

Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.3512

(08/2014)

SÉRIE Y: INFRASTRUCTURE MONDIALE DE
L'INFORMATION, PROTOCOLE INTERNET, RÉSEAUX
DE PROCHAINE GÉNÉRATION, INTERNET DES
OBJETS ET VILLES INTELLIGENTES

Informatique en nuage

**Informatique en nuage – Exigences
fonctionnelles relatives au réseau en tant que
service**

Recommandation UIT-T Y.3512

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET, RÉSEAUX DE PROCHAINE GÉNÉRATION, INTERNET DES OBJETS ET VILLES INTELLIGENTES

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
Télévision IP sur réseaux de prochaine génération	Y.1900–Y.1999
RÉSEAUX DE PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
Améliorations concernant les réseaux de prochaine génération	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Réseaux de transmission par paquets	Y.2600–Y.2699
Sécurité	Y.2700–Y.2799
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999
RÉSEAUX FUTURS	Y.3000–Y.3499
INFORMATIQUE EN NUAGE	Y.3500–Y.3999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T Y.3512

Informatique en nuage – Exigences fonctionnelles relatives au réseau en tant que service

Résumé

La Recommandation UIT-T Y.3512 décrit le concept de réseau en tant que service (NaaS) et les exigences fonctionnelles associées. Elle présente des cas d'utilisation types de réseaux NaaS et spécifie les exigences fonctionnelles relatives à trois aspects, à savoir les applications NaaS, les plates-formes NaaS et la connectivité NaaS, sur la base des cas d'utilisation correspondants et des types de capacités de nuage.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T Y.3512	2014-08-29	13	11.1002/1000/12285

Mots clés

Informatique en nuage, réseau en tant que service, NaaS, application NaaS, connectivité NaaS, plate-forme Naas.

* Pour accéder à la Recommandation, reporter cet URL <http://handle.itu.int/> dans votre navigateur Web, suivi de l'identifiant unique, par exemple <http://handle.itu.int/11.1002/1000/11830-en>.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous <http://www.itu.int/ITU-T/ipr/>.

© UIT 2016

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

		Page
1	Domaine d'application	1
2	Références.....	1
3	Définitions	1
	3.1 Termes définis ailleurs	1
	3.2 Termes définis dans la présente Recommandation	3
4	Abréviations et acronymes	3
5	Conventions	4
6	Description générale	5
	6.1 Difficultés liées aux réseaux dans l'informatique en nuage.....	5
	6.2 Concept de haut niveau du réseau NaaS.....	5
7	Exigences fonctionnelles des applications NaaS	7
	7.1 Qualité de fonctionnement	7
	7.2 Exploitation et gestion.....	7
	7.3 Chaîne de services	8
	7.4 Adresses IP multiples	8
8	Exigences fonctionnelles des plates-formes NaaS	8
	8.1 Plates-formes NaaS programmables.....	8
	8.2 Composition et orientation dynamiques et flexibles des services de réseau ..	8
	8.3 Isolation des chaînes de services destinées aux locataires	9
	8.4 Ajustement flexible des plates-formes NaaS.....	9
	8.5 Intégration des applications logicielles	9
9	Exigences fonctionnelles de la connectivité NaaS	9
	9.1 Mécanisme de commande commun pour la connectivité NaaS.....	9
	9.2 Accord SLA unifié pour de multiples réseaux optimisés.....	9
	9.3 Utilisation de réseaux de transport choisis de façon dynamique.....	10
	9.4 Mécanisme unifié de commande de réseau	10
	9.5 Reconfiguration élastique du réseau.....	10
	9.6 Solution transparente et de bout en bout d'attribution de la bande passante ..	10
	9.7 Capacité symétrique ou asymétrique.....	10
	9.8 Ingénierie du trafic optimisée et à granulation fine.....	10
	9.9 Coexistence avec les services et les fonctions des réseaux existants	10
	9.10 Vue de commande centralisée et vue abstraite des ressources.....	11
	9.11 Commande de service limitée pour le client CSC.....	11
	9.12 Subdivision de réseau isolée logiquement.....	11
	9.13 Mécanisme de réseau superposé.....	11
	9.14 Chevauchement des adresses IP privées.....	11
	9.15 Interfonctionnement de solutions VPN différentes	11

	Page
9.16 Connexion VPN dans un environnement mobile	11
9.17 Connexion au réseau du fournisseur CSP NaaS via l'Internet public.....	11
10 Considérations relatives à la sécurité.....	11
Appendice I – Méthodologie pour la définition des exigences et de l'architecture fonctionnelles des réseaux NaaS	12
Appendice II – Cas d'utilisation des réseaux NaaS.....	13
II.1 Modèle de présentation des cas d'utilisation	13
II.2 Cas d'utilisation relatifs aux applications NaaS.....	13
II.3 Cas d'utilisation relatifs aux plates-formes NaaS	16
II.4 Cas d'utilisation relatifs à la connectivité NaaS	18
Appendice III – Considérations relatives aux activités liées aux réseaux du fournisseur CSP	28
Bibliographie.....	31

Recommandation UIT-T Y.3512

Informatique en nuage – Exigences fonctionnelles relatives au réseau en tant que service

1 Domaine d'application

La présente Recommandation décrit les cas d'utilisation et les exigences fonctionnelles pour le réseau en tant que service (NaaS), qui est l'une des catégories de services de nuage représentatives. Elle porte sur les points suivants:

- Concept de haut niveau des réseaux NaaS
- Exigences fonctionnelles des réseaux NaaS
- Cas d'utilisation types des réseaux NaaS.

La présente Recommandation donne les cas d'utilisation et les exigences fonctionnelles pour les applications NaaS, les plates-formes NaaS et la connectivité NaaS.

NOTE – Les exigences générales concernant les réseaux NaaS sont décrites dans [UIT-T Y.3501].

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut de Recommandation.

[UIT-T X.1601] Recommandation UIT-T X.1601 (2014), *Cadre de sécurité applicable à l'informatique en nuage.*

[UIT-T Y.3011] Recommandation ITU-T Y.3011 (2012), *Cadre applicable à la virtualisation de réseau dans les réseaux futurs.*

[UIT-T Y.3500] Recommandation ITU-T Y.3500 (2014), *Technologies de l'information – Informatique en nuage – Présentation générale et vocabulaire.*

[UIT-T Y.3501] Recommandation UIT-T Y.3501 (2013), *Cadre et exigences de haut niveau applicables à l'informatique en nuage.*

[UIT-T Y.3502] Recommandation ITU-T Y.3502 (2014), *Technologies de l'information – Informatique en nuage – Architecture de référence.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 capacités de type application [UIT-T Y.3500]: type de capacités de nuage selon lequel le client de services de nuage peut utiliser les applications du fournisseur de services de nuage.

3.1.2 type de capacités de nuage [UIT-T Y.3500]: classification de la fonctionnalité fournie par un service de nuage au client de services de nuage, en fonction de la ressource utilisée.

NOTE – Les types de capacités de nuage sont les suivants: capacités de type application, capacités de type infrastructure et capacités de type plate-forme.

3.1.3 informatique en nuage [UIT-T Y.3500]: modèle permettant d'offrir un accès via le réseau à un ensemble modulable et élastique de ressources physiques ou virtuelles mutualisables, fournies et administrées à la demande et en libre-service.

NOTE – Comme exemples de ressources, on peut citer les serveurs, les systèmes d'exploitation, les réseaux, les logiciels, les applications et les équipements de stockage.

3.1.4 service de nuage [UIT-T Y.3500]: une ou plusieurs capacités offertes via l'informatique en nuage invoquées à l'aide d'une interface définie.

3.1.5 catégorie de services de nuage [UIT-T Y.3500]: groupe de services qui possèdent un ensemble de qualités communes.

NOTE – Une catégorie de services de nuage peut comprendre des capacités de nuage d'un ou de plusieurs types.

3.1.6 client de services de nuage [UIT-T Y.3500]: partie à une relation commerciale aux fins de l'utilisation de services de nuage.

3.1.7 fournisseur de services de nuage [UIT-T Y.3500]: partie qui met à disposition des services de nuage.

3.1.8 utilisateur de services de nuage [UIT-T Y.3500]: personne physique, ou entité agissant en son nom, associée à un client de services de nuage qui utilise des services de nuage.

3.1.9 communications en tant que service (CaaS) [UIT-T Y.3500]: catégorie de services de nuage pour laquelle la capacité fournie au client du service de nuage est une interaction et une collaboration en temps réel.

NOTE – La communication CaaS peut correspondre à la fourniture de capacités de plate-forme et de capacités d'application.

3.1.10 capacités de type infrastructure [UIT-T Y.3500]: type de capacités de nuage selon lequel le client de services de nuage peut fournir et utiliser des ressources de traitement, de stockage et de réseau.

3.1.11 subdivision de réseau isolée logiquement [UIT-T Y.3011]: réseau qui est composé de multiples ressources virtuelles et est isolé des autres subdivisions LINP.

NOTE – L'expression "isolé logiquement", qui est le concept opposé à "isolé physiquement", signifie que les objets (en l'espèce les subdivisions de réseau) s'excluent mutuellement, alors que les objets originaux peuvent être unis/partagés sur le plan physique selon les contraintes physiques communes.

3.1.12 réseau en tant que service (NaaS) [UIT-T Y.3500]: catégorie de services de nuage pour laquelle la capacité fournie au client de services de nuage correspond à des capacités de connectivité de transport et à des capacités de réseau connexes.

NOTE – Le réseau NaaS peut fournir l'un quelconque des trois types de capacités de nuage.

3.1.13 capacités de type plate-forme [UIT-T Y.3500]: type de capacités de nuage selon lequel le client du service de nuage peut déployer, gérer et exécuter des applications qu'il a créées ou achetées en utilisant un ou plusieurs langages de programmation et un ou plusieurs environnements d'exécution pris en charge par le fournisseur de services de nuage.

