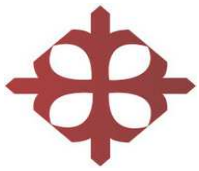

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL

TITULO:

ANÁLISIS DE LOS PROCESOS DE MIGRACIÓN DE REDES BAJO E1 HACIA REDES IP, PROPUESTA DE UN PROCESO DE DESCONGESTIÓN APLICADO AL CANTÓN MILAGRO

AUTOR:

JUAN CARLOS PADILLA RONQUILLO

TUTOR:

ING. ORLANDO PHILCO ASQUI MSC.

GUAYAQUIL - ECUADOR

2015

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES CON MENCIÓN EN GESTIÓN EMPRESARIAL

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por **Juan Carlos Padilla Ronquillo,** como requerimiento parcial para la obtención del Título de Ingeniero en Telecomunicaciones con mención en gestión empresarial.

TUTOR

_____

Ing. Orlando Philco Asqui MSc.

REVISOR

_____

DIRECTOR DE LA CARRERA

_____

Ing. Armando Heras Sánchez

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Juan Carlos Padilla Ronquillo**

DECLARO QUE:

El trabajo de Titulación **"Análisis de los procesos de migración de redes bajo E1 hacia redes IP, propuesta de un proceso de descongestión aplicado al cantón Milagro",** ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que están al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de titulación referido.

Guayaquil, a los 20 días del mes de Febrero del año 2015

EL AUTOR

_____

Juan Carlos Padilla Ronquillo

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Juan Carlos Padilla Ronquillo**

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación en la biblioteca de la institución del Trabajo de Titulación: **"Análisis de los procesos de migración de redes bajo E1 hacia redes IP, propuesta de un proceso de descongestión aplicado al cantón Milagro"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 20 días del mes de Febrero del año 2015

EL AUTOR

_____

Juan Carlos Padilla Ronquillo

AGRADECIMIENTO

A mi Dios, Quien ha sido nuestra guía inagotable quien nos ha brindado compañía ya que aunque siempre nos acompaña para acrecentar nuestra paciencia, espera sobre todo las fuerzas necesarias para Seguir adelante y conseguir nuestras las barreras que se nos han puesto en este tramo del camino ya que este es el inicio y siempre todo comienzo es complicado pero gracias a nuestro señor seguimos adelante.

Al Ing. Orlando Philco que fue nuestro docente y tutor, aporte principal para el desarrollo de este proyecto, ya que nos supo transmitir sus conocimientos, Ing.Armando Heras Sánchez coordinadora del área de Ingeniería en telecomunicaciones de la Unidad Académica, por sus conocimientos Y sabios consejos que oportunamente nos brindó, para la realización del presente proyecto.

Juan Carlos Padilla

DEDICATORIA

Dedico de manera especial este proyecto a Dios mi Señor, a mis padres por haberme

Dado la vida y a mi esposa Linda mendes por los consejos que me ha brindado ya que sin ellos no hubieran podido llegar hasta donde he llegado, por darme ese empuje para culminar mi tesis en todo momento y a mi madre quien deseaba esto Estará siempre guiando mis pasos; a cada uno de mis familiares más Queridos por su apoyo al estar constantemente junto a mí para estimularme y seguir Adelante hasta alcanzar la meta anhelada.

Juan Carlos Padilla

TRIBUNAL DE SUSTENTACIÓN

_____

ING. ORLANDO PHILCO ASQUI MSC.

PROFESOR GUÍA Ó TUTOR

_____

Ing.

PROFESOR DELEGADO

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

INGENIERO EN TELECOMUNICACIONES CON
MENCIÓN EN GESTIÓN EMPRESARIAL

CALIFICACIÓN

_____

ING. ORLANDO PHILCO ASQUI MSC.

PROFESOR GUÍA Ó TUTOR

ÍNDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

El presente trabajo de titulación cumple como objetivo principal la recopilación y análisis de principales investigaciones documentadas a fabricantes y operadores o proveedores de servicios, que de cierta forma la Corporación Nacional de Telecomunicaciones (CNT), busca como modelo de negocio una plataforma tecnológica de vanguardia. La propuesta de migración a redes NGN. Es atrayente por su alto grado de implicación en soluciones de próxima generación o para su influencia significativa en el sector de las telecomunicaciones.

La CNT, tiene destinado para el cantón Milagro, la implementación de una red NGN, y esta debe cumplir con estándares de calidad en dicha implementación, la metodología que se empleada, es la descriptiva y bibliográfica, se destaca la propuesta de un plan de descongestión para la central CNT en Milagro.

Como resultados obtenidos, se plantean procedimientos posibles, que tienen enfoques técnicos estandarizados para la migración y el desarrollo de nuevos modelos de negocio basado en NGN.

Palabras claves: TDM, conmutación, paquete IP, NGN. Migración,

ABSTRACT

The present study degree meets the main objective of collecting and analyzing documented major manufacturers and operators or service providers investigations, which somehow National Telecommunication Corporation (CNT), looking as a business model-edge technology platform. The proposed migration to NGN networks. It is attractive for its high degree of involvement in next generation solutions or for their significant influence on the telecommunications sector.

The cnt, is intended for the canton Milagro, implementing an NGN network, and it must meet quality standards in this implementation, the methodology employed is the descriptive literature, the proposed decongestion plan stands for the cnt center in Milagro city

As results, possible procedures, which have standardized technical approaches to migration and development of new business models based on ngn arise.

Keywords: TDM, switched, NGN, packet IP, Migration.

Capítulo 1: Aspectos Generales

1.1 Introducción

La evolución de las redes y los servicios hacia las redes de próxima generación o NGN (*Next Generation Net*), es una tendencia transcendental en las telecomunicaciones, y de gran interés para el mercado. Se conoce que varios fabricantes exponen sus nuevos productos en ferias y reuniones tecnológicas, y así también se debate el cambio o migración a una red totalmente, bajo protocolo IP, se trata de aprovechar condiciones de aplicación de modelos económicos viables para los operadores y proveedores de servicios de telecomunicaciones.

Las autoridades reguladoras del sector de las telecomunicaciones, tienen que garantizar que el mercado emergente de esta evolución sea equitativa, abierta y competitiva. Ellos también tienen que ser capaces de identificar lo más rápidamente posible las futuras áreas de interés relacionados con su actividad con el fin de cumplir mejor sus misiones. Con la esperanza de una mejor comprensión de las cuestiones técnicas, económicas y regulatorias que se ocupan de esta evolución, que parece ser una tendencia a largo plazo.

La CNT ha tenido que implementar diferentes estructuras de redes para cada servicio que ofrece (telefonía, televisión e internet), que con el tiempo la demanda se hizo mayor y debido a esto CNT se ve obligada a implementar una infraestructura que sea eficiente, sólida y que por sobre todo ampare la convergencia digital, para los servicios de telecomunicaciones de vanguardia. Se analizan estructuras de redes IP, donde puedan converger tecnologías “viejas” con nuevas. El protocolo IP acoge muy bien la adaptación de dichos servicios de telecomunicaciones.

1.2 Planteamiento del Problema

Falta de procedimientos o metodología técnica que permita la descongestión de un proceso de migración de red bajo conmutación (E1) o de TDM en centrales de telecomunicaciones, se desconoce escenarios de usos para aprovechar las fortalezas de las redes NGN.

1.3 Objetivos

1.3.1 Objetivo General.

Analizar la normativa técnica en implementación de red NGN y propuesta de una metodología para proceso de descongestión en migración a red NGN en la central-CNT del cantón Milagro.

1.3.2 Objetivos Específicos

1. Determinar modos de operación de una red de próxima generación NGN
2. Describir los escenarios de red NGN para supervisión remota
3. Proponer una metodología de descongestión en migración a red NGN para la central CNT-Milagro.

1.4 Justificación

Por cuanto una red NGN, es una tecnología ideal para operadores mayoristas como CNT, es fundamental aplicar procedimiento de migración NGN en central del cantón Milagro, el número de clientes crece día a día y estos presentan solicitudes del servicio, voz, video y datos en lugares donde no hay disponibilidad para brindarlo y además exigen mejoramiento en la calidad de servicio y descongestionar la disponibilidad del mismo.

1.5 Hipótesis

Si se implementa una red NGN en la central CNT-Milagro, se debe aplicar un procedimiento de descongestión basado en normativa de la UIT, el cual ofrecerá reducción de costos operativos y mantenimiento, mejorando la calidad de servicio e incrementando el número de usuarios.

1.6 Metodología

La metodología de este trabajo es descriptivo, por cuanto hay que determinar claramente una migración tecnológica de vanguardia que puede analizar bajo esta metodología. Otra metodología, es la bibliográfica, ya que se revisan métodos y estándares ITU-T, se estudia también, otros escenarios existentes de migración hacia las NGN, basado en lo técnico y económico.

1.7 Alcance

Esta fuera del alcance de este trabajo de titulación, realizar estudios económicos a profundidad de una implementación NGN para la central CNT en Milagro, diseñar esquemas de conexión de equipos en una red NGN y de presupuesto de equipos de hardware y software para central CNT-Milagro.

Capítulo 2: Fundamentos de redes NGN

Los operadores de todo el mundo están tratando de implementar nuevas soluciones que puedan abordar adecuadamente las demandas que se les imponen por mercado y por desarrollo tecnológicos. Existe creciente demanda de servicios, de disponibilidad de comunicaciones con altas velocidades, de plataformas integradoras, Sin duda los servicios más innovadores y la inteligencia de red apoyan la evolución de los mercados de la empresa, hacia una mejor integración de sus redes.

En el otro lado, las demandas de lado los inversores radican en aumentar sus ingresos, mejorar la rentabilidad, y el aumento de la productividad.

2.1 Servicios de inteligencia de Red

La migración progresiva del sector de las telecomunicaciones a las redes y servicios de próxima generación es un importante interés tendencia generando entre la mayoría de los jugadores. Es el resultado de una combinación de factores favorables y motivadores.

Los grandes cambios estructurales en el mercado de las telecomunicaciones: la desregulación del bucle local y los mercados de larga distancia, la optimización de la red y la reducción de costes, la externalización, etc.

Los principales cambios en los servicios y usos: explosión de los servicios de datos, en particular Internet y multimedia, la movilidad y la accesibilidad, la necesidad de los operadores y proveedores de servicios para desarrollar nuevos mercados.

La mayor evolución tecnológica, en particular con el desarrollo de las redes de acceso y transporte de muy alta velocidad, la generalización y la evolución hacia protocolo IP, en favor de los diferentes niveles de calidad de servicio.

Este contexto ha generado la necesidad de y la viabilidad técnica de un traslado a las nuevas redes y servicios de modelo llamado NGN (*Next Generation Networks*). Este modelo de red, se basa en una evolución progresiva de extremo a extremo "todo IP" con el fin de adaptarse a las tendencias principales: convergencia y evolución de redes flexibles, distribución de la inteligencia de la red, y la apertura a los servicios de terceros.

El sistema NGN ofrecerá servicios convergentes multimedia clave utilizando una red compartida que se caracteriza por varios elementos esenciales:

- Un único y compartido de red central para todos los tipos de acceso y servicios.
- Una arquitectura de red de núcleo dividido en tres capas: Transporte, Control y Servicios.
- Desarrollo de modo transporte de paquete (transporte IP flujo de IP nativa, o en ATM en el corto plazo con una convergencia progresiva de IP).
- Abrir y estandarizada las interfaces entre cada capa, y en particular para las capas de control y servicios a fin de permitir a terceros desarrollar y crear servicios independientes de la red.
- Soporte para múltiples aplicaciones -Multimedia, en tiempo real, transaccional, capacidad total movilidad adaptable al usuario y la creciente y variada de las redes de acceso y terminales.

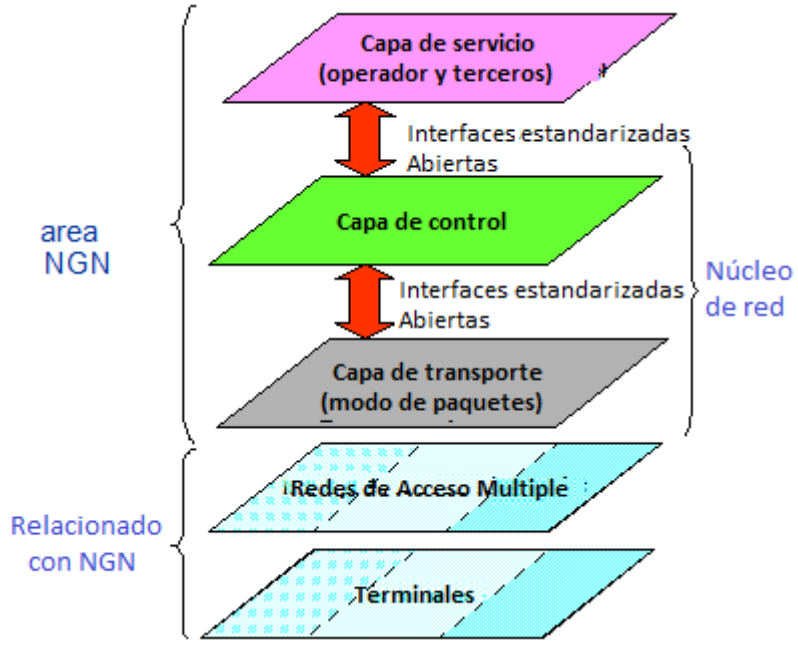

Figura 1 Principios generales de la arquitectura NGN

Fuente: Arcome (2012)

Las redes tradicionales de telecomunicaciones van a evolucionar a un modelo abierto distribuido, firmemente basado en IP y transmisión en modo paquete, en general, que es transparente para los usuarios.

Los servicios NGN, con un fuerte potencial para nuevos usos, se basarán en modelos para la ejecución transparente de la red (el modelo de Internet "servicios Web") o con la contribución de la red (modelo de servicio Arquitectura abierta de telecomunicaciones). La complejidad y la diversidad de nuevos servicios multimedia se retirarán del mercado hacia el mundo del software. Mientras que las tecnologías asociadas son maduros o casi maduros, todavía se deben crear usos.

2.2 Complejidad Tecnológica

Actualmente las ofertas NGN disponibles, son de un grado variable de solidez, por los siguientes aspectos:

Una serie de equipos NGN aún no han alcanzado la madurez o la estabilidad completa, y la atención especial debe ser pagado de la calidad de la gestión del servicio que es visto como un desafío tecnológico clave, a las capacidades iniciales de soluciones de conmutación NGN, y hacer la transición soluciones basadas en propiedad protocolos o las que podrían desaparecer en el mediano plazo.

A corto plazo, esto todavía bajo grado de madurez de las soluciones más probable es que requieren el uso de un solo fabricante soluciones (al menos por tipo NGN de los equipos).

Mientras que el campo móvil muestra signos más visibles de un movimiento hacia la NGN (alta visibilidad en el desarrollo de terminales y redes, ya que UMTS, en su segunda fase, es el primer sistema completo utilizando una arquitectura NGN), los primeros despliegues de efectivos de las NGN Las soluciones están en el dominio de las redes fijas (tránsito de voz, voz sobre IP, xDSL).

Estas nuevas tecnologías convergentes y siempre cambiantes destacan el papel esencial de la normalización. De hecho, la apertura de las redes y servicios requieren el uso de soluciones e interfaces estandarizadas e interoperables. Lo que es más, en el corto plazo, la implementación de las NGN dará lugar a la aparición de variantes de la arquitectura y las sucesivas generaciones de protocolos, lo que crea problemas de interoperabilidad y divergencia riesgos. En este contexto:

Los organismos de normalización (en particular IETF, ETSI e ITU) desempeñarán un papel dominante en la fijación de las especificaciones de los protocolos y los bloques tecnológicos de NGN, el establecimiento de una arquitectura común general, garantizar la accesibilidad y la difusión de las normas aplicables, y la consolidación de los bancos de pruebas de interoperabilidad.

En un momento de acelerar el desarrollo tecnológico, donde los operadores y proveedores de servicios tienden a depender de los fabricantes para establecer las especificaciones de soluciones futuras, el regulador tendrá un papel de liderazgo en la coordinación de los intereses y los avances de todos los actores en el ámbito nacional.

Uno de los temas sería la forma de resolver la singularidad de un modelo de red y los servicios que se supone que es abierto, pero cuya tecnológica complejidad podría impedir la aplicación efectiva de esta apertura, lo cual se impide la libertad de elección del usuario final, especialmente en términos de servicios. Esta dificultad se añade a la de la adopción de nuevos modelos económicos, que requiere un levantamiento de las relaciones entre los jugadores de todo el sector de las comunicaciones electrónicas.

2.3 Varios enfoques de migración

La migración hacia la NGN parece ser una evolución inevitable debido a la doble convergencia de voz/datos/imagen de y fijo/móvil. Ya se ha iniciado debido a una serie de actores en Europa y en otros continentes, y por lo tanto sus impactos tendrán que ser analizado. Aun así, es probable que sea de extendido (de 10 a 20 años aproximadamente), incompleto y difícil en el corto plazo debido a la existencia de soluciones con diferentes características y la madurez de la competencia, y cuestiones de extremo a extremo de interoperabilidad.

