Maestría en Matemática Aplicada
e Informática para la Administración

Procedimiento para el diagnóstico de la red informática de la Universidad de Holguín

Autor: Yandi Fernández Ochoa

Tutor: Dr. C. Rodolfo García Bermúdez

Holguín, Cuba

2013

Resumen

La presente investigación se enfoca en determinar las principales insuficiencias existentes en la red de computadoras de la Universidad de Holguín que repercuten en continuas insatisfacciones de los usuarios, relacionadas con la inestabilidad y lentitud de los servicios.

Para diagnosticar la red se propone la modificación de una metodología diseñada por una empresa dedicada a ofertar servicios de instalación y soporte a redes de datos con la finalidad de crear un procedimiento adecuado a la red estudiada, que tenga en cuenta sus particularidades y abarque todas las etapas que permitan realizar un estudio general o diagnosticar un servicio en específico.

El presente trabajo se propone como objetivo diagnosticar el funcionamiento de los componentes que intervienen en la prestación de servicios, mediante la aplicación de un procedimiento que permita determinar el origen de las deficiencias que repercuten en el funcionamiento de la red.

Para ello se parte de un estudio de metodologías y herramientas para el análisis y diagnóstico de redes informáticas, se presenta un procedimiento con tal fin y se realizan modificaciones para adecuarlo a las características de la red de la Universidad de Holguín. Por último, se aplica el procedimiento propuesto a la red estudiada. Como parte del mismo se incluyen propuestas de optimización con la finalidad de disminuir las insatisfacciones de los usuarios.

Índice general

Índice de tablas

Índice de figuras

Introducción

El proceso de gestión de la información es, en la actualidad, una de las prioridades en cualquier organización, pues de la correcta manipulación y empleo de la misma depende, en gran medida, su adecuado funcionamiento. Diversos son los métodos y herramientas desarrollados por el hombre que permiten el tratamiento de la información. Quizás la más importante entre ellas sea la computadora, que con la evolución de las tecnologías ha sido dotada de la capacidad de comunicarse con otros dispositivos similares, dando lugar al surgimiento de las redes de computadoras [38].

Las redes de computadoras pueden prestar un gran número de servicios, tanto para organizaciones como para individuos, y manejar gran variedad de recursos de información. Su empleo ha facilitado la organización del trabajo en las empresas o instituciones y una mejor atención al cliente o usuario final. Algunas de las características más importantes que se utilizan para describir o caracterizar una red son: velocidad de transmisión, seguridad, disponibilidad, escalabilidad y confiabilidad; elementos que deben tomarse en consideración para el correcto funcionamiento de la misma en correspondencia con los resultados esperados [22].

Los conocidos beneficios de las redes de comunicación han motivado la utilización al máximo de las tecnologías de la información con que cuentan las organizaciones, lo cual ha provocado, en muchos casos, un crecimiento acelerado de la red con una consiguiente generación de sobrecarga en la infraestructura, tanto de hardware como de software. Servidores con disminución en su rendimiento, frecuente desconexión de estaciones de trabajo e interrupciones en los canales de comunicación son problemas a los que se enfrentan las organizaciones. Sin embargo, en muchas ocasiones la situación más crítica se da a partir del desconocimiento del origen de los problemas y de las herramientas para su diagnóstico [5].

Las organizaciones de enseñanza, y dentro de ellas las universidades como máximos exponentes de las instituciones educativas de un país, tienen el deber de garantizar al claustro de profesores y al estudiantado acceso a información, recursos y servicios que potencien su formación científica y profesional. Por lo tanto, es imposible pensar en una institución de la educación superior que no posea una red de computadoras para la socialización interna de la información y con alcance que permita su impacto en el exterior de la misma.

La red de computadoras de la Universidad de Holguín “Oscar Lucero Moya” (Red UHOLM, en lo adelante) presta servicios a estudiantes y trabajadores de la institución. Entre los más necesarios y demandados se pueden citar el correo electrónico, la navegación en internet y la transferencia de ficheros. El rendimiento de la misma ha sido inestable debido a una serie de problemas, en algunos casos determinados por limitaciones tecnológicas debidas a la falta de financiamiento, o por problemas de configuración de dispositivos y servicios.

El crecimiento de la plantilla de trabajadores, de la matrícula de estudiantes y más recientemente la ubicación de algunas facultades en una nueva sede (campus Celia Sánchez Manduley), trajeron consigo cambios en la distribución de servidores, estaciones de trabajo y dispositivos de interconexión. Unido a esto, la remodelación de locales se ha realizado sin considerar el impacto que podría tener en una posible expansión de la red, lo que ha dificultado la escalabilidad de la misma una vez que estos locales han sido dotados de equipamiento informático.

Por otro lado, el tendido de los cables no ha sido uniforme. En la mayoría de los locales se ha instalado mediante el empleo de canaletas, sin embargo en otros, principalmente en exteriores, se encuentran ubicados a la intemperie y sin ninguna norma de seguridad. Se ha mejorado la tecnología en algunos servidores, dispositivos de interconexión y en los servicios, lo que no ha estado en correspondencia con la evolución de los elementos asociados a estos.

Es común que los administradores y la Dirección de Informatización detecten

problemas en la red y procedan a solucionarlos, teniendo en cuenta que son situaciones que se reiteran y cuentan con las herramientas o técnicas que proveen soluciones efectivas. En otros casos es muy difícil o imposible determinar la causa de los mismos, lo cual ha demorado soluciones óptimas o ha generado nuevas situaciones de riesgo para la red.

El nodo central de la Universidad de Holguín mantiene en explotación un conjunto de herramientas para monitorizar el comportamiento de la red informática, controlar los servicios que presta y estudiar sus registros. Aunque la elección de dichas herramientas no ha sido desacertada, el uso de éstas no se corresponde con el nivel de explotación de la red. La más empleada y la que más beneficios aporta es Nagios, considerando que es una herramienta de monitorización en tiempo real e informa a los administradores acerca de las incidencias en el momento en que se desarrollan. Sin embargo, el resto se mantiene ejecutándose sin un chequeo regular por lo que se ignora información relevante en momentos determinantes.

Aunque estudiantes de la carrera Ingeniería Informática han desarrollado trabajos de diploma con el objetivo de mejorar el rendimiento de la Red UHOLM, las soluciones implementadas no logran un aprovechamiento óptimo de las características de la red, lo cual sugiere que existe un número amplio de factores que no se han considerado o estudios que no se han realizado.

La situación antes descrita, con la influencia de otros factores que la presente investigación se encargará de determinar, ha provocado insatisfacciones a los usuarios de la red, quienes se quejan de inestabilidad, lentitud y baja confiabilidad en los servicios que se prestan.

Por tanto, se identifica como situación problemática: La indeterminación del origen de los problemas que provocan un funcionamiento deficiente de la red y el manejo aislado de herramientas para su monitorización, dificultan la solución de situaciones de riesgo y su optimización por el personal encargado.

Tras un estudio de esta situación se hizo evidente el siguiente problema científico: La Dirección de Informatización de la Universidad de Holguín no dispone de técnicas y herramientas que permitan diagnosticar eficientemente la red informática y desarrollar acciones que favorezcan su optimización.

El problema identificado se encuentra enmarcado en el objeto de estudio: Análisis y diagnóstico de redes informáticas, el cual delimita el campo de acción: Análisis y diagnóstico de redes informáticas en la Universidad de Holguín.

Para dar solución al problema se propuso como objetivo: Diagnosticar la red informática de la Universidad de Holguín, mediante la aplicación de un procedimiento que permita determinar el origen de las deficiencias que repercuten en su funcionamiento y establecer oportunidades de mejoras.

Para guiar la investigación se plantearon las siguientes preguntas científicas:

1. ¿Cuáles posiciones teóricas sustentan el análisis y diagnóstico de redes informáticas?
2. ¿Cuál es el estado real de la red informática de la Universidad de Holguín en vistas a su diagnóstico?
3. ¿Cómo diagnosticar la red informática de la Universidad de Holguín?
4. ¿Cómo medir la calidad del diagnóstico realizado a la red informática de la Universidad de Holguín?

Para el desarrollo de la investigación se ejecutaron las siguientes tareas:

1. Compilación de los fundamentos teóricos del análisis y diagnóstico de redes informáticas.
2. Caracterización de la red informática de la Universidad de Holguín.
3. Definición de un procedimiento para el diagnóstico de la red informática de la Universidad de Holguín.

4. Aplicación del procedimiento propuesto en la red informática de la Universidad de Holguín.
5. Valoración del diagnóstico realizado a la red informática de la Universidad de Holguín.

Se emplearon métodos teóricos, empíricos y estadísticos para la ejecución de las tareas. Dentro de los primeros se usó el Análisis y Síntesis para el análisis del proceso de diagnóstico de redes informáticas, la comprensión de las relaciones esenciales y características generales de este proceso, así como la elaboración de las conclusiones de la investigación; el Histórico-Lógico para el estudio de la evolución del empleo de herramientas en el diagnóstico redes informáticas y como fundamento para el diseño del procedimiento propuesto; así como la Modelación para el diseño de la red estudiada. Como métodos empíricos se utilizaron Entrevistas y encuestas con los especialistas para la recopilación de la información necesaria para el desarrollo de la investigación y el Experimental para la obtención de los datos. Para el procesamiento del cúmulo de datos recopilados se emplearon métodos estadísticos.

En un entorno donde el estudio de las redes y la solución de los problemas asociados a éstas se realizan de forma empírica, la investigación presenta, como novedad, un procedimiento para el análisis y diagnóstico de redes informáticas. La aplicación del procedimiento diseñado a la red de la Universidad de Holguín generó suficiente documentación y propició la elaboración de propuestas de optimización, sobre las cuales se basan los principales aportes del trabajo desarrollado.

El presente informe está estructurado en dos capítulos. El primero incluye los fundamentos teóricos del análisis y diagnóstico de redes informáticas y un estudio de metodologías y herramientas empleadas con tal fin, que permitieron la posterior elección de las más adecuadas para el desarrollo de la investigación, así como una caracterización de la Red UHOLM.

El Capítulo 2 presenta un procedimiento para el diagnóstico de la red informática de la Universidad de Holguín en correspondencia con sus características. Se describen sus etapas, se enuncian los objetivos de cada una de ellas, se numeran los pasos a desarrollar y se aplican al entorno para el que fue diseñado. Se muestran los resultados obtenidos del empleo de las herramientas de monitorización empleadas y el diagnóstico realizado a partir de los parámetros analizados, se manejan propuestas de solución a las deficiencias detectadas y se valora la calidad del procedimiento y la ejecución del diagnóstico.

Además de las conclusiones parciales de cada capítulo, se arriba a conclusiones generales que reflejen los principales resultados obtenidos tras la investigación realizada. Como colofón se ofrecen recomendaciones para dar continuidad y mejorar el trabajo desarrollado. El documento incluye, además, la bibliografía empleada y anexos, como complementos de esta investigación.

Capítulo 1. Fundamentos teóricos del análisis y diagnóstico de redes de computadoras

En el presente capítulo se abordan los aspectos necesarios para la comprensión del objeto y campo de estudios. Se realiza un acercamiento a los conceptos fundamentales de las redes de computadoras, así como un estudio de herramientas para el análisis y monitorización de redes que permita la selección de las más adecuadas para el diagnóstico de la red informática de la Universidad de Holguín.

1.1 Redes de Computadoras

Una red de computadoras consiste en un soporte para la transmisión de señales que contienen datos, compuesto por dispositivos activos de tecnologías de la información y comunicaciones como conmutadores y enrutadores, y dispositivos pasivos como cables y conectores. Por lo general se emplean dos dimensiones para clasificar las redes: la tecnología de transmisión y la escala.

De acuerdo a la primera dimensión, las redes pueden ser de difusión o punto a punto. Como regla general, las redes pequeñas geográficamente localizadas tienden a usar la difusión, mientras que las redes más grandes suelen ser punto a punto.

En cuanto al alcance o escala, generalmente se ubican dentro de uno de los siguientes calificativos:

- Red de área local (LAN, *Local Area Network*)
- Red de área metropolitana (MAN, *Metropolitan Area Network*)
- Red de área amplia (WAN, *Wide Area Network*).

Las redes de área local (LAN) son redes de computadoras limitadas a un área reducida, como edificios de oficinas, fábricas, escuelas, etc. Su empleo permite eliminar la redundancia de datos, de hardware y de software, lo que propicia un ahorro de tiempo y de recursos financieros. Se distinguen de otro tipo de redes por tres características: su tamaño, tecnología de transmisión y topología [38].

Sin embargo, y a pesar de sus innegables beneficios, las redes informáticas en las instituciones se vuelven cada vez más complejas y sus servicios son demandados con mayor frecuencia pues son el soporte de aplicaciones y procesos indispensables para el funcionamiento de las organizaciones. Es por ello que el análisis y monitorización de redes se ha convertido en una tarea indispensable para evitar situaciones que puedan repercutir negativamente en el desempeño del trabajo de las instituciones [22].

1.2 Análisis y diagnóstico de redes

El análisis y diagnóstico de redes es un proceso que debe realizarse de forma continua, de manera especial cuando se intente iniciar un nuevo servicio o se instale nuevo hardware o software, y permite:

- Encontrar deficiencias en la red de datos
- Definir las causas de las deficiencias detectadas
- Establecer oportunidades de mejora
- Formular acciones correctivas y de mejoramiento.

La realización de este procedimiento permitirá determinar si existen deficiencias que ameriten acciones para lograr un mejoramiento, y definirá los plazos para el cumplimiento de las mismas, a lo que se denominará optimización de la red [9].

Es de vital importancia trazar estrategias que permitan aislar, identificar, priorizar y resolver los problemas que puedan presentarse en el funcionamiento de la red

para, una vez diagnosticados, localizar las herramientas necesarias para su erradicación.

Para identificar y corregir problemas en la red será necesario aplicar un enfoque estructurado. Por tanto se establece como primer paso la definición del problema. Es importante no ignorar este paso pues en ocasiones se emplea mucho tiempo en resolver problemas sin haber definido las causas. [10]

El siguiente paso es aislar los problemas, comenzando por eliminar los más obvios hasta llegar a lo más complejos, con la intención de acotarlo en una de las categorías anteriormente descritas. De acuerdo a la bibliografía consultada, los problemas intermitentes son los más difíciles de aislar, porque nunca suelen producirse cuando el operador está presente; es por ello que la única forma de resolverlos es recrear las circunstancias que propiciaron la aparición del error, lo cual demanda bastante tiempo y paciencia.

El paso anterior reduce la búsqueda al acotar el problema en determinadas categorías de las descritas anteriormente. Esto permite realizar una planificación de la reparación basada en el conocimiento actual que se tiene de la situación. Es conveniente crear un plan para aislar los problemas partiendo de las soluciones más sencillas a las más complejas, documentando cada acción y su resultado. Se sugiere seguir el plan tal y como ha sido diseñado, pues la ejecución de sus pasos de forma aleatoria puede generar nuevas situaciones. Si el primer plan no tuviera éxito se debe crear otro, basado en los descubrimientos realizados en el plan anterior. Una vez localizado el problema, se debe proceder a reparar o sustituir el componente defectuoso o, en caso de ser un problema de software, registrar los cambios producidos entre el antes y el después.

Para asegurar que la situación que originó el conflicto ya no existe es necesario confirmar los resultados. En función de ello se pide al usuario que pruebe la solución y se percate de que todo funciona normalmente, pues no sólo debe

comprobarse que se ha solucionado el problema, sino que el trabajo realizado no ha tenido un impacto negativo en la red.

Considerándose que situaciones similares pudieran repetirse es conveniente documentar el problema y la reparación. Guardar una copia del procedimiento realizado puede ser de utilidad para aumentar la experiencia en el trabajo con la red y ayuda a enfrentar problemas muy parecidos [20].

En este proceso es necesario definir algunos componentes como el cableado estructurado, la tecnología empleada o el ancho de banda disponible, pues de su correcta integración dependerá el rendimiento de la red y la obtención de resultados.

1.2.1 Criterios y parámetros para estudiar redes informáticas

Para estudiar una red es necesario definir la calidad del servicio. Aunque en el ámbito de la telemática el término tienes dos interpretaciones diferentes, en esta investigación se hace referencia a un conjunto de cualidades medibles en una red de comunicaciones. Estas medidas están relacionadas, generalmente, con el grado de satisfacción del cliente o su percepción acerca del servicio que emplea.

Normalmente se habla de cuatro perspectivas de medición de la calidad de servicio: calidad ofertada y calidad proporcionada, desde el punto de vista de los administradores de la red; y calidad recibida y calidad percibida, desde la perspectiva del usuario. Técnicamente, las medidas que más información brindan son las de calidad proporcionada, pues se pueden obtener de los datos generados por el equipamiento de los administradores, mientras que medir la calidad percibida se complica debido a la componente subjetiva que tiene y requiere la aplicación de encuestas. Entre las medidas de calidad proporcionada se pueden encontrar cuestiones como la disponibilidad de las redes, los tiempos que demora una comunicación, la velocidad de una conexión a Internet, e incluye otras relacionadas directamente con la atención al cliente como el tiempo de atención.

Ejemplo: Algunos parámetros de calidad de servicio aplicados en Brasil

Parámetro	**Criterio**
Disponibilidad	Mayor o igual a 99% (equivalente a 7.2 horas de interrupción, como máximo cada mes)
Flujo / Velocidad media	Media mayor que 60 % del flujo / velocidad máxima contratada
Flujo / Velocidad instantánea	Valor instantáneo mínimo de 20 % del flujo / velocidad máxima contratada
Pérdida de paquetes	Pérdida máxima del 2 % del volumen de datos enviados
Latencia unidireccional	Valor máximo de 40 milisegundos
Latencia bidireccional (RTT)	Valor máximo de 80 milisegundos
Jitter	Variación máxima de 50 milisegundos
Tiempo para establecimiento de conectividad IP	Tiempo máximo de 1 minuto
Número de intentos para establecer la conectividad IP	Máximo de 2 intentos
DNS – tiempo de respuesta del servidor recursivo	Máximo de 80 milisegundos
DNS – obediencia al campo TTL	El servidor recursivo debe obedecer al campo TTL

El cableado estructurado constituye un factor fundamental para cubrir las necesidades tecnológicas de empresas u organizaciones. Según Panduit Corporation, empresa estadounidense desarrolladora de soluciones de infraestructura física para diversos sectores, el 70% de los problemas en las redes informáticas se producen por colisiones en el sistema, relacionadas con el cableado. Esta situación, que disminuye la productividad de la red, puede evitarse mediante la selección de la tecnología de red adecuada, que permita el empleo eficiente del medio de transmisión y de los dispositivos de interconexión [12], [25].

Muy asociado al cableado estructurado se encuentra la tecnología de red. La mayoría del mercado de las redes emplea tecnología Ethernet, en su variante 100BaseT, la cual utiliza el cable UTP categoría 5 y 5e como medio de transmisión (definido para un ancho de banda de 100 MHz y orientado a soluciones de 10/100 Mbps). Sin embargo, algunas compañías visionarias han optado por la instalación de cableado estructurado categoría 6 (definido para un ancho de banda de 250 MHz y orientado a soluciones de 1000 Mbps), de mayor capacidad y velocidad de transmisión. El UTP categoría 6, aunque implica un 30% adicional en el costo de instalación, incrementa en más de un 50% la velocidad de transmisión en comparación con el UTP categoría 5 [18].

Otro de los elementos esenciales a la hora de realizar el estudio de una red es el ancho de banda. El ancho de banda es finito, cuesta dinero y su demanda aumenta a diario. Sus limitaciones están dadas por el tipo de medio de transmisión empleado, las tecnologías de red y los dispositivos de interconexión [3].

El ancho de banda es la medida de la cantidad de información que puede atravesar la red en un período dado de tiempo. Por lo tanto, la cantidad de ancho de banda disponible es un punto crítico de la especificación de la red. Una LAN típica se podría construir para brindar 100 Mbps a cada estación de trabajo individual, pero esto no significa que cada usuario pueda realmente mover cien megabits de datos a través de la red por cada segundo de uso. Esto sólo podría suceder bajo las circunstancias más ideales [2].

La tasa de transferencia se refiere a la medida real del ancho de banda, en un momento dado del día, usando rutas de Internet específicas, y al transmitirse un conjunto específico de datos. Desafortunadamente, por varios motivos, la tasa de transferencia a menudo es mucho menor que el ancho de banda digital máximo posible del medio utilizado. A continuación se detallan algunos de los factores que determinan la tasa de transferencia:

- Dispositivos de interconexión
- Tipo de datos que se transfieren
- Topología de la red
- Cantidad de usuarios en la red
- Computadora del usuario
- Servidores

El ancho de banda teórico de una red es una consideración importante en el diseño de la red, porque el ancho de banda jamás será mayor que los límites impuestos por los medios y las tecnologías de red escogidos. No obstante, es igual de importante que un diseñador y administrador de redes considere los factores que pueden afectar la tasa de transferencia real. Al medirla regularmente, un administrador de red estará al tanto de los cambios en el rendimiento de la red y los cambios en las necesidades de sus usuarios [38].

En ese sentido es muy importante determinar la velocidad de bajada y la de subida. La primera de ella, también conocida como velocidad de descarga (*download speed*) es la tasa de transferencia desde Internet hacia la computadora del usuario o hacia el servidor proxy. La segunda se refiere a la carga de una conexión a Internet o la velocidad a la que se transfieren datos en la dirección opuesta, de la computadora del usuario o del proxy hacia Internet. Es un hecho que los proveedores aseguren a sus clientes una velocidad de bajada mayor que

la de subida debido a que los usuarios reciben muchos más datos de los que envían.

Otro de los parámetros que influyen en el comportamiento de una red es el Round-Trip Time (RTT), que se refiere básicamente a la latencia bidireccional de la red, o el tiempo que demora una trama en ir desde la computadora cliente al servidor y regresar al cliente. Aquí interviene la distancia física que une origen y destino de los datos y la cantidad de dispositivos ubicados entre ellos, pues no es lo mismo un enlace entre dos ciudades mediante satélite que a través de fibra óptica, o que en determinadas locaciones se encuentren ubicados enrutadores que añaden un tiempo adicional en tareas de recepción, almacenamiento, procesamiento y transmisión de datos. En las redes, principalmente en las WAN e Internet, RTT es uno de los factores que influyen en la latencia, que es el tiempo que transcurre entre la solicitud de los datos y la recepción o visualización de estos por el usuario. El RTT puede fluctuar, en condiciones ideales, desde milésimas de segundos entre puntos cercanos, hasta unos cuantos segundos entre puntos separados por largas distancias.

La pérdida de paquetes es uno de los principales errores presentes en una comunicación de datos y ocurre cuando uno o varios paquetes fallan en su intento de alcanzar el destino. Puede ser ocasionada por degradación de la señal que transmite los datos, congestión en el canal de comunicaciones o hardware dañado. Es proporcional al tráfico de la red y su rango permisible depende del tipo de dato que se envíe. Por ejemplo, en una transmisión de voz o video, una pérdida de paquetes entre 5% y 10% es significante y afecta la calidad del servicio, pero una pérdida de uno o dos paquetes es prácticamente imperceptible; mientras que para otros tipos de archivos, como los ficheros de texto, la pérdida de un solo paquete es relevante. Por regla general, en redes que emplean la pila de protocolos TCP/IP, se tolera una pérdida de paquetes por debajo de 0.1%; cualquier valor por encima de éste tendrá un impacto que estará en dependencia de las circunstancias descritas anteriormente.

