ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO DE UN SISTEMA CENTRALIZADO DE AUTENTICACIÓN, AUTORIZACIÓN Y ACCOUNTING (AAA) QUE FACILITE LA PROVISIÓN DE POLÍTICAS DE CALIDAD PARA LOS SERVICIOS DE BANDA ANCHA DE LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES E. P.

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

PAMELA KARINA FERNÁNDEZ MEJÍA

pfernandezmejia@hotmail.com

DIRECTOR: Ing. JOSÉ ADRIÁN ZAMBRANO MIRANDA

jose.zambrano@epn.edu.ec

CODIRECTOR: Ing. XAVIER ALEXANDER CALDERÓN HINOJOSA MSc.

xavier.calderon@epn.edu.ec

Quito, Mayo 2014

DECLARACIÓN

Yo, Pamela Karina Fernández Mejía, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Pamela Karina Fernández Mejía

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Pamela Karina Fernández Mejía, bajo mi supervisión.

Ing. Adrián Zambrano
DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

A Dios por su protección y bendiciones durante la realización de este proyecto.

A mi director por su apoyo y guía a lo largo del desarrollo de este proyecto orientándolo hacia una exitosa culminación.

A todo el personal de la Corporación Nacional de Telecomunicaciones CNT E.P. por darme las facilidades necesarias para ejecutar este proyecto, de manera muy particular a Ing. Jairo Suntaxi y personal que conforma el área de Gestión ATM/IP-MPLS.

A mis queridos amigos y amigas, quienes estuvieron junto a mí durante todo el camino recorrido tanto en momentos difíciles como en los felices, y con quienes seguramente seguiré compartiendo muchas vivencias más.

Pamela.

DEDICATORIA

A mis padres por guiar mi camino y brindarme su apoyo incondicional en todo momento lo cual ha permitido alcance cada uno de mis sueños y metas.

A mi hermano por su cariño y los ánimos brindados.

A mi mamita que ahora me protege desde el cielo.

A Darwin y Nicolás por alentarme y motivarme a alcanzar mis metas.

Pamela.

CONTENIDO

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

ÍNDICE DE TABLAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

RESUMEN

El presente proyecto trata acerca de un estudio para la implementación de un sistema AAA (Autenticación, Autorización y Contabilidad) centralizado para la Corporación Nacional de Telecomunicaciones E. P. (CNT), mismo que facilite la configuración y provisión de servicios de banda ancha de manera independiente a la tecnología de acceso y con la aplicación de políticas de calidad de servicio para una correcta administración de los recursos de red.

En el Capítulo 1 se realiza una descripción teórica de una arquitectura de red inteligente. En forma general, los temas comprendidos dentro del capítulo son: conceptos generales sobre una red de banda ancha, una red inteligente, arquitectura de un sistema AAA, protocolos AAA y calidad de servicio.

En el Capítulo 2 se realiza una descripción de los equipos y procesos que forman parte de la infraestructura actual y que permiten la provisión de servicios de banda ancha dentro de la empresa.

En el Capítulo 3 se realiza la descripción de una solución para el sistema AAA centralizado enfocada en un análisis de funcionalidades, requerimientos del sistema y el planteamiento de una solución.

En el Capítulo 4 se realiza la descripción de un plan de acción para la implementación de la solución AAA. Se presentan alternativas de solución que cumplan con los requerimientos de la empresa y un manual que facilite la capacitación del personal, el mantenimiento de equipos y la implementación del sistema AAA centralizado.

En el Capítulo 5 se realiza una propuesta de un plan de mejora para la solución el cual brinde una guía al personal del área para optimizar y reformar el sistema centralizado AAA en caso de requerirlo. Este plan se desarrollará en base a la etapa de gestión de la continuidad de servicios correspondiente a la fase de

diseño y a las etapas de gestión de eventos y gestión de incidentes orientado en la fase de operación de ITIL v3.

En el Capítulo 6 se presentan un conjunto de conclusiones y recomendaciones derivadas de la realización del proyecto propuesto.

PRESENTACIÓN

El desarrollo de las tecnologías de información y comunicación en los últimos años ha tenido una fuerte repercusión a nivel de la economía y la sociedad, acentuando la brecha digital de los países principalmente los del tercer mundo. Esto provoca que los gobiernos implementen diversos planes para tratar de disminuirla. En nuestro país se ejecuta a nivel nacional el Plan Nacional de Conectividad (PNC) promulgado en el 2007, con el cual se trata de expandir y fomentar la accesibilidad a los servicios de telecomunicaciones.

Para cumplir con los objetivos detallados en el PNC para la provisión de servicios de Internet, la Corporación Nacional de Telecomunicaciones CNT E.P. debe disponer de una infraestructura adecuada que facilite la configuración y provisión de servicios de banda ancha de manera independiente a la tecnología de acceso con la implementación de políticas de calidad de servicio. Por tal motivo, la empresa ha decidido emplear un sistema AAA centralizado el cual integre a los servidores de acceso remoto de banda ancha (BRAS) que permiten la comunicación de la red *backbone* con la red de acceso de la empresa y la plataforma de tarificación mediante la cual se efectúa el cobro del consumo de un servicio por parte de un cliente.

En base a lo expuesto anteriormente se presenta este proyecto mediante el cual se describe una arquitectura de red de banda ancha inteligente con la que se pretende facilitar la operación, administración y diferenciación de servicios de valor agregado de banda ancha, además de permitir el auto-aprovisionamiento del usuario en el sistema AAA mediante el uso de portales.

CAPÍTULO 1

MARCO TEÓRICO

1.1 INTRODUCCIÓN

En la actualidad el desarrollo de servicios de datos de banda ancha han provocado que los operadores de telecomunicaciones integren los servicios de línea fija, móvil y datos en su red para de esta manera brindar soluciones integrales a los clientes, lo que a su vez ha creado un mercado competitivo entre los diversos operadores de telecomunicaciones.

En este capítulo se realizará una descripción teórica de los equipos, protocolos y estándares que permiten la implementación de una arquitectura de red inteligente.

1.2 CONCEPTOS GENERALES [1]

A continuación se expondrán algunos conceptos generales que permitirán comprender de mejor manera una red de banda ancha inteligente y sus servicios.

1.2.1 RED DE BANDA ANCHA

Una red de banda ancha es capaz de proveer el transporte de grandes cantidades de información (ancho de banda) en periodos de tiempo reducidos (velocidad de transmisión). Ofrecen también conexiones permanentes y servicios a los usuarios.

Existen ciertos conceptos que están interrelacionados con esta definición, estos son:

- *Red:* es un conjunto de elementos interconectados entre sí a través de un medio físico y que mediante su interacción permiten compartir recursos y/o información, satisfaciendo así las necesidades de los usuarios.
- *Velocidad de transmisión:* es una medida de la cantidad de información que la red es capaz de absorber por unidad de tiempo.

- *Ancho de banda:* es una medida de capacidad e indica la cantidad de información que la red soporta durante un periodo de tiempo determinado.
- *Integración:* es la variedad de servicios y/o aplicaciones soportadas sobre un mismo medio de transporte.
- *Interoperabilidad:* permite que los diferentes elementos de la red puedan interactuar entre sí mediante el uso de protocolos de comunicación estándar. Por lo general, la forma en la información que se transmite y las características de los equipos puede ser conocida o desconocida por el usuario.

1.2.2 COMPONENTES DE UNA RED

Una red de telecomunicaciones se encuentra conformada por tres niveles funcionales: proveedores, sistema de transporte y usuarios, tal como se muestra en la Figura 1.1.

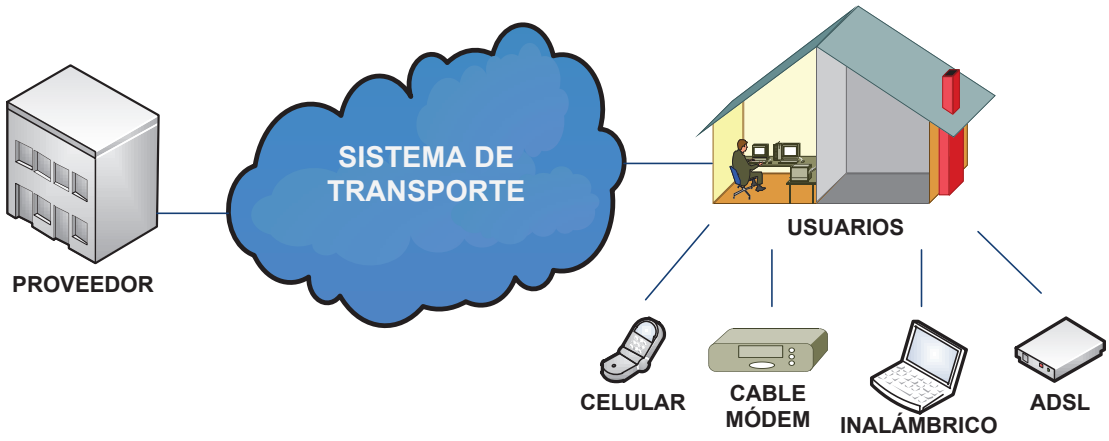


Figura 1.1. Componentes de una red[1]

1.2.2.1 Proveedor

El proveedor es el encargado de generar contenidos o información y entregarlos al sistema de transporte para transmitirlos en tiempo real o almacenarlos en una base de datos.

[1] Basado en [1]

1.2.2.2 Sistema de Transporte

Se encuentra conformado por elementos que permiten enviar y recibir información por parte del usuario. Se las puede dividir de manera jerárquica en:

1.2.2.2.1 Red de Núcleo

Una red de núcleo o *backbone* permite la comunicación de diferentes redes entre sí, es decir, cursan tráfico entre los puntos de acceso a la red de transporte. Este tipo de redes deben soportar varios servicios y aplicaciones, lo que hace que características como velocidad, transparencia de protocolos y escalabilidad sean importantes.

1.2.2.2.2 Red de Transporte

Este tipo de redes permite el transporte de grandes cantidades de información, es por esto que son redes de alta capacidad, disponibilidad y fiabilidad. Contiene los sistemas de transmisión e interconexión entre los distintos elementos de red que puede ser compartida por distintos tipos de servicios, en donde el tráfico que cursan es totalmente transparente para éstas.

1.2.2.2.3 Red de Acceso

Una red de acceso se encuentra constituida por protocolos e infraestructuras que permiten la comunicación entre el usuario y la red. En general, se pueden considerar las siguientes formas de acceso a la red en función del medio de conexión:

- *Red de acceso vía cobre:* emplean los pares trenzados de cobre que conforman las redes telefónicas.
- *Red de acceso vía radio:* emplean el espectro radioeléctrico para transmitir y recibir información. Permiten que usuarios ubicados en áreas de difícil cobertura para otros medios accedan a los diversos servicios de la red, entre estas se tienen redes celulares, inalámbricas y satelitales.

- *Redes de acceso vía fibra óptica:* emplean diversas longitudes de onda para transmitir y recibir información. Permiten que el usuario tengan un gran ancho de banda para una transmisión segura, libre de errores y a altas velocidades.
- *Redes híbridas fibra-coaxial (HFC):* son redes que emplean la infraestructura de la televisión por cable. Transportan la señal por medio de la fibra óptica para cubrir así grandes distancias, y usan el cable coaxial para la distribución a los usuarios, por ejemplo cable-módem.

1.2.2.3 Usuario

Se considera el elemento final de la red, es una estación de trabajo mediante la cual el usuario accede a los recursos y servicios de la red.

1.3 EVOLUCIÓN HACIA UNA RED INTELIGENTE

Internet es una combinación de hardware y software que permite interconectar diferentes equipos o tecnologías de red. Soporta aplicaciones como correo electrónico y *web browsing*, aunque en los últimos años aplicaciones como telefonía IP y conferencia multimedia han incrementado su número de usuarios.

Los proveedores de servicio de Internet (ISP, *Internet Service Provider*) han debido modificar la infraestructura de red y su administración para brindar calidad de servicio sobre Internet para de esta manera satisfacer las necesidades de un mercado creciente de usuarios que requieren servicios de valor añadido.

El crecimiento de sistemas móviles con usuarios que emplean diversas aplicaciones y acceden al Internet y sus servicios al igual que un usuario fijo (persona que usa una computadora y accede a Internet por medio de una red cableada) requieren también de soluciones y/o mecanismos que les ofrezcan calidad de servicio.

En los casos antes expuestos tanto las redes de los ISPs como de los sistemas móviles necesitan de una red con recursos que permitan ofrecer el ancho de

banda requerido por la aplicación o servicio, y mecanismos que controlen las tasas de error que se puede tener al transmitir información de manera que el cliente reciba un servicio adecuado.

La incorporación de los principios de una red inteligente en estas infraestructuras permitiría que su administración, gestión y control sean más eficientes y brinden al usuario servicios nuevos y mejorados.

Por ejemplo la PSTN (*Public Switched Telephone Network* / Red Telefónica Pública Conmutada), que básicamente es una red de conmutación de circuitos que permite realizar comunicaciones de voz en tiempo real, con la implementación de una red inteligente sobre ésta, la ha convertido en una red capaz de proveer diferentes tipos de servicios a nivel de telefonía.

1.3.1 RED DE BANDA ANCHA INTELIGENTE [2]

La definición de red de banda ancha inteligente se basa en la combinación de dos conceptos; el de red inteligente (IN) y el de red digital de servicios integrados de banda ancha (B-ISDN), mismos que se exponen más adelante en este mismo capítulo. Dicha integración da como resultado un mecanismo de control y administración unificado de los servicios de internet entregados al usuario, como son: video bajo demanda, video conferencia, ancho de banda bajo demanda entre otros.

Entre las funcionalidades de red de banda ancha inteligente se tiene:

- *Administración unificada de recursos:* provee al transporte unificado de servicios la capacidad de gestionar los recursos de red.
- *Capacidad de diferenciación de servicios:* permite al operador controlar toda la cadena de valor, incrementando así el valor de sus marcas de servicios.
- *Capacidad de combinación de multi-servicios:* mejora la capacidad de provisión de servicios de la red.

- *Protocolos de servicios abiertos:* mejora la capacidad de expansión así como la interoperabilidad entre los diversos servicios de una red ya que provee protocolos basados en estándares abiertos.
- *Conformidad con estándares:* garantiza la compatibilidad con elementos de red tradicionales de la arquitectura de red y permite una evolución hacia una red de servicios convergentes.

1.3.1.1 Arquitectura

Una red de banda ancha inteligente se encuentra conformada por:

- *Red de acceso,* la cual permite la conexión de diversas tecnologías a la red.
- *Núcleo de red,* provee funciones de transmisión y conmutación así como proporciona un control lógico de servicios mediante el uso de una entidad que permite tener una red inteligente. Debido a esto es capaz de proveer de servicios a diversos tipos de usuarios sin importar el tipo de tecnología que emplee para acceder a la red.

Además posee los siguientes elementos de red:

- *B-SSP (Broadband Service Switching Point / Punto de Conmutación de Servicio de Banda Ancha):* provee servicio de conmutación e interacción con la red inteligente.
- *B-SCP (Broadband Service Control Point / Punto de Control de Servicio de Banda Ancha):* implementa un control lógico de los servicios que se ofrecen a través de la red inteligente.
- *B-IP (Broadband Intelligent Peripheral / Periférico Inteligente de Banda Ancha):* provee los recursos que son requeridos por el usuario para acceder a un servicio.
- *FT (Fixed Terminal / Terminal Fijo):* representa el terminal de un usuario fijo.

- *MT (Mobile Terminal / Terminal Móvil):* representa el terminal de un usuario móvil.

1.3.1.2 Protocolos

Dependiendo del modelo de integración que se utilice en la red existe una diversidad de protocolos que pueden ser empleados, generalmente el modelo que se emplea es para el *stack* del protocolo IP. En base al tipo de interfuncionamiento o *interworking* se pueden definir diferentes niveles de *stacks* de protocolos, entre los que se puede tener:

- *A nivel de aplicación:* se debe conocer los requerimientos del servicio, ya que es dependiente de este.
- *A nivel ATM (Asynchronous Transfer Mode / Modo de Transferencia Asincrónica):* las celdas son transportadas de manera transparente y el *interworking* es independiente del servicio.
- *A nivel de AAL (ATM Adaptation Layer / Capa de Adaptación ATM):* este tipo de *interworking* es independiente del servicio, los paquetes son transportados de manera transparente.

1.3.1.3 Tecnologías de Acceso

1.3.1.3.1 CDMA 450 [3]

Acceso Múltiple por División de Código para la banda de los 450 MHz (CDMA450) es una tecnología inalámbrica aplicada en las bandas de frecuencia de los 450 - 470 MHz. Puede cubrir vastas áreas geográficas debido a la gran propagación que tiene su señal y brindar servicios tanto de telefonía como acceso al Internet de banda ancha.

De acuerdo a la capacidad de transmisión de datos se clasifica en:

- *CDMA 2000 1X:* permite la transmisión de voz y datos a una velocidad de 153 Kbps.

- *CDMA 2000 1xEV-DO:* permite la transmisión de datos a una velocidad de 2,4 Mbps. Se lo emplea para brindar servicio de banda ancha de Internet.

En Figura 1.2 se muestra un modelo de esta arquitectura.

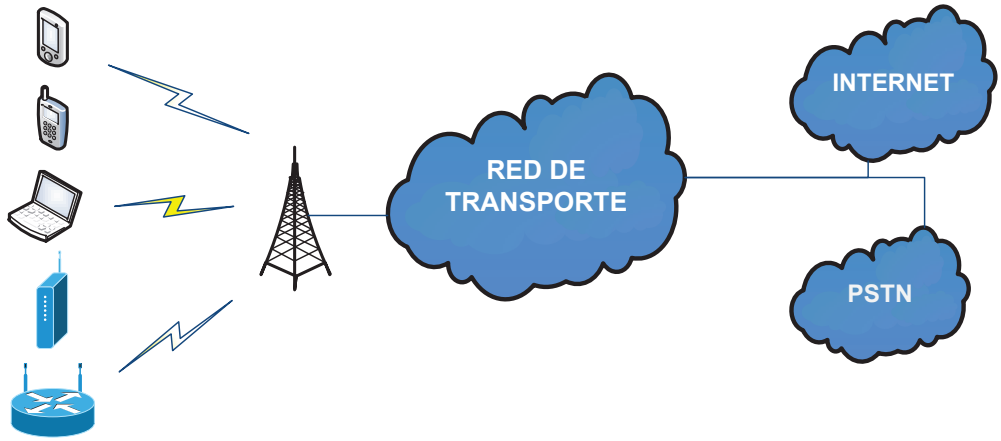


Figura 1.2. Modelo de arquitectura de red CDMA

1.3.1.3.2 WiMAX [4][5]

WiMAX (*Worldwide Interoperability for Microwave Access* / Interoperabilidad Mundial para Acceso por Microondas) es una tecnología de red de área metropolitana inalámbrica que provee una banda ancha inalámbrica para aplicaciones fijas o móviles. Se basa en el estándar inalámbrico IEEE 802.16, mismo que se divide en:

- *IEEE 802.16-2004*: es una tecnología de acceso inalámbrico fijo, es decir, sirve para proveer servicio de voz básico y banda ancha en lugares en donde no existe otra tecnología de acceso, por ejemplo zonas rurales de difícil acceso o alejadas.

  Puede ser utilizada en redes inalámbricas para mejorar el rendimiento de los puntos de acceso de redes Wi-Fi (*Wireless Fidelity*) o como alternativa a conexiones por cable y xDSL. Ofrece velocidades de hasta 70 Mbps.

- *IEEE 802.16e:* está diseñado para ofrecer portabilidad y movilidad al usuario. No es compatible con el estándar mencionado anteriormente por lo

que requiere de una infraestructura diferente para ser implementado. Ofrece soportar sesiones de voz datos a velocidades vehiculares de hasta 120 Km/h.

En la Figura 1.3 se muestra algunas de las aplicaciones de una red WiMAX.

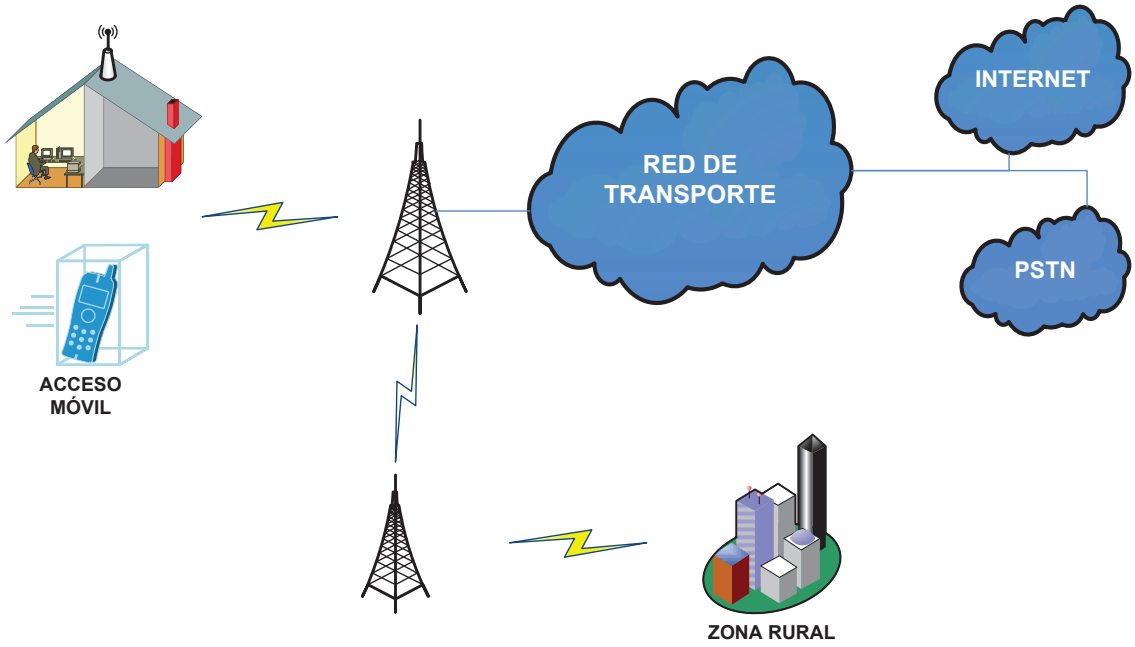


Figura 1.3. Aplicaciones de una red WiMAX[2]

1.3.1.3.3 xDSL [6]

DSL (*Digital Subscriber Line* / Línea Digital de Abonado) es una tecnología que emplea los pares trenzados de cobre de la red telefónica para transportar datos de banda ancha a alta velocidad. En la Figura 1.4 se muestra un modelo de la arquitectura de una red DSL.

xDSL hace referencia a las variaciones que la tecnología DSL posee, y estas son:

- *ADSL (Asymmetric Digital Subscriber Line / Línea de Abonado Digital Asimétrica):* es una tecnología asimétrica que por lo general tiene una velocidad de descarga (de la oficina central hacia el usuario) diferente a la

[2] Basado en [5]

velocidad de subida (del usuario hacia la oficina central). Puede transmitir a velocidades de 6 Mbps.

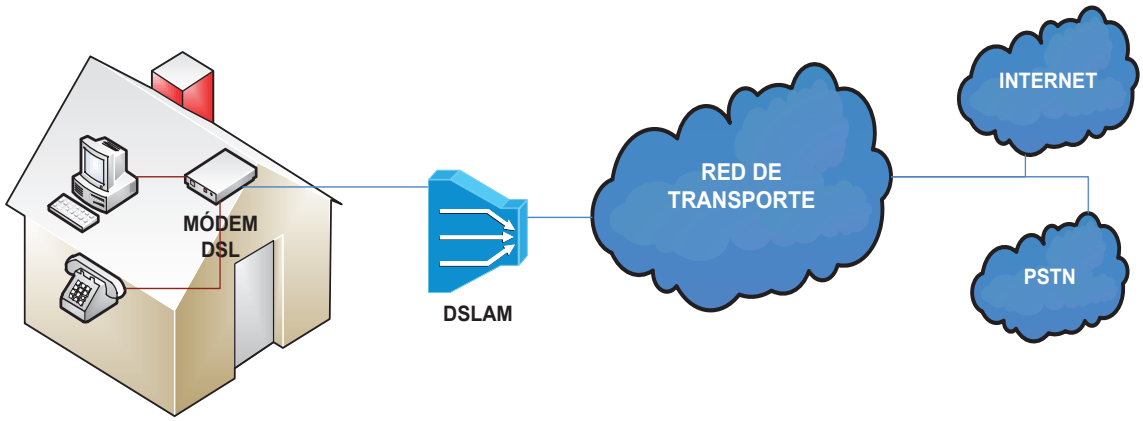


Figura 1.4. Modelo de una arquitectura de red DSL

Los usuarios ADSL disponen de una conexión permanente a Internet, esto es posible porque se dispone de una conexión punto a punto entre el usuario y la red lo que garantiza un ancho de banda dedicado.

  - *ADSL2:* introduce una serie de mejoras orientadas a disminuir el consumo de energía, hace uso del ancho de banda reservado para telefonía para transmitir datos aumentando la velocidad de subida a 256 Kbps.
  - *ADSL2+:* incorpora una capa adicional de corrección de errores y alcanza velocidades de 24 Mbps.

- *SDSL (Symmetric Digital Subscriber Line I Línea Digital de Abonado Simétrica):* es una tecnología simétrica que por lo general tiene una velocidad de descarga igual a la velocidad de subida. Es empleada solo para transmitir datos a una velocidad de 1.54 Mbps sobre un par de hilos de cobre.

- *HDSL (High-bit-rate DSL / Línea de Abonado Digital de Alta Velocidad Binaria):* ofrece transmitir información de manera simétrica sobre dos pares de líneas de cobre a velocidades de T1 (1.544 Mbps) o E1 (2.048 Mbps).

- *HDSL 2:* ofrece un servicio simétrico sobre un solo par trenzado de cobre a 1.5 Mbps.
- *G.SHDSL:* es una versión de HDSL-2 y ofrece velocidades simétricas sobre los 2.3 Mbps.

- *VDSL (Very-High-Data-Rate Digital Subscriber Line / Línea de Abonado Digital de Muy Alta Tasa de Transferencia):* permite transmitir datos a alta velocidad sobre cortas distancias a través de los pares de cobre de la red telefónica. Alcanza una velocidad de descarga de 55 Mbps en distancias de 300 m, y velocidades de subida hasta 2.3 Mbps.

- *IDSL (ISDN Digital Subscriber Line / Línea Digital de Abonado ISDN):* emplea un par de cobre para transmitir datos full dúplex a velocidades de 128 Kbps o sobre los 512 Kbps con comprensión.

1.3.1.4 Servicios de Valor Agregado [7] [8] [9] [10]

En la actualidad día a día se desarrollan nuevas aplicaciones que facilitan la interacción de un usuario con la red así como existe la oferta de nuevos servicios entre los que se tiene:

1.3.1.4.1 Ancho de Banda bajo Demanda

Ancho de Banda bajo Demanda (BoD, *Broadband over demand*) es un servicio que permite a los usuarios ajustar su ancho de banda en base a sus necesidades, es decir, provee a los usuarios la libertad de seleccionar el ancho de banda deseado de acuerdo al o los servicios que empleen.

Este servicio es orientado a conexión y punto a punto lo que garantiza un ancho de banda a los usuarios finales; mismos que pueden estar ubicados o tener diferentes dominios. La capacidad que se puede ofrecer con este servicio depende de las políticas, restricciones o tecnología empleada en la red del operador.

Los usuarios de este servicio pueden ser tarifados en base a la duración de la utilización del servicio o en base al tráfico cursado.

A. Arquitectura

En cuanto a la arquitectura de este servicio se presentan los siguientes módulos:

- *Administrador inter-dominio (IDM):* es responsable por el procesamiento de cada petición del servicio BoD y su trasmisión por la red, ya sea al DM u otro dominio.
- *Administrador de dominio (DM):* se encarga de configurar las entidades que intervendrán dentro de la red para brindar el servicio.
- *Technology Proxies (tecnología de servidores proxy)* este módulo traduce las peticiones de servicio recibidas hacia configuraciones específicas en los equipos del operador.
- *Módulo de políticas:* contiene reglas y políticas a ser empleadas para revisar o elaborar una petición de servicio.
- *Pathfinder module (módulo explorador):* contiene algoritmos que permiten determinar el mejor camino para brindar o transmitir el servicio de acuerdo a las reglas y políticas establecidas para el mismo.
- *Sistema de almacenamiento de información:* almacena la base de datos que contiene las funcionalidades e información útil para el funcionamiento del sistema que permite ofrecer el servicio.
- *Módulo de localización:* almacena información sobre las direcciones de todos los módulos y tipos de servicios que se pueden ofrecer.

1.3.1.4.2 Vídeo bajo Demanda

El servicio de video bajo demanda (*VoD, Video on demand*) permite a los usuarios seleccionar y ver el contenido de un video en el instante que desee sin la

necesidad de una descarga previa ya que emplea la tecnología de *streaming* para su acceso.

Los vídeos se encuentran almacenados en un servidor remoto perteneciente al proveedor de servicio. Este servicio está relacionado con la plataforma IPTV, es muy sensible al retardo y conlleva altos requerimientos de desempeño en tiempo real.

A. Tipos

Los sistemas de VoD se pueden clasificar de acuerdo al tipo de servicio que ofrecen a los clientes en:

- *Pago por ver (PPV, Pay per view):* permite al usuario reservar y pagar por un vídeo determinado.
- *Quasi vídeo bajo demanda (QVoD, Quasi video on demand):* el vídeo es enviado a un grupo de usuarios que hayan solicitado el servicio de manera anticipada.
- *Vídeo bajo demanda aproximado (NVoD, Near video on demand):* el proveedor transmite un contenido específico en intervalos de tiempo regulares, por lo tanto puede que la petición de un usuario no sea atendida de manera inmediata.
- *Vídeo bajo demanda verdadero (TVoD, True video on demand):* le brinda al usuario un control completo sobre lo que quiere visualizar y cuando hacerlo, sin ningún tipo de restricción por parte del operador.

B. Arquitectura

En sistema de VoD se encuentra conformado por tres componentes básicos:

- *Servidor:* es un equipo que almacena los contenidos (vídeos) que pueden ser solicitados por los usuarios.

- *Red de comunicación:* se encarga de transportar las peticiones y datos del servicio a través de la red principal y la red troncal. La red principal es aquella a la que se conectan los servidores de VoD mientras que la red troncal permite interconectar la red principal con la red de distribución local o directamente al usuario.
- *Usuario:* es quien genera peticiones para el servicio, mismo que debe ser recibido y visualizado sin interrupciones o cortes.

1.3.1.4.3 Video Conferencia

El servicio de video conferencia da la posibilidad de transmitir imágenes y sonidos en forma combinada en tiempo real entre grupos de usuarios, es decir, permite la comunicación de manera interactiva entre personas que se encuentran distantes geográficamente. Se la emplea con fines académicos, investigativos, administrativos y técnicos.

A. Arquitectura

Entre los componentes que permiten realizar una vídeo-conferencia se tienen:

- *Sistema de vídeo:* permite capturar imágenes para mostrarlas al usuario. En este se incluyen todo tipo de cámaras de vídeo.
- *Sistema de audio:* permite procesar el sonido para que el usuario lo asimile. En este sistema se incluyen micrófonos, parlantes y auriculares.
- *Sistema de procesamiento y transmisión de la señal:* permite convertir el audio y video en una señal digital para enviarla a través de la red. Este incluye al códec.

1.3.1.4.4 Vídeo Llamada

Este servicio integra el servicio telefónico con el vídeo, es decir, por medio de una llamada telefónica se podrá visualizar al otro interlocutor lo cual facilitará la comunicación principalmente para personas sordo mudas.

Este servicio presenta las mismas funcionalidades de control que una llamada tiene, por ejemplo llamada en espera. Requiere de una conexión con ancho de banda simétrico. Además se basa y emplea en una arquitectura similar a la del servicio de video conferencia. Entre los requerimientos que necesita para un buen funcionamiento se tienen:

- *Calidad de sonido:* debe evitar tener distorsiones y ser mejor o parecido al de un teléfono convencional. Además el sonido necesita ser sincronizado con la imagen.
- *Calidad de imagen:* debe permitir una buena resolución de tal manera que los participantes puedan interactuar de manera comparable con una conversación en persona.
- *Red y sus componentes:* deben asegurar que la transmisión del video no tengan demasiados retardos y pérdidas.

En la Figura 1.5 se muestra un diagrama completo de una red de banda ancha inteligente y sus servicios.

1.4 RED INTELIGENTE [11] [12] [13] [14]

Una red inteligente (IN, *Intelligent Network*) es una plataforma basada en la interconexión de nodos en la que residen centrales de conmutación, sistemas de bases de datos y aplicaciones que emplean sistemas centralizados de determinadas funciones de control o señalización para proveer una variedad de servicios que se implementan de manera independiente definiendo de una manera eficiente recursos y funcionalidades dentro de la red.

Entre los servicios que este tipo de red puede ofrecer se tienen:

- *Servicios de encaminamiento y traducción de número*: permite que las llamadas sean tratadas de manera personalizada por el usuario, por ejemplo desvío de llamadas, número único, llamada en espera, etc.

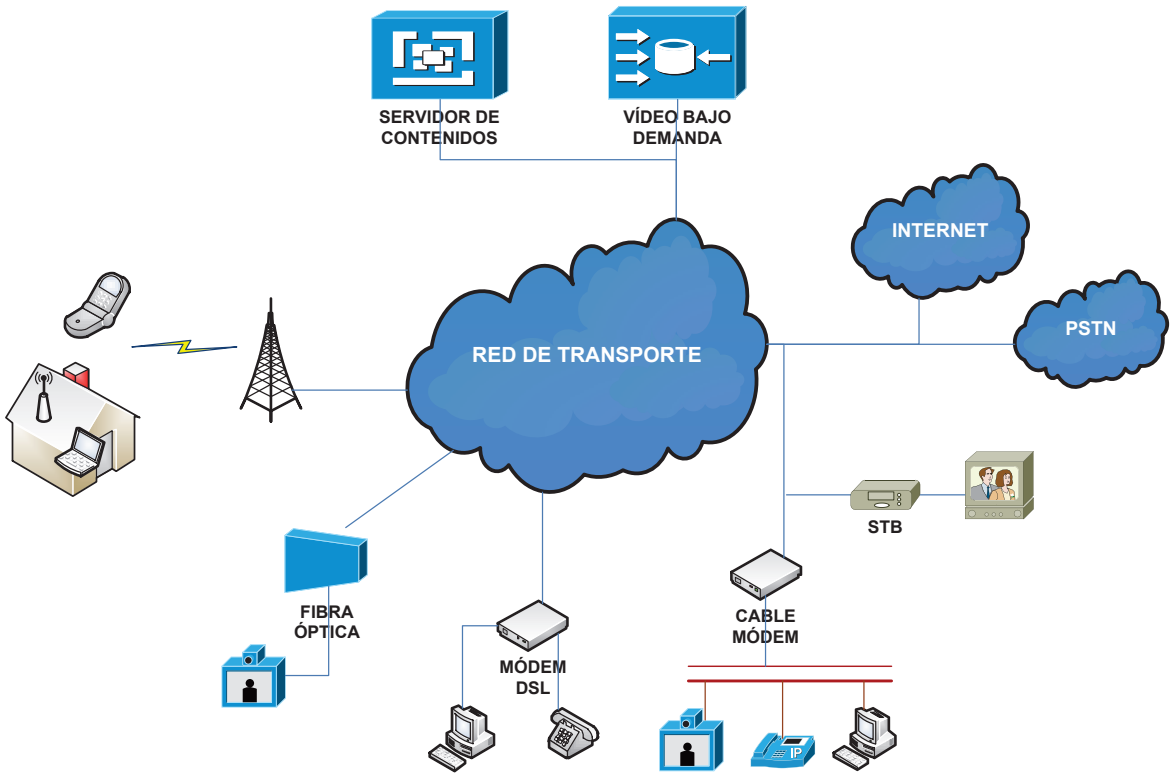


Figura 1.5. Diagrama de una red de banda ancha inteligente y sus servicios[3]

- *Servicios de tarifación especial*: permite repartir el costo de la llamada entre el que la origina y el que la recibe, un ejemplo de estos son los servicios de información 900.
- *Servicios de redes privadas virtuales*: permite crear una red nacional o internacional con numeración privada sin la necesidad de contratar equipos de transmisión específicos.
- *Servicios orientados al operador*: facilita la administración y operación de la red del operador.

1.4.1 ARQUITECTURA

La infraestructura de este tipo de red permite el desarrollo de nuevos servicios, para esto realiza el proceso de conmutación y control de los mismos de manera separada. Los sistemas de red inteligente se basan en los siguientes elementos de red:

[3] Fuente: Corporación Nacional de Telecomunicaciones

- *SSP (Service Switching Point / Punto de Conmutación del Servicio):* provee la funcionalidad de conmutación. Permite el acceso a los servicios, desde cualquier parte de la red telefónica pública conmutada, a los usuarios.
- *SCP (Service Control Point / Punto de Control del Servicio):* facilita el acceso a la base de datos, que almacena la información necesaria para la prestación de un servicio, y responder así a las llamadas generadas por un SSP, es decir, contiene funciones de control de servicio que permiten la distribución de un mensaje a la aplicación correcta.
- *SMS (Service Management System / Sistema de Administración de un Servicio):* administra y gestiona cada uno de los servicios que ofrece una red inteligente. Permite recoger datos estadísticos para elaborar reportes.
- *STP (Service Transfer Point / Punto de Transferencia del Servicio):* permite el transporte de mensajes de señalización entre los nodos de la red.
- *SCEP (Service Creation Enviroment Point / Punto de Entorno de Creación del Servicio):* facilita la creación y personalización de los servicios de la red.
- *IP (Intelligent Peripheral / Periférico Inteligente):* son dispositivos que permiten el manejo de servicios especializados de telecomunicación o servicios de valor agregado.

1.4.2 PROTOCOLOS Y ESTÁNDARES

En una red inteligente se emplean protocolos estándares para la comunicación entre los diversos dispositivos y/o nodos que la conformen.

Entre un SSP y un SCP se ha definido un interfaz normalizado que emplea protocolos basados en SS7[4], los cuales poseen capacidades para el control de congestión y sobrecarga, además de mantener un control de flujo de la

[4] SS7 (*Common Channel Signaling System 7* / Sistema de Señalización de Canal Común 7) provee un canal para la señalización telefónica y otro para la voz, permitiendo que la información de señalización pueda ser intercambiada entre varios equipos, además brida la posibilidad de acceder a bases de datos y procesamiento externo para la provisión de nuevos servicios.

información de establecimiento, mantenimiento y liberación de una petición de servicio entre entidades de la red inteligente.

En un interfaz entre un SCP y un SMS se utilizan protocolos basados en X.25, mientras que en la interfaz entre SCP y un SDP se define protocolos dentro del estándar X.500[5] o LDAP[6].

El estándar en el que se definen recomendaciones para la estructura de una red inteligente se encuentran dentro de la serie Q.1200, mismos que se presentan en la Tabla 1.1.

1.4.3 BENEFICIOS

El desarrollo de la movilidad y la necesidad de una interconexión de alta capacidad entre los nodos de red han provocado en los últimos años que tanto la tecnología como los servicios que un operador puede ofrecer en base a esta progresen rápidamente, debido a esto las redes de telecomunicaciones se han convertido en redes multi-servicio.

Entre los beneficios de tener redes inteligentes es que los operadores pueden aumentar sus ingresos al ofrecer diversos servicios a sus clientes, y disminuir el nivel de inversión y costo operacional al integrar y centralizar la administración de los servicios y recursos de red.

1.5 B-ISDN [15]

La B-ISDN (Red Digital de Servicios Integrados de Banda Ancha / *Broadband Integrated Services Digital Network*) es capaz de integrar servicios como voz, datos y video permitiendo una interoperabilidad con redes públicas y privadas a alta velocidad. Ofrece servicios orientados y no orientados a la conexión, así como administración de conexiones punto a punto y punto a multipunto.

---

[5] DAP: *Directory Access Protocol* / Protocolo de Acceso a Directorios.

[6] LDAP: *Lightweight Directory Access Protocol* / Protocolo Ligero de Acceso a Directorios.

RECOMENDACIÓN	
Q.1210	Conjunto de Características 1 (CS-1)
Q.1220	Conjunto de Características 2 (CS-2)
Q.1230	Conjunto de Características 3 (CS-3)
Q.1240	Conjunto de Características 4 (CS-4)
Q.1250	Conjunto de Características 5 (CS-5)
Q.1260	Conjunto de Características 6 (CS-6)
Q.1270	Conjunto de Características 7 (CS-7)
Q.1280	Conjunto de Características 8 (CS-8)
Q.1290	Glosario
SUBDIVISIÓN	
Q.12x1	Principios de Introducción para CS-x
Q.12x2	Plano de Servicio para CS-x
Q.12x3	Plano Funcional Global para CS-x
Q.12x4	Plano Funcional Distribuido para CS-x
Q.12x5	Plano Físico para CS-x
Q.12x8	Recomendaciones de Interfaz para CS-x
Q.12x9	Guía de Usuario de Red Inteligente para CS-x

Tabla 1.1. Recomendaciones para la estructura de una red inteligente[7]

1.5.1 ARQUITECTURA

Emplea ATM como núcleo de red, ya que esta tecnología transporta de forma transparente la información y es adaptable a cambios en los requerimientos de ancho de banda brindando un uso eficiente de los recursos de red.

Por otro lado usa como medio de transmisión a SONET (*Synchronous Optical Network* / Red Óptica Síncrona) el cual es un estándar que define una jerarquía para las tasas de transmisión y el formato de las tramas de datos.

1.5.2 PROTOCOLOS Y ESTÁNDARES

El modelo de referencia para el protocolo de esta infraestructura se basa en tres planos:

- *Plano de control:* contiene funciones que permiten controlar el establecimiento, duración y liberación de una conexión.

[7] El valor de x corresponde al número de set. La recomendación para el plano de servicio no se encuentra incluida para CS-1.

- *Plano de administración:* contiene las funciones para administrar todo el sistema, y coordina la interacción entre los planos.
- *Plano de usuario:* permite transmitir información entre los elementos de la red. Tiene asociado mecanismos para el control de flujo y congestión, y para recuperación de errores.

Para el control de flujo de información entre los elementos de la red se emplea el sistema SS7 con esto se establece, mantiene y libera las conexiones realizadas por un usuario.

Este tipo de arquitectura se encuentra conformada por entidades que realizan el control y conmutación de servicios, éstas son Intercambio Local (LE, *Local Exchange*) e Intercambio de Tránsito (TX, *Transit eXchange*) y por entidades físicas que representan los equipos finales de usuario y se las denomina Terminales Fijos (FT, *Fixed Terminal*).

1.6 ARQUITECTURA DE UN SISTEMA AAA [16] [17] [18]

El grupo de investigación del IRTF[8] que estudia la arquitectura de un sistema AAA[9] (AAAArch) define un modelo de infraestructura en el cual indica como una arquitectura AAA puede interactuar con otras entidades de la red.

1.6.1 COMPONENTES

Esta plataforma cuenta con uno o varios servidores AAA genéricos que se comunican por medio de un protocolo que maneja las funcionalidades de un sistema AAA, considera también un módulo para el manejo de diversas funcionalidades que requiere una aplicación para su interacción con el servidor AAA.

[8] IRTF: *Internet Research Task Force* / Grupo de Trabajo de Investigación de Internet.

[9] AAA: *Authentication, Authorization, Accounting* / Autorización, Autenticación, Contabilidad.

1.6.1.1 Servidor AAA Genérico

Un servidor AAA tiene la capacidad de autenticar usuarios, autorizar el acceso de éstos a diversos servicios y almacenar la información sobre el manejo de su cuenta. A continuación se da a conocer sus componentes, mismas que permiten el manejo y análisis de peticiones AAA, y ayudan en el desarrollo de aplicaciones que se ajusten a las necesidades de un proveedor de servicios.

- *Autorización:* este módulo le permite al servidor genérico AAA manejar reglas para revisar una petición de un usuario y permitirle el acceso a la red.
- *Módulo específico de aplicación (ASM):* define una interfaz entre el servidor AAA y cualquier tipo de equipo de administración para proveer el servicio requerido por un usuario, es decir, permite gestionar las aplicaciones que interactúan con el servidor AAA.
- *Registro de eventos autorizados (Authorization Event Log):* es una base de datos que contiene información sobre los procesos realizados en el servidor AAA. Por ejemplo puede guardar datos de permisos dados para el caso de que una regla requiera tener acceso previo a un recurso o servicio antes de autorizar el paso a otro.
- *Depósito de políticas (Policy Repository):* contiene información sobre los servicios y recursos disponibles, así como las políticas o reglas que se requieren para poder acceder a estos.
- *Solicitud de transferencia (Request Forwarding):* es un mecanismo que permite comunicar a diversos servidores AAA, mismos que pueden encontrarse en un dominio administrativo distinto.