2.3.1 La pertinencia de las soluciones NGN

Los operadores y proveedores de servicios para los que las soluciones NGN parecen los más adecuados son los futuros nuevos jugadores (aún no establecido), reproductores de datos que desean diversificar sus actividades (en ISP´s particulares), operadores anticipando un fuerte crecimiento y/o una rápida diversificación de sus actividades (por

ejemplo: operadores WLL o xDSL), los operadores esperan una fuerte disminución de su tráfico de voz debido al tráfico de datos y operadores móviles.

Los jugadores que parecen los retrasos más importantes con respecto a las soluciones NGN son aquellos que han invertido recientemente mucho en infraestructuras de conmutación de voz TDM tradicionales, y los operadores que ya tienen acceso al bucle de acceso y conmutadores locales de baja velocidad.

También es interesante observar que el paso a las NGN no es obligatorio, pero los actores claves, ven nueva forma de usos y la creación de valor (introducción de nuevos servicios y mercados) como principales incentivos para migrar a las redes NGN, los argumentos inmediatos planteados en el marco de la migración de los operadores y proveedores de servicios a las NGN están fuertemente influenciadas por la situación económica vigente en el mundo.

Esos argumentos económicos (mejora de los costos de adquisición y de operación, con un rápido retorno de la inversión) tienen prioridad sobre el argumento de marketing de la variación a los nuevos servicios multimedia, que se destaca por los fabricantes, pero es secundario, para los operadores.

El compromiso de las infraestructuras y retorno de la inversión, son preocupaciones existentes, esto significa que tienen que ahorrar en gastos técnicos de la red con el fin de maximizar los ingresos por servicios.

Estas restricciones financieras son en teoría menos importante para las empresas que para el público en general, y las necesidades de las empresas de servicios cambian con mayor rapidez. Los usuarios de cuentas principales podrían impulsar redes de los operadores hacia la NGN.

Por último, es importante señalar que algunos actores de la capa de servicios (en particular, la diversificación de los ISP´s a las actividades de "voz" y otros contenido IP) consideran que sus redes actuales ya son NGN.

Los ahorros financieros esperados de ofertas NGN también deben ser equilibrados en el corto plazo. Mientras que en el medio y largo plazo, todo el mundo espera una importante disminución en los costos de compra de soluciones NGN, en el corto plazo

estas cantidades dependerán en gran medida de las infraestructuras existentes de los operadores y en sus relaciones comerciales con los fabricantes. El Ahorro de inversión inducidos por NGN sólo son eficaces para la implementación inicial sin red preexistente.

En cuanto a recurrentes los costos relacionados con las soluciones NGN, aunque los fabricantes dicen casi unánimemente que las soluciones NGN produciría importantes ahorros inmediatos, los operadores y proveedores de servicios son menos entusiastas y más dividido, en particular debido a las posibles recargos indirectos vinculados a la migración.

La migración hacia la NGN de operadores bien establecidos tener una red grande será aún más larga y más progresista. La mayoría de los entrevistados están de acuerdo en que los operadores ya establecidos favorecen una lenta migración basado en el transporte ATM, aunque los nuevos operadores son más "todo NGN" orientado y favorecen infraestructuras IP nativas.

2.4 Evolución profunda de la relación agentes del mercado.

El desarrollo NGN T permitirá contenido multimedia y el desarrollo de servicios:

• Estas actividades representan un gran potencial para los nuevos operadores de servicios de telecomunicaciones. Este potencial debe fomentarse a través de las condiciones económicas y regulatorias favorables. También podemos esperar a ver la aparición y el creciente papel de terceros, es decir empresas contratista para cumplir con instalación del servicio, autenticación, pago electrónico encriptado, y servicios de portal web.

• Con los servicios cada vez más vinculadas a las nuevas capacidades terminales y con una visibilidad comercial importante, el control de cliente sistemas operativos y aplicaciones de software será una ventaja importante en el posicionamiento de los principales fabricantes de software como proveedores de servicios NGN.

• A pesar de un previsible crecimiento de inicial nuevos jugadores pequeños, esta fase probablemente será seguido por las agrupaciones para mejorar la visibilidad de los clientes. Estos legítimo el reciente posicionamiento de los principales fabricantes de

software como proveedores de servicios NGN, y nos llevan a esperar un papel clave para portales y agregadores de contenido.

• La modificación de las relaciones entre los jugadores hará que la interconexión, la redistribución de los ingresos y las preocupaciones de facturación cruzadas, etc. cada vez más sensibles.

La NGN será oportunidad para la transformación de la relación jugadores de gran envergadura, y en particular entre los operadores y proveedores de servicios.

El elemento clave para el éxito en un contexto NGN es el control de los clientes. Esta es una fuerza histórica de los operadores, sino también la fuente de legitimidad en el posicionamiento potencial de ciertos jugadores del campo del software, o los proveedores de servicios y contenidos.

La competencia en las redes de acceso sigue siendo una prioridad real en el corto plazo para la mayoría de jugadores: todavía hay una fuerte demanda de un movimiento a alta velocidad, para la ampliación de la oferta de desagregación, etc. que tendrá que resolver en relación con cuestiones de desarrollo regional. Sin embargo, este enfoque en los problemas de acceso no está vinculada únicamente a las NGN, y puede muy bien estar ocultando la ausencia actual de apertura entre redes y servicios.

La redistribución de los ingresos entre los jugadores es la clave del éxito: los presupuestos globales de comunicación de los consumidores no se expanden lo suficiente como para permitir a los jugadores para evitar tener que cambiar los modelos de ingresos. Ni impedirá que una redistribución de los ingresos entre todos los actores de la cadena, todo el camino hasta el proveedor de servicios.

Esta redistribución de mediano plazo a lo largo de la cadena de valor (de acceso a los servicios) es una tendencia identificada por todos. Sin embargo, su aplicación dependerá de la voluntad de los operadores, aunque parece inevitable a medio plazo con el fin de garantizar la lealtad a largo plazo de los clientes y la durabilidad de los ingresos.

Otro de los problemas que hay que superar es encontrar formas adecuadas a precio contenido, e implementar nueva facturación modos adecuados para usos de los clientes,

todo ello en un entorno de convergencia de voz/datos, a pesar de que estos dos mundos utilizan métodos muy diferentes sobre este punto.

La apertura de los servicios a los proveedores de terceros plantea diversos aspectos técnicos, operativos, estratégicos y preocupaciones económicas. El impacto de estas nuevas asociaciones en los sistemas de información (facturación, aprovisionamiento, automatización de procesos, pagos, reembolsos, relaciones con los clientes, gestión de la asociación, interconexión, etc.) son un problema que se subestima a nivel técnico (y tratado con muy poco en la Normalización) y en el plano económico y operativo.

Sin embargo, se observa una gran diferencia entre la participación teórica de los roles en el marco de las NGN, y la realidad: establecido actores claves (operadores) apoyamos este modelo abierto, en principio, pero en realidad, aún presentan un cierto grado de desidia y el proteccionismo que conducen nosotros esperamos que los problemas de aplicación.

Por lo tanto, la apertura de las redes a los proveedores de servicios hacia terceros, parece ser más un problema de voluntad y el modelo de negocio en lugar de un obstáculo técnico. Por ello, el regulador podría tratar de fomentar la apertura de inmediato, sin esperar necesariamente a que la aplicación de interfaces multi-red estandarizados.

2.5 Las cuestiones de regulación

La apuesta de los actores claves a las redes NGN, encenderá el panorama técnico y económico de las comunicaciones electrónicas al revés, y afectará inevitablemente a la naturaleza de las misiones de regulación y los medios de satisfacerlas.

Los actores claves, no ven el regulador de jugar un fuerte papel intervencionista, sino más bien ver un fortalecimiento de su papel de liderazgo en la discusión (grupos de trabajo) y su participación en las actividades de normalización, vigilancia del mercado y facilitar la convergencia necesaria para arquitecturas y protocolos unificados.

Se le pide al regulador para establecer un contexto técnico y económico favorable a las NGN, con, en particular:

• La fuerte demanda de un marco regulatorio tecnológicamente neutra, permitiendo a los actores claves la libertad de elección, de acuerdo con el nuevo marco regulador.

• En el corto plazo, la resolución de las dificultades actuales, en particular en lo referente desagregación del bucle local y el traslado a Internet de banda ancha ofertas de acceso

• La aplicación de un marco regulatorio que favorece a largo plazo de los actores claves, las inversiones, así como la puesta en común de infraestructuras en un sentido amplio. Los actores claves hacen que las adaptaciones al contexto normativo de NGN guiarse sobre todo por la demanda del mercado. Por lo tanto, piden, más de anticipación, alta regulación reactividad y un enfoque operativo fuerte. Estas necesidades de adaptación del marco normativo, por lo tanto debe ser, si no previsto, al menos preparados para a través de estudios y/o la creación de grupos de trabajo.

Se identificaron varias áreas para la evolución de la legislación y regulación

- En la legislación:
  - ❖ La definición de la situación de los futuros actores en NGN, en determinados prestadores de servicios, así como sus derechos y obligaciones (en particular, los regímenes de autorización y condiciones de interconexión).
- En la regulación:
  - ❖ La evolución previsible de la vigilancia del mercado, con especial atención a la calidad de servicio (dentro de una red IP, y de extremo a extremo), que se identifica como un riesgo importante y un indicador de la falta de madurez.
  - ❖ Mayor papel de facilitación en las discusiones técnicas y operativas.
- En la vigilancia tecnológica, en preparación para una posible evolución del marco normativo y la regulación:
  - ❖ La discusión en detalle sobre la evolución de los recursos y los mecanismos de gestión de la numeración, denominación y direccionamiento de las redes NGN (evolución a IP).

La evolución necesaria de ciertos servicios corporativos a tener en cuenta una convergencia de voz/datos y entorno móvil/fija, como la portabilidad, los servicios de emergencia (en relación con las preocupaciones de localización geográfica) el perímetro y la definición técnica de los servicios "básicos", la interceptación legal.

- La evolución de la interconexión de redes, servicios y sistemas de información, lo que plantea riesgos para la estandarización de la interfaz, la interoperabilidad y la disposición estratégica de los jugadores para abrir sus redes a los socios.

Parece prudente, en la preparación para el paso a las NGN, que ya fomentar activamente la apertura de las redes de operadores a los proveedores de servicios de terceros, ya sea para el móvil (por ejemplo: GPRS) o redes y servicios fijos.

2.6 Sustitución E1 por NGN

Lo que los operadores necesitan ofrecer a los consumidores (tanto residenciales como empresariales) es la nueva NGN plataforma con varios servicios, el mismo que debe estar ofrecido a los abonados TDM existentes. Por lo tanto, la integración TDM a IP es la respuesta inmediata por el operador para atender esta necesidad mediante conmutadores de software. En cuanto a esta tendencia tecnológica, se puede suponer que la I+D en este ámbito ofrece enormes oportunidades, especialmente a primera empresas de organizador.

La migración de tráfico de las redes tradicionales a las nuevas redes (principalmente IP y móvil) es la reducción de la utilización de los niveles y la creación de ineficiencias operativas y financieras, que se alimentan una espiral viciosa del aumento de los costos unitarios y reducido la rentabilidad. La fijo NGN negocios caso es ante todo sobre excluyendo ineficiencias. Si los operadores pueden optimizar procesos, reducir el número de cabeza racionalizando existente de red activos, e introducen de manera eficiente la tecnología NGN para reemplazar activos heredados, entonces la migración a las NGN puede realizar sustanciales ahorros de costos.

El propósito de la migración es principalmente para reducir el capital de los costos y en curso, y por tanto los resultados de los modelos principales son los diferentes costos de operación, gastos de capital y la depreciación de las diversas redes y escenarios

considerados. La mayoría de las empresas de telecomunicaciones reconocen que en el plazo de 2-5 años que se han adoptado una estrategia de núcleo IP. Lo que todos ellos están ahora luchando con es el proceso de migración. Las tres alternativas viables para la migración de la red son los siguientes:

A. E1 con capacidades de modernización en NGN

El escenario de actualización prevé la introducción de una IP de red central, reemplazos IP del *backbone* de TDM en cada *switch* y las tarjetas de PI que faciliten la conexión a la orilla de los existentes interruptores. Esto requiere de una importante inversión en equipo, así como tendrán que ser actualizados los interruptores. También tiene implicaciones para la estabilidad de la red de voz existente.

B. Reemplazo de TDM por NGN

En el escenario de sustituir los interruptores existentes son barridos y sustituidos por dispositivos basados en IP que ofrecen todo el margen de funcionalidad requerida, ahora y en el futuro. Es también pone en peligro el funcionamiento de la red TDM, pero tiene el inconveniente añadido una alta inversión inicial en equipos temporal "puerta" para apoyar el servicio POTS.

C. TDM superposición con las NGN

El escenario de superposición retiene la red TDM para usuarios POTS e implementa una red paralela de apoyo a usuarios VOIP al servicio asociado; los Conmutadores TDM habilitados para IP pueden ser sometidos en el control del *softswitch*. Las dos redes están conectadas por medio de una pasarela de medios (Gateway). La red TDM puede ser dado de baja una vez que la mayoría de los usuarios POTS han migrado a la NGN. Las experiencias muestran que el enfoque de superposición es la estrategia óptima para la introducción de una NGN multimedia.

Se tiene la CAPEX más bajo y en muchos escenarios, el más bajo OPEX. El enfoque tiene invariablemente el más alto NPV y la recuperación más corto. Esto parece ser cierto a pesar significativo aumento en TDM CAPEX y OPEX necesario para mantener la PSTN. También sostiene que los ingresos de voz NGN son significativamente menor que la de los actuales POTS/RDSI. Un factor importante es que el enfoque de

superposición, también es la que tiene menor riesgo. El POTS/RDSI servicio continúa siendo entregado por la red TDM/PSTN probada.

2.7 Enfoques de implementación de VoIP

Las Redes de voz PSTN basado TDM, se desplegaran para redes basadas en paquetes, donde la voz sobre IP (VoIP) puede ser ofrecido por dos diferentes enfoques:

Red de Próxima Generación (NGN):

Las redes NGN como transportes de aplicación de servicio voz sobre IP gestionada y asegurado red trabaja con garantías bien definidas para fines accesibilidad del usuario, calidad de la comunicación, fiabilidad y conectividad, mientras que el apoyo servicios heredados de la PSTN.

Voz sobre Internet:

La telefonía por Internet con el tráfico de voz enviados sobre una base de "mejor esfuerzo" como un usuario final o peer-to-peer de aplicaciones en la parte superior de la Internet, proporcionando servicio sólo limitado calidad. Desde un proveedores de servicio de telefonía incumbente la perspectiva de ser, a medida que adoptan la migración a una infraestructura de extremo a extremo basada en IP, la NGN enfoque convierte en una forma más eficiente de enrutamiento y la entrega de tráfico de voz, como Internet pide compartir ancho de banda en la red con otras aplicaciones. El objetivo de este trabajo es el enfoque NGN.

2.8 Calidad de servicio y VoIP

En cuanto a calidad de servicio (QoS) en la VoIP aplicación, la red IP de núcleo y el acceso la red tiene que ser distinguido. En cuanto a la red de núcleo, IP QoS se basa ya sea en MPLS o se puede lograr por excesiva de capacidad de ancho de banda. Garantizar la QoS en la red de acceso requiere más atención que la de banda disponible anchura es en general mucho menor que en el núcleo red. Las necesidades del tráfico de la voz el servicio son bastante predecibles, lo que permite el servicio de proveedores para introducir QoS en la red.

La voz sobre Internet usando SIP permite una clara diferenciación entre servicios, que normalmente dará lugar a una buena calidad, pero la calidad sigue siendo impredecible y varía con el tiempo incluso durante una llamada. Por otro lado sólo una llamada con predecible comportamiento puede tener la QoS garantizados. Esta característica será la principal diferenciación entre "voz sobre Internet" y "voz sobre migración del servicio de voz).

El escenario de migración adecuado para empresas de telecomunicaciones que se caracterizan por la conservación preliminar de los *schitches* TDM existentes (E1); la NGN está desplegando en paralelo. Este escenario se llama así como el enfoque de superposición. Este concepto permite a la red del operador migrar de la red TDM a las NGN en pequeños pasos y maximizar el retorno sobre el capital invertido en tecnología. TDM.

Una vez que la mayoría de los usuarios migren a las NGN, los usuarios TDM restantes pueden ser apoyados por medio de una IP *Line Access Gateway* (LAG IP). La persistencia de la red TDM y la protección de la inversión lograda de esta manera significan que los procesos probados y la plataforma examinada tal vez no requieran cambios tecnológicos por el momento. El atractivo de este enfoque es que, en contraste con la red TDM, es que la disponibilidad de una NGN no está ligado a un determinado lugar. Además, paso a paso la provisión de una red NGN se realiza de conformidad con el creciente número de suscriptores. Este enfoque minimiza el costo total de implementación.

2.9 Requisitos NGN

Hay algunas condiciones de la NGN que necesita cumplir para proporcionar a los clientes sus servicios solicitados y para dar a los proveedores de redes y servicios la ventaja competitiva sobre su competencia.