1.2.2 Procedimientos para diagnosticar redes informáticas

Un procedimiento es una sucesión cronológica de operaciones concatenadas entre sí, que se constituyen en una unidad de función para la realización de una actividad o tarea específica dentro de un ámbito predeterminado de aplicación. Consiste en seguir ciertos pasos predefinidos para desarrollar una labor de manera eficaz. Aunque es posible que existan diversos procedimientos con un mismo objetivo, cada uno debe poseer estructuras y etapas diferentes y ofrecer mayor o menos eficiencia.

A partir de la búsqueda realizada se pudo determinar que los procedimientos para la detección de problemas en redes informáticas y su solución se limitan a problemas puntuales que se pueden presentar en determinado momento. Por tanto es válido aclarar que en la bibliografía consultada no fue posible encontrar procedimientos que partieran de un estudio y caracterización de la red de una organización y culminaran con propuestas de mejoras, que permitieran una comparación entre ellos y la selección del más adecuado para su aplicación en la Universidad de Holguín.

Para investigar la existencia de procedimientos administrativos o metodologías en organizaciones que emplean redes informáticas en sus procesos principales y no publican en Internet sus resultados por razones de privacidad o acceso limitado a la red de redes, se decidió contactar al personal encargado de la informatización en sus dependencias. Visitas a algunas instituciones del territorio permitieron conocer la manera en que enfrentan el proceso de solución de problemas en las redes informáticas que administran.

En el caso de la red informática del MININT, los administradores afirman que, por cuestiones de seguridad y protección en la información que manejan, emplean herramientas de simulación para estudiar el comportamiento de la red en caso de introducción de nuevos servicios o ante la incorporación de hardware. Debido a la importancia de los datos que gestiona la institución no se especifican las

herramientas utilizadas. Esta idea es válida para la inserción de equipamiento o servicios a una red, pero en caso de algún dispositivo que ya se encuentre funcionando o un servicio en plena ejecución, es igual de difícil prevenir fallas en el sistema considerando que los simuladores de redes pueden acercarse mucho a situaciones reales de explotación pero nunca podrán abarcarlas todas.

Por otra parte, en el nodo de la Universidad de Ciencias Médicas “Mariana Grajales Coello” los administradores de la red utilizan la herramienta de monitorización Zabbix, combinada con Zenoss y otras que informan mediante correo electrónico o mensajería instantánea cualquier incidencia en la red informática. Estas herramientas, junto a la experiencia alcanzada por los que allí se desempeñan, permiten la detección de situaciones anómalas y en la mayoría de los casos una respuesta lo suficientemente breve como para no afectar el servicio que prestan.

En ambos casos se plantea la inexistencia de procedimientos administrativos que permitan estructurar el proceso de diagnóstico de la red y la resolución de problemas está en dependencia de la pericia del personal encargado de la prestación de servicios. Para el estudio realizado se intentó, sin éxito, entrevistar a administradores de red y encargados de seguridad informática de otras instituciones, sin embargo se considera muy útil la información suministrada por los entrevistados ya que pertenecen a organismos que desarrollan una labor muy seria en la esfera de la informatización de sus procesos.

El único resultado de búsqueda que cumplió con las especificaciones que se necesitaban fue el servicio ofertado por Raytel Telecomunicaciones Limitada, empresa chilena de la esfera de las telecomunicaciones, que se dedica a la instalación de redes y los servicios asociados a telefonía IP y videovigilancia [33]. Entre sus servicios se encuentra el análisis y diagnóstico de redes informáticas, para el que emplean una metodología (ver Figura 1) que deriva en un conjunto de etapas y acciones.

Raytel publica en su sitio web las etapas del servicio de análisis y diagnóstico que oferta a sus clientes: levantamiento de la información, mapeo de la red, instalación de herramientas de monitoreo, análisis de red de datos, análisis de seguridad (servidores críticos), retroalimentación de información obtenida, e informe que resume el estado de los componentes de la red y especialmente el estado de los servicios que presentan fallas. En ellas se desarrollan veintiuna acciones y se genera una documentación importante a la que llaman entregables del servicio de análisis y diagnóstico.

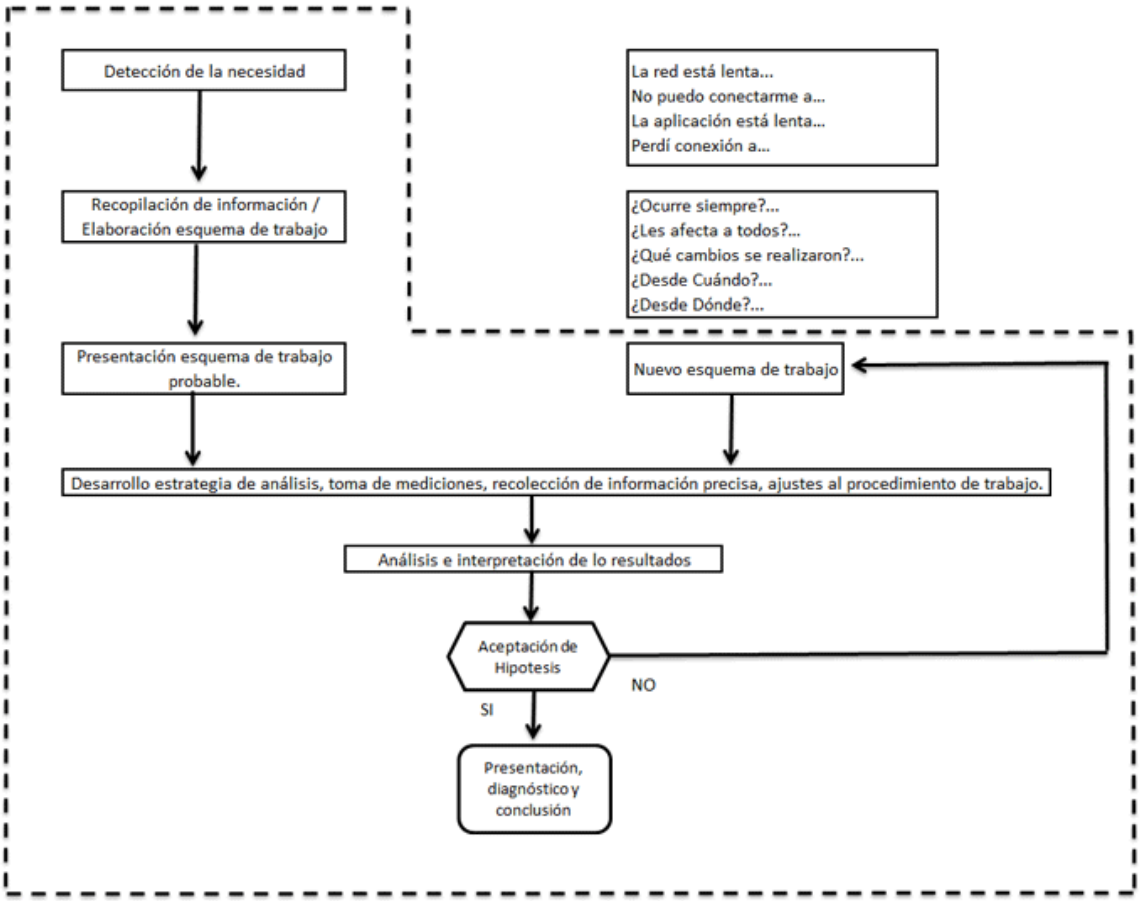


Figura 1 Metodología empleada por Raytel para el análisis y diagnóstico de redes

1.3 Herramientas para la monitorización de redes

Para detectar deficiencias en la red y agilizar la solución de los problemas que se presentan se emplean herramientas de monitorización. Son sistemas que se encargan de analizar la red en busca de componentes lentos o defectuosos, causados por la sobrecarga y/o fallas en los servidores, problemas en la infraestructura de red, y otros, para informar a los administradores.

La mayoría de los programas de monitorización y de almacenamiento de logs no requieren muchos recursos de memoria o almacenamiento y con un rendimiento medio de la CPU logra los resultados esperados. Una buena solución para monitorizar la red sería dedicar una computadora, empleando partes recicladas y con Linux como sistema operativo, como servidor de monitorización [16].

A continuación se definen las características que debe poseer una herramienta de monitorización para resultar elegible al momento de formar el conjunto de aplicaciones que estudiarán el comportamiento de la red [16]:

- Apropiada. Se debe seleccionar aquella que monitorice los parámetros seleccionados y brinde información en correspondencia con los resultados deseados.
- Costeable. Cuando existen limitaciones de presupuesto esta es una condición necesaria. Sin embargo, aun cuando se disponga de presupuesto, se deben comparar los beneficios de herramientas libres o de código abierto con las propietarias.
- Con uso mesurado de recursos de hardware. Esta característica es indispensable para que las computadoras que soportan las herramientas funcionen correctamente y permanezcan así durante largos periodos sin agotar la capacidad de almacenamiento.
- Flexible. La herramienta seleccionada debe adaptarse al entorno de la red objeto de monitorización.

- Con la capacidad de generar gráficos. Aquí entra en juego la idea de que una imagen vale más que cien palabras. Esta característica es útil para alcanzar una comprensión rápida de la actividad de la red.
- Con soporte. Para que se puedan actualizar a través del tiempo.
- Con almacenamiento histórico de datos. Debe poseer la capacidad de salvar la información recopilada de al menos dos o tres años para descubrir patrones de comportamiento.
- Con una interfaz intuitiva. Esta característica facilitará el trabajo del personal encargado de monitorizar la red.

Aunque no todas las herramientas presentan estas características es necesario tenerlas en cuenta a la hora de seleccionar una. De manera general, para lograr un buen servicio de monitorización es necesario combinar varias de ellas para cubrir todas las necesidades de la organización.

Las herramientas de monitorización se pueden clasificar en:

- De prueba selectiva o comprobación al azar: para la solución de problemas y la ejecución interactiva en cortos periodos de tiempo. ping es considerada una herramienta de comprobación selectiva activa, mientras que los analizadores de protocolos, que inspeccionan cada paquete en la red, son considerados pasivos. Estas herramientas ayudan a detectar la fuente del problema y ofrecen una panorámica de qué está sucediendo en nuestra conexión en tiempo real. Algunas, como ntop pueden ejecutarse de manera continua, mientras que otras, como Wireshark [6], son ejecutadas sólo cuando es necesario [4].
- De tendencia: ejecutan una monitorización desatendida por largos periodos y generalmente muestran los resultados de forma gráfica.
- De monitorización en tiempo real: ejecutan una monitorización similar a la anterior pero notifican al administrador de cualquier falla en el sistema.

- De análisis de trazas: resumen las trazas de varios programas y notifican al administrador cuando detectan algún problema. Suelen requerir mucho menos espacio en disco y poder de CPU que las herramientas de prueba selectiva o comprobación al azar.
- De prueba de comprobación: estiman el máximo rendimiento de un servicio o de una conexión de red. Aunque existen muchas herramientas dedicadas a realizar pruebas de velocidad en el navegador, estas pruebas son imprecisas [16].

En el mercado existe un número bastante amplio de aplicaciones que se emplean con fines específicos, y otras menos abundantes que tratan de abarcar muchas de las etapas del análisis y diagnóstico de una red. En este epígrafe se relacionan algunas de las herramientas encontradas en la búsqueda realizada, se detallan aquellas que fueron empleadas para la presente investigación y se lista el resto [20], [31], [34], [35], [36], [37].

- De prueba selectiva o comprobación al azar

Dentro de esta clasificación se pueden encontrar varias herramientas: ipconfig, ping, traceroure, mtr, ntop, ngrep, Wireshark y tcpdump, las que serán descritas a continuación:

▪ ***ipconfig o ifconfig***: muestra los valores de la configuración de la red TCP/IP, como las direcciones IP, máscara de subred y la puerta de enlace predeterminada de todos los adaptadores de red. Se emplea para determinar si la configuración es adecuada y brinda información útil para pruebas posteriores.

La información que brinda esta herramienta permite comunicar a otra persona la configuración IP de determinado equipo para recibir asistencia remota, o saber si un ordenador se encuentra en la misma red que otro con el que se desea conectar.

Este comando posibilita, además, conocer la dirección MAC de un adaptador de red. Esto es útil cuando se realiza la conexión a una red con filtrado MAC, es decir, con una lista de tarjetas de red autorizadas a conectarse, lo cual es más seguro porque, a diferencia de las direcciones IP, las MAC son únicas. El filtrado MAC se suele usar en redes inalámbricas.

Pudiera ocurrir que el usuario asigne a su adaptador de red una dirección IP que ya está en uso, pero esta situación es reportada por el sistema como “Conflicto de dirección IP”.

En caso de que la máscara de red no sea la correcta, el host no podrá reconocer al resto de los equipos ubicados en la propia red de área local. Si la puerta de enlace predeterminada no coincidiera con la real, probablemente no se tenga salida a de la red local (LAN).

Tanto ipconfig como ifconfig informarán si la tarjeta de red no está conectada a la red, pero tanto en Windows como en Linux, si el problema es el cable de red, lo indicarán con un icono que avisa dicha eventualidad. Si apareciera el mensaje “El cable de red está desconectado”, y estuviera conectado a la tarjeta del equipo, pudiera suceder que el extremo correspondiente al concentrador o conmutador sea el que está desconectado o que el cable de alimentación del dispositivo esté desconectado [20].

- ***ping***: verifica si un host puede ser alcanzado. Lo hace enviando un mensaje ICMP y espera respuesta, midiendo el tiempo de ésta. Esta prueba, una vez comprobado que no es problema de nuestro propio equipo, es la más útil en un entorno de red de área local. De los programas de supervisión de red es uno de los más sencillos, pero con resultados más efectivos y el de uso más habitual [20].

- ***traceroute***: es útil si la red está segmentada mediante enrutadores o existen problemas con Internet. Este programa se vale del hecho de que ningún enrutador deja pasar un datagrama con el campo TTL (Time To Live – Tiempo de vida) igual

a 1 o 0, lo cual significa que el destino se encuentra demasiado lejos y ya ha sido manipulado por varios enrutadores.

Esta herramienta, al igual que ping, es encontrada en la mayoría de los sistemas operativos y es conocida como tracert en algunas versiones de Microsoft Windows. Mediante su ejecución se puede detectar la ubicación de los problemas entre la computadora que lo ejecuta y determinado punto en Internet.

Se emplea –n para que no demore convirtiendo nombres en direcciones IP. Si los problemas se detectan en algún punto de la red analizada se debería realizar el análisis de ese punto, pero si no pertenece a dicha red entonces no se podrá hacer mucho [20].

- ***My TraceRoute (mtr)***: este programa combina ping y traceroute en una única herramienta. Mediante su ejecución se puede conocer el RTT (Round Trip Time, tiempo que demora un paquete en regresar al origen pasando por el destino) promedio y los paquetes perdidos hasta un determinado host, en vez de los resultados de un momento determinado que ofrecen ping y traceroute [20].

- ***ntop***: es una de las herramientas más útiles para la monitorización de redes. Es un analizador de protocolos con una interfaz web. Entre la información que brinda se puede citar: tráfico ordenado por varios criterios (fuente, destino, protocolo), identificación de los sistemas operativos de los host, identificación del tráfico P2P, varios gráficos, entre otra. Está disponible para la mayoría de los sistemas operativos y es incluido, a menudo, en muchas de las distribuciones de Linux. Puede hacer un uso intensivo de la CPU, en dependencia del tráfico observado por lo que se debe monitorizar el servidor de monitorización. Su principal desventaja es que sólo ofrece información histórica, lo cual puede resultar incómodo a la hora de solucionar problemas que se hayan presentado de manera sorpresiva [16].

▪ ***ngrep***: permite filtrar el tráfico en dependencia de los métodos empleados. Mediante su empleo se pueden detectar desde actividad de virus hasta correo basura [16].

▪ ***Wireshark***: anteriormente conocido como *Ethereal*. Es uno de los analizadores de analizadores de protocolos más utilizados, pues dispone de interfaz gráfica y ejecución por comandos, es un proyecto de código abierto con una gran comunidad aportando mejoras diariamente y es gratuito.

Funciona sobre Windows y Unix. Permite examinar información de una red en tiempo real o almacenar ficheros en un disco para luego analizarlos. Cuenta con características muy poderosas, como obtener información detallada de cada paquete y la reconstrucción de una cadena de una sesión TCP. Se usa generalmente para aislar y analizar el tráfico específico hacia o desde determinada dirección IP [4], [6], [15], [31], [34], [42].

▪ ***tcpdump***: es una herramienta de línea de comandos para monitorizar el tráfico de la red. Sus funcionalidades son muy parecidas a Wireshark, pero usa menos recursos. Los paquetes capturados pueden ser cargados en Wireshark para realizar un análisis visual y un posterior diagnóstico. Está disponible en los sistemas operativos derivados de Unix, aunque existe una versión para Windows [16].

- De tendencia

MRTG, RRDTool, Cacti, NetFlow, SmokePing y Flowc se encuentran dentro de esta clasificación. Por su amplio uso y conocidas ventajas serán descritas las tres primeras.

▪ ***MRTG*** *(Multi-Router Traffic Grapher)*: monitoriza la carga de tráfico en la red empleando el protocolo SNMP (Simple Network Management Protocol, facilita el intercambio de información de administración entre dispositivos de red). Muestra, mediante gráficos, el tráfico entrante y saliente [16].

▪ ***RRDTool***: se refiere a un conjunto de herramientas que permiten crear y modificar bases de datos RRD (Round Robin Database, base de datos que maneja planificación según el método Round Robin para lograr la selección de los elementos de manera equitativa), así como generar gráficos para mostrar los datos. Se emplea para dar seguimiento a datos en el tiempo como ancho de banda de la red o carga promedio del servidor y graficar dicha información [16].

▪ ***Cacti***: es una de las herramientas que emplea RRDTool, almacenando toda la información necesaria para crear gráficos en una base de datos MySQL. Está escrito en PHP. Es de ayuda para los dispositivos SNMP. Es complejo a la hora de configurarlo pero muestra gráficos impresionantes de los indicadores a analizar [16].

- De monitorización en tiempo real

La búsqueda realizada arrojó que entre las herramientas más empleadas están Nagios, Snort y Zabbix. Aunque Nagios supera ampliamente al resto, a continuación se resumen las características de las restantes.

▪ ***Nagios***: Sistema de código abierto para la monitorización de redes. Es ampliamente utilizado. Chequea el hardware y el software que se especifique y alerta cuando el comportamiento no es el deseado. Está licenciado bajo la GNU General Public License Version 2, publicada por la Free Software Foundation.

Se ejecuta en Linux o BSD y provee una interfaz web que muestra el estado del sistema. Se basa en la ejecución de otras herramientas, como ping y nmap, para realizar informes sofisticados [16].

▪ ***Snort***: es un sniffer de paquetes y traceador que puede ser empleado como sistema de detección de intrusos. Puede ejecutar análisis de protocolos, búsqueda de contenido y comparación de paquetes. Posee capacidades de alerta a los administradores de la red. Su instalación no es trivial y en dependencia de la cantidad de tráfico a analizar se necesitará un servidor de monitorización con considerables recursos. Es una herramienta bien documentada y con una

comunidad de usuarios bastante grande [16].

▪ ***Zabbix***: es presentado como un híbrido entre Cacti y Nagios. Usa una base de datos SQL, tiene su propio paquete de procesamiento de gráficos y ejecuta casi todas las tareas que se desean de una herramienta de este tipo. Fue lanzado bajo la GNU General Public License.

- De análisis de trazas

Las trazas de los proxys contienen suficiente información acerca de los hábitos de los usuarios, por lo que su análisis puede brindar información de quiénes son aquellos usuarios que hacen un uso inapropiado de los recursos de la red e identificar los sitios que deberían tener un espejo. Entre las herramientas con estos fines se pueden citar: Analog, Webalizer, AWStats, Calamaris y Sawmill.

▪ ***Calamaris***: produce impresionantes informes en html y gráficos acerca de la utilización del proxy. Está escrito en Perl y disponible en la mayoría de las distribuciones de Linux [7], [11], [14], [16], [18].

▪ ***Sawmill***: software comercial que produce informes detallados y con una apariencia más profesional que la mayoría de las alternativas de código abierto. Se puede ejecutar sobre Unix y Windows. Requiere una licencia comercial en dependencia del tipo de información a analizar y de su cantidad [7], [11], [14], [16], [18].

- De pruebas de comprobación

Dentro de esta clasificación las herramientas más conocidas son ttcp y bing.

▪ ***ttcp***: forma parte de la mayoría de los sistemas Unix. Es una herramienta sencilla de pruebas de rendimiento en una red, en la que una instancia es ejecutada en cada lado que se desea probar, en la que un nodo funciona como transmisor y el otro como receptor. Se pueden probar tanto cadenas UDP como TCP. Muestra la velocidad en kilobytes. Al igual que ping y traceroute, ttcp se encuentra disponible en gran parte de los sistemas operativos [16].

▪ ***bing***: intenta determinar la capacidad de procesamiento disponible en una conexión punto a punto analizando los tiempos de viaje (RTT) para varios tamaños de paquetes ICMP. Puede dar una idea del comportamiento de la red sin cargarla demasiado ya que usa poco ancho de banda [16].

- Otras herramientas

Existen otras herramientas que también se emplean en la monitorización de redes y sus funcionalidades se incluyen en varias de las clasificaciones realizadas o no llegan a cubrir todas las tareas de una de ellas. Entre ellas se pueden relacionar:

▪ ***SoftPerfect Network Scanner***: Analiza comunicaciones NetBIOS y SNMP y los rangos IP que se le indique. Muestra IP, MAC, tiempo de respuesta a los ping, puertos abiertos de cada equipo, y los recursos compartidos de la red. No requiere privilegios administrativos y exporta resultados a varios formatos. Es gratuito [37].

▪ ***Javvin Packet Analyser***: Este analizador de protocolos es capaz de capturar paquetes Ethernet, analizar protocolos y reconstruir mensajes a nivel de aplicación. Interpreta todos los protocolos relacionados con TCP/IP y permite aplicar filtros. No es gratuito [35].

▪ ***Pandora FMS***: Software de código abierto para la monitorización de aplicaciones y dispositivos de red.

▪ ***Network General Sniffer Basic***: Capaz de capturar paquetes Ethernet, incluye un análisis simple de protocolos. Interpreta los protocolos relacionados con TCP/IP y, además, algunos de los más comunes que no están basados en TCP.

▪ ***Zenoss Core***: Provee una interfaz web que permite a los administradores de sistemas monitorizar la disponibilidad de dispositivos y servicios de red. Detecta automáticamente recursos en una red y cambios en su configuración. Liberado bajo la Licencia Pública General de GNU Versión 2.

▪ ***Axence NetTools***: Integra doce herramientas para monitorizar la disponibilidad de hosts, revisar la paquetería de la red, monitorizar los servicios y puertos y

lanzar trazas y solicitudes de eco, entre otras funcionalidades. Cuenta con una interfaz limpia y bien organizada. Es propietario, con una versión de prueba por 30 días. Se encuentra disponible sólo en inglés y es compatible con Windows 7, Vista y XP [1].

Otras herramientas estudiadas son: Wildpackets Etherpeek, MailGraph, BindGraph, SARG (Squid Analysis Report Generator), FreeRADIUS, Piwik y SqStat.

La mayoría de las herramientas seleccionadas para la monitorización son gratuitas y fueron empleadas con fines específicos. Aunque algunas cumplen su función en las estaciones de trabajo, lo ideal sería ubicarlas en una computadora que esté dedicada completamente a la monitorización, o lo que es lo mismo, un servidor de monitorización.

De manera general, un servidor de monitorización debe tener acceso a toda la red. Para monitorizar una conexión a una WAN, como pudiera ser la conexión a Internet mediante el ISP, el servidor de monitorización debe ser capaz de observar el tráfico que pasa por el enrutador que sirve como frontera a la red.

1.3.1 Tráfico Web. Logs

Entre los servicios que más demanda tienen en una organización se encuentra la navegación en Internet. Para el control de la navegación y por cuestiones administrativas y de seguridad informática se emplean los servidores proxy [26]. En el caso particular de la Universidad de Holguín es utilizado Squid/2.7.STABLE9.

Los logs ofrecen información de mucho valor acerca del funcionamiento de Squid. No sólo registran los accesos, sino los errores de configuración del sistema y el consumo de recursos. Aunque Squid mantiene un considerable número de ficheros logs (squid.out, cache.log, useragent.log, store.log, hierarchy.log, access.log), la mayoría de las herramientas de análisis de logs se basan en las

entradas del access.log, que consiste en, al menos, 10 columnas separadas por uno o más espacios [8] [14] [17].

Las columnas de los elementos que componen el access.log del Squid con su significado se detallan a continuación:

Tiempo: ofrece la fecha y hora en un formato codificado.

Duración: se refiere a cuántos milisegundos la transacción mantuvo ocupada la caché. Su interpretación difiere entre TCP y UDP:

- Para HTTP/1.0 representa el tiempo entre accept() y close()
- Para conexiones persistentes, representa el tiempo entre la planificación de la petición y la culminación de su envío
- Para ICP, representa el tiempo entre la planificación de la petición y su real envío.

Es necesario aclarar que las entradas son registradas después que las peticiones culminan su envío, no durante el tiempo de vida de la transacción.

Dirección del cliente: es la dirección IP del cliente de la instancia que realiza la petición. Se puede configurar con la opción de configuración client_netmask (máscara de red del cliente), que provee privacidad a los usuarios, pues sólo mostraría la dirección de la red, pero hace el análisis más dificultoso al no brindar la dirección IP del cliente.

Códigos de resultado: esta columna está compuesta por dos entradas separadas por el símbolo /. Se encarga de codificar el resultado de la transacción.

El resultado de la caché de la petición contiene información acerca del tipo de petición, cuándo fue satisfecha, o de qué manera falló.

TCP_HIT	Una copia válida del objeto solicitado fue encontrada en la caché
TCP_MISS	El objeto solicitado no se encontraba en la caché.

TCP_DENIED El acceso fue negado para esta solicitud.

La parte del estado contiene el código de resultado HTTP con algunas extensiones específicas de Squid. Estos códigos brindan información sobre el éxito de la transacción, el redireccionamiento de peticiones y los errores en clientes o servidores.

200	Transacción exitosa
302	Movido temporalmente
401	No autorizado
403	Prohibido
407	Autenticación del proxy solicitada
502	Puerta de enlace incorrecta

Bytes: es la cantidad de información entregada al cliente. Aunque la solicitud muestre una página de error, el tamaño de la misma será incluido en el log.

Método de solicitud: se refiere al método para obtener un objeto. Entre los más empleados: GET, POST, CONNECT.

URL: contiene el URL solicitado.

Usuario: muestra la identidad del cliente que realizó la solicitud. Tener activada esta opción repercute en el rendimiento del Squid.

Código de jerarquía: consiste en 3 elementos:

- Etiqueta de jerarquía, con el prefijo TIMEOUT_
- Un código que explica cómo fue manipulada la solicitud. Por ejemplo, si fue reenviada o si se realizó la petición directamente.

- La dirección IP o el nombre de host al cual la solicitud fue reenviada, si el código de resultado fue MISS.

Tipo: tipo de contenido del objeto, tal y como se muestra en la cabecera HTTP.

Un estudio detallado de estos campos puede proporcionar información muy valiosa acerca del empleo del servicio de navegación en Internet [14].

1.4 Estado general de la red informática de la Universidad de Holguín "Oscar Lucero Moya"

El estudio inicial de la Red UHOLM permitió la obtención de una serie de datos a partir de la consulta de la documentación técnica, las encuestas a usuarios y las entrevistas con los administradores de la red.

El hecho de que la Universidad de Holguín cuente con dos sedes (Oscar Lucero Moya - OLM y Celia Sánchez Manduley - CSM), a una distancia aproximada de 5 km y con un número considerable de usuarios, hace necesaria una división entre la administración de los servicios informáticos de ambas sedes.

Los servidores están ubicados en los Nodos, donde trabajan los administradores de los segmentos de red de una o varias áreas y se atienden a los usuarios pertenecientes a un dominio determinado. En la Tabla I se muestra su distribución en la Universidad de Holguín.

Tabla I Distribución de los nodos en la Universidad de Holguín

Nodo	Áreas que atiende
Central	Toda la universidad. Facultad de Informática y Matemática, VRU.
Celia Sánchez Manduley	Sede Celia Sánchez Manduley. Facultad de Humanidades. Facultad de Ciencias Sociales. Facultad

	de Derecho.
ICT	Edificio de la Biblioteca Benito Juárez.
Ingeniería. CADCAM	Facultad de Ingeniería. Facultad de Agronomía. CADCAM
Economía e Ingeniería Industrial	Facultad de Ciencias Contables y Económicas. Facultad de Ingeniería Industrial y Turismo.
VREA	Vice Rectoría Económica. Vice Rectoría de Administración. Dirección de Recursos Humanos.

Estos nodos atienden aproximadamente a poco más de 3200 usuarios, alrededor de 2400 estudiantes y 840 trabajadores, entre los que se encuentran profesores y trabajadores de la Sede Central y de las Filiales Universitarias Municipales (FUM).

El Registro de la Red, emitido por la Agencia de Control y Supervisión del MIC resume los aspectos técnicos más relevantes de la Red UHOLM, que se muestran en la Tabla II.

Tabla II Parámetros técnicos de la Red UHOLM según el Registro de la Red

Topología	Estrella extendida
Alcance geográfico	Provincial
Proveedor	ENET
Velocidad	128 Kbps (para el acceso a Internet)
Dominio	uho.edu.cu

Bloque de direcciones asignadas por el ISP	200.55.148.0/29
Cortafuegos	Untangle

La Figura 2 muestra el esquema general de la Red UHOLM. En el esquema de la red están representados los nodos y los dispositivos principales que componen la red. Por la complejidad en el diseño no se muestran los dispositivos terminales, sólo los servidores principales y los equipos de interconexión (concentradores, conmutadores y enrutadores).

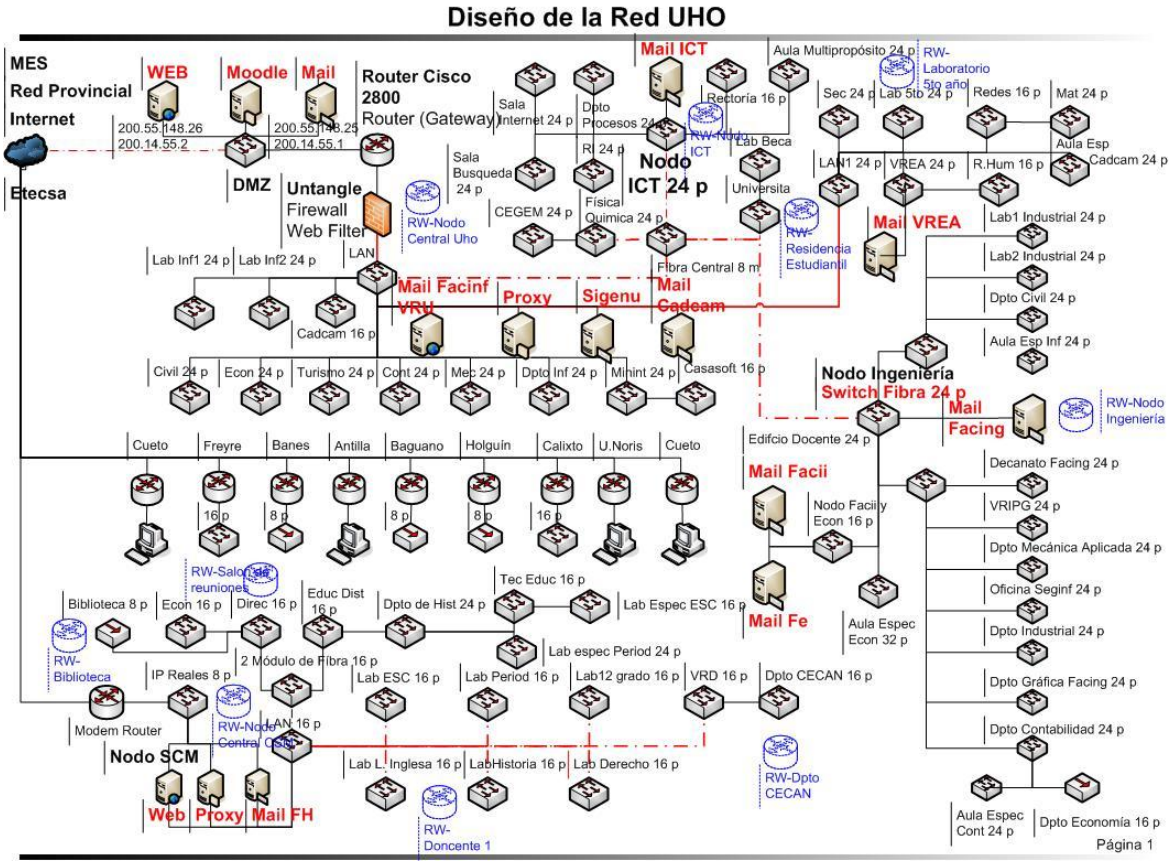


Figura 2 Esquema general de la Red UHOLM

Para una mejor comprensión del diagrama de la red, ésta se puede dividir en tres zonas, cada una con particularidades debido a sus ubicaciones geográficas, usuarios a los que prestan servicios o concentración de servicios de red.

1. Filiales Universitarias Municipales (FUM)

El siguiente segmento representa la forma y distribución de la conectividad de las FUM con la sede central. En la Figura 3 se presentan los detalles.

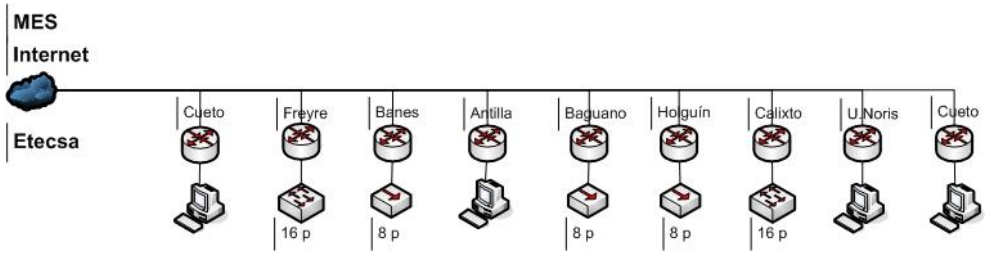


Figura 3 Esquema de la Red UHOLM - FUM

Las FUM (Urbano Noris, Sagua de Tánamo, Mayarí, Maceo, Holguín, Gibara, Rafael Freyre, Frank País, Cueto, Calixto García, Cacocum, Banes, Báguano y Antilla), aunque dispongan de una sola computadora, se conectan a ETECSA a través de módem enrutadores, lo cual permite el acceso a los servicios que se prestan en la sede central. Algunas FUM cuentan con conmutadores o concentradores que permiten que las computadoras de sus LAN se conecten a la Red UHOLM.

2. Sede Celia Sánchez Manduley

El esquema de la red de la sede Celia Sánchez Manduley se presenta en la Figura 4.

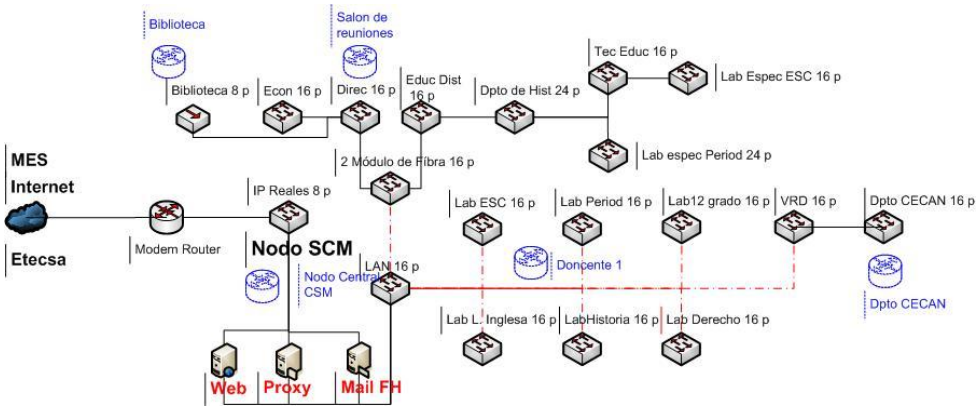


Figura 4 Esquema de la Red UHOLM – Sede Celia Sánchez Manduley

La sede Celia Sánchez Manduley se conecta a ETECSA mediante un módem enrutador. Cuenta con un único nodo que atiende a todos los usuarios de dicha sede, con dominio *fh.uho.edu.cu*. La calidad del equipamiento, así como del cableado estructurado, es buena pues estas edificaciones contaban con una infraestructura adecuada desde que funcionaba como Escuela Formadora de Trabajadores Sociales.

3. Sede Oscar Lucero Moya

La sede Oscar Lucero Moya concentra la mayor cantidad de equipos y servicios. El esquema de la red se muestra en la Figura 5.

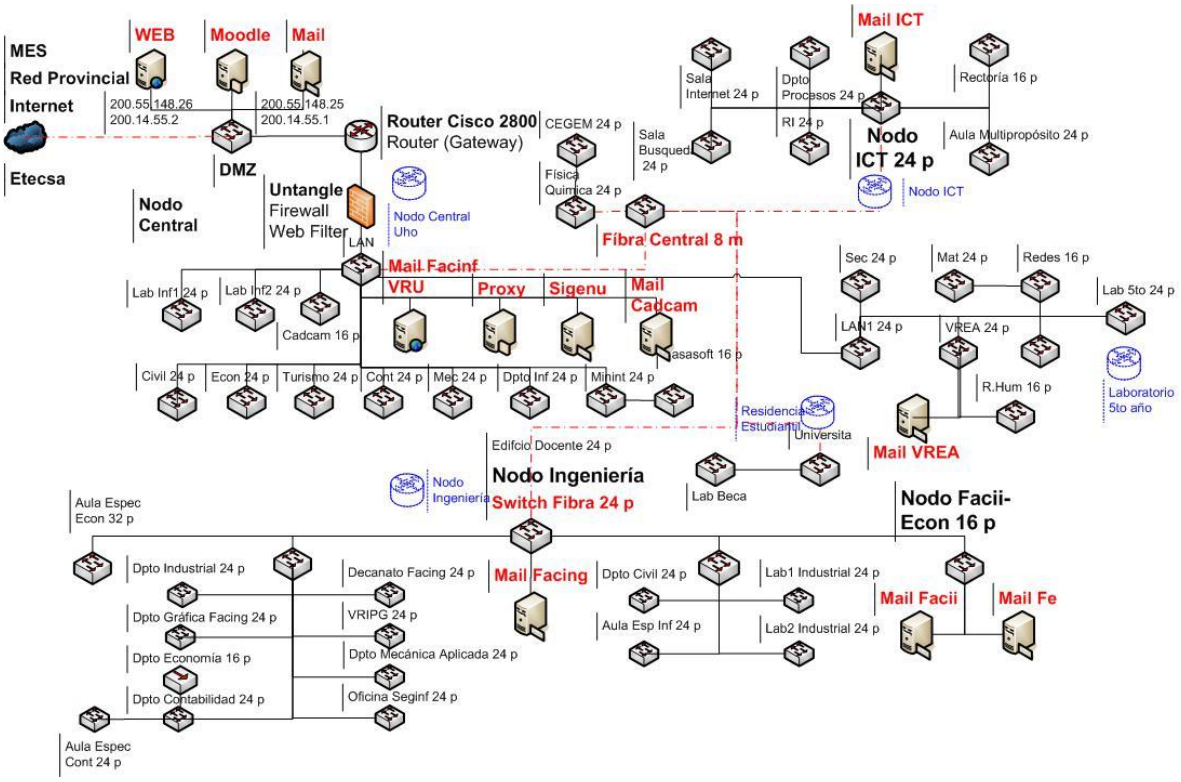


Figura 5 Esquema de la Red UHOLM – Sede Oscar Lucero Moya

Esta sede dispone de fibra óptica para su conexión con ETECSA. Cuenta con un nodo central, que gestiona los servicios de toda la red y otros cuatro para las facultades y áreas. Es la que mayor complejidad presenta en su cableado estructurado ya que, aunque se ha trabajado en eliminar deficiencias, principalmente en áreas exteriores, persiste desorganización en los interiores de los locales.

Aunque no están representados en el esquema, existen más de 200 usuarios de acceso remoto que hacen uso de la red desde sus domicilios. Mediante este servicio los usuarios acceden a los servicios de correo electrónico, mensajería instantánea, la Intranet y a la navegación en Internet.

Ancho de banda disponible para la Universidad de Holguín

En el caso de la red informática de la Universidad de Holguín, el ancho de banda está limitado por el contrato existente entre la institución y el proveedor de servicios de internet (ISP) ETECSA, distribuido como se muestra en el gráfico.

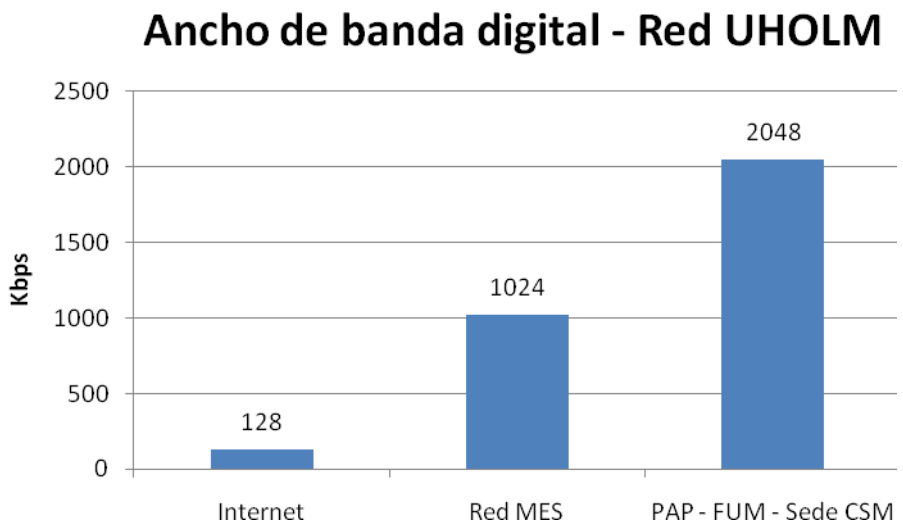


Figura 6 Ancho de banda disponible para la Red UHOLM

La conexión de la Universidad de Holguín con Internet es de sólo 128 Kbps. Esta es la velocidad de transferencia máxima que se puede alcanzar en el acceso a la mayoría de los dominios de Internet, exceptuando a *edu.cu* que tiene disponible un ancho de banda superior. Para acceder al servicio, los usuarios deben autenticarse, excepto para un grupo de dominios (*rimed.cu*, *cult.cu*, *uci.cu*, *jovenclub.cu*, *sld.cu*) y otros relacionados con la investigación y superación profesional, así como los portales digitales de los principales periódicos y revistas nacionales, a los cuales se puede acceder sin necesidad de autenticarse en cualquier horario.

La Red MES incluye el acceso a los sitios del Ministerio de Educación Superior, con dominio *edu.cu.* Estos sitios están disponibles en cualquier horario y sin necesidad de que el usuario se autentique. Para esto está disponible un ancho de banda de 1024 Kbps.

La red informática de la Universidad de Holguín emplea el Protocolo de Autenticación de Contraseñas (PAP, *Password Authentication Protocol*) para autenticar a los usuarios contra el servidor de acceso remoto. El servicio está autenticado en LDAP y anclado a un número en específico.

Para PAP, el acceso a las FUM (Filiales Universitarias Municipales) y la sede Celia Sánchez Manduley se destinan 2048 Kbps [27].

Red inalámbrica de la Universidad de Holguín

La Universidad de Holguín tiene autorización de la Agencia de Control y Supervisión del MIC, mediante el Permiso 11121, para adquirir, instalar y explotar medios inalámbricos en la banda de frecuencias 2400 a 2483.5 MHz. En la actualidad, la red dispone de 10 puntos de acceso inalámbricos TP-Link TL-WR542G ubicados en diversas locaciones de ambas sedes del centro, que permiten que la red llegue a lugares donde es poco factible llevar el cableado o brindar la posibilidad de que aquellos usuarios que disponen de terminales con tecnología wireless puedan conectarse y hacer uso de los servicios.

Los equipos existentes en la red de la Universidad de Holguín están basados en el estándar IEEE 802.11gb, lo que les permite operar a una velocidad de 54 Mbps. La Tabla III, obtenida del Permiso 11121 y en la que se muestra la distribución de los dispositivos en el campus universitario, se reproduce a continuación

Tabla III Relación de dispositivos inalámbricos en la Red UHOLM

No	Equipo	Función	Lugar
1	TP-LINK TL-WR542G	Access Point	Biblioteca. Sede CSM
2	TP-LINK	Access Point	Salón de Reuniones

	TL-WR542G		
3	TP-LINK TL-WR542G	Access Point	Docente I. Sede CSM
4	TP-LINK TL-WR542G	Access Point	Nodo Central. Sede CSM
5	TP-LINK TL-WR542G	Access Point	Residencia Estudiantil. Sede CSM (Dpto CECAN)
6	TP-LINK TL-WR542G	Access Point	Biblioteca Benito Juárez. Sede OLM (Nodo ICT)
7	TP-LINK TL-WR542G	Access Point	Residencia Estudiantil. Sede OLM
8	TP-LINK TL-WR542G	Access Point	Docente I. Sede OLM (Laboratorio 5to año Informática)
9	TP-LINK TL-WR542G	Access Point	Docente II. Sede OLM (Nodo de Ingeniería)
10	TP-LINK TL-WR542G	Access Point	Dirección de Informatización (Nodo Central)

Sistemas operativos instalados en estaciones de trabajo y servidores

En la red informática de la Universidad de Holguín se manifiesta la tendencia mundial de emplear Linux en los servidores y Windows en las estaciones de trabajo. Aunque se desea una migración total a software libre no se ha logrado el

objetivo, en algunos casos por la incompatibilidad de algunos sistemas y en otros por la incomprensión de directivos y el rechazo de los usuarios.

El uso de Debian en los servidores está bastante generalizado, ya que se emplea en los servidores de correo, el servidor proxy, y en los que se ejecutan muchos otros servicios imprescindibles para el flujo informativo de la institución.

Ubuntu se emplea en los laboratorios de la carrera Ingeniería Informática y es la opción elegida por algunos profesores de la Facultad de Informática y Matemática.

El sistema operativo predominante en las estaciones de trabajo es Windows XP, el cual se encuentra instalado en la mayoría de las estaciones de trabajo de los laboratorios docentes, las oficinas de personal administrativo y en los departamentos docentes. En las computadoras con mejores recursos de hardware se puede encontrar Windows 7.

Encuestas y entrevistas a usuarios de la Red UHOLM

La encuesta aplicada a los usuarios de la red informática (ver Anexo I) permitió valorar el estado de satisfacción de los mismos con el acceso a los servicios que habitualmente emplean, como el correo electrónico, la navegación en Internet, la Intranet, los servidores FTP o el acceso remoto; también permitió evaluar el funcionamiento general de la red y conocer los principales problemas a los que se enfrentan los usuarios en su trabajo diario con la red. Esta encuesta fue aplicada a trabajadores, profesores y estudiantes de diferentes facultades de la universidad. En total fueron encuestados 48 usuarios de la Red UHOLM, obteniéndose los resultados que se reflejan en la Figura 7.

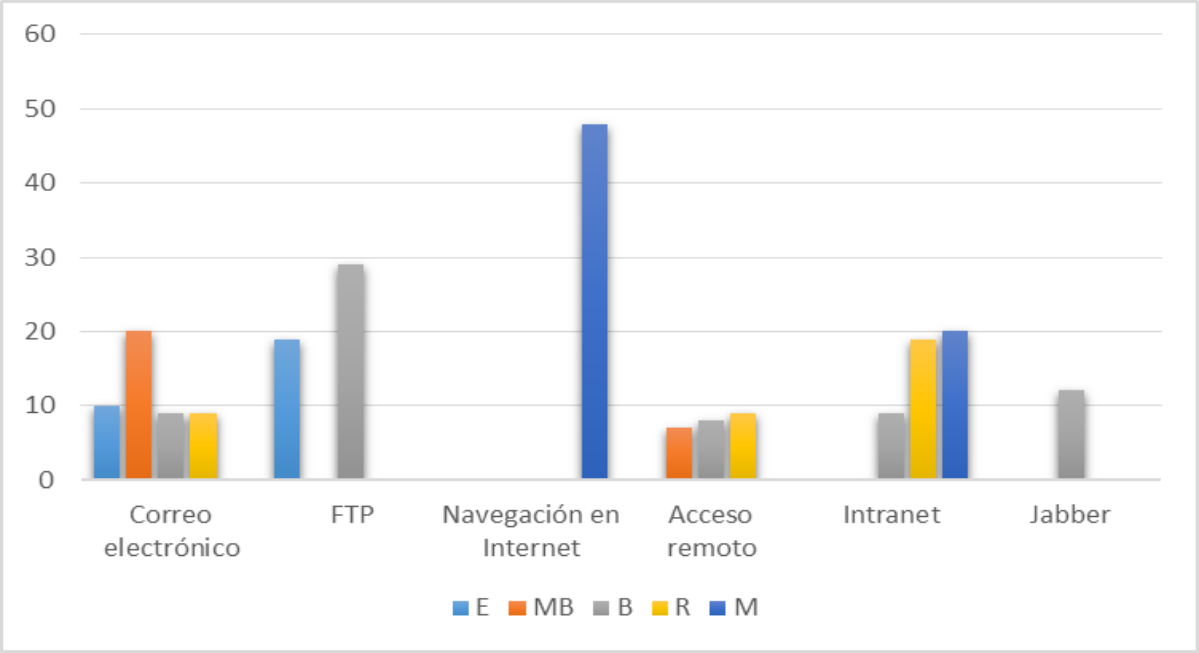


Figura 7 Resultados de la encuesta aplicada a usuarios de la Red UHOLM – Valoración de los servicios

De esta gráfica se puede concluir que los servicios mejor valorados por los encuestados son la transferencia de ficheros (FTP) y la mensajería instantánea, con la totalidad de las respuestas con categoría B o superior. Poco más del 80% reconoce el buen comportamiento del correo electrónico, mientras que más de la mitad de los usuarios que emplean el acceso remoto consideran que el servicio es bueno o muy bueno. En el otro extremo se encuentra la navegación web, ya que el acceso a la Intranet, incluido a los sitios listados en lo que se suele denominar red nacional, es calificado con regular o malo por más del 80% de los encuestados; así como el acceso a Internet con la totalidad de los 48 usuarios que emitieron sus consideraciones reflejando su inconformidad absoluta con este servicio. El desglose de los resultados por cada uno de los servicios puede ser consultado en el Anexo II.

El servicio de navegación en Internet es el que más quejas e insatisfacciones genera en los usuarios. Restricciones de acceso a algunos dominios,

segmentación por horarios, cuotas limitadas e inestabilidad en la navegación son elementos que provocan opiniones desfavorables en los autorizados a emplear el servicio.

Los encuestados definen como problemas recurrentes a los que se han enfrentado al emplear la Red UHOLM los siguientes:

- Lentitud para acceder a Internet
- Intermitencia del servicio de navegación web
- Inaccesibilidad a la mayoría de los dominios *.cu*
- Inestabilidad de los servicios
- Desactivación de los servicios sin previo aviso.

Incluso algunos usuarios realizan sugerencias, como investigar vías alternativas para el acceso a los sitios de dominio *.cu*, y emplear el ancho de banda completo para el acceso exclusivo a Internet.

La valoración general del funcionamiento de la Red UHOLM muestra que 4 de cada 5 usuarios considera el mismo es regular o malo, lo que se encuentra en correspondencia con las respuestas del apartado anterior de la encuesta. La Figura 8 muestra un gráfico con la opinión de los usuarios acerca de la red teniendo en cuenta todos sus servicios.

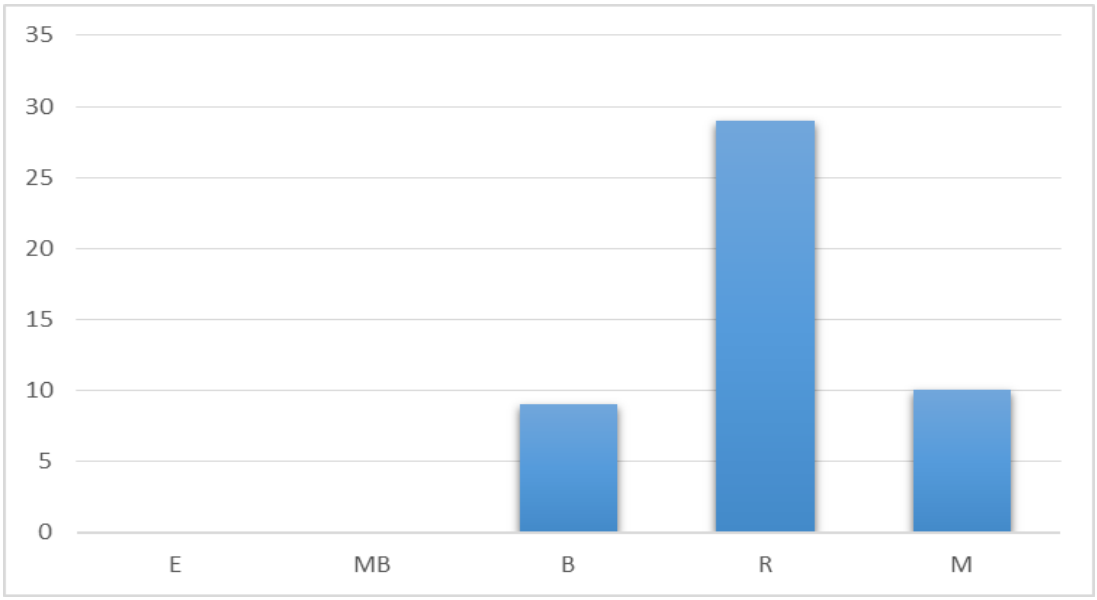


Figura 8 Resultados de la encuesta aplicada a usuarios de la Red UHOLM – Valoración general

En el caso de la entrevista se realizaron preguntas más abiertas que permitieran a los administradores de los nodos abordar con mayor profundidad los tres aspectos referidos a las principales quejas de los usuarios, los problemas frecuentes y las propuestas para mejorar el funcionamiento de la red (ver Anexo III).

La pregunta concerniente a las principales quejas de los usuarios tramitadas a través de los administradores arrojó como resultado:

- Lentitud para acceder a Internet.
- Carencia de recursos informáticos.
- Restricción de acceso a algunos sitios.
- Limitación de Internet por horarios.
- Cuota de navegación baja.

Como se puede apreciar, al realizar una comparación de estas inquietudes expuestas a los administradores con las que abordan los usuarios en sus

encuestas se aprecian situaciones nuevas, como la inconformidad con los horarios de servicio de navegación y la cuota asignada.

Como parte de sus criterios, los administradores exponen como problemas recurrentes que influyen en el correcto funcionamiento de la red:

- Inestabilidad de la conectividad por dispositivos ineficientes.
- Elevado tráfico de la red por usuarios que emplean programas de escaneo.

Por último sugieren, para mejorar el funcionamiento de la red, las siguientes acciones:

- Aumentar el ancho de banda para el acceso a Internet.
- Mejorar la infraestructura informática de los nodos.

1.5 Conclusiones parciales

El análisis del objeto y campo de estudio de la presente investigación permitió determinar que:

- Existe una diversidad de herramientas que permiten la monitorización de una red informática, por lo que es necesario realizar una selección teniendo en cuenta su costo, funciones implementadas, consumo de recursos, flexibilidad y usabilidad.
- El estudio del comportamiento del servicio de navegación en Internet, a través de las trazas generadas por el servidor proxy Squid, permitirá proponer soluciones para mejorar el servicio y disminuir las quejas de los usuarios.
- La Red UHOLM es una red informática de alcance provincial, limitados recursos de hardware y un número considerable de usuarios que manifiestan insatisfacciones con la calidad de los servicios que presta.
- Considerando las condiciones específicas de la Red UHOLM, que no se corresponden con las de aquellos países que se han encargado de

desarrollar metodologías para el estudio de sus redes informáticas, se hace necesario adecuar los procedimientos existentes a las particularidades de la red estudiada.

Capítulo 2. Procedimiento para el diagnóstico de la Red UHOLM y su aplicación

En este capítulo se propone un procedimiento para realizar el diagnóstico de la red informática de la Universidad de Holguín. Se parte de la adecuación de una metodología analizada previamente para su aplicación en la institución, en correspondencia con las características de la misma y se describen las etapas del procedimiento y las acciones a desarrollar en cada una de ellas. Por último se presentan los principales resultados producto de su aplicación en la red informática de la Universidad de Holguín “Oscar Lucero Moya”.

2.1 Procedimiento para el diagnóstico de redes

En la presente investigación se presenta un procedimiento que emplea como base las etapas del servicio de análisis y diagnóstico de redes derivadas de la metodología utilizada por Raytel para el análisis y diagnóstico de redes.

La variante propuesta reduce la cantidad de etapas del procedimiento y de las acciones a desarrollar en cada una de ellas. El diagrama del procedimiento, con el flujo de acciones a desarrollar en cada una de las etapas, se presenta en la Figura 9.

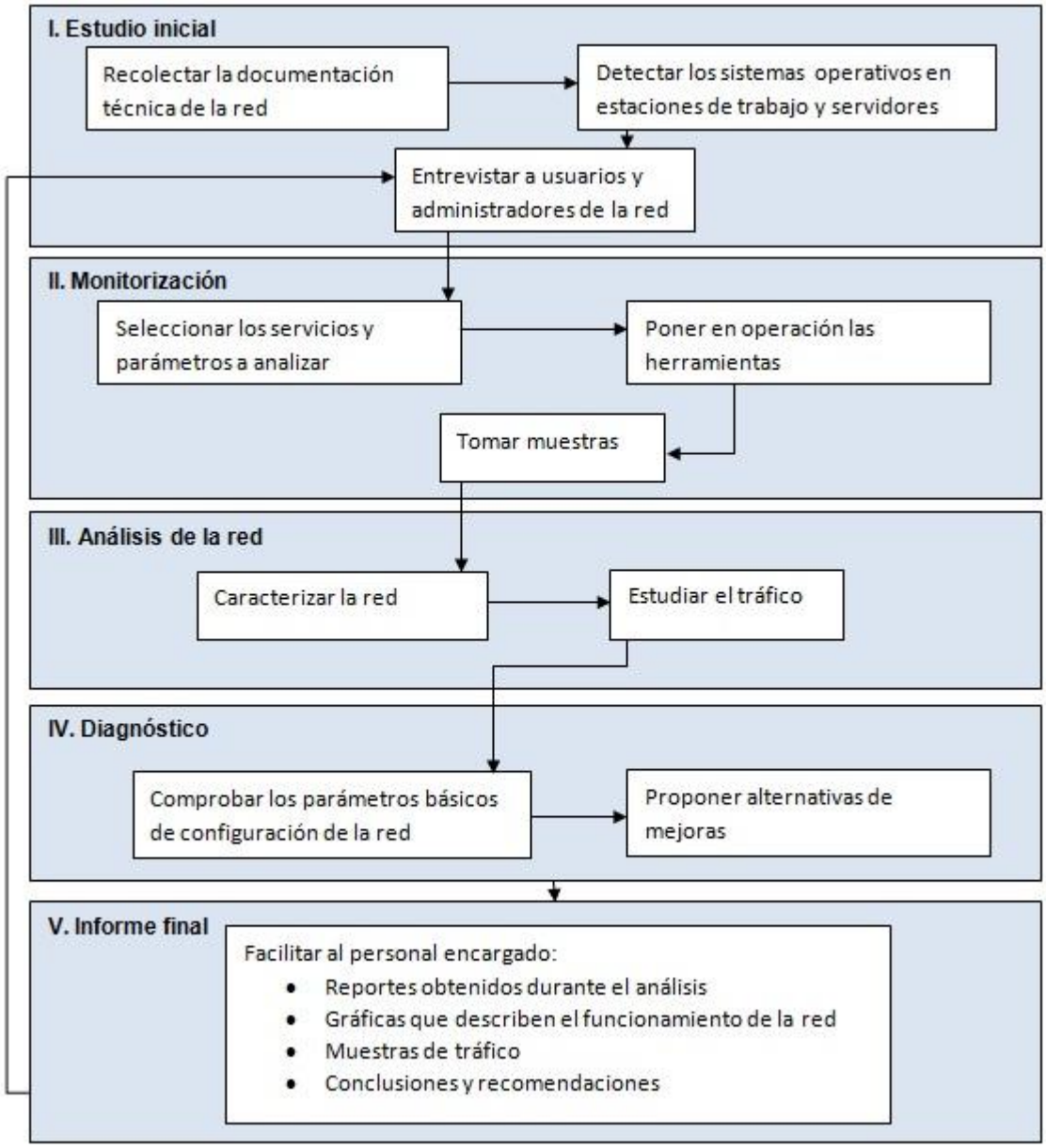


Figura 9 Procedimiento para el diagnóstico de la Red UHOLM

Aunque el objetivo del procedimiento es aplicarlo de forma periódica a toda la red, la etapa de monitorización permite seleccionar determinados parámetros de un solo servicio y continuar el desarrollo de las otras etapas, de manera que se logre profundizar en las deficiencias detectadas para dicho servicio y lograr su optimización.

2.1.1 Descripción de las etapas del procedimiento propuesto

Etapa I. Estudio inicial

Objetivo: recopilar, partiendo de la documentación existente y de la opinión de usuarios y administradores, la información del estado de la red que sirva como base para iniciar el proceso de análisis y diagnóstico.

Para ello se deben desarrollar las acciones siguientes:

- Recolectar la documentación técnica de la red

Se parte del esquema de la red, con la descripción de especificidades de la misma. Se estudian, además, otros documentos que regulen el funcionamiento de la misma como el Registro de la Red emitido por la Agencia de Control y Supervisión del MIC y permisos emitidos para el empleo de medios inalámbricos. Se emplea la observación o herramientas de detección de hardware para actualizar el esquema general de la red, teniéndose en cuenta que pueden ser dados de alta o movidos de locales o áreas dispositivos terminales y de interconexión de redes con un efecto directo en el tráfico de la red.

- Detectar los sistemas operativos en las estaciones de trabajo y servidores

Se emplea la observación o herramientas de detección de software para la determinación de los sistemas operativos instalados. La detección de los sistemas operativos empleados permitirá realizar una adecuada selección de herramientas a utilizar para las etapas posteriores y una valoración del rendimiento de los servicios en los mismos.

- Entrevistar a usuarios y administradores de la red

Se aplican encuestas a los usuarios y entrevistas a los administradores de la red, garantizando una representatividad de las diferentes áreas de la institución. Se procesan los resultados de las mismas y se emiten valoraciones.

Etapa II. Monitorización

Objetivo: obtener datos específicos del funcionamiento de la red, una vez determinados los servicios que mayor insatisfacción provocan en los usuarios de la red y las limitaciones para una correcta administración de esta, mediante el empleo de diversas herramientas.

Para ello se deben desarrollar las acciones siguientes:

- Seleccionar los servicios y parámetros a analizar

Empleando la información recopilada hasta el momento, y tras un estudio de las técnicas para el diagnóstico de redes, se escogen los servicios y parámetros de mayor relevancia que puedan influir en el funcionamiento de la red.

- Poner en operación las herramientas

Una vez escogidos los parámetros a analizar y seleccionado el sistema para la monitorización de la red, se pone en operación el sistema para la obtención de los datos. En este paso se pueden emplear tanto herramientas propias de los sistemas operativos como software profesional para determinar el comportamiento específico de las variables seleccionadas.

- Tomar muestras

Se seleccionan los datos arrojados por el sistema, de forma aleatoria o siguiendo un patrón específico. En este caso pueden ser empleados los registros suministrados por los servicios instalados en los servidores de la red, así como los obtenidos de las herramientas en funcionamiento.

Etapa III: Análisis de la red

Objetivo: estudiar los datos obtenidos de las herramientas de análisis y monitorización para determinar diferentes patrones de comportamiento en dependencia de las situaciones monitorizadas.

Para ello se deben desarrollar las acciones siguientes:

- Caracterizar la red

A partir de la información obtenida de las etapas anteriores se caracteriza el estado actual de la red. Para ello se determina la información relevante obtenida de la etapa anterior y se buscan patrones de comportamiento para circunstancias específicas.

- Estudiar el tráfico

El análisis de tráfico permite obtener información del funcionamiento de una red y estudiar las estadísticas recopiladas en un período dado. Su utilidad está dada en que se puede investigar el flujo de información que emplea un protocolo específico, detectar intercambio no seguro de este flujo, detectar si algún elemento de la red está ocupando un ancho de banda excesivo, entre otras. Todo ello es posible gracias a los sistemas de monitorización de redes, que se encargan de la captura y análisis del tráfico que circula por el nodo en el que se está ejecutando.

Etapa IV. Diagnóstico

Objetivo: determinar los parámetros que inciden en el rendimiento de los servicios de red y proponer soluciones que optimicen su funcionamiento.

Para ello se deben desarrollar las acciones siguientes:

- Comprobar los parámetros básicos de configuración de la red

Esta acción está orientada a que los usuarios realicen, de manera correcta, la configuración de la tarjeta de red de la estación de trabajo, de manera tal que les permita disfrutar de los servicios a los que tienen acceso, así como de los parámetros del navegador web que le permitan hacer uso del servicio de navegación de manera óptima.

- Proponer alternativas de mejoras

Basadas en los resultados obtenidos de la etapa de análisis, se realizan propuestas de mejoras enfocadas en las deficiencias detectadas en los servicios y dispositivos monitorizados.

Etapa V. Informe final

Objetivo: facilitar, a los administradores de la red y al personal autorizado, la documentación obtenida de las etapas anteriores, que favorezca la toma de decisiones.

Esta información incluye:

- Reportes obtenidos durante el análisis

- Gráficas que describen el comportamiento de la red

- Muestras de tráfico

- Conclusiones y recomendaciones

El objetivo del procedimiento consiste en ejecutar las propuestas de mejora y, en correspondencia con los resultados obtenidos, realizar tantas iteraciones como sean necesarias hasta lograr la optimización de la red.

Las principales variaciones respecto al procedimiento original han sido introducidas para lograr adaptarlo al objetivo de la presente investigación, ya que su alcance rebasa al del objetivo propuesto. Algunas etapas se fusionaron por la similitud de las acciones a desarrollar y determinadas acciones se omitieron por considerarse parte de otras en la misma o en diferentes etapas. La información suministrada al cliente final (documentos entregables, ver Anexo IV) en el procedimiento de Raytel es parte del informe final presentado en la etapa V del procedimiento propuesto. En la Tabla IV se muestra una comparación entre las etapas de la metodología de Raytel y el procedimiento propuesto para la Red UHOLM.

Tabla IV Comparación entre el procedimiento para el diagnóstico de redes de la empresa RAYTEL y el propuesto en esta investigación

Procedimiento RAYTEL	Procedimiento Red UHOLM
No. Etapa / Acciones	**No. Etapa / Acciones**

1. Levantamiento de información	I. Estudio inicial
Entrevistas. Recolección de documentación.	Recolectar la documentación técnica de la red. Detectar los sistemas operativos en las estaciones de trabajo y servidores. Entrevistar a usuarios y administradores de la red.
2. Mapeo de la red	
Descubrimiento de dispositivos en la red. Reconocimiento de equipos interesantes en la red. Detección de sistemas operativos en las máquinas interesantes. Recolección de datos de la red.	
3. Instalación de las herramientas de monitoreo	**II. Monitorización**
Puesta en funcionamiento de los indicadores de gestión. Puesta en operación del sistema. Toma de muestras.	Seleccionar los servicios y parámetros a analizar. Poner en operación las herramientas. Tomar muestras.
4. Análisis de red de datos	**III. Análisis de la red**
Caracterización de red. Diagnóstico de tráfico.	Caracterizar la red. Estudiar el tráfico.
5. Análisis de seguridad (servidores críticos)	**IV. Diagnóstico**

<table>
<tr><td>Ubicación de equipos y servicios.
Ejecución de pruebas de vulnerabilidades.
Diagnóstico de vulnerabilidades.</td><td>Comprobar los parámetros básicos de configuración de la red.
Proponer alternativas de mejoras.</td></tr>
<tr><td>6. Retroalimentación de la información obtenida</td><td>V. Informe final</td></tr>
<tr><td>Preinforme técnico (presentación de resultados).
Presentación del informe sobre el estado actual de la red.</td><td rowspan="3">Facilitar al personal encargado:
Reportes obtenidos durante el análisis.
Gráficas que describen el comportamiento de la red.
Muestras de tráfico.
Conclusiones y recomendaciones</td></tr>
<tr><td>7. Informe que resume el estado de los componentes de la red y especialmente el estado de los servicios que presentan fallas</td></tr>
<tr><td>Reportes obtenidos durante el análisis.
Gráficas que describen el comportamiento de la red.
Muestras de tráfico.
Matriz de hallazgos y recomendaciones de seguridad lógica.
Conclusiones y recomendaciones.</td></tr>
</table>

Sin embargo, el principal aporte es la definición formal de un procedimiento, con objetivos en cada una de sus etapas y una argumentación de las acciones a

desarrollar en ellas. A diferencia del servicio de análisis y diagnóstico de redes de Raytel, que sólo define etapas y acciones, sin especificar los objetivos y dejar claras las acciones, el objetivo propuesto para la Red UHOLM respeta la definición de procedimiento y estructura adecuadamente los pasos a seguir para diagnosticar la red estudiada.

Una vez creado el procedimiento se procedió a su aplicación en la institución para la cual fue desarrollado. Los próximos epígrafes se centran en las acciones desarrolladas en cada una de las etapas de éste.

2.2 Estudio Inicial

Las acciones desarrolladas en la etapa de Estudio inicial están, básicamente, descritas en el Epígrafe 1.4 (Estado general de la red informática de la Universidad de Holguín “Oscar Lucero Moya”). Se partió de su estructura, representada mediante el esquema de la red y la descripción de sus componentes, así como de la documentación de autoriza la explotación de la red y el empleo de dispositivos inalámbricos. Por último, la aplicación de encuestas a usuarios y entrevistas a administradores de red permitieron conocer las principales insatisfacciones de los usuarios y posibles propuestas de mejoras que son analizadas en etapas posteriores del procedimiento.

2.3 Monitorización

En esta etapa se procedió a seleccionar las herramientas que, a consideración del autor, fueran factibles para la obtención de los datos que se analizaron, instalar y (o) ejecutar el software seleccionado, solicitar trazas de los servicios que más inconformidades provocan en los usuarios y almacenar toda la información que pudieran ser relevante para la siguiente etapa del procedimiento.

En un principio se realizó la monitorización del tráfico local. Para ello se aplicaron herramientas en los diferentes segmentos que componen la LAN, detectando los concentradores o conmutadores a los que se conectan las estaciones de trabajo y

luego se comprobó el acceso a los dispositivos que constituyen frontera entre la red local y la WAN. Para desarrollar la actividad fue muy útil contar con el esquema actualizado de la red que permitió determinar la localización de los dispositivos y la distribución por niveles en la red. La actualización del esquema de la red fue muy necesaria para comprender las modificaciones que se han realizado; en el período que ha transcurrido desde que se inició esta investigación han sido adicionados varios dispositivos que han mejorado la infraestructura existente.

Para descartar problemas de configuración se seleccionaron varias estaciones de trabajo ubicadas en diferentes locaciones de la Universidad de Holguín y se comprobó, mediante ***ipconfig*** o ***ifconfig***, la correcta elección de los parámetros de configuración de la tarjeta de red. Al estar presente en todos los sistemas operativos que se emplean en la red estudiada no fue necesario instalar esta utilidad, solo ejecutar la acción y preservar los datos para su análisis.

Una de las herramientas utilizadas para el chequeo de disponibilidad fue el comando ***ping***. Este comando permitió obtener el tiempo mínimo, tiempo máximo, tiempo promedio y desviación estándar de los valores anteriores, en que un paquete ICMP demora en contactar un host específico. Se realizaron pruebas para el acceso a estaciones de trabajo conectadas al mismo dispositivo de interconexión, conectadas a dispositivos en otros niveles, a los servidores de los dominios a los que pertenecen, a los servidores centrales y a la puerta de enlace predeterminada. Estos datos se almacenaron y se exportaron a hojas de cálculo para su posterior procesamiento. Se realizó el mismo procedimiento para comprobar la conectividad con algunos dominios de la red externa. Para descartar problemas de DNS se realizó ping tanto a los nombres de host como a las direcciones IP de dichos hosts.

Otra de las herramientas de chequeo de disponibilidad empleadas fue ***traceroute*** con la finalidad de determinar el lugar en que los paquetes se pierden, en aquellos casos en que el comando ping falló en el intento por alcanzar al servidor deseado.

La especificación –n, que no requiere la resolución de nombres mediante el protocolo DNS, fue introducida para realizar este proceso a mayor velocidad.

El comando ***mtr***, del programa My TraceRoute, fue ejecutado para evaluar el resultado obtenido del empleo de ping y traceroute. De la información obtenida de las utilidades anteriores se compararon las estadísticas con las ofrecidas por esta herramienta. La Figura 10 presenta el comando en ejecución.

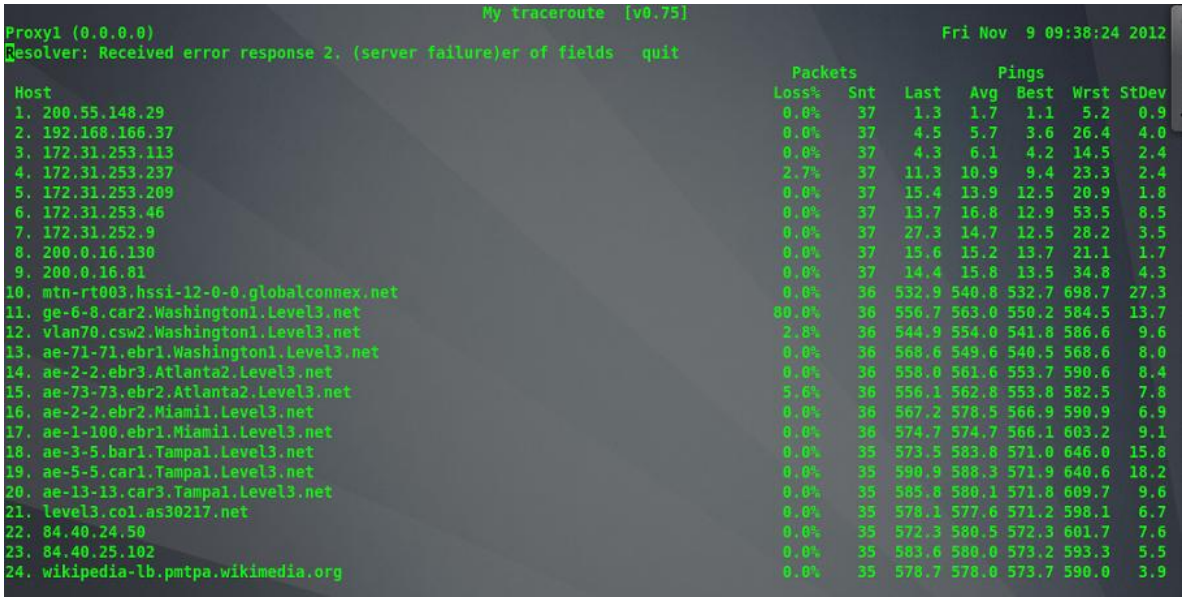


Figura 10 Aplicación de My Traceroute – mtr a www.wikipedia.org

Aunque se valoró la posibilidad de instalar analizadores de protocolos como ***ntop*** y ***Wireshark*** se presentó el inconveniente de que no se tenía acceso a los dispositivos y servidores por los que circula el mayor volumen de tráfico de la red. El empleo de una máquina virtual, a pesar de que hubiera eliminado la limitación de la carencia de privilegios administrativos, no hubiera permitido recrear las condiciones reales de la red. Su instalación hubiera supuesto, además, una carga más para una red ya sobrecargada. De todas maneras, es necesario aclarar que son herramientas útiles a la hora de determinar situaciones muy específicas.

Para el control de la disponibilidad de dispositivos y servicios en tiempo real se empleó ***Nagios***, en su versión 3.2.1 de marzo de 2010, teniendo en cuenta las

quejas recurrentes de los usuarios acerca de las interrupciones que se presentan al momento de acceder a algún dispositivo en la red.

A la herramienta se accedió mediante el URL *http://10.26.0.31/nagios3/*. Su empleo estuvo orientado a determinar el estado de los servicios de red y de los recursos de hardware. Se eligió porque alerta de manera oportuna sobre la paralización de cualquier servicio de la red y notifica al administrador cuando el problema ha sido resuelto. Además, permite visualizar la red de forma jerárquica, lo cual ayuda a determinar los dispositivos cuyo mal funcionamiento influiría en la comunicación entre diferentes áreas de la universidad. La Figura 11 muestra la opción Mapa de Estado de la herramienta Nagios para los dispositivos monitorizados en la Red UHOLM.

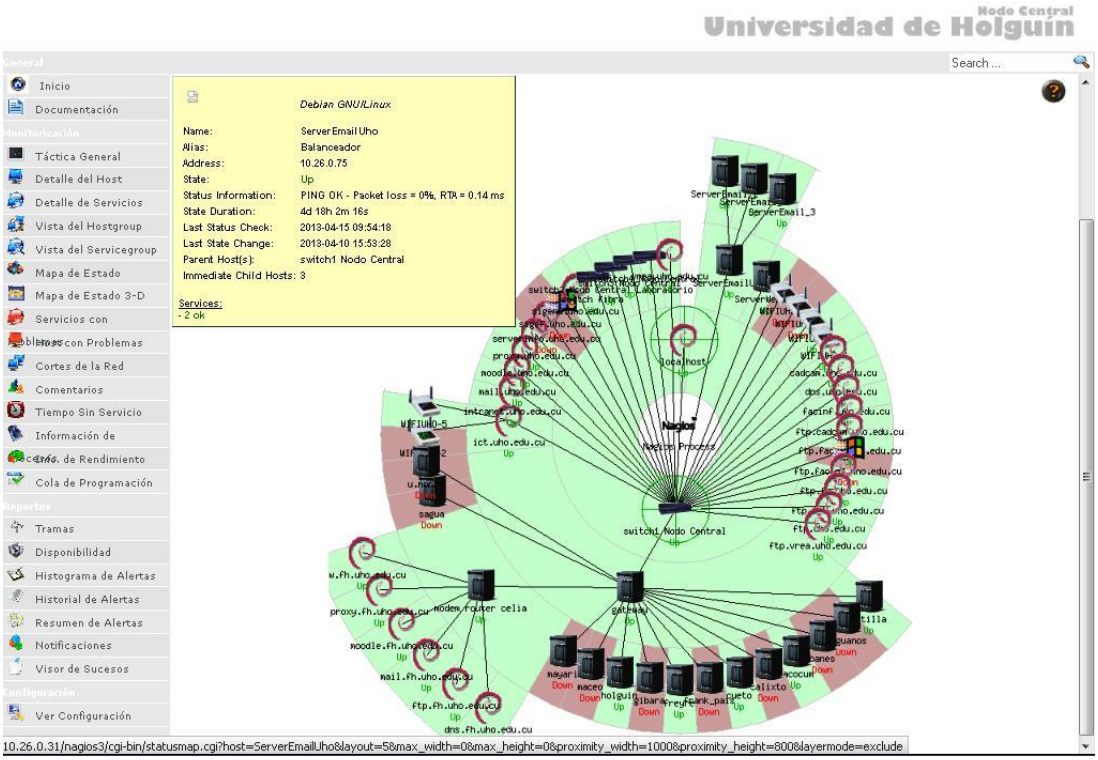


Figura 11 Nagios mostrando el Mapa de Estado de la Red UHOLM

La monitorización del tráfico externo se basó en comprobar que el ancho de banda que emplea la institución es el que realmente ha sido contratado al proveedor de

servicios de Internet. Este tráfico puede ser monitorizado mediante el empleo de ***MRTG*** en algún dispositivo que emplee SNMP, como en enrutadores o en servidores con IP reales conectados directamente a Internet.

Considerando que el mayor número de insatisfacciones respecto a la calidad de los servicios está dirigido al servicio de navegación en Internet se decidió su monitorización. La herramienta MRTG, en su versión 2.16.3 y disponible en *http://10.26.0.10:81/mrtg/eth3/*, se empleó para estudiar el comportamiento del servidor proxy. Su configuración está limitada a mostrar el tráfico entrante y saliente en el día, en el último mes y en el año, y no se pudo obtener otra información relevante como el uso de la CPU, el consumo de memoria y demás estadísticas de interés. La Figura 12 así lo demuestra.

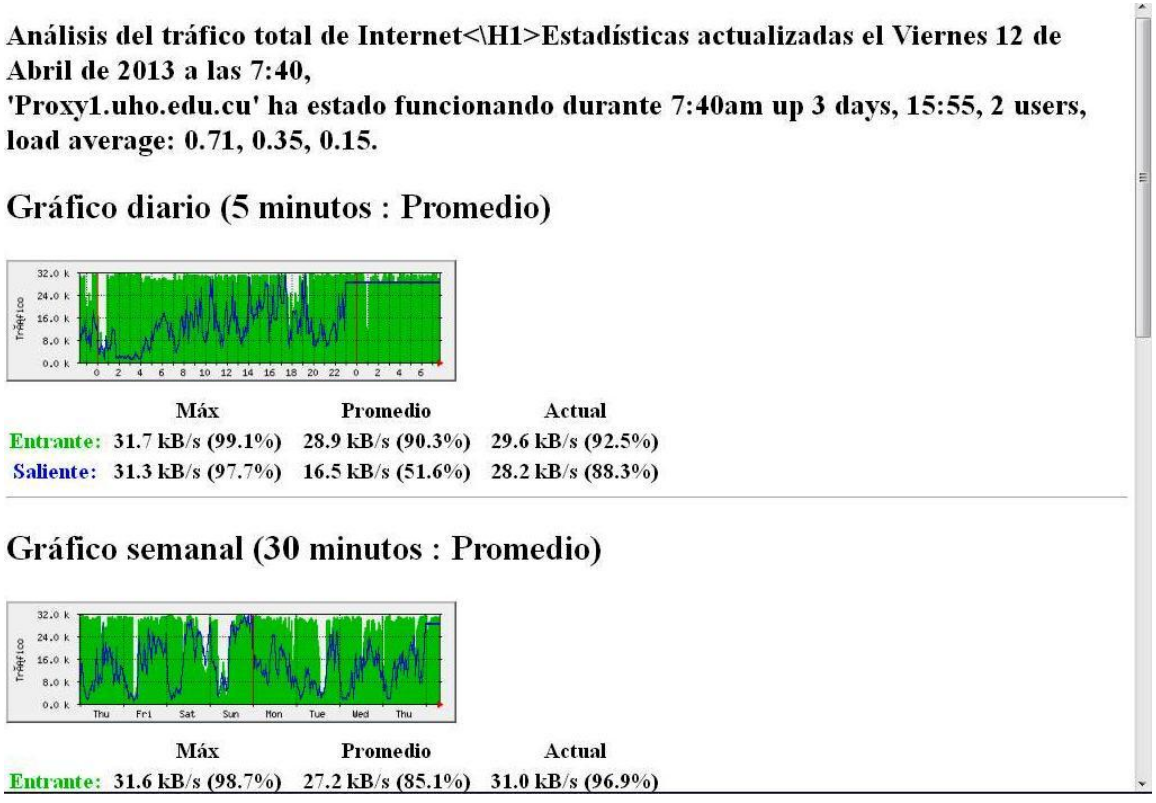


Figura 12 Visualización del tráfico entrante y saliente de la Red UHOM mediante MRTG

Cacti pudo haber sido una opción mucho más atractiva para graficar y monitorizar los parámetros con los que trabaja MRTG; sin embargo, su mayor consumo de recursos y su compleja configuración inclinaron la balanza a favor de MRTG.

Se solicitó al administrador de la red los registros del servicio de navegación en Internet. La Red UHOLM emplea ***Squid*** como servidor proxy y que genera logs de acceso y de uso y almacenamiento en la caché. Se instaló ***Sawmill*** para el procesamiento de los registros en la siguiente etapa del procedimiento y su comparación con los datos obtenidos con otra herramienta, desarrollada en pitón, que permite obtener diferentes campos del fichero access.log de forma ordenada.

También fueron útiles ***MailGraph***, para visualizar el comportamiento de la mensajería a través del correo electrónico y ***BindGraph***, que muestra las peticiones realizadas al servidor DNS, ambas muy parecidas a MRTG y que empelan RRDTool para la graficación de los datos. ***SARG*** se empleó para obtener estadísticas de la navegación en Internet y comparar los resultados que ofrece Sawmill.

Respecto a la infraestructura de la red inalámbrica, en la actualidad se realiza un estudio, con la participación de un estudiante de tercer año de Ingeniería Informática de la Universidad de Holguín y la colaboración de dos estudiantes de cuarto año de Ingeniería en Sistemas Computacionales de la Universidad Autónoma de Tamaulipas, México. El trabajo desarrollado se basa en medir la intensidad de la señal de los puntos de acceso en la sede Oscar Lucero Moya, con el objetivo de desarrollar un mapa que refleje la cobertura existente y proponer, en caso de ser necesario, la reubicación de los dispositivos inalámbricos.

Esta etapa del procedimiento produjo alrededor de 2Gb de información, la mayor parte de ella correspondiente a registros del servidor proxy 10.26.0.10, del que se obtuvieron los ficheros access.log compactados correspondientes a noviembre de 2011 y a abril, mayo, junio, julio, agosto y septiembre de 2012. El resto de los datos, que contienen los resultados de la aplicación de los comandos ping, tracert

y mtr, fueron almacenados en archivos de texto con extensión txt o mediante la captura de pantallas del sistema. Este último fue ejecutado desde el propio servidor proxy, para obtener las estadísticas más cercanas posibles al comportamiento real de la conectividad con los dominios más solicitados.

2.4 Análisis

En la presente etapa se procedió a seleccionar muestras de los datos obtenidos de la etapa de monitorizar.

Se analizó la configuración de la tarjeta de red de varias estaciones de trabajo. Se emplearon los datos de al menos una estación de trabajo de los locales desde donde se ejecutó el comando ***ipconfig***/***ifconfig***: Departamento de Matemática, Departamento de Redes, Decanato de la Facultad de Informática y Matemática, Nodo de la Facultad de Ingeniería, Planificación Docente de la Facultad de Ingeniería Industrial, Laboratorio de Redes, Laboratorio Docente de Informática y Vicerrectoría Económica.

Los resultados obtenidos muestran problemas en la configuración de la máscara de red y en los servidores DNS (primario y secundario) de casi la mitad de las estaciones de trabajo. Esta situación no se limita únicamente a la muestra analizada, sino que se evidencia en las laptops de los usuarios que se conectan a la red y que en ocasiones inhabilitan el acceso de determinada computadora a los servicios al generar un conflicto IP debido al empleo de forma aleatoria de una dirección IP sin previa consulta con los administradores de la red.

Desde esas mismas estaciones de trabajo se ejecutó el comando ***ping*** teniendo como objetivo diferentes servidores del nodo central. En todos los casos se obtuvieron tiempos de respuesta promedio (RTA, por sus siglas en inglés) acordes a la tecnología y a las características de la Red UHOLM, que fluctuaron entre 0.15 ms y 0.32 ms y una pérdida de paquetes del 0%, lo cual no necesariamente significa que la red tenga un comportamiento estable y no descarta, por el momento, que los dispositivos de interconexión sean los

responsables del funcionamiento ineficiente de la red.

La información obtenida de ***tracert*** se empleó casi en su totalidad, pues desde un inicio se definieron los dominios a los que se pretendía acceder. Los resultados muestran problemas en los saltos hacia el destino analizado en determinadas ocasiones, mientras que en otras se accede perfectamente al dominio. Para todos los casos analizados los paquetes se pierden en dispositivos fuera del dominio de la Red UHOLM. Esta situación de intermitencia se corresponde más con problemas de cableado y de funcionamiento de los dispositivos, que debido a configuraciones ineficientes.

Los resultados de ***mtr*** se emplearon en su totalidad. La herramienta mostró resultados muy similares a los de tracert. En la Figura 13 se observa inestabilidad en el acceso a uno de los dominios más visitados.

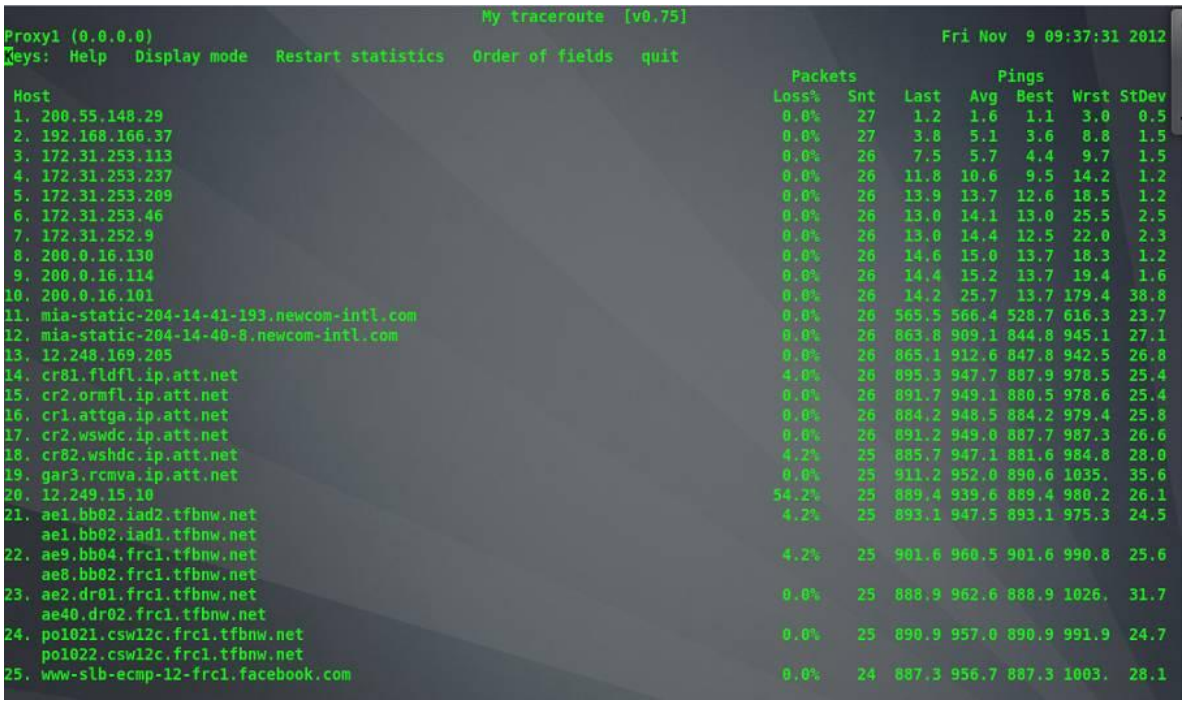


Figura 13 Resultados de la aplicación de My Traceroute – mtr a www.facebook.com

En la ruta a *facebook.com* y a *wikipedia.org*, para algunos periodos analizados, existe una pérdida de paquetes considerable en enrutadores extra fronteras. En el primero de los casos la dirección 12.249.15.10, perteneciente a Estados Unidos, provoca una pérdida del 50% de los paquetes enviados desde el origen.

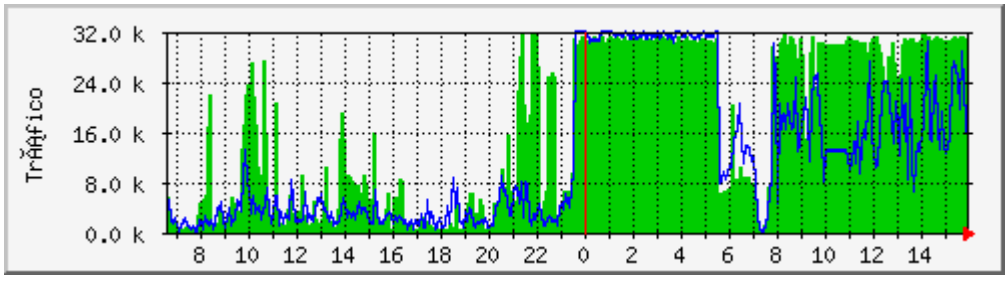
Con ***Nagios***, además de comprobar la disponibilidad de los dispositivos y servicios, se compararon los resultados obtenidos de la ejecución del comando ***ping***. La información acerca del tiempo de respuesta y la pérdida de paquetes se corresponden en ambos casos. En varios dispositivos se detectó pérdida de paquetes, incluso de más de un 50%, en varias de las muestras tomadas, lo cual reveló la inestabilidad de la que se quejan los usuarios. Los dispositivos inalámbricos son los que muestran mayor inestabilidad en su disponibilidad y mayor variación en sus tiempos de respuesta. El acceso a las FUM se torna también bastante inestable y sus tiempos de respuesta son muy superiores al resto de las ubicaciones de la Red UHOLM; en el período analizado se detectaron enlaces casi inoperativos o con una actividad muy pobre. Los resultados de este análisis se muestran en la Tabla V.

Tabla V Pérdida de paquetes y tiempos de respuesta para algunos hosts de la red

Host	Pérdida de paquetes (Packet loss)	Tiempo de respuesta promedio (RTA)
ServerEmailUho	0%	0.15 ms
ftp.facing.uho.edu.cu	0%	0.25 ms
WIFIUHO-2	0%	12.54 ms
WIFIUHO-5	0%	3.54 ms
antilla	0%	46.65 ms

calixto	0%	57.10 ms
dns.fh.uho.edu.cu	50%	1251.06 ms
moodle.fh.uho.edu.cu	50%	1032.73 ms

La Figura 14 muestra el comportamiento del tráfico entrante y saliente mediante el proxy de la Red UHOLM a través de ***MRTG***. Las imágenes corresponden a días seleccionados de forma aleatoria entre la muestra obtenida. En este caso se muestra un uso extensivo del canal en el horario de la madrugada, aunque la tendencia es a emplear mayoritariamente el canal en horario laborable y hacer menos uso del mismo en el horario de la noche y de la madrugada, lo cual se aprecia mejor en el gráfico de la Figura 15.



	Máx	Promedio	Actual
Entrante:	31.8 kB/s (99.5%)	16.1 kB/s (50.4%)	30.7 kB/s (96.0%)
Saliente:	32.0 kB/s (99.9%)	12.0 kB/s (37.4%)	14.4 kB/s (45.1%)

Figura 14 Tráfico de Internet en la Red UHOLM. Jueves 2 de mayo de 2013

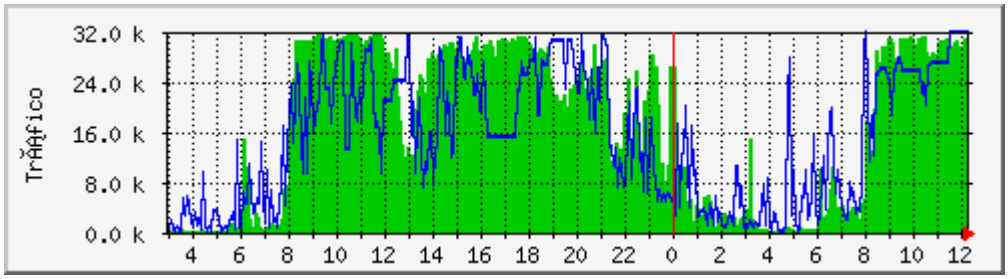


Figura 15 Estadísticas del tráfico de Internet en el servidor proxy de la Universidad de Holguín. Martes 6 de noviembre de 2012 – 12:15 pm

El tráfico de la semana, como se puede observar en la Figura 16, delinea perfectamente la situación: un tráfico entrante ligeramente superior al saliente y la tendencia descrita anteriormente de subutilizar el canal en el horario de la madrugada, lo cual se aprecia en caídas de hasta menos de 3 Kbps, mientras que en el horario comprendido entre las 8:00 am y las 11:00 pm el tráfico alcanza máximos de hasta 99.99% de uso del canal.

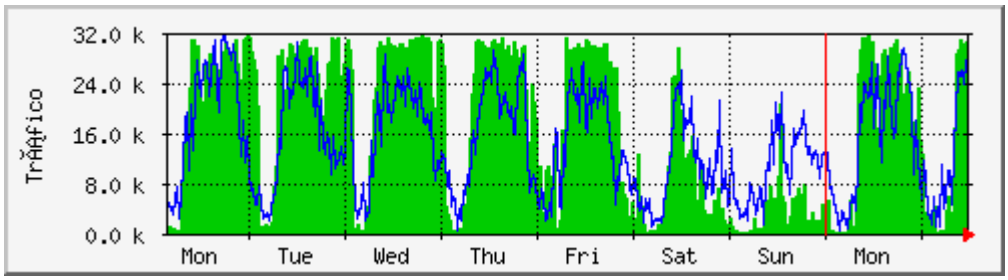


Figura 16 Estadísticas del tráfico de Internet en el servidor proxy de la Universidad de Holguín. Lunes 29 de octubre de 2012 – 6 de noviembre de 2012

La observación de los gráficos que genera MRTG mostró un resultado sorpresivo: la velocidad de conexión a Internet es 256 Kbps, el doble de la contratada. Para comprobar este resultado se emplearon, además, herramientas disponibles en Internet, sitios que se dedican a calcular la velocidad con la que se accede a ellos (*www.speedtest.net* , *www.bandwidthplace.com*, *www.velocidad.info*) y reportaron cifras superiores a los 128 Kbps, lo cual demuestra que los resultados del MRTG

no fueron erróneos. En la Tabla VI se relacionan los resultados de las pruebas realizadas.

Tabla VI Resultados obtenidos en las pruebas de velocidad realizadas

Prueba	Download	Upload
www.speedtest.net	166 Kbps	220 Kbps
www.bandwidthplace.com	129 Kbps	181 Kbps
www.velocidad.info	0.1 Mbps = 102.4 Kbps	0.2 Mbps = 204.8 Kbps
MRTG	14.4 KB/s = 115.2 Kbps	30.7 KB/s = 245.6 Kbps

Una comparación del comportamiento del servidor proxy de la Red UHOLM con el de la Dirección de Información Científico – Técnica de la Universidad de La Habana revela las carencias en cuanto a capacidad del canal. Mientras que la red estudiada muestra un tráfico que satura el canal disponible en el horario laborable, en la segunda se aprecia una holgura a la hora de navegar teniendo en cuenta que multiplican por cuatro el ancho de banda de la Red UHOLM y pueden aplicar técnicas de manejo eficiente del ancho de banda como las delay pools. Los gráficos que se muestran en las Figuras 17 y 18, obtenidos del sitio de monitorización del proxy de la institución que se está comparando y correspondientes a la herramienta MRTG, muestran que no existe tráfico en el horario de la madrugada, probablemente por desconexión de los servicios, y la existencia de delay pools para repartir el canal entre los usuarios que lo demanden.

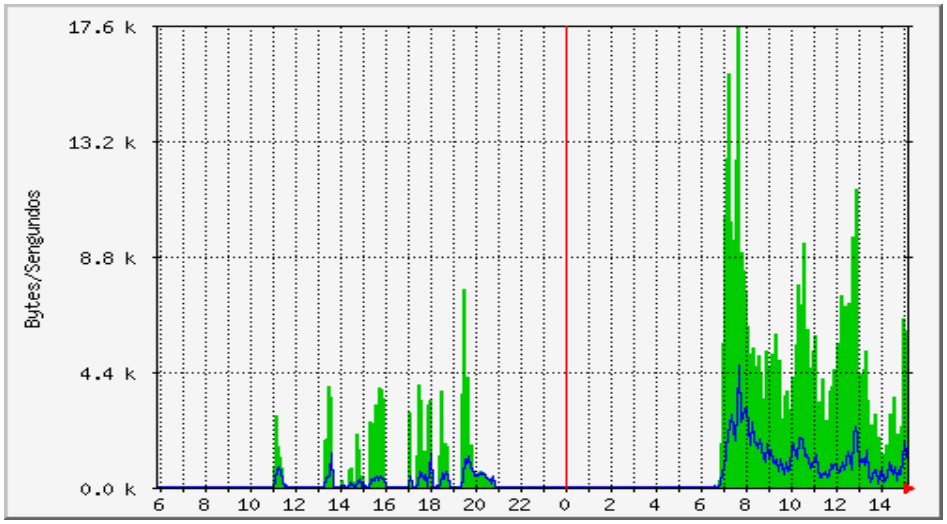


Figura 17 Estadísticas del tráfico de Internet en el servidor proxy de la Dirección de Información Científico – Técnica de la Universidad de La Habana. Lunes 29 de octubre de 2012 – 3:10 pm

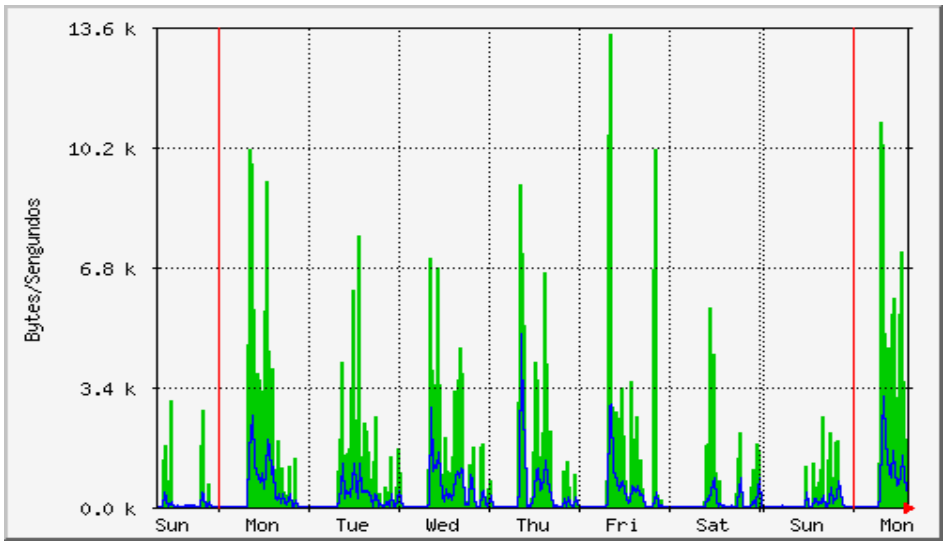


Figura 18 Estadísticas del tráfico de Internet en el servidor proxy de la Dirección de Información Científico – Técnica de la Universidad de La Habana. Domingo 21 de octubre de 2012 – Lunes 29 de octubre de 2012

MailGraph y ***BindGraph*** confirmaron la tendencia descrita anteriormente acerca de los horarios de uso de la red con mayor frecuencia pues tanto el envío de

mensajes como la solicitud transacciones de dominio fueron acciones presentes en mayor medida en horario laborable. ***SARG*** permitió comparar los resultados obtenidos del fichero acces.log del servidor proxy Squid y procesados por la herramienta personalizada creada para la obtención de los campos a analizar y el analizador de logs profesional Sawmill. Aunque en posiciones distintas, esta comparación mostró correspondencia entre los sitios más visitados en la Red UHOLM.

En julio de 2012, la Red UHOLM contaba con 322 usuarios y un poco más de 200 computadoras para acceder al servicio de navegación en Internet. Para lograr un aprovechamiento equitativo del ancho de banda asignado, la Dirección de Informatización distribuyó a los usuarios, en dependencia del área a la que pertenecen, en grupos para acceder al servicio de navegación en Internet, quedando conformado el horario de acceso a Internet que se muestra en la Figura 18, en el que quedan definidos las áreas y el tiempo que dispondrán del servicio.

Recientemente, por reclamos de los usuarios, se logró que el acceso al servicio fuera posible desde cualquier estación de trabajo de la red y no desde las asignadas al área. También se amplió el tiempo en que los estudiantes pueden disfrutar del servicio, aprovechando su menor uso en el horario de la noche, y se brindó el servicio a los usuarios con acceso remoto a partir de las 4:00 am y hasta las 7:00 am, dando uso al canal en un horario en el que permanecía con muy baja ocupación. Estas modificaciones han provocado cambios en el tráfico de la Red UHOLM, logrando una distribución más homogénea del canal en el transcurso del día, y ha beneficiado a los usuarios con acceso remoto que no disponían del servicio con anterioridad.

HORARIO							
Hora	**Lunes**	**Martes**	**Miércoles**	**Jueves**	**Viernes**	**Sábado**	**Domingo**
8:00 am a 12:30 pm	Fac. Ing	Fac. Hum. Derecho y C. Sociales	Fac. Ind.	Fac. Inf.	Fac. Eco.	Est. Inf.	FUM
	C.E.	VRU	Dpto. Cul.Fis	Dpto. Def.	Dpto. Ext.	FUM	
	VREA		C.E.	Sec. Gral.	C.E.		
			VRIPG		VRD		
12:30 pm a 6:00 pm	Fac. Ind	Fac. Inf.	Fac. Eco.	Fac. Ing.	Fac. Hum. Derecho y C. Sociales	FUM	FUM
	Dpto. Cul.Fis.	Dpto. Def.	Dpto. Ext.	VREA	VRU		
	VRIPG	C.E.	VRU				
		Sec. Gral.					
6:00 pm a 12:00 am	Est. Ind.	Est. Inf.	Est. Eco.	Est. Ing.	Est. Hum. Derecho y C. Sociales	FUM	FUM
11:00 pm a 12:00 am	Doctores	Doctores	Doctores	Doctores	Doctores	Doctores	Doctores
12:00 am a 4:00 am	Doctores	Doctores	Doctores	Doctores	Doctores	Doctores	Doctores
4:00 am a 7:00 am	Accesos Remoto	Accesos Remoto	Accesos Remoto	Accesos Remoto	Accesos Remoto	Accesos Remoto	Accesos Remoto

Figura 19 Horario de Internet de la Red UHOLM

Mediante las pruebas realizadas se ha podido determinar que la principal limitación en el servicio de navegación es el insuficiente ancho de banda, que no está en correspondencia con la cantidad de usuarios que emplean el servicio en los horarios establecidos. Ha quedado comprobado que cuando el número de usuarios es bajo las insatisfacciones disminuyen. Por esta situación se decidió priorizar, para este análisis, los parámetros correspondientes al tráfico de bytes en el servidor proxy.

2.4.1 Análisis del fichero access.log

El fichero access.log del Squid fue procesado empleando un código en python que exporta a un fichero csv ciertos parámetros escogidos. Se emplearon dos períodos de 14 días en los que los usuarios de la red deben explotar de forma similar el servicio analizado, del 2 al 15 de noviembre de 2011 y del 1 al 14 de abril de 2012. Ambos corresponden aproximadamente a mediados del primer y segundo

semestre, respectivamente, en los que se puede afirmar que existe una concurrencia bastante alta de estudiantes y profesores y no hay afectaciones planificadas para exámenes, prácticas profesionales u otras actividades, por lo que se puede plantear que ambos períodos son representativos para el estudio que se desarrolla.

Tráfico en bytes y solicitudes

Esta sección está basada la entrada del access.log bytes, sumada para el periodo de una hora de todos los registros de solicitudes que recibe el proxy. La Figura 20 muestra el comportamiento de la cantidad de bytes que Squid recibe y envía ante las consultas de los clientes en el día, mientras que la Figura 21 refleja el número total de solicitudes que recibe Squid para las diferentes horas del día de las semanas analizadas. Como se analizan 14 días de cada periodo, cada barra del gráfico representa la suma de los 14 valores correspondientes a los parámetros analizados (bytes y hits).

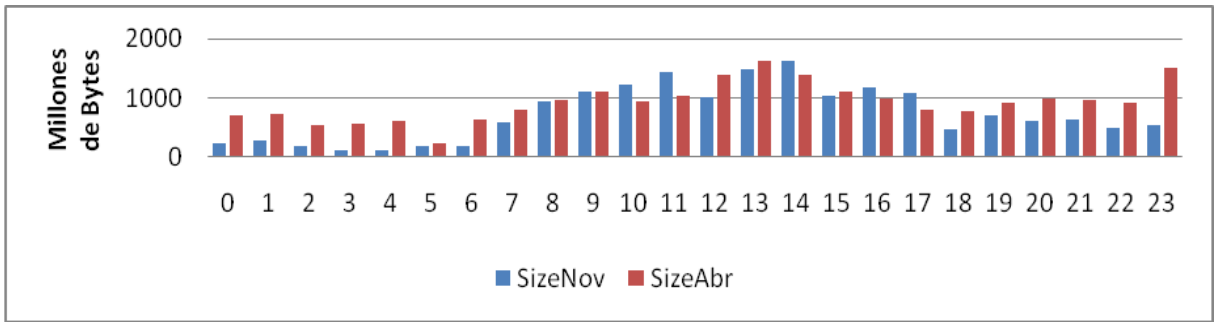


Figura 20 Cantidad de bytes emitidos por Squid por hora del día para los períodos seleccionados

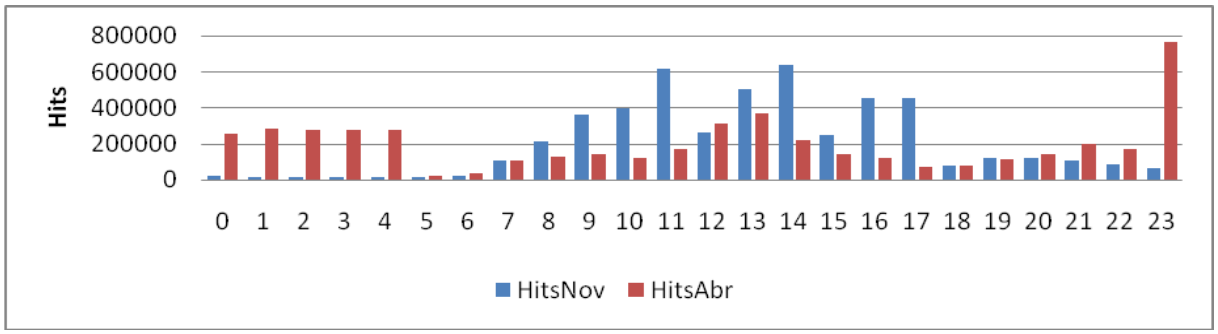


Figura 21 Cantidad de solicitudes recibidas por Squid por hora del día para los períodos seleccionados

Se aprecia un comportamiento en correspondencia con la permanencia de trabajadores y estudiantes en la universidad, pues la mayor concentración del flujo de bytes es en el horario laborable, entre las 8:00 AM y las 5:00 PM. Existen valores máximos similares, 1618906041 bytes en un periodo de una hora en las semanas de noviembre y 1645938559 bytes para las semanas de abril, distribuidos entre la 1:00 PM y las 3:00 PM.

De forma más detallada, el análisis del comportamiento de los horarios de la navegación web muestra un tráfico bastante alto entre las 7:00 AM y las 6:00 PM. De 7:00 AM aproximadamente y hasta las 12:00 M se percibe un incremento gradual, con un descenso entre 12:00 M y 1:00 PM, y ascensos nuevamente a partir de la 1:00 PM, hasta aproximadamente las 3:00 PM. Entre las 3:00 PM y las 6:00 PM se mantiene un tráfico alto, pero no alcanza el de los periodos antes descritos. El horario de la noche muestra un uso medio del proxy, mientras que en la madrugada su empleo es bastante reducido.

En el caso del número de solicitudes, sólo se observan diferencias notables de proporción entre los datos entre las 11:00 PM y las 5:00 AM, determinado, principalmente, por el empleo casi absoluto del servicio por un usuario la noche y madrugada del día 3 de abril.

Para el análisis de los datos se emplearon cuatro estimadores estadísticos, dos de tendencia central (mediana y promedio) y dos de dispersión (desviación estándar y coeficiente de variación). Se prioriza el uso de la mediana porque es más representativa que el promedio en datos tan heterogéneos como los que son objeto de análisis en la presente investigación. La Tabla VII muestra los resultados obtenidos.

Tabla VII Estimadores estadísticos analizados para las variables estudiadas

Estimador	Cantidad de Mb		Hits	
	Nov 2011	Abr 2012	Nov 2011	Abr 2012
Mediana	600	895	114995	155381
Promedio	694	883	205717	199157
Desviación estándar	450	311	205031	150050
Coeficiente de variación	64,8%	35,2%	99,7%	75,3%

Para la cantidad de bytes y las solicitudes se obtuvieron valores de mediana mayores para abril de 2012, lo cual refleja un mayor uso de los servicios de navegación en el segundo periodo. El promedio de solicitudes de noviembre de 2011 fue superior al de abril de 2012 determinado por una alta concentración de éstas en el horario laborable.

El empleo de la desviación estándar permitió definir que existe menor dispersión en los datos referentes a abril de 2012, o lo que es lo mismo que el servidor proxy se empleo de manera más homogénea en las diferentes horas del día. Este era un resultado esperado, ya que en 2011 aún no se había brindado el servicio de acceso a internet en el horario de la madrugada, mientras que para el segundo periodo ya funcionaba el mismo.

Con el objetivo de determinar el comportamiento del tráfico para los días de la semana se filtró la data y se obtuvo como resultado los gráficos que se presentan en las Figuras 22 y 23.

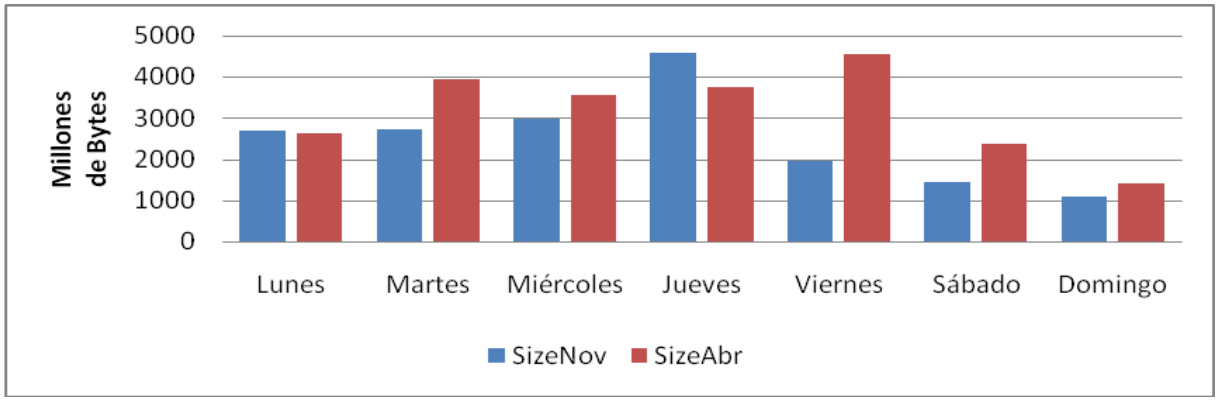


Figura 22 Cantidad de bytes emitidos por Squid por día de la semana para los períodos seleccionados

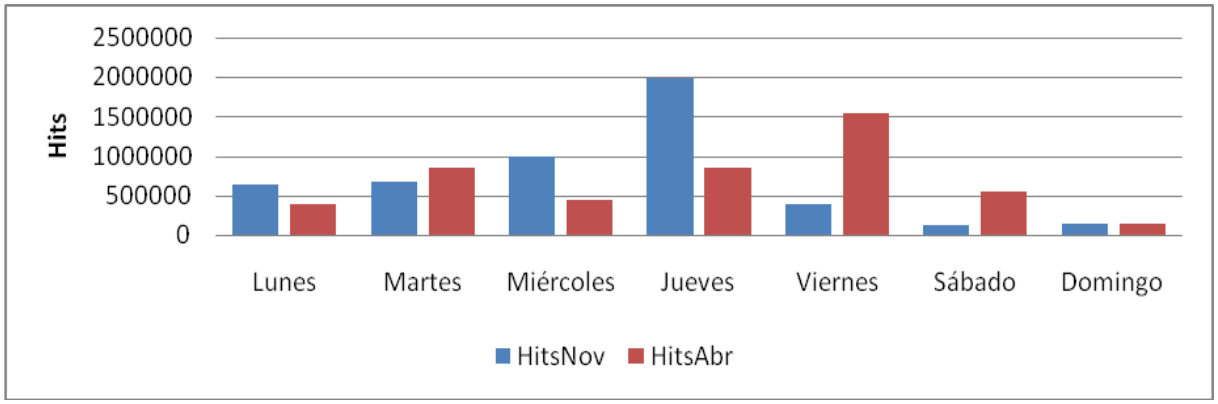


Figura 23 Cantidad de solicitudes recibidas por Squid por día de la semana para los períodos seleccionados

De las figuras se infiere que, según el análisis de tráfico para los días de la semana, sólo existieron valores semejantes en los datos del lunes al comparar ambos periodos, mientras que para el resto de los días no se pudo establecer una correspondencia. De manera general, se puede plantear que no existen días en los que el tráfico sea suficientemente bajo para reubicar a usuarios y liberar un poco el tráfico de otros.

El análisis del comportamiento del tráfico por hora y días de la semana permitirá redefinir, si fuera necesario, el horario de acceso a internet para los grupos de usuarios de la institución.

Dominios

Las Figuras 24 y 25 muestran los dominios más accedidos para ambos períodos analizados. Los resultados se miden en porcientos del total de solicitudes, y aunque los valores no parezcan altos para los primeros lugares, se debe tener en cuenta que se representan los resultados de los 10 primeros dominios entre aproximadamente 14000 solicitudes.

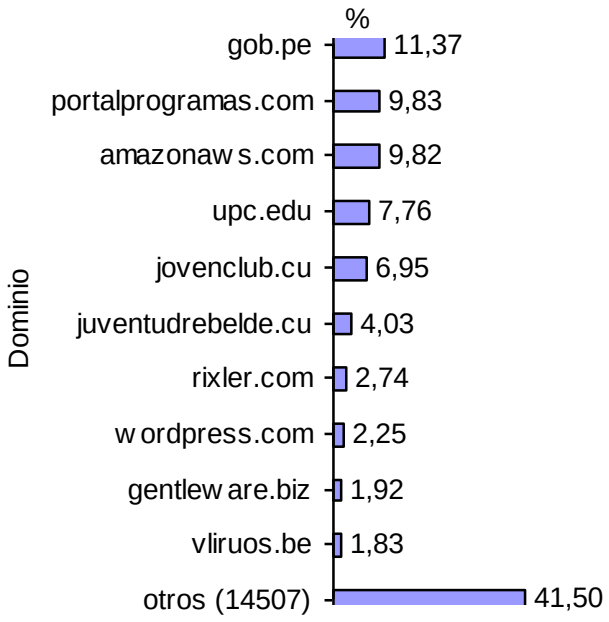


Figura 24 Tráfico web por dominios visitados para el período del 2 al 15 de noviembre de 2011

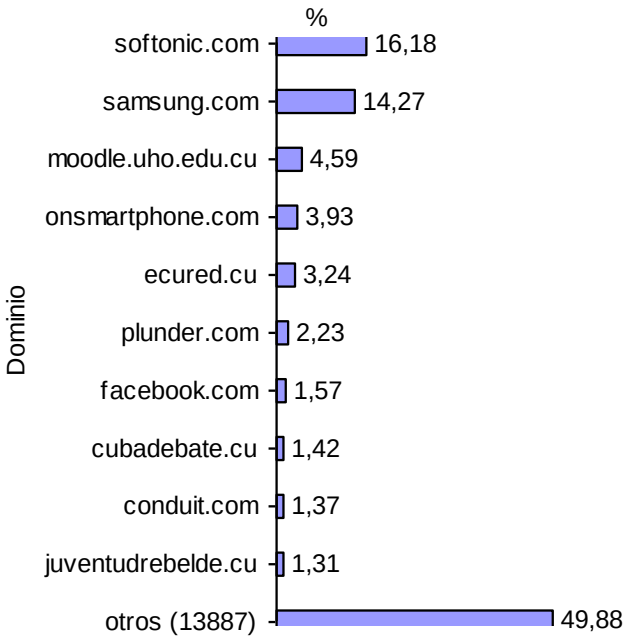


Figura 25 Tráfico web por dominios visitados para el período del 1 al 14 de abril de 2012

Para ambos periodos analizados se destaca la cantidad de solicitudes realizadas a sitios de descarga de software, que en abril ocupa un tercio del total. Con un número considerable de solicitudes se ubica, a continuación, un grupo de sitios nacionales como la enciclopedia Ecured, el portal JovenClub y los de noticias Juventud Rebelde y Cubadebate, los cuales, en términos de tráfico en bytes, representan alrededor del 15% del total.

Para el periodo de abril es relevante la cantidad de solicitudes recibidas desde el exterior de la red local a la plataforma de aprendizaje de la universidad Moodle, sin embargo es más llamativo el hecho de que ocupa el primer lugar del tráfico de bytes con un 30%.

Las tendencias de los usuarios de la Red UHOLM no se corresponden con las tendencias mundiales en cuanto a navegación por dominios pues de los 100 sitios web más populares según Alexa, solo wordpress.com, facebook.com, counduit.com aparecen entre los más populares entre los usuarios de la UHOLM.

Tipos de archivos

En correspondencia con los dominios más visitados se puede apreciar en las Figuras 26 y 27 que la solicitud de archivos de texto son los que generan la mayor cantidad de solicitudes y de tráfico en el servidor proxy.

Los ficheros de aplicación, aunque no reciben tantas solicitudes como los de texto y los de imágenes, representan el 32.34% del tráfico, situación usual al ser archivos de varios MB.

En cuanto a los de imágenes, los porcientos de solicitudes y de cantidad de bytes que ocupan dichas solicitudes son bastantes similares, al ubicarse entre un 15 y un 20%. Los videos y otros ficheros generan el tráfico restante.

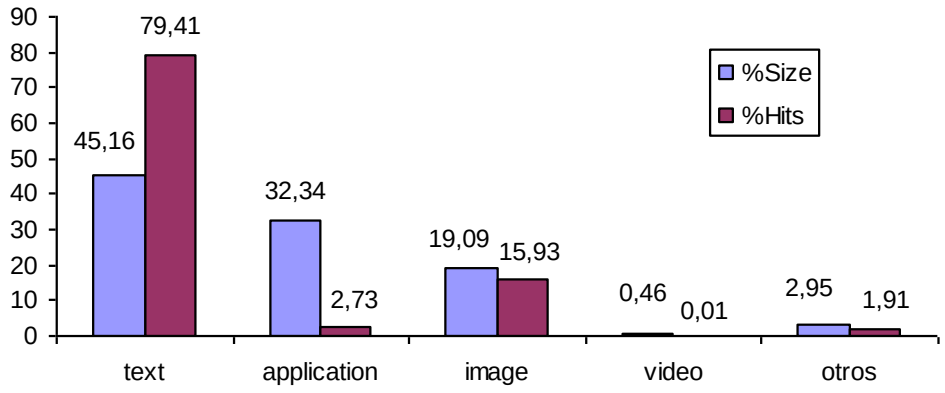


Figura 26 Tipos de archivos por cantidad de solicitudes y de bytes del 2 al 15 de noviembre de 2011

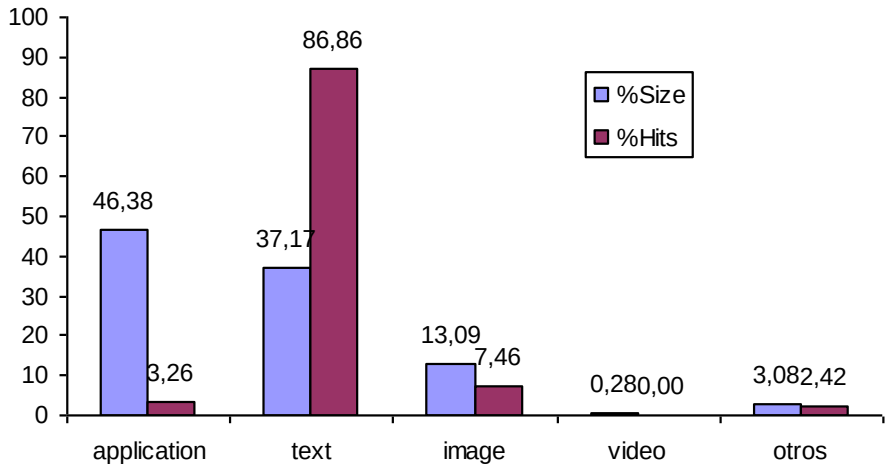


Figura 27 Tipos de archivos por cantidad de solicitudes y del bytes del 1 al 14 de abril de 2012

Respuestas del servidor

El estudio de los códigos de respuesta del servidor para el periodo de abril de 2012 arrojó los resultados que se presentan en los Figuras 28 y 29, en cuanto a los impactos y al nivel de tráfico en la red:

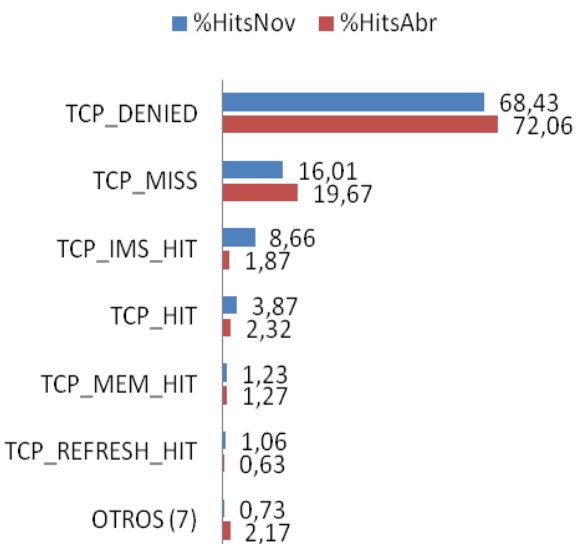


Figura 28 Respuestas de Squid a las solicitudes realizadas en los períodos analizados

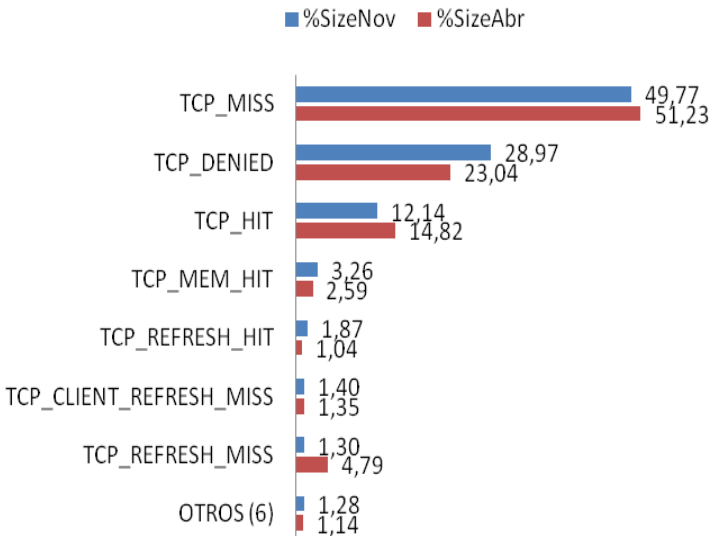


Figura 29 Cantidad de bytes emitidos por Squid como respuesta a las solicitudes realizadas en los períodos analizados

De lo anterior se determina que más del 68% de las solicitudes realizadas al proxy se niegan. Esto está dado por la segmentación del acceso al servicio de

navegación en Internet, lo cual provoca que muchos usuarios realicen peticiones de URL que no pueden ser accedidas en el momento solicitado, por no encontrarse el usuario en el horario en el que tiene autorizado el acceso. En otros casos, en los cuales sí se puede navegar por estar en el horario, sucede que las listas de control de acceso impiden al acceso a determinados sitios por políticas restrictivas o por ser URL que contienen términos no autorizados.

A la hora de analizar la navegación en internet es necesario considerar que ninguna conexión ofrece el 100% del ancho de banda contratado, por lo que no debería ser preocupante si los resultados de las pruebas arrojan resultados que difieran de dicho valor. Los 128 Kbps contratados por la Universidad de Holguín a ETECSA garantizan la descarga de un máximo de 16 KB/seg y no 128 KB como algunos usuarios suelen pensar, que representa 0.016 MB. Esto significa que si en la universidad un usuario dispusiera de todo el ancho de banda para descargar un documento en pdf de 1 MB, el proceso tardaría un minuto y 4 segundos como mínimo, lo cual demuestra las serias limitaciones existentes en la institución para el acceso a Internet, aunque el análisis realizado revela que realmente se navega a 32 KB/seg, velocidad que continúa siendo insuficiente para la cantidad de usuarios que demanda el servicio.

2.5 Diagnóstico

Para diagnosticar correctamente problemas en el funcionamiento de la red es necesario partir de las situaciones más comunes a las que se enfrentan los usuarios, que están relacionadas principalmente con la configuración de los parámetros TCP/IP.

Lo primero que un usuario debe tener en cuenta antes de reportar un incidente de conectividad es comprobar que su adaptador de red está instalado y debidamente configurado. A través del Panel de Control se accede a Conexiones de red para verificar la existencia de alguna tarjeta de red instalada. El hecho de que se disponga físicamente de una no significa que se muestre, pues en la mayoría de

las ocasiones es necesario instalar los controladores para que sea reconocida. En el caso de que ya estén instalados los controladores se mostrará en la ventana el dispositivo de red con el nombre del fabricante. A continuación se deben seleccionar las propiedades de dicha conexión (haciendo clic derecho sobre el icono), elegir el elemento Protocolo Internet (TCP/IP) y presionar el botón Propiedades.

En la ventana siguiente, como se muestra en la Figura 30, quedan definidos los parámetros que establecen la conexión de la tarjeta de red a la red local. Los administradores de la Red UHOLM no han establecido un direccionamiento dinámico, por lo que es necesario configurar manualmente la conexión. En el ejemplo se asigna la dirección IP 10.26.2.90 a la nueva estación en la red. Es necesario que esta dirección haya sido autorizada por el administrador, pues de haber sido seleccionada arbitrariamente se pudiera estar usurpando una dirección previamente en uso y ocasionar un conflicto IP, lo cual provocaría la desconexión de servicios y otros problemas a las estaciones de trabajo que están empleando la misma dirección en la red.

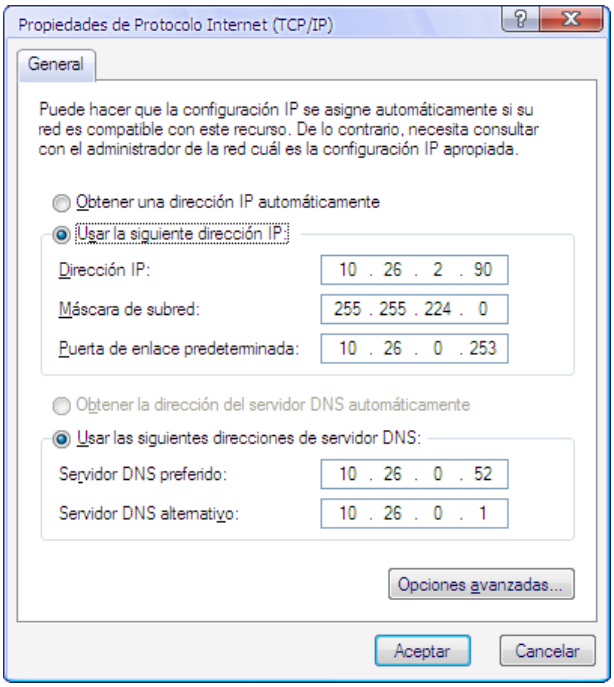


Figura 30 Definición correcta de los parámetros de la Red UHOLM

La máscara de red define el rango de direcciones que se consideran dentro de la subred, las cuales podrán acceder a los servicios a los que están autorizados. Para la Red UHOLM, el rango es 10.26.0.0 – 10.27.31.255, que está subdividido en rangos más pequeños para la distribución de direcciones a las facultades y áreas, regulados por los administradores de los nodos de las áreas. La puerta de enlace predeterminada representa la interfaz por la cual se tiene salida de la red local (generalmente es una interfaz del enrutador) y en el caso particular de la red en cuestión es el 10.26.0.253.

Los servidores DNS cumplen con su función de convertir nombres, mucho más familiares para los usuarios, a direcciones IP para que los protocolos TCP/IP realicen la comunicación. En el caso de que el usuario no configure los servidores DNS no podría acceder al servicio http://correoweb.uho.edu.cu/, aunque puede acceder a través de http://10.26.2.1/.

Una vez determinado que el problema del equipo no es debido a la configuración del mismo, es el momento de emplear el comando ping. Por tanto, lo primero sería hacer ping a la propia dirección IP del ordenador o a la de bucle local 127.0.0.1 Si el ordenador no respondiera a la petición probablemente existe un fallo en la tarjeta, o la configuración TCP/IP debe ser errónea.

Si lo anterior brinda resultados satisfactorios, se debe hacer ping a la puerta de enlace, al servidor DNS o a otro equipo de referencia en la red, preferiblemente a uno conectado al mismo dispositivo de interconexión, lo cual permitirá ir delimitando el alcance del problema.

Si los paquetes de respuesta tienen un tiempo de vida (TTL) inusual pueden existir problemas de enrutamiento entre la computadora y el destino remoto. En caso de que no exista respuesta desde el destino se debe probar con otra dirección, ya que algunos servidores no responden por razones de seguridad. Si no funciona

con el nombre de host, pero sí con la dirección IP, entonces podemos estar en presencia de problemas de DNS.

Otra manera de detectar problemas en la red informática, determinar la causa y llegar a una posible solución, es mediante el empleo de las arquitecturas de red y las funciones de sus capas o niveles, determinando a qué nivel se encuentran las fallas a través del modelo OSI y qué protocolos intervienen en las mismas empleando TCP/IP.

El modelo OSI permite realizar un diagnóstico sistemático en función a los 7 niveles, mientras que el TCP/IP ayuda a determinar los protocolos que intervienen en el proceso de comunicación. [13] Se tomará como ejemplo un incidente para demostrar la utilidad de conocer las funciones de cada una de las capas.

Incidente: “Los trabajadores del Departamento de Computación no tienen acceso al correo electrónico”

Paso 1. Verificar la conectividad de las PC de los usuarios. Para ello se debe emplear el comando *ping* desde la PC hacia la puerta de enlace predeterminada (default gateway, en el caso objeto de investigación 10.26.0.253). Si existiera respuesta se puede concluir que los tres niveles inferiores de OSI funcionan correctamente. De no ser así, se debe revisar la conexión de los cables a la tarjeta de red y a las tomas de usuario y el estado de los dispositivos de interconexión que permiten la comunicación del departamento con el nodo (algún conmutador o concentrador pudiera estar apagado o con cables de comunicación desconectados).

Paso 2. Verificar la disponibilidad del servidor de correo. Para ello se debe emplear el comando *telnet* para acceder al servidor a través del puerto 25 (el protocolo SMTP emplea este puerto para las comunicaciones). Si no existiera respuesta se puede concluir que el servidor de correo no está funcionando correctamente.

Paso 3. Revisar el servidor de correo. Esta acción es ejecutada por los administradores de la red. Se concluye que el problema radica en el nivel de aplicación.

Los usuarios de la red deberían dominar los dos primeros pasos enumerados anteriormente para determinar si el problema al que se enfrentan tiene solución a su alcance, o si es necesario reportarlo al personal informático encargado de la red.

Son varios los factores que pueden influir en el tráfico de la red y por tanto sus patrones de comportamiento estarán en correspondencia con estos. El más influyente es el ancho de banda disponible para el acceso a Internet que pudiera ser suficiente o no en dependencia del siguiente factor: el número de usuarios que emplean el servicio de navegación. Otro elemento relevante, en el caso de la red informática de la Universidad de Holguín, es la existencia de políticas de restricción de acceso a servicios, limitación de navegación por horarios y estaciones de trabajo, y el empleo de cuotas de navegación, por sólo citar algunas. El estado de la red también influye, en gran medida, en los resultados que se obtienen del uso de las herramientas de monitorizar, así como el nivel de capacitación de los usuarios que emplean los servicios y el grado de competencia del personal que administra el hardware y software de red.

Como se planteó en los fundamentos teóricos, el cableado estructurado origina gran parte de los problemas que pueden afectar a una red informática. A continuación se realiza una valoración del impacto que posee el mismo en el funcionamiento de la red que se estudia.

Las deficiencias detectadas en etapas anteriores del presente procedimiento relacionadas con elementos de cableado estructurado han sido corregidas en parte en el periodo en el que ha transcurrido la presente investigación por lo que el impacto negativo que podía traer para el funcionamiento de la Red UHOLM ha disminuido. La Dirección de Informatización realizó la instalación de canaletas y

señalización de las conexiones a los conmutadores y concentradores para una rápida detección de terminales y otros dispositivos conflictivos en la red. Las pruebas de conectividad empleando el comando ping desde las estaciones de trabajo beneficiadas reportaron resultados acordes a los estándares para la Red UHOLM en cuanto a la velocidad de conexión, no así en el porciento de paquetes recibidos o en la disponibilidad real del host.

El empleo adecuado del ancho de banda contratado por la Universidad de Holguín es otro de los elementos a considerar para el diagnóstico de la red. El autor de la presente investigación se desempeño durante dos años como operador de la red en el Nodo Central de la UHOLM, período durante el cual percibió que la mayoría de los problemas de navegación son originados por el escaso ancho de banda disponible.

En encuentros desarrollados con administradores de redes en otras instituciones del municipio se conoció que en aquellas en las que el ancho de banda es similar al de la UHOLM y el número de usuarios es muy inferior se navega de manera adecuada y el nivel de insatisfacción de los usuarios es mucho menor. La solución no sería disminuir la cantidad de usuarios con acceso a este servicio, teniendo en cuenta que los profesores necesitan tener acceso a información reciente y variada y esa es la mejor vía, sino gestionar la contratación de un mayor ancho de banda y, mientras dicha solución se concreta, la implementación de funciones en el servidor proxy para mejorar la navegación web.

La gestión dinámica de las listas de control de acceso (ACL) permitiría, en teoría, acceder al servicio, aunque no corresponda según el horario, siempre que el canal esté siendo subutilizado. La solución dependería de un Squid Helper desarrollado en Python que brinde la información a Squid de qué usuario puede acceder a Internet en un momento determinado. Si un usuario intenta acceder en un horario en el que no le corresponde y existe disponibilidad en el canal puede disfrutar del servicio hasta tanto algún usuario, al que sí le corresponda acceder en dicho horario, se autentique. Esto optimizaría la gestión de las ACL estáticas que se

emplean actualmente y que pudiera provocar un desaprovechamiento del ancho de banda en determinados horarios.

El programa funcionaría de una manera sencilla. Cuando el usuario que no está en su horario de navegación solicita acceder al servicio, analiza si existe disponibilidad. Si así fuera, se añade el usuario a la ACL. En caso de que un usuario autorizado intente acceder, se elimina al usuario temporal de la ACL. En ambos casos se emplea el comando squid –k reconfigure para actualizar la información que evita reiniciar el servidor proxy.

Esta propuesta no mejoraría la velocidad de conexión, pero sería una alternativa para una mejor distribución de los horarios de acceso al servicio. Sin embargo, debido al gran número de usuarios al que le corresponde navegar en cada horario, es muy poco probable que exista disponibilidad real para que se pueda hacer uso de esta alternativa.

La otra propuesta es el uso de las delay pools para manejar el ancho de banda, que controlaría el ancho de banda asignado a los usuarios y evitaría que algunos se adueñen de gran parte del mismo de manera indiscriminada. La idea es garantizar un ancho de banda fijo para cada usuario conectado garantizado cierta estabilidad en el empleo del servicio. En una primera aproximación se propuso hacerlo dinámicamente asignando el límite de acuerdo a la cantidad de usuarios conectados que tiene el inconveniente de determinar el momento en que un usuario ha dejado de emplear el servicio. Otra manera sería hacerlo estáticamente, la que desaprovecharía el ancho de banda de los usuarios autorizados que no se encuentren navegando.

La Tabla VIII muestra los tiempos de accesos a diferentes sitios empleando delay pools. Se han establecido canales de 6 Kbps y 10 Kbps, con un límite de 32 Kbps en ambos casos.

Tabla VIII Resultados de la aplicación de las delay pools en el proxy

Sitio	6Kb/32Kb	10Kb/32Kb
intranet.uclv.edu.cu	3.52 s	1.98 s
antivirus.uclv.edu.cu	5.11 s	2.54 s
intranet.uo.edu.cu	3.95 s	1.76 s
intranet.uho.edu.cu	1.9 s	1.61 s
serverinfo.uho.edu.cu	1.72 s	0.1 s
antivirus.uho.edu.cu	1.04 s	1.5 s

El empleo de una delay pool con límite de 10Kbps mejora sustancialmente el tiempo de acceso a los sitios, sin embargo esta solución permitiría un máximo de 25 usuarios. Para el gran número de usuarios que emplea los servicios de la red sería más efectiva una navegación de 6Kbps, que permite alrededor de 42 usuarios navegando.

En la Red UHOLM son más de 3000 los usuarios de internet en la institución, algunos de ellos están en la categoría directivos (disfrutan diariamente del servicio) y el ancho de banda contratado sólo permite estar conectados a 10 usuarios como máximo, para navegar de forma aceptable. Si se estableciera una rotación para que los usuarios emplearan el servicio según los parámetros de la delay pool, cada usuario podría tener acceso al servicio cada tres semanas, lo cual no resuelve el problema actual.

Ambas soluciones presentan el inconveniente de determinar cuándo un usuario se encuentra inactivo, y sólo serían efectivas en el caso de que el número de usuarios que se encuentre empleando el servicio sea menor de 10, y considerándose que alrededor de 15 emplean el servicio en cualquier instante de

tiempo que se monitorice se puede concluir que la única solución que puede detener las continuas quejas de los usuarios es el incremento del ancho de banda.

Del análisis realizado se puede concluir que:

- El comportamiento ineficiente del servicio de navegación en Internet en la Universidad de Holguín está condicionado por la limitada velocidad de transferencia contratada con el ISP
- Existe un desaprovechamiento del canal en el horario de la madrugada y los sábados y domingos
- Una parte importante del canal se emplea en el acceso a portales nacionales de noticias
- El número de peticiones que se niegan es demasiado alto
- Las propuestas de gestión dinámica de las ACL y el empleo de las delay pools no resuelven, en principio, el problema existente.

Los resultados de la presente investigación, en una etapa incipiente, se presentaron a la Dirección de Informatización de la entidad para su valoración y empleo como apoyo a la toma de decisiones, recibiendo sugerencias para enriquecer el resultado del trabajo desarrollado.

2.5.1 Propuestas

A pesar del insuficiente ancho de banda con que cuenta la Universidad de Holguín y en espera de un incremento del mismo en consideración con el alto número de usuarios, se proponen soluciones como las siguientes:

1. Destinar una computadora, de manera exclusiva, como servidor de monitorización. Esta variante permitirá la ejecución de herramientas más potentes que las aplicadas en la presente investigación y el almacenamiento de datos históricos.

2. Poner en funcionamiento un servicio de descargas centralizado que permita a los usuarios subir el URL de la información que desean descargar. La cola de descarga se activaría en los horarios clasificados como de bajo tráfico. La información descargada permanecería con acceso público para que los usuarios que deseen emplearla no saturen la red descargando ficheros que hayan sido descargados previamente.
3. Implementar un servidor de noticias que reduciría, en gran medida, el empleo del canal al evitar un número considerable de solicitudes a los portales nacionales de noticias.
4. Crear mensajes que informen a los usuarios si están tratando de acceder al servicio de navegación en Internet en un horario en el cual no está autorizado o si la petición incluye términos bloqueados por las listas de control de acceso, lo cual reduciría la cantidad de peticiones realizadas al servidor y la generación de códigos de error.
5. Seguir investigando las propuestas de la gestión dinámica de las ACL y el empleo de delay pools mientras no se produzca un incremento del ancho de banda, pues en este momento no reportarían beneficios por la relación ancho de banda/usuarios y afectaría el rendimiento del servidor proxy.

2.6 Informe final

El informe final del diagnóstico incluye los gráficos y otros documentos que se presentan en los anexos de esta investigación por lo que no se repiten en esta etapa pues ya fueron analizados en las correspondientes. Sólo se añaden algunas consideraciones de situaciones que no han sido analizadas anteriormente.

2.7 Valoración de los resultados de la investigación

Para comprobar la efectividad de la solución propuesta al problema planteado el inicio de la investigación, fueron presentados los resultados del trabajo realizado a

la Dirección de Informatización de la Universidad de Holguín y a investigadores que valoraran el componente administrativo de la tesis presentada.

De acuerdo a la opinión emitida por al Director de Informatización y el Administrador de la Red UHOLM, se realizó una elección adecuada de herramientas para la monitorización de la red y el estudio de los registros de los servidores y señalan la pertinencia de las propuestas presentadas pues:

- Permiten una mejor interpretación de las variables que definen el desempeño de la red
- Contribuyen a que la red no se sature en horario de máxima demanda
- Evitan la descarga innecesaria de archivos
- Logran que los usuarios perciban una velocidad de respuesta mayor al emplear el servicio de navegación
- Informan con mayor precisión acerca de los resultados de las peticiones realizadas al servidor proxy.

El MSc. Yosvani Orlando Lao León avaló la pertinencia y actualidad del procedimiento propuesto y consideró el objetivo cumplido. Manifiesta que este posee una lógica coherente en su desarrollo y destaca su enfoque cíclico en correspondencia con la mejora continua. Considera, además, que aunque es una adaptación de otro procedimiento y fue modificado para su aplicación en la Universidad de Holguín, es general y flexible para su aplicación en otras redes informáticas. No obstante, afirma que es susceptible a mejoras en el orden metodológico que enriquecerían la propuesta y contribuirían a su aplicación. De manera general considera que es un trabajo científico acabado, correctamente fundamentado por el problema científico y que da respuesta a la problemática planteada.

Concluyen que la tesis presentada contribuye a mejorar, de manera discreta, el funcionamiento de la red informática de la Universidad de Holguín y cumple con el objetivo planteado en la investigación.

2.8 Conclusiones parciales

Finalizado el presente capítulo se puede concluir que:

1. La carencia de procedimientos y metodologías para un diagnóstico completo de una red informática propició el desarrollo de la propuesta presentada.
2. El procedimiento propuesto para el diagnóstico de la red informática de la Universidad de Holguín “Oscar Lucero Moya” transita por cinco etapas, que concentran once acciones y abarcan todas las fases del análisis y diagnóstico de una red y es aplicable tanto a un diagnóstico completo como para valorar un servicio determinado.
3. La propuesta, dentro del procedimiento del análisis y seguimiento del tráfico de la red, constituye un elemento distintivo y relevante, al proporcionar información de forma eficiente y oportuna del funcionamiento de la red.
4. Las herramientas seleccionadas para la monitorización de la red suministraron la información que se necesitaba para analizar y diagnosticar la red estudiada.
5. Los tiempos de acceso en la LAN son aceptables, sin embargo la inestabilidad en su funcionamiento sugieren un estudio profundo del cableado estructurado.
6. Existe saturación del canal de acceso a Internet, a pesar de las políticas trazadas y la segmentación del horario de acceso para los usuarios.

7. El limitado ancho de banda impide la puesta en funcionamiento de técnicas de reparto del canal.

Conclusiones

Tras la ejecución de las tareas que guiaron la investigación, se puede plantear que se dio respuesta a las preguntas científicas formuladas y se cumplió el objetivo propuesto. De forma general se puede concluir que:

1. El servicio de diagnóstico de redes informáticas es un proceso no estandarizado, que debe realizarse de forma periódica monitorizando constantemente el funcionamiento de estas.
2. Existe de forma general inconformidad con la mayoría de los servicios que presta la red informática de la UHOLM, constituyendo la navegación en Internet el servicio que más insatisfacciones genera en los usuarios.
3. El procedimiento para el análisis y diagnóstico de redes propuesto en esta investigación propició un estudio general de la red informática de la UHOLM y permitió profundizar en el servicio de navegación en Internet.
4. Los diferentes análisis realizados y las herramientas implementadas en la presente investigación confirmaron que la limitación principal para el acceso de los usuarios de la red informática de la UHOLM es el insuficiente ancho de banda contratado con el ISP (ETECSA).
5. La implementación de las propuestas presentadas permitirá una mejor administración del canal de comunicaciones y una disminución de las insatisfacciones por parte de los usuarios.

Recomendaciones

1. Aplicar las propuestas realizadas y documentar los resultados obtenidos.
2. Realizar una investigación que permita detectar el nivel de impacto del cableado estructurado en la red informática de la Universidad de Holguín.

Bibliografía

1. Doce herramientas de diagnóstico y monitoreo de redes: Axence NetTools. Disponible en: http://www.bloginformatico.com/12-herramientas-de-diagonstico-y-monitoreo-de-redes-axence-nettools.php [Consultado el 28 de junio de 2012]
2. Aguilar, J.; Leiss, E. An adaptative coherence-replacement protocol for web proxy cache systems. Computación y Sistemas, 8(1):1-14, 2004. ISSN 1405-5546
3. Ahumada, Pablo. Análisis experimental de la transmisión de datos. Disponible en: http://profesores.elo.utfsm.cl/~agv/elo322/1s09/project/reports/AnalisisExperimentalTCP.pdf
4. Borja Merino Febrero. Análisis de tráfico con Wireshark. INTECO. Febrero 2011
5. Burgess, Mark. Principles of Network and System Administration. Second Edition. John Wiley & Sons Ltd. 2004.
6. Chapell, L. y Combs, G. Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide. 2010
7. Cobb, J.; ElAarag, H. Web proxy cache replacement scheme based on back-propagation neural network. The Journal of Systems and Software, 81:1539-1558, 2008
8. Customizable Log Formats. Disponible en http://wiki.squid-cache.org/Features/LogFormat.htm [Consultado el 15 de enero de 2012]
9. Diseñar la red para la pequeña empresa. Disponible en http://technet.microsoft.com/es-es/library/dd568932.aspx [Consultado el 22 de agosto de 2011]
10. Diseño de una red LAN para el edificio de cursos básicos de la Universidad de Oriente Núcleo de Sucre. Disponible en http://www.monografias.com/trabajos7/rela/rela.htm [Consultado el 22 de agosto de 2011]

11. Dykes, S.G.; Robbins, K.A. Limitations and benefits of cooperative proxy caching. IEEE Journal, 20(7):1290-1304, 2002. ISSN 0733-8716

12. El Cableado Estructurado ¿un problema o una solución? Disponible en http://www.channelplanet.com/El_Cableado__Estructurado_¿un_problema_o_una solución? – ChannelPlanet Inc.htm [Consultado el 22 de agosto de 2011]

13. El modelo OSI te ayuda a diagnosticar problemas de redes. Disponible en http://www.aprendaredes.com/dev/articulos/el-modelo-osi-te-ayuda-a-diagnosticar-problemas-de-redes.htm [Consultado el 22 de agosto de 2011]

14. FAQs Squid Logs. Disponible en http://wiki.squid-cache.org/SquidFaq/SquidLogs.htm [Consultado el 15 de enero de 2012]

15. Fernández Haro, Alejandro. Entorno de experimentación para generación y monitorización de tráfico P2P. Universidad de Granada. Diciembre 2010. Disponible en: http://tstc.ugr.es/it/pfc/proyectos_realizados/downloads/Memoria2010_AlejandroFernandezHaro.pdf

16. Flickenger, R..: How to accelerate your Internet: A practical guide to Bandwidth Management and Optimization using Open Source Software, INASP/ICTP, 2006.

17. García, R. De Castro, P.; Verdú, M.; Verdú, E.; Regueras, L.; López, P. A cache replacement policy based on neural networks applied to web map tile caching.

18. Gerometta, Oscar A. Guía de preparación para el examen de certificación CCNA – 1ª Ed. Buenos Aires, Libronauta, 2006.

19. Gribble, S.; Brewer, E. System design issues for Internet middleware services: Deductions for a large client trace. Proceedings of the USENIX Symposium on Internet Technologies and Systems. California, 1997

20. Herramienta para análisis de redes locales. Disponible en http://www.elguruinformatico.com/herramienta-para-analisis-de-redes-locales-lan/Herramienta_para_análisis_de_redes_locales_(_LAN_).htm [Consultado el 22 de agosto de 2011]

21. Johnson, D. L.; Belding, E. M.; Almeroth, K. and van Stam G.: "Internet usage and performance analysis of a rural wireless network in Macha, Zambia", NSDR ´10, San Francisco, California, 2010.

22. Karouse, J.F., Ross, K.W. Computer Networking: A top-down Approach. 4th edition. 2007

23. Mahanti, A.; Williamson, C.; Eager, D. Traffic analysis of a web proxy caching hierarchy. IEEE Network Magazine, 2000

24. Manual para el diseño de redes (LAN). Disponible en http://www.monografias.com/trabajos28/manual-redes/manual-redes.zip [Consultado el 22 de agosto de 2011]

25. Martín, Luis Manuel. Cableado estructurado. Disponible en http://platea.pntic.mec.es/~lmarti2/apun_prin.htm [Consultado el 22 de agosto de 2011]

26. Pearson, O. Squid: A user´s guide. Qualica Technologies, 2000

27. Portal Web de la Dirección de Informatización de la Universidad de Holguín. Disponible en http://dirinf.uho.edu.cu/ [Consultado el 13 de marzo de 2012]

28. Rabinovich, M.; Spatscheck, O. Web caching and replication. Addison Wesley, 2001. ISBN 0-201-61570-3

29. Rizzo, L.; Vicisano, L. Replacement policies for a proxy cache. IEEE/ACM Transactions, 8(2):158-170, 2000. ISSN 1063-6692

30. Romano, S.; ElAarag, H. A neural network proxy cache replacement strategy and its implementation in the Squid proxy server. Neural Computing and Applications, 20(1):59-78, 2011

31. Sanders, C. Practical Packet Analysis: Using Wireshark to solve Real-World Network Problems. 2007

32. Sitio de la Red de la Universidad de Holguín. Disponible en http://red.uho.edu.cu/ [Consultado el 1 de mayo de 2012]

33. Sitio web RAYTEL. Disponible en http://www.raytel.cl/ [Consultado el 22 de agosto de 2011]

34. Sitio web Wireshark. Disponible en http://wiki.wireshark.org/ [Consultado el 22 de agosto de 2011]

35. Sito web Javvin. Disponible en http://www.javvin.com/packet.html [Consultado el 22 de agosto de 2011]

36. Sito web Wildpackets. Disponible en http://www.wildpackets.com/ [Consultado el 22 de agosto de 2011]

37. SoftPerfect Network Scanner. Disponible en http://www.softperfect.com/products/networkscanner/ [Consultado el 22 de agosto de 2011]

38. Stallings, W. Comunicaciones y redes de computadoras. 6ta edición

39. Tanenbaum, Andrew S. Computer networks. Prentice Hall, 1981.

40. Tulley, Dominic. Configuring Tomcat and Wireshark to capture and decode SSL communications. 2009

41. Venketesh, P.; Venkatesan, R. A survey on applications of neural networks and evolutionary techniques in web caching. IETE Journals, 23(3):1717-180, 2009

42. Wireless sniffing with Wireshark. Disponible en http://www.syngress.com [Consultado el 22 de agosto de 2011]

43. Wolman, A.; Voelker, G.; Sharma, N.; Cardwell, N.; Brown, M.; Landray, T.; Pinnel, D.; Karlin, A.; Levy, H. Organization-Based analysis of web-object sharing and caching. Department of Computer Science and Engineering. University of Washington

Anexos

I. Encuesta aplicada a usuarios de la red informática de la Universidad de Holguín.

Facultad o Área a la que pertenece: _____

1. Evalúe el acceso a los servicios que emplea habitualmente.

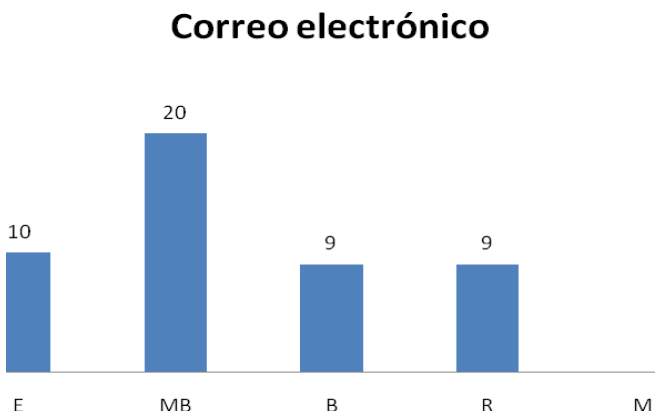
Servicio	E	MB	B	R	M
Correo electrónico					
Navegación en Internet					
Intranet					
FTP					
Acceso Remoto					
Otros _____					

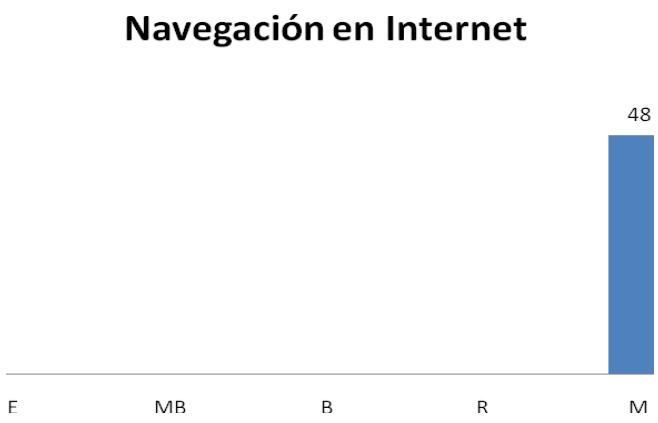
2. Evalúe, según su experiencia, el funcionamiento de la red informática de la Universidad de Holguín.

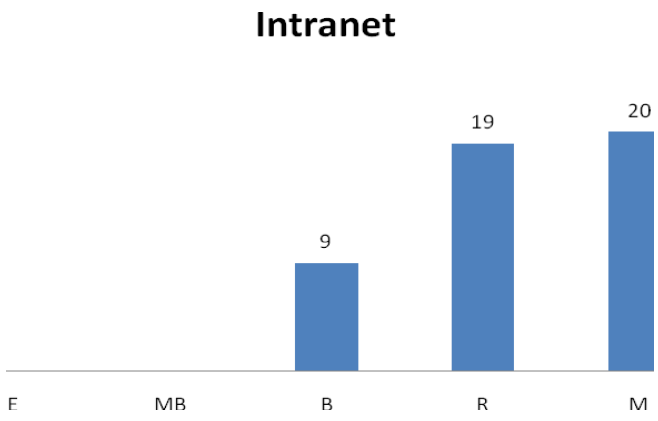
   ___ Excelente ___ Muy bueno ___ Bueno ___ Regular ___ Malo

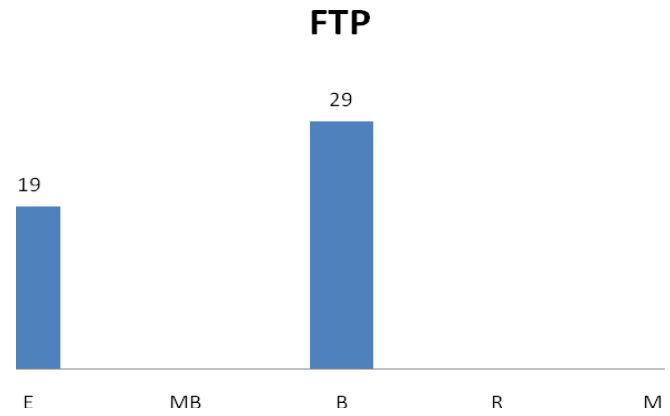
3. ¿Cuáles son los principales problemas a los que se ha enfrentado al trabajar en la red de la Universidad de Holguín?

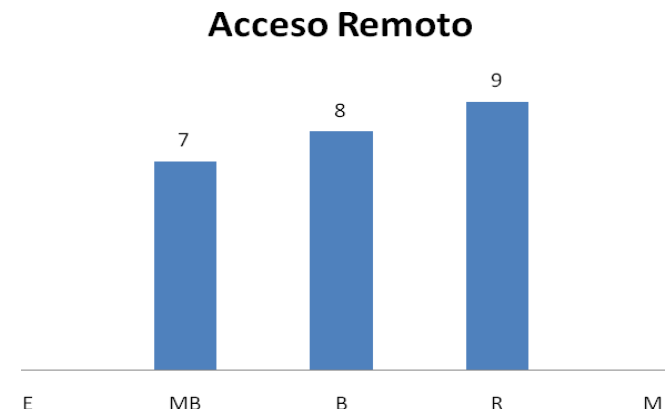
II. Resultados de la encuesta aplicada a usuarios de la red informática de la Universidad de Holguín.

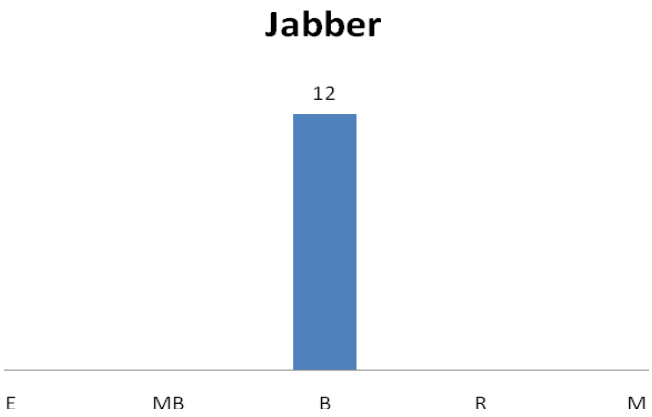







FTP
19
29
E
MB
B
R
M


Acceso Remoto
7
8
9
E
MB
B
R
M


Jabber
12
E
MB
B
R
M

III. Entrevista realizada a administradores de los nodos de la red informática de la Universidad de Holguín.

Nombre y Apellidos: _____

Facultad o Área a la que pertenece: _____

1. ¿Cuáles son las principales quejas de los usuarios de la red del área que usted atiende?
2. ¿Qué problemas se presentan habitualmente que repercuten en el adecuado funcionamiento de la red?
3. ¿Qué sugiere usted para mejorar el funcionamiento de la red de la Universidad de Holguín?

IV. Entregables del servicio de análisis y diagnóstico de RAYTEL.

- *Copia de las actas de reunión (dependiendo de la importancia del caso)*
- *Documento final que incluye:*
  - *Análisis y diagnóstico de la red LAN*
  - *Caracterización de la red*
  - *Gráficas del comportamiento diario de tráfico y del funcionamiento de la red*
- *Análisis de vulnerabilidad en servidores:*
  - *Matriz de hallazgos*
  - *Recomendaciones*
    - *Seguridad*
    - *Gestión*
    - *Eficiencia*
    - *Conclusiones*
- *Documento de acciones a tomar:*
  - *Modelo para lograr los objetivos propuestos*
  - *Recomendaciones*
    - *Seguridad*
    - *Networking*
    - *Conectividad*
    - *Switching*
    - *Segmentación*
- *Recomendaciones para el manejo de algunas aplicaciones.*
- *Correo electrónico, acceso a Internet:*
  - *Proxy, firewall, detector de intrusos, antivirus, etc.*
    - *Seguridad, gráficas y estadísticas del comportamiento de la red.*
    - *Matriz de hallazgos y recomendaciones en seguridad de los servidores.*
- *Informe de recomendaciones de acciones para la optimización de la red.*