ESTUDIO TERMINOLÓGICO *"ENTERPRISE COMMUNICATION IN NEXT GENERATION CORPORATE NETWORKS (NGCN) INVOLVING PUBLIC NEXT GENERATION NETWORKS (NGN)"*

ESTUDIANTE:
ALEXANDRA DELGADO BURBANO

DIRECTORA:
Mag. EMMA RODRÍGUEZ CAMACHO

UNIVERSIDAD DEL VALLE
ESCUELA DE CIENCIAS DEL LENGUAJE
ESPECIALIZACIÓN EN TRADUCCIÓN
CALI, 2011

TABLA DE CONTENIDO

INTRODUCCIÓN

El presente trabajo consiste en la realización de un estudio terminológico sobre las Redes Corporativas de Telecomunicaciones a través de las cuales se lleva a cabo la Comunicación Empresarial o Corporativa que es una de las aplicaciones de las Redes de Comunicaciones, columna vertebral de la Telemática. Este trabajo es de carácter técnico en cuanto a que describe en detalle cada una de las etapas que los especialistas recomiendan para la realización de un estudio terminológico más que un profundo análisis teórico de las mismas. Este estudio terminológico se hizo con base en el texto *"Enterprise Communication in Next Generation Corporate Networks (NGCN) involving Public Next Generation Networks (NGN)",* informe técnico publicado en diciembre de 2005 por la organización *ECMA International (European Computer Manufacturers Association)*, dedicada a desarrollar y publicar estándares e informes técnicos para facilitar y estandarizar el uso de las Tecnologías de la Información y la Comunicación y los Dispositivos Electrónicos. Este informe técnico fue adoptado por el *ETSI* (*European Telecommunications Standards Institute)*, organización que produce estándares para las tecnologías de la información y la comunicación y por la *ISO* (*International Standardization Organization*), organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales.

El estudio terminológico, objeto del presente trabajo, da como resultado la elaboración de una base de datos terminológica en el área de las redes de computadores, en particular sobre las redes corporativas de telecomunicaciones y sus aplicaciones en la comunicación empresarial. Esta base de datos puede ser de utilidad para estudiantes y profesores de telemática, tecnología en telemática, postgrados en telemática e ingeniería electrónica y telecomunicaciones y también para traductores y profesores de inglés con propósitos específicos. Todos ellos son usuarios potenciales de la base de datos terminológica porque en su quehacer diario deben consultar y acceder a fuentes de información tanto en inglés como en español y manejar una terminología en este campo de estudio y en muchas ocasiones no cuentan con herramientas de fácil acceso y confiabilidad por ser estos temas recientes de los que no hay material suficiente en las bibliotecas, hemerotecas y otros sitios de documentación.

Esta base de datos y la traducción del informe técnico pueden contribuir a facilitar la comunicación entre los interesados en el tema porque presenta un registro bilingüe de

la terminología que surge en el campo de las redes de computadores aplicadas a la comunicación empresarial a través de las redes corporativas de comunicaciones.

Los planteamientos teóricos que se han tenido en cuenta en este trabajo son los expresados por diferentes autores tales como Amparo Hurtado Albir en *Traducción y Traductología* (2001) para el caso de la traducción, Silvia Pavel y Diana Nolet en *Manual de Terminología* (2001), Reiner Arntz y Heribert Picht en *Introducción a la Terminología* (1996), al igual que Emma Rodríguez en *Terminología y Traducción* (2004) para el caso de la terminología. Hurtado Albir (2001) proporciona el soporte teórico para el análisis textual del informe técnico base de este estudio terminológico, al igual que la definición de traducción y otros principios básicos de la misma. Pavel y Nolet (2001), Arntz y Pitch (1996) y Rodriguez (2004) proporcionan las teorías sobre terminología y las etapas que se siguen en un estudio terminológico.

En cuanto a la documentación sobre el tema de las redes corporativas de comunicación, se ha hecho una recopilación de fuentes en formato escrito y en formato electrónico en inglés y en español. Algunos de los títulos de las fuentes consultadas que abordan diferentes temas, tales como fundamentos de telemática (*Fundamentos de telemática, Laporta, 2005*), redes de comunicaciones (*Communication networks: fundamental concepts and key architectures*, *García & Widjaja, 2004),* redes corporativas de comunicación (*Next Generation Corporate Networks (NGCN) – General-ECMA TR/95 1st Edition / June 2008)* y redes de próxima generación *(Next Generation Network – Telefonía sobre IP, Znaty, 2001)* han servido para la definición de los campos y sub-campos temáticos, así como también para la elaboración del sistema conceptual en inglés y en español, para la validación, las definiciones y contextos de los términos y en general para la comprensión del tema de estudio y posterior traducción del texto. Adicionalmente, se han utilizado glosarios y diccionarios bilingües y monolingües en formato escrito y en su mayoría en formato electrónico tales como *Diccionario de informática, telecomunicaciones y ciencias afines: inglés-español, Díaz de Santos, 2004; Glossary of Definitions and Terminology for Computer Supported Telecommunications Applications (CSTA) Phase III – ECMA TR/72 3rd Edition – 2000 y* Computer Dictionary: Whatis?.com. IT Encyclopedia and Learning Center TechTarget, 2008, entre otros documentos impresos y electrónicos sobre el área.

La metodología de trabajo que se siguió durante este estudio terminológico tuvo en consideración aspectos del "Manual de Terminología de la Oficina de Traducciones" del Canadá (Pavel y Nolet, 2002) y del libro "Terminología y Traducción" de la profesora Emma Rodríguez (2004). Este estudio se desarrolló en las siguientes fases o etapas:

consideraciones preliminares donde se definieron y limitaron el tema y los subtemas, se definieron los conceptos de trabajo y los criterios para seleccionar los términos, se hizo un análisis del texto base del estudio terminológico donde se tuvieron en cuenta las dimensiones comunicativa, pragmática y semiótica del mismo, se definieron los objetivos y los destinatarios del trabajo, se realizó la primera representación conceptual del campo temático, se determinaron las lenguas de trabajo y el formato de presentación final; ***preparación del trabajo,*** etapa en la cual se inició la documentación sobre el tema y se hizo la revisión y clasificación de este material, se seleccionó el especialista o experto en el área; ***gestión de la terminología***, fase en la cual se estableció la nomenclatura terminológica, se llevó a cabo el procesamiento terminográfico de los datos, la elaboración de las fichas terminológicas y el glosario bilingüe; ***revisión*** que consiste en la validación de los términos por parte del experto o especialista seleccionado; ***presentación final*** donde se presentan los términos y el texto traducido; y por último la fase de ***control permanente del proceso.***

El producto final de este estudio terminológico está disponible y al alcance de los interesados en el tema en formato electrónico en un CD y además se puede encontrar en la plataforma TRADUTERM, Herramienta de Gestión Terminológica del grupo de trabajo en Traducción y Terminología de la Escuela de Ciencias del Lenguaje de la Universidad del Valle.

JUSTIFICACIÓN

Con la vertiginosa evolución de las telecomunicaciones y en especial con la digitalización de las redes en la moderna sociedad industrial, el intercambio de información y las comunicaciones es de vital importancia. Las redes corporativas de comunicaciones juegan un papel fundamental en el éxito de las empresas modernas porque permiten la comunicación entre usuarios ubicados en sitios dispersos. La evolución de estas redes es también enorme y cada día emergen nuevas tecnologías que es necesario conocer para aprovechar aún más sus beneficios y estar preparados para las nuevas etapas de evolución de los sistemas informáticos. Los interesados en áreas como la telemática y la ingeniería electrónica no son ajenos a esta realidad y por el contrario, deben prepararse para enfrentar estos retos tecnológicos que vive nuestro mundo actual. Por esta razón, cada vez más, buscan la posibilidad de acceder a información actualizada y confiable. Sin embargo, no siempre es fácil pues estos son temas emergentes y los recursos existentes pueden estar limitados al uso de especialistas o simplemente hay que pagar algún costo para acceder a ellos.

En el caso de los estudiantes, normalmente deben leer y estudiar diferentes documentos en inglés sobre redes de comunicaciones como parte del material que sus profesores les asignan en algunas áreas de su carrera. Los profesionales y especialistas en su campo laboral, deben estar capacitados para enfrentarse a los retos que impone el desarrollo de las redes en todas las empresas para las que pueden trabajar por lo que hacen uso de materiales que generalmente están publicados en inglés. Por otra parte, los traductores, al ser "intermediarios de la comunicación" requieren tener acceso a recursos terminológicos ágiles, actualizados y confiables para encontrar las descripciones más precisas porque sus conocimientos sobre el área de especialidad son diferentes a los del especialista (Rodríguez, 2004). Por último, los profesores de inglés con propósitos específicos necesitan acceder a la información precisa de los términos con el propósito de adquisición del idioma. En resumidas cuentas, como lo plantean Arntz y Picht en su *Introducción a la Terminología* (1996, p. 18), estos intermediarios deben superar las dificultades de la comunicación especializada en su área. Para esto "es importante registrar los nuevos términos que surgen, aclarar y determinar su significado exacto y promover su uso entre los interesados".
Por estas razones, decidimos hacer un estudio terminológico sobre el tema de las redes de comunicaciones para producir una base de datos terminológica en inglés y español

que sea una herramienta útil y confiable a la cual los estudiantes, profesionales, especialistas, profesores, traductores y todos los interesados, puedan tener fácil acceso en medios electrónicos en la biblioteca de la universidad. El texto traducido puede ser igualmente utilizado como texto de consulta para las personas que puedan tener interés en el tema.

Por otro lado, esperamos que el resultado de este estudio pueda conllevar a otros estudios sobre el mismo tema o temas relacionados y por qué no, incluso hasta la elaboración de un diccionario especializado sobre las telecomunicaciones que sea de utilidad para los estudiantes, profesionales y otros interesados en el tema. Igualmente, aunque el presente trabajo se genera en la Universidad del Valle, la autora tiene vínculos académicos con la Universidad del Cauca, por lo cual, este trabajo también beneficiaría a esta alma máter por cuanto se inicia un trabajo serio en traducción y terminología, áreas que hasta el momento no han surgido de manera formal en ningún ámbito académico en esta institución.

ANTECEDENTES

El tema de las redes corporativas de comunicación ha sido objeto de estudio desde hace varios años particularmente por parte de ECMA International que ha publicado varios informes técnicos que describen aspectos generales y específicos sobre las mismas. Todos estos informes técnicos se pueden descargar sin costo alguno desde la página web de ECMA International http://www.ecma-international.org/. Algunos títulos son ***Corporate Telecommunication Networks – Mobility for Enterprise Communications*** *- ECMA TR/92 1st Edition / December 2005 y* ***Next Generation Corporate Networks (NGCN)*** *–* ***General-*** *ECMA TR/95 1st Edition / June 2008, entre otros.*

Por otro lado, hay diversidad de sitios web que describen proyectos y empresas relacionadas con la implementación de las redes corporativas tales como Corporate Network http://www.corpnet.ca/, una compañía cuyo objetivo es proporcionar a las empresas e individuos formas de mejorar su productividad capacitándolos para comunicarse de manera más efectiva con colegas, vendedores y clientes. Este sitio web y otros similares han servido al presente estudio principalmente para la documentación sobre el tema de las redes corporativas.

Así mismo, a través del Internet se consiguen algunos diccionarios y glosarios de tecnología en general. Los diccionarios o glosarios específicos sobre las redes corporativas de comunicaciones no son muy comunes y podrían ser de acceso restringido ya que en la web no se encuentran con facilidad. Sin embargo, hay una gran cantidad de glosarios y diccionarios sobre todo en inglés relacionados con las comunicaciones y las tecnologías de la información como por ejemplo: http://www.webopedia.com/TERM/N/NGN.htm, enciclopedia dedicada a la tecnología de computadores. Este y otros glosarios y diccionarios han sido una ayuda útil para el trabajo terminológico objeto de esta monografía puesto que es un sitio que se actualiza de acuerdo con la evolución de las tecnologías de la información. Estos se han utilizado para encontrar definiciones y equivalentes en inglés y español.

En cuanto a otros estudios terminológicos sobre las redes corporativas de comunicaciones, no se encuentran al alcance documentos que los describan. En la Escuela de Ciencias del Lenguaje de la Universidad del Valle hay monografías de estudios terminológicos en áreas tales como la odontología, la medicina, la ingeniería

mecánica, la ingeniería civil, entre otras. En cuanto a las tecnologías de la información y la comunicación hay un estudio terminológico sobre el Lenguaje de Programación *Powerbuilder* y una monografía con la traducción comentada *"Como asegurar la calidad del software en los sistemas de tiempo real"*. También se encuentra la monografía titulada *"Centro de Documentación Virtual sobre Materiales y Estructuras Inteligentes"* que describe el diseño de tal centro para los estudiantes del doctorado de la Escuela de Ingeniería Civil de Univalle. Los estudios en mención han servido de guía para este trabajo porque proporcionan parámetros a seguir en la redacción del texto final de la presente monografía, métodos de trabajo terminológico, modelos de fichas terminológicas, etc.

OBJETIVOS

General

Hacer un estudio terminológico sobre el tema de las Redes Corporativas de Telecomunicaciones con base en un informe técnico de ECMA Internacional para crear una base datos terminológica que sirva como herramienta de consulta a los estudiantes, profesionales, especialistas, traductores y otros interesados en el área de la telemática.

Específicos

1. Traducir el texto *"Enterprise Communication in Next Generation Corporate Networks (NGCN) involving Public Next Generation Networks (NGN)"* al español.
2. Identificar los términos que componen el campo conceptual de la telemática con base en el texto objeto de estudio y la documentación sobre el tema.
3. Elaborar una base de datos terminológica bilingüe como recurso de consulta útil y confiable en el área de la telemática, y en particular de las redes de telecomunicaciones.
4. Hacer un aporte significativo al área de la traducción en la Universidad del Valle y la Universidad del Cauca para motivar a otros profesionales en el área de lenguas a vincularse a proyectos de traducción y terminología.

I. MARCO TEÓRICO

Este marco teórico representa los conceptos y teorías fundamentales que se tuvieron en cuenta para la elaboración del estudio terminológico sobre el tema de las Redes Corporativas de Comunicaciones que se desarrolló con base en el texto *"Enterprise Communication in Next Generation Corporate Networks (NGCN) involving Public Next Generation Networks (NGN)" (Ver Anexo 5)*. En él se consideran posiciones de diferentes autores en cuanto a la traducción y a la terminología las cuales se han utilizado como soporte en el desarrollo de cada una de las etapas del presente estudio.

A. NOCIONES SOBRE LA TRADUCCIÓN

Uno de los propósitos del presente trabajo es la traducción de un texto especializado que permitirá comunicar nociones importantes sobre la telemática a los interesados. Por esta razón, es claro que aquí la traducción se toma como un acto de comunicación, necesario para traspasar la barrera lingüística y cultural y lograr que el destinatario que no conoce la lengua de origen pueda entender el texto base del presente estudio. Así, la meta es comunicar y no simplemente reformular un texto en otra lengua sin tener en cuenta los rasgos situacionales y finalidad del mismo según la propuesta de Hurtado (2001), en la que propone la traducción como un "proceso interpretativo y comunicativo consistente en la reformulación de un texto con los medios de otra lengua que se desarrolla en un contexto social y con una finalidad determinada."

Siendo la transmisión del sentido y función del texto, el propósito de nuestra traducción, también es relevante en este trabajo el planteamiento de Rodríguez (2004) según el cual "la traducción no se reduce a una simple transferencia entre lenguas, sino que es una operación compleja de interpretación, de desverbalización y de reconstrucción del sentido que concede un papel determinante al factor extralingüístico" porque a lo largo del trabajo de traducción del texto de ECMA se procuró al máximo interpretar el sentido original que quisieron comunicar los autores del texto original y transmitirlo de la manera más fiel posible.

Tipos de Traducción:

Según Hurtado (2001), en la modalidad de la traducción escrita, los tipos de traducción están relacionados con las áreas convencionales tradicionales: traducción literaria,

traducción general y traducción especializada. Hurtado prefiere hablar de traducción de un texto especializado más que de traducción especializada ya toda traducción es especializada por los conocimientos y habilidades especiales que requiere. En cuanto al tipo de traducción que se hizo con el informe técnico de ECMA se concluyó que es una traducción de un texto especializado porque está escrito por especialistas para especialistas y pertenece a los llamados lenguajes de especialidad: lenguaje técnico y científico.

Método Traductor:

Al emprender cualquier trabajo de traducción es necesario definir un método traductor. Hurtado (2001) lo define como "el desarrollo de un proceso traductor determinado, regulado por un principio en función del objetivo perseguido por el traductor; se trata de una opción global que recorre todo el texto". Hurtado también presenta una propuesta de clasificación de los métodos básicos de traducción. Para la traducción del texto objeto del presente estudio se escogió el Método Interpretativo Comunicativo siguiendo la premisa de que la traducción es un acto comunicativo. Hurtado (2001), define el método interpretativo comunicativo como un "método traductor que se centra en la comprensión y reexpresión del sentido del texto original conservando la traducción la misma finalidad que el original y produciendo el mismo efecto en el destinatario; se mantienen la función y el género textual". Como se enfatizó al comienzo de este marco teórico, la traducción que se hizo del informe técnico de ECMA tuvo como objetivo trasmitir fielmente el sentido y la finalidad del texto original teniendo en cuenta el contexto y la situación de comunicación para no cambiar su efecto en el destinatario.

Etapas de la traducción:

Para la traducción del texto base del presente estudio se tuvo en cuenta el proceso de traducción propuesto por Delisle (1985) y citado por Rodríguez (2004) en el cual se definen tres fases:

A. Fase de comprensión o descodificación de los signos del texto original: el traductor realiza un análisis a nivel sintáctico, semántico y pragmático, capta el sentido y realiza una primera interpretación.

B. Fase no verbal de asimilación de los conceptos a través de mecanismos mentales no lingüísticos: mediante la confrontación de conceptos realiza un proceso analógico y se propone una reformulación mental.

C. Fase de reformulación o codificación en la que verifica las soluciones provisionales de la fase b para hacer la transferencia a la lengua meta. El traductor hace la selección y elección de los equivalentes potenciales y los actualiza en un texto meta.

Estas fases se tuvieron en cuenta al momento de traducir el texto base de este estudio terminológico porque presenta una secuencia lógica de etapas claras que llevan al objetivo de comunicar nociones después de comprender el texto, analizarlo y reformularlo en la lengua meta.

Análisis Textual orientado a la traducción

Como metodología para desarrollar el proceso de interpretación y reconstrucción de sentido en el análisis textual del texto base del presente estudio se utilizó el enfoque textual propuesto por Hatim & Mason (1990) citado en Hurtado (2001). Estos autores identifican tres dimensiones del contexto necesarias para el análisis textual:

Dimensión comunicativa: se refiere a la variación lingüística dependiendo del uso y los usuarios del lenguaje en cada situación de comunicación. Esta variación se refiere al registro, el campo, el modo y el tono.

Dimensión pragmática: se refiere a la intención del emisor del discurso y el efecto que se desea obtener. Aquí se tiene en cuenta la función del texto que puede ser argumentativa, expositiva o exhortativa.

Dimensión semiótica: se refiere a las interacciones de los elementos del texto en tanto que signo: sistema de valores de una cultura con sus géneros, presupuestos y convenciones.

En la sección de este trabajo denominada ANÁLISIS TEXTUAL DEL INFORME TÉCNICO: *"Enterprise Communication in Next Generation Corporate Networks (NGCN) involving Public Next Generation Networks (NGN)"*, página 39, se presenta en detalle el desarrollo de cada una de estas dimensiones teniendo en cuenta el texto objeto de este estudio.

B. NOCIONES SOBRE LA TERMINOLOGÍA

En cuanto a la terminología, las teorías que se destacan como soporte en este trabajo terminológico son las propuestas por María Teresa Cabré (1999) y Arntz y Picht (1996).

Cabré (1999), citada en Rodríguez (1994) propone la Teoría Comunicativa de la Terminología (TCT). Cabré define la TCT según ciertos parámetros: la terminología es un campo interdisciplinario, cuyo objeto de estudio son las unidades terminológicas pertenecientes al lenguaje natural y a la gramática de cada lengua; los términos son unidades léxicas, activadas singularmente por sus condiciones pragmáticas y están constituidos por forma o denominación y por significado o contenido; este último no es absoluto, sino relativo a cada ámbito y situación de uso; los conceptos de un ámbito especializado mantienen relaciones de distinto tipo entre sí, creando la estructura conceptual de una materia; el objetivo de la terminología teórica es describir de modo semántico, formal y funcional las unidades que tienen valor terminológico y explicar sus relaciones con otros signos del mismo u otro sistema; los términos poseen doble función, la representación del conocimiento especializado y su transferencia. En la TCT, la terminología se concibe como el conjunto de unidades usadas efectivamente en la comunicación especializada.

El presente estudio terminológico se fundamenta en la Teoría Comunicativa de la Terminología porque su objetivo es la unidad terminológica del área de especialidad de la telemática. Además de representar el área especializada, las unidades terminológicas aquí definidas sirven también para la transmisión de ese conocimiento especializado, es decir, son unidades de comunicación especializada que responden siempre al esquema comunicativo de un emisor-especialista.

Arntz y Picht (1996) llaman terminología al léxico especializado de un área determinada y señalan la definición de la norma DIN 2342 Parte 1 (1986): la terminología es el conjunto completo de conceptos de un área especializada y sus denominaciones. Arntz y Picht consideran la terminología como un componente de la lengua correspondiente a un área especializada y por consiguiente, como un componente de un lenguaje especializado. Plantean la necesidad de una ciencia como la terminología dadas las dificultades de comunicación cada vez más frecuentes incluso entre especialistas de distintos campos. En concordancia con esto, afirman que la terminología ha ido adquiriendo cada vez más importancia porque se hace necesario aclarar y determinar nuevos términos para propiciar la comunicación en cualquier área a nivel internacional.

El presente trabajo se fundamenta en estas teorías porque tiene el objetivo de crear un recurso terminológico en el área de especialización de las redes de comunicaciones para facilitar el acceso a una fuente adecuada de información terminológica que responda a la necesidad creciente de la comunicación especializada entre usuarios de este campo.

Usuarios de la Terminología

Como parte de la metodología del trabajo terminográfico, es necesario definir quienes son los usuarios potenciales del producto final del estudio.

Rodríguez (2004, p. 51) cita a Sager (1993) y plantea que "la multiplicidad de relaciones de la terminología también se ve reflejada en la variedad de usuarios, con diferentes necesidades y objetivos de comunicación". Los usuarios de la terminología son:

- **Los especialistas en una materia.**
- **Los intermediarios de la comunicación** (traductores, redactores de textos técnicos o científicos, profesores y estudiantes de un área, etc.).
- **Los lexicólogos y los terminólogos.**
- **Los especialistas de la información y la documentación.**
- **Los planificadores del lenguaje.**
- **El usuario general.**
- **Otros** (editores, profesores de lenguas, investigadores de lingüística aplicada).

Además de tener claridad sobre quienes pueden ser los usuarios de la terminología, es necesario tener una definición clara de los elementos básicos de la terminología: las nociones relacionadas con el término, el concepto, la denominación y la definición con el fin de hacer una extracción confiable y pertinente de la terminología del texto seleccionado. Con este fin, para el presente trabajo se tuvieron en cuenta las siguientes definiciones planteadas por Arntz y Picht (1996: 57,58,64,87):

Término

"Un término, como elemento de una terminología, es una unidad constituida por un concepto y su denominación."

Concepto
"Un concepto es una unidad de pensamiento que abarca las características comunes asignadas a objetos. Los conceptos no están vinculados a determinadas lenguas, no obstante reciben la influencia del trasfondo social y/o cultural de cada momento".

Denominación
"Una denominación es la designación, formada por un mínimo de una palabra, de un concepto en el lenguaje especializado".

Definición
"Una definición consiste en la determinación de un concepto con medios lingüísticos".

IDENTIFICACIÓN DE TÉRMINOS

Estos aspectos se han tenido en cuenta al momento de seleccionar lo que se considera un término en el texto base de este estudio. Los criterios que a continuación se mencionan están descritos en *Terminología y Traducción, Rodríguez, 2004.* Los ejemplos tomados del texto objeto del presente estudio se pueden encontrar en la sección de Metodología del Trabajo Terminográfico en el presente documento.

FORMACIÓN DE TÉRMINOS
Los términos siguen la misma formación que las palabras del texto común:

Por derivación: sufijos, prefijos, mixta.
Procesos de sintagmación: por lexicalización, por epónimos, sintagmas con siglas.
Procesos fonológicos: abreviación, siglación, acronimia.
Préstamo y calco: incorporación de unidades léxicas de otras lenguas.

CLASES DE TÉRMINOS:

Según la forma: simples, complejos, siglas, acrónimos, abreviaturas.
Según la función discursiva: verbos, sustantivos, adjetivos.
Según el significado: objetos, procesos, propiedades, relaciones.

CRITERIOS PARA LA IDENTIFICACIÓN DE TÉRMINOS
Rodríguez cita a Cabré (1993:296) quien enumera estos parámetros para la identificación de términos en un texto. Estos parámetros se tuvieron en cuenta al

momento de seleccionar los términos en el texto de ECMA base del presente estudio terminológico, por consiguiente se consideran términos porque:

- Son unidades frecuentes en el texto.
- Representan un concepto reconocido.
- Son unidades semánticamente opacas.
- Son unidades marcadas tipográficamente.
- Son unidades acompañadas de definición aparente.
- Son unidades aparentemente no relacionadas con ninguna otra área de especialidad.
- Hay presencia de estructuras sintagmáticas habituales.

REPRESENTACIÓN CONCEPTUAL

Como lo plantean Arntz y Picht (1995:102), con el fin de comprender una disciplina en profundidad, es necesario conocer la ordenación sistemática de los conceptos y denominaciones del área especializada de estudio. Es por esto que para el presente trabajo terminológico, se desarrolló la estructura conceptual de la telemática y las redes de comunicaciones con base en las teorías de Arntz y Picht y que se resumen a continuación.

Sistema de conceptos: En la terminología, los conceptos deben ordenarse según ciertos esquemas de clasificación y presentarse dentro de una estructura sistemática o sistema conceptual. Sin esta organización, no es posible delimitar un concepto con respecto a otros conceptos de manera verificable (Arntz y Picht, 1995). La Norma DIN 2331, 1980:2, citada en Introducción a la Terminología, define un sistema de conceptos como un conjunto de conceptos entre los cuales existen o se han establecido relaciones formando así un todo coherente.

Representación gráfica de un sistema de conceptos:
La representación conceptual de un sistema permite visualizar los conceptos considerados como piezas de un sistema y las relaciones que existen entre unos y otros. Para hacer la representación conceptual de un área especializada es necesario tener clara la estructura o "diseño" en cuanto a las relaciones que existen entre los conceptos.

Tipos de relaciones

A. Relaciones conceptuales jerárquicas:

1. **De abstracción:** entre un concepto superordinado y su correspondiente concepto subordinado. De ello se deriva como relación especial la coordinación. Si se divide un concepto superordinado empleando en cada nivel un criterio de ordenación, se habla de un **sistema monojerárquico**. En un **sistema polijerárquico** se emplean varios criterios de ordenación en un mismo nivel. Hay relaciones de subordinación, intersección y coordinación.

2. **Ontológicas**: se basan en la relación entre el todo y sus partes. El todo, o sea el concepto en la parte superior, se denomina **concepto incluyente**, el subordinado **concepto específico parcial**. Hay relaciones partitivas, de sucesión y de efecto.

B. Relaciones conceptuales no jerárquicas:

Hay una relación entre conceptos de tipo secuencial, sobre todo de **contigüidad.** En este caso no hay jerarquía. Se presentan relaciones cronológicas, causales, genéticas, de producción, de transmisión, instrumentales y funcionales.

En el capítulo II de este trabajo, fase 2, punto C, denominado "Representación Conceptual" en la página 28, se presenta la descripción de los tipos de relaciones que se encontraron en el texto base del presente estudio.

II. METODOLOGÍA PARA EL TRABAJO TERMINOGRÁFICO DEL INFORME TÉCNICO: *"ENTERPRISE COMMUNICATION IN NEXT GENERATION CORPORATE NETWORKS (NGCN) INVOLVING PUBLIC NEXT GENERATION NETWORKS (NGN)"*

Como lo plantea Rodríguez (2004), si se desea realizar un trabajo terminográfico de calidad, es necesario seguir una metodología apropiada y planear y ejecutar las etapas de manera rigurosa para garantizar la calidad de los resultados. Con este fin, a continuación se describen las etapas que se cumplieron para el desarrollo del estudio terminológico basado en el informe técnico de ECMA:

FASE 1: CONSIDERACIONES PRELIMINARES

Antes de empezar un trabajo terminológico, es necesario preguntarse por los recursos con que se cuenta, plantearse los objetivos del trabajo, determinar las lenguas de trabajo, tomar las decisiones metodológicas pertinentes, etc. para garantizar la calidad del resultado. Estos elementos se definen a continuación:

A. DEFINICIÓN DE CONCEPTOS GENERALES DEL TRABAJO Y SELECCIÓN DEL ÁREA DE CONOCIMIENTO

1. Delimitación del tema y los subtemas:
Para delimitar el campo temático se tuvo en cuenta la clasificación temática de la Agencia Nacional de Evaluación y Prospectiva del Ministerio de Ciencia e Innovación de España que se basa en la Nomenclatura Internacional de la UNESCO para los campos de Ciencia y Tecnología. Esta es la clasificación:
ÁREA: Matemáticas y tecnología de la información y las comunicaciones.
SUB-ÁREA: Tecnología electrónica y de las comunicaciones.
DISCIPLINA: Telecomunicaciones.
ÁREA DE CONOCIMIENTO: Ingeniería telemática.

CAMPO TEMÁTICO: Telemática
SUB-CAMPO TEMÁTICO: Redes de Comunicaciones

2. Definición de conceptos generales: estos son los dos conceptos fundamentales de este estudio terminográfico:

- TELEMÁTICA: existen varias definiciones de este concepto:

a. La **telemática** es la asociación de técnicas propias de las telecomunicaciones y la informática, con la que se realiza a distancia el intercambio de datos y el control de tratamientos automáticos, más concretamente podemos decir que la telemática proporciona a personas no especializadas, la posibilidad de acceder a sistemas de comunicación e información antes reservados a especialistas. La columna vertebral de la telemática está constituida por las **redes de transmisión de datos**.
Fuente*: Introducción a la telemática y a las redes de datos*
Documentación en formato electrónico – Telefónica de España – Dirección de
Servicios de Formación de Telefónica de España, Marzo de 2000. Página 18
b. La palabra **telemática** es un acrónimo que proviene de la conjunción de los vocablos **telecomunicaciones** e **informática**. La telemática trata de todo lo que tiene que ver con la comunicación entre ordenadores, tanto en entornos locales como en entornos más amplios.
Fuente: *Fundamentos de telemática*
Jorge Lázaro Laporta - Colaborador Marcel Miralles Aguiñiga
Ed. Univ. Politéc. Valencia, 2005 - Página 3

c. La **telemática** es el campo de estudio, en que tanto las tecnologías, sistemas, redes o servicios en los que operativamente y en la proporción que sea, están inmersos ordenadores y comunicaciones, en definitiva, la aplicación de la informática como soporte de las comunicaciones.
Fuente: *Fundamentos de telemática*
Jorge Lázaro Laporta - Colaborador Marcel Miralles Aguiñiga
Ed. Univ. Politéc. Valencia, 2005 - Página 3

- RED DE COMUNICACIONES:

a. **Red de comunicaciones:** Una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos (no jerárquica -master/slave-). Normalmente se trata de transmitir datos, audio y vídeo por ondas electromagnéticas a través de diversos medios (aire, vacío, cable de cobre, fibra óptica, etc.)
Fuente: Network + Study Guide
David Groth, Toby Skandier, Todd Lammle, William Tedder
Second Edition, John Wiley and Sons, 2005 – Página: 3

b. **Red de comunicaciones:** es una serie de equipos e instalaciones que brinda un servicio: la transferencia de información entre usuarios localizados en diferentes ubicaciones geográficas.
Fuente: Communication Networks: fundamental concepts and key architectures. Alberto León García – Indira Widjaja. McGrawHill Professional 2004. Página 1.

3. Conceptos básicos para el trabajo: ¿Qué se ha considerado como término?

a. Todos los términos escogidos tienen una función comunicativa dentro del campo especializado de la telemática y las redes de comunicaciones.
b. Algunos de los términos escogidos no pertenecen exclusivamente al campo temático de la telemática, también pueden ser utilizados en otras áreas, pero se tiene en cuenta que "adquieren un sentido particular en cada una y funcionan como término especializado para cada área". (Rodríguez, 2004: 75). Por ejemplo el término *Autenticación* (Ficha # 4) en el contexto de las redes de comunicaciones se refiere al *procedimiento de comprobación de la identidad de un usuario*; mientras que en el campo legal, *autenticación* se refiere al *testimonio que da un notario de que un documento es lo que parece ser*. Para evitar la ambigüedad se nombra el campo temático en cada ficha terminológica.
c. Los términos escogidos se producen en diferentes espacios comunicativos tales como artículos académicos, informes técnicos, estándares, glosarios, diccionarios, bases de datos, libros, revistas especializadas, etc., del área de la telemática y no han sido escogidos de manera aleatoria o aislada.
d. Los términos escogidos siguen las reglas de formación de las palabras del léxico común, entre ellas:
    - ✓ Por derivación: bridging, enrutamiento (con sufijos: -ing, -iento).
    - ✓ Procesos de sintagmación: Black list, circuit-switched network (adj + n), comunicación empresarial (n + adj), Protocolo de Inicio de Sesión (n + prep + n + prep + n). Diffie-Hellman key agreement (epónimos).
    - ✓ Procesos fonológicos: Centrex, codec (Acronimia), IP, NGN (siglas).
    - ✓ Préstamo y calco: firewall, SIP URI.
e. Los términos escogidos son de diferentes clases:
    - ✓ Simples: proxy
    - ✓ Complejos: red heredada
    - ✓ Combinación de palabras: autoridad de certificación
    - ✓ Siglas: RDSI, VoIP
    - ✓ Acrónimos: ENUM

- ✓ Abreviaturas: B2BUA
- ✓ Sustantivos: Gateway
- ✓ Objetos: outbound proxy
- ✓ Procesos: Traducción de Direcciones de Redes
- ✓ Propiedades: Quality of Service, resiliencia

4. Criterios para la identificación de términos:

Para la identificación de los términos en el texto "*ENTERPRISE COMMUNICATION IN NEXT GENERATION CORPORATE NETWORKS" (NGCN) INVOLVING PUBLIC NEXT GENERATION NETWORKS (NGN)*" se tuvieron en cuenta los parámetros definidos por María Teresa Cabré (1993:296) y citados por Rodríguez (2004:77).

- ✓ La unidad es frecuente en el texto: algunos ejemplos de unidades que cumplen con este parámetro son:

Unidad terminológica	Número de ocurrencias en el texto
B2BUA	10
Encryption	10
End-to-end	32
Firewall	36
Gateway	33
ISDN	39

- ✓ La unidad representa un concepto reconocido: las unidades que cumplen con este parámetro representan conceptos reconocidos porque ya han sido definidos en fuentes especializadas sobre el área temática tales como glosarios, diccionarios, libros, artículos, etc.

Unidad terminológica	Fuente especializada
Application Service Provider (ASP)	Computer Dictionary – Whatis?.com. IT encyclopedia and learning center. TechTarget, 2008. http://searchsoa.techtarget.com/sDefinition/0,,sid26_gci213801,00.html
Circuit-switching	Webopedia: online encyclopedia dedicated to computer technology. WebMediaBrands Inc. 2009 http://www.webopedia.com/TERM/C/circuit_switching.html

Corporate Telecommunication Networks (CNs) Signalling	ECMA TR/92 1st Edition / December 2005 **Corporate Telecommunication Networks – Mobility for Enterprise Communications** Página: 2 **Telecommunications technologies reference** Bradley Dunsmore, Toby Skandier Cisco Press, 2002 ISBN 1587050366, 9781587050367 Página 22.

- ✓ La unidad es semánticamente opaca: los siguientes ejemplos de unidades cumplen con este parámetro porque su significado no es claro si tratamos de entenderlo desde la lengua común.

Unidad terminológica
H.323
Keepalive
NAT traversal
Session Border Controller (SBC)
Simple Traversal of UDP through NATs (STUN)
Via header

- ✓ La unidad está marcada tipográficamente: estos son algunos ejemplos de unidades que cumplen con este parámetro porque han sido resaltados en el texto como abreviaturas y siglas que se utilizan a lo largo del informe técnico:

Unidad terminológica
ALG Application Layer Gateway
API Application Protocol Interface
ASP Application Service Provider
B2BUA Back-to-Back User Agent
CN Corporate telecommunication Network
CSTA Computer Supported Telecommunications Applications

- ✓ La unidad está acompañada por una definición aparente: estos son algunos ejemplos de unidades que cumplen con este parámetro porque tienen una definición dentro del mismo texto en la sección denominada *Definitions*:

Unidad terminológica	Definición en el texto
Virtual Private Network (VPN)	Virtual network that can deliver ubiquitous and secure connectivity over a shared network infrastructure (e.g. public carrier networks) using the same access policies as an enterprise network. Página 2.
Application Service Provider (ASP)	An entity that provides telecommunication applications. Página 2.
Session Service Provider (SSP)	An entity that intervenes in and adds value to signalling for the establishment and control of multi-media sessions and optionally intervenes in and adds value to the multi-media sessions themselves. Página 2.
Transport Service Provider (TSP)	An entity that provides IP connectivity. Página 2.

- ✓ La unidad no se relaciona aparentemente con ninguna otra área de especialidad: estos son algunos ejemplos de unidades que cumplen con este parámetro porque aparentemente no definen conceptos en otras áreas del conocimiento lo cual se ha corroborado con la búsqueda de cada unidad en diccionarios y glosarios de áreas afines.

Unidad terminológica
VoIP
User Agent Server (UAS)
Uniform Resource Identifier (URI)
STUN server
Softswitch
Public Next Generation Network

B. DEFINICIÓN DE OBJETIVOS Y DESTINATARIOS DEL TRABAJO

1. Objetivos del trabajo:

Los objetivos del presente trabajo se encuentran definidos en la página 5 en la sección denominada Objetivos.

2. Usuarios potenciales del producto final:

El presente trabajo se dirige básicamente a los usuarios de la terminología en el área de la telemática, por esta razón, los usuarios posibles del producto final son variados:

- Estudiantes y profesores de telemática, tecnología en telemática, postgrados en telemática e ingeniería electrónica y telecomunicaciones. Ellos son usuarios potenciales de la base de datos terminológica porque en su quehacer diario deben consultar y acceder a fuentes de información tanto en inglés como en español y manejar una terminología propia de este campo de estudio y en muchas ocasiones no cuentan con herramientas de fácil acceso y confiabilidad en las universidades al ser estos temas recientes de los que no hay material suficiente en las bibliotecas, hemerotecas y otros sitios de documentación. Si bien es cierto que en nuestra sociedad informatizada el Internet se ha convertido en la herramienta de consulta número uno, no siempre es fácil acceder a este servicio y sobre todo no siempre la información proviene de fuentes confiables. Los estudiantes y profesores más beneficiados serán los de la Universidad del Valle pues el producto final del presente estudio terminológico se pondrá a su alcance en formato electrónico en un CD y en la plataforma TRADUTERM. Así mismo se espera que este producto pueda ser publicado en la Universidad del Cauca pues en esta institución el área de la telemática se estudia de manera profunda en los programas del Departamento de Telemática de la Facultad de Ingeniería Electrónica y Telecomunicaciones. Es posible que este producto también quede al alcance de estudiantes y profesores de otras universidades.

- Especialistas: los ingenieros telemáticos, tecnólogos en telemática, magísteres y doctores en telemática e ingenieros electrónicos. Como lo señala Sager (1993:27), citado por Rodríguez (2004:51), los especialistas son usuarios potenciales de un trabajo terminológico porque hacen referencia ocasional a bases de datos terminológicas para verificar significados, comprobar ortografía, documentarse sobre los términos, etc. Gracias al producto final del presente estudio los especialistas de las Universidades del Valle y del Cauca contarán con una herramienta confiable y de fácil acceso.

- Traductores: al ser "intermediarios de la comunicación" los traductores requieren tener acceso a recursos terminológicos ágiles, actualizados y confiables para encontrar las descripciones más precisas porque sus

conocimientos sobre el área de especialidad son diferentes a los del especialista (Rodríguez, 2004:51).

- ❖ Profesores de inglés con propósitos específicos: necesitan acceder a la información precisa de los términos con el propósito de adquisición del inglés (Rodríguez, 2004:51).

3. Nivel de lengua utilizado:

- El nivel de lengua utilizado en las fichas terminológicas y en la traducción del informe técnico base del presente trabajo terminológico es especializado. Como lo cita Rodríguez (2004:94) el propósito del lenguaje especializado es contribuir a la comunicación entre los especialistas y conocedores del área temática. Para este caso, los especialistas y conocedores del área temática y potenciales usuarios de la base de datos terminológica son los profesionales y estudiantes del área de la telemática de la Universidad del Valle y de la Universidad del Cauca, entre otras. Es por eso que el nivel de lengua utilizado en el presente trabajo es especializado. Si bien es cierto que otros posibles usuarios de la base de datos terminológica pueden ser los traductores y profesores de inglés con propósitos específicos que no son expertos en el área de la telemática, el nivel de lengua debe ser especializado porque en su quehacer éstos deben hacer uso de fuentes confiables que les ilustren de manera precisa sobre los conceptos que componen el área de la telemática. En muchos casos los traductores trabajan con textos que se dirigen a especialistas y otros profesionales del área, por eso deben manejar los conceptos y consultar las fuentes especializadas sobre el tema para comunicar las ideas con precisión en el nivel especializado. Los profesores de inglés con propósitos específicos trabajan textos dirigidos a estudiantes del área que están en proceso de formación y deben manejar los conceptos adecuados a su campo de acción y con el nivel de especialización que su carrera requiere por enfrentarse a materiales especializados, especialistas en la materia, etc.

- De acuerdo con la clasificación de los lenguajes de especialidad propuesta pro Hoffman y citada por Rodríguez (2004:96) el nivel de lengua que se maneja en el presente trabajo terminológico es alto porque se utiliza "lengua natural con terminología especializada y sintaxis rigurosamente controlada" y se utiliza en el ámbito de la tecnología, para este caso las redes de comunicaciones.

C. DELIMITACIÓN TEMÁTICA DEL TRABAJO:

Delimitación del campo conceptual con base en un sistema de clasificación de campos temáticos.

El texto "E*NTERPRISE COMMUNICATION IN NEXT GENERATION CORPORATE NETWORKS (NGCN) INVOLVING PUBLIC NEXT GENERATION NETWORKS (NGN)"* es un informe técnico de Ecma International, una asociación europea dedicada a la estandarización de sistemas de comunicación e información. Ecma desarrolla estándares e informes técnicos para facilitar y estandarizar el uso de la tecnología de la información y la comunicación. En particular, el informe técnico base del presente estudio terminológico presenta una visión general de la comunicación empresarial basada en Protocolos de Internet (IP) desde y hasta Redes Corporativas de Telecomunicaciones. La comunicación empresarial es una de las aplicaciones de las redes de comunicaciones (Laporta, 2005: 142) las cuales son la columna vertebral de la telemática. La telemática trata de todo lo que tiene que ver con la comunicación entre computadores (Laporta, 2005:3), es por eso que el campo temático del presente estudio terminológico es la Telemática y el sub-campo temático, es las Redes de Comunicaciones.

En el presente estudio terminológico se estableció el vocabulario del sub-campo temático de las redes de comunicaciones y se tuvieron en cuenta los diferentes aspectos de las mismas representados en los árboles conceptuales en inglés y español. *(Ver Anexos 1 y 2)*

D. DETERMINACIÓN DE LENGUAS DE TRABAJO Y FORMA DE PRESENTACIÓN FINAL:

Este trabajo terminológico se hizo en dos lenguas: inglés y español. El texto base está escrito en inglés. Se hizo la traducción al español. Se establecieron términos y definiciones en inglés y en español. Además se estableció un glosario bilingüe con las equivalencias en inglés y español. El producto final se publica en soporte electrónico a través de un CD y también en la plataforma TRADUTERM de la Universidad del Valle. La justificación de tal elección, surge de las necesidades de los usuarios potenciales:

- Los materiales de consulta del área de la telemática a los que acceden los profesores, estudiantes y profesionales del área se encuentran en inglés. Los libros, los artículos, los sitios web, etc. hacen sus publicaciones en inglés y algunos pocos en español.

- Los usuarios necesitan manejar la terminología especializada de su campo en inglés y español pues los últimos avances y actualizaciones en el área se publican en inglés por ser la lengua de comunicación internacional. Además, los países donde se desarrollan estos avances, en muchos casos son de habla inglesa.
- Además de las publicaciones y avances en inglés, los usuarios producen en muchos casos artículos, informes, etc. que deben ser publicados en inglés en revistas internacionales. En ocasiones deben preparar ponencias para públicos de habla inglesa o personas que manejan este idioma y si no hacen la presentación completa en inglés, al menos, hay muchos términos que deben manejar en las dos lenguas.
- En general, el idioma que se utiliza para la comunicación entre los especialistas de las áreas relacionadas con la tecnología, es el inglés.
- Actualmente existen múltiples glosarios y diccionarios de términos relacionados con las redes de comunicaciones en inglés, sin embargo en español, la cantidad de materiales terminológicos es muy limitada y la calidad no siempre es la mejor.

E. DECISIONES METODOLÓGICAS:

En esta sección se definió la información que se va a presentar en las fichas terminológicas.