- Continuidad del nivel de operador existente los servicios ofrecidos a los clientes con la misma calidad, seguridad y fiabilidad.
- El Inter funcionamiento y la interoperabilidad entre nuevas redes y sistemas existentes y la flexibilidad para incorporar nuevos servicios

- Calidad de servicio (QoS) para garantizar los acuerdos de nivel de servicio (SLA) para diferentes condiciones y servicios de tránsito
- La continuidad del servicio en la presencia de fallas dentro de la red (de supervivencia), la oferta de líneas de vida (por ejemplo, para los teléfonos de emergencia)
- Movilidad generalizada para coherente prestación ubicua de servicios

2.10 Principios y procedimientos de migración

Para el éxito de la migración hacia la NGN, se tiene que seguir algunos principios:

La migración de la red telefonía tradicional a la red NGN tiene que preservar la inversiones tanto como sea posible ya existentes, por ejemplo, la reutilización de los cables de cobre para DSL acceso, no hay sustitución del cliente aparatos telefónicos y de PABX (al menos en una fase inicial).

El control de costos del proceso de migración, es decir llevar el acceso a datos en banda ancha a los clientes, también significa traer el acceso elementos de red más cerca de los clientes. El acceso de banda ancha debe ser justificado por los servicios apropiados con correspondidos ingresos. Esto implica aplicar un procedimiento de migración inteligente.

Los pasos de migración dependen del específico proveedor de servicios y situación del mercado, por ejemplo, un país en desarrollo versus un país desarrollado, o estado real de la red desplegada de cobre.

Los pasos de migración que se presentan a continuación, no son todos obligatorios y también tienen no que debe seguirse en el orden propuesto.

El procedimiento de migración se puede estructurar en tres pasos principales: Optimización y preparación: hay que optimizar la red telefónica existente una reducción del número de intercambios local y troncal. La red de acceso implementada y sus elementos deben estar preparados para las nuevas redes NGN, por ejemplo, los Nodos de Acceso, Multi Servicio (MSAN) que puede realizar tanto, el acceso TDM y acceso de paquetes.

Aumento de la capacidad, es implementar elementos de red NGN para ampliar la red telefónica. Las redes NGN y PSTN coexisten lado a lado.

Reemplazo PSTN, se sustituye los elementos de red PSTN existentes con su elemento de red NGN equivalente. Los Equipos cliente, se sustituye por equipos basados en paquetes con capacidad multimedia. La PSTN dejará de existir.

Se debe tomar en cuenta que los proveedores de redes y servicios no son capaces de controlar el ritmo de sustitución de teléfonos adquiridos. Muchos clientes que requieren el servicio sólo telefónico, no estarán dispuesto para reemplazar su teléfono familiar. El manejo de este equipo debe mantenerse mediante la implementación de Media Gateway (Mg), en la red de acceso o en el suscriptor de servicios locales.

2.10.1 IMS

El Subsistema Multimedia IP (IMS) es una marco estructural para la entrega de servicios multimedia de internet de protocolo (IP) a los usuarios finales. El IMS se define con los estándares abiertos de 3GPP y ETSI y está basado en protocolos de IETF (SIP, RTP, RTSP, COPS, etc.). el IMS es diseñado para operar tanto en redes alámbricas e inalámbricas, y es la base para convergencia fija y móvil (FMC).

El IMS apoya la operación y el inter funcionamiento con una variedad de redes externas a través de referencia puntos definidos. Específicamente es capaz de inter-trabajar con la red PSTN.

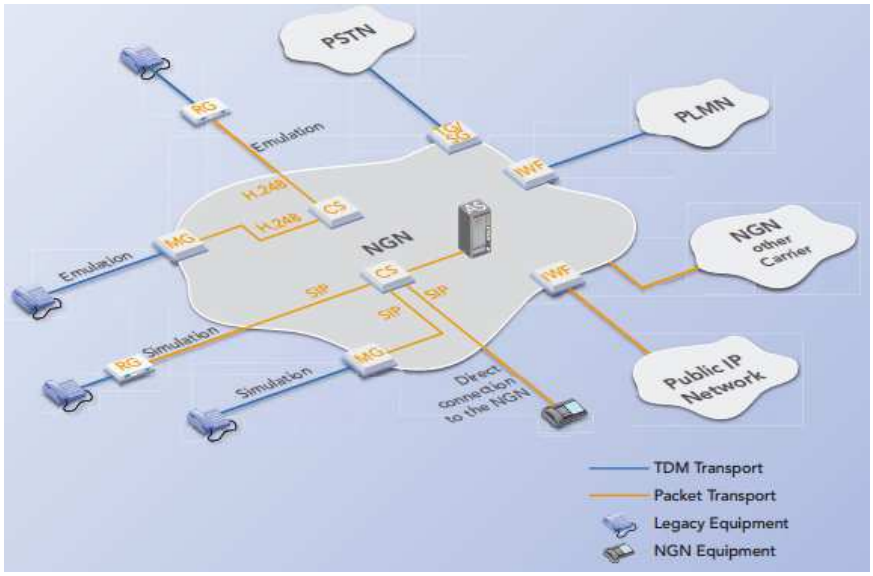

Figura 2. Ejemplos de emulación de PSTN y simulación con NGN

Fuente: Keymile (2008)

2.10.2 Característica del IMS

La IMS entrega comunicaciones multimedia basadas en IP, sea persona a persona y persona a máquina.

La IMS integra completamente en tiempo real con lo de tiempo no real comunicaciones multimedia, por ejemplo, transmisión en vivo y chat.

La IMS permite diferentes servicios y aplicaciones para interactuar, por ejemplo, el uso combinado de presencia y mensajería instantánea.

La IMS proporciona un control de la conectividad IP en redes de acceso (QoS, control de admisión, autenticación, etc.).

La IMS permite el inter funcionamiento y la inter operatividad con sistemas desusados y otras redes.

La IMS es la tecnología independiente de acceso para aplicaciones de sesión y control de llamadas.

2.10.3 Uso de IMS en NGN

En el entorno NGN el servicio de componente IMS apoya la prestación de basado en servicios multimedia SIP a terminales NGN. También apoya el aprovisionamiento de simulación servicios PSTN. En otras palabras, NGN proporciona la comunicación la infraestructura de la red, mientras que IMS es responsable del control del servicio.

2.11 Escenario de migración PSTN a NGN

Un objetivo principal de un operador de red es la reducción de las redes de comunicación paralelos, es decir TDM para voz e IP para datos, a una solo red, preferiblemente basado en el transporte IP. Este objetivo se puede lograr mediante la extensión del alcance de la red IP en el área de red de acceso, es decir, mediante la aplicación de acceso multiservicio basada en nodos IP (MSAN) cerca de ubicación del abonado.

Las ventajas de una red IP común son:

- El costo para evaluación, la puesta en marcha y el funcionamiento de una única red es menor, que para dos o más redes paralelas.
- Los costos operativos en redes IP tienden a ser menor que en PSTN.
- La red de transporte IP es de futuro prometedor.

La red IP es un componente clave de una NGN por cuanto que proporciona claramente por separados el transporte, el control y las capas de servicios. El acoplamiento de las diferentes capas se garantiza mediante estándares interfaces abiertas. Una NGN se prepara para el futuro de servicios multimedia basados en el subsistema multimedia IP (IMS).

2.11.1 Pasos de la migración de Redes de Telefonía

Teniendo en cuenta los tres pasos principales "Principios Migratorios y procedimientos":

1. Optimización y preparación,
2. Aumento de la capacidad, y
3. Reemplazo de PSTN,

Estos pasos principales se dividen en cinco pasos de migración más detallados, es decir hay otros procedimientos de migración para centrales locales operativa de redes fijas. Se debe destacar que no hay ningún procedimiento estándar definido, dependerá de cada despliegue de demanda red o del proveedor de servicios. Puede haber muchas diferencias en las áreas de cobertura geográfica, la cobertura de red crecen, el envejecimiento de los equipos o la demanda para nuevos servicios.

El alcance y la secuencia por lo tanto, pueden variar e incluso algunos pasos pueden omitirse. Ver tabla 1.

Tabla 1. Pasos para migración de voz

Migración	Pasos de Migración	Red
Inicio	Redes existentes	PSTN para voz TDM y banda estrecha de acceso a Internet de banda ancha a través de DSLAM.
Paso 1	Consolidación PSTN	Introducción de alta capacidad centrales locales y troncales, sustitución de DSLAM y Elementos de red DLC por MSAN´s integrados
Paso 2	NGN en el núcleo de red	Sustitución de central troncal (Switch: clase 4) por clase 4 servidores de llamadas y media-gateways troncales (TG)
Paso 3	NGN en la zona residencial	Despliegue de *residencial gateways* para conectarse a teléfonos heredados, y el reemplazo del CPE con clientes de software o teléfonos IP.
Paso 4	NGN en el acceso de red	Sustitución de central local cambios (clase 5) por switches clase 5, servidores de llamadas y *medias gateways*. Los *Media Gateways* puede ser integrado en MSAN´s.
Paso 5	Cierre de PSTN	Reemplazar los usuarios rezagado en TDM.

Fuente: el autor

La red telefónica pública conmutada (PSTN) ofrecida por proveedores mayoristas (*carrier*) con criterios de calidad de servicio, sabrán definir y aplicar reglas de ingeniería estandarizados. En una comunicación de la red de acceso a Internet se proporciona ya sea a través de acceso telefónico de banda estrecha servicios que utilizan el canal portador en banda, o a través de banda ancha DSL, usando divisores a separar la señal de voz de la señal de datos.

La puerta de enlace de datos entre la PSTN y la Red IP es un servidor de acceso de banda estrecha (NAS). La línea DSL está conectado a un DSLAM y es terminado en un acceso remoto de banda ancha servidor (BRAS). En general, los proveedores de servicios de telecomunicaciones ofrecen sus suscriptores de DSL para acceso a datos de banda ancha. Debido al alcance limitado de DSL, se evolucionó a la línea de abonado digital (DSLAM), terminación de la señal digital en lado de la red, debe acercarse más al abonado. En la figura 3, se aprecia un esquema de red PSTN e IP con arquitectura de red para aplicaciones de voz y datos.

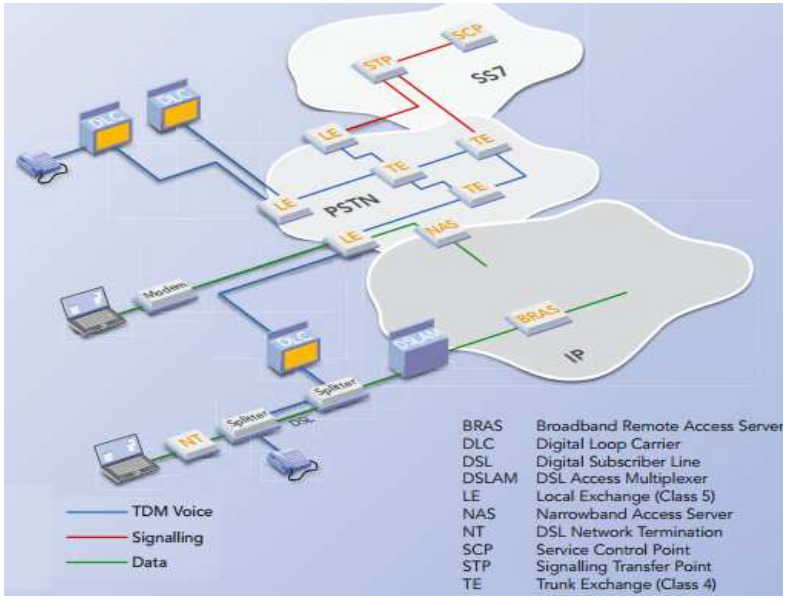

Figura 3. Esquema de arquitectura de red hibrida PSTN-IP para voz y datos

Fuente: Keymile (2008)

2.12 Aplicaciones de redes inalámbricas en NGN

Las redes inalámbricas son sistemas que consisten en docenas, cientos o incluso miles de nodos interconectados a través de canal de conexión inalámbrica y que forman la red única distribuidos espacialmente. La figura 4 representa un ejemplo de una red inalámbrica. Se aprecia en la red, que consta de doce nodos de sensores y un disipador de red, que también funciona como una puerta. Cada nodo sensor es un dispositivo que tiene un transceptor, un microcontrolador, y un elemento sensible (figura 5). Por lo general, nodo sensor es un dispositivo autónomo.

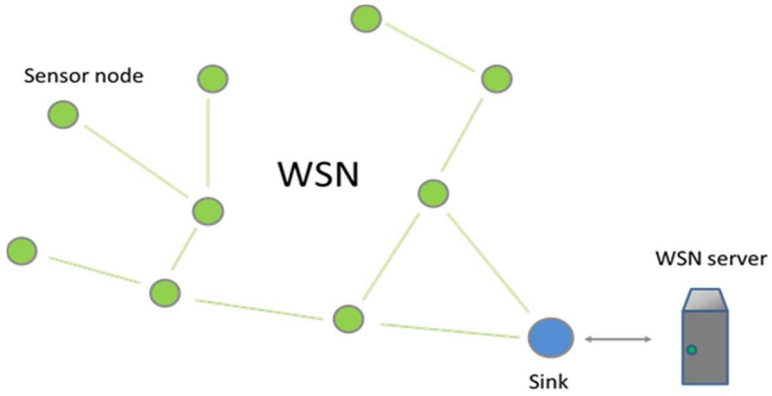

Figura 4. Ejemplo de red inalámbrica

Fuente: Unión Internacional Telecomunicaciones (2014)

Cada nodo sensor en la red inalámbrica mide algunas condiciones físicas, tales como la temperatura, humedad, presión, vibración, y las convierte en datos digitales. El Nodo sensor también puede procesar y almacenar los datos medidos antes de la transmisión.

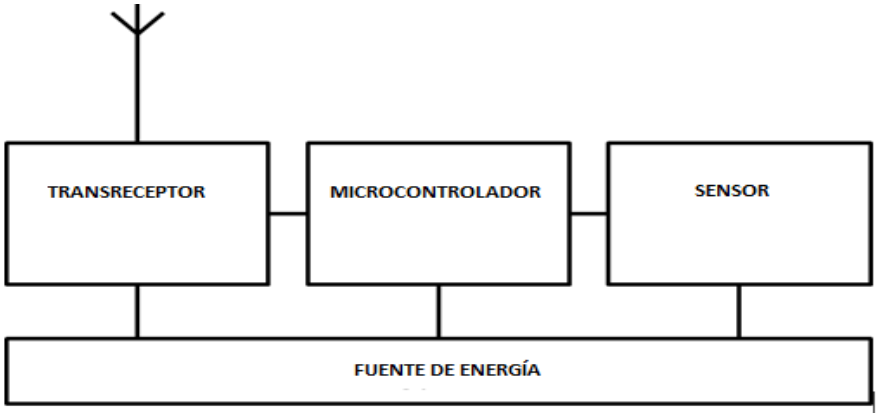

Figura 5. Estructura interna de un nodo

Fuente: El autor

El recipiente de la red es un tipo de un nodo sensor que agrega datos útiles de otros nodos sensores. Como regla general, el recipiente de red tiene una fuente de alimentación estacionaria y está conectado a un servidor que está procesando los datos recibidos de la red inalámbrica. Tal conexión se lleva a cabo directamente, si el servidor y la red inalámbrica se colocan en el mismo objeto. Si es necesario proporcionar un acceso remoto a la red inalámbrica, fregadero de red también funciona como una puerta, y es posible interactuar con la red inalámbrica a través de la red global tal como la Internet.

En redes inalámbricas la comunicación se implementa a través de canal de transmisión inalámbrica mediante bajas transceptores de energía de los nodos sensores. El rango de comunicación de tales transceptores está configurado en primer lugar por razones de eficiencia de energía y la densidad de nodos disposición espacial, y, como regla general, esta cantidad es de aproximadamente unas pocas docenas de metros. Transceptor de nodo sensor tiene contenido energético limitado, y este hecho hace que sea imposible para los nodos de sensores más espacialmente remotas para transmitir sus datos directamente en el recipiente. Así, en red inalámbrica cada nodo sensor transmite sus datos sólo a unos pocos nodos sensores más próximas, que, a su vez, retransmiten esos datos a los suyos nodos sensores cercanos y así sucesivamente. Como resultado, después de un montón de retransmisiones datos de todos los nodos de sensores alcanzar el disipador de red.

Recomendaciones UIT-T relacionadas con redes de nodos inalámbricos

La estandarización es parte integrante del desarrollo efectivo de las TIC, por lo que es útil tener en cuenta las normas y recomendaciones básicas mientras estudia las redes de sensores inalámbricos. En este capítulo vamos a considerar las recomendaciones creadas por la Unión Internacional de Telecomunicaciones (UIT). Todas las recomendaciones de la UIT relacionadas con WSNs definen los requisitos de alto nivel aplicables a cada tipo de WSN con independencia del hardware y el protocolo de pila subyacente. Es por ello que las recomendaciones que vamos a considerar en este capítulo no se cruzan pero complementan la especificación de los protocolos descritos anteriormente en este documento técnico.

2.13 Requisitos para el apoyo de la Red de Sensores Ubicuos (USN)

Como es claro por visión general de la historia, en red de sensores inalámbricos mediados de los años 2000 ya fueron ampliamente utilizados para resolver diversas tareas prácticas, como la automatización industrial, la vigilancia y el control, la automatización del hogar, e-salud, etc. Al mismo tiempo, la primera práctica protocolos para redes de nodos inalámbricos relacionados con la transferencia de datos vía radio, enrutamiento, auto-organización, se habían creado autocuración. La esencia del siguiente nivel de desarrollo red de sensores inalámbricos, fue la integración de

diversos tipos de redes dentro de los marcos de plataforma común, la transición de un gran número de redes de sensores sin coordinación a la infraestructura de información inteligente de la sociedad avanzada. Este proceso se vio reflejado en el concepto de Red de Sensores Ubicuas (USN).

El debate sobre la USN se inició en febrero de 2007 por el Instituto de Electrónica y Telecomunicaciones de Investigación (ETRI) (Corea). Las Comisiones de Estudio del UIT-T. Por consiguiente, consideró necesario reforzar la coordinación a fin de avanzar los estudios sobre los USN, y en este sentido, se decidió iniciar un nuevo tema de trabajo sobre cuestiones generales de la USN en la Comisión de Estudio 13. En enero de 2010, después de casi tres años de activa el trabajo, la Recomendación había sido aprobado y obtuvo el número Y.2221.

2.13.1 Descripción de USN y características

La Recomendación Y.2221, define la USN como una red conceptual construido a través de redes físicas existentes, que hace uso de los datos obtenidos y proporciona servicios de conocimiento a cualquier persona, en cualquier lugar y en cualquier momento, y donde la información es generada por el uso de la sensibilidad al contexto. En esta definición "redes físicas" significa no sólo los distintos tipos de redes inalámbricas de sensores, sino también conectan las redes de sensores y lectores RFID.

En la figura 6, se representa el plan de la estructura USN, ilustra algunas particularidades intermedios además de mencionado previamente en las redes y los servicios físicos

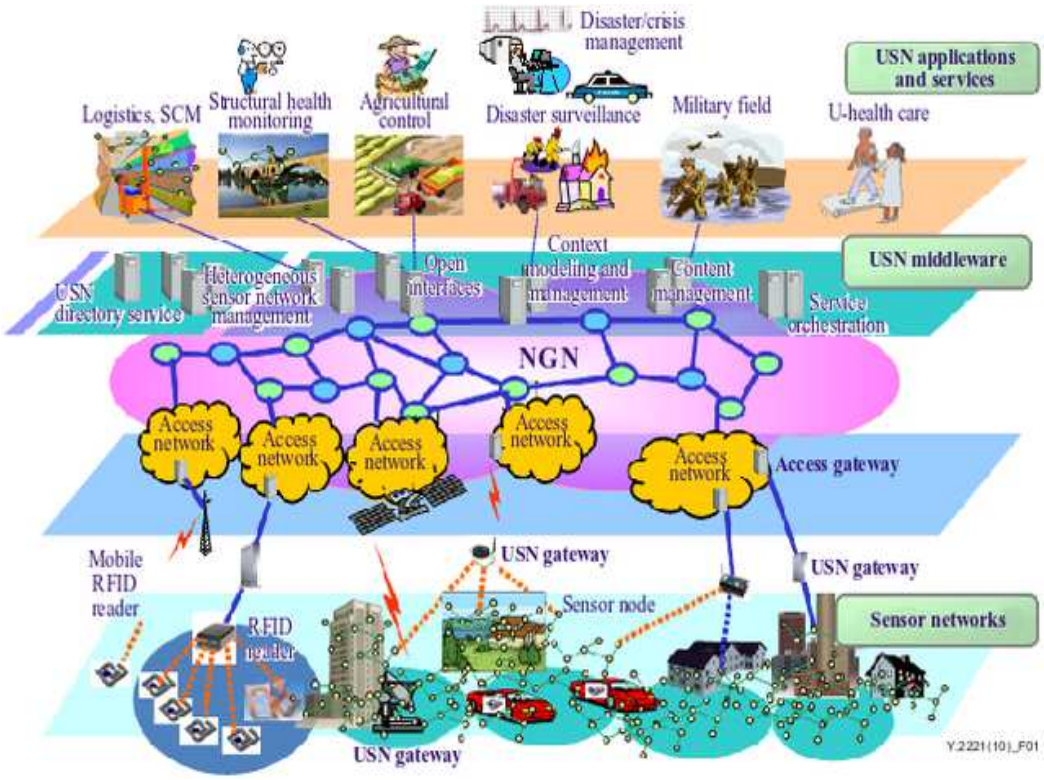

Figura 6. Una visión general de USN

Fuente: Unión Internacional Telecomunicaciones (2014)

El anhelado sueño de una plataforma común de transportes para el vídeo, voz y datos se llevará a cabo. La NGN permitirá aplicaciones como la telefonía IP, acceso a la Web a través de los teléfonos móviles y video *streaming* se convertirá en una realidad.

En primer lugar, una capa adicional middleware USN se está introduciendo, el middleware USN es un software en un servidor especial que funciona como mediador entre la red física y sus usuarios. Se tiene la intención de ocultar todas las complicaciones de las redes físicas de un desarrollador y para dar API conveniente que puede ayudar a controlar la red y obtener acceso a los datos obtenidos por e información relacionada: ubicación del sensor, estructura de la red, el nivel de salud y la batería de dispositivos.

Por otra parte, el middleware puede ser responsable para el examen elementos específicos, organización de planes de consulta, la detección de fallos y eliminación, el control de la fuente de alimentación de dispositivos ', la autenticación, la codificación, que proporciona a la confidencialidad, el almacenamiento de datos, filtrado de datos, minería de datos y otras tareas similares que son común para diferentes servicios y aplicaciones. Como resultado, las aplicaciones se pueden desarrollar en forma de acoplamiento flexible, es decir, sin tener en cuenta las peculiaridades de las redes físicas específicas. Esto ofrece las siguientes ventajas:

Desde el punto de vista del proveedor de red física - la ampliación de la gama de servicios con el apoyo de las redes de sensores producidos por el vendedor.

Desde el punto de vista del proveedor de servicios - aumentar el número de plataforma de destino, es decir, redes físicas producidas por diferentes vendedores, que pueden utilizarse para proporcionar el servicio.

Desde el punto de los desarrolladores de aplicaciones de vista - el desarrollo más fácil que ayuda a reducir los gastos en la nuevas características Además, la detección y recuperación de problemas, portar aplicaciones a diferentes plataformas (por ejemplo, la creación de nuevas interfaces móviles y web).

Desde el punto de vista comercial, el cambio del modelo de negocio vertical a la horizontal uno, cuando en lugar de una gran empresa que le da toda la gama de soluciones no puede haber unos pocos proveedores y vendedores diferentes que compiten en el mercado.

En una red USN NGN cumple dos funciones: el transporte y el servicio. La función de medio de transporte que faciliten la conexión entre las redes y los usuarios de los sensores separados desde cualquier lugar en el mundo. También estas redes de sensores se pueden conectar entre sí la creación de una estructura común. Grupos separados de las redes de sensores pueden conectarse a NGN red de acceso, tanto directa como a través de la pasarela de USN. El uso de la puerta de enlace USN es necesario cuando la red de sensor trabaja con un protocolo incompatible con IP.

La función de servicio de NGN consiste en proporcionar a los usuarios de las mismas posibilidades en los servicios de red de sensores que en otros servicios NGN: el acceso a los servicios a través de varios terminales, interfaz de usuario intuitiva y consistente, proporcionando calidad de servicio a través de diferentes redes de proveedores. En comparación con otros servicios de servicios NGN USN tener una serie de características específicas. Como resultado, NGN tiene que mantener en las capacidades ampliadas establecidos para responder a los requisitos de servicio USN específicos. La lista de estos requisitos y su justificación junto con las correspondientes capacidades NGN son los asuntos del resto de la Recomendación Y.2221.

2.14 Aplicaciones y servicios USN

Un elemento o dispositivo clave en la USN es el Sensor de gestión de red, la configuración y reconfiguración. En el entorno USN, se requiere para administrar diversos tipos de redes de sensores. La configuración y reconfiguración de las redes de sensores pueden requerir diferentes mecanismos que la gestión de red tradicional, como las redes de sensores normalmente son un grupo de nodos.

Una red de sensores no debe perder su conectividad o su funcionalidad a pesar de la pérdida de una conexión con un único nodo de la red debido a la conexión o fallo en el hardware, que tiene una alta probabilidad de ocurrencia en las redes de sensores. La configuración y reconfiguración de una red de sensores se utilizan para apoyar la garantía de la conectividad y la gestión de toda la vida. Para USN los más importantes de ellos son los siguientes:

Servicio de registro - La gestión de la información sobre los servicios (es decir, los perfiles de servicio, que se describe en el punto anterior).

Descubrimiento de uso - Buscar por el usuario por todos los servicios registrados y dándole información de servicios relacionados.

Composición de servicio - Capacidad de crear nuevos servicios de otros servicios existentes por la reutilización de los recursos existentes. Servicio composición puede ocurrir en una estática o de una manera dinámica. Mientras que en la composición estática, servicios compuestos están definidos de antemano, la composición dinámica envía la solicitud de descubrimiento de servicios utilizando la descripción del servicio para encontrar los servicios necesarios y compone los servicios durante el tiempo de ejecución.

La coordinación de servicios - La capacidad de gestionar las relaciones e interacciones entre los servicios para proporcionar una "cadena de servicios", es decir, un conjunto de servicios interconectados que tienen que ser ofrecidos en una secuencia específica.

El uso de lenguaje de descripción de servicio (SDL) para formal (es decir, comprensible para máquinas) que describe la funcionalidad, que ofrece los servicios. Ejemplo de SDL utilizado en la práctica es el de servicios web basados en XML (lenguaje de descripción WSDL), creado por el Consorcio World Wide Web. Es necesario utilizar para USN su propio SDL de acuerdo con sus peculiaridades.

La QoS diferenciados y priorización de datos, Los diferentes tipos de servicios tienen diferentes demandas en las capacidades de transporte de una red. Por ejemplo, si los datos obtenidos se utilizan para tomar decisiones de inmediato, es posible hacer demandas a la latencia. Si se planifica la transmisión de datos urgente e importante a través de un determinado canal, su capacidad completa o una parte de ella se pueden reservar.

Por ejemplo, la notificación de emergencia de un incidente de fuego debe ser entregada de manera oportuna y confiable para los sistemas de monitoreo de desastres adecuados. Datos menos importantes pueden ser transmitidos sobre una base de mejor esfuerzo, es decir, la obtención de tasa de bits y la entrega de tiempo variable no especificado,

dependiendo de la carga de tráfico actual. Cada requisito, similar a los mencionados anteriormente, se define por la calidad de servicio (QoS). Muchos protocolos de red hacen posible especificar el tipo de QoS uno u otros datos se refieren a, y por lo tanto, definir la prioridad de su transmisión y procesamiento.

Los Servicios USN tienen características únicas en términos de prioridad de servicio. Por ejemplo, los datos detectados pueden ser enviados al nodo central no inmediatamente, es posible que la medición de los resultados a primera están siendo reunidos por un nodo sensor o por un par de nodos, y luego ser enviados con otros resultados de medición dentro de una transacción. El volumen de transacción de aplicación puede ser muy alta. Así, las demandas particulares en calidad de servicio se pueden realizar con el fin de gestionar el volumen de transacciones generadas por las aplicaciones y servicios de USN y para que sea posible para evitar la concentración de acceso a un único recurso.

El apoyo de los diferentes tipos de conectividad y redes. En USN nodos sensores puede ser basado en IP o no IP. En el primer caso, aunque el subyacente cableadas y / o control de acceso al medio inalámbrico gestiona la conectividad, las conexiones entre los usuarios finales de la USN y redes de sensores se implementan a través de la IP. En este tipo de redes de sensores, puede ser posible que un nodo único sensor está conectado directamente a las redes de infraestructura sin una puerta de enlace USN.

En las redes de sensores no basados en IP, nodos de sensores no tienen direcciones IP, y las conexiones entre los usuarios finales de la USN y redes de sensores son posibles sólo a través de las puertas de entrada de la USN. Interfaz de red basada en la no-IP se puede utilizar para diferentes razones, como la imposibilidad de dar su propia dirección IP a cada nodo de la red de sensores, la capacidad computacional limitada de nodos de redes de sensores que no proporcionan soporte de IP-pila, ahorro de energía de la batería debido a negarse de operación de paquete IP de procesamiento que requiere gran capacidad computacional.

Ambos tipos de redes tienen que ser apoyado, además, varios tipos de cableados y/o conexiones de medios inalámbricos pueden ser utilizados para la conectividad entre redes de sensores y redes de infraestructura.

Ubicación gestión. capacidad de gestión de la ubicación se especifica en la Recomendación Y.2201 para la ubicación de los usuarios y los dispositivos dentro de las redes. En esta ubicación documento de gestión significa posibilidad de utilizar la información relativa a la posición física de los objetos, por lo tanto, la mejora de las aplicaciones con el contexto local y relevancia.

Además, en los USN la ubicación de redes de sensores y nodos de sensores individuales necesita ser mantenido y gestionado con el fin de apoyar la conciencia contexto con información sobre la ubicación de las aplicaciones y servicios de la USN. Además, el servicio y la detección de dispositivos pueden ser facilitadas por el uso de la información de ubicación.

Apoyo a la movilidad. La movilidad, como se especifica en la Recomendación Y.2201, implica la capacidad de los objetos móviles, como usuarios, terminales y redes, para poder moverse entre las diferentes redes. Se consideran dos tipos de movilidad: la movilidad personal donde los usuarios pueden utilizar los mecanismos de registro de asociarse con un terminal que la red puede asociar con el usuario y la movilidad del terminal aquí los mecanismos de registro se utilizan para asociar el terminal a la red.

Proporcionar movilidad de terminales en USN puede llegar a ser una tarea difícil. Las Tecnologías de movilidad IP existentes pueden ser adaptados para redes de sensores basados en IP.

Además de la clasificación antes mencionada, en USN puede haber tres tipos más de la movilidad:

1. Movilidad red intra-sensor: un nodo sensor de movimiento dentro de una red de sensores.
2. Movilidad red Inter-sensor: un nodo sensor de movimiento a través de múltiples redes de sensores.
3. La movilidad de red: Una red de sensores en movimiento a través de redes de infraestructura (por ejemplo, a través de las NGN y no NGN).

Un escenario que ilustra los requisitos de movilidad se puede encontrar en el dominio de la aplicación de la salud. Por ejemplo, los datos de control médico de un paciente

pueden ser monitoreadas a través de una red de sensores. Varios sensores pueden estar unidos al paciente, resultando en una red de sensores área del cuerpo. Los sensores se reúnen periódicamente los datos de control médico y los envían a médico del paciente a través de una casa de puerta de enlace cuando el paciente está en casa; mientras se mueve, los datos pueden ser enviados a través de una pasarela de acceso en un coche, autobús, tren o metro en red.

Varios casos de movilidad pueden ocurrir en un escenario de dicha aplicación.

Soporte de seguridad. En general, las aplicaciones y servicios de USN necesitan seguridad, debido a los datos detectados muy sensibles. Es por eso que la UIT, ha creado un conjunto de recomendaciones sobre la seguridad en los USN, que va a tener en cuenta en los detalles a continuación en este documento técnico.

La identificación, autenticación y autorización. Identificación (procedimiento de reconocimiento de personas), autenticación (Procedimiento de verificación), la autorización (concediendo derechos a hacer algunas acciones) se consideran a menudo juntos, porque todos ellos tienen por objeto impedir la red no autorizado el uso y acceso de datos. En las aplicaciones y servicios de la USN, los datos pueden tener diferentes niveles de requisitos de autenticación.

Por ejemplo, en los sistemas militares, datos detectados primas son tan importantes como datos de servicio que se derivan de datos detectados primas por el procesamiento y la manipulación de los proveedores de servicios o aplicaciones, si bien esto puede no ser el caso para otros sistemas (por ejemplo, sistemas de hospital). Por lo tanto, los diferentes niveles de autenticación para los diferentes tipos de datos en base a los requisitos de las aplicaciones y servicios de USN deben ser apoyadas.

Apoyo de Privacidad. Al usar USN, existe el peligro de que terceros no autorizados puedan tener acceso a la información crítica. Por ejemplo, la mera observación cuándo y dónde eventos dentro de un USN ocurren, pueden comprometer la seguridad de la propia USN, así como la seguridad de los usuarios finales de la USN. En este sentido, se requieren medidas especiales de privacidad de USN.

Apoyo de las diferentes políticas de contabilidad y de carga. funciones de contabilidad general NGN y de carga se especifican en Y.2233. USN puede requerir el apoyo de las diferentes políticas de contabilidad y de carga de acuerdo a los diferentes tipos de transacciones de datos. Como ejemplo, hay aplicaciones y servicios cuyos datos obtenidos no tienen que ser transmitidos continuamente a los sistemas de aplicación de la USN, pero es suficiente si se transmiten, al menos una vez, en un plazo determinado de tiempo. En estos escenarios, las conexiones de red pueden permanecer en un estado inactivo durante mucho tiempo. Por el contrario, algunas otras aplicaciones y servicios USN pueden generar continuamente y transmitir datos de *streaming*. Es obvio que cada uno de estos casos requiere un enfoque especial de la contabilidad y de carga.

2.14.1 Amenazas en redes de sensores

Amenazas generales en las redes de computadoras / telecomunicaciones se describen en la Rec. UIT-T X.800. Rec. UIT-T X.1311, además de los enumera las amenazas específicas del nodo sensor:

- **Vulnerabilidad de los nodos sensores:** Se espera que las redes de sensores para consistir en cientos o miles de nodos sensores. Cada nodo representa un posible punto de ataque, lo que hace el seguimiento y protección de cada sensor individual ya sea de un físico o un ataque lógico impracticable. Las redes pueden dispersarse sobre un área grande, expone aún más a los atacantes captura y reprogramación de los nodos sensores individuales. Los atacantes también pueden obtener sus propios nodos de sensores de los productos básicos e inducir la red a aceptarlos nodos como legítimas, o que pueden reclamar múltiples identidades para un nodo alterado. Una vez en el control de unos pocos nodos dentro de la red, el atacante puede montar una variedad de ataques, como la falsificación de los datos del sensor, la extracción de información detectada privada de las lecturas de redes de sensores, y negación de servicio.
- **Espionaje:** En las comunicaciones de redes de sensores inalámbricos, un *hacker* puede tener acceso a información privada mediante el control de las transmisiones entre los nodos. Por ejemplo, unos receptores inalámbricos colocados fuera de una casa pueden ser capaces de controlar la luz y temperatura lecturas de redes de

sensores dentro de la casa, lo que revela información detallada sobre las actividades diarias personales de los ocupantes.

- **El hurto de los datos:** Las redes de sensores son herramientas para la recopilación de información; un adversario puede tener acceso a la información sensible, ya sea mediante el acceso a los datos del sensor almacenados o mediante la consulta o el espionaje en la red. Los adversarios pueden utilizar incluso los datos aparentemente inocuos para obtener información sensible si saben cómo correlacionar múltiples entradas de sensor. Las redes de sensores exacerban el problema de privacidad porque hacen grandes volúmenes de información fácilmente disponible a través de acceso remoto. Por lo tanto, los atacantes no tienen que ser físicamente presente para mantener la vigilancia. Pueden recopilar información en un bajo riesgo, de manera anónima. El acceso remoto también permite que un solo adversario para supervisar varios sitios al mismo tiempo.
- **Ataques DoS:** Como las aplicaciones críticas para la seguridad utilizan más las redes de sensores, el daño potencial de errores de funcionamiento se vuelve significativa. La defensa contra denegación de servicio ataques que tienen como objetivo destruir la funcionalidad de red en lugar de subvertir o utilizando la información detectada es extremadamente difícil. Ataques DoS pueden ocurrir en la capa física, por ejemplo, a través de interferencia de radio. También pueden implicar transmisiones maliciosos en la red para interferir con los protocolos de redes de sensores o destruir los nodos de red centrales físicamente.
- **El uso malicioso de las redes de los productos básicos:** La proliferación de redes de sensores inevitablemente extenderse a los criminales que pueden usarlos para propósitos ilegales. Por ejemplo, los ladrones pueden *hackear* sensores domóticos o simplemente espiar su actividad para obtener información privada de la presencia, localización, etc., de los propietarios y actuar en consecuencia. Si los sensores son lo suficientemente pequeños, también pueden ser plantados en las computadoras y teléfonos celulares para extraer la información privada y contraseñas. Este uso generalizado reducirá las barreras de costo y disponibilidad que se supone para desalentar este tipo de ataques.

- **Amenazas de enrutamiento específico:** La Rec. X.1311 especifica siete tipos de ataques que son específicos al sensor protocolos de enrutamiento de red: falsificado, alterado o reproducido la información de enrutamiento; reenvío selectiva; ataques sumidero; ataques Sybil; agujeros de gusano; HOLA ataques de inundación; *spoofing* acuse de recibo.

2.14.2 Dimensiones de Seguridad para las Redes de Sensores Ubicuos (USN)

Una dimensión de la seguridad es un conjunto de medidas de seguridad diseñadas para tratar un aspecto particular de la seguridad de red para proteger frente a las principales amenazas a la seguridad; no se limita a la red sino que se extiende a las aplicaciones y la información del usuario final también. La Rec. X.1311 adopta dimensiones de seguridad, que se describe en la Recomendación X.805:

- **Confidencialidad de los datos:** El enfoque estándar para mantener los datos sensibles es confidencial para cifrar los datos con una clave secreta que sólo los receptores previstos poseen, garantizando así la confidencialidad.
- **Datos de autenticación/identificación:** Autenticación de datos permite a un receptor para verificar que los datos fueron realmente enviado por el remitente dice ser tales. La identificación tiene por objeto demostrar la identidad de la entidad o nodo sensor. Junto con la autenticación de la comunicación de dos partidos, es muy importante proporcionar emisión autenticado en redes de sensores, ya que la construcción del árbol de enrutamiento, consulta de red, actualizaciones de software de sincronización de tiempo, y la gestión de la red todos se basan en la difusión.
- **Integridad de los datos:** La integridad de datos asegura el receptor que los datos recibidos no se altera en tránsito por un adversario.
- **Control de acceso:** El control de acceso garantiza que sólo el usuario o entidad autorizada se le permite tener acceso a la información, recursos o servicios.
- **No repudio:** No repudio asegura que la entidad o usuario no pueden negar las actividades en la red que ha hecho.

- **Seguridad en las comunicaciones:** la seguridad Comunicación asegura que la información sólo fluye desde el origen al destino.
- **Disponibilidad:** disponibilidad garantiza que la información, el servicio, y la aplicación están disponibles para los usuarios legítimos en cualquier momento.
- **Privacidad:** Privacidad asegura que el identificador del usuario o entidades y uso de la red se mantiene confidencial.

La Rec. X3211 identifica dimensión de seguridad adicional - resistencia a los ataques, lo que es aplicable sólo para redes de sensores. La resistencia a los ataques se refiere a las medidas para la recuperación de los diversos ataques contra la USN. Se asegura que el USN es capaz de recuperarse de los ataques de modo que sea capaz de detectar/remanente resistentes a varios ataques a través del diseño apropiado de los protocolos de PHY/MAC/enrutamiento.

2.14.3 Técnicas de Seguridad para las Redes de Sensores Ubicuos-USN

La gestión de claves. La gestión de claves se refiere a la generación, distribución, intercambio, cambio de claves, y la revocación de las claves criptográficas. La seguridad de la gestión de claves es la base de la seguridad de otros servicios de seguridad. En general, hay tres tipos de gestión de claves: esquema de servidores de confianza, auto-esquema de la aplicación, y el esquema de clave pre-distribución.

Pero el esquema de servidor de confianza (por ejemplo, Kerberos) no es adecuado para la red de sensores ya que no hay infraestructura de confianza en la red de sensores; el esquema de auto-aplicación de que utiliza el algoritmo de clave pública (por ejemplo, Diffie-Hellman o RSA algoritmos de clave de transporte) no se puede emplear en la red de sensores debido a la memoria limitada y la complejidad computacional del nodo sensor.

El esquema de clave pre-distribución pre-distribuye la información clave entre todos los nodos de sensores antes del despliegue. Este esquema es el más adecuado para la red inalámbrica de sensores, ya que tiene bajos costos de comunicación, es resistente al nodo compromiso, y no se basa en la confianza de la estación base. Rec. X.3211 identifica los siguientes requisitos para la gestión de claves:

- Capacidad para soportar grandes redes de sensores y la flexibilidad para manejar un aumento sustancial de sensor nodos incluso después de la implementación del nodo sensor.
- Eficiencia del tamaño de la memoria para almacenar la clave en el nodo sensor, la eficiencia de la complejidad de cálculo requerido para establecer la clave, la eficiencia de la comunicación de arriba, es decir, el número de mensajes intercambiados durante el proceso de generación de claves.
- Alta probabilidad de establecimiento de claves de pares si se utilizan algoritmos de gestión de claves aleatorias.

Confirmación de difusión. Debido a la naturaleza de la comunicación inalámbrica en redes de sensores atacantes pueden inyectar fácilmente datos maliciosos o alterar el contenido de los mensajes legítimos durante el avance de múltiples saltos. Aplicaciones de redes de sensores necesitan mecanismos de autenticación para asegurar que los datos de una fuente válida que no se modificarán durante la transmisión. Dos tipos de técnicas se pueden utilizar de acuerdo con el tipo de algoritmo criptográfico. En el caso de la criptografía de clave pública, una firma digital se puede utilizar. Si se utiliza la criptografía simétrica, hay una necesidad de añadir a los datos de los datos de autenticación verificables (es decir, código de autenticación de mensaje), basado en el secreto compartido múltiple entre la estación de base (nodo de sumidero) y el nodo sensor. Debido a las propiedades de la red de sensores, se prefiere el método de autenticación de emisión en la autenticación de mensaje de difusión basado en la criptografía simétrica.

La agregación de datos seguro. La agregación de datos seguro se refiere a un proceso dentro de la red se realiza en el nodo agregador para transferir con seguridad el valor de agregación al nodo de sumidero (es decir, una estación base) mediante la combinación de los valores detectados enviados por un número de nodos de sensores. En este esquema, cada nodo sensor envía un valor detectado cifrada al agregador, el cual calcula los resultados agregador cifrados utilizando funciones de agregación, como la función suma, la función de la media, la función de la mediana, y el valor máximo o el valor

mínimo; el nodo receptor obtiene el valor de agregación descifrando los resultados agregador cifrados.

Actualización de datos. Desde todas las redes de sensores de flujo de algunas formas de medidas variables en el tiempo, garantizando la confidencialidad y la autenticación no es suficiente; también hay que asegurarse de que cada mensaje es fresco. La actualización de datos implica que los datos son reciente y se asegura de que ningún adversario repite los mensajes antiguos.

Resistente a la manipulación del módulo. La técnica mejor conocida para proteger contra compromiso nodo sensor es utilizar el módulo resistente a la manipulación en el nodo sensor. Si cada nodo sensor está equipado con un módulo a prueba de manipulaciones, la protección del almacenamiento de los datos sensibles, por ejemplo, datos de clave, puede ser posible; de lo contrario, el daño puede ser disparados en caso de captura de los nodos sensores. Otra posible técnica en la protección contra un nodo sensor comprometida es limitar la cantidad de información obtenida por el atacante después de leer los datos de los nodos de sensores capturados. El módulo criptográfico (FIPS PUB 140-2) es un ejemplo de un módulo de prueba de manipulaciones que asegura que los datos sensibles sin daños de almacenamiento.

Seguridad middleware USN. Según el Rec. X.1312 describe las siguientes técnicas de seguridad:

- **Control de acceso:** Los bloques de middleware USN el acceso de las aplicaciones de la USN no autenticados y no verificados, así como redes de sensores elementos (por ejemplo, sensores de nodos y estaciones base).
- **Protección de los datos almacenados:** El middleware USN utiliza la gestión de identidades y seguridad de base de datos para mantener los datos de detección, identificación y autenticación de información de redes de sensores y las aplicaciones de la USN segura.
- **Seguridad de los datos de transmisión/recepción:** El *middleware* USN utiliza el cifrado/descifrado y comprobación de integridad en el intercambio de datos sensibles (por ejemplo, contraseñas) con aplicaciones de USN y redes de sensores elementos.

- **Canal seguro:** El *middleware* USN establece un canal seguro para proteger el intercambio de datos entre las aplicaciones y middleware y entre la red de sensores y middleware.

Técnicas de enrutamiento específico. En las primeras etapas de desarrollo de los protocolos de enrutamiento en redes inalámbricas de sensores han sido optimizados para la reducida capacidad de los nodos y la naturaleza específica de la aplicación de las redes, pero no tienen en cuenta la seguridad. Sin embargo, hoy ya se han desarrollado unos algoritmos más eficaces.

Protección de la privacidad en las redes de sensores. Junto con el cifrado de datos y control de acceso a un enfoque típico para asegurar la preservación de privacidad en una red de sensores es limitar la capacidad de la red para recoger los datos detectados en tal nivel de detalle que la privacidad de los individuos en cuestión podría verse comprometida. Por ejemplo, la red de sensores podría informar de la temperatura agregada sobre un área grande en lugar de un área pequeña.

2.14.4 Redes de control del sensor

En el principio del desarrollo redes de nodos inalámbricos, fueron considerados simplemente como el método para la medición de parámetros físicos en grandes espacios. En este modelo (ver figura 7) lecturas recogidas por los nodos sensores son transferidos a un determinado nucleo-centro, donde se procesan estas lecturas y se toman decisiones.

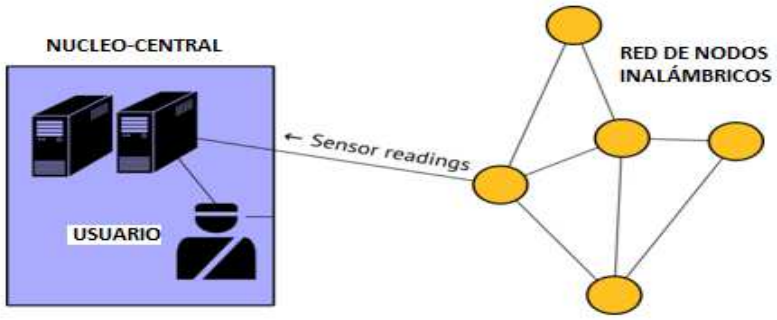

Figura 7. Servicio WSN original modelo de prestación

Fuente. NGN-AWSN-2014

Hoy, el modelo ha sufrido algunos cambios (figura 8). Una nueva esencia apareció en ella, un grupo de usuarios: personas, máquinas o mecanismos, cada uno de ellos es un usuario. Y la decisión puede ser común para todos los usuarios o individuales para cada uno de ellos. El ejemplo del primer caso es la notificación de una población de la ciudad sobre el terremoto que viene; el ejemplo del segundo caso es un sistema médico que notifica al personal médico y familiares sobre posibles problemas en la presión arterial o el pulso del paciente están alcanzando el punto crítico.

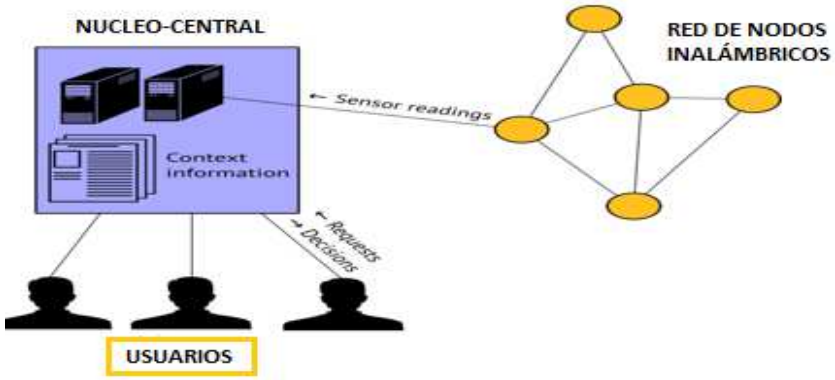

Figura 8. Modelo de prestación de WSN Multi-usuario

Fuente: NGN-AWSN (2014)

Si la decisión es individual para cada usuario, el centro de toma decisiones no sólo basándose en los datos dados por los sensores, sino también de acuerdo con la información de contexto , como caso la historia del paciente, que define algunas reglas para la toma de decisiones para un usuario concreto.

Sin embargo, en algunas aplicaciones de este modelo tiene una variedad de deficiencias:

- **Bajo la escalabilidad.** Aumento del número de WSN conduce a un incremento de la carga en el centro. Cuando se añaden nodos de sensores, se requiere el cálculo de los recursos para procesar gran cantidad de lecturas. Pero el aumento de número de usuarios tiene una influencia aún mayor aquí. Si bien este número es pequeño, el centro puede hacer fácilmente las decisiones para todo el mundo. Puesto que cada usuario tiene peculiaridades y necesidades individuales, que las tenga en cuenta que el centro ha no sólo para ampliar la cantidad de información de contexto en función del tamaño de la base de usuarios, sino también para ampliar

su estructura, y, en consecuencia, su volumen adjunta a cada usuario. Por ejemplo, cuando WSN con la aplicación de la asistencia sanitaria se utiliza para controlar la condición de los pacientes ordenados para el reposo en cama, la aplicación puede emitir una alarma cada vez que la frecuencia del pulso de cualquier paciente excede cierto umbral. Si la aplicación está destinada a ser utilizada tanto por las personas enfermas y sanas, es necesario analizar si las palpitaciones se conecta con la enfermedad o la actividad física normal y si el estado actual es permitido que una persona concreta. En este caso, el centro necesita una base de datos con indicadores médicos de todos los usuarios y tienen que utilizar un complicado sistema de toma de decisiones. Junto con las exigencias de fiabilidad extremadamente pesadas impuestas a las aplicaciones e-salud, que puede conducir a cargas inadmisibles necesarias para equipar el centro.

- **Fiabilidad insuficiente.** El modelo representado en la figura 8, es uno centralizado, en el sentido de que todas las decisiones son tomadas por el centro. Esto significa que si el centro está desactivada, la red se convierta en totalmente inservible. Además, el centro no es el único punto de fallo. Incluso si el centro está en buenas condiciones de trabajo, hay una necesidad de un poco de canal central de comunicación para transmitir las decisiones para el usuario.

El fracaso del núcleo central o de la línea central de la comunicación puede ser causada tanto por la sobrecarga interna (crecimiento no planificado de flujo de datos de los sensores o solicitudes de servicio de los usuarios) y las razones externas (energía eléctrica cortada, la destrucción física de los equipos, acciones de los atacantes). Además, las causas de ambos tipos surgen en el momento en que se necesitan servicios de red de nodos inalámbricos más de todo.

Por supuesto, el problema de la baja fiabilidad se puede resolver por medio de la división de las funciones del centro de entre unos pocos objetos dispersos geográficamente. Pero aquí nos enfrentamos de nuevo la cuestión de costos WSN: además de los cargos en la construcción de centros complementarios, es necesario aumentar la complejidad de los nodos sensores para proporcionar su trabajo con unos pocos centros. Por la razón de que el número de nodos inalámbricos puede ser muy

grande, límites presupuestarios pueden hacer conseguir necesario nivel de fiabilidad imposible.

Problemas aplicaciones en tiempo real. En algún intervalo de tiempo durante el cual las aplicaciones de decisiones se mantienen válido es muy corto. Se produce en los casos en que los usuarios necesitan de control continua de las acciones de ellos, por ejemplo, si hay una necesidad en la navegación en el entorno desconocido y cambiando rápidamente: en la carretera, en el momento de las operaciones de combate o situaciones de emergencia. Estas aplicaciones se denominan aplicaciones en tiempo real.

En la mayoría de los casos, en las decisiones de este tipo de aplicaciones requiere la toma de lecturas de sensores situados en la proximidad inmediata del usuario. El retraso entre el cambio de algunos parámetros físicos que tiene que evocar respuesta del usuario, y trayendo decisión apropiada desde el centro hacia el usuario, se compone con el tiempo de detección de este cambio por un nodo sensor, la transmisión de esta información a través de redes de nodos inalámbricos, los datos procesamiento en el centro y la decisión de transmitir a través del canal central de comunicación para el usuario.

Cuando el número de nodos de sensores está aumentando, de estos cuatro constituyentes está aumentando más rápidamente, porque la cantidad de saltos de un nodo al centro depende de la extensión de la red. Además, todos los elementos temporales están surgiendo junto con el número de usuarios. Como resultado, si el alcance de la red es grande, las decisiones tomadas por el centro pueden ser ya no es válida cuando el usuario los recibe. Estos problemas causan buscando otros modelos de servicio que proporciona para los casos en que hay una necesidad de escalabilidad y soporte de aplicaciones en tiempo real.

2.14.5 Características SCN

En primer lugar, este modelo tiene que ser descentralizado. Esto significa que la importancia del centro tiene que ser lo más pequeño posible, y por lo menos un cierto número de decisiones tienen que hacerse sin ella. Este enfoque se refleja en el concepto de Redes de Control del Sensor (SCN, *Sensor Controller Network*).

La idea de este concepto por primera vez fue declarada en el año 2010 en la Recomendación UIT-T por la Administración de Comunicación de la Federación Rusa. La contribución presentada para su debate en la Comisión de Estudio 13 se basó en investigaciones de Radio Instituto de Investigación y Desarrollo (Moscú) que se produjeron durante la elaboración personalizada Sistema de Gestión de Emergencias (CEMS). Por último, el trabajo del Grupo de Estudio 13 terminó en la producción de Recomendación Y.2222 "Redes de control de sensores y aplicaciones relacionadas en el entorno de red de próxima generación".

El CEMS fue diseñado de tal manera que podría proporcionar la navegación para las personas en los edificios en caso de incendio u otras situaciones de emergencia, incluso cuando la energía eléctrica se corta, algunos nodos de la red son los canales de comunicación con discapacidad y centrales como Internet por cable y GSM/3G/4G son inabordables. Así, las tres deficiencias descritas anteriormente no permitían utilizar el modelo centralizado "corriente" de servicio que proporciona.

En lugar de ello se utilizó el modelo que se muestra en la Figura 9, en contraste con las cifras anteriores, éste no ilustra qué tipo de información se transmite de un objeto a otro. Está conectado con el hecho de que cada objeto puede desempeñar diferentes funciones, como se describirá más adelante.

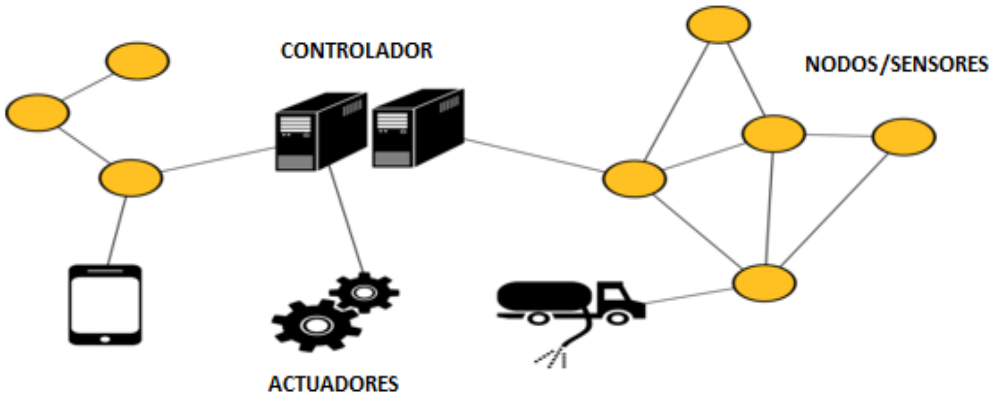

Figura 9. Modelo de la prestación del servicio SCN

Fuente. NGN-AWSN (2014)

Además, una nueva entidad aparece en el modelo, es decir, un actuador, un cierto dispositivo electrónico o electromecánico que puede interactuar con otras entidades

SCN y ser controlados por ellos. Un actuador es un dispositivo que en realidad resuelve las tareas SCN era despliega para, por ejemplo, activa los mecanismos o muestra mensajes para el usuario en la pantalla.

Hay tres tipos de actuadores: Los actuadores de información, que están destinados a proporcionar visual, de audio, la interacción sensorial con el usuario humano; accionadores de puerta de enlace, que están destinados para reenviar los comandos de gestión que ofrece el SCN a otras redes; accionadores de la máquina, que son dispositivos electromecánicos destinados a la interacción física con el medio ambiente externo. En otros modelos que prestan servicio WSN estos dispositivos juegan papel pasivo: simplemente llevar a cabo las órdenes dadas por el centro.

En SCN actuador recibe no decisiones, pero los datos que permite tomar decisiones; tiene software y hardware que hacen posible para seleccionar el mejor escenario de acción, teniendo en cuenta, de una parte, estos datos, desde otro lado, peculiaridades y necesidades del usuario.

La misma afirmación es válida para los nodos sensores. En SCN, además de elemento sensor y modulo-radio previsto para la conexión con otros nodos, tienen un microcontrolador o microprocesador que permite proporcionar un procesamiento de datos. Tales nodos sensores inteligentes se denominan “motas” pero en i es un sensor específico. Debido a las posibilidades y situaciones pueden tomar decisiones sin un núcleo-central, la cooperación con otras motas si es necesario. Para subrayar la parte menos importante del núcleo-central, en el núcleo de SCN se lo suele llamar controlador.

2.15 Nivel de infraestructura de una Red de Control del Sensor (SCN)

Sintetizando la composición de una red de nodos inalámbricos WSN, cada nodo de la red consta de un dispositivo con microcontrolador, sensores y transmisor/receptor, y forma una red con muchos otros nodos, también llamados motas o sensores. Por otra parte, un sensor es capaz de procesar una limitada cantidad de datos. Pero cuando coordinamos la información entre un importante número de nodos, éstos tienen la habilidad de medir un medio físico dado con gran detalle.

La siguiente figura ofrece una visión general de SCN y sus aplicaciones, incluyendo su relación con las NGN.

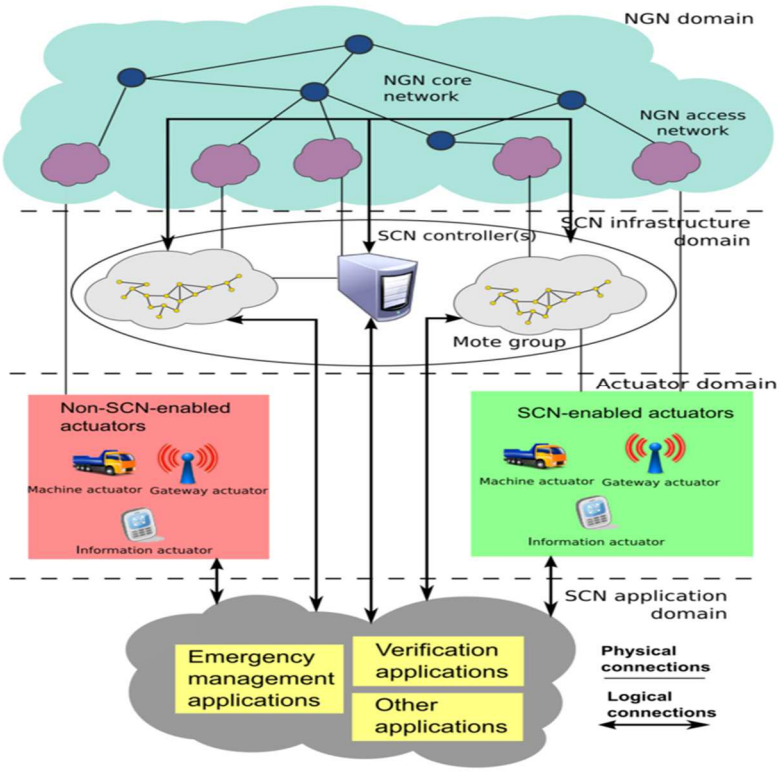

Figura 10. Panorámica de SCN y sus aplicaciones

Fuente. NGN-AWSN (2014)

Así, las redes de nodos inalámbricos comunes compuestos por una gran cantidad de sensores que están recogiendo y automáticamente los parámetros de procesamiento de mediciones físicas son el ejemplo de MOC. Por otro lado, en MOC se paga una gran atención a las preguntas que están más allá del alcance de WSN, como el trabajo con un gran número de dispositivos heterogéneos, integración con actuadores de propiedad, restringir el acceso a ciertas funciones de los dispositivos para diferentes usuarios, etc.

Internet Business Solutions Group de Cisco (IBSG) predice que unos 25 mil millones de dispositivos estarán conectados en 2017 y 50 mil millones para el año 2020. Recomendación aprobada.

La Recomendación, tiene que ver con los aspectos de red de sistemas MOC: entrega de datos, movilidad, calidad de servicio, etc., es decir, las cuestiones relacionadas con

WSN también. Es posible decir que la Recomendación Y.2061 considera los problemas que surgen con el uso de redes inalámbricas de sensores en la práctica para resolver una tarea en particular, la prestación de cooperación entre los objetos de la máquina que no necesariamente requieren la interacción humana. También, en esta Recomendación se consideran importantes casos de uso WSN, tales como e-salud, servicio de alerta, gestión caravana, casa inteligente.

En la Recomendación Y.2061 se consideran las siguientes cuestiones:

- Términos y determinaciones relacionadas con el MOC;
- Información general sobre MOC: visión general de la red, tipos de comunicaciones máquina-orientado, ecosistema MOC,
- características de MOC;
- Requisitos de servicio de aplicaciones MOC;
- Requisitos de capacidades NGN y dispositivos MOC/Gateways capacidades, que se ocupa de estos requisitos;
- Marco de referencia para las capacidades MOC;

Para que sea más fácil de entender, se analiza un caso de uso para los requisitos de servicio realizadas en cada caso, y de acuerdo con estos requisitos vamos a determinar el conjunto necesario de capacidades de dispositivos NGN y MOC.

Caso de uso 1: Monitoreo en salud

Varios tipos de dispositivos están involucrados en la provisión de servicios de salud electrónica. Algunos de estos dispositivos sólo recogen datos e interactuar con la red (por ejemplo, sensores de latidos del corazón), otros pueden interactuar bidireccionalmente (por ejemplo, cámaras), algunos dispositivos suelen generar pequeñas cantidades de datos (por ejemplo, los termómetros), mientras que otros pueden tratar con *streaming* multimedia (por ejemplo, cámaras) o, lidiar con el control de sesión de llamada (por ejemplo, terminales SIP apoyo video llamadas). Algunos dispositivos pueden incluso funcionar tanto como puerta de enlace y las plataformas de servicios en sensores similares.

Los dispositivos electrónicos de salud se reúnen datos y los envían a las partes relevantes, como el centro de la salud donde se aprecia la imagen de la figura 16..

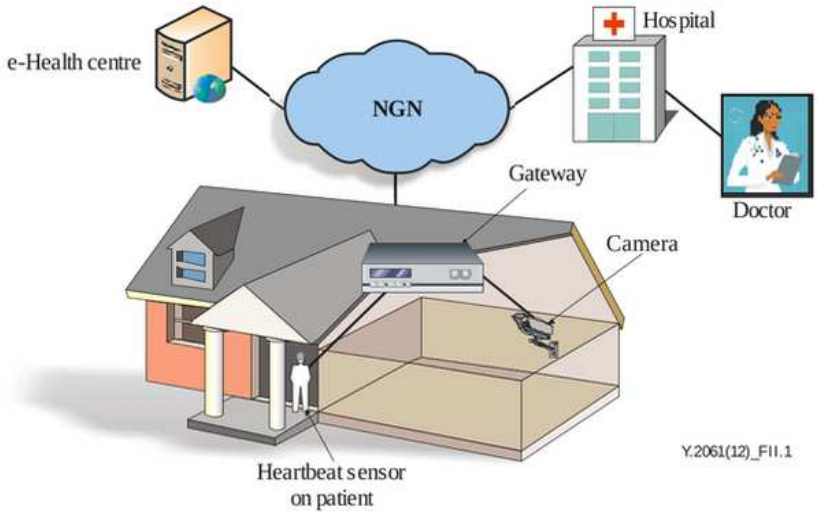

Figura 11. Configuración del servicio de vigilancia típica e-salud

Fuente. El Autor

Los hospitales, médicos y familiares pueden suscribirse al servicio para obtener los datos con procesamiento de análisis.

En la tabla 2. Se muestran los requerimientos o requisitos NGN.

Tabla 2. Requerimientos NGN

Desafíos técnicos de casos de uso	Requisitos de servicio	Requisitos NGN	Dispositivos MOC / requisitos gateways
Agrupación debe ser apoyada. Esto es útil, por ejemplo, para múltiples pacientes con el mismo tipo de enfermedad, o en el caso de un único paciente, para gestionar un conjunto de dispositivos que se pueden gestionar en modo de grupo.	1) Apoyo de la transmisión de datos a / desde uno o todos los miembros de un grupo MOC utilizando identificador de grupo. 2) Apoyar la contabilidad en línea y fuera de línea y la carga sobre la base de las agrupaciones. 3) Apoyo a la política de QoS basado grupo. 4) Apoyo de grupo MOC gestión, incluida la visualización / creación / modificación / eliminación de grupos MOC, los miembros del grupo y los atributos asociados.	1) Grupo basado mecanismos de direccionamiento de acuerdo con la política del proveedor NGN. 2) Mapa del identificador MOC grupo de direcciones de red de dispositivos MOC. 3) por grupo de políticas de QoS de nivel, en paralelo con, o en lugar de una política por QoS a nivel de dispositivos. 4) manejo optimizado de comunicaciones de grupo con el fin de ahorrar recursos de la red y para evitar la congestión de red. 5) Apoyo de la contabilidad y de carga basado en el grupo.	Se requieren gateways MOC para apoyar mapeo entre la identificación de un grupo de dispositivos de MOC y uno o direcciones de red locales MOC más para cada dispositivo MOC dentro del grupo.
Control de tráfico optimizado debe ser apoyado. Por ejemplo, los datos detectados pueden ser muy pequeñas y necesitan ser informado a la red cada hora: en tal caso, es un desperdicio de recursos para estar permanentemente conectados a la red. Además, los dispositivos de una paciente pueden permanecer en modo de reposo y despertar cuando el médico necesita diagnosticar al paciente de forma remota.	1) Mecanismos para la gestión del tráfico de aplicaciones, por ejemplo, para limitar el número máximo de transacciones de aplicaciones por segundo. 2) dispositivos MOC entrar o permanecer en el modo de suspensión con el fin de ahorrar energía (especialmente para los dispositivos que utilizan una batería) y ahorrar recursos de red (especialmente para los dispositivos con acceso a la red inalámbrica).	Permitir el acceso de los usuarios finales MOC (por ejemplo, conexión a la red o el establecimiento de una conexión de datos) durante un intervalo de tiempo de acceso a la red de comunicación concedida definido; de lo contrario rechazarla o permitir con diferentes parámetros de carga.	1) Se requieren dispositivos MOC trabajar sin conexión cuando no se requiere la transmisión de datos y luego entrar en el modo de suspensión de acuerdo con las políticas necesarias. 2) Se requieren pasarelas MOC para permitir el ajuste y la modificación de / red prohibido horarios de acceso de comunicación otorgados y duraciones.
Los diferentes niveles de movilidad deben ser apoyadas. Por ejemplo, en el caso de los pacientes con problemas de movilidad (que se mueve con poca frecuencia y no muy lejos), es un desperdicio de recursos para activar	Apoyo a la gestión de la movilidad para los diferentes niveles de movilidad con el fin de reducir el uso de recursos (por ejemplo, el temporizador de actualización periódica de ubicación debe ser reducida para los dispositivos MOC que tienen movimiento	Apoyo a la gestión diferente nivel de movilidad de acuerdo a las necesidades de movilidad de los dispositivos y gateways MOC, tales como la reducción de la frecuencia de los procedimientos de gestión de la movilidad para los dispositivos y gateways	Se requieren gateways y dispositivos MOC MOC para apoyar las capacidades mejoradas de gestión de la movilidad con el fin de apoyar a los diferentes niveles de movilidad.

capacidades de gestión de movilidad.	poco frecuente).	MOC MOC con escasa movilidad.	
Activación y gestión remota de dispositivos deben ser apoyadas. Por ejemplo, los dispositivos en modo de suspensión se despertaron sólo cuando el médico necesita diagnosticar al paciente de forma remota.	1) Apoyo de seguimiento del estado de los diversos aspectos de los dispositivos MOC y gateways incluyendo el comportamiento anormal, la información del archivo adjunto, la conectividad. 2) El apoyo de los mecanismos para llevar a cabo simple y escalable pre-aprovisionamiento de dispositivos MOC y pasarelas, habilitar y deshabilitar características, reportar errores de dispositivos, y el estado del dispositivo de la consulta.	Apoyo a la gestión y control de dispositivos y gateways MOC, incluyendo los dispositivos de monitoreo MOC y 'operaciones, cambios de monitoreo y acciones conexas, relacionadas con los puntos de conexión a la red de dispositivos y gateways MOC MOC, los dispositivos de seguimiento y gateways' gateways de conectividad de red.	1) Se requieren pasarelas MOC para actuar como un servidor proxy de gestión para dispositivos MOC de la red local MOC conectado. 2) Se requieren gateways y dispositivos MOC MOC para apoyar la gestión de configuración. 3) Se requieren pasarelas MOC para apoyar la recolección de fallos y los datos de rendimiento y almacenamiento.
Los perfiles de dispositivo deben ser apoyados. El paciente puede comprar nuevos dispositivos y conectarlos a la red de forma dinámica: la información del dispositivo correspondiente debe ser incluido en el perfil del dispositivo y se actualiza de forma dinámica para permitir la autenticación de red y el control de los dispositivos recién añadidos y también su eliminación.	El uso y la gestión de perfiles de dispositivo estándar para los dispositivos y gateways MOC, incluyendo su registro y descubrimiento. El perfil de dispositivo MOC es un conjunto de información relacionada con los dispositivos y gateways MOC MOC.	Soporte de perfiles de dispositivos estándar con mejoras para los dispositivos MOC y la información específica de la puerta de enlace.	-
Dispositivos detrás de una puerta de enlace deben ser capaces de ser identificados por la red. La puerta de enlace podría proporcionar sólo un canal portador y actuar como un agregador de datos para los dispositivos conectados a ella o podría proporcionar un control de servicio para los dispositivos conectados a ella. En el primer caso, los dispositivos	1) apoyo de los mecanismos para la gestión de las puertas de enlace actuando como agregadores de tráfico (una puerta de enlace agregados de tráfico y actúa como un canal). 2) dispositivos MOC puede comunicar con diferentes aplicaciones MOC través de una única puerta de enlace MOC o por medio de varias puertas de enlace. 3) dispositivos MOC pueden apoyar no las	-	1) Se requieren gateways MOC para apoyar el mapeo entre la identificación de un dispositivo de MOC y uno o direcciones de red locales MOC más. 2) Una puerta de enlace MOC puede utilizar opcionalmente identificadores temporales para dispositivos MOC de conexión y de desconexión a la red dinámicamente. 3) gateways MOC están obligados a identificar y autenticar las aplicaciones MOC

conectados a la puerta de entrada deben ser controlados por la red, o tanto por la red y puerta de enlace.	direcciones IP cuando se conectan a la red a través de pasarelas MOC. 4) El apoyo de un mecanismo de autenticación y autorización de los dispositivos MOC que se encuentran en una red local MOC (conectado a través de una puerta de enlace MOC).		MOC, otros dispositivos y usuarios finales MOC. 4) pasarelas MOC se recomienda para apoyar diferentes contables y métodos de carga para los dispositivos conectados MOC.
Dispositivos de propiedad deben ser apoyadas. Hay un montón de dispositivos patentados y pasarelas que se ejecutan en las redes: la adaptación a dispositivos y gateways de propiedad existentes debe ser apoyada.	1) La interoperabilidad con los dispositivos de propiedad a través de medios apropiados, por ejemplo, puertas de enlace de MOC. 2) Apoyo de la ocultación efectiva de las operaciones dispositivos patentados.	-	Gateways MOC se recomienda para apoyar la comunicación con dispositivos específicos (por ejemplo, los dispositivos con interfaces propietarias para interfuncionamiento con entidades de red).
Perfil de servicio debe ser apoyado. Los pacientes por lo general no están muy familiarizados con los servicios ofrecidos por diferentes hospitales, pueden por lo general sólo una sesión al portal y acceder a los servicios del centro de e-salud, mientras que el centro de la e-salud es generalmente conocida y puede determinar los hospitales de destino sobre la base de sus conocimientos profesionales .	El uso de perfiles de servicio estándar para el registro y el descubrimiento. El perfil de servicio de una aplicación de MOC específica está compuesta por un conjunto de información específica a esa aplicación MOC. Puede incluir, pero no se limitan a, el identificador de aplicación MOC, identificador de proveedor de aplicaciones MOC y tipos de datos de la aplicación.	Soporte de perfiles de servicio estándar con mejoras para información específica aplicaciones MOC.	-

Fuente. El Autor

Caso de uso 2: Servicio de alerta de Tsunami

El sistema de alerta de tsunami se utiliza para detectar tsunamis y emitir alertas para evitar la pérdida de vidas y bienes.

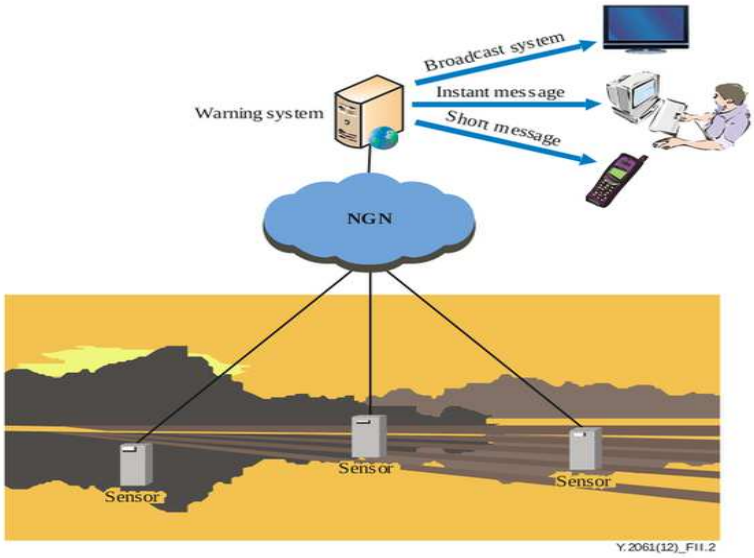

Figura 12. Tsunami típica configuración del servicio de alerta

Fuente. El Autor

Como se muestra en la figura 17, se compone de dos componentes igualmente importantes: una red de sensores para detectar tsunamis y una infraestructura de comunicaciones para emitir alarmas oportunas para ayudar a la evacuación de las zonas costeras. La detección y predicción de tsunamis es sólo la mitad del trabajo del sistema. La otra igual importancia es la capacidad de advertir a la población de las zonas que se verán afectadas. Para salvar vidas con mayor certeza, una orientación adecuada para el escape de acuerdo con su situación en peligro (por ejemplo, tiempo, lugar y ocasión) debe ser considerada. Para un visitante que se acerca a una zona desconocida por la noche, una alarma simple no es suficiente para escapar a un lugar seguro. Todos los sistemas de alerta contra los tsunamis tienen varias líneas de comunicaciones (como

SMS, correo electrónico, fax, radio, texto y télex, a menudo utilizando sistemas dedicados endurecidos) que permite los mensajes de emergencia para ser enviado a los servicios de emergencia y las fuerzas armadas, así como a la población sistemas de alerta (por ejemplo, sirenas).

Tabla 3. Requerimientos para un sistema de alerta ciudadana

Desafíos técnicos de casos de uso	**Requisitos de servicio**	**Requisitos NGN**	**Dispositivos MOC / requisitos gateways**
Agrupación debe ser apoyada. Esto es útil, por ejemplo, para múltiples pacientes con el mismo tipo de enfermedad, o en el caso de un único paciente, para gestionar un conjunto de dispositivos que se pueden gestionar en modo de grupo.	1) El apoyo de los mecanismos de la red y capacidades MOC en el dominio de las NGN para equilibrar la carga. 2) La robustez de la red y las capacidades de MOC en el dominio de las NGN, al tiempo que garantizan un nivel suficiente de calidad de servicio en determinadas circunstancias, por ejemplo, situaciones de emergencia.	-	-
Entrega priorizada de información de emergencia, es decir, el mensaje de emergencia para un terremoto, se debe priorizar en comparación con otros mensajes de servicio.	1) Capacidad para establecer el orden de prioridad de los datos (en una sola aplicación o entre diferentes aplicaciones). 2) Capacidad de gestión de datos diferentes en función de su priorización. 3) Capacidad para transmitir inmediatamente los datos de alta prioridad que se recogen en las aplicaciones sensibles al rendimiento de la red.	1) Capacidad para identificar los datos de acuerdo a las categorías pertinentes. 2) Capacidad para aplicar diferentes de manejo de datos (por ejemplo, el almacenamiento en caché y / o reenviar) basado en la identificación de datos.	1) Se recomiendan gateways y dispositivos MOC MOC para apoyar el establecimiento de prioridades de aplicación. 2) Se requieren gateways y dispositivos MOC MOC para apoyar QoS la diferenciación de acuerdo a diferentes categorías de tráfico.

Fuente. El Autor

Caso de uso 3: Gestión Vehicular

La figura 18 muestra una configuración típica de servicio para la gestión de la caravana vehicular.

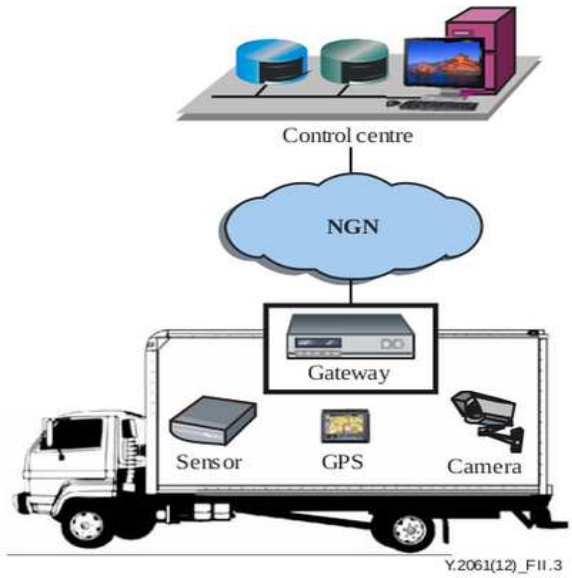

Figura 13. Caravana típica configuración del servicio de gestión

Fuente. El Autor

Cada autobús/camión está equipado con dispositivos y gateways que tienen las mismas características. El centro de control recoge datos relacionados con la ubicación, velocidad y la situación dada de los sensores, sistema de posicionamiento global terminales (GPS) y cámaras del bus. Los datos agregados a través de una pasarela ubicada en el bus se transmiten a la NGN mediante la conexión inalámbrica.

El calendario dinámico se puede remitir a la pantalla del monitor en la parada del autobús por el centro de control de acuerdo con la información de ubicación de recogida del autobús.

Cuando un sensor en el bus detecta una situación anormal, tales como el olor de la gasolina, una indicación de alarma se envía al centro de control.

El autobús siempre tiene una ruta fija que significa que no debe salir de los caminos predefinidos. Cuando un autobús se mueve fuera de un área en particular, una aplicación debe ser activada. Por ejemplo, una llamada puede hacerse que el conductor del autobús, o una indicación de alerta puede ser hecha al administrador del autobús mientras el autobús se mueve fuera de la zona.

Tabla 4. Requerimientos para un sistema de monitoreo vehicular

Desafíos técnicos de casos de uso	**Requisitos de servicio**	**Requisitos NGN**	**Dispositivos MOC / requisitos gateways**
Lugar servicio basado en: una aplicación debe ser activado cuando los dispositivos están dentro o fuera de un área en particular;	1) El conocimiento de la ubicación de los dispositivos MOC. 2) El mantenimiento y la gestión de los diferentes tipos de información sobre la ubicación de los dos un solo dispositivo MOC y un conjunto de dispositivos MOC MOC detrás de una puerta de enlace. Capacidad de gestión que determina la ubicación y la información de los informes acerca de la ubicación de los usuarios y los dispositivos de la NGN.	-	
Nivel de servicio priorizado, por ejemplo, la indicación de alarma se debe priorizar en comparación con otros datos.	*Consulte "entrega priorizada de información de emergencia" en caso de uso 2*	*Consulte "entrega priorizada de información de emergencia" en caso de uso 2*	*Consulte "entrega priorizada de información de emergencia" en caso de uso 2*
La Dirección del Grupo para los dispositivos con las mismas características.	*Consulte "Agrupación" en caso de uso 1*	*Consulte "Agrupación" en caso de uso 1*	*Consulte "Agrupación" en caso de uso 1*

Fuente. El Autor

Caso de uso 4: casa inteligente

Casa inteligente implica generalmente una mezcla de diferentes dispositivos y aplicaciones, como en tiempo real o sensores en tiempo real cerca, notificación de corte de suministro eléctrico y de control de la calidad de energía.

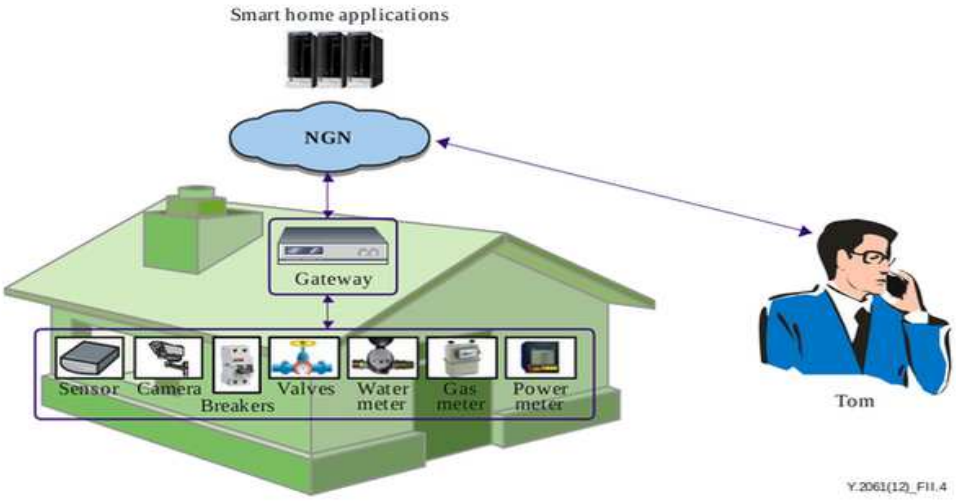

Figura 14. Configuración del servicio de hogar inteligente típico

Fuente. El Autor

Como se muestra en la Figura 19, un escenario de "casa inteligente" a menudo se refiere a los dispositivos (por ejemplo, sensor de humo, contadores de electricidad, contadores de gas, etc.) que están conectados a una plataforma de aplicaciones de casa inteligente a través de una puerta de acceso situada en la casa inteligente. El centro de datos recoge los datos de los dispositivos de "casa inteligente" y es capaz de controlar estos dispositivos de forma remota a través de la puerta de enlace.

En este escenario, la información de la casa de Tom relacionada con el poder, el gas y el consumo de agua puede ser recogida y comunicados a la plataforma inteligente aplicaciones domésticas. Al mismo tiempo, Tom puede gestionar la aplicación

relacionada con las políticas de su casa usando las aplicaciones inteligentes para el hogar y la política relacionada con la solicitud se puede enviar a los dispositivos MOC con el fin de ser ejecutados de acuerdo a los requerimientos de Tom.

Se considera ahora que Tom está fuera de su casa, mientras que se produce un incendio en la cocina de su casa donde su hijo se está cocinando. Cuando la detección de este evento, el dispositivo MOC (es decir, el sensor de humos) envía un mensaje de alarma a Tom directamente.

Al recibir esta información, Tom inicia una comunicación de vídeo con la cámara para comprobar el estado de la cocina, y para decirle a su hijo cómo utilizar el extintor de incendios o para salir. Por razones de seguridad y privacidad, la cámara sólo está conectado y controlado por miembros de la familia de Tom.

Tabla 4. Requerimientos de monitoreo en el hogar

Desafíos técnicos de casos de uso	**Requisitos de servicio**	**Requisitos NGN**	**Dispositivos MOC / requisitos gateways**
Capacidades de vídeo mejoradas de audio basado, como streaming de vídeo concurrente y local breakout.	Prevención de la concentración de acceso en un único recurso cuando QoS se ve afectado por el tráfico de alta solicitud.	Apoyar a las siguientes políticas de calidad de servicio y parámetros de tráfico correspondientes: retardo de paquetes de transferencia, variación del retardo de paquetes, la relación de pérdida de paquetes, la relación de error de paquete.	-
La Dirección del Grupo para dispositivos MOC con las mismas características, por ejemplo, medidores de potencia en diferentes casas inteligentes.	*Consulte "Agrupación" en caso de uso 1*	*Consulte "Agrupación" en caso de uso 1*	*Consulte "Agrupación" en caso de uso 1*

Difusión de mensajes y la multidifusión basándose en las características específicas, como grupo y ubicación, para apoyar funciones tales como la actualización del firmware.	-	Apoyo de la radiodifusión y multidifusión para grupos MOC (con dispositivos MOC y gateways conectados directa o indirectamente a las NGN).	Se requieren gateways MOC para apoyar la radiodifusión y multidifusión.

