Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.3512

(08/2014)

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET, REDES DE PRÓXIMA GENERACIÓN, INTERNET DE LAS COSAS Y CIUDADES INTELIGENTES

Computación en la nube

Computación en la nube – Requisitos funcionales de la red como servicio

Recomendación UIT-T Y.3512

UIT-T

ITU Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET, REDES DE LA PRÓXIMA GENERACIÓN, INTERNET DE LAS COSAS Y CIUDADES INTELIGENTES

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899
Televisión IP sobre redes de próxima generación	Y.1900–Y.1999
REDES DE LA PRÓXIMA GENERACIÓN	
Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de la próxima generación	Y.2250–Y.2299
Mejoras de las NGN	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Redes basadas en paquetes	Y.2600–Y.2699
Seguridad	Y.2700–Y.2799
Movilidad generalizada	Y.2800–Y.2899
Entorno abierto con calidad de operador	Y.2900–Y.2999
REDES FUTURAS	Y.3000–Y.3499
COMPUTACIÓN EN LA NUBE	**Y.3500–Y.3999**

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T Y.3512

Computación en la nube – Requisitos funcionales de la red como servicio

Resumen

En la Recomendación UIT-T Y.3512 se describen el concepto de red como servicio (NaaS) y sus requisitos funcionales. Se presentan casos típicos de utilización de la NaaS y se especifican los requisitos funcionales de tres aspectos, la aplicación NaaS, la plataforma NaaS y la conectividad NaaS, que se basan en los correspondientes casos de uso y tipos de capacidades de la nube.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T Y.3512	2014-08-29	13	11.1002/1000/12285

Palabras clave

Aplicación NaaS, computación en la nube, conectividad NaaS, NaaS, plataforma NaaS, red como servicio.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

© UIT 2016

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

Recomendación UIT-T Y.3512

Computación en la nube – Requisitos funcionales de la red como servicio

1 Alcance

En esta Recomendación se presentan casos de uso y los requisitos funcionales de la red como servicio (NaaS), que es una de las categorías de servicio representativas de la nube. En esta Recomendación se aborda lo siguiente:

– el concepto de Naas de alto nivel;

– los requisitos funcionales de la NaaS;

– los casos de uso de NaaS típicos.

En esta Recomendación se dan casos de uso y los requisitos funcionales de la aplicación NaaS, la plataforma NaaS y la conectividad NaaS.

NOTA – Los requisitos generales de la NaaS pueden encontrarse en [UIT-T Y.3501].

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[UIT-T X.1601] Recomendación UIT-T X.1601 (2014), *Marco de seguridad para la computación en la nube*.

[UIT-T Y.3011] Recomendación UIT-T Y.3011 (2012), *Marco de virtualización de la red para las redes futuras*.

[UIT-T Y.3500] Recomendación UIT-T Y.3500 (2014), *Tecnología de la información – Computación en nube – Visión general y vocabulario*.

[UIT-T Y.3501] Recomendación UIT-T Y.3501 (2013), *Marco de la computación en nube y requisitos de alto nivel*.

[UIT-T Y.3502] Recomendación UIT-T Y.3502 (2014), *Tecnología de la información – Computación en la nube – Arquitectura de referencia*.

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 tipo capacidad de aplicación [UIT-T Y.3500]: Tipo de capacidades de la nube en que el cliente del servicio en la nube puede utilizar las aplicaciones del proveedor de servicios en la nube.

3.1.2 tipo de capacidades de la nube [UIT-T Y.3500]: Clasificación de la funcionalidad facilitada por un servicio en la nube al cliente del servicio en la nube en función del recurso utilizado.

NOTA – Los tipos de capacidades de la nube son el tipo capacidad de aplicación, el tipo capacidad de infraestructura y el tipo capacidad de plataforma.

3.1.3 computación en la nube [UIT-T Y.3500]: Paradigma para dar acceso a la red a un conjunto elástico y ampliable de recursos físicos o virtuales compartibles con administración y configuración en autoservicio previa solicitud.

NOTA – Como ejemplos de recursos pueden citarse los servidores, sistemas operativos, redes, software, aplicaciones y equipos de almacenamiento, entre otros.

3.1.4 servicio en la nube [UIT-T Y.3500]: Una o más capacidades que se ofrecen mediante computación en la nube a las que se accede mediante una interfaz definida.

3.1.5 categoría del servicio en la nube [UIT-T Y.3500]: Grupo de servicios en la nube que poseen un conjunto de cualidades en común.

NOTA – Una categoría de servicio en la nube puede incluir capacidades de uno o más tipos de capacidades de la nube.

3.1.6 cliente del servicio en la nube [UIT-T Y.3500]: Parte que mantiene una relación comercial a fin de utilizar los servicios en la nube.

3.1.7 proveedor del servicio en la nube [UIT-T Y.3500]: Parte que ofrece servicios en la nube.

3.1.8 usuario del servicio en la nube [UIT-T Y.3500]: Persona física, o entidad que la representa, asociada a un cliente del servicio en la nube que utiliza servicios en la nube.

3.1.9 comunicaciones como servicio (CaaS) [UIT-T Y.3500]: Categoría de servicio en la nube que consiste en ofrecer al cliente del servicio en la nube una capacidad de comunicación y colaboración en tiempo real.

NOTA – CaaS puede ofrecer los tipos capacidad de plataforma y capacidad de aplicación.

3.1.10 tipo capacidad de infraestructura [UIT-T Y.3500]: tipo de capacidades en la nube que permite al cliente del servicio en la nube configurar y utilizar recursos de procesamiento, almacenamiento e interconexión de redes.

3.1.11 partición de red lógicamente aislada [UIT-T Y.3011]: Red compuesta de múltiples recursos virtuales, aislada de otras particiones de red lógicamente aisladas (LINP).

NOTA – El término "lógicamente aislada", opuesto a "físicamente aislada", implica la exclusión mutua de los sujetos (por ejemplo, en este caso, la partición de red), mientras que los sujetos originales pueden estar físicamente únicos/compartidos dentro de límites físicos comunes.

3.1.12 red como servicio (NaaS) [UIT-T Y.3500]: Categoría de servicio en la nube que consiste en ofrecer al cliente del servicio en la nube conectividad de transporte y sus correspondientes capacidades de red.

NOTA – NaaS puede ofrecer cualquiera de los tres tipos de capacidades en la nube.

3.1.13 tipo capacidad de plataforma [UIT-T Y.3500]: Tipo de capacidades en la nube que permite al cliente del servicio en la nube desplegar, gestionar y ejecutar aplicaciones creadas o adquiridas por el cliente utilizando uno o más lenguajes de programación y uno o más entornos de ejecución soportados por el proveedor del servicio en la nube.

3.1.14 división [UIT-T Y.3500]: Grupo de usuarios del servicio en la nube que comparten acceso a un conjunto de recursos físicos y virtuales.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 cadena de servicio: Conjunto ordenado de funciones utilizadas para aplicar políticas de tratamiento diferenciado del tráfico a un flujo de tráfico.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

BGP Protocolo de pasarela de frontera (*border gateway protocol*)

BoD Ancho de banda a demanda (*bandwidth on demand*)

BSS Sistema de soporte comercial (*business support system*)

CaaS Comunicaciones como servicio (*communications as a service*)

CDN Red de entrega de contenido (*content delivery network*)

CPE Equipo en los locales del cliente (*customer premises equipment*)

CSC Cliente del servicio en la nube (*cloud service customer*)

CSP Proveedor del servicio en la nube (*cloud service provider*)

CSU Usuario del servicio en la nube (*cloud service user*)

DNS Sistema de nombre de dominio (*domain name system*)

DPI Inspección detallada de paquetes (*deep packet inspection*)

EPC Red medular de paquetes evolutiva (*evolved packet core*)

GW Pasarela (*gateway*)

HQ Sede (*headquarter*)

IaaS Infraestructura como servicio (*infrastructure as a service*)

IDE Entorno de desarrollo integrado (*integrated development environment*)

IMS Subsistema multimedios IP (*IP multimedia subsystem*)

IP Protocolo Internet (*Internet protocol*)

IPS Sistema de protección contra intrusiones (*intrusion protection system*)

IPsec Seguridad IP (*IP security)*

L2 Capa 2 (*layer 2*)

L3 Capa 3 (*layer 3*)

LAN Red de área local (*local area network*)

LINP Partición de red lógicamente aislada (*logically isolated network partition*)

MAC Control de acceso a los medios (*medium access control*)

MEF Foro Ethernet metro (*metro Ethernet forum*)

MEN Red Ethernet metro (*metro Ethernet network*)

MPLS Conmutación por etiquetas multiprotocolo (*multi-protocol label switching*)

NaaS Red como servicio (*network as a service*)

NNI Interfaz red-red (*network-to-network interface*)

NOS Sistema operativo de red (*network operating system*)

OSS Sistema de apoyo de operaciones (*operations support system*)

QoE Calidad percibida (*quality of experience*)

QoS Calidad de servicio (*quality of service*)

P2P Par a par (*peer-to-peer*)

PaaS Plataforma como servicio (*platform as a service*)

PoP Punto de presencia (*point of presence*)

SaaS Software como servicio (*software as a service*)

SAL Capa de abstracción de software (*software abstraction layer*)

SDN Interconexión de redes definida por software (*software defined networking*)

SLA Acuerdo de nivel de servicio (*service level agreement*)

SSL Capa de zócalo segura (*secure socket layer*)

UNI Interfaz usuario-red (*user-to-network interface*)

vCDN Red de entrega de contenido virtual (*virtual content delivery network*)

vDPI Inspección detallada de paquetes virtual (*virtual deep packet inspection*)

vEPC Red medular de paquetes evolutiva virtualizada (*virtualised evolved packet core*)

vFW Cortafuegos virtual (*virtual firewall*)

vRouter Encaminador virtual (*virtual router*)

VDI Infraestructura de escritorio virtual (*virtual desktop infrastructure*)

VM Máquina virtual (*virtual machine*)

VoIP Voz por IP (*voice over IP*)

VPLS Servicio de LAN privada virtual (*virtual private LAN service*)

VPN Red privada virtual (*virtual private network*)

VRF Encaminamiento y reenvío virtual (*virtual routing and forwarding*)

WAN Red de área amplia (*wide area network*)

5 Convenios

La expresión "**se requiere**" indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con este documento.

La expresión "**se recomienda**" indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. Su cumplimiento no es indispensable para poder declarar la conformidad.

La expresión "**se tiene la opción de**" indica que el requisito se permite, sin que ello signifique que se recomienda. No se pretende implicar que el fabricante deba ofrecer esta opción y que el operador de red/proveedor de servicio tenga la posibilidad de activarla. Significa, más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

En el cuerpo de la presente Recomendación y en sus anexos aparecen algunas veces verbos que expresan obligación, prohibición, recomendación y posibilidad, en cuyo caso deben interpretarse en dicho sentido. Cuando estas expresiones o términos aparecen en apéndices o en partes incluidas explícitamente a título informativo no deben interpretarse en su sentido normativo.