3.1.14 locataire [UIT-T Y.3500]: groupe d'utilisateurs de services de nuage partageant l'accès à un ensemble de ressources physiques et virtuelles.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit le terme suivant:

3.2.1 chaîne de services: ensemble ordonné de fonctions qui est utilisé pour appliquer des politiques de traitement du trafic différencié à un flux de trafic.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

BGP	protocole de passerelle frontière (<i>border gateway protocol</i>)
BoD	bande passante à la demande (<i>bandwidth on demand</i>)
BSS	système d'appui aux activités (<i>business support system</i>)
CaaS	communications en tant que service (<i>communications as a service</i>)
CDN	réseau de fourniture de contenu (<i>content delivery network</i>)
CPE	équipement des locaux d'abonné (<i>customer premise equipment</i>)
CSC	client de services de nuage (<i>cloud service customer</i>)
CSP	fournisseur de services de nuage (<i>cloud service provider</i>)
CSU	utilisateur de services de nuage (<i>cloud service user</i>)
DNS	système des noms de domaine (<i>domain name system</i>)
DPI	inspection approfondie des paquets (<i>deep packet inspection</i>)
EPC	noyau paquet évolué (<i>evolved packet core</i>)
GW	passerelle (<i>gateway</i>)
HQ	siège (<i>headquarter</i>)
IaaS	infrastructure en tant que service (<i>infrastructure as a service</i>)
IDE	environnement de développement intégré (<i>integrated development environment</i>)
IMS	sous-système multimédia IP (<i>IP multimedia subsystem</i>)
IP	protocole Internet (<i>Internet protocol</i>)
IPS	système de protection contre les intrusions (<i>intrusion protection system</i>)
IPsec	sécurité IP (<i>IP security</i>)
L2	couche 2 (<i>layer 2</i>)
L3	couche 3 (<i>layer 3</i>)
LAN	réseau local (<i>local area network</i>)
LINP	subdivision de réseau isolée logiquement (<i>logically isolated network partition</i>)
MAC	commande d'accès au support (<i>medium access control</i>)
MEF	Metro Ethernet Forum
MEN	réseau Ethernet métropolitain (<i>metro Ethernet network</i>)
MPLS	commutation par étiquette multiprotocole (<i>multi protocol label switching</i>)
NaaS	réseau en tant que service (<i>network as a service</i>)
NNI	interface réseau-réseau (<i>network-network interface</i>)

NOS	système d'exploitation de réseau (<i>network operating system</i>)
OSS	système d'appui à l'exploitation (<i>operations support system</i>)
QoE	qualité d'expérience (<i>quality of experience</i>)
QoS	qualité de service (<i>quality of service</i>)
P2P	entre homologues (<i>peer-to-peer</i>)
PaaS	plate-forme en tant que service (<i>platform as a service</i>)
PoP	point de présence (<i>point of presence</i>)
SaaS	logiciel en tant que service (<i>software as a service</i>)
SAL	couche d'abstraction logicielle (<i>software abstraction layer</i>)
SDN	réseaux pilotés par logiciel (<i>software defined networking</i>)
SLA	accord de niveau de service (<i>service level agreement</i>)
SSL	couche de connecteurs sécurisés (<i>secure socket layer</i>)
UNI	interface utilisateur-réseau (<i>user-to-network interface</i>)
vCDN	réseau virtuel de fourniture de contenu (<i>virtual content delivery network</i>)
vDPI	inspection approfondie virtuelle des paquets (<i>virtual deep packet inspection</i>)
vEPC	noyau paquet évolué virtualisé (<i>virtualised evolved packet core</i>)
vFW	pare-feu virtuel (<i>virtual firewall</i>)
vRouter	routeur virtuel (<i>virtual router</i>)
VDI	infrastructure de bureau virtuel (<i>virtual desktop infrastructure</i>)
VM	machine virtuelle (<i>virtual machine</i>)
VoIP	protocole de transmission de la voix par Internet (<i>voice over IP</i>)
VPLS	service de réseau local privé virtuel (<i>virtual private LAN service</i>)
VPN	réseau privé virtuel (<i>virtual private network</i>)
VRF	routage et réacheminement virtuels (<i>virtual routing and forwarding</i>)
WAN	réseau étendu (<i>wide area network</i>)

5 Conventions

L'expression "**il est obligatoire**" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

L'expression "**peut, à titre d'option,**" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en oeuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité.

Dans le corps de la présente Recommandation et dans ses Appendices, on trouve parfois les expressions doit, ne doit pas, devrait et peut. Celles-ci doivent respectivement être interprétées comme correspondant aux expressions il est obligatoire, il est interdit, il est recommandé et peut, à

titre d'option. Lorsque ces expressions apparaissent dans un appendice ou dans des parties dans lesquelles il est expressément indiqué qu'elles sont données à titre d'information, elles doivent être interprétées comme étant dépourvues d'intention normative.

6 Description générale

6.1 Difficultés liées aux réseaux dans l'informatique en nuage

La construction d'applications et d'infrastructures de réseau efficaces et fiables pour fournir des services de nuage pose plusieurs difficultés. Le fait d'avoir des capacités à la fois de calcul, de stockage et de réseau peut entraîner les difficultés suivantes:

- Coordination de la virtualisation des capacités de calcul et de stockage avec les capacités de réseau

L'utilisation de la virtualisation comme principale technique permet de résoudre les problèmes liés à la qualité de fonctionnement en termes de calcul et de stockage dans les systèmes d'informatique en nuage. La virtualisation des serveurs a donné lieu à la migration dynamique et statique des machines virtuelles (VM), synonyme de contraintes pour les environnements de réseau. Le réseau est censé permettre la prise en charge adaptée et flexible d'applications de nuage très variables, lorsqu'elles sont exécutées dans une architecture système complexe et hétérogène. Un tel système peut fournir les ressources de calcul et de stockage, mais il est également censé assurer de manière dynamique la prise en charge des réseaux nécessaires pour répondre aux demandes concernant la qualité de fonctionnement globale, la fiabilité et la qualité de service (QoS).

- Commande harmonisée de technologies de réseau hétérogènes

En raison de la répartition géographique de plus en plus vaste des systèmes d'informatique en nuage, plusieurs technologies de réseau peuvent être utilisées pour fournir la connectivité de bout en bout. La prise en charge de mécanismes de commande efficaces pour des technologies de réseau hétérogènes devrait donc être assurée.

- Reconfiguration à la demande

Un système d'informatique en nuage permet la reconfiguration ou la migration dynamique des ressources de calcul et de stockage, afin de faire face à des exigences changeantes. Il est souhaitable que les réseaux assurent une reconfiguration à la demande pour répondre aux exigences des services de nuage (par exemple, modification de la bande passante, modification de la topologie de réseau ou ajout de nouveaux éléments de réseau).

6.2 Concept de haut niveau du réseau NaaS

Selon la définition donnée dans [UIT-T Y.3500], un réseau NaaS est une catégorie de services de nuage pour laquelle la capacité fournie au client de services de nuage (CSC) correspond à des capacités de connectivité de transport et à des capacités de réseau connexes, qui permettent de résoudre les difficultés susmentionnées. Les services NaaS sont divisés en services d'application NaaS, en services de plate-forme NaaS et en services de connectivité NaaS. En particulier, le service de connectivité NaaS est un service de "capacités de type infrastructure" limité aux ressources de réseau.

La Figure 6-1 illustre le concept de haut niveau de réseau NaaS selon le cadre de répartition des couches défini dans [UIT-T Y.3502].

Un réseau NaaS peut fournir l'une quelconque des trois capacités de nuage identifiées dans [UIT-T Y.3500] comme suit:

- **Application NaaS:** service offrant des capacités de type application, dans le cadre duquel un client CSC NaaS peut utiliser des applications de réseau fournies par un fournisseur de

services de nuage NaaS (CSP). Ces applications de réseau sont considérées et utilisées comme des fonctions de réseau virtuel fournies par le fournisseur CSP NaaS. Cette catégorie comprend les fonctions de réseau pour les réseaux fixes ou mobiles, centraux ou d'accès, ainsi que pour les éléments de réseau des plans de commande et de transmission. Comme exemples d'applications NaaS, on peut citer les routeurs virtuels, les réseaux virtuels de fourniture de contenu (vCDN), les noyaux paquets évolués virtualisés et les pare-feu virtuels (vFW).

Dans cette catégorie, le fournisseur CSP offre un ensemble d'interfaces pour les fonctionnalités de réseau.

- **Plate-forme NaaS:** service offrant des capacités de type plate-forme, dans le cadre duquel un client CSC NaaS peut utiliser la plate-forme de réseau fournie par un fournisseur CSP NaaS. La plate-forme NaaS offre un ou plusieurs environnements d'exécution pour les logiciels et un ou plusieurs langages de programmation permettant de déployer, de gérer et d'exécuter des applications de réseau créées ou achetées par le client. Ces applications de réseau peuvent être créées ou achetées par le client CSC en tant que services de réseau auto-mis en oeuvre. Les applications de réseau peuvent mettre en oeuvre différentes fonctionnalités de réseau ou différents services (par exemple, routeur, pare-feu, répartiteur de charge), ainsi que des groupes de fonctionnalités de réseau. Des groupes d'applications et de fonctionnalités de réseau peuvent constituer une solution de réseau intégrée.

Dans cette catégorie, le fournisseur CSP offre un environnement programmable pour les fonctionnalités de réseau qui peuvent être employées par le client de services de nuage ou un logiciel partenaire des services de nuage.

- **Connectivité NaaS:** service offrant des capacités de type infrastructure dans le cadre duquel un client CSC NaaS peut fournir et utiliser des ressources de connectivité de réseau fournies par un fournisseur CSP NaaS. Cette catégorie comprend par exemple les réseaux privés virtuels (VPN) flexibles et étendus, la bande passante à la demande (BoD), etc. Un réseau NaaS peut fournir des fonctionnalités de réseau de base comme la connectivité, en utilisant les capacités de réseau physiques, logiques ou virtuelles que le fournisseur CSP choisit de proposer, quelles que soient ces capacités. Souvent, le souhait est de fournir plus que de simples réseaux IP. Par exemple, un client CSC peut vouloir une commande élastique à la demande pour des réseaux optiques, voire un accès à la fibre inutilisée par commutation photonique.

Dans cette catégorie, le fournisseur CSP offre des connexions de réseau entre deux points d'extrémité ou plus, ce qui peut comprendre des fonctionnalités de réseau additionnelles.

NOTE 1 – La mise en place, la commande, la gestion et la suppression de la connectivité NaaS sont effectuées en tant que service de nuage.

NOTE 2 – Un réseau NaaS offre généralement la connectivité "support" des données brutes, quel que soit le type de données acheminées entre deux points d'extrémité. Les services qui sont propres à un type de données acheminées, comme la téléphonie, la transmission de la voix sur Internet (VoIP), les visioconférences et la messagerie instantanée, sont généralement classés dans la catégorie des communications en tant que service (CaaS).

NOTE 3 – Les points d'extrémité de la connectivité NaaS peuvent être situés dans l'interface de service NaaS elle-même, dans un autre service de nuage, dans un autre service qu'un service de nuage ou au niveau d'un point d'extrémité de réseau traditionnel.

Les services NaaS peuvent être utilisés par des services de nuage ou par d'autres services.

Les capacités de réseau peuvent être fournies moyennant une combinaison quelconque des trois types de capacités de nuage. En particulier, les capacités de réseau pourraient, dans le cas de l'informatique en nuage, prendre en charge l'interconnexion entre le fournisseur CSP et le client CSC, la fonctionnalité liée à la topologie et à l'acheminement afin de partager les topologies, la fonctionnalité liée à la découverte afin de mener à bien d'autres services dont les activités

internuages ont besoin, ainsi que d'autres fonctionnalités liées à la surveillance, à la protection, à la vérification, etc.

Une fonctionnalité de réseau peut être fournie sous la forme d'un service NaaS composite composé de plus d'un service de fonctionnalité de réseau. Il est également possible de fournir des services NaaS composites imbriqués sur le plan hiérarchique. Des services NaaS composites pourraient être utilisés pour différents types de capacités NaaS fournis au client CSC en fonction des objectifs de qualité de fonctionnement indiqués dans l'accord de niveau de service (SLA).