En el Manual de Terminología de la Oficina de Traducciones del Canadá, Pavel y Nolet (2002:10-11), afirman que el formato principal de consignación de los datos en un estudio terminológica es la *ficha terminológica*. La ficha terminológica es un conjunto de campos que debe tener unos elementos mínimos: los campos temáticos a los que pertenece el concepto, las lenguas, los términos, las definiciones del concepto o algún tipo de prueba textual y las fuentes de información. Para el presente estudio terminológico se tuvo en cuenta la propuesta de Pavel y Nolet en el Manual de Terminología y la estructura es la siguiente:

Institución: Universidad del Valle
Ficha Número: *#*
Fecha
Autor
Campo 1: Campo temático, sub-campo temático.
Campo 2: Indicador de lengua
Campo 3: Entrada principal (término)*: categoría gramatical, abreviatura*
Indicador de prueba textual 1: *definición + fuente*
Indicador de prueba textual 2: *contexto + fuente*
Sinónimo
Campo 4: Equivalencia
Campo 5: Sistema Conceptual: *ubicación*
Campo 6: Revisor

FASE 2: PREPARACIÓN DEL TRABAJO

Esta fase es muy importante porque la escogencia apropiada de la documentación en este momento es crucial para lograr que la información que se ofrece a los usuarios sea confiable y pertinente. Además, la selección de un especialista que nos ayude a validar los términos, la traducción y en general el producto final, es necesaria para recibir la orientación que necesitamos al no ser expertos en el tema. Por otro lado, la representación conceptual es vital para establecer el sistema de conceptos inherentes al área. Para realizar el fichero se siguieron las siguientes etapas de manera simultánea:

A. RECOPILACIÓN, SELECCIÓN, REVISIÓN Y CLASIFICACIÓN DE LA DOCUMENTACIÓN RELACIONADA CON EL TEMA

En esta etapa del trabajo se hizo una recopilación de todos los recursos documentales y terminográficos sobre telemática, las redes de comunicaciones y las redes corporativas de forma impresa y en formato electrónico en inglés y en español. La documentación se obtuvo en bibliotecas de la Universidad del Cauca, a través del asesor del trabajo y en la Internet. Esta recopilación incluyó libros, artículos y un diccionario impreso y glosarios, diccionarios y enciclopedias especializadas en línea. En la bibliografía del presente trabajo se encuentra detallada la lista de documentos y recursos tanto físicos como electrónicos utilizados para el desarrollo del estudio terminológico.

B. SELECCIÓN DE ASESOR O ESPECIALISTA

El asesor o especialista colaborador en este trabajo terminológico es el Ingeniero Electrónico con Maestría en Telemática de la Universidad del Cauca, Wilmar Campo. Un ingeniero electrónico con maestría en telemática es el asesor indicado para este trabajo porque su campo de acción son precisamente las telecomunicaciones y ayuda a delimitar el campo y sub-campos temáticos. Además aconseja sobre la documentación que se debe utilizar y facilita material pertinente para la consulta, asesora la selección de términos y los valida.

C. REPRESENTACIÓN CONCEPTUAL

Como se aclara en el marco teórico, para establecer el sistema de conceptos del área temática base del presente estudio terminológico se tuvieron en cuenta las teorías de Arntz y Picht en el libro "Introducción a la terminología" de 1995. Como ya se ha mencionado anteriormente, el área de conocimiento que se estudió es la telemática. Se estableció un sistema conceptual del área teniendo en cuenta los diferentes tipos de relaciones entre los conceptos. Por ejemplo se estableció una relación conceptual jerárquica de abstracción donde la secuencia de conceptos puede ser una serie de abstracción lógica vertical en la que se progresa en sentido descendente. La representación del sistema conceptual se hizo en forma de árbol para darle más claridad y se subdividió ajustándose a la información contenida en el informe técnico base del presente de este estudio y a la documentación. El concepto superordinado es TELEMÁTICA (el todo), cuyo eje central (concepto subordinado) son las REDES DE COMUNICACIONES. Este concepto se dividió utilizando un sólo criterio de ordenación que es el tipo de redes de comunicaciones: RED TELEFÓNICA, RED DE COMPUTADORES y RED TELEGRÁFICA. En esta parte inicial podemos entonces hablar de un sistema monojerárquico. A partir de ahí, se establece el sistema conceptual de uno de los temas que es la RED DE COMPUTADORES concepto central del informe técnico base del presente estudio.

El sistema conceptual del tema de las REDES DE COMPUTADORES se estableció dividiendo este concepto en varios criterios de ordenación en el mismo nivel: CLASIFICACIÓN, ARQUITECTURA, APLICACIONES, TECNOLOGÍA y SEGURIDAD. Dada esta clasificación, se puede decir que a partir de aquí el sistema de conceptos es polijerárquico. Cada concepto subordinado de las REDES DE COMPUTADORES se dividió así: Clasificación de las Redes de Computadores: según su *extensión geográfica*,

su *topología*, la *estructura de funcionamiento*, la *tecnología* y el *propietario*. Arquitectura de las Redes de Computadores: *capas de red*, *servicios* y *protocolos.* Aplicaciones de las Redes de Computadores: *COMUNICACIÓN EMPRESARIAL* y *entornos de usuarios*. Tecnología de las Redes de Computadores: *técnicas*, *conocimientos* y *procesos.* Seguridad de las Redes de Computadores: *prevención*, *detección* y *recuperación*.

Según Arntz y Picht, los sistemas polijerárquicos pueden perder su transparencia debido a la variedad de criterios de ordenación (1995:113), es por eso que para el presente trabajo, a partir de aquí se hizo una subdivisión en sistemas parciales que aparentemente "se separan" del sistema principal (Redes de computadores) para fines de claridad y organización gráfica. Los conceptos subordinados de cada sistema parcial se presentan en el punto b (árbol específico) de la sección de representación conceptual del campo y subcampos temáticos tanto en inglés como en español.

En el sistema conceptual de las Redes de Computadores, se puede establecer que hay una relación ontológica pues hay un todo o concepto incluyente que en este caso viene a ser Redes de Computadores y unos conceptos subordinados (partes) o conceptos específicos parciales. Las relaciones también se establecen en orden descendente, se empieza por el todo y se descompone en sus partes. A partir de aquí, las relaciones se presentaron en forma de lista. *(Ver Anexos 1 y 2)*

FASE 3: GESTIÓN DE LA TERMINOLOGÍA

A. ESTABLECIMIENTO DE LA NOMENCLATURA TERMINOLÓGICA APROPIADA

El proceso de extracción de términos del presente estudio se hizo de manera manual con base en el texto *"Enterprise Communication in Next Generation Corporate Networks (NGCN) involving Public Next Generation Networks (NGN)"*. El corpus o conjunto de textos que sirvió para recoger, comparar y verificar términos y definiciones en inglés incluye otros informes técnicos de ECMA sobre redes corporativas tales como el informe técnico 75 - *Corporate Telecommunication Networks (CN) - Standardization Plan, 2nd edition (June 2000)*, el informe técnico 86 - *Corporate Telecommunication Networks - User Identification in a SIP/QSIG Environment (December 2003)*, el informe técnico 92 - *Corporate Telecommunication Networks – Mobility for Enterprise Communications (December 2005)*, el informe ténico 95 - *Next Generation Corporate Networks (NGCN) - General (June 2008)* y el informe técnico 96 - N*ext Generation Corporate Networks (NGCN) - Identification and Routing (June 2008).* Otras fuentes revisadas y utilizadas para

la extracción y verificación de términos diferentes a los informes técnicos fueron por ejemplo el artículo "*Approach to Next Generation Corporate Networks*" de la revista Fujitsu Science Technology 42,4 de octubre de 2006; la Petición de Comentarios # 3261 "*SIP: Session Initiation Protocol*", por The Internet Society, 2002.

En español, los documentos utilizados para verificar las equivalencias de los términos incluyen el documento "*Estudio Integral de Redes de Nueva Generación y Convergencia*" de la Comisión de Regulación de Telecomunicaciones de la República de Colombia (Junio, 2007); el artículo "*Desarrollo de una Plataforma de VoIP basada en Software Libre*" de André Ríos, Jesús Alcober y Antoni Olle del Departamento de Ingeniería Telemática, Universidad Politécnica de Cataluña, Barcelona, España y el libro Nueva Generación de Redes – Telefonía Sobre IP, de Simon Znaty, ediciones EFORT, 2001.

Otras fuentes de información para la extracción y verificación de términos incluyen los textos sobre telemática, redes de comunicaciones e informática que se encuentran enumerados en la bibliografía del presente trabajo. Todas las fuentes se escogieron porque contienen información sobre uno o varios conceptos que pertenecen al sistema conceptual en estudio útil para la comprensión de los conceptos, confirmación de la terminología en inglés y en español y como fuente de documentación sobre el tema.

También se tuvieron en cuenta glosarios y diccionarios en línea sobre internet, tales como la enciclopedia y centro de aprendizaje sobre tecnologías de la información Whatis?.com cuya página web es: http://whatis.techtarget.com/; la enciclopedia en línea sobre tecnología informática Webopedia en la página web http://www.webopedia.com/TERM/C/circuit_switching.html, entre otros glosarios y diccionarios en línea.

- ✓ *RECONOCIMIENTO DE LOS TÉRMINOS EN EL TEXTO DE PARTIDA*

Para el "proceso de vaciado terminológico" o extracción de términos no se utilizaron sistemas de extracción automática, la selección de términos se hizo de manera manual teniendo en cuenta los criterios definidos por María Teresa Cabré (1993:296) y citados por Rodríguez (2004:77) y mencionados en los puntos 3 y 4 de la sección A de la fase 1 sobre las consideraciones preliminares para el desarrollo de este estudio. Estos son los criterios:

- Frecuencia de aparición en el texto.
- Representación de un concepto reconocido.
- Unidades semánticamente opacas.

- Unidades marcadas tipográficamente.
- Unidades acompañadas de definiciones aparentes.
- Unidades aparentemente no relacionadas con ninguna otra área de especialidad.
- Presencia de estructuras sintagmáticas habituales.
- Unidades de la lengua general con carácter especializado

✓ *DELIMITACIÓN DE LAS UNIDADES TERMINOLÓGICAS*

Con base en tales criterios, se hizo una lista con un total de 202 candidatos a términos que se organizaron por orden alfabético para su posterior análisis. Se hizo un estudio de cada posible término y se fueron descartando como unidades terminológicas por las siguientes razones:

- Imposibilidad de encontrar información sobre tal término que permitiera determinar si representaba un concepto, por ejemplo: *Non-IP-based interoperation, bearer streams, SIP body;* o información en fuentes poco confiables: UDP traffic: http://forums.macrumors.com/showthread.php?t=183096.
- Pertenencia a la lengua general como por ejemplo: *charging, performance monitoring, session policy, emergency call, etc.*
- Necesidad de dividir segmentos: *IP address spaces* (término: IP address), end-to-end IP-based Communication (términos: end-to-end; IP-based Communication) o segmentos incompletos: redirect, en el texto aparece "redirect" pero en la documentación se encuentra "redirect server".
- Siglas que resultaban ser unidades que ya se habían definido como términos: *SRTCP=Secure Real Time Control Protocol*; *STUN=Simple Traversal of UDP through NATs.*

✓ DEFINICIÓN DE UNIDADES DE CONOCIMIENTO ESPECIALIZADO (UCE)

Según Cabré y Estopa, las unidades de conocimiento especializado son las unidades de distinto nivel descriptivo que constituyen los nudos de conocimiento de un texto o forman parte de ellos y que pueden clasificarse por diferentes criterios. En los textos consultados para extraer los términos y en particular en el texto del informe técnico de ECMA hay unidades de conocimiento especializado que se pueden clasificar así:

- Según el sistema al que pertenecen: unidades de conocimiento especializado que pertenecen al lenguaje natural y a sistemas artificiales. Algunos ejemplos de unidades pertenecientes al lenguaje natural son: *call center, certification authority, eavesdropping, file transfer, hop*, entre otros. Hay también una gran

cantidad de unidades pertenecientes a sistemas artificiales representadas en siglas, acrónimos, etc. por ejemplo: *B2BUA (Back-to-back User Agent), Centrex, codec, ENUM, H.323, IPSEC, Multimedia Internet KEYing (MIKEY),* etc. Cabe resaltar que en el texto se presentan muchas siglas y acrónimos, lo cual es característico de los textos especializados en los que por economía del lenguaje, se tiende a reducir expresiones largas y con el tiempo se adoptan como siglas o acrónimos.

- Según su estructura: hay una variedad de unidades con diferentes tipos de estructuras, por ejemplo las unidades morfológicas (que pueden coincidir con morfemas) con sufijos: *-ing: bridging, call logging, circuit switching; -ation: application, authentication; - ment: equipment, agreement, establishment; -ity: authority, security, quality*; con prefijos: *extra-: extranet, infra-: infraestructure; inter-: interface; intra-: intranet*, etc. Otro ejemplo son las unidades monoléxicas: simples: *decryption*, compuestas: *endpoint*, *firewall*, *gateway*, *packet*-based; derivadas: *registrar*, *tunneling*. Por otra lado, hay ejemplos de unidades con sintagmas terminológicos o fraseológicos: *circuit-switched network, customer premises equipment, denial of service attack, integrity checking* y unidades oracionales: *Simple Traversal of UDP through NATs*.
- Según su categoría gramatical: en los textos base del presente estudio y en particular en el informe técnico 91 de ECMA, la mayoría de las unidades de conocimiento especializadas son de carácter nominal: *encryption, firewall, gateway, integrity checking, Internet protocol, IP centrex*; hay algunas de carácter adjetival: *end-to-end, keep-alive*; algunas de carácter verbal: *add value, collocate, traverse* y muy pocas de carácter adverbial: *cryptographically*.
- Según la clase conceptual: hay unidades que expresan entidades: *gateway, proxy, network*, etc.; eventos (acciones o procesos): *authentication, signalling, decryption, denial of service attack*, etc.; y propiedades: *routable, scalable, integrity checked, authenticated*, etc.

✓ ELABORACIÓN DE DEFINICIONES

Después de delimitar las unidades terminológicas y determinar las unidades de conocimiento especializado se procedió a buscar las definiciones de los términos escogidos. Estas definiciones se encontraron en algunos de los libros consultados, los informes técnicos de ECMA y en particular glosarios y diccionarios en línea sobre tecnologías de la información tanto en inglés como en español.

Las definiciones se escogieron tratando al máximo que cumplieran con los requisitos de una buena definición como los descritos por Rodríguez (2004:175): claridad, adecuación y concisión. Ejemplos:

Decryption: *Any procedure used in cryptography to convert ciphertext (encrypted data) into plaintext*.

http://www.computer-dictionary-online.org/decryption.htm?q=decryption

Central telefónica privada: *conmutador de un teléfono analógico o digital ubicado en las instalaciones del suscriptor y que se usa para conectar redes telefónicas privadas y públicas.*

http://www.ciscoredaccionvirtual.com/redaccion/glosario/default.asp?letra=P

B. PROCESAMIENTO TERMINOGRÁFICO DE LOS DATOS

Como se mencionó en el punto E de la Fase A sobre las decisiones metodológicas para el trabajo terminográfico, para elaborar las fichas terminológicas se tuvo en cuenta la propuesta de Pavel y Nolet en su Manual de Terminología (2002). El modelo de ficha tiene en cuenta datos administrativos, terminológicos y conceptuales de cada entrada.

- **Datos Administrativos**: institución, número de codificación, autor de la ficha, fecha, supervisor o revisor.
- **Datos Terminológicos**: idioma, entrada, categoría gramatical, definición y fuente, contexto auténtico y fuente y equivalencia en otra lengua. Para algunos de los términos también se han incluido sinónimos.
- **Datos Conceptuales**: posición del término en el sistema conceptual del área a la que pertenece.

Este es un ejemplo de una ficha terminológica en la que se encuentran los datos e información sobre cada término del presente estudio diseñada con base en la documentación.

Español:

Universidad del Valle
1

Autor: Alexandra Delgado
Fecha: 18/11/2010
Campo Temático: Telemática
Sub-campo temático: Entidades SIP
Idioma: Español
Entrada: AGENTE DE USUARIO n.

DEFINICIÓN:
Es una aplicación con arquitectura cliente/servidor que se utiliza para iniciar y terminar las sesiones.
Fuente:
http://www.grc.upv.es/docencia/tdm/trabajos2007/Abel_H.323%20vs%20SIP%20(1).pdf

CONTEXTO:
Una de las funciones de los servidores SIP es la localización de los usuarios y resolución de nombres. Normalmente, el **agente de usuario** no conoce la dirección IP del destinatario de la llamada, sino su e-mail.
Fuente:
http://www.voipforo.com/SIP/SIPdireccionamiento.php

Inglés: USER AGENT (UA)

Supervisor: Wilmar Campo – Magíster en Telemática – Universidad del Cauca

Inglés:

Universidad del Valle
114

Author: Alexandra Delgado
Date: 18/11/2010
Subject Fields: Information and Communications Technology (ICT)
SIP Entities
Language: English
Entry: USER AGENT UA n.

DEFINITION:
A logical entity that can act as both a user agent client and user agent server.
Source:
http://www.faqs.org/rfcs/rfc3261.html

CONTEXT:
Along with its basic functionality, a fully implemented **User Agent (UA)** can provide extra services to the user. Some of these are provided with the assistance of X.400. For example a UA may flag messages in its storage made obsolete by the reception of a more recent message by using the "obsoleting indication" service element.
Source:
http://ntrg.cs.tcd.ie/undergrad/4ba2/x400/ua.html

Spanish: AGENTE DE USUARIO UA

Supervisor: Wilmar Campo – MSc – Information and Communication Technology – Universidad del Cauca

C. ELABORACIÓN DE UN GLOSARIO BILINGÜE:

En el presente trabajo, después de todo el proceso de selección de términos, descripción de definiciones y elaboración de fichas, se procedió a elaborar un glosario bilingüe con los términos en inglés y en español en orden alfabético con el fin de facilitar la consulta de los interesados. *(Ver Anexos 3 y 4).*

FASE 4: REVISIÓN

En esta fase, el asesor especialista Magister en telemática hizo la revisión de los árboles conceptuales, los glosarios y las fichas en inglés y español e hizo diferentes sugerencias al respecto lo que generó cambios en terminología y representación conceptual. Por ejemplo:

En cuanto a terminología:

- ✓ La sugerencia más importante fue el cambio de la traducción de la palabra NEXT en el término Next Generation Networks que según la literatura se traduce como NUEVA, por sugerencia del asesor se cambió a PRÓXIMA porque según los líderes mundiales en las temáticas, esa es la palabra correcta aun cuando en la literatura la traducción sea NUEVA.
- ✓ La traducción de la palabra MEDIA como SERVICIOS MULTIMEDIA o CONTENIDOS MULTIMEDIA en lugar de MEDIOS como había sido la propuesta de equivalente de la autora del presente estudio.
- ✓ Algunas palabras que han sido incorporados como préstamos del inglés y por consiguiente no se traducen al español. Ejemplos: firewall, streams, interworking, entre otros.

En cuanto a la representación conceptual:

- ✓ El asesor hizo la sugerencia de modificar las representaciones conceptuales tanto en inglés como español en la sección de tipos de redes según su tecnología porque estas redes son redes telefónicas y no de computadores como estaban en la primera versión de la representación conceptual tanto en inglés como en español.

FASE 5: PRESENTACIÓN FINAL

A. Almacenamiento Electrónico

La base de datos terminológica producto final del presente trabajo contiene 121 fichas terminológicas y se presentará en soporte electrónico utilizando un documento HTML que facilita la navegación por medio de vínculos que llevan a las fichas terminológicas y representaciones conceptuales tanto en inglés como en español. La base de datos se presenta en el CD que acompañará el documento definitivo.

B. Presentación del Texto Traducido

La traducción del texto objeto del presente estudio, el informe técnico de ECMA: *"Enterprise Communication in Next Generation Corporate Networks (NGCN) involving Public Next Generation Networks (NGN)"* se hizo a lo largo del trabajo terminográfico en tres diferentes etapas según se expone en el siguiente capítulo del presente trabajo.

FASE 6: CONTROL PERMANENTE DEL PROCESO

El trabajo terminográfico se ha evaluado constantemente y se han hecho cambios y actualizaciones en las representaciones conceptuales, las definiciones, contextos y equivalencias porque se encontraron algunas incongruencias entre los términos y las equivalencias. Se han hecho varias revisiones a la traducción del texto objeto de estudio y a los glosarios bilingües en inglés y español.

III. TRADUCCIÓN AL ESPAÑOL DEL TEXTO: *"ENTERPRISE COMMUNICATION IN NEXT GENERATION CORPORATE NETWORKS (NGCN) INVOLVING PUBLIC NEXT GENERATION NETWORKS (NGN)"*

La traducción del texto objeto del presente estudio se hizo en tres etapas según la propuesta de Delisle (1985:95) citado en Rodríguez (2004:28).

A. ETAPAS DE LA TRADUCCIÓN DEL TEXTO OBJETO

1. COMPRENSIÓN: antes de comenzar la traducción de una lengua a otra, hay que comprender el texto original. Para esto, no sólo es necesario el conocimiento lingüístico, sino que también hace falta tener conocimientos extralingüísticos el cual depende en gran medida del saber general y la experiencia del traductor. Todo esto es imprescindible para evitar la posible ambigüedad que pueda surgir en la traducción.

Es así que en esta etapa de la traducción, se hizo una primera lectura del texto, la revisión de la bibliografía y la lectura de los textos paralelos, entre los cuales se encuentran los mencionados en la sección: Recursos Documentales y Terminográficos Sobre Telemática, las Redes De Comunicaciones y las Redes Corporativas, en la fase 2 de la metodología del trabajo terminográfico en el presente documento. Fue necesario acceder a múltiples recursos documentales dado el limitado conocimiento de la autora sobre el área de la telemática. En esta etapa de comprensión también se hizo el análisis textual que se describe en la sección B de este capítulo.

2. DESVERBALIZACIÓN: en esta segunda etapa, una vez entendido el texto original, se recuerda tan sólo el sentido (Hurtado, 2001), es decir, las ideas dejando a un lado las palabras con las que éstas han sido transmitidas para empezar una reformulación mental. Ésta es una etapa clave, puesto que ayuda a comprender el texto original olvidando las palabras empleadas en él, lo que permite al traductor llevar a cabo la siguiente etapa del proceso con mayor libertad y sin caer en la literalidad.

Esta etapa se llevó a cabo prestando mucha atención a no caer en la literalidad y para eso la autora se apoyó en los recursos documentales y en la orientación del especialista colaborador en este trabajo.

3. REFORMULACIÓN: en esta etapa, el traductor reformula en la lengua meta esas mismas ideas que ha hecho suyas en el paso anterior. Para esto, hay que valerse tanto

los recursos que le ofrece la lengua de llegada, como de los recursos propios (intuición, imaginación y creatividad).

En esta etapa se hizo el primer borrador de la traducción valiéndose de los recursos documentales y teniendo en cuenta las exigencias terminológicas y de estilo de este tipo de texto tales como:

- La equivalencia de los términos en la lengua de llegada.
- La estructura de la lengua de partida y de llegada, en particular, el uso de la voz pasiva predominante en el texto fuente.
- El uso de abreviaturas y acrónimos muy común en el texto fuente y su traducción o equivalencia correcta en la traducción.
- La traducción de las 13 figuras del texto.

En la sección del análisis textual del texto traducido se presentan ejemplos de algunos de los problemas de traducción que se presentaron y de algunas técnicas de traducción empleadas a lo largo del proceso de traducción.

Como parte importante en la traducción del texto, se llevo a cabo una etapa de revisión del texto traducido. Esta etapa se llevó a cabo a lo largo y al final de todo el proceso. Hubo varias revisiones por parte de la autora del presente trabajo y una revisión final del asesor especialista quien hizo diversas recomendaciones en particular en cuanto a la terminología y el uso de las siglas, abreviaturas y acrónimos. Algunos ejemplos son:

- ✓ La importancia de conservar algunas siglas y términos en inglés en las versiones en español porque los especialistas están familiarizados con esos términos y no con traducciones o adaptaciones de los mismos que resultan poco naturales y que no expresan los conceptos con claridad y precisión. Ejemplos: firewall, B2BUA, etc.
- ✓ La palabra Internet es género femenino porque es la red de redes, por lo tanto debe hablarse de la Internet.

Según la apreciación del especialista, el texto traducido es de muy buena calidad porque se transmiten los conceptos de manera fiel al texto original a pesar de la complejidad del mismo y del conocimiento básico de la traductora sobre estos temas. Después de diversas correcciones de la equivalencia de conceptos, del estilo y la

presentación, se obtuvo una versión final del texto traducido que se encuentra en la sección de anexos. *(Ver Anexo 6)*

B. ANÁLISIS TEXTUAL DEL INFORME TÉCNICO: *"Enterprise Communication in Next Generation Corporate Networks (NGCN) involving Public Next Generation Networks (NGN)".*

El análisis textual es el punto de partida que constituye el requisito para la comprensión cabal del texto fuente. Es un análisis relevante para la traducción porque además de permitir una comprensión cabal del texto fuente, proporciona una base sólida para la toma de decisiones del traductor en la tarea de traducción.

Para el análisis textual del informe técnico de ECMA objeto del presente estudio, se tuvo en cuenta el *Enfoque Textual* propuesto por Hatim & Mason (1990). Estos autores conciben la traducción como un acto de comunicación que no puede ser considerado aisladamente sino como parte de la vida social (Hurtado, 2001:542). Para esto, los autores plantean tres dimensiones que permiten analizar el sentido en el que se transmite el texto: dimensión comunicativa, pragmática y semiótica.

1. DIMENSIÓN COMUNICATIVA: se refiere a la variación lingüística según el uso y los usuarios.

a. Situación Discursiva: el texto base del presente estudio es un informe técnico establecido por consenso, aprobado y publicado por ECMA en diciembre de 2005 y adoptado por ETSI e ISO en 2006. Este informe técnico está dirigido fundamentalmente a los mercados europeos de fabricantes de computadores pero tiene alcance global.

b. Campo: variación lingüística según la actividad profesional**.** Para delimitar el campo temático se tuvo en cuenta la clasificación temática de la Agencia Nacional de Evaluación y Prospectiva del Ministerio de Ciencia e Innovación de España que se basa en la Nomenclatura Internacional de la UNESCO para los campos de Ciencia y Tecnología. Esta es la clasificación:

ÁREA: Matemáticas y tecnología de la información y las comunicaciones.
SUBAREA: Tecnología electrónica y de las comunicaciones.
DISCIPLINA: Telecomunicaciones.
ÁREA DE CONOCIMIENTO: Ingeniería telemática.

c. Objetivo de la comunicación: el objetivo de los informes técnicos de ECMA es facilitar y estandarizar el uso de las Tecnologías de la Información y la Comunicación y motivar el uso correcto de los estándares influenciando el medio en que se aplican. El informe técnico base del presente estudio busca presentar una serie de requisitos que las Redes de Nueva Generación NGN deben cumplir para dar soporte a las comunicaciones que involucran Redes Corporativas de Nueva Generación en diferentes escenarios de interconexión.

d. Medio o canal en que se publica: los informes técnicos de ECMA son documentos formales preparados por el Comité Técnico de ECMA y aprobados por la Asamblea General de ECMA. Estos documentos se encuentran disponibles para todas las personas u organizaciones interesadas sin costo alguno en forma impresa y en formato electrónico (PDF). Se pueden descargar de la página web de ECMA: www.ecma-international.org o se puede solicitar el envío a través de la misma página web.

e. Lugar y tiempo de la comunicación: la sede de ECMA se encuentra en Ginebra, Suiza. Desde esta sede se publican los informes técnicos dos veces al año. El informe técnico base del presente estudio fue publicado en Ginebra en diciembre de 2005.

f. Nivel de Lengua: el texto base del presente estudio tiene una función expositiva, instructiva y también algunos aspectos narrativos. Con base en estas funciones del texto y por el tipo de texto (informe técnico) podemos afirmar que la comunicación en este es especializada. (Hurtado, 2001:501). La comunicación especializada se caracteriza por que los emisores son investigadores, especialistas o técnicos, los receptores suelen ser investigadores, especialistas y/o estudiantes de nivel especializado (Rodríguez, 2004:93). El informe técnico de ECMA fue escrito y aprobado por especialistas en el área de las telecomunicaciones y está dirigido a técnicos y/o especialistas fabricantes de computadores. El nivel de lengua del informe técnico es alto, hay terminología especializada y sintaxis controlada. (Clasificación los Lenguajes Especializados de Hoffman, citado en Rodríguez, 2004:96). El informe técnico de ECMA está escrito en inglés británico.

g. Tono: El tono característico de la comunicación especializada es formal porque está dirigida a especialistas, por ende, el tono del informe técnico de ECMA es formal. Un texto escrito con un tono formal se caracteriza primero que todo por el léxico especializado, la terminología que manejan los especialistas en la materia. El informe técnico de ECMA se caracteriza por la especificidad en el léxico, esta terminología es

precisa y propia del área de las telecomunicaciones. En cuanto a la sintaxis, el informe técnico se caracteriza por el empleo de estructuras fijas y concisas (uso de siglas y acrónimos: NGCN, VPN, B2BUA; frases cortas: "*The most basic level of service provision is IP connectivity*", "*In principle, SIP can operate directly between two UAs*"; formas pasivas: "Services provided by an NGN may need to be managed from an NGCN.", "*Firewalls can normally be expected to be configured to allow SIP signalling to pass through.*"), estilo impersonal (no se usan los pronombres personales I, we, etc.)

2. DIMENSIÓN PRAGMÁTICA: se refiere a la intención del emisor y a la función del texto.

a. Intención del autor: ECMA International está dividida en comités técnicos, entre ellos el Comité Técnico 32, encargado de todo lo relacionado con las Comunicaciones Empresariales. A su vez este comité está dividido en grupos de tareas encargados de desarrollar informes técnicos y estándares sobre comunicaciones empresariales, este grupo de tareas, llamado TG-17 *IP-based Multimedia Business Communications,* es el autor del informe técnico 91, base del presente estudio. En términos generales, el grupo de tareas 17, con sus informes técnicos y estándares, pretende identificar los requisitos para la comunicación multimedia basada en protocolos de Internet en un medio de redes empresariales incluyendo aspectos de la arquitectura, movilidad, servicio, protocolos, calidad de servicio, seguridad, administración, entre otros. Más específicamente, con el informe técnico: "*"Enterprise Communication in Next Generation Corporate Networks (NGCN) involving Public Next Generation Networks (NGN)",* el grupo de tareas 17 busca en primer lugar, describir las características de los diferentes escenarios de interconexión entre Redes Corporativas de Nueva Generación y NGNs. En segundo lugar, expone los requisitos que las NGNs deben cumplir para dar soporte a las comunicaciones que involucran Redes Corporativas de Nueva Generación en los escenarios descritos. Finalmente, identifica los aspectos técnicos necesarios para llevar a cabo las configuraciones descritas (escenarios) y expone requisitos adicionales para la comunicación entre Redes Corporativas de Nueva Generación y NGNs. La intención es entonces, describir situaciones (escenarios de interconexión) y presentar informaciones para realizar tareas (requisitos y aspectos técnicos necesarios) con el fin de regular o estandarizar la comunicación empresarial a través de redes corporativas y NGNs.

b. Tipo de texto y función: El informe técnico de ECMA puede clasificarse como un texto con función expositiva. Según varios autores, un texto expositivo se caracteriza

porque presenta análisis y síntesis de ideas y conceptos. El informe técnico de ECMA presenta el análisis de casos de uso clave para la comunicación con o entre Redes Corporativas de Nueva Generación y con base en este análisis identifica los requisitos que deberán cumplirse para que se de la comunicación entre estas redes. Estos requisitos se dan a lo largo del texto y en diferentes aspectos relacionados con la interoperación de las Redes Corporativas de Nueva Generación y de las NGNs, el discurso también es instructivo en gran parte del texto, este informe técnico pretende, además de hacer un análisis de casos de uso y presentar unos resultados, hacer recomendaciones a los lectores sobre las NGNs. Por ende, el texto es también de tipo instructivo, es decir tiene una función apelativa porque presenta información para realizar unas tareas y busca que los lectores adopten las premisas expuestas (recomendaciones). El texto también tiene características de un texto narrativo en la sección de antecedentes donde se presenta un resumen de la evolución de las redes desde sus inicios hasta las próximas etapas de evolución.

La función expositiva del texto, se refleja en que se usan oraciones enunciativas, se utiliza la tercera persona, el registro es formal porque hay gran cantidad de términos técnicos y no se utilizan expresiones subjetivas. En cuanto a la función instructiva, el texto presenta el uso del verbo modal ***shall+verbo***, lo cual indica que se hará algo en el futuro o puede indicar también un comando o instrucción.

c. Expectativas del receptor: los estándares e informes técnicos desarrollados por Ecma están dirigidos principalmente a los mercados europeos de fabricantes, programadores y usuarios de hardware y software, sin embargo, tienen alcance global y cualquier persona u organización interesada puede acceder a estos documentos sin ningún tipo de restricción. Algunos de los usuarios de los estándares e informes técnicos de ECMA son: Canon, Hewlet Packard, IBM, Intel, Microsoft, Samsung, Sony, Yahoo, Google, entre otros. Ecma es una organización que cuenta con amplio prestigio entre todos los fabricantes de software y hardware en el mundo, por ende, los usuarios de los informes técnicos y estándares de ECMA, esperan obtener un documento que les sirva de referencia de calidad, con una serie de lineamientos técnicos detallados, destinados a establecer uniformidad en el desarrollo de software o hardware, es decir, un punto de partida para el desarrollo de servicios, aplicaciones, protocolos, etc. En el caso particular del informe técnico base del presente estudio, los usuarios esperan obtener unos lineamientos a seguir en cuanto a los requisitos que las Redes de Nueva Generación NGN deben cumplir para dar soporte a las comunicaciones que involucran Redes Corporativas de Nueva Generación en diferentes escenarios de interconexión.

d. Estructuración Temática

***Superestructura*:** estructura global que caracteriza el tipo de texto, es independiente del contenido y se refiere más generalmente a la forma del texto. (Huerta & García, 2007). Un informe técnico consta generalmente de partes principales y capítulos secundarios. Las partes constituyen las macro unidades temáticas formadas por uno o más contenidos relacionados, por ejemplo: la introducción, la investigación y las conclusiones. Los capítulos son contenidos temáticos que se agotan en su desarrollo. Los capítulos a su vez pueden contener sub capítulos que desarrollan los elementos más específicos.

En el informe técnico de Ecma, se distinguen claramente las macro unidades temáticas y los capítulos:

1. Introducción:

- **a.** Introducción
- **b.** Alcance
- **c.** Referencias
- **d.** Definiciones
- **e.** Abreviaturas
- **f.** Antecedentes

2. Investigación:
Configuraciones básicas y requisitos generales.

3. Conclusiones:
Aspectos técnicos y requisitos de una NGN en relación con la Provisión de Servicios de Sesión.
Macroestructura: contenido general o global de un texto, se refiere al sentido del mismo como un todo y se conforma a través de proposiciones completas llamadas macroproposiciones. (Huerta & García, 2007)

1. **Título:** *"Enterprise Communication in Next Generation Corporate Networks (NGCN) involving Public Next Generation Networks (NGN)"*. (Resumen)

2. **Introducción:** el informe técnico empieza con una introducción corta que explica de que se trata y en que se basan los resultados que se presentan. (Resumen)

3. **Alcance**: explica qué aspectos relacionados con la comunicación con o entre Redes Corporativas de Nueva Generación se incluyen en el informe y cuáles no. (Resumen)

4. **Referencias:** presenta una lista de otros informes técnicos de ECMA relacionados y de otros documentos llamados "Peticiones de Comentarios" (*Request for comments*) de organizaciones como UIT-T y IETF. (Sucesos previos)

5. **Definiciones**: presenta las definiciones que aplican para el informe técnico. (Aclaraciones)

6. **Abreviaturas:** presenta las abreviaturas de los términos más utilizados a lo largo del informe. (Aclaraciones)

7. **Antecedentes**: presenta un resumen de las etapas de evolución de las telecomunicaciones empresariales. (Sucesos previos, actuales y futuros)

8. **Configuraciones Básicas y Requisitos Generales:** esta sección enumera configuraciones importantes aplicables a una Red Corporativa de Nueva Generación y especifica los requisitos generales de una NGN. (Colección, Descripción y Explicación)

9. **Aspectos técnicos y requisitos de una NGN en relación con la Provisión de Servicios de Sesión:** esta sección estudia los aspectos técnicos necesarios para llevar a cabo las configuraciones que se identifican en la sección 6. (Descripción, Explicación y Conclusión)

El informe técnico de ECMA cumple con las cualidades generales de los textos técnicos pues se caracteriza por su objetividad porque describe hechos y datos antes que opiniones o valoraciones subjetivas de los autores, por su claridad al no expresar sobreentendidos, precisión pues evita la terminología ambigua y se emplean términos unívocos, el tema puede ser comprendido por cualquier miembro del grupo de especialistas a quienes va dirigido por su terminología específica del campo temático.

Microestructura: el nivel de base del texto concreto y se refiere más que nada a las relaciones de coherencia y cohesión que se establecen entre las unidades que forman parte de un texto. (A nivel de oración). (Huerta & García, 2007)

- **Léxico:** como ya se mencionó antes, el informe técnico de ECMA maneja un lenguaje especializado pues fue por creado por especialistas y para especialistas. El rasgo característico de los textos especializados de este tipo es el uso de un léxico técnico específico del campo temático que en este caso es la telemática, concretamente las redes corporativas de nueva generación.

Características del léxico:

- Se puede decir que gran parte del léxico utilizado es monosémico porque su significado es fijo independientemente del contexto, es decir, los términos no están aparentemente relacionados con ninguna otra área de especialidad, por ejemplo: B2BUA, VoIP, Session Border Controller, SIP Trapezoid, entre otros.

- El uso de acrónimos y siglas es muy frecuente en el texto, en cada párrafo hay al menos una sigla o acrónimo que en su mayoría fue definido en la introducción del informe en la sección de abreviaturas. Algunos ejemplos son: SDP, ALG, UA, STUN, IETF, NAT, IPSEC, SIPS URI, etc.

- También se usan algunas palabras del lenguaje general pero que tienen un significado preciso en el área de la telemática: black list, eavesdropping, gateway, hop, packet, etc.

- Hay repetición de palabras y expresiones tales como NGN, NGCN, SIP, IP, ISDN, signalling, entre otros.

- **Redes léxicas:**

Network: Next Generation Network, Telecommunication Network, Home Network, Virtual Private Network, Network Address Translator, Customer Premises Network, Packet Based Public Network, Public Carrier Network, Integrated Services Digital Network, Circuit-Switched Network, IP Based Network, Enterprise Network, Network Operator, Network Borders.

Protocol: Session Initiation Protocol, User Datagram Protocol, Internet Protocol, Application Protocol Interface, Real Time Protocol, Session Description Protocol,

Transmission Control Protocol, signalling protocol, Message Session Relay Protocol, general purpose security protocol, key management protocol.

Signalling: Signalling Architecture, SIP Signalling, Signalling Security, signalling protocol, tunnel control signalling, Application Signalling, VoIP signalling, signalling path, secured end-to-end signalling, signalling communication.

Session: Session Service Provider, Session Service Provision, Session Policy, multimedia session, Session Border Controller, session establishment, communication sessions, session keys, session capabilities.

User: User Agent, User Agent Client, User Agent Server, User Datagram Protocol, IP-based user, residential user, legacy user, NGCN user, SOHO user.

IP: IP-based enterprise communication, Non-IP-based interoperation, IP Centrex, IP-based communications solutions, IP connectivity, IP security, IP-based intranet, IP-PBX, IP-based transmission o f multimedia, IP-technology, IP-based network, IP-based user, IP address, non-tunelled IP.

Enterprise: enterprise communication, enterprise network, enterprise telecommunication network, enterprise-specific next generation corporate network, virtual enterprise network, circuit-switched enterprise network, intra-enterprise traffic, enterprise Emergency Call Center.

Packet: Packet-based multimedia communications systems, packet-based public network, packet rate, outbound packet, inbound packet, keep-alive packet, media packet.

- **Colocaciones:**

Add value, establish a session, provision of services, open a binding, make use of, take an approach, incoming traffic, acceptable solution, outside the scope of, technical difficulties, find a solution to a problem, end user, collect information, carry out a denial of service attack, emergency call, feasible solution.

- **Clases de Oraciones Características en Textos Especializados**

Oraciones Impersonales:

There has been a major evolution in enterprise telecommunications during the last few years…

…there was potential for providing telephony…

…there are other technical issues that may need further consideration…

…there is a lot of interest at present in peer-to-peer (P2P) SIP…

…There should generally be no need for more SIP intermediaries than…

…it is likely that a NAT will exist at the boundary between an NGCN and the NGN…

Voz Pasiva:

It is expected that enterprise networks…

It is considered an unlikely transport protocol…

These value added public IP-based networks are collectively known as Next Generation Networks (NGN)…

General requirements on NGN are specified in 6.6…

The issues are discussed with particular reference…

…where SIP intermediaries are eliminated…

…these are believed to be quite uncommon…

…port numbers are chosen dynamically…

- ***Nominalización***

The handling of a SIP request: handle –handling

NAT traversal: traverse-traversal

The opening of firewall holes by sending initial packets from inside the firewall to outside the firewall will help: open-opening

Reliable identification is crucial to the filtering of unwanted requests: filter-filtering

Provision of identification information will depend on privacy requirements: provide-provision

Security is a major consideration for the deployment of any application on an IP network: deploy-deployment

This information needs to be protected against eavesdropping: eavesdrop-eavesdropping

Key management will be between the UAs with no impact on the NGN: manage-management

- **Repetición:**

A lo largo del texto hay repetición constante de términos y estructuras que expresan la temática de la comunicación entre redes corporativas:
Algunos ejemplos de términos que se repiten:
Corporate Network, NGN, Internet Protocol (IP), SIP, Signalling, proxy, communication, etc.
Algunos ejemplos de estructuras que se repiten:
Sujeto+shall+verbo+complemento: An NGN shall offer service level agreements…
To be+Participio: is assumed, is known, is mentioned, is required, is dealt with, are incurred, are discussed.

- **Referencias:**

This, these, those, his, they.

- **Conectores:**

De tiempo: At present,
De contraste: However, Although, Alternatively, Yet, Otherwise, whereas
De posterioridad: In principle, First, Secondly
De adición: In addition, Furthermore

- **Uso de verbos:**

Uso frecuente de ***shall+verbo*** *para indicar norma:*
An NGN shall support… AN NGN shall allow… An NGN shall not intervene… An NGN shall be able to pass…

Uso de ***must+verbo*** *para indicar obligación:*
The connection must be established in the outbound direction… An initial packet must be sent outbound to open the binding… The NGCN SIP intermediary must therefore have a globally routable IP address… This implies that a UA must accept a certificate from the intervening entity…

Uso de ***may+verbo*** *para expresar posibilidad:*
An NGN may provide services to NGCNs and NGCN users at a number of different levels.
Enterprise customers may use different NGNs for different levels of service provision.
Tunnel control may be directly between the NGCN(s).
The UAs may make use of policy servers…

*Uso de **will+verb** para expresar futuro:*
These requirements will apply in different ways to some or all of the scenarios…
The TE will incorporate a UA that communicates with an inbound / outbound proxy…
Media as well as SIP signalling will flow through the tunnel.
Firewalls will generally exist at the edge of each NGCN, protecting the NGCN from the NGN.

Tiempos verbales:

Condicional:

A SIP intermediary that obeys all the rules of a proxy would be compliant with this.
Otherwise unsolicited SIP requests would be unable to reach the NGCN SIP intermediary.
A preferable solution would be for each UA to use a policy server to open holes.
The opening of holes by a SIP intermediary in the NGN would be subject to the difficulties described in 7.3.
The use of an NGN policy server by each UA would be preferable.
If there is no SIP intermediary in the NGN, an NGCN could provide an asserted identity to the other NGCN.
The NGCN proxy may be unable to determine the location of the TE and therefore it would be the responsibility of the TE to supply its location.
Holes could be opened by the SIP intermediary in the NGCN concerned, but this is subject to the difficulties described in 7.3.

Presente Simple

This Technical Report identifies key use cases for communication…
A third level of service provision is at the application level.
Basically SIP is a protocol that operates between two endpoints known as User Agents (UAs)…
The handling of a SIP request from one UA (the UA client, UAC) to another UA (the UA server, UAS) typically passes through a proxy, which queries the location service in order to locate UAs…
A NAT provides several benefits to the network concerned…

Presente Continuo

Some service providers are planning to offer public IP-based networks…

Presente Perfecto

Several regulatory authorities, e.g. in the USA and in Europe, have started consultations on a regulatory framework for the provision of public VoIP-services.

The market has found the need for an entity known as a Back-to-Back User Agent (B2BUA).

Pasado Simple

Those CNs primarily delivered a voice or telephony service to their users…
Enterprises saw advantages such as savings on infrastructure costs…

Gerundios

Using, including, accessing, involving, transmitting, interworking, etc.
Como adjetivos: Interoperating, following, emerging, cooperating, etc.
Como sustantivos: provisioning, savings, messaging, routing, transcoding, etc.

Problemas de traducción:

A lo largo del texto y por ser una temática sobre la cual la autora no tiene un conocimiento amplio, se presentaron ciertos problemas de traducción, estos son algunos ejemplos:

For most situations in which the medium is transported over UDP*…:* esta oración representó un problema porque en ella se utiliza la palabra *medium* en lugar de *media*. Según el especialista colaborador en el presente estudio esta oración no es coherente aunque la traducción es correcta *(En la mayoría de las situaciones en que el medio se transporta sobre el Protocolo de Datagramas de Usuario (UDP)…),* la versión del texto en inglés tiene un error y lo que se quiso decir no fue *medium* sino *media* que se refiere a contenido multimedia en este caso, entonces la oración correcta sería: *…. en la mayoría de las situaciones en que los contenidos multimedia se transportan sobre el Protocolo …*, ya que los medios no se transportan sino los contenidos.

