storage and physical networks and each tenant is assigned its own logical resources, including VMs, virtual storage and virtual networks. These logical resources need to be isolated from each other and the virtual compute, storage and network resources need to be integrated and matched in a fine granularity. However, the legacy underlay physical routers and switches of CSP's transport network don't contain each tenant's state, including tenant's medium access control (MAC) and IP addresses and the network policies attached to the VM that belongs to the tenant. In other words, the forwarding tables of the underlay physical routers and switches only contain the IP prefixes or MAC addresses of the physical servers.

	The virtual router is software implemented router and can be implemented within the virtualization infrastructure. The virtual router provides connectivity among virtual machines, virtual switches, etc., and contains per tenant state and a separate forwarding table for a virtual network. The forwarding table includes the IP prefixes (in the case of a layer 3 overlay network) or the MAC addresses (in the case of a layer 2 overlay network) of VMs. In addition, no single virtual router needs to contain all IP prefixes or all MAC addresses for all virtual machines in the CSP's data centre. A given virtual router only needs to contain those routing instances that are locally installed on the same server.
Roles	CSC, CSP
Figure (optional)	
Pre-conditions (optional)	– CSP's IP carrier network support overlay network mechnism.
Post-conditions (optional)	– CSC's VMs that run in different CSP's data centres can communicate with each other.
Derived requirements	– Logically isolated network partition (refer to clause 9.12) – Overlay network mechanism (refer to clause 9.13)

II.4.2.7 NaaS connectivity use case for private IP addresses and VPNs

Title	NaaS connectivity use case for private IP addresses and VPNs
Description	Case I: Public cloud site multi-tenant VPN gateway (GW) with overlapping private IP addresses Multi-tenant VPN GW in a public cloud site is shared by CSC-I-A and CSC-I-B. Both of them are interested to use the same private IP address pool for their end points. Both of CSCs are connected to the public cloud VPN GW through a given public IP address of it. The cloud VPN GW should be able to switch the traffic from each CSC to a proper subnet. Case II: Interworking support for different types of VPNs CSC-II has site-to-site proprietary MPLS-VPN connection between its headquarter (HQ) and private data centre. According to the company progress, CSC-II is interested to establish new site-to-site and site-to-client secure VPN connections (e.g., IP security (IPsec) VPN and secure socket layer (SSL) VPN). New VPN connections are planned between their globally distributed branch offices and mobile users, while keeping the CSC-II existing VPN investments. NaaS CSP should be able to provide interworking between the CSC owned existing VPN and different types of new VPNs.

	Case III: On-demand network support for the distributed end points CSC-III requires a solution of delivering reliable, predictable and on-demand network connections for all their locations. This service should be able to be changed dynamically according to the CSC-III's needs. The CSC-III is interested in elastic request parameters for connectivity to their location over the existing links. The connectivity should be established to one or more of the NaaS CSP's points of presence (PoPs) with minimum efforts for deploying additional equipment.
Roles	CSP, CSC
Figure (optional)	 **Figure 1 – Case I: Public Cloud site multi-tenant VPN GW with overlapping private IP addresses**  **Figure 2 – Case II: Interworking support for different types of VPNs**

	 **Figure 3 – Case III: On-demand network support for the distributed end points**
Pre-conditions (optional)	It is assumed that multi-tenant VPN GW in public cloud site is provided by the NaaS CSP.
Post-conditions (optional)	
Derived requirement	– Overlapped private IP addresses (refer to clause 9.14) – Interworking among different VPN solutions (refer to clause 9.15) – VPN connection in mobile environment (refer to clause 9.16) – Connection to NaaS CSP's network through public Internet (refer to clause 9.17)

Appendix III

Considerations on CSP's network related activities

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

This appendix provides considerations on CSP's network related activities.

Each individual service of the NaaS category can be specified by a set of terms including:

- Service interface – It is offered to the CSC and defines the functionality which is implemented by the CSP. Service interface can include functionality related to demarcation points for the interconnection of the CSP and the CSC, topology and route related functionality to share topologies, discovery related functionality to perform other services needed by inter-cloud related activities, and other functionalities related to monitoring, protection, verification, etc. Route related functionality requires information on ingress and egress end points and optionally intermediate points of a network segment. Attributes of a network segment can include edge point attributes, QoS parameters, performance attributes, time attributes, user attributes, service requester identifier, etc.
- Service demarcation point – This is a boundary point between NaaS CSP and NaaS CSC. It is used as a reference point to identify the responsibilities and obligations of all involved entities. For IP/MPLS networks, the demarcation point user-to-network interface (UNI) is a pair of customer edge and provider edge. For other transport networks, UNI and network-to-network interface (NNI) are defined as demarcation points. For example, UNI defined by Metro Ethernet Forum (MEF) is physically implemented over a bi-directional Ethernet link that provides the various data, control and management plane capabilities required by the metro Ethernet network (MEN) service provider to clearly demarcate the two different network domains involved in the operational, administrative, maintenance and provisioning aspects of the service. Often software abstraction layer (SAL) or network operating system (NOS) is used for the demarcation point for network platforms, and TCP/UDP sockets for network applications.
- Service capabilities – This is what NaaS delivers to the CSC via service interfaces as network connectivity and networking related service capabilities. While transport network connectivity capabilities include IP/MPLS network, transmission networks, IP multimedia subsystem (IMS), software defined networking (SDN) and CDN, virtual network connectivity capabilities include pseudo-wire, virtual private LAN service (VPLS), L3 VPN and VLAN. Networking related service capabilities can include WAN optimization, load balancing, domain name system (DNS), firewall, IPS/IDS, telecommunication services and network applications such as peer-to-peer (P2P) based file transfer, etc.

Although infrastructure capability type NaaS can provide such network as a whole, a CSC relies on CSP for the integration and customizing of software, reconfiguring and expanding functionalities of network elements, as well as management and administration of the network. When CSC leverages NaaS platforms to build its own network, the responsibility of CSP is up to the service demarcation point of the platform. CSC is responsible for managing, administering and operating the network as well as network functions and services implemented up on the demarcation point.

The composite services provisioned in cloud environments need SLA support in the following areas [b-EC SLA]:

- SLA specifications capturing the dependencies and interactions between the services. The dependencies should be parametric and express the overall service context (e.g., data movements, relationships between providers, orchestration rules).
- Convergence in SLA management to handle dependencies (e.g., joint management) while retaining the autonomy in resource management for each provider.

Enhanced SLA specification and management approaches should take into consideration that composition may be performed as either centralized (e.g., an entity managing the composition and the corresponding service offerings) or distributed (e.g., achieved through consecutive SLA establishments) approaches. SLA specifications in cross-service scenarios should either include the common terms (limiting however end-to-end quality provision to these terms) or be implemented through links between SLAs (e.g., one SLA for each service with enriched specification to include links to the SLAs of other services), as a protocol to enable interaction between different layers and entities.

SLAs identify, in a clear and precise way, the responsibilities and obligations of all involved entities, as well as their boundaries and limits.

NaaS can be used to support other cloud service CSP's network related activities (e.g., provide network connectivity, deliver network services and provide network management services), where a logically isolated CSC cloud in the CSP's data centre allows a CSC to provision a private, isolated partition of the cloud where the CSC can use cloud capabilities in a virtual network, often using CSC-defined IP address ranges. A CSC cloud can have multiple subnets in a data centre. Network connectivity between the remote CSC and CSC cloud, for example, may include the following:

- IPsec VPN connection over public Internet (CSP edge VPN gateway – CSC premises VPN gateway);
- Dedicated network connection over private lines (CSP edge VPN gateway – customer premises equipment (CPE));
- IPsec VPN connection over private lines (CSP edge VPN gateway – CSC premises VPN gateway);
- VPN connection with a software appliance over public Internet (software VPN appliance – CSP edge Internet gateway - CSC premises VPN gateway, where Internet gateway only routes VPN connection over public Internet);
- Multi-protocol label switching (MPLS) VPN connections.

Cloud services needs interconnecting multiple CSC clouds into a contiguous virtual network as well as to meet this requirement NaaS may provide followings:

- Software VPN appliance based connections between CSC clouds for intra-cloud and inter-cloud (software VPN appliance at CSC cloud-1 – Internet gateway – Internet gateway – software VPN appliance at CSC cloud-2, where Internet gateway only routes VPN connection, over public Internet for inter-cloud case);
- Software VPN appliance to physical VPN connection between CSC clouds (VPN gateway at CSC cloud-1 – Internet gateway – software VPN appliance at CSC cloud-2, where Internet gateway only routes VPN connection);
- CSC managed CSC cloud-to-CSC cloud routing over physical IPsec VPN connections using CSC equipment and public Internet or private lines (VPN gateway at CSC cloud-1 – CSC equipment – VPN gateway at CSC cloud-2).

Bibliography

[b-IETF RFC 4364] IETF RFC 4364 (2006), *BGP/MPLS IP Virtual Private Networks (VPNs)*.

[b-EC SLA] European Commission Directorate General Communications Networks, Content and Technology Unit E2 – Software and Services, Cloud, (Brussels, June 2013), *Cloud Computing Service Level Agreements – Exploitation of Research Results*.

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