Red de supervisión y gestión de acceso y datos de la Dirección Territorial de ETECSA en Las Tunas

Por MSc. Elio R. Ávila Rodríguez, Especialista C en Telemática, Unidad de Control Grupo de Planta Exterior, División Territorial Las Tunas, ETECSA
elio.avila@etecsa.cu

Introducción

Uno de los procesos de negocio más característicos de una compañía operadora de telecomunicaciones es la gestión de las redes y de los servicios que opera. Generalmente, por razones técnicas, económicas y estratégicas, las redes que soportan los servicios son heterogéneas en los elementos que las constituyen, pero el servicio es único y la percepción del cliente no debe depender ni de espacios geográficos ni de condicionantes tecnológicos. Es por eso que una operadora de telecomunicaciones necesita soluciones de gestión que sean independientes de los elementos de las redes. Estas soluciones también deben ser lo suficientemente flexibles para adaptarse a los procesos de reingeniería, tan necesarios en el sector de servicios, un sector en constante lucha competitiva [1].

La gestión de redes es el conjunto de capacidades que permiten el intercambio y el procesamiento de información de gestión, a fin de ayudar a la administración a realizar sus actividades con eficiencia. Esto les permite una mejor planificación, instalación, organización, operación, mantenimiento y control de las redes y los servicios de telecomunicaciones [1], [3].

La sociedad contemporánea es testigo de una notable actividad en todos los sectores de la vida económica, política y social, entre los cuales la tecnología tiene un papel protagónico. El desarrollo de Internet, el correo electrónico, el intercambio de información en formato digital, entre otros avances en esta rama, han posibilitado

que, por primera vez en la historia, se pueda establecer una comunicación entre muchas personas en el momento elegido: tiempo real, instantáneo o diferido. Actualmente, la transmisión de datos y las tecnologías de redes representan una revolución semejante a la que supuso la invención del motor eléctrico durante la época de la revolución industrial. De ahí la proliferación experimentada en las redes de datos desde los años 1990 hasta la fecha, tanto de LANs como WANs, y el interfuncionamiento entre ellas hace que los aspectos relativos a su control y gestión sean tenidos cada vez más en cuenta [1].

En este contexto, la Empresa de Telecomunicaciones de Cuba, S.A. (ETECSA) tiene un rol decisivo en el desarrollo de las comunicaciones de nuestro país. Dentro de estas, la transmisión de datos muestra sin dudas un trabajo en ascenso en los últimos años, con vistas al mejoramiento de la informatización de la sociedad cubana.

Para lograrlo es necesario contar con una efectiva gestión de la red acceso y datos desplegada por todo el país, que permita a ETECSA no solo la intervención y configuración remota de los nodos que la integran, el dimensionamiento correcto y la optimización de los equipos y recursos de red, sino que garantice además conocer en tiempo real su estado de operación, así como la detección y atención oportuna ante los fallos de infraestructura, disponer de estadísticas confiables para lograr una acción más proactiva ante las situaciones detectadas que puedan ocasionar averías de los equipos o interrupciones del servicio, la posible localización de las fallas y los elementos de hardware involucrados en ellas, que permita definir los recursos necesarios para su solución y, de esta forma, reducir el tiempo empleado en las reparaciones. Todo esto, además de los beneficios internos que reporta a la Empresa de Telecomunicaciones, redunda en la prestación de un servicio con mayor calidad de forma que, hacia el exterior, influye significativamente en la satisfacción de los clientes [3].

En este artículo se abordan las labores realizadas para la implementación de la gestión descentralizada de acceso y datos en la Dirección Territorial de ETECSA en Las Tunas, así como los principales resultados obtenidos en cuanto a provisión, supervisión y diagnóstico de dichas tecnologías.

La gestión de redes

Componentes de la gestión de redes

Existen dos tipos básicos de actuación en la gestión de redes: la monitorización y el control. La monitorización engloba todas las operaciones de obtención de datos acerca del estado de los recursos, cuyo procesamiento posterior va a permitir a los sistemas de gestión utilizar los procesamientos de control, para actuar sobre el comportamiento de la red gestionada; permite modificar parámetros y/o invocar acciones sobre los recursos gestionados [3].

Las políticas o mecanismos de monitorización pueden ser [3]:

Sondeo o *polling*: Acceso periódico del gestor a la información de monitorización o gestión. Tiene como ventaja que los objetos solo deben estar preparados para responder y posee mayor simplicidad.

Informe de eventos o notificaciones: Los recursos, a través de los agentes y por su propia iniciativa, envían notificaciones a los gestores bajo algunas condiciones. Su ventaja es que minimiza el tráfico de gestión por la red.

Métodos mixtos: *Proxies*, sondas, entre otras.

A continuación se relacionan los componentes comprendidos en una infraestructura de gestión de red [3]:

1. La entidad gestora

Garantiza la interacción de los elementos de hardware y software repartidos entre las diferentes partes de la red, de modo que permita reunir, procesar, analizar y presentar la información de los elementos que conforman dicha red.

Interactúa con el operador o administrador de red a través de una interfaz por medio de la cual se realizan las operaciones de control y vigilancia de los recursos bajo su responsabilidad. Es el punto central de control de los dispositivos.

2. El dispositivo gestionado

Contiene uno o más objetos gestionados, por ejemplo, una tarjeta de red, la CPU, la pila de protocolos IP, el ventilador, la tarjeta de abonados, etc. Estos objetos contienen información que puede ser recogida —y también cambiada— por la entidad gestora.

Contiene un agente de gestión, cuya función es comunicarse con la entidad gestora y ejecutar acciones localmente —como leer o escribir un dato—.

3. El protocolo de gestión

Provee las reglas de comunicación entre la entidad gestora y los agentes de gestión. Define aspectos como los tipos de mensajes y operaciones, la seguridad —autenticación, privacidad— y el manejo de secuencias.

En la figura 1 se muestran los componentes que integran la infraestructura de gestión y su interrelación. De forma que los agentes de gestión, localizados en los dispositivos gestionados, se sondean periódicamente por la entidad gestora, para lo cual se utiliza un protocolo de gestión.

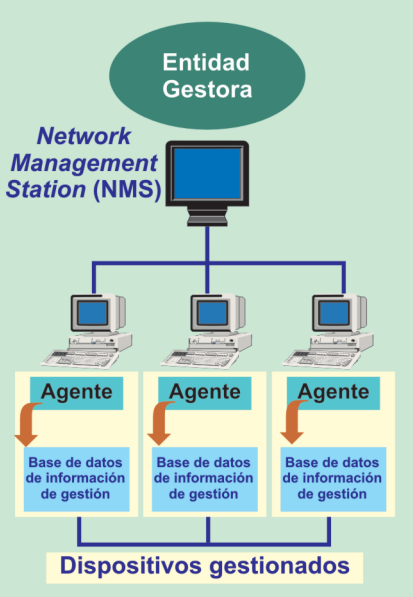


Figura 1 Componentes de la infraestructura de gestión (Fuente: [3]).

Arquitecturas de la gestión de redes

Las arquitecturas de la gestión de redes datan del año 1978, cuando la Organización Internacional de Normas —*International Organization for Standardization* (ISO)— introdujo el Modelo de Interconexión de Sistemas Abiertos —*Open System Interconnection* (OSI)—, siendo este la vía para comprender los fundamentos de la gestión de redes. Los modelos estandarizados desde esos orígenes hasta la fecha son la gestión OSI, la gestión de Internet y la gestión de red —*Telecommunications Management Network* (TMN)— [3], [5].

Gestión OSI

Es la gestión de la torre de protocolos del modelo OSI de la ISO. La figura 2 recoge los elementos de una arquitectura de gestión, según el modelo de referencia OSI, en la que los protocolos inferiores se corresponden con aquellos utilizados en las 3 primeras capas del modelo, es decir, las capas físicas —par trenzado, UTP, coaxial, otros—, de enlace —ATM/FR, Ethernet— y red (IP), que garantizan la conectividad con cada dispositivo gestionado. Sobre estos, a su vez, se soportan los protocolos de gestión definidos, de esta forma se establece la infraestructura de comunicaciones [3], [5]. Una plataforma de gestión de red es un conjunto de herramientas de gestión para desarrollar y suministrar aplicaciones que cumplan con los requisitos que se impongan a la misma [1]. Las aplicaciones pueden ser independientes, donde cada una gestiona por su parte los recursos, o integradas en plataformas para gestionarlos en su conjunto. Pueden incluir diversas posibilidades, por ejemplo, detectar los equipos y la topología de la red, realizar sondeos a los agentes de cada recurso, programar acciones a llevar a cabo ante alarmas, etc. Las plataformas de gestión de redes proporcionan el soporte común para las aplicaciones de gestión y herramientas asociadas. Para ello se pueden apoyar en protocolos de gestión e interfaces normalizadas. Su elección para una red no sólo debe considerar qué es lo que se ofrece, sino con qué calidad se puede implementar. Los aspectos a evaluar para cada plataforma incluyen [1], [5]:

- Aplicaciones genéricas —propias de la plataforma—
- Interfaz de usuario
- Sistemas operativos y protocolos de gestión soportados
- Dependencia de fabricantes de equipos
- Seguridad
- Soporte para Web
- Herramientas para desarrollar aplicaciones de gestión
- Costo

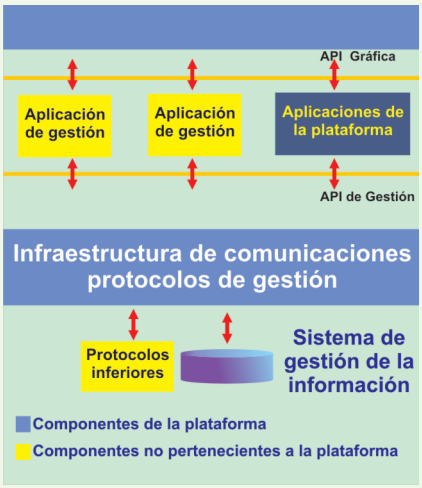


Figura 2 Elementos de una arquitectura de gestión (Fuente: [3]).

Por otra parte, se debe conocer cómo se organiza la red, cuáles son los planes de su crecimiento futuro y, sobre todo, los dispositivos que la conforman y qué es lo que se quiere gestionar.

Las plataformas de mayores prestaciones y, por lo tanto, de mayor impacto en el marco de la gestión de redes son de distribución comercial. En el mercado existe un gran número de aplicaciones de gestión con elevadas prestaciones que satisfacen la información de gestión requerida por los usuarios del sistema. Entre las principales ventajas de las plataformas de gestión mostradas en la figura 2 se encuentran:

- Hacen más simple el desarrollo de aplicaciones específicas

de gestión, pues estas sólo deben conocer la interfaz de programación de aplicaciones de la plataforma —*Interface Programming Application* (API)— sin preocuparse de la implementación de los protocolos de gestión ni de los niveles inferiores, de la gestión de los datos, etc.

- Permiten a los administradores del sistema configurar "a su medida" las herramientas de supervisión y gestión con las que van a trabajar.
- Posibilitan la integración de aplicaciones de gestión específicas, y de diferentes fabricantes, en una única aplicación global de gestión.

Gestión de Internet

Se refiere a la gestión de equipos en las redes TCP/IP. A mediados de los años ochenta del pasado siglo, el Grupo Especial de Ingeniería de Internet —*Internet Engineering Task Force* (IETF)— desarrolló el protocolo simple de gestión de red —*Simple Network Management Protocol* (SNMP)— para proporcionar una gestión de redes normalizada, extensible y, sobre todo, sencilla. SNMP se convirtió en 1990 en la norma dominante para la gestión de redes basadas en la arquitectura TCP/IP, que comprende el gestor de la red —*Network Management Station*— y el agente. Entre sus principales características se encuentran [1], [4-5]:

- Es un protocolo de capa 7 —de aplicación— del modelo OSI que asegura la transmisión de información de gestión entre dos nodos cualesquiera de la red, que permite a los administradores la búsqueda de información con el propósito de modificar, localizar fallas, planear capacidades y generar reportes.
- Está soportado sobre el protocolo UDP —*User Datagram Protocol*— en la capa 4 —de transporte— del modelo OSI.
- Generalmente es utilizado en modo pregunta - respuesta, ya sea para leer (get) o escribir un dato (set). También puede enviar mensajes —no solicitados— a la entidad gestora para notificar acerca de algún estado anormal, conocidos como *traps,* por ejemplo, cuando:
  - —se interrumpe una interfaz
  - —La utilización de la CPU sobrepasa el 85 %
- Utiliza los puertos 161 para el modo pregunta - respuesta y el 162 para el envío de los *traps*
- Tiene tres versiones disponible —V1, V2 y V3—

En la figura 3 se muestra la estructura SNMP. En este caso, el gestor es la estación de trabajo que ejecuta el software o aplicación cliente de gestión. Este se encarga de enviar varios paquetes de solicitud a los dispositivos de red gestionados, de recibir las respuestas y los *traps*, así como de visualizar la información relacionada con el estado de dichos dispositivos a través de su interfaz de usuario. El agente es un proceso que corre en los dispositivos gestionados, recibe y procesa los paquetes de solicitud enviados por el gestor, respondiéndole con el valor de la variable de gestión correspondiente. Cada vez que el agente detecta la ocurrencia de un evento de emergencia en el dispositivo gestionado, envía *traps* para notificar al gestor.

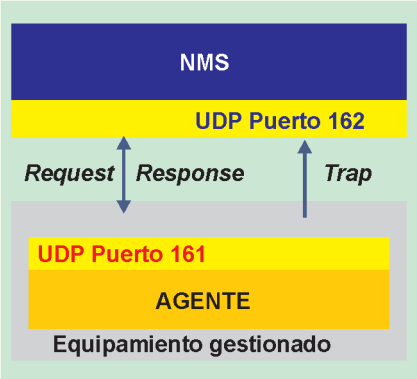


Figura 3 Estructura SNMP (Fuente: elaboración propia).

Red de gestión de telecomunicaciones (TMN)

La gestión de las redes de telecomunicaciones define una estructura de red de gestión basada en modelos de niveles inferiores OSI/ISO, por lo que se considera un modelo genérico para gestionar y administrar redes de telecomunicaciones que comprende un conjunto de especificaciones o recomendaciones para estándares relacionados. El concepto de TMN fue formalmente definido por primera vez en 1988 por la UIT. En el período 1989-1992, la UIT completó el conjunto inicial de especificaciones. Por extensión, también se les denomina TMN a las redes que las cumplen, o sea, una red que posee arquitectura, interfaces y protocolos estandarizados.

TMN permite, mediante el uso de aplicaciones de gestión y una red de datos, la supervisión y el control de una red de telecomunicaciones y de los servicios que sobre ella se ofrecen [5]. Realiza, además, la labor de anfitrión de las funciones de gestión de comunicaciones para la administración operativa y el mantenimiento de las redes y de sus servicios en los entornos donde se trabaja con productos de distintos fabricantes. Su objetivo es conseguir la efectiva interoperatividad de las aplicaciones de gestión de redes y servicios con los equipos de telecomunicaciones, por lo que se enfatiza en el uso de las interfaces normalizadas, a través de las cuales fluye la información de gestión entre los elementos de la red —incluye el operador— y posibilita la operación flexible y eficiente de las redes [5].

La implementación completa de TMN permite realizar una gestión integrada y utiliza una arquitectura organizativa lógica en niveles que se muestran en la figura 4, a cada uno de los cuales se asignan conjuntos de tareas de gestión. Se dice que los niveles son lógicos porque no están necesariamente correlacionados con la implementación física final de los sistemas. Las principales funciones de cada nivel de gestión son la gestión de negocios, la gestión de servicios, la gestión de red y la gestión de los elementos de red [5].

Dentro del modelo TDM existen dos formas de gestión [4]:

1. **Red de gestión en banda —*in-band* o *mainstream*—:** usa los mismos medios de transmisión de la red gestionada, es decir, utiliza recursos del enlace ascendente o *uplink*.

2. **Red de gestión fuera de banda —*outband* o *sidestream*—:** no usa los mismos medios de transmisión de la red gestionada por lo que utiliza recursos independientes exclusivos para la gestión.

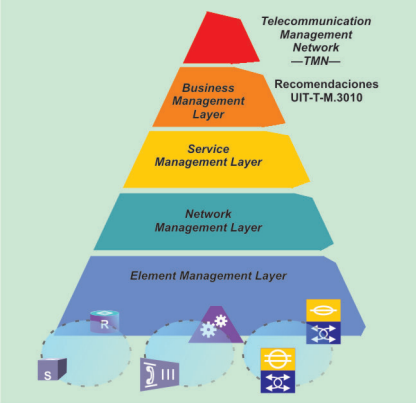


Figura 4 Capas del modelo TMN (Fuente: elaboración propia).

Áreas funcionales de la gestión de red

La gestión de redes se ha estructurado en cinco áreas funcionales, las cuales proporcionan el marco que permite determinar las aplicaciones de dicha gestión, de modo que sea posible satisfacer las necesidades de cada empresa de telecomunicaciones. A continuación se detalla cada una de estas áreas [1], [3], [5]:

Gestión de fallas: Comprende la detección, recuperación y documentación de anomalías y fallas de redes.

Gestión de configuración: Se ocupa de guardar y mantener la configuración de la red, actualizar los parámetros de configuración para asegurar la operación eficaz de la misma.

Gestión de contabilidad: Consiste en actividades de recolección de información de contabilidad y su procesamiento para propósitos de cobro y facturación. Estas actividades establecen un límite contable para que un conjunto de costos se combine con recursos múltiples y se utilice en un contexto de servicio.

Gestión de desempeño: Garantiza un desempeño confiable y de alta calidad a la red. Esto incluye calidad de servicio, con regulación de parámetros como el rendimiento, la utilización de recursos, la demora, los niveles de congestión y la pérdida de paquetes.

Administración de seguridad: Proporciona protección contra los ataques piratas a los recursos de la red, sus servicios y datos. Además, asegura la privacidad del usuario y controla sus derechos de acceso.

Infraestructura de comunicaciones

Desde mediados del año 2009, ETECSA trabaja en el mejoramiento de la gestión de su red de acceso y datos, desplegada en todo el país, a partir de desarrollar un proceso de descentralización gradual hacia los Centros de Gestión Territoriales de la supervisión y gestión de las tecnologías que las integran y, con ello, lograr que las principales tareas relacionadas con las áreas funcionales antes vistas se puedan realizar de manera eficiente a nivel territorial, comenzando en una primera etapa con la provisión, supervisión y el diagnóstico de dichas tecnologías. Seguidamente se exponen algunas consideraciones derivadas de los trabajos desarrollados en la Dirección Territorial de ETECSA en Las Tunas para lograr su implementación.

Ante la heterogeneidad del equipamiento de acceso y datos desplegado en el país y de la diferente ubicación física de los Centros de Gestión Territoriales, fue necesario estudiar e implementar soluciones diversas por cada provincia. Entre las premisas definidas para la descentralización de la gestión se consideró la creación de dos VPN —*Virtual Private Network*— soportadas sobre el robusto *backbone* IP/MPLS, una VPN de elementos de red territorial y otra de gestión, donde se tuvieron en cuenta las siguientes ventajas propias del servicio VPN/MPLS:

Flexibilidad: Posibilidad de cambiar con sencillez el plan de conectividad entre las sedes.

Escalabilidad: Posibilidad de adicionar/eliminar con sencillez la conectividad hacia una sede nueva/existente.

Optimización de la banda: El ancho de banda del acceso se utiliza óptimamente, pues no se subdivide asignando una cuota a cada circuito virtual permanente —*Permanent Virtual Circuit* (PVC)—, sino que está disponible enteramente para cualquier tipo de tráfico.

Seguridad: Segregación del tráfico en paquetes MPLS —*Multiprotocol Label Switching*— y utilización de direcciones privadas.

Invariabilidad del acceso y del equipo de cliente (CE): La VPN/MPLS utiliza el mismo acceso y el mismo CE de la VPN tradicional.

El uso de la VPN de elementos de red territorial, que es la encargada de garantizar la conectividad de todos los equipos o elementos de red que necesitan ser gestionados por cada provincia, introduce también las siguientes ventajas [6]:

- Independiza a la provincia de fallas en la conectividad entre ella y el *router* principal que pueda afectar la supervisión provincial sobre cada uno de los elementos.
- Traspasa a los territorios las fallas que ocurran en los enlaces entre la VPN y cada uno de los elementos. Además, se pueden seccionar con facilidad las fallas sobre la red de gestión.
- El Grupo de Diagnóstico y Control Nacional sólo velará, desde el punto de vista de conectividad, por el estado del enlace entre el *router* principal y cada una de las VPN provinciales.
- Se reduce la cantidad de enlaces sobre el *router* de gestión principal, pues solo se requiere de un enlace por provincia para acceder a todos los elementos a gestionarse en el país.

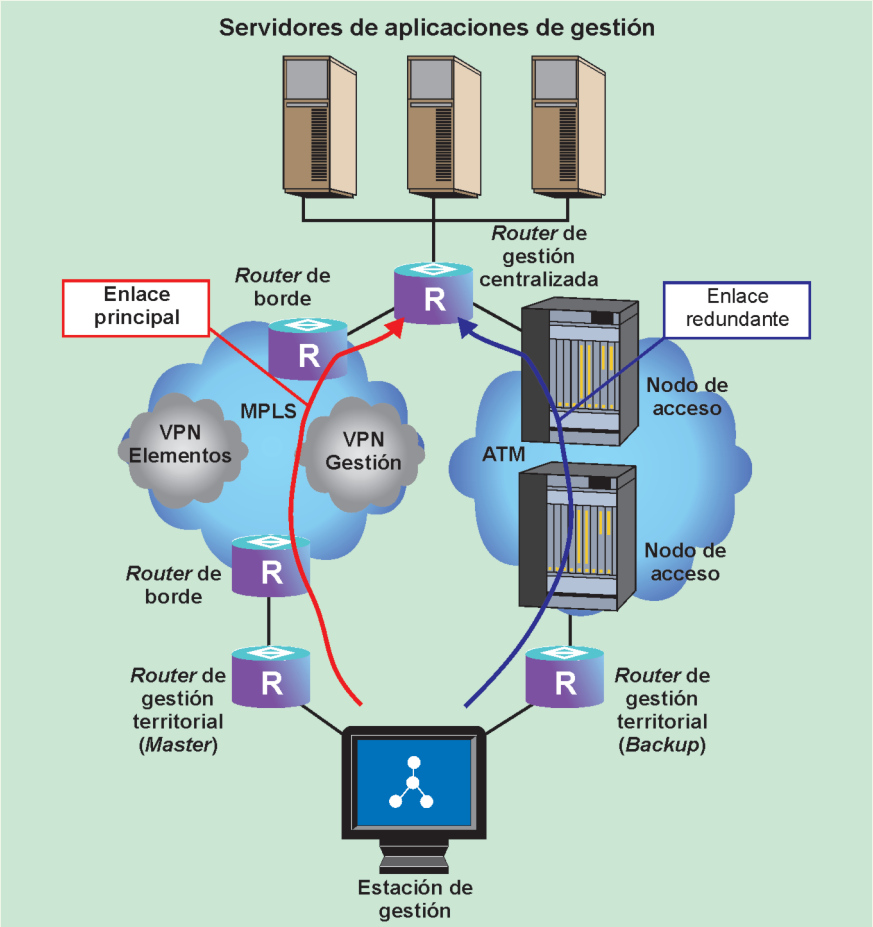


Figura 5 Esquema resumido de la infraestructura de comunicaciones de la red de supervisión y gestión implementada (Fuente: elaboración propia).

La VPN de gestión, a la que tienen acceso las diferentes redes de gestión provinciales, y no los elementos a gestionar, tiene entre sus ventajas que [6]:

- Logra una segmentación entre los elementos de red y las redes de gestión de cada provincia, lo cual permite tener un control más preciso de las direcciones IP.
- Se prepara la red para futuras descentralizaciones o remotizaciones de gestión sobre otras redes de acceso, como pueden ser las redes de acceso DSLAM IP, DSLAM ATM, Metro Ethernet, etc.
- Se incrementa la seguridad de la red pues, además del uso de los usuarios y contraseñas, se pueden definir políticas en el *router* principal o *firewall* que precisen a nivel IP qué usuario puede acceder o no a la red de gestión, a los servidores y a los elementos de red.

Para garantizar en la DT Las Tunas la conectividad con el *backbone* IP/MPLS, específicamente al *router* de borde —*Provider Equipment* (PE)— provincial, se escogió un *router* con dos interfaces LAN. Una de ellas se conectó directamente a una de las interfaces Ethernet del *router* PE, y la otra se destinó para la conexión de la red interna de gestión provincial (Figura 5). Esto permite, en primer lugar, eliminar la conexión directa al PE de las PC de gestión ubicadas en los locales de gestión y supervisión y, de esta forma, evitar que al apagarlas surjan alarmas en el PE al detectar la desconexión física de la interface; por otra parte, permite separar el tráfico de *broadcast* entre la LAN de gestión y el PE, lo que evita posibles colisiones haciéndolo más eficiente.

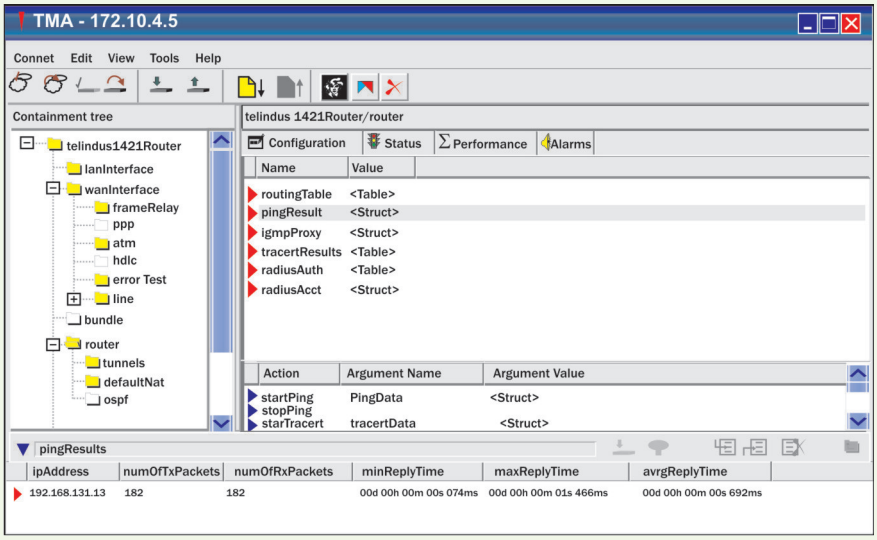
La conexión entre el nodo de transmisión de datos y los locales de gestión y supervisión se logró por medio de VLAN configuradas a través de los conmutadores LAN —*LAN Switch*— de la red corporativa, que cuenta con conexión por fibra óptica entre ellos. De esta forma, se reduce la vulnerabilidad de daño de la interfaz Ethernet en el PE ante la posible inducción por descargas eléctricas, en caso de haber utilizado conexión a través de cable UTP. Esta ventaja permitió la creación de posiciones exclusivas para la red de gestión de acceso y datos en los locales de gestión y supervisión, independizándola así de otras redes.

Para garantizar la conectividad de los elementos de red gestionados a la VPN prevista, se configuraron en banda los PVC de cada uno de ellos, de forma que ha sido posible incorporar a la supervisión y gestión territorial la totalidad de los nodos bajo nuestra responsabilidad. Para esto se utilizó un esquema de direccionamiento IP definido centralizadamente y que prevé el futuro crecimiento de la red de acceso y datos.

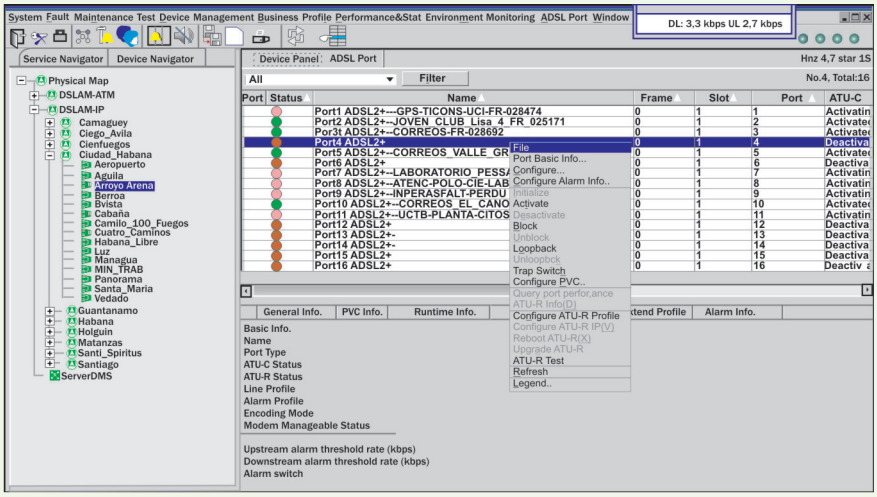
Dada la importancia de mantener una red de gestión con alta disponibilidad, se considera oportuna la implementación de enlace redundante que comprende diferente *backbone*, soporte de transmisión, equipos de acceso y ubicación (Figura 5), debido a que utiliza las funcionalidades del Protocolo de Redundancia de *Router* Virtual —*Virtual Router Redundancy Protocol* (VRRP)—. De este modo, al configurar convenientemente los *routers* que actuan como máster —el conectado a IP/MPLS— y respaldo —el conectado a ATM/FR—, así como las interfaces que pueden comprometer la vitalidad del enlace, se garantiza que ante una falla de conectividad por IP/MPLS exista un enlace redundante a través de ATM/FR, que asuma automáticamente la conectividad de los puestos de gestión contra el *router* de gestión central.

Gestión de configuración

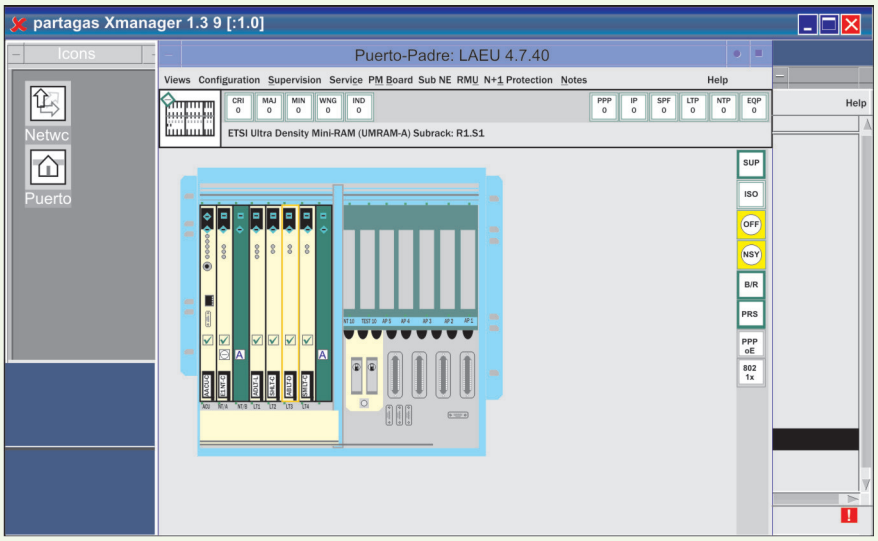
Esta gestión garantiza la intervención y configuración de forma remota de todos los elementos de red gestionados, desde el puesto habilitado para este propósito en el local de Diagnóstico de Control del Centro de Gestión Territorial. Para ello se utilizan los softwares de gestión propietarios de los fabricantes del equipamiento instalado y en servicio. En la figura 6 se muestran ejemplos de su uso.



◀ a) TMA de Telindus/OneAccess



◀ b) N2000 de Huawei



◀ c) AWS de Alcatel

Figura 6 Herramientas de gestión propietarias (Fuente: elaboración propia).

Gestión de fallos

Para garantizar la detección de los fallos de los elementos de red y el desencadenamiento posterior de las acciones para su solución, se instaló en una posición destinada para este fin en el local de supervisión el software *WhatsUp Gold* como plataforma de gestión. Entre sus prestaciones se encuentran que permite conformar un mapa de la red que se desea supervisar para su monitoreo y notificación de fallos, lo que ayuda a conocer su estado y operación y, así, aumentar la disponibilidad del servicio brindado. Permite, además, obtener retroalimentación sobre el desempeño de la red en cuestión. *WhatsUp Gold* se configuró insertando un mapa de la provincia. En él se ubicaron convenientemente los elementos a supervisar (Figura 7), a cada uno de ellos se le configuró la dirección IP que los identifica dentro de la red implementada. El programa hace un sondeo periódico de los mismos a través del uso del protocolo ICMP —*Internet Control Message Protocol*—. En caso de perder la conectividad con alguno de ellos, automáticamente emite alarmas sonoras y visuales que indican el fallo que existe.
De esta forma se monitorizan, en tiempo real y durante las 24 horas, todos los equipos de acceso de datos instalados en la provincia por el personal permanente responsabilizado con estas funciones.

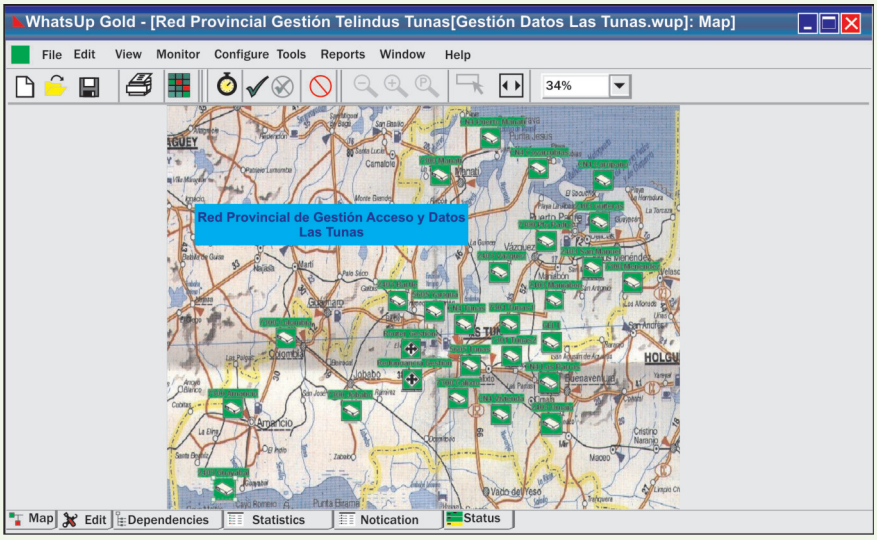


Figura 7 Vista del sistema supervisor implementado con *WhatsUp Gold* (Fuente: elaboración propia).

Gestión de desempeño

Otra plataforma de gestión implementada es el PRTG —*Paessler Router Traffic Grapher*—, la cual emplea el protocolo de gestión SNMP. Esta plataforma se utiliza principalmente para garantizar las estadísticas del tráfico cursado y la recepción de los *traps* de los dispositivos gestionados. Entre sus prestaciones se encuentran la visualización de forma gráfica del ancho de banda cursado en las interfaces accesibles y el registro de los eventos de fallas. Es una herramienta muy útil porque permite conocer el tráfico generado por cada cliente, así como el total del *uplink* del equipo de acceso gestionado, lo que complementa la información y las estadísticas que brindan *WhatsUp Gold* y las herramientas propietarias de los fabricantes de los equipos, entre las cuales se encuentran la disponibilidad del servicio, las alarmas registradas, la hora y el período de ocurrencia, entre otras. En la figura 8 se muestra la imagen de ejemplo de los gráficos que ofrece el PRTG.

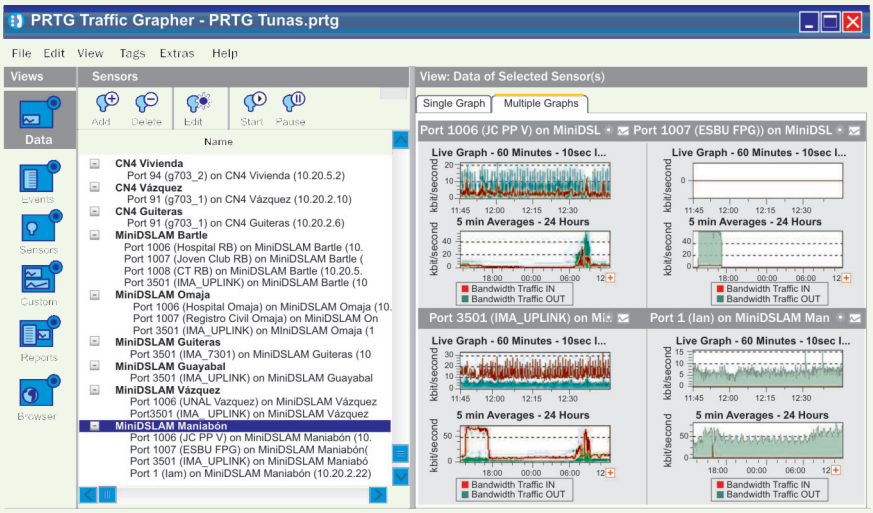


Figura 8 Muestra de las estadísticas de tráfico con el PRTG (Fuente: elaboración propia).

Conclusiones

Las soluciones de conectividad aportadas por la Dirección Territorial de ETECSA en Las Tunas garantizaron una infraestructura de comunicaciones efectiva, acorde con los requerimientos necesarios para responder de forma positiva al proceso de descentralización de la gestión de acceso y datos que tiene lugar en ETECSA. De esta forma, su personal técnico pudo asumir las actividades de intervención y operación sobre las plataformas de gestión propietarias de los fabricantes del equipamiento instalado, que con anterioridad se realizaban de manera centralizada en La Habana o no eran posibles de forma remota. Los trabajos incluyeron, además, la implementación de la supervisión en tiempo real y durante las 24 horas del día de la totalidad de los dispositivos de acceso y datos de la provincia, aspecto que no se había logrado con anterioridad. Las plataformas de gestión incorporadas garantizan una información de gestión y estadísticas confiables que permiten, tanto al personal técnico como a la administración, tener un conocimiento más amplio del estado de la operación y el funcionamiento del equipamiento instalado, así como realizar un mayor diagnóstico y control sobre este.

Todos los resultados han posibilitado la obtención de importantes beneficios:

- Una provisión más rápida de los servicios.
- La reducción de los tiempos relacionados con los fallos de infraestructuras, averías e interrupciones del servicio.
- La reducción de los tiempos de instalación y de las pruebas de aceptación de nuevos equipos incorporados a la red y, con ello, de la puesta en explotación de los mismos.
- El dimensionamiento eficiente de los recursos de la red de transporte que interconectan los equipos.
- La identificación oportuna de fallos de operación de los equipos, que requieren la corrección por los fabricantes y la contribución a su solución.
- El aumento de la capacitación sobre transmisión de datos en los territorios.

Referencias bibliográficas

[1] Torres, N. V. "Herramientas para la Gestión de Equipos de la Red de Transmisión de Datos de ETECSA". Tesis de Maestría, Universidad Central de Las Villas "Marta Abreu", julio, 2004.

[2] Cisco System. *Internetworking Technology Handbook. http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook* (acceso: septiembre 28, 2010).

[3] Anías, C. "Introducción a la Gestión de Redes". Conferencia en el ISPJAE, La Habana, Cuba, 2002.

[4] Anías, C. "Funcionalidad de los Sistemas de Gestión de Redes". Conferencia en el ISPJAE, La Habana, Cuba, 2002.

[5] Collado, H. "Gestión de redes celulares en Cuba". Trabajo de Diploma, ISPJAE, julio, 2006.

[6] Pinillos, R. "Premisas para la descentralización de la gestión". Documento interno de trabajo, Departamento de Desarrollo e Inversiones Datos, Vicepresidencia de Desarrollo y Tecnología, ETECSA, La Habana, 2009.