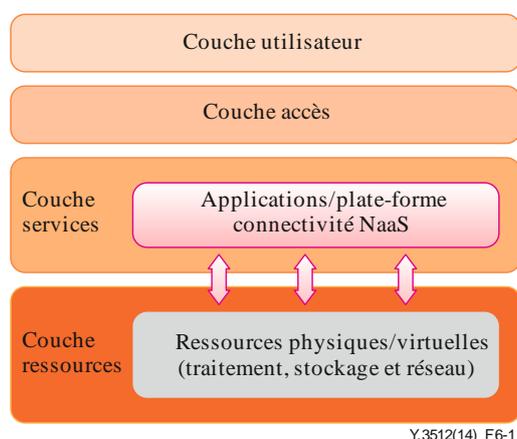


Figure 6-1 – Concept de haut niveau d'un réseau NaaS

L'Appendice II présente des cas d'utilisation de réseaux NaaS, dans lesquels les trois types de capacités de nuage (c'est-à-dire les types application, plate-forme et infrastructure) sont fournis au client CSC.

L'Appendice III présente des considérations relatives aux activités liées au réseau du fournisseur CSP.

NOTE 4 – En ce qui concerne la connectivité de réseau, il existe une différence importante entre l'infrastructure en tant que service (IaaS) et le réseau NaaS, puisque l'infrastructure IaaS est une catégorie de services de nuage qui est proposée uniquement pour un seul type de capacités de nuage, à savoir pour les capacités de type infrastructure [UIT-T Y.3500]. En revanche, un réseau NaaS est une catégorie de services de nuage qui peut être proposée pour les trois types de capacités de nuage.

7 Exigences fonctionnelles des applications NaaS

La présente section donne les exigences des applications NaaS définies à partir des cas d'utilisation décrits dans l'Appendice II.

7.1 Qualité de fonctionnement

- Il est recommandé qu'il soit possible de gérer la qualité de fonctionnement des applications NaaS afin de répondre aux besoins du client CSC.
- Il est recommandé que le fournisseur CSP NaaS surveille la qualité de fonctionnement des applications NaaS du point de vue de l'utilisation et de la fourniture.
- Il est recommandé que l'application NaaS fournie à un client CSC respecte les objectifs de qualité de fonctionnement indiqués dans l'accord SLA correspondant.

7.2 Exploitation et gestion

- Il est obligatoire que l'exploitation d'une application NaaS soit gérable et déterministe conformément aux politiques opérationnelles du fournisseur CSP.

- Il est recommandé que chaque application NaaS soit gérée par le fournisseur CSP NaaS de manière efficace et automatique, conformément au cadre commun de gestion des services et de gestion de l'exploitation des services du fournisseur CSP.
- Il est recommandé que le fournisseur CSP NaaS fournisse au client CSC une solution de gestion efficace permettant d'intégrer dans l'environnement d'exploitation de réseau du client CSC la gestion des applications NaaS mises à disposition.

7.3 Chaîne de services

- Il est recommandé que le fournisseur CSP NaaS fournisse des mécanismes permettant le chaînage des applications NaaS, par exemple les composants des applications NaaS requis et leur ordre.

7.4 Adresses IP multiples

- Il est recommandé que les applications NaaS prennent en charge de multiples adresses IP sur une interface de réseau lorsqu'elles fournissent des fonctions d'appareil de réseau (par exemple, pare-feu, répartiteurs de charge).

NOTE – Cette exigence est également applicable aux plates-formes NaaS et à la connectivité NaaS.

8 Exigences fonctionnelles des plates-formes NaaS

La présente section donne les exigences des plates-formes NaaS définies à partir des cas d'utilisation décrits dans l'Appendice II.

8.1 Plates-formes NaaS programmables

- Il est recommandé que le fournisseur CSP NaaS permette le déploiement d'applications de réseau sur une plate-forme NaaS par le fournisseur CSP et par le client CSC.
- Il est recommandé qu'une plate-forme NaaS fournisse des modules matériels ou logiciels spécialisés permettant l'accélération des fonctions de réseau.
- Il est recommandé qu'une plate-forme NaaS garantisse et indique la qualité de fonctionnement disponible pour les applications du client CSC exécutées sur ladite plate-forme.
- Il est recommandé qu'un service de plate-forme NaaS fournisse un cadre logiciel modulaire permettant de choisir et d'intégrer les fonctions de réseau, les fonctions de sécurité et les applications tierces.
- Il est recommandé que le fournisseur CSP NaaS fournisse un appui pour les plates-formes afin que le client CSC puisse gérer (par exemple installer, mettre à jour ou désinstaller) les modules qui lui appartiennent.
- Il est recommandé qu'une plate-forme NaaS fournisse des activateurs de réseau afin que le client CSC puisse initier (par exemple concevoir, construire, gérer) et exploiter les réseaux flexibles, modulables et à fonctions extensibles.
- Il est recommandé qu'une plate-forme NaaS fournisse une fonction de commande et de gestion unifiée sur des plates-formes NaaS réparties afin que le client CSC puisse modifier, déplacer ou supprimer des activateurs de réseau sur les plates-formes NaaS.

8.2 Composition et orientation dynamiques et flexibles des services de réseau

- Il est recommandé que le fournisseur CSP NaaS oriente le trafic du client CSC en utilisant une chaîne de services composée de manière dynamique et flexible de séquences personnalisées d'applications NaaS sur la plate-forme NaaS conformément à la logique de services propre au client CSC.

8.3 Isolation des chaînes de services destinées aux locataires

- Le fournisseur CSP NaaS peut, à titre d'option, prendre en charge l'isolation des chaînes de services destinées aux locataires qui associent différents services de réseau et sont mises en oeuvre sur la plate-forme NaaS.

8.4 Ajustement flexible des plates-formes NaaS

- Il est recommandé que le fournisseur CSP NaaS assure un ajustement flexible des ressources assignées à la plate-forme NaaS, afin d'atteindre les objectifs de qualité de fonctionnement pour les services et applications de réseau mis en oeuvre sur la plate-forme NaaS.

NOTE – Cette exigence vise à faire face à l'évolution de l'utilisation des services ou des applications dues, par exemple, à l'augmentation du trafic, à la modification du nombre d'utilisateurs, à l'ajout de nouveaux services ou à la mise en oeuvre de nouvelles applications.

8.5 Intégration des applications logicielles

- Il est recommandé que le fournisseur CSP NaaS prenne en charge l'intégration des applications logicielles déployées sur la plate-forme NaaS par le fournisseur CSP ou le client CSC, ou par les deux, afin de permettre la construction des solutions combinées.

9 Exigences fonctionnelles de la connectivité NaaS

La présente section donne les exigences de la connectivité NaaS définies à partir des cas d'utilisation décrits dans l'Appendice II.

9.1 Mécanisme de commande commun pour la connectivité NaaS

- Il est recommandé que le mécanisme de commande de la connectivité NaaS fourni par le fournisseur CSP NaaS prenne en charge la négociation des paramètres de connectivité (comme les caractéristiques des interfaces, les points d'extrémité des connexions, la version IP prise en charge, la qualité de service, le type de VPN L3/L2, la stratégie d'extension de la connectivité (par exemple, partie 10 de [b-IETF RFC 4364], les informations d'acheminement (par exemple, les cibles d'acheminement du protocole de passerelle frontière (BGP))).
- Il est recommandé que le fournisseur CSP NaaS fournisse un mécanisme de commande commun de la connectivité NaaS permettant de fournir la connectivité NaaS identifiée de manière sécurisée et avec une qualité de service garantie.
- Il est recommandé que le mécanisme de commande de la connectivité NaaS soit capable de faire face au cas de figure dans lequel les mécanismes d'identification du client CSC utilisés du côté du fournisseur CSP NaaS et du côté de l'extrémité connectée sont différents.
- Le fournisseur CSP NaaS peut, à titre d'option, fournir une connectivité isolée pour les locataires de réseau.

9.2 Accord SLA unifié pour de multiples réseaux optimisés

- Il est recommandé que le fournisseur CSP NaaS fournisse des services de connectivité de réseau en utilisant un accord SLA unifié relatif à la gestion par le client CSC de multiples réseaux optimisés afin de simplifier et d'unifier la commande et la gestion des réseaux.

NOTE – Grâce à ce mécanisme, le fournisseur CSP est en mesure de créer et d'ajouter de nouvelles fonctionnalités à son réseau, afin de fournir des services de grande qualité qui permettent de répondre aux exigences différenciées du client CSC.

- Il est recommandé que la politique applicable aux services NaaS composites soit définie dans l'accord SLA.

NOTE 1 – Un service NaaS peut être un service composite, comprenant plus d'un service NaaS.

NOTE 2 – Cette exigence est également applicable aux applications NaaS et aux plates-formes NaaS.

9.3 Utilisation de réseaux de transport choisis de façon dynamique

- Il est recommandé que le fournisseur CSP NaaS utilise des réseaux de transport qu'il a choisis de manière dynamique entre plusieurs réseaux physiques et virtuels, afin de fournir des services de connectivité de réseau (rétablissement, bande passante à la demande, qualité de service garantie, etc.).

NOTE – Les réseaux de transport peuvent être hétérogènes en termes de technologie et de domaine administratif.

9.4 Mécanisme unifié de commande de réseau

- Il est recommandé que le fournisseur CSP NaaS fournisse un mécanisme unifié de commande pour la connectivité NaaS de bout en bout offerte à un client CSC.

NOTE – La connectivité NaaS pourrait être fournie par des réseaux hétérogènes multiples ou par un réseau utilisant une ou plusieurs plates-formes ou applications NaaS exécutant des fonctions de réseau.

9.5 Reconfiguration élastique du réseau

- Il est recommandé que le fournisseur CSP assure la reconfiguration élastique du réseau, afin de garantir l'élasticité des ressources de calcul et de stockage et de maintenir la continuité du service.

9.6 Solution transparente et de bout en bout d'attribution de la bande passante

- Il est recommandé que le fournisseur CSP NaaS fournisse une solution transparente et de bout en bout pour l'attribution de la bande passante indépendamment de la technologie et de l'architecture de réseau.

9.7 Capacité symétrique ou asymétrique

- Il est recommandé que le fournisseur CSP NaaS fournisse une capacité de liaison de réseau symétrique ou asymétrique en fonction de la demande du client CSC.

9.8 Ingénierie du trafic optimisée et à granulation fine

- Il est recommandé que le fournisseur CSP NaaS fournisse au client CSC une vue à granulation fine de l'utilisation des ressources de réseau.
- Il est recommandé que le fournisseur CSP NaaS recueille des mesures d'utilisation en temps quasi réel et des données relatives à la topologie provenant de ses propres équipements de réseau.
- Il est recommandé que le fournisseur CSP NaaS commande l'attribution des ressources de réseau en reconfigurant les profils de réseau ainsi que les propriétés (par exemple, topologie, bande passante) en fonction de l'évolution dynamique des demandes de trafic.
- Le fournisseur CSP NaaS peut, à titre d'option, fournir une gestion centralisée du trafic, afin de parvenir à une ingénierie optimisée du trafic.

