UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLANTACIÓN DE UN TERMINAL DE GESTIÓN EN SOLUCIÓN DE ÚLTIMA MILLA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

JUAN CARLOS CAVANI ROJAS

PROMOCIÓN

2003 – I

LIMA – PERÚ
2011

IMPLANTACIÓN DE UN TERMINAL DE GESTIÓN EN SOLUCIÓN DE ÚLTIMA MILLA

A mis padres, quienes han sido desde siempre
mi gran soporte y fuente de mi inspiración y persistencia

SUMARIO

Desde hace algunos años atrás se observa un creciente interés por parte de los usuarios de servicios de telecomunicaciones en realizar “acuerdos de nivel de servicios" (SLA) con sus respectivos “proveedores” (ISP), en el cual se plasman los límites para considerar a un servicio como bueno o malo y se detallan además, penalidades a demandar por parte de los usuarios en un escenario de mal servicio.

En este camino, los ISP han realizado cambios en sus procedimientos operativos haciendo uso de herramientas de gestión de redes, las cuales brindan información de la operación de los servicios ofrecidos a sus clientes; y es en este sentido que el presente informe de suficiencia se enfoca sobre la solución de un problema actual de un ISP en relación a la ausencia de gestión remota sobre los enlaces de última milla en zonas fuera del área de cobertura actual de este ISP.

En el presente informe se proporciona pautas a seguir para la implantación de un terminal de gestión, en la cual se podrá realizar tareas de observación de enlaces de última milla, en nuestro caso, el de un enlace inalámbrico.

El desarrollo de la solución al problema mencionado sigue la estructura del modelo OSI, asegurándonos de este modo, el contar primero con la conexión entre el terminal de gestión de redes ubicado en el centro de operaciones del ISP (NOC) y los equipos utilizados para establecer el enlace inalámbrico de última milla, para luego activar el protocolo de gestión de redes SNMP.

ÍNDICE

PRÓLOGO

En este trabajo se da a conocer la problemática en soluciones de última milla desde el punto de vista de operación de red de un ISP, las ventajas y desventajas de los escenarios actuales de última milla, el desarrollo de una alternativa de solución a las desventajas indicadas, las oportunidades que esta solución propuesta nos ofrece a nivel del negocio del ISP y finalmente, las conclusiones y recomendaciones que nos lleva el implementar la solución desarrollada.

El presente informe ha sido dividido en cinco capítulos, los cuales son detallados a continuación:

En el capítulo I, se brinda el marco teórico sobre el cual se despliegan todas las ideas desarrolladas a lo largo del presente informe.

En el capítulo II, se plantea el problema de la ausencia de gestión remota sobre los equipos de un ISP instalados en la última milla, es decir, el no saber lo que ocurre sobre el enlace que estos equipos establecen. Así también, se mencionaran las ventajas y desventajas de este escenario.

En el capítulo III, se propone el desarrollo de la solución de ingeniería del problema mencionado. Este desarrollo hace referencia al orden brindado del modelo OSI, desde asegurar las conexiones desde el terminal de gestión de redes hacia los equipos de última milla, como el de activar el protocolo de gestión de redes SNMP, el cual transitará sobre el camino establecido. Así también, se mencionará las ventajas y desventajas de este escenario, como las nuevas oportunidades de negocio del ISP a partir de la ejecución de la propuesta de solución desarrollada.

En el capítulo IV, se muestra un plan de costos y tiempos para la ejecución de la solución propuesta.

En el capítulo V, se expone las conclusiones y recomendaciones que nos trae la implantación de la solución propuesta.

Finalmente, cabe señalar que el núcleo de un centro de operaciones de un ISP es el de contar con la gestión de todos los equipos de su red y así obtener información de estos equipos, ya sea con un fin comercial, de operación o de planificación, lo cual conlleva a la toma de decisiones.

CAPÍTULO I
MARCO TEÓRICO

En este capítulo se detallan los conceptos teóricos utilizados en el presente informe de suficiencia, en donde algunos de estos fueron mencionados ligeramente en las páginas anteriores y los cuales serán también mencionados en las secciones posteriores a esta.

1.1 Modelo de referencia OSI

Es un modelo utilizado para representar la comunicación entre dos sistemas. OSI (de sus siglas en inglés, OPEN SYSTEM INTERCONECTION) fue desarrollado por la ISO (Organización Internacional de la Estandarización) en 1984, y es considerado como un modelo base para hacer referencia a las comunicaciones entre computadores. OSI proporciona a la industria de comunicaciones un conjunto de estándares que asegura una compatibilidad e interoperatividad entre los distintos tipos de tecnologías de red producidos por las proveedores de equipos de comunicaciones a nivel mundial.

Este modelo de red se define en base a siete capas, desde la capa número uno en el nivel inferior de la pila de capas, hasta la capa número siete ubicada en el nivel superior (figura 1.1).

Figura 1.1: Modelo de referencia OSI (Fuente: Propio)

En el presente informe, pondremos especial énfasis en las primeras tres capas, en

donde, la transmisión de las unidades de datos de un ente a otro se definen como bits, tramas y paquetes, las cuales corresponden a la capa uno, dos y tres, respectivamente (figura 1.2).

Figura 1.2: Las tres primeras capas del modelo de referencia OSI (Fuente: Propio)

1.2 Modelo Internet

El modelo Internet es conocido también como modelo TCP/IP, debido a que los principales protocolos que la componen son TCP (capa de transporte) e IP (capa Internet). La equivalencia entre este modelo y el modelo de referencia OSI puede ser vista en la figura 1.3.

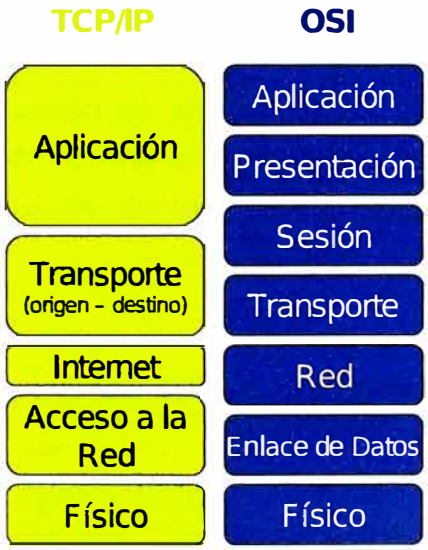


Figura 1.3: Modelo TCP/IP y Modelo de Referencia OSI (Fuente: Propio)

1.2.1 Protocolo TCP

El Protocolo de Control de Transmisión (TRANSMISSION CONTROL PROTOCOL) es uno de los principales protocolos en Internet, debido a que muchas aplicaciones que se montan sobre una red de datos hacen uso de TCP para el establecimiento de conexiones entre dos puntos (origen y destino). TCP garantiza que los datos sean entregados a un destino sin errores (cuenta con un mecanismo de detección de errores) y en el orden en que la información ha sido transmitida (cuenta con

indicadores de secuencia de la información transmitida). Así también, TCP nos lleva a la utilización de SOCKET, el cual permite diferenciar distintas aplicaciones desde un mismo origen, identificadas éstas por el número de puerto (identificador de conexión) a utilizar.

1.2.2 Protocolo IP

El Protocolo de Internet (INTERNET PROTOCOL) es un protocolo no orientado a la conexión, es decir, que en esta capa no existe aseguramiento del camino a seguir para llegar a un determinado destino. Este protocolo nos sirve para identificar parámetros de la comunicación a establecer entre dos puntos (origen y destino) y se encarga de encapsular toda la información procesada en las capas superiores para su envío a la capa de acceso de red.

1.3 Direccionamiento IP

Una dirección IP es un número que identifica lógicamente y de modo jerárquico a una interfaz de red que soporte el protocolo IP. En el presente informe, se va a trabajar con la versión 4 de IP, por lo cual la dirección IP va a estar representada por cuatro octetos separados por puntos y en donde cada octeto se expresa en su notación decimal (de 0 a 255). Los octetos se encuentran conformados por 8 bits.

Las direcciones IP constan de dos partes (ver figura 1.4), la primera (lado izquierdo) identifica a la sección denominada “red”, y la segunda (lado derecho) identifica a la sección denominada “usuario”. En base a esto, se definen cinco clases de redes según sus direcciones IP.

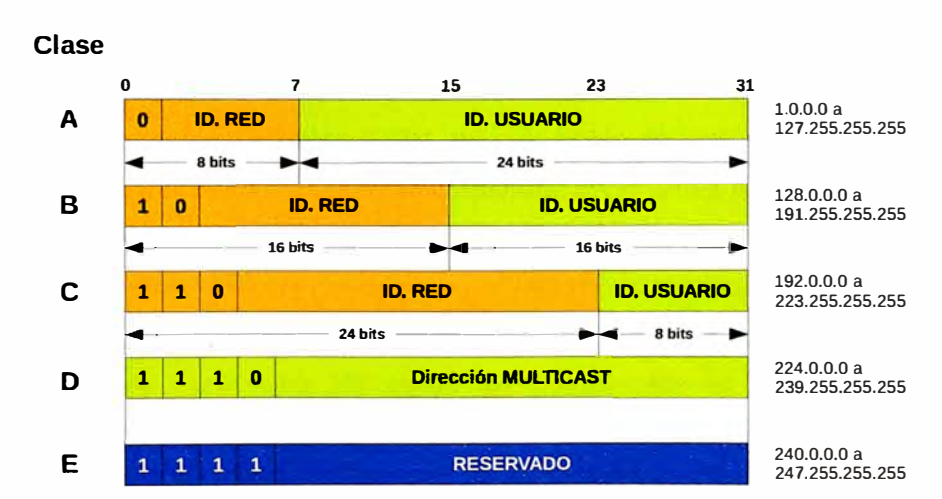


Figura 1.4: Clases de direccionamiento IP versión 4 (Fuente: Propio)

1.4 MULTI PROTOCOL LABEL SWITCHING

El concepto de MPLS (MULTI PROTOCOL LABEL SWITCHING) proviene de un

estándar del IETF que surgió a partir de propuestas brindadas por distintos proveedores de equipos de comunicaciones, para resolver los problemas de comunicación eficiente en el núcleo de una red de datos.

MPLS utiliza lo mejor de dos arquitecturas, el enrutamiento de direcciones IP de la arquitectura IP y la velocidad de conmutación de paquetes en la arquitectura ATM. Sobre una red MPLS, los proveedores de servicios establecen dos servicios, el de acceso a Internet y el de redes privadas virtuales, utilizando túneles para este último. Ver figura 1.5.

En el presente informe, se trabajará con el concepto de redes privadas virtuales (VPN) creadas sobre una red MPLS.

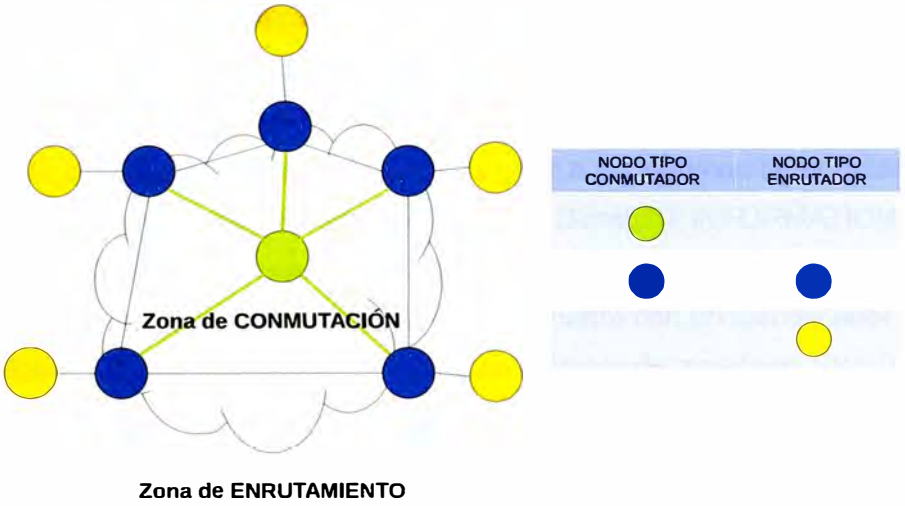


Figura 1.5: Red IP MPLS (Fuente: Propio)

1.4.1 Red privada virtual

Las redes privadas virtuales (VPN, de sus siglas en inglés) nos permiten obtener cierto grado de funcionalidad y seguridad adquiridos en la redes privadas de tiempo atrás, las cuales se basaban en conexiones dedicadas de extremo a extremo.

Las conexiones VPN se establecen sobre una infraestructura de red compartida sobre la cual se configuran parámetros identificadores de cada una de las VPN declaradas y sobre cada una de estas se personaliza el tipo de seguridad y/o funcionalidad de red a gestionar. Para el presente informe, se utilizará la configuración de VPN sobre una red IP MPLS, siendo el identificador mencionado el parámetro VRF (VIRTUAL ROUTING FORWARDING).

1.5 SIMPLE NETWORK MANAGEMENT PROTOCOL

La complejidad de las redes de ruteadores, conmutadores y servidores de hoy en

día hace difícil el imaginar la realización de una gestión eficiente sobre estos equipos de red. Es en este escenario que entra el SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP). SNMP fue introducido en 1988 como parte del desarrollo necesario estandarizado para la administración de dispositivos IP. SNMP provee a estos usuarios con un "simple" conjunto de operaciones que permiten la administración remota de estos dispositivos.

Sobre las operaciones antes mencionadas, estas se envían utilizando PDU. El PDU (Unidad de Datos de Protocolo) es el mensaje que los administradores y los agentes usan para el envío y recepción de información. Hay un formato PDU estandarizado para cada uno de las siguientes operaciones SNMP: GET, GET-NEXT, GET-BULK, SET, GET-RESPONSE, TRAP, NOTIFICATION, INFORM y REPORT.

El modelo de gestión SNMP se encuentra conformado por una estación de gestión, la cual sirve como interfaz entre el gestor humano y el sistema de gestión de red; por un agente, los cuales son la parte que responde a las ordenes de la estación gestora de un dispositivo de red; y finalmente la MIB (MANAGEMENT INFORMATION BASE) que viene a ser un modelo o esquema que contiene el ordenamiento jerárquico de todos los objetos gestionados, en donde cada uno de estos cuenta con un identificador único(OID).

La figura 1.6 muestra un escenario de intercambio de mensajes SNMP.

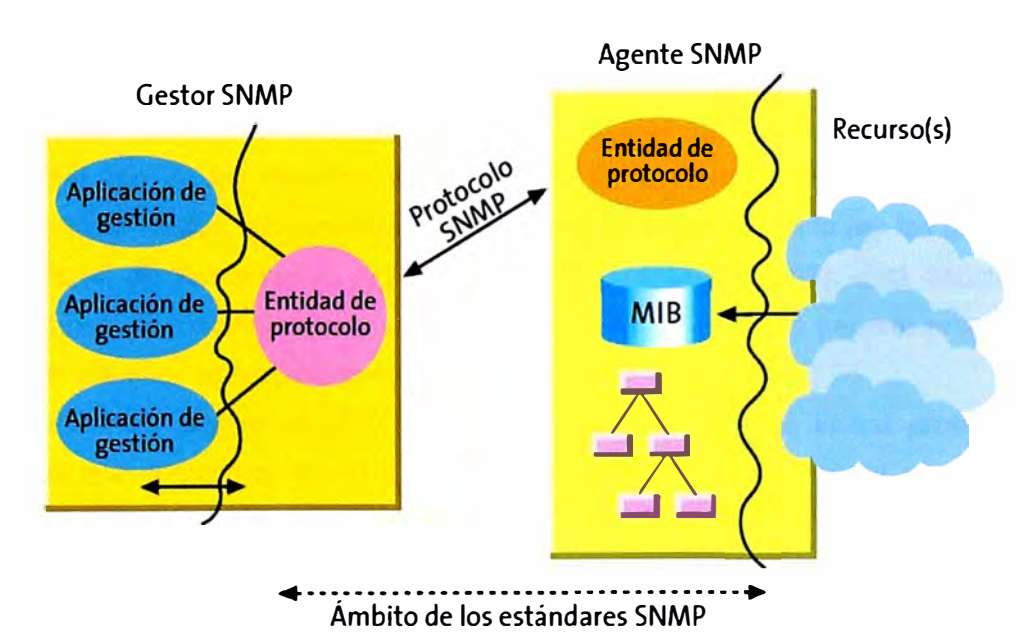


Figura 1.6: Estándar SNMP (Fuente: Las Telecomunicaciones de Nueva Generación – Telefónica)

Las versiones de SNMP más utilizadas son dos: SNMP versión 1 (SNMP v1) y

SNMP versión 2 (SNMP v2). Ambas versiones tienen un número de características en común, pero SNMP v2 ofrece operaciones adicionales. SNMP en su última versión (SNMP v3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo, no ha sido mayoritariamente aceptado en la industria. En el presente informe se trabajará con la versión 2 de SNMP.

1.6 Modelo FCAPS (FAULT, CONFIGURATION, ACCOUNTING, PERFORMANCE and SECURITY)

FCAPS es un modelo de Gestión de Redes propuesto por la ISO el cual fue introducido inicialmente por la ITU-T (M.3010 y M.3400). La ISO a ISO define a la gestión de redes como el conjunto de procesos y actividades que se realizan para controlar, coordinar y observar a todos los recursos involucrados en que las comunicaciones se lleven a cabo bajo un escenario OSI.