En la Figura 1.6 se indica la interacción de ciertos componentes en el servidor AAA para autorizar el acceso de un usuario a un servicio y/o recurso de la red. A continuación se da un ejemplo de las acciones que se efectuarían.

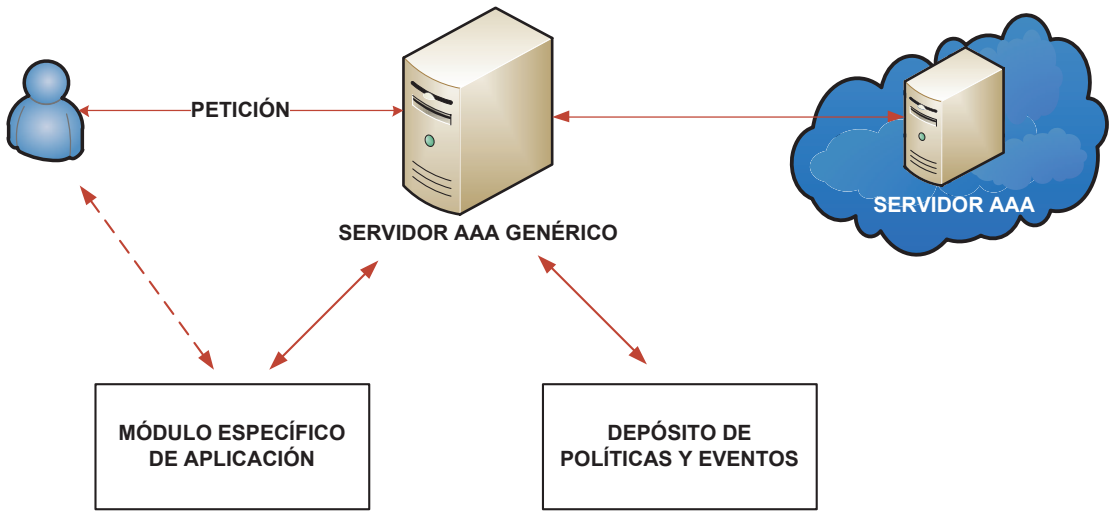


Figura 1.6. Interacción de un servidor AAA[10]

- El cliente envía una petición de acceso a los recursos y/o servicios de la red hacia el servidor AAA.
- El servidor verifica la identidad del usuario para autorizar el acceso. Para esto consulta las bases de datos y/o el depósito de políticas. En algunos casos puede acceder a otro servidor AAA para obtener la información requerida.
- El servidor envía una respuesta al usuario. Ésta puede ser de aceptación o denegación de acceso al servicio.

1.6.1.2 Protocolo de Comunicación

El protocolo AAA es considerado un protocolo de capa de aplicación, y por lo general se emplea uno que permita una comunicación punto a punto. Este debe ser capaz de transportar información de diversos servicios pertenecientes a diferentes aplicaciones que pueden estar ubicadas en distintos dominios administrativos en un solo mensaje. Los tipos de protocolos AAA existentes se describirán más adelante.

[10] Tomado de [16]

1.6.1.3 Cliente AAA

Un cliente AAA puede encontrarse generalmente en un dispositivo conocido como NAS (*Network Access Server* / Servidor de Acceso a la Red) el cual se encuentra en el extremo de la red, responde llamadas y permite el acceso a clientes *dial-up*, a través de la PSTN o ISDN, hacia ésta. Puede ser un *router*, un *switch*, un servidor o un *host*.

A continuación se describe la interacción de estas componentes en el funcionamiento del sistema AAA:

1. Un usuario se conecta al NAS y solicita el ingreso a la red o sus recursos.
2. El NAS recolecta la información del usuario y la envía al servidor AAA.
3. El servidor AAA procesa la información recibida comparándola con la que éste tiene almacenada en su base de datos y envía un mensaje de respuesta (aceptación o negación) hacia el NAS.
4. El NAS recibe el mensaje notifica al usuario si el acceso le ha sido concedido o no.

En la Figura 1.7 se indica el proceso antes descrito.

1.6.2 SERVICIOS

La arquitectura AAA asume una topología multi-dominio, en la cual reside por lo menos un servidor AAA por cada dominio administrativo. Ofrece servicios de autenticación, autorización y contabilidad. Para ofrecer este tipo de servicios se requiere de una comunicación confiable y segura entre el cliente y el servidor o servidores AAA.

1.6.2.1 Autenticación

La autenticación es el proceso mediante el cual un cliente es identificado antes de permitirle el acceso a la red y sus servicios. Esto puede realizarse mediante el uso

de credenciales de identificación como una combinación usuario y contraseña, un desafío (*challenge*), certificados digitales, entre otras.

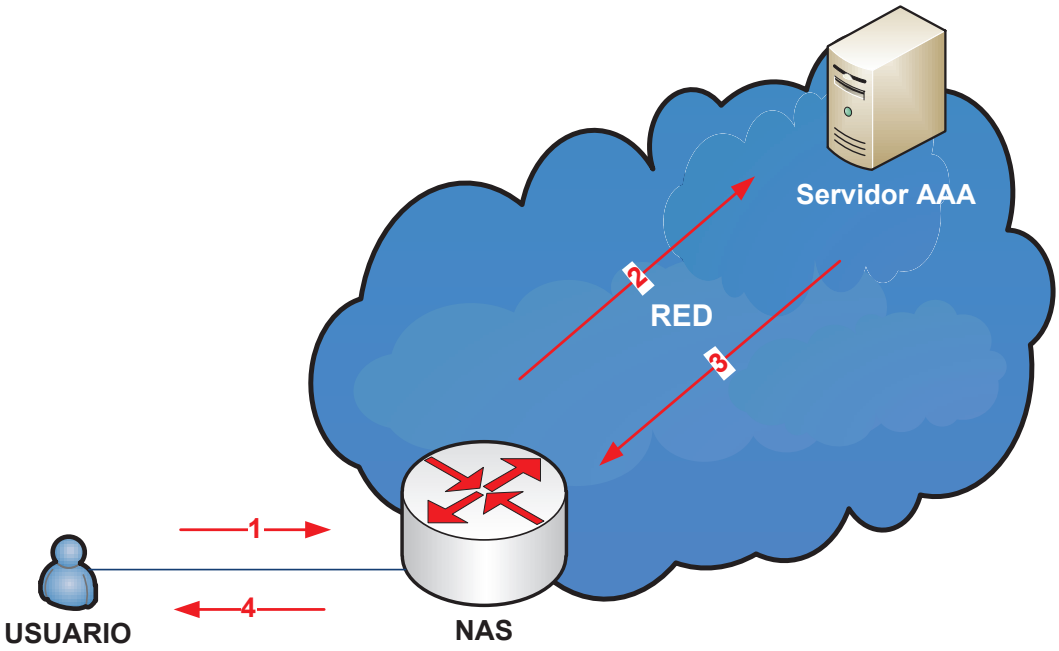


Figura 1.7. Funcionamiento de un sistema AAA[11]

1.6.2.2 Autorización

La autorización define los servicios o recursos a los que el usuario puede acceder una vez que su ingreso a la red ha sido concedido, por ejemplo asignación de una dirección IP, administración del ancho de banda, calidad de servicio o restricciones de acuerdo a su ubicación.

1.6.2.3 Accounting

La contabilidad (*accounting*) permite almacenar información acerca del consumo de recursos de red que tiene un usuario por ejemplo número de paquetes enviados, protocolos empleados, tiempo de consumo. Esto puede ser empleado para auditorías, facturación, reportes, administración o *capacity-planning*.

[11] Basado en [17]

1.7 PROTOCOLOS AAA [18] [19]

Entre los protocolos que consideran relacionados directamente con un sistema AAA se tiene a RADIUS, *Diameter*, TACACS+ y COPS[12], mismos que se describan más adelante.

Por lo general, la conexión entre los elementos que conforman un sistema AAA es punto a punto la cual requiere de seguridad para poder transmitir información. Para esto existen ciertos protocolos que permiten implementarla y también pueden ser considerados, entre estos se tiene a PAP (*Password Authentication Protocol* / Protocolo de Autenticación por Contraseña), CHAP (*Challenge Handshake Authentication Protocol* / Protocolo de Autenticación por Desafío Mutuo) o EAP (*Extensible Authentication Protocol* / Protocolo de Autenticación Extensible).

Actualmente las redes existentes han aumentado su densidad y complejidad debido al crecimiento del internet y las tecnologías de acceso como *wireless*, *Mobile IP* y *Ethernet*, provocando que los protocolos AAA deban modificar sus características y de esta manera mejorar el acceso de los usuarios a la red y sus recursos.

Entre los requerimientos que éstos deben cumplir se tiene:

- Escalabilidad.
- *Fail-over*.
- Seguridad a nivel de transmisión.
- Confiabilidad e integridad.
- Soporte de agentes (*Proxy*).
- Soporte de protocolo IPv4 e IPv6.

[12] El protocolo COPS ha sido considerado como un protocolo AAA por el grupo de trabajo AAA en el RFC 3127.

1.7.1 RADIUS [20] [21]

RADIUS (*Remote Authentication Dial In User Service* / Servicio de Usuario Telefónico de Autenticación Remota) es un protocolo que se emplea para proveer servicio de autenticación, autorización y configuración, entre un cliente y un servidor RADIUS, para permitir el acceso de un usuario PPP/IP *dial-up* a la red.

Fue desarrollado por las empresas Livingston para proveer autenticación a sus equipos NAS. Posteriormente la IETF[13] formalizó este trabajo y lo estandarizó en el RFC 2865. Emplea como protocolo de transporte a UDP (*User Datagram Protocol* / Protocolo Datagrama de Usuario) y como número de puerto el 1812 para autenticación y autorización, y el puerto 1813 para contabilidad.

1.7.1.1 Formato del Paquete

Los paquetes que emplea RADIUS para enviar información se encuentran conformados por una cabecera y AVPs (*Attribute-Value-Pair*) como se muestra en la Figura 1.8.

La cabecera se encuentra conformada por los siguientes campos:

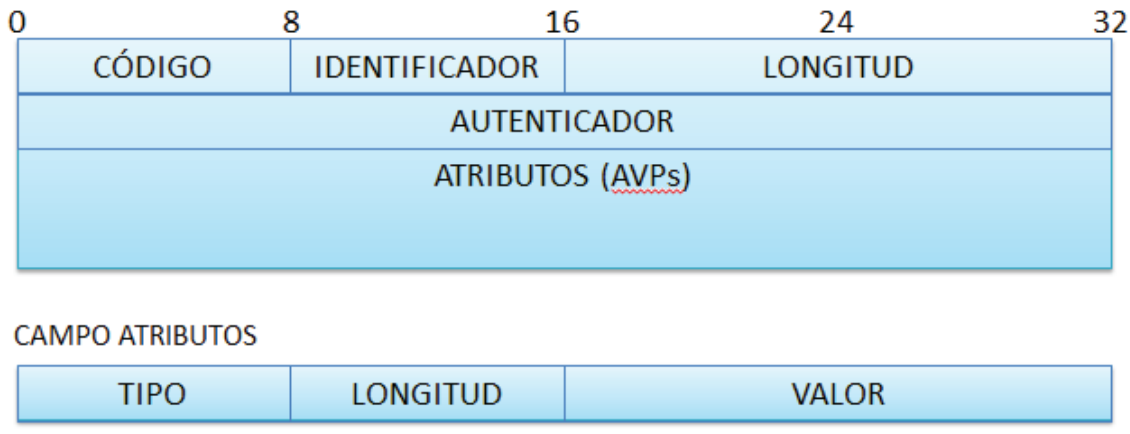


Figura 1.8. Formato de paquete RADIUS[14]

[13] IETF: *Internet Engineering Task Force* / Grupo de Tareas de Ingeniería de Internet.

[14] Tomado de [20]

- *Código:* permite identificar el tipo de paquete RADIUS. Se encuentra conformado por un octeto (1 Byte). En la Tabla 1.2 se muestra algunos valores que este campo puede tener.

VALOR	DESCRIPCIÓN
1	Solicitud de acceso
2	Acceso aceptado
3	Acceso denegado
4	Solicitud de *accounting*
5	Respuesta de *accounting*
11	Desafío de acceso
12	Estado del servidor (experimental)
13	Estado del cliente (experimental)
255	Reservado

Tabla 1.2. Valores para el campo código del protocolo RADIUS

- *Identificador:* da correspondencia a las peticiones con las respuestas. Se encuentra conformado por un octeto (1Byte).
- *Longitud:* indica el tamaño total del paquete (cabecera y campo de atributos). Se encuentra conformado por dos octetos (2B).
- *Autenticador:* se lo emplea para autenticar la respuesta recibida desde un servidor RADIUS y para el algoritmo de clave oculta. Se encuentra conformado por dieciséis octetos (16B).

El campo de *atributos* (AVPs) contienen los detalles de configuración e información de autenticación y autorización para las peticiones y sus respectivas respuestas. Su tamaño puede ser determinado en el campo Longitud. Algunos atributos pueden ser incluidos más de una vez. Se encuentra conformado por los siguientes campos:

- *Tipo:* se encuentra conformado por un octeto (1Byte) y contiene valores asignados. En la Tabla 1.3 se tiene una lista de algunos valores que puede tomar este campo.

VALOR	DESCRIPCIÓN
1	Nombre de usuario
2	Contraseña de usuario
3	Contraseña CHAP
4	Dirección IP del NAS
5	Puerto de NAS
6	Tipo de Servicio
18	Mensaje de respuesta
26	Especificación del vendedor
27	Duración de la sesión
32	Identificador del NAS
33	Estado del *Proxy*
60	Desafío CHAP
61	Tipo de puerto de NAS
62	Límite de puerto
192 al 223	Reservados para uso experimental
224 al 240	Reservados para uso específico o implementación
241 al 255	Reservados (no se lo puede utilizar)

Tabla 1.3. Valores para el campo tipo de los atributos RADIUS

- *Longitud:* este campo se encuentra conformado por un octeto e indica la longitud del atributo. Si su longitud no es la correcta puede provocar que el mensaje sea descartado o que el servidor envíe un paquete de rechazo de acceso.

- *Valor:* este campo puede contener cero o más octetos y contiene la información del atributo. Su formato y tamaño dependen de los campos tipo y longitud. En la Tabla 1.4 se muestra algunos tipos de datos que este campo puede contener.

TIPO DE DATO	DESCRIPCIÓN
Texto	1-253 octetos que contienen UTF-8 codificados en 10646 caracteres.
String	1-253 octetos que contiene datos binarios (0 a 255).
Dirección	32 bit, el octeto más significativo va primero.
Entero	Valor de 32 bit sin signo, el octeto más significativo va primero.
Tiempo	Valor de 32 bit sin signo, el octeto más significativo va primero (00:00:00 UTC, 1 Enero de 1970).

Tabla 1.4. Tipos de datos para el campo valor de los atributos RADIUS

1.7.1.1.1 Tipos de Paquetes

- *Petición de Acceso (Access-Request):* son paquetes enviados a un servidor RADIUS y contiene información que permite determinar si un usuario puede acceder a un NAS o a cualquier servicio que solicite.

  Contiene información como el nombre de usuario, dirección IP del NAS, identificador del NAS, contraseña de usuario o contraseña CHAP, puerto y tipo de puerto del NAS. Cuando se emplea la contraseña de usuario esta va oculta por medio del método de encripción MD5 (*Message Digest Algorithm 5* / Algoritmo de Resumen del Mensaje 5).

- *Petición de aceptación (Access-Accept):* son paquetes enviados por un servidor RADIUS y contienen información de configuración específica para dotar de un servicio al usuario. Se origina cuando los valores de un paquete de petición de acceso concuerdan con los datos almacenados en la base de datos del servidor RADIUS.

  Este tipo de mensaje se encuentra conformado por valores que permiten la configuración del usuario, entre estos se tiene el tipo de servicio (SLIP, PPP) y los requerimientos para proporcionarlo (dirección IP, máscara de red, MTU, protocolo, etc.).

- *Rechazo de acceso (Access-Reject):* es transmitido por el servidor RADIUS cuando alguno de los atributos recibidos están incorrectos y niega el acceso del usuario a la red o sus servicios.

- *Desafío de acceso (Access-Challenge):* este mensaje es enviado por el servidor RADIUS cuando requiere un desafío como respuesta, el cual al ser recibido por el cliente provoca que mediante un *prompt* se pida una respuesta del mismo al usuario y la envié al servidor para su confirmación a través de una petición de acceso. En caso de que el equipo NAS no soporte este tipo de paquetes si los recibe los trata como un mensaje de rechazo de acceso.

1.7.1.2 Modo de Operación

Cuando un cliente desea acceder a un servicio de la red éste se conecta a un NAS, el cual crea una "*petición de acceso"* la cual es enviada hacia al servidor RADIUS. Éste procede a consultar la base de datos de usuarios que posee para determinar el usuario al cual le corresponde la petición recibida y los requerimientos que debe cumplir para poder tener acceso a la red. Usualmente, recibe solo la información pertinente a la contraseña del usuario encriptada.
Si alguno de los datos no concuerda con los de la base el servidor emite un mensaje de "*rechazo de acceso"*; por otro lado si todos los requerimientos se cumplen el servidor puede responder con un *"mensaje de aceptación"* o con un "*mensaje de desafío*". Dependiendo del mensaje recibido el cliente accede a la red o vuelve a intentar el proceso de conexión a la misma.

En la Figura 1.9 se indica el modo de operación del protocolo RADIUS.

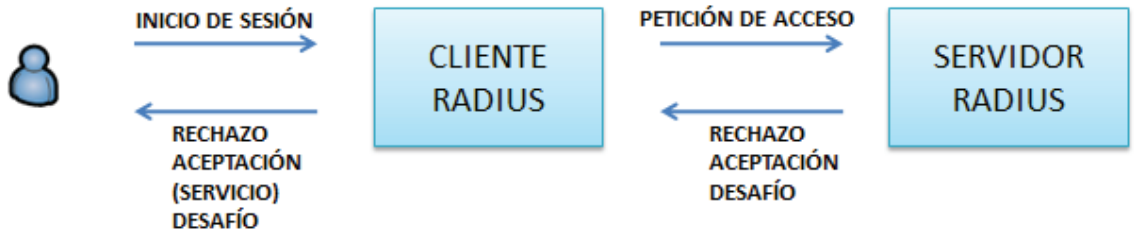


Figura 1.9. Modo operación del protocolo RADIUS[15]

1.7.1.3 Seguridad

El protocolo RADIUS emplea la función *hash*[16] MD5, la cual permite ocultar la contraseña del usuario así como revisar la integridad del mensaje que se comparte entre el servidor RADIUS y el NAS.

[15] Basado en [20]

[16] Una función *hash* es un algoritmo de una sola vía que permite obtener un código de longitud fija y único que representa un mensaje que puede tener una longitud arbitraria.

1.7.2 DIAMETER [22] [23] [24]

El protocolo *Diameter* provee autenticación, autorización y contabilidad para usuarios que acceden a la red mediante aplicaciones *Mobile IP* y NASREQ[17] (*Network Access Server Requirements* / Requerimientos para el Servidor de Acceso a la Red). Ésta última a su vez soporta *dial-in* PPP/IP.

Emplea como protocolos de capa de transporte TCP (*Transmission Control Protocol* / Protocolo de Control de Transmisión) y SCTP[18] (*Stream Control Transmission Protocol*) con el número de puerto 3868. Fue estandarizado por la IETF en el RFC 3588. Ofrece características adicionales a las correspondientes a un protocolo AAA, éstas son:

- Distribución y entrega de AVPs.
- Capacidad de negociación.
- Notificación de errores.
- Posibilidad de expansión, ya que permite agregar nuevos comandos y AVPs.
- Servicios Básicos necesarios para aplicaciones como contabilidad o el manejo de sesiones.

El protocolo *Diameter* define los siguientes tipos de nodos:

- *Cliente:* es un dispositivo que se encuentra al borde de la red y permite el acceso a ésta, por ejemplo un NAS.

[17] NASREQ es una aplicación que permite la interacción y funcionamiento entre el protocolo *Diameter* y RADIUS.

[18] SCTP es un protocolo de capa de transporte que brinda un servicio de transmisión confiable y orientada a la conexión. Permite el envío de un flujo de mensajes sin pérdidas o duplicados; si se produce una pérdida, los datos enviados y recibidos correctamente se mantienen en el *buffer* a la espera que se retransmita el dato faltante.

- *Servidor:* es un dispositivo que maneja peticiones de autenticación, autorización y *accounting* de una red de datos.
- *Agente de Transmisión:* es un dispositivo que enruta mensajes *Diameter* en base a la información que este contiene; puede modificar el mensaje solo añadiendo o retirando información de enrutamiento; los demás campos permanecen intactos.
- *Agente Proxy:* es un dispositivo que enruta mensajes *Diameter* y puede modificarlos para implementar políticas como control del uso de recursos, aprovisionamiento.
- *Agente de Redirección:* es un dispositivo que provee funciones de enrutamiento que permite que un puerto envíe una petición nuevamente al servidor de destino correcto.
- *Agente Traductor:* es un dispositivo que permite la traducción entre dos protocolos por ejemplo la migración de RADIUS a *Diameter*.

1.7.2.1 Formato del Paquete

Diameter se encuentra conformado por un protocolo base, el cual define reglas que son aplicadas a los mensajes que se intercambian entre nodos, así como mecanismos para el transporte confiable y manejo de errores de los mismos. Además define un formato básico para el mensaje a ser empleado por aplicaciones e implementaciones *Diameter*.

En la Figura 1.10 se muestra el formato de un paquete *Diameter*, el cual se encuentra conformado por una cabecera seguida del campo de atributos.

Los campos que conforman la cabecera son:

- *Versión:* este campo indica la versión del protocolo *Diameter*.
- *Longitud del mensaje:* este campo nos indica la longitud total del paquete *Diameter*. Se encuentra conformado por tres octetos.

Figura 1.10. Formato del paquete del protocolo Diameter[19]

- *Banderas:* este campo se encuentra conformado por ocho bits, los cuales son:
    - *Petición (R):* si este bit se encuentra seteado el mensaje es una petición caso contrario es una respuesta.
    - *Proxiable (P):* si este bit se encuentra seteado el mensaje puede ser redireccionado, retransmitido o dirigido a un *proxy*.
    - *Error (E):* si este bit se encuentra seteado el mensaje contiene un protocolo de error indicando que es un mensaje de error.

[19] Tomado de [24]

- *Mensaje potencialmente retransmitible (T):* este bit se setea cuando no se recibe respuesta a una petición desde el servidor debido a una falla o error en el enlace y ésta debe ser reenviada.
- *Reservado (r):* son bits que se encuentran reservados para un uso futuro, es ignorado por el receptor y su valor es cero.

- *Código-comando:* este campo se lo emplea para indicar el tipo de comando que está asociado al mensaje y de esta manera determinar la acción a ser ejecutada. Se encuentra conformado por tres octetos los cuales con administrados por el IANA.

  En la Tabla 1.5 se muestran algunos códigos que están definidos para el protocolo *Diameter*.

NOMBRE DEL COMANDO	ABREVIATURA	CÓDIGO
Solicitud de terminación de la sesión	ASR	274
Respuesta a la terminación de la sesión	ASA	274
Solicitud de *accounting*	ACR	271
Respuesta de *accounting*	ACA	271
Solicitud de desconexión de puerto	DPR	282
Respuesta a desconexión de puerto	DPA	282
Solicitud de re-autenticación	RAR	258
Respuesta de re-autenticación	RAA	258
Solicitud de finalización de sesión	STR	275
Respuesta a finalización de sesión	STA	275

Tabla 1.5. Tabla de códigos para el protocolo *Diameter*

- *Identificador de aplicación:* este campo se lo emplea para identificar la aplicación a la que corresponde el mensaje (autenticación, *accounting* o de un vendedor especifico). Se encuentra conformado por cuatro octetos.
- *Identificador salto por salto:* este campo permite enlazar peticiones con sus respuestas. Su valor es único para cada conexión, se genera de manera aleatoria y se incrementa de uno en uno. Se encuentra conformado por un valor entero sin signo de 32 bits.

- *Identificador extremo a extremo:* este campo se lo emplea para detector mensajes duplicados. Se encuentra conformado por un valor entero sin signo de 32 bits.

El campo de atributos (AVP) contiene información de autenticación, autorización, contabilidad, enrutamiento y seguridad, así como detalles de configuración para peticiones y respuestas que se comparten entre el cliente y el servidor. Se encuentra conformado por los siguientes campos:

- *Código AVP:* permite junto con el campo de identificación del vendedor determinar un atributo único. Valores de 1 a 255 se encuentran reservados para la compatibilidad con RADIUS.
- *Banderas:* informa al receptor como debe ser manejado cada uno de los atributos. Está conformado por los siguientes bits:
    - *r:* son bits reservados, no se los emplea.
    - *P:* indica si se requiere encripción para brindar seguridad extremo a extremo.
    - *M:* indica si se tiene soporte para un determinado AVP, caso contrario se descarta el mensaje.
    - *V:* indica si el campo de identificación del vendedor (Vendor-ID) se encuentra presente en la cabecera. Este campo no debe ser seteado si el bit M está seteado.
- *Longitud AVP:* indica la longitud del campo AVP, y está conformado por tres octetos.
- *Identificador del vendedor:* contiene información que permite identificar a diversos fabricantes, es asignada por el IANA. Está conformado por cuatro octetos.
- *Datos:* este campo puede contener cero o más octetos y contiene la información del AVP. Su formato y tamaño dependen de los campos código

y longitud del AVP. En la Tabla 1.6 se muestra algunos tipos de datos que este campo puede contener.

TIPO DE DATO	DESCRIPCIÓN
OctetString	Contiene información de longitud variable. En caso de necesitar completar un octeto emplea relleno de bits.
Integer32	Valor de 32bit con signo.
Integer64	Valor de 64bit con signo.
Unsigned32	Valor de 32 bit sin signo.
Unsigned64	Valor de 64bit sin signo.
Float32	Valor de punto flotante de precisión simple.
Float64	Valor de punto flotante de doble precisión.
Grouped	Contiene información de una secuencia de AVPs.
Address	Se deriva del tipo de dato *OctetString* y permite representar direcciones IPv4 (32bit) o IPv6 (128bit).
Time	Se deriva del tipo de dato *OctetString*, son cuatro octetos que tienen el formato de tiempo en base a UTC.
UTF8String	Está representado por un set de caracteres dados por ISO/IEC IS 10646-1 mismos que son codificados por medio de UTF-8 en el tipo de dato *OctectString*.
DiameterIdentity	Valor único que permite identificar a un nodo *Diameter*. Se deriva del tipo de dato *OctetString*.
Enumerated	Contiene una lista de valores válidos y su interpretación. Se deriva del tipo de dato Integer32.
IPFilterRule	Permite filtrar paquetes por medio de reglas. Emplea caracteres ASCII y se deriva del tipo de dato *OctetString*.
QoSFilterRule	Evalua paquetes en base dirección IP, protocolo, puerto y valores DSCP (*Differentiated Services Code Point*). Emplea caracteres ASCII y se deriva del tipo de dato *OctetString*.

Tabla 1.6. Tipos de datos para el campo datos del AVP en el protocolo *Diameter*

1.7.2.2 Modo de Operación

Antes de establecer la comunicación entre un servidor y cliente *Diameter* se realiza una búsqueda de puertos en la cual se determina el nodo o agente *Diameter* que intervendrá en la conexión.

Cuando se ha establecido la conexión, a nivel de capa de transporte, los nodos pueden intercambiar mensajes que les permitan establecer su identidad y propiedades.

Un nodo *Diameter* requiere como mínimo dos puertos por dominio para establecer una conexión, uno de estos es el principal y el otro actúa como secundario. Se debe tener en cuenta que se puede realizar balanceo de carga entre los puertos que intervengan en la conexión.

En la Figura 1.11 se muestra el modo de operación de este protocolo.

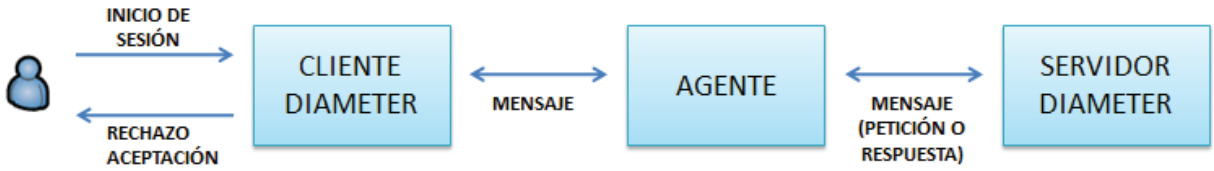


Figura 1.11. Modo operación del protocolo *Diameter*[20]

1.7.2.3 Seguridad

Este protocolo emplea IPSec (*Internet Protocol Security* / Seguridad del Protocolo Internet) o TLS (*Transport Layer Security* / Seguridad de la Capa de Transporte) como mecanismos de seguridad para el flujo de información que se transmite en una red.

1.7.3 TACACS+ [25] [26]

TACACS+ (*Terminal Access Controller Access Control System Plus* / Sistema de Control de Acceso del Controlador de Acceso a Terminales) implementa las funciones de autenticación, autorización y contabilidad de manera separada; además todo el tráfico que se intercambia entre el NAS y el nodo TACACS+ se encuentra encriptado por ejemplo utilizando un algoritmo de *hash*. Emplea el protocolo de transporte TCP con el puerto 49.

1.7.3.1 Formato del Mensaje

El mensaje TACACS+ define una cabecera de 12 bytes, cuyos campos son:

- *Versión:* indica el tipo de versión del protocolo.

[20] Basado en [24]

- *Tipo:* indica el tipo de servicio que transporta el mensaje. Por ejemplo se tiene 0x01 para autenticación, 0x02 para autorización y 0x03 para *accounting*.
- *Número de Secuencia:* indica la secuencia del paquete durante la sesión. Emplea solo números impares.
- *Banderas:* indica el tipo de registro.
- *Identificador de sesión:* es un valor aleatorio designado para la sesión entre el cliente y el servidor.
- *Longitud:* indica la longitud total del mensaje TACACS+.

1.7.3.2 Modo de Operación

1.7.3.2.1 Autenticación

Para la autenticación se emplean tres paquetes:

- *Inicio (start):* se lo emplea para establecer la conexión, es enviado por el NAS hacia el servidor.
- *Respuesta (replay):* es un mensaje enviado por el servidor, durante el proceso de autenticación, hacia el NAS. Entre estas se tiene:
    - *Aceptación (accept):* se envía cuando el usuario se ha autenticado correctamente.
    - *Rechazo (reject):* se envía cuando la autenticación del usuario ha fallado debido a una equivocación en el ingreso del nombre de usuario y/o contraseña.
    - *Error:* se envía cuando ha existido un error durante la fase de autenticación debido a problemas con el protocolo.
- *Continuar (continue):* es empleado por el cliente para enviar información como el nombre de usuario y contraseña al servidor.

1.7.3.2.2 Autorización

Para la autorización se emplean los siguientes paquetes:

- *Solicitud o petición (request):* mensaje enviado del cliente hacia el servidor.
- *Respuesta (response):* enviado del servidor al cliente, entre estas se pueden tener:
    - *Fallo (fail):* se envía cuando no se ha concedido la autorización al o los servicios requeridos por el usuario.
    - *Pass_Add:* se envía cuando la petición o solicitud ha sido autorizada, contiene la información solicitada por el usuario.
    - *Pass_Repl:* se envía cuando el servidor requiere otros argumentos para autorizar el acceso.
    - *Siguiente (follow):* se lo envía cuando el servidor requiere que la autorización se realice en otro servidor. El mensaje contiene la dirección del servidor que efectuará la autorización.
    - *Error:* indica que existe algún error en el servidor durante la fase de autorización.

1.7.3.2.3 Accounting

Para la contabilidad (*accounting*) se emplea un registro al servidor AAA. Entre estos se pueden tener:

- *Inicio (start):* indica al servidor que el servicio está por comenzar.
- *Parar (stop):* indica al servidor que el servicio ha terminado.
- *Continuar (continue):* indica si una sesión se encuentra activa. Provee información de actualización entre el cliente y el servidor.

Entre las respuestas que el servidor puede enviar se tiene:

- *Éxito (success):* cuando el servidor ha recibido el registro con éxito.

- *Error:* cuando el servidor ha tenido fallas para almacenar el registro en su base de datos.
- *Siguiente (follow):* cuando se re-direcciona el registro de un cliente hacia otro servidor.

En la Figura 1.12 se puede observar la forma en la que se intercambian los paquetes descritos anteriormente.

Figura 1.12. Intercambio de paquetes entre un servidor y cliente TACACS+[21]

1.7.4 COPS [27] [28]

El protocolo COPS (*Common Open Policy Service* / Servicio Común de Políticas Abiertas) se encuentra definido dentro del RFC 2748 y principalmente se lo

[21] Tomado de [26].

emplea para definir políticas de calidad de servicio en redes IP. Entre sus características principales se tiene:

- Se basa en un modelo cliente/servidor, en el cual el cliente PEP (*Policy Enforcement Points* / Punto de Aplicación de Políticas) envía peticiones y actualizaciones hacia el servidor PDP (*Policy Decision Points* / Punto de Decisión de Políticas), el cual devuelve las acciones que se deben ejecutar.
- Para un intercambio confiable de mensajes entre el servidor y el cliente emplea como protocolo de capa de transporte a TCP.
- Provee seguridad a nivel de mensaje para autenticación, integridad y protección del mismo frente a retrasmisiones. Puede utilizar protocolos de seguridad como IPSec o TLS para autenticar y asegurar el enlace. Además soporta diversos tipos de información como calidad de servicio proveniente de los clientes sin la necesidad de requerir modificación, es un protocolo extensible creado para la administración, configuración y aplicación general de políticas.
- Es un protocolo de estado, el cual maneja dos características principales:
    - Estado petición/decisión es compartido entre el servidor y el cliente, es decir, las peticiones del cliente son recordadas o instaladas en el servidor hasta que sean borradas al no ser aplicables, mientras que las decisiones pueden ser generadas de manera asincrónica por el servidor.
    - El estado de diversos eventos puede estar inter-asociado, es decir, debido a una asociación con peticiones y decisiones previamente instaladas en el servidor, este puede responder de manera diferente a nuevas peticiones.

El intercambio de información de control de políticas entre el servidor de políticas y su cliente se realiza a través de una base de información de políticas (PIB), incluso se puede tener un dispositivo local (LPDP, *Local Policy Decision Point* / Punto de Decisión de Políticas Local) que efectúe el trabajo del servidor PDP

principal en caso que este sufra algún daño y su comunicación se interrumpa. Esta interacción se muestra en la Figura 1.13.

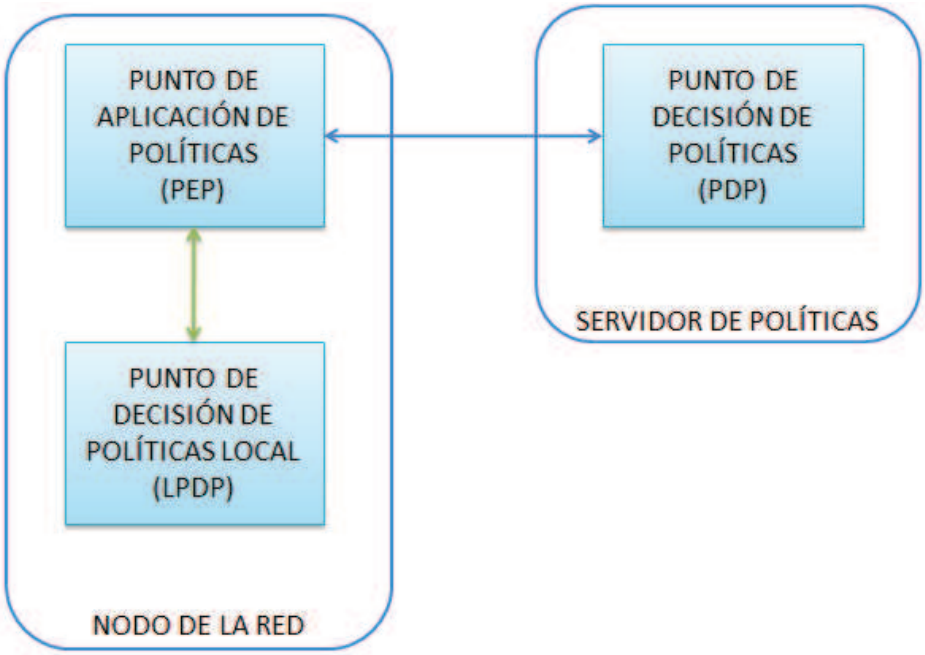


Figura 1.13. Interacción entre servidor y cliente del protocolo COPS[22]

1.7.4.1 Formato del Paquete

En la Figura 1.14 se muestra el formato de un paquete COPS, el cual se encuentra conformado por una cabecera seguida de un número de tipo de objeto.

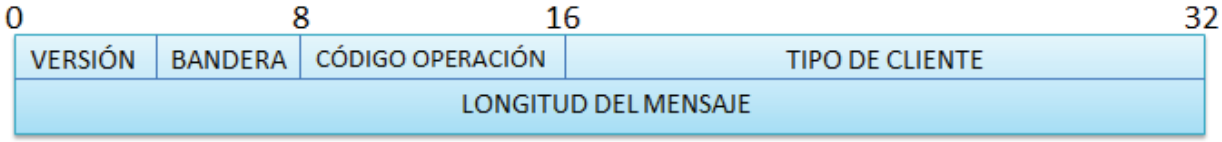


Figura 1.14. Formato del paquete del protocolo COPS[23]

La cabecera se encuentra formada por los siguientes campos:

[22] Tomado de [28]

[23] Tomado de [28]

- *Versión:* indica la versión del protocolo COPS. Se encuentra conformado por 4 bits.
- *Banderas (Flags):* define el valor de las banderas. Se encuentra conformado por 4 bits.
- *Código de operación:* se encuentra conformado por 8 bits e indica diversas operaciones que el protocolo COPS puede ejecutar, mismas que se pueden observar en la Tabla 1.7.

CÓDIGO	NOMBRE DEL CÓDIGO	ABREVIATURA	DESCRIPCIÓN
1	Solicitud	REQ	La petición es realizada por un PEP hacia el PDP para el intercambio de información.
2	Decisión	DEC	Es la respuesta del PDP a una petición.
3	Reporte de estado	RPT	Es empleado por un PEP para informar a un PDP sobre el éxito o fallo al transmitir una decisión.
4	Solicitud de Borrado	DRQ	Es enviado de un PEP a un PDP e indica que un usuario no se encuentra disponible y debe ser removido.
5	Solicitud de Sincronización	SSQ	Es enviado del PDP a un PEP para solicitar que el cliente reenvie su estado para determinar si se encuentra sincronizado.
6	Client-Open	OPN	Es empleado por un PEP para indicar al PDP los tipos de clientes que puede soportar, el último servidor al que estuvo conectado y/o características de negación del cliente.
7	Cliente-Aceptación	CAT	Es empleado en respuesta a un mensaje *Client-Open*. Contiene un *timer* que indica el intervalo que debe haber entre mensajes *keep-alive*.
8	Cliente-Cierre	CC	Puede ser enviado tanto por el PEP como el PDP para notificar que algún cliente ya no se encuentra activo o debido a algún error en el formato del mensaje recibido.
9	Keep-Alive	KA	Provee una validación de funcionamiento de cada lado de la conexión. Es transmitido por PEP dentro de un periodo de tiempo definido en un mensaje CAT.
10	Sincronización Completa	SSC	Es enviado por un PEP a un PDP después de terminar con la sincronización solicitada con un mensaje SSQ.

Tabla 1.7. Tipos de códigos del protocolo COPS

- *Tipo de cliente:* permite identificar la política que tiene el cliente. Se encuentra conformado por 16 bits.
- *Longitud del mensaje:* indica el tamaño total del paquete COPS, su tamaño es en octetos.

1.7.4.2 Modo de Operación

El protocolo COPS emplea la definición de datos dado por COPS-PR (*COPS Policy Provisioning*) para el manejo de decisiones de autenticación y/o autorización y reportes para información de contabilidad. A continuación se describe el modo de operación de este protocolo:

- El cliente establece una conexión con el servidor para esto envía un mensaje *Client-Open*.
- El servidor analiza la petición del cliente y determina la manera en cómo esta puede ser manejada. Si la petición es manejada de manera local el servidor envía su respuesta (aceptación o rechazo) hacia el cliente, caso contrario el servidor puede enviar una decisión de redirección indicando al cliente el servidor apropiado para que maneje su petición.
- El cliente recibe la respuesta, si su acceso ha sido aceptado debe cumplir con las directrices y especificaciones dadas por el servidor, además de enviar reportes de estado de manera periódica para el *accounting*. En caso de ser rechazado el cliente debe eliminar el estado de petición e intentarlo nuevamente.
- El cliente puede finalizar la conexión enviando un mensaje de *Cliente-Cierre*.

Durante el primer intercambio de mensajes *Client-Open/Cliente-Aceptación* entre un cliente y servidor COPS se puede negociar el nivel de seguridad de la conexión misma que cubre todas las comunicaciones que se den sobre ésta. En caso de que no se requiera de un nivel de seguridad el intercambio de mensajes no contendrá información de integridad de los mismos.

Una vez completado el proceso antes descrito el intercambio de mensajes se realizara en base a un número de secuencia, el cual incrementará su valor conforme se intercambie información entre el servidor y el cliente, de esta manera se controla el flujo correcto de paquetes. En caso de que alguno de estos reciba un mensaje con un número de secuencia erróneo se emitirá un mensaje de *Cliente-Cierre* y la conexión se cerrará.

1.8 CALIDAD DE SERVICIO [29] [30] [31] [32]

La calidad de servicio es un término que describe el cumplimiento de un conjunto de parámetros o requisitos sobre el tráfico que cursa por una red mismos que tienen una influencia en como el usuario percibe su experiencia o interacción con esta red. Entre los parámetros que permiten determinar la calidad de servicio se tienen:

- *Disponibilidad de la red:* asegura que los elementos que conforman la red sean redundantes entre sí para garantizar un mejor rendimiento de la red principalmente cuando existen fallas en alguno de sus elementos.
- *Ancho de banda:* es un parámetro que permite determinar si la infraestructura de la red es capaz de soportar y brindar un ancho de banda adecuado para cada uno de los servicios que ofrecen así como para los usuarios que acceden a éstos. Además este parámetro ayuda a clasificar, priorizar y garantizar el ancho de banda para el tráfico de ciertos suscriptores sobre todo cuando existe congestión en la red.
- *Retardo:* es el tiempo que transcurre y que el usuario experimenta mientras un mensaje ingresa, se propaga y sale por la red.
- *Jitter:* es la medida de la variación del retardo entre paquetes consecutivos dentro de un flujo de datos determinado. Tiene un gran impacto en aplicaciones que son transmitidas en tiempo real y que son sensibles al retardo como la voz y el vídeo.

- *Pérdida:* se produce cuando los errores se originan a través del medio de transmisión debido a diversas variables como las condiciones geográficas o medio ambientales, o cuando debido a la congestión de la red los nodos de ésta descartan paquetes provocando que el rendimiento de la red disminuya y posiblemente el ancho de banda de ésta se vea comprometido debido a las retransmisiones que se deban realizar.

1.8.1 MECANISMOS DE CALIDAD DE SERVICIO

La calidad de servicio permite implementar mecanismos que definen ciertos parámetros de operación para la red y de esta manera se pueda brindar un servicio de manera adecuada. Estos mecanismos suelen imponer prioridades y/o restricciones en el acceso a los recursos de la red. Entre estos se tienen:

1.8.1.1 Servicio del Mejor Esfuerzo

Este tipo de servicio implica que en la red no se provea de calidad de servicio, es decir, no se garantiza que la información transmitida a través de ésta llegue a su destino, aunque se hace lo posible por intentar entregarla.

1.8.1.2 Servicios Integrados (IntServ)

IntServ provee de un nivel garantizado de servicio a una aplicación o flujo de datos en particular, ya que permite reservar los recursos de red que esta necesite para que opere de una manera adecuada.
Se basa en el protocolo de reservación de recursos (RSVP) el cual permite mantener los requerimientos de reserva de recursos en cada nodo de la red por el cual se transmitirá el flujo de datos y así garantizar la calidad de servicio requerida por éstos. Se lo puede clasificar en:

- *Servicio garantizado:* provee condiciones seguras y garantizadas en la provisión de los recursos necesarios como un ancho de banda específico para un flujo de datos.

- *Servicio de carga controlada:* asegura que el tráfico será transmitido en su totalidad aun cuando la red tenga sobrecargas.

- *Servicio del mejor esfuerzo:* no se garantiza ningún servicio.

1.8.1.3 Servicios Diferenciados (DiffServ)

DiffServ permite realizar una clasificación del tráfico que circula por la red, por ejemplo por protocolo, puerto o interfaz de ingreso. Además ayudan a los dispositivos de red a operar rápido ya que minimizan la carga de tráfico que deben procesar.

Emplea un código específico para identificar una clase de tráfico, lo que permite asignar prioridades a los diferentes paquetes que son transmitidos por la red logrando así una diferenciación en los servicios que la red presta. Se lo puede clasificar en:

- *Expedited forwarding (Reenvío expeditivo):* es el que brinda mayor seguridad y garantía ya que suministra un servicio con una prioridad alta, parecido al de una línea dedicada. Se lo ejecuta mediante un SLA[24] (Acuerdo de Nivel de Servicio / *Service Level Agreement*).

- *Assured forwarding (Reenvío asegurado):* asegura un trato preferente y suministra un servicio garantizado para cierto nivel de tráfico y no garantiza la transmisión de tráfico excedente.

- *Servicio del mejor esfuerzo:* no se garantiza ningún servicio.

1.8.1.4 IEEE 802.1p

Esta especificación permite asignar prioridades a nivel de capa de enlace de datos (capa 2 del modelo OSI), es decir, trabaja con la cabecera MAC (*Media Access Control* / Control de Acceso al Medio) de los paquetes que pasan por la red añadiendo tres bits que indican la priorización y permiten agrupar a los

[24] SLA: es un contrato de servicio entre un cliente y un proveedor de servicios, en el cual se describe el tipo o clase de servicio con los que será provisto el cliente.

paquetes de acuerdo a la clase de tráfico y cuando exista congestión en la red determinan un trato diferenciado en la entrega de los mismos.

1.9 SERVIDOR DE ACCESO REMOTO DE BANDA ANCHA (BRAS)[33]

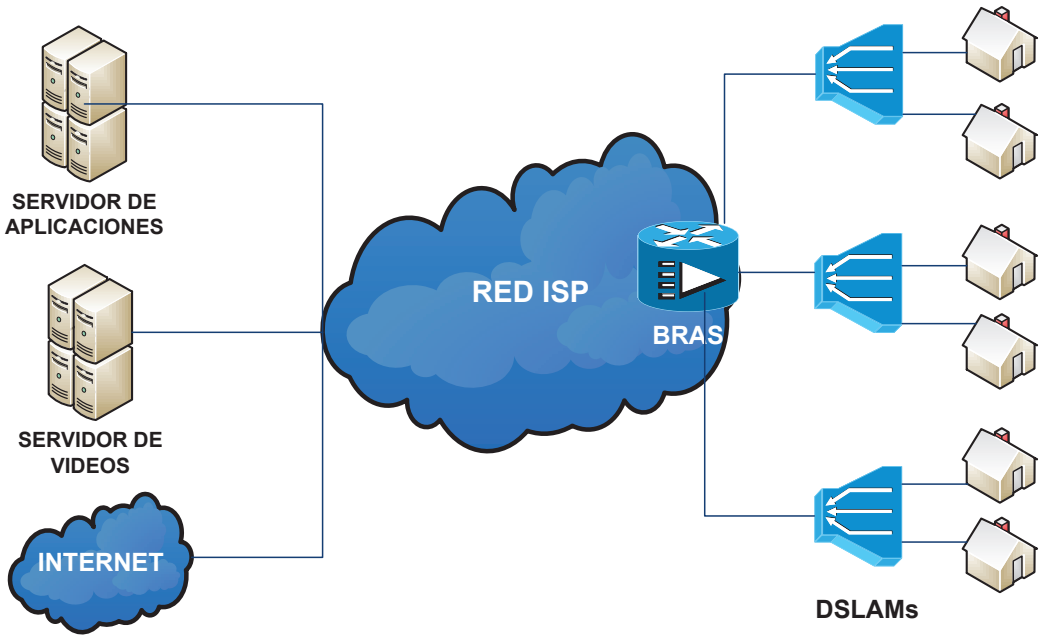
El BRAS es un punto de agregación para el tráfico de abonados, es decir, es un servidor especializado que facilita la convergencia del tráfico en una red.

Este dispositivo, por lo general, se localiza entre la red del proveedor de servicios y el cliente, posee funciones y políticas que permiten administrar el tráfico que atraviesa por éste. De acuerdo a su desarrollo y arquitectura se los puede clasificar en:

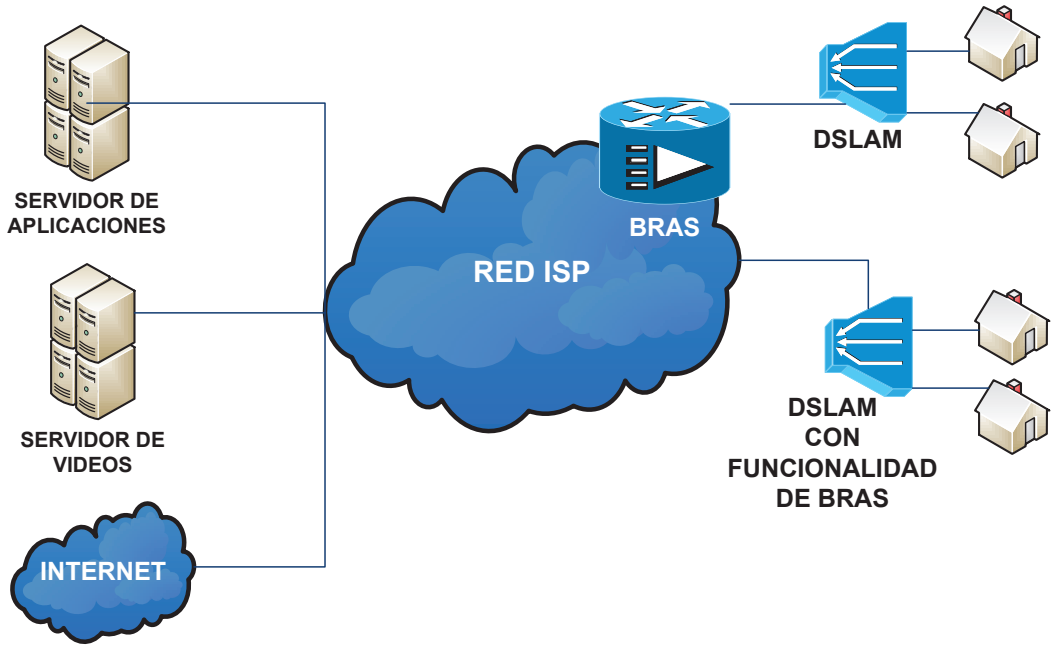
- *Arquitectura basada en software:* son plataformas de *hardware* de propósito general que poseen un *software* el cual les proporciona funcionalidades que les permiten actuar como un BRAS.
- *Arquitectura basada en hardware centralizado:* posee una unidad de procesamiento central y actúa como un *router* de agregación para varios equipos DSLAM[25].
- *Arquitectura basada en hardware modular o distribuido:* posee una inteligencia funcional distribuida entre los módulos de enrutamiento y las tarjetas que contienen las interfaces brindando flexibilidad y escalabilidad ya que permite añadir elementos conforme la red lo necesite.

En la Figura 1.15 se muestra un ejemplo de implementación de estos casos.

[25] DSLAM (*Digital Subscriber Line Access Multiplexer* / Multiplexor de acceso a la línea digital de abonado): es un dispositivo que concentra el tráfico proveniente de varios usuarios DSL en una única línea de alta velocidad (ATM o IP).



ARQUITECTURA DE BRAS CENTRALIZADO



ARQUITECTURA DE BRAS DISTRIBUIDO Y BASADO EN SOFTWARE

Figura 1.15. Ejemplos de arquitecturas de BRAS[26]

[26] Basado en [33]

CAPÍTULO 2

INFRAESTRUCTURA Y ADMINISTRACIÓN ACTUAL DE EQUIPOS DE LA CNT

2.1 INTRODUCCIÓN

La Corporación Nacional de Telecomunicaciones, CNT E.P. como empresa estatal se encuentra inmersa en una serie de proyectos que permitirán asegurar una mejor calidad y disponibilidad de los servicios que presta a nivel nacional, es por esto que requiere de un mejoramiento constante de su infraestructura de red.

Uno de los servicios que ha tenido una gran apertura y acogida a nivel nacional es el de Internet y para poder brindarlo se requiere de una infraestructura robusta que facilite y simplifique la configuración y provisión de servicios de banda ancha de manera independiente a su tecnología de acceso.

En el presente capítulo se describirán los procesos utilizados para la provisión de servicios de banda ancha dentro de la empresa así como de los equipos que forman parte de la infraestructura que permite el funcionamiento de los mismos.

2.2 DESCRIPCIÓN DE LA INFRAESTRUCTURA Y ADMINISTRACIÓN ACTUAL

2.2.1 ADMINISTRACIÓN DE SERVICIOS [1] [2] [3]

2.2.1.1 Modelo de Administración

Actualmente existen diferentes metodologías que permiten proveer al operador de telecomunicaciones de estrategias enfocadas a la administración de su negocio. Estas le permiten proporcionar un conjunto de normas para organizar y definir procesos para el manejo de los servicios y sus niveles de calidad, así como

determinar los recursos que necesita para tener una infraestructura adecuada para poder proveerlos a los usuarios.

Por lo general, los operadores emplean el proyecto NGOSS (*New Generation Operations Systems and Software* / Software y Sistemas de Operación de Nueva Generación) desarrollado por el grupo TMF (*TeleManagement Forum*) debido a que, en muchos casos, existe una desunión entre la tecnología y el modelo de negocio.

Este describe la forma en que pueden interoperar las aplicaciones de soporte de negocio (BSS) con las aplicaciones de soporte de operaciones (OSS); tiene asociado algunas herramientas, mismas que se describen a continuación y se presentan en la Figura 2.1.

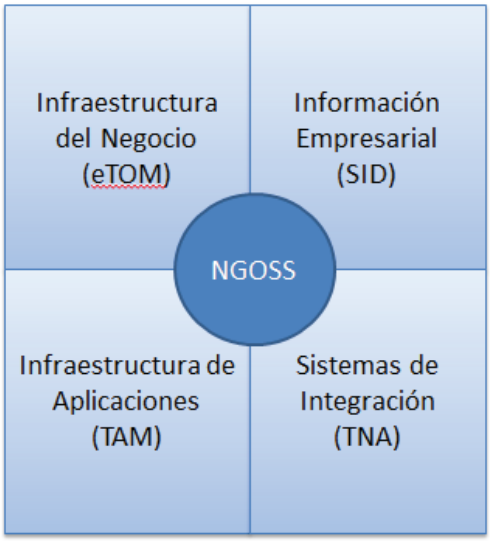


Figura 2.1. Herramientas del proceso NGOSS

2.2.1.1.1 eTOM

eTOM (*enhanced Telecommunication Operations Map* / Mapa de Operaciones de Telecomunicaciones Mejorado) describe un conjunto de operaciones y lineamientos asociados al funcionamiento de una organización. Contiene los procesos de negocio usados por el proveedor de servicios, así como la

identificación de interfaces y el uso de información del tipo cliente, servicio o recurso entre múltiples procesos.

Se lo encuentra en la Recomendación M.3050 de la Unión Internacional de Telecomunicaciones (UIT). Se encuentra organizado por niveles y de manera jerárquica, en base a esto presenta las siguientes áreas:

- *Área de procesos operacionales*: incluyen a los procesos que soportan las operaciones y su administración.
- *Área de procesos de estrategia, infraestructura y producto*: incluye los procesos necesarios para desarrollar estrategias, construir infraestructuras, y el desarrollo y administración de servicios.
- *Área de procesos de la gestión empresarial:* incluye los procesos necesarios que permiten la administración corporativa y dan soporte al negocio.

2.2.1.1.2 SID

SID (*Shared Information Data* / Compartición Información y Datos) proporciona una representación de conceptos de negocio, sus características y relaciones. Se enfoca en los datos e informaciones que se relacionan en procesos de negocios, personas, finanzas, productos y servicios. Permite la comunicación, integración e interoperabilidad entre aplicaciones de los OSS y los BSS.

2.2.1.1.3 TAM

TAM (*Telecommunications Application Map* / Mapa de Aplicaciones de Telecomunicaciones) define un grupo de aplicaciones con las cuales los operadores deben brindar el servicio permitiendo así la integración entre la información, los procesos y los sistemas que intervienen en esto. Funciona como un puente entre eTOM y SID, mediante la provisión de sistemas operacionales que agrupan las funciones de los procesos y la información que transmiten por medio de los OSS y BSS.

2.2.1.1.4 TNA

TNA (*Technology Neutral Architecture* / Arquitectura Neutral de Tecnologías) define una infraestructura para las aplicaciones, datos y procesos que deben trabajar de manera conjunta con los sistemas del operador. Por ejemplo especifica la forma de comunicación entre las aplicaciones mediante el uso de una interfaz común.

Existen otras metodologías que permiten implementar y gestionar servicios de calidad, y que se pueden utilizar como complemento a ese modelo, entre estos se tiene:

- *ITIL (Information Technology Infrastructure Library / Biblioteca de Infraestructura de Tecnologías de la Información)*: propone el establecimiento de estándares que ayuden al control, operación y administración de los recursos, permitiendo la entrega de servicios de tecnologías de la información con eficiencia y calidad. Es independiente de la plataforma tecnológica en el que se la emplee.
- *COBIT (Control Objectives for Information and Related Technologies / Objetivos de Control para Tecnología de Información Relacionadas):* investiga, desarrolla, publica y promueve un conjunto de objetivos de control de las tecnologías de la información enfocado al control de métricas pero sin considerar el flujo de procesos y con la implantación de poca seguridad.

2.2.1.2 Aplicación del Modelo

En la CNT específicamente no se ha definido una metodología para la administración del negocio, maneja un modelo de integración entre eTOM e ITIL con tendencia a la implementación del proyecto NGOSS.

En base a lo planteado se describirá de manera general el modelo de operaciones para la provisión (activación, cambio o retiro) de servicios que la empresa maneja.

Primeramente se debe realizar el ingreso de la petición del servicio, esto lo realiza un asesor comercial por medio de una aplicación conocida como AXIS. Para el presente caso de análisis las peticiones ingresadas pueden ser:

- Activaciones: provienen de personas que contratan por primera vez el servicio de internet de banda ancha.
- Cambios: suscriptores que realizan modificaciones, principalmente de velocidades, al plan comercial que tienen contratado.
- Retiros: son clientes que cancelan o finalizan el contrato que poseen con la empresa.

Esta información a su vez se ve replicada en la plataforma Open Flex la cual, de acuerdo a los requerimientos del servicio, genera órdenes de trabajo para las diferentes áreas de gestión en la empresa. Entre las órdenes que esta plataforma puede generar se tiene la configuración, el mantenimiento (solución de problemas de un servicio) o la facturación de un servicio siendo esta última funcionalidad de la más relevante para el presente caso de análisis.

En la Figura 2.2 se muestra el funcionamiento del proceso antes descrito.

2.2.2 ANÁLISIS DE LA TOPOLOGIA DE RED [4]

La Corporación Nacional de Telecomunicaciones posee una red de datos que emplea un modelo jerárquico, en el que se distinguen los siguientes niveles:

- Capa de Núcleo.
- Capa de Distribución.
- Capa de Acceso.

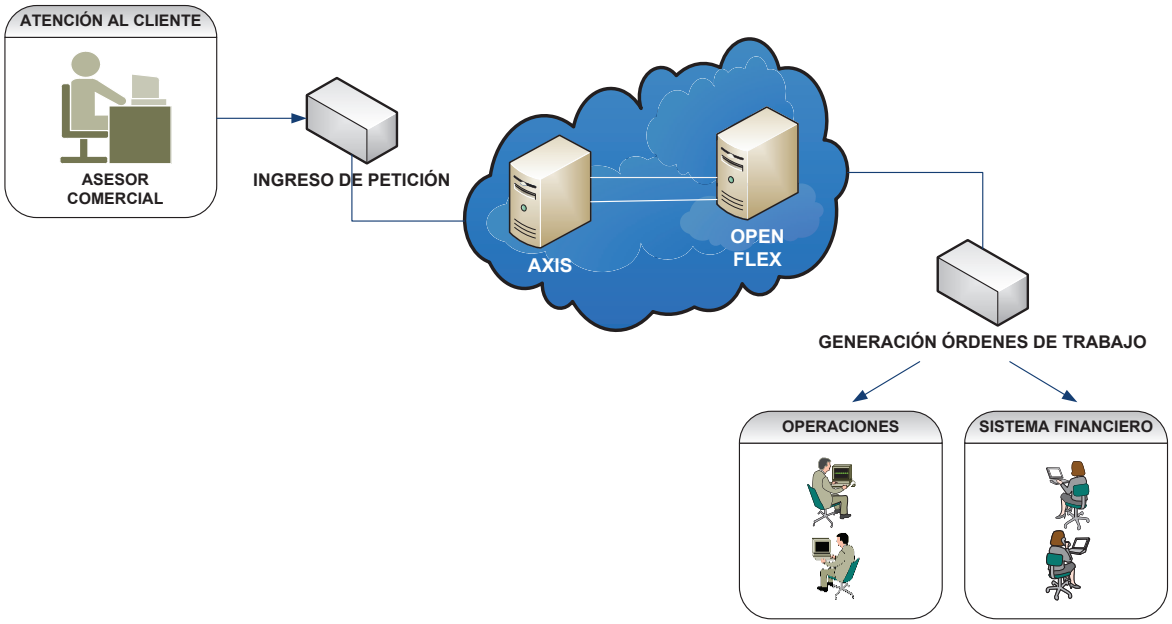


Figura 2.2. Proceso de aprovisionamiento de un servicio

2.2.2.1 Capa de Núcleo

El núcleo de la red se encuentra conformado por la tecnología IP/MPLS[27] (Protocolo Internet, *Internet Protocol* / Multi Protocolo de Conmutación de Etiquetas, *Multi Protocol Label Switching*). Cuenta con seis equipos los cuales están ubicados en la ciudad de Quito, Guayaquil y Ambato.

2.2.2.2 Capa de Distribución y Acceso

A nivel de estas capas se cuenta con equipos que emplean la tecnología IP/MPLS, aunque también se encuentran conformadas por elementos de red correspondientes a redes legadas existentes en la empresa como ATM[28] y Metro

[27] Red IP/MPLS: es una red multi-servicio (voz, datos y vídeo) compuesta por equipos MPLS en el núcleo e IP a nivel de acceso, estos últimos adaptan paquetes IP a MPLS. Optimiza el enrutamiento y conmutación de paquetes a nivel de capa 3 y 2 respectivamente. Dan convergencia para diversas redes como ATM. [5]

[28] Red ATM: es capaz de manejar diferentes tipos de tráfico y realiza su transmisión en forma de celdas. Tiene una arquitectura basada en capas, es orientado a la conexión y ésta se identifica por medio de un identificador de canal virtual (VCI) o/y un identificador de camino virtual (VPI). [6]

Ethernet[29]. Se tiene aproximadamente 70 nodos, en las capas de distribución y acceso, mismos que se encuentran ubicados alrededor de todo el país.

A la capa de acceso convergen ciertas tecnologías que permiten la comunicación con los equipos de los usuarios, entre las que se tiene: WIMAX, xDSL y CDMA-450.

A la red también se enlazan otros componentes como bordes[30] de Internet y equipos BRAS/AAA. Los equipos BRAS/AAA permiten administrar y gestionar clientes de banda ancha, autenticarlos para asignarles un perfil de acuerdo al plan contratado y con fines de facturación.

De acuerdo al alcance de este proyecto de titulación, el análisis básicamente se centrará en los equipos y componentes del sistema AAA y su integración e interacción con la red de datos perteneciente a la CNT, lo que se puede visualizar en la Figura 2.3.

2.2.3 EQUIPAMIENTO

2.2.3.1 Descripción de Equipos

La CNT a nivel nacional posee cinco equipos BRAS/AAA, los cuales se encuentran ubicados en las ciudades de Quito y Guayaquil. A continuación se explica la distribución de estos puntos de acuerdo a la estructura organizacional de la empresa.

2.2.3.1.1 Zona Andina

CNT, para las provincias que conforman la región andina emplea dos equipos BRAS/AAA que permiten administrar los servicios de banda ancha tanto para

[29] Red Metro Ethernet: se refiere al uso de la tecnología *Ethernet* sobre redes de área metropolitanas permitiendo el trasporte de grandes cantidades de información a velocidades que van desde los 10 Mbps a los 10 Gbps. [7]

[30] Borde de Internet: equipo que permite enrutar el tráfico de Internet hacia la red de los proveedores internacionales.

clientes con infraestructura IP como ATM. Estos se encuentran ubicados en la ciudad de Quito.

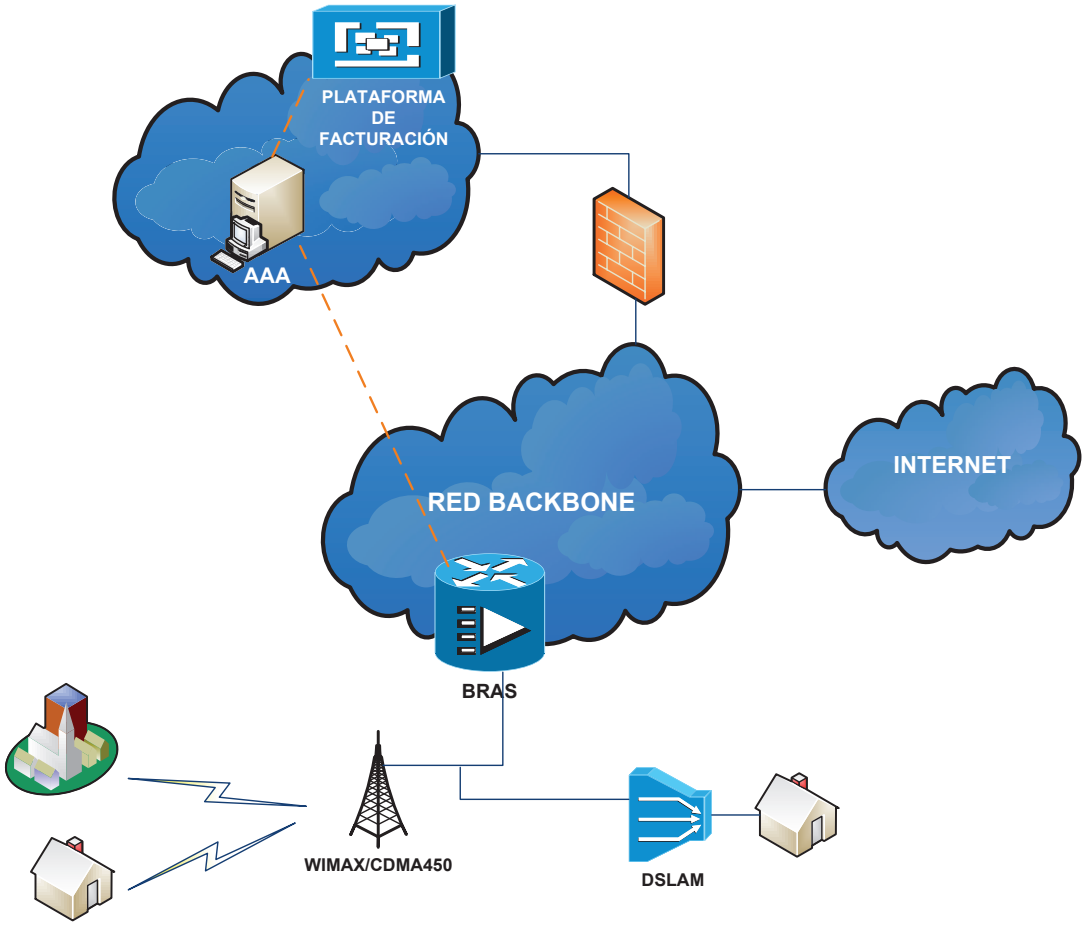


Figura 2.3. Interconexión del sistema AAA con la red de datos perteneciente a la CNT

A. Nodo Iñaquito

En este nodo se encuentra situado un BRAS modelo MA5200G de marca Huawei cuyo sistema AAA se lo conoce como iTELLIN. Este equipo opera con una base de datos en la plataforma Informix, en la cual se almacenan datos de los usuarios.

B. Nodo Mariscal

En este nodo se encuentra situado un BRAS modelo SE800 de marca Redback cuyo sistema AAA se lo conoce como NetOp. Este equipo opera con una base de datos en la plataforma Oracle.

La región Andina cuenta también con un sistema AAA para los usuarios WiMAX conocido como Info-X cuya base de datos se maneja en la plataforma MySQL.

2.2.3.1.2 Zona Pacífico

CNT, para las provincias que conforman la región del pacífico emplea tres equipos BRAS/AAA que permiten administrar los servicios de banda ancha para clientes con infraestructura IP. Estos se encuentran ubicados en la ciudad de Guayaquil.

A. Nodo Correos

En este nodo se encuentran situados los siguientes equipos:

A.1. BRAS/AAA Ericsson

Se tienen dos equipos de marca Redback, mismos que se describen a continuación:

- *BRAS modelo SE800*, cuyo sistema AAA se lo conoce como NetOp y opera con una base de datos en la plataforma Oracle.
- *BRAS modelo SE400*, mismo que trabaja con un sistema AAA FreeRADIUS y opera con la base de datos proporcionado por el sistema AXIS.

A.2. BRAS/AAA Huawei

Se tiene un BRAS modelo MA5200G de marca Huawei cuyo sistema AAA se lo conoce como Info-X. Este equipo opera con una base de datos en la plataforma Oracle.

A.3. FreeRADIUS

Se tiene un BRAS marca Redback modelo SE800 cuyo sistema AAA se lo conoce como FreeRADIUS. Este equipo opera con la base de datos que se almacena en el sistema AXIS.

En la zona Pacífico existe también un sistema AAA CDMA de marca Info-X cuya base de datos se maneja en la plataforma MySQL.

En la Tabla 2.1 se presenta un resumen de los BRAS y plataformas AAA existentes en la CNT.

UBICACIÓN	BRAS		PLATAFORMA AAA	
	MARCA	***MODELO***	***MARCA***	***BASE DE DATOS***
Zona Andina	Huawei	MA5200G	iTELLIN	Informix
	Redback	SE800	NetOp	Oracle
			InfoX (WiMAX)	MySQL
Zona Pacífico	Huawei	MA5200G	InfoX	MySQL
	Redback	SE800	NetOp	Oracle
	Redback	SE400	FreeRADIUS	AXIS
			InfoX (CDMA)	MySQL

Fuente: Corporación Nacional de Telecomunicaciones

Tabla 2.1. BRAS y plataformas AAA existentes en la CNT

2.2.3.2 Características de los Equipos

A continuación se procederá a realizar una descripción de las características de los equipos que formarán parte del sistema AAA centralizado.

2.2.3.2.1 Plataforma AAA

Actualmente en la empresa, los sistemas AAA con los que cuentan se encuentran implementados en servidores de marca SUN Microsystems. En la Tabla 2.2 se enlistan los servidores existentes y algunas de sus características principales.

A continuación se procederá con la descripción de las plataformas AAA y equipos BRAS que la empresa posee.

A. iTELLIN [12]

iTELLIN es el sistema AAA de Huawei, el cual por lo general se encuentra ubicado en la capa de servicios de la red del operador. Se comunica con el BRAS a través del protocolo RADIUS y con los dispositivos de tarifación mediante FTP

(*File Transfer Protocol* / Protocolo de Transferencia de Archivos) y/o MML (*Man-Machine Language* / Lenguaje Hombre-Máquina).

Esta plataforma AAA se encuentra conformada por subsistemas tanto a nivel de hardware como de software, que permiten que brinde diversas aplicaciones como:

- *Centro de autenticación y autorización*, permite determinar en base a parámetros como nombre de usuario, contraseña, dominio si un suscriptor puede o no ingresar a la red. Una vez permitido el acceso envía un mensaje al BRAS en el cual se indica el tipo de recursos al que el usuario puede acceder.
- *Centro de contabilidad*, provee de funciones para la facturación de un servicio en tiempo real. La información de *accounting* la maneja por medio de CDRs[31].
- *Centro de administración*, almacena información sobre el usuario y los servicios a los que puede acceder. Soporta el protocolo LDAP[32] el cual le permite integrarse con el OSS.
- *Centro de portales*, mediante el uso un *web browser* permite acceder y administrar los servicios de una manera remota.
- *Redundancia de equipos*, que permite que ante cualquier desastre en el ambiente de producción el equipamiento secundario pueda sustituir a este y continuar con la provisión de servicios.

Entre las funcionalidades que esta plataforma ofrece actualmente en la empresa se tiene:

[31] Un CDR (*Call Detail Record* / Registro de Detalle de Llamada) es un archivo que contiene información acerca de un servicio al que accede un usuario, generalmente esta permite facturar el consumo de un cliente.

[32] LDAP es un protocolo estándar que permite administrar directorios y de esta manera acceder a bases de datos que contienen información de usuarios de una red. Ofrece una capacidad de filtrado sobre la información que está siendo solicitada.

SERVIDOR	CARACTERÍSTICAS	
SUN FIRE V880	*Procesador*	8-core 1.2 GHz UltraSPARC III
	Disco duro	Hasta 12 discos SCSI[33] de 73 GB
	Memoria	8 GB, expandible hasta 64 GB
	Interfaz de red	Una interfaz Gigabit Ethernet y una interfaz Fast Ethernet
	Sistema operativo	Solaris 8
	Potencia	1500 W (AC)
	Aplicaciones	Puede ser empleado para: • Aplicaciones de base de datos e Internet. • Comercio electrónico.

SERVIDOR	CARACTERÍSTICAS	
SUN SPARC ENTERPRISE T5220	*Procesador*	4-core 1.2 GHz UltraSPARC T2
	Disco duro	De 8 a 16 discos SAS[34] 146GB/300GB
	Memoria	8 GB, expandible hasta 64 GB
	Interfaz de red	Cuatro puertos Ethernet 10/100/1000 Mbps
	Sistema Operativo	Solaris 10
	Potencia	750 W (AC)
	Aplicaciones	Puede ser empleado para: • Aplicaciones de seguridad. • Virtualización. • Servidor web, base de datos, *streaming media*. Arquitectura orientada a servicios (SOA) y plataformas de integración de negocios.

SERVIDOR	CARACTERÍSTICAS	
SUN FIRE V245	*Procesador*	2-core 1.5 GHz UltraSPARC IIIi
	Disco duro	Hasta 4 discos SAS de 73 GB (146 GB opcionales)
	Memoria	8 GB
	Interfaz de red	Cuatro puertos Ethernet 10/100/1000Base-T
	Sistema Operativo	Solaris 10
	Potencia	400 W (DC)

CONTINÚA

[33] SCSI: (*Small Computer System Interface* / Interfaz de Sistema para Pequeñas Computadoras) es una interfaz estándar empleada para la transferencia de datos entre computadoras y dispositivos periféricos.

[34] SAS: (*Serial Attached SCSI*) es una tecnología diseñada para la transferencia de datos hacia dispositivos de almacenamiento por medio de una interfaz serial.

SERVIDOR		CARACTERÍSTICAS
SUN FIRE V245	*Aplicaciones*	Puede ser empleado para: • Servidor de aplicaciones, web, portal de seguridad. • Comercio electrónico.

Tabla 2.2. Características de los servidores existentes en la CNT[35]

- Administración de suscriptores post-pago:
  - Permite crear o eliminar un usuario.
  - Permite modificar información como la contraseña, plan de navegación de un cliente.
  - Permite crear y almacenar diferentes dominios para su consiguiente asignación a un usuario.
  - Permite suspender o desactivar el servicio de un usuario.
- Permite la configuración de un pool de direcciones IP a un usuario, así como la asignación de una dirección IP de manera dinámica o estática de acuerdo al tipo de plan del suscriptor.
- Almacenamiento de la información relacionada con el consumo de servicio de Internet de banda ancha en CDRs, para la correspondiente tarifación del mismo.
- Manejo de usuarios ATM.

B. NetOp [14]

El sistema de administración NetOp provee una plataforma robusta y escalable que permite gestionar configuraciones y fallas de una manera fácil y segura a través de una interfaz gráfica de usuario. Además posee otras herramientas que ayudan con estas funcionalidades:

[35] Fuente: Corporación Nacional de Telecomunicaciones. [9], [10] y [11].

- CLI (Interfaz de Línea de Comandos), contiene una lista de comandos que ayudan en la configuración o en la resolución de problemas que la plataforma Redback pueda tener.
- SNMP (Protocolo Simple de Administración de Red), posee un agente SNMP el cual soporta las tres versiones de dicho protocolo y puede ser empleado para recolectar estadísticas en base a MIBs (Base de Información Gestionada).
- *BulkStats,* esta característica permite la recolección de estadísticas como errores o tráfico en forma de objetos específicos por ejemplo por puerto o circuito.
- *Accounting* basado en el atributo BGP, soporta políticas de contabilidad para el protocolo BGP (*Border Gateway Protocol*) las cuales permiten diferenciar las cuentas para tráfico IP para de esta manera aplicar la facturación de acuerdo a la ruta que este atraviese.
- Posee la funcionalidad de RADIUS *proxy* para enviar datos hacia otros servidores RADIUS o el sistema de tarifación.
- Soporta interfaces CORBA y SOAP/XML (*Simple Object Access Protocol* / Extensible Markup Language).

Este sistema se encuentra conformado por un servidor en el cual va instalado el software NetOp EMS (*Element Management System*) el cual almacena las bases de datos y permite manejar uno o más nodos que actúen como *proxy*; y el NetOp PM (*Policy Manager*) el cual permite al operador administrar a los usuarios y los servicios mediante el establecimiento de políticas. Puede almacenar información relacionada con *accounting.*

Entre las funcionalidades que esta plataforma ofrece actualmente en la empresa se tiene:

- Administración de suscriptores post-pago:

  - Permite crear o eliminar un usuario.
  - Permite modificar información como la contraseña, plan de navegación de un cliente.
  - Permite suspender o desactivar el servicio de un usuario.

- Permite la configuración y la asignación de una dirección IP de manera dinámica a un suscriptor.
- Almacenamiento de la información relacionada con el consumo de servicio de Internet de banda ancha en CDRs, para la correspondiente tarifación del mismo.
- Manejo de usuarios ATM.

C. Info-X [19]

Este sistema AAA se encuentra conformado por cinco subsistemas: un servidor RADIUS, un servidor de *accounting*, un sistema de administración, un servidor de reportes y una base de datos central; los cuales brindan seguridad de aplicación, acceso, comunicación y almacenamiento de datos.

Soporta el acceso de usuario de diversas tecnologías como banda ancha, CDMA y WiMAX brindando estabilidad y un buen rendimiento para el operador. Soporta servicios de tarifación prepago y postpago. Además puede ser administrado a través de una página web.

D. FreeRADIUS [18]

Es un sistema AAA de distribución gratuita, entre sus componentes principales cuenta con un servidor RADIUS y una librería que almacena datos de los clientes cuya interacción permite la autenticación de los usuarios en una red y posteriormente el acceso a los servicios que en esta se prestan.

El servidor RADIUS soporta diferentes tipos de bases de datos como SQL, así como variados protocolos de autenticación como PAP, CHAP, EAP, etc.

2.2.3.2.2 EQUIPOS BRAS

A. Huawei [13]

El Quidway MA5200G es un equipo desarrollado por Huawei Technologies Co. Ltda., el cual cuenta con funciones como autenticación a nivel de usuario, políticas de control de acceso, calidad de servicio (QoS) y control *multicast* permitiendo al operador o proveedor de servicios mejorar la forma de administración de usuarios, seguridad y control de la provisión de un servicio.

Este equipo puede ser ubicado en la capa de acceso a la red permitiendo la administración de usuarios de acceso y la convergencia entre los extremos de la red. En la Figura 2.4 se muestra el diagrama de una aplicación del sistema.

El MA5200G posee tres series MA5200G-2, MA5200G-4 y MA5200G-8 cuya diferencia principal se encuentra en su rendimiento y capacidad de expansión. Cada uno se encuentra formado por un *backplane* pasivo, módulos para suministro de energía, ventiladores y tarjetas, mismos que pueden ser instalados en un chasis integrado de 19 pulgadas.

Dentro de la infraestructura de la empresa se cuenta con un equipo MA5200G-8 mismo que se muestra en la Figura 2.5. Este tiene una dimensión de 482.6 mm x 797.3 mm x 420 mm (ancho x alto x profundidad) y un peso aproximado de 85 Kg. Está conformado por dos *slots* SMU[36] y ocho *slots* SFU[37].

El MA5200G-8 cuenta con una velocidad de *backplane* de 256 Gbps y utiliza 64 Gbps de velocidad para SMUs, mismos que tienen una redundancia de respaldo

[36] Módulo de administración del sistema (SMU), permite la administración del sistema y sus recursos. Provee una interfaz de control y funciones como el mantenimiento del equipo, enrutamiento, intercambio de datos y señales del reloj. El sistema provee un puerto de red y/o dos puertos seriales para el mantenimiento del mismo.

[37] Módulo de servicio y transferencia (SFU), provee funciones de administración y control de acceso de usuarios. Ésta se encuentra equipada con procesadores de red (NP) e interfaces Ethernet, ATM, POS, CPOS (*Channelized* POS), CE1 y E3/T3.

de 1+1. En la Tabla 2.3 se presenta un resumen de las características técnicas del equipo.

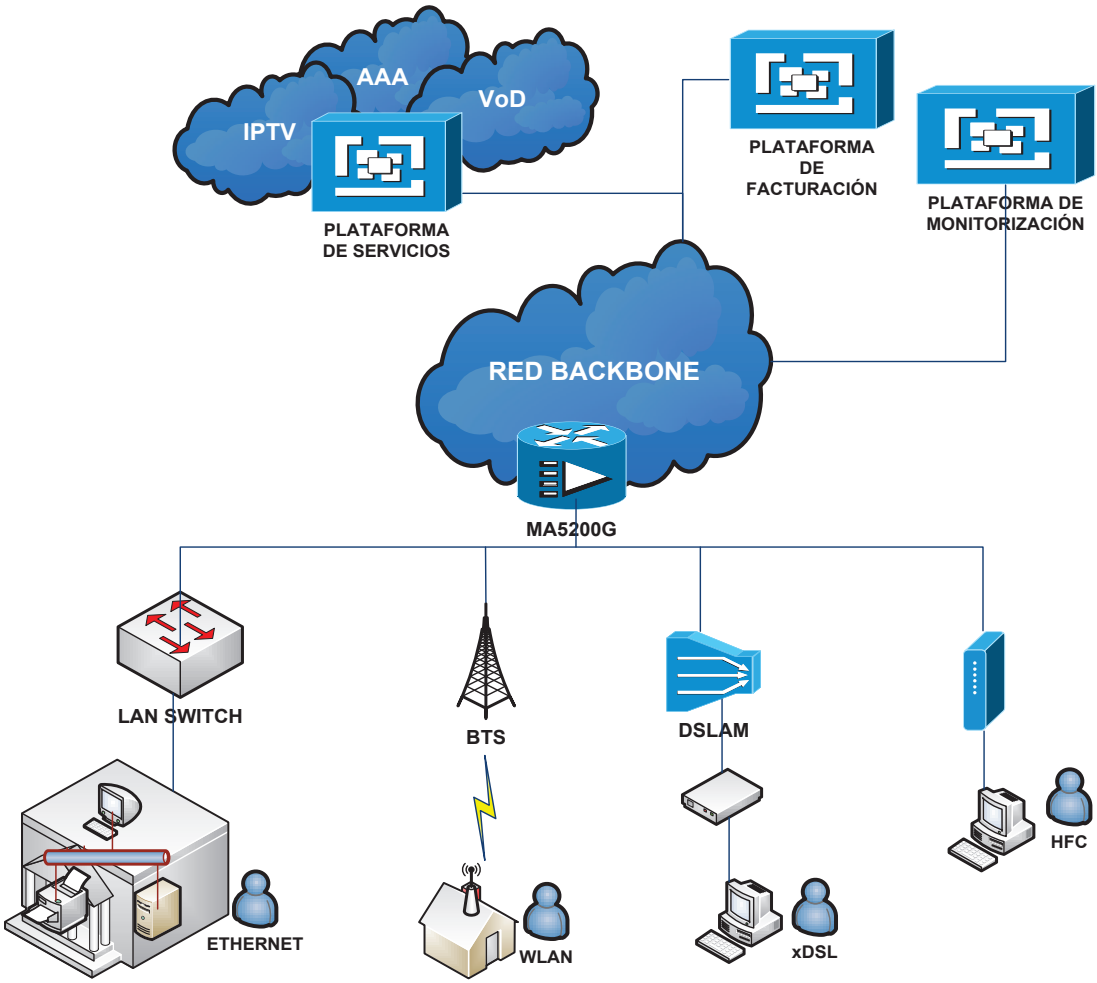


Figura 2.4. Aplicación de red del sistema MA5200G[38]

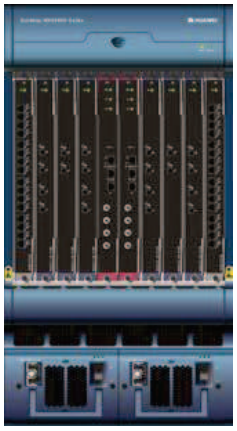


Figura 2.5. Infraestructura del equipo MA5200G-8

[38] Basado en [13]

CARACTERÍSTICAS ELÉCTRICAS	
AC	
Parámetro	**Valor**
Voltaje de Entrada	220 V / 110 VAC
Máxima Potencia de Salida	1.200 W x 2
Modo de Redundancia	1 + 1
DC	
Parámetro	**Valor**
Voltaje de Entrada	-48 VDC
Máxima Potencia de Salida	1200W x 2
Modo de Redundancia	1 + 1
REQUERIMIENTOS MEDIO AMBIENTALES	
Temperatura	Operación a largo plazo 5ºC a 45ºC
	Operación a corto plazo -5ºC a 55ºC
	De almacenamiento -40ºC a 60ºC
Humedad	10% a 95% (sin condensación)
Altitud	< a 4000 m
CARACTERÍSTICAS DE RENDIMIENTO	
Parámetro	**Valor**
Número de slots	10 slots (2 para SMU y 8 SFU)
Capacidad de conmutación de *backplane*	256 Gbps
Capacidad de conmutación de todo el equipo	64 Gbps
Número de usuarios concurrentes	8.000 usuarios por SFU, 48.000 por equipo
Protocolos de acceso de usuario	PPPoE, PPPoEoVLAN, PPPoEoA, PPPoA, IPoE, IPoEoVLAN, IPoEoA, IPoA, 802.1x y L2TP
Protocolo de autenticación de usuario	PAP, CHAP, MSCHAP, RADIUS y HWTACACS
Protocolo de autorización de usuario	RADIUS y HWTACACS
Protocolo de *accounting* de usuario	RADIUS y HWTACACS
Protocolos *multicast*	PIM-SM, PIM-DM, MBGP, MSDP, IGMP v1 e IGMP v2
Protocolos de enrutamiento	Rutas estáticas, RIP, OSPF, IS-IS y BGP
VLAN	4.000 por puerto Ethernet, 64.000 por tarjeta y 512.000 por equipo
PVC	64.000 por puerto ATM, 128000 por tarjeta y 512.000 por equipo
ISP	1.000
Pool de direcciones	4.000 (96.000 direcciones en total)
L2TP/LAC	8.000 sesiones por SFU, 16.000 túneles y 48.000 sesiones por equipo

CONTINÚA

CARACTERÍSTICAS DE RENDIMIENTO	
Parámetro	**Valor**
MPLS	10.000 LSPs por SFU
MPLS VPN	1000 VRFs
ACL	64.000 por SFU y 512.000 reglas
UCL	1.024 grupos de usuarios

Tabla 2.3. Características técnicas del equipo MA5200G-8

B. Ericsson

B.1. SE800 [15]

El SmartEdge 800 es un equipo desarrollado por la compañía Ericsson de Redback Networks y se lo observa en la Figura 2.6. Es una plataforma multi-funcional que consolida y simplifica la provisión de servicios a través de la red del operador pues integra funcionalidades como agregación Ethernet, enrutamiento de borde y administración de suscriptores.

Posee una arquitectura modular, y los procesos como el enrutamiento y la configuración son implementados de manera separada, es decir, en el caso de que alguno de éstos sufra algún daño puede ser reiniciado sin afectar a los demás procesos que se encuentren en ejecución evitando, así, un fallo de todo el sistema.

Figura 2.6. SmartEdge 800

Esta plataforma tiene diversas formas para procesar paquetes por ejemplo, clasificación o filtrado de paquetes basado en el puerto de ingreso, dirección IP de destino u origen, tipo de protocolo o puerto. Puede emplear listas de control de acceso para el proceso de selección de paquetes, así como incluir funciones de calidad de servicio para el tráfico que ingresa o sale del equipo.

La arquitectura del sistema es redundante para todas las componentes que afecten el tráfico; para esto posee dos tomas para la conexión eléctrica, y una protección de conmutación automática 1+1 para tráfico sobre las tarjetas SONET/SDH (POS).

Su chasis está diseñado para ser colocado en un *rack* de 19 a 23 pulgadas, y se encuentra conformado por 14 *slots*, dos de los cuales se emplea para el control del procesador y doce son para módulos de interfaces.

Soporta varios tipos de interfaz como Ethernet y ATM, los cuales son *hot-swap* (intercambiables en caliente). La mayoría de estas tarjetas son instaladas en la parte frontal a excepción de las tarjetas DS-3 y E3.

El equipo también posee una tarjeta controladora que es la encargada de manejar los protocolos de enrutamiento, la interfaz de línea de comandos (CLI) y las comunicaciones con el sistema de administración que ejecuta el sistema NetOp en la red. También carga la configuración requerida para el funcionamiento de las tarjetas que contienen las interfaces.

En la Tabla 2.4 se presenta un resumen de las características técnicas del equipo.

B.2. SE400 [16]

El SmartEdge 400 es un equipo desarrollado por la compañía Ericsson de Redback Networks y se lo observa en la Figura 2.7. De manera similar al SE800 es una plataforma multi-servicio que permite el aprovisionamiento de servicios de una manera confiable a través de la red.

CARACTERÍSTICAS ELÉCTRICAS	
Parámetro	**Valor**
Voltaje de Entrada	-40 a -57.6 VDC
Corriente Máxima	< 40 A
Potencia Máxima del Sistema	1.920 W
REQUERIMIENTOS MEDIO AMBIENTALES	
Temperatura	Operación a largo plazo 5ºC a 40ºC
	Operación a corto plazo -5ºC a 55ºC
Humedad	5% a 95% (sin condensación)
Altitud	3.048m
CARACTERÍSTICAS FÍSICAS	
Parámetro	**Valor**
Dimensiones del chasis	Altura: 15,75 pulgadas
	Ancho: 17,50 pulgadas
	Profundidad: 22 pulgadas
Peso del chasis	50 libras chasis vacío
	95 libras chasis con tarjetas
CARACTERÍSTICAS FÍSICAS	
Parámetro	**Valor**
Número de slots	14
Capacidad de conmutación de *backplane*	240 Gbps
Número máximo de usuarios	256.000
Número máximo de VLANS	256.000
Administración suscriptores de banda ancha	RADIUS, *Diameter*, Clientes IP estáticos o dinámicos
Encapsulación	PPP/HDCL, cHDCL, Ethernet, IEEE 802.1q, MPLS, 802.3ad, PPPoE, PPP sobre ATM
Protocolos *multicast*	PIM-SM, PIM-DM, MBGP, MSDP, SSM, IGMP v1, IGMP v2, IGMP v3, IPv6
Protocolos de enrutamiento	VRRP, RIP v2, OSPF v2, IS-IS y BGP
Calidad de servicio	802.1p (clase de servicio), *DiffServ*, Clasificación de paquetes según RFC 2474, 2475, 2697 y 2598.

Tabla 2.4. Características técnicas del equipo SE800

Su chasis se encuentra diseñado para ser colocado en un rack de 19 a 23 pulgadas, y está conformado por 6 *slots*, dos de los cuales se emplea para el control del procesador y cuatro son para módulos de interfaces.

Soporta varios tipos de interfaces como Ethernet y ATM. La mayoría de estas tarjetas son instaladas en la parte frontal a excepción de las tarjetas que poseen conectores BNC.

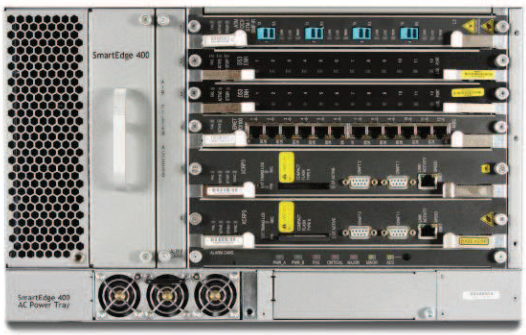


Figura 2.7. SmartEdge 400

En la Tabla 2.5 se presenta un resumen de las características técnicas del equipo.

Estos equipos (SE800 y SE400) son capaces de soportar de manera simultánea servicios como distribuidor de contenidos, *routers* virtuales, VPNs (Red Privada Virtual) y tráfico diferenciado permitiendo que la red del proveedor pueda garantizar un servicio de calidad e ininterrumpido al usuario.

En la Figura 2.8 se muestra el diagrama de una aplicación de estas plataformas.

2.2.3.2.3 Otras Plataformas

A. Plataforma Prepago [20]

La plataforma prepago que la empresa posee es de marca Huawei, Modelo UVC TELLIN. Entre las funcionalidades que esta posee se tiene:

- Permite ofrecer un servicio de recargas para usuarios prepago y de cobro de servicios para usuarios post-pago.
- Ofrece diversas formas de recargas por ejemplo el empleo de mensajes SMS, uso de tarjetas prepago.

- Ofrece seguridad proveyendo almacenamiento y transmisión de datos de las recargas cifrados.
- Permite que el operador administre y monitoree las transacciones realizadas y el tipo de tarjetas prepago que se emplearán.

CARACTERÍSTICAS ELÉCTRICAS	
Parámetro	**Valor**
Voltaje de Entrada	-38.4 a -57.6 VDC
Potencia Máxima	525 W
Potencia Máxima del Sistema	700 W
REQUERIMIENTOS MEDIO AMBIENTALES	
Temperatura	Operación a largo plazo 0ºC a 40ºC
	Operación a corto plazo -5ºC a 55ºC
Humedad	5% a 90% (sin condensación)
CARACTERÍSTICAS FÍSICAS	
Parámetro	**Valor**
Dimensiones del chasis	Altura: 8,75 a 10,5 pulgadas
	Ancho: 17,50 pulgadas
	Profundidad: 16 pulgadas
Peso del chasis	28 libras chasis vacío
	47 libras chasis con tarjetas
Número de *slots*	6
Capacidad de conmutación de *backplane*	80 Gbps
Número máximo de usuarios	128.000
Número máximo de VLANS	128.000
CARACTERÍSTICAS FÍSICAS	
Parámetro	**Valor**
Administración suscriptores de banda ancha	RADIUS, Clientes IP estáticos o dinámicos
Encapsulación	PPP/HDCL, cHDCL, Ethernet, IEEE 802.1q, MPLS, 802.3ad, PPPoE, PPP sobre ATM
Protocolos *multicast*	PIM-SM, PIM-DM, MBGP, MSDP, SSM, IGMP v1, IGMP v2, IGMP v3,
Protocolos de enrutamiento	VRRP, RIP v2, OSPF v2, IS-IS y BGP
Calidad de servicio	Políticas de ingreso y egreso, *DiffServ*, Clasificación de paquetes según RFC 2474, 2475, 2697 y 2598.

Tabla 2.5. Características técnicas del equipo SE400

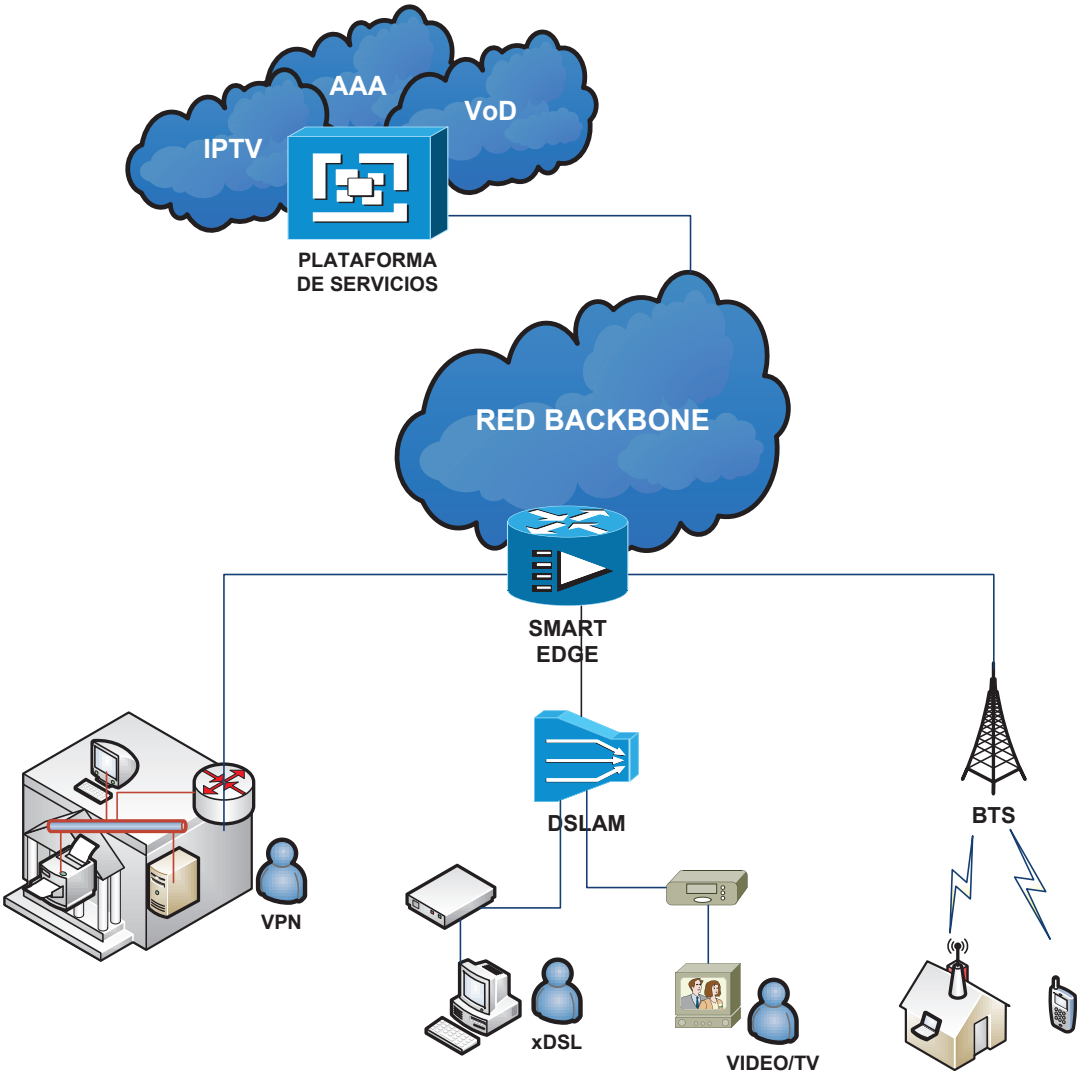


Figura 2.8. Aplicación de la plataforma SmartEdge[39]

B. PDSN 9660 [21]

Este equipo es de marca Huawei y trabaja como *gateway* entre la red PDN (*Packet Data Network* / Red de Paquete de Datos) y el sistema CDMA 2000, es decir, permite que un dispositivo móvil se conecte a una red IP y pueda acceder a sus funcionalidades y servicios. Entre las características de este dispositivo se tiene:

- Soporte de paquetes de datos del servicio prepago.
- Soporte protocolos de autenticación PAP y CHAP.

[39] Basado en [15]

- Puede soportar un total de 100 mil conexiones PPP activas simultáneamente, y un *throughput* máximo de 300 Mbps.
- Soporta calidad de servicio, clasificación de tráfico, control de congestión, políticas de enrutamiento.
- Posee interfaces: *Fast Ethernet*, *Gigabit Ethernet*, POS y ATM.
- Sus dimensiones son 800 mm de profundidad, 600 mm de ancho y 210 mm de altura.

C. WASN 9770 [22]

Este equipo de marca Huawei trabaja como *gateway* entre la red PDN (*Packet Data Network* / Red de Paquete de Datos) y el sistema WiMAX permitiendo de esta manera el acceso a diversas funcionalidades y servicios de una red IP. Entre las características de este dispositivo se tiene:

- Soporte protocolos de autenticación PAP, CHAP y EAP.
- Posee mecanismos de filtrado de paquetes y lista de control de acceso (ACL).
- Soporta el protocolo de seguridad IP.
- Posee interfaces: Ethernet, GBIC Ethernet (*Gigabit Interface Converter* / Convertidor de Interfaz Gigabit).

2.2.4 DESCRIPCIÓN DE CLIENTES

Los clientes banda ancha que se autentican en el sistema BRAS/AAA de la Corporación Nacional de Telecomunicaciones se los puede clasificar, de manera general, en:

- PPPoE.[40]
- PPPoE con IP FIJA.

[40] PPPoE: Protocolo Punto a Punto sobre Ethernet.

- PPPoE con dominio.

La diferencia entre los clientes PPPoE y cliente PPPoE con IP fija básicamente radica en la forma en que se les asigna la dirección de red al usuario, los primeros la obtienen de una manera dinámica mientras que a los segundos se les asigna una dentro de un rango definido y se mantiene constante en cualquier momento que el usuario se conecte a la red. Por otro lado, los clientes PPPoE con dominio son suscriptores masificados de otros ISPs que emplean de la infraestructura BRAS/AAA de la CNT para autenticarse.

El nombre que se les asigna a los clientes se encuentra basado en el tipo de conexión que estos tienen para acceder a la red, la cual está basada en el protocolo punto a punto (PPP).

Originalmente, el protocolo punto a punto define una conexión directa entre dos dispositivos, es empleado por los proveedores de servicio de Internet para permitir que usuarios que empleen conexiones telefónicas (*dial up*) accedan a Internet, dependiendo del medio se puede tener PPP sobre ATM (PPPoA), PPP sobre Ethernet (PPPoE) o PPP sobre SONET/SDH (POS).

Una conexión PPPoE permite la comunicación entre dos puntos de red (computadores, nodos) mediante el uso de un protocolo de red que tiene encapsulación PPP sobre la capa Ethernet como se muestra en la Figura 2.9. Generalmente las conexiones se concentran en un equipo como un DSLAM o un *router* extremo antes de tener acceso a los servicios de la red.

En el establecimiento de la conexión punto a punto se puede distinguir los siguientes pasos:

- Se establece un enlace punto a punto.
- Se realiza una autenticación del usuario.
- Se asigna una dirección de red o dirección IP al usuario.

- Se permite el acceso del usuario a los recursos o servicios de la red a los que tenga permiso.
- Se monitorea la conexión para verificar si el usuario sigue o no conectado a la red.

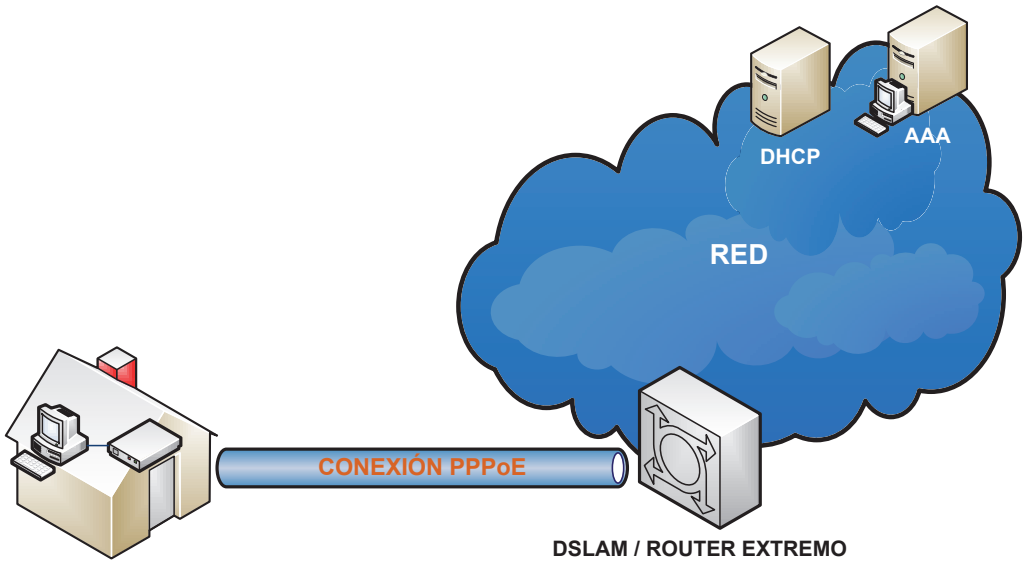


Figura 2.9. Diagrama de una conexión PPPoE

2.2.4.1 Clientes Actuales

Las plataformas AAA son las que se encargan de administrar a los diversos clientes y el número de éstos se encuentra condicionado al número de licencias que cada uno de los sistemas posea. En la Tabla 2.6 se indica las licencias que la empresa tiene disponibles por cada plataforma AAA.

UBICACIÓN	PLATAFORMA AAA	NÚMERO DE LICENCIAS
Zona Andina	iTELLIN	60.000
	NetOp	90.000
	InfoX (WiMAX)	15.000
Zona Pacífico	InfoX	27.000
	NetOp	10.000
	FreeRADIUS	10.000
	InfoX (CDMA)	26.000

Fuente: Corporación Nacional De Telecomunicaciones

Tabla 2.6. Número de licencias por plataforma AAA

CAPÍTULO 3

DESCRIPCIÓN DE UNA SOLUCIÓN DE SISTEMA AAA CENTRALIZADO

3.1 INTRODUCCIÓN

En la actualidad, existe una gran demanda de usuarios que acceden a Internet debido a la diversidad de servicios que se ofrecen por medio de éste, provocando que los proveedores de servicio deban modificar su infraestructura para poder satisfacer las necesidades de sus clientes. Esto conlleva a que la red requiera de un control de acceso adecuado hacia sus recursos y servicios.

En el presente capítulo se realizará una descripción de las funcionalidades de un sistema centralizado AAA el cual permita crear una arquitectura de red de banda ancha inteligente, con mayores opciones de administración orientadas a mejorar los procesos y facilitar al usuario nuevos servicios basados en las mismas.

Además, a partir del análisis de los requerimientos se planteará una solución para el sistema centralizado AAA.

3.2 DESCRIPCIÓN DE LA SOLUCIÓN AAA

Para determinar las características que la solución debe poseer, dentro de la empresa se procedió a realizar reuniones con personal del área durante las cuales se expusieron diversos criterios en cuanto al funcionamiento de las plataformas existentes y su interacción para brindar el servicio AAA a los usuarios, así como las experiencias adquiridas durante la implementación del sistema AAA existente actualmente. En base a esto se procedió a determinar los requerimientos que el sistema AAA centralizado debería poseer para garantizar el cumplimiento de las funcionalidades expuestas.

A continuación se expone un resumen de las principales funcionalidades analizadas y las características que debe poseer el sistema AAA centralizado, en base a las necesidades de la empresa.

3.2.1 ANÁLISIS DE FUNCIONALIDADES

El sistema AAA actual de la CNT se encuentra distribuido en diferentes plataformas las mismas que están ubicadas en diferentes nodos a nivel nacional. Cada una administra cierta cantidad de usuarios, controla el acceso a los recursos de la red, refuerza políticas, audita el uso de sus recursos y provee de la información necesaria para la facturación de un servicio.

En la actualidad, la afluencia de nuevos servicios que se ofrecen a través de una red de datos ha ocasionado que los operadores deban mejorar la infraestructura de su red para evitar que se presenten problemas como limitaciones en ciertos recursos de la red, además de brindar seguridad.

Para mejorar la provisión de estos servicios se requiere de una plataforma en la que se pueda diferenciar usuarios y servicios, y facilitar el monitoreo y asignación de los recursos de red para de esta manera poder implementar y mejorar varios servicios como los de valor agregado y permitir su personalización de acuerdo a las necesidades del usuario.

Para poder satisfacer estas necesidades se puede implementar una solución centralizada para el control de los recursos de red la cual permita aprovisionar los servicios y usuarios, diferenciar y personalizar los recursos de red, examinar y monitorear tanto los usuarios como el tipo de tráfico que cursa sobre esta, controlar la calidad de servicio y brindar seguridad mediante el control de acceso hacia sus recursos.

De esta manera se podría tener una infraestructura inteligente que permita al operador administrar los recursos de toda la red, conforme los requerimientos de sus clientes garantizando la provisión adecuada de un servicio.

La centralización del sistema AAA facilitaría la administración de usuarios de banda ancha pertenecientes a diferentes tecnologías de acceso. En el caso de la empresa, permitiría integrar clientes xDSL, WiMAX y CDMA450.

En la actualidad, el sistema AAA brinda servicio a clientes post-pago entre los que se puede tener usuarios residenciales (*fast boy*) y corporativos, a los cuales se les concede un dominio y para su navegación se les puede asignar una dirección IP de manera dinámica o estática, o un conjunto de direcciones IP dependiendo del plan contratado. En la región Pacífico existe un grupo de clientes que no emplean dominio para el proceso de autenticación, éstos se encuentra configurados en una plataforma FreeRADIUS.

Por otro lado, la empresa pretende extender su mercado hacia usuarios prepago razón por la cual el sistema deberá soportar el manejo de este tipo de usuarios quienes mediante el uso de una tarjeta podrán acceder a los recursos y servicios de la red. Su consumo debe ser descontado en línea del saldo otorgado por la tarjeta.

Dadas estas características el sistema AAA debe poder integrarse con el sistema de facturación (usuarios post-pago) y la plataforma prepago (usuarios prepago) permitiendo de esta manera al operador generar el cobro del servicio. Para esto el sistema debe ser capaz de generar CDRs en los cuales se almacenará la información necesaria para dicha tarifación.

Adicionalmente debe soportar el uso de portales o páginas de web ya que éstos permitirán a los usuarios acceder a diversos servicios que se oferten en la red. Entre las funcionalidades o acciones a las que tendrá acceso un usuario se tiene:

- Revisión de su plan comercial.
- Obtener un reporte del histórico de conexiones de su cuenta.
- Modificación de su ancho de banda.

Todo cambio que el usuario realice a través del portal debe verse reflejado de manera automática al sistema de facturación o a la plataforma prepago de acuerdo al tipo de cliente.

El sistema debe poseer también de mecanismos para el control de tráfico y seguridad; en base a esto éste debe permitir la implementación de políticas de calidad de servicio mediante las cuales el operador pueda definir prioridad en la transmisión de información. Esto permitirá diferenciar a los usuarios por categorías otorgando un privilegio mayor a ciertos clientes, principalmente cuando existan fallas en la red.

Dentro del manejo de políticas se debe considerar la implementación de funcionalidades como control parental, filtrado de contenido y de URLs, control y análisis del tráfico de servicios que circula por la red, así como el control de ancho de banda requerido por una aplicación. De esta manera se podrán ofrecer servicios de valor agregado como video bajo demanda, televisión y ancho de banda bajo demanda.

El sistema debe ser escalable y ofrecer una alta disponibilidad para asegurar que un usuario siempre pueda autenticarse, es decir, en caso de cualquier desastre la operación del sistema AAA se debe mantener, para esto se requiere que todo el sistema posea redundancia.

Las funcionalidades antes descritas permitirán determinar las características de la solución AAA que la empresa necesita y de esta manera poder generar una arquitectura de banda ancha inteligente que se acople a un nuevo modelo de negocio que se desea implementar a futuro en la empresa el cual permitirá adicionar nuevos servicios y la administración de los mismos por parte del usuario.

3.2.2 REQUERIMIENTOS DEL SISTEMA

En base a las funcionalidades que el sistema AAA tiene actualmente y las que se desean implementar se han obtenido los siguientes requerimientos:

3.2.2.1 Requerimientos para la Interconexión

La empresa requiere de un sistema AAA centralizado que permita implementar las funciones de autenticación, autorización y contabilidad para clientes provenientes de diversas redes de acceso como xDSL, WiMAX y CDMA. Éste debe permitir integrar las siguientes plataformas existentes en la empresa:

- BRAS
    - Marca Redback modelos SE800 y SE400.
    - Marca Huawei modelo MA5200G-8.
- PDSN de la red CDMA450 marca Huawei, modelo PDSN 9660.
- Plataforma prepago marca Huawei, modelo UVC TELLIN.
- Plataforma de facturación conformada por los aplicativos OPEN/AXIS.

Para que el sistema AAA pueda interactuar con las plataformas señaladas, éste debe poseer y/o soportar para su comunicación con las mismas los siguientes protocolos:

- Al protocolo RADIUS conforme el RFC 2865[41], RFC 2866[42] y sus extensiones lo cual permitirá la integración de los BRAS hacia el sistema AAA. Se escoge este protocolo, en base a los RFCs señalados, dado que este protocolo es el que actualmente se emplea en la comunicación entre estos equipos, además de su capacidad de notificar cuando comienza y

[41] RFC 2865 describe la manera en que se emplea el protocolo RADIUS para brindar un servicio de autenticación y autorización de un NAS con el servidor.

[42] RFC 2866 describe la manera en la que el protocolo RADIUS trabaja con la información de *accounting* para la tarifación de un servicio.

termina una conexión permitiendo de esta manera determinar y facturar el consumo de un usuario.

- Al protocolo *Diameter* según el RFC 3588[43] y RFC 4005[44] para su integración con la plataforma prepago. Se escoge este protocolo, en base a los RFCs señalados, dado que se lo emplea en la comunicación entre estos equipos; además de que permitirá la interacción entre estos u otros equipos cuando el protocolo RADIUS no sea soportado de una manera adecuada en situaciones como el acceso remoto y movilidad IP.

- Al protocolo FTP[45] y/o *Web services*[46] para la integración con la plataforma de facturación. Se escoge este protocolo dado que es el actualmente se emplea en la comunicación entre estos equipos.

- Al protocolo RADIUS con IPv6, ya que a futuro debe poder interactuar con diversos equipos que manejen direcciones de red IPv6, dado que la tendencia actual por el crecimiento de número de usuarios que se tiene requieren que trabajen tanto con direccionamiento IPv4 como con IPv6.

- RADIUS *Proxy*[47], se adiciona esta funcionalidad ya que permitirá que el sistema AAA se comunique con otras plataformas AAA, por ejemplo éstas pueden ser de respaldo principalmente cuando existan fallos en la red.

En la Figura 3.1 se puede observar la integración que se desea entre la solución AAA y las plataformas antes mencionadas. Las peticiones de autenticación de los usuarios de banda ancha xDSL y WiMAX llegarán a través de los BRAS, mientras

[43] RFC 3588 especifica como proveer servicio AAA a aplicaciones IP móviles y de acceso a la red mediante el protocolo *Diameter*.

[44] RFC 4005 especifica los requerimientos para permitir la interacción entre el protocolo *Diameter* y el protocolo RADIUS. Se lo puede considerar una extensión al RFC 3588.

[45] FTP (Protocolo de Transferencia de Archivos) permite transferir archivos de manera confiable. Promueve la compartición de archivos y el uso de dispositivos de forma remota. [1]

[46] *Web services* es una tecnología diseñada para soportar la interacción dispositivo a dispositivo sobre una red, es decir, permite que las aplicaciones o servicios puedan interactuar entre sí sin la necesidad de intervención humana. [2]

[47] RADIUS *proxy* permite la redirección de un paquete hacia otro servidor RADIUS para que lleve a cabo el proceso de autenticación. Esta funcionalidad es útil cuando existe fallos en la red y el servidor principal queda incomunicado, las peticiones se dirigirán hacia un servidor de respaldo.

que, las solicitudes de los usuarios de datos de la red CDMA450 llegarán por medio de la PDSN. En los dos casos la comunicación se efectuará mediante el protocolo RADIUS. La integración con la plataforma de tarifación se ejecutará mediante los protocolos *Diameter*, FTP y *Web Services* lo cual permitirá la facturación del consumo del servicio al usuario.

3.2.2.2 Requerimientos para Manejo de Usuarios

El sistema AAA actual permite la asignación de direcciones IP tanto de manera estática como dinámica a un usuario dependiendo del tipo de plan que tenga contratado. Las direcciones IP se encuentran dentro de un conjunto de direcciones, mismas que pueden estar separadas por dominios y de las cuales un usuario puede recibir una dirección o un pool de direcciones. En base a esto, la solución AAA centralizada debe permitir la asignación estática o dinámica de direcciones IP, así como la designación de una sola dirección IP o un pool de direcciones IP a los suscriptores.

Por otro lado, dado que se tienen usuarios con diferentes dominios como @andinanet, el sistema AAA debe permitir la creación de dominios, ya que por ejemplo puede darse el caso que se asigne un mismo nombre de usuario a otro cliente pero con un dominio diferente, en este caso el sistema debe admitir el acceso a la red a un mismo usuario pero con diferente dominio.

Se debe considerar también que existen ciertos clientes que acceden a la red empleando en su autenticación solamente el nombre de usuario sin su dominio razón por la cual el sistema AAA debe poder autenticar suscriptores cuyos nombres de usuarios no posean dominio.

Dado que se desea implementar el manejo de usuarios prepago, el sistema AAA debe ser capaz de soportar el manejo de una tarjeta prepago para acceder a los servicios de la red. La facturación para este tipo de usuarios debe realizarse en tiempo real descontando el consumo en línea del total que se indica en cada tarjeta.

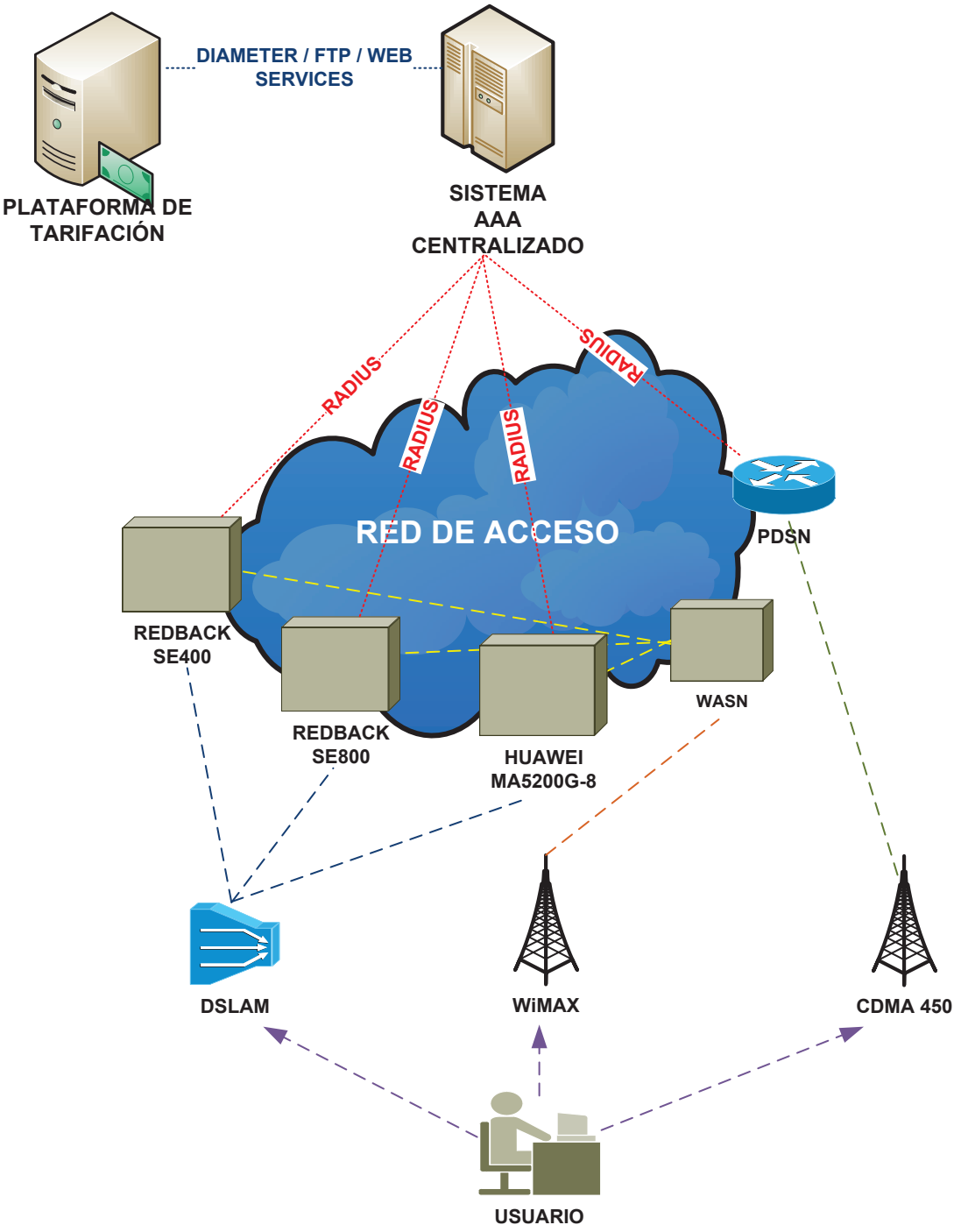


Figura 3.1. Integración del sistema AAA centralizado con las plataformas existentes en CNT

El sistema AAA actualmente maneja usuarios post-pago y almacena los datos sobre el consumo que cada uno de ellos genera en un CDR. Esta información a su vez se envía al sistema de tarifación para la generación de la factura y posterior cobro del servicio al cliente. Un CDR guarda datos como dirección IP asignada, fecha y hora de inicio y fin de la conexión y cantidad de datos que se

transmitieron y recibieron. El sistema AAA que se propone debe poder generar y almacenar CDR para el manejo de usuarios post-pago y prepago, de manera similar al proceso que se realiza con la plataforma actual.

3.2.2.3 Requerimientos de Alta Disponibilidad

El sistema AAA centralizado debe poseer una alta disponibilidad debido a que tiene que estar funcionando 24 horas al día, los 365 días del año, atendiendo las peticiones de los usuarios que se encuentran a nivel nacional; por lo tanto la solución para este sistema debe contemplar técnicas que le permitan asegurar su correcto funcionamiento dado que es uno de los equipos que se consideraría crítico dentro de la red.

Una manera de brindar alta disponibilidad es mediante la aplicación de redundancia a nivel de hardware. Para aprovechar la infraestructura que la empresa posee, ya que actualmente los centros de gestión y la infraestructura de los sistemas AAA que la empresa tiene se encuentran ubicados en Quito y Guayaquil y cada uno de estos recibe y maneja las peticiones de autenticación de los clientes de acuerdo a la zona en donde se ubican, se debe considerar brindar una redundancia geográfica de manera tal, que si falla el sistema AAA de Quito las peticiones de autenticación se re-direccionen al sistema AAA de Guayaquil o viceversa permitiendo que el usuario siempre se pueda autenticar en caso de cualquier desperfecto.

Por otro lado, dado que el sistema AAA maneja bases datos para el almacenamiento de diverso tipo de información relacionada con los clientes se debe considerar también la implementación de una solución que brinde protección ante fallas a las bases de datos para asegurar la integridad y fiabilidad de los datos almacenados, además de ofrecer una alta disponibilidad para el acceso a los mismos.

Para esto se considerará una base de datos de producción única, y al igual que el sistema AAA la base de datos principal se ubicara en Quito y su respaldo en Guayaquil. Las bases de datos deben trabajar de preferencia en la plataforma

Oracle ya que sobre ésta plataforma se encuentran las bases que la empresa posee.

Además, se debe considerar que el sistema sea escalable para asegurar su crecimiento futuro, y ofrecer confiablidad para asegurar que un usuario pueda autenticarse y acceder a los servicios de la red aun cuando existan fallos en el sistema.

3.2.2.4 Requerimientos para Autenticación de Usuarios [3]

Actualmente, el sistema AAA realiza la autenticación de sus usuarios, a través de los NAS, mediante el uso de los protocolos PAP y CHAP empleando un nombre de usuario y contraseña.

Para el sistema AAA centralizado se debe considerar que este permita la autenticación mediante los protocolos PAP, CHAP y EAP[48] el cual se encuentra definido en el estándar IEEE 802.1x para seguridad en redes inalámbricas.

Por otro lado como el sistema AAA debe permitir la autenticación de usuarios de la red CDMA, en base a los requerimientos señalados en el RFC 3141[49] la solución debe poder operar de las siguientes formas:

- *Access Network AAA (AN-AAA):* permite habilitar las funciones de autenticación y autorización en el acceso a la red.
- *Broker AAA (B-AAA):* actúa como un intermediario que envía el tráfico y provee seguridad entre redes *roaming*, es decir, entre el H-AAA y V-AAA.

[48] EAP (Protocolo de Autenticación Extensible) es un protocolo empleado en redes inalámbricas y conexiones punto a punto desarrollado en base a la creciente demanda de métodos de autenticación que utilizan dispositivos de seguridad como las tarjetas inteligentes o de identificación. [4]

[49] RFC 3141 describe la arquitectura de una red de datos inalámbrica CDMA2000 diseñada como medio de acceso a una red celular, además especifica requerimientos para soportar autenticación, autorización y contabilidad.

- *Home AAA (H-AAA):* almacena información del perfil y facturación del suscriptor, y responde a solicitudes de autenticación. Se encuentra en la red origen del cliente.
- *Visited AAA (V-AAA):* permite brindar servicio a un usuario que se encuentra en estado de *roaming* enviando su información de perfil y facturación a su red origen.

3.2.2.5 Requerimientos de Políticas de Calidad de Servicio [5] [6]

Debido a que el sistema AAA centralizado va a manejar nuevos servicios, este debe permitir la implementación de políticas de calidad de servicio las cuales garanticen que el suscriptor reciba de manera adecuada los mismos.

Para la implementación de estas políticas se puede enfocar en varios puntos de acuerdo a los requerimientos que se consideren necesarios para la oferta de nuevos servicios dentro del modelo de negocios de la empresa pretende implementar en el futuro, entre éstos se tiene la asignación del ancho de banda en forma diferenciada, manejo de prioridades de acuerdo al tipo de servicio que se ofrezca y la prevención de congestión en la red.

Para una correcta provisión de administración de estos servicios se pueden tomar a consideración las siguientes políticas de calidad de servicio.

3.2.2.5.1 Filtrado de Contenido

El filtrado de contenido permite determinar qué tipo de tráfico puede acceder a los recursos de la red ya sea de manera definitiva o en periodos de tiempo, por ejemplo se podría configurar que el tráfico P2P no sea permitido en horas de la tarde provocando que cuando el sistema detecte este tipo de tráfico dentro del periodo establecido simplemente lo bloquee.

Dentro de esta opción se podría considerar también el filtrado de URL, mediante las cuales el operador podría determinar el tipo de información a la que un usuario

accede de manera constante y de esta manera mejorar su servicio u ofrecerle servicios que podrían complementar los que ya emplea.

Esta opción permitiría también crear grupos de usuarios a los cuales no se les permita acceder a cierto tipo de información permitiendo de esta manera implementar la funcionalidad de control parental.

A. Control de Tráfico de Servicios

Para poder determinar el tipo de tráfico que cursa por la red, y de esta manera implementar funcionalidades como el filtrado de contenido, se debe poseer el equipamiento necesario para implementar la funcionalidad DPI (Inspección Profunda de Paquetes / *Deep Packet Inspection*), la cual es una tecnología que permite inspeccionar, en tiempo real, el contenido de un flujo de tráfico que atraviesa la red. Se la puede encontrar en *routers* o equipos de *hardware* dedicado, mismos que pueden ser instalados dentro o en el borde de la red.

Por otro lado, la implementación de la tecnología DPI puede ofrecer a la red del operador un mecanismo de seguridad ya que debido a sus funcionalidades permite detectar el tráfico malicioso que puede ser generado en el Internet y puede afectar al usuario y a la red.

3.2.2.5.2 Control de Ancho de Banda

El control del ancho de banda permite el ajuste del ancho de banda de acuerdo a las necesidades de un servicio de manera tal que el ancho de banda asignado no sobrepase el ancho de banda total de la red.

Dado que la administración del ancho de banda en una red se encuentra relacionada con el rendimiento que esta tenga en el manejo del tráfico, el control de la congestión que exista sobre esta, permitirá trasmitir información en base a un nivel de prioridades y de esta manera se garantizará que usuarios de alto nivel o servicios especiales tengan acceso a los recursos de la red sin inconvenientes.

El manejo de la congestión puede ser realizado empleando métodos de encolamiento como encolamiento de prioridad[50] y encolamiento equitativo ponderado[51] en las cuales se da prioridad a cierto tipo de tráfico como el generado por IPTV para que experimente la menor latencia posible.

3.2.2.5.3 Gestión de Umbrales

Gestión de umbrales de servicio (limitación en el uso de un servicio) basado en su duración o volumen de descarga.

3.2.2.5.4 Caching

La técnica de *caching* consiste en colocar un dispositivo de caché entre los clientes y los servicios a los que éstos tratan de acceder. En el equipo caché se almacena una copia de la información o aplicación más utilizada por los clientes. Permite un ahorro del ancho de banda ya que si un usuario realiza una petición a una información ya consultada o empleada, ésta es enviada desde el equipo caché al usuario sin la necesidad de emplear recursos extras para su obtención.

El intercambio de información correspondiente a las políticas entre los equipos que conformen la solución AAA se lo realiza por medio del protocolo COPS[52] razón por la cual se debería considerar también que el sistema AAA soporte este protocolo.

3.2.2.6 Requerimientos de Seguridad

Dado que la seguridad en una red permite proteger la información que por esta circula de amenazas o ataques que pueden alterar el funcionamiento de la red así como acceder a la información y robarla.

---

[50] *Priority Queuing* / Encolamiento de Prioridad (PQ): permite la clasificación de colas en base a prioridades. Se atiende primero a los paquetes pertenecientes a la cola con la mayor prioridad.

[51] *Weighted Fair Queuing* / Encolamiento Equitativo Ponderado (WFQ): permite organizar el tráfico y lo asigna a una cola a la cual luego se le asigna un ancho de banda para ser trasmitida. Se prioriza el tráfico que tenga una mayor sensibilidad al retardo.

[52] Referencia a capítulo 1.

El sistema AAA centralizado debe poseer mecanismos de seguridad, principalmente dirigidos a evitar ataques de denegación del servicio (DoS, *Denial of Service*), ya que éste permitirá la autenticación de los usuarios para el acceso a la red y sus servicios. Además estos tipos de ataques son los que más afectan a las redes de datos en la actualidad, provocando que éstas queden inaccesibles debido a la pérdida de conectividad que afronta la red por el consumo de recursos que genera la sobrecarga de información que le transmite el atacante.

3.2.2.7 Requerimientos para Gestión

Para que el administrador de la red pueda gestionar de manera adecuada el sistema AAA, éste debe permitir su gestión de manera gráfica para facilitar el aprovisionamiento y administración de usuarios y servicios, y por medio de CLI (*Command Line Interface* / Línea de Comandos) para acceso al sistema por medio de consola cuando sea necesario.

Además debe poseer una aplicación que permita obtener estadísticas y reportes del tráfico generado por los suscriptores y los servicios en la red, para de esta manera permitir un monitoreo de la plataforma y determinar, de ser el caso, si se requiere de un rediseño de la solución para ampliar los recursos de ésta.

3.2.2.8 Requerimientos para Interacción con el Usuario

Como parte de la solución, para obtener una red inteligente banda ancha, a futuro la empresa desea implementar la funcionalidad de auto-aprovisionamiento por parte del usuario mediante la cual sea éste quien administre los diversos servicios que posea o desee contratar, o simplemente consulte el estado de su cuenta. Esto lo realizará por medio del acceso a portales que permitan dicha interacción.

Para esto el sistema AAA centralizado debe poder manejar portales, los mismos que permitan la interacción del usuario y sea éste quien realice un auto-aprovisionamiento del servicio deseado. A continuación se detallan los portales que se deben desarrollar para poder tener esta funcionalidad en la red.

- *Portal cautivo*: permite que los usuarios dentro de un dominio o característica específica sean re-direccionados a una IP o URL definida.
- *Portal de autenticación*: permite el registro del suscriptor para el acceso a los servicios de la red, para esto debe ingresar el nombre de usuario y la contraseña mismos que le permitirán autenticarse en el sistema.
- *Portal de error:* se muestra cuando el usuario ingresa los datos de nombre de usuario y contraseña erróneamente e indica al mismo la información específica del error y sobre su correspondiente soporte para corregirlo.
- *Portal de auto-aprovisionamiento*: permitirá al suscriptor gestionar su cuenta, por ejemplo realizar cambios relacionados a la información del usuario, consultar su saldo, modificar su ancho de banda, recargar se servicio prepago, entre otros.