9.9 Coexistence avec les services et les fonctions des réseaux existants

- Il est recommandé que le fournisseur CSP NaaS évite ou limite les incidences que la mise en place de nouveaux services de connectivité de réseau pourrait avoir sur la qualité de fonctionnement et sur la flexibilité.

- Il est recommandé que le fournisseur CSP NaaS prenne en charge la coexistence des nouveaux services de connectivité de réseau avec les systèmes existants.

9.10 Vue de commande centralisée et vue abstraite des ressources

- Le fournisseur CSP NaaS peut, à titre d'option, prendre en charge la vue centralisée sur le plan logique de la commande et de la gestion des ressources de réseau.
- Le fournisseur CSP NaaS peut, à titre d'option, fournir au client CSC une vue abstraite des ressources de réseau sous-jacentes.

9.11 Commande de service limitée pour le client CSC

- Il est recommandé que le fournisseur CSP NaaS donne au client CSC des moyens de commande de service adaptés afin de répondre aux exigences de qualité de service sensibles au facteur temps, comme les quantités de bande passante, les temps de latence maximum et d'autres paramètres de qualité de service.

9.12 Subdivision de réseau isolée logiquement

- Le fournisseur CSP NaaS peut, à titre d'option, mettre en oeuvre une subdivision de réseau isolée logiquement (LINP).

NOTE – Les subdivisions LINP sont décrites dans [UIT-T Y.3011]. Voir le § 3.1.14.

9.13 Mécanisme de réseau superposé

- Il est possible, à titre d'option, que la connectivité NaaS prenne en charge les réseaux superposés virtuels venant au-dessus du réseau physique sous-jacent.

9.14 Chevauchement des adresses IP privées

- Il est recommandé que le fournisseur CSP NaaS permette aux différents clients CSC d'utiliser leurs propres adresses IP privées, même en cas de chevauchement avec les adresses de sous-réseau.

9.15 Interfonctionnement de solutions VPN différentes

- Il est recommandé que le fournisseur CSP NaaS prenne en charge l'interfonctionnement entre des technologies VPN différentes.

9.16 Connexion VPN dans un environnement mobile

- Il est recommandé que le fournisseur CSP NaaS prenne en charge la connectivité VPN dans un environnement mobile.

9.17 Connexion au réseau du fournisseur CSP NaaS via l'Internet public

- Il est recommandé que le fournisseur CSP NaaS permette au client CSC de se connecter au fournisseur CSP NaaS via l'Internet public.

10 Considérations relatives à la sécurité

Les éléments liés à la sécurité devant être pris en considération dans les environnements de l'informatique en nuage, y compris pour les réseaux NaaS, correspondent aux problèmes de sécurité décrits pour les fournisseurs CSP dans [UIT-T X.1601]. En particulier, [UIT-T X.1601] présente une analyse des menaces et des problèmes de sécurité et décrit les capacités de sécurité qui pourraient atténuer ces menaces et résoudre les problèmes de sécurité.

Appendice I

Méthodologie pour la définition des exigences et de l'architecture fonctionnelles des réseaux NaaS

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Vu la méthodologie de normalisation et le déroulement classique des études, les représentations abstraites des entités fonctionnelles et leurs interactions mutuelles reposent sur les exigences fonctionnelles et sur l'analyse des cas d'utilisation correspondants, qui, ensemble, constituent une unité de normalisation. Par conséquent, il est obligatoire de définir les exigences et l'architecture fonctionnelles des réseaux NaaS selon les étapes et les priorités suivantes.

Etape 1: Cas d'utilisation et exigences fonctionnelles des réseaux NaaS qui sont décrits respectivement dans l'Appendice II et dans les § 7 à 9 de la présente Recommandation. Il est à noter que toutes les exigences fonctionnelles sont définies à partir des cas d'utilisation correspondants.

Etape 2: L'architecture fonctionnelle des réseaux NaaS devrait être fondée sur la présente Recommandation.

En outre, les exigences générales concernant les réseaux NaaS sont décrites dans [UIT-T Y.3501].

Appendice II

Cas d'utilisation des réseaux NaaS

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Le présent appendice porte sur trois types de cas d'utilisation NaaS: les cas d'utilisation relatifs aux applications NaaS, les cas d'utilisation relatifs aux plates-formes NaaS et les cas d'utilisation relatifs à la connectivité NaaS. Chaque type de cas d'utilisation NaaS est également divisé en cas d'utilisation généraux et en cas d'utilisation détaillés.

II.1 Modèle de présentation des cas d'utilisation

Pour faciliter la lecture et l'organisation pratique des éléments, les cas d'utilisation définis dans l'Appendice II sont présentés selon le format harmonisé suivant.

Titre	Intitulé du cas d'utilisation.
Description	Description du cas d'utilisation.
Rôles	Rôles intervenant dans le cas d'utilisation.
Figure (facultatif)	Figure présentant le cas d'utilisation (facultatif); elle n'est pas obligatoire.
Conditions préalables (facultatif)	Conditions préalables nécessaires qui devraient être réunies avant que la mise en oeuvre du cas d'utilisation débute.
Conditions, après mise en oeuvre (facultatif)	Conditions résultant de la mise en oeuvre du cas d'utilisation.
Exigences définies	Exigences définies à partir du cas d'utilisation, qui sont décrites en détail dans les paragraphes correspondants.

II.2 Cas d'utilisation relatifs aux applications NaaS

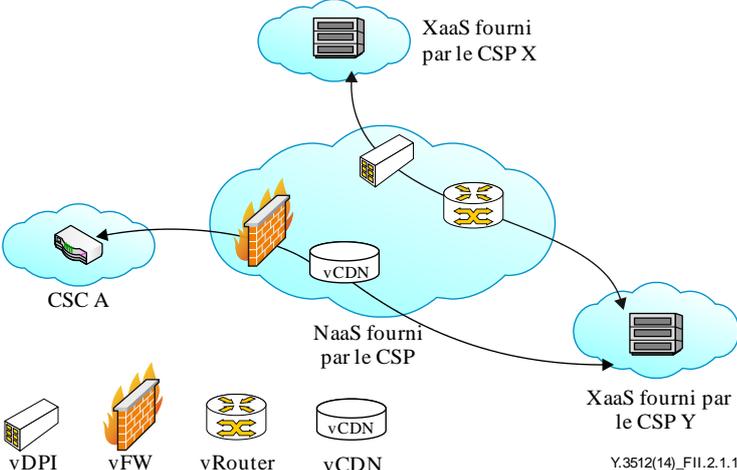
Les paragraphes ci-après décrivent les cas d'utilisation dans lesquels le client CSC NaaS peut fournir et utiliser des applications de réseau.

NOTE – Dans les paragraphes suivants, l'abréviation XaaS représente l'une quelconque catégorie de services de nuage, comme les logiciels en tant que service (SaaS), les plates-formes en tant que service (PaaS), l'infrastructure en tant que service (IaaS), les communications en tant que service (CaaS), etc.

II.2.1 Cas d'utilisation généraux

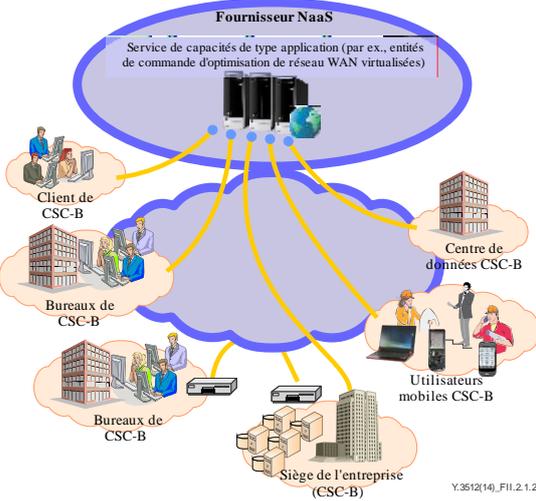
II.2.1.1 Cas d'utilisation général des applications NaaS

Titre	Cas d'utilisation général des applications NaaS
Description	Un client CSC XaaS A utilise les applications de réseau (par exemple, inspection DPI virtuelle (vDPI), pare-feu vFW, réseau vCDN) fournies par un fournisseur CSP NaaS. Ces applications peuvent être chaînées par le fournisseur CSP NaaS.
Rôles	Client CSC, fournisseur CSP.

Figure	 <p>NOTE – Les routeurs virtuels (vRouter) peuvent également être utilisés pour la connectivité NaaS.</p>
Conditions préalables (facultatif)	<ul style="list-style-type: none"> – Il y a une connectivité entre le client CSC XaaS A et le fournisseur CSP XaaS Y. – Il y a une connectivité entre le fournisseur CSP XaaS X et le fournisseur CSP XaaS Y. – Le fournisseur CSP XaaS ou le client CSC demande qu'une application de réseau (vFW, vCDN, vDPI, vRouter, etc.) soit chaînée avec la connectivité.
Conditions après mise en oeuvre (facultatif)	<ul style="list-style-type: none"> – Le fournisseur CSP NaaS propose des applications de réseau au client CSC/fournisseur CSP XaaS sur la connectivité de réseau existante.
Exigences définies	<ul style="list-style-type: none"> – Application de réseau virtuel à la demande – Application de réseau modulable – Chaîne d'applications de réseau – Applications à qualité de service garantie – Applications de réseau sécurisées – Applications de réseau résilientes – Adresses IP multiples (voir le § 7.4) <p>NOTE – Les six premières exigences correspondent aux exigences générales des réseaux NaaS indiquées dans [UIT-T Y.3501].</p>

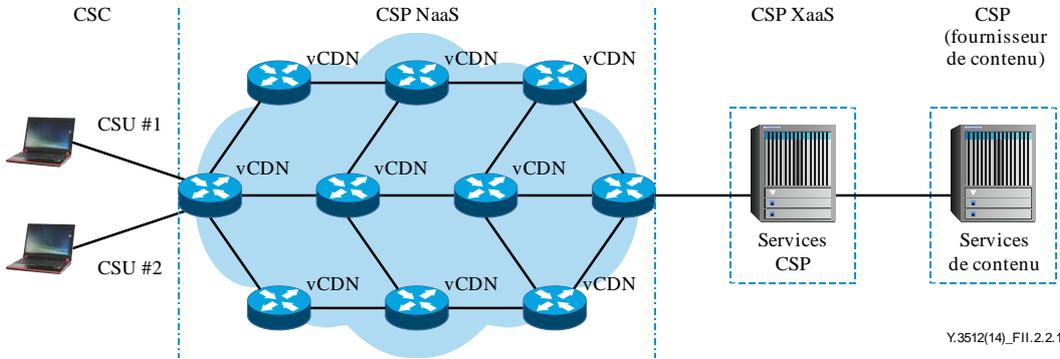
II.2.1.2 Cas d'utilisation des applications NaaS pour la fourniture d'applications