FCAPS proviene de las siguientes palabras en inglés, FAULT, CONFIGURATION, ACCOUNTING, PERFORMANCE, SECURITY que son categorías de gestión de redes sobre las cuales ISO define algunas tareas.

Gestión de Fallas (FAULT MANAGEMENT), contiene a los procesos que nos permiten localizar, diagnosticar, y corregir problemas de redes de datos.

Gestión de Configuración (CONFIGURATION MANAGEMENT), es aquella que nos permite obtener información desde la red y usar esta información para la configuración de todos los dispositivos de redes.

Gestión de Contabilidad (ACCOUNTING MANAGEMENT), está asociada a la medición del uso de los recursos de la red por los usuarios, con el fin de establecer métricas, revisar límites, determinar costos y el tipo de tráfico cursado por los usuarios.

Gestión de Rendimiento (PERFORMANCE MANAGEMENT), está asociado con una línea base de funcionamiento esperado de la red, lo cual nos permite proveer a los usuarios de un nivel de servicio consistente.

Gestión de Seguridad (SECURITY MANAGEMENT), nos indica proteger a los dispositivos que conforman la red a gestionar, al controlar los puntos de acceso a estos dispositivos.

1.6.1 Gestión de fallas

Las fallas son un defecto en el funcionamiento de algún dispositivo o grupo de dispositivos de nuestra red. La figura 1.7 muestra el ciclo de procesos de la gestión de fallas que abarcan los procesos de ocurrencias de fallas, detección, correlación, diagnóstico, corrección y retorno a la línea base, los cuales se detallarán indicando la

aplicación de las mismas en el terminal de gestión a implantar.

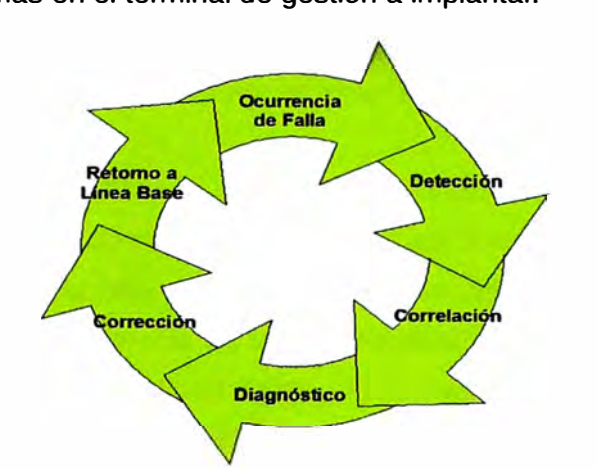


Figura 1.7: Ciclo de procesos de la gestión de fallas (Fuente: Propio)

Sobre la **ocurrencia de la falla**, ésta puede ocurrir en cualquier parte de nuestra red y es nuestra labor, como administrador de red, asegurar que el terminal de gestión a implantar tenga conectividad con todos los equipos involucrados en el funcionamiento del servicio ofrecido.

Así también, hay que tener en cuenta, en nuestro escenario de gestión, al cliente del ISP, quien es la persona o entidad que utiliza el servicio ofrecido. Debido a que muchas veces una falla que podamos detectar desde nuestro terminal de gestión, por ejemplo el de inserción de errores en el medio de transmisión de la última milla, puede no impactar al negocio de nuestro cliente, debido al nivel de tasa de errores registrado. A partir de este conocimiento, podemos definir umbrales sobre el cual el cliente percibe fallas sobre el servicio adquirido.

Sobre la **detección**, ésta es posible debido a una rutina periódica ejecutada en el terminal de gestión que verifica la conectividad y estado de los dispositivos de red a gestionar. Así también, como parte del proceso de detección, tenemos la obligación siendo administradores de una red de datos, el ser pro activos a las fallas, detectando éstas a tiempo y realizando el esfuerzo necesario para su corrección. Para este fin, es recomendable la habilitación de un recolector de eventos, el cual se encuentra recibiendo permanentemente información del estado de los dispositivos gestionados.

Sobre la **correlación**, ésta es necesaria para poder identificar eventos en un tiempo específico y por el cual todos los dispositivos de red deberán de tener sus relojes sincronizados.

Sobre el **diagnóstico**, éste se lleva a cabo haciendo uso de computadores con sistemas inteligentes de gestión y con personal entrenado en las buenas prácticas para realizar análisis de obtención de la causa raíz a la falla presentada.

Sin embargo, para llevar a cabo lo mencionado, es importante contar con el conocimiento de toda la topología de la red a gestionar, debido a que la falla puede afectar a más de un equipo y la respuesta de estos equipos a la falla nos podrá dar pistas de la naturaleza de la misma.

Sobre la **corrección**, éste se encuentra relacionado con la toma de decisión de acciones necesarias para superar la falla presentada. Como se comentó en el primer proceso de ocurrencia de la falla, las acciones a tomar dependen del nivel de afectación al negocio del cliente en presencia de la falla detectada. Estas acciones van desde la actuación inmediata ya sea de forma remota o local sobre el tramo afectado del servicio, hasta el de coordinar con el cliente del ISP una ventana de mantenimiento para realizar acciones correctivas, las cuales resolverán el problema detectado.

Sobre el **retorno a la línea base**, ésta se encuentra relacionada a todas las características que ofrece la red, la cual permite que ésta se considere en un estado óptimo. Este estado es utilizado como referencia y al cual se debe retornar luego de corregir alguna incidencia o falla detectada sobre la red. Esta idea está relacionada con el concepto de SLA y el nivel de disponibilidad ofrecida por la red.

1.6.2 Gestión de configuración

Es una buena práctica el contar con el histórico de configuraciones realizadas a los equipos de red sobre el cual se soportan los servicios ofrecidos a los clientes del ISP.

Para este fin, se deberá implementar tareas o rutinas para la descarga manual o automática de las configuraciones de los equipos de red mencionados.

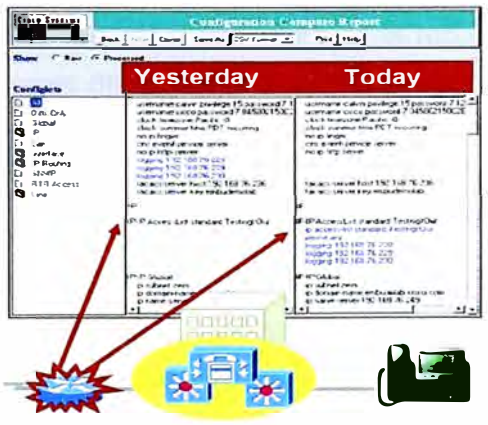


Figura 1.8: Comparación de configuraciones (Fuente: NMS-1000 – CISCO SYSTEM)

La figura 1.8 muestra la pantalla de un programa propietario cuya función es mantener un inventario de configuraciones de equipos gestionados y nos permite

visualizar los cambios efectuados entre dos configuraciones (de la figura, la configuración de ayer y la de hoy).

1.6.3 Gestión de contabilidad

El recolectar tráfico y mostrarlo está relacionado con la medición del uso de los recursos de la red por parte de los clientes del ISP, con la finalidad de establecer métricas, revisar límites, determinar costos y el tipo de tráfico cursado. Así también, con la información recolectada, nos es posible generar reportes y en base a éstos tomar decisiones.

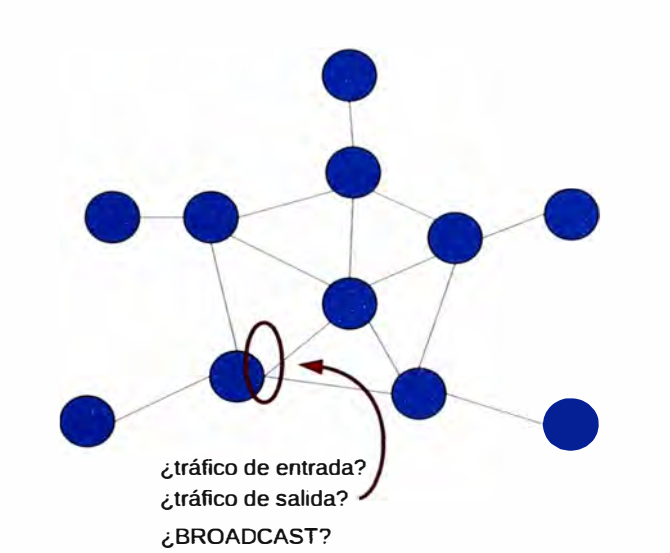


Figura 1.9: Medición del uso de los enlaces de red (Fuente: Propio)

1.6.4 Gestión de rendimiento

Se refiere a la verificación del rendimiento de la red gestionada sobre la cual se determinan algunos parámetros (línea base), como el de carga de tráfico, procesamiento de los dispositivos de red, etc.

1.6.5 Gestión de seguridad

El presente informe de suficiencia hace mención a la utilización del protocolo IP en versión 4, el cual de por si no fue creado pensando en la seguridad de las redes y es en esta sección en la cual se brindarán algunas tareas para incrementar el nivel de seguridad que tiene por defecto la red a gestionar. Los pilares de la seguridad (de acuerdo a las ISO 27001) son la confidencialidad, la integridad y la disponibilidad.

Sobre la **confidencialidad**, ésta abarca las configuraciones que permitan un acceso limitado al personal autorizado a gestionar todos los dispositivos de red.

Sobre la **integridad**, éste contempla el preservar la configuración actual de los

dispositivos de red y registrar a los usuarios que realice modificaciones a éstas.

Sobre la **disponibilidad**, ésta se encuentra relacionada con el aseguramiento del funcionamiento del servicio ofrecido al cliente del ISP, para lo cual se requiere tener en cuenta el tipo de acceso a habilitar a los dispositivos de red gestionados (y por ende los accesos a denegar).

Finalmente, cabe señalar que la gestión de los equipos de red pueden ser "en banda", es decir los paquetes de gestión cursan sobre los enlaces utilizados para el tráfico de los clientes, o puede ser "fuera de banda" utilizando un canal de comunicaciones alternativo para el transporte de estos paquetes de gestión.

1.7 WIRELESS IP LOCAL LOOP

Proviene del concepto de WIRELESS LOCAL LOOP (WLL). Es un sistema de última milla, el cual se establece a través de un radio enlace entre dos extremos que utilizan tecnología IP. En el presente informe, un extremo es el local remoto de un cliente de un ISP (local cliente) y el punto de acceso a la red de un ISP (nodo). Este tipo de enlaces es utilizado frecuentemente en soluciones residenciales o de usuarios empresariales ubicados en zonas rurales o en áreas ubicadas fuera de la cobertura ofrecida por los proveedores de servicios de comunicaciones. La figura 1.10 muestra un ejemplo de una instalación WIPLL.

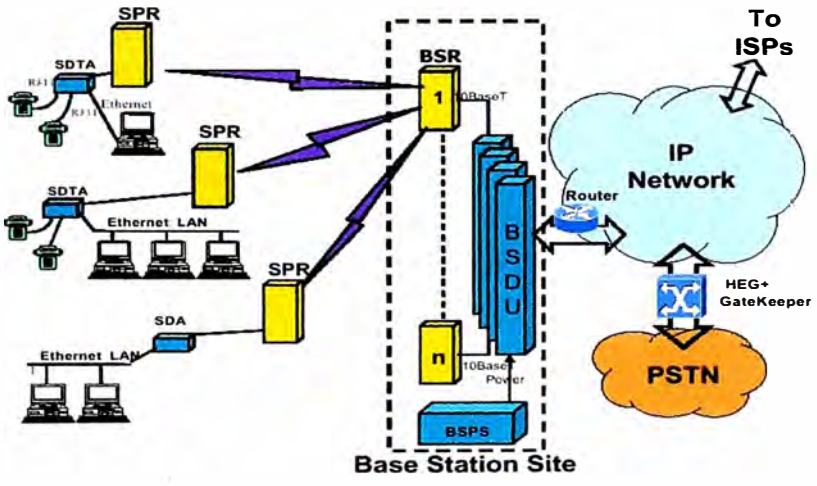


Figura 1.10: Instalación WIPLL (Fuente: AIRSPAN WIPLL – E-LIFE GROUPING)

A continuación, se detallan las nomenclaturas de los equipos mostrados en la figura anterior.

BSDU, proviene de BASE STATION DISTRIBUTION UNIT, es un equipo de comunicaciones, instalado en el local del ISP, de capa 2 del modelo OSI el cual sirve de

interfaz entre la antena en el nodo y la red IP del ISP. Así también, este equipo se encarga de suministrar energía al equipo BSR.

BSR, proviene de BASE STATION RADIO, viene a ser la antena instalada en el nodo la cual permite la comunicación hacia una o varias antenas remotas (enlace punto a punto o punto – multipunto respectivamente). Este equipo de comunicaciones opera hasta la capa 3 del modelo OSI, es decir, cuenta con la funcionalidad de procesar información en paquetes IP.

SPR, proviene de SUSCRIBER PREMISES RADIO, viene a ser la antena instalada en el local del cliente del ISP y que junto con el BSR establecen un enlace inalámbrico. Al igual que el equipo BSR, el SPR opera también hasta la capa 3 del modelo OSI.

SDA, proviene de SUSCRIBER DATA ADAPTER, viene a ser el equipo de comunicaciones instalado en el cliente que sirve de interfaz entre la antena SPR y el router instalado en el local cliente. Este equipo opera en la capa 1 del modelo OSI. Así también, este equipo se encarga de suministrar energía al equipo SPR.

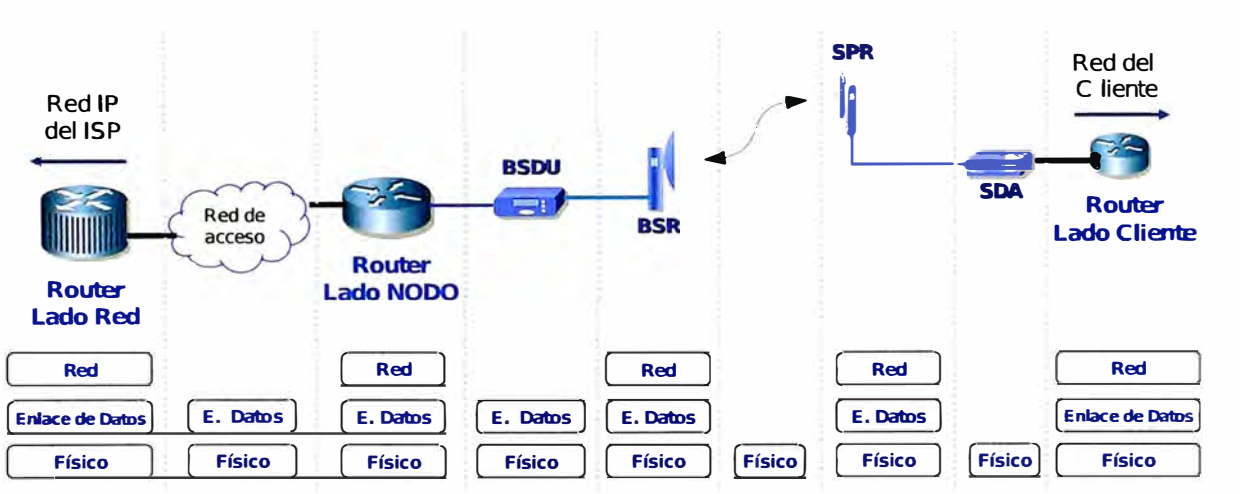


Figura 1.11: Capas OSI en instalación WIPLL (Fuente: Propio)

La figura 1.11 muestra el esquema de comunicaciones basado en el modelo OSI de una instalación WIPLL, y sirve como referencia para llevar a cabo la puesta en marcha de este sistema.

CAPÍTULO II
PLANTEAMIENTO DEL PROBLEMA

2.1 Operación del escenario actual

Un ISP brinda soluciones de comunicación a empresas a través de equipos de red que conforman un red IP MPLS. Este ISP inclusive ofrece sus servicios a aquellas empresas cuyas sedes remotas se encuentran en zonas fuera de la cobertura actual de su red de acceso (ver figura 2.1). Para este fin, hace uso de enlaces de última milla, los cuales pueden ser de fibra óptica o por medio de radio enlaces, dependiendo su elección del costo y/o factibilidad técnica de la instalación del mismo sobre la localidad del local remoto mencionado.

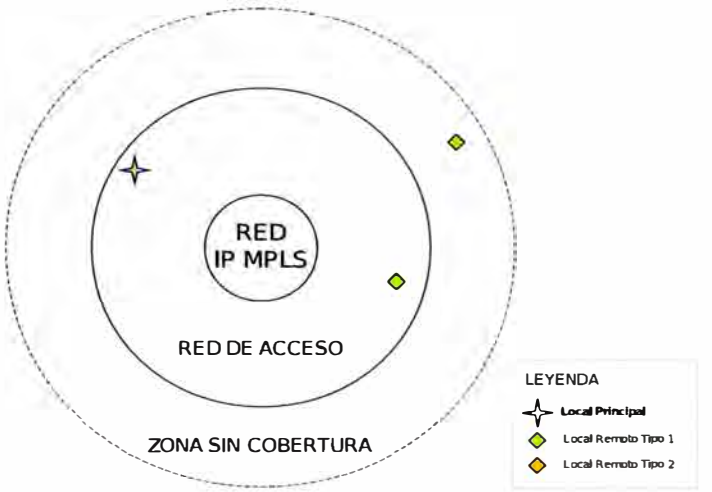


Figura 2.1: Esquema de cobertura (Fuente: Propio)

Bajo lo mencionado, consideremos a la empresa ABC como cliente del ISP. La empresa ABC cuenta con cuatro locales (ver figura 2.1), su local “principal” ubicado dentro de la cobertura de la red de acceso del ISP, dos locales remotos “tipo 1” ubicado también dentro de la cobertura mencionada y un local remoto “tipo 2” ubicado en una zona fuera de la cobertura de la red de acceso brindada por el ISP.