6 Descripción general

6.1 Problemas de interconexión de redes en la computación en la nube

Para construir una infraestructura y aplicación de red fiable y eficiente a fin de facilitar servicios en la nube hay que superar diversos retos. Para disponer de capacidades de computación, almacenamiento y red puede haber que superar los siguientes obstáculos:

- Coordinación de la virtualización de la computación y el almacenamiento con las capacidades de red

  Los problemas de rendimiento de la computación y el almacenamiento en los sistemas de computación en la nube se resuelven satisfactoriamente empleando principalmente la virtualización. La virtualización de los servidores implica la migración dinámica y estática de las máquinas virtuales (VM), lo que impone demandas en los entornos de red. Se supone que la red prestará un apoyo adecuado y flexible a las muy variables aplicaciones en la red cuando éstas se ejecutan dentro de una arquitectura de sistema compleja y diversa. En tales sistemas es posible facilitar recursos de computación y almacenamiento, pero también se prevé la prestación dinámica de la interconexión de redes necesaria para garantizar los requisitos de rendimiento, fiabilidad y calidad de servicio (QoS) del sistema en general.

- Control armonizado de tecnologías de red heterogéneas

  Debido a la creciente distribución geográfica de los sistemas de computación en la nube, es necesario utilizar diversas tecnologías de red para garantizar la conectividad de extremo a extremo. Se cuenta con el apoyo de mecanismos de control eficientes para las diversas tecnologías de red.

- Reconfiguración a la demanda

  El sistema de computación en la nube permite reconfigurar dinámicamente los recursos de computación y almacenamiento, o su migración para satisfacer cambios en los requisitos. Conviene que las redes permitan la reconfiguración a la demanda a fin de satisfacer los requisitos de los servicios en la nube, por ejemplo, el cambio de ancho de banda, la modificación de la topología de red o la adición de nuevos elementos de red.

6.2 Concepto de NaaS de alto nivel

Como se define en [UIT-T Y.3500], la red como servicio (NaaS) es una categoría de servicios en la nube en que la capacidad ofrecida al cliente del servicio en la nube (CSC) es la conectividad de transporte y otras capacidades de red conexas para resolver los problemas mencionados anteriormente. Los servicios NaaS se dividen en servicio de aplicación NaaS, servicio de plataforma NaaS y servicio de conectividad NaaS. Concretamente, el servicio de conectividad NaaS es un servicio "tipo capacidad de infraestructura" limitado a los recursos de interconexión de redes.

En la Figura 6-1 se ilustra el concepto de Naas de alto nivel utilizando el marco de capas definido en [UIT-T Y.3502].

NaaS puede ofrecer cualquiera de las tres capacidades en la nube identificadas en [UIT-T Y.3500]:

- **Aplicación NaaS**: tipo de servicio capacidades de aplicación donde el CSC NaaS puede utilizar las aplicaciones de red facilitadas por el proveedor de servicios en la nube (CSP) NaaS. Estas aplicaciones de red se consideran y utilizan como funciones de red virtual facilitadas por el CSP NaaS, lo que incluye cualquier función de red para redes fijas o móviles, tanto medulares como de acceso, además de los elementos de red de los planos de control y reenvío. Como ejemplos de aplicaciones NaaS se pueden citar el encaminador virtual, la red de entrega de contenido virtual (vCDN), la red medular de paquetes evolutiva virtualizada (vEPC) y el cortafuegos virtual (vFW).

  En esta categoría, el CSP ofrece una serie de interfaces para las funcionalidades de red.

- **Plataforma NaaS**: tipo de servicio capacidades de plataforma en que el CSC NaaS puede utilizar la plataforma de red facilitada por el CSP NaaS. La plataforma NaaS ofrece uno o más entornos de ejecución de software y uno o más lenguajes de programación y gestiona y ejecuta aplicaciones de red creadas por el cliente o adquiridas por él. El CSC puede adquirir o crear tales aplicaciones de red como servicios de red autoimplantados. Las aplicaciones de red pueden adoptar la forma de diversas funcionalidades o servicios de red, por ejemplo, encaminador, contrafuegos, equilibrado de cargas, así como grupos de funcionalidades de red. Los grupos de aplicaciones y funcionalidades de red pueden formar una solución de red integrada.

  En esta categoría, el CSP ofrece un entorno programable para las funcionalidades de red que pueden emplear el cliente del servicio en la nube o el software asociado al servicio en la nube.
- **Conectividad NaaS**: tipo de servicio capacidades de infraestructura en que el CSC NaaS puede configurar y utilizar recursos de conectividad de redes facilitados por el CSP NaaS, lo que incluye, por ejemplo, redes privadas virtuales flexibles y ampliadas (VPN), ancho de banda a la demanda (BoD), etc. NaaS puede ofrecer funcionalidades de interconexión de redes básicas, como la conectividad, utilizando las capacidades de interconexión de redes físicas, lógicas o virtuales que el CSP decida ofrecer. Generalmente se busca ofrecer más que la interconexión de redes IP. Por ejemplo, un CSC puede optar por el control elástico a la demanda de redes ópticas o, incluso, por acceder a la fibra oscura utilizando la conmutación fotónica.

  En esta categoría el CSP ofrece conexiones de red entre dos o más puntos extremos, que pueden incluir funcionalidades de red adicionales.

  NOTA 1 – La creación, el control, la gestión y la supresión de la conectividad NaaS se realizan como un servicio en la nube.

  NOTA 2 – NaaS suele ofrecer conectividad "portadora" de datos brutos independientemente del tipo de datos transportados entre los puntos extremos. Los servicios específicamente vinculados al tipo de datos transportados, como la telefonía, la voz por IP (VoIP), la vídeoconferencia y la mensajería instantánea, suelen categorizarse como comunicaciones como servicio (CaaS).

  NOTA 3 – Los puntos extremos de la conectividad NaaS pueden encontrarse dentro de la misma interfaz del servicio NaaS, en otro servicio en la nube, en un servicio independiente de la nube o en un punto extremo de red tradicional.

Tanto los servicios en la nube como los servicios independientes de la misma pueden utilizar el servicio NaaS.

Las capacidades de red pueden entregarse mediante cualquier combinación de los tres tipos de capacidades en la nube. Concretamente, las capacidades de red pueden soportar la computación en la nube en algunos elementos de la interconexión del CSP y el CSC, las funcionalidades de topología y encaminamiento para la compartición de topologías, la funcionalidad de descubrimiento para ejecutar otros servicios necesarios para las actividades entre nubes y otras funcionalidades conexas relacionadas con la supervisión, la protección, la verificación, etc.

La funcionalidad de red puede ofrecerse como un servicio NaaS compuesto donde el servicio NaaS está formado por más de un servicio de funcionalidad de red. También pueden ofrecerse servicios Naas compuestos incorporados jerárquicamente. Es posible recurrir a los servicios NaaS compuestos para ofrecer al CSC tipos de capacidades NaaS diferentes en función de los objetivos de rendimiento expresados en el acuerdo de nivel de servicio (SLA).

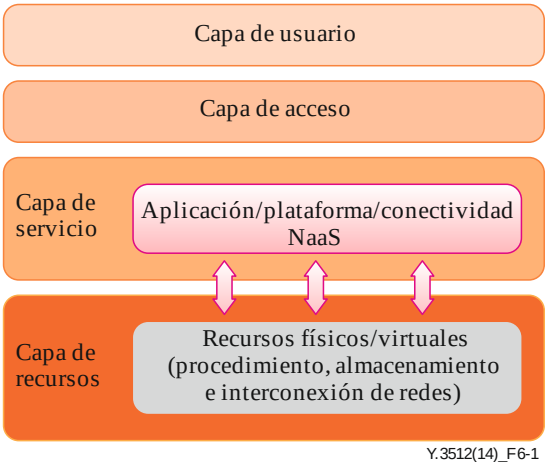


Figura 6-1 – Concepto de NaaS de alto nivel

En el Apéndice II se presentan casos de uso de NaaS en que se facilitan al CSC los tres tipos de capacidades en la nube (es decir, capacidades de aplicación, plataforma e infraestructura).

En el Apéndice III se presentan las consideraciones sobre las actividades relacionadas con la red del CSP.

NOTA 4 – En lo que se refiere a la conectividad de red, una gran diferencia entre la infraestructura como servicio (IaaS) y NaaS es que la IaaS es una categoría de servicio en la nube que sólo se ofrece en un tipo de capacidad en la nube, a saber, el tipo de capacidad de infraestructura [UIT-T Y.3500]. Sin embargo, NaaS es una categoría de servicio en la nube que puede ofrecerse en los tres tipos de capacidades en la nube.

7 Requisitos funcionales de la aplicación NaaS

En esta cláusula se presentan los requisitos de la aplicación NaaS derivados de los casos de uso descritos en el Apéndice II.

7.1 Rendimiento

– Se recomienda que el rendimiento de la aplicación NaaS sea gestionable a fin de satisfacer las necesidades del CSC.

– Se recomienda que el CSP NaaS supervise el rendimiento de la utilización y entrega de la aplicación NaaS.

– Se recomienda que la aplicación NaaS se facilite al CSC de acuerdo con los objetivos de rendimiento consignados en el SLA.

7.2 Funcionamiento y gestión

– Es necesario que el funcionamiento de la aplicación NaaS sea gestionable y determinista de acuerdo con las políticas operativas del CSP.

– Se recomienda que los CSP NaaS gestionen cada aplicación NaaS de manera eficiente y automática, respetando el marco común de gestión de servicio y gestión del funcionamiento del servicio del CSP.

– Se recomienda que el CSP NaaS facilite al CSC una solución de gestión eficiente de las aplicaciones NaaS configuradas que permita integrar la gestión de las aplicaciones NaaS configuradas en el entorno de funcionamiento de red del CSC.

7.3 Cadena de servicio

– Se recomienda que los CSP NaaS ofrezcan mecanismos que permitan el encadenado de las aplicaciones NaaS, por ejemplo, los componentes de las aplicaciones NaaS necesarios y su orden correspondiente.

7.4 Múltiples direcciones IP

– Se recomienda que la aplicación NaaS soporte múltiples direcciones IP en una interfaz de red al entregar las funciones de aplicación de red (como cortafuegos y equilibrado de carga).

NOTA – Este requisito también se aplica a la plataforma NaaS y a la conectividad NaaS.

8 Requisitos funcionales de la plataforma NaaS

En esta cláusula se presentan los requisitos de la plataforma NaaS derivados de los casos de uso descritos en el Apéndice II.

8.1 Plataforma NaaS programable

– Se recomienda que el CSP NaaS soporte la implantación de aplicaciones de red en la plataforma NaaS tanto por el CSP como por el CSC.

– Se recomienda que la plataforma NaaS ofrezca módulos de hardware o software para acelerar la función de red.

– Se recomienda que la plataforma NaaS garantice e indique el rendimiento disponible a las aplicaciones del CSC que se ejecutan en ella.

– Se recomienda que el servicio de plataforma NaaS facilite un marco de software modulable para seleccionar e integrar las funciones de interconexión de redes, las funciones de seguridad y las aplicaciones de terceros.

– Se recomienda que el CSP NaaS ofrezca apoyo de plataforma para que el CSC gestione (por ejemplo, instale, actualice o desinstale) sus propios módulos.

– se recomienda que la plataforma NaaS ofrezca activadores de red para que el CSC pueda iniciar (por ejemplo, diseñar, construir, gestionar) y operar las redes flexibles, adaptables y con funciones ampliables.

– Se recomienda que la plataforma NaaS ofrezca una función de control y gestión unificados en las plataformas NaaS distribuidas a fin de que el CSC pueda cambiar, mover o eliminar activadores de red entre plataformas NaaS.

8.2 Composición y dirección de servicios de red dinámicos y flexibles

– Se recomienda que el CSP NaaS dirija el tráfico del CSC a través de la cadena de servicio, que está dinámica y flexiblemente compuesta por secuencias personalizadas de aplicaciones NaaS en la plataforma NaaS, en función de la lógica de servicio específica del CSC.

8.3 Aislamiento de las cadenas de servicio para las divisiones

– el CSP Naas puede optativamente soportar el aislamiento de cadenas de servicio para las divisiones, mediante la combinación de distintos servicios de red implantados en la plataforma NaaS.

8.4 Adaptación flexible de la plataforma NaaS

– Se recomienda que el CSP NaaS garantice la adaptación flexible de los recursos asignados a la plataforma NaaS para lograr los objetivos de rendimiento de los servicios y aplicaciones de red implantados en la plataforma NaaS.

NOTA – Este requisito tiene por objetivo adaptarse a los cambios en la utilización de servicios o aplicaciones causados, por ejemplo, por un aumento del tráfico, un cambio en el número de usuarios, la adición de nuevos servicios o la implantación de nuevas aplicaciones.

8.5 integración de aplicaciones de software

– Se recomienda que el CSP NaaS soporte la integración de las aplicaciones de software introducidas en la plataforma NaaS por el CSP, el CSC o ambos, a fin de que se puedan hacer combinaciones.

9 Requisitos funcionales de la conectividad NaaS

En esta cláusula se presentan los requisitos de la conectividad NaaS derivados de los casos de uso descritos en el Apéndice II.

9.1 Mecanismo de control común para la conectividad NaaS

– Se recomienda que el mecanismo de control de conectividad facilitado por el CSP NaaS soporte la negociación de los parámetros de conectividad (como las características de interfaz, los puntos extremos de conexión, el soporte de versión IP, la QoS, el tipo de VPN L3/L2, el método de extensión de la conectividad (por ejemplo, la cláusula 10 de [b-IETF RFC 4364]) y la información de encaminamiento (por ejemplo, el objetivo de encaminamiento del protocolo de pasarela de frontera (BGP)).

– Se recomienda que el CSP NaaS facilite un mecanismo de control de conectividad NaaS común que permita identificar la conectividad NaaS que se ha de ofrecer de manea segura y con una QoS garantizada.

– Se recomienda que el mecanismo de control de conectividad NaaS pueda soportar esquemas de identificación de CSD potencialmente distintos en el lado del CSP NaaS y en el punto extremo conectado.

– El CSP NaaS tiene la opción de ofrecer conectividad aislada para las divisiones de red.

9.2 SLA unificado para múltiples redes optimizadas

– Se recomienda que el CSP NaaS ofrezca servicios de conectividad de red utilizando SLA unificados para la gestión por el CSC de múltiples redes optimizadas a fin de simplificar y unificar el control y la gestión de las redes.

NOTA 1 – Este mecanismo permite al CSP crear y añadir nuevas características a sus redes a fin de ofrecer servicios de alta calidad que se ajusten a las distintas necesidades de los CSC.

– Se recomienda que la política de servicios NaaS compuestos se consigne en el SLA.

NOTA 2 – El servicio NaaS puede ser un servicio compuesto cuando el servicio consista en más de un servicio NaaS.

NOTA 3 – Este requisito también se aplica a la aplicación NaaS y a la plataforma NaaS.

9.3 Aprovechamiento dinámico de las redes de transporte

– Se recomienda que el CSP NaaS aproveche dinámicamente las redes de transporte, a partir de múltiples opciones de redes físicas y virtuales, a fin de ofrecer servicios de conexión de red, como la recuperación, la BoD, la QoS garantizada, etc.

NOTA – Las redes de transporte pueden ser heterogéneas en términos de tecnología y de dominio administrativo.

9.4 Mecanismo de control de red unificado

– Se recomienda que el CSP NaaS ofrezca un mecanismo de control unificado para la conectividad NaaS de extremo a extremo que se da al CSC.

NOTA – La conectividad NaaS puede ofrecerse por múltiples redes heterogéneas o por una sola red, empleando una o más plataformas o aplicaciones NaaS que realice(n) las funciones de red.

9.5 Reconfiguración elástica de la red

– Se recomienda que el CSP ofrezca la configuración elástica de la red a fin de adaptar la elasticidad de la computación y del almacenamiento y mantener la continuidad del servicio.

9.6 atribución de ancho de banda ininterrumpida y de extremo a extremo

– Se recomienda que el CSP NaaS ofrezca la atribución de ancho de banda ininterrumpida y de extremo a extremo, independientemente de la tecnología y la arquitectura de red utilizadas.

9.7 Capacidad simétrica o asimétrica

– Se recomienda que el CSP NaaS ofrezca capacidad de enlace de red simétrica o asimétrica en función de la demanda del CSC.

9.8 ingeniería de tráfico optimizada y detallada

– Se recomienda que el CSP NaaS ofrezca al CSC una visión detallada de la utilización de los recursos de red.

– Se recomienda que el CSP NaaS recompile datos sobre la utilización en tiempo real y la topología de su propio equipo de red.

– Se recomienda que el CSP NaaS controle la atribución de recursos de red reconfigurando los perfiles de red y las propiedades (por ejemplo, topología, ancho de banda) en respuesta a la modificación dinámica de la demanda de tráfico.

– El CSP NaaS puede optativamente ofrecer una gestión centralizada del tráfico para optimizar la ingeniería de tráfico.

9.9 Coexistencia con servicios y funciones de redes heredadas

– Se recomienda que el CSP NaaS evite o reduzca las consecuencias que sobre el rendimiento y la flexibilidad puede tener la introducción de nuevos servicios de conectividad de red.

– Se recomienda que el CSP NaaS soporte la coexistencia de nuevos servicios de conectividad de red con sistemas heredados.

9.10 Visión de control y visión de abstracción de recursos centralizada

– El CSP NaaS puede optativamente soportar la gestión lógicamente centralizada y la visión de control de los recursos de red.

– El CSP NaaS puede optativamente ofrecer al CSC una visión de abstracción de los recursos de red subyacentes.

9.11 control limitado de los servicios por el CSC

– Se recomienda que el CSP NaaS facilite al CSC un control adecuado de los servicios a fin de responder a requisitos de rendimiento urgentes, incluida la cantidad de ancho de banda, la latencia máxima y demás parámetros de QoS.

9.12 partición de red lógicamente aislada

– El CSP NaaS puede optativamente crear una partición de red lógicamente aislada (LINP).

NOTA – La LINP se describe en [UIT-T Y.3011]. Véase la cláusula 3.1.14.

9.13 mecanismo de red superpuesta

– La conectividad NaaS puede optativamente soportar redes virtuales superpuestas a la red física subyacente.

9.14 Solapamiento de direcciones IP privadas

– Se recomienda que el CSP NaaS permita a distintos CSC utilizar sus propias direcciones IP incluso cuando las direcciones de subred estén solapadas.

9.15 Interfuncionamiento entre distintas soluciones VPN

– Se recomienda que el CSP NaaS soporte el interfuncionamiento entre distintas tecnologías de VPN.

9.16 Conexión VPN en el entorno móvil

– Se recomienda que el CSP NaaS soporte la conectividad VPN en el entorno móvil.

9.17 Conexión a la red del CSP NaaS a través de la Internet pública

– Se recomienda que el CSP NaaS permita al CSC conectarse al CSP NaaS a través de la Internet pública.

10 Consideraciones de seguridad

En [UIT-T X.1601] se examinan los aspectos de seguridad de los entornos de computación en la nube, incluida la NaaS como problemas de seguridad para el CSP. Concretamente, en [UIT-T X.1601] se analizan las amenazas y problemas de seguridad y se describen las capacidades de seguridad que pueden contrarrestar esas amenazas y resolver los problemas de seguridad.

Apéndice I

Método de definición de los requisitos funcionales y la arquitectura de NaaS

(Este Apéndice no forma parte integrante de la presente Recomendación.)

Habida cuenta de la metodología de normalización y de la secuencia de estudio convencional, las abstracciones de las entidades funcionales y las interacciones entre ellas se basan en los requisitos funcionales y el correspondiente análisis de los casos de uso, que forman en conjunto un cuerpo de normalización. Por consiguiente, es necesario que los requisitos funcionales y la arquitectura de NaaS se definan ajustándose a los siguientes pasos y prioridades.

Paso 1: Casos de uso y requisitos de NaaS incluidos en el Apéndice II y las cláusulas 7 a 9, respectivamente, de esta Recomendación. Téngase en cuenta que todos los requisitos funcionales se derivan de los correspondientes casos de uso.

Paso 2: La arquitectura funcional de NaaS debe basarse en esta Recomendación.

Además, en [UIT-T Y.3501] se describen los requisitos generales de la NaaS.

Apéndice II

Casos de uso de NaaS

(Este Apéndice no forma parte integrante de la presente Recomendación.)

En este Apéndice se presentan tres tipos de casos de uso de NaaS: casos de uso relacionados con la aplicación NaaS, casos de uso relacionados con la plataforma NaaS y casos de uso relacionados con la conectividad NaaS. Cada tipo de caso de uso se divide, además, en casos de uso generales y detallados.

II.1 Plantilla de casos de uso

Los casos de uso del Apéndice II deben ajustarse al siguiente formato unificado para facilitar su lectura y organizar convenientemente el material.

Título	Título del caso de uso
Descripción	Descripción hipotética del caso de uso
Funciones	Funciones participantes en el caso de uso
Figura (opcional)	Figura explicativa del caso de uso. No es obligatoria
Precondiciones (opcional)	Condiciones previas que se han de cumplir antes del inicio del caso de uso
Postcondiciones (opcional)	Condiciones que se arrastrarán una vez terminado el caso de uso
Requisitos derivados	Requisitos derivados de los casos de uso, cuya descripción detallada se presenta en las cláusulas correspondientes

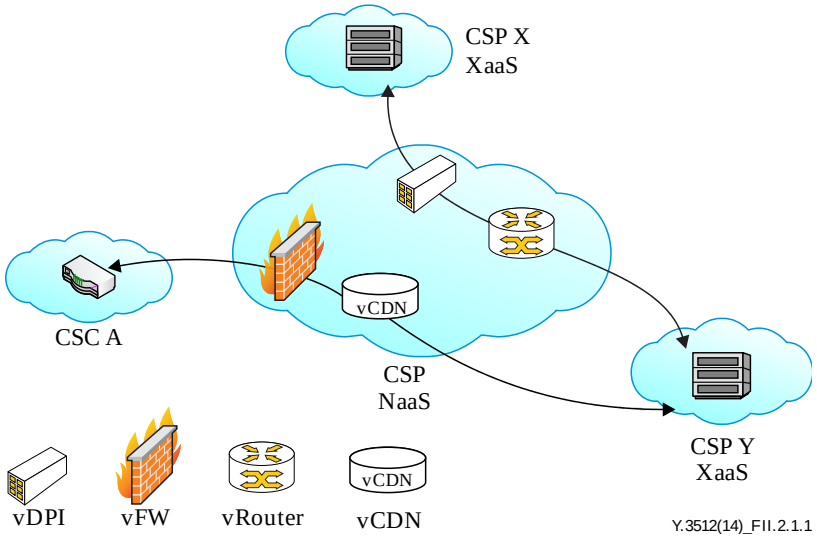
II.2 Casos de uso relacionados con las aplicaciones NaaS

En esta cláusula se describen los casos de uso que pueden dares cuando el CSC NaaS puede configurar y utilizar las aplicaciones de red.

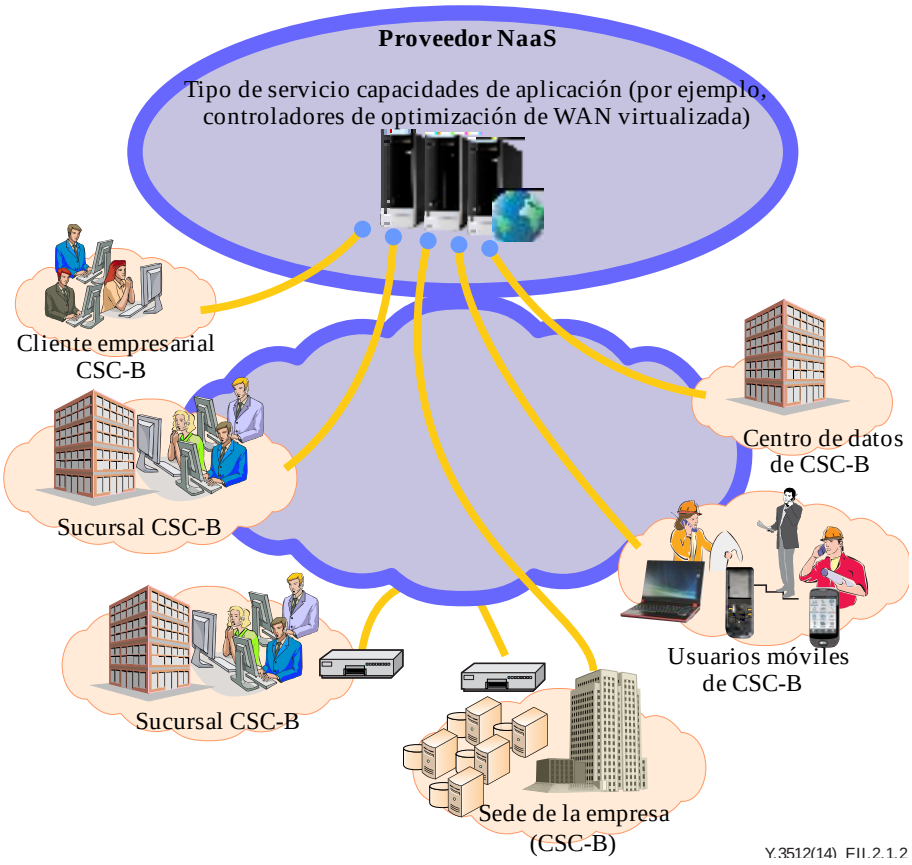
NOTA – En las siguientes cláusulas XaaS denomina todas las categorías de servicios en la nube, como el software como servicio (SaaS), la plataforma como servicio (PaaS), IaaS, CaaS, etc.

II.2.1 Casos de uso generales

II.2.1.1 Caso de uso de aplicación NaaS general

Nombre	Caso de uso de aplicación NaaS general
Descripción	Un CSC XaaS o un CSP XaaS utilizan las aplicaciones de red (por ejemplo, DPI virtual (vDPI), vFW, vCDN) facilitadas por el CSP NaaS. El CSP NaaS puede encadenar esas aplicaciones de red.
Funciones	CSC, CSP
Figura	 NOTA – El encaminador virtual (vRouter) también es aplicable a la conectividad NaaS.
Precondiciones (opcional)	– Hay conectividad entre el CSC XaaS A y el CSP XaaS Y. – Hay conectividad entre el CSP XaaS X y el CSP XaaS Y. – El CSP o el CSC XaaS solicitan el encadenamiento de una aplicación de red (vFW, vCDN, vDPI, vRouter etc.) con la conectividad.
Postcondiciones (opcional)	– El CSP NaaS ofrece aplicaciones de red al CSC/CSP XaaS a través de la conectividad de red existente.
Requisitos derivados	– Aplicación de red virtual a la demanda. – Aplicación de red adaptable. – Cadena de aplicaciones de red. – Aplicaciones con QoS garantizada. – Aplicaciones de red seguras. – Aplicaciones de red resistentes. – Múltiples direcciones IP (véase la cláusula 7.4). NOTA – los primeros seis requisitos son requisitos NaaS de orden general definidos en [UIT-T Y.3501].

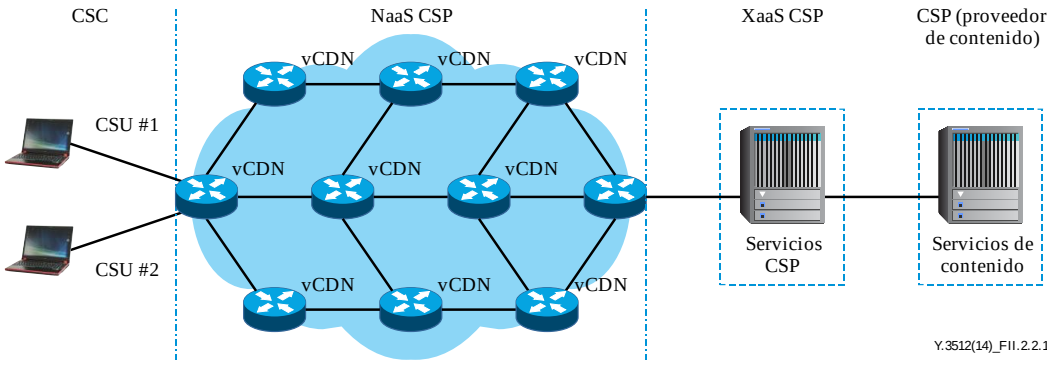
II.2.1.2 Caso de uso de aplicación NaaS para la configuración de la aplicación

Título	Caso de uso de aplicación NaaS para la configuración de la aplicación
Descripción	Se supone que la empresa CSC-B busca servicios de aplicación NaaS para aprovechar las principales características de los servicios de computación en la nube. Por ejemplo, la empresa desea acelerar el tráfico de red saturado con aplicaciones empresariales. La optimización de la red de área amplia (WAN) es más que fundamental para el éxito de sus aplicaciones empresariales. La CSC-B quiere optimizar la WAN en función de la utilización y el soporte de características flexibles a la demanda. Los dispositivos de optimización de WAN tradicionales no cumplen esos requisitos, en particular en lo que respecta al coste total de la propiedad y la elasticidad de la implantación. El CSP NaaS debe ofrecer a la CSC-B una solución de aceleración de WAN virtual que se adapte a sus necesidades empresariales dinámicas.
Funciones	CSP, CSC
Figura (opcional)	
Precondiciones (opcional)	La CSC-B necesita acelerar el tráfico de red saturado con aplicaciones empresariales.
Postcondiciones (opcional)	La CSC-B utiliza la solución de aceleración de WAN virtual facilitada por el CSP NaaS para satisfacer sus necesidades empresariales dinámicas.
Requisitos derivados	– Autoservicio a la demanda. – Multidivisión. – Agrupación de recursos. – Elasticidad y adaptabilidad rápidas. – Servicio medido. – Supervisión y garantía de rendimiento. – Coexistencia y compatibilidad con equipos de red heredada del CSC. – Soporte de interoperatividad para la gestión y la orquestación. – Seguridad y resistencia.

	– Rendimiento (véase la cláusula 7.1). – Funcionamiento y gestión (véase la cláusula 7.2). NOTA – Los primeros nueve requisitos son requisitos NaaS de orden general definidos en [UIT-T Y.3501].

II.2.2 Casos de uso detallados

II.2.2.1 Caso de uso de plataforma NaaS para la CDN en la nube

Título	Caso de uso de plataforma NaaS para la red de entrega de contenido (CDN) en la nube
Descripción	El proveedor de contenido, que actúa como CSC, almacena el contenido en el centro de datos y supervisa su utilización. Cuando la utilización del contenido alcanza un determinado nivel de popularidad o si, de acuerdo con las predicciones, el proveedor de contenido espera un crecimiento de la popularidad en un determinado periodo de tiempo, por ejemplo, la transmisión por vídeo de un acontecimiento deportivo, el proveedor de contenido crea una CDN virtual para trasladar temporalmente el contenido del centro de datos a la red (vCDN). El CSP XaaS recibe el contenido del proveedor de contenido (que puede, a su vez, crear un servicio de distribución). El contenido se entrega a los usuarios del servicio en la nube (CSU) desde el centro de datos del CSP XaaS utilizando la red del CSP NaaS. El CSP XaaS ofrece la posibilidad de almacenar el contenido y supervisar los parámetros de utilización. El CSP XaaS en cooperación con el CSP NaaS puede duplicar el contenido en los nodos de la red, creando un servicio CDN virtual. Básicamente, el CSP XaaS soporta las funciones CDN, por lo que, en cierto modo, el CSP XaaS "emula" la CDN cooperando con el CSP NaaS.
Funciones	CSU, CSC, CSP
Figura (opcional)	
Precondiciones (opcional)	– El proveedor de contenido, que actúa como CSC, almacena el contenido en los centros de datos del CSP XaaS. – El proveedor de contenido que actúa como CSC supervisa la utilización del contenido.
Postcondiciones (opcional)	– El CSP XaaS ofrece el servicio CDN virtual utilizando los recursos de red del CSP NaaS. – El proveedor de contenido que actúa como CSC decide trasladar el contenido del centro de datos a la CDN virtual durante un periodo definido de tiempo.
Requisitos derivados	– Rendimiento (véase la cláusula 7.1). – Funcionamiento y gestión (véase la cláusula 7.2). – Cadena de servicio (véase la cláusula 7.3).

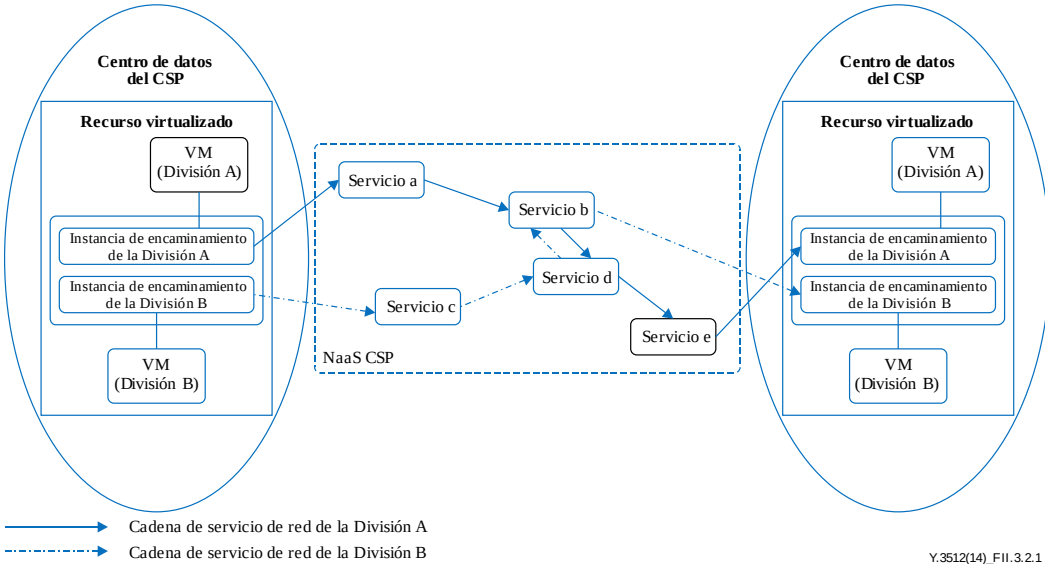
II.3 Casos de uso relacionados con la plataforma NaaS

II.3.1 Casos de uso generales

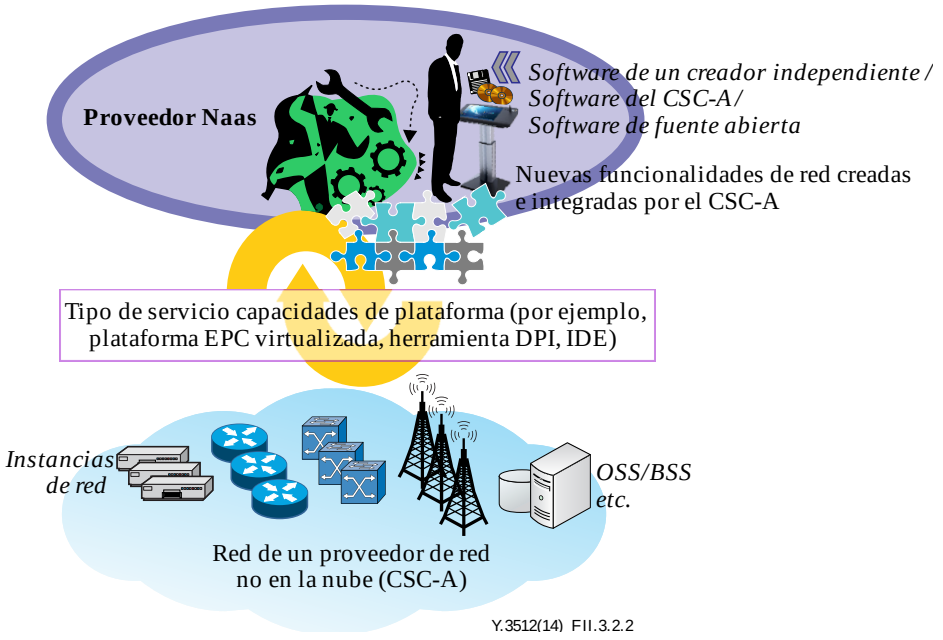
Ninguno.

II.3.2 Casos de uso detallados

II.3.2.1 Caso de uso de la plataforma NaaS para la cadena de servicio

Título	Caso de uso de la plataforma NaaS para la cadena de servicio.
Descripción	Dado que las divisiones CSC tienen cada vez más requisitos de diversidad y complejidad de la red, el CSP debe ofrecer servicios de aplicación de red integrados, como la inspección detallada de paquetes (DPI), la detección de intrusión, la prevención contra intrusiones, el equilibrado de cargas, el cortafuegos, etc. Tradicionalmente los servicios de prestan a través de elementos de la red física dedicados, que tienen una capacidad y unas funcionalidades de red limitadas, una configuración y actualización complejas y un largo periodo de configuración. Cuando la salida de un servicio se utiliza como entrada de otro servicio se crea lo que se conoce como una cadena de servicio. En las redes tradicionales la creación de cadenas de servicio, por ejemplo, una cadena compuesta de un sistema de protección contra intrusiones (IPS), un equilibrado de cargas y una DPI, necesita una configuración propia y no es flexible cuando, por ejemplo, aumenta el tráfico o se añaden/suprimen servicios a/de la cadena. Para flexibilizar el servicio se recomienda que el CSP NaaS ofrezca una plataforma NaaS programable donde puedan implantarse aplicaciones como vRouter, vCDN, vEPC, etc., a fin de dirigir el tráfico del CSC por una secuencia de aplicaciones NaaS personalizada.
Funciones	CSC (División A, División B), CSP
Figura (opcional)	
Precondiciones (opcional)	– El CSP puede ofrecer soluciones de red física dedicada para servicios como DPI, detección de intrusión, prevención contra intrusiones, equilibrado de cargas, cortafuegos, etc.
Postcondiciones (opcional)	– El CSP puede ofrecer servicios de red física, virtual o ambas, o cadenas de servicio de manera dinámica y flexible en función de la lógica de servicio específica del CSC en intervalos de implantación configuración y actualización más cortos que los que ofrecen las soluciones de red física dedicada.
Requisitos derivados	– Plataforma NaaS programable (véase la cláusula 8.1). – Composición y dirección dinámica y flexible de los servicios de red (véase la cláusula 8.2). – Aislamiento de las cadenas de servicio de las divisiones (véase la cláusula 8.3).

II.3.2.2 Caso de uso de la plataforma NaaS para la configuración de la plataforma

Título	Caso de uso de la plataforma NaaS para la configuración de la plataforma
Descripción	El CSC-A es un operador de red. El CSC-A quiere construir un sistema de análisis de tráfico avanzado y de generación de informes multimendionales utilizando funcionalidades DPI adaptables dinámicamente, servicios oportunistas con bajo riesgo, una implantación rápida, una CDN multidivisión, etc., en redes móviles. Sin embargo, las redes de hardware privadas clásicas impiden la rápida implantación de las nuevas funcionalidades de redes convergentes y de servicios que generan ingresos. Además, no se adaptan a la demanda ni son bastante flexibles. El CSC-A tiene la posibilidad de colmar sus necesidades de innovación desarrollando las características y servicios necesarios utilizando la plataforma NaaS. La innovación con la plataforma NaaS le permite utilizar los servicios de la red del CSP y combinarlos con las funcionalidades creadas por el CSC-A. El CSC-A puede integrar todas las funcionalidades en la plataforma NaaS a fin de construir servicios de red mejorados, por ejemplo, red medular de paquetes evolutiva (EPC) virtualizada, plataforma DPI de software, entornos de desarrollo integrados (IDE). La capacidad de la plataforma NaaS debe adaptarse elásticamente en función de la utilización de los servicios de red mejorados para garantizar el rendimiento necesario. También se necesitan soluciones que soporten la integración de los servicios de red del CSP con el software elaborado por el CSC-A.
Funciones	CSP, CSC
Figura (opcional)	
Precondiciones (opcional)	El CSC-A necesita crear servicios de red mejorados utilizando equipos de hardware específicos para cada funcionalidad y gestionar toda la red.
Postcondiciones (opcional)	El CSC-A utiliza la plataforma NaaS para combinar los servicios de red del CSP con las funcionalidades creadas por él mismo e integrarlas en los servicios de red mejorado.
Requisitos derivados	– Adaptación flexible de la plataforma NaaS (véase la cláusula 8.4). – Integración de las aplicaciones de software (véase la cláusula 8.5).

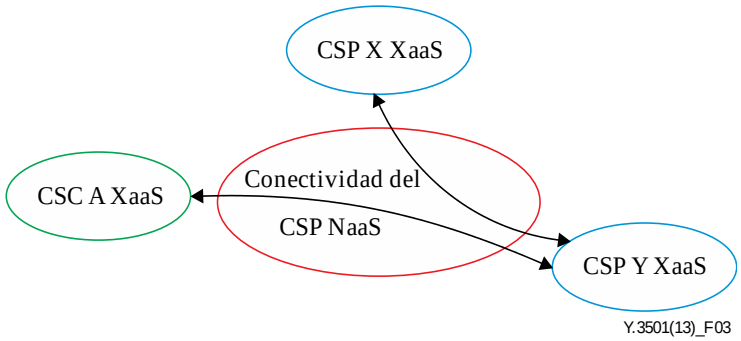
II.4 Casos de uso relacionados con la conectividad NaaS

En esta cláusula se describen los casos de uso en que el CSC NaaS puede configurar y utilizar la conectividad de red.

II.4.1 Casos de uso generales

II.4.1.1 Caso de uso de conectividad NaaS general

NOTA – El siguiente caso de uso se basa en el presentado en [UIT-T Y.3501].

Nombre	Caso de uso de conectividad NaaS general
Descripción	Un CSP NaaS configure, mantiene y libera conectividad de red entre los CSC y entre el CSP y cada CSC como un servicio en la nube, lo que permite incluir conectividad a la demanda y semipermanente.
Funciones	CSC, CSP
Figura	
Precondiciones (opcional)	– No existe conectividad entre el CSC A XaaS y el CSP Y XaaS. – No existe conectividad entre el CSP X XaaS y el CSP Y XaaS. – El CSC A XaaS o el CSP Y XaaS solicitan la conectividad entre sí junto con sus identificadores de punto extremo y características asociadas (relativas a QoS y seguridad) necesarias para establecer la conectividad. – El CSP X XaaS o el CSP Y XaaS solicitan la conectividad entre sí junto con sus identificadores de punto extremo y características asociadas (relativas a QoS y seguridad) necesarias para establecer la conectividad.
Postcondiciones (opcional)	– El CSC A XaaS y el CSP Y XaaS pueden comunicarse entre sí. – El CSC X XaaS y el CSP Y XaaS pueden comunicarse entre sí.
Requisitos	– Configuración de red a la demanda. – Compatibilidad de redes heterogéneas. – Conectividad con QoS garantizada. – Conectividad segura. – Mecanismo de control común para la conectividad NaaS (véase la cláusula 9.1). NOTA – Los primeros 4 requisitos son requisitos generales de NaaS definidos en [UIT-T Y.3501].

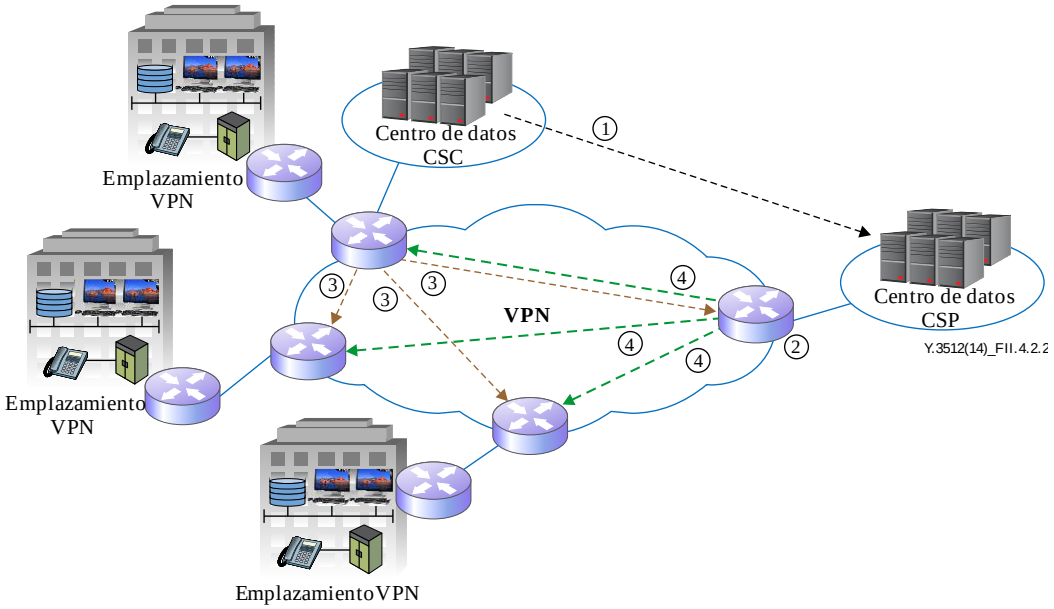
II.4.2 Casos de uso detallados

II.4.2.1 Caso de uso de conectividad NaaS para la red de transporte dinámica

Título	Caso de uso de conectividad NaaS para la red de transporte dinámica
Descripción	El CSC necesita un servicio de conectividad con distribución geográfica y una capacidad de tráfico dinámica que puedan acomodar ráfagas en la nube (por ejemplo, migración VM o transferencia de grandes ficheros de datos entre centros de datos sitos en distintos lugares), que crean un aumento repentino del tráfico que atraviesa la red medular del CSP. Las redes IP y de transporte del CSP se gestionan por separado, por lo que no pueden ofrecer un mecanismo de control común para el ajuste dinámico del ancho de banda. A fin de garantizar la continuidad del servicio y respetar el SLA contraído con el CSC, el CSP tendrá que ofrecer una sobreconfiguración de los enlactes, la mayoría de los cuales no se utiliza efectivamente, malgastando así los recursos. Se recomienda que el CSP soporte los aumentos repentinos del tráfico que atraviesa su red medular sin recurrir a la sobreconfiguración de los recursos de red.
Funciones	CSC, CSP
Figura (opcional)	
Precondiciones (opcional)	
Postcondiciones (opcional)	
Requisitos derivados	– SLA unificado para múltiples redes optimizadas (véase la cláusula 9.2). – Aprovechamiento dinámico de las redes de transporte (véase la cláusula 9.3). – Mecanismo de control de red unificado (véase la cláusula 9.4).

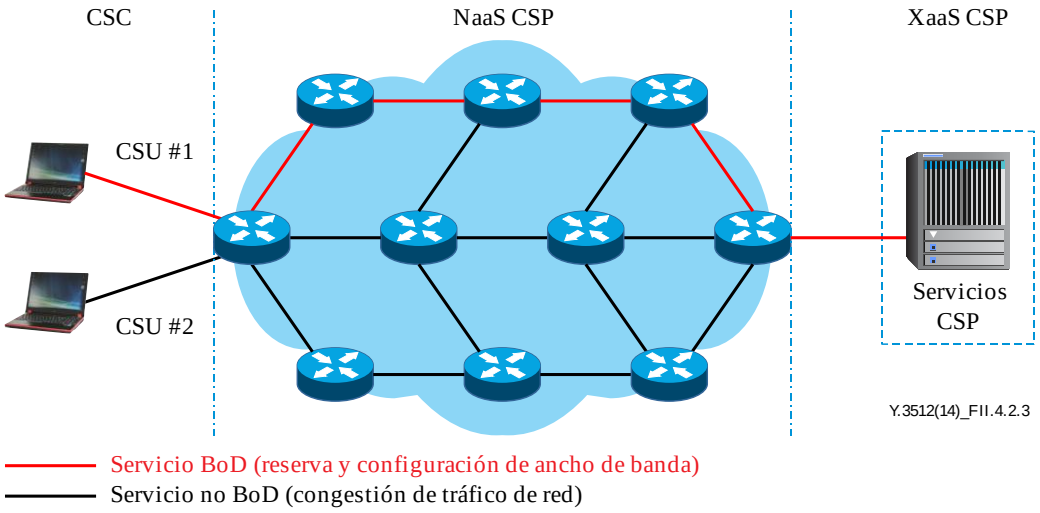
II.4.2.2 Caso de uso de conectividad NaaS para VPN flexible y ampliada

Título	Caso de uso de conectividad NaaS para VPN flexible y ampliada
Descripción	Los distintos emplazamientos de la VPN están conectados por IPVPN BGP/MPLS. Los recursos de procesamiento y la subred correspondiente se trasladan del centro de datos del CSC al centro de datos del CSP, que aún no forma parte de la VPN como emplazamiento VPN. Para añadir este nuevo emplazamiento a la VPN existente es necesario configurar una nueva subred en el centro de datos del CSP y crear un nuevo encaminamiento y reenvío virtual (VRF) en su encaminador de frontera. La migración de la correspondiente subred del centro de datos del CSC al centro de datos del CSP y la supresión de la subred del centro de datos del CSC se deben anunciar a los demás encaminadores de frontera. En la figura siguiente se muestra detalladamente el proceso: 1) Los recursos de procesamiento y la subred correspondiente se trasladan del centro de datos del CSC al centro de datos del CSP. 2) Se configure un nuevo VRF en el encaminador de frontera del centro de datos del CSP. 3) La supresión de la subred del CSC se anuncia con una actualización MP-BGP a todos los emplazamientos VPN. 4) La nueva subred del CSP se anuncia con una actualización MP-BGP a todos los emplazamientos VPN. Se ha de garantizar la continuidad del servicio durante todo el procedimiento de migración y reconfiguración. Sin embargo, desde el punto de vista del CSC, la VPN es una caja negra, por lo que el CSC no puede configurarla o reconfigurarla. Además, la actual tecnología de VPN no soporta la adición y reducción dinámicas de emplazamientos VPN y de la capacidad de ancho de banda.

Funciones	CSC, CSP
Figura (opcional)	
Precondiciones (opcional)	
Postcondiciones (opcional)	
Requisitos derivados	– Reconfiguración elástica de la red (véase la cláusula 9.5).

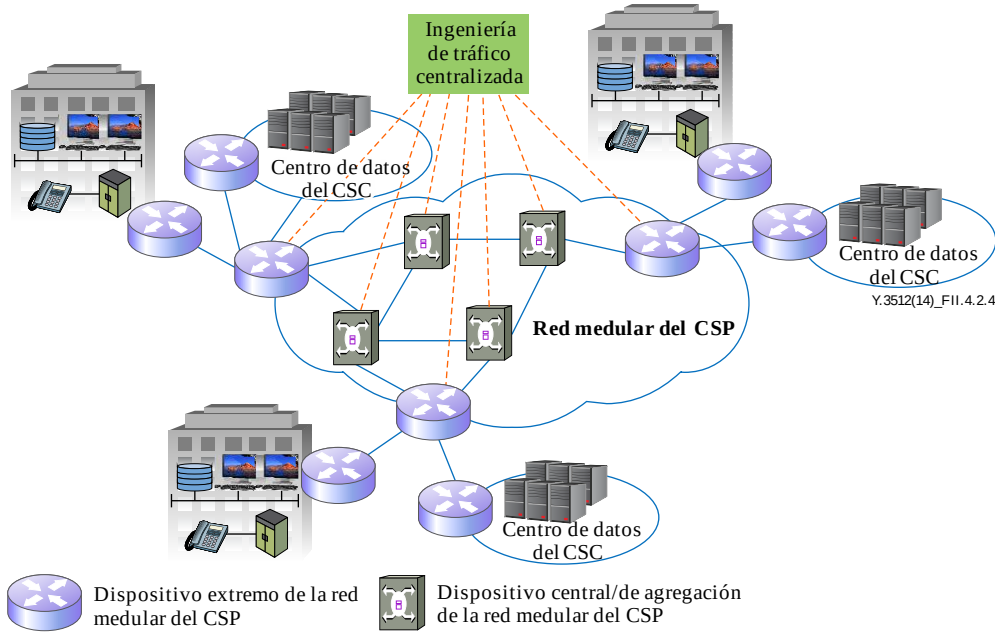
II.4.2.3 Caso de uso de la conectividad NaaS para el servicio BoD

Título	Caso de uso de la conectividad NaaS para el servicio BoD
Descripción	En este caso se considera el acceso del CSU al servicio de computación en la nube que ofrece el CSP XaaS (por ejemplo, infraestructura de escritorio virtual (VDI), difusión continua de vídeo). El CSU accede al servicio desde un emplazamiento fijo, por ejemplo, a través de la red de área local (LAN) de una empresa, o desde un emplazamiento móvil, por ejemplo, un terminal móvil. El CSP XaaS ofrece el servicio sobre la base de sus propios centros de datos y no influye en el rendimiento de una determinada conexión entre usuarios extremos y el centro de datos que alberga el servicio. Desde el punto de vista del CSU, la calidad percibida (QoE) del servicio depende de una combinación de centros de datos y rendimiento de la red. El CSP XaaS puede garantizar una determinada calidad de servicio limitada por su propio centro de datos. Tal calidad puede ser inferior, como el rendimiento de la red, en una conexión entre el CSC y un centro de datos concreto. Por sí solo, el CSP no puede influir en el rendimiento de la red sin interactuar con el CSP NaaS. Como solución para garantizar la calidad de servicio de extremo a extremo, se puede reservar ancho de banda en la red entre el CSU y el centro de datos. De este modo se puede garantizar un determinado rendimiento de la red, que puede servir de base para el SLA de extremo a extremo establecido par aun servicio entre el CSU y el CSP XaaS. Para colmar esos requisitos, el CSP XaaS interactúa con el CSP NaaS. El CSP NaaS puede ser cualquier entidad con capacidad para ofrecer conectividad entre el CSP XaaS y el CSC al que pertenece el CSU.
Funciones	CSU, CSC, CSP

Figura (opcional)	
Precondiciones (opcional)	– El CSP XaaS no influye en los parámetros de conectividad entre el servicio y el CSU.
Postcondiciones (opcional)	– El CSP XaaS ofrece calidad de servicio de extremo a extremo o SLA al CSC, en cooperación con el CSP NaaS.
Requisitos derivados	– Atribución de banda ininterrumpida de extremo a extremo (véase la cláusula 9.6). – Capacidad simétrica o asimétrica (véase la cláusula 9.7).

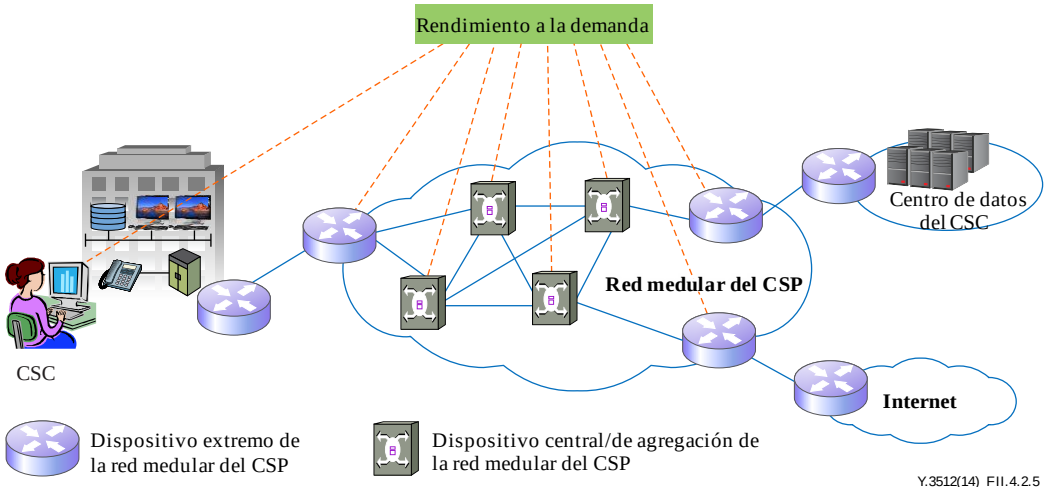
II.4.2.4 Caso de uso de la conectividad NaaS para la ingeniería de tráfico optimizada

Título	Caso de uso de la conectividad NaaS para la ingeniería de tráfico optimizada
Descripción	El CSP ofrece servicios de conectividad de red a un CSC a fin de que éste interconecte sus múltiples centros de datos geográficamente distribuidos. Al aumentar los servicios en la nube implantados en los centros de datos del CSC, cada vez más tráfico, por ejemplo, para el reflejo de datos, la redundancia, la sincronización de bases de datos, la migración V o la replicación de almacenamiento activo-activo, atraviesa la red dorsal del CSP debido al aumento de los servicios distribuidos del CSC." En la actualidad, el CSP suele ofrecer al CSC servicios de conectividad estáticos cuyo resultado es una sobreconfiguración o infrautilización de la capacidad del servicio o una infraconfiguración de servicios con capacidad limitada. Para utilizar más eficazmente sus recursos de conectividad, el CSP tiene la opción de soportar una función de toma de decisiones central para la ingeniería de tráfico de la red medular. Como mínimo, tal solución deberá coexistir con otras soluciones de redes heredadas utilizadas por el CSP para soportar otros servicios.
Funciones	CSC, CSP

Figura (opcional)	
Precondiciones (opcional)	
Postcondiciones (opcional)	
Requisitos derivados	– Ingeniería de tráfico optimizada y detallada (véase la cláusula 9.8). – Coexistencia con servicios y funciones de redes heredadas (véase la cláusula 9.9). – Visión de control y visión de abstracción centralizadas de los recursos (véase la cláusula 9.10).

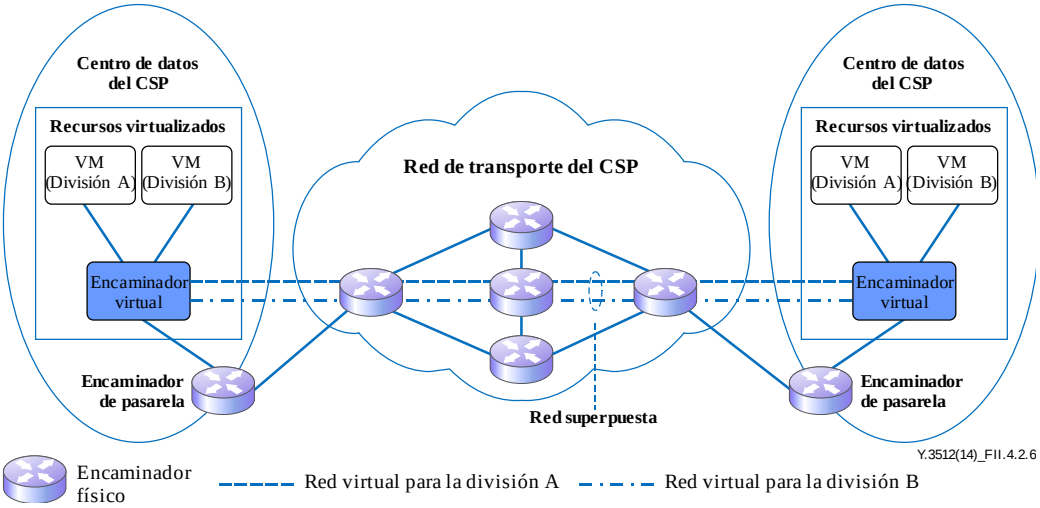
II.4.2.5 Caso de uso de la conectividad NaaS para el rendimiento a la demanda

Título	Caso de uso de la conectividad NaaS para el rendimiento a la demanda
Descripción	El CSC solicita al CSP que facilite rendimiento de red a la demanda (por ejemplo, cantidad de ancho de banda, latencia máxima y demás parámetros de QoS), lo que incluye el establecimiento dinámico y el cambio y el redimensionamiento de la capacidad de los enlaces. Sin embargo, la solución tradicional basada en la intervención humana carece de capacidades de automatización, lo que dificulta la entrega de servicios autoconfigurados y la respuesta a cambios urgentes de los requisitos de rendimiento de la red. Además, los cambios frecuentes pueden en ocasiones causar congestión e inestabilidad, pues el tráfico, que procede de diversas fuentes, comparte los mismos enlaces de red. El CSP facilita al CSC el control adecuado a fin de solicitar servicios a través de un portal y de proteger la red física subyacente del CSC.
Funciones	CSC, CSP

Figura (opcional)	
Precondiciones (opcional)	
Postcondiciones (opcional)	
Requisitos derivados	– Visión de control y visión de abstracción centralizadas de los recursos (véase la cláusula 9.10). – Control limitado de los servicios por el CSC (véase la cláusula 9.11).

II.4.2.6 Caso de uso de la conectividad NaaS para el encaminador virtual

Título	Caso de uso de la conectividad NaaS para el encaminador virtual.
Descripción	De acuerdo con [UIT-T Y.3500], la multidivisión es una característica clave del servicio en la nube, que necesita que el CSP ofrezca al CSC recursos físicos o virtuales, o de ambos tipos, compartidos, de manera que las diversas divisiones y sus recursos estén aislados y sean inaccesibles entre ellos. Esas divisiones comparten los mismos recursos físicos subyacentes, incluidos los servidores físicos, el almacenamiento físico y las redes físicas, y cada división tiene asignados sus propios recursos lógicos, incluidas las VM, el almacenamiento virtual y las redes virtuales. Esos recursos lógicos deben estar aislados unos de otros, y la computación, el almacenamiento y los recursos de red virtuales deben estar integrados y ajustados con granularidad fina. Sin embargo, los encaminadores y conmutadores físicos subyacentes heredados de la red de transporte del CSP no contienen el estado de cada división, incluidos el control de acceso a los medios (MAC) de la división y las direcciones IP y políticas de red de la VM que pertenece a la división. Dicho de otro modo, las tablas de reenvío de los encaminadores y conmutadores físicos subyacentes sólo contienen los prefijos IP o las direcciones MAC de los servidores físicos. El encaminador virtual es un encaminador de software que puede introducirse en la infraestructura de virtualización. El encaminador virtual establece la conectividad entre máquinas virtuales, conmutadores virtuales, etc., y contiene el estado de cada división, además de una tabla de reenvío distinta para una red virtual. La tabla de reenvío comprende los prefijos IP (en el caso de una red superpuesta de capa 3) o las direcciones MAC (en el caso de una red superpuesta de capa 2) de las VM. Además, no es necesario que un solo encaminador virtual contenga todos los prefijos IP o todas las direcciones MAC de todas las máquinas virtuales del centro de datos del CSP. Un encaminador virtual sólo necesita contener las instancias de encaminamiento instaladas localmente en el mismo servidor.
Funciones	CSC, CSP

Figura (opcional)	
Precondiciones (opcional)	– La red portadora IP del CSP soporta el mecanismo de superposición de red.
Postcondiciones (opcional)	– Las VM del CSC que operan en distintos centros de datos del CSP puede comunicarse unas con otras.
Requisitos derivados	– Partición de red lógicamente aislada (véase la cláusula 9.12). – Mecanismo de superposición de red (véase la cláusula 9.13).

II.4.2.7 Caso de uso de la conectividad NaaS para direcciones IP privadas y VPN

Título	Caso de uso de la conectividad NaaS para direcciones IP privadas y VPN.
Descripción	Caso I: pasarela (GW) VPN multidivisión en la nube pública con direcciones IP privadas solapantes. El CSC-I-A y el CSC-I-B comparten una GW VPN multidivisión en un emplazamiento público en la nube y ambos desean utilizar el mismo grupo de direcciones IP privadas para sus puntos extremos. Ambos CSC están conectados a la GW VPN en la nube pública a través de una de sus direcciones IP públicas. La GW VPN en la nube debe poder conmutar el tráfico de cada uno de los CSC a la subred adecuada. Caso II: Soporte de interfuncionamiento para distintos tipos de VPN. El CSC-II tiene una conexión MPLS-VPN propia de emplazamiento a emplazamiento entre su sede (HQ) y su centro de datos privado. Dada la evolución de la empresa, el CSC-II desea establecer nuevas conexiones VPN seguras de emplazamiento a emplazamiento y de emplazamiento a cliente (por ejemplo, VPN con seguridad IP (IPsec) y VPN de capa de zócalo segura (SSL)). Se ha planificado que las nuevas conexiones VPN se establezcan entre sus sucursales por todo el mundo y los usuarios móviles, manteniendo al mismo tiempo las inversiones en VPN del CSC-II existentes. Del CSP NaaS debe poder ofrecer la interconexión entre las VPN existentes del CSC y los distintos tipos de nuevas VPN. Caso III: soporte de red a la demanda para los puntos extremos distribuidos. El CSC-III necesita una solución para ofrecer conexiones de red fiables, predecibles y a la demanda para todos sus emplazamientos. Este servicio debe poder modificarse dinámicamente en función de las necesidades del CSC-III. El CSC-III desea parámetros de petición elásticos para la conectividad a los emplazamientos a través de los enlaces existentes. Se debe establecer la conectividad a uno o más puntos de presencia (PoP) del CSP NaaS invirtiendo el mínimo esfuerzo en la implantación de equipos adicionales.
Funciones	CSP, CSC

Figura (opcional)

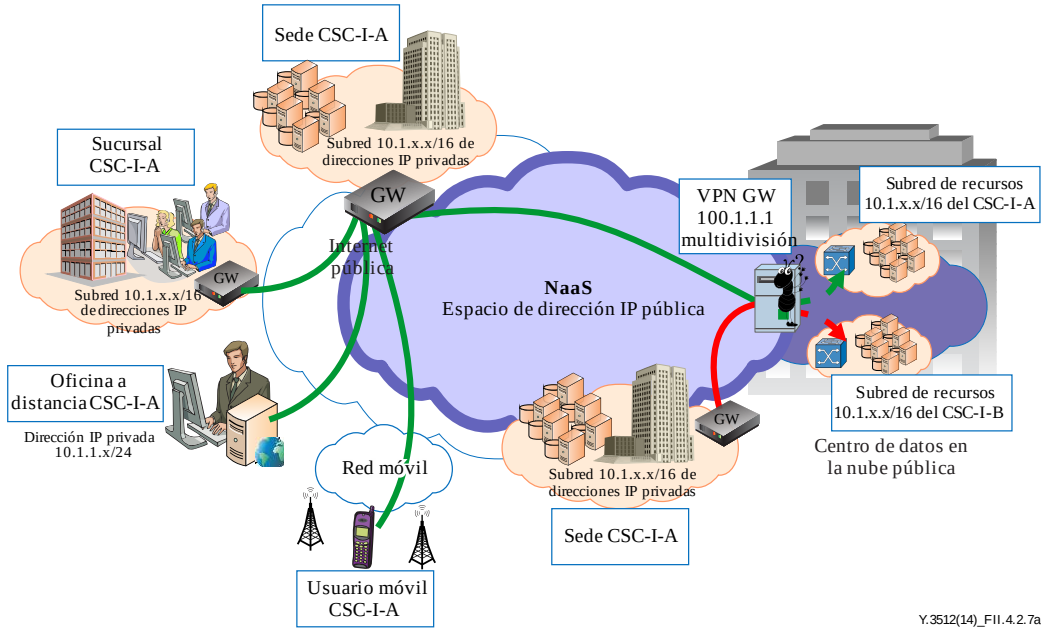


Figura 1 – Caso I: GW VPN multidivisión en la nube pública con direcciones IP privadas solapantes

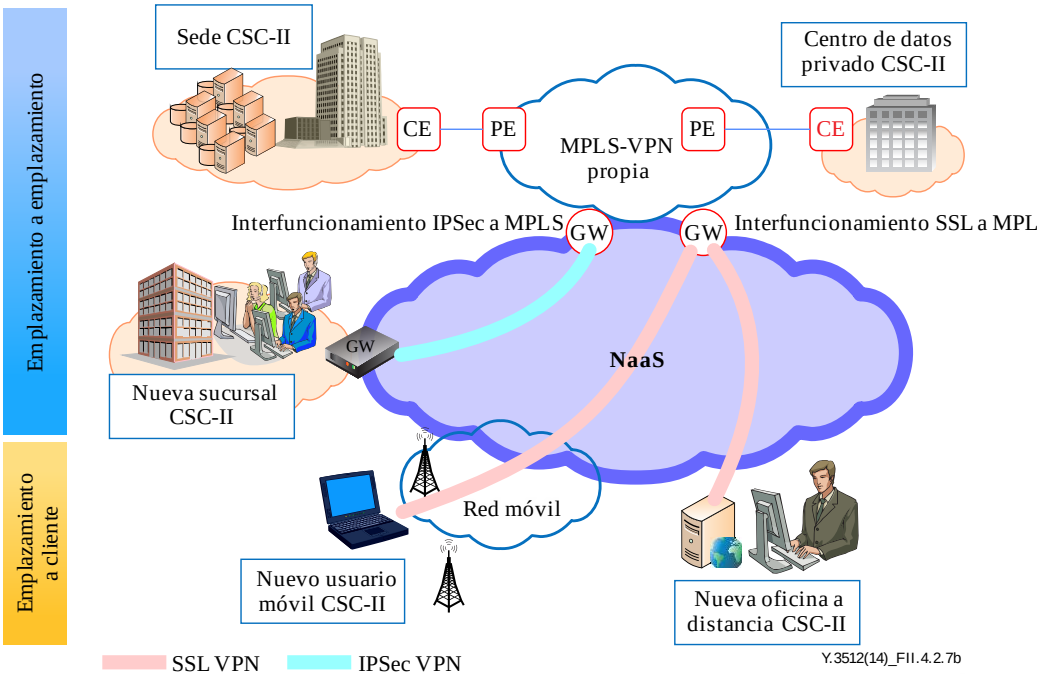
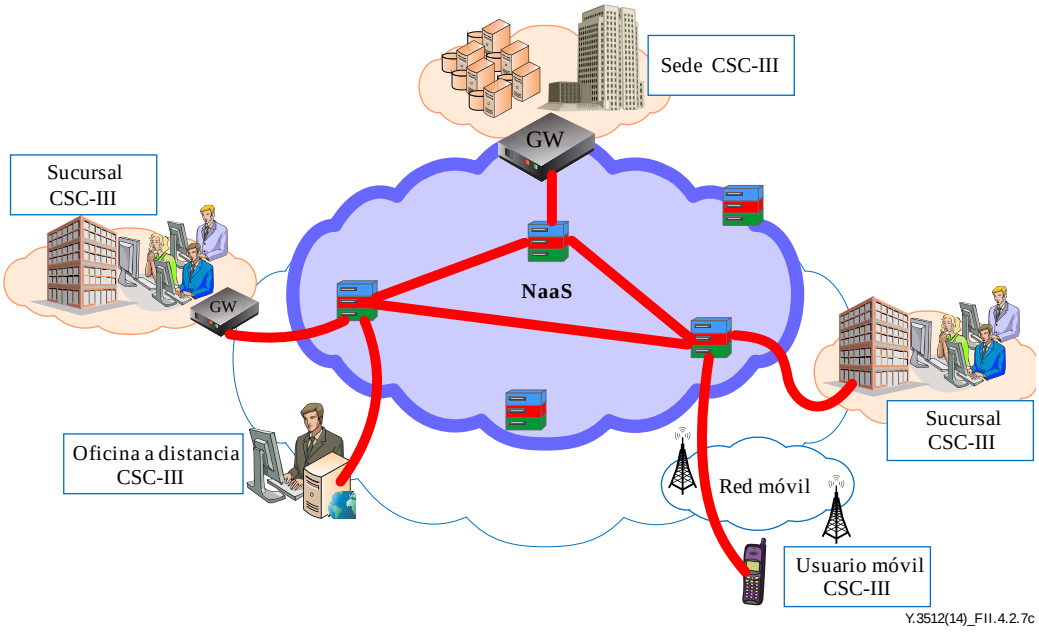


Figura 2 – Caso II: Soporte de interfuncionamiento para distintos tipos de VPN

	 **Figura 3 – Caso III: Soporte de red a la demanda para puntos extremos distribuidos**
Precondiciones (opcional)	Se supone que el CSP NaaS ofrece una GW VPN multidivisión en la nube pública.
Postcondiciones (opcional)	
Requisitos derivados	– Solapamiento de direcciones IP privadas (véase la cláusula 9.14). – Interfuncionamiento de diversas VPN (véase la cláusula 9.15). – Conexión VPN en el entorno móvil (véase la cláusula 9.16). – Conexión a la red del CSP NaaS a través de Internet pública (véase la cláusula 9.17).

Apéndice III

Consideraciones sobre las actividades relacionadas con la red del CSP

(Este Apéndice no forma parte integrante de la presente Recomendación.)

En este Apéndice se consideran las actividades relacionadas con la red del CSP.

Cada uno de los servicios pertenecientes a la categoría NaaS puede especificarse en función de una serie de términos, entre los que se cuentan los siguientes:

- Interfaz de servicio – Se ofrece al CSC y define la funcionalidad implementada por el CSP. La interfaz de servicio puede incluir funcionalidades relacionadas con los puntos de demarcación para la interconexión del CSP y el CSC, funcionalidades relacionadas con la topología y el encaminamiento para la compartición de topologías, funcionalidades relacionadas con el descubrimiento para realizar otros servicios necesarios para las actividades entre nubes, y otras funcionalidades de supervisión, protección, verificación, etc. Las funcionalidades relacionadas con el encaminamiento necesitan información sobre los puntos extremos de ingreso y egreso, y opcionalmente de los puntos intermedios, de un segmento de red. Entre los atributos de un segmento de red se pueden contar los atributos de punto frontera, los parámetros de QoS, los atributos de rendimiento, los atributos temporales, los atributos de usuario, el identificador del solicitante del servicio, etc.
- Punto de demarcación del servicio – Se trata de un punto frontera entre el CSP NaaS y el CSC NaaS que se utiliza como punto de referencia para identificar las responsabilidades y obligaciones de todas las entidades involucradas. En el caso de las redes IP/MPLS, el punto de demarcación interfaz usuario-red (UNI) es un par de frontera de cliente y frontera de proveedor. En las demás redes de transporte, la UNI y la interfaz red-red (NNI) se definen como puntos de demarcación. Por ejemplo, una UNI definida por el Foro Metro Ethernet (MEF) se implanta físicamente en un enlace Ethernet bidireccional que ofrece las diversas capacidades del plano de datos, control y gestión que necesita el proveedor de servicios en la red metro Ethernet (MEN) para delimitar claramente los dos dominios de red participantes en la operación, la administración, el mantenimiento y la configuración del servicio. Con frecuencia se utilizan la capa de abstracción de software (SAL) o el sistema operativo de red (NOS) como punto de demarcación para las plataformas de red, y los zócalos TCP/UDP para las aplicaciones de red.
- Capacidades de servicio – Es lo que NaaS ofrece al CSC a través de las interfaces de servicio, como las capacidades de servicio de conectividad y de interconexión de redes. Si bien las capacidades de conectividad de la red de transporte comprenden la red IP/MPLS, las redes de trasmisión, el subsistema multimedios IP (IMS), la interconexión de redes definida por software (SDN) y la CDN, las capacidades de conectividad de red virtual incluyen el pseudocableado, el servicio de LAN privada virtual (VPLS), la VPN L3 y la VLAN. Las capacidades de servicio de interconexión de redes pueden incluir la optimización WAN, el equilibrado de cargas, el sistema de nombres de dominio (DNS), el cortafuegos, el IPS/IDS, servicios de telecomunicaciones y aplicaciones de red como la transferencia de ficheros par a par (P2P), etc.

Aunque la NaaS de tipo capacidad de infraestructura puede ofrecer tal red como un todo, el CSC depende del CSP para la integración y personalización del software, las funcionalidades de reconfiguración y expansión de los elementos de red, así como la gestión y administración de la red. Cuando el CSC aprovecha las plataformas NaaS para construir su propia red, la responsabilidad del CSP llega hasta el punto de demarcación del servicio de la plataforma. El CSC es responsable de la gestión, la administración y la explotación de la red, así como de las funciones y servicios de red implementados hasta el punto de demarcación.

Los servicios compuestos configurados en entornos de red necesitan el respaldo de SLA en las siguientes esferas [b-EC SLA]:

- Las especificaciones del SLA capturan las dependencias e interacciones de los servicios. Las dependencias deben ser paramétricas y expresar el contexto global del servicio (por ejemplo, movimientos de datos, relaciones entre proveedores, reglas de orquestación).
- Convergencia en la gestión del SLA para manejar las dependencias (por ejemplo, gestión mixta), manteniendo al mismo tiempo la autonomía de cada proveedor en la gestión de recursos.

La especificación de los SLA y los métodos de gestión avanzados deben tener en cuenta que la composición se puede efectuar de manera centralizada (por ejemplo, con una entidad que gestiones la composición y las correspondientes ofertas de servicio) o distribuida (por ejemplo, mediante la definición de SLA consecutivos). En caso de que haya servicios cruzados, las especificaciones de los SLA han de incluir los términos comunes (que limiten de alguna manera a esos términos la obligación de calidad de extremo a extremo) o aplicarse mediante enlaces entre SLA (por ejemplo, un SLA para cada servicio con especificaciones más detalladas que incluyan enlaces a los SLA de otros servicios), como protocolo que permita la interacción entre distintas capas y entidades.

En los SLA se identifican de manera clara y precisa las responsabilidades y obligaciones de todas las entidades participantes, así como sus límites y fronteras.

NaaS puede emplearse para soportar otras actividades relacionadas con la red del CSP de servicios en la nube (por ejemplo, dar conectividad de red, entregar servicios de red y facilitar servicios de gestión de red), cuando una nube de CSC lógicamente aislada en el centro de datos del CSP permita que el CSC configure una partición privada y asilada de la nube donde el CSC puede utilizar las capacidades de la nube en una red virtual, generalmente utilizando gamas de direcciones IP definidas por él mismo. Una nube de CSC puede tener multiples subredes en un centro de datos. La conectividad de red entre un CSC distante y una nube de CSC, por ejemplo, puede incluir lo siguiente:

- Conexión VPN IPsec por la Internet pública (pasarela VPN en la frontera del CSP – pasarela VPN en los locales del CSC).
- Conexión de red dedicada por líneas privadas (pasarela VPN en la frontera del CSP – equipos en los locales del cliente (CPE)).
- Conexión VPN IPsec por líneas privadas (pasarela VPN en la frontera del CSP – pasarela VPN en los locales del CSC).
- Conexión VPN con aplicación de software por la Internet pública (aplicación VPN de software – pasarela Internet en la frontera del CSP – pasarela VPN en los locales del CSC, donde la pasarela Internet sólo encamina la conexión VPN por la Internet pública).
- Conexiones VPN con conmutación por etiquetas multiprotocolo (MPLS).

Los servicios en la nube necesitan la interconexión de múltiples nubes de CSC en una red virtual contigua y para cumplir tal requisito, la NaaS puede ofrecer lo siguiente:

- Conexiones por aplicación VPN de software dentro de la nube del CSC o entre nubes de CSC (aplicación VPN de software en la nube de CSC-1 – pasarela Internet – pasarela Internet – aplicación VPN de software en la nube de CSC-2, donde la pasarela Internet sólo encamina la conexión VPN por la Internet pública en el caso de conexión entre nubes).
- Conexión entre la aplicación VPN de software y una VPN física entre nubes de CSC (pasarela VPN en la nube de CSC-1 – pasarela Internet – aplicación VPN de software en la nube de CSC-2, donde la pasarela Internet sólo encamina la conexión VPN).
- Encaminamiento de nube de CSC a nube de CSC gestionado por el CSC por conexiones VPN IPSec físicas utilizando equipos de CSC y la Internet pública o líneas privadas (pasarela VPN en la nube de CSC-1 – equipo de CSC – pasarela VPN en la nube de CSC-2).

Bibliografía

[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 DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	**Infraestructura mundial de la información, aspectos del protocolo Internet, redes de la próxima generación, Internet de las cosas y ciudades inteligentes**
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2016