Media: este término representó un problema para la traducción porque se encontraron varios significaciones y equivalentes que podrían aplicarse al contexto de las redes de comunicaciones, por ejemplo, según el especialista colaborador, en inglés, este término puede referirse a los servicios multimedia o al contenido multimedia, a lo largo del texto fue necesario ser muy cuidadosos con la escogencia de una u otra equivalencia porque según el contexto podría aplicar la una o la otra. Por ejemplo:

- ✓ Texto original. *Media as well as SIP signalling will flow through the tunnel.*
  Traducción: *Los contenidos multimedia al igual que la señalización SIP circularán a través del túnel.*
- ✓ Texto Original*: With the advent of technologies for transmitting voice and other real-time media over the Internet Protocol (IP)…*

Traducción: *Con la llegada de las tecnologías para la transmisión de voz y otros servicios multimedia en tiempo real sobre el Protocolo de Internet (IP)…*

Durante la traducción se encontraron otros problemas en el plano léxico que se presentaron dada la dificultad para encontrar equivalentes en español. En algunos casos se encontraron definiciones en inglés pero no equivalentes en español, el especialista asesor ayudó en la solución de este problema proporcionando propuestas de traducción que fueran validadas según la literatura existente en el área. Estos son los términos:
Bearer streams: según el asesor, éste término no se traduce, pero si fuera necesario, se puede traducir como*:* portador de flujos*.*
End-to-middle security: seguridad extremo a medio
Session Policy: política de sesión
Session Service Provider: proveedor de servicios de sesión
SIP body: cuerpo del mensaje SIP

Técnicas de traducción:
Durante la traducción del texto base del presente estudio se hizo uso de varias técnicas de traducción basadas en la noción propuesta por Hurtado (2001): procedimiento verbal concreto, visible en el resultado de la traducción, para conseguir equivalencias traductoras. Estos son algunos ejemplos de las técnicas empleadas:

Ampliación lingüística:
T.O: A CN that fully embraces IP technology is referred to ***here*** *as a Next Generation CN (NGCN).*
T.F: ***En este documento****, una CN que abarca totalmente la tecnología IP se denomina Red Corporativa de Próxima Generación (NGCN).*
Se añadieron elementos lingüísticos tales como la preposición *in* y el adjetivo *este.*
Inversión:
T.O: (*except where required by* ***existing investment*** *or* ***economic considerations***)
T.F: (*excepto donde las inversiones existentes o las consideraciones económicas así lo requieran*)
Se trasladaron las palabras *existing investment* y *economic considerations* antes del verbo en la oración en español para evitar la voz pasiva típica de los textos especializados en inglés pero poco natural en español.
Préstamo: préstamo de términos tales como **Back-to-Back User Agent, Firewall, World Wide Web.**

Transposición:

- ✓ *T.O: There has been a major **evolution** in enterprise telecommunications during the last few years.*
  *T:T: En los últimos años, las telecomunicaciones empresariales han **evolucionado** de manera significativa.*
  Se modificó la categoría gramatical de una parte de la oración: *evolution* (sustantivo) a *evolucionar* (verbo) sin que se produzca modificación alguna del sentido general.
- ✓ *T.O: A CN that fully embraces IP technology is referred to **here** as a Next Generation CN (NGCN).*
  *T.F: En **este documento**, una CN que abarca totalmente la tecnología IP se denomina Red Corporativa de Próxima Generación (NGCN).*
  Se cambió el adverbio *here* por el adjetivo *este* y el sustantivo *documento.*

Elementos gráficos: el informe técnico tiene diversos gráficos a lo largo del texto: el logo de ECMA internacional se encuentra en cada página del documento, desde la portada hasta la última página. Igualmente, hay 13 figuras que ilustran los procedimientos, escenarios de interconexión y arquitecturas que se describen a lo largo del informe. Estas gráficas están en colores. Otra característica de tipo gráfico es una serie de cuadros de texto donde se describen los requisitos que deberán cumplirse para que se de la comunicación entre Redes Corporativas de Nueva Generación.

3. DIMENSIÓN SEMIÓTICA: se refiere a los textos como signos dentro del sistema de valores de una cultura.

a. Género: el texto base del presente estudio es un informe técnico. Por definición un informe técnico se caracteriza por describir o exponer el proceso, progreso y resultados de una investigación científica o técnica y puede incluir recomendaciones y conclusiones de la investigación.
Características estructurales de un informe técnico:

- ✓ Un informe técnico es un documento que ilustra y suministra elementos de juicio.
- ✓ Orienta las acciones de la autoridad, particularmente en el tratamiento, esclarecimiento o solución de problemas que requieren conocimientos especializados.
- ✓ Es un instrumento valioso para la toma de decisiones.
- ✓ Es elaborado por uno o más especialistas.

Subtítulos del texto del informe técnico:

- Introducción: especifica el motivo o las razones que impulsan la redacción del informe.
- Antecedentes: ofrece una breve historia de cómo se suscitan los actos o hechos que se estudian.
- Análisis: examina minuciosamente los hechos con el fin de llegar a conclusiones fundamentadas.
- Conclusiones: contiene el resultado del análisis que se realiza en relación con los hechos y las ideas expuestas.
- Recomendaciones: sugiere las posibles soluciones o medidas a adoptar con relación al asunto trabajado en el informe.

El informe técnico base del presente estudio desarrolla claramente cada una de estas secciones:

La parte introductoria del informe técnico consta de sub-secciones entre las que se encuentran: introducción, alcance, referencias, definiciones, abreviaturas y antecedentes. Después hay una sección en la que se identifican y se analizan casos de uso clave para la comunicación con y entre redes de próxima generación. Igualmente, a manera de conclusión se presentan unas recomendaciones sobre los requisitos que deben cumplirse para que se dé la comunicación.

b. Repercusión del contenido del texto:

Gracias a la asociación que existe entre ECMA internacional e ISO, muchos de los estándares e informes técnicos desarrollados por los comités técnicos de ECMA han sido adoptados por ISO como estándares, entre ellos, el informe técnico de ECMA base del presente estudio bajo el nombre de ISO/IEC TR 26905:2006. ISO es el desarrollador y publicador de estándares más grande el mundo, tales estándares sirven para mejorar los niveles de calidad, seguridad, confiabilidad y eficacia de productos y servicios. Tienen repercusiones económicas y sociales importantes pues solucionan problemas básicos en la producción y distribución no sólo a los fabricantes sino también a los usuarios finales. Por ende, las repercusiones del contenido del texto del informe técnico de ECMA son globales y muy importantes para la sociedad pues se ha convertido en una norma internacional para la estandarización de las comunicaciones entre redes corporativas de nueva generación.

c. Relación con otros textos del mismo tema:

Del mismo autor:

El informe técnico 91 de ECMA se cita como referencia en el informe técnico 92 de ECMA: Corporate Telecommunication Networks – Mobility for Enterprise Communications para:

- Aclarar que en ese informe técnico (TR 91) se tratan temas más generales sobre la comunicación empresarial.
- Aclarar que en ese informe técnico hay más información sobre los dispositivos de seguridad que protegen las redes y sobre como traspasarlos.

En el informe técnico 95 de ECMA (Next Generation Corporate Networks (NGCN) – General), se citan apartes del contenido del informe técnico 91 en particular en la sección de antecedentes.

De otros autores:

Se cita como referencia en el artículo: IMS for Enterprises de Khlifi, H.; Gregoire, J.-C. publicado en Communications Magazine, IEEE, volumen 45, número 7, julio de 2007, página 68-75.

IV. CONCLUSIONES

- El desarrollo de un estudio terminológico como parte del proceso de formación del traductor es útil para que el trabajo de traducción sea dinámico y genere productos de utilidad no sólo para los traductores mismos sino para el público en general especialista y no especialista.

- El desarrollo de un estudio terminológico requiere de un proceso exigente que se debe llevar a cabo aprovechando los diferentes medios electrónicos al alcance con el fin de maximizar el rendimiento y disminuir la inversión de tiempo sin olvidar que estos representan una ayuda pero no reemplazan el trabajo intelectual del traductor o terminólogo.

- Las necesidades de comunicación en la sociedad actual exigen la producción de diferentes medios que contribuyan a facilitar el intercambio en lenguas como el inglés y español y es por esto que los estudios terminológicos se convierten en un requerimiento cada vez más significativo en el área de la traducción y las áreas de especialidad.

- Para el traductor en formación es importante conocer las diferentes posibilidades que el estudio de la traducción genera como es el caso de la terminología para contribuir a la comunicación entre los especialistas y el público general y porque la terminología y la traducción son inseparables una de la otra.

- Los términos que componen el campo conceptual de la telemática identificados en el texto objeto de estudio y la traducción del mismo son una herramienta útil y confiable en el área de la telemática que servirá para facilitar la comunicación entre los usuarios de la terminología en el área de las redes de comunicaciones.

- El registro bilingüe de la terminología que surgió en el campo de las redes de comunicaciones a través del presente estudio aporta significativamente al área de la traducción en la Universidad del Valle porque genera un recurso que podrá ser consultado en la biblioteca de la Universidad.

- El presente estudio también hace un aporte significativo al área de la traducción en la Universidad del Cauca y en la ciudad de Popayán para motivar a otros profesionales en el área de lenguas a vincularse a proyectos de traducción y terminología que hasta el momento no se han desarrollado en la ciudad.

- El estudio terminológico sobre el tema de las Redes Corporativas de Telecomunicaciones con base en un informe técnico de ECMA Internacional y la base de datos terminológica producto final del estudio servirá como herramienta de consulta a los estudiantes, profesionales, especialistas, traductores y otros interesados en el área de la telemática por ser un recurso confiable creado con seriedad.

V. BIBLIOGRAFÍA

1. En el campo de la traducción y la terminología:

ARNTZ, Reiner y PICHT, Heribert (1996) *Introducción a la Terminología.* Traducción del alemán por: Amelia de Irazazábal, María José Jiménez, Erika Schwarz, Susana Yunquera. Fundación Germán Sánchez Ruiperez. Madrid.

HUERTA HURTADO, María de Jesús y GARCÍA NÚÑEZ, Roberto (2007) *Lingüística de texto (superestructuras).* Sincronía, a Journal for the Humanities and Social Sciences. Department of Literature. University of Guadalajara. ISSN 1562-384X, Number 1.

HURTADO ALBIR, Amparo (2001) *Traducción y Traductología*. Ediciones Cátedra. Madrid.

PAVEL, Silvia y NOLET, Diana (2001) *Manual de Terminología,* Travaux publics et Services Gouvernementaux Canada, Bureau de la traduction / Public Works and Government Services Canada Translation Bureau, Québec.

RODRÍGUEZ, Emma (2004) *Terminología y Traducción*. Unidad de Artes Gráficas. Facultad de Humanidades. Universidad del Valle. Cali.

2. En el campo de la telemática, la informática y las redes de comunicaciones:

DOCUMENTACIÓN IMPRESA

En inglés:

BLUNDO, Carlo y CLIMATO Stelvio (2005) *Security in communication networks: 4th international conference, SCN 2004, September 8-10, 2004: revised selected papers.* Amalfi, Italia.

GARCÍA, Alberto León, WIDJAJA Indira (2004) *Communication Networks: fundamental concepts and key architectures.* McGrawHill Professional. Nueva York.

HILL ASSOCIATES, INC (2001) *Telecommunications: a beginner's guide. Network professional's library.* Editor McGraw-Hill Professional.

SATHYA Rao, KAARE Ingar Sletta (2000) *Next generation networks: networks and services for the information society: 5th IFIP TC6 international symposium, INTERWORKING.* Bergen, Noruega.

WILKINSON, Neil (2002) *Next generation network services: technologies and strategies. Editor John Wiley and Sons.*

En Español:

LAPORTA, Jorge Lázaro (2005) *Fundamentos de telemática* - Colaborador Marcel Miralles Aguiñiga. Editorial de la Universidad Politécnica de Valencia, España.

LEÓN, Mario (2004) *Diccionario de informática, telecomunicaciones y ciencias afines: inglés-español E*diciones Díaz de Santos. Madrid.

HERRERA, Enrique (2003) *Tecnologías y redes de transmisión de datos.* Editorial Limusa, México.

HERRERA, Enrique (2003) *Introducción a las telecomunicaciones modernas.* Editorial Limusa, México.

TANENBAUM, Andrew S. (2003) *Redes de computadoras*. Prentice Hall, México.

D. BLACK, Uyless (1987) *Redes de transmisión de datos y proceso distribuido.* Ediciones Díaz de Santos. Madrid.

ESPAÑA BOQUERA, María Carmen (2003) *Servicios avanzados de telecomunicación. E*diciones Díaz de Santos. Madrid.

MAÑAS, José Antonio *(2004) Mundo IP: introducción a los secretos de Internet y las redes de datos.* Ediciones Nowtilus, Madrid.

PURSER, Michael (1990) *Redes de telecomunicación y ordenadores.* Ediciones Díaz de Santos, Madrid.

ZNATY, Simón (2002) *Next Generation Network – Telefonía sobre IP* – Editorial EFFORT (Études et FORmations en Télecomumunication)

DOCUMENTACIÓN EN FORMATO ELECTRÓNICO

En inglés:

EUROPEAN COMPUTERS MANUFACTURERS ASSOCIATION, ECMA. (Junio, 2000) *Corporate Telecommunication Networks (CN) – Standardization Plan – ECMA TR/75.*
Recuperado en http://www.ecma-international.org/publications/files/ECMA-TR/TR-075.pdf
21 de mayo de 2011.

EUROPEAN COMPUTERS MANUFACTURERS ASSOCIATION, ECMA. (Diciembre, 2003) *Corporate Telecommunication Networks – User Identification in a SIP/QSIG Environment - ECMA TR/86 First Edition / December.*
Recuperado en http://www.ecma-international.org/publications/files/ECMA-TR/TR-086.pdf
21 de mayo de 2011.

EUROPEAN COMPUTERS MANUFACTURERS ASSOCIATION, ECMA. (Diciembre, 2005) *Corporate Telecommunication Networks – Mobility for Enterprise Communications - ECMA TR/92 First Edition*
Recuperado en http://www.ecma-international.org/publications/files/ECMA-TR/TR-092.pdf
21 de mayo de 2011.

EUROPEAN COMPUTERS MANUFACTURERS ASSOCIATION, ECMA. (Diciembre, 2005) Technical Report 91: Enterprise Communication in Next Generation Corporate Networks (NGCN) involving Public Next Generation Networks (NGN)".
Recuperado en
http://www.ecma-international.org/publications/techreports/E-TR-091.htm
21 de mayo de 2011.

EUROPEAN COMPUTERS MANUFACTURERS ASSOCIATION, ECMA. (Junio, 2008) *Next Generation Corporate Networks (NGCN) – General. ECMA TR/95 First Edition.*
Recuperado en http://www.ecma-international.org/publications/files/ECMA-TR/TR-095.pdf
21 de mayo de 2011.

EUROPEAN COMPUTERS MANUFACTURERS ASSOCIATION, ECMA. (Junio, 2008) *Next Generation Corporate Networks (NGCN) – Identification and Routing - ECMA TR/96 First Edition. Recuperado en*
http://www.ecma-international.org/publications/files/ECMA-TR/TR-096.pdf.
21 de mayo de 2011.

INOMATA, Akihiro (Octubre, 2006) *Approach to Next Generation Corporate Networks – FUJITSU Sci. Tech. J.*
Recuperado en
http://www.fujitsu.com/downloads/MAG/vol42-4/paper16.pdf
21 de mayo de 2011.

TELCORDIA TECHNOLOGIES (*2007) Next Generation Network (NGN) Services*
Recuperado en http://www.mobilein.com/NGN_Svcs_WP.pdf
21 de mayo de 2011.

En español:

ArCERT, COORDINACIÓN DE EMERGENCIA EN REDES TELEINFORMÁTICAS DE LA ADMINISTRACIÓN PÚBLICA ARGENTINA (Diciembre, 1998) *Manual de Seguridad en Redes. Equipo de Seguridad en Redes Subsecretaría de Tecnologías Informáticas Secretaría de la Función Pública Versión 1.0.*
Recuperado en
http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf
21 de mayo de 2011.

COMISIÓN DE REGULACIÓN DE TELECOMUNICACIONES – REPÚBLICA DE COLOMBIA *(Junio, 2007) Estudio Integral de Redes de Nueva Generación y Convergencia. - Documento Amarillo Centro de Conocimiento del Negocio.*
Recuperado en
http://radiogis.uis.edu.co/gestion/Bliblioteca/Articulos%20NGN/NGN-EstudioIntegral_MinComunicaciones.pdf
21 de mayo de 2011.

TELEFÓNICA DE ESPAÑA (Marzo, 2000) *Introducción a la telemática y a las redes de datos. Documentación en formato electrónico – Dirección de Servicios de Formación de Telefónica de España.*
Recuperado en
http://www.herramientasuamac.uat.edu.mx/biblioteca/libros/Introduccion%20a%20la%20Telematica%20y%20Redes%20de%20Datos%28Telefonica%29.pdf
21 de mayo de 2011.

GLOSARIOS Y DICCIONARIOS EN FORMATO ELECTRÓNICO

Inglés

DICCIONARIO EN LÍNEA YOURDICTIONARY.COM, Love To Know, Corp (1996-2011)
Recuperado en
http://www.yourdictionary.com/
21 de mayo de 2011.

DICCIONARIO EN LÍNEA DE TECNOLOGÍA TECHABULARY.COM, Packetizer, Inc (2011)
Recuperado en
http://www.techabulary.com/p/pstn/
21 de mayo de 2011.

DICCIONARIO EN LÍNEA DE REDES Y TELECOMUNICACIONES
NETWORKDICTIONARY.COM (2004-2011)
Recuperado en
http://www.networkdictionary.com/telecom/pstn.php
21 de mayo de 2011.

DICCIONARIO EN LÍNEA BIRDS-EYE.NET, Birds-Eye.Net.
Recuperado en
http://birds-eye.net/definition/a/
21 de mayo de 2011.

ENCICLOPEDIA Y GLOSARIO EN LÍNEA whatis.com, TechTarget (2011)
Recuperado en
http://whatis.techtarget.com/
21 de mayo de 2011.

ENCICLOPEDIA EN LÍNEA Webopedia.com, QuinStreet Inc (2011)
Recuperado en
http://www.webopedia.com/TERM/N/NGN.htm
21 de mayo de 2011.

EUROPEAN COMPUTERS MANUFACTURERS ASSOCIATION, ECMA. (2000) *Glossary of Definitions and Terminology for Computer Supported Telecommunications Applications (CSTA) Phase III – ECMA TR/72 Third Edition.*

Recuperado en
http://www.ecma-international.org/publications/files/ECMA-TR/TR-072.pdf
21 de mayo de 2011.

GLOSARIO EN LÍNEA THEMANUALPAGE.COM, Themanualpage.org (2002-2011)
Recuperado en
http://www2.themanualpage.org/
21 de mayo de 2011.

DICCIONARIO EN LÍNEA DE COMPUTADORES Computerdictionaryonline.com, Computer Dictionary On Line (2011)
Recuperado en
http://www.computer-dictionary-online.org/
21 de mayo de 2011.

DICCIONARIO TÉCNICO EN LÍNEA Geek.com, Ziff Dvais, Inc (1996-2011)
Recuperado en
http://www.geek.com/technical-glossary/
21 de mayo de 2011.

Español

GLOSARIO DE TECNOLOGÍA, Ciscoredaccionvistual.com, Cisco (2011)
Recuperado en
http://www.ciscoredaccionvirtual.com/redaccion/glosario/default.asp
5 de mayo de 2011.

LA WEB DE LOS DICCIONARIOS, Glosarium.com, David Carrero Fernandez-Baillo (1995-2010)
Recuperado en
http://www.glosarium.com/index.php
21 de mayo de 2011.

VI. ANEXOS

1. **Representación Conceptual en Español**
   a. Árbol Conceptual General *Telemática*
   b. Árbol Conceptual Específico
2. **Representación Conceptual en Inglés**
   a. Árbol Conceptual General *Information and Communications Technology*
   b. Árbol Conceptual Específico
3. **Glosario Bilingüe Inglés – Español**
4. **Glosario Bilingüe Español – Inglés**
5. **Texto Original en inglés:** *"Enterprise Communication In Next Generation Corporate Networks (NGCN) Involving Public Next Generation Networks (NGN)"*
6. **Traducción Final del Texto Original:** *"Comunicación Empresarial en Redes Corporativas de Próxima Generación Relacionadas con Redes Públicas de Próxima Generación (NGN)"*

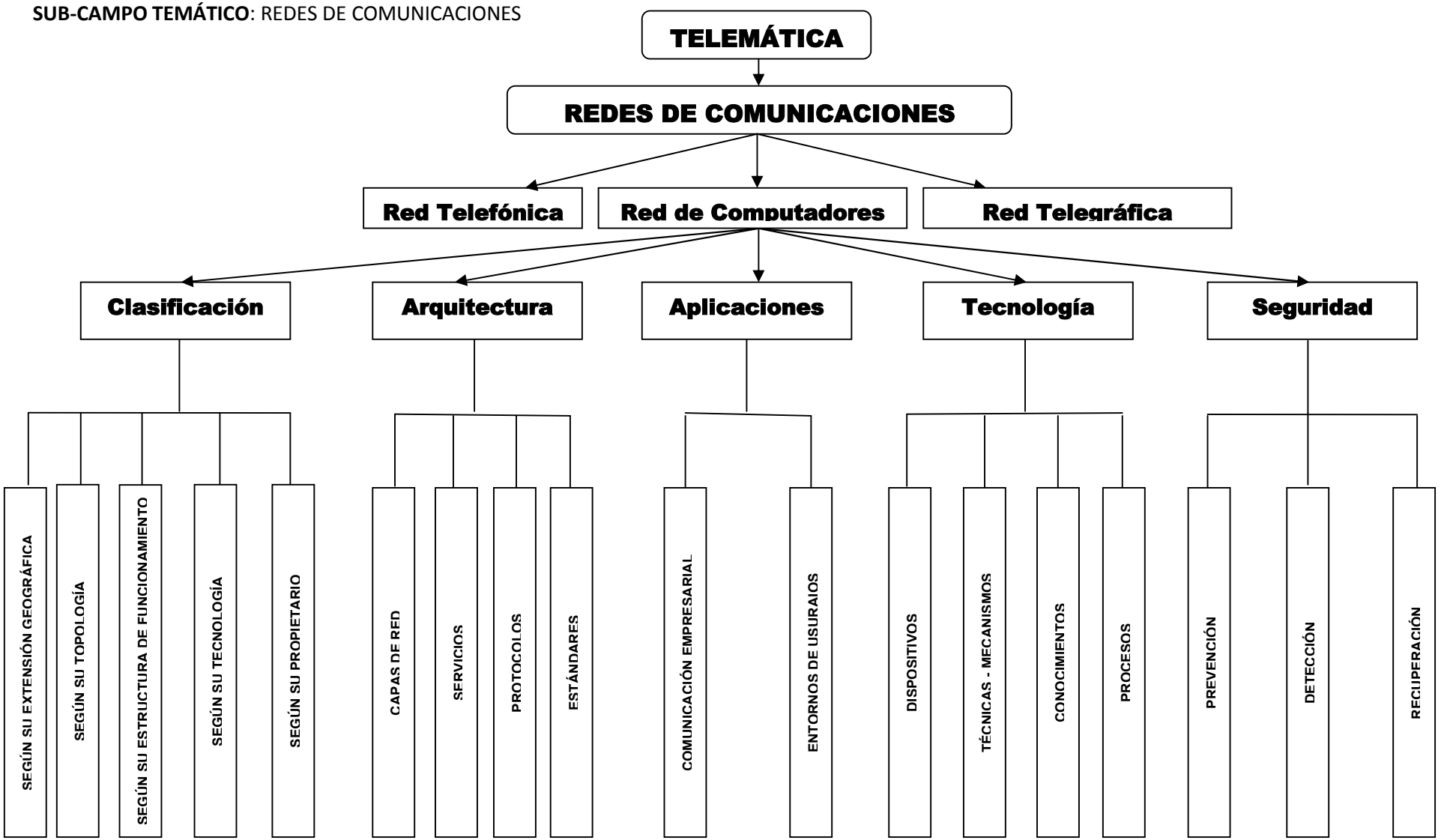
1. REPRESENTACIÓN CONCEPTUAL DEL CAMPO Y SUBCAMPO TEMÁTICO (ESPAÑOL)

"ENTERPRISE COMMUNICATION IN NEXT GENERATION CORPORATE NETWORKS (NGCN) INVOLVING PUBLIC NEXT GENERATION NETWORKS (NGN)"

a. Árbol Conceptual General

CAMPO TEMÁTICO: TELEMÁTICA

SUB-CAMPO TEMÁTICO: REDES DE COMUNICACIONES



b. Árbol conceptual específico

REPRESENTACIÓN CONCEPTUAL DEL CAMPO Y SUBCAMPOS TEMÁTICOS (ESPAÑOL):
"ENTERPRISE COMMUNICATION IN NEXT GENERATION CORPORATE NETWORKS (NGCN) INVOLVING PUBLIC NEXT GENERATION NETWORKS (NGN)"

TELEMÁTICA

1. REDES DE COMUNICACIONES

1.1. RED TELEFÓNICA
Red de Conmutación de Circuitos
Red Digital de Servicios Integrados (RDSI)
Punto de Referencia T
Red Telefónica Pública Conmutada (RTPC)

1.2. RED TELEGRÁFICA

1.3. RED DE COMPUTADORES

1.3.1. CLASIFICACIÓN DE LAS REDES

1.3.1.1. Según su Extensión Geográfica
LAN
Red doméstica
Switch LAN
MAN
WAN
Sistema Multiprocesador
1.3.1.2. Según su Topología
Red punto a punto
Red multipunto
En estrella
En malla
En árbol
1.3.1.3. Según su Estructura de Funcionamiento
1.3.1.4. Según su Tecnología
Conmutadas
No Conmutadas
Red Heredada
Con conmutación de circuitos
Con conmutación de paquetes

1.3.1.5. Según su Propietario
Pública
Privada
Extranet
Intranet
Red de Valor Agregado
Red Privada Virtual
Túnel VPN

1.3.2. ARQUITECTURA DE RED

1.3.2.1. Capas de Red (Modelo OSI)
Capa de aplicación
Pasarela de la Capa de Aplicación
Capa de Presentación
Capa de Sesión
Capa de Transporte
Protocolo de Seguridad de la Capa de Transporte TLS
Capa de Red
Capa de Enlace
Capa Física

1.3.2.2. Servicios
Servicios de Presencia
Transferencia de Archivos

1.3.2.3. Protocolos
ENUM
Protocolo de Gestión de Claves MIKEY
Protocolo de Inicio de Sesión SIP
Entidades SIP
Agente de Usuario UA
Agente de Usuario Cliente UAC
Agente de Usuario Servidor UAS
Back-to-Back User Agent B2BUA
Servidor de Redirección
Servidor de Registro
Esquema Trapezoide SIP
Mensaje SIP
Encabezado del Mensaje SIP
Petición SIP
P2P SIP

SIP URI
Protocolo de Internet IP
Dirección IP
Protocolo de Seguridad IP
Voz sobre Protocolo de Internet VoIP
Controlador de Sesión de Borde SBC
Protocolo de Control de Sesión SCP
Protocolo de Control en Tiempo Real RTCP
Protocolo de Control de Transmisión TCP
Protocolo de Datagramas de Usuario UDP
Protocolo de Descripción de Sesión SDP
Protocolo MSRP
Protocolo de Señalización
Protocolo de Transporte en Tiempo Real RTP
Protocolo de Transporte Seguro en Tiempo Real SRTP
STUN
Servidor STUN

1.3.2.4 Estándares

CSTA Aplicaciones en Telecomunicaciones Asistidas por Computador
H.323
Punto Terminal
Estándar ICE

1.3.3. APLICACIONES DE LAS REDES

1.3.3.1. Comunicación Empresarial

Call Center
Registro de Llamadas
Correo Electrónico Empresarial
E.164
IP Centrex
IP-PBX
Línea Alquilada
PBX
Proveedor de Servicios de Aplicaciones (PSA)
Red Corporativa de Telecomunicaciones
Equipo Local del Cliente
Punto a Punto
Red de Instalaciones del Cliente
Red Corporativa de Próxima Generación

Servicio Centrex
Softswitch
SOHO

1.3.3.2. Entornos de Usuarios

Información Remota
Comunicaciones
Entretenimiento

1.3.4. TECNOLOGÍA DE RED

1.3.4.1. Dispositivos

Equipo Terminal
Pasarela
Proxy de Entrada
Proxy de Salida
Servidor Proxy
Túnel

1.3.4.2. Técnicas y Mecanismos

Balanceo de Carga
Codecs
Configuración de Tráfico
Conmutación de Circuitos
Calidad de Servicio QoS
Enrutamiento
Reenvío de llamadas
Extensiones de Correo Internet de Propósitos Múltiples/Seguro (S/MIME)
Identificador Uniforme de Recursos
Keep-alive
Multiplexación por División de Tiempo MDT
Paquete
Puenteo
Salto
Traducción de Direcciones de Red NAT
NAT Simétrico
Traducción/Traductor de Direcciones de Red Transversal (NAT-T)
URI de Teléfono

1.3.4.3. Conocimientos

1.3.4.4. Procesos

Resiliencia
Señalización

Ruta de Señalización
Tiempo Real
Transcodificación

1.3.5. SEGURIDAD DE RED

1.3.5.1. Mecanismos de Prevención

Autoridad de Certificación
Cifrado
Clave Compartida
Clave de Sesión
Cifrado Punto a Punto
Cifrado de Medios
Cifrado de Clave Pública
Infraestructura de Clave Pública PKI
Decodificación
Firewall
Protocolo de Intercambio de Claves Diffie-Hellman
Seguridad Extremo a Extremo

1.3.5.2. Mecanismos de Detección

Autenticación
Lista Blanca
Lista Negra
Servidor de Políticas
Verificación de Integridad

1.3.5.3. Mecanismos de Recuperación

1.3.5.4. Incidentes

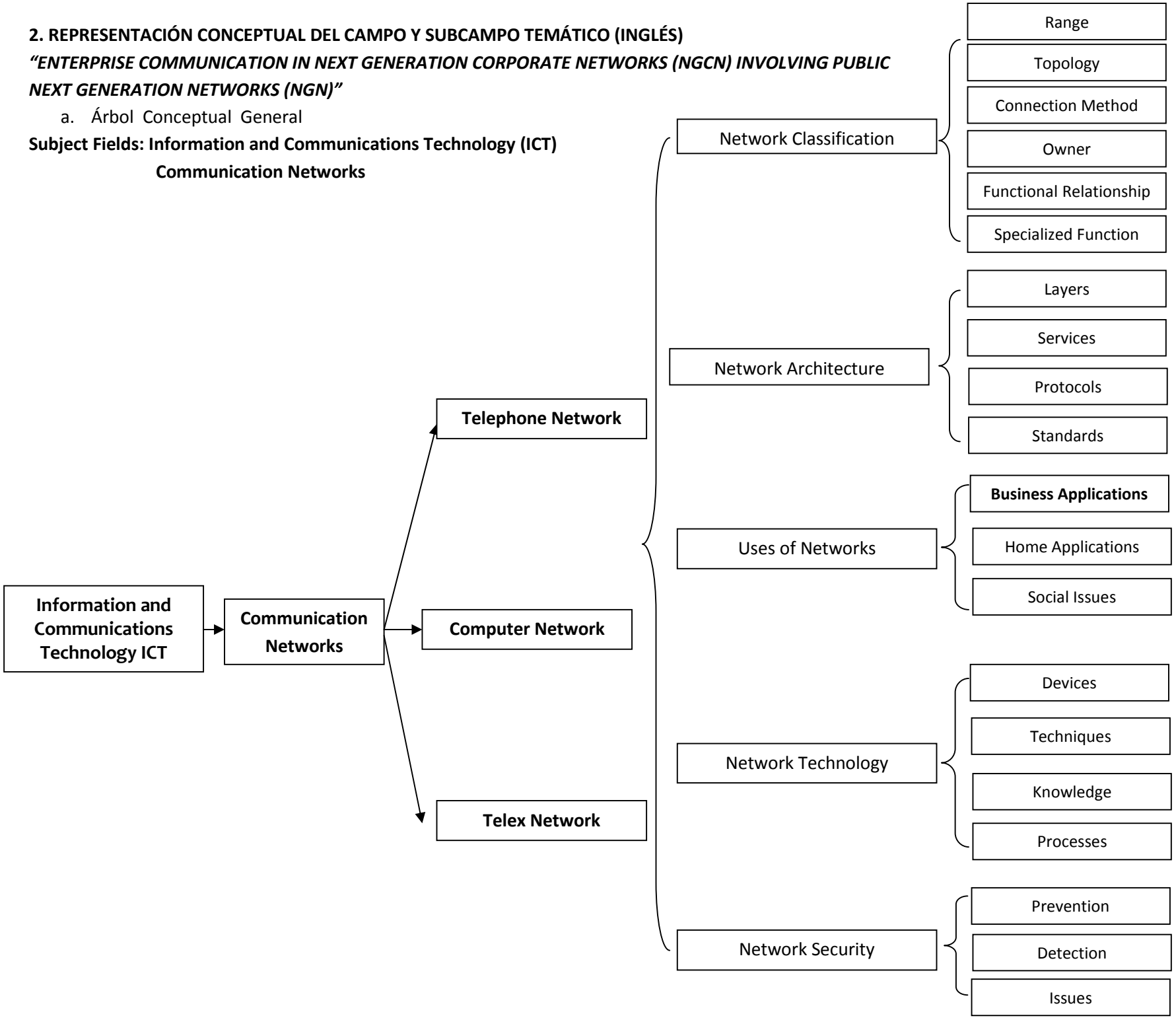
Ataque de denegación de servicios (DoS)
Eavesdropping

2. REPRESENTACIÓN CONCEPTUAL DEL CAMPO Y SUBCAMPO TEMÁTICO (INGLÉS)

"ENTERPRISE COMMUNICATION IN NEXT GENERATION CORPORATE NETWORKS (NGCN) INVOLVING PUBLIC NEXT GENERATION NETWORKS (NGN)"

a. Árbol Conceptual General

Subject Fields: Information and Communications Technology (ICT)
Communication Networks



b. Árbol Conceptual Específico:

SUBJECT FIELDS BASED ON "ENTERPRISE COMMUNICATION IN NEXT GENERATION CORPORATE NETWORKS (NGCN) INVOLVING PUBLIC NEXT GENERATION NETWORKS (NGN)"

INFORMATION AND COMMUNICATIONS TECHNOLOGY

1. COMMUNICATION NETWORKS

1.1. TELEPHONE NETWORK
Circuit-Switched Network
Integrated Services Digital Network ISDN
T-reference pont
Public Switched Telephone Newtork PSTN

1.2. TELEX NETWORK

1.3. COMPUTER NETWORK

1.3.1. NETWORK CLASSIFICATION

1.3.1.1. By Range
PAN
LAN
Home Network
LAN Switch
MAN
WAN

1.3.1.2. By Topology
Bus Network
Star Network
Ring Network
Grid Network
Toroidal Networks and Hypercubes
Tree and Hypertree Networks

1.3.1.3. By Connection Method
Legacy Network
Next Generation Network

1.3.1.4. By Owner

Public

Private

Extranet

Intranet

Value-Added Network

Virtual Private Network VPN

VPN Tunnel

1.3.1.5. By Functional Relationship

1.3.1.6. By Specialized Function

1.3.2. NETWORK ARCHITECTURE

1.3.2.1. Layers (OSI Model)

Application Layer

Application Layer Gateway (ALG)

Presentation Layer

Session Layer

Transport Layer

Transport Layer Security TLS

Network Layer

Data Link Layer

Physical Layer

1.3.2.2. Services

File Transfer

Presence Services

1.3.2.3. Protocols

ENUM

Internet Protocol IP

IP Address

IP Security

VoIP

Session Border Controller SBC

Message Session Relay Protocol (MSRP)

Multimedia Internet KEYing (MIKEY)

P2P SIP

Real Time Protocol RTP

Real Time Control Protocol RTCP
Secure Real Time Protocol SRTP
Session Control Protocol SCP
Session Description Protocol SDP
Signalling Protocol
Session Initiation Protocol SIP
Endpoint
SIP Entities
Back-to-Back User Agent
Redirect Server
Registrar
User Agent (UA)
User Agent Client (UAC)
User Agent Server (UAS)
SIP Message
SIP Header
SIP Request
SIP Trapezoid
SIP URI
Simple Traversal of User Datagram Protocol (UDP) Through Network Address
Translators STUN
STUN Server
Transmission Control Protocol TCP
User Datagram Protocol UDP

1.3.2.4. Standards

Computer Supported Telecommunications Applications CSTA
H.323
Endpoint
Interactive Connectivity Establishment ICE

1.3.3. USES OF NETWORKS

1.3.3.1. Business Applications

Enterprise Communication
Application Service Provider ASP
Call Center
Call Logging
Centrex Services
Corporate Email
Corporate Telecommunication Networks

Customer Premises Equipment CPE
Customer Premises Network
End-to-end
Next Generation Corporate Network (NGCN)
E.164
IP Centrex
IP-PBX
Leased Line
Private Branch Exchange PBX
Softswitch
SOHO

1.3.3.2. Home Applications

1.3.3.3. Social Issues

1.3.4. NETWORK TECHNOLOGY

1.3.4.1. Devices

Gateway
Inbound Proxy
Outbound Proxy
Proxy Server
Terminal Equipment TE
Tunnel

1.3.4.2. Techniques

Bridging
Circuit Switching
Codecs
Hop
Keep-alive
Load Balancing
Network Address Translation NAT
Symmetric NAT
NAT Traversal
Packet
Port Number
Presence Services
Quality of Service
Routing
Onward Routing
Session Border Controller (SBC)
Secure Multipurpose Internet Mail Extension S/MIME

Tel URI
Traffic Shaping
Time-Division Multiplexing TDM
Uniform Resource Identifier URI

1.3.4.3. Knowledge

1.3.4.4. Processes

Real Time
Resilience
Signalling
  Signalling Path
Transcoding

1.3.5. NETWORK SECURITY

1.3.5.1. Prevention

Certification Authority
Decryption
Diffie-Hellman Key Agreement
End-to-End Security
Encryption
  End-to-end Encryption
  Media Encryption
  Public Key Cryptography
  Session Key
  Shared Key
Firewall
Public Key Infrastructure PKI

1.3.5.2. Detection

Authentication
Black List
Integrity Check
Policy Server
White List

1.3.5.3. Issues

Denial of Service Attack (DoS)
Eavesdropping

GLOSARIO BILINGÜE INGLÉS – ESPAÑOL

INGLÉS	ESPAÑOL
1. Application Layer Gateway (ALG)	Pasarela de la Capa de Aplicación/Pasarela a Nivel de Aplicación
2. Application Service Provider (ASP)	Proveedor de Servicios de Aplicaciones (PSA)
3. Authentication	Autenticación, Autentificación
4. Back-to-back User Agent (B2BUA)	Back-to-back User Agent (B2BUA)
5. Black List/Blocklist	Lista Negra
6. Bridging	Puenteo/Puenteado
7. Call Center	Centro de Llamadas/Call Center/Central de Atención de Llamadas/Centro de Atención Telefónica
8. Call Logging	Grabación de Llamadas/Registro de Llamadas/ Monitoreo de Llamadas
9. Centrex Services	Servicio Centrex
10. Certification Authority(CA)	Autoridad de Certificación
11. Circuit Switching	Conmutación de Circuitos
12. Circuit-Switched Network	Red de Conmutación de Circuitos
13. Codecs	Codecs
14. Computer Supported Telecommunications Applications (CSTA)	Aplicaciones en Telecomunicaciones Asistidas por Computador (CSTA)/ Aplicaciones de Telecomunicaciones Compatibles con Equipos Informáticos
15. Corporate Email	Correo Electrónico Empresarial/Correo Electrónico Corporativo/E-mail Empresarial
16. Corporate/Enterprise Telecommunication Networks (CNs)	Redes Corporativas/Empresariales de Telecomunicaciones.
17. Customer Premises Equipment (CPE)	Equipo Local del Cliente/Equipo en las Instalaciones del Cliente/Equipamiento de Usuario
18. Customer Premises Network	Red de Instalaciones del Cliente/Red de Abonados/Red de Instalación de Abonado/ Red Local de Abonado Móvil/Red de Usuario
19. Decryption	Decodificación
20. Denial of Service Attack	Ataque de Denegación de Servicios (DoS)
21. Diffie-Hellman Key Agreement	Protocolo de Intercambio de Claves Diffie-Hellman/Acuerdo de Clave Diffie-Hellman/ Acuerdo de Clave Exponencial de Diffie-Hellman
22. E.164	E.164
23. Eavesdropping	Eavesdropping/Espionaje
24. Encryption	Cifrado/Transformación Criptográfica/ Encriptación/Criptografía
25. End-to-end encryption	Cifrado Punto a Punto/Cifrado Extremo a Extremo

INGLÉS	ESPAÑOL
26. End-to-End	Punto a Punto/ Extremo a Extremo/Puntos Finales/Puntos Extremos
27. Endpoint	Punto Terminal/Punto Extremo/Punto Final
28. End-to-End Security	Seguridad Extremo a Extremo
29. Enterprise communication/Corporate Communication	Comunicación Empresarial/Comunicación Corporativa
30. ENUM	ENUM
31. Extranet	Extranet
32. File transfer	Transferencia de Archivos/Ficheros
33. Firewall	Firewall/Cortafuegos
34. Gateway (GW)	Pasarela/Puerta de Enlace/Compuerta
35. H.323	H.323
36. Home Networks	Redes Domésticas
37. Hop	Salto
38. Inbound Proxy	Proxy de Entrada/Proxy Entrante
39. Integrated Services Digital Network (ISDN)	Red Digital de Servicios Integrados (RDSI)
40. Integrity Checking	Verificación/Comprobación de Integridad
41. Interactive Connectivity Establishment (ICE)	Estándar ICE
42. Internet Protocol (IP)	Protocolo de Internet
43. Intranet	Intranet/Intrarred
44. IP address	Dirección IP
45. IP Centrex	IP Centrex/PBX alojado
46. IP Security (IPSEC)	IPSEC/Protocolo de seguridad IP
47. IP-PBX: (Internet Protocol Public Branch Exchange)	IP-PBX
48. Keep-alive	Keep-alive
49. LAN switch	Switch LAN/Switch de Red de Área Local/ Conmutador de Red de Área Local/Switch de LAN
50. Leased Line	Línea Alquilada/Arrendada/Dedicada
51. Legacy Network	Red Heredada/Red Preexistente
52. Load Balancing	Balanceo de Carga
53. Media encryption	Cifrado de Medios
54. Message Session Relay Protocol (MSRP)	Protocolo MSRP/Protocolo de Retransmisión de Mensajes
55. Multimedia Internet KEYing (MIKEY)	Protocolo de Gestión de Claves MIKEY
56. NAT Network Address Translation	Traducción de Direcciones de Redes
57. NAT Traversal	Traducción/Traductor de Direcciones de Red Transversal (NAT-T)
58. Network Layer	Capa/Nivel de red
59. Next Generation Network (NGN)	Red de Próxima Generación/Red de Nueva Generación/Red de Siguiente Generación

INGLÉS	ESPAÑOL
60. Next Generation Corporate Network (NGCN)	Red Corporativa de Próxima Generación
61. Onward Routing	Reenvío de Llamadas/Desvío del Llamado/ Encaminamiento Hacia Adelante
62. Outbound Proxy	Proxy de Salida/Proxy Saliente
63. Packet	Paquete
64. Peer-to-Peer (P2P) SIP	P2P SIP
65. Policy Server	Servidor de Políticas
66. Port Number	Número de Puerto
67. Presence Services	Servicios de Presencia
68. Private Branch Exchange (PBX)	Centralita Automática Privada/Central Telefónica para Negocios Privados/Central Telefónica Digital/Centralita Telefónica Privada/Conmutador
69. Proxy/Proxy Server	Servidor Proxy
70. Public-Key Cryptography	Cifrado de Clave Pública/Criptografía Asimétrica/Cifrado Asimétrico/Criptografía de Clave Pública
71. Public Key Infrastructure (PKI)	Infraestructura de Clave Pública, Arquitectura de Clave Pública
72. PSTN Public Switched Telephone Network	Red Telefónica Pública Conmutada (RTPC)
73. Quality of Service, QoS	Calidad de Servicio QoS
74. Real-time/Real Time/Realtime	Tiempo Real
75. Real Time Protocol (RTP)	Protocolo de Tiempo Real/Protocolo de Transporte en Tiempo Real
76. Redirect/Redirect Server	Servidor de Redirección/Servidor de Redireccionamiento/Servidor Redirector
77. Registrar	Servidor de Registro
78. Resilience	Resiliencia
79. Routing	Enrutamiento/Encaminamiento
80. RTP Control Protocol (RTCP)	Protocolo de Control en Tiempo Real
81. S/MIME Secure Multipurpose Internet Mail Extension	Extensiones Polivalentes de Correo por Internet/Extensiones de Correo de Internet de Propósitos Múltiples/Seguro
82. Secure RTP (SRTP)	Protocolo de Transporte Seguro en Tiempo Real
83. Session Border Controller (SBC)	Controlador de Sesión de Borde (SBC)
84. Session Control Protocol SCP	Protocolo de Control de Sesión SCP
85. Session Description Protocol (SDP)	Protocolo de Descripción de Sesión
86. Session Initiation Protocol (SIP)	Protocolo de Inicio de Sesión
87. Session Initiation Protocol Uniform Resource Identifier - SIP URI	Identificador Uniforme de Recursos de SIP
88. Session Key	Clave de Sesión
89. Shared Key/Shared Secret	Clave Compartida
90. Signalling	Señalización

INGLÉS	ESPAÑOL
91. Signalling Path	Ruta de Señalización
92. Signalling Protocol	Protocolo de Señalización
93. Simple Traversal of UDP through NATs (STUN)	Simple Traversal of User Datagram Protocol a través de Network Address Translators (NATs) STUN
94. Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) – STUN Server	Servidor STUN
95. SIP Headers	Encabezado del Mensaje SIP/ Encabezamiento del Mensaje SIP, Cabecera del Mensaje SIP
96. SIP Messages	Mensajes SIP
97. SIP Request	Petición SIP
98. SIP Trapezoid	Esquema Trapezoide SIP
99. Softswitch	Softswitch/Conmutación por Software
100. SOHO	SOHO "Oficina Pequeña, Oficina en Casa"
101. Symmetric NAT	NAT Simétrico
102. Tel URI	URI de teléfono "tel"
103. Terminal Equipment (TE)	Equipo Terminal
104. Time-Division Multiplexing -TDM	Multiplexación por División de Tiempo (MDT)
105. T- Reference Point	Punto de referencia T (de terminal)
106. Transmission Control Protocol (TCP)	Protocolo de Control de Transmisión
107. Traffic Shaping	Configuración de Tráfico
108. Transcoding	Transcodificación
109. Transport Layer	Capa de Transporte
110. Transport Layer Security (TLS)	Protocolo de Seguridad de la Capa de Transporte
111. Tunnel	Túnel
112. Uniform resource Identifiers (URIs)	Identificador Uniforme de Recursos
113. User Agent (UA)	Agente de Usuario
114. User Agent Client (UAC)	Agente de usuario cliente/Cliente de Agente de Usuario
115. User Agent Server (UAS)	Agente de Usuario Servidor/Servidor de Agente de Usuario
116. User Datagram Protocol - UDP	Protocolo de Datagramas de Usuario
117. Value-added Network	Red con Valor Agregado
118. Virtual Private Network (VPN)	Red Privada Virtual
119. VoIP - Voice over Internet Protocol	Voz sobre Protocolo de Internet
120. VPN Tunnel	Túnel VPN
121. Whitelist	Lista Blanca

GLOSARIO BILINGÜE ESPAÑOL - INGLÉS

ESPAÑOL	INGLÉS
1. Agente de Usuario	User Agent (UA)
2. Agente de Usuario Cliente	User Agent Client (UAC)
3. Agente de Usuario Servidor	User Agent Server (UAS)
4. Ataque de Denegación de Servicio	Denial of Service Attack (DoS)
5. Autenticación/Autentificación	Authentication
6. Autoridad de Certificación	Certification Authority CA
7. Back-to-back User Agent (B2BUA)	Back-to-back User Agent (B2BUA)
8. Balanceo de Carga	Load Balancing
9. Calidad de Servicio QoS	QoS Quality of Service
10. Capa de Transporte	Transport Layer
11. Capa/Nivel de Red	Network Layer
12. Centro de Llamadas	Call Center
13. Cifrado	Encryption
14. Cifrado de Clave Pública	Public-key Cryptography
15. Cifrado de Medios	Media Encryption
16. Cifrado Punto a Punto	End-to-end Encryption
17. Clave Compartida	Shared Key or Shared Secret
18. Clave de sesión	Session Key
19. Codec	Codecs
20. Comunicación Empresarial/Corporativa	Enterprise Communication/ Corporate Communication
21. Configuración de Tráfico	Traffic Shaping
22. Conmutación de Circuitos	Circuit Switching
23. Controlador de Sesión de Borde (SBC)	Session Border Controller (SBC)
24. Correo Electrónico Empresarial /Corporativo	Corporate Email
25. CSTA - Aplicaciones en Telecomunicaciones Asistidas por Computador	Computer Supported Telecommunications Applications (CSTA)
26. Decodificación	Decryption
27. Dirección IP	IP address
28. E.164	E.164
29. Eavesdropping /Espionaje	Eavesdropping
30. Encabezado del Mensaje SIP	SIP Header
31. Enrutamiento	Routing
32. ENUM	ENUM
33. Equipo Local del Cliente CPE	Customer Premises Equipment (CPE)
34. Equipo Terminal	Terminal Equipment (TE)
35. Esquema Trapezoide SIP	SIP Trapezoid
36. Estándar ICE	Interactive Connectivity Establishment (ICE)
37. Extranet	Extranet

ESPAÑOL	INGLÉS
38. Firewall	Firewall
39. H.323	H.323
40. Identificador Uniforme de Recursos	Uniform Resource Identifiers (URIs)
41. Infraestructura de Clave Pública	Public Key Infrastructure (PKI)
42. Intranet	Intranet
43. IP Centrex o PBX alojado	IP Centrex
44. IP-PBX (Internet Protocol Public Branch Exchange)	IP-PBX
45. IPsec/Protocolo de seguridad IP	IP Security (IPSEC)
46. Keep-alive	Keep-alive
47. Línea Alquilada	Leased Line
48. Lista Blanca	Whitelist
49. Lista Negra	Black List/Blocklist
50. Mensajes SIP	SIP messages
51. Multiplexación por División de Tiempo MDT	TDM = Time-Division Multiplexing
52. NAT Simétrico	Symmetric NAT
53. Número de Puerto	Port Number
54. P2P SIP	Peer-to-peer (P2P) SIP
55. Paquete	Packet
56. Pasarela	Gateway (GW)
57. Pasarela de la Capa de Aplicación	Application Layer Gateway (ALG
58. PBX	Private Branch Exchange (PBX)
59. Petición SIP	SIP Request
60. Protocolo de Control de Sesión SCP	Session Control Protocol SCP
61. Protocolo de Control de Transmisión TCP	Transmission Control Protocol (TCP)
62. Protocolo de Control en Tiempo Real (RTCP)	Real Time Control Protocol RTCP
63. Protocolo de Datagramas de Usuario UDP	User Datagram Protocol UDP
64. Protocolo de Descripción de Sesión	Session Description Protocol (SDP)
65. Protocolo de Gestión de Claves MIKEY	Multimedia Internet KEYing (MIKEY)
66. Protocolo de Inicio de Sesión	Session Initiation Protocol (SIP)
67. Protocolo de Internet	Internet Protocol (IP)
68. Protocolo de Seguridad de la Capa de Transporte	Transport Layer Security (TLS)
69. Protocolo de Señalización	Signalling Protocol
70. Protocolo de Transporte en Tiempo Real	Real Time Protocol (RTP)
71. Protocolo De Transporte Seguro En Tiempo Real	Secure RTP (SRTP)
72. Protocolo Diffie-Hellman	Diffie-Hellman Key Agreement
73. Protocolo MSRP/Protocolo de Retransmisión de Mensajes	Message Session Relay Protocol (MSRP)
74. Proveedor de Servicios de Aplicaciones (PSA)	Application Service Provider (ASP)

ESPAÑOL	INGLÉS
75. Proxy de Entrada/Entrante	Inbound Proxy
76. Proxy de Salida/Saliente	Outbound proxy
77. Puenteo	Bridging
78. Punto a Punto	End-to-End
79. Punto de Referencia T (de terminal)	T- Reference Point
80. Punto Terminal	Endpoint
81. Red Corporativa de Próxima Generación	Next Generation Corporate Network (NGCN)
82. Red Corporativa de Telecomunicaciones:	Corporate/Enterprise Telecommunication Network (CN)
83. Red de Conmutación de Circuitos	Circuit-Switched Network
84. Red De Instalaciones Del Cliente	Customer Premises Network
85. Red de Próxima Generación	Next Generation Network (NGN)
86. Red de Valor Agregado	Value-Added Network
87. Red Digital de Servicios Integrados (RDSI)	Integrated Services Digital Network (ISDN)
88. Red Doméstica	Home Network
89. Red Heredada	Legacy Network
90. Red Privada Virtual	Virtual Private Network (VPN)
91. Red Telefónica Pública Conmutada (RTPC)	PSTN Public Switched Telephone Network
92. Reenvío de Llamadas	Onward Routing
93. Registro de Llamadas	Call Logging
94. Resiliencia	Resilience
95. Ruta de Señalización	Signalling Path
96. S/MIME: Extensiones de Correo de Internet de Propósitos Múltiples/Seguro	S/MIME: Secure Multipurpose Internet Mail Extension
97. Salto	Hop
98. Seguridad Extremo a Extremo	End-to-End Security
99. Señalización	Signalling
100. Servicio Centrex	Centrex Services
101. Servicios de Presencia	Presence Services
102. Servidor de Políticas	Policy Server
103. Servidor de Redirección	Redirect/Redirect Server
104. Servidor de Registro	Registrar
105. Servidor Proxy	Proxy/Proxy Server
106. Servidor STUN	Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators Server
107. Simple Traversal of User Datagram Protocol a través de Network Address Translators (NATs) STUN	STUN - Simple Traversal of UDP through NATs (STUN)
108. SIP URI	Session Initiation Protocol Uniform Resource Identifier
109. Softswitch/Conmutación por Software	Softswitch
110. SOHO "Oficina Pequeña, Oficina en Casa"	SOHO
111. Switch LAN	LAN Switch
112. Tiempo Real	Real-time, Real time, Realtime

ESPAÑOL	INGLÉS
113. Traduccion de Direcciones de Redes	Network Address Translation NAT
114. Traducción/Traductor de Direcciones de Red Transversal (NAT-T)	NAT Traversal
115. Transcodificación	Transcoding
116. Transferencia de Archivos	File Transfer
117. Túnel	Tunnel
118. Túnel VPN	VPN tunnel
119. URI de teléfono "tel"	Tel URI
120. Verificacion de Integridad	Integrity Check
121. Voz sobre Protocolo de Internet/Voice over Internet Protocol	VoIP, Voice over IP

ecma INTERNATIONAL

Technical Report

ECMA TR/91

1st Edition / December 2005

Enterprise Communication in Next Generation Corporate Networks (NGCN) involving Public Next Generation Networks (NGN)

Rue du Rhône 114 CH-1204 Geneva T: +41 22 849 6000 F: +41 22 849 6001

Technical Report

ECMA TR/91

1st Edition / December 2005

Enterprise Communication in Next Generation Corporate Networks (NGCN) involving Public Next Generation Networks (NGN)

Introduction

This Ecma Technical Report provides an overview of IP-based enterprise communication from/to Corporate telecommunication Networks (CNs) (also known as enterprise networks) including aspects of privately used home networks accessing public next generation networks (NGN).

This Technical Report is based upon the practical experience of Ecma member companies and the results of their active and continuous participation in the work of ISO/IEC JTC1, ITU-T, ETSI, IETF and other international and national standardization bodies. It represents a pragmatic and widely based consensus.

This Ecma Technical Report has been adopted by the General Assembly of December 2005.

Table of contents

1 Scope

This Technical Report identifies key use cases for communication with or between IP-based Next Generation Corporate Networks (NGCN) involving public next generation networks (NGN), analyses these use cases in terms of available or planned standardised technology and identifies requirements that will have to be met.

This Technical Report investigates configurations involving NGCNs and NGNs and their interoperating requirements. Non-IP-based interoperation, i.e. using circuit-switched technology, between NGCNs and NGNs is outside the scope of this Technical Report.

This Technical Report does not discriminate between wireless and wired access technology.

All mobility aspects are outside the scope of this Technical Report. They are covered by a companion Technical Report ECMA TR/92 [1].

Application considerations such as IP Centrex and CSTA (Computer Supported Telecommunications Applications) are outside the scope of this Technical Report.

2 References

[1] ECMA TR/92	Corporate Telecommunication Networks – Mobility for Enterprise Communication
[2] ECMA-307	Corporate Telecommunication Networks - Signalling Interworking between QSIG and H.323 - Generic Functional Protocol for the Support of Supplementary Services (June 2000)
[3] ITU-T Rec. H.323	Packet-based multimedia communications systems
[4] IETF RFC 3261	SIP: Session Initiation Protocol
[5] IETF RFC 3489	Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) (STUN)
[6] IETF RFC 3711	The Secure Real-time Transport Protocol (SRTP)
[7] IETF RFC 3761	The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)
[8] IETF RFC 3966	The tel URI for Telephone Numbers
[9] IETF RFC 2401	Security Architecture for the Internet Protocol (IPSEC)

3 Definitions

For the purposes of this Technical Report the following definitions apply:

3.1 Corporate telecommunication Network (CN) [2]

Sets of equipment (Customer Premises Equipment and/or Customer Premises Networks) that are located at geographically dispersed locations and are interconnected to provide telecommunication services to a defined group of users.

3.2 Next Generation CN (NGCN)

A self-contained corporate network designed to take advantage of emerging IP-based communications solutions and that can have its own applications and service provisioning.

3.3 Next Generation Network (NGN)

A packet based public network able to provide telecommunication services, able to make use of multiple QoS enabled transport technologies and in which service related functions are independent of underlying transport related technologies.

3.4 Virtual Private Network (VPN) [1]

Virtual network that can deliver ubiquitous and secure connectivity over a shared network infrastructure (e.g. public carrier networks) using the same access policies as an enterprise network.

3.5 Application Service Provider (ASP)

An entity that provides telecommunication applications.

3.6 Session Service Provider (SSP)

An entity that intervenes in and adds value to signalling for the establishment and control of multi-media sessions and optionally intervenes in and adds value to the multi-media sessions themselves.

3.7 Transport Service Provider (TSP)

An entity that provides IP connectivity.

4 Abbreviations

ALG	Application Layer Gateway
API	Application Protocol Interface
ASP	Application Service Provider
B2BUA	Back-to-Back User Agent
CN	Corporate telecommunication Network
CSTA	Computer Supported Telecommunications Applications
IP	Internet Protocol
IPSEC	IP Security
ISDN	Integrated Services Digital Network
NAT	Network Address Translator
NGCN	Next Generation Corporate Network
NGN	public Next Generation Network
RTP	Real-Time Protocol
QoS	Quality of Service
SBC	Session Border Controller
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SRTP	Secure Real-time Transport Protocol
SSP	Session Service Provider
TCP	Transmission Control Protocol
TE	Terminal Equipment
TLS	Transport Layer Security
TSP	Transport Service Provider
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server

UDP	User Datagram Protocol
VoIP	Voice over IP
VPN	Virtual Private Network

5 Background

There has been a major evolution in enterprise telecommunications during the last few years. Prior to that, enterprise telecommunication networks (or corporate telecommunication networks, CN) were based on 64 kbit/s circuit-switched technology, which had synergy with corresponding technology deployed in public Integrated Services Digital Networks (ISDN) and traditional analogue services. Those CNs primarily delivered a voice or telephony service to their users, although in principle they were capable of other services too, including video and various types of data service. For communication outside the enterprise, CNs were able to interwork with public ISDNs.

Many public networks also offered optional services to corporate customers, such as Centrex services and premise equipment leasing and maintenance.

With the advent of technologies for transmitting voice and other real-time media over the Internet Protocol (IP) (e.g., based on Real Time Protocol (RTP)) and corresponding new signalling protocols (e.g., H.323, SIP), there was potential for providing telephony and other real-time person-to-person services in the public Internet. Moreover, such services also became possible in the IP-based "intranets" already deployed in enterprises for data services such as corporate email, file transfer, corporate web services and access to the world wide web. Enterprises saw advantages such as savings on infrastructure costs (e.g., one wire to the desk) and the introduction of innovative services that exploited the convergence of real-time and data communication. The traditional PBX (Private Branch Exchange) was replaced by or evolved to an "IP-PBX" or soft switch that supported IP connectivity to the desktop and IP connectivity between nodes. Direct IP-based transmission of multimedia between endpoints meant that switching capabilities were no longer required, except gateways for interworking with "legacy" circuit-switched networks.

IP-based CNs are continuing to evolve, to support additional services, improved security, improved QoS, etc.. A CN that fully embraces IP technology is referred to here as a Next Generation CN (NGCN).

At present, NGCNs generally fall back to legacy circuit-switched techniques for communication outside the enterprise, e.g., using public ISDN or circuit-switching over leased lines. Gateways provide the necessary interworking of signalling and media.

The next stage of evolution will be for NGCNs to extend IP-based communication outside the enterprise by using a public network that also supports IP-based communication. The public IP-based network may provide communication between the NGCN and another NGCN, between the NGCN and another IP-based user (e.g., residential user) or, via a gateway in the public network, between the NGCN and a legacy user or network. With this the NGCN no longer needs gateways to legacy networks (except where required by existing investment or economic considerations) and can enjoy the benefits of end-to-end IP-based communication with appropriately equipped communication partners.

The public Internet is one example of a public IP-based network that an NGCN can use for external communications. In addition, some service providers are planning to offer public IP-based networks that offer improvements compared with the public Internet, e.g., in terms of QoS, security, mobility, applications, etc. These value added public IP-based networks are collectively known as Next Generation Networks (NGN).

This Technical Report aims to contribute to this next stage of evolution by looking at the issues involved in interoperating NGCNs and NGNs and to identify requirements on NGNs.

5.1 Provision of services by NGNs

5.1.1 Levels of service provision

An NGN may provide services to NGCNs and NGCN users at a number of different levels.

The most basic level of service provision is IP connectivity. Differentiation from the Internet can be in the form of improved or guaranteed quality of service or security. For the purposes of this Technical Report an NGN that provides this level of service acts as a Transport Service Provider (TSP).

A second level of service provision is in session establishment and control of communication sessions, e.g., voice, multimedia, messaging. Here the NGN adds value by being involved in the signalling protocol used to establish and control media sessions. For the purposes of this Technical Report the primary session control signalling protocol concerned is assumed to be the Session Initiation Protocol (SIP). Added value can include routing, provision of quality of service for media, provision of gateway services to legacy networks, assistance in NAT traversal, etc.. For the purposes of this Technical Report an NGN that provides this level of service is known as a Session Service Provider (SSP).

A third level of service provision is at the application level. Applications can be many and varied, but for the purposes of this Technical Report an application is assumed to be related to telecommunication in some way. An application may be able to monitor or control multi-media sessions (either directly or through a protocol or API such as CSTA) and may or may not be involved in media as well. Examples of applications that involve media include conferencing services, transcoding and translation services and call distribution centres. Examples of applications that monitor or control sessions but do not involve media include presence services, call logging services and UA configuration services. In addition, an application may be accessed through a session control protocol such as SIP. For the purposes of this Technical Report an NGN that provides this level of service is known as an Application Service Provider (ASP).

An NGN may provide services at one or more of these levels. Not all services offered will be of interest to enterprise customers and of relevance for interworking with NGCNs. Enterprise customers may use different NGNs for different levels of service provision and may have different contractual relationships with each of these NGNs. In addition, for a given communication and depending on the number of parties to be interconnected and/or the number of services to be accessed, multiple providers may be involved.

Figure 1 shows an example of one or more NGNs providing services at the three levels.

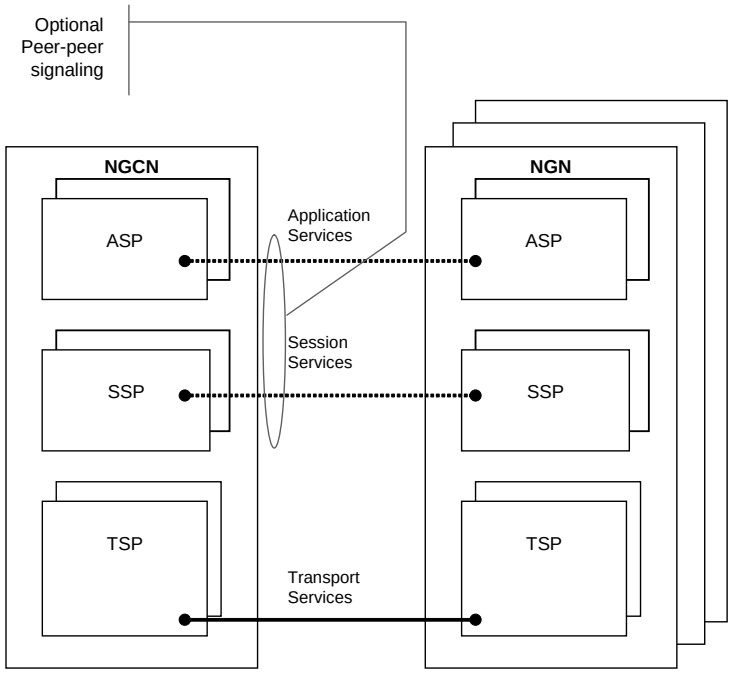


Figure 1 - TSP, SSP, and ASP provided by NGN(s)

5.1.2 Use of NGN services by NGCNs

In providing communication services to its users, an NGCN can make use of services of one or more NGNs. For communication with another entity (e.g., another NGCN or a residential user), an NGCN may make use of just TSP services, TSP and SSP services, or TSP, SSP and ASP services from the same NGN or different NGNs. In addition, an NGCN can make use of ASP services in their own right, rather than as part of communication with another entity (e.g., a presence service).

5.1.3 Home NGN

An NGCN customer may have contractual relationships with one or more NGNs for the provision of certain services, each NGN being known as the Home NGN for the services that it provides. Some parts of the NGCN may not have direct connectivity to the Home NGN and will need to access services of the Home NGN via other NGNs. The customer may have contractual relationships with those other NGNs too (e.g., just for IP connectivity) or reliance may be placed on agreements between the Home NGN and those other NGNs for such use.

Figure 2 shows an example of two parts of an NGCN, each part accessing services of the same Home NGN, one directly and the other via a different NGN. The solid lines represent connectivity and the broken lines represent service access.

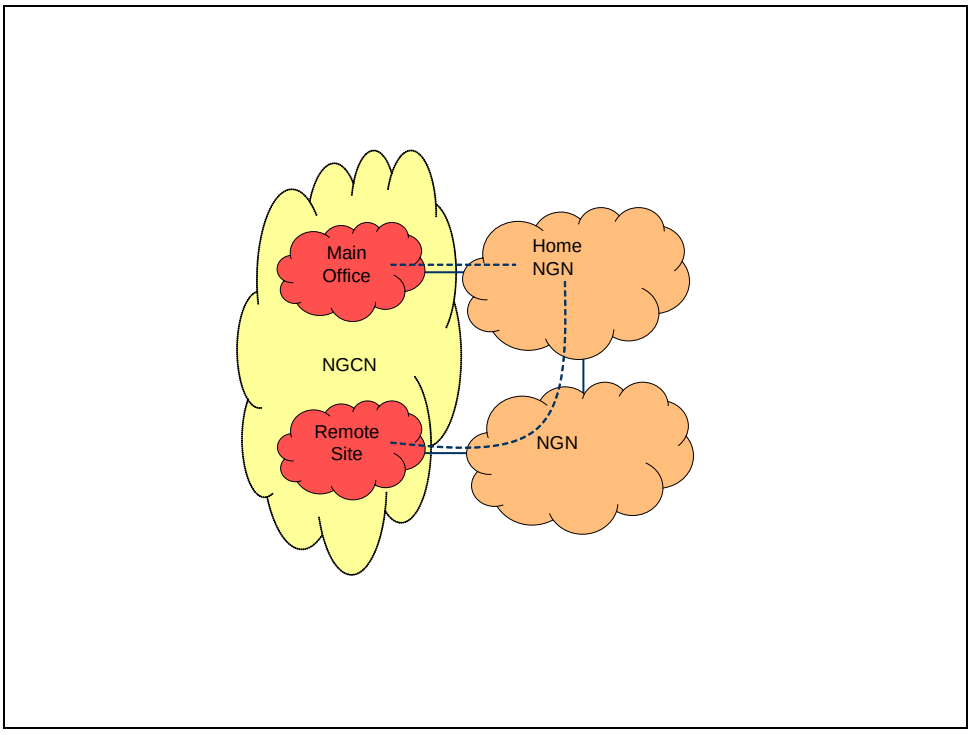


Figure 2 - Home NGN and other NGN

5.2 Management considerations

Services provided by an NGN may need to be managed from an NGCN. In addition, an NGN may provide a service for managing aspects of an NGCN. For both these purposes industry standard management interfaces should be used between the NGN and the NGCN. However, consideration of these interfaces is outside the scope of this edition of this Technical Report.

6 Basic Configurations and General Requirements

This clause lists important configurations which apply to an enterprise-specific next generation corporate network (NGCN) and its equipment (terminal equipment, servers, ...) when connected to public next generation networks (NGN). In addition, general requirements on NGN are specified in 6.6.

The following interconnection **Scenarios** will have to be considered:

- Scenario 1 - Communication between NGCNs via an NGN using a VPN

  Use cases: typically closely related partners

  - Two peer offices of one enterprise
  - Main office and branch office of an enterprise
  - Two closely-related enterprises (“extranet”)

- Scenario 2 - Communication between NGCNs via an NGN **not** using a VPN

  Use cases: typically **not** closely related partners

  - Two enterprises (not closely-related)

- Scenario 3 - Communication between NGCN and TE via an NGN using a VPN

  Use cases: typically closely related partners

  - Between enterprise and residential or SOHO user (e.g., home worker)

- Scenario 4 - Communication between NGCN and TE via an NGN **not** using a VPN

  Use cases: typically **not** closely related partners

  - Residential or SOHO user (e.g., member of public)

- Scenario 5 - Communication between NGCN and PSTN/ISDN via an NGN

Clause 7 discusses the Technical Issues and requirements for each of the main scenarios in detail.

6.1 Scenario 1 - Communication between NGCNs via an NGN using a VPN

Enterprise 1 and 2 are closely enough related to have a security association that allows use of a VPN, which provides a tunnel through which inter-NGCN signalling, media and other data can flow. The tunnel provides functions such as security, transparency for private IP addresses, NAT and firewall traversal, etc..

Typically this close relation is used between:

- Offices A and B of a single enterprise,
- Enterprise main office and branch office,
- An Enterprise 1 and a closely-related (e.g., partner) Enterprise 2.

Tunnel control may be directly between the NGCN(s) (i.e. tunnel control end-to-end) with no NGN involvement other than as a TSP, or tunnel control may be provided/owned by the NGN or a third party.

The NGN in this scenario acts only as TSP. Multiple TSPs within the NGN, e.g. one for each enterprise, may be involved.

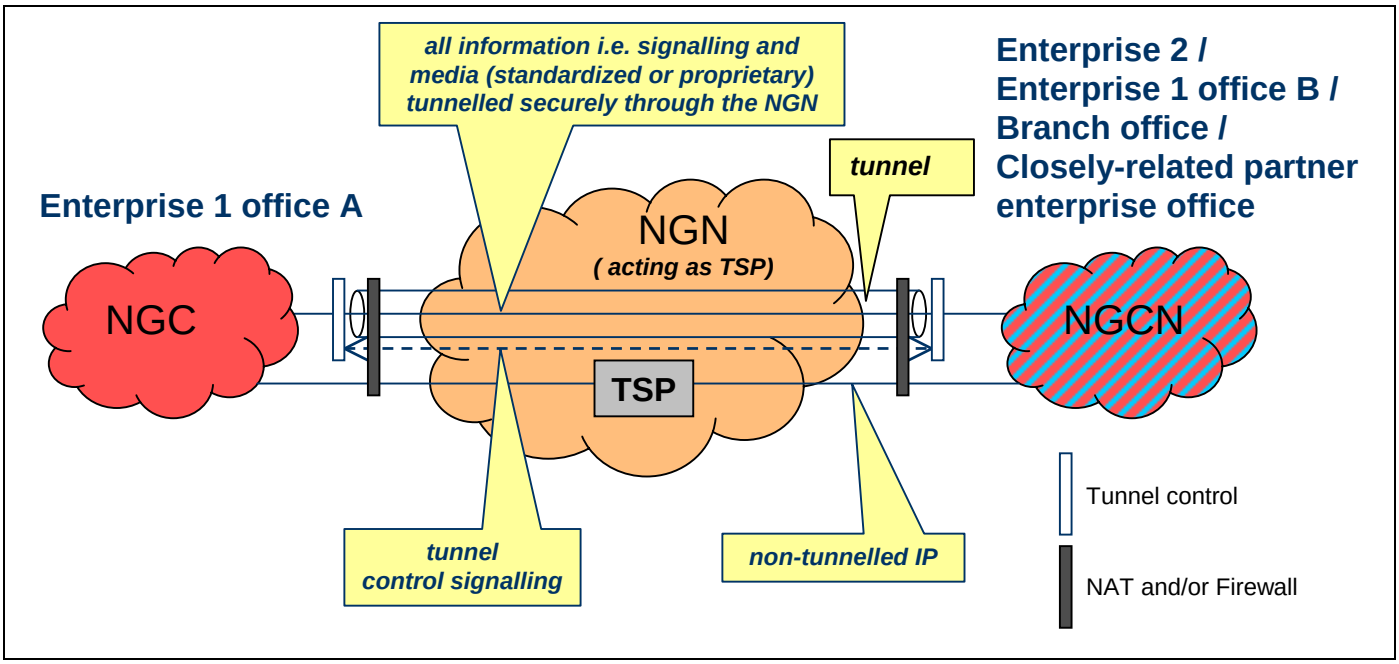


Figure 3 - Scenario 1 - Communication between NGCNs using a VPN

NAT and firewall at each end of the tunnel are optional, depending on the relationship between the two enterprises.

6.2 Scenario 2 - Communication between NGCNs via an NGN not using a VPN

This scenario typically applies to not closely related enterprises (i.e. no common security, no secure tunnel). It may also apply to closely related enterprises (or even between two locations of the same enterprise) if, due to whatever reasons, they are not able to establish a tunnel through the NGN.

The NGN in this scenario as a minimum acts as a TSP. It may also act as a SSP (provision of session services) and/or as an ASP (provision of applications such as conference, presence, voice mail, unified mail, etc.). Depending on the number of services to be accessed also multiple TSPs, SSPs and/or ASPs may be involved.

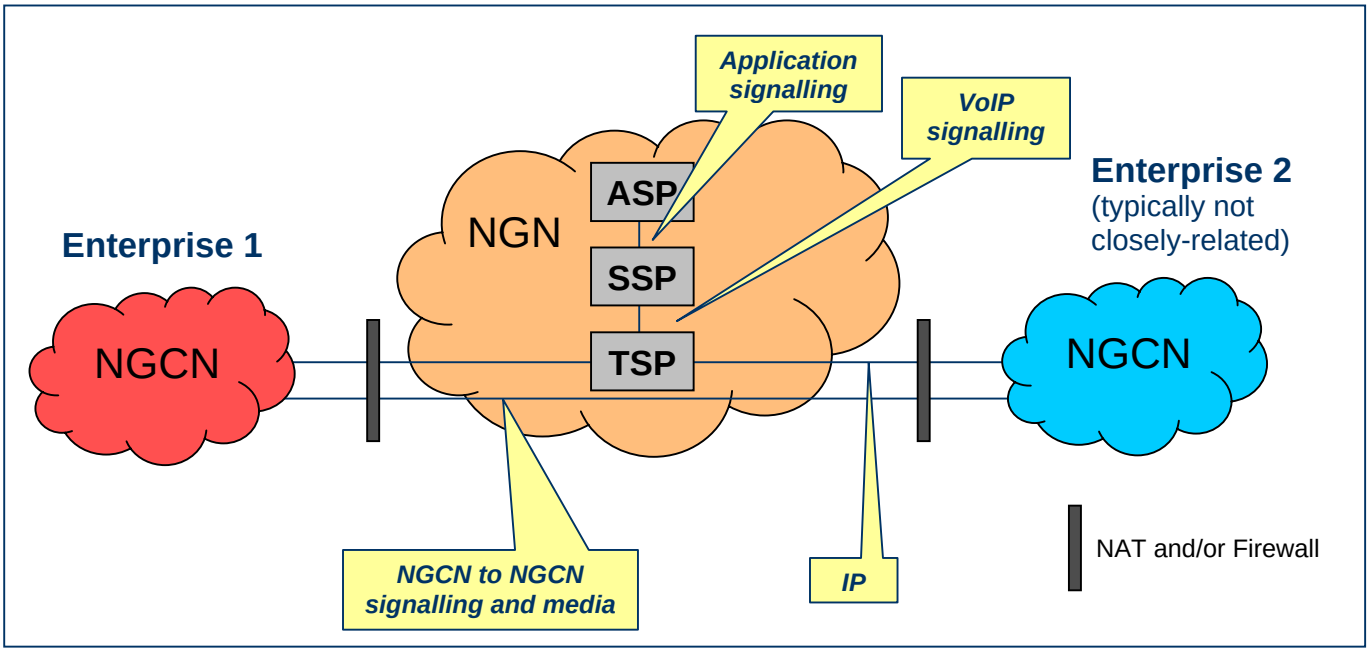


Figure 4 - Scenario 2 - Communication between NGCNs not using a VPN

6.3 Scenario 3 - Communication between NGCN and TE via an NGN using a VPN

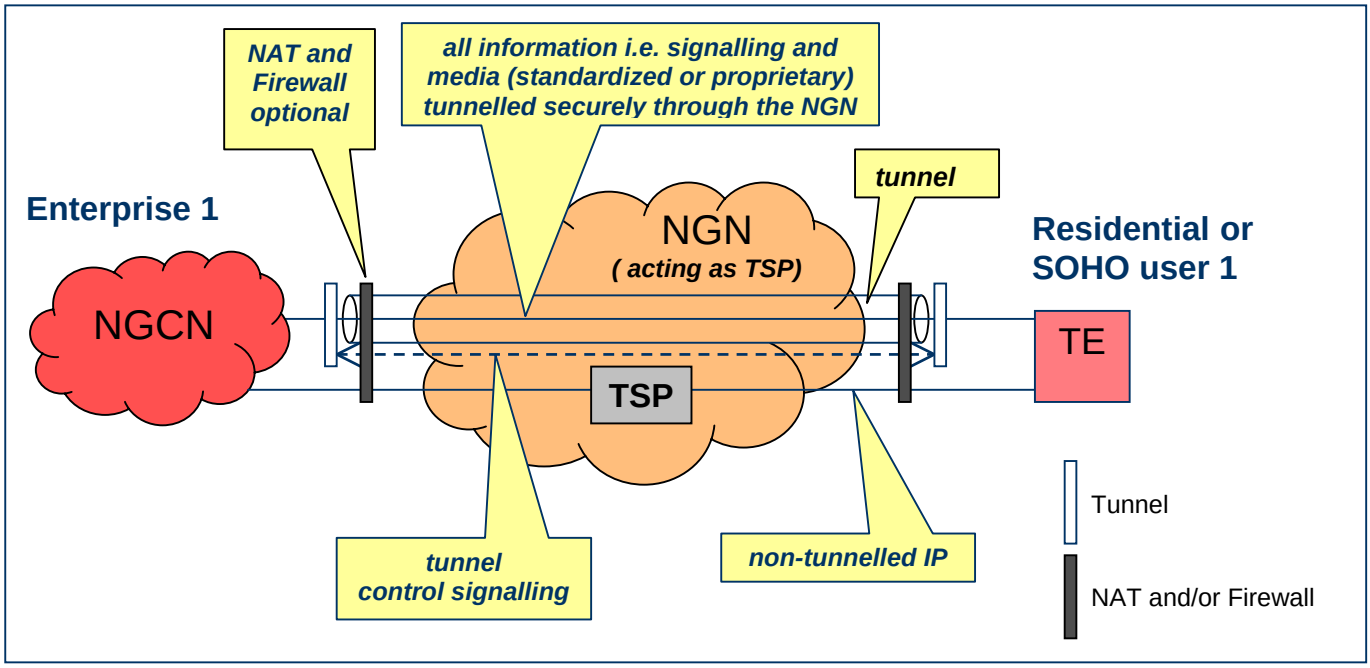


Figure 5 - Scenario 3 - Communication between NGCN and TE using a VPN

NAT and firewall for the tunnel are optional, depending on the relationship between enterprise and TE.

6.4 Scenario 4 - Communication between NGCN and TE via an NGN not using a VPN

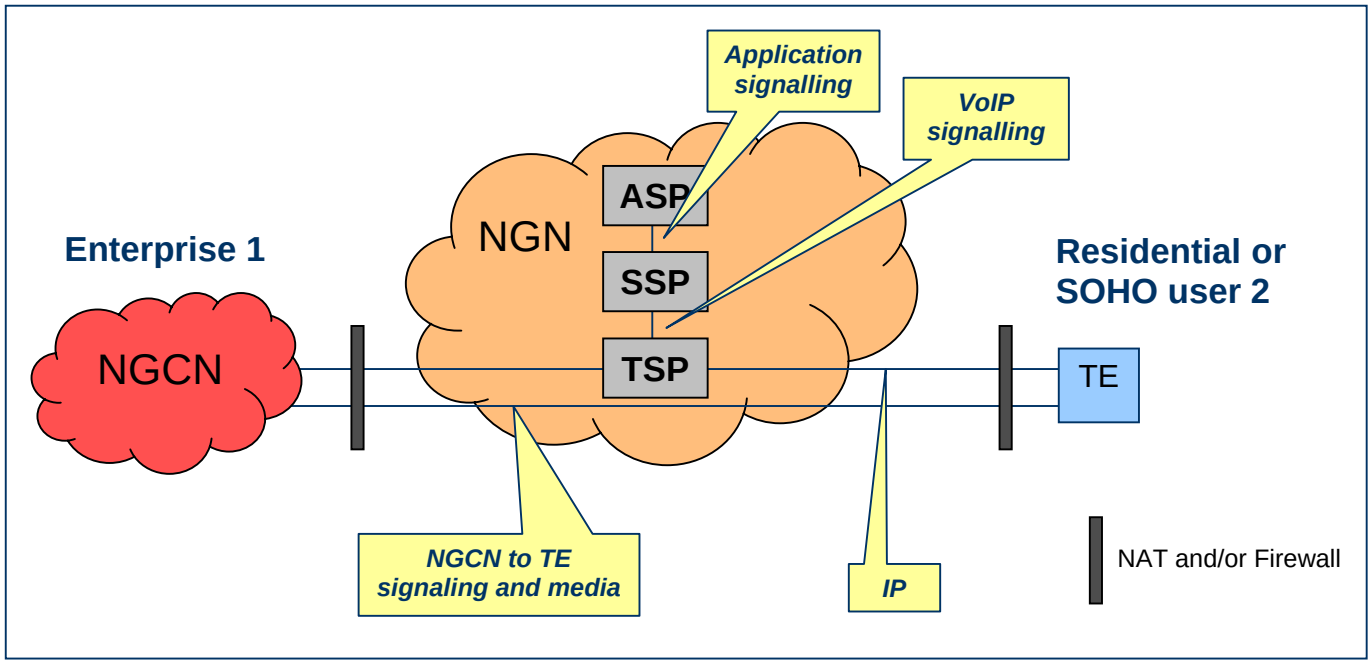


Figure 6 - Scenario 4 - Communication between NGCN and TE not using a VPN

6.5 Scenario 5 - Communication between NGCN and PSTN/ISDN via an NGN

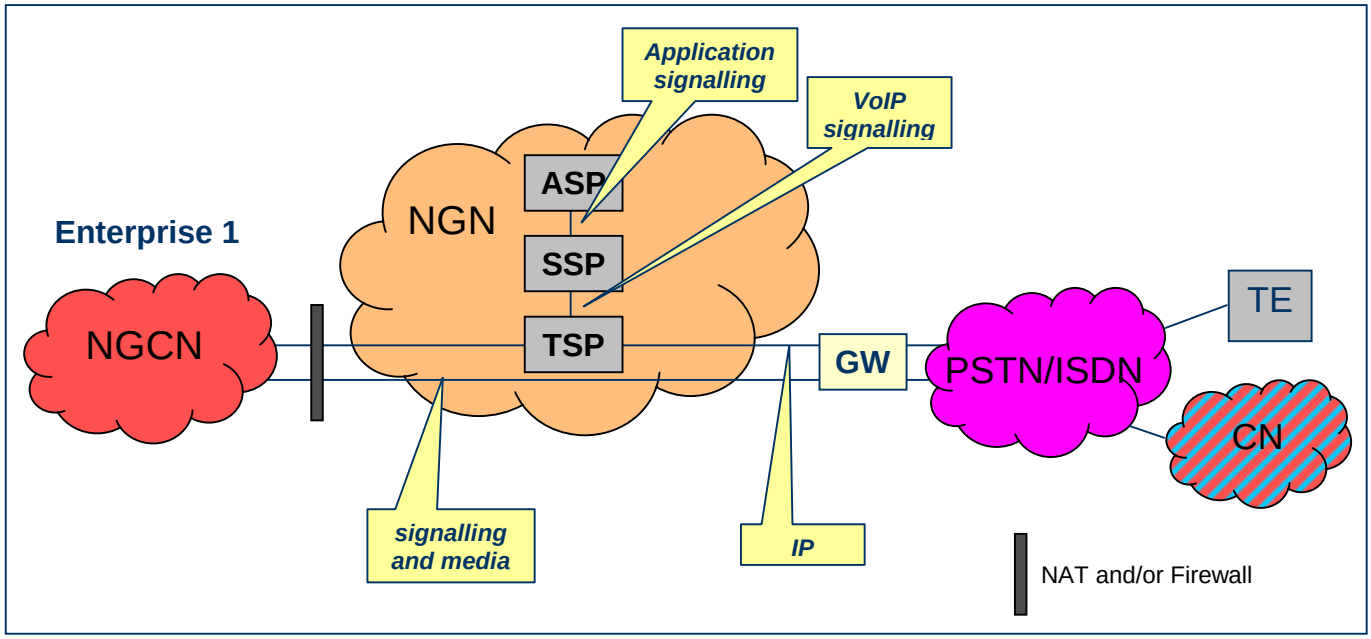


Figure 7 - Scenario 5 - Communication between NGCN and PSTN/ISDN via an NGN

The gateway (GW) may be provided by the NGN as part of its SSP or it may be a 3rd party gateway.

6.6 General requirements on NGNs

In order to support communications involving NGCNs, NGNs need to meet certain requirements. Some generic requirements are identified here. These requirements will apply in different ways to some or all of the scenarios identified in clause 6 and influence the technical considerations of clause 7. Where an NGN is mentioned, this can be either a single NGN or a number of cooperating NGNs.

REQUIREMENT ON NGN 1: An NGN shall support communication sessions established in either direction between an NGCN user and a user in another NGCN, a user in the NGN or a user in a PSTN/IDSN accessed via a gateway in the NGN.

REQUIREMENT ON NGN 2: An NGN shall allow the use of any IP-based media during a communication session subject to the availability of resources and contractual arrangements.

REQUIREMENT ON NGN 3: Except where explicitly agreed with the NGCN (by signalling or contract) or because of formal legal requirements, an NGN shall not intervene in media transport above the transport layer.

NOTE
Functions such as transcoding, translation and bridging can be provided where agreed.

NOTE
The applicability of formal legal requirements may depend on whether media is transported between two parts of the same NGCN (i.e., within an enterprise) or outside the enterprise.

REQUIREMENT ON NGN 4: An NGN shall offer service level agreements in which quality of service of media, signalling and other data is fit for enterprise use.

REQUIREMENT ON NGN 5: An NGN shall provide industry standard functionality for assisting with traversal of commonly encountered NAT arrangements at an NGCN boundary.

NOTE
In general the endpoint should be responsible for signalling IP addresses and ports that are suitable for use by the remote endpoint, but to achieve this the NGN may need to provide functionality such as a STUN server.

REQUIREMENT ON NGN 6: An NGN shall support identification of users and services by means or SIP or SIPS URIs and optionally by means of telephone URIs, when not in conflict with available end point user contractual or privacy settings.

REQUIREMENT ON NGN 7: An NGN shall provide authenticated caller identity to an NGCN when available, or an appropriate and meaningful datum when not.

REQUIREMENT ON NGN 8: An NGN shall be able to pass an authenticated caller identity from an NGCN towards a called user during call establishment and call re-arrangements.

REQUIREMENT ON NGN 9: An NGN shall offer a standard SIP signalling interface to an NGCN based on standards track RFCs from the IETF.

REQUIREMENT ON NGN 10: Except when providing a gateway to PSTN/ISDN or an application service, an NGN shall be transparent to signalling that is of an end-to-end nature and shall be tolerant of any that is not supported.

NOTE
This includes SIP bodies and certain SIP headers. In the case of SDP bodies the NGN is required to be tolerant of unsupported SDP extensions and next generation SDP.

REQUIREMENT ON NGN 11: When transporting signalling messages, an NGN shall not carry out actions that will invalidate cryptographic integrity checks on parts of messages intended for delivery unchanged, except when required by local regulation.

NOTE
The applicability of formal legal requirements may depend on whether signalling is transported between two parts of the same NGCN (i.e., within an enterprise) or outside the enterprise.

REQUIREMENT ON NGN 12: When transporting signalling messages, an NGN shall allow end-to-end information to be encrypted and shall not require access to the key.

NOTE
Examples are geographic location information and key information for media security. Where certain parts of encrypted end-to-end data need to be accessed, the NGCN should arrange for this to be delivered separately, either encrypted (for decryption by the NGN) or unencrypted.

REQUIREMENT ON NGN 13: An NGN shall be able to provide optional security (encryption, authentication and integrity checking) of signalling services at the NGCN-NGN interface.

REQUIREMENT ON NGN 14: An NGN shall be able to provide security (encryption, authentication and integrity checking) of signalling on each signalling hop between communication partners on request and each NGN shall be able to provide to the NGCN evidence that this is provided.

NOTE
This can be provided through use of the SIPS URI scheme.

REQUIREMENT ON NGN 15: An NGN shall permit media to be secured (encrypted, authenticated and integrity checked) end-to-end.

REQUIREMENT ON NGN 16: An NGN shall permit key management for the purpose of media encryption to take place within signalling between the end devices.

NOTE
Key management exchange between an NGCN user and an NGN intermediary will often be unacceptable to NGCN users and their partners. For example, a residential user calling a bank may require authentication based on a bank-provided certificate before talking. See REQ3 and REQ11.

REQUIREMENT ON NGN 17: An NGN shall be able to provide advice of charge information to an NGCN at the time charges are incurred.

6.7 General requirements on NGNs concerning measures for compliance with regulations

Potential issues for regulatory authorities and administrations are: emergency services, (including emergency telecommunication and disaster relief), lawful interception and privacy (to be considered in the context of presentation of business user's or terminal's identity, name, address and location information).

Several regulatory authorities, e.g. in the USA and in Europe, have started consultations on a regulatory framework for the provision of public VoIP-services.

However, at the time of preparation of this Technical report it is not clear, whether or to what extent enterprise networks and in particular their internal communications traffic will be affected by those regulations that already apply to public network operators (e.g. on lawful interception, data retention). Beyond that, it is a still an open issue how to define the boundaries of an enterprise network, which, especially in the case of remote access, could share the network infrastructure of a universal services provider to which regulations apply. The challenge is how to handle such virtual enterprise networks.

NOTE
In a circuit switched environment the T-reference point acted as demarcation between private and public network infrastructures and thus the boundary for regulation.

It is expected that enterprise networks, including virtual enterprise networks, will not be subject to more regulation than circuit switched enterprise networks.

REQUIREMENT ON NGN 18: An NGN shall be able to discriminate between normal traffic and intra-enterprise traffic when applying measures for complying with regulations, thus keeping enterprise network internal communications free from any unwanted intervention.

7 Technical issues and requirements on NGN related to session service provision

In order to realise the configurations identified in clause 6, certain technical issues will arise. This clause discusses these technical issues in general terms and also in relationship to specific configurations and derives requirements on NGN in addition to those identified in 6.6. This edition of this Technical Report addresses only certain fundamental technical issues, and there are other technical issues that may need further consideration, e.g., charging, routing, transcoding, performance, performance monitoring, resilience, etc., and also applications such as presence.

The issues are discussed with particular reference to SIP-based multi-media communication, but generally apply to any form of multi-media communication, e.g., communication based on H.323 signalling.

7.1 Signalling architecture

Basically SIP is a protocol that operates between two endpoints known as User Agents (UAs), enabling those UAs to establish a communication session comprising one or more media connections (i.e. bearer streams) such as audio, video, fax, instant messaging or real-time text. A session is established by exchanging session descriptions in accordance with the Session Description Protocol (SDP) within SIP messages. Session descriptions indicate factors such as the media to be used, codecs, packet rates, security contexts and IP addresses and port numbers for media reception.

In principle, SIP can operate directly between two UAs. However, the SIP standards do define other SIP entities that can assist. In particular the main SIP standard [4] defines the concept of a location service at which UAs can register to assist in locating UAs representing a particular user. Related to this are the concepts of a registrar (a SIP entity that registers UAs at the location service) and a proxy (a SIP entity that queries the location service in order to assist in the forwarding of requests to appropriate UAs).

NOTE
Also there is a redirect, which is similar to a proxy but redirects rather than forwards requests. For the purposes of this Technical Report a redirect is treated as a proxy unless otherwise stated.

The handling of a SIP request from one UA (the UA client, UAC) to another UA (the UA server, UAS) typically passes through a proxy, which queries the location service in order to locate UAs that might be able to handle the request. Also the UAC often sends requests to a local proxy, known as an outbound proxy) in order to reduce the routing burden on the UAC. This gives rise to the typical SIP trapezoid involving two UAs and two proxies (see Figure 9).

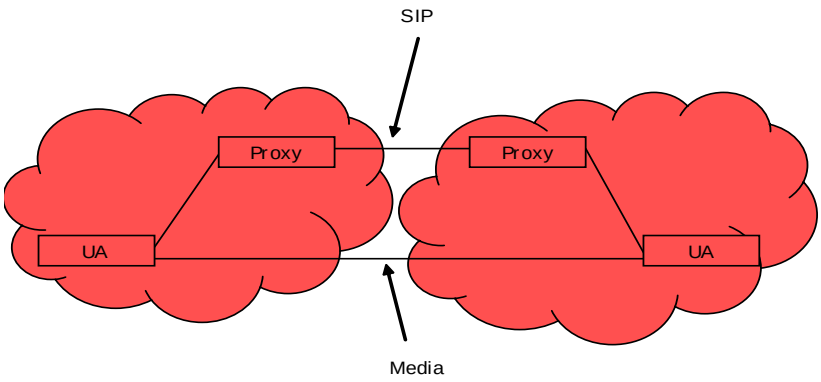


Figure 8 – Typical SIP trapezoid

Sometimes a SIP request can result in the formation of an association between two UAs, in the context of which further SIP requests in either direction can be sent. This is known as a dialog. The most important dialog in SIP is that initiated by an INVITE request, because such a dialog has an associated session, comprising a collection of media between the UAs. An INVITE-initiated dialog and its associated session can be regarded as a call. Proxies involved in routing the dialog-initiating request may or may not remain involved in the dialog for routing subsequent requests.

Typically a proxy is collocated with a location service and a registrar, so the whole entity tends to be known as a proxy. The behaviour of a proxy is standardised in SIP [4] and other SIP RFCs and its behaviour is quite tightly constrained by the standards in order not to jeopardise the end-to-end character that is fundamental to much of SIP.

Although not defined in the SIP [4] the market has found the need for an entity known as a Back-to-Back User Agent (B2BUA). In some respects a B2BUA acts like a proxy, being an intermediate entity on a signalling path between two UAs, but in other respects a B2BUA acts as two UAs back-to-back. The behaviour of a B2BUA is not standardised, and because it is not constrained by standards a B2BUA can behave more flexibly than a proxy. This allows a B2BUA to fulfil certain roles that a proxy cannot (e.g., by offering transcoding capabilities for media). On the other hand by not behaving as a proxy a badly designed B2BUA can behave in ways that are inconsistent with the expectations of UAs and can cause problems.

Other forms of entity that can intervene either actively or passively in a SIP signalling path include Application Layer Gateways (ALGs) and Session Border Controllers (SBCs). These have knowledge of the SIP protocol and can monitor or modify it for certain purposes, e.g., control of NATs and firewalls, security, privacy, etc..

In the rest of this clause, the term SIP intermediary is used to refer to any intermediate entity involved either actively or passively in SIP signalling between two UAs, including but not limited to proxies, B2BUAs, ALGs and SBCs.

As stated above, SIP can in principle operate directly between UAs, and indeed there is a lot of interest at present in peer-to-peer (P2P) SIP where SIP intermediaries are eliminated. Whether and how soon this ideal will be realised is open to speculation, but the trend is expected to be away from the TDM concept of signalling passing through an arbitrary number of intermediaries (e.g., associated with switches) towards a lightweight solution with a minimal number of SIP intermediaries. There should generally be no need for more SIP intermediaries than in the typical SIP trapezoid mentioned above. An excessive number of SIP intermediaries can have the negative impact of adding to signalling delays (e.g., during call establishment). Also undue intervention by any SIP intermediary can have a harmful effect by not complying with the expectations of UAs.

These lead to general requirements on NGNs that act as SSPs as follows. More specific requirements apply in the context of specific scenarios and specific technical issues.

REQUIREMENT ON NGN 19: SIP intermediaries in a signalling path should be kept to a minimum.

REQUIREMENT ON NGN 20: A SIP intermediary in an NGN shall behave in a way that is not harmful to UAs that are trying to communicate through it. A SIP intermediary that obeys all the rules of a proxy would be compliant with this. This includes transparency to SIP signalling information that is not relevant to the intermediary, including any unsupported SIP extensions (standardised or proprietary).

The above requirements apply also where two or more NGNs in series act as SSPs for a given communication.

Although SIP signalling typically passes through one or more SIP intermediaries, media in general flow directly between the UAs concerned, with no involvement of intermediaries above the transport layer (intermediaries such as NATs and firewalls can be involved up to the transport layer). The exception to this is when an intermediary performs some function on the media such as transcoding, translating or bridging, in which case the intermediary really acts as two or more UAs in a back-to-back arrangement (similar to and perhaps coincident with a SIP B2BUA).

7.1.1 Scenario 1 - Communication between NGCNs using a VPN

Two SIP intermediaries, one in each part of the NGCN, should suffice. The NGN acts only as a TSP. In any case, encryption through the tunnel will mean that the NGN cannot provide any SIP intermediaries. Media as well as SIP signalling will flow through the tunnel.

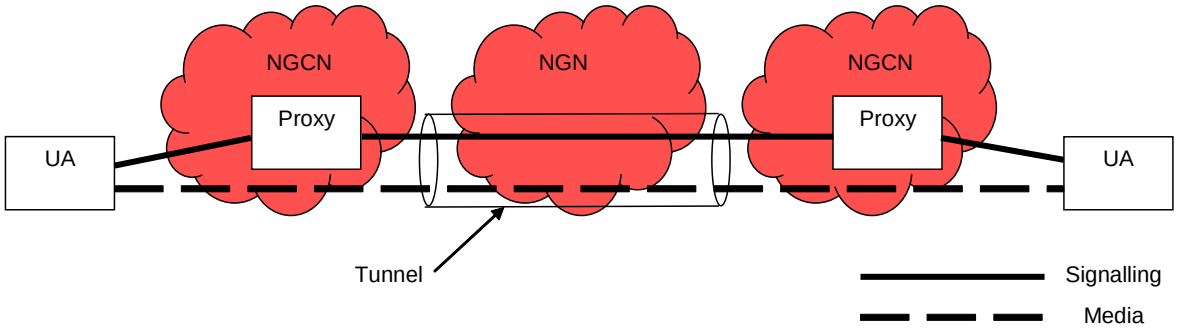


Figure 9 - Typical signalling architecture for scenario 1

7.1.2 Scenario 2 - Communication between NGCNs not using a VPN

Two SIP intermediaries, one in each NGCN, should in principle suffice. SIP intermediaries in the NGN should be provided only if they allow the NGN to add value, e.g., by providing QoS guarantees for media. SIP intermediaries in the NGN should be transparent to SIP signalling information that is not relevant to those intermediaries, including any unsupported SIP extensions (standardised or proprietary). Whether or not the NGN provides any SIP intermediaries, media may or may not flow via the same NGN.

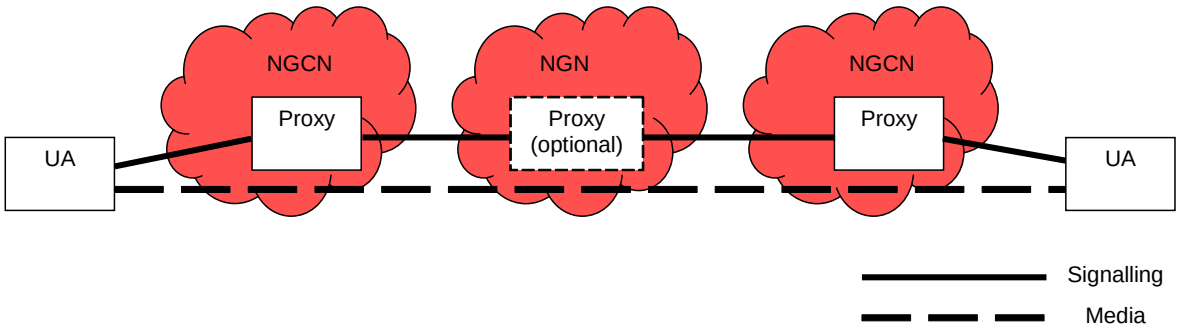


Figure 10 - Typical signalling architecture for scenario 2

7.1.3 Scenario 3 - Communication between NGCN and TE using a VPN

SIP intermediaries should be confined to the NGCN. The NGN acts only as a TSP. The TE will incorporate a UA that communicates with an inbound / outbound proxy or other intermediary in the NGCN via the tunnel. Media as well as SIP signalling will flow through the tunnel.

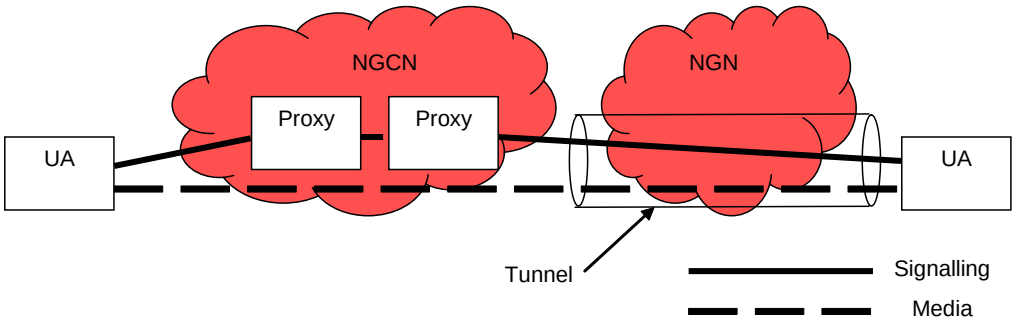


Figure 11 - Typical signalling architecture for scenario 3

7.1.4 Scenario 4 - Communication between NGCN and TE not using a VPN

Two SIP intermediaries, one in the NGCN and one in the NGN, should suffice. Additional SIP intermediaries in the NGN should be provided only if they allow the NGN to add value, e.g., by providing QoS guarantees for media. SIP intermediaries in the NGN should be transparent to SIP signalling information that is not relevant to those intermediaries, including any unsupported SIP extensions (standardised or proprietary). Media may or may not flow through the same NGN.

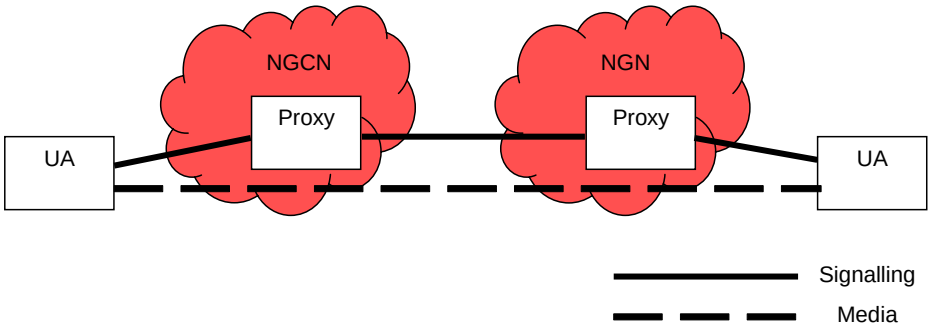


Figure 12 - Typical signalling architecture for scenario 4

7.1.5 Scenario 5 - Communication between NGCN and PSTN/ISDN

Two SIP intermediaries, one in the NGCN and one in the NGN, should suffice. The SIP intermediary in the NGN will act as the inbound / outbound proxy for the gateway UA. Additional SIP intermediaries in the NGN should be provided only if they allow the NGN to add value. Media may or may not flow through the same NGN.

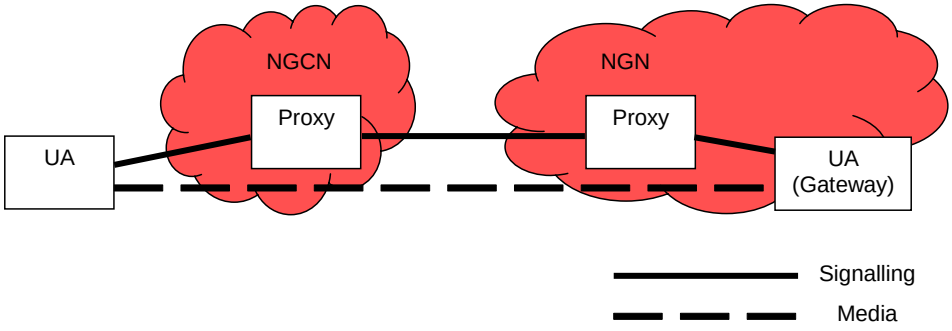


Figure 13 - Typical signalling architecture for scenario 5

7.2 NAT traversal

Network Address Translation (NAT) devices are typically present at network borders to provide a binding, typically on a temporary basis, between IP addresses and ports belonging to the internal address space and IP addresses and ports belonging to the external address space. A NAT provides several benefits to the network concerned, including provision of a larger address space internally without using a corresponding amount of public address space and the firewall effect of not allowing packets to flow from the external network to the internal network (inbound) without first opening a binding by transmitting packets from the internal network to the external network (outbound).

NAT traversal can be a significant issue for SIP-based communication, firstly because SIP signalling may need to traverse a NAT and secondly because media streams may need to traverse a NAT.

7.2.1 NAT traversal for SIP signalling

The first NAT traversal problem concerns SIP signalling. In general this is not a problem if communication is initiated from inside the NAT, since the first outbound packet will open a binding, which will then apply to both outbound and inbound packets.

For the typical transport mechanism, Transmission Control Protocol (TCP) (including Transport Layer Security (TLS) over TCP), this means the connection must be established in the outbound direction. It also means the connection must be retained even after completion of any outbound transactions (outbound request and inbound response) in case inbound requests arrive subsequently. By refreshing a connection periodically, NAT bindings can be kept alive. Where there are multiple SIP entities on one side or both sides of the NAT. Multiple TCP connections might need to be established and maintained for load sharing purposes.

For User Datagram Protocol (UDP), an initial packet must be sent outbound to open the binding. Because a response is not associated at the transport level with the request, the response to an outbound request needs to be sent explicitly to the port from which it was received rather than to the port indicated in the Via header of the SIP request. Keep-alive packets need to be sent periodically to keep the binding open for inbound requests. Because of the unreliability of UDP and its inability to be secured by TLS and also the limited maximum payload size of UDP, it is considered an unlikely transport protocol for NGN access and therefore is not considered further in this Technical Report.

7.2.1.1 Scenario 1 - Communication between NGCNs using a VPN

NAT traversal should not be an issue if the VPN tunnel links two parts of an NGCN sharing the same IP address space, even though the VPN may extend across any number of NATs.

If the VPN tunnel links two parts of an NGCN having different IP address spaces (e.g., two closely related enterprises), this is equivalent to the use of NATs between different parts of an NGCN when there is no intervening NGN. Since it is not an issue arising from the involvement of an NGN, it is considered outside the scope of this Technical Report.

7.2.1.2 Scenario 2 - Communication between NGCNs not using a VPN

In this scenario there is a need for SIP requests to be sent from the SIP intermediary in one NGCN to the SIP intermediary in the other NGCN. In this scenario it is likely that a NAT will exist at the boundary between an NGCN and the NGN and likewise between the peer NGCN and the NGN. Assuming the NGCN SIP intermediaries are located on the internal side of their respective NATs, SIP requests (and responses) may have to traverse two NATs. Each NGCN SIP intermediary must therefore have a globally routable IP address (or an IP address from the address space in use within the NGN) in order to receive SIP requests from SIP intermediaries in other NGCNs and each NAT must be configured to allow unsolicited inbound packets from any source to be mapped through to the appropriate internal IP address and port of the SIP intermediary. Otherwise unsolicited SIP requests would be unable to reach the SIP intermediary. A SIP intermediary cannot know where unsolicited requests will come from and therefore cannot open NAT bindings in advance by issuing outbound packets.

Alternatively the SIP intermediary could be located on the external side of the NAT, i.e., between the NAT and the NGN. In this case NAT traversal is an intra-NGCN matter.

Additional considerations will apply where requests pass through multiple NGNs having different IP address spaces or when SIP intermediaries exist within the NGN(s).

7.2.1.3 Scenario 3 - Communication between NGCN and TE using a VPN

The considerations of 7.2.1.1 apply, where the TE acts as a part of the NGCN.

7.2.1.4 Scenario 4 - Communication between NGCN and TE not using a VPN

In this scenario there is a need for SIP requests to be sent from the SIP intermediary in the NGCN to the SIP intermediary in the NGN and vice versa. It is likely that a NAT will exist at the boundary between the NGCN and the NGN. Assuming the NGCN SIP intermediary is located on the internal side of its NAT, SIP requests (and responses) have to traverse the NAT. The NGCN SIP intermediary must therefore have a globally routable IP address (or an IP address from the address space in use within the NGN) in order to receive SIP requests from SIP intermediaries in the NGN and the NAT must be configured to allow unsolicited inbound packets from any source to be mapped through to the internal IP address and port of the NGCN SIP intermediary. Otherwise unsolicited SIP requests would be unable to reach the NGCN SIP intermediary. It is assumed that the NGCN SIP intermediary cannot know where unsolicited requests will come from and therefore cannot open NAT bindings in advance by issuing outbound packets.

Additional considerations will apply where requests pass through multiple NGNs having different IP address spaces or when SIP intermediaries exist within the NGN(s).

7.2.1.5 Scenario 5 - Communication between NGCN and PSTN/ISDN

Considerations are similar to scenario 4.

7.2.2 NAT traversal for media streams

The second and more serious issue with NAT traversal concerns media streams. IP addresses and ports for reception of media are signalled in SIP messages using the Session Description Protocol (SDP). If an internal UA signals its reception IP address and port to an external UA, the internal IP address and port will in general be useless to the external UA. The address and port may not exist in the external address space or they may be assigned to a different device. Therefore the external IP address and port need to be signalled in SDP. To do this the internal UA needs to discover its external IP address and port.

For most situations in which the medium is transported over UDP, STUN (Simple Traversal of UDP through NATs) [5] provides an adequate means of discovering the IP address and port. The internal UA sends a request to a STUN server in the external network and the STUN server responds with the IP address and port from which the request appeared to have come, i.e., the external IP address and port. This requires a STUN server in the external network. The act of sending a STUN request will open a NAT binding if one did not already exist, and this same NAT binding is used for the medium itself. There are a few NAT types for which this does not work, but these are believed to be quite uncommon.

NOTE
In particular it does not work for the NAT type commonly known as "symmetric", where a binding is to a particular address and port on the public side, and therefore a binding opened to the STUN server cannot be used for media from a different address and port.

Although STUN provides a means of discovering the external IP address and port, there is a further issue of determining whether NAT traversal is applicable, since if the peer UA is internal the internal IP address and port should be used, and not the external IP address and port. Furthermore, if the internal network has interfaces to more than one external network, different NAT bindings will apply to each and it is important to know which external network applies and obtain the external IP address and port applicable to that external network. Further complications arise if more than one NAT is traversed between the two UAs. Most of these problems can be solved if the UAs concerned implement ICE (Interactive Connectivity Establishment) (ongoing work in the IETF), which provides a means for candidate IP addresses and ports to be tested before use.

Other considerations apply to media transported over TCP, e.g., text messages within the context of a session in accordance with the Message Session Relay Protocol (MSRP) (ongoing work in the IETF). These are not addressed in this edition of this Technical Report.

Another approach sometimes taken to solve the problem of NAT traversal for media streams is the use of an Application Layer Gateway (ALG) that is on the SIP signalling path (it may be combined with a SIP intermediary, for example) and opens NAT bindings and adjusts SDP addresses and ports accordingly. This is contrary to SIP architectural principles, since it requires examination and modification of a SIP body (SDP) by a SIP intermediary. In particular, examination will fail if the body is encrypted and modification will fail if the body is integrity protected. Therefore this approach cannot be recommended.

Yet another approach involves the use of a policy server accessed by UAs to establish NAT bindings (see 7.7).

7.2.2.1 Scenario 1 - Communication between NGCNs using a VPN

The considerations in 7.2.1.1 apply.

7.2.2.2 Scenario 2 - Communication between NGCNs not using a VPN

For a medium transported over UDP, each UA must determine the external IP address and port corresponding to the internal IP address and port on which that medium will be received and include this in SDP offer or answer to the peer UA. The use of ICE may be required to determine whether this is required. Each UA will need to use a STUN server in the NGN to discover its own external IP address and port.

REQUIREMENT ON NGN 21: The NGN is required to provide a STUN server.

Alternatively the UAs may make use of policy servers (see 7.7).

7.2.2.3 Scenario 3 - Communication between NGCN and TE using a VPN

The considerations in 7.2.1.3 apply.

7.2.2.4 Scenario 4 - Communication between NGCN and TE not using a VPN

For a medium transported over UDP, a UA in the NGCN must determine the external IP address and port corresponding to the internal IP address and port on which that medium will be received and include this in SDP offer or answer to the peer UA. The use of ICE may be required to determine whether this is required. The NGCN UA will need to use a STUN server in the NGN to discover its own external IP address and port. The use of ICE requires corresponding support at UAs in the NGN.

Alternatively the UAs may make use of policy servers (see 7.7).

7.2.2.5 Scenario 5 - Communication between NGCN and PSTN/ISDN

For a medium transported over UDP, a UA in the NGCN must determine the external IP address and port corresponding to the internal IP address and port on which that medium will be received and include this in SDP offer or answer to the gateway. The use of ICE may be required to determine whether this is required. The NGCN UA will need to use a STUN server in the NGN to discover its own external IP address and port. The use of ICE requires corresponding support at the gateway.

Alternatively the UAs may make use of policy servers (see 7.7).

REQUIREMENT ON NGN 22: Gateways in an NGN may need to support ICE.

7.3 Firewall traversal

Firewalls are generally present at network borders to prevent unwanted traffic across the border, particularly incoming traffic. NATs also provide a partial firewall capability by virtue of not allowing bindings to be opened by requests from the external side to the internal side, and this is dealt with in 7.1. Firewalls can impose additional restrictions, some of which can be harmful to SIP-based multi-media communication (e.g., the denial of all UDP traffic).

In general, the opening of firewall holes by sending initial packets from inside the firewall to outside the firewall will help. This needs to be done anyway for NAT traversal.

Firewalls can normally be expected to be configured to allow SIP signalling to pass through, since SIP signalling normally involves specific SIP intermediary IP addresses and specific port numbers. Media streams are likely to be a far bigger problem because port numbers are chosen dynamically and it is unlikely that firewalls will keep holes open for the full range of possibilities.

If firewalls can be opened in each direction by sending an initial packet in the outbound direction, then this might be an acceptable solution. Sending and receiving on the same port is generally a pre-requisite for this to work.

An approach sometimes taken to solve the problem of firewall traversal for media streams is the use of an Application Layer Gateway (ALG) that is on the SIP signalling path (it may be combined with a SIP intermediary, for example) and opens firewall holes based on IP addresses and ports in SDP bodies of SIP messages. This is contrary to SIP architectural principles, since it requires examination of a SIP body (SDP) by a SIP intermediary. In particular, examination will fail if the body is encrypted. It may also fail if there is information in the SDP that needs to be taken into account but is not understood by the ALG. End-to-middle security studies in the IETF may provide a solution to the encryption problem.

Another approach involves the use of a policy server accessed by UAs to open firewall holes (see 7.7).

7.3.1 Scenario 1 - Communication between NGCNs using a VPN

Firewall traversal should not be an issue if the VPN tunnel passes across any intervening firewalls. VPN tunnel establishment is outside the scope of this Technical Report.

7.3.2 Scenario 2 - Communication between NGCNs not using a VPN

Firewalls will generally exist at the edge of each NGCN, protecting the NGCN from the NGN. For cases where firewalls are not opened simply by sending outbound packets, other solutions will be required. Holes could be opened by the SIP intermediary in the NGCN concerned, but this is subject to the difficulties described in 7.3. A preferable solution would be for each UA to use a policy server to open holes, based on the send and receive IP addresses and ports exchanged via SDP.

Firewalls might also exist at the edge of the NGN, protecting the NGN from each NGCN. In this case, the use of outbound packets to open holes is not possible. The opening of holes by a SIP intermediary in the NGN would be subject to the difficulties described in 7.3. The use of an NGN policy server by each UA (under instruction from a SIP intermediary in the NGN) would be preferable.

REQUIREMENT ON NGN 23: If an NGN provides firewalls, it shall provide a means to open holes through the firewall for media between two NGCN UAs without relying on the ability to examine SDP passing between those UAs.

7.3.3 Scenario 3 - Communication between NGCN and TE using a VPN

The considerations in 7.3.1 apply.

7.3.4 Scenario 4 - Communication between NGCN and TE not using a VPN

The considerations in 7.3.2 apply.

7.3.5 Scenario 5 - Communication between NGCN and PSTN/ISDN

The considerations in 7.3.2 apply, except that here it may be possible for media packets transmitted by the gateway to open a firewall in the NGN at the boundary to the NGCN.

7.4 Identification

With the SIP as the means of signalling, identification of users and other entities is assumed to be by means of sip (or sips) Uniform Resource Identifiers (URIs) [4] or tel URIs [8].

A SIP URI is of the form SIP:user@domain. Each domain (as identified by the domain part) is responsible for allocating user parts to its users (human users, services, etc.). An NGCN will comprise one or more domains. A request from an NGN towards an entity in an NGCN will normally bear the SIP URI of that entity as its desired destination. The NGN only needs to understand the domain part of the SIP URI in order to route such a request to the NGCN domain,

which is then responsible for routing to the entity concerned. Thus there is no need for an NGN to have prior knowledge of user parts within an NGCN domain, and an NGCN should be at liberty to assign or revoke SIP URIs within its domain(s) without reference to the NGN.

However, it is necessary that any NGCN entity that needs to be reachable on calls from PSTN/ISDN has an identity that can be mapped to/from an E.164 telephone number that is one of a block of telephone numbers allocated to the NGCN. This could be achieved by use of tel URIs, whereby an identifiable entity in the NGCN has a tel URI as its sole or alternative identity. If the entity also has a SIP identity, this could be simply derivable from the tel URI, e.g., by having the telephone number as the user part of the SIP URI. Either the NGCN or the NGN could be responsible for mapping telephone numbers to/from SIP URIs.

For a call from PSTN/ISDN to an entity in an NGCN, the NGN shall first identify the NGCN domain concerned (e.g., by ENUM [7] look-up). There are then various possibilities for proceeding:

- the NGN forms a tel URI and uses this as the desired destination of the request to the NGCN, which then routes using the tel URI to the destination UA;
- the NGN forms a tel URI and uses this as the desired destination of the request to the NGCN, which then converts to a SIP URI for onward routing;
- The NGN converts the telephone number to a SIP URI for the NGCN domain concerned and uses this as the desired destination of the request to the NGCN.

REQUIREMENT ON NGN 24: An NGN shall be able to accept any user part in a SIP URI for an NGCN domain as valid.

REQUIREMENT ON NGN 25: An NGN shall be able to map telephone numbers assigned to an NGCN to/from URIs that are valid within that NGCN.

7.5 Provision of identification information

The recipient of a SIP request (the UAS) often requires reliable identification of the source of the request. Reliable identification is crucial to the filtering of unwanted requests, e.g., to support the use of black lists and white lists.

There are two basic methods of achieving this: hop-by-hop assertion of identity or cryptographically signed identity.

With hop-by-hop assertion, each SIP entity in the signalling path receives an assertion of the identity of the source of the request from the previous SIP entity, which has been authenticated by some means. The outbound SIP intermediary for the UAC will in general be able to authenticate the UAC and therefore can assert the UAC's identity to the next SIP entity in the signalling path, which in turn can assert that identity to the next entity. This only works if there is an unbroken chain of trust and authenticated signalling hops. If an entity does not trust the asserted identity from the preceding entity, it should not use that information and should not pass it on to other entities.

A cryptographically signed identity can be inserted by the UAC itself (if the UAC has a private key and certificate suitable for this purpose) or by an identity server within the same domain (e.g., collocated with the outbound SIP intermediary) that has authenticated the UAC by other means. A recipient of a cryptographically signed identity can assess whether to trust the identity based on the certificate of the signer.

There is a similar requirement for a UAC to be able to obtain reliable identification of the source of a response. Because a request can be retargeted, a response does not necessarily come from an entity with the same identity as that in the original request. Because of technical difficulties, no solution has been found yet to this problem.

Provision of identification information will depend on privacy requirements of the user concerned. If an NGCN does not wish his identity to be disclosed to other parties, the NGCN will either not supply the identity to the NGN or, if there is a trust relationship in place, pass the identity with a privacy marking. In the latter case the NGN is responsible for ensuring that it is not disclosed.

Similar privacy considerations apply in the opposite direction.

7.5.1 Scenario 1 - Communication between NGCNs using a VPN

This is an intra-NGCN or inter-NGCN problem with no impact on NGN.

7.5.2 Scenario 2 - Communication between NGCNs not using a VPN

If an NGCN provides a cryptographically signed identity, this is an inter-NGCN problem with no impact on NGN (other than transport).

If there is no SIP intermediary in the NGN, an NGCN could provide an asserted identity to the other NGCN, although this might not be accepted unless there is a trust relationship between the two NGCNs.

If there is a SIP intermediary in the NGN, an asserted identity would depend on transitive trust: the NGN trusting the first NGCN and the second NGCN trusting the NGN.

7.5.3 Scenario 3 - Communication between NGCN and TE using a VPN

The considerations in 7.5.1 apply.

7.5.4 Scenario 4 - Communication between NGCN and TE not using a VPN

For identification information sent from the NGN to the NGCN, the NGCN should be able to accept either an asserted identity or a signed identity. The former requires trust in the NGN and the latter requires trust in the signer of the identification information as indicated by a certificate.

REQUIREMENT ON NGN 26: An NGN shall be able to supply either an asserted identity or a cryptographically signed identity to an NGCN.

In the opposite direction the NGCN could supply either an asserted identity or a signed identity. If the NGN regards the NGCN as a peer it may accept an asserted identity and in turn assert this identity when forwarding the request towards the UAS.

REQUIREMENT ON NGN 27: An NGN should be able to accept an asserted identity as the source of a request from an NGCN if that NGCN is trusted.

Otherwise the NGN might only accept a cryptographically signed identity and even then may require the signer's certificate to be signed by a known certification authority (CA) in order to trust it. Whether or not the signed identity is trusted by the NGN, the NGN should still be able to forward the signed identity with the request towards the UAS. The UAS or the end user can then decide whether to trust the identity.

REQUIREMENT ON NGN 28: An NGN shall be able to accept a cryptographically signed identity as the source of a request from an NGCN if the NGCN does not provide an asserted identity or if the NGN is unable to trust an asserted identity.

7.5.5 Scenario 5 - Communication between NGCN and PSTN/ISDN

For identification information sent from the NGN to the NGCN the NGCN should be able to accept either an asserted identity or a signed identity. The former requires trust in the NGN and the latter requires trust in the signer of the identification information as indicated by a certificate.

REQUIREMENT ON NGN 29: An NGN shall be able to supply either an asserted identity or a cryptographically signed identity to an NGCN.

In the opposite direction the NGCN could supply either an asserted identity or a signed identity. If the NGN regards the NGCN as a peer it may accept an asserted identity and in turn use this asserted identity to derive an identity to be sent to the PSTN/ISDN.

Otherwise the NGN might only accept a cryptographically signed identity and even then may require the signer's certificate to be signed by a known certification authority (CA) in order to trust it and derive an identity to be sent to the PSTN/ISDN.

In either case the NGCN should supply an identity from which the NGN can derive a telephone number.

REQUIREMENT ON NGN 30: An NGN shall be able to accept a cryptographically signed identity as the source of a request from an NGCN if the NGCN does not provide an asserted identity or if the NGN is unable to trust an asserted identity.

7.6 Security

Security is a major consideration for the deployment of any application on an IP network, because of the ability for an attacker with access to the network to eavesdrop, impersonate, modify data in transit, etc.. Whilst obviously true for the public Internet, it is also true for "closed" IP networks (e.g., within an enterprise). In fact, security is a major consideration for NGNs, for NGCNs and for interworking of NGNs and NGCNs.

One aspect of security is privacy. Privacy considerations in the context of NGCNs are expected to differ compared with considerations for NGNs and are likely to be governed by the requirements of the enterprise concerned rather than regulatory requirements. Whereas in public networks the regulator might have a public interest in collecting information about certain users and their communications, this would not be acceptable for intra-NGCN communications between business users of a single NGCN.

REQUIREMENT ON NGN 31: An NGN shall be able to discriminate intra- from extra-NGCN communications, and thus to be able to decide where and when regulatory requirements (e.g. lawful interception, provision of location information, etc.) may apply and where such requests shall be refused.

For SIP-based multi-media communications, security has to be considered both for signalling (SIP) and for media.

7.6.1 Signalling security

Signalling security is important for several reasons. First, it is important to authenticate the source of a message, in order to authorise any action to be taken on the message. Otherwise an attacker could gain unauthorised access to services or information or carry out a denial of service attack. Secondly, even if the source of a message is authenticated, it is important to be sure that data integrity has not been compromised en route. Thirdly, signalling can contain sensitive information (e.g., the identities of parties in communication, IP addresses and ports to be used for media reception, etc.). This information needs to be protected against eavesdropping.

Because SIP uses SIP intermediaries, signalling between two UAs in general comprises one or more hops (e.g., from UA to SIP intermediary, SIP intermediary to next SIP intermediary, etc.). Signalling can be secured separately on each hop using general purpose security protocols at the transport layer (TLS) or the network layer (IPSEC[9]). These can provide authentication, integrity protection and secrecy. Authentication is achieved using public key cryptography, whereby an entity has a private key for signing messages and a certificate that it can publish to allow other entities to verify its signature. Between two SIP intermediaries mutual certificate-based authentication is the norm. However, between a SIP UA and its local SIP intermediary, a shared secret is normally used to allow the SIP intermediary to authenticate the UA (a certificate still being used to allow the UA to authenticate the SIP intermediary). An established secure connection should normally be retained on a semi-permanent basis for use by multiple SIP transactions in either direction, because of the overhead involved in establishing a new secure connection for each transaction.

Security should be considered essential for any SIP signalling hop, whether it be wholly within an NGCN, wholly within an NGN or spanning more than one network. For any given signalling transaction security will be expected on every hop linking the peer UAs (hop-by-hop security). The SIPS URI scheme is aimed at assuring hop-by-hop security, although it falls short of mandating the method of achieving security on a request's last hop, i.e., from the intermediary responsible for the domain in the request URI to the UAS (TLS is mandated on all other hops).

However, from the perspective of the UA, SIPS and hop-by-hop security might be insufficient. It relies on the UAs trusting the SIP intermediaries to conform to the SIP specification and not to disclose or modify information that is intended for end-to-end use. Whilst there is some information that SIP intermediaries need to inspect and perhaps also modify for routing or other

purposes, there is other information that should not be relevant for SIP intermediaries. If the integrity or secrecy of that other information is important to the UAs, they may require that information to be secured end-to-end.

For example, the session description carried in SDP might be relevant only to the UAs and not to SIP intermediaries. Thus SDP is a candidate for being secured end-to-end. In particular, with end-to-end encryption, IP addresses and ports need not be revealed to SIP intermediaries. More importantly, encryption keys for media security need not be revealed.

Another example is the transport of geographic location information between UAs. In general this is not relevant to SIP intermediaries (emergency calls excepted).

SIP allows bodies of SIP messages to be encrypted, authenticated and integrity protected using S/MIME. To use this capability, UAs need private keys and certificates, implying the need for a public key infrastructure (PKI) to provide this information. Similar considerations apply to key management for media security (see 7.6.2), and indeed S/MIME is one mechanism that can be used for securing key management. The implications of this are discussed in the context of key management for media security.

On the other hand, SIP intermediaries may require access to some aspects of SDP, e.g., for ensuring firewall traversal or ensuring bandwidth availability. This might lead to the need for "end-to-middle" security, whereby a UA can secure information between itself and a known SIP intermediary.

7.6.1.1 Scenario 1 - Communication between NGCNs using a VPN

The VPN tunnel will provide encryption and integrity protection of SIP signalling as it traverses the NGCN. However hop-by-hop and end-to-end security of SIP signalling may still be required, but this is an internal matter for the NGCN and outside the scope of this Technical Report.

7.6.1.2 Scenario 2 - Communication between NGCNs not using a VPN

SIP signalling will normally be routed via a SIP intermediary in each NGCN. The hop of interest is that between these two SIP intermediaries. It is essential that this hop be secured by TLS or IPSEC since it traverses an NGN (TLS according to SIPS). The two SIP intermediaries will need to accept each other's certificate, which implies possession of the Certification Authority (CA) certificate concerned.

If the NGN does provide a SIP intermediary, the considerations in 7.6.1.4 apply.

End-to-end security may be applied between the UAs for certain bodies of SIP messages. If either of the NGCN SIP intermediaries requires access to encrypted data, then end-to-middle security techniques will need to be applied. This is an NGCN matter with no impact on the NGN.

7.6.1.3 Scenario 3 - Communication between NGCN and TE using a VPN

The considerations in 7.6.1.1 apply.

7.6.1.4 Scenario 4 - Communication between NGCN and TE not using a VPN

SIP signalling will normally be routed via a SIP intermediary in the NGCN and a SIP intermediary in the NGN. The hop of interest is that between these two SIP intermediaries. It is essential that this hop be secured by TLS or IPSEC (TLS according to SIPS), since part of it traverses the NGN. The two SIP intermediaries will need to accept each other's certificate, which implies possession of the CA certificate concerned.

REQUIREMENT ON NGN 32: An NGN shall be able to support establishment of secure connections from an NGN SIP intermediary to an NGCN SIP intermediary and vice versa and retain connections on a semi-permanent basis for use by multiple SIP transactions in either direction.

REQUIREMENT ON NGN 33: An NGN shall be able to hold the CA certificate for a given NGCN and be able to authenticate an NGCN SIP intermediary's certificate during establishment of a secure connection to/from that SIP intermediary.

REQUIREMENT ON NGN 34: An NGN SIP intermediary shall have a private key and associated certificate and use them to allow authentication by an NGCN SIP intermediary.

Furthermore, it is essential that the NGN conform to the rules of SIPS to give users a guarantee of hop-by-hop security (subject to trust).

REQUIREMENT ON NGN 35: An NGN shall support SIPS by not allowing a request to a SIPS URI to be forwarded on an insecure link.

End-to-end security may be applied between the UAs for certain bodies of SIP messages. If either the NGCN SIP intermediary or the NGN SIP intermediary requires access to encrypted data, then end-to-middle security techniques will need to be applied.

REQUIREMENT ON NGN 36: An NGN SIP intermediary shall not require to modify end-to-end SIP signalling.

REQUIREMENT ON NGN 37: Ideally an NGN SIP intermediary should not require read access to end-to-end secured signalling. If it does it will need to employ end-to-middle security techniques, but this will require the cooperation of the UAs concerned and might not be acceptable to users or their enterprises.

7.6.1.5 Scenario 5 - Communication between NGCN and PSTN/ISDN

The considerations in 7.6.1.4 apply, except that here the gateway in the NGN is one of the UAs and therefore will have access to secured end-to-end signalling, if applicable. For this purpose the gateway will need a private key and certificate, which the UA in the NGCN will need to be able to verify in order to authenticate the gateway.

REQUIREMENT ON NGN 38: An NGN shall support SIPS on calls to/from a PSTN/ISDN gateway.

7.6.2 Media security

Media security is discussed here in terms of security of real-time media (voice and video) transported over RTP. Media transmitted over RTP can be secured by means of Secure RTP (SRTP) [6], which extends RTP by allowing media to be encrypted and by adding information for authentication and integrity checking. Secure RTCP (SRTCP) provides similar capabilities for RTP Control Protocol (RTCP).

Because RTP normally flows end-to-end between UAs, SRTP likewise is end-to-end. Intermediate entities may, however, be involved to provide specific services (e.g., transcoding, conferencing), in which case SRTP will operate between each UA and the intermediate entity (which itself appears as a UA to each of the other UAs).

To enable the use of SRTP (and SRTCP), a key management capability is required for providing the two UAs with a secret master key from which session keys can be derived. The key management capability must ensure that:

- the secret key (or information from which to derive it) is delivered to or accepted from only a known, authenticated entity; and
- the secret key (or information from which to derive it) cannot be eavesdropped en route.

For the first of these, basically during any key exchange a UA must ensure that the peer UA to which it sends the key or from which it receives the key is a UA with credentials to prove that it belongs to the user with whom the local user wishes to communicate. The use of a shared secret for this purpose is not normally scalable beyond a relatively small community, and therefore the use of public key cryptography is normally the only feasible solution. The sender of key information signs it using the private key associated with a certificate that the peer user can associate with a user with which he expects to or is willing to communicate. This may be a direct association or an indirect association (e.g., the user can associate the certificate with the identity delivered in signalling (see 7.4), which the user can then associate with a user with which he expects to or is willing to communicate.

Therefore to support media security in a scalable way, UAs need to have private keys and associated certificates. Furthermore they need to be in possession of a means of verifying signatures from peers, either by having an independent secure means of obtaining peer certificates or by having appropriate CA certificates for verifying certificates received from peers. This imposes a significant public key infrastructure (PKI) requirement on environments in which media security is required. In particular:

- a private key and associated certificate have to be produced for each user;
- this information has to be installed securely on any UA that the user uses, e.g., by secure download from a credentials server;
- peer UAs need to be able to obtain certificates from a reliable source for checking signatures (either peer certificates for checking peer signatures or CA certificates for checking the signatures of peer certificates).

Given that such a PKI is in place, it can also be used as the basis for encrypting key information for transmission end-to-end between UAs, thereby preventing eavesdropping. A UA can generate a key, sign it with its own private key and encrypt it using the peer UA's public key (from the peer UA's certificate). The peer UA can verify the signature using the sending UA's public key (from the sending UA's certificate) and decrypt the key using its own private key. This can be achieved using SIP's general purpose end-to-end security mechanism (i.e., S/MIME) to secure SDP, including any key management information. Alternatively, security can be achieved by embedding a key management protocol such as Multimedia Internet KEYing (MIKEY) within SDP. MIKEY provides its own means for authenticating and encrypting key information, again based on PKI. An advantage of MIKEY is that it is not necessary to send a key in each direction: a single key sent in one direction can be used to derive two different SRTP master keys, one for each direction. Another advantage is that it does not require the entire SDP to be secured.

A disadvantage of sending an encrypted key is that the sending UA needs to know in advance the public key of the receiving UA. Even if a certificate can be obtained for the user represented by the request URI in a SIP INVITE request, retargeting by SIP intermediaries can result in the request reaching a UAS that does not have the key to decrypt. This can result in additional rounds of SIP signalling. An alternative being considered for MIKEY is for the UAC to send its certificate to the UAS and then, in the response, the UAS can encrypt key information using that certificate.

An alternative is to use Diffie-Hellman key agreement, whereby a Diffie-Hellman component can be sent signed but not encrypted, thereby avoiding the need to acquire the certificate of the destination UA. MIKEY provides support for Diffie-Hellman key agreement protected by digital signatures based on PKI.

7.6.2.1 Scenario 1 - Communication between NGCNs using a VPN

Although the VPN tunnel will provide security for all traffic across the NGN, including media, SRTP will normally still be required end-to-end between the UAs to provide security within the NGCN as well.

Key management will be between the UAs with no impact on the NGN. The VPN tunnel provides secures the key exchange across the NGN, but in practice security will be needed end-to-end between the UAs to cover also transmission within the NGCN.

Within the NGCN it is likely that all certificates are signed by a single CA, and therefore verification of certificates is relatively easy.

Because in this scenario the NGN is transparent to media security and key management, media security in this scenario is not discussed further in this Technical Report.

7.6.2.2 Scenario 2 - Communication between NGCNs not using a VPN

SRTP will normally need to be provided end-to-end between the UAs in the different NGCNs, thereby securing the media through each NGCN and the NGN. The exception is if the NGN intervenes in media in some way, e.g., monitoring, transcoding and conferencing.

Key management will be between the UAs with no impact on the NGN. It will need to be secured end-to-end.

Because two NGCNs are involved it is likely that certificates will be signed by different CAs. Therefore each UA has to recognise the other UA's CA. If there has been no previous contact the CAs may not be readily acceptable and the users may need to be consulted.

If the NGCN does provide any SIP intermediaries in this scenario they will need to be transparent to SRTP and to key management.

REQUIREMENT ON NGN 39: Except where an NGN intervenes in media in some way, in order to add value and with the knowledge and permission of the users concerned, the NGN shall be transparent to SRTP and to key management.

If the NGN intervenes in media in any way, it will need to terminate SRTP and key management. In other words, it will need to appear as a UA to the UAs in the NGCNs. This has significant impact, since it means the UAs in the NGCN will need to perform key management not with each other but with the intervening entity. This implies that a UA must accept a certificate from the intervening entity rather than from the peer UA in the remote NGCN. A UA must have the means to verify such a certificate, which means having the appropriate CA certificate available and also being able to associate the subject of the certificate with something meaningful. It is likely that users will need to be involved in sanctioning such an arrangement. A user who is unwilling to sanction such an arrangement would need to find some other means of achieving the required communication, i.e., without the NGN being involved in media.

REQUIREMENT ON NGN 40: An NGN shall be able to avoid intervening in media if media is required to be secured end-to-end.

REQUIREMENT ON NGN 41: An NGN that intervenes in media will need to provide media security and associated key management between the intervening entity and each UA.

REQUIREMENT ON NGN 42: In order to provide key management between an intervening entity and a UA in an NGCN, the NGN will need to provide a certificate for that entity that can be verified by the NGCN UA.

7.6.2.3 Scenario 3 - Communication between NGCN and TE using a VPN

The considerations of 7.6.2.1 apply.

7.6.2.4 Scenario 4 - Communication between NGCN and TE not using a VPN

SRTP will normally need to be provided end-to-end between the UA in the NGCN and the UA in the NGN. Considerations are very similar to scenario 2.

7.6.2.5 Scenario 5 - Communication between NGCN and PSTN/ISDN

SRTP will normally need to be provided end-to-end between the UA in the NGCN and the gateway in the NGN, thereby securing the media through the NGCN and the NGN. The exception is if the NGN intervenes in media in some way other than at the gateway, e.g., monitoring, transcoding and conferencing.

Key management will be between the UA and the gateway, with no other impact on the NGN. It will need to be secured end-to-end.

The UA and the gateway will each require a private key and a certificate and will need to accept each other's certificate. The UA should normally be provisioned to accept certificates from any anticipated gateways. Similarly the gateway should be provisioned to accept certificates from legitimate users.

REQUIREMENT ON NGN 43: A PSTN/ISDN gateway in an NGN shall be able to supply a certificate that NGCN users are able to verify as being genuine.

REQUIREMENT ON NGN 44: A PSTN/ISDN gateway in an NGN shall be able to verify certificates from legitimate NGCN users.

7.7 Session policy

A network may wish to impose certain policies on use of its communication infrastructure. In particular it may wish to insert a media intermediary or impose limitations on the media that make up a session. Examples of reasons for inserting a media intermediary include traffic monitoring, enforcing service level agreements and access control, load balancing and traffic shaping, QoS marking, NAT/firewall traversal, media-level topology hiding and IPv4/IPv6 interworking. Most of these can be achieved through intervention at the transport layer or below. Intervention at a higher layer (e.g., RTP) may not be feasible if media are secured. Examples of limitations on media include media types allowed, codecs allowed and maximum bandwidth allowed.

Limitations for the local network (or segment thereof) will typically be made available to UAs during UA configuration, but the insertion of media intermediaries will depend on the session being established. Some sessions will extend beyond the local network segment and involve other segments or networks, which may also wish to insert a media intermediary or impose limitations on sessions.

SIP intermediaries are not necessarily well placed to impose policy by inserting media intermediaries and limiting session capabilities. This is because of the end-to-end nature of SDP in SIP and in particular the fact that it can be encrypted, thereby preventing viewing by SIP intermediaries, or integrity checked, thereby preventing modification. The purpose of SIP intermediaries is to establish signalling communication between SIP UAs by routing SIP requests and responses. The separate function of imposing session policy is better left to other entities, known as policy servers. SIP UAs can contact policy servers with details of the session to be established (based on sent and received SDP) and the policy servers can propose adjustments in order to insert intermediaries or limit session capabilities. Different domains will typically have different policy servers, and a SIP intermediary for a given domain can signal the identity of the policy server for that domain to the UAs. Thus the UAs can contact any relevant policy servers. Details of this mechanism are still being studied in the IETF.

7.7.1 Scenario 1 - Communication between NGCNs using a VPN

NGN policy may impact VPN tunnel establishment, but this is outside the scope of this Technical Report. NGCN policy is an internal mater for the NGCN.

7.7.2 Scenario 2 - Communication between NGCNs not using a VPN

The NGN and the two NGCNs can each potentially impose session policy.

7.7.3 Scenario 3 - Communication between NGCN and TE using a VPN

The considerations of 7.7.1 apply.

7.7.4 Scenario 4 - Communication between NGCN and TE not using a VPN

The NGN and the NGCN can each potentially impose session policy.

7.7.5 Scenario 5 - Communication between NGCN and PSTN/ISDN

The NGN and the NGCN can each potentially impose session policy.

7.8 Emergency calls

Networks need to allow users to make emergency calls to Emergency Call Centres (ECC), which may be PSTN/ISDN-based or IP-based. Some NGCNs may operate their own enterprise ECCs. There are several challenges involved in this, including:

- identification of an emergency call;
- routing an emergency call to the most appropriate ECC;
- allocating appropriate resources to an emergency call, if necessary at the expense of less important calls;
- providing correct identification information to the ECC to allow a return call to be made;
- providing caller location information to the ECC.

Identification of an emergency call in the SIP INVITE request from the UAC can be explicit (by means of the SOS SIP URI) or implicit. In the latter case a local SIP intermediary must determine it is an emergency call be analysing the request URI.

In order to route an emergency call to the most appropriate ECC, a SIP intermediary (generally the first, i.e. NGCN- or NGN-based) must attempt to obtain geographic location information (geographic coordinates and/or civil location) for the UAC. It may be able to obtain this from the network infrastructure (e.g., from LAN switches or by wireless base station triangulation), or information may be supplied by the UAC itself. Location information may be available from more than source, in which case all information should be forwarded to the ECC.

Identification information should be supplied in accordance with considerations in 7.5. However, privacy requirements must be overridden. Any other information that could possibly be of relevance should also be forwarded, subject to the capabilities of the signalling protocol.

Some NGCNs may require identification and location information sent to an ECC via an NGN to be encrypted. Likewise sensitive information may be divulged in the media, and therefore media encryption may also be required.

REQUIREMENT ON NGN 45: An NGN shall provide a means for encrypting sensitive information supplied by an NGCN for delivery to an ECC.

REQUIREMENT ON NGN 46: An NGN shall provide a means for encrypting media between an NGCN and an ECC.

7.8.1 Scenario 1 - Communication between NGCNs using a VPN

Emergency calls are not applicable to this scenario unless the NGCN provides its own ECC for emergencies inside the enterprise. This would not involve the NGN.

7.8.2 Scenario 2 - Communication between NGCNs not using a VPN

Emergency calls are not generally applicable to this scenario, except when used to route an emergency call to an ECC in a different part of same NGCN (intra-enterprise.

REQUIREMENT ON NGN 47: An NGN shall not interfere with the routing of a call to an enterprise ECC and shall not modify information for delivery to the enterprise ECC.

7.8.3 Scenario 3 - Communication between NGCN and TE using a VPN

The considerations of 7.8.1 apply. However, the NGCN proxy may be unable to determine the location of the TE and therefore it would be the responsibility of the TE to supply its location.

7.8.4 Scenario 4 - Communication between NGCN and TE not using a VPN

Emergency calls could be applicable to this scenario, the ECC being the TE in the NGN. In this case the SIP intermediary in the NGCN should determine that the call is an emergency call and forward the necessary information (caller identity and location). The SIP intermediary in the NGCN may not be able to determine the most appropriate ECC, in which case the SIP intermediary in the NGN should perform this function. All SIP intermediaries should assign appropriate resources.

NOTE
The calling TE in this scenario could be an enterprise ECC, which makes an emergency call to a public ECC.

7.8.5 Scenario 5 - Communication between NGCN and PSTN/ISDN

Emergency calls could be applicable to this scenario, the ECC being in the PSTN/ISDN. In this case the SIP intermediary in the NGCN should determine that the call is an emergency call and forward the necessary information (caller identity and location). The SIP intermediary in the NGCN may not be able to determine the most appropriate ECC, in which case the SIP intermediary in the NGN should perform this function. All SIP intermediaries should assign appropriate resources.

7.9 Geographic location

A UA may determine its geographic location (geographic coordinates and/or civil location) and make this available to authorised entities. These might be only the peer UA or they might include one or more SIP intermediaries. However, in general this information is sensitive and will need to be encrypted at least on a hop-by-hop basis. If it is not to be made available to SIP intermediaries then end-to-end encryption (using S/MIME) would be appropriate. If it is to be made available to designated SIP intermediaries, then end-to-middle security would be appropriate. There is ongoing work in the IETF on conveying location information in SIP.

Alternatively a SIP intermediary local to a UA may have the means to determine the UA's geographic information from the network infrastructure (e.g., from LAN switches or by wireless base station triangulation). Again it would need to be signalled securely to those SIP entities that are authorised to receive it. One solution being considered in the IETF is to signal the location information back to the UAC (using TLS on that hop) and ask the UA to signal it securely end-to-end.

In the case of an NGCN-owned TE connected to an NGN, the NGCN may wish to obtain location information for that TE from the NGN.

REQUIREMENT ON NGN 48: An NGN shall provide a means for an NGCN to obtain available location information of an NGCN-owned TE.

The provision of geographic location to an ECC is an important part of emergency calls (see 7.8).

7.9.1 Scenario 1 - Communication between NGCNs using a VPN

Geographic location is an internal matter for the NGCN.

7.9.2 Scenario 2 - Communication between NGCNs not using a VPN

Geographic location is a matter for the two NGCNs. There should be no reason for a SIP intermediary in the NGN to generate or have visibility of geographic location information. This information may be encrypted across the NGN.

7.9.3 Scenario 3 - Communication between NGCN and TE using a VPN

Geographic location is an internal matter for the NGCN. However, the NGCN proxy may be unable to determine the location of the TE and therefore it would be the responsibility of the TE to supply its location.

7.9.4 Scenario 4 - Communication between NGCN and TE not using a VPN

Geographic location information concerning the TE in the NGCN could be delivered to the TE in the NGN. There should be no reason for a SIP intermediary in the NGN to generate or have visibility of this information, which may be encrypted.

Geographic location information concerning the TE in the NGN could be generated by the TE or by a SIP intermediary in the NGN. If delivered to the TE in the NGCN, there should be no reason for a SIP intermediary in the NGCN to have visibility of this information, which may be encrypted.

7.9.5 Scenario 5 - Communication between NGCN and PSTN/ISDN

Geographic location information concerning the TE in the NGCN could be delivered to the PSTN/ISDN. There should be no reason for a SIP intermediary in the NGN to generate or have visibility of this information, which may be encrypted as far as the gateway.

Geographic location information concerning the TE in the PSTN/ISDN could be generated by the PSTN/ISDN, the gateway, or a SIP intermediary in the NGN. If delivered to the TE in the NGCN, there should be no reason for a SIP intermediary in the NGCN to have visibility of this information, which may be encrypted.

ecma INTERNATIONAL

Technical Report

INFORME TÉCNICO/91 ECMA

1ª Edición/Diciembre de 2005

Comunicación Empresarial en Redes Corporativas de Próxima Generación relacionadas con Redes Públicas de Próxima Generación (NGN)

Rue du Rhône 114 CH-1204 Geneva T: +41 22 849 6000 F: +41 22 849 6001

Informe Técnico
ECMA Informe Técnico/ 91
1ª Edición/Diciembre de 2005

Comunicación Empresarial en Redes Corporativas de Próxima Generación relacionadas con Redes Públicas de Próxima Generación (NGN)

Introducción

El presente informe técnico de Ecma ofrece una visión general de la comunicación empresarial basada en el Protocolo de Internet IP desde/hasta Redes Corporativas de Telecomunicaciones (también conocidas como redes empresariales) incluyendo aspectos de las redes domésticas de uso privado que tienen acceso a redes públicas de próxima generación (NGN).

Este Informe Técnico se basa en la experiencia práctica de compañías miembro de Ecma y en los resultados de su participación activa y continua en el trabajo de ISO/IEC, JTC1, UIT-T, ETSI, IETF y otros organismos nacionales e internacionales de normalización. Este informe representa un consenso general y pragmático.

El presente Informe Técnico de Ecma fue aprobado por la Asamblea General de diciembre de 2005.

Tabla de Contenidos

1. Alcance

Este Informe Técnico identifica casos de uso clave para la comunicación con o entre Redes Corporativas de Próxima Generación (NGCN) basadas en el Protocolo de Internet relacionadas con Redes Públicas de Próxima Generación (NGN), analiza estos casos de uso en términos de tecnología normalizada disponible o planeada e identifica los requisitos que deberán cumplirse.

Este Informe Técnico investiga las configuraciones que involucran las NGCNs y las NGNs y sus requisitos de interoperación. La interoperación que no se basa en el Protocolo de Internet, es decir aquella que usa tecnología de conmutación de circuitos entre NGCNs y NGNs, está fuera del alcance de este Informe Técnico.

Este informe técnico no diferencia entre tecnología inalámbrica y tecnología de acceso cableado.

Todos los aspectos de movilidad están fuera del alcance del presente Informe Técnico. Estos aspectos se estudian en el Informe Técnico Ecma 92. [1]

Las consideraciones relacionadas con las aplicaciones tales como IP Centrex y CSTA (del inglés *Computer Supported Telecommunications Applications)* están fuera del alcance del presente informe técnico.

2. Referencias

[1] ECMA TR/92	Corporate Telecommunication Networks – Mobility for Enterprise Communication
[2] ECMA-307	Corporate Telecommunication Networks - Signalling Interworking between QSIG and H.323 - Generic Functional Protocol for the Support of Supplementary Services (June 2000)
[3] ITU-T Rec. H.323	Packet-based multimedia communications systems
[4] IETF RFC 3261	SIP: Session Initiation Protocol
[5] IETF RFC 3489	Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) (STUN)
[6] IETF RFC 3711	The Secure Real-time Transport Protocol (SRTP)
[7] IETF RFC 3761	The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)
[8] IETF RFC 3966	The tel URI for Telephone Numbers
[9] IETF RFC 2401	Security Architecture for the Internet Protocol (IPSEC)

3. Definiciones

Para este Informe Técnico aplican las definiciones que se presentan a continuación:

3.1 Red Corporativa de Telecomunicaciones (CN) [2]

Conjuntos de equipos (Equipo Local del Cliente y/o Red de Instalaciones del Cliente) que se encuentran en ubicaciones geográficamente dispersas y están interconectados para prestar servicios de telecomunicaciones a un grupo definido de usuarios.

3.2 Red Corporativa de Próxima Generación (NGCN)

Red corporativa independiente diseñada para aprovechar las soluciones en comunicaciones emergentes basadas en el Protocolo de Internet y que pueden tener sus propias aplicaciones y prestación de servicios.

3.3 Red de Próxima Generación (NGN)

Red pública basada en paquetes, apta para prestar servicios de telecomunicaciones, para utilizar múltiples tecnologías de transmisión habilitadas con Calidad de Servicio (QoS) y en la cual las funciones relacionadas con la prestación de servicios son independientes de tecnologías subyacentes relacionadas con la transmisión.

3.4 Red Privada Virtual (VPN) [1]

Red virtual que puede ofrecer conectividad ubicua y segura sobre una infraestructura de red compartida (por ejemplo: las redes públicas portadoras) utilizando las mismas políticas de acceso que una red corporativa.

3.5 Proveedor de Servicios de Aplicaciones (PSA)

Una entidad que presta servicios de aplicaciones en telecomunicaciones.

3.6 Proveedor de Servicios de Sesión (SSP)

Una entidad que interviene y agrega valor a la señalización para el establecimiento y control de sesiones multimedia y opcionalmente interviene y agrega valor a las sesiones multimedia mismas.

3.7 Proveedor de servicios de transporte (TSP)

Una entidad que proporciona conectividad IP.

4. Abreviaturas:

ALG:	(Application Layer Gateway) Pasarela de la Capa de Aplicación
API:	(Application Protocol Interface) Interfaz del Protocolo de Aplicación
ASP:	(Application Service Provider) Proveedor de Servicios de Aplicación (PSA)
B2BUA:	(Back-to-Back User Agent) Back-to-Back User Agent
CN:	(Corporate Telecommunication Network) Red Corporativa de Telecomunicaciones.
CSTA:	(Computer Supported Telecommunications Applications) Aplicaciones en Telecomunicaciones Asistidas por Computador
IP:	(Internet Protocol) Protocolo de Internet
IPSEC:	(IP Security) Protocolo de Seguridad IP
ISDN:	(Integrated Services Digital Network) Red Digital de Servicios Integrados
NAT:	(Network Address Translator) Traductor de Direcciones de Redes
NGCN:	(Next Generation Corporate Network) Red Corporativa de Próxima Generación
NGN:	(Public Next Generation Network) Red Pública de Próxima Generación
RTP:	(Real-Time Protocol) Protocolo de Transporte en Tiempo Real.
QoS:	(Quality of Service) Calidad de servicio (QoS)
SBC:	(Session Border Controller) Controlador de Sesión de Borde
SDP:	(Session Description Protocol) Protocolo de Descripción de Sesión
SIP:	(Session Initiation Protocol) Protocolo de Inicio de Sesión
SRTP:	(Secure Real-time Transport Protocol) Protocolo Seguro de Transporte en Tiempo Real
SSP:	(Session Service Provider) Proveedor de Servicios de Sesión
TCP:	(Transmission Control Protocol) Protocolo de Control de Transmisión
TE:	(Terminal Equipment) Equipo Terminal
TLS:	(Transport Layer Security) Seguridad en la Capa de Transporte
TSP:	(Transport Service Provider) Proveedor de servicio de transporte

UA:	(User Agent) Agente de Usuario
UAC:	(User Agent Client) Agente de Usuario Cliente
UAS:	(User Agent Server) Agente de Usuario Servidor
UDP:	(User Datagram Protocol) Protocolo de Datagramas de Usuario
VoIp:	(Voice over IP) Voz sobre Protocolo de Internet
VPN:	(Virtual Private Network) Red Privada Virtual

5. Antecedentes

En los últimos años, las telecomunicaciones empresariales han evolucionado de manera significativa. Antes de eso, las redes empresariales de telecomunicaciones (o redes corporativas de telecomunicaciones, CN) se basaban en la tecnología de conmutación de circuitos a 64kbit/s, que tenía afinidad con la tecnología correspondiente utilizada en las Redes Digitales de Servicios Integrados (RDSI) y en servicios analógicos tradicionales. Esas Redes Corporativas de Telecomunicaciones prestaban primordialmente un servicio de voz o telefonía a sus usuarios, aunque en principio estaban en capacidad de brindar otros servicios incluyendo video y varios tipos de servicios de datos. Las Redes Corporativas de Telecomunicaciones eran aptas para interactuar con las RDSI para la comunicación fuera de la empresa.

Muchas redes públicas también ofrecían servicios opcionales a clientes empresariales tales como el Servicio Centrex y el alquiler y mantenimiento del equipo local.

Con la llegada de las tecnologías para la transmisión de voz y otros servicios multimedia en tiempo real sobre el Protocolo de Internet (IP) (por ejemplo, las basadas en Protocolos de Transporte en Tiempo Real (RTP) y los nuevos protocolos de señalización correspondientes (por ejemplo, H. 323 y Protocolo de Inicio de Sesión, SIP), había potencial para prestar servicios de telefonía y otros servicios en tiempo real y de persona a persona en la Internet pública. Además, tales servicios también se hicieron posibles en las “intranets” basadas en IP que ya se utilizaban en las empresas para ofrecer servicios de datos tales como el correo electrónico empresarial, la transferencia de archivos, los servicios web empresariales y el acceso a la world wide web. Las empresas percibieron ventajas tales como el ahorro en costos de infraestructura (por ejemplo: un cable hasta el escritorio) y la introducción de servicios novedosos que explotaban la convergencia del tiempo real y la comunicación de datos. El tradicional PBX (del inglés: Private Branch Exchange) o conmutador se reemplazó o evolucionó a un “IP-PBX” (del inglés, Internet Protocol Public Branch Exchange) o softswitch que admitía la conectividad IP hasta el escritorio y la conectividad IP entre nodos. La transmisión directa de datos multimedia basada en IP entre los puntos terminales suponía que las habilidades de conmutación ya no eran necesarias a excepción de las pasarelas para trabajar conjuntamente con redes “heredadas” de circuitos conmutados.

Las CNs basadas en IP siguen evolucionando y respaldando servicios adicionales, seguridad mejorada y QoS mejorada, etc. En este documento, una CN que abarca totalmente la tecnología IP se denomina Red Corporativa de Próxima Generación (NGCN).

En la actualidad, las NGCN generalmente recurren a técnicas heredadas de circuitos conmutados para la comunicación fuera de la empresa, por ejemplo el uso de la RDSI de carácter público o conmutación de circuitos sobre líneas alquiladas. Las pasarelas proporcionan la interacción necesaria de la señalización y los servicios multimedia.

En la próxima etapa de evolución, las NGCNs expandirán la comunicación basada en IP fuera de la empresa utilizando una red pública que también respalde dicha comunicación. La red pública basada en IP puede proporcionar comunicación entre la NGCN y otra NGCN, entre la NGCN y otro usuario IP (por ejemplo un usuario residencial) o, entre la NGCN y un usuario o red heredados a través de una pasarela en la red pública. Con esto, la

NGCN ya no necesita pasarelas hacia redes heredadas (excepto donde las inversiones existentes o las consideraciones económicas así lo requieran) y puede disfrutar de los beneficios de la comunicación de extremo a extremo basada en IP con socios de comunicación adecuadamente equipados.

La Internet pública es un ejemplo de una red pública basada en IP que una NGCN puede utilizar para las comunicaciones externas. Además, algunos proveedores de servicios están planeando ofrecer redes públicas basadas en IP que proponen mejoramientos en comparación con la Internet pública en términos de QoS, seguridad, movilidad, aplicaciones, etc. Estas redes públicas de valor agregado basadas en IP se conocen colectivamente como Redes de Próxima Generación (NGN).

El presente Informe Técnico apunta a contribuir a esta siguiente etapa de evolución explorando los temas relacionados con la interoperatividad de las NGCNs y las NGNs y a identificar los requisitos de las últimas.

5.1 Prestación de Servicios de las NGNs

5.1.1 Niveles de prestación de servicios

Una NGN puede prestar servicios a las NGCNs y a los usuarios de las mismas a diferentes niveles.

El nivel más básico de prestación de servicios es la conectividad IP. La diferencia con la Internet puede darse en la calidad de servicio o seguridad mejorada o garantizada. Para los propósitos de este Informe Técnico, una NGN que presta este nivel de servicio funciona como un Proveedor de Servicio de Transporte (TSP).

Un segundo nivel de prestación de servicios se da en el establecimiento de las sesiones y en el control de las sesiones de comunicación, por ejemplo: voz, multimedia y mensajería. Aquí, la NGN agrega valor al estar involucrada en el protocolo de señalización que se usa para establecer y controlar las sesiones multimedia. Para los propósitos de este Informe Técnico, se asume que el protocolo de señalización para el control de la sesión primaria en cuestión es el Protocolo de Inicio de Sesión (SIP). El valor agregado puede incluir: enrutamiento, provisión de calidad de servicio (QoS) para multimedia, provisión de servicios de pasarela a redes heredadas, asistencia en Traducción de Direcciones de Red Transversal (NAT-T) etc. Para los propósitos de este informe técnico, una NGN que presta este nivel de servicio se conoce como un Proveedor de Servicios de Sesión (SSP).

Un tercer nivel de prestación de servicios se da a nivel de aplicación. Las aplicaciones pueden ser muchas y muy variadas, pero para los propósitos de este Informe Técnico, se asume que una aplicación está relacionada de alguna manera con las telecomunicaciones. Una aplicación puede monitorear o controlar sesiones multimedia (directamente o a través de un protocolo o API (Interfaz de Protocolo de Aplicación) como por ejemplo CSTA) y puede o no tener que ver con los servicios multimedia. Los servicios de conferencias, servicios de transcodificación y traducción y los centros de distribución de llamadas son ejemplos de aplicaciones relacionadas con multimedia. Algunos ejemplos de aplicaciones que monitorean o controlan las sesiones pero que no involucran multimedia, incluyen servicios de presencia, servicios de grabación o registro de llamadas y servicios de configuración de Agente de Usuario (UA). Igualmente, se puede acceder a una aplicación a través de un Protocolo de Control de Sesión como SIP. Para los propósitos de este informe técnico, una NGN que presta este nivel de servicio se conoce como un Proveedor de Servicios de Aplicacion (PSA).

Una NGN puede prestar servicios a uno o más de estos niveles. No todos los servicios que se ofrecen serán de interés para los clientes empresariales y de relevancia para la interacción con las NGCNs. Los clientes empresariales pueden usar diferentes NGNs para niveles diferentes de prestación de servicios y pueden tener relaciones contractuales diferentes con cada una de estas NGNs. Además, para una comunicación determinada y dependiendo de la cantidad de partes que se van a interconectar y/o la cantidad de servicios a los que se va a acceder, se pueden involucrar proveedores múltiples.

La figura 1 muestra un ejemplo de una o más NGNs prestando servicios en los tres niveles.

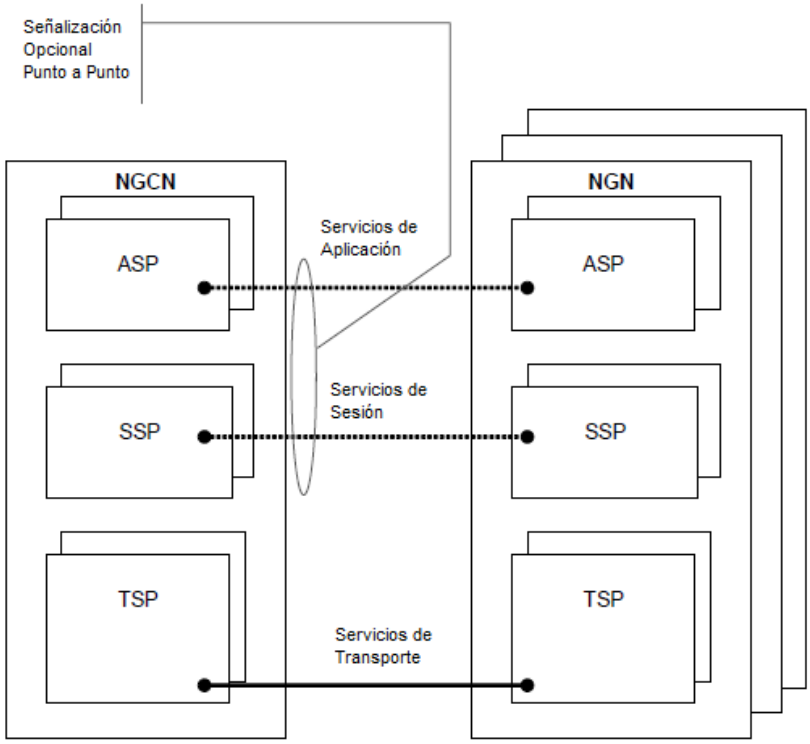


Figura 1 – TSP, SSP y PSA suministrados por NGN(s)

5.1.2 Utilización de los servicios de una NGN por las NGCNs.

Al prestar servicios de comunicación a sus usuarios, una NGCN puede usar los servicios de una o más NGNs. Para la comunicación con otra entidad (por ejemplo otra NGCN o un usuario residencial), una NGCN puede utilizar únicamente los servicios TSP, los servicios TSP y SSP, o los servicios TSP, SSP y PSA de la misma o de diferentes NGNs. Además, una NGCN puede utilizar servicios PSA por derecho propio más que como parte de la comunicación con otra entidad (por ejemplo, un servicio de presencia).

5.1.3 NGN Principal

Un cliente de una NGCN puede mantener relaciones contractuales con una o más NGNs para la provisión de ciertos servicios, cada NGN se conoce como la NGN Principal por los servicios que presta. Algunas partes de la NGCN pueden no tener conectividad directa con la NGN Principal y tendrán que acceder a los servicios de la misma a través de otras NGNs. El cliente también puede tener relaciones contractuales con esas NGNs (por ejemplo sólo para conectividad IP) o puede depender de los acuerdos entre la NGN Principal y las otras NGNs para tal uso.

La figura 2 muestra un ejemplo de dos partes de una NGCN donde cada parte tiene acceso a los servicios de la misma NGN principal, una directamente y otra a través de una NGN diferente. Las líneas sólidas representan la conectividad y las líneas punteadas representan el acceso al servicio.

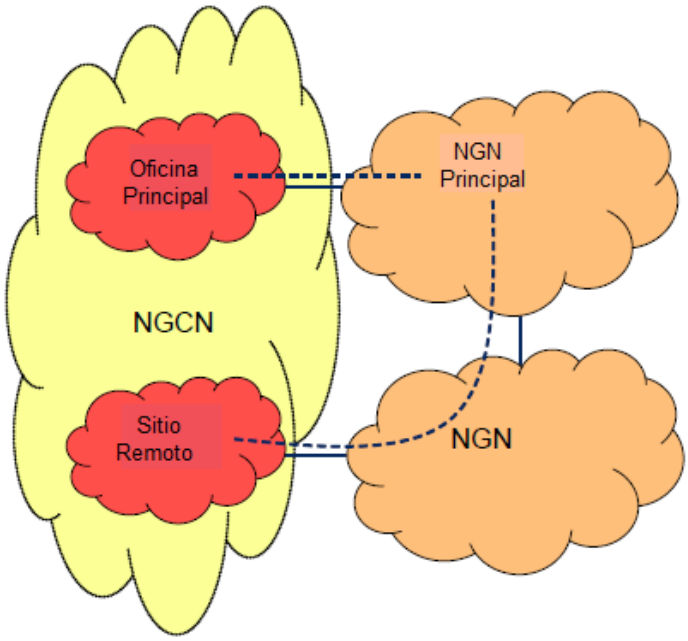


Figura 2 – NGN Principal y otra NGN

5.2 Consideraciones de Gestión

Puede ser necesario que los servicios que presta una NGN sean gestionados desde una NGCN. Además, una NGN puede prestar un servicio para manejar aspectos de una NGCN. Para estos dos propósitos deben usarse interfaces de gestión estándares de la industria entre la NGN y la NGCN. Sin embargo, el estudio de estas interfaces se encuentra fuera del alcance de la presente edición de este Informe Técnico.

6. Configuraciones Básicas y Requisitos Generales

Esta cláusula enumera configuraciones importantes aplicables a una NGCN específica de una empresa y su equipo (Equipo terminal, servidores,…) cuando está conectada con NGNs públicas. Además, en la sección 6.6, se especifican los requisitos generales de una NGN.

Deberán considerarse los siguientes **Escenarios** de interconexión:

- Escenario 1: Comunicación entre NGCNs a través de una NGN utilizando una VPN.
  Casos de uso: normalmente socios estrechamente relacionados
  - Dos oficinas semejantes de una misma empresa
  - Oficina principal y sucursal de una empresa
  - Dos empresas estrechamente relacionadas (“extranet”)
- Escenario 2: Comunicación entre NGCNs a través de una NGN **sin** utilizar una VPN.
  Casos de uso: normalmente socios **no** relacionados estrechamente
  - Dos empresas (no relacionadas)
- Escenario 3: Comunicación entre una NGCN y un Equipo Terminal (TE) a través de una NGN utilizando una VPN.

Casos de uso: normalmente socios estrechamente relacionados.

- Entre una empresa y un usuario residencial o SOHO (por ejemplo: un teletrabajador)

- Escenario 4: Comunicación entre una NGCN y un TE a través de una NGN sin utilizar una VPN.
  Casos de uso: normalmente socios **no** relacionados estrechamente
  - Usuario residencial o SOHO (por ejemplo: un miembro de una red pública)
- Escenario 5: Comunicación entre una NGCN y una Red Telefónica Pública Conmutada (RTPC)/ Red Digital de Servicios Integrados (RDSI) a través de una NGN.

La cláusula 7 estudia en detalle los aspectos técnicos y requisitos para cada uno de los escenarios principales.

6.1 Escenario 1 - Comunicación entre NGCNs a través de una NGN utilizando una VPN.

La empresa 1 y 2 tienen una relación lo suficientemente estrecha para tener una asociación de seguridad que permita el uso de una VPN que proporcione un túnel a través del cual puedan circular datos de señalización entre la NGCN, datos multimedia y otros datos. El túnel presta funciones tales como seguridad, transparencia para direcciones IP privadas, Traducción de Direcciones de Red Transversal NAT y traspaso de firewall, etc. Normalmente, esta relación cercana se usa entre:

- Las oficinas A y B de una sola empresa.
- La oficina principal y la sucursal de una empresa.
- Una empresa 1 y una empresa 2 estrechamente relacionadas (por ejemplo, una empresa asociada).

El control de túneles puede darse directamente entre la/las NGCN(s) (es decir control de túneles de extremo a extremo) sin involucrar otra NGN que no sea TSP, o puede ser suministrado por/pertenecer a la NGN o a un tercero.

En este escenario, la NGN actúa únicamente como TSP. Pueden estar involucrados múltiples TSP dentro de la NGN, es decir uno por cada empresa.

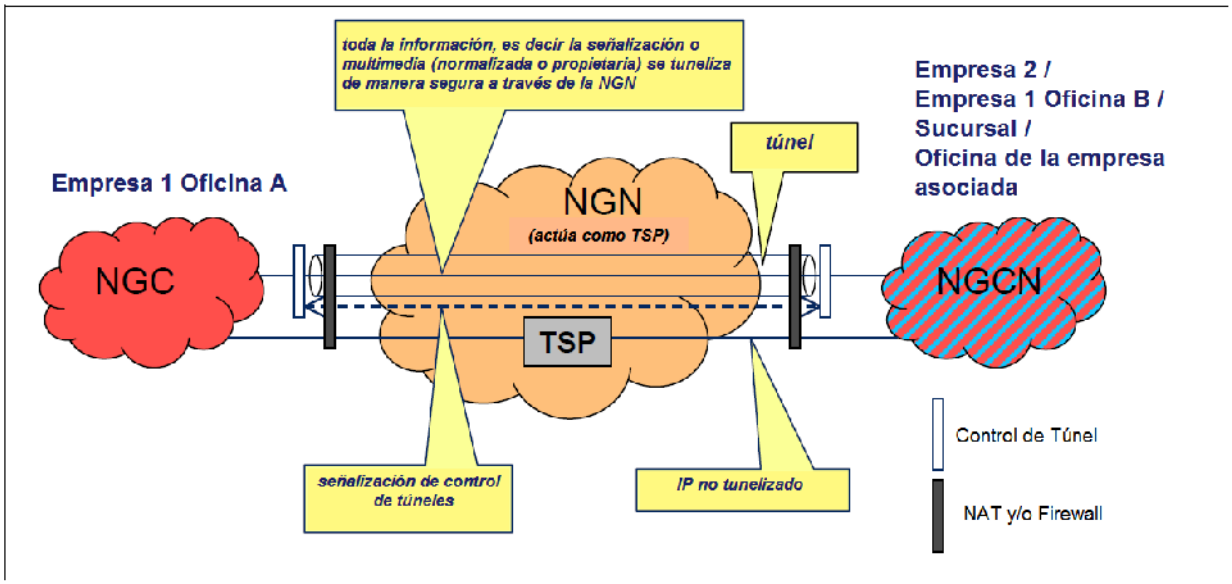


Figura 3 – Escenario 1 – Comunicación entre NGCNs utilizando una VPN

La Traducción de Direcciones de Redes y los firewalls en cada extremo del túnel son opcionales dependiendo de la relación entre las dos empresas.

6.2 Escenario 2 - Comunicación entre NGCNs a través de una NGN sin utilizar una VPN.

Este escenario aplica normalmente a empresas que no están relacionadas estrechamente (es decir, sin seguridad en común, sin túnel seguro). También puede aplicar a empresas estrechamente relacionadas (o incluso entre dos ubicaciones en una misma empresa) si por cualquier razón, estas no están en capacidad de establecer un túnel a través de la NGN.

En este escenario, la NGN actúa al menos como un TSP. También puede actuar como un SSP (provisión de servicios de sesión) y/o como un ASP (provisión de aplicaciones tales como conferencias, presencia, correo de voz, correo unificado, etc.). También se pueden involucrar múltiples TSP, SSP y/o ASP dependiendo de la cantidad de servicios a los que se tiene acceso.

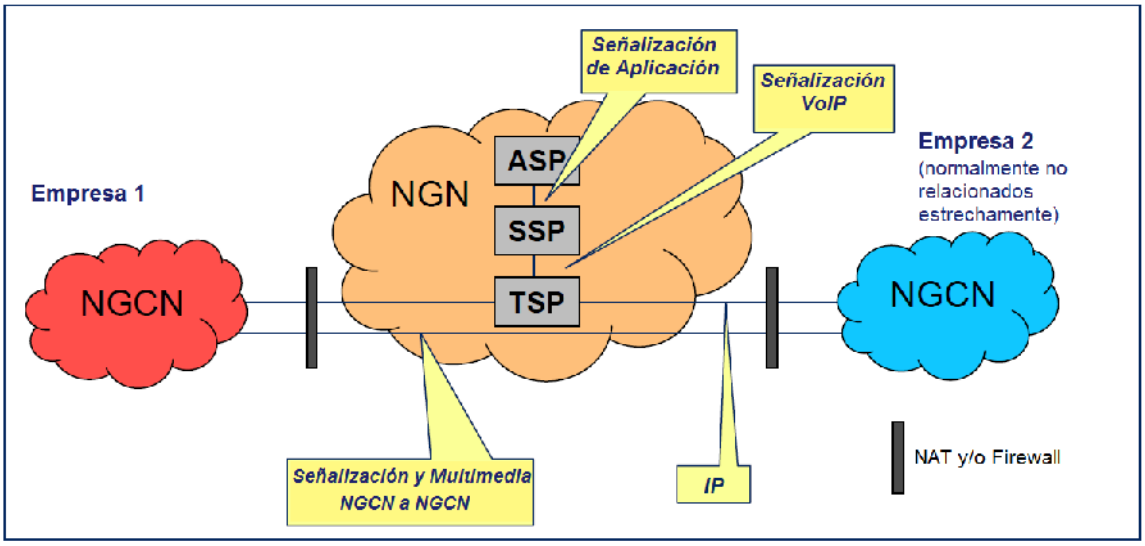


Figura 4 – Escenario 2 – Comunicación entre NGCNs sin utilizar una VPN

6.3 Escenario 3: Comunicación entre una NGCN y un TE a través de una NGN utilizando una VPN.

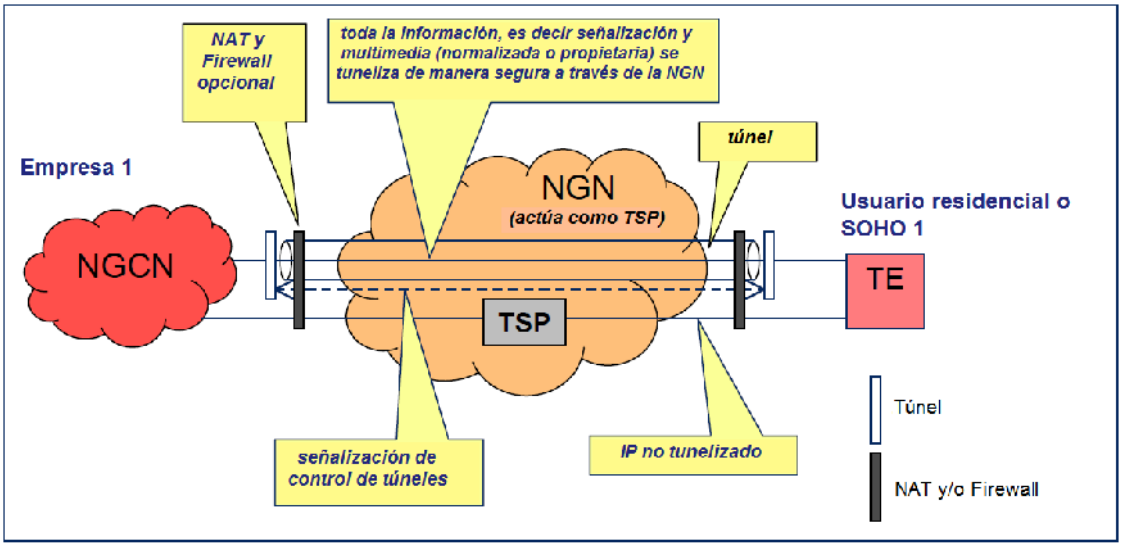


Figura 5 – Escenario 3 - Comunicación entre una Red Corporativa de Próxima Generación y un Equipo Terminal a través de una NGN utilizando una VPN

La Traducción de Direcciones de Redes y los firewalls para el túnel son opcionales dependiendo de la relación entre la empresa y el TE.

6.4 Escenario 4: Comunicación entre una NGCN y un TE a través de una NGN sin utilizar una VPN.

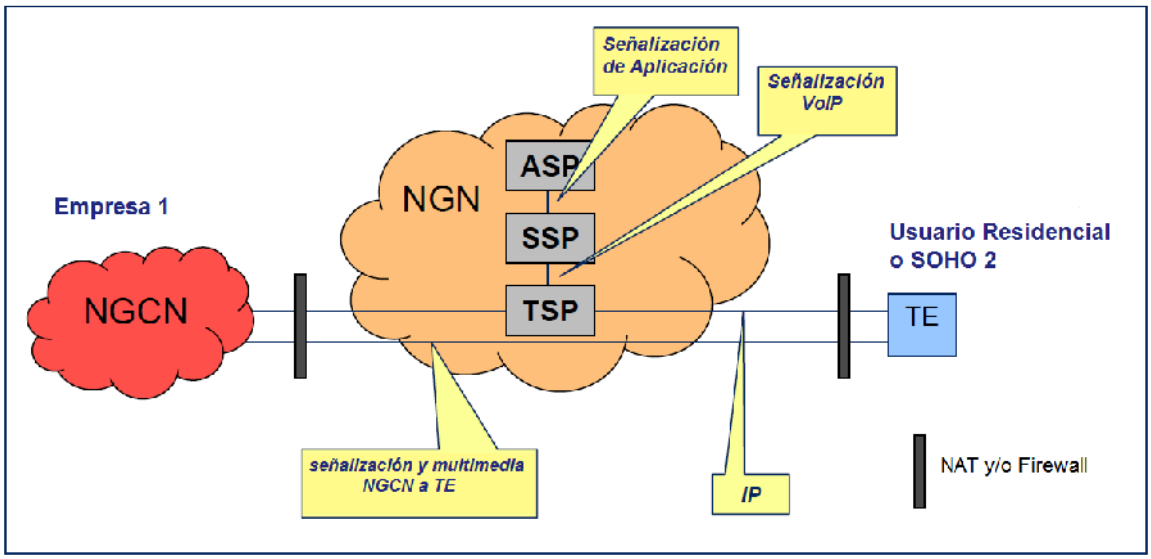


Figura 6 – Escenario 4 - Comunicación entre una NGCN y un TE a través de una NGN sin utilizar una VPN

6.5 Escenario 5 – Comunicación entre una NGCN y una RTPC/RDSI a través de una NGN.

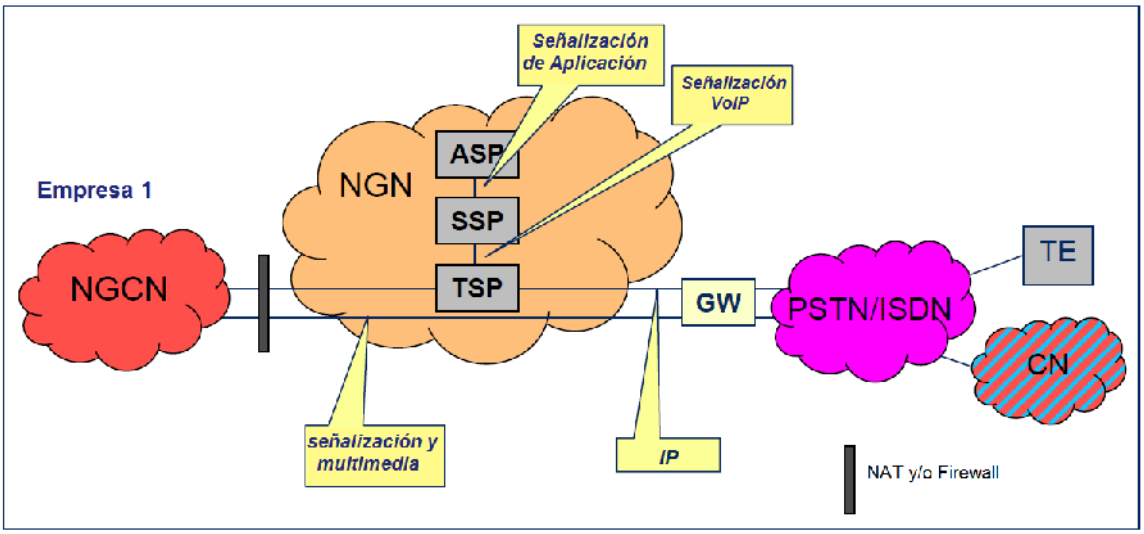


Figura 7 – Escenario 5 – Comunicación entre una NGCN y una RTPC/RDSI a través de una NGN.

La NGN puede proporcionar la pasarela como parte de su SSP. La pasarela también puede pertenecer a un tercero.

6.6 Requisitos Generales de las NGNs

Para dar soporte a las comunicaciones que involucran NGCNs, las NGNs deben cumplir ciertos requisitos. En esta sección se señalan algunos requisitos generales. Estos requisitos aplicarán de maneras diferentes a algunos o a todos los escenarios descritos en la cláusula 6 e influyen en las consideraciones técnicas de la cláusula 7. Al mencionar una NGN, esta puede ser una sola NGN o varias NGNs que cooperan entre si.

REQUISITO # 1 DE UNA NGN: una NGN tendrá que dar soporte a las sesiones de comunicación establecidas en cualquier dirección entre un usuario de una NGCN y un usuario en otra NGCN, un usuario en la NGN o un usuario en una RTPC/ RDSI a la que se tiene acceso a través de una pasarela en la NGN.

REQUISITO # 2 DE UNA NGN: Una NGN tendrá que permitir el uso de cualquier contenido multimedia basado en IP durante una sesión de comunicación sujeta a la disponibilidad de recursos y disposiciones contractuales.

REQUISITO # 3 DE UNA NGN: una NGN no deberá intervenir en el transporte de contenidos multimedia por encima de la capa de transporte excepto cuando esto se pacta explícitamente con la NGCN (mediante señalización o contrato) o debido a requisitos legales.

NOTA
Es posible prestar funciones tales como transcodificación, traducción y puenteo si se llega a un acuerdo al respecto.

NOTA
La aplicabilidad de requisitos legales puede depender de si los contenidos multimedia se transportan entre dos partes de la misma NGCN (es decir dentro de una empresa) o fuera de la empresa.

REQUISITO # 4 DE UNA NGN: una NGN tendrá que ofrecer acuerdos a nivel de servicios en los cuales la calidad de servicio de los contenidos multimedia, de la señalización y de otros datos sea apropiada para uso de la empresa.

REQUISITO # 5 DE UNA NGN: una NGN tendrá que proporcionar funcionalidad estándar de industria para colaborar con el traspaso de acuerdos de Traducción de Dirección de Redes que normalmente se encuentran en el límite de una NGCN.

NOTA
En general, el punto terminal debe ser responsable de la señalización de direcciones IP y puertos adecuados para uso del punto terminal remoto. Sin embargo, para conseguir esto, puede ser necesario que la NGN proporcione funcionalidad como por ejemplo un servidor STUN.

REQUISITO # 6 DE UNA NGN: una NGN tendrá que soportar la identificación de los usuarios y los servicios por medio de SIP o por medio de Identificadores Uniformes de Recursos (SIPS URIs) y opcionalmente a través de los URIs de teléfono, si esto no entra en conflicto con los parámetros contractuales y de privacidad disponibles del usuario del punto terminal.

REQUISITO # 7 DE UNA NGN: una NGN tendrá que proporcionar a una NGCN, la identidad autenticada de quien llama si hay disponibilidad, o un dato adecuado y significativo, si no hay tal disponibilidad.

REQUISITO # 8 DE UNA NGN: una NGN tendrá que estar en capacidad de pasar la identidad autenticada del usuario que desea conectarse, desde una NGCN hacia un usuario llamado durante el establecimiento y reestructuración de la comunicación.

REQUISITO # 9 DE UNA NGN: una NGN tendrá que ofrecer una interfaz estándar de señalización SIP a una NGCN con base en estándares RFCs (Petición de Comentarios) del IETF.

REQUISITO # 10 DE UNA NGN: una NGN tendrá que ser transparente para la señalización de extremo a extremo y tolerante para cualquiera que no tenga respaldo, excepto si proporciona una pasarela a una RTPC/RDSI o un servicio de aplicaciones.

NOTA
Esto incluye el cuerpo y ciertos encabezados del mensaje SIP. En el caso de los cuerpos de mensaje SDP, es necesario que la NGN tolere extensiones SDP sin soporte y SDP de próxima generación.

REQUISITO # 11 DE UNA NGN: una NGN no deberá efectuar acciones que invaliden la verificación criptográfica de integridad sobre fragmentos de mensajes que pretenden enviarse sin cambios, durante el transporte de mensajes de señalización excepto cuando una norma local así lo requiera.

NOTA
La aplicabilidad de los requisitos legales puede depender de si la señalización se transporta entre dos partes de la misma NGCN (es decir dentro de una empresa) o fuera de la empresa.

REQUISITO # 12 DE UNA NGN: una NGN tendrá que permitir que la información de extremo a extremo sea cifrada y no deberá exigir acceso a la clave durante el transporte de mensajes de señalización.

NOTA
Ejemplos: información sobre la ubicación geográfica e información clave para la seguridad de los contenidos multimedia. Cuando sea necesario tener acceso a ciertas partes de los datos cifrados de extremo a extremo, la NGCN debe hacer los arreglos necesarios para que estos se envíen en forma separada, ya sea cifrados (para que la NGN los descodifique) o sin cifrar.

REQUISITO # 13 DE UNA NGN: una NGN deberá estar en capacidad de proporcionar seguridad opcional (cifrado, autenticación y verificación de integridad) de los servicios de señalización en la interfaz entre la NGCN y la NGN.

REQUISITO # 14 DE UNA NGN: una NGN deberá estar en capacidad de proporcionar seguridad (cifrado, autenticación y verificación de integridad) de señalización en cada salto de señalización entre los socios de comunicación mediante solicitud y cada NGN deberá estar en capacidad de mostrar la evidencia necesaria de que esta se proporciona.

NOTA
La seguridad de señalización puede ofrecerse mediante el uso del esquema SIPS URI.

REQUISITO # 15 DE UNA NGN: una NGN tendrá que permitir que los contenidos multimedia se aseguren (cifrados, autenticados, y con verificación de integridad) en los extremos.

REQUISITO # 16 DE UNA NGN: una NGN deberá permitir la gestión de claves para que el cifrado de los contenidos multimedia ocurra dentro de la señalización entre dispositivos finales.

NOTA
La gestión del intercambio de claves entre un usuario de una NGCN y un intermediario NGN será con frecuencia inaceptable para los usuarios de una NGCN y sus socios. Por ejemplo, un usuario residencial que llame a un banco puede necesitar autenticación basada en un certificado suministrado por el banco antes de hablar. Ver Requisito # 3 y # 11.

REQUISITO # 17 DE UNA NGN: una NGN tendrá que ofrecer asesoría a una NGCN sobre la información de las tarifas cuando se incurra en gastos.

6.7 Requisitos generales de las NGNs con respecto a las medidas para el cumplimiento de las normas.

Los temas potenciales para las autoridades reguladoras y para los administradores son: servicios de emergencias (incluyendo telecomunicación de emergencia y auxilio de desastre), intercepción legal y privacidad (para tomar en consideración en el contexto de presentación de la identidad, nombre, dirección e información sobre la ubicación del usuario comercial o terminal).

Diversas autoridades reguladoras, por ejemplo en los Estados Unidos y en Europa, han iniciado consultas en un marco regulador para la prestación de servicios públicos VoIP.

Sin embargo, al momento de la preparación de este Informe Técnico no es claro si o hasta qué punto las redes empresariales y en particular su tráfico interno de comunicaciones se verá afectado por esas normas que ya aplican a los operadores de redes públicas (en intercepción legal, retención de datos). Mas allá de eso, todavía está en discusión, cómo definir los límites de una red empresarial, que especialmente en el caso del acceso remoto, pueda compartir la infraestructura de red de un proveedor universal de servicios al cual apliquen las reglas. El desafío está en cómo manejar tales redes empresariales virtuales.

NOTA
En un entorno de conmutación de circuitos, el punto de referencia T (de terminal) funcionó como delimitación entre infraestructuras de redes públicas y privadas y por consiguiente, como el límite para la regulación.

Se espera que las redes empresariales, incluyendo las redes empresariales virtuales, no estén sujetas a más regulación que las redes empresariales de conmutación de circuitos.

REQUISITO # 18 DE UNA NGN: una NGN deberá estar en capacidad de distinguir entre el tráfico normal y el tráfico intra empresarial al aplicar medidas para el cumplimiento de las normas, lo cual mantendrá las comunicaciones internas de las redes empresariales libres de intervenciones no deseadas.

7. Aspectos técnicos y requisitos de una NGN en relación con la Prestación de Servicios de Sesión.

Para llevar a cabo las configuraciones que se identifican en la cláusula 6 surgirán ciertos aspectos técnicos. Esta cláusula estudia estos aspectos técnicos en términos generales y también en relación con configuraciones específicas y genera requisitos de NGN adicionales a los descritos en la sección 6.6. La presente edición de este Informe Técnico aborda únicamente ciertos aspectos técnicos fundamentales y existen otros aspectos técnicos que pueden requerir consideración posterior, por ejemplo, tarifas, enrutamiento, transcodificación, calidad de funcionamiento, observación de la calidad de funcionamiento, resiliencia, etc., y también aplicaciones como presencia.

Los aspectos se discuten con referencia particular a la comunicación multimedia basada en SIP, pero generalmente aplican a cualquier forma de comunicación multimedia, como por ejemplo la comunicación basada en señalización H.323.

7.1 Arquitectura de Señalización

El protocolo SIP es básicamente un protocolo que funciona entre dos puntos finales que se conocen como Agentes de Usuario (UA). Este protocolo le permite a esos UA establecer una sesión de comunicación que incluye una o más conexiones multimedia (es decir, bearer streams (portadores de flujos) tales como audio, video, fax, mensajería instantánea o texto en tiempo real. Una sesión se establece intercambiando descripciones de sesión de conformidad con el Protocolo de Descripción de Sesión (SDP) dentro de los mensajes SIP. Las descripciones de sesión indican factores tales como los contenidos multimedia a usar, codecs, tasa de procesamiento de paquetes, contextos de seguridad, direcciones IP y números de puerto para la recepción de servicios multimedia

En principio, el protocolo SIP puede funcionar directamente entre dos UAs. Sin embargo, los estándares SIP definen otras entidades SIP que pueden colaborar. En particular, el estándar SIP principal [4] define el concepto de un servicio de ubicación en el cual los UAs pueden registrarse para colaborar en la localización de los UAs que representan a un usuario particular. Se relacionan con esto, los conceptos de servidor de registro (una entidad SIP que registra UAs en el servicio de ubicación) y servidor proxy (una entidad SIP que consulta el servicio de ubicación para colaborar en el envío de peticiones a los UAs apropiados).

NOTA
También existe un servidor de redireccionamiento, que es similar a un proxy pero no envía las peticiones sino que las desvía. Para los propósitos de este Informe Técnico, un servidor de redireccionamiento se toma como un proxy a menos que se afirme lo contrario.

El manejo de una petición SIP desde un UA (el Agente de Usuario Cliente, UAC) hasta otro UA (el Agente de Usuario Servidor, UAS) normalmente pasa por un servidor proxy, que consulta al servicio de ubicación para localizar los UAs que puedan manejar la petición. El UAC con frecuencia también envía peticiones a un servidor proxy local, (que se conoce como un proxy de salida) con el fin de reducir la carga de enrutamiento en el UAC. Esto da origen al esquema típico Trapezoide SIP que involucra dos UAs y dos proxys (Ver figura 9).

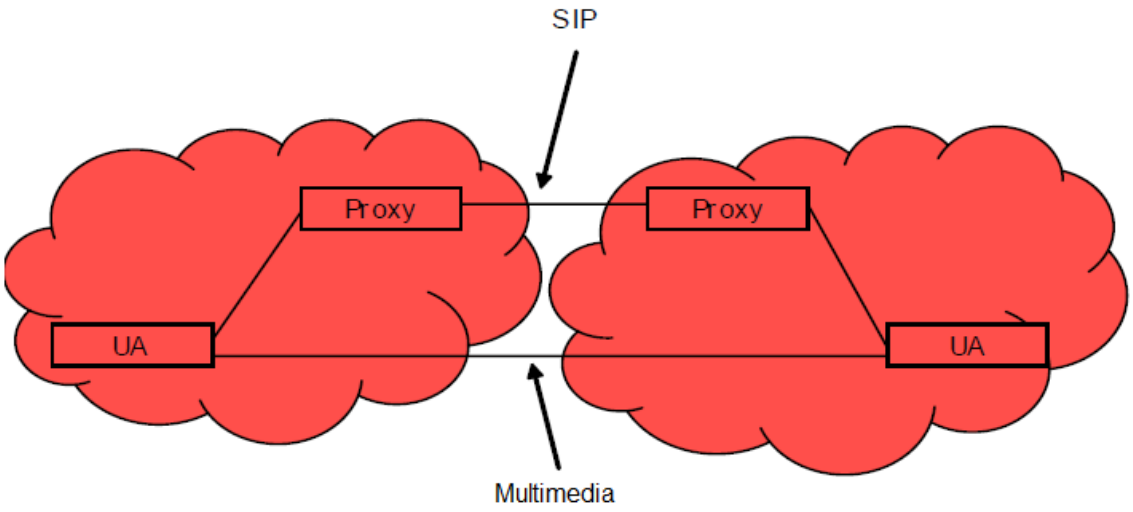


Figura 8: Trapezoide SIP típico

A veces, una petición SIP puede resultar en la formación de una asociación entre dos UAs, en cuyo contexto pueden enviarse peticiones SIP posteriores en cualquier dirección. Esto se conoce como diálogo. El diálogo más importante en SIP es el que inicia una petición INVITE, porque tal diálogo tiene una sesión asociada que comprende una colección de contenidos multimedia entre los UAs. Un diálogo iniciado por una petición INVITE y su sesión asociada

puede percibirse como una llamada. Los proxys involucrados en el enrutamiento de la petición iniciadora del diálogo pueden o no permanecer involucrados en el diálogo para el enrutamiento de peticiones posteriores.

Normalmente, un proxy se combina con un servicio de ubicación y un servidor de registro, es por eso que la entidad completa tiende a conocerse como un proxy. El comportamiento de un proxy, se normaliza en SIP[4] y en otros RFCs sobre SIP y su comportamiento se encuentra rigurosamente restringido por los estándares para no poner en peligro el carácter de extremo a extremo que es fundamental para gran parte del protocolo SIP.

Aunque no esté definido en el protocolo SIP, el mercado ha visto la necesidad de una entidad conocida como Back-to-Back User Agent (B2BUA). En algunos aspectos, un B2BUA funciona como un proxy al ser una entidad intermedia en una ruta de señalización entre dos UAs, pero en otros aspectos, un B2BUA funciona como dos UAs recíprocos. El comportamiento de un B2BUA no está normalizado, y puesto que no está restringido por los estándares, puede comportarse de manera más flexible que un proxy. Esto le permite a un B2BUA cumplir ciertos roles que un proxy no puede cumplir (por ejemplo, ofrecer servicios de transcodificación para los medios). Por otro lado, al no comportarse como un proxy, un B2BUA mal diseñado puede operar de manera inconsistente con las expectativas de los UAs y puede ocasionar problemas.

Otros tipos de entidad que pueden intervenir activa o pasivamente en una ruta de señalización SIP incluyen Pasarelas de la Capa de Aplicación (ALGs) y Controladores de Sesión de Borde (SBC). Estos poseen el conocimiento del protocolo SIP y pueden monitorearlo o modificarlo para ciertos propósitos, por ejemplo, control de Traducciones de Direcciones de Redes NATs y firewalls, seguridad, privacidad, etc.

En el resto de esta cláusula, el término intermediario SIP, se usa para referirse a cualquier entidad intermedia involucrada activa o pasivamente en la señalización SIP entre dos UAs, incluyendo entre otros a los proxys, B2BUAs, ALGs y SBCs.

Como se mencionó anteriormente, el protocolo SIP puede en principio funcionar directamente entre UAs, y de hecho en la actualidad hay mucho interés en el protocolo SIP P2P (punto a punto) donde se eliminan los intermediarios SIP. Afirmar que este ideal se llevará a cabo y predecir cuándo, es algo incierto, sin embargo, se espera que las tendencias se alejen del concepto de señalización MDT (del inglés Time-Division Multiplexing: Multiplexación por División de Tiempo) pasando a través de un número arbitrario de intermediarios (por ejemplo relacionados con switches) hacia una solución ligera con un número mínimo de intermediarios SIP. Generalmente, no debería haber necesidad de más intermediarios SIP que en el trapezoide SIP típico que se mencionó antes. Un número excesivo de intermediarios SIP puede tener un impacto negativo y aumentar los retrasos en la señalización (por ejemplo, durante el establecimiento de una llamada). Igualmente, la intervención excesiva de cualquier intermediario SIP puede tener un efecto perjudicial al no cumplir con las expectativas de los UAs.

Esto conlleva a los requisitos generales de las NGNs que funcionan como SSPs y que se describen a continuación. En el contexto de escenarios y aspectos técnicos específicos aplican requisitos más específicos.

REQUISITO # 19 DE UNA NGN: los intermediarios SIP en una ruta de señalización deben ser mínimos.

REQUISITO # 20 DE UNA NGN: un intermediario SIP en una NGN deberá comportarse de tal manera que no sea perjudicial para los UAs que están tratando de comunicarse a través de el. Un intermediario SIP que cumpla las reglas de un proxy estaría en conformidad con esto. Esto incluye transparencia en la información de la señalización SIP que no es relevante al intermediario, incluyendo cualquier extensión SIP no respaldada (normalizada o propietaria).

Los requisitos anteriores aplican también donde dos o más NGNs en serie funcionan como SSPs para una comunicación dada.

Aunque la señalización SIP normalmente pasa a través de uno o más intermediarios SIP, los contenidos multimedia en general circulan directamente entre los UAs en cuestión, sin la participación de intermediarios más allá de la capa de transporte (los intermediarios como los NATs y los firewalls pueden estar involucrados hasta la capa de transporte). La excepción se da cuando un intermediario cumple alguna función en los contenidos multimedia, como por ejemplo transcodificación, traducción o puenteo, en cuyo caso el intermediario realmente actúa como dos o más UAs en un arreglo recíproco (similares y tal vez coincidentes con un SIP B2BUA).

7.1.1 Escenario 1 - Comunicación entre NGCNs a través de una NGN utilizando una VPN.

Deberá ser suficiente con dos intermediarios SIP, uno en cada parte de la NGCN. La NGN funciona únicamente como un TSP. En todo caso, el cifrado a través del túnel significará que la NGN no puede proporcionar ningún intermediario SIP. Los contenidos multimedia al igual que la señalización SIP circularán a través del túnel.

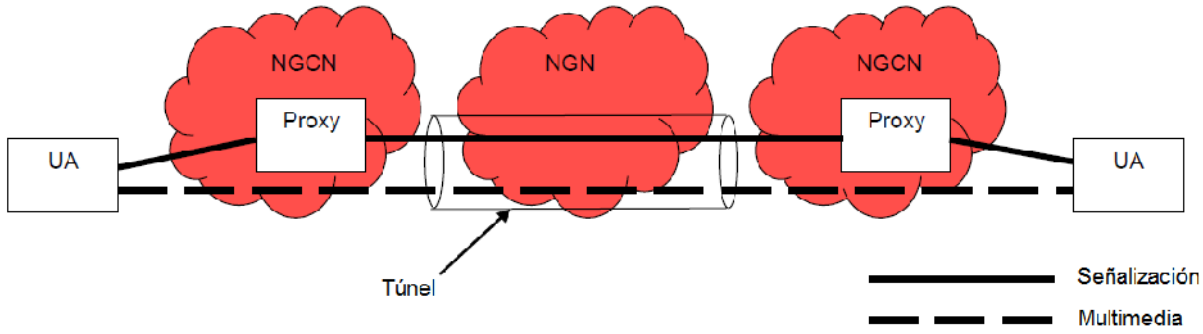


Figura 9 – Arquitectura de Señalización típica para el escenario 1

7.1.2 Escenario 2 – Comunicación entre NGCNS a través de una NGN sin utilizar una VPN.

En principio, deberá ser suficiente con dos intermediarios SIP, uno en cada NGCN. Los intermediarios SIP en la NGN deben proporcionarse únicamente si permiten a la NGN ofrecer servicios complementarios, por ejemplo, dar garantías de Calidad de Servicio (QoS) para los servicios multimedia. Los intermediarios SIP en la NGN deben ser transparentes a la información de la señalización SIP que no es relevante a aquellos intermediarios, incluyendo cualquier extensión SIP no respaldada (normalizada o propietaria). Ya sea que la NGN proporcione o no cualquier intermediario SIP, los contenidos multimedia pueden o no circular a través de la misma NGN.

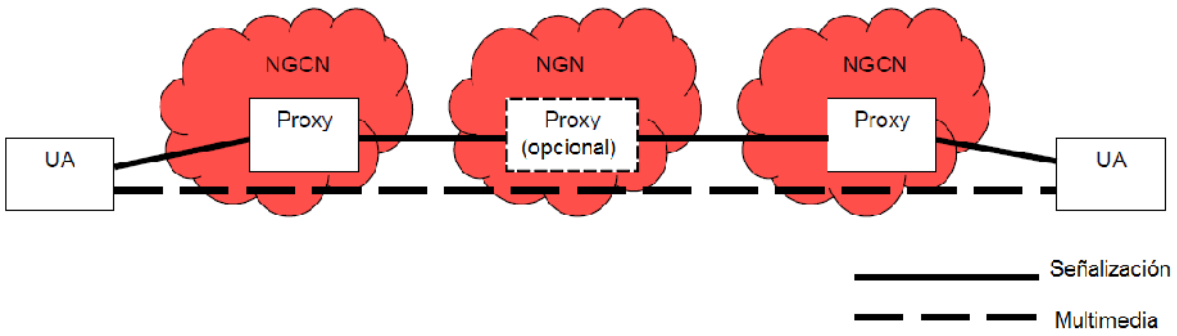


Figura 10 – Arquitectura de Señalización típica para el escenario 2

7.1.3 Escenario 3 – Comunicación entre una NGCN y un TE utilizando una VPN.

Los intermediarios SIP deben limitarse a la NGCN. La NGN funciona únicamente como un TSP. El TE incorporará un UA que se comunique con un proxy de entrada/salida u otro intermediario en la NGCN a través del túnel. Los contenidos multimedia al igual que la señalización SIP circularán a través del túnel.

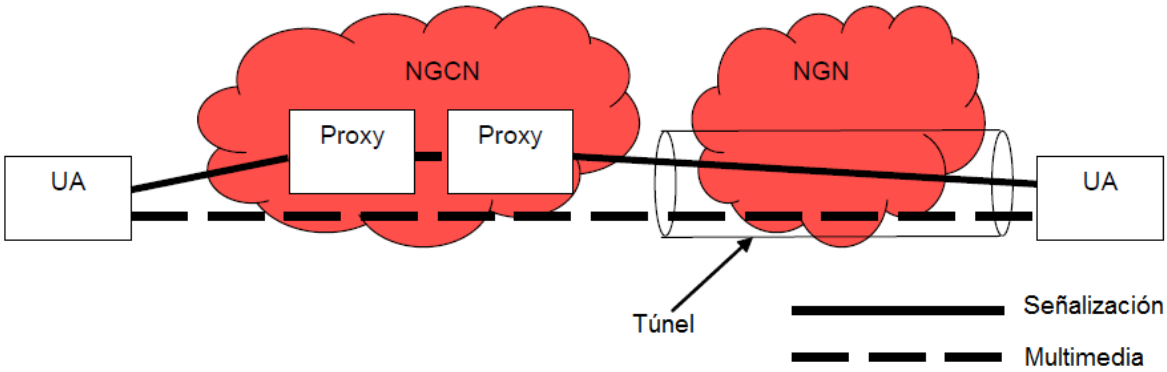


Figura 11 – Arquitectura de Señalización típica para el escenario 3

7.1.4 Escenario 4: Comunicación entre una NGCN y un TE sin utilizar una VPN.

Deberá ser suficiente con dos intermediarios SIP, uno en la NGCN y uno en la NGN. Deberán proporcionarse intermediarios SIP adicionales en la NGN únicamente si estos le permiten a la NGN ofrecer servicios complementarios, por ejemplo, dar garantías de Calidad de Servicio (QoS) para los contenidos multimedia. Los intermediarios SIP en la NGN deben ser transparentes a la información de la señalización SIP que no es relevante a aquellos intermediarios, incluyendo cualquier extensión SIP no respaldada (normalizada o propietaria). Ya sea que la NGN proporcione o no cualquier intermediario SIP, los contenidos multimedia pueden o no circular a través de la misma NGN.

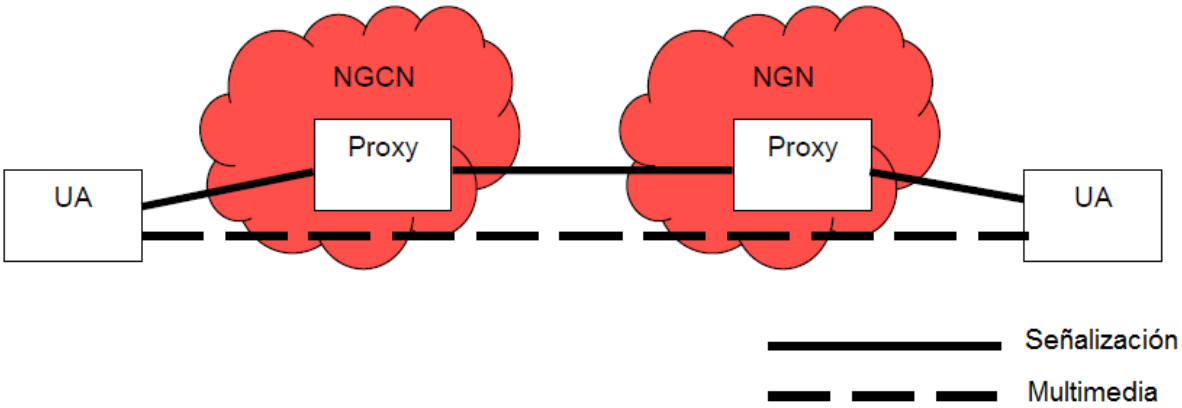


Figura 12 – Arquitectura de Señalización típica para el escenario 4

7.1.5 Escenario 5 – Comunicación entre una NGCN y una RTPC/RDSI.

Deberá ser suficiente con dos intermediarios SIP, uno en la NGCN y uno en la NGN. El intermediario SIP en la NGN funcionará como el proxy de entrada/salida para el UA de la pasarela. Deberán proporcionarse intermediarios SIP adicionales en la NGN únicamente si estos le permiten a la NGN ofrecer servicios complementarios. Los contenidos multimedia pueden o no circular a través de la misma NGN.

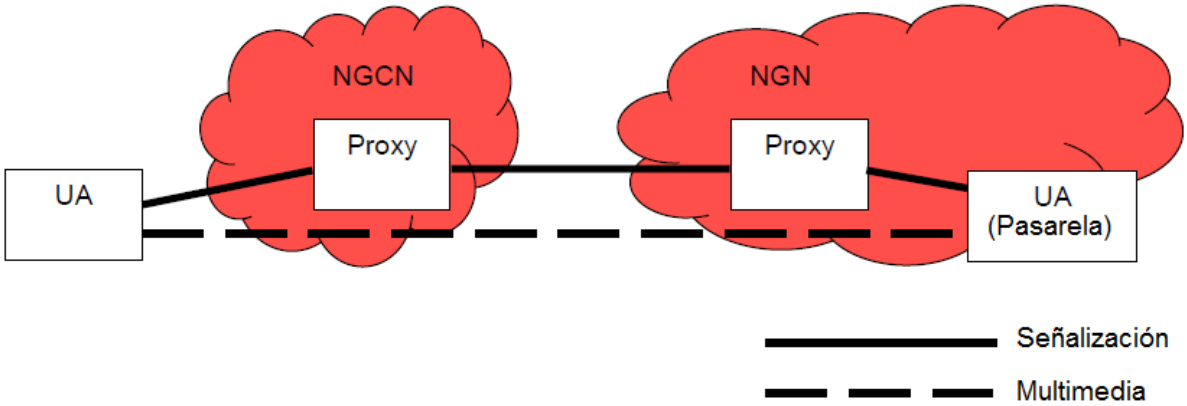


Figura 13 – Arquitectura de Señalización típica para el escenario 5

7.2 Traducción de Direcciones de Red Transversal (NAT-T)

Los dispositivos NAT están presentes generalmente en los límites de la red para proporcionar una conexión, normalmente de manera temporal, entre las direcciones IP y los puertos que pertenecen al espacio interno de la dirección y direcciones IP y puertos que pertenecen al espacio externo de la dirección. Un Traductor de Direcciones de Red ofrece varios beneficios a la red en cuestión, entre otros: provisión de un espacio de dirección más extenso internamente sin utilizar la cantidad correspondiente de espacio público de direcciones y el efecto firewall de no permitir la circulación de paquetes desde la red externa hasta la red interna (entrante) sin antes abrir una conexión transfiriendo paquetes desde la red interna hasta la red externa (saliente).

La Traducción de Direcciones de Red Transversal puede ser un tema importante para la comunicación basada en SIP, porque puede ser necesario que la señalización SIP o el flujo multimedia traspasen un Traductor de Direcciones de Red.

7.2.1 Traducción de Direcciones de Red Transversal (NAT-T) para señalización SIP

El primer problema de la Traducción de Direcciones de Red Transversal tiene que ver con la señalización SIP. En términos generales, este no es un problema si la comunicación se inicia desde el interior del Traductor de Direcciones de Red Transversal, puesto que el primer paquete saliente abrirá una conexión que después aplicará tanto para paquetes salientes como para paquetes entrantes.

Para el mecanismo común de transporte, el Protocolo de Control de Transmisión (TCP) (incluyendo la Seguridad en la Capa de Transporte (TLS) sobre TCP), esto significa que la conexión debe establecerse en la dirección saliente. También quiere decir que la conexión debe mantenerse incluso después de la finalización de cualquier transacción saliente (petición saliente y respuesta entrante) en caso de que las peticiones entrantes lleguen posteriormente. Las conexiones NAT pueden mantenerse activas refrescando la conexión periódicamente. Podría ser necesario establecer y mantener conexiones TCP múltiples donde haya entidades SIP múltiples en uno o ambos lados del NAT con el propósito de repartir las cargas.

Para el Protocolo de Datagramas de Usuario (UDP) debe enviarse un paquete inicial de salida para abrir la conexión. Dado que la respuesta no se relaciona con la petición a nivel de transporte, es necesario enviar explícitamente la respuesta a una petición saliente al puerto desde el que se recibió en vez de al puerto que se indica en el encabezado de direccionamiento de la petición SIP. Es necesario enviar paquetes keepalive periódicamente para mantener la conexión abierta para peticiones entrantes. El UDP se considera un protocolo de transporte improbable para el acceso a una NGN debido a su falta de fiabilidad, su incapacidad para ser asegurado por la TLS y también por su limitado tamaño máximo de carga útil. Por consiguiente, no se tendrá en cuenta en secciones posteriores del presente Informe Técnico.

7.2.1.1 Escenario 1 – Comunicación entre NGCNs utilizando una VPN.

La Traducción de Direcciones de Red Transversal no debe ser un problema si el túnel VPN conecta dos partes de una NGCN que comparten el mismo espacio de dirección IP, aunque la VPN puede extenderse a través de cualquier cantidad de Traductores de Direcciones de Red Transversal.

Si el túnel VPN conecta dos partes de una NGCN con espacios de dirección IP diferentes (por ejemplo, dos empresas estrechamente relacionadas), esto equivale al uso de Traductores de Direcciones de Red Transversal entre partes diferentes de una NGCN cuando no hay una NGN intermedia. Este no es un problema que surge de la participación de una NGN, en consecuencia se considera fuera del alcance de este Informe Técnico.

7.2.1.2 Escenario 2 – Comunicación entre NGCNs sin utilizar una VPN

En este escenario, es necesario enviar las peticiones SIP desde el intermediario SIP en una NGCN hasta el intermediario SIP en la otra NGCN. En este escenario, es probable que exista un Traductor de Direcciones de Red Transversal en el límite entre la NGCN y la NGN y asimismo entre la NGCN homóloga y la NGN. Suponiendo que los intermediarios SIP de la NGCN se encuentren en el lado interno de su Traductor de Direcciones de Red Transversal respectivo, puede ser necesario que las peticiones SIP (y las respuestas) traspasen dos Traductores de Direcciones de Red Transversal. Cada intermediario SIP de la NGCN debe por tanto tener una dirección IP enrutable globalmente (o una dirección IP del espacio de dirección en uso dentro de la NGN) para recibir peticiones SIP de los intermediarios SIP en otras NGCNs y cada Traductor de Direcciones de Red Transversal debe configurarse para permitir que los paquetes entrantes no solicitados desde cualquier fuente sean dirigidos a la dirección IP interna apropiada y al puerto del intermediario SIP. De lo contrario, las peticiones SIP no pedidas no podrían alcanzar el intermediario SIP. Un intermediario SIP no puede saber de dónde vendrán las peticiones no solicitadas y por consiguiente no puede abrir conexiones NAT anticipadamente emitiendo paquetes salientes. Si no, el intermediario SIP podría ubicarse en el lado externo del Traductor de Direcciones de Red Transversal, es decir entre el Traductor de Direcciones de Red Transversal y la NGN. En este caso, la Traducción de Direcciones de Red Transversal es un asunto interno de la NGCN.

Aplicarán consideraciones adicionales cuando las peticiones pasen a través de NGNs múltiples con espacios de dirección IP diferentes o cuando los intermediarios SIP existan dentro de las NGNs.

7.2.1.3 Escenario 3 - Comunicación entre una NGCN y un TE utilizando una VPN.

Las consideraciones de la sección 7.2.1.1 aplican cuando el TE actúa como parte de la NGCN.

7.2.1.4 Escenario 4 - Comunicación entre una NGCN y un TE sin utilizar una VPN.

En este escenario, es necesario enviar las peticiones SIP desde el intermediario SIP en la NGCN hasta el intermediario SIP en la NGN y viceversa. Es probable que exista un Traductor de Direcciones de Red Transversal en el límite entre la NGCN y la NGN. Suponiendo que el intermediario SIP de la NGCN se encuentre en el lado interno de su Traductor de Direcciones de Red Transversal, las peticiones SIP (y las respuestas) tienen que traspasar el Traductor de Direcciones de Red Transversal. El intermediario SIP de la NGCN debe por tanto tener una dirección IP enrutable globalmente (o una dirección IP del espacio de dirección en uso dentro de la NGN) para recibir peticiones SIP de los intermediarios SIP en otras NGCNs y cada Traductor de Direcciones de Red Transversal debe

configurarse para permitir que los paquetes entrantes no solicitados desde cualquier fuente sean dirigidos a la dirección IP interna apropiada y al puerto del intermediario SIP de la NGCN. De lo contrario, las peticiones SIP no pedidas no podrían alcanzar el intermediario SIP de la NGCN. Se supone que el intermediario SIP no puede saber de dónde vendrán las peticiones no solicitadas y por consiguiente no puede abrir conexiones NAT anticipadamente emitiendo paquetes salientes.

Aplicarán consideraciones adicionales cuando las peticiones pasen a través de NGNs múltiples con espacios de direcciones IP diferentes o cuando los intermediarios SIP existen dentro de las NGNs.

7.2.1.5 Escenario 5 - Comunicación entre una NGCN y una RTPC/RDSI.
Las consideraciones son similares a las del escenario 4.

7.2.2 Traducción de Direcciones de Red Transversal (NAT-T) para flujos multimedia.
El segundo tema más serio relacionado con la Traducción de Direcciones de Red Transversal tiene que ver con los flujos multimedia. Las direcciones IP y los puertos de recepción de contenidos multimedia se señalizan en mensajes SIP utilizando el protocolo SDP. Si un UA interno señaliza su dirección IP y puerto de recepción a un UA externo, la dirección IP y el puerto interno serán en general inútiles para el UA externo. La dirección y el puerto pueden no existir en el espacio de dirección externo o pueden estar asignados a un dispositivo diferente. Por consiguiente, la dirección IP y el puerto externos deben estar señalizados en el protocolo SDP. Para hacer esto, el UA interno debe descubrir su dirección IP y puerto externos.

En la mayoría de las situaciones en que los contenidos multimedia se transportan sobre el Protocolo UDP, el servidor STUN (Simple Traversal of UDP through NATs) proporciona el medio adecuado para encontrar la dirección IP y el puerto. El UA interno envía una petición a un servidor STUN en la red externa y el servidor STUN responde con la dirección IP y el puerto de donde parece venir la petición, es decir, la dirección IP y puerto externos. Esto requiere de un servidor STUN en la red externa. El hecho de enviar una petición STUN abrirá una conexión NAT si ya no existía una, y esta conexión NAT se usa para el contenido multimedia mismo. Esto no funciona para algunos tipos de NAT, pero se cree que estos son poco comunes.

NOTA
En particular, esto no funciona para el tipo de NAT conocido comúnmente como "simétrico", donde se abre una conexión a una dirección y puerto especifico en el lado público, por lo tanto una conexión abierta al servidor STUN no puede usarse para los contenidos multimedia desde una dirección y puerto diferente.

Aunque el STUN proporciona la forma de descubrir la dirección IP y el puerto externo, hay otro asunto que consiste en determinar si el Traductor de Direcciones de Red Transversal es válido, ya que si el UA semejante es interno, deben usarse la dirección IP y el puerto interno, y no los externos. Es más, si la red interna tiene interfaces a más de una red externa, aplicarán diferentes conexiones NAT para cada una y es importante saber cual red externa aplica y obtener la dirección IP y el puerto externo aplicable a esa red externa. Surgen complicaciones posteriores si se traspasa más de un Traductor de Direcciones de Red Transversal entre los dos UAs. La mayoría de estos problemas pueden solucionarse si los UAs en cuestión implementan el estándar ICE (Interactive Connectivity Establishment) (trabajo en curso en el IETF), lo que proporciona la forma de probar las direcciones IP y los puertos candidatos antes de usarse.

Otras consideraciones aplican a los contenidos multimedia que se transportan sobre el Protocolo TCP, por ejemplo, mensajes de texto dentro del contexto de una sesión de conformidad con el protocolo MSRP (Message Session Relay Protocol) (trabajo en curso en el IETF). Estos no se consideran en la presente edición de este Informe Técnico.

Otro enfoque que en ocasiones se adopta para solucionar el problema de la Traducción de Direcciones de Red Transversal para el tráfico multimedia es el uso de una ALG que se encuentra en la ruta de señalización SIP (puede combinarse con un intermediario SIP, por ejemplo) y abre conexiones NAT y regula direcciones SDP y puertos apropiadamente. Esto se opone a los principios de la arquitectura del protocolo SIP ya que exige que un

intermediario SIP registre y modifique el cuerpo del mensaje SIP (SDP). El registro fracasará si el cuerpo del mensaje se cifra y la modificación fallará si el cuerpo del mensaje tiene integridad protegida. En consecuencia, no se recomienda este enfoque.

Sin embargo, otro enfoque involucra el uso de un Servidor de Políticas de Red (NPS) al que acceden los UAs para establecer conexiones NAT (ver 7.7).

7.2.2.1 Escenario 1 – Comunicación entre NGCNs utilizando una VPN.

Aplican las consideraciones de la sección 7.2.1.1

7.2.2.2 Escenario 2 – Comunicación entre NGCN sin utilizar una VPN.

Para los contenidos multimedia que se transportan sobre el Protocolo UDP, cada UA debe determinar la dirección IP y el puerto externos que corresponden a la dirección IP y puerto internos en los que se recibirá tal contenido multimedia y debe incluir esto en la oferta o respuesta SDP al UA semejante. Puede ser necesario utilizar el estándar ICE para determinar si esto se requiere. Cada UA tendrá que utilizar un servidor STUN en la NGN para descubrir su propia dirección IP y puerto externos.

REQUISITO # 21 DE UNA NGN: la NGN debe proporcionar un servidor STUN.

Alternativamente, los UAs pueden utilizar Servidores de Políticas de Red (NPS) (ver 7.7)

7.2.2.3 Escenario 3 – Comunicación entre una NGCN y un TE utilizando una VPN.

Aplican las consideraciones de la sección 7.2.1.3

7.2.2.4 Escenario 4 – Comunicación entre una NGCN y un TE sin utilizar una VPN.

Para los contenidos multimedia que se transportan sobre el Protocolo UDP, un UA en la NGCN debe determinar la dirección IP y el puerto externos que corresponden a la dirección IP y puerto internos en los que se recibirá tal contenido multimedia y debe incluir esto en la oferta o respuesta SDP al UA semejante. Puede ser necesario utilizar el estándar ICE para determinar si esto se requiere. El UA de la NGCN tendrá que utilizar un servidor STUN en la NGN para descubrir su propia dirección IP y puerto externos. El uso del estándar ICE requiere del soporte correspondiente a los UAs en la NGN.

Alternativamente, los UAs pueden utilizar servidores de políticas (ver 7.7)

7.2.2.5 Escenario 5 – Comunicación entre una NGCN y una RTPC/RDSI.

Para un contenido multimedia que se transporta sobre el Protocolo UDP, un UA en la NGCN debe determinar la dirección IP y el puerto externos que corresponden a la dirección IP y puerto internos en los que se recibirá tal contenido multimedia y debe incluir esto en la oferta o respuesta SDP a la pasarela. Puede ser necesario utilizar el estándar ICE para determinar si esto se requiere. El UA de la NGCN tendrá que utilizar un servidor STUN en la NGN para descubrir su propia dirección IP y puerto externos. El uso del estándar ICE requiere del soporte correspondiente en la pasarela.

Alternativamente, los UAs pueden utilizar servidores de políticas (ver 7.7)

REQUISITO 22 DE UNA NGN: Puede ser necesario que las pasarelas en una NGN respalden el estándar ICE.

7.3 Traspaso de Firewall

Los firewalls están presentes generalmente en los “bordes” de las redes para evitar el tráfico no deseado a través de los mismos, en especial el tráfico entrante. Los Traductores de Red Transversal también prestan un servicio parcial de firewall al no permitir que las peticiones que provienen desde el lado externo hasta el interno abran las

conexiones. Este tema se discute en la sección 7.1. Los firewalls pueden imponer restricciones adicionales, algunas de las cuales pueden ser perjudiciales para la comunicación multimedia basada en el protocolo SIP (por ejemplo el rechazo de todo el tráfico UDP).

En general, la apertura de los canales del firewall enviando paquetes iniciales desde el interior al exterior del mismo ayudará. De todas maneras, esto debe hacerse para la Traducción de Direcciones de Red Transversal.

Normalmente, se espera que los firewalls estén configurados para permitir que la señalización SIP se lleve a cabo pues ésta usualmente involucra direcciones IP de Intermediarios SIP y números de puerto específicos. Es probable que el flujo multimedia sea un problema mucho más grande porque los números de puerto se escogen de manera dinámica y es improbable que los firewalls mantengan canales abiertos para toda la gran cantidad de posibilidades.

Si los firewalls pueden abrirse en cada dirección enviando un paquete inicial en dirección de salida, entonces esta puede ser una solución aceptable. Enviar y recibir en el mismo puerto es generalmente un pre-requisito para que esto funcione.

Un enfoque que a veces se adopta para solucionar el problema del Traspaso de Firewall para flujo multimedia, es el uso de una ALG que se encuentra en la ruta de señalización SIP (Puede combinarse con un intermediario SIP, por ejemplo) y abre canales de firewall que se basan en direcciones IP y puertos en los cuerpos SDP de los mensajes SIP. Esto se opone a los principios de la arquitectura del protocolo SIP ya que exige que un intermediario SIP registre el cuerpo del mensaje SIP (SDP). En especial, el registro fracasará si el cuerpo del mensaje se cifra. También puede fallar si hay información en el SDP que debe tenerse en cuenta pero la ALG no la comprende. Los estudios sobre seguridad extremo a medio en el IETF pueden ofrecer una solución al problema de cifrado.