Titre	Cas d'utilisation des applications NaaS pour la fourniture d'applications
Description	<p>Prenons l'hypothèse où l'entreprise CSC-B cherche des services d'application NaaS pour profiter des principales caractéristiques des services d'informatique en nuage. Par exemple, l'entreprise veut accélérer le trafic du réseau saturé du fait d'applications commerciales. L'optimisation du réseau étendu (WAN) est particulièrement essentielle pour le bon fonctionnement des applications commerciales de l'entreprise. L'entreprise CSC-B veut que le déploiement des solutions d'optimisation du réseau WAN soit fondé sur l'utilisation et que des fonctionnalités flexibles soient prises en charge à la demande. Les équipements traditionnels d'optimisation WAN ne permettent pas de répondre à ces exigences, en particulier en ce qui concerne le coût total de propriété et l'élasticité de déploiement. Le fournisseur CSP NaaS doit pouvoir fournir au client CSC-B des solutions virtuelles d'accélération WAN en adéquation avec ses besoins opérationnels dynamiques.</p>
Rôles	Fournisseur CSP, client CSC

<p>Figure (facultatif)</p>	
<p>Conditions préalables (facultatif)</p>	<p>L'entreprise CSC-B a besoin d'accélérer le trafic de réseau qui est saturé à cause d'applications commerciales.</p>
<p>Conditions après mise en oeuvre (facultatif)</p>	<p>L'entreprise CSC-B a utilisé une solution virtuelle d'accélération WAN fournie par le fournisseur CSP NaaS afin de répondre aux besoins opérationnels dynamiques.</p>
<p>Exigences définies</p>	<ul style="list-style-type: none"> – Self-service à la demande – Multilocataires – Mutualisation des ressources – Elasticité et modularité rapides – Service en fonction de l'utilisation – Garantie et surveillance de la qualité de fonctionnement – Co-existence et compatibilité avec les équipements de réseau existants du client CSC – Prise en charge de l'interopérabilité pour la gestion et l'orchestration – Sécurité et résilience – Qualité de fonctionnement (voir le § 7.1) – Exploitation et gestion (voir le § 7.2) <p>NOTE – Les neuf premières exigences correspondent aux exigences générales des réseaux NaaS indiquées dans [UIT-T Y.3501].</p>

II.2.2 Cas d'utilisation détaillés

II.2.2.1 Cas d'utilisation des plates-formes NaaS pour les réseaux CDN en nuage

Titre	Cas d'utilisation des plates-formes NaaS pour les réseaux de fourniture de contenu (CDN) en nuage
Description	<p>Le fournisseur de contenu agissant en tant que client CSC stocke le contenu dans le centre de données et surveille son utilisation. Lorsque l'utilisation du contenu atteint un niveau donné de popularité ou si des prévisions laissent penser au fournisseur de contenu que la popularité du contenu devrait augmenter pendant une période de temps définie (par exemple, transmission vidéo d'une manifestation sportive), le fournisseur de contenu crée un réseau CDN virtuel afin de déplacer temporairement le contenu du centre de données vers le réseau (vCDN). Le fournisseur CSP XaaS reçoit le contenu provenant du fournisseur de contenu (qui peut lui-même créer un service de distribution). Le contenu est fourni aux utilisateurs de services de nuage (CSU) depuis le centre de données du fournisseur CSP XaaS grâce au réseau du fournisseur CSP NaaS. Le fournisseur CSP XaaS offre la possibilité de stocker le contenu et de surveiller les paramètres d'utilisation. Le fournisseur CSP XaaS, en coopération avec le fournisseur CSP NaaS, peut reproduire le contenu dans les noeuds du réseau, créant ainsi un service CDN virtuel. Dans l'ensemble, le fournisseur CSP XaaS prend en charge les fonctions CDN, le réseau CDN étant d'une certaine manière ainsi "émulé" par le fournisseur CSP XaaS, qui coopère avec le fournisseur CSP NaaS.</p>
Rôles	Utilisateur CSU, client CSC, fournisseur CSP
Figure (facultatif)	 <p style="text-align: right; font-size: small;">Y.3512(14)_FII.2.2.1</p>
Conditions préalables (facultatif)	<ul style="list-style-type: none"> - Le fournisseur de contenu agissant en tant que client CSC stocke le contenu dans les centres de données du fournisseur CSP XaaS. - Le fournisseur de contenu agissant en tant que client CSC surveille l'utilisation du contenu.
Conditions après mise en oeuvre (facultatif)	<ul style="list-style-type: none"> - Le fournisseur CSP XaaS offre le service CDN virtuel en utilisant les ressources de réseau du fournisseur CSP NaaS. - Le fournisseur de contenu agissant en tant que client CSC décide de déplacer le contenu depuis le centre de données vers le réseau CDN virtuel pour une période de temps donnée.
Exigences définies	<ul style="list-style-type: none"> - Qualité de fonctionnement (voir le § 7.1) - Exploitation et gestion (voir le § 7.2) - Chaîne de services (voir le § 7.3)

II.3 Cas d'utilisation relatifs aux plates-formes NaaS

II.3.1 Cas d'utilisation généraux

Aucun.

II.3.2 Cas d'utilisation détaillés

II.3.2.1 Cas d'utilisation des plates-formes NaaS pour les chaînes de services

Titre	Cas d'utilisation des plates-formes NaaS pour les chaînes de services.
Description	<p>Etant donné que les locataires d'un client CSC ont de plus en plus d'exigences concernant la diversité et la complexité des services, le fournisseur CSP a besoin de fournir des services d'application de réseau intégrés, comme l'inspection approfondie des paquets (DPI), la détection des intrusions, la prévention des intrusions, la répartition de charge, les pare-feu, etc. Traditionnellement, cet ensemble de services est fourni grâce à des éléments de réseau physique dédiés, qui ont une capacité et des fonctionnalités de réseau limitées, des modalités de configuration et de mise à jour complexes et des délais de fourniture importants. On appelle chaîne de services le cas dans lequel le résultat d'un service est utilisé comme élément de base pour fournir un autre service. Dans les réseaux traditionnels, l'organisation de la chaîne de services, par exemple une chaîne composée d'un système de protection contre les intrusions (IPS), d'un répartiteur de charge et d'un dispositif DPI, nécessite une configuration dédiée et n'est pas flexible en cas, par exemple, d'augmentation du trafic, d'ajout/de suppression de services dans la chaîne.</p> <p>Pour une plus grande flexibilité des services, il est recommandé que le fournisseur CSP NaaS fournisse une plate-forme NaaS programmable, sur laquelle des applications NaaS (par exemple, vRouter, vCDN, vEPC, etc.) peuvent être déployées, afin de diriger le trafic du client CSC grâce à une séquence d'applications NaaS personnalisée.</p>
Rôles	Client CSC (locataire A, locataire B), fournisseur CSP
Figure (facultatif)	<p>—> Chaîne de services de réseau du locataire A - - -> Chaîne de services de réseau du locataire B</p> <p style="text-align: right;">Y.3512(14)_F11.3.2.1</p>
Conditions préalables (facultatif)	<ul style="list-style-type: none"> – Le fournisseur CSP peut fournir des solutions utilisant des appareils de réseau physique dédiés pour des services comme l'inspection DPI, la détection des intrusions, la prévention des intrusions, la répartition de charge, les pare-feu, etc.
Conditions après mise en oeuvre (facultatif)	<ul style="list-style-type: none"> – Le fournisseur CSP peut fournir des services de réseau composites virtuels ou physiques ou les deux, ou des chaînes de services de manière dynamique et flexible conformément à la logique de service propre au client CSC avec des délais de déploiement, de configuration et de mise à plus courts qu'avec une solution utilisant des appareils de réseau physique dédiés.
Exigences définies	<ul style="list-style-type: none"> – Plate-forme NaaS programmable (voir le § 8.1). – Composition et orientation dynamiques et flexibles des services de réseau (voir le § 8.2). – Isolation des chaînes de services destinés aux locataires (voir le § 8.3).

II.3.2.2 Cas d'utilisation des plates-formes NaaS pour la fourniture de plates-formes

Titre	Cas d'utilisation des plates-formes NaaS pour la fourniture de plates-formes
Description	<p>Le client CSC-A est un opérateur de réseau. Il souhaite construire un système d'analyse du trafic évolué et un mécanisme d'élaboration de rapports multidimensionnels utilisant des fonctionnalités DPI s'ajustant de manière dynamique, des services opportunistes à faible risque et, dans un court délai de mise en oeuvre, un réseau CDN multilocataires, etc., dans les réseaux mobiles. Or, les appareils de réseau fondés sur du matériel classique proposés par les fabricants empêchent le déploiement rapide de nouvelles fonctionnalités de réseaux convergentes et de services rentables. Ils ne sont en effet ni ajustables à la demande ni suffisamment flexibles.</p> <p>Le client CSC-A a la possibilité de répondre à ses besoins en matière d'innovation fonctionnelle en utilisant une plate-forme NaaS pour développer les fonctionnalités et les services nécessaires. L'innovation grâce à une plate-forme NaaS lui permet d'utiliser les services de réseau du fournisseur CSP et de les combiner avec les fonctionnalités qu'il a mises au point. Toutes les fonctionnalités peuvent être intégrées par le client CSC-A sur la base de la plate-forme NaaS, afin de construire des services de réseau évolués, par exemple un noyau paquet évolué (EPC) virtualisé, une plate-forme DPI logicielle, des environnements de développement intégré (IDE). La capacité de la plate-forme NaaS doit pouvoir s'ajuster de manière élastique en fonction de l'utilisation des services de réseau évolués, afin de fournir la qualité de fonctionnement requise. Il faut en outre des solutions permettant l'intégration des services de réseau du fournisseur CSP et du logiciel développé par le client CSC-A.</p>
Rôles	Fournisseur CSP, client CSC.
Figure (facultatif)	
Conditions préalables (facultatif)	Le client CSC-A a besoin de construire des services de réseau évolués en utilisant des équipements matériels dédiés pour chaque fonctionnalité et de gérer l'ensemble du réseau.
Conditions après mise en oeuvre (facultatif)	Le client CSC-A a utilisé la plate-forme NaaS pour combiner des services de réseau du fournisseur CSP avec des fonctionnalités qu'il a lui-même élaborées et pour les intégrer dans des services de réseau évolués.
Exigences définies	<ul style="list-style-type: none"> - Ajustement flexible des plates-formes NaaS (voir le § 8.4) - Intégration des applications logicielles (voir le § 8.5)

II.4 Cas d'utilisation relatifs à la connectivité NaaS

Les paragraphes décrivent ci-après les cas d'utilisation pour lesquels le client CSC NaaS peut fournir et utiliser la connectivité de réseau.

II.4.1 Cas d'utilisation généraux

II.4.1.1 Cas d'utilisation général de la connectivité NaaS

NOTE – Le cas d'utilisation ci-après repose sur un cas d'utilisation présenté dans [UIT-T Y.3501].