La interacción del usuario con el portal para acceder a los servicios de la red se detalla a manera general a continuación, y el proceso se indica en la Figura 3.2.

1. El usuario solicita su ingreso a la red, para esto su petición ingresa por medio del BRAS y es redirigida hacia un portal de autenticación.
2. En el portal el usuario procede a ingresar su nombre de usuario y contraseña.
3. La información ingresada es enviada al sistema AAA para proceder con la autenticación. Si ésta se realiza con éxito se le presenta al usuario un portal de auto-aprovisionamiento, el cual emitirá información sobre su cuenta y los diversos servicios que puede contratar.
4. Una vez seleccionado el servicio, el portal envía esta información al sistema AAA y este a su vez remite al BRAS las políticas a aplicar para proporcionar el servicio al usuario.
5. Una vez establecidas las políticas en el BRAS, el usuario puede acceder al servicio o servicios de la red hasta cuando éste termine la sesión (se

desconecte) o haya consumido en su totalidad el valor de su tarjeta prepago.

6. Para la facturación del servicio, el BRAS es el que debe enviar la información de duración del mismo hacia el sistema AAA y éste a su vez debe generar los CDRs correspondientes y enviarlos al sistema de tarifación.

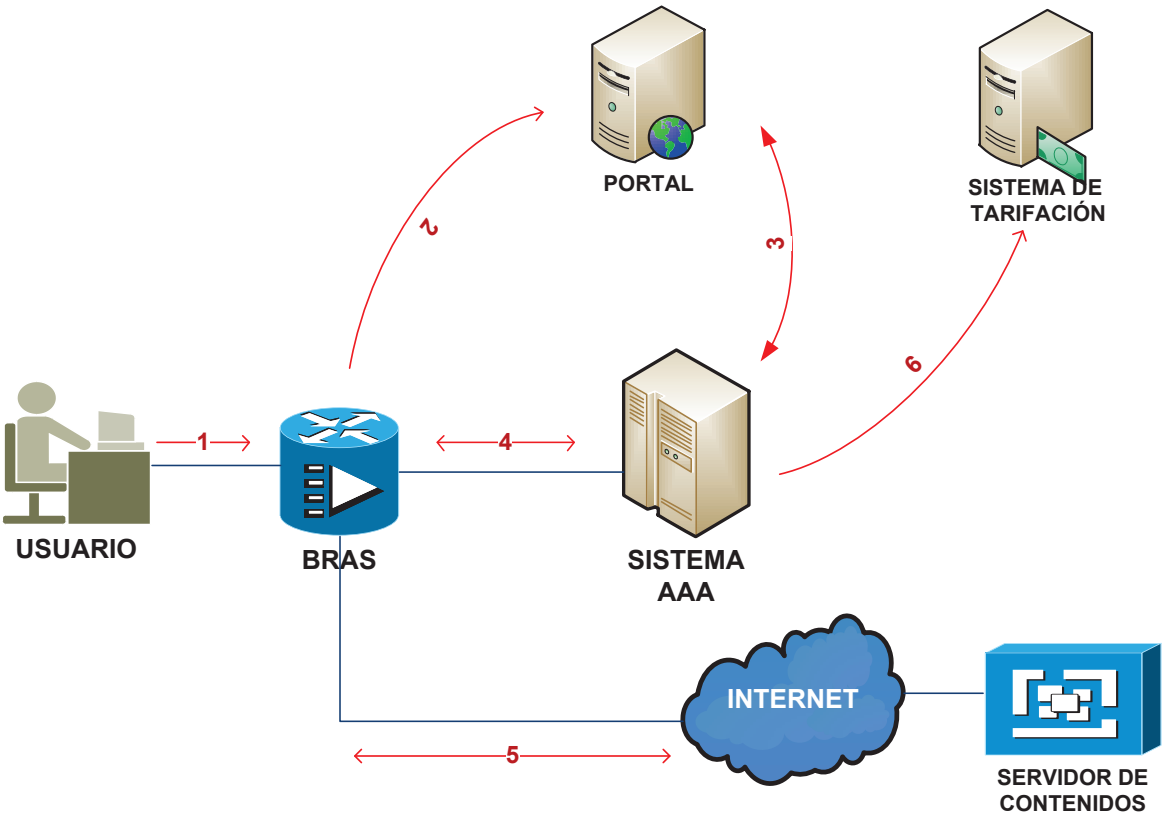


Figura 3.2. Interacción de un usuario con el portal para el acceso a un servicio

3.2.2.9 Requerimiento de Cuentas de Usuario

Para definir el número de cuentas de usuario que se establecen como requerimiento inicial al dimensionamiento del proyecto se consideraron variables técnicas, comerciales, de licenciamiento y políticas.

3.2.2.9.1 Plan de Nacional de Conectividad

En el Plan Nacional de Conectividad[53] promulgado en el año 2007 se plantea como una de sus políticas el desarrollar la infraestructura para la provisión de acceso a Internet cuya meta es lograr una densidad de banda ancha fija del 7% en el territorio nacional, que son aproximadamente un millón de usuarios, de los cuales 690 mil deberán ser manejados por operadores estatales.

Este plan forma parte de una serie de políticas trazadas dentro del Plan de Desarrollo de las Telecomunicaciones del Ecuador cuyo objetivo es impulsar el sector de las telecomunicaciones en el país cuya vigencia se estima hasta el año 2013 en el cual finaliza el período de presente gobierno pero puede ampliarse durante 4 años más, dependiendo de la posibilidad de un nuevo período gubernamental.

3.2.2.9.2 Proyección de Crecimiento de Usuarios

Siendo que la variable de crecimiento planteada en el Plan Nacional de Conectividad es una medida netamente política hace falta realizar un cálculo técnico que muestre un valor más real del verdadero crecimiento que puede llegar a darse a futuro, para ello se plantea una proyección de crecimiento de usuarios basada en datos del número de usuarios registrados en trimestres anteriores.

En la Tabla 3.1 se presentan los datos de cuentas y usuarios correspondientes a los años 2010, 2011 y 2012; se tomará principal atención a las cuentas dedicadas, puesto que estas contemplan los clientes que tienen acceso a Internet banda ancha quienes a su vez podrían acceder a los servicios banda ancha ofertados, además permitirían determinar la capacidad de los equipos a ser adquiridos.

Al analizar los datos presentados en la tabla anterior se observa que el crecimiento del número de usuarios tiene un aumento constante, por lo que para

[53] Anexo B

determinar el número de usuarios potenciales que existen en el mercado para esta nueva tecnología se considera que una proyección de tipo lineal sería la adecuada.

En la Figura 3.3 se puede observar la tendencia de crecimiento proyectada a cinco años para los datos correspondientes al valor de las cuentas dedicadas de los datos obtenidos de la Superintendencia de Telecomunicaciones. Como puede observarse la tendencia de crecimiento señala que en un período de 5 años (20 trimestres) el número de usuarios alcanzaría un aproximado de 600 mil, que es una medida más real del número de usuarios que el sistema AAA debe sostener en su totalidad.

	DICIEMBRE 2010	DICIEMBRE 2011	DICIEMBRE 2012
Cuentas Conmutadas	2.524	1.796	1.371
Cuentas Dedicadas	247.340	354.378	478.059
Cuentas Totales	249.864	356.174	479.430
Usuarios Conmutados	10.096	7.184	5.484
Usuarios Dedicados	1.228.930	1.895.993	2.721.602
Usuarios Totales	1.239.026	1.903.177	2.727.086

Dónde:

Cuentas conmutadas: **son cuentas de Internet en las que el usuario debe realizar la acción de marcar a un número determinado, ya sea por medio de las redes de telefonía fija o móvil, para acceder al servicio.**

Cuentas dedicadas: **son cuentan que utilizan otros medios para acceder a Internet por ejemplo ADSL, cable módem, etc.**

Usuarios conmutados: **se estima que por cada una de estas cuentas cuatro usuarios.**

Usuarios dedicados: **número total de usuarios que los Proveedores de Servicios de Internet.**

Tabla 3.1. Número de usuarios a nivel nacional[54]

3.2.2.9.3 Licenciamiento Previamente Adquirido[55]

En base a estudios previamente realizados por la empresa, los cuales van más allá del alcance del presente proyecto, se han adquirido 26.000 licencias para usuarios CDMA-450 y 15.000 licencias para usuarios WiMAX. Este licenciamiento

[54] Fuente: Superintendencia de Telecomunicaciones (SUPERTEL). [7]

[55] Referencia a Tabla 2.6.

delimitará tanto el número de usuarios CDMA-450 como el número de usuarios WiMAX que el sistema AAA manejará inicialmente.

Figura 3.3. Proyección de cuentas dedicadas

Por otro lado, la empresa posee alrededor de 197.000 licencias correspondientes a usuarios de banda ancha.

3.2.2.9.4 Usuarios Prepago

Para definir el número de usuarios prepago se realizaron estudios de mercado que señalaron el número potencial de clientes que pueden y desean adoptar esta nueva tecnología de aprovisionamiento prepago. Este estudio y sus detalles van más allá del alcance del presente proyecto y solo se cuenta con los resultados de los mismos que indican la necesidad de manejar un número de 50 mil usuarios.

3.2.2.9.5 Conjunción de Variables de Cálculo de Usuarios

Tomando en cuenta todas las variables señaladas con anterioridad, se puede determinar que el número total de usuarios que el sistema AAA debe estar en capacidad manejar; como se muestra en la Tabla 3.2 el número de usuarios totales es de aproximadamente 691 mil.

TIPO DE USUARIOS	NÚMERO DE USUARIOS
Banda ancha	600.000
CDMA-450	26.000
Prepago	50.000
WiMAX	15.000
TOTAL	***691.000***

Tabla 3.2. Sumatoria final de número de usuarios

3.2.3 PLANTEAMIENTO DE LA SOLUCIÓN

3.2.3.1 Sistema AAA

En el mercado actual se pueden encontrar diferentes tipos de sistemas AAA mismos que pueden encontrarse como *software* para ser implementado en diversos equipos o formando parte de un equipamiento en especial.

Entre el *software* para ser implementado, comercialmente se puede encontrar versiones libres y propietarias del mismo. En la empresa se manejan diversos tipos de sistemas AAA, cada uno posee implementado un *software* diferente, cabe recalcar que los usuarios se encuentran distribuidos principalmente dentro de la infraestructura de los sistemas AAA propietarios, razón por la cual serán estas plataformas las que se tendrán en cuenta para el análisis y de las cuales se presenta una descripción general de sus características en la Tabla 3.3.

3.2.3.2 Dimensionamiento de Equipos

3.2.3.2.1 Servidor AAA

Dado que el sistema AAA se encuentra implementado sobre servidores RADIUS, puesto que generalmente se emplea al protocolo RADIUS para la autenticación de clientes, se procederá a analizar y determinar ciertas características físicas de estos equipos para la implementación de la plataforma AAA.

CARACTERÍSTICAS	PLATAFORMA	
	HUAWEI	**ERICSSON**
Red de acceso que soporta	xDSL, WiMAX, GSM y CDMA450/1X/2000/EV-DO	DSL, cable, inalámbricas y Ethernet
Protocolos que soporta	RADIUS, *Diameter*, LDAP, SOAP	RADIUS, *Diameter*, LDAP, SNMP, SOAP, HTTP y DHCP
Manejo de direcciones IP	Asignación estática y dinámica de direcciones IP	Asignación estática y dinámica de direcciones IP
Protocolos de autenticación	CHAP, PAP, EAP-TTLS, EAP-TLS, EAP-SIM, EAP-AKA y EAP-MD5	PAP, CHAP, EAP-MD5, EAP-TLS, EAP-TTLS
Tipos de usuarios acceso	Prepago y post-pago	Prepago y post-pago
Manejo portales	Si	Si

Tabla 3.3. Características generales de plataformas AAA

A. Análisis de las características de los nuevos servidores

Entre las características que se deberían considerar para la elección del nuevo equipamiento se tienen:

- Tipo de procesador.
- Tamaño de la memoria.
- Tamaño de disco duro.

Para facilitar el análisis de los requerimientos antes descritos se considerará el número de usuarios que el sistema deberá soportar, así como, sugerencias que los proveedores de estos equipos ofrezcan.

Los servidores con los que cuenta la empresa manejan un aproximado de 240.000 usuarios y algunas de sus características se presentan en la Tabla 3.4.

En la Tabla 3.5 se muestra parte de la información concerniente a los requerimientos de *hardware* necesarios para la implementación de plataformas AAA en base al número de usuarios, correspondiente a una guía proporcionada por uno de los fabricantes de los sistemas AAA instaladas en la empresa.

CARACTERÍSTICAS	SUN FIRE V880
Procesador	8-core 1.2 GHz UltraSPARC III
Memoria RAM	8 GB, expandible hasta 64 GB
Número de discos duros y capacidad mínima	Hasta 12 discos de 73 GB
Tipo disco duro	SCSI
Tarjeta de red	Una interfaz *Gigabit Ethernet* y una interfaz *Fast Ethernet*
CARACTERÍSTICAS	SUN SPARC ENTERPRISE T5220
Procesador	4-core 1.2 GHz UltraSPARC T2 tecnología QPI
Memoria RAM	8 GB, expandible hasta 64 GB
Número de discos duros y capacidad mínima	De 8 a 16 discos 146GB/300GB
Tipo disco duro	SAS
Tarjeta de red	Cuatro puertos *Ethernet* 10/100/1.000 Mbps
CARACTERÍSTICAS	SUN FIRE V245
Procesador	2-core 1.5 GHz UltraSPARC IIIi
Memoria RAM	8 GB
Número de discos duros y capacidad mínima	Hasta 4 discos de 73 GB (146 GB opcionales)
Tipo disco duro	SAS
Tarjeta de red	Cuatro puertos *Ethernet* 10/100/1.000Base-T

Tabla 3.4. Características generales de los servidores RADIUS de la empresa[56]

Para dimensionar los nuevos equipos, en función del número de usuarios que el sistema AAA deberá soportar, se considera la información señalada en las Tablas 3.4 y 3.5. Esta información se presenta en la Tabla 3.6.

CARACTERÍSTICAS	DESCRIPCIÓN
Procesador	4-core 1.2 GHz UltraSPARC III o IIIi
Memoria RAM	8 GB
Capacidad disco duro	250 GB
Número de discos duros	4

Tabla 3.5. Requerimientos para nuevo servidor AAA

[56] Referencia Tabla 2.2.

TAMAÑO	NÚMERO MÁXIMO DE SUSCRIPTORES	REQUERIMIENTOS DE HARDWARE	NÚMERO DE DISCOS Y TAMAÑO MÍNIMO
Pequeño	30.000	• Procesador: Dual Sun UltraSPARC III or IIIi a 1.28 GHz de velocidad mínima. • 2-GB de memoria RAM. • Mínimo 2 discos duros. • Discos duros SCSI Ultra 3 o superior con 10.000 RPM. • Una tarjeta de red de un *gigabit ethernet* o dos interfaces *fast ethernet.* • Unidad de DVD, teclado, mouse, monitor. • Unidad de cinta u otro mecanismo para respaldo.	Disco 1–26 GB Disco 2–3 GB
Mediano	600.000	• Procesador: Dual Sun UltraSPARC III or IIIi a 1.28 GHz de velocidad mínima. • 2-GB de memoria RAM • Mínimo tres discos duros. • Discos duros SCSI Ultra 3 o superior con 10.000 RPM. • Una tarjeta de red de un *gigabit ethernet* o dos interfaces *fast ethernet.* • Unidad de DVD, teclado, mouse, monitor. • Unidad de cinta u otro mecanismo para respaldo.	Disco 1–72 GB Disco 2–36 GB Disco 3–800 MB
Grande	2.000.000	• Procesador: Quad Sun UltraSPARC III or IIIi a 1.28 GHz de velocidad mínima. • Mínimo doce discos duros configurados en RAID 10. Discos duros SCSI Ultra 3 o superior con 10.000 RPM. • Una tarjeta de red de *un gigabit ethernet* o dos interfaces *fast ethernet.* • Unidad de DVD, teclado, mouse, monitor. • Unidad de cinta u otro mecanismo para respaldo.	Disco 1–73 GB RAID 10- 216 GB

Tabla 3.6. Requerimientos de hardware de acuerdo al proveedor

B. Análisis de Servidores con los que cuenta la empresa

Al comparar los requerimientos de *hardware* de los servidores con los que cuenta la empresa con los requerimientos que debe poseer (ver Tabla 3.7) se puede observar que cada uno de estos posee características iguales o superiores a las recomendadas.

Para poder determinar cuál de estos equipos es el adecuado para implementar la solución AAA se recurrirá al análisis de la tecnología que actualmente el fabricante de los equipos considera es la mejor.

De este análisis se tiene como resultado que el servidor Sun SPARC T5220 posee una mejor capacidad de procesamiento dado que emplea una nueva tecnología en su procesador y por lo tanto este equipo se consideraría adecuado para formar parte de la solución.

Por otro lado, los servidores restantes podrían ser considerados para su reutilización como servidores web para la implementación de los portales de auto-aprovisionamiento del usuario.

C. Análisis de Servidores a Adquirir

En el caso de que no se considere una solución adecuada la reutilización del equipo mencionado en el literal anterior debido a que se encuentra en producción y se desea evitar el corte del servicio a los usuarios durante la implementación de la solución, a continuación se procederá a analizar al menos dos alternativas de servidores que se pueden encontrar en el mercado y que se ajusten a las características presentadas en la Tabla 3.6.

En la Tabla 3.8 se presenta las alternativas que se encontraron en el mercado, las cuales una vez revisadas se considera que el Sun Blade T6340 Server Module es el más adecuado para fungir como servidor AAA ya que este tipo de servidores dada la tecnología que emplean por lo general ocupan menos espacio y permiten añadir o quitar módulos en caso de requerirlo sin detener el servicio.

CARACTERÍSTICAS	REQUERIMIENTOS HARDWARE	SUN FIRE V880	CUMPLE
Procesador	4-core 1.2 GHz UltraSPARC III o IIIi	8-core 1.2 GHz UltraSPARC III	Si
Memoria RAM	8-GB	8 GB, expandible hasta 64 GB	Si
Número de discos duros y capacidad mínima	• Número de discos: 4 • Capacidad del disco: 250 GB	Hasta 12 discos de 73 GB	No
CARACTERÍSTICAS	REQUERIMIENTOS HARDWARE	SUN SPARC ENTERPRISE T5220	CUMPLE
Procesador	4-core 1.2 GHz UltraSPARC III o IIIi	4-core 1.2 GHz UltraSPARC T2 tecnología QPI	Si
Memoria RAM	8-GB	8 GB, expandible hasta 64 GB	Si
Número de discos duros y capacidad mínima	• Número de discos: 4 • Capacidad del disco: 250 GB	De 8 a 16 discos 146GB/300GB	Si
CARACTERÍSTICAS	REQUERIMIENTOS HARDWARE	SUN FIRE V245	CUMPLE
Procesador	4-core 1.2 GHz UltraSPARC III o IIIi	2-core 1.5 GHz UltraSPARC IIIi	No
Memoria RAM	8-GB	8 GB	Si
Número de discos duros y capacidad mínima	• Número de discos: 4 • Capacidad del disco: 250 GB	Hasta 4 discos de 73 GB (146 GB opcionales)	No

Tabla 3.7. Comparación características servidores actuales

3.2.3.2.2 Servidor para portales

Dado que el servicio de portales que permitan a un usuario realizar el auto-aprovisionamiento de un servicio no se encuentra implementado en la empresa, para poder determinar las características que debería poseer el equipo para este fin se considerará los requerimientos básicos para la instalación del sistema operativo sobre el cual correrá la aplicación.

En la Tabla 3.9 se presenta información del *hardware* mínimo recomendado para instalar un sistema operativo en el servidor. En este caso se ha seleccionado dos tipos de *software* existente en el mercado.

SERVIDOR	CARACTERÍSTICAS	
Sun SPARC Enterprise T5120 [8]	*Procesador*	4-core 1.2 GHz, 8-core 1.2 GHz, 8-core 1.4 GHz o 8-core 1. GHz UltraSPARC T2
	Memoria	8 GB, expandible hasta 128 GB
	Disco duro	4 a 8 discos SAS de 146 GB/300 GB
	Interfaz de red	4 puertos *Ethernet* de 10/100/1.000 Mbps
	Potencia	660 W (DC)
	Dimensiones	44mm x 425mm x 714mm (alto x ancho x profundidad)
	Sistema operativo	Solaris 10
SERVIDOR	**CARACTERÍSTICAS**	
Sun Blade T6340 Server Module [9]	*Procesador*	2 de 6-core 1.2 GHz, 8-core 1.2 GHz o 8-core 1.4 GHz UltraSPARC T2 Plus
	Memoria	8 GB, expandible a 256 GB
	Disco duro	Soporta discos de SAS de 146GB / 300GB
	Interfaz de red	2 puertos *Ethernet* de 10/100/1.000 Base-T
	Dimensiones	44.45mm x 327.15mm x 496.82mm (alto x ancho x profundidad)
	Sistema operativo	Solaris 10
	Chasis	Sun Blade 6000

Tabla 3.8. Características de alternativas de servidores

SISTEMA OPERATIVO	CARACTERÍSTICAS	
Windows Server 2003	*Procesador*	Intel Pentium o compatible con mínimo 133 MHz (recomendado 550 MHz)
	Memoria	Mínimo 128 MB, recomendado 256 MB, máximo 4 GB
	Disco duro	3 GB de espacio libre
SISTEMA OPERATIVO	**CARACTERÍSTICAS**	
Solaris 10	*Procesador*	Mínimo SPARC 250 MHz
	Memoria	Mínimo 256 MB
	Disco duro	2 GB de espacio libre

Tabla 3.9. Características de hardware mínimo de acuerdo al sistema operativo [10], [11]

Una alternativa propuesta es la reutilización de los equipos que se darán de baja una vez implementada la solución. En base a esto, en la Tabla 3.10, se realiza

una comparación de los requisitos mínimos de acuerdo al sistema operativo para poder determinar si los equipos pueden ser reutilizados.

Como resultado del análisis se tiene que los tres servidores podrían ser reutilizados, pero dado que el servidor SUN SPARC Enterprice T5220 puede ser empleado también para implementar el nuevo sistema AAA luego de realizar un *upgrade* de su *hardware* y *software*, se sugiere que se empleen los servidores de la serie SUN FIRE para la implementación de los portales y de esta manera se estaría inclusive ahorrando costos a la empresa.

3.2.3.2.3 Licenciamiento

Debido a que el sistema AAA debe poseer un número de licencias adecuadas para poder registrar el número de usuarios que se estima en un futuro la plataforma debe soportar, en la Tabla 3.11 se indica el número de licencias que la empresa debe adquirir junto con el equipo para poder brindar acceso a todos estos usuarios.

Cabe recalcar que el número de licencias a adquirir dependerá si todas las licencias que la empresa posee por cada proveedor pueden ser reutilizadas en su totalidad. En la tabla presentada se considera que todas las licencias existentes se pueden reutilizar.

3.2.3.3 Tolerancia a Fallos [12] [13]

Uno de los requerimientos es que el servidor AAA debe poseer redundancia geográfica, en la cual los servidores principales se ubicarán en la ciudad de Quito mientras que los de respaldo se dispondrán en Guayaquil de manera tal que el sistema continúe funcionando aunque se produzcan fallos.

Para brindar una correcta prevención y tolerancia de fallos se puede emplear la redundancia a nivel de *hardware*, en la cual se utilizan componentes adicionales para detectar los fallos y recuperar el comportamiento correcto de un sistema. Dentro de esta técnica se puede recurrir a los *clusters* de alta disponibilidad, los

cuales son grupos de computadores que soportan aplicaciones de servidores y pueden operar de manera redundante proveyendo un servicio continuo cuando un sistema falla.

CARACTERÍSTICAS	REQUERIMIENTOS MÍNIMO DE HARWARE	SUN FIRE V880	CUMPLE
Procesador	250 MHz	8-core 1.2 GHz UltraSPARC III	Si
Memoria RAM	256 MB	8 GB, expandible hasta 64 GB	Si
Disco duro	3 GB de espacio libre	Hasta 12 discos de 73 GB	Si
CARACTERÍSTICAS	REQUERIMIENTOS MÍNIMO DE HARWARE	SUN SPARC ENTERPRISE T5220	CUMPLE
Procesador	250 MHz	4-core 1.2 GHz UltraSPARC T2 tecnología QPI	Si
Memoria RAM	256 MB	8 GB, expandible hasta 64 GB	Si
Disco duro	3 GB de espacio libre	De 8 a 16 discos 146GB/300GB	Si
CARACTERÍSTICAS	**REQUERIMIENTOS MÍNIMO DE HARWARE**	**SUN FIRE V245**	**CUMPLE**
Procesador	250 MHz	2-core 1.5 GHz UltraSPARC IIIi	Si
Memoria RAM	256 MB	8 GB	Si
Disco duro	3 GB de espacio libre	Hasta 4 discos de 73 GB (146 GB opcionales)	Si

Tabla 3.10. Comparación de requerimientos mínimo de hardware para el servidor de portales

USUARIOS	NÚMERO DE LICENCIAS		
	EXISTENTES	**REQUERIDAS**	**TOTALES**
Banda Ancha	Huawei: 87.000 Ericsson: 110.000	403.000	600.000
Prepago	--	50.000	50.000
CDMA	26.000	--	26.000
WiMAX	15.000	--	15.000

Tabla 3.11. Número de licencias a adquirir

Para proveer el requerimiento solicitado se propone como parte de la solución el empleo de un esquema de redundancia N+1 que manejan este tipo de *clusters*, en cada ciudad, de manera que se tenga un nodo extra para ser empleado

cuando uno de los equipos principales han fallado; además dado que este esquema se usa cuando se tienen múltiples servicios ejecutándose de manera simultánea es el más adecuado para el sistema AAA centralizado.

Para evitar que un solo servidor se sobrecargue de trabajo, dada la cantidad de tráfico que debe manejar, se propone el uso de balanceadores de carga, de esta manera se tendría un mejor rendimiento y distribución del tráfico que el sistema debe manejar. Además esto permitirá emplear de manera eficiente el ancho de banda del enlace o enlaces que se dispongan para la conexión el sistema AAA.

Por otro lado parte de la solución debe contemplar también protección ante fallas para la base de datos dado que un fallo en un dispositivo de almacenamiento puede provocar el manejo de datos erróneos lo cual afectaría a la empresa.

Existen diversos métodos que permiten realizar una replicación de bases de datos por medio de software, los cuales ofrecen ante una interrupción planeada o inesperada del sistema primario que la réplica entre en funcionamiento ofreciendo de esta manera una alta disponibilidad ya que siempre se tendrá acceso a los datos. Una vez que el sistema primario se encuentre disponible nuevamente, la réplica se sincroniza con éste para trasferir la información que se ejecutó durante su ausencia y éste continúe con su funcionamiento regular.

Dado que las bases de datos que la empresa posee se encuentran elaboradas mayoritariamente sobre la plataforma Oracle, se propone el uso de la tecnología Oracle Data Guard, la cual permite crear, administrar y monitorear una o más bases de datos de reserva para proteger datos de la empresa de fallos o errores. Esta tecnología se encuentra conformada por una base de datos de producción y una o más bases de datos de respaldo o *standby* las cuales son copias de la base de datos de producción. Las bases de datos de respaldo se encuentran sincronizadas con las bases de producción y pueden conmutar entre sí de tal manera que se previene la pérdida de datos y el tiempo de transición ante una falla es corto. Cuenta también con un aplicativo denominado Data Guard Broker

que controla la configuración, creación, mantenimiento y monitoreo de la arquitectura Data Guard.

Dentro de la solución se debe considerar también que los equipos brinden la posibilidad de reemplazar sus partes en caliente (*hot swap*[57]) para de esta forma evitar la interrupción del servicio cuando se deba reemplazar alguna de sus componentes ya sea por daño o por mantenimiento del equipo. Además el equipo debe poseer redundancia en componentes como fuentes de energía, interfaces de red y el disco duro.

En la Figura 3.4 se puede observar la solución de tolerancia a fallos planteada.

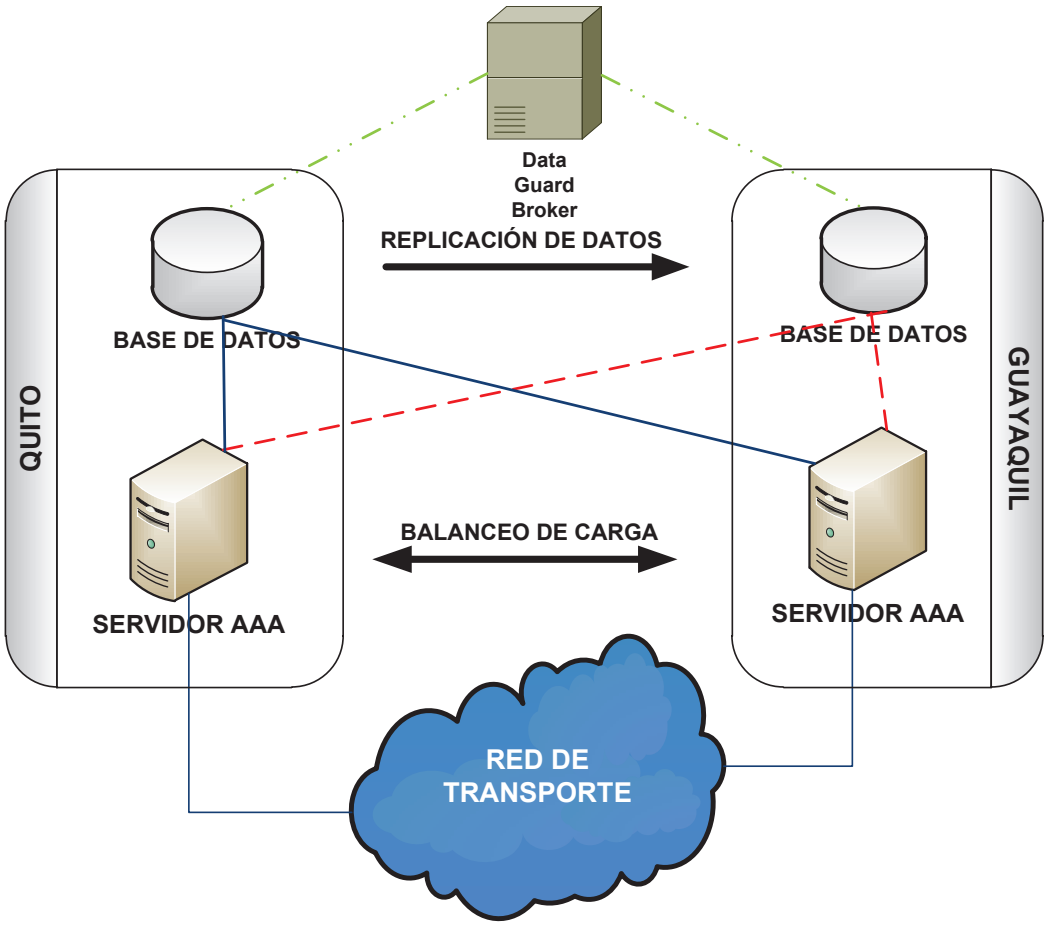


Figura 3.4. Arquitectura propuesta para la tolerancia a fallos

[57] *Hot Swap* indica la capacidad de poder sustituir el componente averiado sin la necesidad de apagar el equipo, por lo tanto sin afectar al funcionamiento integral del sistema.

3.2.3.4 Políticas de Calidad de Servicio

Dados los requerimientos planteados para la provisión de políticas de calidad de servicio a través del sistema AAA centralizado se observa que la mayor parte de éstos requieren de equipos externos al sistema, es decir el sistema AAA deberá interactuar con una infraestructura dedicada a la provisión de las políticas de calidad de servicio.

Como uno de los requerimientos a cumplir es la implementación de la inspección profunda de paquetes, dependiendo del fabricante se puede encontrar en el mercado soluciones que permiten realizar este proceso mediante una tarjeta que se coloca a un equipo y mediante *software* se realiza su administración, o mediante un equipo especializado para esta funcionalidad.

Para características como el filtrado de contenido se podría emplear los equipos de la red de datos de la empresa para que sean estos los que filtren el tráfico dependiendo de su prioridad, pero dado que la idea general es que desde el sistema AAA se detecte el tipo de tráfico que va a cursar por la red se debería emplear para este caso un equipo especializado para esta funcionalidad.

En la Figura 3.5 se puede observar la propuesta de solución para la implementación de calidad de servicio.

3.2.3.5 Interconexión de Equipos [14] [15]

En base al planteamiento dado para la solución, los elementos que conforman parte de la solución AAA, principalmente los servidores AAA deben encontrarse interconectados dentro de la misma subred. La interconexión entre estos elementos de manera física debería ser en una topología anillo-estrella mediante la cual si un equipo del sistema sufre algún desperfecto el resto de equipos que los conforman pueden trabajar sin problemas. Por otro lado, la comunicación entre los diversos dispositivos (BRAS, sistemas de tarifación) se realizará

mediante una interconexión lógica basada en VRFs [58] para de esta manera aprovechar la red de transporte que posee la empresa.

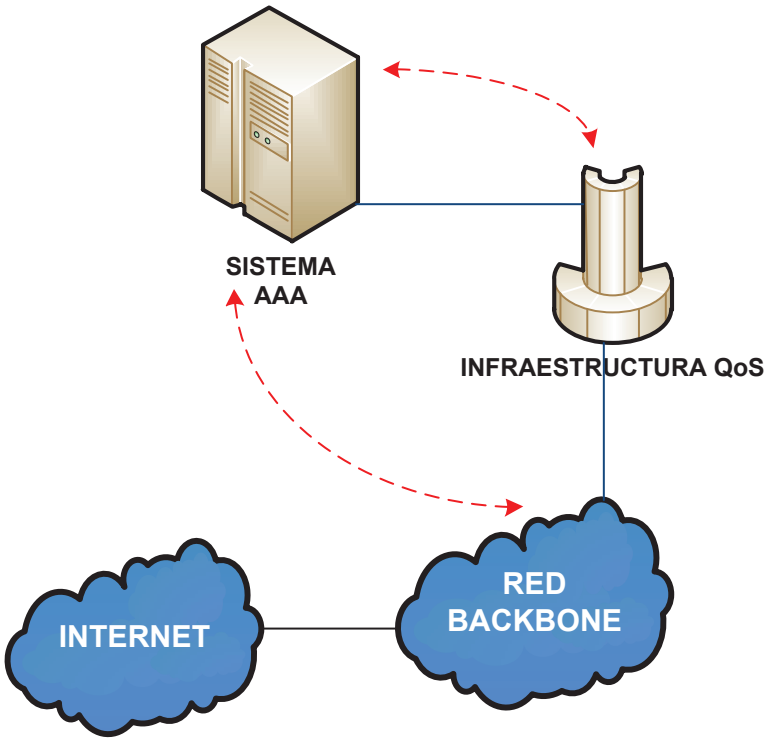


Figura 3.5. Arquitectura propuesta para implementación de calidad de servicio

El direccionamiento IP[59] a ser empleado para la solución AAA depende de los enlaces que se tendrían para la interconexión de los equipos que conforman la solución, los cuales a su vez dependen del diseño que se realice para cumplir con cada una de las especificaciones técnicas expuestas anteriormente. El número de redes que se requieran para satisfacerlo debe ser solicitado a la CNT.

En base al diseño para la solución AAA propuesta se tendrían 2 equipos distribuidos entre Quito y Guayaquil los cuales se interconectarían entre sí, y a su vez con los BRAS, el sistema de tarifación y los portales. En la Tabla 3.12 se

[58] La tecnología VRF (*Virtual Routing and Forwarding*) permite que múltiples instancias de tablas de enrutamiento puedan coexistir al mismo tiempo en un mismo *router*, es decir, se puede tener las mismas direcciones IP en el equipo. Además, permite incrementar la seguridad en la red mediante la segregación de servicios.

[59] El direccionamiento IP para la presente solución no será mostrado debido a un acuerdo de confidencialidad existente con la empresa. Para el ejemplo se ha tomado una dirección de red privada.

indica el tipo de direccionamiento que en este caso se podría tener para las interconexiones entre estos dispositivos.

La interconexión entre los equipos AAA y la red de transporte se puede efectuar mediante el uso de interfaces de 1 Gbps dado que el tráfico que maneja no es muy alto (ver Tabla 3.13), pero dado que se desea implementar manejo de políticas de calidad de servicio mediante este sistema puede darse el caso que el tráfico se incremente para lo cual, previendo a futuro el aumento de clientes, se podría sugerir que esta plataforma cuente con interfaces de 10 Gbps. Esto permitiría un flujo rápido de la información tanto de los clientes como de los servicios que el sistema AAA centralizado proporcionaría a estos.

ENLACE	DIRECCIÓN IP
AAA con los BRAS	10.8.X.X / 27
AAA con los portales	10.8.X.X / 29
AAA con el sistema de tarifación	10.8.X.X / 29
Base de datos de los AAA	10.8.X.X / 29
AAA con infraestructura para QoS	10.8.X.X / 28

Tabla 3.12. Direccionamiento propuesto

EQUIPO		TIPO TRÁFICO		
		ACTUAL	**PROMEDIO**	**MÁXIMO**
BRAS 1	ENTRADA	56.31 K	24.83 K	285.22 K
	SALIDA	165.55 K	72.86 K	981.83 K
BRAS 2	ENTRADA	31.69 K	29.45 K	449.30 K
	SALIDA	96.95 K	90.30 K	1.09 M
BRAS 3	ENTRADA	39.95 K	48.70 K	393.73 K
	SALIDA	120.15 K	146.90 K	1.11 M
BRAS 4	ENTRADA	76.79 K	52.32 K	375.90 K
	SALIDA	218.77 K	150.63 K	1.04 M
BRAS 5	ENTRADA	42.14 K	34.06 K	131.09 K
	SALIDA	117.66 K	94.77 K	673.57 K

Tabla 3.13. Promedio del tráfico AAA en los BRAS[60]

[60] Fuente: Corporación Nacional del Telecomunicaciones Julio 2011

Por otro lado, como el sistema AAA va a tener interacción con los portales, se debe implementar ciertas normas que permitan brindar seguridad principalmente a la red interna; para esto se podría colocar un *firewall* entre la red de portales y el internet y un *firewall* entre el sistema AAA y la red de transporte como se observa en Figura 3.6.

En la Figura 3.7 se presenta un diagrama general de la solución planteada; en éste se observa que los usuarios provienen de diversas tecnologías de acceso (WIMAX, CDMA 450, xDSL) cuyas peticiones se reciben a través de los BRAS o la PDSN y son enviadas al sistema AAA en donde se autentica y autoriza el acceso del usuario a la red, y a su vez almacena información necesaria para la facturación del servicio misma que también es trasmitida a la plataforma de tarifación.

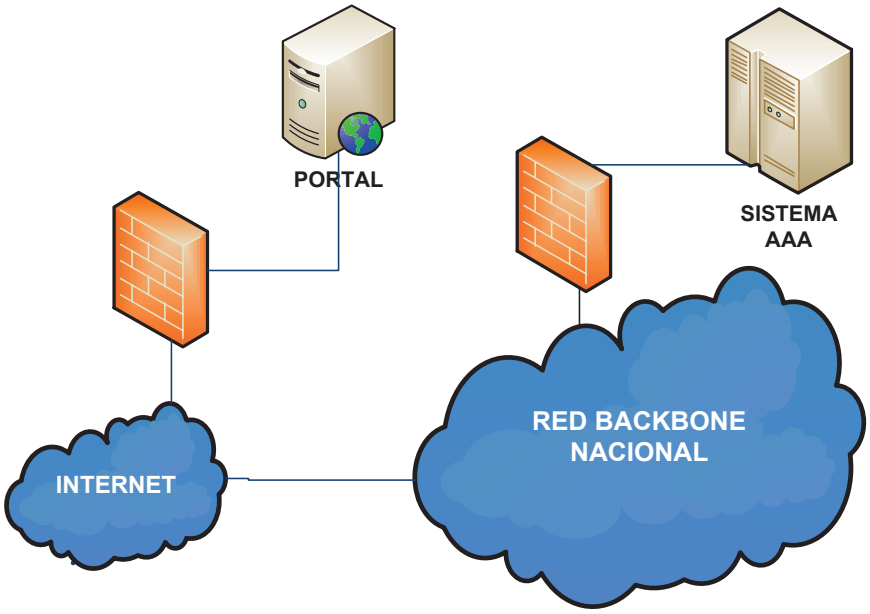


Figura 3.6. Seguridad en la red de portales

El sistema AAA se comunica también con la infraestructura de calidad de servicio mediante la cual se ejecutará el control de las políticas y los recursos requeridos por los servicios de valor agregado como el vídeo bajo demanda. Por otro lado, el usuario podrá interactuar con el sistema AAA por medio de un portal mediante el cual realizará un auto-aprovisionamiento del servicio deseado.

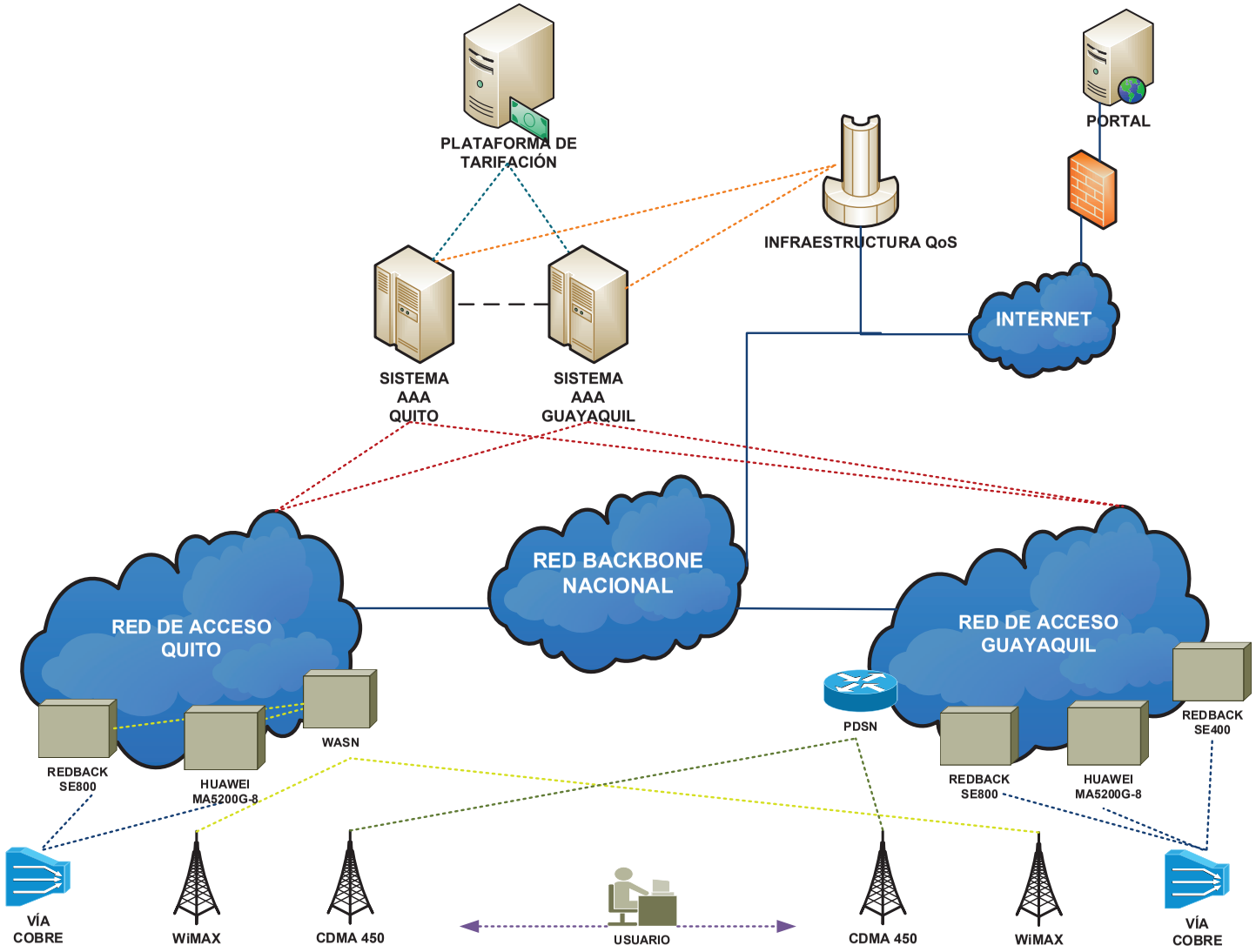


Figura 3.7. Arquitectura general de la solución de un sistema AAA centralizado

CAPÍTULO 4

PLAN DE ACCIÓN PARA LA IMPLEMENTACIÓN DE LA SOLUCIÓN AAA SOBRE LA INFRAESTRUCTURA ACTUAL

4.1 INTRODUCCIÓN

En el presente capítulo se analizarán alternativas de soluciones existentes en el mercado que cumplan con los requisitos especificados y se ajusten al modelo de negocio planteado. Se describirán de manera general las características y funcionalidades requeridas por los equipos que formarán parte de la solución para la implementación del sistema AAA centralizado.

Se describirá el proceso de integración de equipos, el de migración de los clientes y el mecanismo mediante el cual un usuario puede autenticarse y realizar un auto-aprovisionamiento con el sistema AAA centralizado.

Y finalmente un manual de administración en el cual se recopilarán datos teóricos y técnicos que ayuden con la capacitación del personal, el mantenimiento de equipos y la administración del sistema AAA centralizado.

4.2 PROCESO INICIAL

Debido a que la Corporación Nacional de Telecomunicaciones es una empresa pública, la licitación de un proyecto para la implementación de la solución AAA sobre la infraestructura actual debe ser presentada mediante el portal de compras públicas.

Para esto se debe elaborar un pliego en el cual se detallen tanto requerimientos técnicos como administrativos/financieros que requiere el proyecto. Las empresas que deseen participar en la licitación adquieren los pliegos por medio del portal

antes mencionado y deben proporcionar toda la información pedida dentro del periodo estimado para esto.

Una vez culminado el periodo de espera los sobres que contienen las propuestas son abiertos y analizados por personal especializado de la empresa. La determinación del concursante ganador, por lo general, depende de varios factores como el aspecto técnico, financiero y el legal.

En base a lo expuesto, a nivel técnico, para poder definir la alternativa de solución que más se ajusta a los requerimientos de la empresa, en la Tabla 4.1 se presenta las especificaciones técnicas que se deben considerar para la selección de la misma. Con el fin facilitar la determinación de la mejor solución se ha asignado un valor a cada requerimiento de acuerdo a su relevancia. Se ha asignado 30 puntos a las características que deben ser cumplidas de manera específica y cuya ejecución se basa el sistema AAA, 20 puntos a características complementarias a las primeras, ya que si éstas no están implementadas, la plataforma no podrá brindar todas las funcionalidades propuestas, y 10 puntos a aquellas que se consideran facilitarían la gestión de la plataforma.

4.3 ALTERNATIVAS DE SOLUCIONES

La solución a los requerimientos planteados por la CNT para la implementación del sistema AAA no se encuentra directamente en el mercado, dadas las dimensiones del proyecto, siendo que busca la interacción entre un gran número de tecnologías, marcas y programas propietarios. Es por ello que el planteamiento de la solución puede ser una combinación de productos y soluciones a más de módulos desarrollados exclusivamente para el cumplimiento de algunos requerimientos específicos por parte del fabricante.

Este modelo de proyecto no se enmarca en la solución tradicional de implementaciones que suelen manejarse de forma directa, planteando primeramente los recursos técnicos y solicitando varias opciones de costos para decidirse finalmente por la opción económicamente más factible. En este caso, es

necesario primero buscar resolver el problema de la heterogeneidad de las tecnologías para luego definir si la solución es factible económicamente en base a la asignación presupuestaria del estado.

Las alternativas presentadas a continuación son las soluciones planteadas en base a dos fabricantes que poseen infraestructura AAA en la empresa. Adicional a esto se mostrará una tabla indicativa del cumplimiento de los principales puntos del proyecto.

4.3.1 PRIMERA ALTERNATIVA [1] [2] [3] [8]

Como primera alternativa se analizará la solución con equipos pertenecientes a la casa fabricante Huawei y la forma cómo estos satisfacen los requerimientos de la empresa. A continuación se presentan las principales características del sistema AAA infoX-AAA de Huawei.

- La plataforma soporta varios tipos de redes de acceso como xDSL, WiMAX, GSM y CDMA450/1X/2000/EV-DO.
- Soporta el protocolo RADIUS definido en el RFC 2865, RFC 2866 y 3GPP2[61]. Además soporta las especificaciones dadas por NWG (*Network Working Group*).
- Soporta al protocolo *Diameter* en base al RFC 3588 y RFC 4006.
- Soporta usuarios tanto prepago como post-pago y la generación de CDRs. Para usuarios prepago posee un soporte de servicio de tarjeta integrada.
- Puede actuar como un servidor RADIUS *proxy* mismo que puede ser configurado como un servidor activo o de respaldo (*standby*).
- Soporta asignación de direcciones IP de manera estática y dinámica, así como la asignación de un pool de direcciones IP en base a un dominio, nombre de usuario o NAS.

[61] 3GPP2: *Third Generation Partnership Project 2*.

NUMERAL	REQUERIMIENTO	PUNTUACIÓN
1	Soportar la autenticación de clientes de diversas tecnologías de acceso como xDSL, WiMAX, y CDMA450.	30
2	Integración con las plataformas existentes en la CNT:	
2.1	BRAS marca Redback.	30
2.2	BRAS marca Huawei.	30
2.4	PDSN marca Huawei de la red CDMA450.	30
2.5	Plataforma prepago marca Huawei.	30
2.6	Plataforma de facturación.	30
3	Soportar protocolo RADIUS en base al RFC 2865, RFC 2866 y sus extensiones.	30
4	Soportar al protocolo *Diameter* en base al RFC 3588 y RFC 4005.	30
5	Soportar el protocolo FTP y/o *Web services*.	30
6	Poseer funcionalidad de RADIUS *proxy*.	30
7	Soportar clientes prepago y post-pago.	30
8	Permitir la generación de CDRs para enviar información al sistema de tarifación.	30
9	Permitir asignación estática o dinámica de direcciones IP a los suscriptores.	30
10	Permitir la asignación de una dirección IP o un pool de direcciones IP a un suscriptor.	30
11	Autenticar clientes que no tengan dominio.	20
12	Soportar el manejo de una tarjeta prepago.	20
13	Permitir la facturación en tiempo real.	20
14	Debe disponer de redundancia geográfica de manera que se garantice que en caso de fallos en Quito o en Guayaquil la solución se mantendrá operativa.	30
15	Permitir autenticación mediante protocolos PAP, CHAP, EAP.	20
16	Operar como *Access Network* AAA, *Broker* AAA, *Home* AAA y *Visited* AAA para la autenticación de usuarios de la red CDMA.	20
17	Permitir la aplicación de políticas de calidad de servicio.	20
18	Permitir el filtrado de contenido.	20
19	Permitir el control de tráfico de servicios.	20
20	Permitir el control de ancho de banda.	20
21	Permitir la gestión de umbrales.	20
22	Permitir el *caching*.	20
23	Poseer mecanismos de seguridad para evitar ataques de denegación de servicio.	20
24	Permitir su gestión de manera gráfica y por medio de CLI.	10
25	Poseer de mecanismos para monitoreo de la plataforma.	10
26	Soportar el manejo de portales que interactúen con el usuario.	20
27	Soportar 600.000 usuarios.	30

Tabla 4.1. Características para selección de la solución

- Permite crear dominios y como sus delimitadores usa %, #, @ y /. Además posee la funcionalidad de remoción de dominio con la cual se puede autenticar un usuario con solo el valor correspondiente al nombre de usuario.
- Puede limitar el acceso de los usuarios basado en tiempo o utilización. También permite determinar el puerto por el cual el usuario accede a la red.
- Para aplicaciones CDMA soporta *visited* AAA, *broker* AAA y *home* AAA.
- El sistema AAA se encuentra con un módulo de administración el cual le permitirá realizar la gestión del equipo y el monitoreo de los usuarios.
- Soporta autenticación mediante protocolo CHAP, PAP, EAP-TTLS, EAP-TLS, EAP-SIM, EAP-AKA y EAP-MD5.

El sistema AAA expuesto no posee como característica la funcionalidad DPI. Para poder implementarla dentro de la red se lo puede realizar mediante la incorporación de un dispositivo externo. De igual manera, dentro de la solución se debe incorporar un equipo que permita el control de políticas y recursos para de esta manera poder implementar características como control de tráfico que definen una red inteligente de banda ancha.

Entre las opciones de equipos que esta casa comercial ofrece en el mercado para cumplir con lo descrito anteriormente se presentan los siguientes dispositivos:

- SIG9800 (*Service Inspection Gateway*), el cual provee un servicio inteligente para el control de tráfico, administración de ancho de banda y seguridad de la red. Las características de este equipo se presentan en la Tabla 4.2 y Tabla 4.3.
- RM9000 (*Resource and Policy Control System*), el cual permite la aplicación de políticas de calidad de servicio y filtrado de contenido lo que facilita la provisión de servicios de valor agregado pues permite controlar

el ancho de banda que un servicio requiere. Por otro lado, este equipo permite también el uso de portales para la interacción con el cliente para el auto-aprovisionamiento del servicio. En la Tabla 4.4 y Tabla 4.5 se presentan las principales características de este equipo.

CARACTERÍSTICAS TÉCNICAS		
	SIG9810	***SIG9820***
Capacidad *backplane*	640 Gbps	1,28 Tbps
Potencia	2.100 a 2.600 W	3.600 a 5.000 W
Peso	65 a 120 Kg	85 a 250 Kg
Voltaje de entrada AC	180 a 264 V	180 a 275 V
Voltaje de entrada DC	-75 a -38 V	
Dimensión de Rack	19 pulgadas	
Temperatura de operación	0ºC a 45ºC	
Número de usuarios configurados	10´000.000	
Capacidad de procesamiento total	2.000 Gbps	
Número máximo de dispositivos	80	
Capacidad de procesamiento en ambientes fijos		
Capacidad de procesamiento máxima	20 Gbps a 40 Gbps	50 Gbps a 80 Gbps
Número de conexiones concurrentes	24´000.000 a 48´000.000	60´000.000 a 96´000.000
Número máximo de usuarios concurrentes	1´000.000	
Número máximo de políticas por usuario	1.000	
Capacidad de procesamiento en ambientes móviles		
Capacidad de procesamiento máxima	20 Gbps a 30 Gbps	40 Gbps a 60 Gbps
Número de conexiones concurrentes	24´000.000 a 36´000.000	48´000.000 a 72´000.000
Número máximo de usuarios concurrentes	2´000.000 a 4´000.000	5´000.000 a 8´000.000
Número máximo de políticas por usuario	1.000	

Tabla 4.2. Características técnicas del equipo SIG9800 [2]

4.3.1.1 Integración

A continuación se procederá a indicar la manera en la cual la plataforma infoX-AAA realizará la integración con las plataformas existentes en la CNT.

CARACTERÍSTICAS GENERALES

• **Realiza el control de tráfico en base a políticas determinadas por el operador.**
• **Se encuentra conformado por:**
  ○ **Un sistema *foreground* que contiene módulos dedicados a funciones como el control de tráfico en base a las políticas establecidas en el sistema *background*, interfaces de comunicación y funciones de alarma y exportación de *logs*.**
  ○ **Un sistema *background* se encuentra conformado por servidores, mismos que proveen funciones como la administración de usuarios y políticas, almacenamiento de información para la generación de reportes y actualización de repositorios.**
• **Puede operar de dos modos:**
  ○ ***In-line*. En este modo el dispositivo se conecta a la red por medio de un equipo de *bypass*, el cual permite, en caso de falla del sistema, re-direccionar los datos de manera directa sin interrumpir el servicio. Este modo se lo emplea en escenarios como capa de acceso, salida de la MAN y los *gateways* internacionales.**
  ○ ***Off-line*. Este modo emplea la función de división óptica para interferir con el tráfico de la red y poder duplicarlo para sus análisis. El equipo puede ser ubicado en la capa de núcleo o de convergencia de la red.**
• **Se lo puede emplear para inspeccionar clientes, grupos de enlaces, sistemas autónomos, subredes y tipos de servicios.**
• **Puede realizar un análisis de tráfico en base a protocolos de acuerdo a un área y el tipo de suscripción del cliente.**
• **Puede detectar y controlar información spam por medio del uso del protocolo SMTP (*Simple Message Transfer Protocol*).**
• **Posee un módulo que le permite medir la transmisión de paquetes y en base a esto, determinar tráfico malicioso dado principalmente por ataques como *TCP flood*, *UDP flood* o *DNS flood*. Como medidas defensivas este módulo incluye funcionalidades para limitar el tráfico.**
• **Permite controlar el comportamiento de navegación de los usuarios en base a categorías dadas por direcciones URL a las cuales un usuario ha accedido por ejemplo a noticias o juegos.**
• **Posee una función que permite implementar la función de control paternal mediante las siguientes opciones:**
  ○ **Filtrado de URLs mediante el uso de una lista proporcionada por el operador o por medio de la creación de listas por parte del cliente.**
  ○ **Control sobre aplicaciones.**
  ○ **Control de la duración de la cuenta hijo.**
• **Puede interactuar con un NMS (*Network Management System*) ya que soporta las tres versiones del protocolo SNMP.**
• **El equipo ofrece redundancia 1+1 en las fuentes de poder y ventilación, N+1 para las tarjetas de procesamiento y un balanceo de carga 3+1 para el sistema *background*.**

Tabla 4.3. Características generales del equipo SIG9800[2]

CARACTERÍSTICAS GENERALES
• **Provee una plataforma para el control de servicios y recursos para servicios de valor agregado y servicios de datos móviles.** • **Puede ser interconectado con dispositivos externos para mejorar su funcionamiento y el de la red brindando al usuario una calidad de servicio extremo a extremo.** • **Provee una estructura de *software* en base a módulos que se encuentran distribuidos en tarjetas y servidores.** • **A nivel de *hardware*, el equipo se encuentra conformado por un chasis, *subrack*, tarjetas, *switch* LAN y un arreglo de discos.** • **A nivel a *hardware* y *software* trabaja con modo de redundancia 1+1 de tal manera que si un módulo sufre algún daño, esto no afecta al funcionamiento del sistema.** • **Permite realizar el control de servicios en base al uso de la dirección IP origen, dirección IP destino, puerto origen, puerto destino y tipo de protocolo.** • **Permite que el usuario realice un auto-aprovisionamiento de servicio por medio del uso de un portal.** • **Posee funcionalidad de DPI para determinar el tipo de servicio y en base a esto proporcionar las políticas adecuadas para controlar el ancho de banda y los parámetros de calidad de servicio que éste requiere.** • **Permite el manejo de políticas basadas en el usuario, servicio, ubicación, duración y tráfico.** • **Provee funciones para la administración de información de suscriptores y servicios permitiendo funcionalidades como creación, modificación y borrado de estos. Además permite la conformación de grupos de usuarios para su administración.** • **Soporta la administración tanto de usuarios post-pago como prepago.** • **Permite definir un tipo y monto de cuota de consumo para los servicios. Si ésta es excedida se aplicarán las políticas definidas por el operador y/o se enviarán mensajes a los usuarios informando del evento para permitirle realizar una recarga y que de esta manera el servicio no se vea interrumpido.** • **Soporta protocolos como SOAP, COPS, RADIUS, *Diameter*, FTP y LDAP.** • **Permite la generación de CDRs.** • **Para usuarios móviles ofrece servicios como *roaming*.** • **Posee una interfaz basada en lenguaje MML que permite al operador realizar operaciones de configuración y mantenimiento. Para esto también posee una interfaz de usuario web.**

Tabla 4.4. Características generales del equipo RM9000[3]

4.3.1.1.1 BRAS

Para la integración de los BRAS el sistema AAA emplea el protocolo RADIUS y sus extensiones, incluso soporta el atributo VSA (*Vendor Specific Attribute*) lo cual le permite comunicarse con un sistema AAA de otro fabricante.

CARACTERÍSTICAS TÉCNICAS	
Número máximo de usuarios registrados	3´000.000
Número máximo de usuarios concurrentes	1´000.000
Número máximo de sesiones concurrentes para aplicaciones móviles	2´100.000
Tarjeta de procesamiento	Memoria de 8GB Sistema operativo: SUSE Linux
Dimensiones	2.200mm x 600mm x 800 mm
Peso	365 Kg
Altura del rack	46 U
Voltaje de operación	-72 VDC a -40.5 VDC
Consumo de potencia máximo	~ 2.640 W
Temperatura	5ºC a 45ºC

Tabla 4.5. Características técnicas del equipo RM9000[3]

4.3.1.1.2 Plataforma CDMA

La integración hacia la red CDMA 450 utilizará el protocolo RADIUS.

4.3.1.1.3 Sistema de Tarifación

Para la integración del sistema AAA con la plataforma prepago, el sistema emplea el protocolo *Diameter* el cual permitirá intercambiar información concerniente a la función de cobro en línea del sistema.

Para la integración del sistema AAA con la plataforma de facturación lo realiza utilizando *web services* y/o FTP. También puede utilizar MML (*Man-Machine Language* / Lenguaje Hombre-Máquina).

En la Figura 4.1 se puede observar de manera general la integración del sistema AAA con las plataformas existentes en la CNT.

En la Figura 4.2 se muestra un diagrama general de la solución a la primera alternativa.

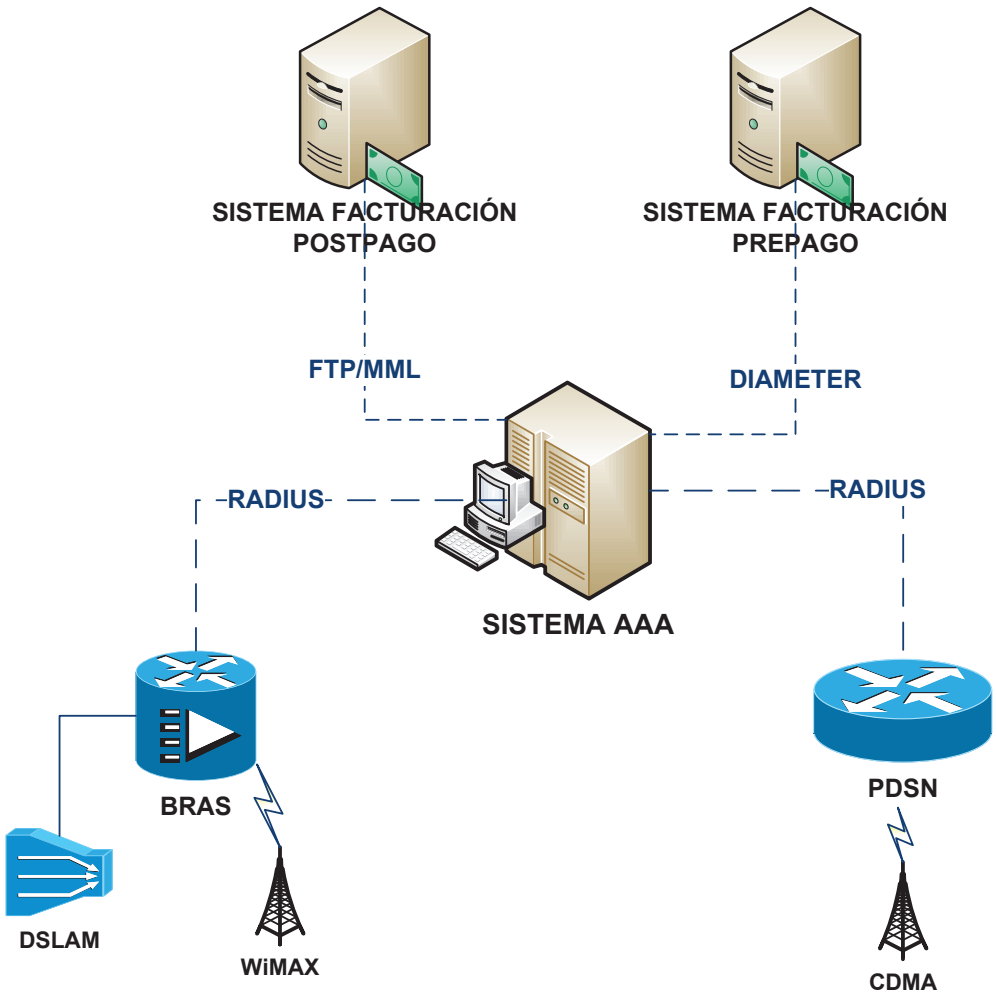


Figura 4.1. Solución de integración de plataformas Huawei

4.3.2 SEGUNDA ALTERNATIVA [4] [5] [6] [7] [8]

Como segunda alternativa se analizarán equipos pertenecientes a la casa fabricante Ericsson y la forma cómo estos satisfacen los requerimientos de la empresa.

Ericsson maneja la plataforma NetOp Policy Manager para ofrecer un servicio AAA. Éste trabaja de manera conjunta con los equipos SmartEdge que son los equipos que se emplean como BRAS. A continuación se presentan algunas de las características principales del sistema AAA:

- Admite usuarios provenientes de diferentes tecnologías de acceso como DSL, cable, inalámbricas y Ethernet.

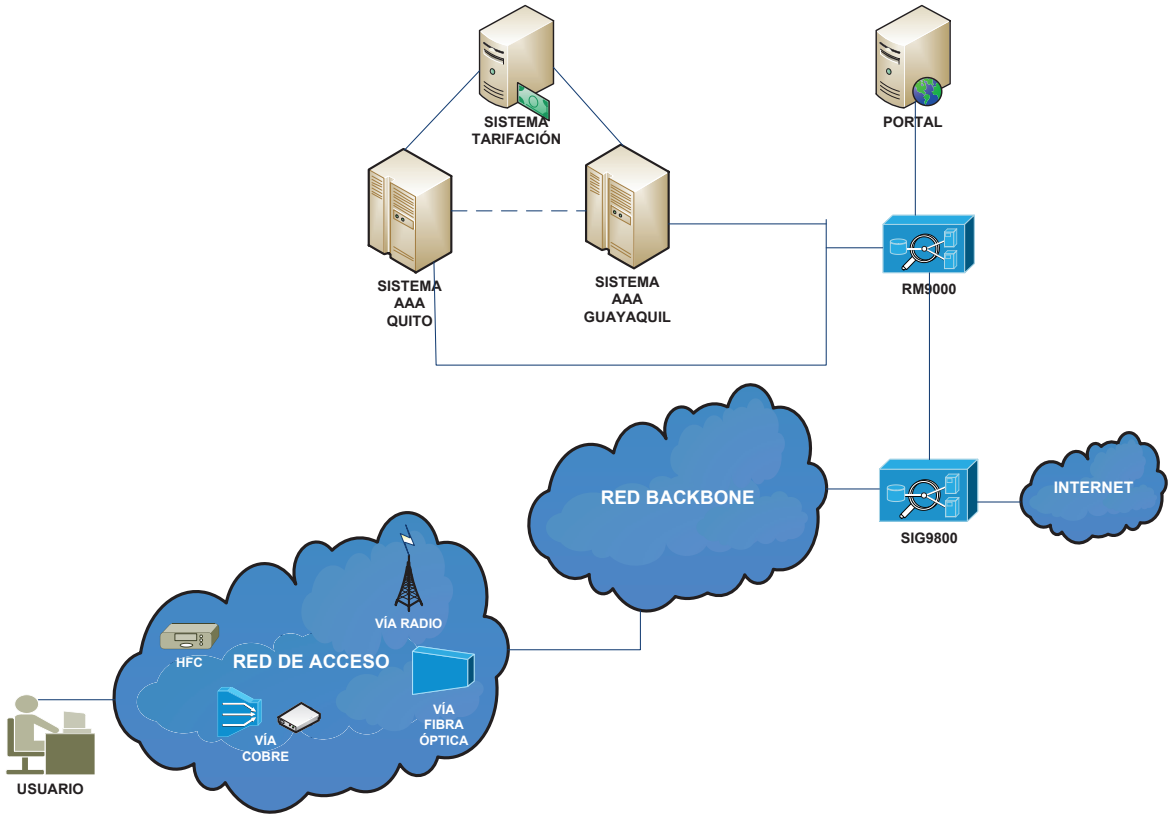


Figura 4.2. Diagrama de la solución general planteada a la primera alternativa[62]

- Soporta los protocolos: RADIUS, *Diameter*, LDAP, SNMP, SOAP, HTTP y DHCP.
- Soporta autenticación por PAP, CHAP, EAP-MD5, EAP-TLS, EAP-TTLS.
- Permite que los suscriptores seleccionen los servicios que deseen a través de un portal.
- Permite la adición y gestión de servicios de valor agregado como vídeo bajo demanda, ancho de banda bajo demanda.
- Garantiza el ancho de banda para los servicios.
- Permite realizar filtrado de contenido en base a URLs.
- Soporta la administración de usuarios prepago y post-pago.
- Permite personalizar y controlar la autenticación de un usuario. Además maneja la funcionalidad de RADIUS *proxy*.

[62] Fuente: Corporación Nacional de Telecomunicaciones.

- Soporta el atributo VSA permitiendo la comunicación con un servidor o cliente RADIUS de otro vendedor.
- Ofrece escalabilidad y redundancia por medio de balanceo de carga entre los servidores que conformen la solución.
- Provee un repositorio para información relacionada con los suscriptores, historial de servicios, de sesiones de autenticación y *accounting*, entre otras.
- Permite la comunicación con sistemas externos como portales web y OSSs (*Operations Support Systems* / Sistemas de Soporte de Operaciones) como el sistema de facturación.
- Permite determinar qué servicios deben estar activos o inactivos en base a métricas como el tiempo o ancho de banda de un servicio.
- Posee una interfaz gráfica de usuario (GUI) que permite configurar servicios y suscriptores.
- Posee un módulo para el monitoreo de la red el cual provee estadísticas de tráfico en tiempo real.

El sistema AAA expuesto no posee como característica la funcionalidad DPI, para poder implementarla se lo puede realizar mediante la incorporación del módulo *ASE (Advanced Services Engine / Motor de Servicios Avanzados)*, el cual se lo ubicaría en el equipo SmartEdge (BRAS). Este módulo puede identificar principalmente aplicaciones P2P proveyendo una mayor seguridad y eficiencia a la red debido a que permite la limitación de recursos por aplicación o por grupo de aplicaciones.

Dentro de la solución los portales para la interacción con el cliente para el auto-aprovisionamiento del servicio se desarrollan en base a una aplicación web misma que se comunicará con el sistema AAA por medio de XML.

En la Tabla 4.6 se presenta un resumen de las características del o los equipos requeridos para implementar esta solución.

NetOp PM Application Server		
Servidor Sun SPARC Enterprise T5220	Procesador	Quad-Core 1.2GHz UltraSPARC T2
	Memoria	8 GB (4 x 2GB DIMMs)
	Disco Duro	292 GB (2x146 GB)
	Interfaces	4 x 10/100/1000 Ethernet, 4 USB, 1 puerto serial
	Potencia	750 W a 1000 W
	Temperatura de operación	5ºC a 35ºC
	Peso	25 Kg aprox.
	Dimensiones	88mm x 425mm x 714mm (Alto x ancho x profundidad)
	Sistema operativo	Solaris 10
	Cantidad de equipos	2
NetOp PM Database Host		
Servidor Sun SPARC Enterprise T5220	Procesador	8-Core 1.2 GHz UltraSPARC T2
	Memoria	8 GB (4 x 2GB DIMMs)
	Disco Duro	292 GB (2x146 GB)
	Interfaces	4 x 10/100/1000 Ethernet, 4 USB, 1 puerto serial
	Sistema operativo	Solaris Med
	Cantidad de equipos	2
ORACLE Data Guard Observer Host		
Estación de trabajo Sun Ultra 20	Procesador	Dual Core 2.4GHz
	Memoria	2 GB (2x1GB DIMM)
	Disco duro	250 GB SATA HDD
	Cantidad de equipos	1

Tabla 4.6. Características generales del sistema AAA Ericsson

4.3.2.1 Integración

En esta sección se detallará la manera en la cual la plataforma AAA NetOp PM realizará la integración con las plataformas existentes en la CNT.

4.3.2.1.1 BRAS

Para la integración de los BRAS con el sistema AAA emplea el protocolo RADIUS. Se debe adicionar la licencia para la funcionalidad *Radius Change-of-Authorization (CoA)* para la integración con otros fabricantes.

4.3.2.1.2 Plataforma CDMA

La integración hacia la red CDMA 450 se realizará en base a las funcionalidades del protocolo RADIUS.

4.3.2.1.3 Sistema de Tarifación

Para la integración del sistema AAA con la plataforma prepago se va realizar en base a la especificación *Diameter Credit Control Application (DCCA)* la cual emplea el protocolo *Diameter* para realizar una tarifación en tiempo real del servicio y *Diameter interface Ro*.
Para la integración del sistema AAA con la plataforma post-pago lo realiza utilizando SOAP/XML.

Para la integración de esta solución con el sistema de tarifación que la empresa posee se requiere que éste cumpla con la especificación DCCA y cuente con la interfaz Ro.

En la Figura 4.3 se puede observar de manera general la integración del sistema AAA con las plataformas existentes en la CNT.

En la Figura 4.4 se muestra un diagrama general de la solución a la primera alternativa.

4.3.3 ANÁLISIS DE LA SOLUCIÓN

En base a los requerimientos presentados en la Tabla 4.1 se procederá a realizar un análisis de las soluciones presentadas. En base a esto se determinará si éstas

cumplen o no con los requerimientos que debe poseer el sistema AAA (ver Tabla 4.7).

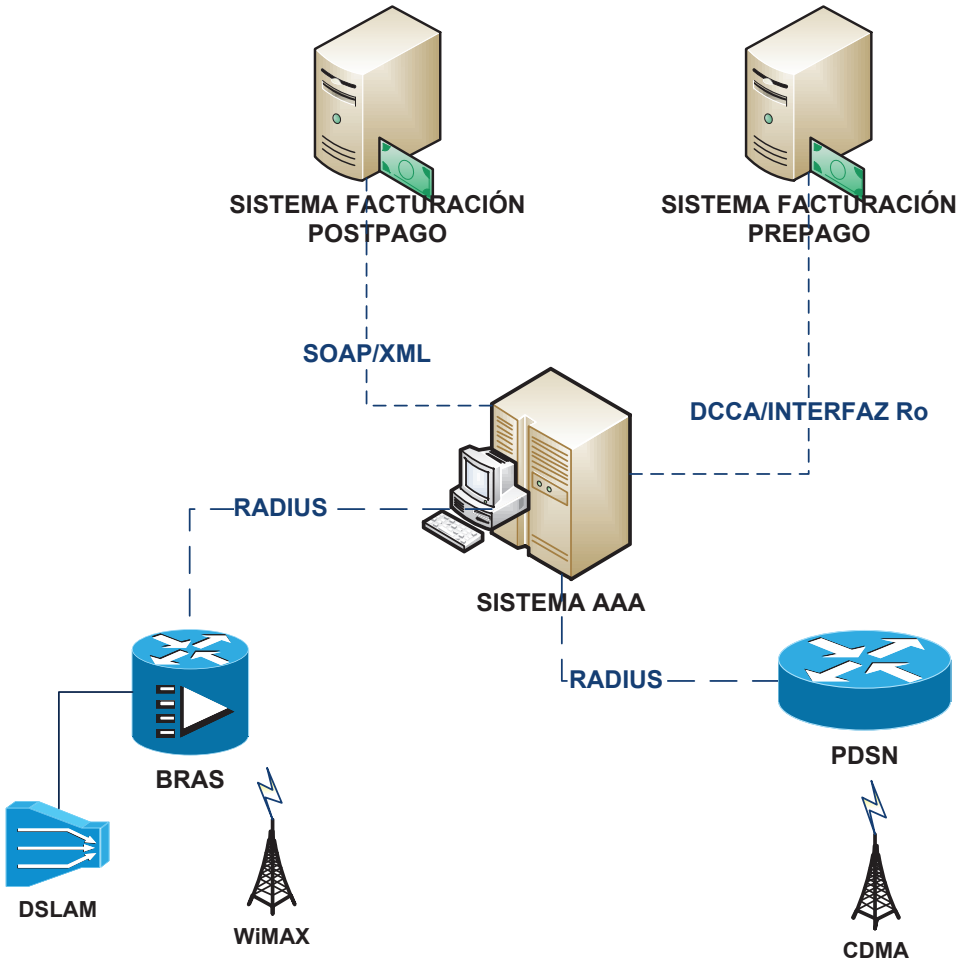


Figura 4.3. Solución de integración de plataformas Ericsson

4.3.3.1 Selección de la Solución

En base a lo expuesto en la Tabla 4.7 se puede observar que las dos soluciones cumplen “a su manera” con los requisitos del sistema AAA que la empresa necesita. Sin embargo, se requiere determinar cuál de las dos soluciones sería la más adecuada para la empresa; para esto se podría emplear la sugerencia de calificar cada una de las alternativas en base a un modelo de puntuación indicado en la Tabla 4.1 y cuyos resultados se muestran en la Tabla 4.8. De las características o requerimientos que se deben cumplir, aquellos que conllevan un mayor detenimiento en su análisis tienen relación con la integración de las diferentes plataformas con el sistema AAA centralizado.

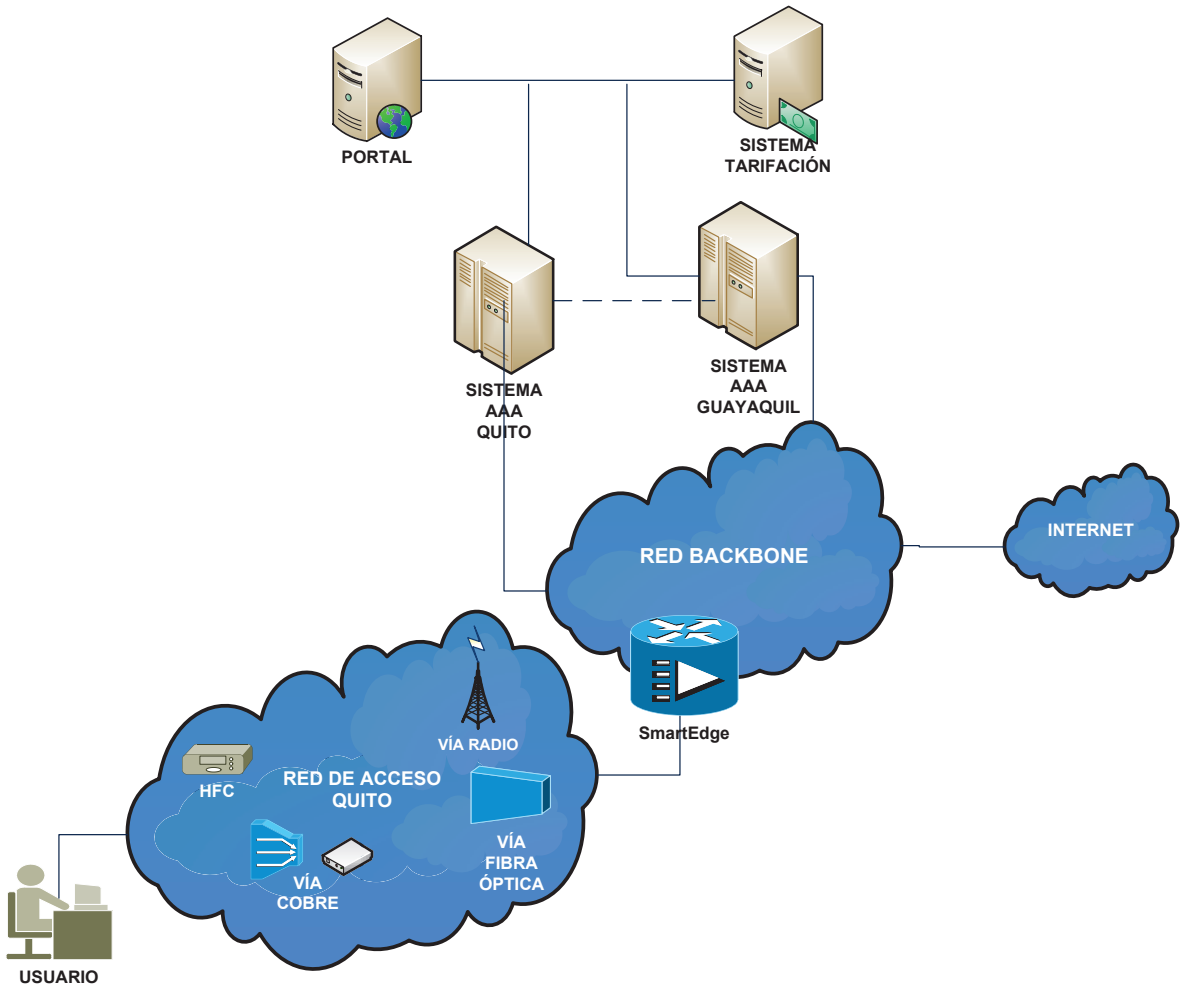


Figura 4.4. Diagrama de la solución general planteada a la segunda alternativa[63]

En el caso de Huawei, el sistema AAA cumple con los estándares dados por IETF, 3GPP, *WiMAX Forum*, 3GPP2 permitiendo que la integración con plataformas o dispositivos de otros fabricantes se realice sin problemas siempre y cuando estos cumplan con los estándares mencionados. Esta característica sería muy útil para la integración de los BRAS Ericsson existentes.

Además, esta empresa tendría una ventaja significativa ya que tanto la plataforma prepago como la PDSN de la red CDMA450 y ciertos equipos BRAS pertenecen a esta casa comercial y su integración con el sistema AAA centralizado sería más sencilla y podrían garantizar la interoperabilidad entre estas infraestructuras.

[63] Fuente: Corporación Nacional de Telecomunicaciones.

		SOLUCIÓN AAA HUAWEI	*SOLUCIÓN AAA ERICSSON*
NUMERAL	**REQUERIMIENTO**	**CUMPLE**	**CUMPLE**
1	Soportar la autenticación de clientes de diversas tecnologías de acceso como xDSL, WiMAX, y CDMA450.	Si	Si
2	Integración con las plataformas existentes en la CNT:		
2.1	BRAS marca Redback.	Si	Si
2.2	BRAS marca Huawei.	Si	Si*
2.3	PDSN marca Huawei de la red CDMA450.	Si	Si*
2.4	Plataforma prepago marca Huawei.	Si	Si*,**
2.5	Plataforma de facturación.	Si	Si*
3	Soportar protocolo RADIUS en base al RFC 2865, RFC 2866 y sus extensiones.	Si	Si
4	Soportar al protocolo *Diameter* en base al RFC 3588 y RFC 4005.	Si	Si
5	Soportar el protocolo FTP y/o *Web services*.	Si	Si
6	Poseer funcionalidad de RADIUS *proxy*.	Si	Si
7	Soportar clientes prepago y post-pago.	Si	Si
8	Permitir la generación de CDRs para enviar información al sistema de tarifación.	Si	Si
9	Permitir asignación estática o dinámica de direcciones IP a los suscriptores.	Si	Si
10	Permitir la asignación de una dirección IP o un pool de direcciones IP a un suscriptor.	Si	Si
11	Autenticar clientes que no tengan dominio.	Si	Si
12	Soportar el manejo de una tarjeta prepago.	Si	Si
13	Permitir la facturación en tiempo real.	Si	Si
14	Debe disponer de redundancia geográfica de manera que se garantice que en caso de fallos en Quito o en Guayaquil la solución se mantendrá operativa.	Si	Si
15	Permitir autenticación mediante protocolos PAP, CHAP, EAP.	Si	Si
16	Operar como *Access Network* AAA, *Broker* AAA, *Home* AAA y *Visited* AAA para la autenticación de usuarios de la red CDMA.	Si	Si***
17	Permitir la aplicación de políticas de calidad de servicio.	Si	Si
18	Permitir el filtrado de contenido.	Si	Si
19	Permitir el control de tráfico de servicios.	Si	Si
20	Permitir el control de ancho de banda.	Si	Si
21	Permitir la gestión de umbrales.	Si	Si

CONTINÚA

		SOLUCIÓN AAA HUAWEI	*SOLUCIÓN AAA ERICSSON*
NUMERAL	**REQUERIMIENTO**	**CUMPLE**	**CUMPLE**
22	Permitir el *caching*.	Si	Si
23	Poseer mecanismos de seguridad para evitar ataques de denegación de servicio.	Si	Si
24	Permitir su gestión de manera gráfica y por medio de CLI.	Si	Si
25	Poseer de mecanismos para monitoreo de la plataforma.	Si	Si
26	Soportar el manejo de portales que interactúen con el usuario.	Si	Si
27	Soportar 600.000 usuarios.	Si	Si
Nota: ***: Requiere de la realización de pruebas de interoperabilidad.** ****: Este proceso requiere que se cumplan funcionalidades específicas caso contrario la CNT debe tomar la responsabilidad de conseguir los recursos necesarios para realizar los cambios.** *****: Desarrollo bajo pedido.**			

Tabla 4.7. Análisis de los requerimientos

En el caso de Ericsson, dado que se requiere que los equipos cumplan con ciertas características para la integración, se debería llevar a cabo pruebas de interoperabilidad entre los dispositivos que se van a integrar al sistema AAA centralizado para evaluar si es posible o no realizar la integración de plataformas con los protocolos que soporta este equipamiento.

Para llevar a cabo dichas pruebas se deberá simular un ambiente de laboratorio empleando los equipos que intervienen en la integración y se encuentran en producción teniendo que elaborarse un cronograma de actividades para que el momento que se ejecuten, estas causen el menor impacto en los usuarios. En el caso que en estos estudios se determine que las plataformas necesitan características adicionales para poder llevar a cabo la integración, se deberá coordinar con Huawei para que las implemente en sus equipos. Esto conlleva a que se tengan que invertir mayores recursos tanto de tiempo como económicos puesto que si deben integrar nuevas funcionalidades al equipo, esto requerirá de un desarrollo por parte de Huawei mismo que tomará tiempo y tendrá un costo en base a las modificaciones pedidas.

En cuanto a las licencias existentes en la CNT y que se presentan en la Tabla 3.8 se puede decir que al momento de implementar la solución de Huawei se podría reutilizar un mayor número de licencias en relación a la solución de Ericsson.

En base a lo expuesto, se puede decir que la solución AAA de Huawei es la más adecuada y viable para ser implementada por la empresa puesto que satisface de mejor manera los requerimientos de la misma. Además, al ser propietarios de la mayor cantidad de equipos que participan en la integración se facilita la interacción, actualización e interoperabilidad de éstos con la nueva plataforma AAA. En el caso de que se requiera de un desarrollo adicional sobre los dispositivos, los tiempos de ejecución serán menores.

4.4 PLAN DE MIGRACIÓN DE CLIENTES

El plan de migración de clientes debe ser coordinado en conjunto con personal de CNT. A continuación se indican algunas sugerencias de los procedimientos que se pueden seguir para su ejecución:

- Recopilar la información de clientes que se encuentran en cada una de las plataformas que la empresa maneja para la provisión de autenticación, autorización y *accounting.*
- Homologar la información obtenida, de esta manera se podrá definir campos críticos a ser migrados, además de garantizar que se maneja el mismo tipo de datos y así evitar una pérdida de los mismos. Esto también permitirá establecer el volumen de los datos que deben ser migrados.
- Migrar los clientes de manera progresiva a la nueva plataforma; para lo cual se podría elaborar un *script*[64] que permita la migración de datos de manera automática debida a la cantidad de usuarios a ser migrados.

[64] Un script es un programa que contiene diversos comandos, mismos que pueden ser ejecutados de una manera sencilla por parte del usuario.

			SOLUCIÓN AAA HUAWEI	*SOLUCIÓN AAA ERICSSON*
NUMERAL	**REQUERIMIENTO**		**PUNTAJE**	**PUNTAJE**
1	Soportar la autenticación de clientes de diversas tecnologías de acceso como xDSL, WiMAX, y CDMA450.	30	30	30
2	Integración con las plataformas existentes en la CNT:			
2.1	BRAS marca Redback.	30	25	30
2.2	BRAS marca Huawei.	30	30	20
2.3	PDSN marca Huawei de la red CDMA450.	30	30	20
2.4	Plataforma prepago marca Huawei.	30	30	20
2.5	Plataforma de facturación.	30	25	20
3	Soportar protocolo RADIUS en base al RFC 2865, RFC 2866 y sus extensiones.	30	30	30
4	Soportar al protocolo *Diameter* en base al RFC 3588 y RFC 4005.	30	30	30
5	Soportar el protocolo FTP y/o *Web services*.	30	30	30
6	Poseer funcionalidad de RADIUS *proxy*.	30	30	30
7	Soportar clientes prepago y post-pago.	30	30	30
8	Permitir la generación de CDRs para enviar información al sistema de tarifación.	30	30	30
9	Permitir asignación estática o dinámica de direcciones IP a los suscriptores.	30	30	30
10	Permitir la asignación de una dirección IP o un pool de direcciones IP a un suscriptor.	30	30	30
11	Autenticar clientes que no tengan dominio.	20	20	20
12	Soportar el manejo de una tarjeta prepago.	20	20	20
13	Permitir la facturación en tiempo real.	20	20	20
14	Debe disponer de redundancia geográfica de manera que se garantice que en caso de fallos en Quito o en Guayaquil la solución se mantendrá operativa.	30	30	30
15	Permitir autenticación mediante protocolos PAP, CHAP, EAP.	20	20	20
16	Operar como *Access Network* AAA, *Broker* AAA, *Home* AAA y *Visited* AAA para la autenticación de usuarios de la red CDMA.	20	20	20
17	Permitir la aplicación de políticas de calidad de servicio.	20	20	20
18	Permitir el filtrado de contenido.	20	20	20
19	Permitir el control de tráfico de servicios.	20	20	20
20	Permitir el control de ancho de banda.	20	20	20

CONTINÚA

			SOLUCIÓN AAA HUAWEI	*SOLUCIÓN AAA ERICSSON*
NUMERAL	**REQUERIMIENTO**		**PUNTAJE**	**PUNTAJE**
21	Permitir la gestión de umbrales.	20	20	20
22	Permitir el *caching*.	20	20	20
23	Poseer mecanismos de seguridad para evitar ataques de denegación de servicio.	20	20	20
24	Permitir su gestión de manera gráfica y por medio de CLI.	10	10	10
25	Poseer de mecanismos para monitoreo de la plataforma.	10	10	10
26	Soportar el manejo de portales que interactúen con el usuario.	20	20	20
27	Soportar 600.000 usuarios.	30	30	30
TOTAL			750	720

Tabla 4.8. Análisis de requerimientos mediante un esquema de puntuación

- Crear un ambiente de pruebas con el nuevo equipamiento y que sea independiente del sistema AAA actual. De esta manera se podrá depurar la información además de observar y determinar soluciones a posibles problemas que se presenten.
- Monitorear el sistema para asegurarse que no existan errores en su configuración y que impidan la provisión correcta del servicio.

En la Figura 4.5 se muestra un diagrama de flujo del procedimiento sugerido para la migración de clientes.

4.5 CRONOGRAMA DE ACTIVIDADES

En la Figura 4.6 se expone un cronograma base de las diversas actividades a ser ejecutadas para la realización del presente proyecto.

Como primera fase se procederá con el levantamiento de información lo que permitirá definir los requerimientos de la empresa y proceder con la ingeniería del proyecto, etapa en la cual se realizará el diseño de la solución.

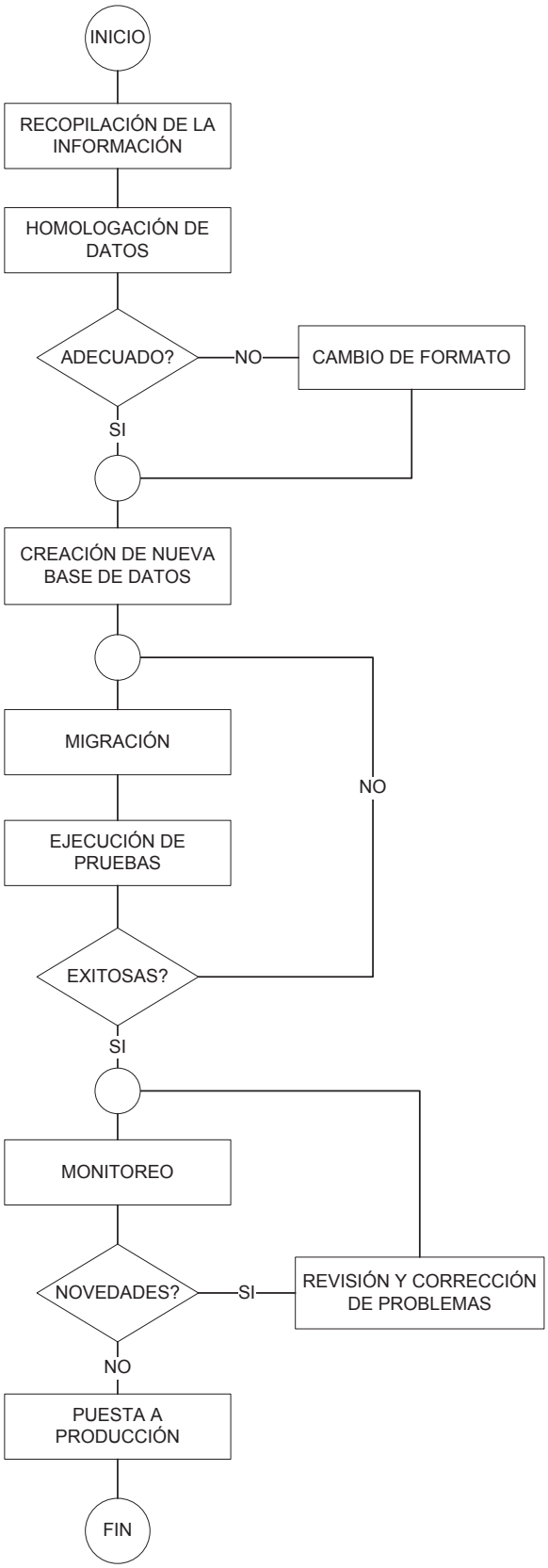


Figura 4.5. Diagrama de flujo del proceso sugerido para migración de clientes

En base a la fase anterior se elaborarán las bases para la licitación pública del proyecto, la cual se efectuará mediante el Portal de Compras de Públicas de acuerdo al reglamento general de la Ley Orgánica del Sistema Nacional de Contratación Pública.

Luego de concluir con la etapa de licitación se ejecutará la fase de instalación de la nueva plataforma, así como la integración de ésta a la infraestructura de la empresa y la remoción de los equipos antiguos.

4.6 MANUAL DE ADMINISTRACIÓN

En el anexo A se presenta un manual que permite la administración del sistema AAA centralizado. En éste se expondrán datos teóricos y técnicos que ayuden con la capacitación del personal, el mantenimiento de equipos y la administración del sistema AAA centralizado.

Éste se basa en la solución propuesta en la primera alternativa ya que del análisis realizado se cree que ésta se acopla de mejor manera a los requerimientos expuestos.

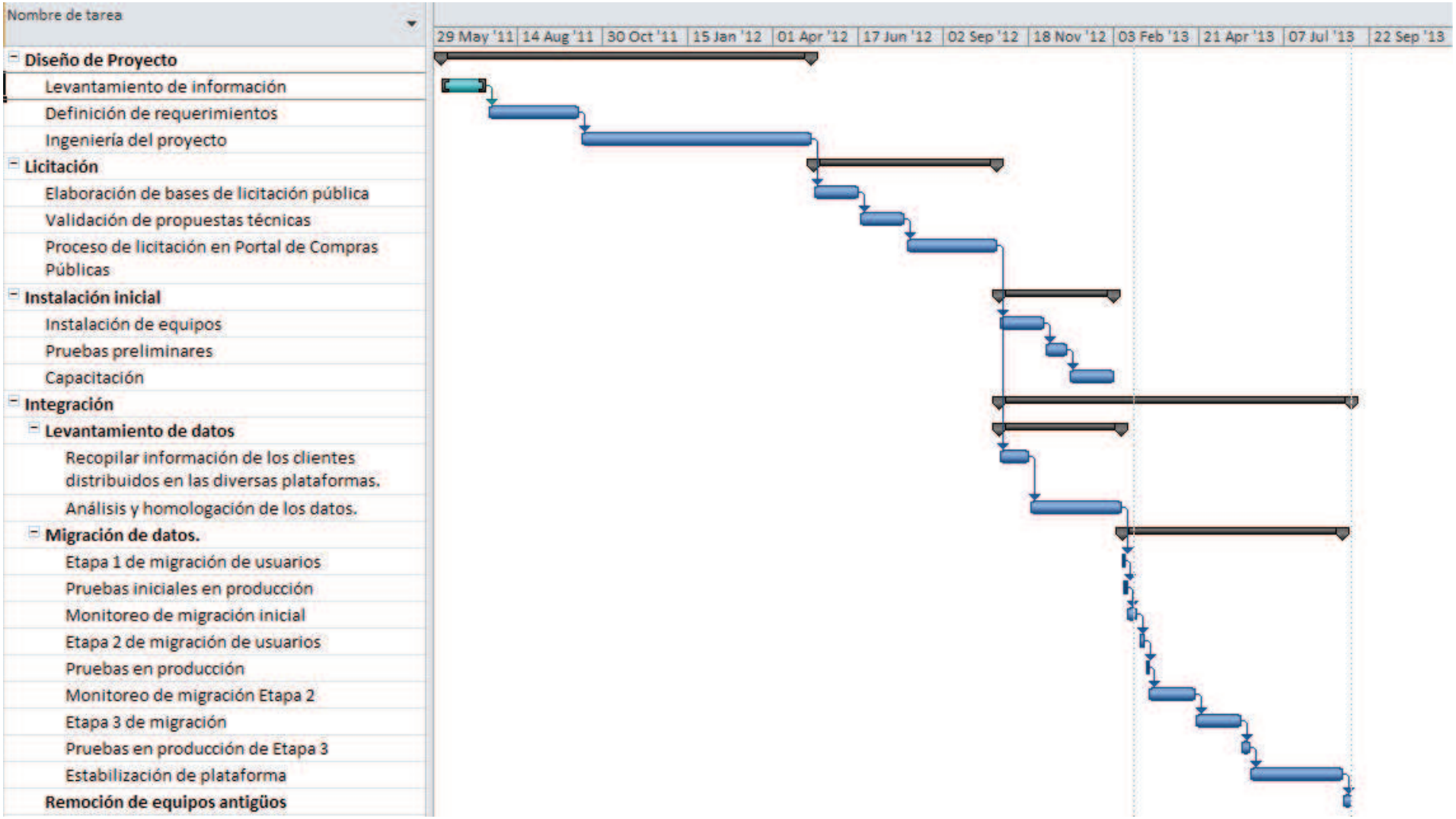


Figura 4.6. Cronograma de actividades propuesto

CAPÍTULO 5

PLAN PARA MEJORA DEL SERVICIO

5.1 INTRODUCCIÓN

En la actualidad, dado el avance de la tecnología, las empresas requieren innovarse periódicamente con el fin de mejorar los servicios que ofertan así como proporcionar nuevos servicios a sus clientes. Esto ha originado que las empresas incorporen a su forma de administrar diversas metodologías que permitan un manejo eficaz de los procesos del negocio y sus clientes, sin afectar su rentabilidad.

Existen varias metodologías a nivel de gestión que ofertan lineamientos para la administración de una empresa tanto a nivel comercial, financiero como tecnológico. Algunos de estos procedimientos se encuentran enfocados principalmente a empresas de telecomunicaciones o del sector IT (*Information Technology* / Tecnología de Información).

Como se menciona en el Capítulo 2, en la CNT no se ha definido una metodología específica para la administración del negocio, maneja un modelo de integración entre eTOM e ITIL con tendencia a la implementación del proyecto NGOSS.

En el presente capítulo se desarrollará un plan de mejora para la solución AAA en base a la etapa de gestión de la continuidad del servicio correspondiente a la fase de diseño y a las etapas de gestión de eventos y gestión de incidentes orientado en la fase de operación de ITIL v3.

5.2 LINEAMIENTOS BASE PARA ELABORAR EL PLAN [1] [2]

Como se conoce ITIL (*Information Technology Infrastructure Library* / Biblioteca de Infraestructura de Tecnologías de la Información) es un conjunto de normas

y/o procedimientos que permiten el control, dirección y gestión de servicios de tecnologías de la información, las cuales ayudan a una empresa a ofrecer servicios de acuerdo a sus necesidades y a un costo aceptable.

Una de las etapas de ITIL V3 corresponde a la gestión de la continuidad de los servicios IT el cual establece planes de contingencia que aseguren la continuidad del servicio frente a una grave interrupción provocada por desastres naturales u otras causas de fuerza mayor.

Dentro de ésta se define el proceso de análisis de riesgos, el cual permitirá determinar la severidad de la interrupción de un servicio para de esta manera diseñar una estrategia que facilite el manejo de los problemas generados y así poder asegurar los niveles de disponibilidad del servicio. A continuación se detallan algunas opciones para su manejo:

- Creación de un manual para el manejo del servicio.
- Establecer el tipo de recuperación frente a desastres que el servicio requiere en base a las necesidades de la empresa.
- Capacitar al personal para el manejo adecuado de la infraestructura que conforma el servicio.

La operación de servicio constituye otra de las fases de ITIL v3 y entre sus procesos se definen la gestión de eventos y la gestión de incidentes lo cuales proporcionarán soluciones y procedimientos para asegurar el uso estructurado de recursos con el fin de prevenir y reducir problemas provocados por fallas en un servicio. A continuación se detallan algunas opciones para su uso:

- Establecer el monitoreo de la solución.
- Detectar posibles incidentes.
- Determinar el tipo de evento que se presenta.

Una vez establecidos los puntos antes detallados se podrán identificar problemas sobre el servicio o su infraestructura y a su vez proponer soluciones o tomar decisiones sobre las acciones a efectuarse para corregir el evento.

5.3 PLAN PROPUESTO

5.3.1 PRIMER PASO

Como primer paso se procederá con la elaboración de un catálogo de servicio el cual contendrá información que ayudará al personal a conocer el estado de un servicio, además facilitará su difusión con otras áreas. Este catálogo, por lo general contiene la siguiente información:

- Características del servicio.
- Formas de acceso al servicio.
- Información del costo del servicio (si se considera relevante).
- Información de contacto de proveedores (si los hay).
- Información sobre los niveles de servicio.
- Estado del servicio.
- Cambios y/o excepciones.
- Fecha de revisión y versión.

En base a las características antes expuestas, en la Tabla 5.1 se indica un modelo sugerido de este documento para la solución AAA.

5.3.2 SEGUNDO PASO

Como segundo paso se establece el monitoreo del servicio para lo cual se describen algunas tareas a ser definidas antes de efectuarlo.

1. Los servicios o componentes a ser monitoreados.
2. La frecuencia del monitoreo.

3. Las herramientas o programas a emplear para el monitoreo.

CARACTERÍSTICA	DESCRIPCIÓN
Nombre del servicio	Sistema AAA Centralizado
Descripción del Servicio	Este sistema administra a los usuarios y controla el acceso de estos a los recursos de la red. Además refuerza políticas, audita el uso de los recursos y provee de la información necesaria para la facturación de un servicio.
Propietario del servicio	Gestión ATM / IP-MPLS
Niveles de servicio	El servicio deberá estar disponible 24 horas al día los siete días de la semana (24/7).
Forma de acceso al servicio	Para acceder al sistema, el administrador, lo puede realizar por medio de una interfaz gráfica o por medio de la línea de comandos.
Estado del servicio	En diseño
Clientes y/o usuarios	Usuarios banda ancha prepago y post-pago provenientes de diversas plataformas de acceso.
Proveedores	Empresas que brinden soporte a los equipos empleados en la solución por ejemplo Huawei, Ericsson.
Cambios y/o excepciones	Al momento no se tienen cambios, una vez puesto en producción se deberá monitorizar el sistema para evaluar el rendimiento del mismo y proponer modificaciones al mismo si es necesario.
Fecha de revisión y versión	Septiembre 2012 – versión 1.0

Tabla 5.1. Catálogo del servicio para la solución AAA

Antes de empezar con el monitoreo del servicio y/o sus componentes es necesario definir los siguientes aspectos:

- Parámetros que se deben medir.
- Parámetros que se pueden medir.

Para definir los parámetros que se deben medir se puede recurrir a la siguiente información:

- Catálogo de servicio.
- Metas y/u objetivos de la empresa.
- Metas y/u objetivos del área donde se encuentra el servicio (si las hay).

Para definir los parámetros que se pueden medir, se debe:

- Enlistar las herramientas de monitoreo con las que se cuenta en el área que gestiona el servicio.
- Obtener reportes de monitoreo (si los hay).
- Poseer los manuales técnicos y de usuario de las herramientas y/o servicio.
- Conocer las funcionalidades o flujos de trabajo que se manejen en la empresa para el servicio.

Se debe definir también la frecuencia y la manera de presentación de la información obtenida del monitoreo, dado que esto permitirá la elaboración de reportes que ayudarán al análisis de los datos. Por ejemplo, dependiendo del volumen e importancia de datos obtenidos se puede procesar la información de manera semanal o mensual, y la misma puede ser separada en base a las siguientes directrices:

- Frecuencia de uso del servicio.
- Momentos del día en el cual se tiene mayor uso del servicio.
- El rendimiento de cada componente empleada para brindar el servicio.
- Disponibilidad del servicio.

En base a lo expuesto, a continuación se sugieren los procedimientos a seguir para instaurar el monitoreo del sistema AAA centralizado por el área de gestión

ATM / IP-MPLS, mismo que ayudará a detectar fallas o eventos que pueden afectar la provisión de sus servicios.

1. Definir lo que se debería monitorizar.
2. Determinar lo que se puede medir.
3. Enlistar las herramientas de monitoreo con las que el área cuenta para realizar el monitoreo y definir sus características principales.
4. Seleccionar la herramienta o herramientas de monitoreo a emplearse.
5. Determinar la frecuencia del monitoreo.
6. Iniciar el monitoreo.

Para definir los parámetros que se deberían medir en el sistema AAA centralizado, se debe establecer el o los objetivos y/o metas que la empresa y/o área de gestión ATM / IP-MPLS desean alcanzar con el proyecto, además emplear el catálogo de servicios. Entre los objetivos a tomar en cuenta para establecer estos parámetros se tienen:

- Objetivo de la empresa: *"Integrar al país al mundo, mediante la provisión de soluciones de telecomunicaciones innovadoras, con talento humano comprometido y calidad de servicio de clase mundial."*[65]
- Objetivo del proyecto en el área ATM / IP-MPLS: "*Implementar un sistema AAA centralizado que permita aprovisionar los servicios y usuarios, diferenciar y personalizar los recursos de red, examinar y monitorear los usuarios y el tipo de tráfico que cursa por el sistema, controlar la calidad de servicio y brindar seguridad mediante el control de acceso a los recursos*."

En base a lo expuesto se establecen los siguientes parámetros que deberían ser medidos:

[65] Fuente: Corporación Nacional de Telecomunicaciones (http://www.cnt.gob.ec/index.php/mision-vision-valores).

- Número de clientes que se conectan a la plataforma AAA.
- Acceso a los portales.
- Tráfico generado por la plataforma AAA.
- Servicios de valor agregado como video bajo demanda, ancho de banda bajo demanda.
- Funcionamiento de alta disponibilidad.
- Calidad de servicio.

Para determinar los parámetros que podrían ser medidos, se debe considerar las funcionalidades del servicio que el personal del área considere importantes para ser monitoreadas, ya que esto les ayudará a determinar futuros eventos sobre la plataforma. Entre estas características se tienen:

- Tráfico generado por la plataforma.
- Número de clientes que se conectan a la plataforma.

Una vez definidas las características más importantes del servicio a ser medidas se procede a identificar si las herramientas de monitoreo con las que cuenta la empresa permiten o no medir las funcionalidades que se requiere.

El área ATM / IP-MPLS cuenta con los siguientes programas para realizar el monitoreo de la red *backbone*:

- Cacti.
- Cisco ANA.

El primero, es un programa gratuito que permite monitorizar y visualizar mediante gráficas los dispositivos conectados a una red por medio del protocolo SNMP; mientras que el segundo, es un programa propietario que permite monitorizar los equipos de red marca Cisco, así como una variada tecnología de red como MPLS.

Dado que Cacti es una herramienta que permite incorporar al monitoreo diversos equipos, si estos cuentan con el protocolo SNMP, se considera que éste es el adecuado para efectuar el monitoreo de las características a ser medidas en el sistema AAA centralizado; pero se debe tener en cuenta que si existe la necesidad de incorporar nuevas características para monitorearlas y este programa no las puede cumplir la empresa deberá adquirir una herramienta más sofisticada.

La frecuencia con la que se debe efectuar el monitoreo se encuentra relacionada con los parámetros a ser medidos y los requerimientos del área que efectúa el monitoreo; al combinar estos factores se establece un monitoreo de 24/7, es decir, las 24 horas los siete días de la semana.

Por otro lado, la información obtenida del monitoreo debe ser almacenada para posteriormente ser procesada y analizada. Por lo general, los programas de monitoreo dentro de su estructura manejan una base de datos en la cual se almacena toda la información recopilada durante el tiempo que se efectúa el monitoreo de un componente, y a su vez permiten visualizarla de maneras diferentes. Estas características son útiles, una vez definido como se van a presentar los datos al personal del área encargado de analizarlos, y su periodicidad.

Para el sistema AAA centralizado se considera importante efectuar un análisis mensual de los datos, enfocándose en los momentos del día en los cuales se tiene el mayor número de usuarios, ya que esto permitirá determinar si existe un crecimiento de los usuarios que usan el servicio, o si la plataforma está llegando a su saturarse.

Los procedimientos antes detallados se presentan en la Tabla 5.2.

Para llevar a cabo las etapas de procesamiento y análisis de datos, a continuación se detallar algunas sugerencias.

PROCEDIMIENTO	CARACTERÍSTICA
Objetivo del proyecto	Implementar un sistema AAA centralizado que permita aprovisionar los servicios y usuarios, diferenciar y personalizar los recursos de red, examinar y monitorear los usuarios y el tipo de tráfico que cursa por el sistema, controlar la calidad de servicio y brindar seguridad mediante el control de acceso a los recursos.
Parámetros que se deben medir	• Clientes que se conectan a la plataforma. • Acceso a portales. • Tráfico generado por la plataforma. • Servicios de valor agregado. • Funcionamiento de alta disponibilidad. • Calidad de servicio
Herramientas de monitoreo con las que cuenta el área	• Cacti, es un programa gratuito que permite monitorizar y visualizar mediante gráficas los dispositivos conectados a una red. • Cisco ANA, programa propietario que permite monitorizar los equipos de red Cisco así como una variada tecnología de red como MPLS.
Herramienta escogida	• Cacti
Parámetros que se pueden medir	• Tráfico generado por la plataforma. • Número de clientes que se conectan a la plataforma.
Frecuencia del monitoreo	• 24/7
Frecuencia procesamiento de datos	• Mensual
Forma de presentación de los datos	• Momentos del día en el cual se tiene mayor uso del servicio.

Tabla 5.2. Procedimientos a seguir para establecer el monitoreo de la solución AAA

- Procesamiento de los datos

Parte del procesamiento de los datos obtenidos durante el monitoreo lo conforma la elaboración de reportes o informes que faciliten posteriormente el análisis de los mismos; para esto se puede establecer un formato que sirva de guía para la preparación de éstos, por ejemplo:

1. Fecha de elaboración del reporte.
2. Elaborar un resumen sobre los resultados obtenidos.
3. Colocar gráficas y/o tablas que faciliten la comprensión de los resultados.
4. Señalar eventos y/o actividades que hayan afectado directa o indirectamente a la prestación de un servicio.

5.3.2.1 Análisis de los datos

Esta etapa consiste en efectuar una evaluación de la información obtenida por medio del procesamiento de los datos para poder identificar si el servicio presenta problemas, y requiere o no de modificaciones.

Para efectuar el análisis de los datos se sugiere contar con:

- Reportes previos.
- Crear un cuadro en el cual se definan los principales requerimientos o metas en base a los cuales el servicio fue diseñado o debe poseer para su buen funcionamiento.
- Manuales o información técnica de los equipos que conforman la infraestructura del servicio.

5.3.3 TERCER PASO

El mantenimiento preventivo de la solución AAA es un procedimiento que se lo debe realizar de manera periódica para de esta manera minimizar el riesgo de fallos y asegurar la correcta operación de los equipos, así como prolongar su tiempo de vida útil.

Para facilitar el mantenimiento de los equipos que conforman la infraestructura del sistema centralizado AAA se sugiere la elaboración de documentación que contenga información básica sobre los equipos, en ésta se debe incluir lo siguiente:

- Nombre del equipo.
- Modelo.
- Fabricante o proveedor.
- Ubicación.
- Frecuencia de mantenimiento.
- Fecha de operación del equipo.
- Duración de la garantía.

En la Tabla 5.3 se presenta un resumen de las características antes señaladas para los equipos que conforman la solución AAA.

Para el presente proyecto se han determinado algunos pasos generales a seguir para la rutina de mantenimiento:

- Inspeccionar las condiciones ambientales del equipo, por ejemplo humedad, polvo, temperatura, instalación eléctrica.
- Inspeccionar el equipo.
- Efectuar la limpieza del equipo.
- Ajustar y calibrar partes del equipo que se consideren necesarias.
- Revisar la configuración de la conectividad de los equipos.
- Realizar y revisar respaldos de la información relevante, por ejemplo bases de datos.

En la Figura 5.1 se presenta un diagrama de flujo para el proceso antes descrito.

Para el equipamiento nuevo y que posea garantía del proveedor o fabricante del mismo, no todas las tareas antes descritas pueden ser cumplidas por parte del personal de la empresa; en este caso, solo se podría ejecutar lo siguiente:

CARACTERÍSTICA	DESCRIPCIÓN
Nombre del equipo	Servidor AAA
Modelo	BLADE T6340
Fabricante o Proveedor	SUN
Ubicación	Quito, Guayaquil
Frecuencia del mantenimiento	Trimestral
Duración de la garantía	1 año
Fecha de operación del equipo	Junio 2013

CARACTERÍSTICA	DESCRIPCIÓN
Nombre del equipo	Controlador de tráfico
Modelo	SIG9800
Fabricante o Proveedor	HUAWEI
Ubicación	Quito, Guayaquil
Frecuencia del mantenimiento	Trimestral
Duración de la garantía	1 año
Fecha de operación del equipo	Junio 2013

CARACTERÍSTICA	**DESCRIPCIÓN**
Nombre del equipo	Controlador de políticas y filtrado de contenido
Modelo	RM9000
Fabricante o Proveedor	HUAWEI
Ubicación	Quito
Frecuencia del mantenimiento	Trimestral
Duración de la garantía	1 año
Fecha de operación del equipo	Junio 2013

CARACTERÍSTICA	DESCRIPCIÓN
Nombre del equipo	BRAS
Modelo	SE800
Fabricante o Proveedor	REDBACK
Ubicación	Quito, Guayaquil
Frecuencia del mantenimiento	Trimestral

CONTINÚA

Duración de la garantía	-
Fecha de operación del equipo	2006
CARACTERÍSTICA	DESCRIPCIÓN
Nombre del equipo	BRAS
Modelo	SE400
Fabricante o Proveedor	REDBACK
Ubicación	Guayaquil
Frecuencia del mantenimiento	Trimestral
Duración de la garantía	-
Fecha de operación del equipo	2006
CARACTERÍSTICA	DESCRIPCIÓN
Nombre del equipo	BRAS
Modelo	MA5200G
Fabricante o Proveedor	HUAWEI
Ubicación	Quito, Guayaquil
Frecuencia del mantenimiento	Trimestral
Duración de la garantía	-
Fecha de operación del equipo	2006
CARACTERÍSTICA	**DESCRIPCIÓN**
Nombre del equipo	Plataforma prepago
Modelo	UVC TELLIN
Fabricante o Proveedor	HUAWEI
Ubicación	Quito
Frecuencia del mantenimiento	Trimestral
Duración de la garantía	-
Fecha de operación del equipo	-
CARACTERÍSTICA	**DESCRIPCIÓN**
Nombre del equipo	PDSN
Modelo	9660
Fabricante o Proveedor	HUAWEI

CONTINÚA

Ubicación	Guayaquil
Frecuencia del mantenimiento	Trimestral
Duración de la garantía	-
Fecha de operación del equipo	2007
CARACTERÍSTICA	**DESCRIPCIÓN**
Nombre del equipo	WASN
Modelo	9770
Fabricante o Proveedor	HUAWEI
Ubicación	Quito
Frecuencia del mantenimiento	Trimestral
Duración de la garantía	-
Fecha de operación del equipo	2007

Tabla 5.3. Características básicas de los equipos del sistema AAA para su mantenimiento

- Inspeccionar las condiciones ambientales del equipo, por ejemplo humedad, polvo, temperatura, instalación eléctrica.
- Revisar la configuración de la conectividad de los equipos.
- Realizar y revisar respaldos de la información relevante, por ejemplo bases de datos.

En la Figura 5.2 se presenta un diagrama de flujo para el proceso antes descrito.

5.3.4 CUARTO PASO

Como resultado del análisis de datos o del mantenimiento realizado a la infraestructura se pueden identificar problemas en la misma, y dependiendo del tipo de inconveniente se puede establecer una guía para su tratamiento, por ejemplo:

1. Identificar el tipo de incidente, es decir, determinar que parte de la infraestructura está siendo afectada.

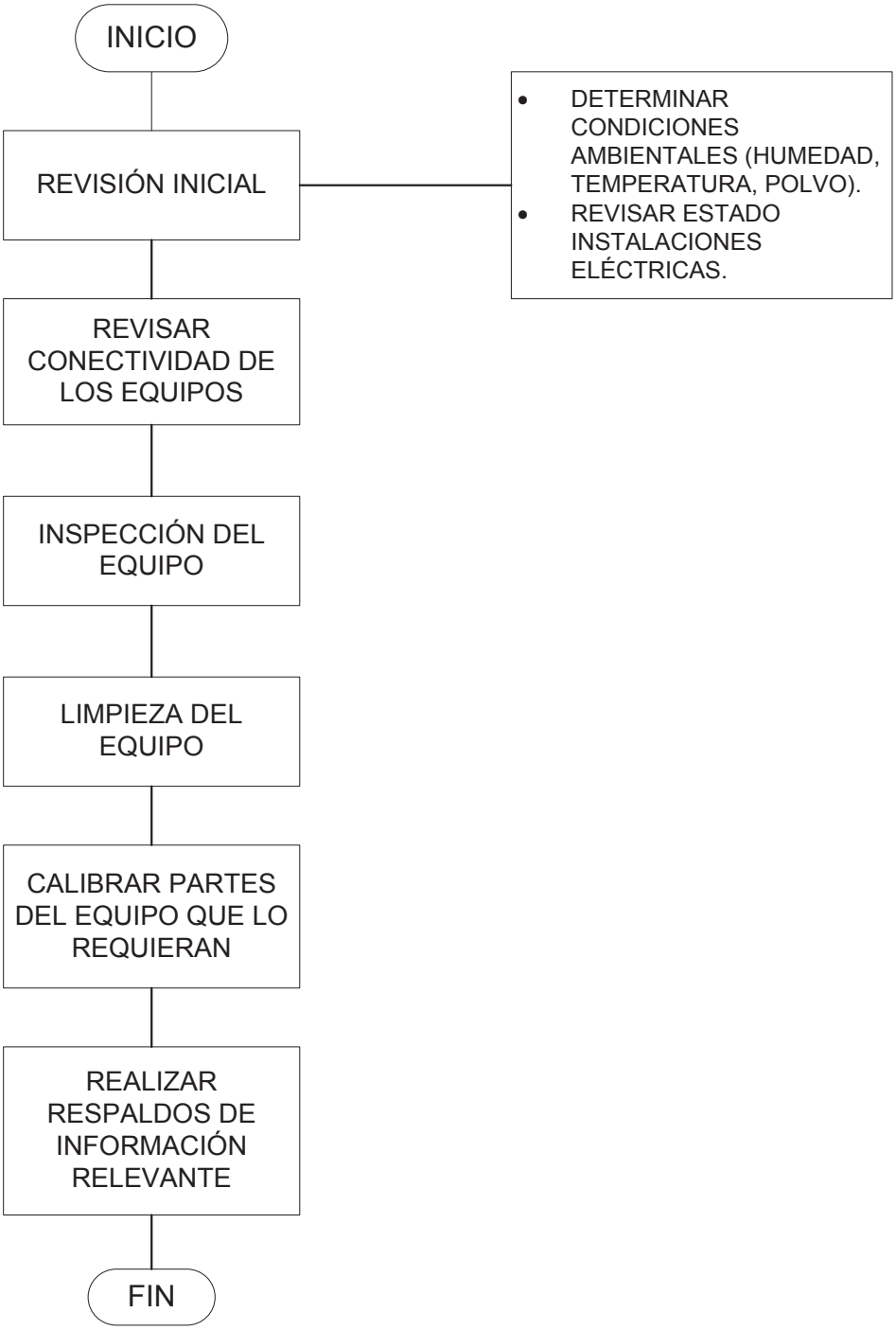


Figura 5.1. Diagrama de flujo para mantenimiento de equipos

2. Categorizar el incidente, para esto se debe determinar si el evento se produjo a nivel de hardware o software

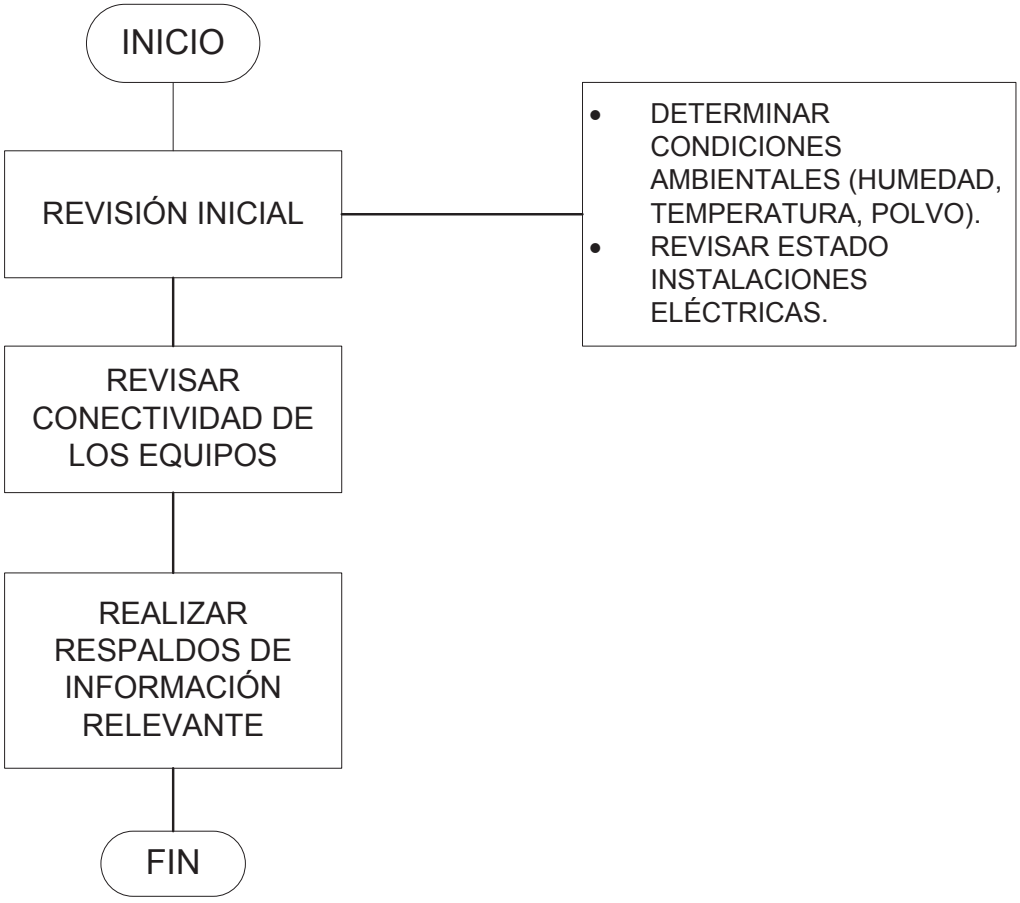


Figura 5.2. Diagrama de flujo para mantenimiento de equipos nuevos y/o garantía vigente

3. La prioridad de solución del incidente se basa en el impacto o nivel de afectación que este cause, por ejemplo, el número de usuarios afectados, número de servicios afectados.

4. Diagnóstico inicial del incidente permite tratar de determinar los errores o problemas que está generando el incidente sobre la infraestructura.

5. Una vez efectuada la revisión inicial se puede determinar si el problema puede ser solventado por personal del área o debe ser escalado bien a otra área de trabajo o a terceros.

6. Efectuar un análisis del evento y/o problemas encontrados en la revisión inicial y proceder con la solución de los mismos.

Dependiendo del impacto y la urgencia del evento sobre la plataforma se deben establecer niveles de prioridad, esto a su vez permitirá al área definir el tiempo

que se tendrá para su resolución y el personal que deberá atenderlo. Para el proyecto se han definido los siguientes niveles para clasificar los incidentes:

- Críticos.
- Medios.
- Bajos.

Se considerará un evento como critico cuando este afecte a un alto de número de usuarios al dejarlos sin servicio. Este tipo de eventos requerirán un tiempo de resolución de máximo 2 horas y será solventado por personal del área clasificado como nivel 2.

Se considerará un evento como medio cuando este afecte a un cierto número de usuarios. Este tipo de eventos requerirán un tiempo de resolución de máximo 4 horas y será resuelto por personal del área clasificado como nivel 1 y nivel 2.

Se considerará un evento como bajo cuando su afectación sea mínima, es decir, esta no interfiere con la prestación del servicio. Este tipo de eventos requerirán un tiempo de resolución de máximo 8 horas y será resuelto por personal del área clasificado como nivel 1.

Cabe aclarar que la clasificación del personal de la Gestión ATM / IP-MPLS lo efectúa el jefe del área, en base a criterios como certificaciones, experiencia en el manejo de herramientas.

Por otro lado, para la resolución de un evento se puede requerir del apoyo de algún experto para lo cual es necesario señalar los niveles de escalamiento que se manejarían para el proyecto, estos son:

- Nivel 1.
- Nivel 2.
- Nivel 3.

- Nivel 4.

Se considera como escalamiento de nivel 1 al soporte realizado por personal de área considerado de nivel 1, mientras que el escalamiento de nivel 2 lo conforma el soporte realizado por personal del área considerado de nivel 2, o por personal correspondiente a otra área de trabajo. El escalamiento de nivel 3 se lo efectúa cuando se requiere de un especialista que se encuentra fuera de la empresa, en este caso podría ser proporcionado por el proveedor o fabricante del equipamiento que constituye la plataforma AAA; este tipo de escalamiento se daría también, cuando se requiera contar con autorización del Jefe de área para efectuar algún cambio. El escalamiento de nivel 4 se presenta cuando se requiere permisos a nivel de Gerencias para toma de decisiones en las modificaciones o en el presupuesto.

En la Figura 5.3 se señalan los pasos a seguir para el manejo de incidentes.

A continuación se presentan algunos ejemplos de los eventos que se podrían presentar en los componentes de la solución AAA.

- Daño en el clúster del servidor del sistema AAA.
- Daño en el BRAS.
- Daño en la base de datos.
- Falta de licencias para la configuración de usuarios.
- Problemas de conectividad de los equipos.
- Información mal configurada.

5.3.5 QUINTO PASO

En base a los resultados obtenidos del punto anterior se proponen algunas acciones correctivas a ser consideradas para solventar los posibles problemas que se presenten en la plataforma.

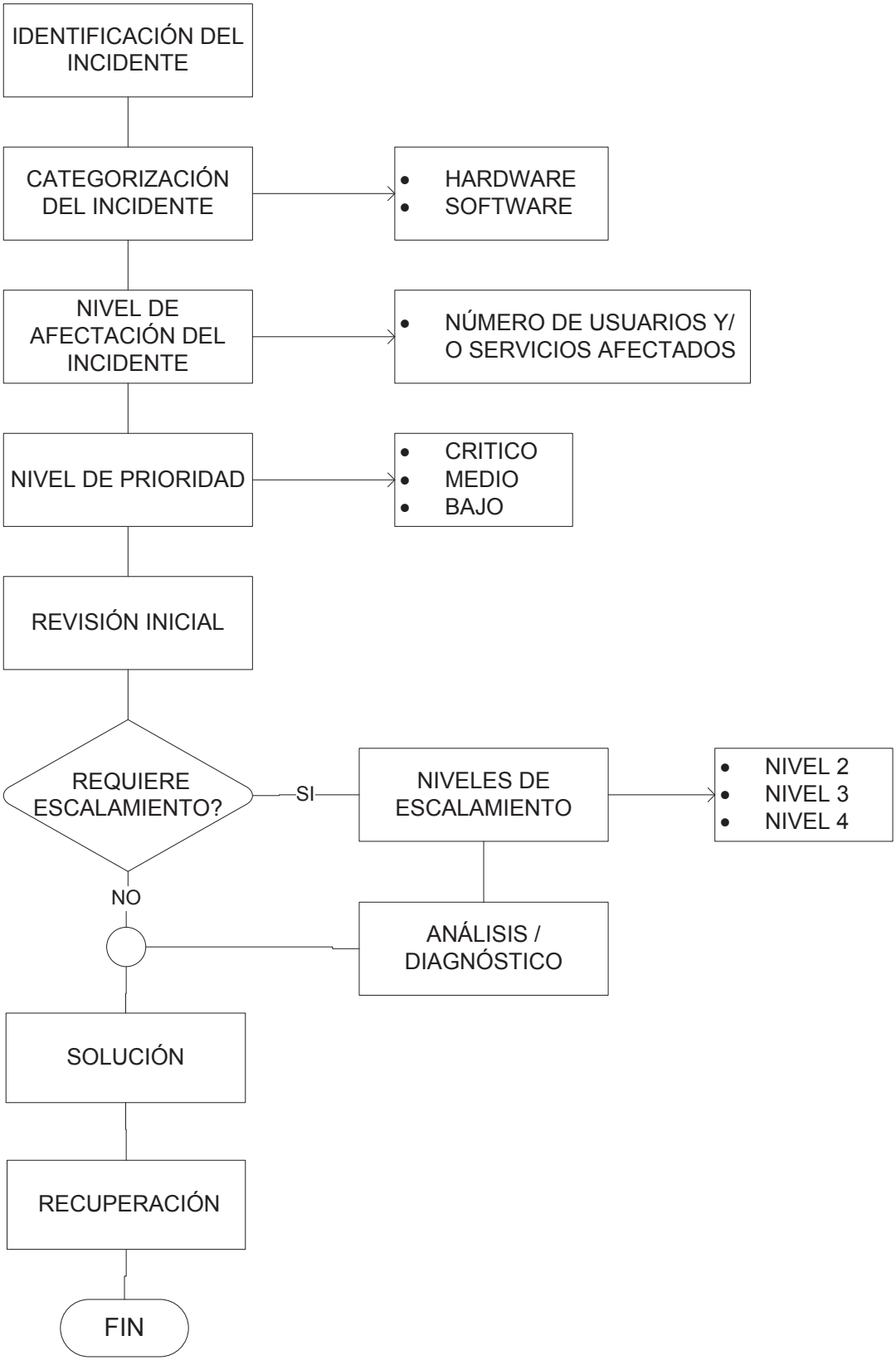


Figura 5.3. Diagrama de flujo para el manejo de incidentes

5.3.5.1 Cambios en la infraestructura

Los cambios sobre la infraestructura pueden originarse debido a la afectación de algún componente de la plataforma ya sea a nivel de hardware o de software. A continuación se detallan los pasos a seguir para este caso:

1. Determinar que componente de la plataforma requiere el cambio.
2. Determinar la prioridad para la realización del cambio.
3. Determinar los beneficios y la afectación que el cambio tendrá sobre la plataforma y los servicios que se ofrezcan por medio de esta.
4. Coordinar su implementación para generar el menor impacto a los usuarios.
5. Evaluar el correcto funcionamiento del cambio o cambios realizados sobre la infraestructura.

A continuación se presentan algunos ejemplos de los cambios que se podrían realizar en los componentes de la solución AAA.

5.3.5.1.1 Disco duro

En caso que el clúster que conforma el servidor AAA sufra algún daño en uno de sus discos, por la configuración que posee (RAID N+1), la información que se encuentre en el disco con fallo se replicará de forma automática al disco vacío, y el sistema AAA no tendrá problemas de funcionamiento, por lo que es necesario realizar el mantenimiento del equipo, ya que por medio de esto se podrá detectar fallas en el mismo. El disco dañado indicará su estado mediante el led de falla que se encuentra en el chasis.

Dado que el disco es un componente *hot-swap* se puede efectuar el cambio del mismo en caliente, por lo que, para reemplazar el disco dañado solo se requiere poseer un disco nuevo con características similares al dañado. Éste debe ser

insertado en la controladora, en el lugar del disco con daño, la cual reconocerá el disco y lo configurará de manera automática, y el RAID se regenerará.