Otro enfoque tiene que ver con el uso de un servidor de políticas al que acceden los UAs para abrir canales de firewall (ver 7.7).

7.3.1 Escenario 1 – Comunicación entre NGCNs utilizando una VPN.

El traspaso de firewall no debería ser un problema si el túnel VPN pasa a través de cualquier firewall intermedio. El establecimiento de un túnel VPN está fuera del alcance de este Informe Técnico.

7.3.2 Escenario 2 – Comunicación entre NGCNs sin utilizar una VPN.

Los firewalls generalmente se encuentran en el límite de cada NGCN protegiéndola desde la NGN. Se necesitan otras soluciones para los casos donde los firewalls no se abren simplemente enviando paquetes de salida. El intermediario SIP podría abrir canales en la NGCN en cuestión, pero esto está sujeto a las dificultades que se describen en la sección 7.3. Una mejor solución sería que cada UA utilice un servidor de políticas para abrir canales, con base en las direcciones IP y puertos de salida y llegada que se intercambian a través del protocolo SDP.

Los firewalls también pueden existir en el límite de la NGN protegiéndola desde cada NGCN. En este caso, no es posible utilizar paquetes de salida para abrir canales. La apertura de canales por parte de un intermediario SIP estaría sujeta a las dificultades que se describen en la sección 7.3. Sería mejor que cada UA utilizara un servidor de políticas de la NGN (bajo instrucción de un intermediario SIP en la NGN).

REQUISITO # 23 DE UNA NGN: si una NGN proporciona firewalls, tendrá que proporcionar la manera de abrir canales a través del firewall para los contenidos multimedia entre dos UAs de la NGCN sin depender de la habilidad para examinar el Protocolo SDP que pasa entre esos UAs.

7.3.3 Escenario 3 – Comunicación entre una NGCN y un TE utilizando una VPN.

Para este escenario aplican las consideraciones descritas en la sección 7.3.1.

7.3.4 Escenario 4 - Comunicación entre una NGCN y un TE sin utilizar una VPN.
Para este escenario aplican las consideraciones descritas en la sección 7.3.2.

7.3.5 Escenario 5 – Comunicación entre una NGCN y una RTPC/RDSI.
Para este escenario aplican las consideraciones descritas en la sección 7.3.2, excepto que aquí es posible que los paquetes multimedia que se transmiten por la pasarela abran un firewall en la NGN en el límite de la NGCN.

7.4 Identificación

Con el Protocolo SIP como el método de señalización, la identificación de los usuarios y otras entidades debe hacerse a través de Identificadores Uniformes de Recursos (URIs) [4] sip (o sips) o URIs de teléfono "tel" [8].

Un SIP URI tiene el siguiente formato: SIP: user@domain. Cada dominio (como se identifica en el campo de dominio) es responsable de asignar campos de usuario a sus usuarios (usuarios humanos, servicios, etc.). Una NGCN comprenderá uno o más dominios. Una petición de una NGN a una entidad en una NGCN normalmente porta el SIP URI de esa entidad como su destino deseado. La NGN solo necesita entender el campo de dominio del SIP URI para enrutar tal petición al dominio de la NGCN, que es entonces responsable de enrutar la petición a la entidad en cuestión. De este modo, no es necesario que una NGN tenga conocimiento previo de los campos de usuario dentro del dominio de una NGCN, y una NGCN debe tener la libertad de asignar o revocar SIP URIs dentro de su dominio(s) sin consultar a la NGN.

Sin embargo, es preciso que cualquier entidad de la NGCN que necesite ser accesible durante las llamadas desde la RTPC/RDSI tenga una identidad que pueda dirigirse desde/hasta un número telefónico E.164 que es uno entre un grupo de números telefónicos que se asignan a la NGCN. Esto puede lograrse usando URIs de teléfono "tel" donde una entidad identificable en la NGCN tenga un URI de teléfono "tel" como su única identidad o como una identidad alternativa. Si la entidad también tiene una identidad SIP, esta podría simplemente derivar del URI de teléfono "tel", por ejemplo, teniendo el número telefónico como el campo de usuario del SIP URI. La NGCN o la NGN podrían ser responsables de dirigir números telefónicos desde/hasta los SIP URIs.

Para una llamada desde una RTPC/RDSI a una entidad en una NGCN, la NGN tendrá que identificar primero el dominio de la NGCN en cuestión (por ejemplo, búsqueda con ENUM [7]). Hay entonces varias maneras de proceder:

- la NGN forma un URI de teléfono "tel" y lo utiliza como el destino deseado de la petición para la NGCN, que después enruta utilizando el URI de teléfono "tel" hasta el UA destino.

- la NGN forma un URI de teléfono "tel" y lo utiliza como el destino deseado de la petición para la NGCN, que después se transforma en SIP URI para un reenvío de llamadas.

- la NGN transforma el número telefónico en SIP URI para el dominio de la NGCN en cuestión y lo utiliza como el destino deseado de la petición para la NGCN.

REQUISITO # 24 DE UNA NGN: una NGN deberá estar en capacidad de aceptar como válido cualquier campo de usuario en un SIP URI para un dominio de la NGCN.

REQUISITO # 25 DE UNA NGN: una NGN tendrá que estar en capacidad de dirigir números telefónicos asignados a una NGCN desde/hasta URIs que son válidos dentro de esa NGCN.

7.5 Suministro de información sobre la identificación.

El destinatario de una petición SIP (los UAS) frecuentemente necesita identificación confiable del origen de la petición. La identificación confiable es crucial para el filtrado de peticiones no deseadas, por ejemplo, para respaldar el uso de listas negras y listas blancas.

Existen dos métodos básicos para lograr esto: la confirmación de identidad salto a salto o la identidad firmada criptográficamente.

Con la confirmación de identidad salto a salto, cada entidad SIP en la ruta de señalización recibe una confirmación de la identidad del origen de la petición desde la entidad SIP anterior, que ha sido autenticada con algunos métodos. El intermediario SIP de salida para el UAC será en general capaz de autenticar el UAC y en consecuencia podrá confirmar la identidad del UAC a la entidad SIP siguiente en la ruta de señalización, que a su vez podrá confirmar esa identidad a la siguiente entidad. Esto funciona únicamente si existe una cadena de confianza ininterrumpida y unos saltos de señalización autenticados. Si una entidad no confía en la identidad confirmada desde la entidad anterior, no debería usar esa información y no debería transmitirla a otras entidades.

El mismo UAC (si tiene una clave y un certificado privados convenientes para este propósito) o un servidor de identidad dentro del mismo dominio (por ejemplo, combinado con el intermediario SIP de salida) que haya autenticado el UAC por otros medios, pueden introducir una identidad firmada criptográficamente. Un destinatario de una entidad firmada criptográficamente puede decidir si confía en la identidad con base en el certificado del firmante.

Existe un requisito similar para que un UAC sea capaz de obtener identificación confiable del origen de la respuesta. Una respuesta no necesariamente proviene de una entidad con la misma identidad que la de la petición original ya que una petición puede redestinarse. Por dificultades técnicas todavía no se ha encontrado solución a este problema.

El suministro de información sobre la identificación dependerá de los requisitos de privacidad del usuario en cuestión. Si una NGCN no desea que su identidad se revele a otras partes, esta no suministrará la identidad a la NGN o, si hay una relación de confianza establecida, pasará la identidad con un marcador de privacidad. En el último caso, la NGN es responsable de asegurar que la identidad no se revele.

Existen consideraciones similares sobre la privacidad que aplican en el sentido opuesto.

7.5.1 Escenario 1 – Comunicación entre NGCNs utilizando una VPN.

Este es un problema al interior de la NGCN o entre NGCNs que no tiene ningún impacto en la NGN.

7.5.2 Escenario 2 – Comunicación entre NGCNs sin utilizar una VPN.

Si una NGCN proporciona una identidad firmada criptográficamente, este es un problema entre NGCNs que no tiene impacto en la NGN (más que en el transporte).

Si no hay un intermediario SIP en la NGN, una NGCN puede proporcionar una identidad confirmada a la otra NGCN, aunque esto podría no ser aceptado a menos que haya una relación de confianza entre las dos.

Si hay un intermediario SIP en la NGN, una identidad confirmada dependería de una relación de confianza transitiva: la NGN confía en la primera NGCN y la segunda NGCN confía en la NGN.

7.5.3 Escenario 3 – Comunicación entre una NGCN y un TE utilizando una VPN.

Para este escenario aplican las consideraciones descritas en la sección 7.5.1.

7.5.4 Escenario 4 – Comunicación entre una NGCN y un TE sin utilizar una VPN.

Para la información sobre la identificación enviada desde la NGN hasta la NGCN, esta última debería estar en capacidad de aceptar ya sea una identidad confirmada o una identidad firmada. La primera requiere de confianza en la NGN y la segunda requiere de confianza en el firmante de la información sobre la identidad como se indica en un certificado.

REQUISITO # 26 DE UNA NGN: una NGN deberá estar en capacidad de suministrar a una NGCN ya sea una identidad confirmada o una identidad firmada criptográficamente.

En el sentido opuesto, la NGCN podría suministrar o una identidad confirmada o una identidad firmada. Si la NGN percibe a la NGCN como un semejante, podría aceptar una identidad confirmada y a su vez afirmar esta identidad al reenviar la petición hacia los UAS.

REQUISITO # 27 DE UNA NGN: una NGN debe estar en capacidad de aceptar una identidad confirmada como el origen de una petición desde una NGCN si tal red es confiable.

De lo contrario, la NGN podría únicamente aceptar una identidad firmada criptográficamente y aún entonces podría requerir que una Autoridad de Certificación (CA) conocida firme el certificado del firmante para poder confiar en ella. Ya sea que la NGN confíe o no en la identidad firmada, esta debería de todas formas estar en capacidad de enviar la identidad firmada con la petición hacia los UAS. Los UAS o el usuario final pueden entonces decidir si confiar o no en la identidad.

REQUISITO # 28 DE UNA NGN: una NGN debe estar en capacidad de aceptar una identidad firmada criptográficamente como el origen de una petición desde una NGCN si ésta no proporciona una identidad confirmada o si la NGN es incapaz de confiar en una identidad confirmada.

7.5.5 Escenario 5 – Comunicación entre una NGCN y una RTPC/RDSI.

Para la información sobre la identidad enviada desde la NGN hasta la NGCN, esta última debería estar en capacidad de aceptar ya sea una identidad confirmada o una identidad firmada. La primera requiere de confianza en la NGN y la segunda requiere de confianza en el firmante de la información sobre la identidad como se indica en un certificado.

REQUISITO # 29 DE UNA NGN: una NGN deberá estar en capacidad de suministrar a una Red Corporativa de Próxima Generación ya sea una identidad confirmada o una identidad firmada criptográficamente.

En el sentido opuesto, la NGCN podría suministrar o una identidad confirmada o una identidad firmada. Si la NGN percibe a la NGCN como un semejante, podría aceptar una identidad confirmada y a su vez utilizar esta identidad confirmada para obtener una identidad que sea enviada a la RTPC/RDSI.

De lo contrario, la NGN podría únicamente aceptar una identidad firmada criptográficamente y aún entonces podría requerir que una CA conocida firme el certificado del firmante para poder confiar en ella y obtener una identidad que sea enviada a la RTPC/RDSI.

En todo caso, la NGCN debe suministrar una identidad desde la cual la NGN pueda obtener un número telefónico.

REQUISITO # 30 DE UNA NGN: una NGN debe estar en capacidad de aceptar una identidad firmada criptográficamente como el origen de una petición desde una NGCN si ésta no proporciona una identidad confirmada o si la NGN es incapaz de confiar en una identidad confirmada.

7.6 Seguridad

La seguridad es un factor importante a tener en cuenta para el despliegue de cualquier aplicación en una red IP debido a la habilidad para espiar, hacerse pasar por alguien, modificar datos en tránsito, etc., que puede tener un atacante con acceso a la red. Si bien esto es obviamente cierto para la Internet pública, también es cierto para las redes IP "cerradas" (por ejemplo, dentro de una empresa). De hecho, la seguridad es un asunto importante para las NGNs, las NGCNs y para trabajar conjuntamente con NGNs y NGCNs.

Uno de los aspectos de la seguridad es la privacidad. Se espera que las consideraciones sobre la privacidad en el contexto de las NGCN sean diferentes a las consideraciones de las NGNs y es probable que estén reguladas por los requisitos de la empresa en cuestión antes que por requisitos de regulación. Mientras que en las redes públicas el regulador puede tener un interés público de recolectar información sobre ciertos usuarios y sus comunicaciones, esto no sería aceptable para las comunicaciones al interior de las NGCNs entre usuarios comerciales de una única red de este tipo.

REQUISITO # 31 DE UNA NGN: una NGN deberá estar en capacidad de distinguir entre las comunicaciones al interior de la NGCN y las comunicaciones externas y de este modo ser capaz de decidir donde y cuando aplican los requisitos reguladores (por ejemplo, intercepción legal, suministro de información sobre la ubicación, etc.) y donde deben denegarse tales peticiones.

Para las comunicaciones multimedia basadas en protocolos SIP, debe considerarse la seguridad tanto para la señalización (SIP) como para los medios.

7.6.1 Seguridad de Señalización

La seguridad de señalización es importante por varias razones. Primero, es importante autentificar el origen de un mensaje para autorizar cualquier acción que se tome con respecto al mensaje. De lo contrario, un atacante podría obtener acceso no autorizado a los servicios o a la información o llevar a cabo un Ataque de Denegación de Servicios (DoS). Segundo, aunque se autentifique el origen de un mensaje, es importante asegurarse de que no se haya comprometido la integridad de los datos en tránsito. Tercero, la señalización puede contener información confidencial (por ejemplo, las identidades de las partes comprometidas en la comunicación, direcciones IP y puertos a usar para la recepción de los medios, etc.). Esta información debe protegerse del espionaje (eavesdropping).

Puesto que el protocolo SIP utiliza intermediarios SIP, la señalización entre dos UAs comprende en general uno o más saltos (por ejemplo, desde el UA hasta el intermediario SIP, desde el intermediario SIP hasta el siguiente intermediario SIP, etc.). La señalización puede asegurarse separadamente en cada salto utilizando protocolos de seguridad de uso general en la capa de transporte (TLS) o en la capa de red (IPSEC[9]). Estos pueden proporcionar autenticación, protección de identidad y confidencialidad. La autenticación se logra utilizando el cifrado de clave pública a través del cual una entidad tiene una clave privada para firmar mensajes y un certificado que puede publicar para permitir a otras entidades que verifiquen su firma. La autenticación mutua basada en certificados es la norma entre dos intermediarios SIP. Sin embargo, normalmente se utiliza una clave compartida entre el Agente de Usuario SIP y su intermediario SIP local para permitir que el intermediario SIP autentique el UA (un certificado que todavía se usa para permitir que el UA autentique el intermediario SIP). Normalmente, una conexión segura establecida debería conservarse en un modo semi permanente para ser usado por transacciones SIP múltiples en cualquier dirección dada la sobrecarga que implica establecer una nueva conexión segura para cada transacción.

La seguridad debe ser un aspecto esencial para cualquier salto de señalización SIP, ya sea que esté totalmente dentro de una NGCN, totalmente dentro de una NGN o que abarque más de una red. Se espera que exista seguridad en cada salto que conecta los UAs pares/homólogos en cualquier transacción de señalización (seguridad tipo salto a salto). El esquema SIPS URI apunta a asegurar la seguridad tipo salto a salto, pero presenta deficiencias en la autorización del método para lograr la seguridad en el último salto de una petición, es decir, desde el intermediario responsable del dominio en la petición URI a los UAS (Se exige Seguridad en la Capa de Transporte (TLS) en todos los otros saltos).

Sin embargo, desde la perspectiva del UA, los SIPS y la seguridad tipo salto a salto podrían ser insuficientes. Depende de los UAs que confían en los intermediarios SIP ajustarse a la especificación del SIP y no revelar o modificar la información destinada al uso de extremo a extremo. Aunque existe información que los intermediarios SIP deben examinar y quizá también modificar para el enrutamiento o para otros propósitos, hay otro tipo de información que no debería ser relevante para los intermediarios SIP. Si la integridad o confidencialidad de esta información es importante para los UAs, ellos pueden requerir que esa información se asegure de extremo a extremo.

Por ejemplo, la descripción de sesión que se lleva en el protocolo SDP podría ser importante sólo para los UAs y no para los intermediarios SIP. Así, el protocolo SDP es candidato para ser asegurado en los puntos finales. En particular, con el cifrado punto a punto, las direcciones IP y los puertos no necesitan revelarse a los intermediarios SIP. Lo que es más importante, no es necesario revelar las claves de cifrado para la seguridad de los contenidos multimedia.

Otro ejemplo es el transporte de información sobre ubicación geográfica entre UAs. En general, esto no es relevante para los intermediarios SIP (exceptuando las llamadas de emergencia).

El protocolo SIP permite cifrar, autentificar y proteger la integridad de los cuerpos de los mensajes SIP utilizando S/MIME (Extensiones de correo de Internet de Propósitos Múltiples/Seguro). Para hacer uso de esta habilidad, los UAs necesitan claves y certificados privados lo que implica la necesidad de una Infraestructura de Clave Pública (PKI) para proporcionar esta información. Para la gestión de las claves de seguridad de los medios aplican consideraciones similares (ver la sección 7.6.2) y de hecho S/MIME es un mecanismo que puede usarse para asegurar la gestión de claves. Sus implicaciones se discuten en el contexto de gestión de claves para la seguridad de los contenidos multimedia.

Por otro lado, los intermediarios SIP pueden necesitar acceso a algunos aspectos del protocolo SDP, por ejemplo para garantizar el traspaso del firewall o disponibilidad de ancho de banda. Esto puede conllevar a la necesidad de seguridad “extremo a medio”, con la cual un UA pueda asegurar la información entre si mismo y un intermediario SIP conocido.

7.6.1.1 Escenario 1 – Comunicación entre NGCN utilizando una VPN

El túnel VPN proporcionará el cifrado y la protección de la integridad de la señalización SIP cuando atraviese la NGCN. No obstante, la seguridad tipo salto a salto y de extremo a extremo de la señalización SIP pueden aún ser necesarias, pero esto es un asunto interno de la NGCN y está fuera del alcance de este informe técnico.

7.6.1.2 Escenario 2 – Comunicación entre NGCNs sin utilizar una VPN

La señalización SIP se enruta normalmente a través de un intermediario SIP en cada NGCN. El salto de interés es el que se encuentra entre estos dos intermediarios SIP. Es esencial asegurar este salto con TLS o IPSEC (TLS según los SIPS) ya que atraviesa una NGN. Los dos intermediarios SIP tendrán que aceptar los certificados del uno y del otro lo que implica posesión del certificado de la CA en cuestión.

Si la NGN proporciona un intermediario SIP, aplican las consideraciones de la sección 7.6.1.4.

La seguridad de extremo a extremo puede aplicarse entre los UAs para ciertos cuerpos de mensajes SIP. Si cualquiera de los intermediarios SIP de la NGCN requiere acceso a datos cifrados, entonces, tendrán que aplicarse técnicas de seguridad "extremo a medio". Este es un asunto de la NGCN que no tiene ningún impacto en la NGN.

7.6.1.3 Escenario 3 – Comunicación entre una NGCN y un TE utilizando una VPN.

Para este escenario aplican las consideraciones descritas en la sección 7.6.1.1.

7.6.1.4 Escenario 4 - Comunicación entre una NGCN y un TE sin utilizar una VPN.

La señalización SIP se enruta normalmente a través de un intermediario SIP en cada NGCN. El salto de interés es el que se encuentra entre estos dos intermediarios SIP. Es esencial asegurar este salto con TLS o IPSEC (TLS según los SIPS) ya que parte de él atraviesa la NGN. Los dos intermediarios SIP tendrán que aceptar los certificados del uno y del otro lo que implica posesión del certificado de la CA en cuestión.

REQUISITO # 32 DE UNA NGN: una NGN deberá estar en capacidad de respaldar el establecimiento de conexiones seguras desde un intermediario SIP de una NGN hasta un intermediario SIP de una NGCN y viceversa. Además deberá conservar conexiones de un modo semi permanente para uso de transacciones SIP múltiples en cualquier dirección.

REQUISITO # 33 DE UNA NGN: una NGN deberá estar en capacidad de guardar el certificado de la CA para una determinada NGCN y de autenticar el certificado de un intermediario SIP de una NGCN durante el establecimiento de una conexión segura desde/hasta tal intermediario SIP.

REQUISITO # 34 DE UNA NGN: un intermediario SIP de una NGN deberá tener una clave privada y un certificado asociado y usarlos para permitir la autenticación por el intermediario SIP de una NGCN.

Además, es esencial que la NGN se ajuste a las reglas de los SIPS para garantizar a los usuarios la seguridad tipo salto a salto (sujeta a la confianza).

REQUISITO # 35 DE UNA NGN: una NGN deberá respaldar los SIPS al no permitir que una petición a un SIP URI sea remitida en una conexión insegura.

La seguridad de extremo a extremo puede aplicarse entre los UAs para ciertos cuerpos de mensajes SIP. Si el intermediario SIP de la NGCN o el intermediario SIP de la NGN requieren acceso a datos cifrados, entonces, tendrán que aplicarse técnicas de seguridad "extremo a medio".

REQUISITO # 36 DE UNA NGN: un intermediario SIP de una NGN no necesitará modificar la señalización SIP de extremo a extremo.

REQUISITO # 37 DE UNA NGN: en circunstancias ideales, un intermediario SIP de una NGN no debería necesitar acceso de lectura a la señalización de extremo a extremo asegurada. Si así lo requiere, tendrá que utilizar técnicas de seguridad "extremo a medio", pero esto necesitará de la cooperación de los UAs en cuestión y podría no ser aceptable para los usuarios o sus empresas.

7.6.1.5 Escenario 5 – Comunicación entre una NGCN y una RTPC/RDSI

Para este escenario aplican las consideraciones descritas en la sección 7.6.1.4, excepto que aquí la pasarela en la NGN es uno de los UAs y en consecuencia tendrá acceso a la señalización asegurada de puntos finales, si es válido. Para este propósito, la pasarela necesitará una clave privada y un certificado que el UA de la NGCN tendrá que verificar para autenticar la pasarela.

REQUISITO # 38 DE UNA NGN: una NGN deberá respaldar los SIPS en llamadas desde/hasta la pasarela de una RTPC/RDSI.

7.6.2 Seguridad Multimedia

En el presente informe técnico, la seguridad multimedia se estudia en términos de seguridad multimedia en tiempo real (voz y video) que se transporta sobre el Protocolo RTP. Los datos multimedia que se transmiten en el protocolo RTP pueden asegurarse a través del Protocolo Seguro de Transporte en Tiempo Real (SRTP) que expande el protocolo RTP permitiendo que se cifren datos multimedia y añadiendo información para la autenticación y la verificación de la integridad. El Protocolo Seguro de Control de Tiempo Real (SRTCP) proporciona capacidades similares para el Protocolo de Control en Tiempo Real (RTCP).

Puesto que el protocolo RTP normalmente circula de extremo a extremo entre los UAs, el protocolo SRTP también es extremo a extremo. Sin embargo, las entidades intermedias pueden involucrarse para prestar servicios específicos (por ejemplo, transcodificación, conferencias). En este caso, el protocolo SRTP funcionará entre cada UA y la entidad intermedia (que aparece como un UA para cada uno de los otros UAs).

Para activar el uso del protocolo SRTP (y SRTCP) es necesaria la gestión de claves que proporcione a los dos UAs una clave maestra secreta de la que pueden obtenerse claves de sesión. La gestión de claves debe asegurar que:

- la clave secreta (o la información de la cual se obtiene) se entrega a o se acepta únicamente desde una entidad conocida y autenticada; y
- la clave secreta (o la información de la cual se obtiene) no puede espiarse en tránsito.

Para el primer caso, básicamente durante cualquier intercambio de claves, un UA debe asegurar que el UA semejante al que envía la clave o desde el cual la recibe, es un UA con pruebas de que pertenece al usuario con quien el usuario local desea comunicarse. El uso de una clave compartida con este propósito normalmente no es escalable más allá de una comunidad relativamente pequeña, y en consecuencia el uso de cifrado de clave pública es normalmente la única solución viable. El remitente de la información clave la firma utilizando la clave privada asociada con un certificado que el usuario semejante puede asociar con un usuario con el cual espera o desea comunicarse. Esta puede ser una asociación directa o indirecta (por ejemplo, el usuario puede asociar el certificado con la identidad enviada en la señalización (ver la sección 7.4), que el usuario puede entonces asociar con un usuario con el cual espera o desea comunicarse.

En consecuencia, para respaldar la seguridad multimedia de un modo escalable, los UAs deben tener claves privadas y certificados asociados. Además, necesitan tener un medio para verificar las firmas de los pares, ya sea con un medio seguro e independiente para obtener certificados de estos últimos o con certificados apropiados de la CA para verificar los certificados recibidos de los pares. Esto impone un requisito importante y es la Infraestructura PKI en medios en los que se requiere seguridad multimedia. En particular:

- deben producirse una clave privada y un certificado asociado para cada usuario;
- esta información debe instalarse de manera segura en cualquier UA que el usuario utilice, por ejemplo, por descarga segura de un servidor de credenciales;
- los UAs semejantes deben estar en capacidad de obtener certificados de una fuente confiable para comprobar firmas (bien sea certificados pares para confirmar las firmas o certificados de una CA para confirmar las firmas de los certificados pares).

Ya que tal Infraestructura PKI está en su sitio, también puede usarse como la base para cifrar información clave para la transmisión de extremo a extremo entre UAs, previniendo así el espionaje o eavesdropping. Un UA puede generar una clave, firmarla con su propia clave privada y cifrarla utilizando la clave pública del UA semejante (del certificado del UA semejante). El UA semejante puede verificar la firma utilizando la clave pública del UA remitente

(del certificado del UA remitente) y descifrar la clave utilizando su propia clave privada. Esto puede lograrse utilizando un mecanismo SIP de seguridad extremo a extremo de propósito general (es decir S/MIME) para asegurar el protocolo SDP incluyendo cualquier información sobre gestión de claves. Alternativamente, la seguridad puede lograrse incluyendo un protocolo de gestión de claves como por ejemplo MIKEY (Multimedia Internet KEYing) dentro del protocolo SDP. MIKEY proporciona su propio medio para autenticar y cifrar información clave, nuevamente con base en la Infraestructura PKI. Una ventaja de MIKEY es que no es necesario enviar un clave en cada dirección, una clave única enviada en una dirección puede usarse para obtener dos claves maestras SRTP diferentes, una para cada dirección. Otra ventaja es que no necesita que el SDP entero se asegure.

Una desventaja de enviar una clave cifrada es que el UA remitente necesita conocer la clave pública del UA destinatario con antelación. Aún si se puede obtener un certificado para el usuario representado por la petición URI en una petición SIP INVITE, el redireccionamiento de los intermediarios SIP puede resultar en que la petición llegue a un UAS que no tenga la clave para descifrar. Esto puede provocar ciclos adicionales de señalización SIP. Una alternativa que se encuentra en consideración para MIKEY es que el UAC envíe su certificado a los UAS y después, en la respuesta, los UAS pueden cifrar información clave utilizando ese certificado.

Una alternativa es utilizar el Protocolo de Intercambio de Claves Diffie-Hellman, por el cual un componente Diffie-Hellman puede enviarse firmado pero no cifrado, evitando así la necesidad de adquirir el certificado del UA destinatario. MIKEY proporciona respaldo para el Protocolo de Intercambio de Claves Diffie-Hellman protegido por firmas digitales con base en la Infraestructura de Clave Pública (PKI).

7.6.2.1 Escenario 1 – Comunicación entre NGCNs utilizando una VPN.

El túnel VPN proporcionará seguridad para todo el tráfico a través de la NGN, incluyendo el tráfico multimedia, no obstante el protocolo SRTP punto a punto será necesario entre los UAs para proporcionar seguridad también dentro de la NGCN.

La gestión de claves se hará entre los UA sin impacto en la NGN. El túnel VPN asegura el intercambio de claves a través de la NGN, pero en la práctica, se necesitará seguridad de extremo a extremo entre los UA para cubrir también la transmisión dentro de la NGCN.

Es probable que una única CA firme todos los certificados dentro de la NGCN y en consecuencia la verificación de los certificados es relativamente fácil.

En este escenario la NGN es transparente para la seguridad multimedia y la gestión de claves, por lo tanto, la seguridad multimedia en este escenario no se estudia posteriormente en este Informe Técnico.

7.6.2.2 Escenario 2 – Comunicación entre NGCN sin utilizar una VPN.

Normalmente, será necesario proporcionar SRTP de extremo a extremo entre los UAs en las diferentes NGCN, asegurando de ese modo los contenidos multimedia a través de cada NGCN y la NGN. La excepción es si la NGN interviene en los contenidos multimedia de alguna manera, por ejemplo, controlando o monitoreando, transcodificando y ofreciendo servicios de conferencia.

La gestión de claves será entre los UAs sin impacto en la NGN. Necesitará asegurarse de extremo a extremo.
Puesto que hay dos NGCNs involucradas, es probable que CA diferentes firmen los certificados. Por consiguiente, cada UA tiene que reconocer la CA del otro UA. Si no ha habido contacto previo, las CA pueden no ser fácilmente aceptables y puede ser necesario consultar a los usuarios.

Si la NGCN proporciona intermediarios SIP en este escenario, tendrán que ser transparentes al protocolo SRTP y a la gestión de claves.

REQUISITO # 39 DE UNA NGN: la NGN tendrá que ser transparente al protocolo SRTP y a la gestión de claves para ofrecer servicios complementarios y con el conocimiento y permiso de los usuarios en cuestión, excepto donde una NGN interviene en los contenidos multimedia de alguna manera.

Si la NGN interviene en los contenidos multimedia de cualquier forma, tendrá que poner fin al protocolo SRTP y a la gestión de claves. En otras palabras, tendrá que aparecer como un UA a los UAs en las NGCN. Esto tiene un impacto significativo ya que quiere decir que los UAs en la NGCN tendrán que efectuar gestión de claves no entre sí sino con la entidad intermedia. Esto implica que un UA debe aceptar un certificado de la entidad intermedia antes que del UA semejante en la NGCN remota. Un UA debe tener los medios para verificar tal certificado, lo que significa tener disponible el certificado apropiado de la CA y también estar en capacidad de asociar el sujeto del certificado con algo significativo. Es probable que los usuarios tengan que involucrarse en la autorización de tal acuerdo. Un usuario no dispuesto a autorizar tal acuerdo tendrá que encontrar otras formas de lograr la comunicación requerida, es decir, sin que la NGN esté involucrada con los medios.

REQUISITO # 40 DE UNA NGN: una NGN deberá estar en capacidad de evitar intervenir en los contenidos multimedia si es necesario asegurarlos de extremo a extremo.

REQUISITO # 41 DE UNA NGN: una NGN que interviene en los contenidos multimedia tendrá que proporcionar seguridad multimedia y gestión asociada de claves entre la entidad intermedia y cada UA.

REQUISITO # 42 DE UNA NGN: la NGN tendrá que proporcionar un certificado para una entidad intermedia que pueda ser verificado por el UA de la NGCN para proporcionar gestión de claves entre esa entidad intermedia y un UA en una NGCN.

7.6.2.3 Escenario 3 – Comunicación entre una NGCN y un TE utilizando una VPN.

Para este escenario aplican las consideraciones descritas en la sección 7.6.2.1.

7.6.2.4 Escenario 4 – Comunicación entre una NGCN y un TE sin utilizar una VPN.

El protocolo SRTP de extremo a extremo normalmente será necesario entre el UA en la NGCN y el UA en la NGN. Las consideraciones son muy similares a las del escenario dos.

7.6.2.5 Escenario 5 – Comunicación entre una NGCN y una RTPC/RDSI

El protocolo SRTP de extremo a extremo normalmente será necesario entre el UA en la NGCN y la pasarela en la NGN, asegurando así los medios a través de la NGCN y la NGN excepto si la NGN interviene en los medios de un modo diferente a la pasarela, por ejemplo, controlando o monitoreando, transcodificando y ofreciendo servicios de conferencia.

La gestión de claves será entre el UA y la pasarela, sin otro impacto en la NGN. Tendrá que asegurarse en los puntos finales.

Tanto el UA como la pasarela necesitarán una clave privada y un certificado y tendrán que aceptar el certificado de cada uno. Normalmente, el UA deberá aprovisionarse para aceptar certificados de cualquier pasarela anticipada. De igual manera, la pasarela deberá aprovisionarse para aceptar certificados de usuarios legítimos.

REQUISITO # 43 DE UNA NGN: una pasarela de una RTPC/RDSI en una NGN deberá estar en capacidad de proporcionar un certificado que los usuarios de la NGCN puedan reconocer como auténtico.

REQUISITO # 44 DE UNA NGN: una pasarela de una RTPC/RDSI en una NGN deberá estar en capacidad de confirmar/verificar certificados de usuarios legítimos de una NGCN.

7.7 Política de Sesión

Una red debería imponer ciertas políticas en el uso de su infraestructura de comunicación. En particular, debería introducir un intermediario multimedia o imponer limitaciones en los contenidos multimedia que componen una sesión. Algunas razones para introducir un intermediario multimedia incluyen monitoreo de tráfico, cumplimiento de acuerdos a nivel de servicio y control de acceso, balanceo de carga y configuración de tráfico, marcado de paquetes con QoS, Traducción de direcciones de red transversal/traspaso de firewall, ocultamiento a nivel de multimedia de la topología e interworking (interredes) IPv4/IPv6. La mayoría pueden lograrse a través de la intervención en la capa de transporte o más abajo. La intervención en una capa más alta, por ejemplo en el protocolo RTP, puede no ser factible si los medios están asegurados. Algunos ejemplos de limitaciones en los medios incluyen tipos de contenidos multimedia permitidos, codecs (codificadores y decodificadores) permitidos y ancho de banda máximo permitido.

Normalmente, las limitaciones para las redes locales (o para segmentos de redes locales) estarán disponibles para los usuarios durante la configuración del UA, pero la introducción de los intermediarios multimedia dependerá de la sesión que se establece. Algunas sesiones se extenderán más allá de los segmentos de redes locales e involucrarán otros segmentos o redes, que también deberían introducir un intermediario multimedia o imponer limitaciones en las sesiones.

Los intermediarios SIP no están necesariamente en buena posición para imponer políticas introduciendo intermediarios multimedia y limitando las capacidades de sesión. Esto se debe al carácter extremo a extremo del protocolo SDP en el Protocolo de Inicio de Sesión SIP y en particular al hecho de que puede cifrarse previniendo así que sea visible para los intermediarios SIP o que puede verificarse la integridad previniendo así la modificación. El propósito de los intermediarios SIP es establecer comunicación de señalización entre los UAs SIP enrutando las peticiones y respuestas SIP. Es mejor dejar que otras entidades conocidas como Servidores de Políticas de Red (NPS) asuman la función independiente de imponer políticas de sesión. Los UAs SIP pueden contactar a los NP con detalles de la sesión que se va a establecer (con base en el protocolo SDP enviado y recibido) y estos últimos pueden proponer ajustes para introducir intermediarios o para limitar las capacidades de sesión. Dominios diferentes tendrán normalmente NPS diferentes y un intermediario SIP para un dominio determinado puede señalizar la identidad del NPS para ese dominio de los UAs. De este modo, los UAs pueden hacer contacto con cualquier NPS relevante. Se siguen estudiando detalles de este mecanismo en el IETF:

7.7.1 Escenario 1 – Comunicación entre NGCNs utilizando una VPN.

La política de la NGN puede tener un impacto en el establecimiento del túnel VPN, pero esto se encuentra fuera del alcance de este informe técnico. La política de la NGCN es un asunto interno de la misma.

7.7.2 Escenario 2 – Comunicación entre NGCN sin utilizar una VPN.

Tanto la NGN como las dos NGCNs pueden imponer potencialmente políticas de sesión.

7.7.3 Escenario 3 – Comunicación entre NGCNs y un TE utilizando una VPN.

Para este escenario aplican las consideraciones descritas en la sección 7.7.1.

7.7.4 Escenario 4 – Comunicación entre NGCNs y un TE sin utilizar una VPN.

Tanto la NGN como la NGCN pueden imponer potencialmente políticas de sesión.

7.7.5 Escenario 5 – Comunicación entre una NGCN y una RTPC/RDSI

Tanto la NGN como la NGCN pueden imponer potencialmente políticas de sesión.

7.8 Llamadas de emergencia

Las redes deben permitir a sus usuarios hacer llamadas de emergencia a las Centrales de Atención de Llamadas de Emergencia, que pueden basarse en una RTPC/RDSI o en IP. Algunas NGCN pueden manejar sus propias Centrales de Atención de Llamadas de Emergencia empresariales. Hay varios desafíos involucrados en esto, incluyendo:

- identificar una llamada de emergencia;
- enrutar una llamada de emergencia a la Central de Atención de Llamadas de Emergencia más apropiada;
- asignar los recursos apropiados para una llamada de emergencia; si es necesario, a costa de llamadas menos importantes;
- proporcionar a la Central de Atención de Llamadas de Emergencia información correcta sobre identificación para permitir que se devuelva la llamada;
- proporcionar a la Central de Atención de Llamadas de Emergencia información sobre la ubicación de quien llama.

La identificación de una llamada de emergencia en la petición SIP INVITE del UAC puede ser explicita (a través de SOS SIP URI) o implícita. En el último caso un intermediario SIP local debe determinar si es una llamada de emergencia analizando la petición URI.

Para enrutar una llamada de emergencia a la Central de Atención de Llamadas de Emergencia más apropiada, un intermediario SIP (por lo general, el primero, es decir uno basado en una NGCN o una NGN) debe tratar de obtener información sobre la ubicación geográfica (coordenadas geográficas y/o ubicación civil) para el UAC. El intermediario SIP puede obtener esa información de la infraestructura de red (por ejemplo, de switches LAN o por triangulación con estaciones base inalámbricas), o el mismo UAC la puede suministrar. La información sobre la ubicación puede provenir de más de una fuente; en tal caso la información debe remitirse a la Central de Atención de Llamadas de Emergencia.

La información sobre la identificación debe suministrarse en conformidad con las consideraciones de la sección 7.5. Sin embargo deben anteponerse los requisitos de privacidad. También debe enviarse cualquier información que pueda ser importante, esto sujeto a las capacidades del protocolo de señalización. Para algunas NGCN puede ser necesario que la información sobre la ubicación y la identificación enviada a una Central de Atención de Llamadas de Emergencia a través de una NGN sea cifrada. Asimismo, la información confidencial puede darse a conocer en los contenidos multimedia, por consiguiente también puede ser necesario cifrarlos.

REQUISITO # 45 DE UNA NGN: una NGN deberá proporcionar un medio para cifrar la información confidencial que suministra una NGCN para ser entregada a una Central de Atención de Llamadas de Emergencia.
REQUISITO # 46 DE UNA NGN: una NGN deberá proporcionar una manera de cifrar los medios entre una NGCN y una Central de Atención de Llamadas de Emergencia.

7.8.1 Escenario 1 – Comunicación entre NGCNs utilizando una VPN

Las llamadas de emergencia no son válidas en este escenario a menos que la NGCN proporcione su propia Central de Atención de Llamadas de Emergencia para las emergencias dentro de la empresa. Esto no involucraría la NGN.

7.8.2 Escenario 2 – Comunicación entre NGCNs sin utilizar una VPN

Por lo general, las llamadas de emergencia no son válidas en este escenario excepto cuando este se usa para enrutar una llamada de emergencia a una Central de Atención de Llamadas de Emergencia en una parte diferente de la misma NGCN (dentro de la empresa).

REQUISITO # 47 DE UNA NGN: una NGN no deberá interferir en el enrutamiento de una llamada para una Central de Atención de Llamadas de Emergencia empresarial y no deberá modificar la información a entregar a la misma central.

7.8.3 Escenario 3 – Comunicación entre NGCNs y un TE utilizando una VPN.
Para este escenario aplican las consideraciones descritas en la sección 7.8.1. Sin embargo, el proxy de la NGCN puede ser incapaz de determinar la ubicación del TE y por lo tanto, este mismo sería responsable de suministrar su ubicación.

7.8.4 Escenario 4 – Comunicación entre NGCNs y un TE sin utilizar una VPN.
Las llamadas de emergencia pueden ser válidas para este escenario si la Central de Atención de Llamadas de Emergencia es el Equipo Terminal de la NGN. En este caso, el intermediario SIP en la NGCN debe determinar que la llamada es una llamada de emergencia y debe enviar la información necesaria (identidad y ubicación de quien llama). El intermediario SIP en la NGCN puede no ser capaz de determinar la Central de Atención de Llamadas de Emergencia más apropiada, en tal caso el intermediario SIP en la NGN debe desempeñar esta función. Todos los intermediarios SIP deben asignar los recursos apropiados.

NOTA
En este escenario, el TE que llama podría ser una Central de Atención de Llamadas de Emergencia empresarial que hace una llamada de emergencia a una Central pública de Atención de Llamadas de Emergencia.

7.8.5 Escenario 5 – Comunicación entre una NGCN y una RTPC/RDSI
Las llamadas de emergencia pueden ser válidas para este escenario si la Central de Atención de Llamadas de Emergencia está en la RTPC/RDSI. En este caso, el intermediario SIP en la NGCN debe determinar que la llamada es una llamada de emergencia y debe enviar la información necesaria (identidad y ubicación de quien llama). El intermediario SIP en la NGCN puede no ser capaz de determinar la Central de Atención de Llamadas de Emergencia más apropiada, en cuyo caso el intermediario SIP en la NGN debe desempeñar esta función. Todos los intermediarios SIP deben asignar los recursos apropiados.

7.9 Ubicación Geográfica

Un UA puede determinar su ubicación geográfica (coordenadas geográficas y/o ubicación civil) y ponerla a disposición de las entidades autorizadas. Estas pueden ser únicamente el UA semejante o pueden incluir uno o más intermediarios SIP. Sin embargo, esta información es por lo general confidencial y tendrá que cifrarse al menos a nivel de salto a salto. Si esta información no puede ponerse a disposición de los intermediarios SIP, entonces el cifrado de extremo a extremo (utilizando S/MIME: Extensiones de correo de Internet de Propósitos Múltiples/Seguro) sería apropiado. Si la información puede estar disponible para intermediarios SIP designados entonces sería apropiado utilizar la seguridad extremo a medio. En este momento hay trabajos en curso en el IETF en relación con la transmisión de la información sobre la ubicación en el protocolo SIP.

Alternativamente, un intermediario SIP local a un UA puede tener los medios para determinar la información geográfica del UA de la infraestructura de red (por ejemplo, de switches LAN o por triangulación con estación base inalámbrica). Una vez más, sería necesario señalizar la información de manera segura a esas entidades SIP que están autorizadas para recibirla. Una solución que se encuentra en consideración en el IETF es volver a señalizar la información sobre la ubicación al UAC (utilizando TLS: Seguridad de la Capa de Transporte en ese salto) y pedirle al UA que señalice esta información de manera segura en los puntos finales.

En el caso de un TE de propiedad de una NGCN conectado a una NGN, la NGCN podría obtener de la NGN información disponible sobre la ubicación para ese TE.

REQUISITO # 48 DE UNA NGN: Una NGN deberá proporcionar un medio para que una NGCN obtenga información disponible sobre la ubicación de un TE de propiedad de una NGCN.

El suministro de la ubicación geográfica a una Central de Atención de Llamadas de Emergencia es una parte importante de las llamadas de emergencia (Ver la sección 7.8)

7.9.1 Escenario 1 – Comunicación entre NGCN utilizando una VPN
La ubicación geográfica es un asunto interno de la Red Corporativa de Próxima Generación.

7.9.2 Escenario 2 – Comunicación entre NGCN sin utilizar una VPN
La ubicación geográfica es un asunto interno de las dos Redes Corporativas de Próxima Generación. No debería haber ninguna razón para que un intermediario SIP en la NGN genere o deje ver la información sobre la ubicación geográfica. Esta información puede cifrarse a través de la NGN.

7.9.3 Escenario 3 – Comunicación entre una NGCN y un TE utilizando una VPN.
La ubicación geográfica es un asunto interno para la NGCN. Sin embargo, el proxy de la misma red puede no estar en capacidad de determinar la ubicación del TE y en consecuencia sería responsabilidad del TE proporcionar su ubicación.

7.9.4 Escenario 4 – Comunicación entre una NGCN y un TE sin utilizar una VPN.
La información sobre la ubicación geográfica relacionada con el TE en la NGCN podría enviarse al Equipo Terminal en la NGN. No debería haber ninguna razón para que un intermediario SIP en la NGN genere o deje ver esta información que puede cifrarse.

La información sobre la ubicación geográfica relacionada con el TE en la NGN podría ser generada por el Equipo Terminal o por un intermediario SIP en la NGN. Si se entrega al TE en la NGCN, no debería haber ninguna razón para que un intermediario SIP en esta red genere o deje ver esta información que puede cifrarse.

7.9.5 Escenario 5 – Comunicación entre una NGCN y una RTPC/RDSI
La información sobre la ubicación geográfica relacionada con el TE en la NGCN podría enviarse a la RTPC/RDSI. No debería haber ninguna razón para que un intermediario SIP en la NGN genere o deje ver esta información que puede cifrarse hasta la pasarela.

La información sobre la ubicación geográfica relacionada con el TE en la RTPC/RDSI podría ser generada por tal red, la pasarela o por un intermediario SIP en la NGN. Si se entrega al TE en la NGCN, no debería haber ninguna razón para que un intermediario SIP en esta red genere o deje ver esta información que puede cifrarse.