Nom	Cas d'utilisation général de la connectivité NaaS.
Description	Un fournisseur CSP NaaS établi, maintient et libère la connectivité de réseau entre des clients CSC et entre un fournisseur CSP et un client CSC en tant que service de nuage. Il peut s'agir d'une connectivité à la demande ou semi-permanente.
Rôles	Client CSC, fournisseur CSP.
Figure	
Conditions préalables (facultatif)	<ul style="list-style-type: none"> – Il n'y a pas de connectivité entre le client CSC XaaS A et le fournisseur CSP XaaS Y. – Il n'y a pas de connectivité entre le fournisseur CSP XaaS X et le fournisseur CSP XaaS Y. – Soit le client CSC XaaS A, soit le fournisseur CSP XaaS Y demande que la connectivité soit assurée entre eux en donnant leurs identificateurs de point d'extrémité et les caractéristiques associées (concernant la qualité de service et la sécurité) pour la connectivité. – Soit le fournisseur CSP XaaS X, soit le fournisseur CSP XaaS Y demande que la connectivité soit assurée entre eux en donnant leurs identificateurs de point d'extrémité et les caractéristiques associées (concernant la qualité de service et la sécurité) pour la connectivité.
Conditions après mise en oeuvre (facultatif)	<ul style="list-style-type: none"> – Le client CSC XaaS A et le fournisseur CSP XaaS Y peuvent communiquer entre eux. – Le fournisseur CSP XaaS X et le fournisseur CSP XaaS Y peuvent communiquer entre eux.
Exigences	<ul style="list-style-type: none"> – Configuration du réseau à la demande. – Compatibilité avec des réseaux hétérogènes. – Connectivité à qualité de service garantie. – Connectivité sécurisée. – Mécanisme de commande commun pour la connectivité NaaS (voir le § 9.1). <p>NOTE – Les 4 premières exigences correspondent aux exigences générales des réseaux NaaS indiquées dans [UIT-T Y.3501].</p>

II.4.2 Cas d'utilisation détaillés

II.4.2.1 Cas d'utilisation de la connectivité NaaS pour les réseaux de transport dynamiques

Titre	Cas d'utilisation de la connectivité NaaS pour les réseaux de transport dynamiques
Description	<p>Le client CSC demande un service de connectivité réparti sur le plan géographique et une capacité de trafic dynamique pouvant prendre en charge l'éclatement du nuage (par exemple, migration des machines virtuelles ou transfert de fichiers de données volumineux vers des centres de données situés à différents endroits), qui entraîne une forte augmentation du trafic passant par le réseau dorsal du fournisseur CSP.</p> <p>Le réseau IP et le réseau de transport du fournisseur CSP sont gérés séparément et, par conséquent, ne peuvent pas fournir le mécanisme de commande commun pour l'ajustement dynamique de la bande passante. Afin de garantir la continuité des services et un accord SLA cohérent pour le client CSC, le fournisseur CSP devrait dans ce cas proposer un surdimensionnement des liaisons, dont la plupart ne seraient pas utilisées efficacement, ce qui entraînerait un gaspillage des ressources.</p> <p>Il est recommandé que le fournisseur CSP prenne en charge la forte augmentation du</p>

	trafic de transit passant par son réseau dorsal sans avoir recours à des approches classiques de surdimensionnement des ressources de réseau.
Rôles	Client CSC, fournisseur CSP.
Figure (facultatif)	
Conditions préalables (facultatif)	
Conditions après mise en oeuvre (facultatif)	
Exigences définies	<ul style="list-style-type: none"> – Accord SLA unifié pour de multiples réseaux optimisés (voir le § 9.2). – Utilisation de réseaux de transport choisis de façon dynamique (voir le § 9.3). – Mécanisme unifié de commande de réseau (voir le § 9.4).

II.4.2.2 Cas d'utilisation de la connectivité Naas pour des VPN flexibles et étendus

Titre	Cas d'utilisation de la connectivité Naas pour des VPN flexibles et étendus
Description	<p>Les différents sites VPN sont raccordés grâce à un VPN IP BGP/MPLS. Les ressources de traitement et le sous-réseau correspondant sont déplacés depuis le centre de données du client CSC vers le centre de données du fournisseur CSP, qui n'est pas encore associé au VPN en tant que site VPN. Afin d'ajouter ce nouveau site au VPN existant, il est nécessaire de fournir un nouveau sous-réseau dans le centre de données du fournisseur CSP et d'organiser un nouveau routage et réacheminement virtuels (VRF) dans son routeur périphérique. La migration du sous-réseau correspondant depuis le centre de données du client CSC vers le centre de données du client CSP et la suppression du sous-réseau dans le centre de données du client CSC doivent être annoncées aux autres routeurs périphériques. La procédure pratique est présentée dans la figure ci-après.</p> <ol style="list-style-type: none"> 1) Les ressources de traitement et le sous-réseau correspondant sont déplacés depuis le centre de données du client CSC vers le centre de données du client CSP. 2) Un nouveau type de VRF est configuré dans le routeur périphérique du centre de données du fournisseur CSP. 3) La suppression du sous-réseau du client CSC est annoncée à tous les sites VPN grâce à une mise à jour MP-BGP. 4) Le nouveau sous-réseau du fournisseur CSP est annoncé à tous les sites VPN grâce à une mise à jour MP-BGP. <p>Il est nécessaire d'assurer la continuité des services pendant toute la durée de la procédure de migration et de reconfiguration. Or, le VPN existant est une boîte noire du point de vue du client CSC et, à ce titre, il ne peut être fourni et reconfiguré par le client CSC. En outre, la technologie VPN actuelle ne permet pas de prendre en charge l'ajout ou la suppression dynamique de sites VPN et l'augmentation et la réduction de la capacité de bande passante.</p>
Rôles	Client CSC, fournisseur CSP.

<p>Figure (facultatif)</p>	<p>① Migration des ressources ② Nouveau VRF ③ Mise à jour MP-BGP ④ Mise à jour MP-BGP</p>
<p>Conditions préalables (facultatif)</p>	
<p>Conditions après mise en oeuvre (facultatif)</p>	
<p>Exigences définies</p>	<p>– Reconfiguration élastique du réseau (voir le § 9.5).</p>

II.4.2.3 Cas d'utilisation de la connectivité NaaS pour les services BoD

<p>Titre</p>	<p>Cas d'utilisation de la connectivité NaaS pour les services BoD</p>
<p>Description</p>	<p>Ce scénario concerne l'accès du client CSU au service d'informatique en nuage offert par le fournisseur CSP XaaS (par exemple, infrastructure de bureau virtuel (VDI), diffusion de vidéos en continu). Le client CSU accède au service depuis un emplacement fixe, par exemple en utilisant un réseau local (LAN) d'entreprise, ou depuis un emplacement mobile (par exemple un terminal mobile). Le fournisseur CSP XaaS dessert les services sur la base de ses propres centres de données et n'a aucune incidence sur la qualité de fonctionnement d'une connectivité donnée entre les utilisateurs finals et le centre de données où le service est hébergé. Du point de vue de l'utilisateur CSU, la qualité d'expérience pour le service dépend à la fois de la qualité de fonctionnement du centre de données et de la qualité de fonctionnement du réseau. Le fournisseur CSP XaaS est en mesure de garantir une qualité de service donnée uniquement pour son propre centre de données. Cette qualité pourrait être détériorée par la qualité de fonctionnement du réseau sur la connexion entre le client CSC et un centre de données particulier. Le fournisseur CSP XaaS à lui seul n'est pas en mesure d'avoir une incidence sur la qualité de fonctionnement du réseau sans interagir avec le fournisseur CSP NaaS.</p> <p>Pour garantir la qualité de service de bout en bout, il est par exemple possible d'appliquer des réservations de bande passante dans le réseau entre l'utilisateur CSU et le centre de données. Cette solution permet de garantir à une certaine qualité de fonctionnement du réseau et peut servir de base pour l'accord SLA de bout en bout relatif au service conclu entre un utilisateur CSU et le fournisseur CSP XaaS. Pour répondre à ces besoins, fournisseur CSP XaaS interagit avec le fournisseur CSP NaaS. Le fournisseur CSP NaaS peut être un acteur quelconque qui a la capacité d'offrir une connectivité entre le fournisseur CSP XaaS et le client CSC auquel l'utilisateur CSU</p>

	appartient.
Rôles	Utilisateur CSU, client CSC, fournisseur CSP.
Figure (facultatif)	<p>Y.3512(14)_FII.4.2.3</p> <p>— Service BoD (réservation et fourniture de bande passante) — Service autre que service BoD (engorgement du trafic de réseau)</p>
Conditions préalables (facultatif)	<ul style="list-style-type: none"> – Le fournisseur CSP XaaS n'a aucune incidence sur les paramètres de connectivité entre le service et l'utilisateur CSU.
Conditions après mise en oeuvre (facultatif)	<ul style="list-style-type: none"> – Le fournisseur CSP XaaS offre une qualité de service ou un accord SLA de bout en bout au client CSC, en se fondant sur une coopération avec le fournisseur CSP NaaS.
Exigences définies	<ul style="list-style-type: none"> – Solution transparente et de bout en bout d'attribution de la bande passante (voir le § 9.6). – Capacité symétrique ou asymétrique (voir le § 9.7).

II.4.2.4 Cas d'utilisation de la connectivité NaaS pour l'ingénierie du trafic optimisée

Titre	Cas d'utilisation de la connectivité NaaS pour l'ingénierie du trafic optimisée
Description	<p>Le fournisseur CSP fournit des services de connectivité de réseau à un client CSC, afin que celui-ci puisse interconnecter ses propres centres de données situés à différents endroits. Avec l'augmentation des services de nuage déployés dans les centres de données du client CSC, un volume croissant de trafic, par exemple pour la mise en miroir des données, la redondance, la synchronisation des bases de données, la migration des machines virtuelles, la duplication de mémoire active-active, traverse le réseau dorsal du fournisseur CSP du fait du nombre croissant de services répartis du client CSC.</p> <p>Actuellement, le fournisseur CSP fournit généralement au client CSC des services de connectivité statiques qui se traduisent soit par une capacité de service surdimensionnée et sous-utilisée, soit par des services surdimensionnés à capacité plafonnée.</p> <p>Afin d'utiliser plus efficacement ses ressources de connectivité, le fournisseur CSP peut, à titre de solution, prendre en charge une fonction décisionnelle centrale pour l'ingénierie de trafic du réseau dorsal. Cette solution doit au minimum coexister avec les autres solutions de réseau existantes utilisées par le fournisseur CSP pour la prise en charge des autres services.</p>
Rôles	Client CSC, fournisseur CSP

<p>Figure (facultatif)</p>	
<p>Conditions préalables (facultatif)</p>	
<p>Conditions après mise en oeuvre (facultatif)</p>	
<p>Exigences définies</p>	<ul style="list-style-type: none"> – Ingénierie du trafic optimisée et à granulation fine (voir le § 9.8). – Coexistence avec les services et les fonctions de réseau existants (voir le § 9.9). – Vue de commande centralisée et vue abstraite des ressources (voir le § 9.10).