Por la tecnología del servidor no importaría el momento en el cual se efectúe el cambio, pero se recomienda que el mismo se efectúe en un horario en el cual no se tenga mucho tráfico sobre el equipo o la afectación, en caso de daño, sea mínima, éstas características, por lo general, pueden ser cumplidas en horarios nocturnos o madrugadas.

Se recomienda también, contar con un soporte externo en caso de que se presente algún evento que no pueda ser solventado por personal de la empresa.

Para cambiar el disco se deben efectuar los siguientes pasos:

1. Identificar el slot que presenta problemas, en el chasis se encenderá el led de fallo representado por una luz roja.
2. Se procede a quitar el broche que sujeta al disco con el chasis.
3. Con cuidado se procede a desconectar el disco de la controladora, se lo retira y se lo coloca en una bolsa antiestática.
4. Se toma el disco duro nuevo y con cuidado se lo coloca en el espacio dejado por el componente anterior, y se lo conecta a la controladora.
5. Se asegura el disco al chasis.

Para este tipo de acciones se debe procurar emplear pulsera antiestáticas y de esta manera evitar daños en otras componentes.

5.3.5.1.2 Tarjeta del BRAS

Puede darse el caso que se presente alarma en una de los slots que corresponden a las tarjetas del BRAS indicando un daño en la misma y requiera que se la cambie, para este proceso se debe seguir los siguientes pasos:

1. Se procede a retirar los tornillos que sujetan la tarjeta al chasis del equipo.
2. Se procede a pulsar de manera simultánea las palancas que encuentran en los extremos de la tarjeta (eyectores).
3. Con cuidado se procede a retirar la tarjeta y colocarla en un bolsa antiestática.
4. Se toma la tarjeta nueva y con cuidado se la alinea en el espacio dejado por el componente anterior y se la inserta.
5. Se presiona los eyectores sobre la tarjeta.
6. Se asegura la tarjeta al chasis con los tornillos.

Para este tipo de acciones se debe procurar emplear pulsera antiestáticas y de esta manera evitar daños en otras componentes.

Se recomienda que el cambio de las tarjetas se efectúe en un horario en el cual no se tenga mucho tráfico sobre el equipo, podría ser ejecutado en horarios nocturnos o madrugadas.

5.3.5.2 Adición de licencias

Dependiendo del número de usuarios que la plataforma vaya adquiriendo, puede darse el caso que las licencias adquiridas no sean suficientes para configurar a los usuarios en la misma y se requiera adicionar más al sistema para continuar brindando el servicio.

Una vez adquiridas las nuevas licencias, se debe seguir los siguientes pasos para activarlas:

1. Ingresar a la consola de administración del sistema AAA como un usuario de nivel administrador.
2. Elegir del menú la opción *Administración de Licencias*.

3. Elegir del submenú desplegado la opción *Activación de Licencias.*
4. Dar clic en la opción *Browse.*
5. Seleccionar el archivo (.dat) en el cual se encuentran las licencias.
6. Dar clic en el botón OK.
7. Una vez finalizado el proceso, las nuevas licencias se activarán y se podrá seguir configurando usuarios.

5.3.5.3 Rediseño de la solución

Como resultado del análisis de los datos obtenidos por medio del monitoreo se puede llegar a la conclusión de que la plataforma requiere de un rediseño, para lo cual a continuación se detallan ciertos criterios a ser tomados en cuenta y que ayudarán con esta fase.

Como punto de partida para el diseño de un proyecto se deben considerar los siguientes lineamientos para el desarrollo de un servicio:

- Los nuevos requerimientos del servicio.
- Las herramientas y sistemas que permiten la administración del servicio.
- Arquitecturas tecnológicas empleadas por el servicio.
- Sistemas de medición o métricas empleadas para medir el rendimiento del servicio.

Se consideraría un rediseño del sistema AAA centralizado cuando se observe saturación en algunos de sus componentes debido a que la plataforma esté por alcanzar el número de usuarios para el cual fue diseñado inicialmente. En la Tabla 5.4 que se presenta a continuación, se describen brevemente algunas características a ser consideras en el rediseño de un servicio.

CARACTERÍSTICA	DESCRIPCIÓN
Aplicación del servicio	Define cómo y dónde será empleado el servicio.
Requerimientos funcionales del servicio	Define las funcionalidades que se espera conseguir con el cambio o inclusión de un nuevo servicio.
Requerimientos para la gestión del servicio	Define la manera como se va a administrar el servicio y sus componentes.
Diseño del servicio	Definir los componentes y/o infraestructura que conforma o conformaría al servicio. Elaborar documentación que facilite la gestión del servicio.
Implementación del servicio	Elaborar un plan de pruebas en el cual se incluyan: • Pruebas de funcionamiento del servicio. • Pruebas de integración y compatibilidad de los sistemas y componentes del servicio. • Pruebas de rendimiento del servicio y sus componentes. • Pruebas de seguridad del servicio.
Operación del servicio	Elaborar documentación relevante a cambios y/o problemas con el servicio, lo cual permita desarrollar políticas para el manejo de incidentes.

Tabla 5.4. Características para el diseño de un servicio

Como se considera un aumento de capacidad de la solución AAA, sería necesario conocer el número de usuarios que van a ser agregados para definir las nuevas características del nuevo equipamiento ya que las funcionalidades y requerimientos del sistema se mantendrían.

Por otro lado, cuando el servicio sea implementado se sugieren ejecutar las siguientes pruebas antes de ponerlo en producción:

- Pruebas de funcionamiento del servicio. Este tipo de pruebas permitirán verificar la operación adecuada de las funcionalidades de la plataforma. Entre las características que se pueden corroborar están la creación, edición y eliminación de clientes mediante interfaz gráfica de usuario. Se debe validar los datos ingresados en la base de datos que corresponda.

Dentro de este tipo de pruebas se deben incluir las de falla y recuperación, por ejemplo, emular fallos de energía o desconexión de alguno de los equipos.

- Pruebas de integración y compatibilidad de los sistemas y componentes del servicio, para esto, una vez instalada la nueva infraestructura se procede a realizar pruebas de conectividad entre equipos mediante el comando ping el cual permitirá diagnosticarse el estado, velocidad y calidad de la conexión.
- Pruebas de rendimiento del servicio y sus componentes, para este tipo de pruebas lo ideal sería tratar de saturar la plataforma con el número de usuarios para el cual fue diseñada y de esta manera observar su comportamiento.
- Pruebas de seguridad del servicio, que permitan verificar que el sistema no admite el ingreso a la plataforma con datos de usuario y/o contraseña inválidos o por otros medios que puedan violentar el aplicativo.

En la Tabla 5.5 se presenta un ejemplo de guía para ejecutar las pruebas antes descritas.

Una vez efectuadas las pruebas, se debe evaluar los resultados obtenidos de las mismas con el fin de determinar si existen problemas con el servicio o su infraestructura antes de ponerlo en operación. En el caso de existir algún inconveniente se debe proceder a corregirlo y ejecutar nuevamente la prueba para verificar que el evento ha sido solucionado.

5.3.6 SEXTO PASO

Como último paso en el plan de mejora se propone la capacitación del personal de la gestión ATM / IP-MPLS. Para esto se debe considerar una capacitación básica y una avanzada conforme al *expertise* que se requiere para el manejo de eventos sobre la plataforma.

PRUEBAS A EFECTUARSE	
Tipo de prueba	Funcionamiento
Objetivo de prueba	Crear un usuario
Táctica	Por medio de interfaz gráfica de usuario ingresar los datos solicitados para la creación de un cliente y guardarlos.
Criterio de éxito	Revisar la base de datos correspondiente a los clientes y verificar si el registro ingresado se encuentra en la base.
Consideraciones especiales	Tener acceso a la base de datos.
Observaciones	
Tipo de prueba	Funcionamiento
Objetivo de prueba	Eliminar un usuario
Táctica	Por medio de interfaz gráfica de usuario ingresar los datos solicitados para la eliminar un cliente y guardarlos.
Criterio de éxito	Revisar la base de datos correspondiente a los clientes y verificar si el registro ha sido eliminado de la base.
Consideraciones especiales	Tener acceso a la base de datos.
Observaciones	
Tipo de prueba	Funcionamiento
Objetivo de prueba	Editar un usuario
Táctica	Por medio de interfaz gráfica de usuario ingresar los datos solicitados para buscar el cliente. Editar la información requerida y guardar.
Criterio de éxito	Revisar la base de datos correspondiente a los clientes y verificar si el registro ha sido modificado en la base.
Consideraciones especiales	Tener acceso a la base de datos.
Observaciones	
Tipo de prueba	Funcionamiento
Objetivo de prueba	Fallo de energía
Táctica	Mientras la infraestructura se encuentre funcionando se

CONTINÚA

	procederá a suspender el suministro de energía eléctrica a la misma con el fin de verificar que ésta no sufra daos al momento de su recuperación.
Criterio de éxito	La infraestructura debe operar sin inconvenientes luego del corte.
Consideraciones especiales	En caso de que el circuito que alimente la infraestructura involucre otros equipos o áreas, se debe informar al personal correspondiente de la ejecución de la prueba.
Observaciones	
Tipo de prueba	Seguridad
Objetivo de prueba	Verificar la seguridad en la plataforma.
Táctica	Se probará el ingreso con datos inválidos.
Criterio de éxito	El sistema no debe permitir el ingreso al mismo con el uso de datos erróneos.
Consideraciones especiales	Tener permisos de acceso a los equipos de la red.
Observaciones	
Tipo de prueba	Integración y compatibilidad
Objetivo de prueba	Verificar conectividad entre equipos.
Táctica	Se procede a enviar un comando ping entre los equipos de conformación la infraestructura AAA.
Criterio de éxito	Se tener una respuesta exitosa entre cada uno de los equipos.
Consideraciones especiales	Tener permisos de acceso a los equipos de la red.
Observaciones	

Tabla 5.5. Ejemplo de guía para ejecución de pruebas de funcionamiento

La capacitación básica, deben ser dictada tanto en Quito como en Guayaquil, y su duración debe ser de un mínimo de 80 horas. Debe ser dictada en español por personal calificado, y tener contenido tanto teórico como práctico. Además se debe proporcionar un certificado de aprobación. Como temario de ésta, para el presente proyecto, se sugieren los siguientes temas:

- Características del equipamiento.
- Interconexión de los equipos.
- Configuraciones básicas de los equipos.
- Descripción posibles problemas que se pueden tener en los equipos y su solución.

La capacitación avanzada, debe ser dictada en un centro especializado con un contenido teórico y práctico. Debe tener una duración de mínimo de 40 horas y podría ser dictada en inglés o español. Además se debe proporcionar un certificado de aprobación de la misma. Como temario de ésta, para el presente proyecto, se sugieren los siguientes temas:

- Descripción detallada de los equipos.
- Configuración avanzada del equipamiento.
- Mantenimiento y operación avanzados de los equipos.
- Gestión avanzada de los problemas que se puedan presentar en la solución.

CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Las características que definen la arquitectura de una red de banda ancha inteligente son:

    - Permitir que el usuario pueda provisionar mediante un portal web el recurso de ancho de banda de acuerdo a su necesidad, dándole el control de este servicio de acuerdo a su consumo real.

    - Soportar que el costo generado por el consumo de un usuario se origine en base a una facturación automatizada, en tiempo real, del valor de ancho de banda provisionado por el mismo usuario final.

    - Facultar que la administración del sistema se vea simplificada permitiendo realizar no solo labores de control meramente técnicos, sino también implementar de forma sencilla cambios masivos enfocados a temas de mercadeo como promociones y paquetes especiales de servicios.

- La calidad de servicio en una red de datos se encuentra relacionada de manera directa en la forma como un usuario percibe la recepción de un servicio por parte de un operador. La provisión de un servicio de manera precisa y segura le brinda confiabilidad al cliente, además de que puede percibir eficiencia y rapidez al momento de acceder a los servicios que se ofrecen en la red.

- La evolución tecnológica ha ocasionado que el equipamiento de diversos fabricantes forme parte de la infraestructura de red de la empresa generando de esta manera una red de entornos heterogéneos, la cual requiere de sistemas de administración que permitan compatibilizar los

diversos protocolos y estándares de información que se emplean sobre la misma, además de facilitar al operador su gestión y control y brindar al usuario un entorno confiable, seguro y rápido.

- La inteligenciación de la red de banda ancha genera una nueva etapa en la prestación de servicios y en el modelo de negocios de la empresa, esto a su vez produce mayores ingresos en dos frentes definidos. Por un lado, genera mayores ingresos al facilitar la asignación dinámica del ancho de banda, acceso a velocidades adicionales, por parte de los usuarios; por otro lado una fuente de rentabilidad viene del ahorro de recursos asignados a la administración de la plataforma que ahora se gestiona en su configuración inicial y mantenimiento pero son los usuarios quienes esencialmente mantendrán el control de su servicio.

- La implementación de un sistema AAA centralizado que permita proveer diversas políticas de calidad de servicio, permite al operador establecer, en base a la capacidad de la red y los servicios que ofrece de manera predefinida, ciertas condiciones mediantes las cuales un usuario puede acceder a un determinado servicio como por ejemplo los recursos de red que tiene asignado, la capacidad de transmisión, diferenciación del tipo de tráfico a transmitir para priorizarlo sobre otro, etc.; de esta manera brinda al usuario una percepción diferente de cada servicio que emplee.

- La implementación de un sistema AAA centralizado en la red del proveedor permitirá que el control de acceso de los diversos usuarios se consolide dentro de una sola plataforma, facilitando de esta manera al operador la administración y gestión de los clientes y los servicios. Además este tipo de soluciones en las cuales convergen varias tecnologías de acceso brinda un escenario en el cual se considera la inclusión de usuarios con sistemas móviles quienes pueden acceder a los servicios de una red desde cualquier parte en la que se localicen.

- Para cumplir con el objetivo de poseer un sistema AAA centralizado que permita la inteligenciación de la red hace falta la implementación de una solución conformada por la integración de varios productos ofertados por un mismo fabricante, puesto que los requerimientos no encajan en las funcionalidades de ningún equipo definido. Es así que la solución final está integrada por: El administrador de recursos RM9000, el controlador de tráfico SIG9800 con funcionalidad DPI (*Deep Packet Inspection*), el servidor AAA, el balanceador de carga y demás dispositivos que permitan la comunicación entre estos y además les brinden seguridad. Cada una de estas tecnologías bien puede ser vendida e implementada individualmente pero que, para el presente proyecto, se integran para formar una única solución.

- Las soluciones tecnológicas a gran escala para TELCOS (Empresas de Telecomunicaciones) requieren de un proyecto armado en conjunto con los fabricantes de equipos de telecomunicaciones. Estos aportan con los detalles acera de las innovaciones tecnológicas que pueden acoplarse a la necesidad global del proyecto y la empresa define los requerimientos técnicos que deben cumplir estas soluciones. Finalmente un trabajo conjunto define la forma como se puede y debe desarrollar, integrar e implementar los productos que forman parte de la solución. Esto no encaja en el modelo tradicional de proyecto tecnológico en el cual la determinación de los requisitos técnicos se realiza a partir de la definición de una necesidad puesto que en el mercado no existen soluciones predefinidas ni empaquetadas previamente para éste nivel de empresa, principalmente por la complejidad y heterogeneidad de la infraestructura.

- El plan de mejora permitirá optimizar, mejorar y corregir la provisión de un servicio al aplicar los lineamientos que ITIL proporciona para el manejo eficiente de la infraestructura tecnológica de una empresa al permitirle ofertar servicios adecuados a las necesidades del mercado con costos rentables tanto para la empresa como el usuario.

6.2 RECOMENDACIONES

- Debido a las múltiples plataformas y tecnologías con las cuales cuenta la empresa, el tiempo y la dificultad de una implementación se incrementan enormemente, por lo cual es una recomendación realizar una renovación continua de equipos la cual debe orientarse a la estandarización de los mismos para evitar que futuros proyectos presenten dificultades al momento de integrar tecnologías.

- Se recomienda una revisión periódica del crecimiento del número clientes suscritos al servicio de red inteligente para verificar que su número sea acorde a las previsiones descritas en el presente trabajo y poder planificar la renovación o escalamiento de equipos en los tiempos definidos.

- El registro de usuarios en la solución AAA requiere de licenciamiento por usuario, es decir que se asigna una licencia a cada suscriptor. Actualmente la asignación y retiro de licencias a un suscriptor se realiza de forma manual con lo cual no se mantiene un control correcto de licencias. La recomendación es que a corto plazo se implemente una solución que automatice la asignación de licencias de tal forma que no sea necesario adquirir licencias sino cuando realmente se requiera.

- Para efectivizar la utilización de los recursos en la red, principalmente durante la interacción de un cliente con el servidor de contenidos, se recomienda la implementación de un servidor de caché como alternativa adicional a las políticas de calidad de servicio que la solución maneja. De esta manera en el servidor caché se almacenaría una copia de la información que ha sido más visitada por los usuarios la cual podría ser desplegada desde este servidor a un cliente disminuyendo así el procesamiento, consumo de ancho de banda y tráfico generado sobre la red por la petición realizada al servidor original.

- La integración de esta nueva solución con los equipos y tecnologías existentes limitan el nivel tecnológico que se puede aplicar a nivel de seguridad, especialmente en el caso de la autenticación que se ve forzada a utilizar los protocolos PAP y CHAP que no son los más vigentes. Como siguiente paso en la mejora de este tema se recomienda la actualización o el cambio de los equipos que limitan la utilización de protocolos de autenticación más robustos como EAP que darían una infraestructura más segura.

- Dado que la provisión de políticas de calidad de servicio por parte del sistema AAA en la solución propuesta se basa en una interacción entre el sistema AAA y una infraestructura destinada a proveer calidad de servicio se debe tener en cuenta los modelos de calidad de servicio que se van desarrollando y que permiten una adecuada interacción entre estas plataformas para de esta manera brindar el control y la administración de usuarios que se desea. Para el caso que se analiza se debe tener en cuenta que los equipos a futuro soporten el protocolo *Diameter* para de esta manera poder implementar un modelo de calidad de servicio basado en *DiffServ*.

- Dado que ITIL es una librería de libre utilización basada en las mejores prácticas para la gestión de infraestructuras de tecnologías de la información se recomienda emplear los procedimientos que esta dicta para facilitar el diseño y la implementación de un servicio dentro de la empresa.

BIBLIOGRAFÍA

CAPÍTULO 1

[1] Huidobro, J. & Roldán, D. (2004). *Redes y servicios de banda ancha*. España: McGraw-Hill.

[2] Karagiannis, G. (2002). *Scalability and congestion control in broadband intelligent and mobile networks*. Recuperado el 10 de octubre de 2010, de http://www.ub.utwente.nl/webdocs/inf/1/t0000022.pdf

[3] Campoverde Pesántez, M. (2008). *Estudio y diseño de una red inalámbrica utilizando CDMA450 para dar el servicio de telefonía fija para varias localidades en el sector noroccidental de la Provincia de Pichincha para Andinatel S.A.* (pp. 1-71). Tesis de grado no publicada de Ingeniería Electrónica y Telecomunicaciones. Escuela Politécnica Nacional. Quito.

[4] Thelander, M. (2005) *WiMAX: Oportunidades y desafíos en un mundo inalámbrico*. Recuperado el 13 de octubre de 2010, de http://www.cdg.org/resources/white_papers/files/WiMAX%20FINAL%20Spanish.pdf

[5] Mera Salgado, D. (2005). *Análisis de la tecnología WIMAX (Worldwide Interoperability for Microwave Access) y sus aplicaciones de banda ancha en Telecomunicaciones*. (pp. 58 -77). Tesis de grado no publicada de Ingeniería Electrónica y Telecomunicaciones. Escuela Politécnica Nacional. Quito.

[6] *Internetworking technologies handbook: digital subscriber line.* (Chapter 21, s.f.). Recuperado el 14 de octubre de 2010, de http://docwiki.cisco.com/wiki/Digital_Subscriber_Line

[7] Büchli, M. & otros. (2005). *Deliverable DJ.3.3.1: GÉANT2 Bandwidth on Demand Framework and General Architecture*. Recuperado el 15 de octubre de 2010, de http://geant2.archive.geant.net/upload/pdf/GN2-05-208v7_DJ3-3-1_GEANT2_Initial_Bandwidth_on_Demand_Framework_and_Architecture.pdf

[8] Cores, F. (2003). *Arquitecturas Distribuidas para Sistemas de Video-bajo-Demanda a gran escala*. (Capitulo 1). Tesis de Doctorado no publicada. Universitat Autònoma de Barcelona, Barcelona. Recuperada el 15 de octubre de 2010, de http://www.tdx.cat/bitstream/handle/10803/3041/fcp1de4.pdf?sequence=1

[9] TANDBERG. (s.f.). *Video Conferencing Guide: Eight steps to understanding the possibilities of video*. Recuperado el 19 de octubre de 2010, de http://www.corogen.com/cms/images/corogen/General/Tandberg_Video_Guide.pdf

[10] Sijben, P. (2006). *What does it take to get good video telephony.* Recuperado el 14 de noviembre de 2010, de http://www.citynet.nl/upload/What-does-it-take-to-get-good-videotelephony.pdf

[11] Huidobro, J. (s.f.). *La Red Inteligente*. Recuperada el 29 de septiembre de 2010, de http://www.coit.es/publicac/publbit/bit111/quees.htm

[12] Cueva Ramirez, J. (2008). *Aplicación de Red Inteligente en el funcionamiento de Roaming Internacional para clientes de redes móviles celulares GSM.* (pp. 72, 77-79). Tesis de grado no publicada de Ingeniería Electrónica y Telecomunicaciones. Escuela Politécnica Nacional. Quito.

[13] WORLDLINGO. (s.f.). *Intelligent Network.* Recuperada el 30 de junio de 2011, de http://www.worldlingo.com/ma/enwiki/en/Intelligent_network/1

[14] Martikainen, O., Lipiäinen, J. & Molin, K. (1995). *Tutorial on Intelligent Networks*. Recuperado el 7 de octubre de 2010, de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.196.1075&rep=rep1&type=pdf

[15] International Telecommunication Union. (1991). *I.321: B-ISDN Protocol Reference Model and its Application*. Recuperada el 13 de octubre de 2010, de http://www.itu.int/rec/T-REC-I.321-199104-I/en

[16] De Laat, C., entre otros. (2000). *RFC 2903: Generic AAA architecture*. Recuperada de 31 de mayo de 2010, de http://tools.ietf.org/pdf/rfc2903.pdf

[17] *The 3 "A"s: Authentication, Authorization, Accounting*. (2005). Recuperado de 5 de noviembre de 2010, de http://media.wiley.com/product_data/excerpt/47/04700119/0470011947.pdf

[18] Rensing, C. & Karsten, M. (2002). *AAA: A survey and a policy-based Architecture and Framework*. IEEE Network. Recuperada el 31 de agosto de 2010, de http://ieeexplore.ieee.org

[19] Aboba, B., entre otros. (2000). *RFC 2989: Criteria for Evaluating AAA Protocols for Network Access*. Recuperada el 18 de agosto de 2010, de http://tools.ietf.org/pdf/rfc2989.pdf

[20] Rigney, C., entre otros. (2000). *RFC 2865: Remote Authentication Dial In User Service (RADIUS)*. Recuperada el 13 de marzo de 2010, de http://tools.ietf.org/pdf/rfc2865.pdf

[21] Rigney, C., entre otros. (2000). *RFC 2866: RADIUS Accounting*. Recuperada el 13 de marzo de 2010, de http://tools.ietf.org/pdf/rfc2866.pdf

[22] Ventura, H. (2002). *Diameter next generation's AAA protocol*. Tesis de maestría no publicada. Linköpings Universitet. Recuperada el 31 de mayo de 2010, de http://liu.diva-portal.org/smash/get/diva2:18347/FULLTEXT01

[23] Hewlett-Packard. (2002). *Introduction to Diameter*. Recuperado el 16 de septiembre de 2010, de http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=9466739D4B54EBC6C0DAD199CD441337?doi=10.1.1.170.7071&rep=rep1&type=pdf&ei=uUMEUMu0OcLLrQfNw7moBg&usg=AFQjCNGKS4zweR5hj8Hb2sDEOhNPt5UNsQ&sig2=If1RXUuYdaOj4II1_V8nRg

[24] Calhoun, P. (2003). *RFC 3588: Diameter Base Protocol*. Recuperada el 13 de marzo de 2010, de http://tools.ietf.org/pdf/rfc3588.pdf

[25] Vybhav, R. (s.f.). *RADIUS details and TACACS+*. Recuperado el 8 de noviembre de 2010, de http://tacack.com/wp-content/uploads/2009/12/RADIUS+TACACS-cheatsheet.pdf

[26] *Overview of Authentication, Authorization, and Accounting (AAA)*. (s.f.). Recuperada el 8 de noviembre de 2010, de http://cisconetwork.org.ua/1587051893/ch09lev1sec1.html

[27] Durham, D. (2000). *RFC 2748: The COPS (Common Open Policy Service) Protocol*. Recuperado el 27 de septiembre de 2010, de http://tools.ietf.org/pdf/rfc2748.pdf

[28] Durham, D., entre otros. (2000). *COPS Usage for AAA*. Recuperada el septiembre de 2010, de http://tools.ietf.org/pdf/draft-durham-aaa-cops-ext-00.pdf

[29] Nortel Networks. (2003). *Introduction to Quality of Service*. Recuperada el 13 de noviembre de 2010, de http://netdev.docenti.di.unimi.it/teaching/2009-2010/archimedia/nortel%20-%20introduction%20to%20qos.pdf

[30] Mercado, G., Raimondo, H. & Díaz J. (2005). *Calidad de Servicio en Redes IP*. Recuperada el 18 de noviembre de 2010, de http://www.codarec.frm.utn.edu.ar/areas/QoS/Publicaciones/Calidad%20de%20Servicio%20en%20Redes%20IP.pdf

[31] Escribano, J., García, C., Seldas, C. & Moreno, J. I. (2002). *Diffserv como solución a la provisión de QoS en Internet*. Recuperado el 18 de noviembre de 2010, de http://www.it.uc3m.es/cgarcia/articulos/cita2002_diffserv.pdf

[32] *IEEE 802.1p: LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization*. (s.f.). Recuperado el 20 de enero de 2014, de http://lordinicus.blogspot.com/2013/09/ieee-8021p-lan-layer-2-qoscos.html

[33] Agilent Technologies. (2006). *Understanding DSLAM and BRAS Access Devices*. Recuperado el 1 de diciembre de 2010, de http://cp.literature.agilent.com/litweb/pdf/5989-4766EN.pdf

CAPÍTULO 2

[1] Rodriguez, R. & García, L. (2008). *La Gestión de los Procesos de Negocio en las Empresas de Telecomunicaciones*. Recuperado el 21 de octubre de 2010, de http://www.monografias.com/trabajos-pdf/gestion-procesos-negocios-telecomuncaciones/gestion-procesos-negocios-telecomuncaciones.pdf

[2] Osiatis. (s.f.). *Fundamentos de la Gestión TI*. Recuperado el 21 de octubre de 2010, de http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php

[3] IT Governance Institute. *Cobit: Resumen Ejecutivo.* (3ra. ed.). Recuperado el 21 de octubre de 2010, de http://cobit.athost.net/documentos/1.-Resumen-Ejecutivo.pdf

[4] Regalado Iglesias, C. (s.f.). El Aporte del Operador de Telecomunicaciones presentado en seminario internacional UIT-ASETA *Cerrando la Brecha Digital a través del Desarrollo de Estrategias de TIC*. Recuperado el 23 de octubre de 2010, de http://www.imaginar.org/brecha_mintel/5_CNT-CesarRegalado.pdf

[5] Velásquez Rivera, J. A. (2010). *Estudio de una red IP/MPLS para agregar servicios de televisión IP en operadoras telefónicas fijas tradicionales para usuarios residenciales mediante tecnologías XDSL para la ciudad de Quito*.

(pp.11–18). Tesis de grado no publicada de Ingeniería Electrónica y Telecomunicaciones. Escuela Politécnica Nacional. Quito.

[6] *Red ATM conceptos básicos*. (s.f.). Recuperado el 24 de octubre de 2010, de http://pitagoras.usach.cl/~eflores/Icc/cd_redes/ATMBASICO.pdf

[7] Santitoro, R. (2003). *Metro Ethernet Services: A Technical Overview*. Recuperado el 24 de octubre de 2010, de http://metroethernetforum.org/Assets/White_Papers/Metro-Ethernet-Services.pdf

[8] Juniper Networks. (2008). *Using PPPoE and IPoE in Ethernet Broadband Networks*. Recuperado el 2 de noviembre de 2010, de http://www.juniper.net/solutions/literature/white_papers/200187.pdf

[9] *Sun Fire V880 Server*. (s.f.). Recuperado el 20 de febrero de 2011, de http://www.on-queue.com/sun/servers/entry/Sun_Fire_V880_Server.html

[10] Sun Microsystems. (2007). *Sun SPARC Enterprise T5220 Server*. Recuperado el 20 de febrero de 2011, de http://www.crocom.com.pl/ulotki/t5220.pdf

[11] Sun Microsystems. (2007). *Sun Fire V245 Server*. Recuperado el 20 de febrero de 2011, de http://www.sun.com/servers/entry/v245/specs.xml

[12] Huawei. (2004). *Manual de usuario de iTELLIN AAA*. Recuperado el 10 de mayo de 2010, de http://www.huawei.com

[13] Huawei. (2007). *Quidway MA5200G Broadband Access Server: Product description.* Recuperado el 28 de octubre de 2010, de http://globaltele.com.ua/rus/filesarhiv/187/MA5200G%20Product%20Description.pdf

[14] Redback Networks. (2005). *NetOp Element Management System*. Recuperado el 15 de noviembre de 2010, de http://www.telcoline.pl/Data%20Sheet%20NetOP%20Element%20Manager.pdf

[15] Redback Networks. (2005). *SmartEdge 800 Service Gateway*. Recuperado el 6 de agosto de 2010, de http://www.falesia.pl/pdf/SE800.pdf

[16] Redback Networks. (2005). *SmartEdge 400 Service Gateway*. Recuperado el 6 de agosto de 2010, de http://www.ericsson.com/pl/redback/pdf/Data_Sheet_SE400.pdf

[17] Ericsson. (2010). *Smartedge: Multi-service Edge Routers*. Recuperado el 6 de agosto de 2010, de http://archive.ericsson.net/service/internet/picov/get?DocNo=2/28701-FGC1010723&Lang=EN&HighestFree=Y

[18] *The FreeRADIUS Project*. (2010). Recuperado el 8 de agosto de 2010, de http://freeradius.org/

[19] Huawei. InfoX-AAA. Recuperado el 8 de agosto de 2010, de http://www.huawei.com

[20] Huawei. (2006). *Huawei's TELLIN UVC.* Recuperado el 8 de agosto de 2010, de http://www.huawei.com/en/about-huawei/newsroom/product_launch/hw-090886-productlaunch.htm

[21] Campoverde Pesántez, M. A. (2008). *Estudio y diseño de una red inalámbrica utilizando CDMA450 para dar el servicio de telefonía fija para varias localidades en el sector noroccidental de la Provincia de Pichincha para Andinatel S.A. (*Anexo 1C). Tesis de grado no publicada de Ingeniería Electrónica y Telecomunicaciones. Escuela Politécnica Nacional: Quito.

[22] Huawei. (s.f.). *WASN9770.* Recuperado el 8 de agosto de 2010, de http://www.huawei.com/es/products/core-network/singleepc/wasn/index.htm

CAPÍTULO 3

[1] South River Technologies. (2001-2006). *FTP: The File Transfer Protocol*. Recuperado el 11 de enero de 2011, de http://www.webdrive.com/docs/geninfo/wpftpbasics.pdf

[2] W3C working group. (2004). *Web Services Architecture*. Recuperado el 11 de enero de 2011, de http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/wsa.pdf

[3] Wikipedia. (s.f.). *AAA protocol*. Recuperado el 31 de mayo de 2010, de http://en.wikipedia.org/wiki/AAA_protocol

[4] *Protocolo de autenticación extensible (EAP)*. (2005). Recuperado el 11 de enero de 2011, de http://technet.microsoft.com/es-es/library/cc782159%28WS.10%29.aspx

[5] Network Strategy Partners, LLC. (2007). *Next Generation Deep Packet Inspection: An Overview of Requirements and Applications*. Recuperado el 25 de noviembre de 2010, de http://www.nspllc.com/NewPages/DPI.pdf

[6] Janet. (s.f.). *Quality of Service (QoS)*. Recuperado el 25 de noviembre de 2010, de https://community.ja.net/library/janet-services-documentation/quality-service-overview

[7] SUPERTEL. Estadísticas de Servicios de Telecomunicaciones: *Datos de cuentas y usuarios de Internet*. Extraído en septiembre de 2012, de http://www.supertel.gob.ec/index.php?option=com_k2&view=item&id=21:servicios-de-telecomunicaciones&Itemid=90

[8] Oracle. (2009). *Sun SPARC Enterprise T5120 Server*. Recuperado el 20 de febrero de 2011, de

http://www.Oracle.com/us/products/servers-storage/servers/sparc-enterprise/t-series/035999.pdf

[9] Oracle. (2009). *Sun Blade T6340 Server Module*. Recuperado el 17 de junio de 2011, de http://www.Oracle.com/us/products/servers-storage/servers/blades/034667.pdf

[10] Duban, M. Y. (2008). *Sistema operativo Solaris Requerimientos mínimos de hardware.* Recuperado el 18 de junio de 2012, de http://solarismyd.blogspot.com/2008/07/instalacion.html

[11] *Requisitos del sistema Windows Server.* (2007). Recuperado el 18 de junio de 2012, de http://technet.microsoft.com/es-es/windowsserver/bb430827.aspx

[12] Wikipedia. (s.f.). *High-Availability Cluster.* Recuperado el 27 de enero de 2011, de http://en.wikipedia.org/wiki/High-availability_cluster

[13] Oracle. (2003). Oracle Data Guard in Oracle Database 10g *Disaster Recovery for the Enterprise*. Recuperado el 18 de enero de 2011, de http://www.dbazone.com/docs/oracle_10gDataGuard_overview.pdf

[14] Cisco. (s.f.). *Virtual Routing and Forwarding.* Recuperado el 21 de enero de 2011, de http://www.cisco.com/en/US/docs/net_mgmt/active_network_abstraction/3.7/reference/guide/vrf.pdf

[15] Microsoft TechNet. (s.f.). *Diseño de un Servidor de Seguridad Interno*. Recuperado el 21 de enero de 2011, de http://www.microsoft.com/spain/technet/recursos/articulos/secmod155.mspx

CAPÍTULO 4

[1] Huawei. (2010). *Manual de usuario de la plataforma AAA*.

[2] Huawei. (2009). *Manual de usuario Quidway SIG9810/9820 Service Inspection Gateway*.

[3] Huawei. (2009). Manual de usuario Quidway RM9000 Resource and Policy Control System.

[4] Ericsson. (2009). *NetOp Police Manager*. Recuperado el 16 de enero de 2011, de http://archive.ericsson.net/service/internet/picov/get?DocNo=7/28701-FGB101651&Lang=EN&HighestFree=Y

[5] Redback Networks. (s.f.). *Manual de administración de NetOp Policy Manager*.

[6] Redback Networks. (s.f.). *Manual de instalación de NetOp Policy Manager*.

[7] Ericsson. (2009). *Smartedge Advanced Services Engine (ASE)*. Recuperado el 27 de octubre de 2010, de http://shop.nag.ru/uploads/ASE-RBAK.pdf

[8] National Instruments. (2008). *Redundant System Basic Concepts*. Recuperado el 7 de diciembre de 2010, de http://www.ni.com/white-paper/6874/en/

CAPÍTULO 5

[1] Best Management Practice. (2010). *ITIL®: The Basics*. Recuperado el 2 de julio de 2013, de http://www.best-management-practice.com/gempdf/ITIL_The_Basics.pdf

[2] Xelere. (2012). *Manual del Curso de Fundamentos de ITIL v3*.

ANEXOS

[1] Ministerio de Telecomunicaciones. (s.f.). *Plan Nacional de Conectividad*. Recuperado el 5 de diciembre de 2012, de http://www.mintel.gob.ec/index.php?option=com_content&view=article&id=107:incremento-de-internet-banda-ancha&catid=40:plan-nacional-de-conectividad

GLOSARIO

ABREVIATURAS	DESCRIPCIÓN
AAA	*Authentication, Authorization, Accounting* / Autorización, Autenticación, Contabilidad
AAL	*ATM Adaptation Layer* / Capa de Adaptación ATM
ATM	*Asynchronous Transfer Mode* / Modo de Transferencia Asincrónica
ADSL	*Asymmetric Digital Subscriber Line* / Línea de Abonado Digital Asimétrica
AVP	*Attribute-Value-Pair* / Atributo-Valor-Par
ASE	*Advanced Services Engine* / Motor de Servicios Avanzados
B-ISDN	*Broadband Integrated Services Digital Network* / Red Digital de Servicios Integrados de Banda Ancha
B-SSP	*Broadband Service Switching Point* / Punto de Conmutación de Servicio de Banda Ancha
B-SCP	*Broadband Service Control Point* / Punto de Control de Servicio de Banda Ancha
B-IP	*Broadband Intelligent Peripheral* / Periférico Inteligente de Banda Ancha
BoD	*Broadband over demand* / Ancho de Banda bajo Demanda
BRAS	*Broadband Remote Access Server* / Servidor de Acceso Remoto de Banda Ancha
BSS	*Business Suport System* / Soporte de Negocio
BGP	*Border Gateway Protocol*
CDMA	*Code División Múltiple Acces* / Acceso Múltiple por División de Código
CHAP	*Challenge Handshake Authentication Protocol* / Protocolo de Autenticación por Desafío Mutuo
COPS	*Common Open Policy Service* / Servicio Común de Políticas Abiertas

COBIT	*Control Objectives for Information and Related Technologies* / Objetivos de Control para Tecnología de Información Relacionadas
CDR	*Call Detail Record* / Registro de Detalle de Llamada
CLI	*Command Line Interface* / Línea de Comandos
DSL	*Digital Subscriber Line* / Línea Digital de Abonado
DM	*Domain Management* / Administrador de dominio
DAP	*Directory Access Protocol* / Protocolo de Acceso a Directorios
DiffServ	*Differentiated services* / Servicios Diferenciados
DSLAM	*Digital Subscriber Line Access Multiplexer* / Multiplexor de acceso a la línea digital de abonado
DPI	*Deep Packet Inspection* / Inspección Profunda de Paquetes
DoS	*Denial of Service* / Denegación del Servicio
EAP	*Extensible Authentication Protocol* / Protocolo de Autenticación Extensible
eTOM	*enhanced Telecommunication Operations Map* / Mapa de Operaciones de Telecomunicaciones Mejorado
FT	*Fixed Terminal* / Terminal Fijo
FTP	*File Transfer Protocol* / Protocolo de Transferencia de Archivos
HFC	*Hybrid Fiber Coaxial* / Redes híbridas fibra-coaxial
HDSL	*High-bit-rate DSL* / Línea de Abonado Digital de Alta Velocidad Binaria
ISDN	*Integrated Services for Digital Network* / Red Digital de Servicios Integrados
IDSL	*ISDN Digital Subscriber Line* / Línea Digital de Abonado ISDN
IN	*Intelligent Network* / Red Inteligente
ISP	*Internet Service Provider* / Proveedor de Servicio de Internet
IP	*Intelligent Peripheral* / Periférico Inteligente

IRTF	*Internet Research Task Force* / Grupo de Trabajo de Investigación de Internet
IETF	*Internet Engineering Task Force* / Grupo de Tareas de Ingeniería de Internet
IPSec	*Internet Protocol Security* / Seguridad del Protocolo Internet
IntServ	Integrated Services / Servicios Integrados
IDM	*Inter-domain Management* / Administrador inter-dominio
ITIL	*Information Technology Infrastructure Library* / Biblioteca de Infraestructura de Tecnologías de la Información
IP	*Internet Protocol* / Protocolo Internet
IT	*Information Technology* / Tecnología de la Información
LDAP	*Lightweight Directory Access Protocol* / Protocolo Ligero de Acceso a Directorios
LE	*Local Exchange* / Intercambio Local
LPDP	*Local Policy Decision Point* / Punto de Decisión de Políticas Local
MT	*Mobile Terminal* / Terminal Móvil
MD5	*Message Digest Algorithm 5* / Algoritmo de Resumen del Mensaje 5
MML	*Man-Machine Language* / Lenguaje Hombre-Máquina
MIB	*Management Information Base* / Base de Información Gestionada
MPLS	*Multi Protocol Label Switching* / Multi Protocolo de Conmutación de Etiquetas
NVoD	*Near video on Demand* / Vídeo bajo de/manda aproximado
NAS	*Network Access Server* / Servidor de Acceso a la Red
NASREQ	*Network Access Server Requirements* / Requerimientos para el Servidor de Acceso a la Red
NGOSS	*New Generation Operations Systems and Software* / Software y Sistemas de Operación de Nueva Generación
OSS	*Operations Support Systems* / Sistemas de Soporte de Operaciones

OLA	*Operational Level Agreements* / Acuerdo de Nivel de Operación
PSTN	*Public Switched Telephone Network* / Red Telefónica Pública Conmutada
PPV	*Pay per view* / Pago por ver
PAP	*Password Authentication Protocol* / Protocolo de Autenticación por Contraseña
PEP	*Policy Enforcement Points* / Punto de Aplicación de Políticas
PDP	*Policy Decision Points* / Punto de Decisión de Políticas
PDN	*Packet Data Network* / Red de Paquete de Datos
QVoD	*Quasi video on demand* / Quasi vídeo bajo demanda
QoS	*Quality of Service* / Calidad de Servicio
RADIUS	*Remote Authentication Dial In User Service* / Servicio de Usuario Telefónico de Autenticación Remota
RSVP	*Resource Reservation Protocol* / Protocolo de Reservación de Recursos
RFC	*Request for comments* / Petición de comentarios
SDSL	*Symmetric Digital Subscriber Line* / Línea Digital de Abonado Simétrica
SSP	*Service Switching Point* / Punto de Conmutación del Servicio
SCP	*Service Control Point* / Punto de Control del Servicio
SMS	*Service Management System* / Sistema de Administración de un Servicio
STP	*Service Transfer Point* / Punto de Transferencia del Servicio
SCEP	*Service Creation Enviroment Point* / Punto de Entorno de Creación del Servicio
SS7	*Common Channel Signaling System 7* / Sistema de Señalización de Canal Común 7
SONET	*Synchronous Optical Network* / Red Óptica Síncrona
SCTP	*Stream Control Transmission Protocol* / Protocolo de

	Control de Transmisión Real
SLA	*Service Level Agreement* / Acuerdo de Nivel de Servicio
SID	*Shared Information and Data* / Compartición Información y Datos
SCSI	*Small Computer System Interface* / Interfaz de Sistema para Pequeñas Computadoras
SOA	*Service-oriented architecture* / Arquitectura orientada a servicios
SAS	*Serial Attached SCSI*
SNMP	*Simple Network Management Protocol* / Protocolo Simple de Administración de Red
SOAP	*Simple Object Access Protocol* / Protocolo Simple de Acceso a Objetos
SMU	*Service Management Unit* / Módulo de administración del sistema
SFU	*Service Management Unit* / Módulo de servicio y transferencia
SLR	*Service Level Requirement* / Requisitos de Nivel de Servicio
TVoD	*True Video on Demand* / Vídeo bajo demanda verdadero
TCP	*Transmission Control Protocol* / Protocolo de Control de Transmisión
TX	*Transit eXchange* / Intercambio de Tránsito
TLS	*Transport Layer Security* / Seguridad de la Capa de Transporte
TACACS+	*Terminal Access Controller Access Control System Plus* / Sistema de Control de Acceso del Controlador de Acceso a Terminales
TMF	*TeleManagement Forum* / Foro de Teleadministrativo
TAM	*Telecommunications Application Map* / Mapa de Aplicaciones de Telecomunicaciones
TNA	*Technology Neutral Architecture* / Arquitectura Neutral de Tecnologías

UDP	*User Datagram Protocol* / Protocolo Datagrama de Usuario
UIT	Unión Internacional de Telecomunicaciones / *International Telecommunication Union*
VDSL	*Very-High-Data-Rate Digital Subscriber Line* / Línea de Abonado Digital de Muy Alta Tasa de Transferencia
VoD	*Video on Demand* / Video Bajo Demanda
VPN	*Virtual Private Network* / Red Privada Virtual
VRF	*Virtual Routing and Forwarding*
WiMAX	*Worldwide Interoperability for Microwave Access* / Interoperabilidad Mundial para Acceso por Microondas
Wi-Fi	*Wireless Fidelity*
XML	*Extensible Markup Language*

ANEXOS

ANEXO A

ANEXO B