Fuente. El Autor

Capítulo 3. Metodología de Migración NGN para Central-Milagro-CNT

La siguiente metodología es un procedimiento para la migración a NGN en la central de Milagro. Se debe tener un contrato previamente, a continuación se muestra una metodología de descongestión, ideal para migración a red NGN:

1. Alcance

2. Impacto

3. Equipos involucrados (HW /SW)

3. Fecha y hora programada

3.1 Duración y Resumen de Actividades

4. Procedimiento implantación

5. Matriz de Pruebas / Validaciones

6. Rollback:

7. Responsables y Requerimientos

7.1. Responsables.

7.2 Requerimientos

3.1 Modelo de metodología de descongestión

Se describe, un modelo de los 7 pasos mencionados para una descongestión técnica basado en estándares de ITU, recomendado para la Central-Milagro CNT en la provincia del Guayas.

Alcance del proyecto

El Nodo de Próxima Generación de la Central CNT-Milagro, adquirido bajo el contrato (se especificará la identificación/numeración), suscrito con la empresa (por ejemplo: ALCATEL LUCENT/HUAWEI), se encuentra instalado y se han realizado las Pruebas de aceptación de todo el equipamiento (Banda Ancha y Banda Angosta), por lo que es procedente realizar la migración de los abonado de este Nodo que remplazara al MSAN de Tecnología Huawei.

Impacto

Conforme se indica en el numeral. 2.2, de la Migración de Centrales, Nodos y o plataformas sin participación de un Proveedor del procedimiento para migración de Centrales, Nodos y/o plataformas vigentes, que en la parte pertinente indica que la Gerencia de Ingeniería se encargará de la coordinación entre todas las áreas de la CNT E.P.: Gerencia regional del Guayas y Pichincha, Ingeniería, Implementación, Gestión de red y servicio O&M Core y Plataformas Fijas, Transmisión, accesos, soluciones de Internet datos e IPTV, TI, aseguramiento de ingresos, regulación e interconexión, comercial, energía.

Equipo involucrado

El Nodo de Próxima Generación adquirido es de tecnología ALCATEL/HUAWEI, se trata de un equipamiento tipo INDOOR conformado por 1 MSAN en Central-Milagro la capacidad adquirida se indica a continuación:

La migración se refiere al NODO MSAN ALCATEL que reemplazará al MSAN HUAWEI La Central-Milagro, los equipamientos se encuentran instalados en el local de

Central-Milagro, provincia del Guayas de la Corporación Nacional de Telecomunicaciones CNT E.P.

Fecha Propuesta para la Migración:

(Definir fecha y hora de inicio y finalización)

Responsabilidades de cada Área:

Gerencia Provincial del Guayas y Pichincha

Procedimientos

El Sistema 1.- GYE, informa que los ATPs del MSAN Alcatel de Central-Milagro, fueron Ejecutados el 2uao5t14 posterior fueron solicitados al área de la NGN GYE que envíen dichos CDRs a validación con fecha (definir). El área de Aseguramiento de ingresos informa que los CDRs fueron validados con fecha (definir)

Responsables: lng (designado),/ lng (designado),

El área de Gestión de la Red - GYE indica que el registro del equipo a la SENATEL se Encuentra realizado y la ampliación de la serie numérica.

Responsables: lng. Xavier Macías:

El área de XDSL solicitara al área de Gestión de la Red el día (fecha), se suba la infraestructura a los sistemas open del DSLAM y MSAN Alcatel.

Responsables: lng (designado),

El Sistema 1 - GYE, informará el día (fecha), la serie configurada a nivel del MSAN HUAWEI, el puerto donde se conecta a la MPLS, y su Ancho de Banda (FE/GE). Esta

información se enviara a las áreas de Activación de servicios GYE, e ingeniería. Serie numérica actual 042639000 - 042639191, serie numérica futura 042639000

042639999 - 042638000 _ 042638099.

Responsables: lng (designado),

El sistema 'l - GYE, en conjunto con el área de Telefonía pública - GYE, validaran los números que tienen inversión de polaridad y enviaran el día (fecha) dicha información al área de ingeniería y Activación de servicios GYE.

Responsables: (Ing. Designado) / (Ing. Designado)

Será tramitada por parte de ingeniería (lng (designado), una ventana de mantenimiento por los clientes de datos del MSAN Huawei con el área de Soluciones internet Datos y TV Hasta el día (fecha).

Responsables. Lng. (desigandos)

La Jefatura del Sistema 1 - GYE, informará el día (fecha) a las áreas de Gestión de la Red, Negocios, Comercial, Operaciones y Tl que a partir del día (fecha)

Hasta el día (fecha) se paralicen todas las gestiones relacionadas con los clientes del MSAN Huawei de la Central-Milagro

Responsable: lng. Freddy Potes / lng. Xavier Macías.

El día (fecha), el área de Activación de Servicios-GYE (lng (designado), obtendrá la pre-data del listado definitivo de los abonados del MSAN HUÁWEI de la Central-Milagro enviara a la Jefatura de la Zona Accesos (lng (designado), - GYE) y al lng (designado), para la depuración de tos datos, una vez que sea confirmada la información

hasta el día (fecha) por parte de la Jefatura de la Zona de Accesos -GYE, el área de Activación de Servicios - GYE enviara al área de ingeniería la data final (fecha).

El Área de Activación de Servicios - GYE enviara el día (fecha) al área de ingeniería la

Macro (SCRIPT) que se ejecutara para la migración.

Responsable: lng (designado), / lng (designado), /lng (designado).

El sistema 1 - GYE ingresara y comunicará a través del sistema SARl el servicio (3 horas). Fecha limite (especificarlo).

Responsables: lng (designado), lng (designado), lng (designado),

Interrupción del Nivel 1, 2 y 3

El día (fecha) el Sistema 1-GYE en coordinación con NGN-GYE verificará las rutas de tos números de emergencia del MSAN Huawei Central Milagro y enviara dicha información al área de ingeniería (lng (designado) para qué emita la-OT respectiva a ser configurada posterior en la NGN.

Responsable. lng (designado), / lng (designado),

Personal de Operaciones de la Zona de Accesos del Guayas realizará las conexiones en paralelo desde las líneas de planta externa, al MDF ALCATEL nuevo, así como las cruzadas en el nuevo MDF. Se realizara el timbrado de los LENS de planta interna y timbrado de planta externa (distribuidor, botellón), las mismas finalizaran (determinar fecha) para la migración del MSAN Alcatel/Huawei en la Central-Milagro.

También delegados de las áreas de Planta Externa, ADSL, supervisaran en sitio y el NOC

(022802533) en forma remota las cruzadas de las migraciones de los clientes corporativos y residenciales elite de acuerdo al listado obtenido por la CNT.E.P.

Responsable: lng. (designado).

Matriz de prueba

Verificar que se encuentren configurados los TID en la totalidad de puertos del equipamiento MSAN Alcatel hasta el Viernes 18tWayot2}12, de no tener activados se debe solicitar al sistema 1 - GYE configure los TID en las tarjetas de servicio.

Responsables: lng. (designado)

A la migración, el Sistema 1 - GYE, informara por correo que la serie telefónica del MSAN Huawei de Central-Milagro, fue migrado a un MSAN Alcatel y seguirán grabando CDRs a las áreas, Tl (SlS DATA CENTER GYE, SIS MEDIACION, AIN Ing. 1, AIN Ing.2, AIN Ing. 3) para que conozcan la fecha de generación de CDR con el nuevo equipo Alcatel, incluido llamadas locales.

Responsables: lng (designado),

El área de Activación de Servicios-GYE, el domingo 20 de mayo a las 23H5g ejecutara la macro para la migración en la gestión de la NGN.

Responsable: lng (designado),

Se aclara que la serie numérica no cambia. El área de Gestión de la Red y Servicios comunicará la serie de la ampliación.

La serie de ampliación se ingresará al sistema Open el (fecha) luego de la migración del MSAN de abonados.

Responsable: lng (designado), / seguimiento lng (designado),

Rollback

El día (fecha y hora) al área de Gestión de la Red-GYE enviara la orden de trabajo respectiva a las centrales Transito, Tandem, COMAG´s y a nivel nacional, para la ampliación de la serie telefónica del MSAN Central-Milagro, de la Prov. Del Guayas.

Responsable: lng (designado), / lng (designado),

Responsables

El área de Gestión de la Red y Servicios el día (fecha y hora) ingresará al sistema OPEN, para cortes y reconexiones automáticas de los abonados del MSAN ALCATEL Central-Milagro, en la forma ATMCPL. Este cambio él área de Gestión de la Red y servicio informara a las áreas de Activación de servicios GYE.

Responsable: lng. lng (designado),

Personal del Área de Sistema 1 retirará el MDF actual una vez que se haya realizado el corte de servicio a los clientes.

Responsables: lng (designado),

3.2 Activación de Servicios

El área de Activación de servicios de GYE realizará los cortes y reconexiones automáticas para los abonados del MSAN Alcatel Central-Milagro además las actividades de servicios restantes, así como la creación de nuevos números, se realizará desde el día (fecha).

Responsables: lng (designado).

Transmisión

Integración a la red IP-MPLS:

El día (fecha programada), se verificara y confirmara que las redes del MSAN

Alcatel de Central-Milagro, tengan conexión hacia la red MPLS de la Zona Ex Andina y con todas las redes de la CNT. Se remitirá un correo a lng (designado), de UIO por parte de ingeniería.

Responsable. lng (designado), / lng (designado),

Energía

El MSAN HUAWEI de Central-Milagro permanecerá en funcionamiento durante el periodo de un día luego OL la migración, para la migración únicamente se desconectarán las tarjetas de abonados. Luego de este periodo, se desconectará la energía del MSAN HUAWEI cuidando que el corte de energía no afecte a los otros servicios en funcionamiento en el local y otros equipos

Responsables: lng (designado),

3.3 Varios

Para la migración debe estar presente el personal-técnico de la CNT E'P' de los sistemas de Core & plataformas, Transmisión, Accesos, ADSL, Energía de la Prov. del Guayas

El (fecha programada) el área de ingeniería emitirá la OT respectiva para proceder con la migración del (fecha) para clientes POTS, para los clientes

ADSL se remitirá la OT (fecha programada).

Responsables: lng (designado)/ lng (designado),

Si existiese algún inconveniente con el funcionamiento del MSAN Alcatel el sistema 1-GYE deberá solicitar la asistencia técnica de O&M Core y Plataformas Fijas y soporte de

Alcatel según contrato (especificar)

Responsables: lng (designado),

Esta metodología más la base practica del personal técnico de milagro, podrán culminar con éxito la migración a NGN, se espera que los muy pronto sean beneficiados con contenidos de calidad en los servicios de voz, datos,l todos los ciudadanos y ciudadanas de Milagro.

CONCLUSIONES

De acuerdo con la UIT-T, NGN es una red basada en paquetes capaz de proporcionar servicios de telecomunicaciones a los usuarios y poder hacer uso de múltiples banda ancha, QoS habilitado para las tecnologías de transporte y en la que las funciones relacionadas con el servicio son independientes de las tecnologías subyacentes relacionadas con el transporte.

La sustitución de TDM por NGN basadas en IP debe ser planificada, implementar plataformas IP/ MPLS que llevan el tráfico tanto para los negocios fijos y móviles.

El ahorro de inversión inducidos por NGN sólo son eficaces para la implementación inicial sin red preexistente.

Las redes NGN próximos, tanto en telefonía fija y entorno inalámbrico, será capaz de proporcionar mucho más potentes servicios que la regular, voz relacionada servicio. Ellos proveerán siempre-en, relativamente alto ancho de banda y de paquetes basada en conexión que permite un ancho variedad de servicios convergentes.

Hoy en día, la mayoría de los servicios están estrechamente unida con una determinada red de transporte y protocolo de señalización, por lo que la regulación ha sido aplicado principalmente en dirección vertical (por ejemplo, reglamento para el servicio siempre se aplica también a la red de transportes).

NGN está anclada en torno al principio de una red (All-IP) para el transporte de todos los servicios (voz, datos y video).

RECOMENDACIONES

Se recomienda que la empresa CNT y en especial la central en Milagro. Logre también integrar la señal de televisión pagada a una sola red NGN

Se recomienda adquirir un software de gestión de red profesional para supervisar la calidad del servicio.

Se recomienda implementar procedimientos de seguridad informática, por cuanto el protocolo IP, es susceptible a ataques informáticos, y las organizaciones y empresas no están libre de ataque a sus redes.

Es recomendable certificarse en gestión de seguridad de información y datos, alcanzar un ISO 27000 u otro estándar de seguridad internacional.

Se debe capacitar a los técnicos de la CNT-Milagro en configuraciones y aplicaciones de sensores y actuadores de una red de nodos bajo NGN.

Se debe cumplir planes de mantenimiento a la plataforma NGN.

Potencia en el área de marketing la calidad y cantidad de contenidos multimedias, que solo se puede lograr con redes de nueva generación.

BIBLIOGRAFÍA

CANTV (2009) Nuevas Plataformas y servicios de Red Recuperado de: http://www.scribd.com/doc/89810407/NGN-Solutions-Huawei-Technologies#scribd

Cortez (2010) Propuesta de mejora de la red de transporte CANTV en el estado anzoátegui del tramo comprendido entre las poblaciones el Alambre –Clarines – Puerto Píritu. Recuperado de: http://ri.bib.udo.edu.ve/bitstream/123456789/3130/1/18-TESIS.IE010C24.pdf

Huawei. Transformación de la red fija - Un imperativo para NGN, Portal. Recuperado de: http://www.huawei.com/en/about-huawei/publications/communicate/hw-081685.htm

Keymile (2008) Sistemas de Telecomunicaciones. Redes NGN. Recuperado de: http://www.railway-technology.com/contractors/signal/keymile/presskeymile-presents-new-generation-of-linerunner-scada-ng.html

Unión Internacional de Telecomunicaciones (2014) Redes de Próxima Generación. Serie Y.200 0: Documento Técnico.

GLOSARIO

Circuit switching (conmutación de circuitos). Técnica de comunicación en la que se establece un canal (o circuito dedicado) durante toda la duración de la comunicación. La red de conmutación de circuitos más ubicua es la red telefónica, que asigna recursos de comunicaciones (sean segmentos de cable, ranuras de tiempo o frecuencias) dedicados para cada llamada telefónica.

Codec (codec). Algoritmo software usado para comprimir/ descomprimir señales de voz o audio. Se caracterizan por varios parámetros como la cantidad de bits, el tamaño de la trama (frame), los retardos de proceso, etc. Algunos ejemplos de codecs típicos son G.711, G.723.1, G.729 o G.726.

Dirección IP: Las direcciones IP son el método mediante el cual se identifican los computadores individuales (o, en una interpretación más estricta, las interfaces de red de dichos computadores) dentro de un red TCP/IP. Todas las direcciones IP consisten en cuatro números separados por puntos, donde cada número está entre 0 y 255.

Framework: (plataforma, entorno, marco de trabajo). Desde el punto de vista del desarrollo de software, un framework es una estructura de soporte definida, en la cual otro proyecto de software puede ser organizado y desarrollado.

Gatekeeper (portero). Entidad de red H.323 que proporciona traducción de direcciones y controla el acceso a la red de los terminales, pasarelas y MCU´s H.323. Puede proporcionar otros servicios como la localización de pasarelas.

Gateway (pasarela). Dispositivo empleado para conectar redes que usan diferentes protocolos de comunicación de forma que la información puede pasar de una a otra. En

VoIP existen dos tipos principales de pasarelas: la Pasarela de Medios (Media Gateways), para la conversión de datos (voz), y la Pasarela de Señalización (Signalling Gateway), para convertir información de señalización.

NOC (Network Operation Center): Representa al centro de operaciones en el cual se realiza el monitoreo y resolución de fallas en una red de servicios.

Packet switching (conmutación de paquetes). Técnica de conmutación en la cual los mensajes se dividen en paquetes antes de su envío. A continuación, cada paquete se transmite de forma individual y puede incluso seguir rutas diferentes hasta su destino. Una vez que los paquetes llegan a éste se agrupan para reconstruir el mensaje original.

Real Time Streaming Protocol (RTSP) Es un control de la red de protocolo diseñado para su uso en sistemas de entretenimiento y comunicaciones para controlar la transmisión de medios servidores . El protocolo se utiliza para establecer y controlar sesiones de medios entre los puntos finales. Los clientes del tema servidores de medios VCR -estilo comandos, como juego y pausa, para facilitar el control en tiempo real de la reproducción de archivos multimedia desde el servidor.

SNMP (Simple Network Management Protocol): Protocolo que se encarga del direccionamiento de red, se utiliza para grandes redes.

Softswitch (conmutación por software). Programa que realiza las funciones de un conmutador telefónico y sustituye a éste al emular muchas de sus funciones de dirigir el tráfico de voz, pero además añade la flexibilidad y las prestaciones propias del tráfico de paquetes.