II.4.2.5 Cas d'utilisation de la connectivité NaaS pour la qualité de fonctionnement à la demande

<p>Titre</p>	<p>Cas d'utilisation de la connectivité NaaS pour la qualité de fonctionnement à la demande</p>
<p>Description</p>	<p>Le client CSC demande au fournisseur CSP de fournir une qualité de fonctionnement de réseau à la demande (par exemple, quantités de bande passante, latences maximales et autres paramètres de qualité de service), qui comprend la capacité de créer, de modifier et de redimensionner de manière dynamique les liaisons. Or, la solution traditionnelle nécessitant une intervention humaine n'offre pas de fonctionnalités d'automatisation, d'où la difficulté d'offrir des services autonomes et de faire face à l'évolution dans le temps des exigences de qualité de fonctionnement du réseau. En outre, des changements fréquents se traduisent parfois par un encombrement et une instabilité car le trafic, qui vient de multiples sources, passe par une seule et même liaison de réseau.</p> <p>Le fournisseur CSP fournit au client CSC une capacité de commande adéquate qui lui permet de demander des services via un portail, le réseau physique sous-jacent n'étant pas visible pour le client CSC.</p>
<p>Rôles</p>	<p>Client CSC, fournisseur CSP.</p>

<p>Figure (facultatif)</p>	
<p>Conditions préalables (facultatif)</p>	
<p>Conditions après mise en oeuvre (facultatif)</p>	
<p>Exigences définies</p>	<ul style="list-style-type: none"> – Vue de commande centralisée et vue abstraite des ressources (voir le § 9.10). – Commande de services limitée pour le client CSC (voir le § 9.11).

II.4.2.6 Cas d'utilisation de la connectivité NaaS pour les routeurs virtuels

<p>Titre</p>	<p>Cas d'utilisation de la connectivité NaaS pour les routeurs virtuels</p>
<p>Description</p>	<p>Selon [UIT-T Y.3500], l'une des principales caractéristiques d'un service de nuage est d'être multilocataires, ce qui oblige les fournisseurs CSP à fournir au client CSC soit des ressources physiques ou virtuelles partagées soit les deux, afin que de multiples locataires et leurs ressources et données soient isolés les uns des autres et inaccessibles les uns aux autres. Ces locataires partagent les mêmes ressources physiques sous-jacentes, y compris les serveurs physiques, les mémoires physiques et les réseaux physiques, et chaque locataire se voit attribuer ses propres ressources logiques (machines virtuelles, mémoire virtuelle et réseaux virtuels notamment). Ces ressources logiques doivent être isolées les unes des autres et les ressources virtuelles de calcul, de stockage et de réseau doivent être intégrées et adaptées avec une granularité fine.</p> <p>Or, les routeurs et les commutateurs physiques sous-jacents existants du réseau de transport d'un fournisseur CSP ne contiennent pas l'état pour chaque locataire, notamment les adresses de commande d'accès au support (MAC) et les adresses IP du locataire, ainsi que les politiques de réseau associées à la machine virtuelle appartenant au locataire. En d'autres termes, les tables de transmission des routeurs et commutateurs physiques sous-jacents contiennent uniquement les préfixes IP ou les adresses MAC des serveurs physiques.</p> <p>Un routeur virtuel est un routeur mis en oeuvre par logiciel, possiblement à l'intérieur de l'infrastructure de virtualisation. Il fournit la connectivité entre les machines virtuelles, les commutateurs virtuels, etc., et contient un état par locataire, ainsi qu'une table de transmission distincte pour un réseau virtuel. La table de transmission comprend les préfixes IP (dans le cas d'un réseau superposé de couche 3) ou les adresses MAC (dans le cas d'un réseau superposé de couche 2) des machines virtuelles. En outre, il n'est pas nécessaire qu'un routeur virtuel unique contienne tous les préfixes IP ou toutes les adresses MAC de toutes les machines virtuelles du centre de données d'un fournisseur CSP. Un routeur virtuel doit uniquement contenir les instances de routage qui sont installées localement sur le même serveur.</p>

Rôles	CSC, CSP.
Figure (facultatif)	
Conditions préalables (facultatif)	<ul style="list-style-type: none"> Le réseau d'exploitant IP du fournisseur CSP prend en charge le mécanisme de réseau superposé.
Conditions après mise en oeuvre (facultatif)	<ul style="list-style-type: none"> Les machines virtuelles du client CSC exécutées dans les différents centres de données du fournisseur CSP peuvent communiquer entre elles.
Exigences définies	<ul style="list-style-type: none"> Subdivision de réseau isolée logiquement (voir le § 9.12). Mécanisme de réseau superposé (voir le § 9.13).

II.4.2.7 Cas d'utilisation de la connectivité NaaS pour les adresses IP privées et les VPN

Titre	Cas d'utilisation de la connectivité NaaS pour les adresses IP privées et les VPN
Description	<p>Cas I: Passerelle VPN multilocataires située sur un site de nuage public avec chevauchement d'adresses IP privées</p> <p>Une passerelle VPN multilocataires située sur un site de nuage public est partagée par un client CSC-I-A et un client CSC-I-B. Tous deux souhaitent utiliser la même réserve d'adresses IP privées pour leurs points d'extrémité.</p> <p>Tous deux sont raccordés à la passerelle VPN de nuage public grâce à une adresse IP publique donnée. La passerelle VPN de nuage devrait être capable d'assurer la commutation du trafic de chaque client CSC vers un sous-réseau adapté.</p> <p>Cas II: Prise en charge de l'interfonctionnement pour différents types de VPN</p> <p>Un client CSC-II dispose d'une connexion MPLS-VPN propriétaire de site à site entre son siège et un centre de données privé. Compte tenu de l'évolution de l'entreprise, le client CSC-II souhaite établir de nouvelles connexions VPN sécurisées de site à site et de site à client (par exemple, VPN de sécurité IP (IPsec) et VPN de couche de connecteurs sécurisés (SSL)). De nouvelles connexions VPN entre les succursales de l'entreprise réparties dans le monde et les utilisateurs mobiles sont prévues et les VPN existants du client CSC-II sont conservés. Le fournisseur CSP NaaS devrait être capable d'assurer l'interfonctionnement entre le VPN existant appartenant au client CSC et les différents types de nouveaux VPN.</p> <p>Cas III: Prise en charge des réseaux à la demande pour les points d'extrémité répartis</p> <p>Le client CSC-III a besoin d'une solution offrant des connexions de réseau fiables, prévisibles et à la demande pour tous ses emplacements. Ce service devrait pouvoir être modifié de manière dynamique en fonction de ses besoins. Le client CSC-III souhaite des paramètres de demande élastiques pour la connectivité vers ses emplacements sur les liaisons existantes. La connectivité devrait être établie vers un ou plusieurs points</p>

de présence (PoP) du fournisseur CSP NaaS avec la possibilité de déployer des équipements supplémentaires avec un minimum d'efforts.

Rôles Fournisseur CSP, client CSC.

Figure (facultatif)

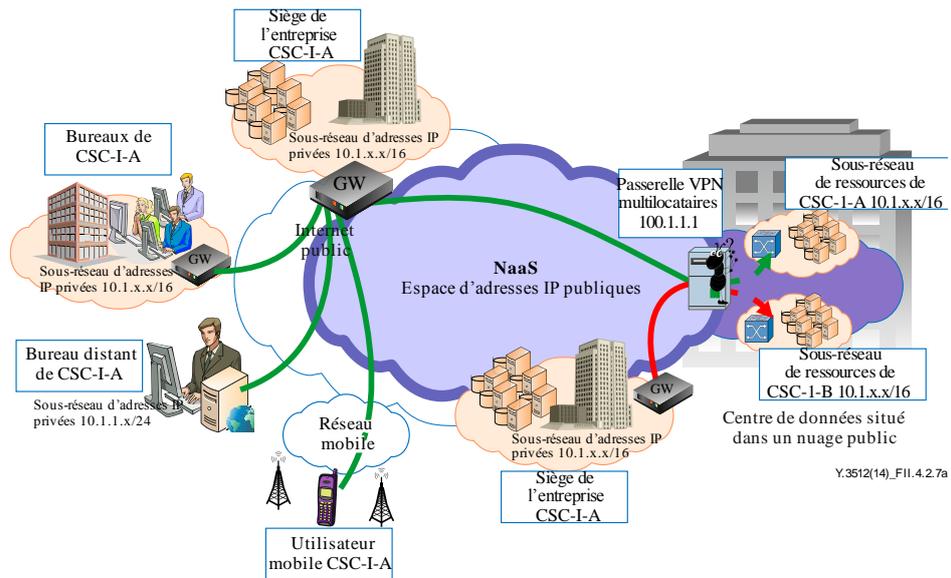


Figure 1 – Cas I: Passerelle VPN multilocataires située sur un site de nuage public avec chevauchement d'adresses IP privées

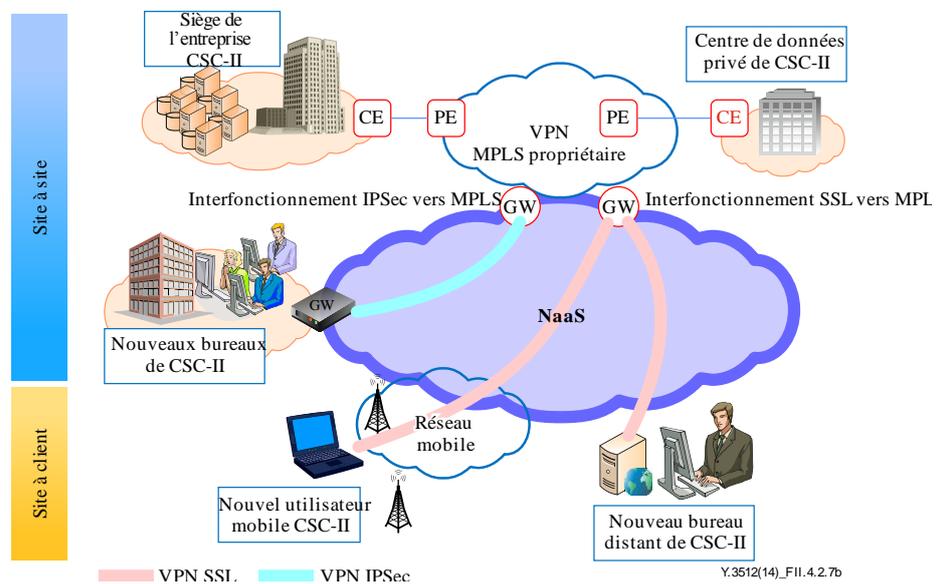
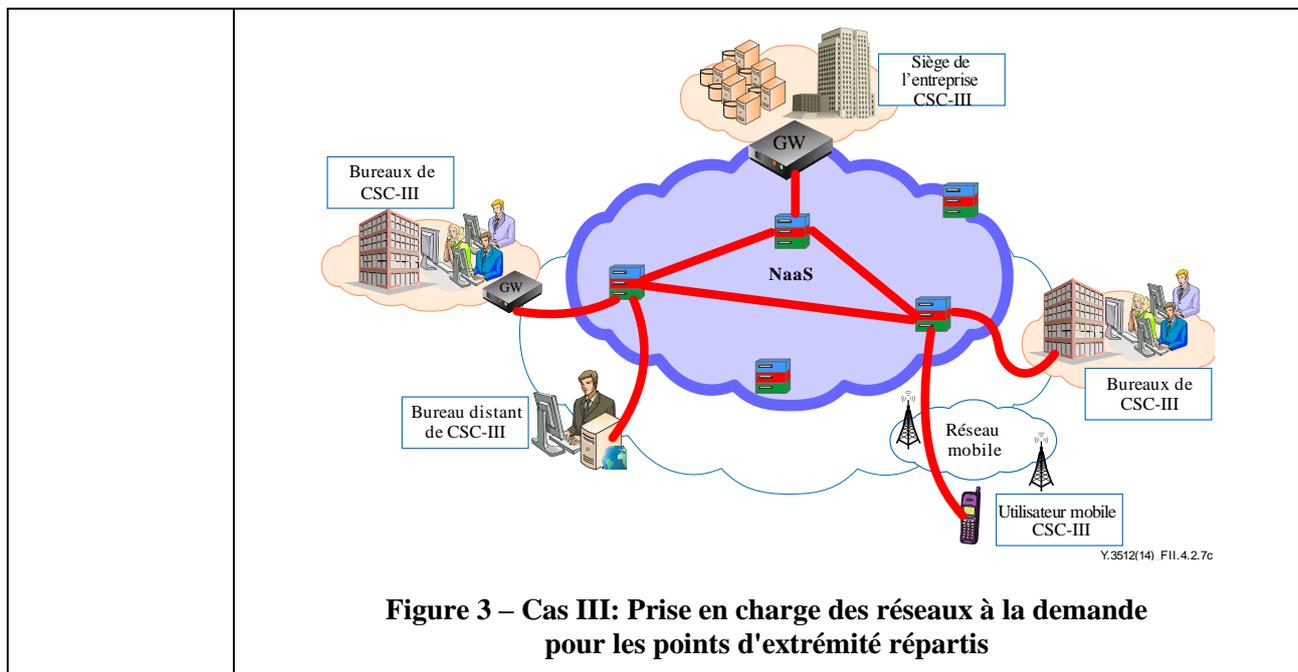