A continuación, se brindará mayor detalle del escenario actual dividido en dos partes, el referente al de conectividad entre los locales del cliente ABC y el centro de operaciones del ISP (NOC); como el de gestión remota (desde el NOC) de los equipos

involucrados en la solución ofrecida al cliente ABC por parte del ISP.

2.1.1 Conectividad del escenario actual

Sobre la base del concepto de VPN en una red IP MPLS, cada local de la empresa ABC es comunicada una con otra asegurándose la integridad de los canales de comunicación establecidos. La figura 2.2 muestra la topología de red de la empresa ABC.

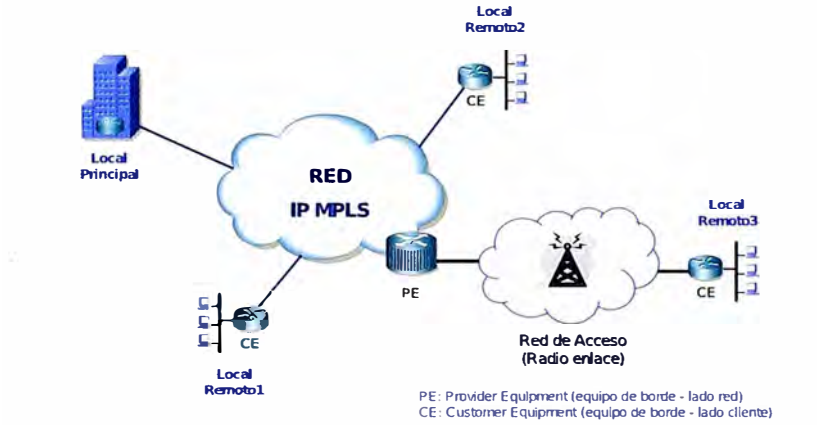


Figura 2.2: Topología de la empresa ABC (Fuente: Propio)

El local remoto 3 es el que se encuentra en la zona fuera de cobertura de la red de acceso actual y para la cual se ha instalado un radio enlace que lo comunica con el equipo PE de la Red IP MPLS. Así también, se debe señalar que la VPN sobre la Red IP MPLS creada se establece mediante la asignación de una VRF en cada uno de los ruteadores de borde (PE) involucrados en la topología de red de la empresa ABC.

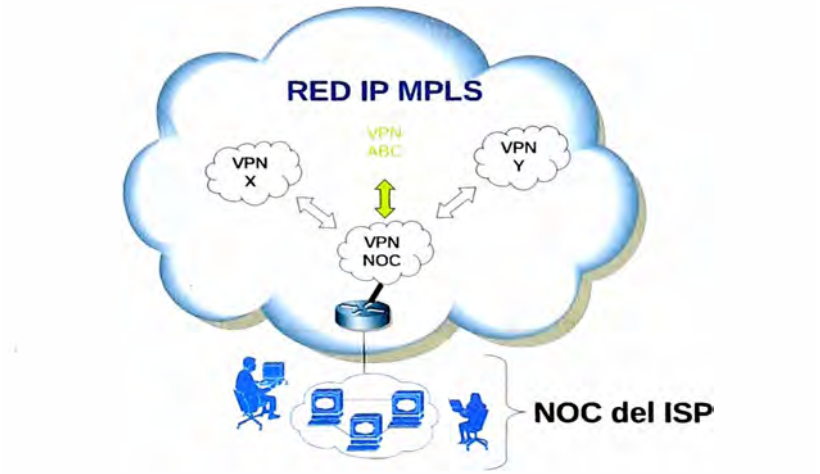


Figura 2.3: Comunicación entre el NOC y las VPN de la red IP MPLS (Fuente: Propio)

La figura 2.3 hace referencia a la interacción del NOC sobre lo configurado en la

red IP MPLS del ISP, esta interacción se abarca el intercambio de rutas IP del NOC hacia la VPN de la empresa ABC y viceversa, es decir, el envío de las rutas IP del la empresa ABC (sólo las correspondientes al de los enlaces PE-CE) hacia la red del NOC. La interacción mencionada abarca hasta la capa 3 del modelo OSI (direccionamiento IP).

Finalmente, realizando un análisis por capas OSI del enlace de última milla del local remoto 3 (ver figura 2.4), llegaremos en cuenta que los únicos equipos que podremos verificar su comunicación son tanto el router PE de borde al local remoto 3, así como también el router CE de este mismo local, siendo los equipos en el medio de este enlace invisibles para la gestión realizada desde el NOC del ISP.

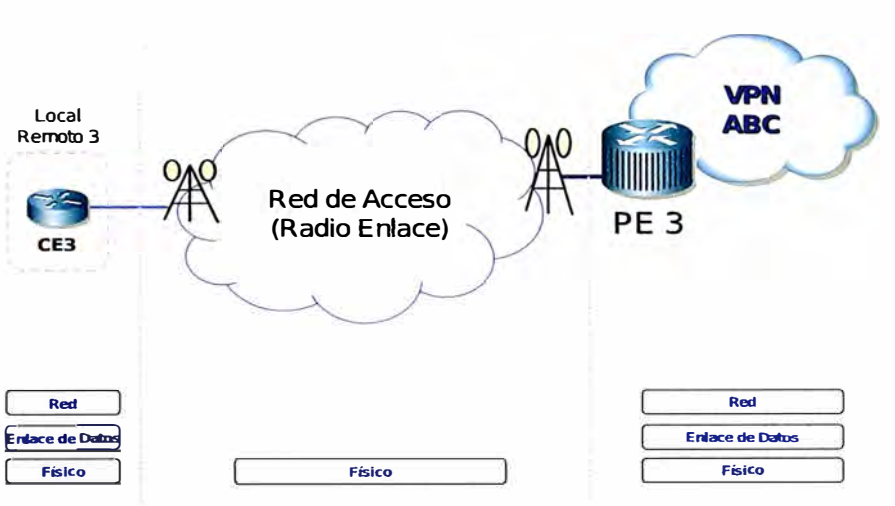


Figura 2.4: Enlace del local remoto 3 (Fuente: Propio)

2.1.2 Gestión remota

Cada local de la empresa ABC utiliza un tipo de red de acceso que se adecúa, tanto a su ubicación como a las facilidades técnicas que ésta requiera. Para nuestro caso, el local principal y el local remoto 1 utilizan una la red de acceso TDM del ISP, el cual cuenta con su propio sistema de gestión; el local remoto 2 utiliza la red de acceso ADSL del ISP, el cual también cuenta con su propio sistema de gestión; y finalmente, el local remoto 3, no utiliza un sistema de gestión debido a la capacidad de los equipos de radio enlace utilizados. Ver figura 2.5.

Cada uno de los equipos involucrados en los distintos tipos de acceso con gestión remota habilitada (TDM y ADSL), soporta el protocolo SNMP a través del cual envían los paquetes de notificación SNMP (TRAP) a los servidores recolectores de eventos alojados en el NOC del ISP. Los equipos de radio enlace utilizados no soportan SNMP y cuentan con una gestión local, el cual permite realizar pruebas y brindar datos que son de utilidad para el diagnóstico de incidencias, sin embargo, éstos se tienen que realizar en lugar donde se encuentra instalados los equipos de radio enlace al no existir alguna interfaz de

salida de esta gestión hacia algún terminal externo. Ver figura 2.6.

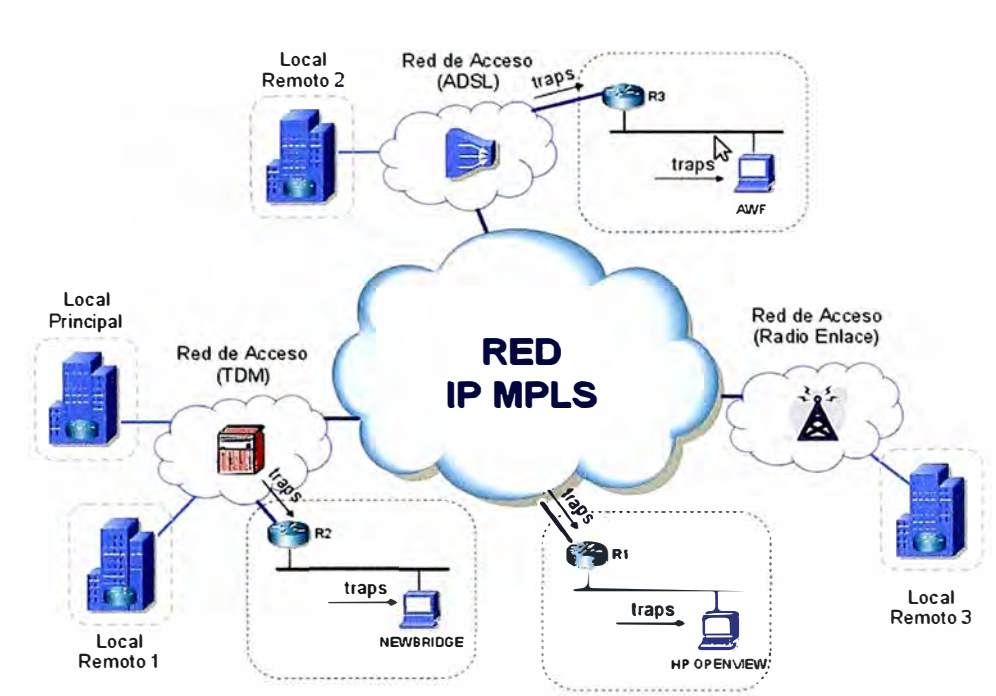


Figura 2.5: Gestión remota por tipo de red de acceso (Fuente: Propio)

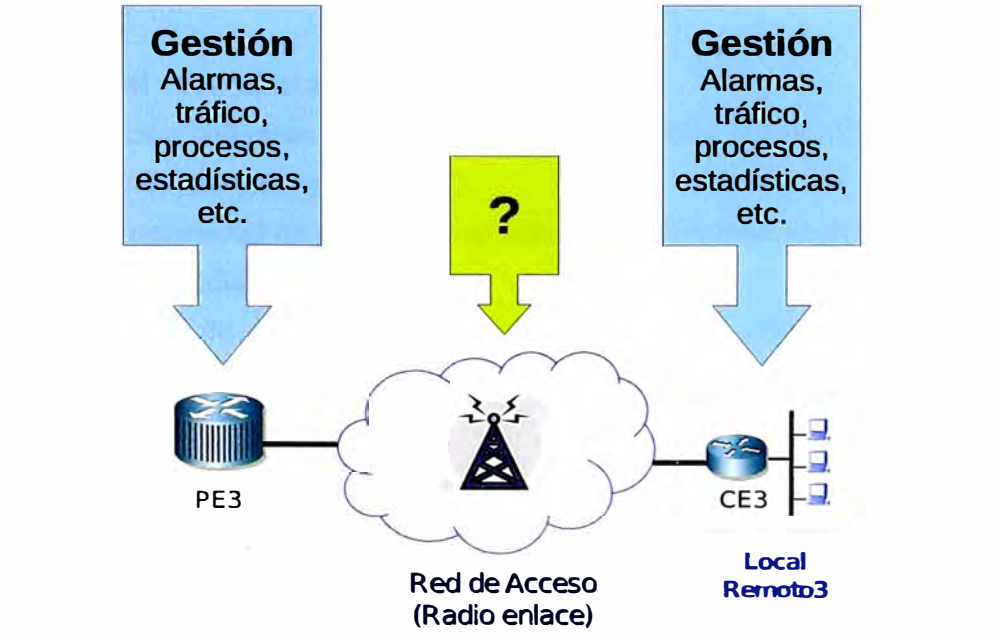


Figura 2.6: Ausencia de gestión remota en radio enlace (Fuente: Propia)

Finalmente, cabe señalar que como parte de las buenas prácticas de gestión de redes, se emplea un equipo recolector de eventos, independiente de la plataforma a gestionar, NEWBRIDGE para la red TDM, AWF para la red ADSL y HP OPENVIEW para

la red IP MPLS marcas utilizadas por el ISP. Ver figura 2.7.

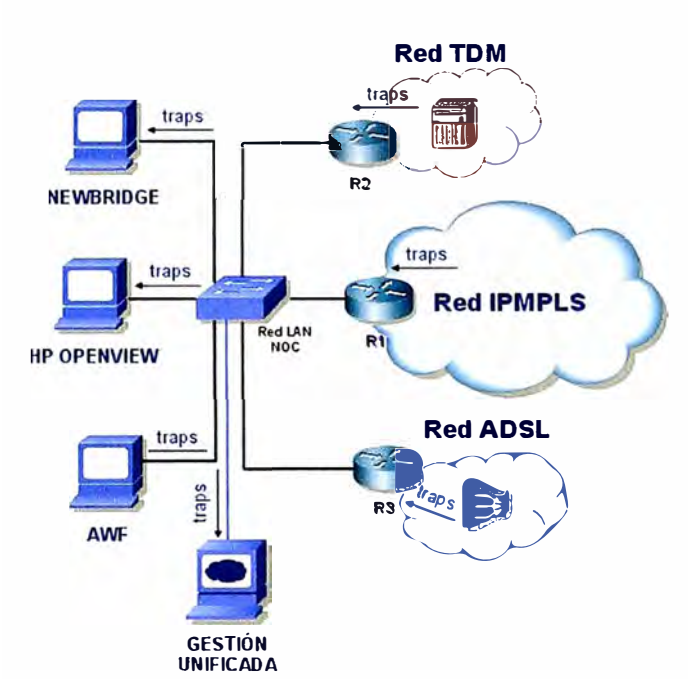


Figura 2.7: Gestión unificada (Fuente: Propia)

2.2 Ventajas y desventajas del escenario actual

2.2.1 Ventajas del escenario actual

1. Fácil interacción con otras redes, en nuestro caso, entre la Red IP MPLS del ISP y la red del local remoto 3 (empresa ABC).
2. No existe la necesidad de configuración adicional en el sistema de Gestión del ISP al instalar enlaces radiales.
3. No se requiere de una inversión en recursos físicos adicionales (unidades de almacenamiento, computadores) para mantener la información relacionada con esta red de enlaces no gestionados.

2.2.2 Desventajas del escenario actual

1. La planificación sobre la red no es eficiente, al no contar con el análisis de lo que sucede sobre ésta en tiempo real o con un tratamiento de información por históricos del funcionamiento.
2. Los recursos sobre la red no son asignados eficientemente, se requiere contar con personal de campo para realizar cambios sobre esta red.
3. El tiempo en la atención de incidencias viene a ser una de las principales desventajas, debido a que se requiere movilizar personal técnico capacitado para

realizar el diagnóstico y la solución de la incidencia desde los equipos de comunicaciones involucrados.

2.3 Detalle de la problemática

El ISP involucrado en el presente trabajo, al realizar un análisis de las ventajas y desventajas mostradas, determinó adquirir equipos de radio enlace con gestión remota habilitada (que soporten SNMP versión 2), los cuales serán instalados en el límite de la cobertura actual de las redes de acceso, con la finalidad de cubrir la demanda de comunicación de empresas cuyos locales remotos sean del tipo 2, indicados en la sección 2.1 del presente informe. Por lo cual, aparece la problemática de la habilitación de la conectividad hacia estos equipos (lado ISP y lado cliente) desde el NOC; así como también, el permitir el tránsito de los paquetes SNMP, su manejo en el terminal de gestión a implementar siguiendo las recomendaciones sugeridas por el modelo FCAPS mencionado en la sección 1.6. Ver figura 2.8.

Para la implantación del terminal de gestión podremos utilizar el software propietario de los equipos de radio enlace adquiridos por el ISP o podremos utilizar la opción de software libre, realizando la personalización requerida por parte del personal del NOC. Para ambos casos, la conectividad hacia los equipos adquiridos será lo primero en solucionar.

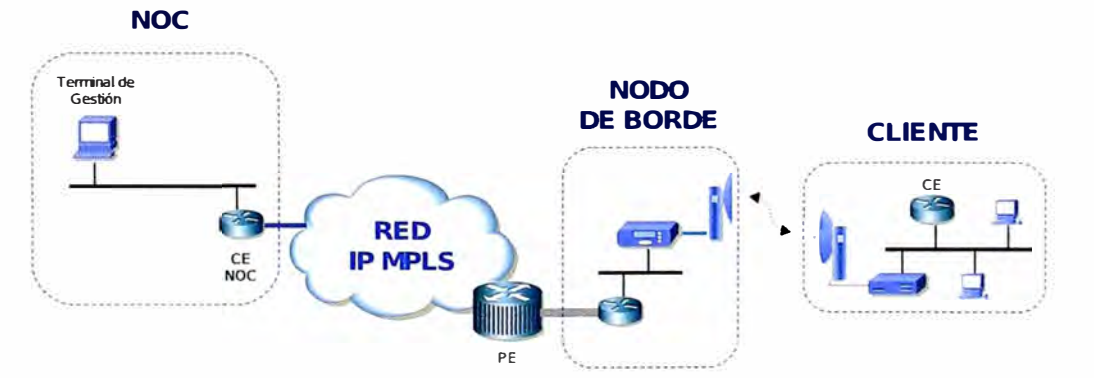


Figura 2.8: Solución con equipos gestionados de radio enlace (Fuente: Propio)

CAPÍTULO III
SOLUCIÓN DE INGENIERÍA DEL PROBLEMA

Para el desarrollo de la solución de ingeniería del problema, y basado en el modelo OSI, se empieza a resolver los puntos pendientes de conectividad entre el terminal de gestión a implementar contra los equipos de comunicaciones a gestionar (capa 3); para luego resolver los puntos pendientes en relación a la información de gestión de equipos a transmitir, sobre el camino establecido, basada en el modelo FCAPS (capa 7). Cabe señalar que la conectividad entre el terminal de gestión ubicado en el NOC contra los equipos de acceso a la red IP MPLS (equipo PE de la figura 2.8) ya se encuentran establecidos, quedando pendiente resolver la conectividad hacia los equipos instalados en una solución WIPLL (equipo router lado nodo, lado cliente, BSR y SPR).

3.1 Conectividad

3.1.1 Primer tramo

Se requiere establecer comunicación a nivel IP (capa 3 del modelo OSI) entre el router lado red (PE - PROVIDER EDGE) y el router lado nodo; para lo cual, debemos asegurarnos que tanto el nivel de capa física como el nivel de capa lógica o de enlace de datos se encuentren establecidos entre estos dos puntos. (Ver Figura 3.1)

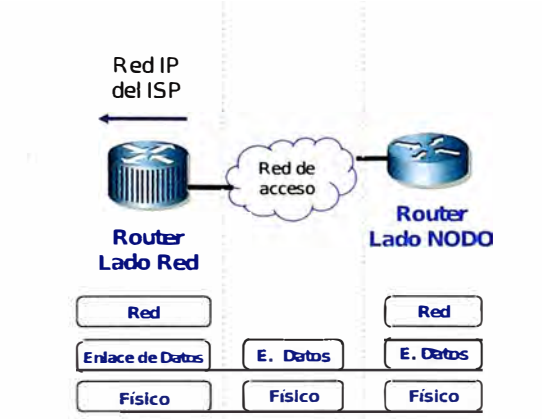


Figura 3.1: Conectividad - Primer tramo. (Fuente: Propio)

Sobre la capa física, la conexión entre el router lado red y el del lado nodo depende de la tecnología usada en la red de acceso. Actualmente se utilizan dos tipos de acceso, por interfaz tipo serial (para enlaces troncales de 2Mbps como máximo) o del tipo ETHERNET (para enlaces troncales mayores a 2Mbps). Cabe señalar, que a nivel de capa física, ya sea para uno o mas clientes configurados en el nodo, todos utilizan el mismo enlace troncal para el transporte de su información.

Sobre la capa de enlace de datos, y debido a que esta solución soporta enlaces punto multipunto, se utilizará la tecnología FRAME-RELAY para las interfaces tipo serial, y la tecnología de VLANS para las interfaces tipo ETHERNET. Para diferenciar un cliente de otro a nivel de la capa de enlace de datos, se realizará por el valor del DLCI en FRAME-RELAY asignado a cada cliente o el valor de VLAN ID en ETHERNET.

Sobre la capa de red, debemos tener en cuenta dos puntos para su establecimiento, la dirección IP a asignar y el tipo de protocolo de enrutamiento a establecer para la propagación y aprendizaje de rutas IP. El direccionamiento IP seguirá las políticas pre definidas por el NOC para la gestión de sus equipos de red, en donde cada equipo de comunicaciones a gestionar contará con una dirección IP conocida desde la red LAN del NOC. Así también, en el router lado nodo se utilizará el concepto de MULTI VRF, el cual refiere a la creación de una VRF por cliente con la intención de separar, a nivel de capa de red, las rutas aprendidas entre el router lado nodo y el lado red (PE); este aprendizaje de rutas se lleva a cabo a través de un protocolo de enrutamiento previamente seleccionado. Finalmente, cada cliente tendrá su respectiva tabla de enrutamiento en el equipo router lado nodo.

Hasta este punto, queda establecido la conectividad entre el router lado nodo y el lado red (PE), así como el camino sobre el cual cursarán los datos de gestión remota (mediante protocolo SNMP) desde el NOC hacia el router lado nodo.

3.1.2 Segundo tramo

Se requiere establecer comunicación a nivel IP entre el router lado nodo y el equipo BSR, para lo cual debemos asegurarnos, que tanto el nivel de capa física como el nivel de capa lógica o de enlace de datos se encuentren establecidos entre estos dos puntos. (Ver Figura 3.2).

Sobre la capa física, la conexión entre el router lado nodo y el equipo BSR se realiza a través del equipo BSDU, el cual cuenta con una interfaz ETHERNET (RJ45), tanto hacía el router lado nodo como hacia el equipo BSR. El equipo BSDU actúa para este caso como un conmutador. Cabe señalar, que a nivel de capa física, ya sea para uno o más clientes configurados en el nodo, todos utilizan el mismo enlace troncal para el

transporte de su información.

Sobre la capa de enlace de datos, y debido a que esta solución soporta enlaces punto multipunto, se utilizará tecnología de VLANS, por ser el medio físico del tipo ETHERNET. Para diferenciar un cliente de otro a nivel de la capa de enlace de datos, se realizará por el valor de VLAN ID asignado.

Sobre la capa de red, al igual que en el primer tramo, asignaremos una dirección IP, tanto a la interfaz ETHERNET del router lado nodo como al equipo BSR utilizando el rango de direcciones IP definidos por el NOC. El router lado nodo se encargará del enrutamiento de esta dirección IP propagada hacia el NOC del ISP. Así también, se configurará una ruta por defecto al equipo BSR, la cual apuntará a la interfaz ETHERNET del router lado nodo, asegurando así la comunicación entre el terminal de gestión implementado en el NOC con el equipo BSR.

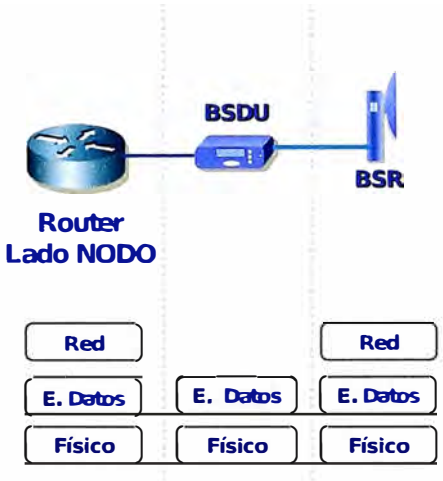


Figura 3.2: Conectividad - Segundo tramo. (Fuente: Propio)

Hasta este punto, queda establecido la conectividad entre el router lado nodo y el equipo BSR, así como el camino sobre el cual cursarán los datos de gestión remota (mediante protocolo SNMP) desde el NOC hacia el equipo BSR.

3.1.3 Tercer tramo

Se requiere establecer comunicación a nivel de capa física entre el equipo BSR y el equipo SPR. Esto se logra a través del establecimiento de un enlace inalámbrico entre ambos equipos en la banda de 3.55 GHz.

Cabe señalar, que a este nivel de capa física, ya sea para uno o más clientes configurados en el nodo, cada uno de ellos levantará su respectivo enlace inalámbrico, teniendo todos estos como punto común, al equipo BSR. (Ver Figura 3.3)

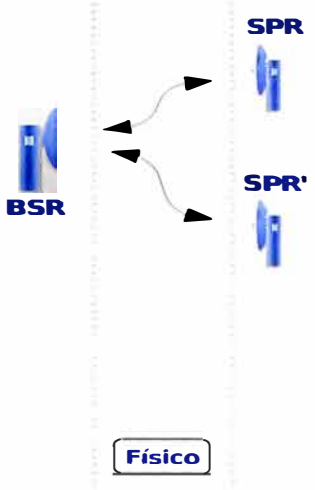


Figura 3.3: Conectividad – Tercer tramo. (Fuente: Propio)

3.1.4 Cuarto tramo

Se requiere establecer comunicación a nivel IP entre el equipo SPR y el router lado cliente; para lo cual, debemos asegurarnos que tanto el nivel de capa física como el nivel de capa lógica o de enlace de datos se encuentren establecidos entre estos dos puntos. (Ver Figura 3.4)

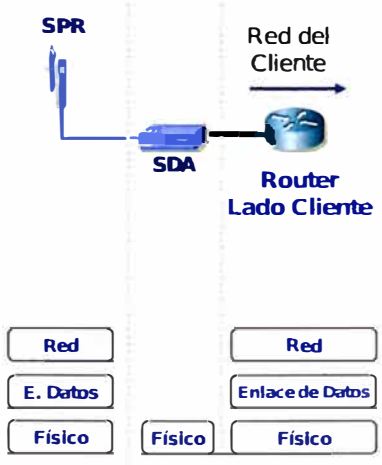


Figura 3.4: Conectividad – Cuarto tramo. (Fuente: Propio)

Sobre la capa física, la conexión entre el equipo SPR y el router lado cliente se realiza a través del equipo SDA, el cual cuenta con una interfaz ETHERNET (RJ45), tanto hacía el equipo SPR como hacia el router lado cliente. El equipo SDA actúa para este caso como un HUB.

Sobre la capa de enlace de datos, y debido a que en este punto de la solución se hace referencia a la conexión de un cliente hacia la red IP del ISP, no se utilizará

tecnología de VLANS y se procede a definir ARPA como encapsulado ETHERNET.

Sobre la capa de red, al igual que en el primer y segundo tramo, asignaremos una dirección IP, tanto a la interfaz ETHERNET del equipo SPR como al router lado cliente utilizando el rango de direcciones IP definidos por el NOC. El router lado cliente se encargará del enrutamiento de estas direcciones IP anunciándolas hacia el router lado nodo, el cual a su vez llegará al NOC del ISP. Así también, se configurará una ruta por defecto al equipo SPR, la cual apuntará a la interfaz ETHERNET del equipo BSR en el nodo, asegurando así la comunicación entre el terminal de gestión implementado en el NOC con el equipo SPR.

Hasta este punto, queda establecido la conectividad entre el equipo SPR y el router lado cliente, así como el camino sobre el cual cursarán los datos de gestión remota (mediante protocolo SNMP) desde el NOC hacia ambos equipos.

3.2 Gestión de redes

Como se ha venido mencionando en las secciones anteriores, se utilizará como protocolo de gestión de redes al SNMP (versión 2), el cual es soportado por todos los equipos involucrados en la presente problemática a resolver.

3.2.1 Generalidades

Sobre lo referente a la habilitación propia de la gestión SNMP sobre los equipos a gestionar (router lado nodo, BSR, SPR y router lado cliente), se seleccionará un mismo nombre de comunidad, tanto de lectura como de escritura, el cual será definido también en el terminal de gestión a implementar.

El terminal de gestión se instalará dentro de la red LAN del NOC del ISP desde la cual existe conectividad hacia todos los equipos clientes identificados con direcciones IP previamente definidas por el NOC. (Ver Figura 3.5)

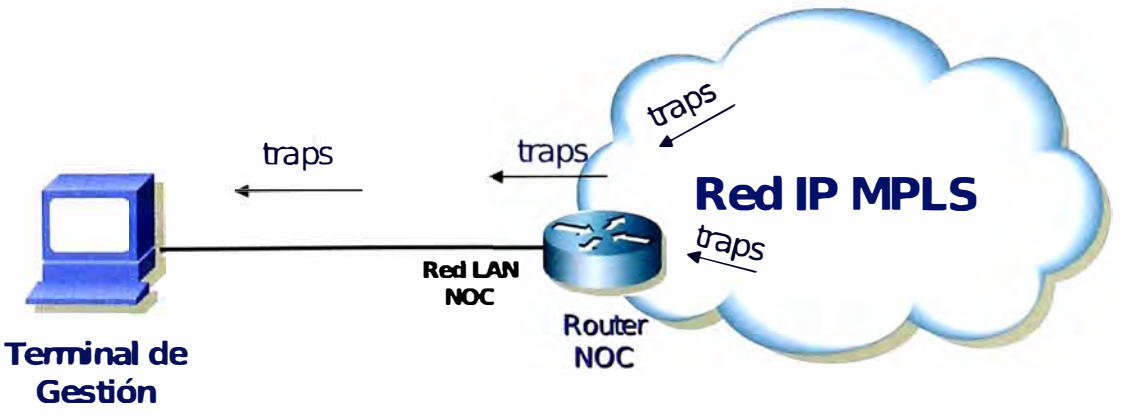


Figura 3.5: Gestión SNMP – Terminal de gestión. (Fuente: Propio)

3.2.2 Herramientas de gestión de redes

Sobre los equipos de la marca AIRSPAN, ésta brinda una herramienta de gestión propietaria para sus productos, la cual se denomina WIP-MANAGE. Este software corre bajo WINDOWS 2000, 2003, XP. Así también, debido al uso del protocolo SNMP, se puede utilizar otras herramientas de gestión propietarias (por ejemplo, HP OPENVIEW) o libres (por ejemplo, TKINED) para la lectura de TRAPS y consultas SNMP una vez cargado el MIB correspondiente de la marca.

El software de distribución libre TKINED nos permite realizar actividades de gestión remota de equipos IP. Está basado en el lenguaje de programación TCL/TK y corre bajo WINDOWS, LINUX y SOLARIS. Con este software podremos cubrir en un primer momento las áreas de gestión de fallas (alarmas visuales, mapa de estaciones remotas, etc.), de configuración (se realizará provisiones remotas o locales de ruteadores) y de contabilidad (se registrará el tráfico por cada sede remota).

Sobre los equipos router, la gestión de los mismos formaría parte del sistema actual de gestión del NOC del ISP, el cual ya cuenta con plataformas de gestión de ruteadores lado nodo y lado cliente. Sin embargo, la integración de ambas gestiones sólo puede llevarse a cabo a través de la personalización de un sistema de gestión libre (no propietario).

La decisión del uso de una u otra herramienta forma parte del planeamiento técnico económico mencionado en el capítulo 4 del presente informe de suficiencia.

3.2.3 Herramientas de generación de gráficas de tráfico

RRDTOOL es el acrónimo de ROUND ROBIN DATABASE TOOL, el cual nos permite almacenar y representar datos en intervalos temporales (ancho de banda, errores sobre el enlace, tiempos de respuesta, etc.). Los datos son almacenados en una base de datos que no crece en el tiempo y permite crear gráficas para su representación visual.

Esta base de datos es circular, reemplazando los datos más antiguos por los nuevos cuando se llegue al límite de tiempo predeterminado.

Al ser RRDTOOL una herramienta de software libre, su interacción con TKINED se logrará mediante el uso de SCRIPTS escritos en lenguaje de programación PERL. (Ver Figura 3.6)

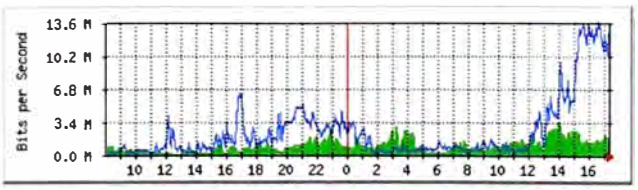


Figura 3.6: Gráfica RRDTOOL (Fuente: http://oss.oetiker.ch/mrtg/)

3.2.4 Gestión de fallas

Sobre la **ocurrencia de falla**, es nuestra tarea definir los parámetros como consumo de ancho de banda, nivel de BER (BIT ERROR RATE), nivel de RSSI (RECEIVED SIGNAL STRENGTH INDICATOR) de los equipos BSR y SPR, etc.; a partir de los cuales el cliente del ISP detecta deficiencias en el servicio ofrecido. Una vez definidos estos umbrales, estos mismos pueden reflejarse, en la opción de software libre, en la gráfica estadística obtenida mediante RRDTOOL y MRTG (MULTI ROUTER TRAFFIC GRAPHER), ese último también es de distribución libre. (Ver Figura 3.7)

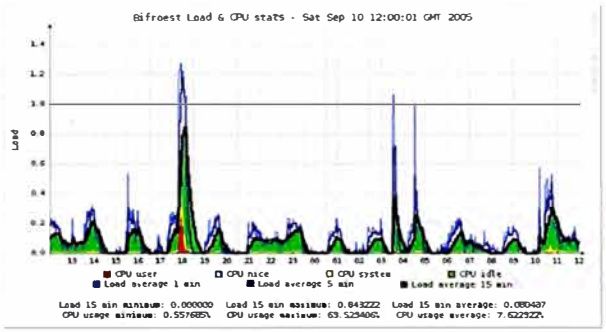


Figura 3.7: Umbral sobre gráficas RRDTOOL (Fuente: http://www.larsko.org/)

Sobre la **detección**, ésta es posible mediante una rutina periódica ejecutada en el terminal de gestión que verifica tanto la conectividad como el estado de los equipos IP a gestionar.

Para la verificación de la conectividad, se habilitará las consultas ICMP desde el terminal de gestión a implementar hacia cada equipo IP de la solución definida (router lado nodo, BSR, SPR y router lado cliente). Estas consultas ICMP deberán ser cada cierto tiempo predeterminado, lo cual se reflejará en la interfaz de administración del software de gestión. (Ver Figura 3.8)

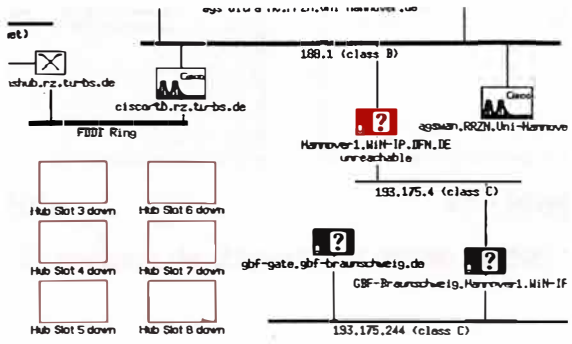


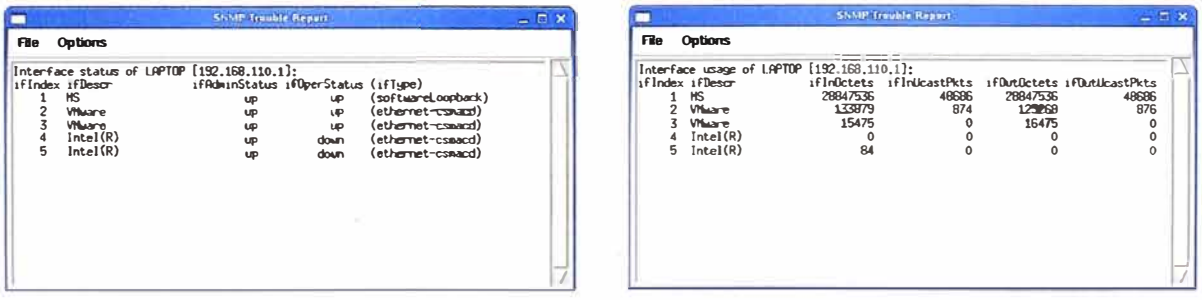
Figura 3.8: Dispositivos alarmados en color rojo (Fuente: http://www.ibr.cs.tu-bs.de)

Para la verificación del estado de los dispositivos, éstas se obtendrán mediante consultas SNMP y pueden ser por ejemplo, la cantidad de tráfico cursado por una interfaz, el estado de las interfaces de red, la cantidad de errores acumulados sobre una interfaz, etc. Para lograr esto, se deberá identificar dentro de la MIB correspondiente el valor de OID requerido para el estado buscado. La tabla 3.1 muestra los OID frecuentemente utilizados para la captura de tráfico los cuales pertenecen a la MIB denominada como RFC1213.

Tabla 3.1: OID utilizados (Fuente: Propio)

Objeto	Identificador del objeto (OID)	MIB asociada
IFINDEX	1.3.6.1.2.1.2.2.1.1	RFC1213
IFDESCR	1.3.6.1.2.1.2.2.1.2	RFC1213
IFADMINSTATUS	1.3.6.1.2.1.2.2.1.7	RFC1213
IFOPERSTATUS	1.3.6.1.2.1.2.2.1.8	RFC1213
IFTYPE	1.3.6.1.2.1.2.2.1.3	RFC1213
IFINOCTETS	1.3.6.1.2.1.2.2.1.10	RFC1213
IFINUCASTPKTS	1.3.6.1.2.1.2.2.1.11	RFC1213
IFOUTOCTETS	1.3.6.1.2.1.2.2.1.16	RFC1213
IFOUTUCASTPKTS	1.3.6.1.2.1.2.2.1.17	RFC1213

Al cargar la MIB RFC1213 en el software de gestión TKINED, la visualización de lo detectado se obtendrá al ejecutar el proceso SNMP_TROUBLE. (Ver Figura 3.9)



IF Status IF Usage Statistics

Figura 3.9: Verificación de estados de dispositivos desde TKINED (Fuente: Propia)

En ambos casos, tanto para la conectividad como para el estado de las interfaces de un equipo de red, se identifica que el valor obtenido se encuentra fuera de los

parámetros esperados de operación, se emitirá una alarma ya sea esta visual, sonora o mediante ventana emergente.

Finalmente, como parte del proceso de detección se requiere dejar activado el proceso de registro de eventos en el terminal de gestión a implementar. En el caso de TKINED, se requiere habilitar un registro de eventos (LOG), el cual esté periódicamente recibiendo información del estado de todos los dispositivos de red gestionados.

Sobre la **correlación**, ésta se logrará al tener sincronizados a todos los equipos de red, los cuales conforman la presente solución. Para lograr esto se hará uso del protocolo NTP, haciendo a los equipos de red clientes NTP, los cuales se actualizarán mediante un servidor NTP alcanzable a través de la red LAN del NOC. Los equipos que soportan NTP son el router lado nodo, el router lado cliente y el terminal de gestión a implementar. Los equipo BSR y SPR no soportan esta funcionalidad, por lo que debemos asegurarnos de configurar manualmente la fecha y hora de estos equipos igual al otorgado por el servidor NTP.

Sobre el **diagnóstico**, éste se logra con la utilización de las herramientas desarrolladas en la sección de "fallas" y "correlación" sumado a la experiencia del operador. Sin embargo, para llevar a cabo un buen diagnóstico, es importante contar con el conocimiento de toda la topología de red involucrado en el problema. Para este fin, la creación de mapas que reflejen el estado de los servicios en tiempo real son muy útiles. (Ver Figura 3.10)

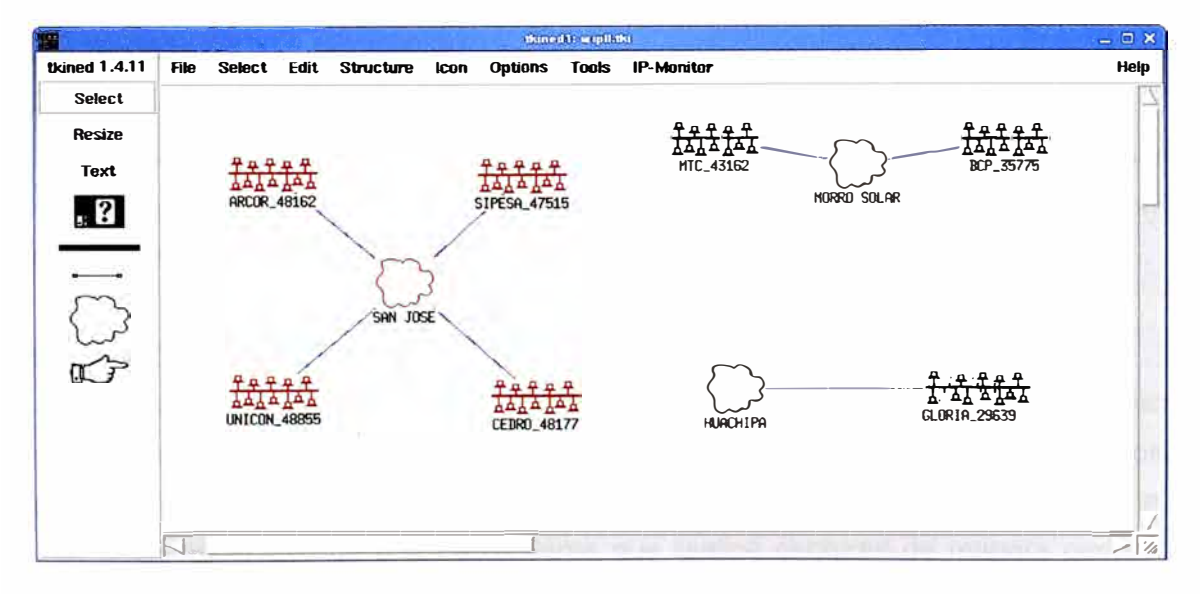


Figura 3.10: Topología de clientes WIPLL (Fuente: Propia)

Sobre la **corrección**, ésta se encuentra relacionada con la toma de decisiones para superar una falla detectada y reducir el tiempo de no disponibilidad del servicio de

los clientes del ISP. El terminal de gestión a implementar deberá contar con herramientas que generen gráficas de disponibilidad de los servicios gestionados y umbrales de niveles de servicio acordado (SLA) con sus clientes.

Sobre el **retorno a la línea base**, el terminal de gestión permitirá la funcionalidad de realizar acuse de recibo a cada una de las alarmas obtenidas por la no disponibilidad de un servicio del ISP, con la intención de llevar estadísticas de eventos que nos llevaron a salirnos de la línea base identifica por cliente. (Ver Figura 3.11)

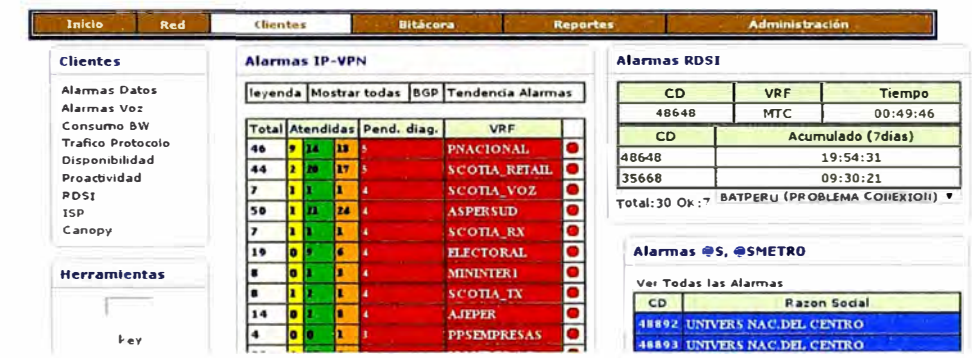


Figura 3.11: Alarmas de servicios IP-VPN (Fuente: Sistema SIGMARS - Telefónica)

3.2.5 Gestión de configuración

Se desarrollarán SCRIPTS en el terminal de gestión a implementar para realizar actividades de descarga de configuraciones de los equipos router lado nodo y lado cliente de forma periódica. Así también, el protocolo de transferencia de archivos a utilizar es SFTP (SECURE FILE TRANSFER PROTOCOL), el cual deberá ser activado, tanto en el terminal de gestión como en los equipos router involucrados.

Los equipos BSR y SPR no soportan ninguna clase de transferencia de archivos. La rutina de BACKUP de su configuración es manual o podría ser automática haciendo uso de herramientas de rutinas gráficas disponibles en INTERNET.

3.2.6 Gestión de contabilidad

En este punto se desarrollarán SCRIPTS que combinen la captura de estadísticas recolectadas vía SNMP con su registro en una base de datos mediante RRDTOOL, para luego generar gráficas en rangos de tiempo diario, semanal, mensual y anual. Para este fin, se debe hacer uso de una herramienta que realicé capturas de manera periódica, siendo el CRONTAB (software libre) una buena opción.

3.2.7 Gestión de rendimiento

Se utilizará las consultas SNMP, realizadas por el terminal de gestión a

implementar, para capturar información de tráfico relativo cursado sobre las interfaces de los equipos router lado nodo y cliente por cada uno de los clientes del ISP. Estos valores puede ser exportados a una base de datos RRDTOOL para luego ser mostrados de forma gráfica. Así también, se podrá realizar captura de estadísticas de JITTER previa configuración de los equipos router lado cliente (local principal y local remoto 3 de la Figura 2.2)

3.2.8 Gestión de seguridad

Sobre la **confidencialidad**, el acceso será controlado mediante la autenticación TACACS+ desplegado en el NOC del ISP. Así también, se habilitará en el router lado nodo y el del lado cliente, listas de acceso que permitan las consultas SNMP a los equipos router lado nodo, BSR, SPR y al router lado cliente desde la dirección IP del terminal de gestión a implementar.

Sobre la **integridad**, y haciendo uso de TACACS+, se habilitará la autorización de los tipos de comandos a ejecutar para cada uno de los usuarios autorizados. Los cambios en las configuraciones serán mostrados en cada uno de los equipos que trabajen con TACACS+. Así también, los cambios de configuraciones pueden ser mostrados en una herramienta que realicé comparaciones de configuraciones, utilizando por ejemplo la herramienta DIFF de software libre.

Sobre la **disponibilidad**, para su continuidad es recomendable hacer uso de gestión fuera de banda utilizando enlaces alternos como los ofrecidos por la red de telefónica convencional (DIAL-UP).

3.3 Ventajas y desventajas del escenario propuesto

3.3.1 Ventajas del escenario propuesto

1. Gestión de extremo a extremo de la red WIPLL, la cual soporta al servicio contratado por el cliente. Esto conlleva a un mayor conocimiento del estado del servicio ofrecido en tiempo real.
2. Mejor toma de decisiones para actividades de planificación o corrección de la red de acceso. Se podrá planificar (analizando el entorno), organizar (asignación de recursos), dirigir y controlar (seguimiento, correcciones) la topología de la red.
3. Brindar un mejor servicio a los clientes del ISP asegurando calidad en el mismo de extremo a extremo.
4. Reducción del tiempo de no disponibilidad del servicio, al contar con un diagnóstico más acertado de lo que esta ocurriendo sobre la red soportado por un mejor

conocimiento de la red.

5. Mejor control de costos, en equipos y personal. Por ejemplo, no se tendrá que desplazar en vano a un personal de campo al local del cliente si desde el NOC se identifica que el problema se encuentra en los equipos instalados en el nodo.
6. Realizar actividades de pro-actividad, detectando eventos de los servicios del cliente o de la red (lado nodo) involucrados en la presente solución.

3.3.2 Desventajas del escenario propuesto

1. Mayor complejidad en la red de acceso, debido a su interacción con redes ya existentes (lado red y lado nodo).
2. Configuración adicional en los equipos router lado cliente y lado red para acondicionar la gestión remota desde el NOC del ISP.
3. Gastos en recursos físicos (PC, discos de almacenamiento, de energía, sitio físico) para la habilitación del terminal de gestión a implementar, y recursos de personal (contratación de personal para desarrollo de sistemas, capacitación de los operadores, etc.)

CAPÍTULO IV
GESTIÓN DE TIEMPOS Y COSTOS DE LA SOLUCIÓN PROPUESTA

4.1 Definición del alcance

Habilitación de un terminal de gestión de redes el cual tendrá acción sobre equipos de comunicaciones de última milla, requiriéndose para este fin, el desarrollo de un canal de comunicación sobre el cual cursarán mensajes de gestión de redes entre este terminal y los equipos de red instalados, así como la configuración de niveles de gestión basados en el modelo FCAPS de la ISO.

4.2 Elaboración de la estructura del desglose del trabajo

La estructura del desglose del trabajo (EDT) para llevar a cabo la presente implantación se muestra en la figura 4.1.

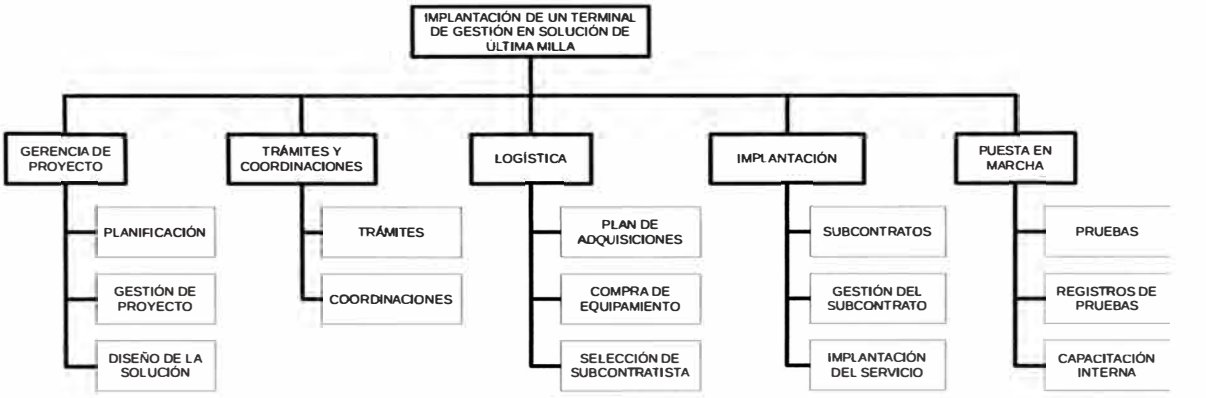


Figura 4.1: EDT del proyecto

4.2.1 Diccionario EDT

Cada paquete de trabajo mostrado en la figura 4.1 es identificado con un código EDT. Por ejemplo: “Código EDT 1.1.1”, “Código EDT 1.3.3”, etc.

a) Gerencia de Proyecto (código EDT: 1.1)

Fase que incluye el diseño, planeamiento y gestión de la implantación del proyecto.

b) Planificación (código EDT: 1.1.1)

El propósito de esta actividad consiste en coordinar los esfuerzos y recursos dentro del proyecto, estableciendo un orden dentro de las fases del proyecto.

c) Gestión de proyecto (código EDT: 1.1.2)

Se desarrolla la lista de trabajos requeridos para la correcta ejecución, seguimiento y control del proyecto luego que sea iniciada su ejecución.

d) Diseño de la solución (código EDT: 1.1.3)

El diseño de la solución va de la mano con los requerimientos y especificaciones indicados por el responsable del NOC del ISP.

e) Trámites y coordinaciones (código EDT: 1.2)

Fase en la que se incluye las actividades de soporte documental y operativo en gestiones de obtención de permisos y licencias tanto de organismos gubernamentales locales como de departamentos internos del ISP para la ejecución del proyecto.

f) Trámites (código EDT: 1.2.1)

Para el desarrollo del proyecto en zonas pertenecientes al límite de la cobertura actual del ISP (zonas rurales), se necesita establecer la documentación necesaria para ejecutar los trámites correspondiente a la implantación de la solución.

g) Coordinaciones (código EDT: 1.2.2)

Para el buen desarrollo del proyecto, se requiere que tanto las entidades gubernamentales nos otorguen los permisos correspondientes a la instalación de los equipos de borde como la autorización de los departamentos internos del ISP.

h) Logística (código EDT: 1.3)

Fase que involucra las acciones necesarias de para obtener bienes y servicios de terceros necesarios para el Desarrollo del Proyecto.

i) Plan de Adquisiciones (código EDT: 1.3.1)

Elaboración y aprobación de los documentos necesarios para planificar el plazo y costos de los bienes y servicios a ser adquiridos.

j) Compra de equipamiento (código EDT: 1.3.2)

Conjunto de actividades cuyo fin es la adquisición de bienes y servicios requeridos para la implantación del proyecto y recibirlos en las condiciones establecidas en los correspondientes contratos u órdenes de compra.

k) Selección de subcontratista (código EDT: 1.3.3)

Conjunto de actividades cuyo fin es realizar el contrato de los servicios necesarios para el proyecto.

l) Implantación (código EDT: 1.4)

Fase que involucra actividades que tienen como fin la adecuación de espacios físicos y la instalación y conexiones del equipamiento y materiales adquiridos en la fase de “compra de equipamiento”. No incluye las pruebas de funcionamiento.

ll) Subcontratos (código EDT: 1.4.1)

Conjunto de actividades cuyo fin es el seguimiento, control y aseguramiento de la calidad de los trabajos efectuados por los proveedores seleccionados.

m) Gestión del Subcontrato (código EDT: 1.4.2)

Asociado a la administración del subcontrato: comunicaciones, pagos y reportes de entrega de equipos.

n) Implantación del servicio (código EDT: 1.4.3)

Conjunto de actividades que tiene como fin realizar las instalaciones y configuraciones de los equipos de telecomunicaciones, tanto en el NOC del ISP como en el local del ISP ubicado en el límite de su área de cobertura de acuerdo a los resultados de la fase de diseño de la solución (código EDT 1.1.3).

ñ) Puesta en marcha (código EDT: 1.5)

Fase que incluye las pruebas de funcionamiento que se aplican con el fin de verificar el cumplimiento de la solución. Así también, contiene actividades de capacitación a nivel de usuarios del NOC del ISP.

o) Pruebas (código EDT: 1.5.1)

Se establecerán las pruebas necesarias para verificar la calidad de la solución ofrecida teniendo como referencia los parámetros de aceptación indicados por el personal responsable del NOC del ISP.

p) Registro de pruebas (código EDT: 1.5.2)

Los resultados de las pruebas quedaran registradas en un documento de "puesta en servicio" (RFS) para la aceptación por parte del personal responsable del NOC sobre la solución brindada.

q) Capacitación interna (código EDT: 1.5.3)

Incluye los mecanismos a emplear en la capacitación del personal del NOC que operará el sistema. A su vez mostrará los sistemas de evaluación a ser aplicados.

4.3 Plan de gestión del tiempo

4.3.1 Definición de actividades

La lista de actividades se desarrollará en base a los paquetes de trabajo definidos en el EDT. Para cada paquete de trabajo, la lista parcial será desarrollada por el miembro del equipo responsable del mismo, con el apoyo del resto en casos puntuales. Todas las listas parciales serán compiladas por un "Jefe de Planeamiento", quien preparará una lista general de actividades.

Las tablas mostradas a continuación brindarán las listas de actividades identificadas para cada uno de los paquetes de trabajo listados en la sección "Gerencia de Proyecto". Cabe señalar que cada actividad ha sido codificada siguiente la nomenclatura indicada en el código EDT de la sección anterior.

a) Gerencia de Proyecto

Tabla 4.1: Actividades definidas dentro del paquete de trabajo de planificación (código EDT 1.1.1)

Código	Paquete de trabajo / Actividad
1.1.1.1	**Elaboración de planes**
1.1.1.1.A01	Definición de responsables para cada plan de gestión
1.1.1.1.A02	Definición del grupo de trabajo por parte de cada responsable
1.1.1.1.A03	Entrega a cada responsable del formato de definición de plan y detalle del mismo
1.1.1.1.A04	Publicación de fechas de entrega de plan según cronograma
1.1.1.2	**Establecimiento de sistemas de control**

1.1.1.2.A01	Entrega y revisión de los planes requeridos
1.1.1.2.A02	Elaboración de un procedimiento de seguimiento y control de cada plan por parte del responsable
1.1.1.2.A03	Publicación de entrega de procedimientos
1.1.1.2.A04	Entrega de los procedimientos al jefe de planeamiento del cronograma, para la posterior puesta en marcha

Tabla 4.2: Actividades definidas dentro del paquete de trabajo de gestión del proyecto (código EDT 1.1.2)

Código	Paquete de trabajo / Actividad
1.1.2.1	**Adquisición del equipo del proyecto**
1.1.2.1.A01	Consultas y definición de personal requerido en cada área del Proyecto
1.1.2.1.A02	Revisión de recursos internos
1.1.2.1.A03	Convocatoria de recursos externos (personal de energía, cableado estructurado, aire acondicionado,etc.)
1.1.2.1.A04	Evaluación de Candidatos
1.1.2.1.A05	Entrevistas de Candidatos
1.1.2.1.A06	Selección
1.1.2.1.A07	Contratación
1.1.2.1.A08	Inducción
1.1.2.1.A09	Incorporación al Proyecto
1.1.2.2	**Seguimiento y control**
1.1.2.2.A01	Definición de líneas base
1.1.2.2.A02	Definición de reportes
1.1.2.2.A03	Definición de plantillas de seguimiento
1.1.2.2.A04	Establecimiento de Sistema informático para seguimiento (SIS)
1.1.2.2.A05	Levantamiento de información
1.1.2.2.A06	Ingreso de información al SIS
1.1.2.2.A07	Revisión y comparación con línea base
1.1.2.2.A08	Elaboración y presentación de informes
1.1.2.3	**Plan de aseguramiento de la calidad**
1.1.2.3.A01	Definición de responsable para elaboración del plan
1.1.2.3.A02	Definición del grupo de trabajo con el cual desarrollará el plan por parte del responsable asignado
1.1.2.3.A03	Definición de los controles y los procedimientos relacionados al plan
1.1.2.3.A04	Publicación de fechas de entrega de plan según cronograma

1.1.2.3.A05	Entrega del plan para aprobación de gerente de proyecto (GP)
1.1.2.3.A06	Publicación de plan para visualización del equipo de trabajo y posterior práctica del mismo

Las actividades 1.1.2.2.A05, 1.1.2.2.A06, 1.1.2.2.A07 y 1.1.2.2.A08 son actividades de seguimiento que se repiten semanalmente hasta el término del proyecto.

Tabla 4.3: Actividades definidas dentro del paquete de trabajo de diseño de la solución (código EDT 1.1.3)

Código	Paquete de trabajo / Actividad
1.1.3.1	**Diseño de la solución**
1.1.3.1.A01	Identificación de los requerimientos
1.1.3.1.A02	Documentación de requerimiento por parte del responsable asignado del NOC
1.1.3.1.A03	Designación del equipo de ingeniería para realizar el levantamiento de información
1.1.3.1.A04	Ejecución del levantamiento de información
1.1.3.1.A05	Consolidación de documentación de requerimientos con el responsable asignado del NOC
1.1.3.2	**Especificaciones Técnicas**
1.1.3.2.A01	Revisión del documento consolidado de requerimientos NOC
1.1.3.2.A02	Presentación de los requerimientos a la jefatura del NOC
1.1.3.2.A03	Elaboración de documentación de especificaciones técnicas: Conectividad
1.1.3.2.A04	Elaboración de documentación de especificaciones técnicas: Gestión de Redes
1.1.3.2.A05	Elaboración de documentación de especificaciones técnicas: Equipos a instalar en el NOC
1.1.3.2.A06	Elaboración de documentación de especificaciones técnicas: Local remoto del ISP (nodo)
1.1.3.2.A07	Elaboración de documentación de especificaciones técnicas: Acondicionamiento de equipos
1.1.3.3	**Diagramas del proceso**
1.1.3.3.A01	Elaboración del EDT
1.1.3.3.A02	Elaboración del diagrama del proceso
1.1.3.3.A03	Verificación y control
1.1.3.4	**Configuración de equipos**

1.1.3.4.A01	Revisión de la documentación de especificaciones técnicas generado de la actividad 1.1.3.1.A04
1.1.3.4.A02	Desarrollo del diseño preliminar de las configuraciones requeridas para la solución
1.1.3.4.A03	Instalación de equipos para realizar simulación y pruebas de configuración de la solución
1.1.3.4.A04	Configuración de equipos y pruebas de simulación
1.1.3.4.A05	Evaluación de resultados y afinamiento de las configuraciones de los equipos
1.1.3.4.A06	Desarrollo del documento del diseño final de la solución propuesta (no se indica marca de equipos)
1.1.3.5	**Selección de equipos**
1.1.3.5.A01	Revisión del documento final de configuración de los equipos generado de la actividad 1.1.3.4.A06
1.1.3.5.A02	Revisión de los catálogos de los proveedores de equipos, computadores, de cableado estructurado y de acondicionamiento de ambiente de telecomunicaciones
1.1.3.5.A03	Reuniones con proveedores
1.1.3.5.A04	Preparación de informe general sobre los equipos probados (comparativos)
1.1.3.5.A05	Desarrollo de documento de diseño final de la solución con selección de equipos. Reporte de cierre de selección
1.1.3.6	**Selección del local remoto del ISP (nodo)**
1.1.3.6.A01	Revisión del documento final de configuración de los equipos generado de la actividad 1.1.3.5.A05
1.1.3.6.A02	Evaluación preliminar de lugares a elegir como local remoto (nodo) a implantar la gestión de última milla
1.1.3.6.A03	Desarrollo de documento de especificaciones del local remoto
1.1.3.6.A04	Requerimiento de contratación de personal para el estudio de la gestión fuera de banda (a través de la red de telefonía básica)
1.1.3.6.A05	Reunión con contrata seleccionada y definición de plazos de entrega y futuras revisiones de resultados preliminares
1.1.3.6.A06	Revisión de resultados entregados por contrata
1.1.3.6.A07	Selección de local remoto (nodo)
1.1.3.6.A08	Desarrollo de documento de selección de local remoto (nodo)

A continuación se brindarán las listas de actividades identificadas para cada paquete de trabajo de la sección “Trámites y coordinaciones”. Cabe señalar que cada actividad ha sido codificada siguiente la nomenclatura indicada en el código EDT de la sección anterior.

b) Trámites y coordinaciones

Tabla 4.4: Actividades definidas dentro del paquete de trabajo de trámites (código EDT 1.2.1)

Código	Paquete de trabajo / Actividad
1.2.1.1	**Definición de los requisitos**
1.2.1.1.A01	Solicitud de un especialista legal que apoye a la recolección de documentación necesaria
1.2.1.1.A02	Recolección de los requisitos solicitados para realizar los trámites respectivos
1.2.1.1.A03	Se programan reuniones con el responsable por parte del equipo de trabajo para que vea el avance de este proceso
1.2.1.1.A04	El equipo del proyecto entrega los documentos requeridos por el especialista para que él elabore el expediente
1.2.1.2	**Elaboración de expedientes**
1.2.1.2.A01	Elaboración de expediente para entregar a las autoridades pertinentes
1.2.1.2.A02	El especialista lo entrega a las autoridades en espera de su aprobación
1.2.1.3	**Gestión de licencias**
1.2.1.3.A01	Presentación de documentación para su aceptación por parte del especialista
1.2.1.3.A02	Entrega del documento probatorio de la documentación hacia el especialista
1.2.1.3.A03	Entrega de la documentación al equipo del proyecto por parte del especialista

Tabla 4.5: Actividades definidas dentro del paquete de trabajo de coordinaciones (código EDT 1.2.2)

Código	Paquete de trabajo / Actividad
1.2.2.1	**Definición de los requisitos**
1.2.2.1.A01	Recolección de los requisitos solicitados para realizar los trámites respectivos
1.2.2.1.A02	Se programan reuniones con el responsable por parte del equipo de trabajo para que vea el avance de este proceso
1.2.2.2	**Elaboración de actas de compromiso**
1.2.2.2.A01	Se tiene como base el documento aprobado por el gerente de proyecto y se formaliza las actas

1.2.2.2.A02	Se solicita soporte a la oficina de proyectos (PMO) del ISP para el desarrollo de las actas de compromiso
1.2.2.2.A03	Se agrupan las actas de compromiso
1.2.2.3	**Gestión de actas de compromiso**
1.2.2.3.A01	El especialista de la PMO presenta documentación para su aceptación
1.2.2.3.A02	Aprobación del análisis de la documentación entregada
1.2.2.3.A03	Documentación recopilada de las actas de compromiso firmadas

A continuación se brindarán las listas de actividades identificadas para cada paquete de trabajo de la sección "Logística". Cabe señalar que cada actividad ha sido codificada siguiente la nomenclatura indicada en el código EDT de la sección anterior.

c) Logística

Tabla 4.6: Actividades definidas dentro del paquete de trabajo del plan de adquisiciones (código EDT 1.3.1)

Código	Paquete de trabajo / Actividad
1.3.1.1	**Expediente técnico de instalación**
1.3.1.1.A01	Recopilación y revisión de documentos de ingeniería
1.3.1.1.A02	Recopilación y revisión de documentos logísticos
1.3.1.1.A03	Elaboración de Expediente técnico
1.3.1.2	**Elaboración del plan de adquisiciones**
1.3.1.2.A01	Revisión de plan de gestión del proyecto
1.3.1.2.A02	Revisión de documentos de ingeniería
1.3.1.2.A03	Revisión de listas de materiales requeridos
1.3.1.2.A04	Revisión de servicios requeridos
1.3.1.2.A05	Definición de plazos y costos para adquisición de equipos y materiales
1.3.1.2.A06	Definición de plazos y costos para adquisición de subcontrato
1.3.1.2.A07	Elaboración de plan de adquisiciones
1.3.1.2.A08	Revisión y aprobación de plan de adquisiciones
1.3.1.2.A09	Publicación del plan de adquisiciones
1.3.1.3	**Expediente técnico de equipamiento**
1.3.1.3.A01	Recopilación y revisión de documentos de ingeniería
1.3.1.3.A02	Recopilación y revisión de documentos logísticos
1.3.1.3.A03	Elaboración de Expediente técnico

1.3.1.4	**Elaboración de lista de proveedores**
1.3.1.4.A01	Revisión de listas de requerimientos
1.3.1.4.A02	Revisión de listas de proveedores por tipo de requerimiento
1.3.1.4.A03	Contactos preliminares con proveedores
1.3.1.4.A04	Elaboración de lista de proveedores propuesta
1.3.1.4.A05	Revisión y aprobación de lista de proveedores
1.3.1.4.A06	Emisión de lista de proveedores a ser convocados

Tabla 4.7: Actividades definidas dentro del paquete de trabajo de compras (código EDT 1.3.2)

Código	Paquete de trabajo / Actividad
1.3.2.1	**Convocatoria a concurso de proveedores**
1.3.2.1.A01	Convocatoria a concurso
1.3.2.1.A02	Entrega de documentos a postores
1.3.2.1.A03	Absolución de consultas
1.3.2.1.A04	Recepción y verificación de ofertas
1.3.2.2	**Evaluación y selección**
1.3.2.2.A01	Evaluación técnica de propuestas
1.3.2.2.A02	Evaluación económica de propuestas
1.3.2.2.A03	Ronda de consultas
1.3.2.2.A04	Elaboración de Informe de Evaluación
1.3.2.2.A05	Ronda de negociación con finalistas
1.3.2.2.A06	Selección de adjudicados
1.3.2.3	**Ordenes de compra**
1.3.2.3.A01	Preparación de borrador de órdenes de compra
1.3.2.3.A02	Revisiones
1.3.2.3.A03	Correcciones
1.3.2.3.A04	Aprobaciones
1.3.2.3.A05	Envío de ordenes de compra a proveedores
1.3.2.3.A06	Distribución de información al equipo de proyecto
1.3.2.4	**Revisión de documentos**
1.3.2.4.A01	Revisión de documentos técnicos
1.3.2.4.A02	Revisión de documentos de despacho
1.3.2.4.A03	Re-alimentación a proveedores

Tabla 4.8: Actividades definidas dentro del paquete de trabajo de selección de subcontratista (código EDT 1.3.3)

Código	Paquete de trabajo / Actividad
1.3.3.1	**Concurso de subcontratista**
1.3.3.1.A01	Convocatoria a concurso
1.3.3.1.A02	Entrega de documentos a postores
1.3.3.1.A03	Absolución de consultas
1.3.3.1.A04	Recepción y verificación de ofertas
1.3.3.2	**Evaluación y selección**
1.3.3.2.A01	Evaluación técnica de propuestas
1.3.3.2.A02	Evaluación económica de propuestas
1.3.3.2.A03	Ronda de consultas
1.3.3.2.A04	Elaboración de Informe de Evaluación
1.3.3.2.A05	Ronda de negociación con finalistas
1.3.3.2.A06	Selección de adjudicados
1.3.3.3	**Contrato**
1.3.3.3.A01	Preparación del borrador del subcontrato
1.3.3.3.A02	Revisiones
1.3.3.3.A03	Correcciones
1.3.3.3.A04	Aprobaciones
1.3.3.3.A05	Envío de subcontrato a postor ganador
1.3.3.3.A06	Revisiones
1.3.3.3.A07	Correcciones
1.3.3.3.A08	Firma de subcontrato
1.3.3.3.A09	Distribución de información al equipo de proyecto

A continuación se brindarán las listas de actividades identificadas para cada paquete de trabajo de la sección "Implantación". Cabe señalar que cada actividad ha sido codificada siguiente la nomenclatura indicada en el código EDT de la sección anterior.

d) Implantación

Tabla 4.9: Actividades definidas dentro del paquete de trabajo de subcontratos (código EDT 1.4.1)

Código	Paquete de trabajo / Actividad
1.4.1.1	**Transporte de equipos**
1.4.1.1.A01	Coordinación con empresa de transportes
1.4.1.1.A02	Verificación de carga en transporte
1.4.1.1.A03	Verificación de recepción en obra
1.4.1.2	**Instalación física de equipos y línea telefónica**
1.4.1.2.A01	Ejecución de subcontrato de instalación
1.4.1.2.A02	Supervisión de subcontrato de instalación
1.4.1.3	**Acondicionamiento de ambientes de telecomunicaciones (Sala de equipos NOC, nodo ISP)**
1.4.1.3.A01	Instalación del diseño eléctrico de la solución
1.4.1.3.A02	Instalación del diseño de cableado estructurado de la solución
1.4.1.3.A03	Instalación del diseño de aire acondicionado de la solución
1.4.1.3.A04	Supervisión del subcontrato

Tabla 4.10: Actividades definidas dentro del paquete de trabajo de gestión del subcontrato (código EDT 1.4.2)

Código	Paquete de trabajo / Actividad
1.4.2.1	**Seguimiento**
1.4.2.1.A01	Reporte final del subcontrato
1.4.2.1.A02	Revisión y aprobación de valorizaciones del subcontrato

Tabla 4.11: Actividades definidas dentro del paquete de trabajo de gestión de implantación del servicio (código EDT 1.4.3)

Código	Paquete de trabajo / Actividad
1.4.3.1	**Instalación de equipos ubicados en el local remoto del ISP (nodo)**
1.4.3.1.A01	Revisión del documento de selección de equipos generado en la actividad 1.1.3.5.A05
1.4.3.1.A02	Revisión de documento de equipos adquiridos y revisión de los mismos
1.4.3.1.A03	Puesta en línea de los equipos instalados

1.4.3.1.A04	Elaboración del documento de instalación de equipos en el local remoto del ISP (sin configurar)
1.4.3.2	**Instalación de equipos ubicados en la sala de equipos del NOC**
1.4.3.2.A01	Revisión del documento de selección de equipos generado en la actividad 1.1.3.5.A05
1.4.3.2.A02	Revisión de documento de equipos adquiridos y revisión de los mismos
1.4.3.2.A03	Puesta en línea de los equipos instalados
1.4.3.2.A04	Elaboración de documento de instalación de equipos en la sala de equipos del NOC (sin configurar)
1.4.3.3	**Configuración de equipos ubicados en el local remoto del ISP (nodo)**
1.4.3.3.A01	Revisión del documento de selección de equipos generado en la actividad 1.1.3.4.A06
1.4.3.3.A02	Revisión del documento generado por la actividad 1.4.3.1.A04
1.4.3.3.A03	Configuración de equipos para levantar la conectividad entre los equipos del NOC y los del local remoto (nodo)
1.4.3.3.A04	Configuración de equipos para levantar la gestión remota entre los equipos del NOC y los del local remoto (nodo)
1.4.3.3.A05	Elaboración del documento de "puesta de servicio" de los equipos ubicados en el local remoto del ISP (nodo)
1.4.3.4	**Configuración de equipos ubicados en la sala de equipos del NOC**
1.4.3.4.A01	Revisión del documento de selección de equipos generado en la actividad 1.1.3.4.A06
1.4.3.4.A02	Revisión del documento generado por la actividad 1.4.3.2.A04
1.4.3.4.A03	Configuración de equipos para levantar la conectividad entre los equipos del NOC y los del local remoto (nodo)
1.4.3.4.A04	Configuración de equipos para levantar la gestión remota entre los equipos del NOC y los del local remoto (nodo)
1.4.3.4.A05	Elaboración del documento de "puesta de servicio" de los equipos ubicados en la sala de equipos del NOC

A continuación se brindarán las listas de actividades identificadas para cada paquete de trabajo de la sección "Puesta en marcha". Cabe señalar que cada actividad ha sido codificada siguiente la nomenclatura indicada en el código EDT de la sección anterior.

e) Puesta en marcha

Tabla 4.12: Actividades definidas dentro del paquete de trabajo de pruebas (código EDT 1.5.1)

Código	Paquete de trabajo / Actividad
1.5.1.1	**Pruebas de servicio**
1.5.1.1.A01	Prueba de conectividad desde los equipos del NOC hacia los del local remoto del ISP (y viceversa)
1.5.1.1.A02	Prueba de la gestión remota de los equipos instalados en el local remoto del ISP
1.5.1.1.A03	Pruebas de la gestión fuera de banda
1.5.1.2	**Elaboración de informe de resultados obtenidos**
1.5.1.2.A01	Informe de resultados de las pruebas de conectividad
1.5.1.2.A02	Informe de resultados de las pruebas de gestión remota

Tabla 4.13: Actividades definidas dentro del paquete de trabajo de registro de pruebas (código EDT 1.5.2)

Código	Paquete de trabajo / Actividad
1.5.2.1	**Consolidación de los informes de resultados**
1.5.2.1.A01	Revisión del documento generado por la actividad 1.5.1.2.A01
1.5.2.1.A02	Revisión del documento generado por la actividad 1.5.1.2.A02
1.5.2.1.A03	Elaboración del registro de pruebas de la solución implantada

Tabla 4.14: Actividades definidas dentro del paquete de trabajo de capacitación interna (código EDT 1.5.3)

Código	Paquete de trabajo / Actividad
1.5.3.1	**Coordinación con el responsable del NOC**
1.5.3.1.A01	Entrega de la relación de personas a capacitar por parte del responsable del NOC
1.5.3.1.A02	Se coordina lugar, fechas y hora de capacitación a disponer por parte del responsable del NOC
1.5.3.2	**Coordinaciones con el capacitador**
1.5.3.2.A01	Selección del capacitador
1.5.3.2.A02	Elaboración del cronograma de clases y preparación del material

1.5.3.3	Clases
1.5.3.3.A01	Dictado de clases
1.5.3.3.A02	Evaluación de alumnos
1.5.3.3.A03	Elaboración del desempeño del grupo y se entrega al responsable del NOC

4.3.2 Secuencia de actividades

La secuencia de actividades será representada por medio de un diagrama de red utilizando el método de diagramación mediante flechas en donde cada flecha representa las actividades a realizar y la cual a su vez conecta a nodos para mostrar sus dependencias.

El Jefe de Planeamiento será el responsable de revisar el diagrama de red elaborado por cada uno de los miembros del equipo del proyecto.

4.3.3 Estimación de recursos y costos

Luego de aprobada la lista de actividades y el diagrama de red, cada responsable de paquete de trabajo, elaborará la estimación de recursos (costo, tiempo, personal) en base a la cantidad de trabajo, teniendo como referencia, su propia experiencia en este tipo de actividades.

La estimación de la duración de actividades se desarrollará en paralelo y estará a cargo de cada responsable de paquete de trabajo, y al igual que en la estimación de recursos, la estimación de la duración de actividades tendrá como base la experiencia del responsable del paquete de trabajo.

4.3.4 Cronograma de la solución propuesta

El Jefe de Planeamiento utiliza el diagrama de red establecido y recopila la lista de actividades, los atributos de actividades, la información de recursos y duraciones estimadas para elaborar el cronograma del proyecto.

La elaboración del cronograma se realizará por el método de ruta crítica, utilizando para esto el cálculo de fechas teóricas de inicio y fin, temprano y tardío. La figura 4.16 muestra el diagrama de GANTT del proyecto elaborado en el software de gestión PLANNER.

Se debe tener en cuenta que la fecha de inicio del proyecto es 3 de enero del 2011 y la de fin, el 10 de junio de 2011.

Cabe señalar que la actividad de seguimiento y control que forma parte de la "gestión del proyecto" (código EDT 1.1.2) esta conformado por actividades periódicas con frecuencia semanal (una vez por semana) desde el inicio hasta el fin del proyecto.

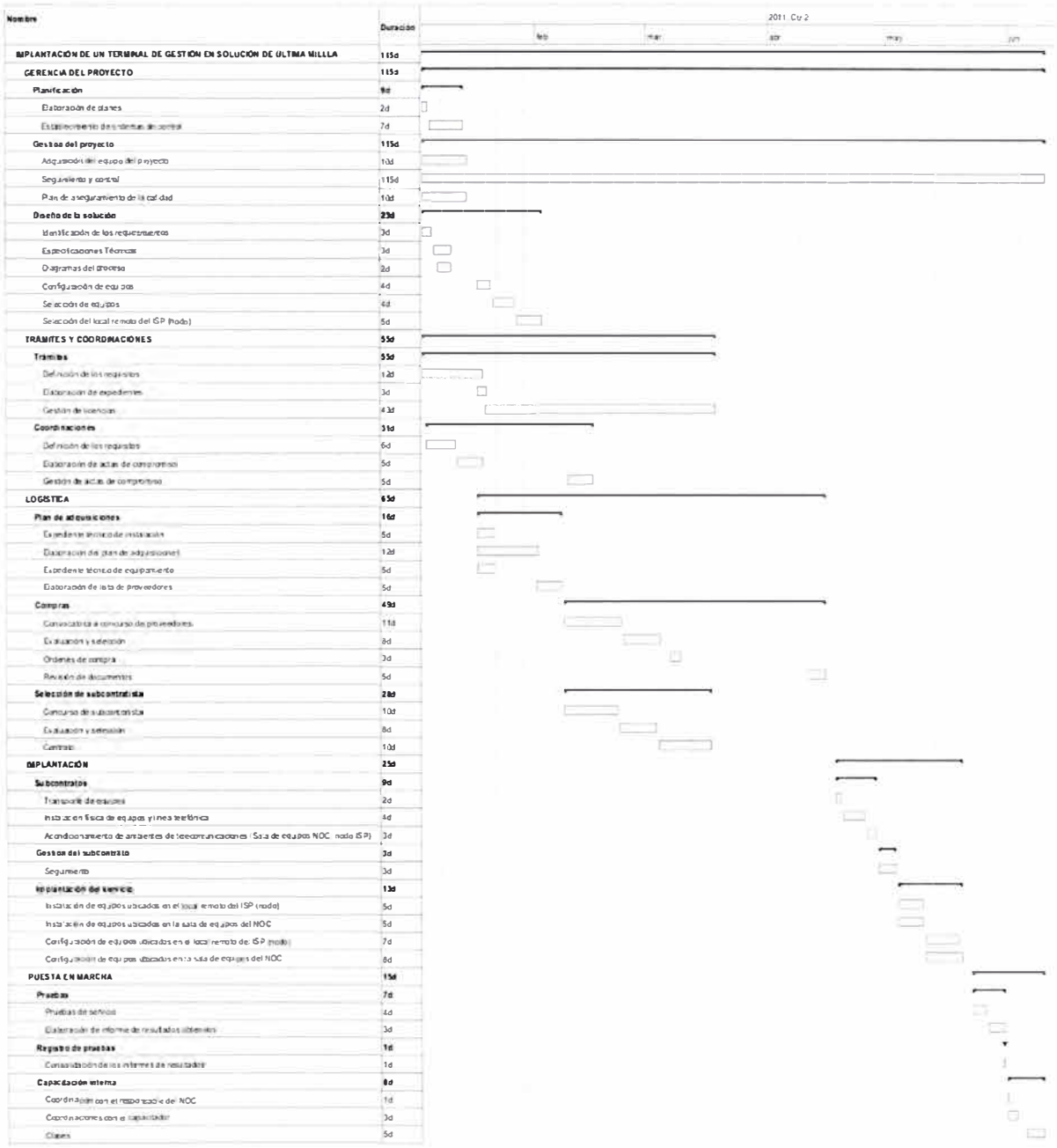


Figura 4.16: Diagrama de GANTT del proyecto

4.4 Plan de gestión de costos

El proyecto ha sido puesto en ejecucion en base a un presupuesto preliminar elaborado por la gerencia ejecutiva del NOC del ISP basado en estimados y supuestos de los recursos necesarios. Para efectos de estimación, presupuesto, seguimiento y control del proyecto no se considerará el monto correspondiente al IGV.

Los costos de materiales importados deben registrarse en términos DDP (DELIVERY DUTY PAID) en los almacenes del ISP. El presupuesto preliminar presentado

por la gerencia ejecutiva del NOC se muestra en la tabla 4.15.

Tabla 4.15: Presupuesto preliminar

Ítem	Precio sin IGV (US$)	Precio con IGV (US$)
Gestión de proyecto	3 000,00	3 570,00
Costo de equipamiento (incluye transporte de equipos)	5 000,00	5 950,00
Instalación del servicio	500,00	595,00
Permisos para la puesta en operación	300,00	357,00
Seguros de los equipos contra perjuicios de terceros	1 500,00	1 785,00
Imprevistos	1 000,00	1 190,00
Visitas técnicas y supervisión	500,00	595,00

Los costos indicados ascienden a $ 11 800,00 (sin IGV) y la mayoría de estos son únicos, de tal forma que cuando se requiera levantar la gestión remota de un nuevo local remoto del ISP, sólo se considerarán los costos de equipos y línea telefónica a instalar en el local remoto del ISP, así como la configuración de estos equipos y su correcta relación con los equipos ubicados en el NOC.

Los lineamientos indicados en el presente plan deben apuntar a alcanzar dicho compromiso, enmarcados dentro de los componentes de tiempo y calidad.

4.4.1 Estimación de costos

La estimación de costos se realizará a partir de los paquetes de trabajo disgregados en la sección anterior (plan de tiempo). Se tomarán en cuenta las siguientes consideraciones:

1. La unidad monetaria a utilizar es el dólar americano.
2. Se utilizarán las cifras en dos decimales.

Los costos de cada paquete de trabajo se calcularán a partir de una cantidad de unidad de medida de recursos a ser multiplicada por un costo unitario. Por cada paquete de trabajo se preparará una hoja de detalle de costos, la cual incluye todos los recursos utilizados, las cantidades, los costos unitarios y los costos totales correspondientes. El consolidado de esta información será responsabilidad del jefe de costos designado en el presente proyecto. Para el cálculo de las estimaciones de costos, se seguirán los siguientes lineamientos de personal, equipamiento y materiales:

1. Personal

+ Para cada paquete de trabajo se lista la cantidad y el tipo de recurso de personal (puesto) requerido.
+ La unidad de medida aplicable es la Hora Hombre (HH).
+ La cantidad de HH asignada por recurso es definida durante la estimación de recursos y duraciones del plan de gestión del tiempo.
+ Los costos unitarios por HH de cada recurso de personal son definidos por la gerencia de Recursos Humanos del ISP.
+ A efectos del presente proyecto no debe considerarse el uso de horas extras.

2. Equipamiento

+ El equipamiento de la empresa es compartido con el desarrollo de otros proyectos.
+ Para el equipamiento de oficina, se tomará en cuenta las mismas consideraciones que las indicadas para el personal, en cuanto a que cada equipo de oficina tiene como responsable a un miembro del equipo del proyecto.
+ En el caso de equipamiento de trabajo, se tomará en cuenta las estimaciones de uso elaboradas por la gerencia de operaciones del ISP.
+ Para cada paquete de trabajo se lista la cantidad y el tipo de recurso de equipamiento requerido.
+ La unidad de medida aplicable es la Hora Equipo (HE).
+ La cantidad de HE asignada por recurso es definida durante la estimación de recursos y duraciones del plan de gestión del tiempo. Normalmente es asociada a la cantidad de HH del responsable del mencionado equipamiento.
+ Los costos unitarios por HE de cada recurso de personal son definidos según la tarifa de costos internos del ISP.

3. Materiales

+ Bajo el rubro de materiales encontramos el de insumos requeridos, bienes requeridos y el de servicios requeridos para la ejecución del Proyecto.
+ Los materiales requeridos para la ejecución del proyecto son adquiridos exclusivamente para este uso. No se adquirirán materiales para stock del ISP.
+ Para cada paquete de trabajo se lista la cantidad y el tipo de recurso de materiales requerido.
+ La unidad de medida aplicable depende de cada tipo de material.
+ La cantidad de materiales requerido se estima según la información base disponible, mediante análisis de cada paquete de trabajo.
+ Los costos unitarios por cada material pueden obtenerse de las siguientes fuentes (según disponibilidad): cotizaciones de proveedores, tarifarios vigentes de materiales, y estimación aproximada de materiales a partir de bases históricas.

4.4.2 Preparación del presupuesto de costos

Una vez definidos los costos de cada paquete de trabajo, se realiza la suma total de los mismos para calcular el Presupuesto de Costos. Se considerará un 5% del costo estimado a modo de reserva de contingencia, la cual se añadirá a la línea base.

El presupuesto total se compara con la estimación inicial del proyecto. En caso que el presupuesto exceda la estimación inicial, se realizará nuevamente el estimado de costos, comenzando por aquellos paquetes de trabajo donde se muestre la mayor variación. Esta revisión de costos debe realizarse revisando de manera constante las otras variables de la triple restricción (alcance, costos y tiempo), controlando que se mantenga la línea base correspondiente.

Finalmente, se considera que el área de proyectos del ISP estará a cargo del presente proyecto, teniendo como honorarios el valor de $700,00 (margen) por uso de sus flujos de gestión de proyectos.

Flujo de Caja Neto

Teniendo en cuenta los ingresos y gastos del presente proyecto siguiendo lo definido en la sección 4.1.1 del presente informe (estimación de costos) se realizará el cálculo del flujo de caja neto por semana. Este cálculo resulta de la suma del valor del flujo de caja inicial con el valor del saldo inicial en la semana analizada; en donde, el flujo de caja inicial por semana se obtiene de la diferencia del ingreso ocurrido en la semana con el valor del gasto realizado en la semana analizada.

La figura 4.2 muestra el flujo de caja desarrollado para el presente proyecto y cada cálculo individual se resume en la tabla 4.15 en donde se mostrarán los cálculos efectuados por semana (valores sin IGV).

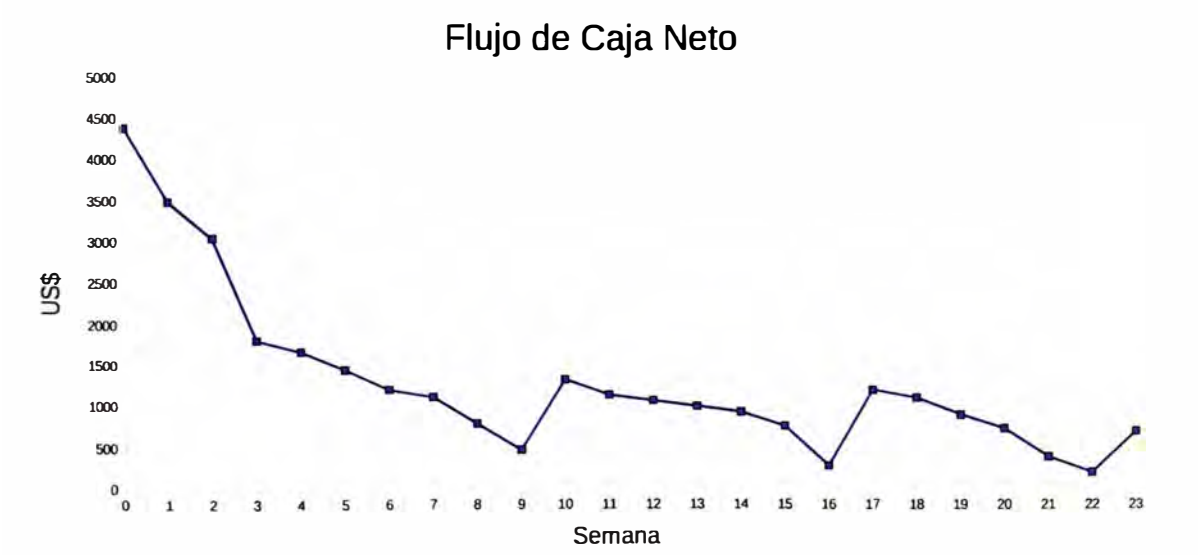


Figura 4.2: Flujo de Caja Neto del proyecto

Tabla 4.15: Cálculo del Flujo de Caja Neto del proyecto

Semana	Gasto en la semana (US$)	Ingreso (US$)	Flujo de Caja Inicial (US$)	Saldo Inicial (US$)	Flujo de Caja Neto (US$)
0	0,00	4 375,00	4 375,00	0,00	4 375,00
1	895,00	0,00	(-) 895,00	4 375,00	3 480,00
2	440,00	0,00	(-) 440,00	3 480,00	3 040,00
3	1235,00	0,00	(-) 1235,00	3 040,00	1 805,00
4	140,00	0,00	(-) 140,00	1 805,00	1 665,00
5	220,00	0,00	(-) 220,00	1 665,00	1 445,00
6	240,00	0,00	(-) 240,00	1 445,00	1 205,00
7	90,00	0,00	(-) 90,00	1 205,00	1 115,00
8	320,00	0,00	(-) 320,00	1 115,00	795,00
9	320,00	0,00	(-) 320,00	795,00	475,00
10	4 770,00	5 625,00	855,00	475,00	1 330,00
11	190,00	0,00	(-) 190,00	1 330,00	1 140,00
12	70,00	0,00	(-) 70,00	1 140,00	1 070,00
13	70,00	0,00	(-) 70,00	1 070,00	1 000,00
14	70,00	0,00	(-) 70,00	1 000,00	930,00
15	170,00	0,00	(-) 170,00	930,00	760,00
16	480,00	0,00	(-) 480,00	760,00	280,00
17	960,00	1 875,00	915,00	280,00	1 195,00
18	96,00	0,00	(-) 96,00	1 195,00	1 099,00
19	199,00	0,00	(-) 199,00	1 099,00	900,00
20	165,00	0,00	(-) 165,00	900,00	735,00
21	345,00	0,00	(-) 345,00	735,00	390,00
22	190,00	0,00	(-) 190,00	390,00	200,00
23	125,00	625,00	500,00	200,00	700,00
TOTAL	11 800,00	12 500,00			

Curva S

La curva S del proyecto resulta al mostrar el valor del costo (gasto) acumulativo del proyecto por semana. La figura 4.3 muestra la Curva S del presente proyecto sobre el cual podemos observar el valor planeado (PV) para cada una de las semanas del proyecto (valores sin IGV).

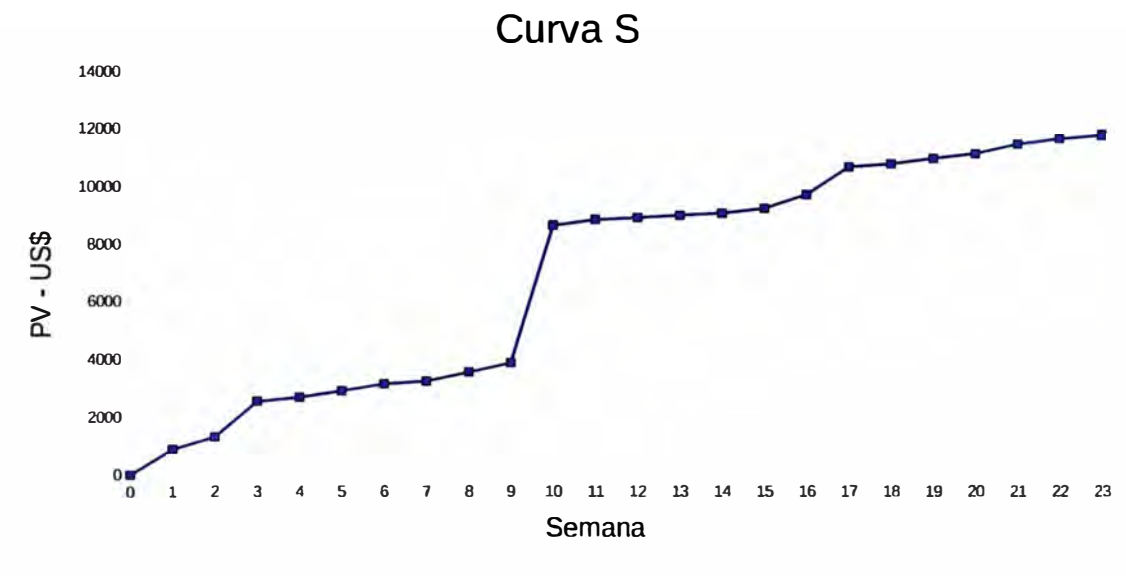


Figura 4.3: Curva S del proyecto

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

El núcleo de un NOC es la gestión misma sobre los equipos de red que tienen a cargo gestionar. Cuando tenemos elementos en la red sobre el cual no podemos realizar esta función, esta deficiencia se refleja en el desconocimiento de lo que esta pasando en el momento sobre ese equipo y sobre su interacción con los equipos al cual se conecta. Muchas veces, en el análisis de una incidencia se hace necesario ver la versión de lo que está ocurriendo desde todos los equipos involucrados sobre el servicio contratado que presenta la incidencia, si bien podemos realizar el análisis al considerar este equipo como una caja negra y ver lo que recibimos al enviarle ciertos paquetes para obtener respuestas esperadas, este análisis toma tiempo, el cual muchas veces no se cuenta por tener al cliente al lado exigiendo una pronta respuesta.

Como se evidenció en el capítulo III, solución de ingeniería del problema, la gestión de redes y servicio juega un papel muy importante en la gestión de un cliente, al permitirnos ofrecer servicios, los cuales cumplen con la calidad contratada por el cliente y también, obtener un rendimiento óptimo de la inversión realizada en la infraestructura de la red desplegada.

Todo este esfuerzo tiene finalmente una orientación, la del cliente, el cual marca cambios rotundos en la red, pasando de una red con menor complejidad a una de mayor, pero la cual a su vez trae beneficios, tanto técnicos como económicos.

En el mercado, el cliente puede elegir entre ISP no por la red o el nivel de gestión de redes que esta tiene, sino por la atención que los ISP pueden dar al cliente, esto se convierte en un factor de negocio importante. Al mejorar los tiempos de atención, ya sea los de peticiones comerciales o el de atención de incidencias.

Finalmente, cada vez se hace mayor el compromiso que el cliente hace firmar al operador de un nivel de disponibilidad mínimo conocido como SLA el cual abarca penalidades en caso de incumplimiento por parte del ISP. Para controlar esto, debemos manejar al máximo toda la información relevante de los servicios contratados por el cliente y de las redes que la soporta, ahí entra la gestión de redes y servicios que viene a ser el núcleo del presente informe de suficiencia.

5.2 Recomendaciones

A continuación se lista las siguientes recomendaciones:

1. Utilizar herramientas de sistema abierto como los indicados en el capítulo III del presente informe, nos permiten personalizar el nivel de gestión a obtener de los equipos a implementar, en este caso el de una solución de última milla de nivel 3.
2. Conocer a detalle la MIB de los fabricantes hace posible la obtención de información que puede ser clave al momento de realizar análisis de la operación de los equipos instalados ya sea para incidencias sobre estos o para tareas de planificación sobre la red.
3. Utilizar los modelos de gestión de redes OSI y FCAPS forma parte de una buena práctica al momento de realizar la implantación de equipos de red tanto a nivel de conectividad como el de gestión de redes.
4. Trasladar el enfoque cliente impulsado por la empresa operadora a la gestión de los servicios ofrecidos, tal como se comentó en la sección 3.2.4 (Gestión de fallas).

ANEXO A
GLOSARIO DE TÉRMINOS

ADSL (ASYMMETRIC DIGITAL SUBSCRIBER LINE)

Es una tipo de tecnología DSL, la cual permite la transmisión de datos sobre las líneas de par de cobre, con mayor velocidad en comparación al de un enlace tipo DIAL-UP. ADSL utiliza frecuencias que no son usadas por la comunicación de voz, frecuencias superiores que no pueden ser escuchadas por el oído humano. Es asimétrico, debido a que el valor de la velocidad de subida y de bajada difieren entre sí.

BSDU (BASE STATION DISTRIBUTION UNIT)

Es un equipo de comunicaciones, instalado en el local del ISP, de capa 2 del modelo OSI el cual sirve de interfaz entre la antena en el nodo y la red IP del ISP. Así también, éste equipo se encarga de suministrar energía al equipo BSR.

BSR (BASE STATION RADIO)

Es la antena instalada en el nodo la cual permite la comunicación hacia una o varias antenas remotas (enlace punto a punto o punto – multipunto respectivamente). Así también, éste equipo opera hasta la capa 3 del modelo OSI, es decir, cuenta con la funcionalidad de procesar información en paquetes IP.

CRON

En el sistema operativo UNIX, CRON es un administrador regular de procesos en segundo plano (demonio) el cual ejecuta programas a intervalos regulares (por ejemplo, cada minuto, día, semana o mes). Los procesos que deben ejecutarse y la hora en la que deben hacerlo se especifican en el archivo CRONTAB.

DSLAM (DIGITAL SUBSCRIBER LINE ACCESSS MULTIPLEXER)

Es un multiplexor localizado en la central telefónica la cual proporciona a los abonados de la red de telefonía básica acceso a los servicios DSL utilizando el mismo cable de par trenzado de cobre. Así también, algunos DSLAM cuentan con tarjetas divisoras (SPLITTER) que separan el tráfico de voz y de datos, enviando el tráfico de voz a la central de conmutación.

ETHERNET

Es el nombre de una tecnología de redes de computadoras de área local (LAN) basada en tramas de datos. ETHERNET define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI. ETHERNET se encuentra estandarizado bajo el IEEE 802.3.

ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

Sirve para envíar anuncios de errores en la transmisión de paquetes de datos. Esta definido en el STD 5, RFC 792.

IP (INTERNET PROTOCOL)

Es un protocolo, no orientado a conexión, usado para la comunicación de datos a través de una red de paquetes conmutados.

ISP (INTERNET SERVICE PROVIDER)

Hace referencia a aquellas empresas proveedores de servicios de comunicaciones hacia Internet.

MIB (MANAGEMENT INFORMATION BASE)

Es un esquema o un modelo que contiene la orden jerárquica de todos los objetos manejados. Cada objeto manejado en un MIB tiene un identificador único. El identificador incluye el tipo (tal como contador, secuencia o dirección), el nivel de acceso (tal como lectura ó escritura), restricciones del tamaño, y la información de la gama del objeto.

MODELO OSI (OPEN SYSTEM INTERCONNECTION)

Es un modelo de red descriptivo creado por la ISO (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION). Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

MPLS (MULTI PROTOCOL LABEL SWITCHING)

Es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

MRTG (MULTI ROUTER TRAFFIC GRAPHER)

Es una herramienta para supervisar la carga de tráfico en los enlaces de red, y otras variables. Genera páginas HTML que contienen imágenes gráficas que proporcionan una representación visual en línea de este tráfico y se basa en PERL y C y funciona bajo UNIX y Windows NT.

NOC (NETWORK OPERATION CENTER)

Es el punto central de un ISP en donde se monitorean los servicios ofrecidos a sus clientes, así como, a las redes que el ISP ha desplegado.

NTP (NETWORK TIME PROTOCOL)

Es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través de ruteo de paquetes en redes con latencia variable. NTP utiliza el puerto UDP 123 como su capa de transporte. Esta diseñado para resistir los efectos de la latencia variable.

OID (OBJETCT IDENTIFIER)

Es un identificador usado para nombrar a un objeto. Estructuralmente, un OID consta de un nodo en una jerarquía establecida. El OID se encuentra conformada por una secuencia de números enteros no negativos separados por un punto los cuales forman un árbol. (RFC 1340)

RRDTOOL (ROUND ROBIN DATABASE TOOL)

Se trata de una herramienta que menaja una serie datos recolectadas en el tiempo. Estos datos son almacenados en una base de datos la cual utiliza la técnica ROUND-ROBIN (almacenamiento circular).

SDA (SUSCRIBER DATA ADAPTER)

Es el equipo de comunicaciones instalado en el local del cliente que sirve de interfaz entre la antena SPR y el router instalado en el local cliente. Este equipo opera en la capa 1 del modelo OSI. Así también, este equipo se encarga de suministrar energía al equipo SPR.

SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

Es un protocolo de la capa de aplicación el cual facilita el intercambio de información de administración entre dispositivos de red. SNMP es parte de la suite de protocolos TCP/IP y permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.

SPR (SUSCRIBER PREMISES RADIO)

Es la antena instalada en el local del cliente del ISP y que junto con el BSR establecen un enlace inalámbrico. Al igual que el equipo BSR, el SPR opera también hasta la capa 3 del modelo OSI.

TCP (TRANSMISSION CONTROL PROCOTOL)

TCP garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. Además proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma estación, a través del concepto de puerto.

TDM (TIME DIVISION MULTIPLEXING)

La multiplexación por división de tiempo es la más utilizada en la actualidad, especialmente en los sistemas de transmisión digitales. En ella, el ancho de banda total del medio de transmisión es asignado a cada canal durante una fracción del tiempo total (intervalo de tiempo).

UDP (USER DATAGRAM PROTOCOL)

Es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, debido a que estos incorporan suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco sabemos si ha llegado correctamente, ya que no hay confirmación de entrega o de recepción.

VLAN (VIRTUAL LAN)

Una VLAN consiste en una red de computadores que se comportan como si estuviesen conectados al mismo cable, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLAN's mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLAN's surge cuando se traslada físicamente una computadora a otra ubicación: puede permanecer en la misma VLAN sin necesidad de ninguna configuración adicional en el hardware.

VPN (VIRTUAL PRIVATE NETWORK)

Es una tecnología de red que permite una extensión de la red local sobre una red pública, como por ejemplo la red IP MPLS de un ISP.

WIPLL (WIRELESS IP LOCAL LOOP)

Es un sistema de acceso inalámbrico punto multipunto basado sobre IP el cual utiliza la WLL (WIRELESS LOCAL LOOP) como tecnología de acceso en la última milla.

BIBLIOGRAFÍA

[1] Telefónica, "Las Telecomunicaciones de Nueva Generación", Telefónica I+D España, 2002

[2] Francisco Argüello Pedreira, "Redes de Computadores", Departamento de Electrónica y Computación - Universidad de Santiago (España), 2001

[3] IBM, "TCP/IP Tutorial and Technical Overview", International Technical Support Organization, 1998

[4] Francois Le Faucheur, "MPLS Tutorial", Cisco Systems, 1999

[5] The WipII Team, "WipLL System Description", Airspan, 2002

[6] Networkers 2006, "Introduction to Network Management", Cisco System, 2003

[7] Networkers 2006, "Principles of Fault Management", Cisco System, 2003

[8] J. Schönwälder, "Married with TCL", Computer Science Department - Technical University Braunschweig, 2000