Figure 2 – Cas II: Prise en charge l'interfonctionnement pour différents types de VPN



Conditions préalables (facultatif)	On part du principe que la passerelle VPN multilocataires située sur le site de nuage public est fournie par le fournisseur CSP NaaS.
Conditions après mise en oeuvre (facultatif)	
Exigences définies	<ul style="list-style-type: none"> – Chevauchement des adresses IP privées (voir le § 9.14). – Interfonctionnement de solutions VPN différentes (voir le § 9.15). – Connexion VPN dans un environnement mobile (voir le § 9.16). – Connexion au réseau du fournisseur CSP NaaS via l'Internet public (voir le § 9.17).

Appendice III

Considérations relatives aux activités liées aux réseaux du fournisseur CSP

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

On trouvera dans le présent Appendice des considérations relatives aux activités liées au réseau du fournisseur CSP.

Chaque service de la catégorie NaaS peut être spécifié par un ensemble de termes:

- Interface de service – L'interface de service, qui est offerte au client CSC, définit la fonctionnalité qui est mise en oeuvre par le fournisseur CSP. Elle peut comprendre une fonctionnalité liée aux points de démarcation pour l'interconnexion du fournisseur CSP et du client CSC, une fonctionnalité liée à la topologie et au trajet afin de partager les topologies, une fonctionnalité liée à la découverte pour mener à bien d'autres services dont ont besoin les activités internuages, ainsi que d'autres fonctionnalités liées à la surveillance, à la protection, à la vérification, etc. La fonctionnalité liée au trajet nécessite des informations sur les points d'extrémité d'entrée et de sortie et, éventuellement, sur les points intermédiaires d'un segment de réseau. Les attributs d'un segment de réseau peuvent comprendre les attributs des points d'extrémité, les paramètres de qualité de service, les attributs de qualité de fonctionnement, les attributs d'heure, les attributs d'utilisateur, l'identifiant de demandeur de service, etc.
- Point de démarcation du service – Il s'agit d'un point marquant la limite entre le fournisseur CSP NaaS et le client CSC NaaS. Il sert de point de référence pour identifier les responsabilités et les obligations de toutes les entités concernées. Dans le cas des réseaux IP/MPLS, l'interface utilisateur-réseau (UNI) du point de démarcation est une paire extrémité client-extrémité fournisseur. Pour les autres réseaux de transports, l'interface UNI et l'interface réseau-réseau (NNI) sont définies comme étant des points de démarcation. Par exemple, l'interface UNI définie par le Metro Ethernet Forum (MEF) est mise en oeuvre sur le plan physique sur une liaison Ethernet bidirectionnelle qui fournit les différentes capacités dans les plans de données, de commande et de gestion, dont le fournisseur de service de réseau Ethernet métropolitain (MEN) a besoin pour indiquer clairement la démarcation entre les deux domaines de réseau différents impliqués dans les aspects opérationnels, administratifs, de maintenance et de fourniture du service. Souvent, la couche d'abstraction logicielle (SAL) ou le système d'exploitation du réseau (NOS) est utilisé comme point de démarcation pour les plates-formes de réseau, tandis que les connecteurs TCP/UDP sont utilisés comme points de démarcation pour les applications de réseau.
- Capacités de service – Il s'agit de ce que le réseau NaaS fournit au client CSC via les interfaces de service comme les capacités de la connectivité de réseau et les capacités de service liées à la mise en réseau. Les capacités de connectivité pour le réseau de transport comprennent le réseau IP/MPLS, les réseaux de transmission, le sous-système multimédia IP (IMS), les réseaux pilotés par logiciel (SDN) et les réseaux CDN, tandis que les capacités de connectivité pour le réseau virtuel comprennent les pseudo-circuits, le service LAN privé virtuel (VPLS), le VPN L3 et le réseau local virtuel. Les capacités de service liées à la mise en réseau peuvent comprendre l'optimisation WAN, la répartition de charge, le système des noms de domaine (DNS), les pare-feu, les systèmes de détection ou de prévention des intrusions, les services de télécommunication et des applications de réseau comme le transfert de fichiers entre homologues (P2P), etc.

Même si un réseau NaaS à capacités de type infrastructure peut fournir un tel réseau comme un tout, un client CSC dépend du fournisseur CSP pour l'intégration et la personnalisation des

fonctionnalités de logiciel, de reconfiguration et d'expansion des éléments de réseau, ainsi que pour la gestion et l'administration du réseau. Lorsque le client CSC fait appel à des plates-formes NaaS pour construire son propre réseau, la responsabilité du fournisseur CSP va jusqu'au point de démarcation de service de la plate-forme. Le client CSC est responsable de la gestion, de l'administration et de l'exploitation du réseau, ainsi que des fonctions et des services de réseau mis en oeuvre jusqu'au point de démarcation.

Les services composites fournis dans des environnements en nuage doivent s'accompagner d'un accord SLA dans les domaines suivants [b-EC SLA]:

- Spécifications de l'accord SLA rendant compte des dépendances et des interactions entre les services. Les dépendances devraient être exprimées sous la forme de paramètres et refléter le contexte général du service (par exemple, mouvements de données, relations entre les fournisseurs, règles d'orchestration).
- Convergence dans la gestion de l'accord SLA afin de gérer les dépendances (par exemple, gestion commune) tout en conservant l'autonomie de chaque fournisseur en ce qui concerne la gestion des ressources.

Dans le cadre des approches de spécification et de gestion améliorées de l'accord SLA, il devrait être tenu compte du fait que la composition peut être réalisée selon une approche centralisée (par exemple, une entité gère la composition et les offres de services correspondantes) ou répartie (par exemple, moyennant la conclusion d'accords SLA consécutifs). Les spécifications d'un accord SLA pour les scénarios entre services devraient énoncer les conditions communes (limitant toutefois la fourniture de la qualité de bout en bout à ces conditions) ou être mises en oeuvre grâce à des renvois entre accords SLA (par exemple, un accord SLA pour chaque service avec une spécification plus détaillée renvoyant aux accords SLA pour d'autres services), et serviraient de protocole pour permettre l'interaction entre différentes couches et entités.

Les accords SLA identifient, de manière claire et précise, les responsabilités et les obligations de toutes les entités concernées, ainsi que leurs frontières et limites.

Un réseau NaaS peut être utilisé pour prendre en charge d'autres activités liées au réseau du fournisseur CSP (par exemple, fournir la connectivité de réseau, acheminer des services de réseau et fournir des services de gestion de réseau), dès lors que le nuage d'un client CSC isolé sur le plan logique situé dans le centre de données du fournisseur CSP permet à ce client CSC de fournir une partition privée et isolée du nuage dans laquelle il peut utiliser des capacités de nuage dans un réseau virtuel, souvent grâce à des intervalles d'adresses IP qu'il a définis. Le nuage d'un client CSC peut avoir de multiples sous-réseaux dans un centre de données. La connectivité de réseau entre le client CSC distant et le nuage du CSC, par exemple, peut comprendre les éléments suivants:

- Connexion VPN IPsec via l'Internet public (passerelle VPN côté fournisseur CSP – passerelle VPN situé dans les locaux du client CSC).
- Connexion de réseau dédiée via des lignes privées (passerelle VPN côté fournisseur CSP – équipement des locaux d'abonné (CPE)).
- Connexion VPN IPsec via des lignes privées (passerelle VPN côté fournisseur CSP – passerelle VPN situé dans les locaux du client CSC).
- Connexion VPN avec un appareil logiciel via l'Internet public (appareil VPN logiciel – passerelle Internet côté fournisseur CSP – passerelle VPN située dans les locaux du client CSC, où la passerelle Internet uniquement achemine uniquement des connexions VPN via l'Internet public).
- Connexion VPN par commutation par étiquette multiprotocoles (MPLS).

Les services de nuage nécessitent l'interconnexion de multiples nuages du client CSC pour former un réseau virtuel contigu; de plus, pour répondre à cette exigence, le réseau NaaS peut fournir les éléments suivants:

- Connexions fondées sur des appareils VPN logiciels entre les nuages du client CSC pour les cas intranuage et internuages (appareil VPN logiciel au niveau du nuage 1 du client CSC – passerelle Internet – passerelle Internet – équipement VPN logiciel au niveau du nuage 2 du client CSC, où la passerelle Internet achemine uniquement des connexions VPN, via l'Internet public dans les cas internuages).
- Appareil VPN logiciel raccordé à une connexion VPN physique entre les nuages du client CSC (passerelle VPN au niveau du nuage 1 du client CSC – passerelle Internet – appareil VPN logiciel au niveau du nuage 2 du client CSC, où la passerelle Internet achemine uniquement des connexions VPN).
- Acheminement entre nuages du client CSC géré par le client CSC sur des connexions VPN IPsec physiques en utilisant des équipements du client CSC et l'Internet public ou des lignes privées (passerelle VPN au niveau du nuage 1 du client CSC – équipement du client CSC – passerelle VPN au niveau du nuage 2 du client CSC).

Bibliographie

- [b-IETF RFC 4364] IETF RFC 4364 (2006), *BGP/MPLS IP Virtual Private Networks (VPNs)*.
- [b-EC SLA] Direction générale des réseaux de communication, du contenu et des technologies, Unité E2 – Software and Services, Cloud, (Bruxelles, juin 2013), *Cloud Computing Service Level Agreements – Exploitation of Research Results*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication