UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

ÁREA TÉCNICA

TITULACIÓN DE INGENIERO EN INFORMÁTICA

TEMA:

“Diseño de red de área local del Centro Universitario de la Universidad Técnica Particular de Loja en Cariamanga, basado en el modelo Jerárquico de tres capas.”

Trabajo de Fin de Titulación

Autor:

Torres Torres, Andrea Cecilia

Director:

Jaramillo Campoverde, Byron Gustavo, Ing.

Torres Tandazo, Rommel Vicente, PhD.

CENTRO PROVINCIAL CARIAMANGA

2013

CERTIFICACIÓN

Ing.

Byron Gustavo Jaramillo Campoverde.

DIRECTOR DEL TRABAJO DE FIN DE CARRERA

CERTIFICA:

Que el presente trabajo, denominado **"Diseño de la red de área local del Centro Universitario de la Universidad Técnica Particular de Loja en Cariamanga, basado en el modelo Jerárquico de tres capas"**, realizado por el profesional en formación Torres Torres Andrea Cecilia, cumple con los requisitos establecidos en las normas generales para la Graduación en la Universidad Técnica Particular de Loja, tanto en el aspecto de forma como contenido, por lo cual me permito autorizar su presentación para fines pertinentes.

Loja, junio del 2013

f)……..

CI:……...

CERTIFICACIÓN

PhD.

Rommel Vicente Torres Tandazo.

DIRECTOR DEL TRABAJO DE FIN DE CARRERA

CERTIFICA:

Que el presente trabajo, denominado **"Diseño de la red de área local del Centro Universitario de la Universidad Técnica Particular de Loja en Cariamanga, basado en el modelo Jerárquico de tres capas",** realizado por el profesional en formación Torres Torres Andrea Cecilia, cumple con los requisitos establecidos en las normas generales para la Graduación en la Universidad Técnica Particular de Loja, tanto en el aspecto de forma como contenido, por lo cual me permito autorizar su presentación para fines pertinentes.

Loja, junio del 2013

.

f)…….

CI:……...

Declaración de autoría y cesión de derechos.

Yo, Torres Torres Andrea Cecilia, declaro ser autora del presente trabajo y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales.

Adicionalmente declaro conocer y aceptar la disposición el Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: “Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través o con el apoyo financiero, académico o institucional (operativo) de la Universidad”.

f)……

Torres Torres Andrea Cecilia

CI:1104415417

DEDICATORIA.

Con gran alegría y satisfacción me complace dedicar este trabajo a mi esposo Pablo, a mis dos hijos Pablito y Steve: quienes han sido mi razón de vivir y por quienes me esfuerzo día a día en la consecución de mis metas venciendo los obstáculos que se me han presentado a lo largo de la carrera y de la vida.

A mis queridos padres Floresmilo y Luisa por ser el pilar fundamental de mi vida y estar junto a mí en todo momento, quienes con su amor, apoyo incondicional me dieron un enorme impulso e inspiración. A mis hermanos para quienes deseo marcar un precedente y ejemplo a seguir. En fin a toda la familia quienes de una u otra manera me apoyaron en la realización de este gran sueño.

Andrea Cecilia Torres Torres

AGRADECIMIENTO.

A Dios por permitirme seguir adelante siempre en la realización de mis sueños, mis metas y mis aspiraciones, por no dejarme caer nunca, por haberme dado una hermosa familia y la oportunidad de vivir este momento.

A mi esposo Pablo, mis hijos Pablo Andrés y Steve Alexander, a mis queridos padres Floresmilo y Luisa, a mis suegros Jaime y Elsa por su apoyo incondicional haciendo posible que concluya este objetivo trascendental de mi vida.

Expreso mi más sincero agradecimiento, a la Universidad Técnica Particular de Loja, a la escuela de Informática, directivos, personal administrativo y docente, quienes día a día contribuyeron con mi formación académica y personal. Quiero enfatizar mi agradecimiento al Ing. Byron Jaramillo y al PhD. Rommel Torres quienes en calidad de directores aportaron su experiencia profesional guiándome, ayudándome en la realización y culminación exitosa de este proyecto de tesis.

Agradecer así mismo a todos quienes conforman el Centro Regional Asociado Cariamanga por permitirme ejecutar el proyecto de tesis sin ningún inconveniente y absoluta confianza.

A todos ustedes muchas gracias, y que Dios les bendiga siempre.

Andrea Cecilia Torres Torres.

Contenido

INDICE DE FIGURAS.

INDICE DE TABLAS.

RESUMEN EJECUTIVO.

El trabajo presenta el diseño de una red de área local para el CUP de la UTPL; basado en el modelo Jerárquico de tres capas; para solucionar la falta de rendimiento y los problemas asociados con los entornos crecientes de redes de datos, para ello se acopla las redes de datos existentes utilizando esquemas de comunicación mediante redes virtuales establecidas de acuerdo a las áreas funcionales, permitiendo que la transmisión de datos sea segura y confiable.

Se propone la implementación de un NOC que permita conocer el estado de la red e identificar los problemas que se presentan de forma inmediata, utilizando sistemas de monitoreo Cacti y WhatsUp.

Para comprobar el rendimiento de las redes se realizaron pruebas de broadcast utilizando NTGM. En la red de datos actual se genera más tráfico, debido a que se tiene que inundar toda la red, con 10000 paquetes se generó un tráfico de 700 kilobits por segundo. Mientras en la red jerárquica con 10000 paquetes se generó 1.5 kilobits por segundo, ya que los paquetes enviados solamente viajan a la VLAN específica.

ABSTRACT.

The paper presents the local area network design for UTPL's CUP, based on three-layer hierarchical model; to address the performance lack and problems associated with growing environments data networks, for it fits existing data networks using communication schemes virtual networks, set according to the functional areas, allowing data transmission is secure and reliable.

It is proposed to implement a NOC to know the network status and identify problems that arise immediately across Cacti and WhatsUp monitoring systems.

To check the network performance tests, broadcast tests were performed using NTGM. The current data network generates more traffic because it has to flood the entire network with 10000 packets; it generated traffic 700 kilobits per second. While the hierarchical network with 10000 packets, which generated 1.5 kilobits per second, since only the packets traveling to the specific VLAN.

OBJETIVOS.

Objetivo General.

Diseñar la infraestructura de red de datos idónea utilizando el Modelo de red Jerárquica de tres capas para el Centro Universitario Provincial Cariamanga de la UTPL.

Objetivos específicos.

- Determinar el estado actual de las redes de datos existentes.
- Realizar el estudio detallado del Modelo de red Jerárquica de tres capas.
- Crear VLANs, para incrementar la seguridad y el rendimiento de la red.
- Proponer la implementación de un NOC, que monitoree el estado de la red permanentemente.

1. MARCO TEÓRICO.

1.1. Información del Modelo Jerárquico de tres capas.

Las redes de datos deben estar adecuadamente organizadas para facilitar la administración y gestión ante su crecimiento acelerado en tamaño y complejidad, lo que obliga a implementar modelos de administración que garanticen su disponibilidad, rendimiento, escalabilidad y confiabilidad ante el número creciente de aplicaciones de software que se desarrollan en torno del protocolo IP y la Web.

Diseñar una red de datos óptima aplicando el modelo Jerárquico de tres capas, hace que esta sea más predecible, brindando la oportunidad de incorporar nuevos dispositivos o la posibilidad de ampliar su alcance fácilmente, de lo contrario, sería complicado si no hubiese un diseño de conexión adecuada.

La información que se presenta a continuación nos permitirá diseñar redes de datos aplicando el modelo propuesto.

1.1.1 Modelo Jerárquico de tres capas.

El modelo Jerárquico de tres capas, está constituido por capas o niveles: la capa núcleo, capa de distribución y la capa de acceso, tal como lo podemos observar en la figura 1.1 Cada una de estas capas cumple con funciones específicas lo que hace que la red sea más flexible, rápida, eficiente y de fácil administración, permitiendo adaptarse fácilmente a los cambios requeridos de acuerdo a su crecimiento, además define el tipo de conectividad que se necesita entre los diferentes dispositivos en la red.

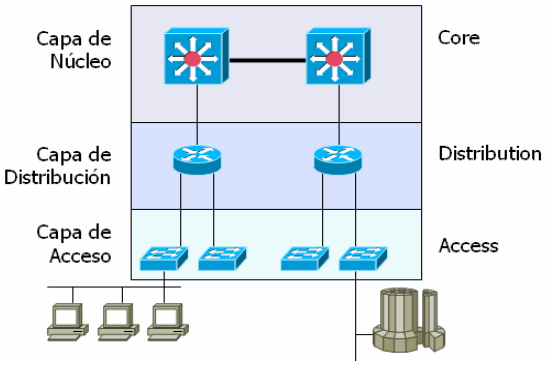


Figura1. 1. Modelo Jerárquico de tres capas. [1]

1.2. Estructura del Modelo Jerárquico de tres capas.

1.2.1. Capa de núcleo.

“El tráfico de todos los dispositivos de la capa de distribución, puede llegar a ser enviado a la capa núcleo, por lo tanto debe poder reenviar grandes cantidades de datos rápidamente de manera confiable” [3]. Se la conoce como espina dorsal, es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo esté disponible y sea redundante.

La capa núcleo se caracteriza por transportar los paquetes de datos a gran velocidad, y para garantizarlo se debe considerar las siguientes características: alta velocidad, baja latencia, alta disponibilidad, alta fiabilidad y conectividad. Cuando se requiere implementar un mayor número de dispositivos de red para satisfacer las necesidades de crecimiento, se debe evitar incrementar el número de dispositivos en esta capa. Una falla en la capa núcleo afecta a todos los dispositivos de la red.

Núcleo de alta disponibilidad.

Para garantizar la disponibilidad de la capa núcleo, ésta deber ser redundante, con lo cual se asegura que siga trabajando si uno de sus componentes falla.

Núcleo Rápido.

Se debe procurar que el núcleo de la red funcione a la velocidad máxima posible, es por ello que la única función a la que debe limitarse es al reenvío de paquetes tan rápido como sea posible.

1.2.2. Capa de Distribución.

“La capa de distribución agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final” [3].
Esta capa es la capa de enrutamiento, denominada también como capa de grupo de trabajo, está encargada del enrutamiento de paquetes entre o desde los nodos conectados en la capa de acceso. También controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de broadcast al realizar el enrutamiento del tráfico de las VLAN definidas en la capa de acceso.

Funciones de la capa de distribución

Las funciones de la capa de distribución, se describen a continuación [3]:

- Proveer ruteo de paquetes entre la capa de acceso y los routers de la capa núcleo.
- Retransmisión de paquetes a la capa base según sea necesario, filtrado.
- Interconexión de LANs.
- Acceso a la red LAN y WAN.
- Determinar que paquetes deben llegar a la capa núcleo.
- Gestión de listas de acceso, estas se deben configurar en la capa de distribución.
- Filtrado de paquetes
- Traducir direcciones de red (NAT-Network Address Translation).
    - Firewalls Gestión. Aislar la red privada interna de las redes públicas.
    - Enrutamiento de paquetes entre VLANs.

1.2.3. Capa de Acceso.

"La capa de acceso, es la capa de conmutación que controla a los usuarios, el acceso a los grupos de trabajo o los recursos de internetwork." [3]. La capa de acceso es donde el grupo de trabajo de las LAN se define, aquí se conectan los dispositivos finales, tales como, PCs impresoras, teléfonos IP, etc. Esta capa puede incluir routers, switches, hubs y rutas de acceso inalámbricos. El propósito principal de la capa de acceso es servir como un medio de conexión de los dispositivos a la red y controlar qué exista comunicación.

Funciones de la capa de acceso.

Las funciones de la capa de acceso son [3]:

- Creación de dominios de colisión separados (segmentación).
- Conectividad de los grupos de trabajo en la capa de distribución.

Si la capa de acceso puede incluir routers y switches, es necesario conocer las funciones que deben cumplir:

- Conexión de los dispositivos a una LAN.
- Segmentación del tráfico de una red en las LAN y VLAN.
- Retransmisión del tráfico de los switches y routers a la capa de distribución.

1.3. Ventajas de diseñar el modelo Jerárquico de tres capas.

Existen varias ventajas para diseñar e implementar una red de datos creada bajo el modelo Jerárquico de tres capas, entre ellas se destaca las siguientes [2]:

Facilidad de ampliación. La capacidad de compartir información cada vez más rápida y económica ha hecho que la población incremente su necesidad de comunicación simultánea haciendo uso de la tecnología de las redes de datos, razón por la cual deben estar adecuadamente diseñadas para permitir su ampliación en cualquier momento. Las redes que siguen el modelo jerárquico*,* "pueden aumentar el tamaño sin sacrificar el control o facilidad de administración, porque la funcionalidad se encuentra limitada a una ubicación en particular, y los problemas potenciales se pueden reconocer con mayor facilidad" [2] .La administración se vuelve fácil lo que asegura su buen funcionamiento y adaptabilidad ante los cambios, sin tener que reconfigurar toda la red. Para aumentar el tamaño de una red jerárquica, no es necesario rediseñarla basta adaptar los equipos necesarios en la capa correspondiente, esto iniciando desde la capa de acceso.

Facilidad de implementación. "Un diseño jerárquico asigna una funcionalidad clara a cada capa" [2]. Cada una de las capas del modelo Jerárquico, cumple con una función específica, lo que le permite al administrador identificar que equipos asignar a cada capa y así aplicar la configuración requerida, garantizando el correcto funcionamiento de la red de datos.

Facilidad de detección de fallas. "Las funciones de cada capa se encuentran bien definidas, por lo que el aislamiento de los problemas de la red es menos complicado. También es más fácil segmentar temporalmente la red para reducir el alcance de un problema" [2].

Este modelo al estar estructurado y configurados los equipos de acuerdo a la función de cada capa, permite realizar el análisis de los incidentes que afecten la operatividad y disponibilidad de la red. Esta estructura brinda la posibilidad de aislar el segmento afectado sin intervenir o disminuir el rendimiento del resto de la red, para corregir los problemas identificados en el menor tiempo posible.

Facilidad de pronóstico. "El comportamiento de una red que usa capas funcionales es bastante predecible, lo que facilita la planificación de capacidad para el crecimiento" [2].

El predecir el crecimiento de una red está estrictamente ligada con factores como: el incremento de personal de trabajo, aumento de la población estudiantil, la creación de nuevas áreas funcionales, secciones de investigación, servicios, aplicaciones, etc.; el análisis de los factores mencionados permiten determinar con exactitud qué y cuantos equipos, ancho de banda, medios de transmisión, etc. que se requieren incrementar en determinado momento garantizando la disponibilidad de la red y satisfaciendo las necesidades inmediatas de la institución.

Soporte de protocolo. "La mezcla de aplicaciones y protocolos actuales y futuros es mucho más fácil en las redes que siguen los principios del diseño jerárquico porque la infraestructura subyacente ya se encuentra lógicamente organizada" [2].

El modelo Jerárquico de tres capas es escalable, lo que le permite implementar los diversos protocolos de comunicación presentes y futuros, adaptándose a circunstancias actuales, manteniendo su calidad de comunicación y servicios, sin tener que modificar su estructura para adaptarse a los nuevos protocolos.

Facilidad de administración. "El modelo de diseño jerárquico contribuye a hacer que la red sea más fácil de administrar" [2]. Tener la red segmentada por capas y conocer su función hace que la administración sea mucho más fácil. Es posible administrar la red a través de los dispositivos conectados y de equipos remotos, empezando por los routers de la capa núcleo hasta los switches de la capa de acceso; todo esto de acuerdo a los requerimientos de la institución y siguiendo los protocolos de la red.

El que tenga cada capa una función específica mejora el rendimiento y velocidad, ofreciendo la posibilidad de incorporar a una red de datos sistemas con demandas de velocidad y ancho de banda mayor que son los requerimientos actuales de toda institución. Una fácil administración asegura la supervisión, implementación de nuevas tecnologías y fácil mantenimiento de la red.

1.4. Principios Claves del diseño de la Red Jerárquica

1.4.1. Diámetro de la red.

"El diámetro de la red es el número de dispositivos que un paquete debe cruzar antes de alcanzar su destino. Mantener bajo el diámetro asegura una latencia baja y predecible entre los dispositivos" [5]. La figura 1.2 nos muestra el diámetro de la red.
Entre menor es el diámetro o número de dispositivos para llevar un paquete a su destino, más rápido es el tiempo de respuesta, es decir a menor dispositivos a recorrer mayor rapidez en la transmisión de los datos a su destino. El menor diámetro es seleccionado por el router como la mejor ruta para cumplir con su objetivo.

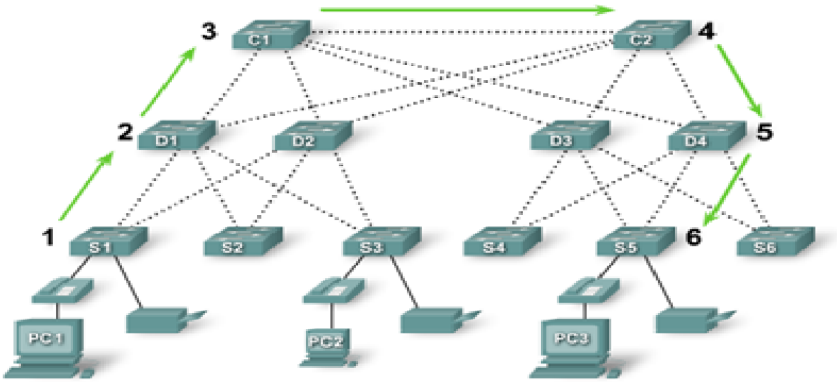


Figura1. 2. Diámetro de la Red. [4]

1.4.2. Agregado del Ancho de banda.

"El agregado del ancho de banda, se implementa normalmente al combinar varios enlaces paralelos entre 2 switches en un enlace lógico" [5].

El agregado de ancho de banda se lo debe configurar en la capa de distribución y en la capa núcleo combinando 2 enlaces paralelos, para ello se debe tomar en cuenta el ancho de banda requerido. La figura 1.3, nos muestra el agregado del ancho de banda.

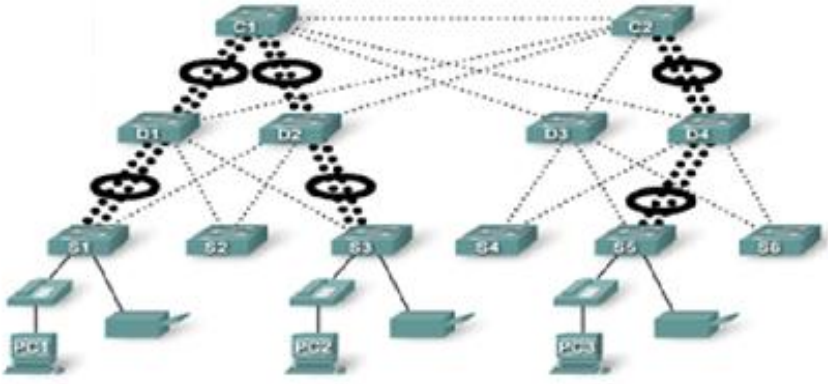


Figura1. 3. Agregado del Ancho de banda. [4]

1.4.3. Redundancia.

"Una de las ventajas del modelo jerárquico es la redundancia entre las capas de redes a fin de asegurar la disponibilidad de la red" [5].La figura 1.4, nos muestra la redundancia en una red Jerárquica.

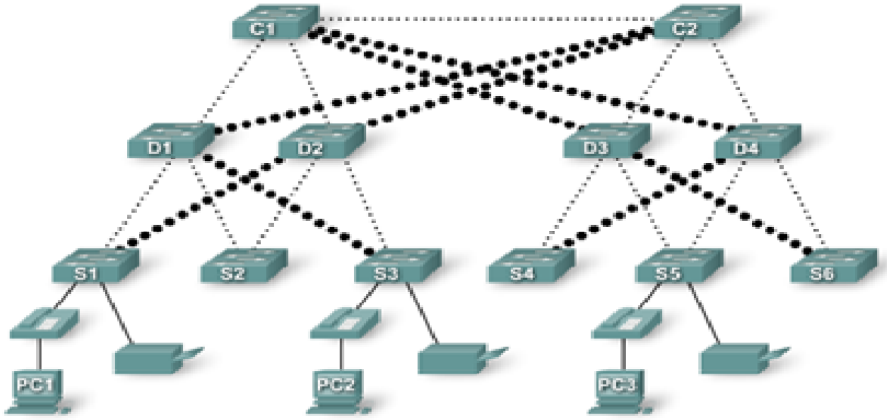


Figura1. 4.Redundancia. [4]

La redundancia de los equipos y conexiones garantiza que cuando se produce una falla en un segmento de la red, esta siga funcionando con normalidad, tal es el caso de que si uno de los switches de la capa de distribución falla, el switch de la capa de acceso afectado tiene la alternativa de conectarse a otro puerto del switch de distribución, lo mismo pasaría si el caso se diera a nivel de la capa núcleo. La redundancia permite asegurar la disponibilidad de la red.

1.4.4. Convergencia.

"La convergencia es el proceso en el cual se logra la combinación de las comunicaciones con voz y video en una red de datos" [5]. El proceso de convergencia, se lo puede observar en la figura 1.5.

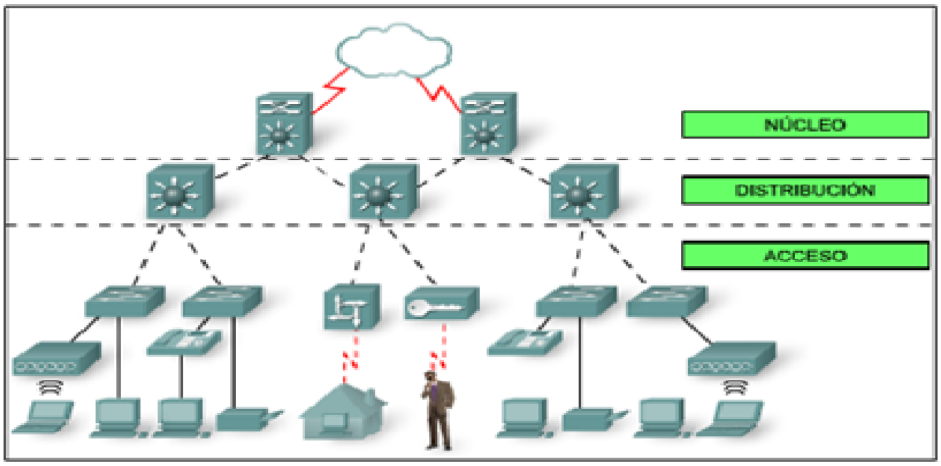


Figura1. 5. Convergencia. [4]

Las aplicaciones colaborativas utilizadas para trabajos en grupo exigen la transmisión simultánea de datos, video y voz, ya que no es fácil trasladarse físicamente hasta otros lugares de forma inmediata o los recursos económicos no nos lo permiten. Las redes jerárquicas abren la posibilidad de convergencia.

1.5. Seguridad de la Red.

La seguridad de la red corresponde a cada uno de los procesos que se llevan a cabo para controlar el acceso a la red de datos, con la finalidad de proteger la información que es el recurso más valioso que tiene una institución; para ello es necesario diseñar una red segura y confiable que garantice la confidencialidad, integridad y disponibilidad de la información. Para lograrlo se requiere implementar el estándar de seguridad ISO 17799, que es la agrupación de reglas y mejores prácticas para garantizar la seguridad de la información, está organizado en 10 secciones, y se hace conocer a continuación [25]:

1. **Planeación de la continuidad del negocio**

   "Contrarrestar las interrupciones de las actividades productivas críticas del negocio. Evitar fallas mayores o desastres"

   El plan de contingencia ante los problemas que se presenten y que afecten en mayor grado a la Institución.

2. **Sistemas de control de acceso.**

   Se debe implementar todos los mecanismos necesarios para proteger la integridad de la información.

   "Controlar el acceso a la información.

   Prevenir los accesos no autorizados a sistemas de información.

   Garantizar la protección de servicios de red.

   Prevenir los accesos no autorizados a las computadoras.

   Detectar actividades no autorizadas.

   Garantizar la seguridad de la información cuando se utilice cómputo móvil remoto"

   Establecer políticas para el uso de la infraestructura tecnológica.

3. Desarrollo y mantenimiento de Sistemas.

Los sistemas deben ser construidos con las seguridades necesarias para salvaguardar la información.

"La seguridad del sistema debe estar construida dentro de la aplicación para prevenir perdidas, abusos y modificaciones de los datos. Debe proteger la confidencialidad, autenticidad e integridad de la información".

4. Seguridad Física y Ambiental

La seguridad física y externa, también contribuyen a proteger la información, por ello se debe implementar mecanismos de seguridad, tales como: guardias de seguridad, cámaras, sistemas de control contra incendios, etc.

"Prevenir el acceso no autorizado a las instalaciones para prevenir la pérdida, robo, daño de los bienes y evitar la interrupción de las actividades productivas. Prevenir el robo de información y de los procesos de la empresa".

5. Cumplimiento.

Los directivos de una Institución deben crear y hacer cumplir las normas internas de seguridad, con finalidad de garantizar la integridad de la información, así como los equipos que intervienen en los diferentes procesos para el desarrollo de las funciones encomendadas a sus integrantes.

"Evitar infringir cualquier norma civil o penal, ley, reglamento, obligación contractual o cualquier requerimiento de seguridad.

Asegurar la compatibilidad de los sistemas con las políticas y estándares de seguridad.

Maximizar la efectividad y minimizar las interferencias hacia y del sistema de auditoría del proceso".

6. Seguridad del Personal.

"Reducir el riesgo de error humano, robo, fraude, abuso de la información, sistemas y equipos. Asegurarse que el personal este consiente de las amenazas de la información y sus implicaciones. Deberán apoyar la política corporativa de seguridad en contra de accidentes o fallas. A la vez aprender de estos incidentes".

El capacitar a los integrantes de la Institución, garantiza el correcto desenvolvimiento en sus funciones asignadas, minimizando de esta manera el riesgo de error. Es importante que todos ellos conozcan las normas de seguridad creadas, para que le puedan dar cumplimiento.

7. Seguridad de la Organización.

"Administrar la seguridad de la información dentro de la compañía.

Mantener la seguridad de las instalaciones de procesamiento de la información y los activos informáticos ingresados por terceros (provedores, clientes, etc)

Mantener la seguridad de la información cuando la responsabilidad del procesamiento de la información es ejecutada por terceros".

8. Administración de operaciones y equipo de cómputo.

El contar con personal especializado en Informática asegura el correcto funcionamiento de los equipos que intervienen en el procesamiento de la información, mismo que debe garantizar los siguientes parámetros.

"Asegurar la correcta operación de las instalaciones de procesamiento.

Minimizar el riesgo de las fallas en el sistema.

Proteger la integridad del software y la información.

Mantener la integridad y disponibilidad del procesamiento de la información y comunicaciones.

Asegurar la protección de la información en la red y de la infraestructura que soporta.

Prevenir el daño a los activos y procesos críticos del negocio.

La seguridad de una red depende principalmente de la administración y las prestaciones de los equipos de red.

Es relevante aclarar que no existe la seguridad absoluta, pues siempre existe riesgo, independientemente de las medidas que se tomen, sin embargo es necesario implementar altos niveles de seguridad en una red de datos.

Prevenir la pérdida, modificación o mal uso de la información intercambiada entre las empresas".

9. Clasificación y control de los activos.

Los activos que intervienen en el procesamiento de la información deben ser protegidos para evitar daños y pérdidas que afecten a la institución.

"Mantener la protección adecuada de los activos corporativos y garantizar que los activos informáticos reciban un nivel adecuado de protección".

10. Políticas de Seguridad.

"Prever la directriz y el soporte de la dirección general de la empresa para seguridad de la información".

Los directivos de la institución son quienes deben establecer las normas de seguridad aplicables para proteger la información,

Es relevante aclarar que no existe la seguridad absoluta, pues siempre existe riesgo, independientemente de las medidas que se tomen, sin embargo es necesario implementar altos niveles de seguridad en una red de datos debido a la necesidad imperante de tener una transmisión segura. El estándar ISO 17799 no solo contribuye a la homogenización sino que proporciona a los administradores una guía para hacer que su red de datos sea segura.

Además se debe implementar mecanismos que contribuyen a la seguridad, se detallan a continuación:

- **Firewall.** Es un dispositivo que protege a la red contra intervenciones maliciosas.
- **Autenticación.** Identifica si los usuarios de la red pertenecen a la institución.
- **Sistemas de detección de intrusos.** Permiten identificar las actividades anómalas que se presenten en la red en tiempo real, para definir la acción a tomar ante la incidencia.
- **Encriptación.** Vuelve ilegible la información con la finalidad de protegerla ante los rastreos, robos, y manipulación.

1.5.1. Seguridad en el Modelo Jerárquico de tres capas.

La seguridad en una red Jerárquica se implementa en la capa de acceso y en la capa de distribución, con la finalidad de mantener la integridad y disponibilidad de la información, evitando que esta pudiera ser hurtada o distorsionada.

1.5.1.1. Seguridad en la capa de Acceso.

Es posible incrementar la seguridad en esta capa a través de los siguientes mecanismos [7]:

Se puede controlar el acceso a estas zonas utilizando métodos de autenticación y reglas definidas, implementadas en los firewalls, routers u otros dispositivos de seguridad tales como:

- Routers Perímetro, "la primera línea de defensa contra ataques externos". Con las configuraciones realizadas en los routers perímetro, solamente el tráfico permitido puede entrar en la red, creando una barrera ante los ataques externos.
- Routers internos, se colocan detrás de los routers en la topología de la red perimetral de una organización.
- Routers Firewall, proporciona una frontera segura que filtra el tráfico de red entre redes de confianza. Se utilizan para filtrar el tráfico en función de las políticas de acceso entre subredes. Estas políticas pueden ser estatales y permitir o denegar el acceso a la zona desmilitarizada (DMZ) a nivel local.
    - Zona desmilitarizada (DMZ), se encuentra entre el interior y exterior de la red, ofrece servicios externos para el acceso exterior a través de uno o más servidores de seguridad. La DMZ es menos seguro que la red interna pero más seguro que la red externa.

1.5.1.2. Seguridad en la Capa de Distribución.

La seguridad a nivel de la capa de distribución, se la realiza a través de Listas de control de acceso (ACL), para permitir o denegar el acceso a la red de datos al usuario final, de acuerdo a los privilegios o restricciones configuradas por el administrador de la red.

1.5.2. Listas de Control de Acceso (ACLs)

"Las ACL son listas de condiciones que se aplican al tráfico que viaja a través de la interfaz del router" [7]. Con el uso de las ACL se puede restringir o permitir el tipo de tráfico que debe llegar o no a la red de datos, de acuerdo a las normas de seguridad establecidas por la institución.

Las ACL deben ser creadas en los routers, utilizando los comandos correspondientes. La estructura de una ACL se muestra en la figura 1.6.

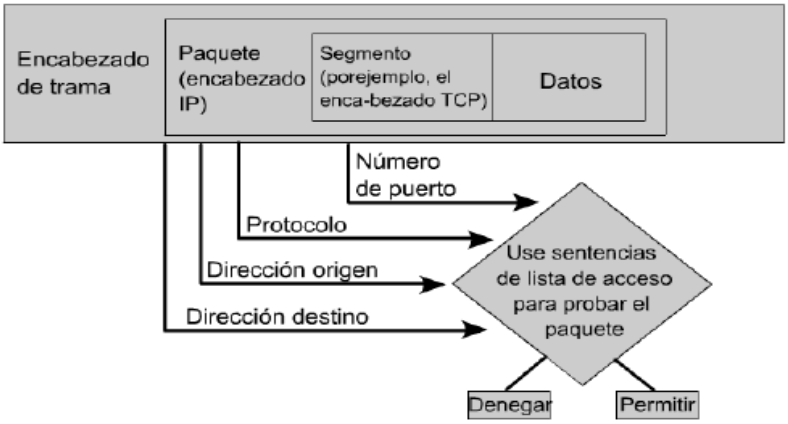


Figura1. 6. Estructura de una ACL. [8]

1.6. VLAN.

"Una VLAN es una agrupación lógica de los recursos de red y los dispositivos basados en host, en los puertos donde los host se conectan al switch o basados en la MAC de estos equipos. Una VLAN puede abarcar más de un interruptor físico" [10].

A las redes LAN es posible dividirlas en varias VLAN, sin necesidad de incrementar el equipo físico, pues como su nombre mismo lo dice son redes virtuales que se comunican entre sí como si estuvieran a la misma red. Sin embargo los equipos mencionados deben estar diseñados para soportar los estándares de comunicación de las VLANs, tal es el caso del de la norma IEEE 802.1Q, que define la estructura de la red como un puente virtual. Cuando se genera tráfico dentro de una VLAN los paquetes son enviados solamente a este grupo, lo que da como resultado una mejora en el rendimiento, fiabilidad y velocidad.

Los esquemas de comunicación que implementan VLANs, permiten que los miembros de un mismo grupo estén ubicados en diferentes espacios físicos, ya que la ubicuidad es su característica.

La seguridad es visible en la inexistencia de riesgos ante los posibles ataques; las VLANs forman parte de la seguridad de una red de datos, debido a que la segmentan y permiten la administración de los puertos, dejando ingresar sólo los paquetes permitidos o dirigidos a determinada VLAN, actuando como si fuese una red LAN independiente, esta seguridad

depende esencialmente de la administración así como también de las prestaciones de los equipos.

Existen tres métodos para la definición de pertenencia a una VLAN.

VLAN por puerto. Cada puerto de entrada que posee el switch, puede estar configurado para que se asociae a una VLAN.

Las ventajas de crear VLANs por puerto son:

- Facilidad de movimientos y cambios.
- Microsegmentación y reducción del dominio de broadcast.
- Multiprotocolo.

Desventajas.

- Administración.

VLAN por dirección MAC(Control de Acceso al Medio). La pertenencia de un equipo, está directamente relacionada con su dirección MAC, es decir que un equipo puede moverse a cualquier ubicación física, perteneciendo siempre a la misma VLAN, sin que se requiera reconfigurar el switch debio al cambio de ubicación del equipo.

Ventajas.

- Facilidad de movimientos.
- Multiprotocolo.

Desventajas.

- Problemas de rendimiento.
- Complejidad en la administración.

VLAN por filtros o por dirección de red, se basa en la información del direccionamiento IP, facilita la movilidad de los usuarios que pertenencen a una VLAN.

Ventajas.

- Segmentación por protocolo

- Asignación dinámica.

Desventajas.

- Problemas de rendimiento y control de broadcast.
- No soporta protocolos de nivel 2 ni protocolos dinámicos.

La figura 1.7 nos muestra un ejemplo de VLANs.

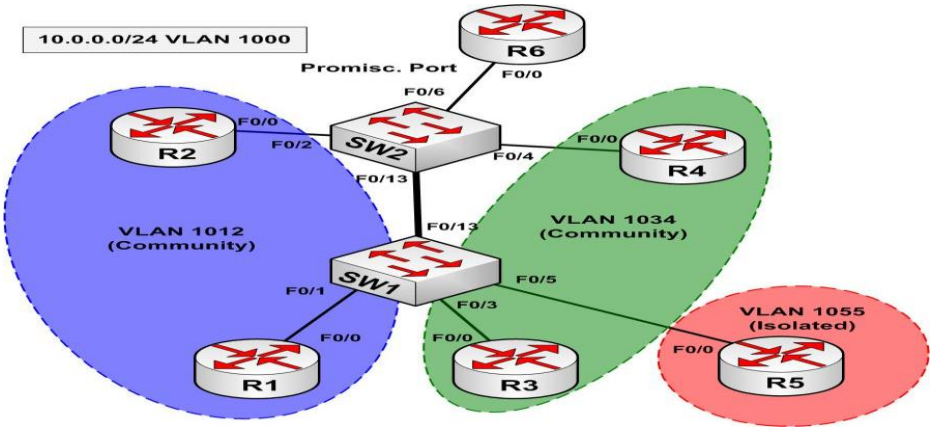


Figura 1. 7. Ejemplo de VLANs.[1]

[1] http://blog.internetworkexpert.com/wp-content/uploads/2008/07/private-vlans1.jpg.

2. LEVANTAMIENTO DE INFORMACIÓN.

2.1. Análisis de la situación actual del Centro Universitario Provincial Cariamanga (CUP).

Éste capítulo muestra el estado actual de la red del CUP, sus elementos y la forma como ésta se encuentra administrada, dicha información ha sido recolectada a través de las herramientas de investigación aplicadas, tales como: observación, entrevistas, consultas en los documentos disponibles y cuyos resultados se ven reflejados en esquemas que más adelante se muestran.

La Universidad Técnica Particular de Loja se caracteriza por estar a la vanguardia en la administración de la educación, a través de las herramientas tecnológicos y de procesos, para adaptarse a lo que la era del conocimiento exige, es por ello que continuamente brinda a sus estudiantes las mejores oportunidades de superación.

En ese mismo contexto la UTPL respalda a sus centros asociados dotándoles de todas las herramientas tecnológicas necesarias para su eficiente desempeño. Entre estos centros está el Centro Universitario Provincial de Cariamanga, lugar en el cual se desarrolla esta investigación. Se aprovecha el respaldo de la UTPL para organizar la red de datos basado en el modelo jerárquico de tres capas y los estándares 802.X de la IEEE (Instituto de Ingenieros Eléctricos y Electrónicos); además de las normas TIA(Asociación de la Industria de las Telecomunicaciones) – EIA(Asociación de la Industria Electrónica) 568 y 569, con la finalidad de optimizar sus recursos y eliminar los inconvenientes que ésta presenta en la actualidad.

Las redes de datos deben ser escalables y una forma de lograrlo es empleando el modelo jerárquico de tres capas, ya que permite solventar las necesidades de crecimiento de la red de datos cuando la población que la utiliza se incrementa, en este caso la población estudiantil del CUP se incrementa constantemente, tanto en la modalidad abierta como clásica.

Podemos demostrar que la población estudiantil del CUP ha crecido, de acuerdo a los datos proporcionados por la Secretaría, estos datos corresponden a la modalidad Abierta que van desde el período Octubre 2006 - Febrero 2007 hasta Octubre 2011 - Febrero 2012. En la figura 2.1 se observa el crecimiento progresivo, hasta llegar a un nivel que supera los 470 estudiantes a partir de Octubre 2010-Febrero 2011.

De acuerdo a las estadísticas obtenidas en el presente análisis se puede establecer que el índice de crecimiento entre el primer y último periodo académico corresponde al 53.3%, con lo

que queda demostrado que la red de datos debe estar diseñada para soportar los cambios requeridos en tamaño y complejidad.

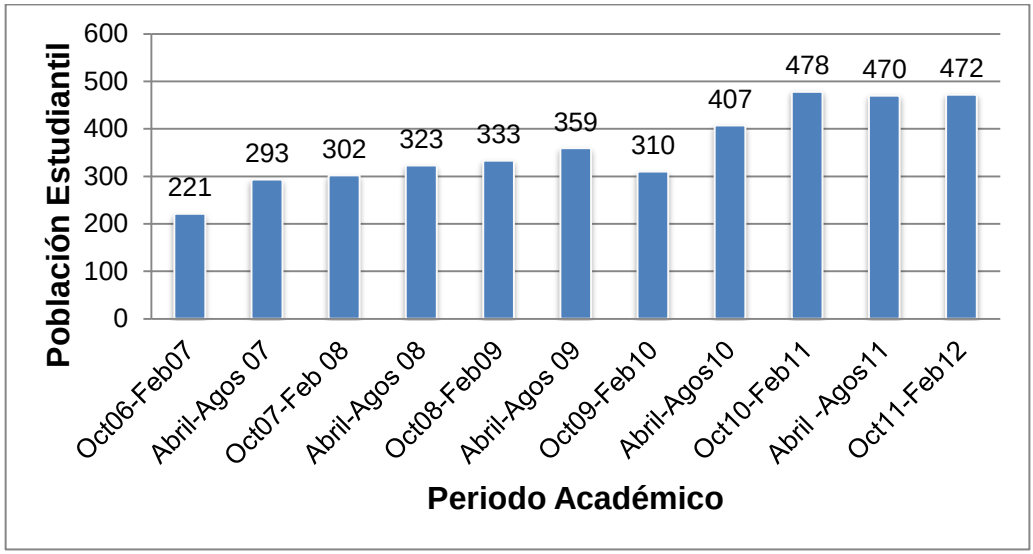


Figura 2. 1. Crecimiento Anual del CUP .

El crecimiento del CUP es dado por la calidad académica que ofrece, así como también por la tecnología de punta con la cual se le ha provisto al CUP, misma que ha ido desde la adecuación de los Centros de Cómputo con acceso a internet de banda ancha, servicio de Wifi y un Aula virtual.

El incrementar la calidad de sus servicios y la cobertura en cuanto al uso de los recursos académicos (Sistema de gestión académica, matrículas y pagos en línea, videoconferencias, biblioteca digital, correo electrónico, servicios en línea al estudiante) es un objetivo más que tiene la UTPL, es por ello que ha implementado 2 salas de cómputo con 23 computadores con el fin de procurar su uso equitativo por parte de los estudiantes y profesores en horas de clase y en prácticas de trabajo, con el fin contribuir en su formación académica. También se ha provisto de computadoras a las oficinas de las áreas funcionales y en la sala de reuniones.

2.2. Esquema de la Red de la UTPL Cariamanga.

El CUP cuenta con 2 infraestructuras de red de datos de topologías en estrella para la red del área administrativa y en árbol para el canal de videoconferencias, red inalámbrica y salas de cómputo, cuyo funcionamiento no se encuentra segmentado en capas; sus equipos de red principales son de marca CISCO. La figura 2.2 muestra cómo se encuentran físicamente constituidas las redes.

2.3. Descripción del esquema de la red.

2.3.1. Área Administrativa.

El área administrativa está constituida por cuatro dependencias y conforma la red de datos del mismo nombre, cuyo dispositivo de red principal es un router Cisco 2600. Las dependencias mencionadas se enumeran a continuación:

- Dirección.
- Secretaría.
- Coordinación Técnica.
- Biblioteca.

Cada dependencia cuenta con 2 puntos de red, pero actualmente solo uno es utilizado.

La red del área administrativa, se conecta a la red de datos de la matriz UTPL y a Internet, proporcionado por el proveedor de Internet 1 con un ancho de banda de 1 Megabit por segundo (Mbps).

2.3.2. Área de Centros de cómputo.

El área de Centro de cómputo pertenece a la red del mismo nombre, el router utilizado es de tipo Cisco 881, está conformado por:

- Sala A.
- Sala B.
- Red inalámbrica.

Esta red de datos se conecta a Internet a través del proveedor de Internet 2 con un ancho de banda de 1Mbps.

La red de centros de cómputo cuenta con dos servidores, uno de ellos tiene instalado BrazilFW que actúa como cortafuegos (bloqueando los accesos no autorizados), mientras que el segundo es un servidor dedicado que administra el antivirus Kaspersky, manteniéndolo actualizado para evitar que programas maliciosos afecten la red de datos.

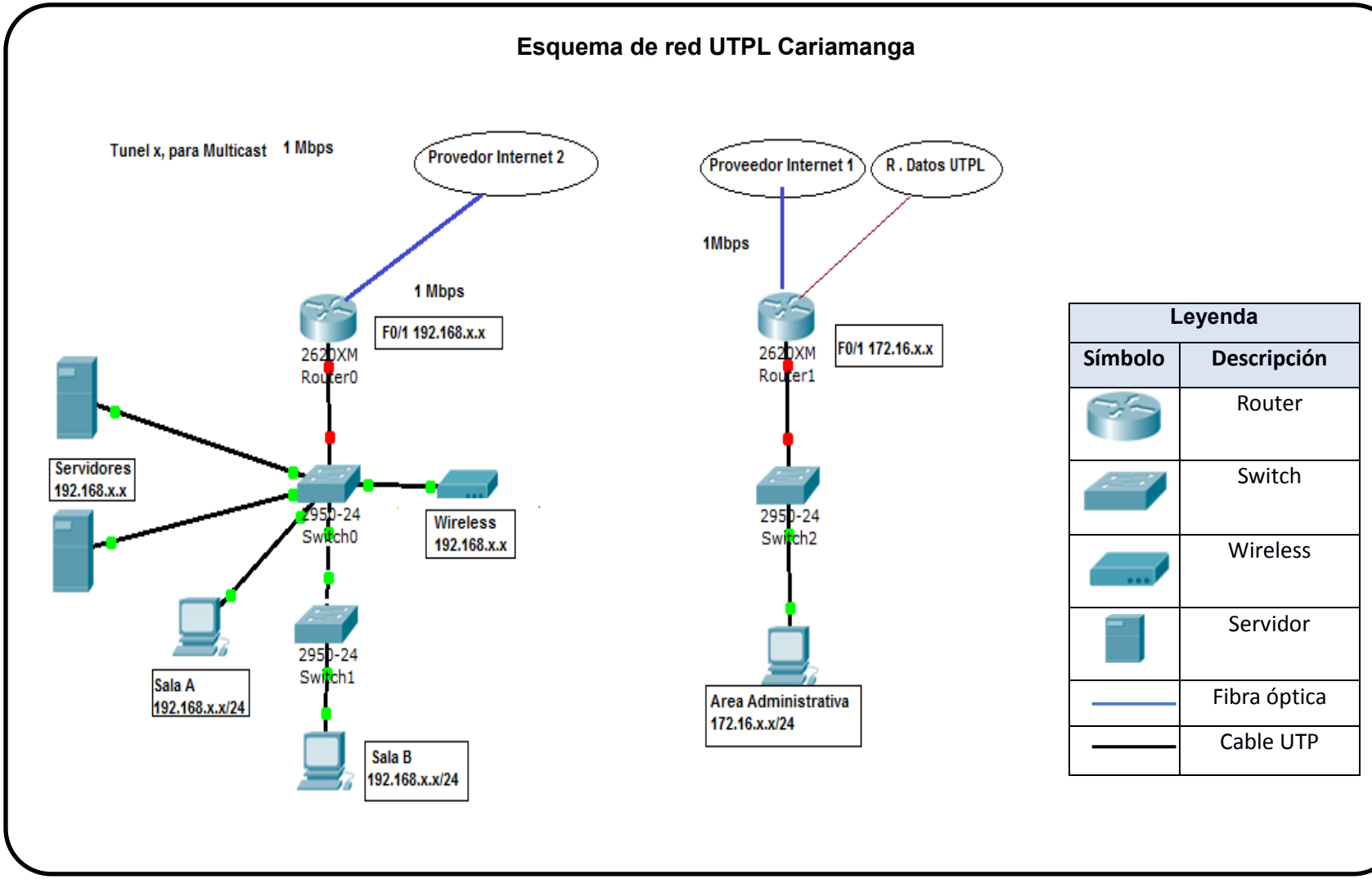


Figura 2. 2. Redes LAN del CUP.

Las salas de cómputo están dotadas de 23 computadoras, distribuidas entre la Sala A y B (13 y 10 respectivamente) asignadas para los estudiantes y profesores. El CUP además cuenta con una red inalámbrica para brindar una mejor atención y accesibilidad informática a los estudiantes, que hacen uso de los recursos educativos disponibles en la red, a través de sus portátiles y teléfonos inteligentes en cualquier sitio dentro del campus universitario. A la red de datos de centros de cómputo se conecta el aula virtual (mecanismo de distribución de información a través de Internet en tiempo real), está debidamente equipada y cuenta con tecnología sincrónica (interacción en tiempo real entre el facilitador y los estudiantes, es decir de uno a uno, de uno a muchos o de muchos a muchos), con una conexión de tipo multicast.

2.3.3. Distribución de computadores personales (PCs) dentro del CUP.

EL CUP dispone de los siguientes PCs para el desarrollo normal de sus funciones. A mayor detalle la cantidad y el área asignada para su uso la podemos observar en la tabla 2.1.

Tabla 2. 1. Distribución de PCs dentro del CUP.

Área	Nº de máquinas Disponibles
Secretaría	1
Dirección	1
Coordinación Técnica	1
Biblioteca	1
Control de Asistencia	1
Aula Virtual	1
Sala de Server (Proxy+DHCP+ Antivirus, BrazilFW)	2
Sala A	13
Sala B	10
Total	**31**

2.4. Esquema de Direccionamiento.

La infraestructura de red del área administrativa cuenta con un direccionamiento IP (Protocolo de Internet) de tipo privado clase B y es la siguiente 172.16.251.X/24.
Para la red de datos de Centros de Cómputo se emplea un direccionamiento IP privado de clase C 192.168.X.X/24. A continuación se hace conocer cuál es la dirección IP asignada a cada uno de dispositivos principales, que conforman las redes de datos.
Empezaremos mostrando las direcciones IP más relevantes en la tabla 2.2.

Tabla 2. 2. Direccionamiento IP del CUP.

Área	Dirección
Administrativa	172.16.251.0/24
Sala de Server	192.168.3.2(BrazilFW) 192.168.3.3(Antivirus)
Sala A	192.168.0.10/24
Sala B	192.168.0.31/24
Red inalámbrica	192.168.0.100

2.4.1. Direccionamiento principal.

El direccionamiento IP de los equipos principales de las redes de datos pertenecientes al CUP, corresponden a los routers y servidores, las podemos observar en la Tabla 2.3.

Tabla 2. 3. Direccionamiento principal de las redes de datos del CUP.

Sumario	Dispositivo	Interfaz	Hostname	IP	Máscara de Subred	Gateway por Defecto	DNS 1	DNS 2
Datos	Proveedor 1	Fa0/0		172.16.251.10	255.255.255.0	172.16.251.10	172.16.50.55	172.16.50.58
Internet y Multicast	Proveedor 2	WAN	Unknow	192.168.3.1	255.255.255.0	192.168.3.1	200.31.6.34	200.31.30.47
		Fa0/0	BrazilFW	192.168.3.2	255.255.255.0	192.168.3.1	200.31.6.34	200.31.30.47
		Fa0/1	Server AV	192.168.3.3	255.255.255.0	192.168.3.1	200.31.6.34	200.31.30.47
		Fa1/0	n/n	192.168.3.4	255.255.255.0	192.168.3.1	200.31.6.34	200.31.30.47
		Fa1/1	n/n	192.168.3.5	255.255.255.0	192.168.3.1	200.31.6.34	200.31.30.47

2.4.2. Direccionamiento IP del Área Administrativa.

Las direcciones IP asignadas a cada dependencia del área administrativa se muestran en la tabla 2.4.

Tabla 2. 4. .Direccionamiento IP del Área Administrativa del CUP.

Dispositivo	Interfaz	IP	Máscara de Subred	Gateway por Defecto
Secretaria1	NIC	172.16.251.1	172.16.251.10	172.16.50.55
Secretaria2	n/n	172.16.251.2	172.16.251.10	172.16.50.55
Biblioteca1	NIC	172.16.251.3	172.16.251.10	172.16.50.55
Biblioteca2	n/n	172.16.251.4	172.16.251.10	172.16.50.55
Dirección	NIC	172.16.251.5	172.16.251.10	172.16.50.55
Coord. Tec	NIC	172.16.251.6	172.16.251.10	172.16.50.55
Sala Reunión	n/n	172.16.251.7	172.16.251.10	172.16.50.55

2.4.3. Direccionamiento IP de la Sala A.

El direccionamiento IP de la Sala A se muestra en la tabla 2.5.

2.4.4. Direccionamiento IP de la Sala B.

El direccionamiento IP de la Sala B, se encuentra detallada en el tabla 2.6.

Tabla 2. 5. Direccionamiento IP de la Sala A del CUP.

Dispositivo	Interfaz	IP	Máscara de Subred	Gateway por Defecto
SalaA_PC1	NIC	192.168.3.11	255.255.255.0	192.168.0.1
SalaA_PC2	NIC	192.168.3.12	255.255.255.0	192.168.0.1
SalaA_PC3	NIC	192.168.3.13	255.255.255.0	192.168.0.1
SalaA_PC4	NIC	192.168.3.14	255.255.255.0	192.168.0.1
SalaA_PC5	NIC	192.168.3.15	255.255.255.0	192.168.0.1
SalaA_PC6	NIC	192.168.3.16	255.255.255.0	192.168.0.1
SalaA_PC7	NIC	192.168.3.17	255.255.255.0	192.168.0.1
SalaA_PC8	NIC	192.168.3.18	255.255.255.0	192.168.0.1
SalaA_PC9	NIC	192.168.3.19	255.255.255.0	192.168.0.1
SalaA_PC10	NIC	192.168.3.20	255.255.255.0	192.168.0.1
SalaA_PC11	NIC	192.168.3.21	255.255.255.0	192.168.0.1
SalaA_PC12	NIC	192.168.3.22	255.255.255.0	192.168.0.1
SalaA_PC13	NIC	192.168.3.23	255.255.255.0	192.168.0.1
SalaB_PC10	NIC	192.168.3.40	255.255.255.0	192.168.0.1

Tabla 2. 6. .Direccionamiento IP de la sala B del CUP.

Dispositivo	Interfaz	IP	Máscara de Subred	Gateway por Defecto
SalaB_PC1	NIC	192.168.3.31	255.255.255.0	192.168.0.1
SalaB_PC2	NIC	192.168.3.32	255.255.255.0	192.168.0.1
SalaB_PC3	NIC	192.168.3.33	255.255.255.0	192.168.0.1
SalaB_PC4	NIC	192.168.3.34	255.255.255.0	192.168.0.1
SalaB_PC5	NIC	192.168.3.35	255.255.255.0	192.168.0.1
SalaB_PC6	NIC	192.168.3.36	255.255.255.0	192.168.0.1
SalaB_PC7	NIC	192.168.3.37	255.255.255.0	192.168.0.1
SalaB_PC8	NIC	192.168.3.38	255.255.255.0	192.168.0.1
SalaB_PC9	NIC	192.168.3.39	255.255.255.0	192.168.0.1

2.5. Tipo de tráfico de la red.

El tráfico de una red de datos es la cantidad de información que fluye a través de esta, es decir toda la información que envía y recepta.

El identificar el tipo de tráfico que circula a través de la red, ayuda a conocer su estado, congestión y rendimiento. Con esta información podemos incrementar su productividad evitando su congestionamiento y disminuyendo los costos. Además permite establecer el número de VLANs que se requieren implementar en la red de datos del CUP.

Con la finalidad de determinar el tipo de tráfico que circula a través de las redes de datos del CUP, se las ha segmentado en secciones tal y como podemos observar en la figura 2.3

Para realizar el análisis de identificación del tipo de tráfico se toma en cuenta los parámetros de la tabla 2.7 [19]. El resultado del análisis realizado se observa en la tabla 2.8, en donde se encuentra especificado el tipo de tráfico que circula a través de las redes de datos del CUP.

Tabla 2. 7.Parámetros para identificar el tipo de tráfico de una red de datos.

Tráfico	Latencia	Fluctuación de Base	Ancho de banda
Voz	Bajo	Bajo	Medio
Datos de Transacción	Medio	Medio	Medio
Mensajería	Alto	Alto	Alto
Transferencia de archivos	Alto	Alto	Alto
Datos en lote	Alto	Alto	Alto
Administración de red.	Alto	Alto	Bajo
Videoconferencia	Bajo	Bajo	Alto

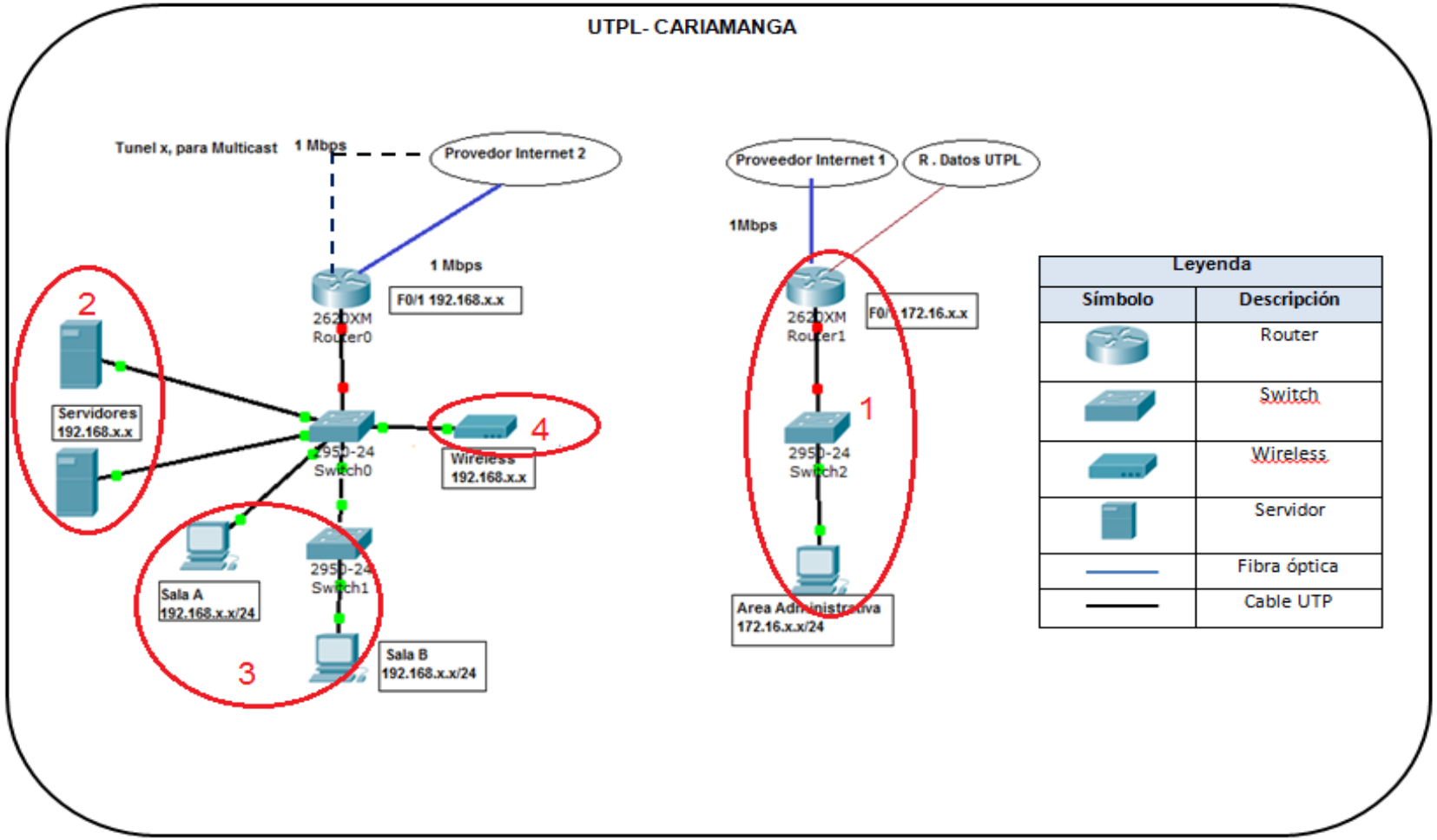


Figura 2. 3. Áreas para identificar el tráfico de la red.

Tabla 2. 8. Tipo de tráfico de las redes de datos del CUP.

Sección	Área	Tipo de tráfico	Sistemas que generan tráfico
1	Área Administrativa	Datos de Transacción	Syllabus II Sistemas de Gestión Académica Pagos en línea Servicios Online al Estudiante
		Mensajería	EVA (Entorno Virtual de Aprendizaje) Correo Electrónico UTPL
2	Sala Server	Transferencia de archivos externa	Servidor 2.- Base de datos del Antivirus (actualización de la base de datos de virus)
3	Salas de Cómputo.	Datos de Transacción	Sistemas de Gestión Académica Servicios Online al Estudiante
		Mensajería	EVA (Entorno Virtual de Aprendizaje) Correo Electrónico UTPL
4	Red Inalámbrica	Datos de Transacción Videoconferencia	Sistemas de Gestión Académica One Touch.

Es importante señalar que un análisis exhaustivo determinará la importancia de implementar esta propuesta, que va a permitir el mejoramiento de la red de datos con el fin de tener un crecimiento ordenado y escalable de la red a futuro. En la tabla 2.9 se muestra el tipo de tráfico que circula por la Red de datos de la UTPL, así como también los sistemas que generan dicho tráfico.

Tabla 2. 9. Tipo de tráfico generado en la red de datos de la UTPL.

Tráfico	Descripción	Sistemas que generan tráfico
Voz	Transmisión de voz a través del protocolo IP.	Para lograr esta comunicación, se implementó en la UTPL la arquitectura Asterisk: Actualmente está implementado para establecer comunicación entre algunos centros asociados: Quito, Cuenca y New York. Este servicio también está habilitado para algunas áreas pertenecientes a la UTPL en la ciudad de Loja.
Datos de Transacción	Sistemas de Gestión de Base de Datos.	Las bases de datos a las que se pueden acceder son: Sistemas de Gestión Académica, Sistema Financiero, Sistema de Trámites Académicos, Sistema Online al Estudiante, Pagos en línea, Intranet, CITTES(Centros de Investigación, Transferencia de Tecnología Extensión y Servicios), CEDIB(Centro de distribución bibliográfica), TIAP, Portafolio Electrónico, QULView
Mensajería	Envío y recepción de mensajes escritos en tiempo real.	Se puede hacer uso del servicio de mensajería a través del EVA, y a través del correo electrónico de UTPL cuyo servicio es brindado por google.
	Servicio brindado a través de un servidor FTP. En el	

Transferencia de archivos.	cual los usuarios subimos un determinado archivo al servidor, para luego poder descargarlo las veces que sea necesario.	Actualmente la UTPL no cuenta con este servicio.
Datos en lote	Manejo de grandes cantidades de Información.	El Sistema de la UTPL: Interface Financiero Baan.
Administración de red.	Sistemas utilizados para administrar una red de datos.	La administración de las redes de la UTPL se las hace a través de SSH(Secure SHell) que sirve para acceder a máquinas remotas, HTTP (protocolo de transferencia de hipertexto) y HTTPS(Protocolo seguro de Hipertexto) Además la UTPL utiliza, sistemas de monitoreo como: Cacti, Nagios, Allot, WLC (Controlador Inalámbrico LAN)
Videoconferencia	Comunicación simultánea de audio y video.	Para acceder a las videoconferencias los diferentes Centros Asociados lo hacen a través de One Touch o a través del EVA.

2.6. Análisis de Requerimientos.

En base al análisis de la situación actual, se identifica que el CUP requiere implementar un diseño eficiente de red de datos que garantice su rendimiento y disponibilidad. La tabla 2.10 describe los requerimientos funcionales.

Tabla 2. 10. Requerimientos Funcionales.

Requerimientos	**Descripción.**
Diseñar una red de datos eficiente.	Un diseño eficiente de la red de datos garantiza su rendimiento.
Solución basada en el modelo Jerárquico de tres capas.	Le permite adaptarse a los cambios de acuerdo al crecimiento de la red.
Mejorar el rendimiento y seguridad de la red.	Utilizar esquemas de comunicación que resuelvan la falta de rendimiento y seguridad de la red.
Adaptar la infraestructura de red.	Una infraestructura de red óptima garantiza la transmisión de datos a mayor velocidad, adaptándose a las necesidades de la institución.
Monitorear la red de datos.	Conocer el estado de la red actual.

2.7. Solución planteada.

Ante los requerimientos identificados se propone:

- Diseñar una infraestructura de red de datos óptima, basada en el modelo jerárquico de tres capas, lo que permitirá una fácil administración e identificación rápida de los problemas.
- Optimizar los recursos disponibles, uniendo las redes existentes.
- Segmentar lógicamente la red de datos, mediante VLANs basadas en las áreas de trabajo, para mejorar el rendimiento y seguridad.
- Organizar la red de datos cumpliendo los estándares TIA/EIA 568 -569, para actualizar la infraestructura asegurando interconectividad entre todas las áreas funcionales del CUP.
- Monitorear el estado de la red de datos actual (ver figura 2.2), haciendo uso de las herramientas tecnológicas disponibles, con la finalidad de conocer el estado de la red,

ofrecer un soporte rápido, eficiente y oportuno si surgiera una falla que afecte su disponibilidad y rendimiento.

- Adquirir los equipos de red configurables, necesarios para la implementación de la Red Jerárquica de tres capas.

3. SELECCIÓN DE LA HERRAMIENTA TECNOLÓGICA PARA LA IMPLEMENTACIÓN DE LA PROPUESTA.

3.1. Selección de la herramienta para la implementación del modelo jerárquico de tres capas en un ambiente simulado.

La evaluación de los diseños de redes de datos, en las diferentes herramientas disponibles para su simulación permite conocer de antemano su funcionamiento antes de implementarlo.

Debido a que existen muchas herramientas disponibles ya sea gratuitas o pagadas creadas para la simulación de redes, se propone realizar el estudio de las herramientas gratuitas y de calidad entre ellas las más populares GNS3 y Packet Tracer debido a las ventajas que nos ofrecen: robustez, disponibilidad, eficacia, flexibilidad, etc.

3.1.1. GNS3. [26]

GNS3 es una herramienta especializada en la simulación gráfica de redes de datos que permite implementar el diseño de redes de datos en las diferentes topologías. “Soporta el IOS de los routers, ATM/Frame Relay/ switches Ethernet y PIX firewall”.

GNS3 está basado en Dynamips, PEMU(incluyendo el encapsulador) y Dynagen, desarrollado en Phyton, utiliza la tecnología SVG (gráficos vectoriales escalables), que lo provee de símbolos para el diseño de las topologías de redes

Dynamips. Es un emulador de routers Cisco, “permite probar las funciones de Cisco IOS” [26] y las configuraciones realizadas.

Dynagen. Es un front end, provee una separada OOP API utilizada por GNS3 para interactuar con Dynamips.

3.1.2. Packet Tracer.

Packet Tracer es un simulador de redes que permite modelar y probar diseños de redes de datos, seleccionando los equipos necesarios para conocer su funcionamiento y evaluar su desempeño. Brinda la oportunidad de crear grandes redes sin la necesidad de tener 2 o más computadores o demás dispositivos de red, interfaces y cables, etc.

Durante la simulación se pueden detectar y resolver los problemas que pudieran darse en la infraestructura de comunicaciones.

3.1.3. Análisis y Selección de la herramienta.

Las herramientas expuestas en la sección anterior, permiten simular las diferentes infraestructuras de redes, para que al ser implementadas las comunicaciones sean confiables. La tabla 3.1 permite establecer un análisis comparativo de las herramientas antes mencionadas.

Con la información reolectada, se establece que la mejor alternativa es utilizar el Packet Tracer por las características que ofrece, sobre todo porque permite comprobar el funcionamiento y configuración de la red de datos que se propone para el CUP, en donde intervienen 6 switches y 5 routers a más de los PCs. La adaptabilidad de la herramienta permite realizar la simulación desde un computador de medianas prestaciones sin disminuir su productividad, por lo que no se requiere incrementar más equipos para ejecutar la simulación.

Si la simulación se la llegara a realizar en GNS3 se necesitaría Pcs adicionales para distribuir la carga de trabajo que se produce durante la simulación, además se necesita adquirir el IOS de Cisco ya que los equipos a implementar son de tipo Cisco, convirtiéndose en desventajas.

Tabla 3. 1. Análisis comparativo entre GNS3 y Packet Tracer.

GNS3[23]	Packet Tracer [24]
Es un simulador de redes.	Es un simulador de redes.
Fácil de usar.	Fácil de usar.
Fácil instalación.	Fácil instalación.
Gratuito.	Gratuito.
Trabajo con sistemas IOS reales, y no distribuye los IOS de Cisco por lo que los usuarios deben comprarlo.	Permite la configuración global en el IOS que provee CISCO.
Apropiado para simular grandes redes, ya que permite que un cliente GNS3 pueda correr en una máquina diferente al que contiene el emulador repartiendo el procesamiento entre varios PCs.	No necesita tener dispositivos como computadoras, routers, cables, etc para conocer el comportamiento físico y real de una red.
Al emular más de 3 routers en un solo computador, esta no responde.	Permite simular grandes cantidades de routers y switches en un mismo computador sin inconveniente.
Para su correcto funcionamiento requiere un computador o computadoras con altos recursos.	Permite la ejecución de la simulación en un computador con recursos básicos.

3.2. Selección de la herramienta para el monitoreo de la red de datos actual.

En la actualidad existen herramientas disponibles que permiten monitorear y dar a conocer el estado de la red de forma permanentemente, razón por la cual se las debe aprovechar y aplicar, generalmente son fáciles de usar, robustos, escalables, etc. A continuación se hace conocer algunas de las herramientas disponibles:

3.2.1. Cacti. [15]

- Cacti es una solución de red completa de gráficos diseñado para aprovechar el poder de RRDtool's (es el estándar de la industria OpenSource, los datos de registro de alto rendimiento y la representación gráfica del sistema de datos de series temporales) en almacenamiento de datos y la funcionalidad de gráficos.
- Ofrece una rápida poller, una gráfica avanzada de plantillas, múltiples métodos de adquisición de datos. Presenta una interfaz intuitiva y fácil de usar.
- Es adaptable a las pequeñas y grandes redes.
- Gratuito.

3.2.2. NetCrunch 6. [16]

- NetCrunch descubre automáticamente su red de forma instantánea y crea vistas personalizadas de su infraestructura.
- NetCrunch es una solución de monitoreo multiplataforma.
- Se puede monitorizar redes sin agentes.
- NetCrunch permite monitorizar estaciones de trabajo y servidores Windows, Linux, Mac OS X, BSD, NetWare.
- NetCrunch unifica y consolida la administración de fallas colectando y alertando eventos recibidos de una variedad de fuentes externas tales como: Windows Event Logs, syslog, SNMP trampa.
- El programa presenta en tiempo real los datos recién guardados usando los gráficos que muestran los valores de los contadores de las últimas horas. Es posible también ver los datos históricos con su distribución de los valores.
- Herramienta pagada.

3.2.3. WhatsUp Gold [16].

- Administra todos los tamaños de redes.

- Capa 3 automatizada y rápida detección de dispositivos, utilizando varios tipos de opciones de detección incluyendo SNMP SmartScan, análisis de rango de direcciones IP, análisis de dispositivos individuales.
- Consigue mapas jerárquicos de la capa 3 de la red, incluyendo una representación completa de la red real y entorno de aplicación, con desgloses a subredes y redes LAN virtuales.
- Utiliza una estrategia de vigilancia activa y pasiva, el Whatsup realiza el seguimiento del estado y la salud de todos sus dispositivos de red.
- Recibe una alerta temprana de escucha para las capturas de SNMP y mensajes de syslog de los dispositivos de la infraestructura.
- Centro de Alerta de WhatsUp Gold le da un único panel de control integrado que consolida todas las alertas, notificaciones y acuses de recibo de alerta para una fácil configuración y gestión**.**
- Permite obtener una visión completa de la salud y el rendimiento de su red con informes de WhatsUp Gold, estos informes son personalizables.
- Herramienta pagada.

3.2.4. Munin. [18]

- Permite realizar una recopilación gráfica de la evolución del uso de los recursos durante el tiempo.
- Cuenta con una interfaz web que muestra la evolución histórica del uso de recursos durante el tiempo.
- Munin monitorea el uso de recurso de cada máquina, recursos como disco, red, uso de CPU, RAM, Carga (load).
- También es capaz de monitorear indicadores de algunas aplicaciones como procesos de apache, consultas de mysql entre otras.
- Genera gráficas por día, semana, mes y año de cada uno de los indicadores.

- Muestra el mínimo, máximo, media y valor actual los indicadores en cada periodo de tiempo.
- Es posible configurar umbrales de alerta para estado de advertencia y crítico.
- El servidor corre sobre Linux, el agente corre sobre Linux y Windows (con algunas limitaciones).
- Gratuita.

3.2.5. Nagios. [18].

- Permite tener un control exhaustivo del estado de los servicios de los diferentes servidores de manera centralizada.
- El principal objetivo de esta herramienta es censar el estado de aplicaciones mediante escaneo de puertos, ejecución de comandos o la ejecución de cualquier prueba que pueda determinar si un servicio está corriendo correctamente.
- Permite realizar pruebas sobre infinidad de servicios.
- Permite ejecutar alertas según el tipo de evento.
- Permite detectar los problemas antes que causen daños mayores.

3.2.6. Análisis y Selección de la Herramienta.

Todas las herramientas expuestas anteriormente permiten monitorear redes de datos, algunas con prestaciones diferentes. La tabla 3.2 se muestra el análisis comparativo, que permitirá seleccionar la herramienta que se adapte a nuestras necesidades, estableciendo un análisis de las herramientas por el número de servicios que cada una nos ofrece y se evidencia que todas no disponen de todos los servicios, siendo unas más efectivas que otras de acuerdo a la aplicabilidad.

El CUP requiere de herramientas, que permitan monitorear el estado y los dispositivos de red, las 24 horas del día y los 7 días a la semana y para ello se ha elegido como la mejor alternativa las herramientas Cacti y WhatsUp Gold, cuya descripción consta en la sección anterior.

Tabla 3. 2. Servicios de las herramientas de monitoreo.

Servicios	Cacti	NetCrunch 6	WhatsUp	Munin	Nagios
Representación gráfica.	x	x	x	x	x
Descubre automáticamente la red.		x	x		
Multiplataforma.	x	x			
Alertas.	x		x		x
Almacena datos históricos.	x	x	x	x	
Capturas SNMP.	x		x		
Monitorea los dispositivos de red.		x	x	x	
Monitorea el rendimiento de la red.	x				
Censar aplicaciones.					x
Presentación de informes.			x	x	
Gratuito.	x			x	

Cacti y WhatsUp Gold permiten:

- Monitorear cada uno de los equipos que forman parte de la red en tiempo real. Los equipos a monitorear son los routers, switches y servidores.

- Permite monitorear las interfaces de los dispositivos de red.
- La información de la red se presenta en modo gráfico de acuerdo a los datos recolectados en determinado momento, ya sea, por hora, día, mes.
- Permiten monitorear el tráfico entrante y saliente de la red.
- Permiten configuraciones para enviar alertas cuando alguna falla se suscita.
- Permiten generar reportes.

Con el uso de estas herramientas, se logrará tener la red monitoreada y controlada, pues los problemas que puedan surgir, serán solucionados en el menor tiempo posible.

4. DISEÑO DE LA PROPUESTA.

Con la información recolectada durante el levantamiento de la información, se crea el diseño de la red LAN basado en el modelo Jerárquico de tres capas que se adapte a las necesidades del CUP, adicionalmente la implantación del NOC (Centro de Control de Operaciones de la Red) que permitirá monitorear constantemente el estado actual de la red de datos.

4.1. Propuesta del Modelo Jerárquico de tres Capas.

Las redes de datos basadas en el modelo jerárquico de tres capas son adaptables a los requerimientos de cada institución, la infraestructura de red propuesta se muestra en la figura 4.1, esta está basada en los principios claves del diseño de la red jerárquica expuestos en la sección 1.4

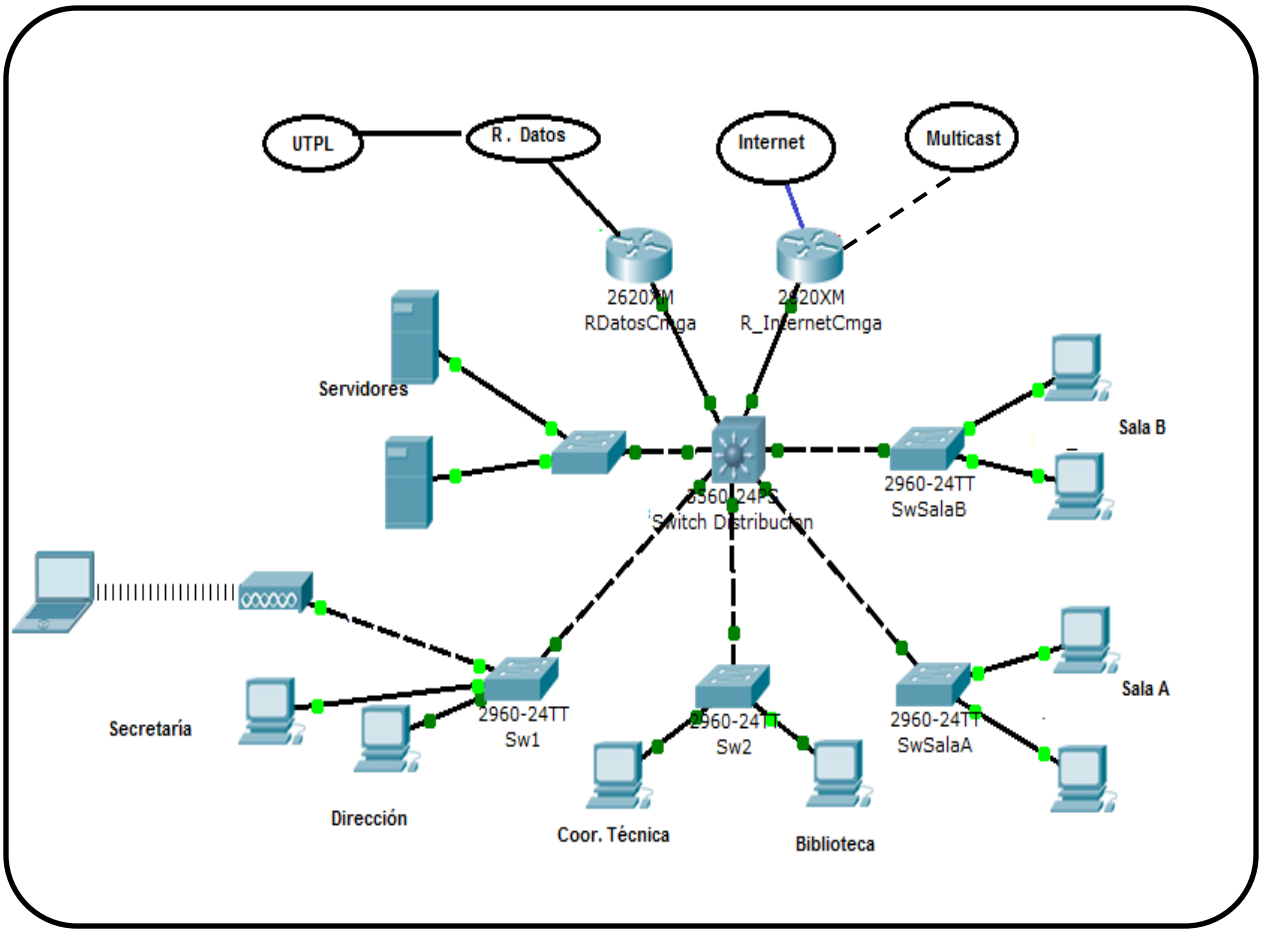


Figura 4. 1. Diseño de Red basado en el Modelo Jerárquico de tres capas para el CUP.

El diseño de infraestructura de red propuesto para el CUP, está creado bajo el modelo jerárquico de tres capas, para asegurar su rendimiento, disponibilidad, seguridad, escalabilidad, administración, mantenimiento y utilizar mejor los recursos.

La red Jerárquica propuesta acopla las 2 redes de datos existentes del CUP, es decir, la red denominada Área de Administración y la red de Centros de Cómputo. En el modelo propuesto claramente se identifican las capas de acceso, distribución y núcleo, cada una está constituida de la siguiente manera:

Capa de acceso. Está conformada por 5 switches, proporciona a los usuarios el acceso a la red y es el encargado de conmutar paquetes hacia la capa de distribución. A esta capa estarán asociadas las VLANs necesarias previamente establecidas.

Capa de distribución. Está compuesta por un switch de capa 3 o de distribución, que conmuta los paquetes de datos a gran velocidad, en esta capa se segmenta la red de datos en varios dominios de broadcast de acuerdo a las configuraciones que se establecerán.

Este switch estará configurado como VTP(protocolo de enlace troncal de VLAN) en modo servidor, que permitirá tener un dominio administrativo unificado de la red; los switches de la capa de acceso conectados a este dispositivo deben estar configurados en modo cliente.

Capa Núcleo. Esta capa está compuesta por 2 routers, estos permitirán la comunicación con la Red de datos de la UTPL y con Internet.

El detalle de los switches que conforman la red jerárquica de tres capas, la encontramos en la tabla 4.1. Cada uno de los switches de la capa de acceso se conecta al SW1, que a su vez se interconecta con los routers que conforman la capa núcleo.

La red inalámbrica está creada bajo el estándar IEEE 802.11 [20] y cuyo punto de acceso (Access Point) se conecta al SW3. La red inalámbrica es para uso de los estudiantes y docentes o en fin para los miembros del CUP que hacen uso de sus computadores portátiles dentro del campus universitario. Además la red inalámbrica es usada como una vía alterna para las videoconferencias, en caso de que fuese necesario.

Tabla 4. 1. Distribución de los Switches de la Red Jerárquica de tres capas.

Switch	Detalle
SW1	Switch de distribución o de capa 3, al cual se conectan los diferentes switches de la capa de acceso.
SW2	Se conecta a los servidores de la red.
SW3	A este switch se conecta el área de Dirección, Secretaria y el Access Point.
SW4	Conecta el área de Coordinación Técnica y Biblioteca.
SW5	Conecta la Sala A
SW6	Conecta a la sala B

Los switches que conforman el modelo jerárquico de tres capas deberán poseer un número mayor de puertos que el número de PCs disponibles en la actualidad en el CUP, lo que posteriormente permitirá el crecimiento y adaptación de la red a los nuevos requerimientos.

4.2. Identificación de VLANs de acuerdo al tráfico de la red para el CUP.

Todos los componentes de un sistema informático que se encuentren en red datos, son vulnerables ante los ataques tanto de hardware, software y datos, siendo este último objeto principal de protección, por lo que se debe garantizar su confidencialidad, integridad y disponibilidad. Como medida para incrementar la seguridad de la red, se propone crear VLANs, puesto que solo los miembros que pertenecen a una VLAN podrán compartir información y recursos tal y como si fuera una LAN creada para un grupo específico, incrementando de tal manera la seguridad.

Luego de haber analizado el tipo de tráfico que circula por la red del CUP, de acuerdo a la tabla 2.8 y 2.9, se han identificado 5 VLANs con la finalidad de proporcionar a la red mayor rendimiento y seguridad de la red de datos.Las VLANs identificadas son:

- VLAN10: Datos.
- VLAN11: Internet.
- VLAN12: VoIP.

- VLAN13: Videoconferencias.
- VLAN100: Administración del Switch.

Se puede observar y comprender como las VLANs están relacionadas con cada switch en la figura 4.2.

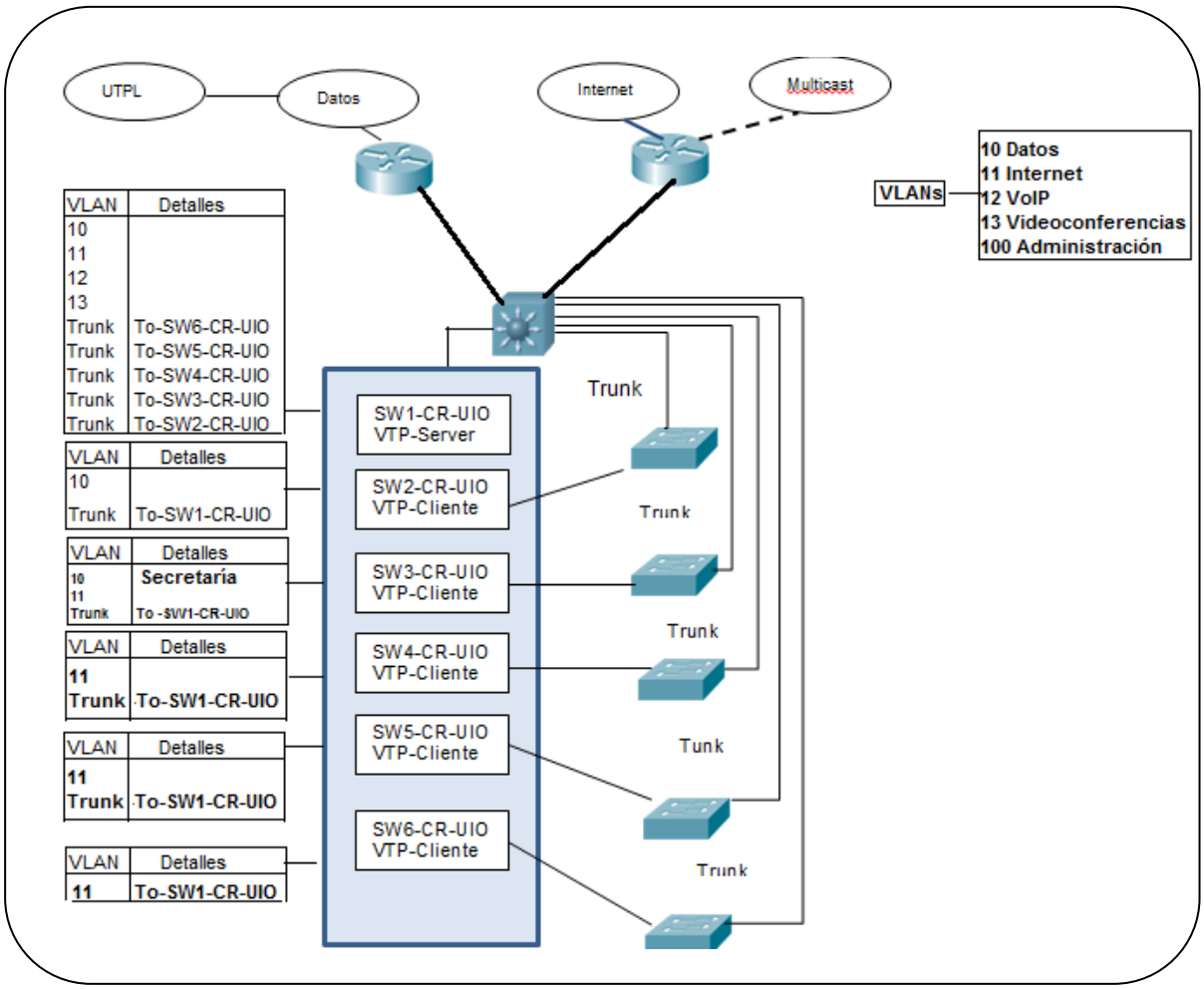


Figura 4. 2. Identificación de las VLANs de acuerdo al tráfico que circula por la red del CUP.

En la figura 4.2, la mayor parte del tráfico proviene de internet, ya que es la herramienta principal de investigación y comunicación. La única VLAN que requiere tener acceso a la red de datos es la de secretaría, que continuamente necesita conectarse a la red de datos de la UTPL para hacer uso de los sistemas: académico, financiero, de gestión, entre otros, necesarios para el cumplimiento de sus funciones. Para ello cuando se requiere trabajar con datos de la UTPL, el tráfico llega hasta el switch de distribución (Catalyst 3550), en donde se analiza hacia donde

van dirigidos los paquetes (a la red de datos, o a la red de Internet), una vez identificado hacia qué red necesitan viajar las tramas o paquetes, se dirigen hacia los routers quienes finalmente permiten o deniegan el paso de los paquetes a determinada red.

4.3. Esquema de Direccionamiento.

Para la creación del direccionamiento IP se ha considerado utilizar una dirección IPv4, de tipo privada clase B. Esto debido a que estas direcciones pueden ser utilizadas por cualquier empresa sin ningún inconveniente, ya que fueron creadas precisamente para superar la falta de direcciones disponibles.

Estas direcciones solamente son válidas dentro de su respectiva red LAN, permitiendo de esta manera la duplicación de las mismas, pero siempre y cuando no tengan conexión entre las redes LAN que las estén utilizando, a menos que se conecten con el protocolo NAT (Traducción de dirección IP). Por ejemplo en una empresa "X" pueden estar utilizando esta dirección 192.168.0.0, mientras que en otra u otras empresas pueden estar utilizando la misma, sin provocar inconveniente alguno, debido a que son redes LAN independientes.

Las direcciones IP privadas de clase B, se encuentran en el siguiente rango 172.16.0.0 a 172.31.255.255.

Cabe recalcar que no se utiliza una dirección pública de clase B, porque estas direcciones son asignadas a servidores a los cuales accedemos a través de Internet, además estas direcciones públicas funcionan como un identificador único, razón por la cual no se pueden repetir.

Para la red jerárquica propuesta utilizaremos la dirección IP **172.18.0.0/24**, misma que es de clase B de tipo privada, la máscara de subred /24 debido a que cada subred o VLAN en este caso permitirá un crecimiento máximo de hasta 256 host.

Una vez identificado el tipo de direccionamiento IP a utilizar, es conveniente dividir la red en 8 VLANs por razones de rendimiento, privacidad y seguridad y de acuerdo al tráfico identificado en la red de datos del CUP. Las VLANs están establecidas de acuerdo a las áreas que funcionan en este centro universitario.

La identificación de cada VLAN está basada en la información del direccionamiento IP, en este caso corresponde al tercer número decimal de la dirección de subred. El detalle del direccionamiento está disponible en la tabla 4.2.

4.4. Implementación del Modelo Jerárquico de tres capas en un Ambiente Simulado.

De acuerdo a la sección 3.1.3, se establece que el Packet Tracer es la mejor alternativa para realizar la simulación de la red propuesta para el CUP. Esta simulación evita que ocurran imprevistos durante la implementación y como consecuencia la falta de productividad y pérdida económica.

El diseño de la propuesta muestra: la infraestructura de red necesaria, el número de dispositivos, servicios, el número VLANS, así como el tráfico que se necesita enrutar a través de la red o hacia fuera.

Para realizar la simulación de la red Jerárquica de tres capas es necesario agregar algunos dispositivos adicionales, con la finalidad de comprobar la configuración, funcionamiento y rendimiento de la red.

Los dispositivos adicionales son:

- Un router, que pertenece a la red de datos de la matriz de la UTPL, junto con un switch y el respectivo servidor de datos.
- Un router para Multicast y un servidor de multicast.
- Un router, para la red de Internet y el respectivo servidor de Internet.

La Topología utilizada para la simulación en el Packet Tracer es la que se visualiza en la figura 4.3.

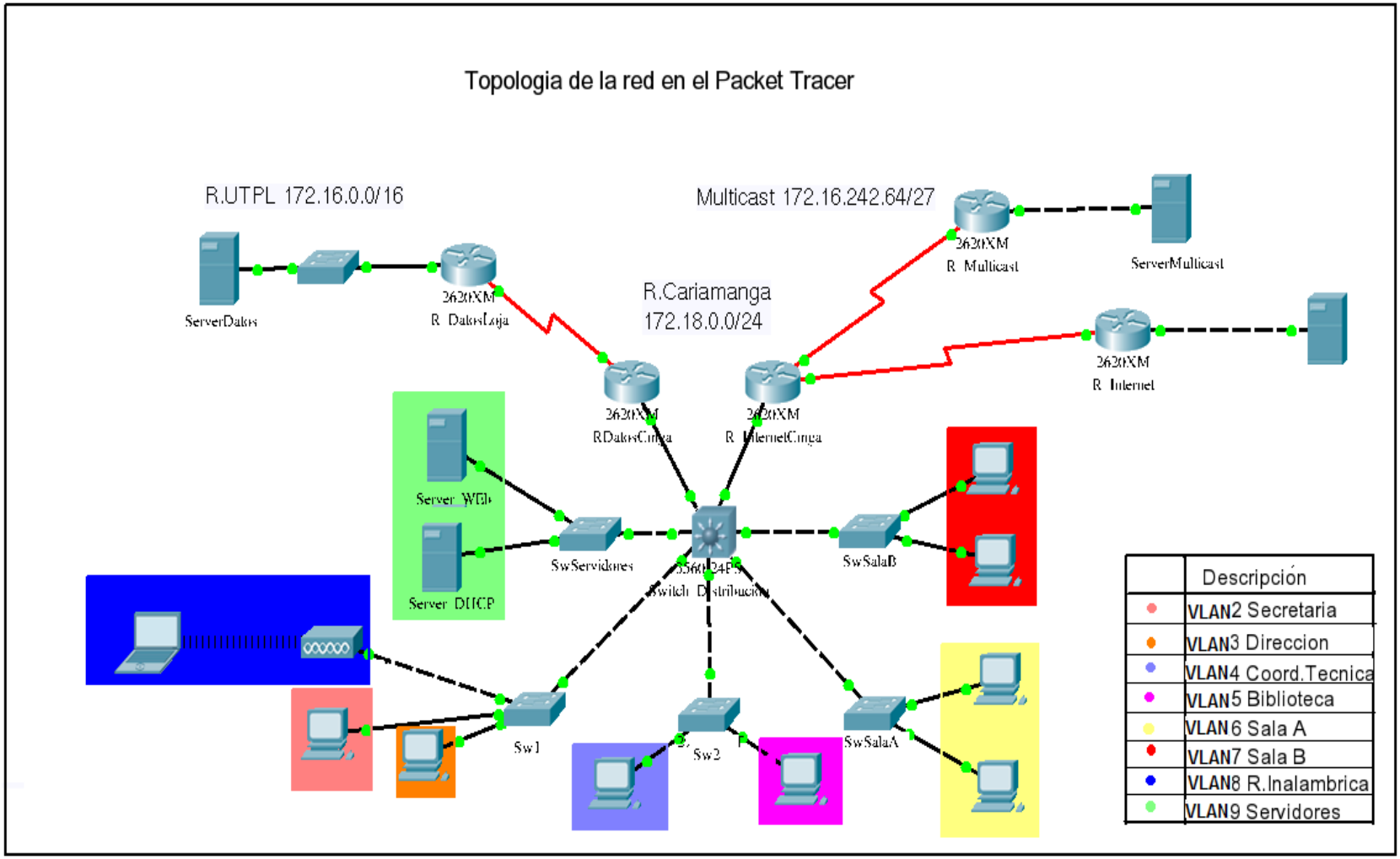


Figura 4. 3. Topología de la Red Jerárquica para la Simulación en el Packet Tracer.

4.4.1. Esquema de Direccionamiento.

El direccionamiento IP para la implementación de la propuesta, está creada como se mencionó en base a la dirección de clase B de tipo privada 172.18.0.0 empleando la máscara 255.255.255.0 ó /24, obteniéndose 8 subredes con un máximo de 256 host (2^8) por cada subred. Para la identificación de las VLANs, se toma como base la trama IEEE 802.1P/Q expuesta en la figura 4.4, que contiene el campo TAG y que incluye 3 bits para niveles de prioridad y el identificador de VLAN.

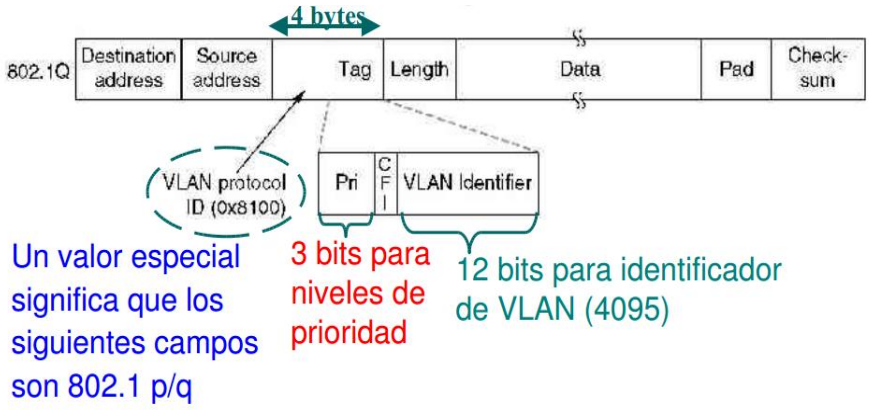


Figura 4. 4. Trama IEEE 802.1 P/Q.[27]

La tabla 4.2 resume el esquema de direccionamiento necesario para realizar la configuración de los equipos que intervienen en la red de datos, esto permitirá garantizar su óptimo funcionamiento en la red simulada y posteriormente en la real.

Tabla 4. 2. Direccionamiento IP de las VLANs para la Red Jerárquica.

Red VLAN	Descripción	Máscara	Primer Host	Gateway	Ultimo Host
172.18.1.0	VLAN9 Servidores	255.255.255.0	172.18.1.2	172.18.1.1	172.18.1.254
172.18.2.0	VLAN2 Secretaría	255.255.255.0	172.18.2.2	172.18.2.1	172.18.2.254
172.18.3.0	VLAN3Dirección.	255.255.255.0	172.18.3.2	172.18.3.1	172.18.3.254
172.18.4.0	VLAN4 Cord. Técnica	255.255.255.0	172.18.4.2	172.18.4.1	172.18.4.254
172.18.5.0	VLAN5 Biblioteca.	255.255.255.0	172.18.5.2	172.18.5.1	172.18.5.254
172.18.6.0	VLAN6 Sala A.	255.255.255.0	172.18.6.2	172.18.6.1	172.18.6.254
172.18.7.0	VLAN7 Sala B.	255.255.255.0	172.18.7.2	172.18.7.1	172.18.7.254
172.18.8.0	VLAN8 R. inalámbrica	255.255.255.0	172.18.8.2	172.18.8.1	172.18.8.254
172.18.99.0	VLAN99 de Administración	255.255.255.0			

4.4.2. Direccionamiento IP de los Routers de la Capa núcleo.

La capa núcleo de la red Jerárquica de tres capas está conformada por 2 routers, su direccionamiento IP deben ser configurados de acuerdo a los datos expuestos en la tabla 4.3.

Tabla 4. 3. Direccionamiento IP de los Routers de la capa núcleo.

Dispositivo	Nombre	Interfaz	Dirección IP	Máscara de Subred
Router 1	R. Datos Cariamanga	Fa0/0.1	172.18.10.2	255.255.255.0
		S0/0	192.168.10.1	255.255.255.252
Router2	R. Internet Cariamanga	Fa0/0.1	172.18.11.2	255.255.255.0
		S0/0	192.168.10.5	255.255.255.252
		S0/1	192.168.10.9	255.255.255.252

4.4.3. Direccionamiento IP de los Routers adicionales para la Simulación.

Para una adecuada simulación y comprobación de la funcionalidad de la red de datos, es necesario incrementar 3 routers, con los datos descritos en la tabla 4.4.

Tabla 4. 4. Direccionamiento IP de los Routers adicionales para la Simulación.

Dispositivos	Nombre	Interfaz	Dirección IP	Máscara de Subred
Router 3	R.DatosLoja	Fa0/0	172.16.24.10	255.255.255.0
		S0/0	192.168.10.2	255.255.255.252
Router 4	R.Multicast	Fa0/0	172.16.242.65	255.255.255.224
		S0/0	192.168.10.6	255.255.255.252
Router 5	R.Internet	Fa0/0	10.10.10.1	255.255.255.0
		S0/0	192.168.10.10	255.255.255.252

4.4.4. Configuración del Switch de la capa de distribución.

El switch de la capa de distribución debe ser configurado como servidor para todos los switches de la capa de acceso. Es en el switch de distribución donde se deben configurar las VLANs establecidas en la propuesta, los switches de acceso aprenden esta configuración del servidor.

Este switch de distribución se configura de acuerdo a los datos que se presentan en la tabla 4.5 que viene a continuación:

Tabla 4. 5. Direccionamiento IP de las VLANs.

Nombre	Dirección IP	Descripción
SwDis	172.18.2.0	VLAN 2
	172.18.3.0	VLAN 3
	172.18.4.0	VLAN 4
	172.18.5.0	VLAN 5
	172.18.6.0	VLAN 6
	172.18.7.0	VLAN 7
	172.18.8.0	VLAN 8
	172.18.1.0	VLAN 9
	172.18.99.0	VLAN 99 de Administración

Para tener conexión con el resto de equipos de red, es necesario crear enlaces troncales. Un enlace troncal es la conexión entre dos dispositivos de red, que sirve como medio de conducción de las VLANs. La tabla 4.6 presenta la información necesaria para realizar la configuración correspondiente a los enlaces troncales.

Tabla 4. 6. Asignación de las interfaces para los enlaces troncales.

Enlaces Troncales	
Interfaz	**Dispositivo al que se dirige el enlace**
Fa 0/1	Router de Datos Cariamanga
Fa 0/2	Router Internet Cariamanga
Fa 0/3	Switch Servidores
Gi 0/1	Switch 1
Fa 0/5	Switch 2
Fa 0/6	Switch Sala A
Fa0/7	Switch Sala B

4.4.5. Configuración de los Switches de la capa de acceso.

Cada uno de los switches que conforman la capa de acceso, deben ser configurados en modo cliente. En este caso únicamente en el switch 2 estarán configuradas 2 VLANs.

A cada VLAN solamente se le asigna un PC durante la simulación. La tabla 4.7 muestra los datos principales para configurar los dispositivos.

Tabla 4. 7. Configuración de los Switches.

Switch	Nombre	Interface Vlan	Interface	Descripción
SW 1	Sw1	172.18.99.2	Gi1/1 F0/1 F0/2 F0/3	Enlace Trunk PC VLAN2 PC VLAN3 Conexión al Access Point
SW2	Sw2	172.18.99.3	F0/1 F0/2 F0/4	Enlace Trunk PC VLAN 4 PC VLAN 5
SW3	SwSalaA	172.18.99.4	F0/2 F0/1, F0/3	Enlace Trunk PCs VLAN 6
SW4	SwSalaB	172.18.99.5	F0/1 F0/2,F0/3	Enlace Trunk PCs VLAN 7
SW5	SwServidores	172.18.99.1	F0/1 F0/2, F0/3	Enlace Trunk Conexión a la Vlan 9 (Servidores)

4.4.6. Dirección IP específica de los PCs en la simulación.

El direccionamiento IP de cada uno de los PCs que intervienen en la simulación se muestran en la tabla 4.8.

Tabla 4. 8. Direccionamiento IP de los PCs.

VLAN 2			
Nombre	**IP**	**Máscara de Subred**	**Gateway**
PC_VLAN2	172.18.2.3	255.255.255.0	172.18.2.1
VLAN3			
PC_VLAN3	172.18.3.2	255.255.255.0	172.18.3.1
VLAN4			
PC_VLAN4	172.18.4.2	255.255.255.0	172.18.4.1
VLAN5			
PC-VLAN5	172.18.5.2	255.255.255.0	172.18.5.1
VLAN6			
PC1	172.18.6.2	255.255.255.0	172.18.6.1
PC2	172.18.6.3	255.255.255.0	172.18.6.1
VLAN7			
PC1	172.18.7.2	255.255.255.0	172.18.7.1
PC2	172.18.7.3	255.255.255.0	172.18.7.1
VLAN 8			
Las direcciones para las portátiles que accedan a la red inalámbrica, se les asigna una dirección IP dinámica (DHCP).			
VLAN 9			
Servidor DHCP	172.18.1.2	255.255.255.0	172.18.1.1
Servidor Web	172.18.1.3	255.255.255.0	172.18.1.1

4.4.7. Direccionamiento IP de los Servidores de los Routers adicionales.

Es necesario configurar los servidores de los routers adicionales con los datos expuestos en la tabla 4.9.

Tabla 4. 9. Direccionamiento IP de los Routers adicionales.

Nombre	IP	Máscara de Subred	Gateway
ServerDatos	172.16.24.11	255.255.255.0	172.16.24.10
ServerMulticast	172.16.242.66	255.255.255.0	172.16.242.65
ServerInternet	10.10.10.2	255.255.255.0	10.10.10.1

Con todos los datos expuestos desde la tabla 4.2 a la 4.9, se debe realizar la configuración de los equipos de red correspondientes en el Packet Tracer. Los comandos necesarios para cumplir con configuración se encuentran disponibles en el Anexo 2.

4.5. Cableado.

Todo edificio ya sea comercial o institucional que cuente con una infraestructura de red, debe presentar un diseño óptimo del cableado construido de acuerdo a los estándares TIA/EIA 568 y 569, con la finalidad de soportar los requerimientos actuales y futuros, por tal razón se propone utilizar el cableado horizontal en el edificio principal del CUP utilizando cable UTP (Unshielded Twisted Pair/ Par Trenzado no blindado) cat. 6 tanto en la planta baja como en el primer piso, que interconecte las diferentes áreas funcionales.

Cuando se requiere instalar el cableado horizontal se lo debe realizar bajo los estándares TIA/EIA-568, que se detallan a continuación: [21]

- El cableado horizontal debe estar conectado en topología estrella.
- Cada conector en el área de trabajo, debe estar conectado a la cruzada horizontal.
- Si se necesitan equipos especiales como acopladores de impedancia, estos no deben formar parte del cableado horizontal.
- No debe existir más de un punto de transición o consolidación entre la cruzada horizontal y el cuarto de telecomunicaciones.
- No deben existir empalmes o splitters dentro de cableado horizontal.

Cables permitidos [21]

- Cable de 4 pares de 100 Ohm, UTP o ScTP (ANSI/TIA/EIA-568B.2)-(STP-A 150 Ω).
- Dos o más pares de fibra óptica multimodo de 62.5/125μm o 50/125μm (ANSI/TIA/EIA-568B.3).
- Fibra óptica MM de 62.5/125μm y dos fibras.

Salidas multiusuario y puntos de consolidación. [21]

- El conector para el servicio de voz debe ser RJ-45 hembra y debe ser compatible con el cable de cobre de 4 pares trenzados de 100 Ohm.
- El conector para el servicio de datos puede ser RJ-45 hembra y debe ser compatible con el cable de cobre de 4 pares trenzados de 100 Ohm o también un conector óptico 568 SC o ST .

El cableado horizontal se extiende por todo el edificio principal conectando la sala de comunicaciones con las diferentes áreas funcionales de trabajo. Este debe pasar por canalizaciones, en este caso se recomienda la utilización de ductos aparentes de acuerdo con el estándar TIA-569 tal como los que se posee en la actualidad, cuando se pasa los cables a través de la canalización se debe prever el crecimiento futuro por lo que no se debe llenar completamente el espacio disponible. "Se recomienda que no existan tramos mayores de 30 metros sin puntos de registro o inspección, y que no existan más de 2 quiebres de 90 grados en cada tramo" [22].

Es importante mencionar que los cables de energía no deben pasar por los ductos donde pasan los cables de red, deben estar adecuadamente distanciadas con la finalidad de evitar ruido e interferencia. Las distancias mínimas entre los cables de red o telecomunicaciones se muestran en la tabla 4.10.

Una vez realizado el cableado horizontal, se elabora el cableado vertical con la finalidad de interconectar la planta baja con el primer piso. De acuerdo con la norma TIA/EIA-568 [21], que establece que se puede utilizar cable UTP o fibra óptica, en nuestro caso recomendamos utilizar fibra óptica de 50/125µm o de 62.5/125µm ya que es resistente a las condiciones climáticas, garantizando su funcionalidad debido a que estará ubicado en la parte posterior externa del edificio interconectando las salas de comunicación (IDF y MDF cuyo tema lo abordaremos más adelante), la fibra óptica deberá ir a través de un ducto con la finalidad de protegerlo de la abrasión.

Tabla 4. 10. Distancias entre el cableado de red y de energía.

	Potencia		
	Distancia Mínima		
	2 kVA	**2 - 5 kVA**	**> 5 kVA**
Líneas de potencia no blindadas, o equipos eléctricos próximos a canalizaciones no metálicas	127 mm	305 mm	610 mm
Líneas de potencia no blindadas, o equipos eléctricos próximos a canalizaciones metálicas aterradas	64 mm	152 mm	305 mm
Líneas de potencia en canalizaciones metálicas aterradas próximos a canalizaciones metálicas aterradas	-	76 mm	152 mm

La fibra óptica nos ofrece las siguientes ventajas:

- Permite transmitir grandes volúmenes de información, permitiendo aprovechar todo el ancho de banda disponible.
- La fibra óptica no es afectada por la interferencia eléctrica o por la interferencia de radiofrecuencia y ruidos que son los más comunes.
- Permite el servicio de datos, video y voz.

Los principales elementos de un enlace de fibra óptica son el emisor, el receptor y guía de fibra.

En cuanto a la conexión desde el edificio principal hasta el salón de aulas virtuales que se encuentra ubicado a aproximadamente 60 metros, se recomienda usar fibra óptica por los

beneficios y la distancia antes mencionada, esta conexión debe ir desde el SW1 hasta el SW6, al cual se conecta el salón de aulas virtuales.

Una vez establecidos los parámetros necesarios para el cableado estructurado de la red del CUP, también es necesario establecer el lugar adecuado para la instalación del MDF (servicio de distribución principal) e IDF (Servicios de distribución intermedia), áreas necesarias para el correcto funcionamiento de la red.

Para una mayor comprensión se recomienda visualizar la infraestructura física del edifico principal, que es lugar en donde se debe realizar el cableado, las figuras 4-5 y 4-6 nos muestran dicha infraestructura.

4.6. Ubicación del MDF e IDF.

MDF.

El denominado MDF no es más que el cuarto principal de telecomunicaciones, en donde se encuentran los paneles de conexión, los equipos de red, servidores, el punto de demarcación que es el punto en donde se conectan los cables del proveedor. Para ubicar el MDF en un sitio estratégico se debe tomar en cuenta dos criterios:[2]

- "Se debe colocar lo más centrado posible en la instalación de red. Recordando que es el punto central de una topología física en estrella extendida
- Se debe colocar lo más cerca posible al punto de demarcación. "

El CUP ya posee un cuarto de comunicaciones que se encuentra situado en la parte posterior del primer piso del edifico principal, está estratégicamente ubicado cerca del punto de demarcación del proveedor, tal y como lo podemos observar en la figura 4-5, razón por la cual se sugiere que el MDF siga estando situado en este lugar.

[2] Información disponible en la web: https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCgQFjAA&url=http%3A%2F%2Fgustanet.files.wordpress.com%2F2010%2F05%2Fcomo-se-hace-un-cableado-estructurado.doc&ei=jLfwUMfWBOO10QH1k4GACA&usg=AFQjCNG_ddc3bw9ILShA84SZ1bYLICH1Sw&bvm=bv.1357700187,d.dmQ

El MDF debe estar creado bajo las normas TIA/EIA-568 y TIA/EIA-569. A continuación se hacen conocer dichas normas:

- "La altura máxima recomendada es de 2.6 metros.
- Se recomienda usar por lo menos 3 ductos de 3" cada uno para la distribución del cableado Backbone.
- Debe haber una sala o armario por cada 1000m^2 de área utilizable.
- Si no se dispone de datos exactos, estimar el área utilizable como el 75% del área total.
- La distancia horizontal de cableado desde el armario de telecomunicaciones al área de trabajo no puede exceder en ningún caso los 90m.
- Los ductos de entrada deben contar con elementos de retardo de propagación de incendio "firestops".
- Las puertas deben ser de apertura completa, con llave y con al menos 91cm. de ancho y 2 m de largo, debe ser removible y abrir hacia afuera al ras del piso.
- Se debe evitar polvo y la electricidad estática usando piso de concreto, terrazo loza, no usar alfombra. De ser posible aplicar tratamiento especial a las paredes, piso y cielo para minimizar polvo y la electricidad estática.
- Los racks deben contar con al menos 82cm de espacio de trabajo libre alrededor (al frente y detrás) de los equipos y paneles de comunicaciones.
- La temperatura en el interior del cuarto de comunicaciones debe ser controlada para proporcionar rangos de operación continua de 18°C a 24°C con 30% a 55% de humedad relativa.
- De haber un mínimo de un metro de espacio libre para trabajar de equipo con partes expuestas sin aislamiento.
- Se recomienda dejar un espacio libre de 30 cm en las esquinas" [21].

Al aplicar los estándares mencionados, se garantiza la adecuación óptima del espacio físico destinado para la instalación del MDF. Adicionalmente a las normas indicadas se recomienda tener una iluminación adecuada y para mejorarla se recomienda que el piso, las paredes y el techo sean de color blanco, alimentación eléctrica de emergencia con activación automática de UPS (fuente de alimentación interrumpible) para proteger los equipos contra las fallas eléctricas, y sistemas de prevención de incendios, todo esto con la finalidad de proteger y evitar daños en los equipos.

La figura 4.5 muestra la ubicación del MDF en el edificio principal.

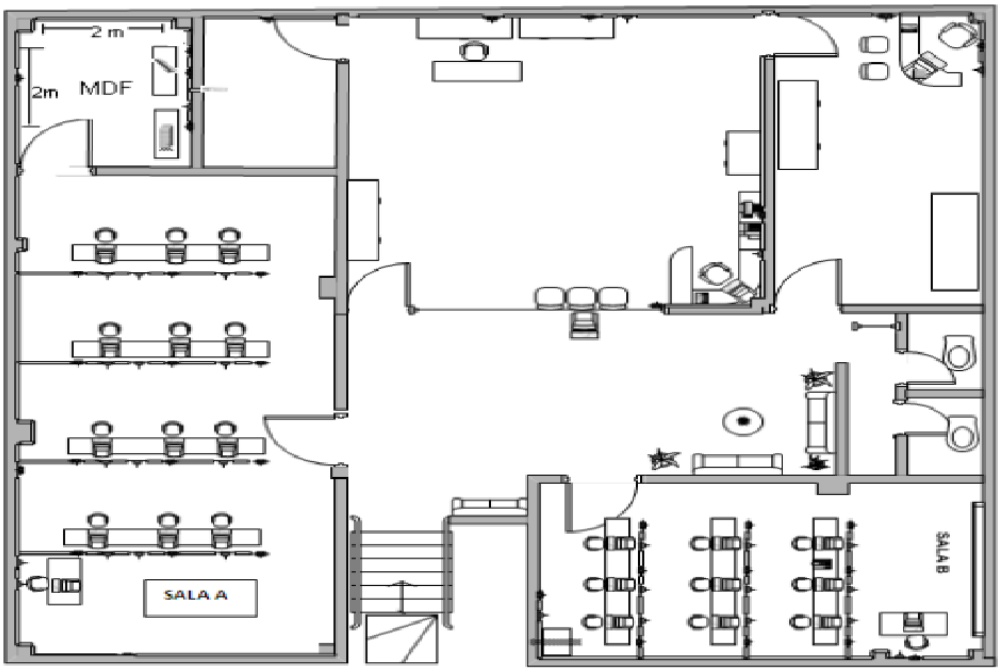


Figura 4. 5. Ubicación del MDF en el primer piso del edificio principal.

IDF.

Un IDF en cambio es un cuarto o recinto de comunicación secundario, que depende del MDF, estos recintos se conectan a través del cableado vertical, normalmente se recomienda tener un MDF por piso de un edificio, en el caso del CUP no es necesario ya que en la planta baja solamente funcionan 2 áreas con 2 PCs, es decir un PC por cada área y la infraestructura del edificio solamente tiene 2 pisos. El IDF permitirá sin ningún inconveniente el crecimiento de la red, en cualquier momento.

Como podemos observar en la figura 4.6 se ha asignado el espacio para la ubicación del IDF, tomando en cuenta que debe conectarse al MDF, razón por la cual deberá estar ubicado en la misma dirección evitando de esta manera la el incremento de cableado para poder conectar las áreas mencionadas. Por lo tanto el IDF deberá estar ubicado en la parte posterior de la planta baja.

Para la implementación del IDF resulta factible utilizar un rack de pared cerrado, con lo que se proporciona seguridad física y una mejor estética en este lugar. En el rack solamente irá un switch y un organizador de cables.

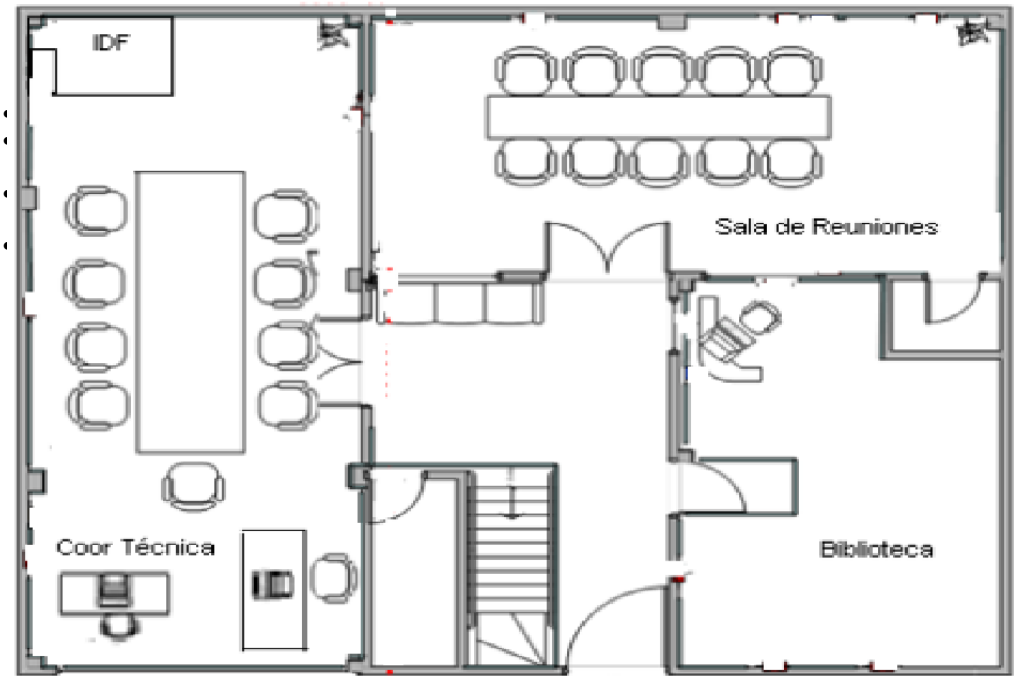


Figura 4. 6. Ubicación del IDF en la planta baja del edificio principal del CUP.

4.7. Implantación del NOC.

El NOC (Centro de Control de Operaciones) se encarga de monitorear el estado de la toda Red LAN las 24 horas del día y los 7 días a la semana, permitiendo una adecuada administración y mantener un control centralizado. Se podrán identificar los problemas de manera casi inmediata, brindando de esta manera la posibilidad de solucionarlo en el menor tiempo posible, esto nos da la posibilidad de tener una visión global de la red de datos, reduciendo los costos operacionales.

La detección oportuna de los problemas identificados en la red, nos permite ahorrar recursos importantes que son estrictamente necesarios para una institución.

Es muy importante aclarar que el NOC fue implantado solamente en la red de Centros de cómputo, que fue la red a la que los directivos del CUP nos permitieron el acceso. Para una mayor comprensión dirigirse a la figura 2.2.

Los sistemas de monitoreo elegidos para esta función son los siguientes: WhatsUp Gold y Cacti (más información del NOC y de los sistemas de monitoreo a mayor detalle en el Anexo 3).

4.7.1. Dispositivos a monitorear.

EL monitoreo, se lo debe realizar a todos los equipos activos de la red de datos, para objeto de nuestro estudio se monitorearan los dispositivos más relevantes, que soporten el servicio SNMP.

Los dispositivos que requieren ser monitoreados en el CUP se muestran en la tabla 4.11

Tabla 4. 11. Dispositivos a ser monitoreados.

Router	Interfaces	El estado de todas las interfaces (up or down)
	Utilización	Qué porcentaje del canal de transmisión está siendo utilizado
	Memoria	Memoria y disco duro
	Procesador	Uso de la CPU
Switch	Interfaces	El estado de todas las interfaces (up or down), así como los protocolos que se están utilizando.
	Procesamiento	Uso de la CPU
Servidor	Estado	Si este tiene conectividad o no
	Memoria	Memoria que tiene el servidor.
	Procesamiento	Uso de la CPU
Enlace	Estado	Si la interfaz está arriba o abajo (up or down)
	Tráfico	Cantidad de tráfico que pasa a través del enlace.

En cada uno de estos dispositivos se deben monitorear: la disponibilidad, carga y status ,La información completa y detallada de la implementación llevada a cabo en el CUP la podemos ver en el Anexo 3.

4.8. Hardware necesario para la implementación del Modelo Jerárquico de tres capas en el CUP.

4.8.1. Capa de acceso.

Tomando en cuenta que la red necesita crecer a medida que la población estudiantil, el personal y las necesidades de la institución se incrementan, es necesario utilizar dispositivos de red que lo permitan, tal como, switches modulares para la capa de acceso, ya que ofrecen mayor flexibilidad en su configuración y permiten la instalación de tarjetas de línea, facilitando incrementar el número de puertos para conectar PCs o dispositivos de red; mientras que los switches fijos no permiten agregar características u opciones más allá de los predeterminados.

A su vez también se debe considerar que los switches modulares son mucho más costosos y el CUP no es tan grande como la matriz, razón por la cual es mejor adquirir switches apilables, que tienen un costo menor, y que se pueden interconectar con el uso de un cable especial denominado blackplane. Los switches apilables presentan los mismos servicios que los switches modulares, además permite hasta 10000 Mb/s de tráfico por puerto.

Tomando en consideración lo antes mencionado la mejor opción para implementar la red jerárquica de tres capas, es utilizar los switches de la serie Catalyst 2960 en la capa de acceso, considerando que tienen las siguientes características [11]:

- Tasas de reenvío de 16 Gb/s.
- Switching de capas múltiples.
- QoS para admitir comunicaciones.
- Listas de control de acceso.
- Conectividad Fast Ethernet y Gigabit Ethernet.
- Enlaces gigabit adicionales de doble propósito.

- Admite Cisco IOS (Internetwork Operating System) CLI(La interfaz de línea de comandos de IOS).
- Interfaz de administración de Web integrada y Cisco Network Assistant.
- Admite acceso de consola y puerto auxiliar al switch.

A continuación se expone la tabla 4.12, en donde podemos observar los switches propuestos a implementar en la capa de acceso.

Tabla 4. 12. Características del Switch de Acceso.

Área	Características	Modelo	Total Puertos	Enlaces ascendentes	Enlaces ascendentes de suministro de alimentación
Servidores	**LAN Base Layer 2**	WS-C2960-8TC-L	8	1 Dual Purpose	20W
Dirección y Secretaría	**LAN Base Layer 2**	WS-C2960-8TC-L	8	1 Dual Purpose	20W
Cord. Téc. Y Biblioteca	**LAN Base Layer 2**	WS-C2960-8TC-L	8	1 Dual Purpose	20W
Sala A.	**LAN Lite Entry Layer 2**	WS-C2960-24TC-L	24	2 Dual Purpose	30W
Sala B.	**LAN Lite Entry Layer 2**	WS-C2960-24TC-L	24	2 Dual Purpose	30W

4.8.2. Capa de distribución.

El switch de distribución o de capa 3 es el encargado de recopilar toda la información de los switches de la capa de acceso y a su vez enviarla a los equipos de red que forman la capa núcleo. Además deben proporcionar funciones de enrutamiento entre las diferentes VLANs.

Una vez analizadas las funcionalidades que nos ofrecen los switches: Catalyst Express 500, Catalyst 2960, Catalyst 3560, Catalyst 3750, Catalyst 4500, Catalyst 4900 y Catalyst 650º , se ha establecido el uso del switch Catalyst 3750, ya que presenta las características que se adaptan a las necesidades del CUP, a continuación hacemos conocer las principales características del switch 3750 [11]:

Switch de distribución modelo WS-C3750G-12S-S

Cuyas características más relevantes son las siguientes:

- Conectividad Fast Ethernet y Gigabit Ethernet.
- 12 puertos basados en STP Gigabit Ethernet.
- 32 Gbps y de alta velocidad del bus de apilamiento.
- 1 unidad de rack switch apilable multicapa.
- El software IP Base conjunto de características (IPB).

4.8.3. Capa núcleo.

Para la capa núcleo se recomienda utilizar routers, o si fuera el caso se puede utilizar switches de capa 3 siempre y cuando se adapte a las necesidades de la red; estos dispositivos deben ser de alta velocidad y manejar altas tasas de reenvío.

Habiendo analizado los diferentes routers, se estableció que el router tipo Cisco de la serie 1841 es una buena alternativa; sin embargo tomando en cuenta que el CUP, posee ya un router cisco 2600, y que reúne las características necesarias para ser implementado en la red jerárquica, es conveniente utilizar este router. A continuación se hace conocer las características del router 2600:

La serie Cisco 2600, ofrece una solución rentable para satisfacer las necesidades actuales y futuras de instituciones medianas.

Servicios soportados:

- Integración multiservicio de voz y datos
- Acceso a redes privadas virtuales (VPN) con opciones de firewall.
- Servicios de acceso telefónico analógico y digital.
- Enrutamiento con gestión de ancho de banda.
- Enrutamiento entre VLAN.

Dispone de dos ranuras para tarjetas de interfaz WAN (WIC), una ranura para el módulo de red y una ranura para un módulo de integración avanzada (AIM). Estas ranuras comparten más de cincuenta módulos distintos entre cuatro líneas de productos de Cisco.

De acuerdo con el diseño de la red Jerárquica de tres capas propuesto, aún nos hace falta un router por lo que se recomienda utilizar un router Cisco 1841 debido a que nos proporciona gran velocidad y las siguientes herramientas [12]:

- Velocidad de cable de rendimiento para servicios simultáneos en las tasas de WAN T1/E1.
- Mayor protección de la inversión a través de un mayor rendimiento y modularidad.
- Aumento de la densidad a través de las ranuras de alta velocidad.
- Tarjeta de interfaz WAN.
- Soporte para más de 90 módulos existente.
- Soporte para la mayoría de WIC existente, VWIC y VIC (modo solo de datos).
- La densidad a través de las ranuras de alta velocidad Tarjeta de interfaz WAN.
- Dos puertos integrados 10/100 Fast Ethernet.
- Seguridad
    - A bordo de encriptación.
    - Apoyo de hasta 800 túneles VPN con el módulo AIM.
    - Antivirus de defensa a través de NAC (Netork Admission Control) o prevención de intrusiones, así como de estado Cisco IOS.
    - Firewall de apoyo.

4.9. Presupuesto estimado para la Implementación del Modelo Jerárquico de tres capas en el CUP.

Son los recursos en los que se requiere invertir para poner en marcha la propuesta del modelo Jerárquico de tres capas en el CUP. El costo total aproximado se presenta en la tabla 4.13, en donde constan los activos fijos que han sido identificados como hardware necesario por sus características descritas en la sección anterior y cotización de la inversión.

Los precios de referencia han sido tomados de la cotización realizada por algunas empresas a través de la web.[3] Es importante recalcar que este presupuesto puede cambiar debido a algunas variaciones de los precios establecidos a la fecha.

Tabla 4. 13. Presupuesto para la implementación de la red Jerárquica de tres capas.

Ítem	Descripción	Cantidad	Precio Unitario USD$	Precio Total USD $
1	Router 2600	1	758,00	758,00
2	Switch de capa 3 (WS-C2960-24TC-L)	1	3598,00	3598,00
3	Switch para la capa de acceso(WS-C2960-24TC-L)	5	583,00	2915,00
4	Cable UTP Cat 6ª	2	150,00	300,00
5	Jack Cat 6ª	34	6,62	225,08
6	Rack de pared cerrado AR 8009 9U Prof400MM	1	183,99	183,99
7	Organizador de cables horizontal AR 2U 19P cerrado	1	16,99	16,99
8	Varios			150,00
			TOTAL	8147,06

[3] http://www.router-switch.com/Price-cisco-switches-cisco-switch-catalyst-2960_c19?gclid=COv5u9n32q0CFY1b7AodeWgDUw
http://www.router-switch.com/ws-c2960-24tc-l-p-433.html
http://www.router-switch.com/ws-c3750g-12s-s-p-510.html?gclid=ClOv28Li3K0
http://www.router-switch.com

5. PRUEBAS Y VALIDACIÓN.

Uno de los parámetros que se debe evaluar en una red de datos es su rendimiento, esto garantiza que la infraestructura y funcionamiento de la red sea óptimo. Para verificar el rendimiento de la red plana y la red basada en el modelo de tres capas se realizaron pruebas de broadcast, que se enfocan en detectar los posibles problemas en la transmisión de paquetes, con esta información recolectada podremos establecer una comparativa real acerca del rendimiento de dichas redes.

Los dispositivos empleados para realizar las pruebas de broadcast son los que a continuación se hace conocer:

- 3 Switches Cisco 2600.
- 1 Router Cisco 1840
- 6 computadoras: 4 PCs y 2 portátiles.

En cuanto a software implementado se utilizó las siguientes herramientas:

- **NTGM.** Que es un monitor y emulador de tráfico de red, que permite predecir el rendimiento de la red bajo condiciones de carga realistas.
- **Cacti**. Sistema de monitoreo de la red empleado también en la implementación del NOC CUP. Más información acerca de esta herramienta se encuentra disponible en el anexo 4 y 6.

La figura 5.1 muestra la topología empleada para la realización de las pruebas de broadcast.

Figura 5. 1. Topología empleada para pruebas de broadcast.

5.1. Monitoreo con NTGMs.

5.1.1. Red Plana.

La figura 5.2 muestra el direccionamiento IP de la red, así como también el número de paquetes que se requieren enviar, utilizando la herramienta NTGMs para generar tráfico, en este caso se puede observar que se envió 10000 paquetes a la red de datos a través del router cuya dirección IP es 192.168.1.254, al hacer clic en botón ping se inicia la generación de tráfico. En este tipo de red todos los paquetes enviados, circulan a través de toda la red antes de llegar destino, la información recolectada y mostrada por NTGMs permitirá conocer el desempeño de la red de datos.

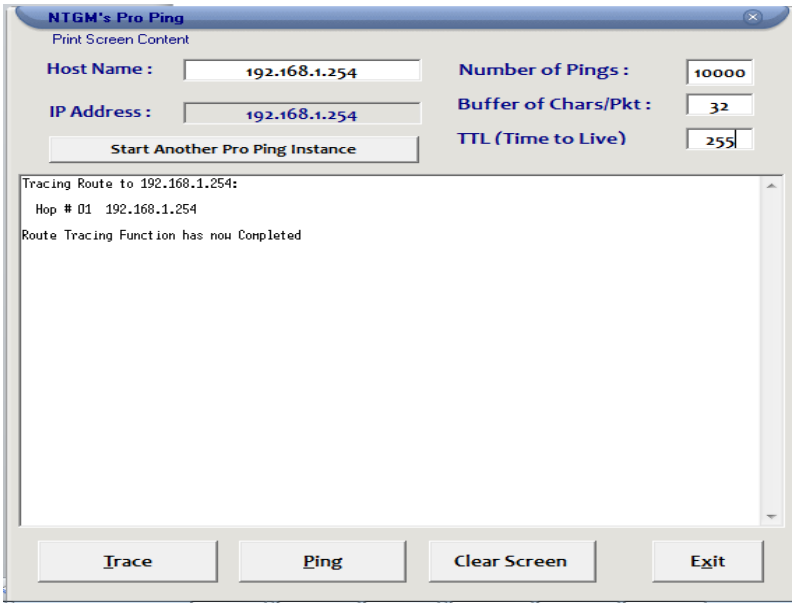


Figura 5. 2. Generación de tráfico con NTGM.

Cuando se inicia la generación de tráfico con NTGMs, también muestra el avance o monitoreo de los paquetes enviados, tal y como se muestra en la figura 5.3.

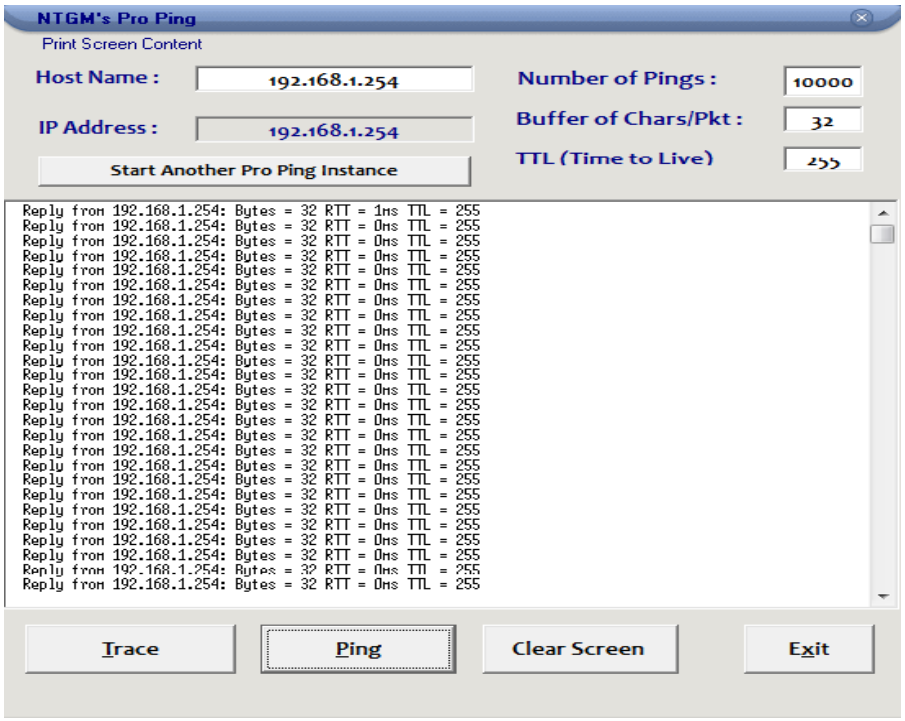


Figura 5. 3 .Informe del estado del envío de paquetes.

Conjuntamente con la ventana de la figura 5.3, se muestra el estado del monitoreo realizado a la red mediante datos estadísticos, lo cual ayuda a determinar con mayor precisión cuál el rendimiento de la red. La figura 5.4 muestra el resultado de la generación de tráfico luego de haber iniciado la acción.

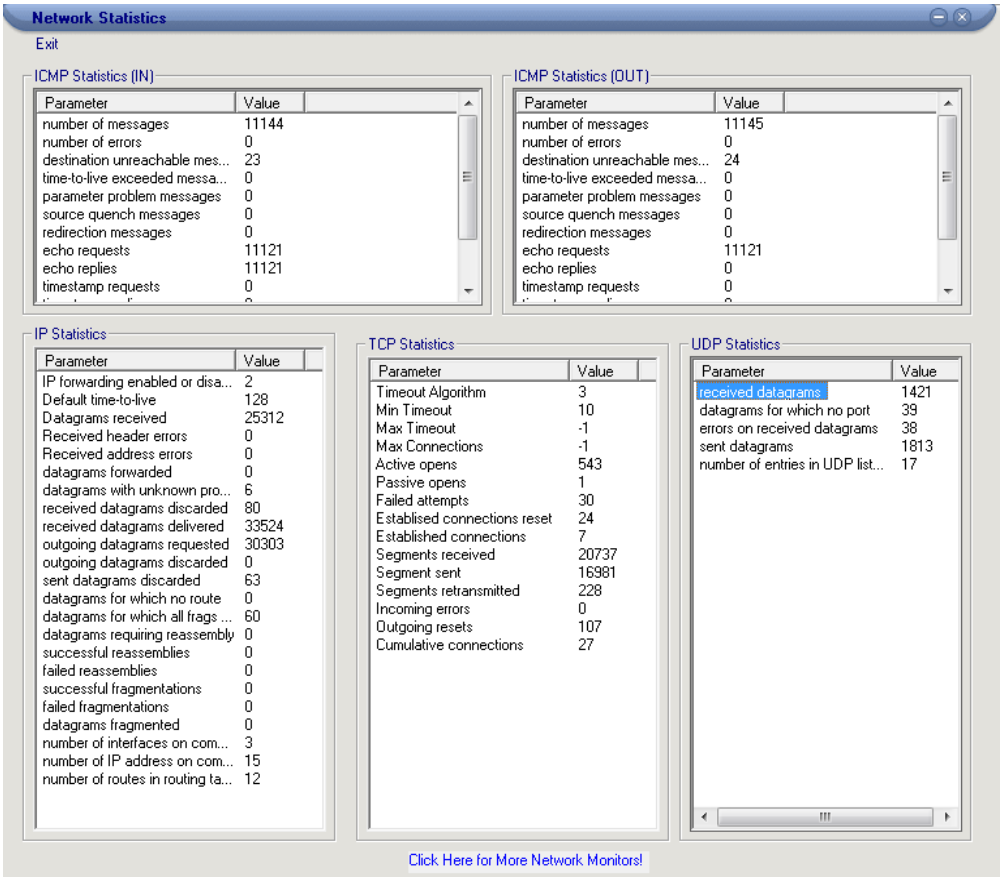


Figura 5. 4. Resultado del monitoreo de la red.

Estadísticas ICMP[4], como se observa en la figura 5.4 el número de mensajes enviados corresponden a un total de 11144. La pérdida de mensajes cuyo destino fue inalcanzable fueron en total de 23, finalmente también nos muestra la solicitud de eco con 11121 mensajes y las respuestas de eco con un total de 11121, lo que demuestra que de 11144 mensajes enviados solamente 11121 llegaron.

[4] Protocolo de Mensajes de Control de internet.

Estadísticas IP[5], muestra que el tiempo predeterminado de vida de los mensajes enviadas es de 128, los datagramas recibidos con un total de 25312, datagramas descartados 80, datagramas entregados 33524 y de más datos que nos permiten analizar el rendimiento de la red.

Estadísticas de TCP[6], Estas estadísticas muestran datos adicionales acerca de la transmisión de segmentos. En la figura 5.4 tenemos los intentos fallidos con un total de 30, segmentos recibidos 20737, los segmentos enviados, segmentos retransmitidos y conexiones acumuladas.

Estadísticas UDP[7], las estadísticas mostradas nos indican que han sido recibidos 1421 datagramas, puertos no disponibles para los datagramas 39, además los errores en los datagramas recibidos con un total de 38.

Al finalizar la generación de tráfico en la red los datos estadísticos arrojados por esta herramienta se muestran en la figura 5.5

Considerando los resultados ICMP el número de mensajes enviados son 586227, de los cuales 49 de los mensajes tuvieron un destino inalcanzable, y los mensajes entregados con un total de 371908 y reenviados 211270.

De acuerdo con las estadísticas TCP los segmentos recibidos fueron un total de 57857, 49080 segmentos enviados y total de segmentos retransmitidos de 576.

[5] Protocolo de Internet
[6] Protocolo de Control de Transmisión
[7] Protocolo del nivel de transporte basado en el intercambio de datagramas.

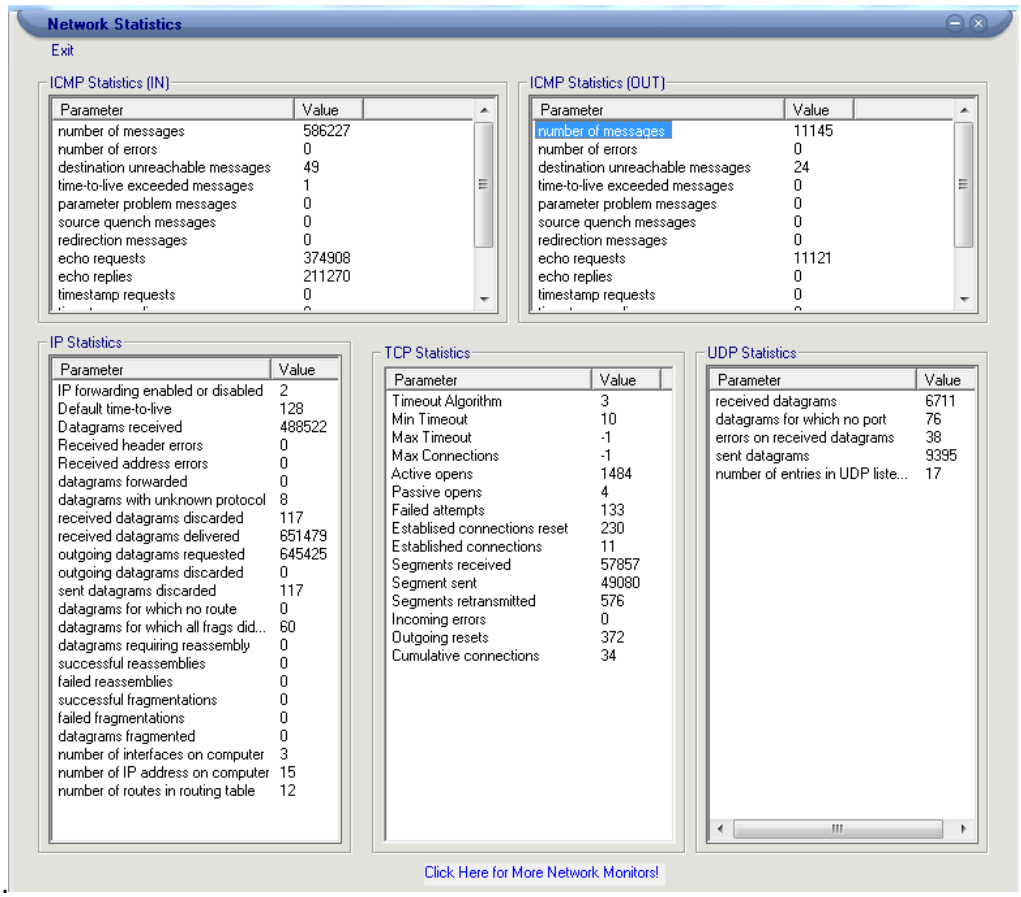


Figura 5. 5. Estadísticas del monitoreo al finalizar la generación de tráfico.

5.1.2. Red Jerárquica.

La red Jerárquica implementada, tiene el mismo direccionamiento IP, pero ahora la red está segmentada en 3 VLANs: VLAN 2, 3 y la 99 que corresponde a la VLAN de administración.

Es importante mencionar que al iniciar la generación de tráfico se inició enviando mensajes a cada una de las VLANs, a través de los enlaces troncales tal y como se muestra en la figura 5.6.

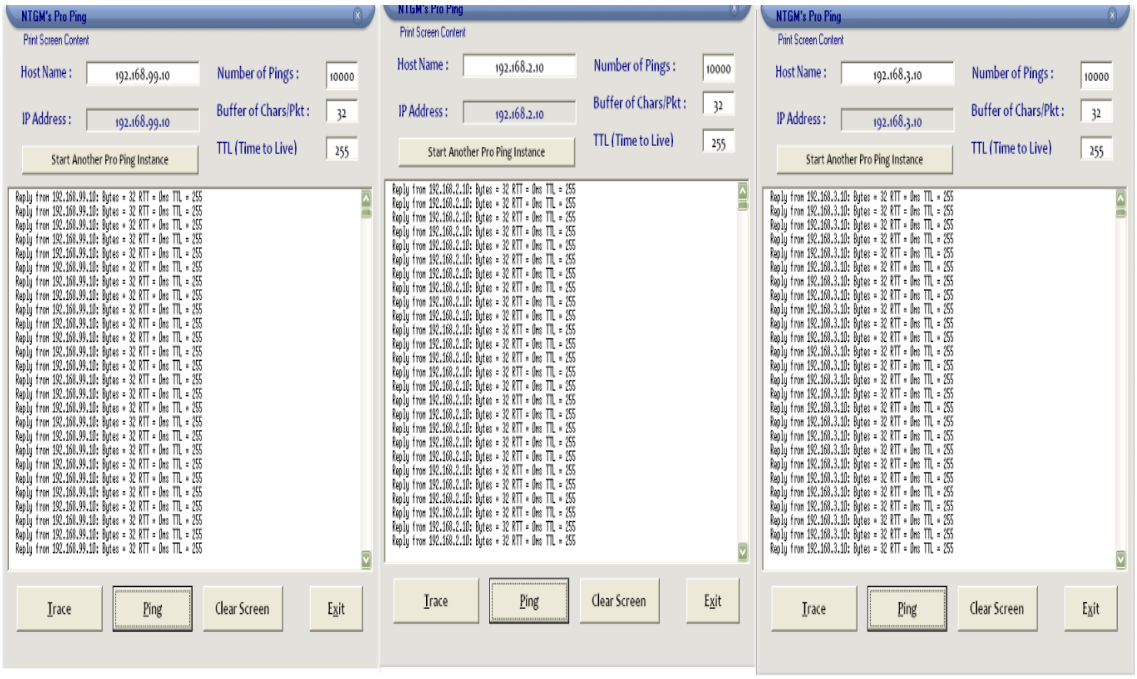


Figura 5. 6. Generación de tráfico con NGTM en la red Jerárquica.

La figura 5.7 muestra ya un resultado de la generación de tráfico en donde ya podemos establecer una opinión con datos reales acerca del rendimiento de las redes.

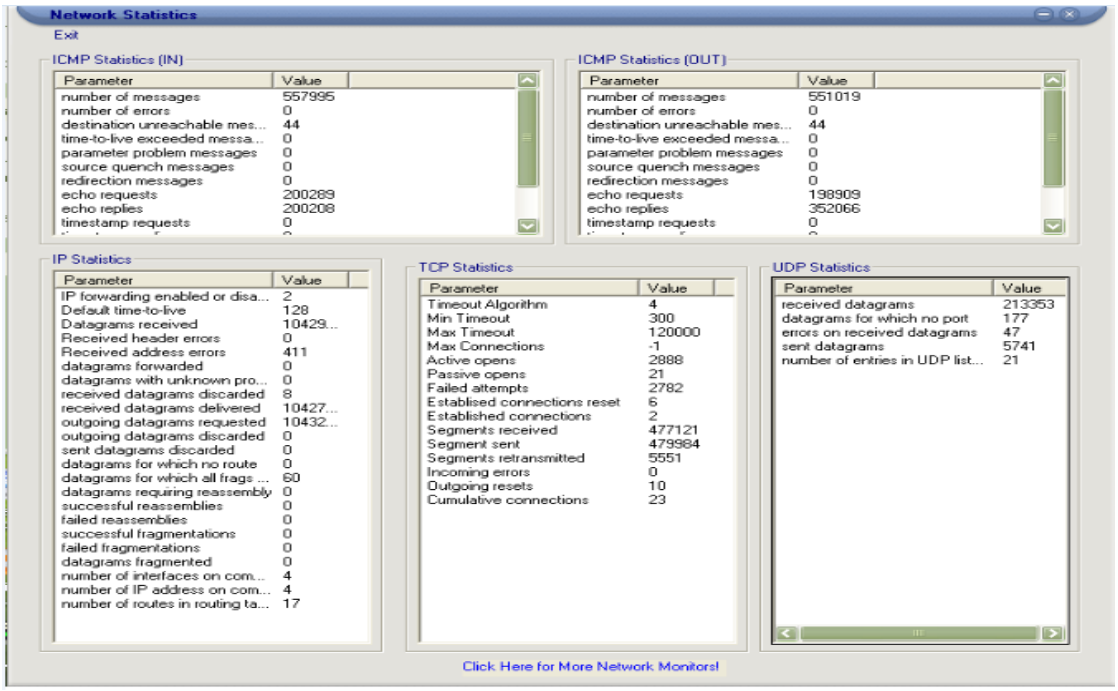


Figura 5. 7. Monitoreo de la Generación de tráfico con NTGM en la Red Jerárquica.

El monitoreo de la generación de tráfico en la red Jerárquica, nos muestra la estadística ICMP con un total de 557995 mensajes enviados, 44 destinos inalcanzables número menor que el generado en la red plana, un total de respuestas de 200289 y 200208 respuestas de eco.

En cuanto a las estadísticas TCP, el número de segmentos recibidos con un total de 477121.

5.2. Monitoreo con Cacti.

Durante la generación de tráfico con NTGM las redes de datos fueron monitoreadas con Cacti, cuya finalidad es establecer cuál de las redes nos ofrece un mayor rendimiento en base a las pruebas realizadas. A continuación se hace conocer los resultados arrojados por Cacti.

5.2.1. Red Plana.

Antes de iniciar el monitoreo es necesario agregar el router a monitorear, la figura 5.8 nos muestra que el router ya está agregado e identificadas sus interfaces.

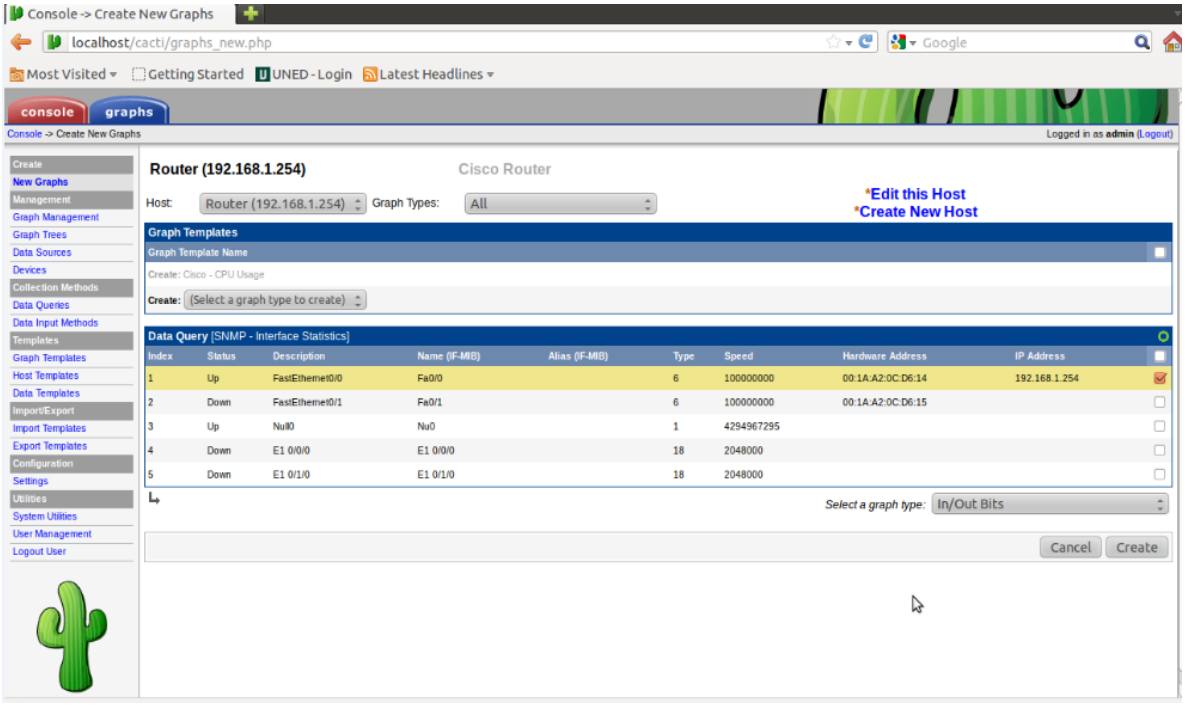


Figura 5. 8. Router agregado e identificadas sus interfaces.

Una vez agregado el router automáticamente identifica sus interfaces, luego de esto se puede añadir las gráficas necesarias de acuerdo a nuestros requerimientos. Para que el sistema de

monitoreo nos muestre los resultados, solamente basta esperar 5 minutos para ver los resultados generados.

Para objeto de nuestro estudio las gráficas que se desean observar son las siguientes:

- Tráfico de la interfaz fa0/0.
- Ancho de banda utilizado.

Los resultados del monitoreo los podemos observar en la figura 5.9.

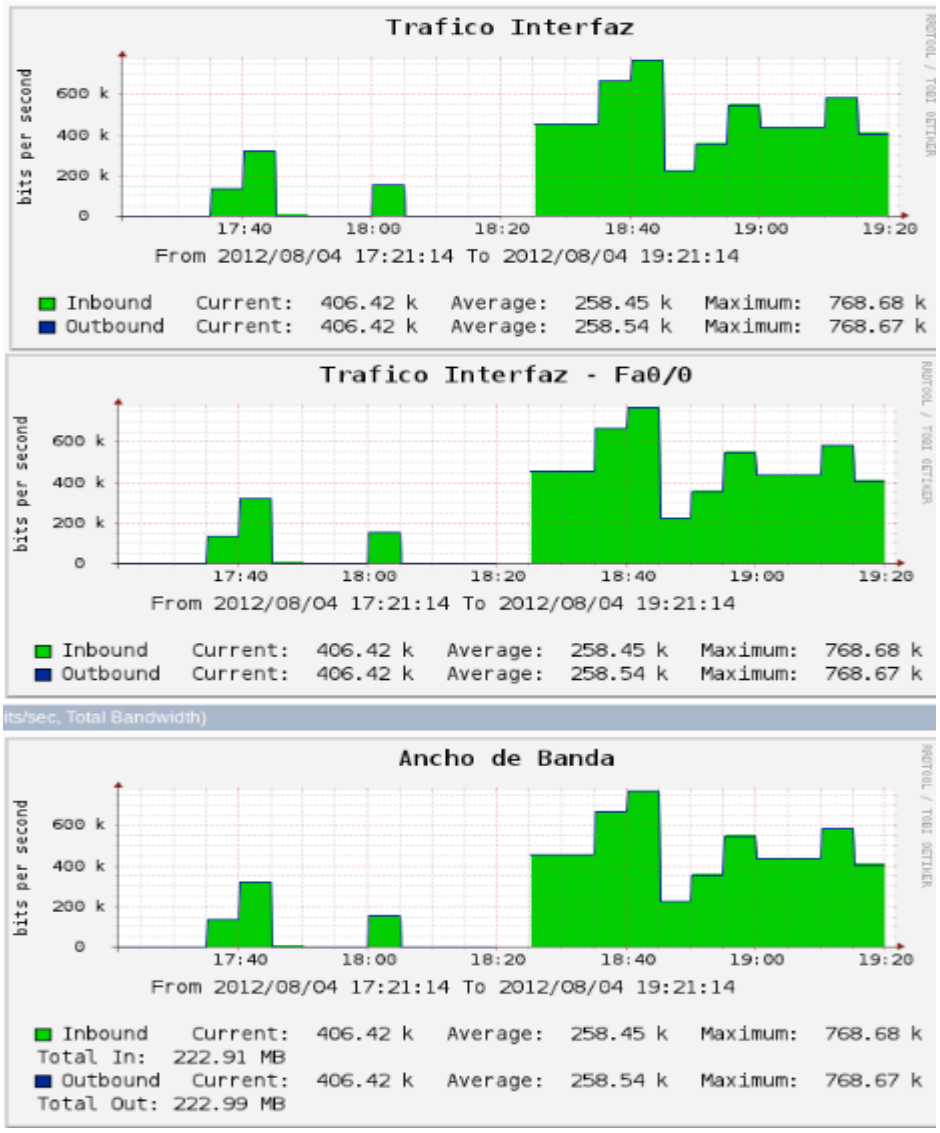


Figura 5. 9. Monitoreo de la Red Plana con Cacti.

En esta gráfica podemos darnos cuenta que el flujo de tráfico es constante, en donde la mayor cantidad de tráfico generado es de aproximadamente 768.68 Kilobits por segundo, y que el ancho de banda utilizado entre las 18:30 y 18:40 es aproximadamente de 768.68k por segundo.

5.2.2. Red Jerárquica.

El tráfico generado en la red Jerárquica, viaja hacia la VLAN correspondiente a la que se le envían los paquetes de datos.

La figura 5.10 nos muestra el router agregado. Cuando un router o dispositivo ha sido agregado satisfactoriamente, los datos correspondientes aparecen automáticamente, tal y como se muestra en la figura mencionada.

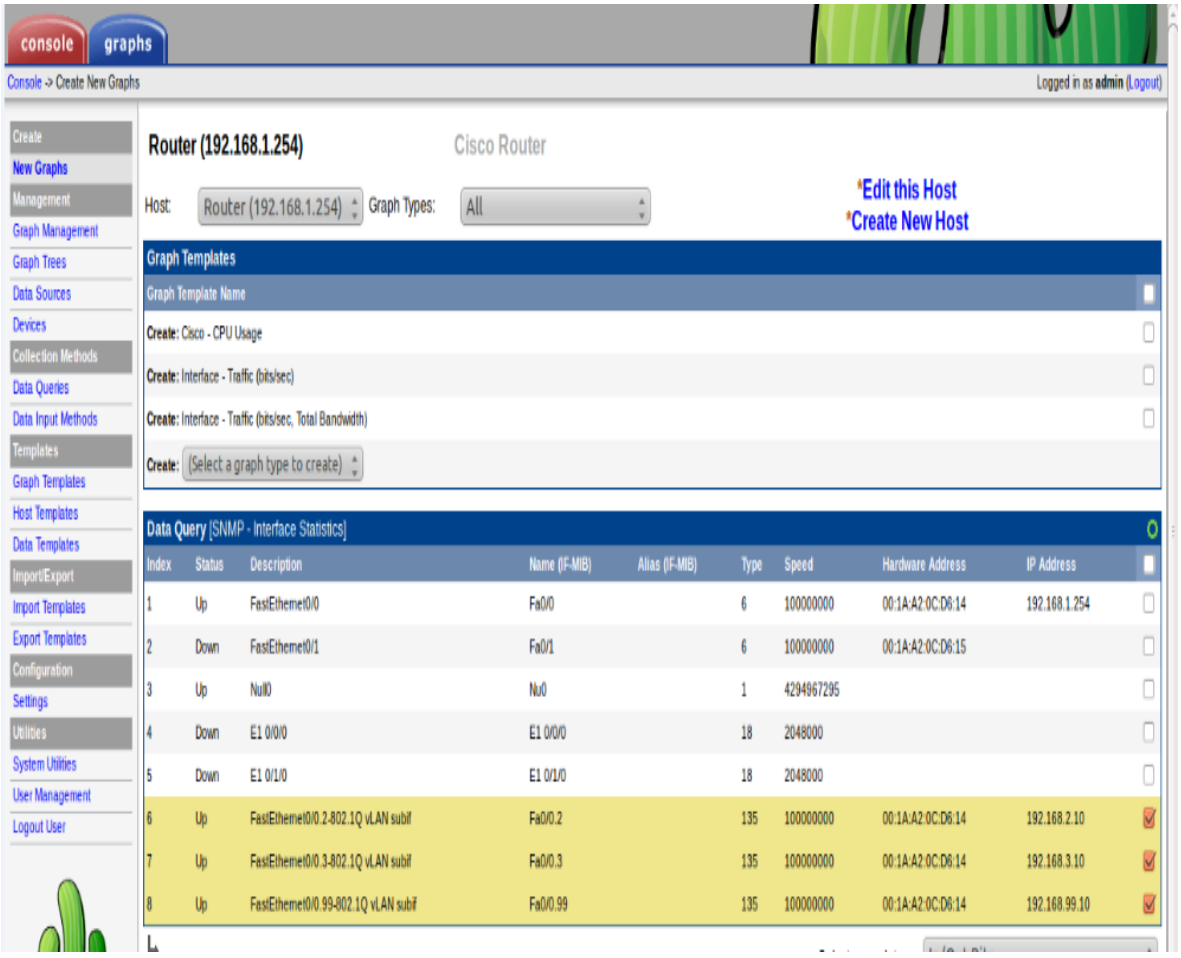


Figura 5. 10. Routers con las VLANs identificadas.

Una vez agregados los dispositivos, debemos seleccionar el tipo de monitoreo que queremos realizar, para que el Cacti nos genere las gráficas correspondientes. Luego de esto ya se puede iniciar la generación del tráfico, las gráficas se actualizan cada 5 minutos.

La figura 5.11 muestra que existe una mayor cantidad de tráfico generado en la VLAN 2, y que durante un mismo periodo de tiempo existe tráfico en las diferentes VLANs, esto nos demuestra que puede existir mucho tráfico de forma simultánea y que esto no provoca una colisión, ya que cada VLAN es independiente, mejorando significativamente el rendimiento de la red.

La generación de tráfico en la Red Jerárquica se inició enviando mensajes a todas las VLAN, para luego solamente generar tráfico en la VLAN 2, es por ello que la interfaz Fa/0.02 presenta más tráfico que el resto de las VLANs, tal y como se muestra en la figura 5.11, con lo cual se demuestra que el tráfico generado dentro de una VLAN no interfiere en el resto de la red, lo que hace que mejore significativamente su rendimiento.

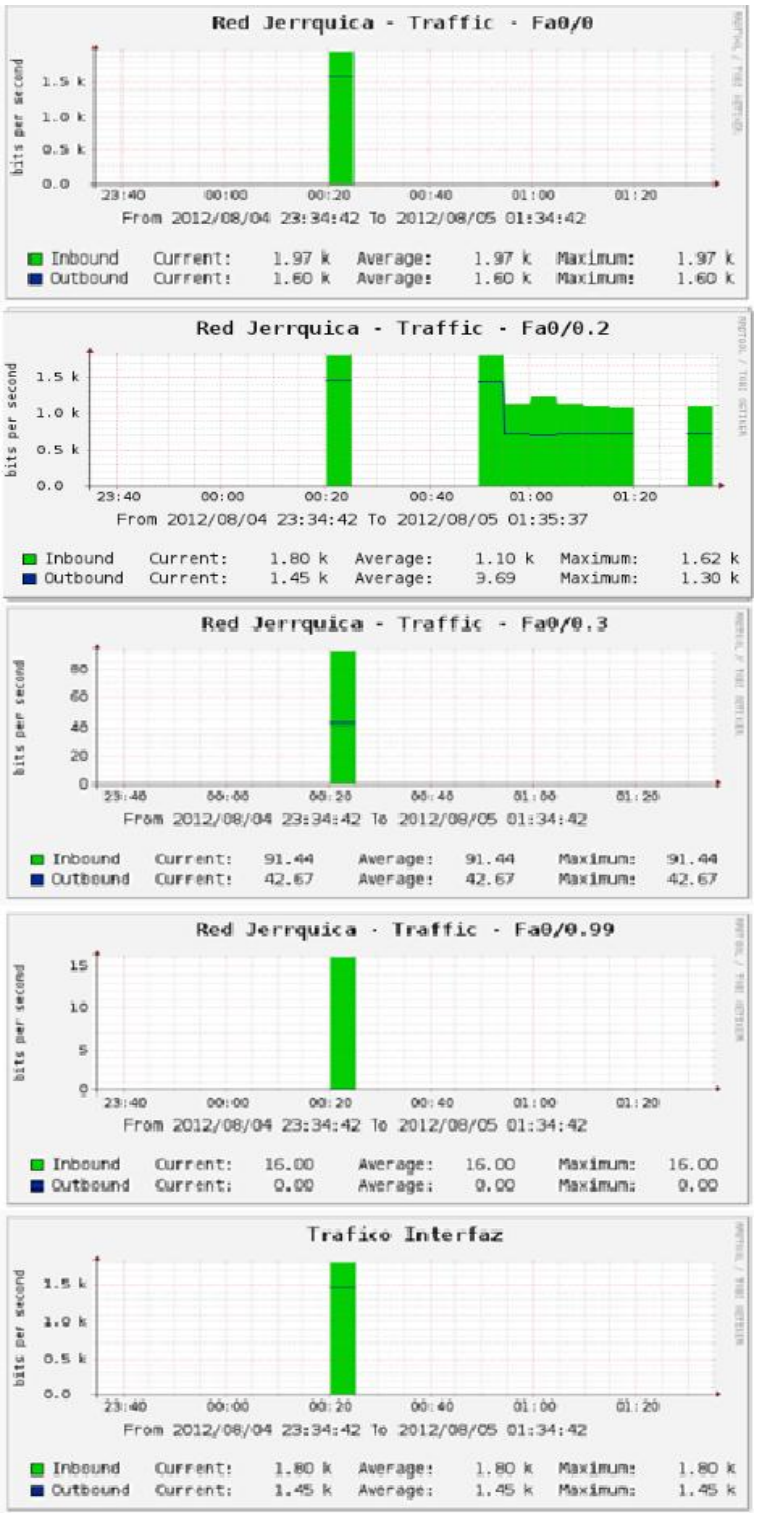


Figura 5. 11. Monitoreo de la Red Jerárquica con Cacti.

5.3. Análisis de Resultados.

A más de los beneficios que una red jerárquica de tres capas nos brinda, tal como: la escalabilidad, redundancia, seguridad, facilidad de administración y mantenimiento, se realizó pruebas de broadcast con equipos reales en donde se verificó el rendimiento de cada una de las redes.

A mayor detalle podemos decir que con las herramientas utilizadas para monitorear la red, pudimos observar y concluir que en la red Plana se genera mayor tráfico o carga debido a que tiene un solo dominio de broadcast, ya que no cuenta con ninguna configuración para dividir lógicamente la red. Los paquetes que se envían en una red plana viajan a través de toda red hasta llegar a su destino, lo que provoca que el rendimiento de la red sea bajo, debido a que tiene que inundar toda la red para llegar a su destino, dando lugar a la pérdida de paquetes por las colisiones.

Mientras que en la red Jerárquica de tres capas los paquetes enviados no viajan a través de la toda red de datos, sino que viajan solamente a la VLAN específica, la segmentación de la red en varias VLAN hace que por cada una haya un dominio de broadcast, ya que el tráfico es direccionado a la VLAN específica.

De acuerdo a los datos obtenidos a través de las herramientas de monitoreo, en la red plana existe mayor cantidad de tráfico generado que es de aproximadamente 700 kilobits por segundo, mientras que en la red jerárquica se tiene un valor máximo de 1.5 kilobits por segundo.

Estadísticas ICMP. De acuerdo con las estadísticas reportadas por NTGM, en la red plana si bien es cierto tenemos una mayor carga de mensajes enviados, sin embargo tenemos un número de 374908 solicitudes de eco y 211270 respuestas de eco, con lo que podemos determinar que hubo un mayor número de paquetes perdidos en esta red, causado por la congestión dada. Mientras que en la red jerárquica las solicitudes de eco fueron un número de 200289 y las respuestas de eco en un número de 200208, con lo que queda demostrado que la red jerárquica el número de paquetes perdidos es mucho menor lo que hace que la red sea más eficiente.

Estadísticas IP, nos muestra que el tiempo predeterminado de vida de los mensajes enviadas tanto a la red plana como a la red jerárquica es de 128. Pese a que el número paquetes generados para cada red fueron en un número aproximado como podemos ver en las figuras 5.5 y 5.7. El número de paquetes descartados en la red plana es de un 94%, mientras que en la red jerárquica solamente fue el 6% por lo que nuevamente confirmamos que la red jerárquica garantiza su rendimiento.

Estadísticas de TCP, En estas estadísticas como podemos observar en las figuras 5.5 y 5.7, los segmentos retransmitidos en la red plana es del 9%, mientras que en la red jerárquica es del 91%, con lo que en la red jerárquica se asegura que los segmentos perdidos puedan llegar a su destino retransmitiéndolos un mayor número de veces o reenviando todos los segmentos que se ha identificado que aún no han llegado a su destino.

5.4. Discusión.

El CUP, ha sido una Institución pionera en educación Superior en la ciudad de Cariamanga, debido a ello también debe contar la infraestructura tecnológica de comunicaciones adecuada, que mejore la productividad de la misma. Por tal motivo necesita implementar una red basada en el modelo Jerárquico de tres capas que garantice su rendimiento.

Cabe recalcar que en un inicio la infraestructura de red era una sola (y no 2 como la que actualmente posee), lo que provocaba la falta de rendimiento en el periodo de matrículas, y como medida los estudiantes no podían acceder a Internet ya que el ancho de banda disponible debía ser dedicado sólo para el uso de secretaría por los procesos que se deben llevar a cabo para este fin. Esta es la razón para que en la actualidad existan 2 redes LAN, una para el área administrativa y otra para centros de cómputo.

En base a la propuesta diseñada y pruebas realizadas, el CUP encontró varios beneficios en la red de datos propuesta. La tabla 5.1. nos muestra las beneficios mencionados al establecer una comparativa con la red de datos actual.

Tabla 5. 1.Comparativa entre la red de datos actual y la red jerárquica de tres capas.

Red de datos actual	Red Jerárquica de tres capas.
El centro universitario cuenta con 2 LAN, lo que hace que la administración se duplique, pese a que pudieran utilizarse las mismas configuraciones.	La red jerárquica une las 2 redes lo que facilita la administración de la misma.
Se necesita contratar más ancho de banda, para satisfacer el ancho de banda necesario para cada red.	Al implementar la red jerárquica se debe contratar un solo servicio de ancho de banda y asignar mayor ancho de banda para el área que más lo requiera, distribuyendo de esta manera adecuadamente el recurso. Para distribuir el ancho es necesario adquirir un dispositivo que intervenga en la red asignando el ancho de banda necesario

	para cada segmento.
La red nos muestra que la capa de núcleo y de distribución se combinan lo que hace que la comunicación se colapse y por consecuencia más lenta.	La red jerárquica propuesta, al tener funciones específicas hace posible que la productividad y velocidad se incrementen.
Las redes actuales cuentan con cierto nivel de seguridad debido a que se encuentran en redes diferentes. Pero sin embargo puede darse el caso de que la información que fluye a través de una red pueda ser interceptada por alguien que se encuentre conectado en la misma red. Ó también puede darse el caso que se conecte una máquina con virus lo cual puede infectar a toda la red.	Al implementar el modelo jerárquico, incrementa el nivel de seguridad, ya que cada área estaría dentro de una VLAN independiente, sin necesidad de que se encuentren en redes distintas. En caso de que si una máquina infectada con virus se conecte a un segmento de red solamente afectará a ese segmento, evitando de esta manera que dicho virus se propague a través de toda red.
Solamente la red de centros de cómputo posee servidores, mientras que la red de administrativa no, siendo estos también necesarios en esta área ya que determinan la forma y productividad del trabajo de toda la institución. En la figura 2.2 podemos ver que el área administrativa no cuenta con los servidores lo que hace que este proceso se realice de forma manual. Otra manera de solventarlo sería adquiriendo otros servidores para esta red, lo que provoca un gasto económico innecesario.	Al crear un modelo jerárquico uniendo las 2 redes, toda la red contaría con el área de servidores necesarios, en donde cada segmento de la red cuenta con el servicio que nos brindado por los servidores.
Al producirse una falla en la red, se ve afectada toda la red, quedándose incomunicada. El identificar cuál es la falla	Con el modelo jerárquico propuesto, se identifican con mayor facilidad cuál es el segmento de la red afectado con la falla, por

podría tardar varios minutos u horas.	ende aislarlo y darle solución en el menor tiempo posible.
Los switches disponibles actualmente en el centro universitario no son programables.	Con el modelo jerárquico se propone utilizar switches programables para garantizar la seguridad al menos en un nivel medio, además de facilitar la administración.
El crecimiento de la red puede implicar el rediseño de toda la red, para agregar los diferentes dispositivos de red.	Permite el crecimiento de la red con mucha facilidad, generalmente este crecimiento se da en la capa de acceso ya que si se requiere interconectar más equipos simplemente se agrega uno más y la configuración del equipo se puede reproducir de los equipos ya configurados, a menos que requiera uno diferente.

CONCLUSIONES Y RECOMENDACIONES DEL PROYECTO DE TESIS.

Conclusiones.

De acuerdo con las investigaciones, procesos y pruebas realizadas para el presente proyecto de tesis, se ha podido concluir que:

- Implementar el modelo jerárquico de tres capas, permite tener una red organizada, ofreciendo la posibilidad de crecimiento en cualquier momento, agregando solamente dispositivos de red desde la capa de acceso hasta la capa de distribución; también hace posible reutilizar la misma configuración para los nuevos dispositivos. Con lo anteriormente expuesto ya no es necesario rediseñar toda la red para adaptarla a los nuevos requerimientos de la institución.
- Unir las redes aplicando el modelo Jerárquico, permite una mejora considerable en su rendimiento con un incremento del 90% según datos obtenidos a través de las pruebas realizadas con NTGM; esto se logra por la organización mediante capas, en donde cada una tiene funciones específicas.
- Cuando se crean VLANs en una red de datos, todos los equipos que pertenecen a una VLAN están interconectados sin necesidad de estar ubicados dentro de un mismo espacio físico, lo que le permite al CUP adaptarse a los cambios de ubicación física del personal dentro del campus.
- Cuando existe un daño en la red jerárquica, se analiza desde la capa de acceso hasta la capa núcleo, identificando con exactitud el segmento de la red en donde se encuentra la falla, permitiendo aislar el problema sin afectar el resto de la red y solucionarlo de manera eficiente.
- Las herramientas de monitoreo WhatsUp y Cacti, facilitan la identificación rápida de las fallas, a través de alarmas enviadas al correo electrónico y de su entorno gráfico.
- Hoy en día es muy importante administrar la red de manera eficaz, ya que la mayoría de procesos que se llevan a cabo en una institución se las realiza en línea, y una falla que afecte a la red causaría muchas pérdidas, de ahí radica la importancia de implementar una NOC.

- El NOC permite tener un control centralizado de la red, pudiendo hacer uso de un SSH para tener acceso o acceder a la consola del sistema, a través de la dirección IP del servidor de monitoreo, permitiendo que la información se concentre en un solo punto, al cual pueden acceder el personal encargado de la red, permitiendo atacar los problemas, analizar las estadísticas, conocer el estado de los dispositivos. Esto permite tomar acciones proactivas en base a los reportes.

- El NOC nos ayuda a mejorar la calidad de los servicios, generando alarmas cuando la red o parte de ella está siendo afectada, lo que permite a los administradores de la red ser proactivos y estar preparados ante las fallas.

- El uso de sistemas de monitoreo, permitió analizar datos importantes acerca del rendimiento de la red, además de permitir detectar los problemas de manera rápida, ya sea mediante algún tipo de alerta o incluso observándolo en la consola del sistema de monitoreo, con lo que se identifica de manera exacta el dispositivo o área afectada.

Recomendaciones.

- Adquirir Switches programables de alto rendimiento, que permitan crear VLANs para incrementar la productividad, seguridad y privacidad de la red.

- Respaldar la configuración de los dispositivos de red, con la finalidad de restaurarlos en el momento que así se requiera.

- Crear una DMZ centralizada, para proteger la red contra agentes externos que afecten el correcto funcionamiento de la red.

- Organizar la infraestructura de red utilizando cable UTP Cat 6, para incrementar la velocidad de transmisión. Este cable al no ser afectado por la diafonía asegura su desempeño ya que cuenta con un separador de polietileno.

- Es importante que el cuarto de comunicaciones, esté organizado y adecuado de acuerdo con las normas TIA/EIA-568 y TIA/EIA- 569 de tal manera que garantice su correcto funcionamiento y evite daños en los equipos.

- Implementar un NOC, para monitorear permanentemente la red e identificar fallos in situ; de esta manera podrán analizar el problema y establecer soluciones óptimas.

- Seleccionar el sistema de monitoreo que nos proporcione los datos requeridos para el análisis, de acuerdo a las necesidades de la institución.

- Crear normas y políticas de seguridad, que permitan tener un control acerca del uso de la infraestructura de la red.

- Elaborar plan de contingencia, para los procesos más relevantes de la institución.

- Respaldar la información más relevante de la institución, de ser posible fuera de ella.

- Las plantillas propuestas para el informe de fallas pueden ser ingresadas en una base de datos, con la finalidad de poder acceder rápidamente a ellas.

- Se recomienda, poner énfasis en la creación de políticas de seguridad, para restringir el acceso físico al MDF, así como también crear mayor seguridad para la infraestructura lógica.

- Actualizar constantemente los procedimientos ante los fallos, buscando siempre las mejores alternativas de solución, a la par con los problemas que se vayan suscitando en la red.

BIBLIOGRAFÍA.

[1] LUIS R, *El modelo Jerárquico 3 capas de* Cisco [ref. 10 de Noviembre del 2011].disponible en Web: <http://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/>.

[2] STAKY, Cisco Networking Academy Program CCNA 3 and 4 versión 3.1., 67-70 pp

[3] SILVIU ANGELESCU Y ANDREW SWERCZEK, Networking Basics, Editorial Wiley Publishing, Inc. Pp 99-105

[4] CISCO, CCNA Explorarion 4.0, Conmutación y conexión inalámbrica de LAN, [ref. 04 de mayo del 2011], disponible en Web http://es.scribd.com/doc-17481738/Cisco-CCNA-3-Exploration-Conmutacion-y-Conexion-Inalambrica-de-LAn-Version-40-Español-

[5] Diseño de LAN, Conmutación y conexión inalámbrica de LAN, Capítulo1 [ref. 22, de octubre del 2011] disponible en Web: RedesWeb.com

[6] SILVIU ANGELESCU Y ANDREW SWERCZEK,Book VI Network Security, Editorial Wiley Publishing, Inc. pp 717-725

[7] SILVIU ANGELESCU Y ANDREW SWERCZEK, Book VI Netword Security, Editorial Wiley Publising, Inc pp735-755.

[8] CISCO NETWORKING ACADEMY PROGRAM, CCNA 1and 2 versión 3.1

[9] STAKY, Cisco Networking Academy Program CCNA 1and 2 versión 3.1, pp400, 401

[10] SILVIU ANGELESCU Y ANDREW SWERCZEK,Book III Switching whith Cisco Switches, Editorial Wiley Publishing, Inc. pp 415-438

[11] CISCO, *Cisco Catalyst 2960 Series Switches Compare Models*, [3 de diciembre del 2011], disponible en Web:

http://www.cisco.com/en/US/products/ps6406/prod_models_comparison.html

[12]CISCO, *Cisco Router Compare Models*, <http://www.cisco.com/en/US/products/ps6406/prod_models_comparison.html>[3 de diciembre del 2011]

[13] DIANA D, STIZLER;PATRICIA G; SMITH; ABRIL N. MARINE, Building a Network, Information Services Infrastructure,[ref. 25 de enero del 2012], Disponible en Web:http://tools.ietf.org/html/rfc1302

[14] DANNY BASTIDAS, DANIEL USHIÑA, *Estudio para la Implementación de una NOC, pp 15-22*

[15]CACTI, *Cacti*, [ref. 29 de enero del 2012], Disponible en Web:<www.cacti.net>

[16] ADREM SOFTWARE, NetCrunch 6, [ref, 29 de enero del 2012], Disponible en Web :http://www.adremsoft.com.mx/netcrunch/?gclid=CO37tMPkm64CFQxX7Aod0HruAg

[17] WHATSUP,CACTI, *WhatsUP Gold*,[ref. 29 de enero del 2012], Disponible en Web:http://www.whatsupgold.com/

[18] GUSTAVO HIGAS MIYASHIRO, Herramientas de monitoreo en infraestructuras de TI,[ref. 30 de enero del 2012], Disponible en Web:http://blogs.antartec.com/opensource/2011/05/herramientas-de-monitoreo/

[19] GUIDO PINEDA REYES, Evaluación de Redes –EPN, [ref. noviembre 2010], disponible en la Web: http://www.slideshare.net/gpino86/informe-evaluacion-trafico-2868264

[20] UNIVERSIDAD DE OVIEDO, Redes – Tema 4: Redes Locales,[ref. octubre 2011], disponible en la Web: http://www.isa.uniovi.es/docencia/redes/Apuntes/tema4.pdf

[21] ALVARO JARVIER MORENO BALDERRAMA, Normas y Estándares para un Sistema de cableado Estructurado(SCE) [ref octubre 2011] , disponible en la Web : http://www.slideshare.net/riftbol/normas-y-estndares-para-un-sistema-de-cableado-estructurado-sce

[22] JOSÉ JOSKOWICS. ING , Cableado Estructurado[ref noviembre 2011].

[23]LISSET, DÍAZ CERVANTES, Evaluación de la herramienta GNS3 con conectividad a enrutadores reales [ref diciembre 2012], disponible en la Web: http://upcommons.upc.edu/pfc/bitstream/2099.1/9989/1/PFC_Lisset_D%C3%ADaz.pdf

[24] Manual de Packet Tracer 4.0, [ref enero 2012], disponible en la Web: http://www.nubis.es/manuales/packet4.pdf.

[25]LUIS ALBERTO, ORELLANA BENAVIDES; RAFAEL CRISTOBAL HERNÁNDEZ VAZQUEZ; Seguridad en redes de datos, [ref. 19 de enero del 2013]. Disponible en la Web: http://rd.udb.edu.sv:8080/jspui/bitstream/123456789/265/1/033380_tesis.pdf.

[26]JUNIOR SUMOSA; GNS3 Simulador de Redes Gráfico, [ref, enero 2012], disponible en la Web:]http://es.scribd.com/doc/11840950/GNS3-Simulador-de-Redes-Grafico

[27] EMILIO, HERNÁNDEZ; CARLOS FIGUEIRA, Redes Locales Virtuales (VLANs), [red. 12 de diciembre del 2012], Disponible en la Web: http://ldc.usb.ve/~figueira/Cursos/redes3/Material/LaminasTeoria/VLAN.pdf

ANEXOS

Anexo 1.

A.1.1. Documentos de Solicitud emitidos.

Cariamanga, 16 de Agosto del 2011.

Eco.

Ricardo Donoso.

DIRECTOR DE LA UNIVERSIDAD TECNICA PARTICULAR DE LOJA EXT. CARIAMANGA.

Presente.

De mi consideración:

Yo, Andrea Cecilia Torres Torres con número de cédula 1104415417, estudiante de la UTPL, me dirijo a Ud. con la finalidad de informar, que como parte de mi formación académica para obtener el título de Ingeniera en Informática, he presentado como proyecto de tesis "**Diseño de la Red de área Local de la UTPL extensión Cariamanga, basado en el modelo Jerárquico de tres capas"** ,mismo que luego de haber seguido procesos respectivos, ha sido aprobado por el director de la Escuela de Ciencias de la Computación, Ing. Nelson Piedra Pullaguari; por tal motivo, muy comedidamente me permito solicitarte se me facilite la información necesaria para cumplir exitosamente con mi proyecto.

Segura de contar con su ayuda, hago propicia la oportunidad para expresarle mi consideración y estima.

Atentamente.

Andrea Cecilia Torres Torres

Estudiante de la UTPL.

Anexo 2.

A.2.1. Configuración de los equipos de la Red Jerárquica Cisco, en el Packet Tracer.

Luego de haber emulado satisfactoriamente la red Jerárquica de Cisco para el centro universitario Cariamanga en el Packet Tracer Cisco, es importante hacer conocer la configuración de cada uno de los equipos de red, esto con la finalidad de facilitar la implementación del modelo Jerárquico a la persona que se encarga de la administración de la red.

A continuación se presenta la configuración correspondiente:

A.2.1.1. Configuración del Switch de distribución.

Configurar el switch como servidor.

Switch> enable

Switch#configure terminal

Switch(config)#hostname SwDis

SwDis(config)# vtp mode server

SwDis(config)#vtp domain todopacketracer

SwDis(config)#vtp password 1234

Creación de las vlans

SwDis(config)#vlan 2

SwDis(config)#name vlan VlanSecretaria

SwDis(config)#exit

SwDis(config)#vlan 3

SwDis(config)#name vlan VlanDireccion

SwDis(config)#exit

SwDis(config)#vlan 4

SwDis(config)#name vlan VlanCoordT

SwDis(config)#exit

SwDis(config)#vlan 5

SwDis(config)#name vlan VlanBiblioteca

SwDis(config)#exit

SwDis(config)#vlan 6

SwDis(config)#name vlan VlanSalaA

SwDis(config)#exit

SwDis(config)#vlan 7

SwDis(config)#name vlan VlanSalaB

SwDis(config)#exit

SwDis(config)#vlan 8

SwDis(config)#name vlan VlanInalambrica

SwDis(config)#exit

SwDis(config)#vlan 9

SwDis(config)#name vlan VlanServidores

SwDis(config)#exit

SwDis(config)#vlan 10

SwDis(config)#name vlan Datos-Loja

SwDis(config)#exit

SwDis(config)#vlan 11

SwDis(config)#name vlan Multicast-Internet

SwDis(config)#exit

Direccionamiento de las interfaces de las vlan

SwDis(config)#interface vlan 2

SwDis(config-if)#ip address 172.18.2.1 255.255.255.0

SwDis(config-if)#exit

SwDis(config)#interface vlan 3

SwDis(config-if)#ip address 172.18.3.1 255.255.255.0

SwDis(config-if)#exit

SwDis(config)#interface vlan 4

SwDis(config-if)#ip address 172.18.4.1 255.255.255.0

SwDis(config-if)#exit

SwDis(config)#interface vlan 5

SwDis(config-if)#ip address 172.18.5.1 255.255.255.0

SwDis(config-if)#exit

SwDis(config)#interface vlan 6

SwDis(config-if)#ip address 172.18.6.1 255.255.255.0

SwDis(config-if)#exit

SwDis(config)#interface vlan 7

SwDis(config-if)#ip address 172.18.7.1 255.255.255.0

SwDis(config-if)#exit

SwDis(config)#interface vlan 8

SwDis(config-if)#ip address 172.18.8.1 255.255.255.0

SwDis(config-if)#exit

SwDis(config)#interface vlan 9

SwDis(config-if)#ip address 172.18.9.1 255.255.255.0

SwDis(config-if)#exit

SwDis(config)#interface vlan 10

SwDis(config-if)#ip address 172.18.10.1 255.255.255.0

SwDis(config-if)#exit

SwDis(config)#interface vlan 11

SwDis(config-if)#ip address 172.18.11.1 255.255.255.0

SwDis(config-if)#exit

Configurar los enlaces troncales

SwDis(config)#interface fa0/1

SwDis(config-if)#switchport trunk

SwDis(config-if)#exit

SwDis(config)#interface fa0/2

SwDis(config-if)#switchport trunk

SwDis(config-if)#exit

SwDis(config)#interface fa0/3

SwDis(config-if)#switchport trunk

SwDis(config-if)#exit

SwDis(config)#interface fa0/5

SwDis(config-if)#switchport trunk

SwDis(config-if)#exit

SwDis(config)#interface fa0/6

SwDis(config-if)#switchport trunk

SwDis(config-if)#exit

SwDis(config)#interface fa0/7

SwDis(config-if)#switchport trunk

SwDis(config-if)#exit

SwDis(config)#interface gi0/1

SwDis(config-if)#switchport trunk

SwDis(config-if)#exit

A.2.1.2. Configuración de los switches de la capa de acceso.

A.2.1.2.1. Configuración del SwitchServidores.

Configuración Básica

Switch>enable

Swich#configure terminal

Switch(config)#enable password cisco

Switch(config)#enable secret class

Switch(config)#line console 0

Switch(config-line)#password cisco

Switch(config-line)#exit

Switch(config)#line vty 0 4

Switch(config-line)#password cisco

Switch(config-line)#exit

Switch(config)#hostname SwServidores

Configuración del Switch en modo cliente

SwServidores(config)#vtp domain todopacketracer

SwServidores(config)#vtp mode client

SwServidores(config)#vtp password 1234

SwServidores(config) # exit

Asignación de los puertos a la Vlan respectiva

SwServidores(config) #int fa0/2

SwServidores(config-if)#sw mode access

SwServidores(config-if)#sw access vlan 9

SwServidores(config-if)exit

SwServidores(config) #int fa0/3

SwServidores(config-if)#sw mode access

SwServidores(config-if)#sw access vlan 9

SwServidores(config-if)exit

Configuración del enlace troncal.

SwServidores(config)#int fa0/1

SwServidores(config-if)#sw mode trunk

SwServidores(config-if)exit

A.2.1.2.2. Configuración del Sw1

Switch>enable

Swich#configure terminal

Switch(config)#enable password cisco

Switch(config)#enable secret class

Switch(config)#line console 0

Switch(config-line)#password cisco

Switch(config-line)#exit

Switch(config)#line vty 0 4

Switch(config-line)#password cisco

Switch(config-line)#exit

Switch(config)#hostname Sw1

Sw1(config)#vtp domain todopacketracer

Sw1(config)#vtp mode client

Sw1(config)#vtp password 1234

Sw1(config) # exit

Sw1(config) #int fa0/1

Sw1(config-if)#sw mode access

Sw1(config-if)#sw access vlan 2

Sw1(config-if)exit

Sw1(config) #int fa0/2

Sw1(config-if)#sw mode access

Sw1(config-if)#sw access vlan 3

Sw1(config-if)exit

Sw1(config) #int fa0/3

Sw1(config-if)#sw mode access

Sw1(config-if)#sw access vlan 9

Sw1(config-if)exit

Sw1(config)#int gi1/1

Sw1(config-if)#sw mode trunk

Sw1(config-if)exit

A.2.1.2.3. Configuración del Sw2

Switch>enable

Swich#configure terminal

Switch(config)#enable password cisco

Switch(config)#enable secret class

Switch(config)#line console 0

Switch(config-line)#password cisco

```
Switch(config-line)#exit

Switch(config)#line vty 0 4

Switch(config-line)#password cisco

Switch(config-line)#exit

Switch(config)#hostname Sw2

Sw2(config)#vtp domain todopacketracer

Sw2(config)#vtp mode client

Sw2(config)#vtp password 1234

Sw2(config) # exit

Sw2(config) #int fa0/2

Sw2(config-if)#sw mode access

Sw2(config-if)#sw access vlan 4

Sw2(config-if)exit

Sw2(config) #int fa0/3

Sw2(config-if)#sw mode access

Sw2(config-if)#sw access vlan 5

Sw2(config-if)exit

Sw2(config)#int fa0/1

Sw2(config-if)#sw mode trunk

Sw2(config-if)exit
```

A.2.1.2.4. Configuración del SwSalaA.

Switch>enable

Swich#configure terminal

Switch(config)#enable password cisco

Switch(config)#enable secret class

Switch(config)#line console 0

Switch(config-line)#password cisco

Switch(config-line)#exit

Switch(config)#line vty 0 4

Switch(config-line)#password cisco

Switch(config-line)#exit

Switch(config)#hostname SwSalaA

SwSalaA(config)#vtp domain todopacketracer

SwSalaA(config)#vtp mode client

SwSalaA(config)#vtp password 1234

SwSalaA(config) # exit

SwSalaA(config) #int fa0/1

SwSalaA(config-if)#sw mode access

SwSalaA(config-if)#sw access vlan 6

SwSalaA(config-if)exit

SwSalaA(config) #int fa0/3

SwSalaA(config-if)#sw mode access

SwSalaA(config-if)#sw access vlan 6

SwSalaA(config-if)exit

SwSalaA(config)#int fa0/2

SwSalaA(config-if)#sw mode trunk

SwSalaA(config-if)exit

A.2.1.2.5. Configuración del SwSalaB.

Switch>enable

Swich#configure terminal

Switch(config)#enable password cisco

Switch(config)#enable secret class

Switch(config)#line console 0

Switch(config-line)#password cisco

Switch(config-line)#exit

Switch(config)#line vty 0 4

Switch(config-line)#password cisco

Switch(config-line)#exit

Switch(config)#hostname SwSalaB

SwSalaB(config)#vtp domain todopacketracer

SwSalaB(config)#vtp mode client

SwSalaB(config)#vtp password 1234

SwSalaB(config) # exit

SwSalaB(config) #int fa0/2

SwSalaB(config-if)#sw mode access

SwSalaB(config-if)#sw access vlan 7

SwSalaB(config-if)exit

SwSalaB(config) #int fa0/3

SwSalaB(config-if)#sw mode access

SwSalaB(config-if)#sw access vlan 7

SwSalaB(config-if)exit

SwSalaB(config)#int fa0/1

SwSalaB(config-if)#sw mode trunk

SwSalaB(config-if)exit

A.2.1.3. Configuración de los Routers.

A.2.1.3.1. Router Datos Cariamanga.

Router>enable

Router#configure terminal

Router(config)# hostname RDatosCmga

RDatosCmga(config)#line console 0

RDatosCmga(config-line)#password cisco

RDatosCmga(config-line)#login

RDatosCmga(config-line)#exit

RDatosCmga(config)#line vty 0 4

RDatosCmga(config-line)#password cisco

RDatosCmga(config-line)#login

RDatosCmga(config-line)#exit

RdatosCmga(config)#int fa0/0

RdatosCmga(config-if)#int fa0/0.1

RdatosCmga(config-subif)# encapsulation dot1Q 10

RdatosCmga(config-subif)#ip address 172.18.10.2 255.255.255.0

RdatosCmga(config-subif)#no shutdown

RdatosCmga(config-subif)#end

RdatosCmga#configure terminal

RdatosCmga(config)#int serial0/0

RdatosCmga(config-if)# ip address 192.168.10.1 255.255.255.252

RdatosCmga(config-if)#no shutdown

RdatosCmga(config-if)#exit

Configuración de las rutas[8]

RdatosCmga(config)#ip route 172.16.24.0 255.255.255.0 192.168.10.2

RdatosCmga(config)#ip route 172.18.2.0 255.255.255.0 1172.18.10.1

RdatosCmga(config)#exit

RdatosCmga#

[8]A través de este router solamente la VLAN de secretaría puede comunicarse con la Red de datos Loja.

A.2.1.3.2. Router Datos Loja.

```
Router>enable

Router#configure terminal

Router(config)# hostname RDatosLoja

RDatosLoja(config)#line console 0

RDatosLoja(config-line)#password cisco

RDatosLoja(config-line)#login

RDatosLoja(config-line)#exit

RDatosLoja(config)#line vty 0 4

RDatosLoja(config-line)#password cisco

RDatosLoja(config-line)#login

RDatosLoja(config-line)#exit

RDatosLoja(config)#int fa0/0

RdatosLoja(config-if)#ip address 172.16.24.10 255.255.255.0

RdatosLoja(config)#no shutdown

RdatosLoja(config)interface serial 0/0

RdatosLoja(config-if)ip address 192.168.10.2 255.255.255.252

RdatosLoja(config-if)clock rate 56000

RdatosLoja(config-if)no shutdown

RdatosLoja(config-if)exit

RdatosLoja(config)#ip route 172.18.2.0 255.255.255.0  192.18.10.1

RdatosCmga(config)#exit
```

A.2.1.3.3. Router Internet Cariamanga.

Router>enable

Router#configure terminal

Router(config)# hostname RInternetCmga

RInternetCmga(config)#line console 0

RInternetCmga(config-line)#password cisco

RInternetCmga(config-line)#login

RInternetCmga(config-line)#exit

RInternetCmga(config)#line vty 0 4

RInternetCmga(config-line)#password cisco

RInternetCmga(config-line)#login

RInternetCmga(config-line)#exit

RInternetCmga(config)#int fa0/0

RInternetCmgaconfig-if)#int fa0/0.1

RInternetCmga(config-subif)# encapsulation dot1Q 11

RInternetCmga(config-subif)#ip address 172.18.11.2 255.255.255.0

RInternetCmga(config-subif)#no shutdown

RInternetCmga(config-subif)#end

RInternetCmga#configure terminal

RInternetCmga(config)# int serial0/0

RInternetCmga(config-if)#ip address 192.168.10.5 255.255.255.252

RInternetCmga(config-if)#no shutdown

RinternetCmga(config-if)#exit

RInternetCmga(config)#int serial0/1

RInternetCmga(config-if)# ip address 192.168.10.9 255.255.255.252

RInternetCmga(config-if)#no shutdown

RInternetCmga(config-if)#exit

RInternetCmga(config)#ip route 172.16.242.64 255.255.255.224 192.168.10.2

RInternetCmga(config)#ip route 172.18.0.0 255.255.0.0 172.18.11.1

RInternetCmga(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.10

RInternetCmga(config)#exit

RinternetCmga#

A.2.1.3.4. Router Multicast.

Router>enable

Router#configure terminal

Router(config)# hostname RMulticast

RMulticast(config)#line console 0

RMulticast(config-line)#password cisco

RMulticast(config-line)#login

RMulticast(config-line)#exit

RMulticast(config)#line vty 0 4

RMulticast(config-line)#password cisco

RMulticast(config-line)#login

RMulticast(config-line)#exit

RMulticast(config)#int fa0/0

RMulticast(config-if)#ip address 172.16.242.65 255.255.255.224

RMulticast(config)#no shutdown

RMulticast(config)# int serial0/0

RMulticast(config-if)#ip address 192.168.10.6 255.255.255.252

Rmulticast(config-if)#clock rate 56000

RMulticast(config-if)#no shutdown

RMulticast(config-if)#exit

RMulticast(config)#ip route 172.18.0.0 255.255.0.0 192.168.10.5

Rmulticast(config)#exit

Rmulticast#

A.2.1.3.5. Router Internet.

Router>enable

Router#configure terminal

Router(config)# hostname RInternet

RInternet(config)#line console 0

RInternet(config-line)#password cisco

RInternet(config-line)#login

```
RInternet(config-line)#exit

RInternet(config)#line vty 0 4

RInternet(config-line)#password cisco

RInternet(config-line)#login

RInternet(config-line)#exit

RInternet(config)#int fa0/0

RInternet(config-if)#ip address 10.10.10.1 255.255.255.0

RInternet(config)#no shutdown

RInternet(config)# int serial0/0

RInternet(config-if)#ip address 192.168.10.10 255.255.255.252

Rmulticast(config-if)#clock rate 56000

RMulticast(config-if)#no shutdown

RMulticast(config-if)#exit

RMulticast(config)#ip route 172.18.0.0 255.255.0.0 192.168.10.9

Rmulticast(config)#exit

Rmulticast#
```

Anexo 3.

A.3.1. NOC.

De acuerdo al RFC 1302, se la define a la NOC (Centro de Control de Operaciones de la Red), como “una organización cuyo objetivo es supervisar y mantener las operaciones diarias de una red” [13].

El NOC se encarga de monitorear permanentemente la red de datos, garantizando su buen funcionamiento y una adecuada administración, para ello establece políticas y procedimientos para llevar a cabo las actividades requeridas, además de asignar el personal idóneo para una determinada actividad.

A.3.1.1. Objetivos de un NOC.

Los objetivos principales de un NOC son los siguientes:

- Monitorear permanentemente la situación actual de la red.
- Identificar los problemas que se susciten en la red monitoreada.
- Alertar de forma inmediata, acerca del problema identificado en la red.
- Crear los diferentes reportes acerca de la situación presente y pasada de la red de datos, esto a partir de la fecha en que ha sido implantado el NOC.

A.3.1.2. Elementos principales que monitorea una NOC.

Una NOC se encarga de monitorear las siguientes parámetros [14]:

- Disponibilidad.
- Carga.
- Status.

Disponibilidad. Un elemento de la red está disponible o no, es decir si se encuentra activo o inactivo, en caso de estar inactivo inmediatamente se envían las alertas programadas ante este tipo de eventos para dar solución al problema identificado.

Carga. Identifica que área de la red está utilizando más o menos ancho de banda, dando a conocer la carga en cada segmento de la red.

Status. Permite conocer el estado de la red en determinado momento.

A.3.1.3. Áreas funcionales de una NOC.

Un NOC, está compuesta por diferentes áreas que se adaptan a las redes de datos que requieren ser monitoreadas, brindando seguridad a la red. En la siguiente figura a.3.1 se pueden identificar las diferentes áreas pertenecientes a un NOC.

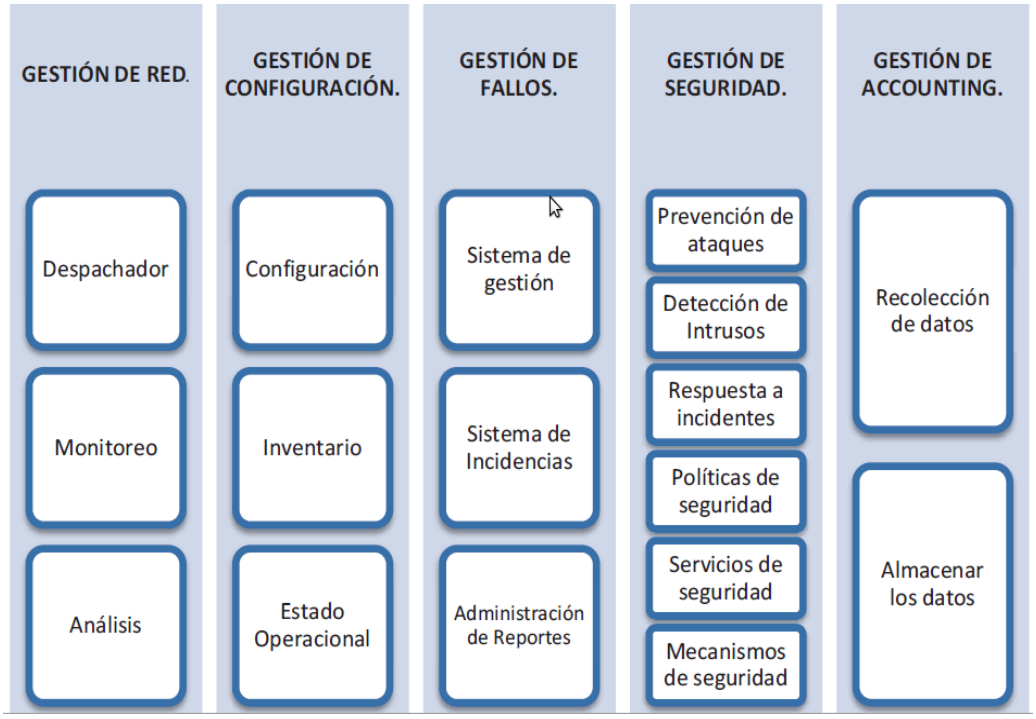


Figura a.3. 1. Áreas Funcionales del NOC. [14]

A.3.1.3.1. Gestión de Red.

Monitoreo permanente de la red de datos, en busca de cualquier anormalidad, dando lugar a la detección oportuna ante las incidencias para dar una solución efectiva en el menor tiempo posible.

- **Despachador,** Un despachador "establece el punto de ingreso de solicitudes y reportes para su posterior direccionamiento al área de operación correspondiente para su seguimiento y solución" [14]. Una vez identificado el problema o falla de la red, se identifica a la persona idónea para solventar dicho problema, facilitando de esta manera el trabajo. El NOC nos sugiere a la persona apta para dar solución al problema en el menor tiempo posible.

- **Monitoreo,** encargado de vigilar siempre el estado actual de la red de datos, verificando su correcto funcionamiento, e identificando las diversas fallas o problemas que puedan darse.

- **Análisis de datos,** en base a lo monitoreado se realiza el análisis con la finalidad de interpretar como se encuentra la red de datos en un momento dado. Este análisis permite mejorar significativamente el rendimiento de la red o mantenerla en excelente funcionamiento.

A.3.1.3.2. Gestión de configuración.

"Es tarea de un NOC hacer que cada nodo esté bajo las configuraciones y el esquema topológico establecido, a fin de garantizar su operatividad**"** [14].

Cuando uno de los equipos de la red no está con las configuraciones establecidas, sin haber sido comunicado dicho cambio, se deben realizar los informes correspondientes para determinar cuál ha sido la causa y corregir dicho problema o conocer simplemente las nuevas configuraciones.

- **Configuración***,* se establece como debe estar constituida y configurada la red de datos para su correcto funcionamiento.

- **Inventario***,* detalles de cómo se encuentra constituida la red, así como todo el historial de lo acontecido en la red.

A.3.1.3.3. Gestión de Fallas.

Garantiza la oportuna detección de las fallas, para una pronta corrección, previo a un seguimiento del problema para determinar la solución más óptima.

- **Sistema de gestión**, la figura a.3.2 nos muestra cual es el proceso a seguir ante cualquier falla identificada:

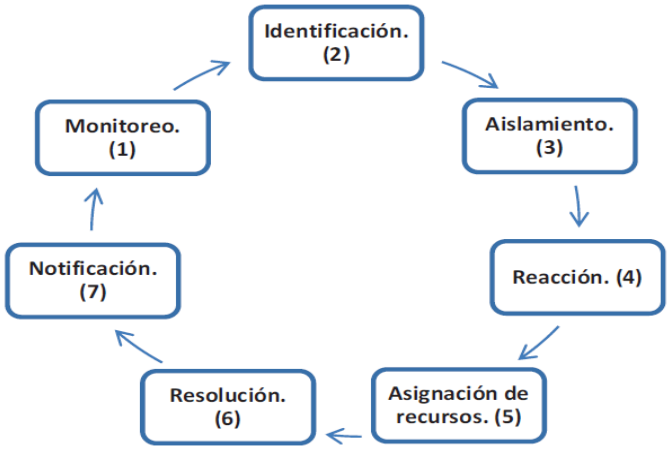


Figura a.3. 2. Gestión de Fallas del NOC. [14]

El objetivo principal del NOC es monitorear permanentemente la red de datos, y ante cualquier falla identificada alertar a las personas encargadas de la administración de la red, con la finalidad de solucionar el problema en el menor tiempo posible.

Antes de llegar a la solución del problema se llevan a cabo los procesos identificados en el gráfico anterior. Además de lo dicho se debe realizar las actividades de los sistemas de incidencias y reportes, de los cuales se habla a continuación.

- **Sistemas de incidencias**. "Programas que asignan tareas delegando responsabilidades, a su vez supervisa las actividades realizadas durante la resolución de la falla y realiza un análisis de los problemas surgidos" [14]. Es importante dar seguimiento a las fallas que han sido identificadas con anterioridad, para conocer a detalle la causa de la falla, el personal que ha sido asignado para dar solución al problema, así como las actividades que llevaran a cabo y el tiempo estimado para el cumplimiento de dicha actividad. Los sistemas de incidencias son

- **Seguimiento de reportes**. Cada uno de los reportes del estado de una falla en determinado momento quedan almacenados ya sea en una herramienta informática o en documentos impresos, para que sirva como una fuente de consulta y en lo posterior hacer una comparación con los problemas identificados, registrando las actividades realizadas para la resolución del problema.

A.3.1.3.4. Gestión de Seguridad.

Como su nombre mismo lo dice se encarga mantener la seguridad de toda la red de datos. El constante monitoreo le permite estar preparado ante cualquier incidencia que pueda darse.

- **Prevención de ataques**, la seguridad implementada intenta prevenir toda clase de ataque a la red.

- **Detección de intrusos**, debe identificar en tiempo real y con exactitud el momento en que la red está siendo atacada la red de datos, con la finalidad de alertar al personal, para que tome medidas y detenga el ataque.

- **Respuesta a incidentes**, las medidas tomadas ante el incidente identificado.

- **Políticas de seguridad**, todas las políticas implementadas para salvaguardar la integridad de la red.

- **Servicios de seguridad**, son los servicios principales que debe ofrecer una red de datos, para que esta sea segura. Los servicios de seguridad son los siguientes: “Confidencialidad, autenticación, integridad, control de acceso” [14].

- **Mecanismos de Seguridad**, existen diversos mecanismos de seguridad aplicables a una red de datos, tal como: antivirus, cortafuegos, ACL, IPSec, entre otros.

- Procedimiento de seguridad, los procedimientos para la seguridad abarcan todas las actividades que se llevan a cabo, con la finalidad de incrementar la seguridad de la red.

A.3.1.3.5. Gestión de Análisis de datos.

El monitoreo permanente de la red permite obtener datos precisos, que son almacenados y en base a estos generar datos estadísticos que permitan conocer con exactitud la situación de la red de datos en determinado momento, generando de esta manera información útil.

Los objetivos que se persigue en la gestión de análisis son los siguientes:

- "Identificar el uso ineficiente de la red.
- Evitar sobrecargas dentro de la red y perjuicios a otros usuarios.
- Planificar el crecimiento de la red.
- Verificar los servicios a los usuarios en función de sus necesidades"[14]

A.3.1.4.Herramientas de Monitoreo.

En la actualidad existen muchas herramientas para monitorear el estado de la red (sección 3.2). Las herramientas que fueron analizadas es la presente tesis son:

- Cacti.
- Whatsup Gold .
- NetCrunch 6.
- Munin.
- Nagios.

A.3.2. Propuesta del NOC para el CUP.

El esfuerzo de diseñar e implementar una red adecuada para el CUP no concluye allí, es necesario también tener un control y monitoreo permanente de la red, con la finalidad de identificar las fallas que ocurran en tiempo real y darle una pronta solución al problema.

El NOC, debe ser aplicado a la red actual del CUP (observemos la figura 2.2), con la finalidad conocer su estado. El NOC requiere del trabajo en equipo, para cumplir con sus objetivos.

Sabemos que es ilusorio creer que los riesgos y problemas pueden eliminarse por completo, pero deben reducirse a niveles aceptables y esto se logra con una adecuada administración de la red de datos, y para lograrlo se propone la implementación de una NOC, que requiere poca inversión, frente a los beneficios que este nos ofrece.

A.3.2.1. Requerimientos para Implantar el NOC en el Centro Universitario Cariamanga.

Con la finalidad de elegir los sistemas de monitoreo adecuados, que se adapten a los requerimientos del Centro Universitario, es necesario identificar los requerimientos.

- Monitorear cada uno de los equipos que conforman la red, en todo momento, específicamente en los routers, switches, servidores.
- Los agentes o equipos a ser monitoreados deben brindar la información suficiente para llevar el control del estado de funcionamiento.
- Los sistemas de monitoreo deben emitir alertas, ante la presencia de anormalidades en su operación, para que el encargado de la red mediante la alarma sepa de forma inmediata que existe un problema en la red.
- Monitorear las interfaces, con la finalidad de conocer los paquetes que entran y salen de cada interfaz de red.
- Se necesita monitorear el uso de recurso de cada máquina, recursos como disco, red, uso de CPU, RAM.
- Monitorear cuanto ancho de banda se está utilizando en la red.
- Conocer los protocolos se están utilizando en la red.
- Se requiere tener datos estadísticos sobre el estado de la red, componentes y la utilización del ancho de banda por día, mes, etc, de acuerdo al informe que se requiera obtener en determinado momento.

A.3.2.2. Áreas funcionales del NOC.

A.3.2.2.1. Gestión de Monitoreo.

Como habíamos mencionado es necesario monitorear la red las 24 horas y los 7 días a la semana, por parte del personal encargado de la administración de la red, el mismo que debe estar atento ante cualquier evento o alarma generado por los sistemas de monitoreo, con la finalidad de tomar las acciones pertinentes.

A.3.2.2.2. Gestión de análisis de los datos.

Mediante el monitoreo podemos obtener datos estadísticos acerca de la red de datos. Estos datos estadísticos facilitan la administración, permitiendo la prevención de algunos eventos que afecten su estado.

Para poder realizar un análisis de los datos obtenidos a través de los agentes de monitoreo, se establecen algunos parámetros que nos permitan tener una noción clara acerca del funcionamiento de la red.

- Tráfico entrante y saliente de los enlaces principales, entre los equipos de red.
- Datos acerca del uso de los recursos de cada dispositivos de red, recursos tales como:
    - Discos duro.
    - Uso del CPU.
    - Memoria RAM.
- Conocer el ancho de banda se está utilizando por grupo de usuarios.
- Reportes automáticos de los eventos sucedidos en los dispositivos o por periodos de tiempo.
- Saber que protocolos se están utilizando en la red.
- Se requiere tener datos estadísticos sobre el estado de la red, por día, mes, etc. de acuerdo al informe que se requiera en determinado momento.

Procedimiento para el análisis de los datos.

Para un adecuado análisis de los datos es necesario determinar los procedimientos a seguir:

- Determinar los parámetros de los cuales se necesita obtener sus datos estadísticos, es decir que es lo que se desea monitorear.
- Establecer el lapso de tiempo o los intervalos en que se requiere conocer los datos.
- Hacer uso de las herramientas disponibles para este fin.
- Respaldar los datos obtenidos desde las herramientas de monitoreo.
- Evaluar los datos obtenidos

A.3.2.2.3. Gestión de Configuración.

La gestión de configuración abarca la configuración de las herramientas necesarias para la implementación del NOC, previo estudio de los datos que se requiere monitorear.

Para poder obtener los datos de los dispositivos, es indispensable configurar en los equipos el agente SNMP.

Para configurar el servicio SNMP seguimos los pasos que a continuación se detallan:

A.3.2.2.3.1. Configurar el agente SNMP.

Para poder capturar los datos que requieren ser monitoreados es necesario activar el servicio SNMP, tanto en los servidores como en los dispositivos que se deben monitorear. Toda esta información la podemos encontrar en el Anexo 4.

Configuración de SNMP en Routers Cisco.

Para habilitar el servicio SNMP en un router Cisco, se lo debe configurar en modo privilegiado, en configuración global, para luego ejecutar los comandos necesarios para habilitar el servicio SNMP. Dichos comandos están disponibles en el Anexo 4.

A.3.2.2.3.2. Configuraciones de conectividad.

Se debe garantizar la conectividad entre los diferentes usuarios y servicios, para que exista una comunicación eficiente se debe tener en cuenta algunos aspectos tanto en los routers y los switches:

- Se debe configurar los enlaces troncales para garantizar la conectividad.
- Para que exista comunicación se debe configurar las rutas, ya sean dinámicas o estáticas.
- Comunicación permanente con el proveedor de enlaces WAN de fibra.

A.3.2.2.3.3. Configuraciones de Análisis de datos.

Se debe permitir ciertos servicios en los dispositivos principales de la red.

- Permitir herramientas para obtener toda la información requerida de la red.
- Habilitar los traps de los equipos.
- Estrictamente necesario el uso de SNMP, en cada uno de los dispositivos a monitorear.
- Herramientas de captura de información utilizando sistemas de monitoreo, en nuestro caso utilizaremos WhatsUp Gold y Cacti.
- Permitir la presentación estadística de los datos solicitados para el análisis.

A.3.2.2.3.4. Configuraciones de Seguridad.

Es necesario contar con la seguridad adecuada, para salvaguardar los equipos que conforman la red de datos, y sobre todo el recurso más importante de toda institución la información. A continuación se enlistan algunos parámetros que se deben o pueden aplicar:

- Hacer uso del firewall, para prevenir en parte los accesos internos y externos.
- Hacer uso de usuarios y contraseñas seguras para acceder a un determinado dispositivo.
- Cambiar periódicamente las contraseñas.

- Limitar el número de intentos para ingresar al sistema a través de contraseña, con la finalidad de evitar ataques debido a que han acertado la contraseña correcta.

- Si los switches de la red son configurables, se debe configurar una VLAN de administración de dispositivos.

- Crear un direccionamiento de red exclusivo para la institución, y cuyo direccionamiento solamente sea conocido por el personal que se encuentra a cargo de la administración de la red.

- Es recomendable usar un SHH como Putty u otros, para ingreso o configuración remota de los dispositivos. Habilitado siempre para uso exclusivo de la red interna.

- Si se crea permisos de acceso para el personal, tener en cuenta que cuando ya no labore en la institución, eliminar dicho acceso.

- Como parte de la seguridad se debe implementar las listas de control de acceso para permitir o denegar cierto tráfico o servicio.

- Aplicar las normas ISO 17799 de Seguridad informática, estas reglas contribuyen a la homogenización de la seguridad

Aplicar las políticas de seguridad establecidas por la institución.

A.3.2.2.4.Procedimientos de Gestión de Fallos.

Es importante saber qué hacer en caso de que alguna falla ocurra.

- Como primer punto se debe usar la Metodología Troubleshooting (proceso para la resolución del problema), en donde se debe identificar el problema analizando capa por capa de la infraestructura de red, iniciando desde la capa física. Todo esto una vez que se ha detectado una falla gracias a las alertas emitidas por el sistema de monitoreo.

- Mediante los resultados del monitoreo en modo gráfico o por las alertas emitidas por el sistema, se identifica el dispositivo en el cual ha surgido el problema.

- Una vez identificado el problema se procede a aislar el problema o fallo. En caso de que el equipo que presenta el fallo está siendo usado por un usuario x, se le debe pedir que no use dicho equipo hasta darle solución al problema.

Es importante establecer un nivel de criticidad, para identificar en qué grado afecta la falla a la red de datos. La tabla a.3.1 describe los niveles de criticidad posibles.

Tabla a.3. 1. Niveles de Criticidad.

Nivel De Criticidad	**Afectación a la red.**
Altamente crítico	Afecta al tráfico de toda la red.
Muy crítico	Afectan a la gestión de la red. Como por ejemplo el problema se presenta en un switch
Crítico	Afectan a los equipos finales.
Criticidad baja	Problemas tolerables, la red o equipo puede seguir operando sin mayor inconveniente.

Una vez identificada la criticidad del problema, se debe asignar a la persona idónea para la solución del mismo, luego de ello se debe seguir los siguientes pasos:

- Aislar el problema.
- Revisar los informes de los problemas que se han presentado anteriormente. De coincidir el problema analizar la solución empleada, para establecer si puede ser aplicada en el problema actual.
- Si el problema es nuevo, se debe empezar probando soluciones desde las más sencillas a las más complejas. Es indispensable que el personal encargado de la red notifique el problema y lo documente.

- Dar solución al problema en el menor tiempo posible.
- Una vez solucionado el problema se procede a verificar si efectivamente el problema ha sido resuelto exitosamente.
- Se debe notificar que el problema ha sido resuelto y elaborar el reporte.

A.3.2.2.5. Documentación.

Toda red está conformada por varios dispositivos de red y dispositivos finales, de los cuales se debe conocer sus características. Esta documentación es necesaria para una adecuada administración y control de la red.

A continuación se enlistan algunos parámetros necesarios:

- Nombre del equipo.
- Marca y Modelo.
- Procesador.
- Memoria.
- La ubicación exacta en el edificio donde funciona.
- Etiquetado con el número de rack en donde se encuentra ubicado.
- Dirección IP.
- Contraseña y usuario.
- Sistema Operativo.
- Número de interfaces configuradas.
- Tabla de enrutamiento.
- Fallos presentados y su solución.

Cabe recalcar que estos parámetros deben adaptarse de acuerdo al dispositivo a documentar.

A.3.2.2.5.1 Documentación de las fallas o problemas.

La documentación permitirá identificar las soluciones más efectivas, si el problema ya se hubiese dado y con ello se aplicaría la misma o una mejor solución, permitiendo un ahorro en tiempo y dinero, pero sobre todo disminuye el tiempo de respuesta ante el problema dado aplicando una solución ya comprobada.

Para elaborar la documentación acerca de los problemas, se propone utilizar una plantilla, misma que la podemos encontrar en el Anexo 5.

A.3.2.2.6. Cómo actuar ante las fallas?

Para contrarrestar las fallas que se presenten, es necesario contar con un plan de contingencia mientras se da solución a la falla en el menor tiempo posible.

Se debe tratar de identificar la falla realizando las pruebas pertinentes, para establecer la solución adecuada. A continuación se muestran los procedimientos ante la identificación de una falla.

A.3.2.2.6.1. Procedimientos comunes a utilizar frente a un fallo.

Es muy importante contar con toda la información, correspondiente a la red, como topología, cableado, direccionamiento, protocolos, etc. Todo con la finalidad de facilitar la resolución del problema.

Una vez identificada la falla, se realiza los siguientes procedimientos:

- Si la falla, ya se había presentado antes, es importante recurrir al informe de la falla para ver cuál ha sido la solución aplicada y en base a ello aplicar el mismo o en su defecto aplicar uno más óptimo. Lo que permite un ahorro importante de tiempo.
- Si el problema es nuevo, debe aplicar las soluciones más óptimas a probar, empezando desde las más básicas a las más complejas.
- Todas las soluciones aplicar deben ser notificadas y aprobadas por los miembros de jerarquía alta de la institución.
- Una vez autorizada la ejecución de la solución se la debe documentar.

A.3.2.2.6.2. Recomendaciones para identificar y corregir la falla.

- Se debe revisar el switch en el puerto donde está conectado dicho dispositivo, si el led de dicho puerto está de color verde significa que el puerto está funcional, operando normalmente. Si la luz está de color naranja nos indica el software del equipo ha desactivado el puerto, es decir el puerto está en estado down.

- Revisar el cableado en los dos extremos, así como el tipo de cable que está siendo utilizado.

- Investigar si el administrador fue quien bajó el estado del puerto, algunas veces también puede tratarse de una falla interna del equipo.

- Cuando todos los leds del switch están de color naranja, nos indica que el problema es de hardware.

- Aplicar los diferentes comandos de Cisco, para verificar las configuraciones de los dispositivos, esto nos puede ayudar a conocer la falla.

A.3.2.2.7. Sistema de Seguridad.

Para que la seguridad sea efectiva, debe haber la colaboración de todos los miembros que forma parte de la institución empezando por la parte superior de la jerárquica. Las siguientes recomendaciones constituyen el sistema de seguridad.

- La comunicación constante entre los miembros de la institución contribuye a la seguridad.

- Hacer conocer las normas de seguridad creadas e implementadas por la institución.

- Asignar a una persona para reportar los incidentes de seguridad o puede ser el email.

- Dar mantenimiento constante a todos los equipos que forman parte de la red.

- Cambiar las contraseñas por intervalos de tiempo, con un nivel de seguridad alta, sobre todo en lo que se refiere a los equipos de red.

La seguridad física también es parte importante, se debe aplicar las siguientes recomendaciones:

- Control ante incendios.
- Respaldo de las configuraciones de los equipos de red.
- Respaldo de la información más relevante de la institución.
- Restringir acceso al cuarto de comunicaciones.

A.3.2.2.8. Responsabilidades del Personal del CUP.

El CUP cuenta con poco personal, por lo que es estrictamente necesario asignar las responsabilidades de cada uno.

- Director del CUP, toma las decisiones importantes para llevarse a cabo los proyectos a presentar, que luego deberán ser aprobados por el personal encargado de la sede Loja.
- Administrador de la red, persona que se encarga de la administración de la red de datos. Ante cualquier problema que se presente, debe intentar resolverlo verificando primero los elementos de la red, y realizar las pruebas básicas de conectividad. Pero antes de eso notificar al resto personal CUP.

En caso de no resolver el problema pese a los intentos por lograrlo, se debe notificar al personal encargado de redes en la sede, en donde se asignará el personal especializado para resolver dicha falla.

Cualquier cambio en la red debe ser aprobado por el personal encargado en la sede, una vez aprobado se debe notificar al director del CUP y finalmente ejecutar una acción determinada.

Realizar todas las configuraciones necesarias, para el correcto funcionamiento del NOC.

A.3.2.2.9. Herramientas a utilizar para la implementación del NOC.

Para un correcto funcionamiento del NOC hacen falta algunos elementos adicionales tanto en software como en hardware.

A.3.2.2.9.1. Herramientas de Software.

Para lograr una implementación del NOC de forma eficiente, se requiere hacer uso del software existente que facilite el monitoreo de la red las 24 horas del día y los 7 días de la semana, y que se adapten a los requerimientos del CUP, para ello se han establecido 2 herramientas a utilizar, mismas que se las enlista a continuación.

- Cacti
- WhatsUp Gold

Requerimientos para implantar el NOC en el CUP.

Para cumplir con el propósito planteado, es necesario cumplir con los siguientes requerimientos:

Requisitos del sistema operativo.

WhatsUp funciona correctamente con Windows, por lo que se ha elegido Windows 7. La instalación del sistema de monitoreo Cacti, se la realiza bajo el Sistema Operativo Linux, aunque también es compatible con otros sistemas operativos.

Para instalar estos sistemas de monitoreo, se requiere:

- Contar con MySql, para almacenar los diferentes resultados del monitoreo.
- Cacti, requiere tener previamente software instalado en el sistema, estos son:
  - RRDTool 1.0.49 o superior
  - PHP 4.3.6 o superior.
  - Un servidor Web Apache o IIS.

A.3.2.2.9.2. Requisitos de hardware.

Los sistemas de monitoreo pueden ser instalados en un PC de recursos promedios, no necesita un PC con altos recursos. Además del PC es necesario incluir un monitor, que se conecte al servidor en donde estarán corriendo los sistemas de monitoreo, con la finalidad de tener una mejor visibilidad por parte de quien está encargado de la administración de la red de datos.

El monitor debe ser instalado en la oficina de Coordinación Técnica, en donde se encuentra el personal encargado de la administración de la red.

A.3.2.2.10. Equipos a ser monitoreados

Se debe monitorear los equipos de red:

- Routers.
- Switchs.
- Servidores.

Se debe monitorear los equipos antes mencionados, con la finalidad de administrar adecuadamente la red y obtener la información detallada de estos equipos.

A.3.2.2.11. Presupuesto NOC.

Para hacer un presupuesto estimado para la implementación del NOC, se toman en cuenta los recursos requeridos. En la tabla a.3.2 se hace conocer el presupuesto necesario para la implantación del NOC.

Tabla a.3. 2. Presupuesto estimado para la implementación del NOC.

Descripción	Precio Unitario	Total
2 Computadores con las siguientes características: Procesador Intel, Memoria Ram 2 GB, espacio libre en disco duro, tarjeta de video, Monitor y demás complementos.	1100,00	2200,00
Monitor 32” LCD Sony Bravia,	700,00	700.00
Cable de video VGA 30	45,00	45,00
Soporte de pared para monitor	23,00	23,00
Total		**2968,00**

A.3.3. Monitoreo de la red de datos del CUP

Para monitorear la red, se requiere implementar las siguientes herramientas de monitoreo:

- Cacti.
- WhatsUp Gold.

Estos sistemas permiten recolectar los datos acerca del estado de cada uno de los equipos y de los diferentes parámetros necesarios para el análisis del rendimiento de la red de datos.

Para una adecuada recolección de datos, es importante seguir algunas pautas que se detallan a continuación:

- Cada dispositivo debe identificarse correctamente, con la finalidad de poder realizar una configuración con éxito en cada uno de los sistemas.
- Solamente se podrán monitorear aquellos dispositivos que soporten SNMP, aunque si dichos dispositivos no soportan SNMP si es posible visualizar el ping.
- Monitorear los dispositivos de acuerdo a los parámetros aplicables por cada sistema de monitoreo.
- Saber reconocer el momento de un fallo, solamente con las gráficas arrojados por los sistemas de monitoreo.

A.3.3. Equipo físico para la instalación de los Sistemas de Monitoreo.

Para la implementación de los sistemas de monitoreo, es necesario hacer uso de 2 servidores, uno para el WhatsUp que será instalado en Windows 7, y otro para el Cacti que será instalado en Ubuntu, esto debido a que Cacti funciona sin inconvenientes en Linux. El CUP, facilitó los servidores para la implementación de los sistemas, encargados de monitorear permanentemente la red. Las características físicas de los servidores se encuentran en la tabla a.3.3.

Tabla a.3. 3. Características Físicas de los Servidores.

Servidores.	
Característica	**Descripción**
Marca	ThinkCentre 8149 KSM
Procesador	P4 3 Ghz
Memoria	122
Disco Duro	120 GB
Unidades	Unidad de CD y un Floppy
Tarjetas	2 tarjetas de red
Puertos	4 puertos USB 1 serial.

A continuación se detallan las características de los servidores:

El Sistema Operativo del servidor 1, ha sido instalado bajo las siguientes características, descritas en la tabla a.3.4. En este servidor se encuentra instalado el Sistema de Monitoreo WhatsUp:

Tabla a.3. 4. Configuración del Servidor 1.

Servidor 1	
Características de configuración del Sistema Operativo.	
Característica	**Detalle**
S.O	Windows 7
Idioma	Español
Teclado	Latinoamericano
Zona Horaria	Guayaquil-Ecuador
Disco	Uso de toda la capacidad del disco sin particiones.
Usuarios	Server_ cmga; Password xxxx root; Password xxxx

El Sistema Operativo del servidor 2, ha sido instalado bajo los siguientes características, que se hacen conocer en la tabla a.3.5. que viene a continuación, en este servidor se encuentra instalado el Sistema de monitoreo Cacti.

Tabla a.3. 5. Configuración del Servidor 2.

Servidor 2	
Características de configuración del Sistema Operativo.	
Característica	**Detalle**
S.O	Linux Ubuntu 11.4
Idioma	Español
Teclado	Latinoamericano
Zona Horaria	Guayaquil-Ecuador
Disco	Uso de toda la capacidad del disco sin particiones.
Usuarios	Server_ cmga; Password xxxx root; Password xxxx

A.3.3.1. Equipos que se requiere monitorear.

Se requiere monitorear los equipos de red que conforman las 2 redes, para ello estos equipos deben soportar el Protocolo SNMP. Para conocer cuántos equipos de nuestra red LAN deben ser monitoreados, les invitamos a observar la figura 2.2, para una mayor comprensión, se los describe en la tabla a.3.6.

A.3.3.2. Configuración de los Sistemas de Monitoreo.

Para que los Sistemas de monitoreo, puedan recolectar la información requerida para el análisis de la red de datos se debe configurar e iniciar el protocolo SNMP.

En el S.O Windows se debe iniciar el servicio, que previamente tiene configurado, mientras que en los S.O Linux se debe instalar este servicio, de lo contrario no se podrá capturar la información proveniente de los equipos de red.

Adicionalmente a esto se debe realizar la instalación del protocolo SNMP, en los routers mediante sesiones telnet.

Tabla a.3. 6. Descripción de los equipos que se requiere monitorear.

Dispositivos	Detalle
Servidores	
Servidor 1	En donde tenemos instalado el Sistema de monitoreo WhatsUp Gold,
Servidor 2	Servidor de antivirus, también tiene instalado el Sistema de monitoreo Cacti.
Switches	
Catalyst	Pertenece a la red del Área Administrativa
Switch BaseLine 2816 -16	Pertenece a la red de Centros de Cómputo.
Access Point	Conforma la red inalambrica, cuyo modelo es D-LinK / DWL-3200AP
Routers	
Cisco 2600	Este router pertenece a la red del Area Administrativa
Cisco 881	Este router pertenece a la red de Centros de Cómputo.

A.3.3.2.1. Instalación, configuración de WhatsUp Gold y Cacti.

En el servidor 1, se instaló la versión demo de WhatsUp, con una vigencia de 30 días. Una vez descargado el instalador y de obtener la clave para activarlo, se procedió a instalar y configurar.

El Sistema de monitoreo Cacti se instaló en el servidor 2.

Los procesos de instalación y configuración de los Sistemas de monitoreo, tanto del WhatsUp como del Cacti podemos observarlos a mayor detalle en el Anexo 6.

A.3.3.3. Pruebas de Monitoreo.

Una vez configurados los sistemas de monitoreo, se realizaron varias pruebas con la finalidad de comprobar su correcto funcionamiento, realizando para ellos algunas actividades:

- Provocar las caídas de las interfaces, pertenecientes a los servidores.

- Verificar los datos recibidos, específicamente los datos de disco duro.

Caída de las interfaces.

Dado que no se tiene acceso a los routers y a los switches (además de ser estos últimos no configurables), solamente se realizó la desconexión del cable UTP, que va dirigido a un determinado host, para realizar esta prueba.

Como se había configurado en el sistema de monitoreo la alarma se envió, después de 5 min de haberse producido dicho cambio en el estado de la interfaz.

Cabe mencionar que es importante tener siempre visual el mapa de la red de datos configurada en los sistemas de monitoreo, ya que también al observar podemos darnos cuenta que existe una caída en un determinado dispositivo.

Con estas alarmas enviadas el administrador de la red puede ir al dispositivo exacto, para tratar de dar solución a la falla suscitada.

Una vez solucionado el problema, se puede observar en el mapa que el dispositivo está activo.

Ante la caída de la interfaz, se la debe registrar en el formato propuesto el informe de la falla, con la finalidad de que quede registrado y en lo posterior almacenarla en la base de datos, para tomarlo como referencia ante una falla igual o similar. Este informe de fallas lo podemos encontrar en el Anexo 5.

A.3.3.5. Verificar los datos recibidos.

Los sistemas de monitoreo nos brindan la información de espacio del disco y de la memoria utilizada.

Esta información la podemos verificar en el mismo equipo. Los administradores de la red deben estar atentos cuando la utilización del disco supere el 85% de su capacidad, con esta información se deben tomar las acciones requeridas, antes de que la capacidad del disco este totalmente llena.

A.3.3.6. Monitoreo de los Equipos de Red.

Se debe monitorear los equipos principales de la red, con la finalidad de conocer su estado y el momento en que ocurre una falla. El monitoreo también permite prevenir problemas, o que estos tomen niveles bajos de criticidad afectando de manera mínima a la red. Todo esto debido a que cuando se presenta un problema a nivel de estos equipos afecta de forma sustancial a la red.

A.3.3.6.1. Monitoreo con WhatsUp.

Una vez configurado este sistema de monitoreo, el mapa de red elaborado para el CUP, es tal y como se muestra en la figura a.3.3.

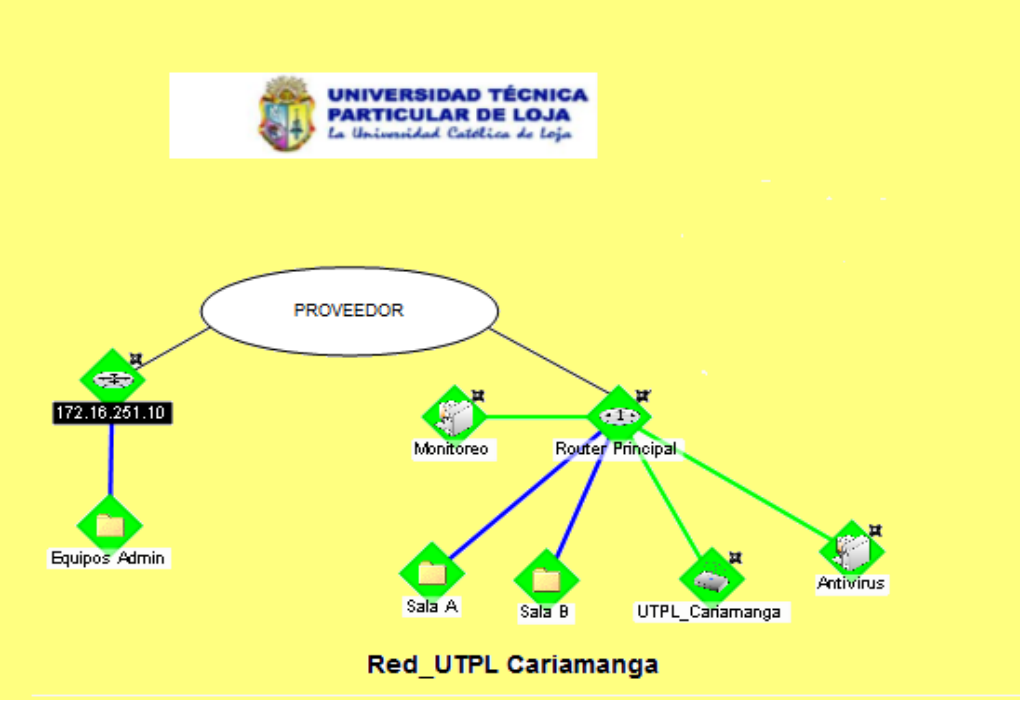


Figura a.3. 3. Esquema de la Red en WhatsUp.

Como podemos observar está conformada por 2 redes, dicha infraestructura la podemos ver en la figura 2.2.

Los equipos que requieren ser monitoreados son los routers, servidores y switches, estos últimos no pueden ser monitoreados debido a que no son configurables y por ende no tienen

una dirección IP que pertenezca a una VLAN, razón por la cual el WhatsUp no puede ubicarlo y agregarlo al esquema.

El servidor de monitoreo está conectado a red 192.168.3.0 y como se requiere monitorear las 2 redes se hizo ping y un tracert la red 172.251.1.0, siendo esta segunda red alcanzable.

Los saltos para alcanzar la red 172.251.1.10 son los siguientes, este comando fue ejecutado desde el servidor de monitoreo, y se muestra en la figura a.3.4.

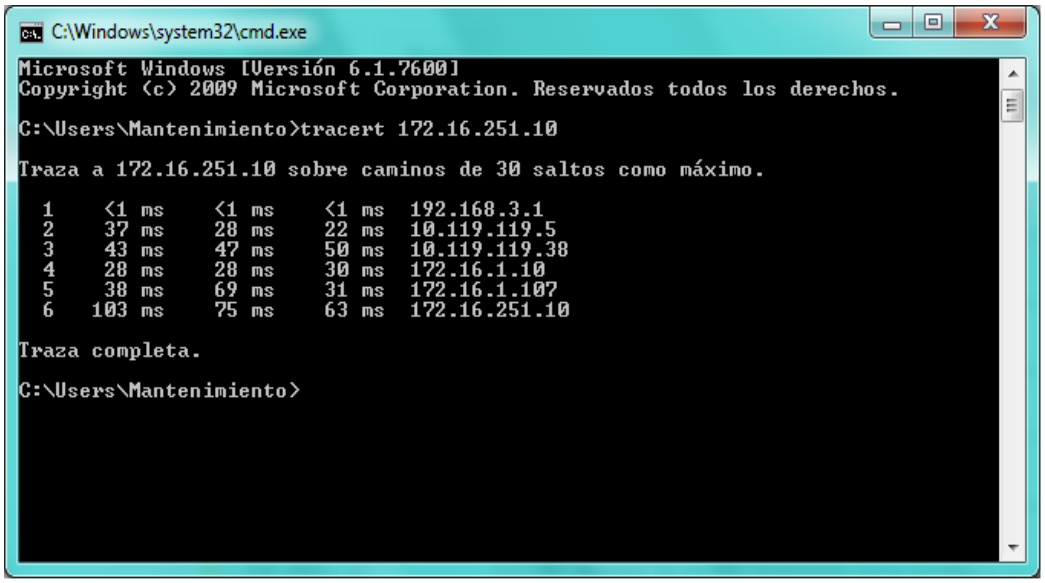


Figura a.3. 4. Saltos para llegar a la siguiente red.

Este Sistema también nos permite conocer el tamaño de la base de datos utilizada para almacenar los resultados del monitoreo, la figura a.3.5., nos muestra el tamaño real de la Bdd.

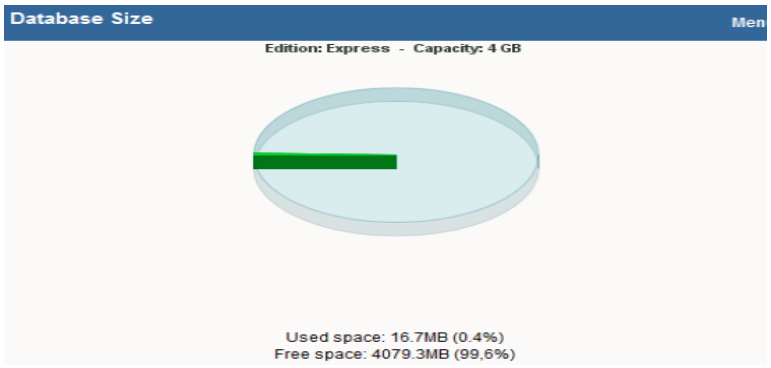


Figura a.3. 5. Tamaño de la Base de datos del WhatsUp.

El gráfico corresponde al monitoreo del 2 de abril del 2012, es por ello que aún el espacio utilizado es de 16.7 MB, ya que el sistema fue instalado el 31 de marzo del mismo año.

Dentro de la página principal también nos detalla el número y tipo de dispositivos que están siendo monitoreados, lo dicho anterior lo podemos observar en la figura a.3.6.

Figura a.3. 6. Dispositivos Monitoreados.

También nos indica el total de dispositivos activos en determinado momento, por lo que es posible hacerles ping, la figura a.3.7 nos muestra que todos los dispositivos sujetos de monitoreo están activos.

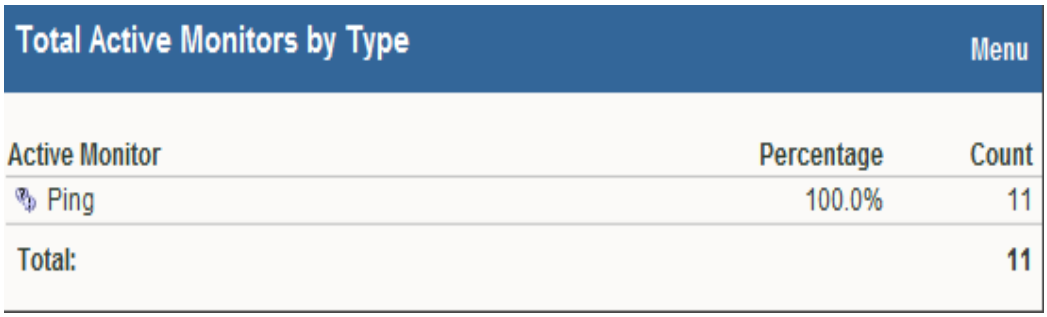
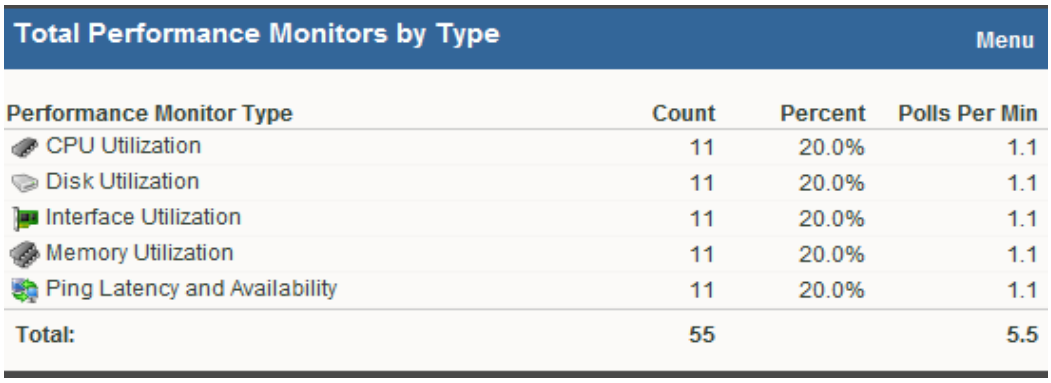


Figura a.3. 7. Total de dispositivos activos.

Además de toda la información presentada, también se muestra el rendimiento total del monitoreo por cada parámetro a monitorear, dichos parámetros los podemos observar en la figura a.3.8.



Total Performance Monitors by Type — Menu

Performance Monitor Type	Count	Percent	Polls Per Min
CPU Utilization	11	20.0%	1.1
Disk Utilization	11	20.0%	1.1
Interface Utilization	11	20.0%	1.1
Memory Utilization	11	20.0%	1.1
Ping Latency and Availability	11	20.0%	1.1
Total:	**55**		**5.5**

Figura a.3. 8. Parámetros monitoreados.

Routers.

Se deben monitorear los routers de cada red: el router de área administrativa, y el de la salas de cómputo. Como se había mencionado anteriormente, tiene que estar activado el SNMP, de lo contrario no se mostraran los datos.

Router de Administración.

Para una mejor explicación se ha numerado los datos presentados por WhatsUp, se muestran en la figura a.3.9, este reporte fue tomado el 2 de abril del 2011.

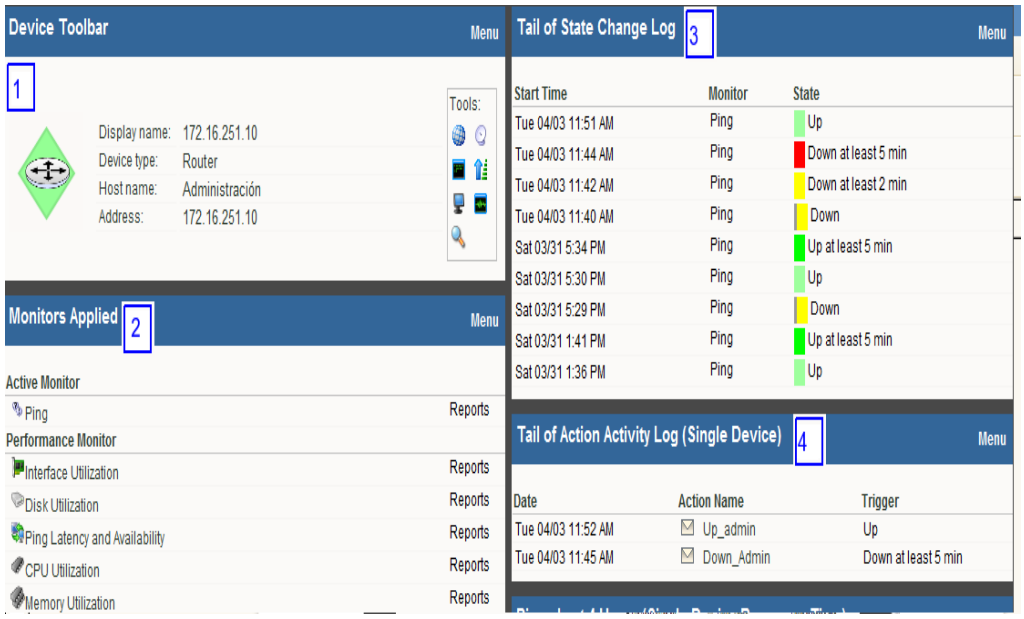


Figura a.3. 9. Reporte del Router del Área administrativa.

- En el área 1 tenemos la barra de herramientas para modificar y buscar algunos parámetros del dispositivo, junto con los datos del router.

- En el área 2, podemos observar los tipos de monitoreo aplicados al router.
- En el área 3, vemos los reportes del estado del router en las últimas horas. Solamente observando la figura a.3.9 podemos darnos cuenta del estado, sin embargo las describiremos brevemente a continuación, empezando desde la parte inferior. Sábado 03/31 a la 1:36 pm, el router está en estado activo.
    - Sábado 03/31 a la 1:41 pm, nos indica que el dispositivo se encuentra en estado up por más de 5 min.
    - Sábado 03/31 a la 5:29 pm, el color amarillo nos indica que el enlace esta caído, es decir que esta desactivado, apagado o sin servicio de internet momentáneamente por menos de 2min.
    - Sábado 03/31 a la 5:30 pm, el router nuevamente está en estado activo.
    - Sábado 03/31 a la 5:34 pm, este estado nos muestra que el router está activo casi 5 min.
    - Luego se registran nuevos estado el martes 04/03 a las 11:40 am, nos indica que el enlace esta caído, es decir que esta desactivado, apagado o sin servicio de internet momentáneamente por menos de 2min.
    - Martes 04/03 a las 11:42 am, nos muestra que el router está desactivado, o no hay servicio de internet por al menos 2 minutos.
    - Martes 04/03 a las 11:44 am, nos indica que el router está desactivado o sin servicio de internet por al menos 5 min, con lo que genera una alarma vía correo electrónico tal y como se configuró.
    - Finalmente el martes 04/03 a las 11:51, el router muestra actividad.
- El área 4 nos indica el registro de actividades del dispositivo, por ejemplo en la acción 2, nos indica que a las 11:45 min, se ha enviado la alerta debido a que ese dispositivo

  estaba en estado down o sin conexión por más de 5 minutos.

• El área 5 se muestra en la figura a.3.10. y corresponde a la respuesta del dispositivo, a continuación se hace conocer la gráfica generada.

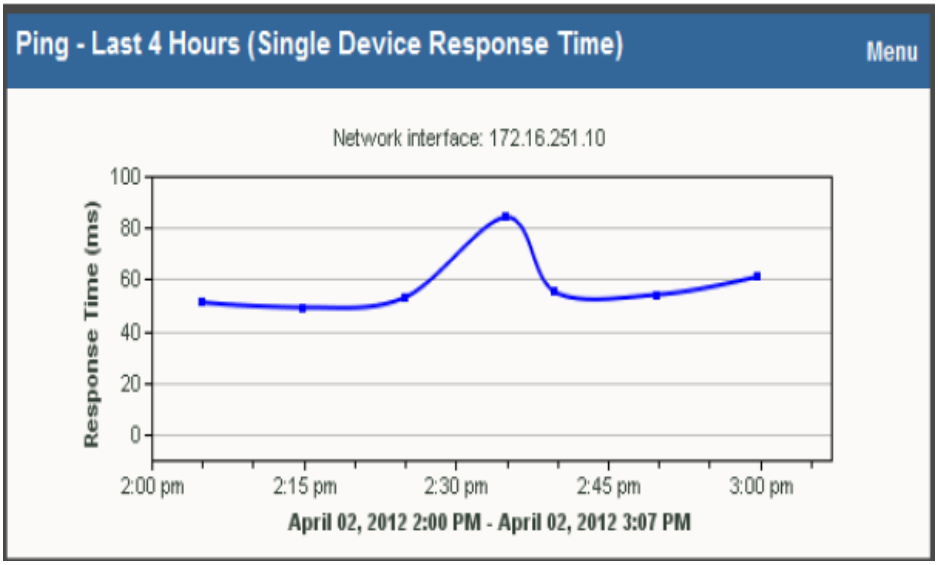


Figura a.3. 10. Figura Respuesta Ping.

Router de Centros de cómputo.

En las próximas gráficas podremos darnos cuenta, que los reportes emitidos por el WhatsUp son mayores, esto es debido a que se tuvo acceso a este router, para activar el servicio SNMP. A continuación la figura a.3.11, nos muestra el reporte del Router de Centros de Cómputo.

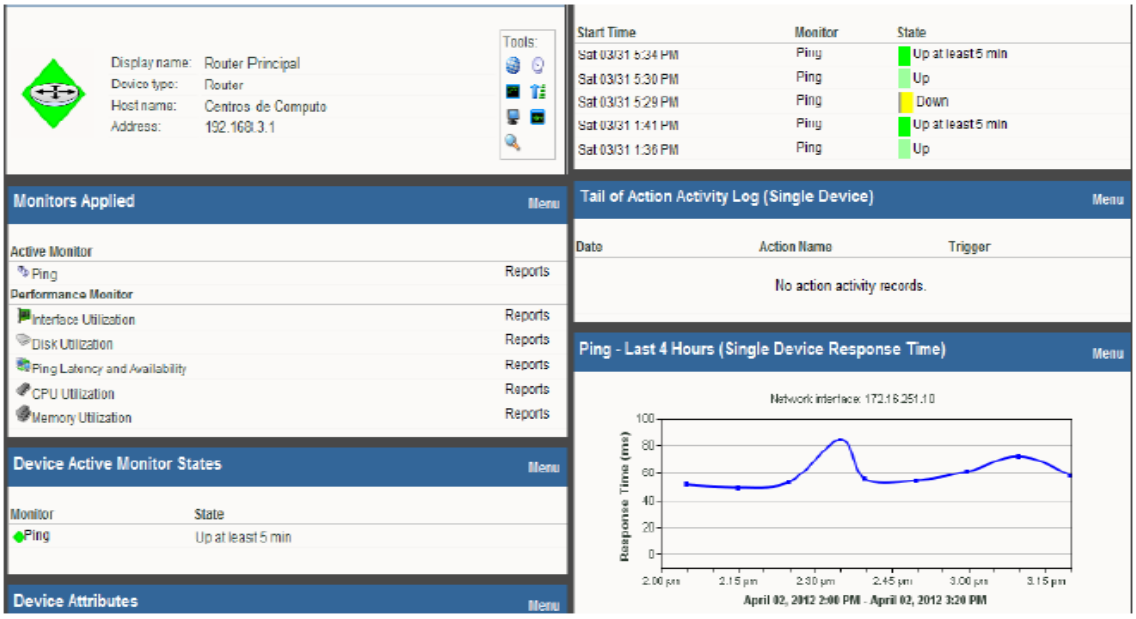


Figura a.3. 11. Reporte del Router de centros de Cómputo.

Además de estos datos también nos muestra la utilización del CPU, así como la utilización de memoria con sus respectivas particiones y el porcentaje de utilización de las interfaces del router.

Servidores.

El CUP cuenta con 2 servidores:

- Servidor de antivirus.
- Servidor de monitoreo.

Es importante mencionar que al servidor de antivirus solamente se le puede monitorear el ping, dicho resultado se muestra en la figura a.3.12. No se cuenta con la contraseña para activar el servicio SNMP, que es indispensable para el monitoreo de los demás parámetros, razón por la cual es el único parámetro presentado por el sistema de monitoreo.

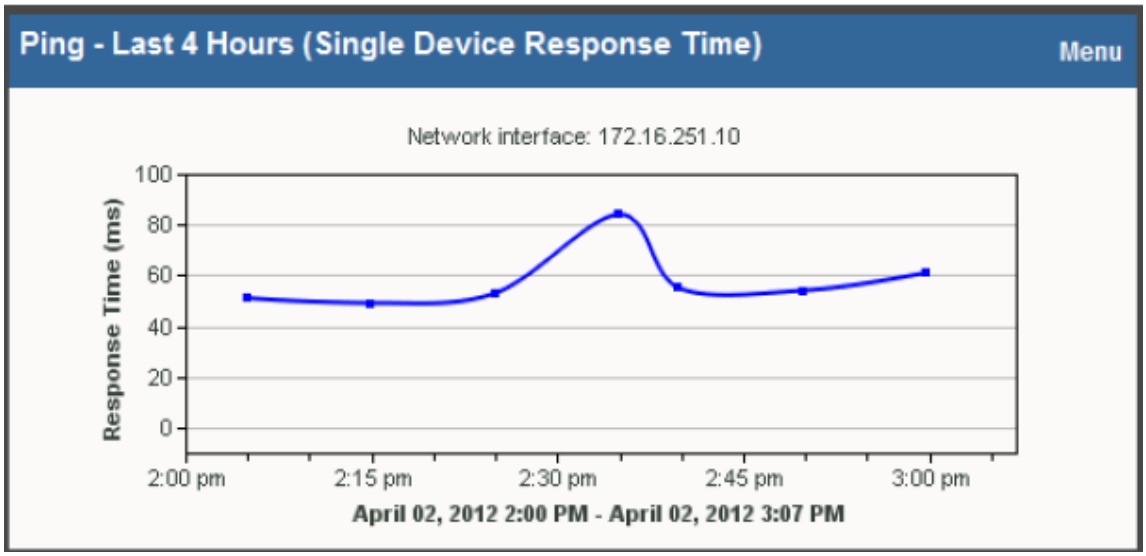


Figura a.3. 12. Respuesta Ping.

Servidor de Monitoreo.

La figura a.3.13 presenta los resultados del monitoreo, correspondiente al servidor de monitoreo, en el que se puede apreciar el uso de CPU, el uso de los discos, y la utilización de la memoria Física y virtual.

Servidor de Antivirus.

No se presentan gráficas del servidor de antivirus, debido a que no cuenta con el permiso para acceder a esta máquina y activar el servicio SNMP.

Access Point.

En figura a.3.14, se puede observar respuesta de actividad del dispositivo, es decir el ping de respuesta, no se muestran más datos debido a este dispositivo no soporta el servicio SNMP.

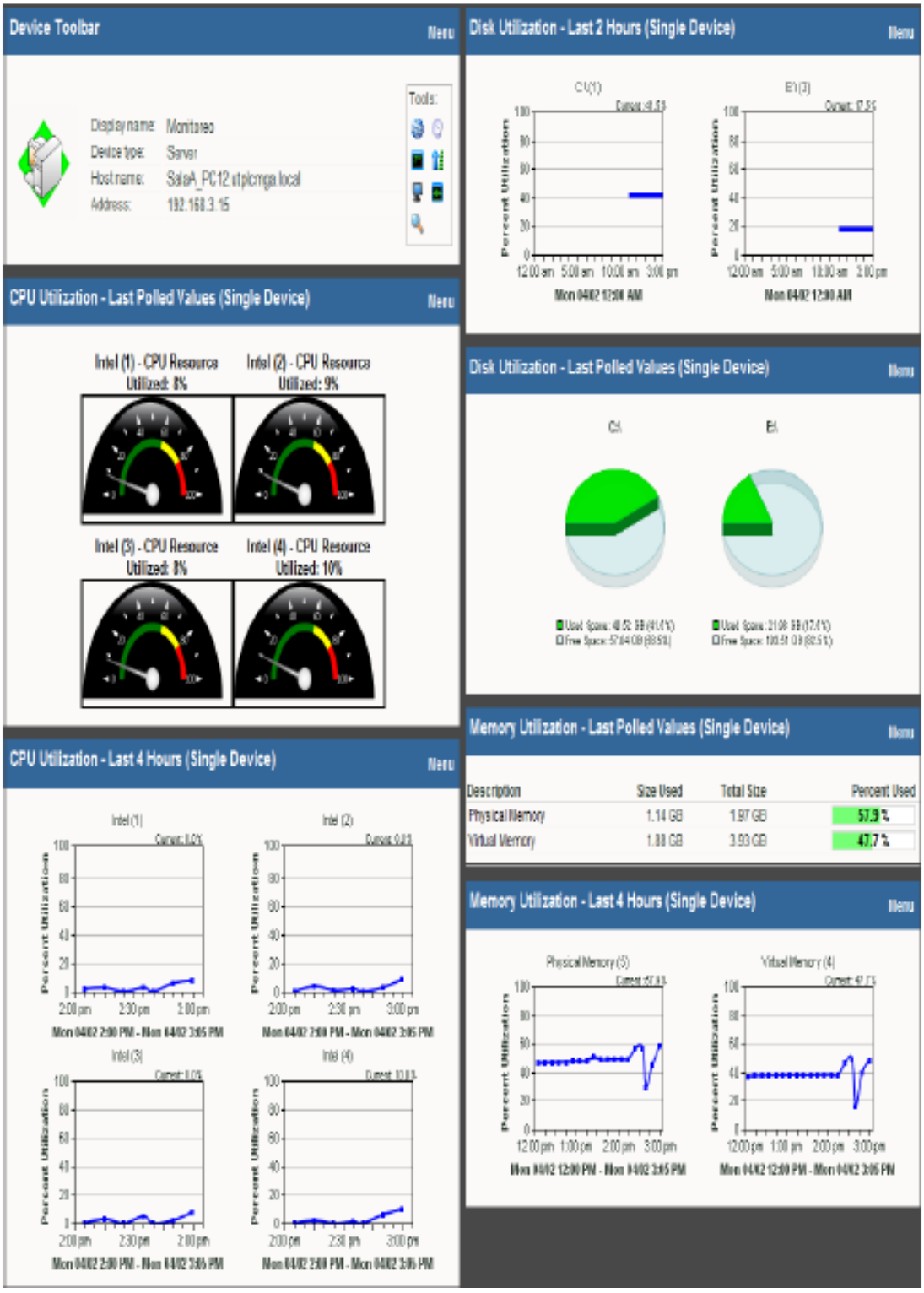


Figura a.3. 13. Informe del Servidor de Monitoreo.

Figura a.3. 14. Monitoreo del Access Point.

A.3.3.6.2. Monitoreo con el Cacti.

Con el Sistema de Monitoreo Cacti, solamente se monitoreará el Router Principal, cuyo nombre corresponde al Router de Centros de Cómputo. El Router de Administración no se puede monitorear ya que no se cuenta con el acceso para configurar el Servicio SNMP, y puesto que en el monitoreo con el WhatsUp, ya nos muestra el ping, razón por la cual ya no es necesario volver a monitorearlo, para obtener la misma respuesta.

Una vez Configurado el Cacti, los reportes que nos muestra del Router 192.168.3.1, se muestran en la figura a.3.15 y a.3.16. Cacti, permite mostrar mucha más información, en las siguientes figuras se muestran, la memoria usada, la respuesta del ping, la carga de procesos y

el tráfico de cada interfaz del router. Esta información corresponde al Router de Salas de Cómputo.

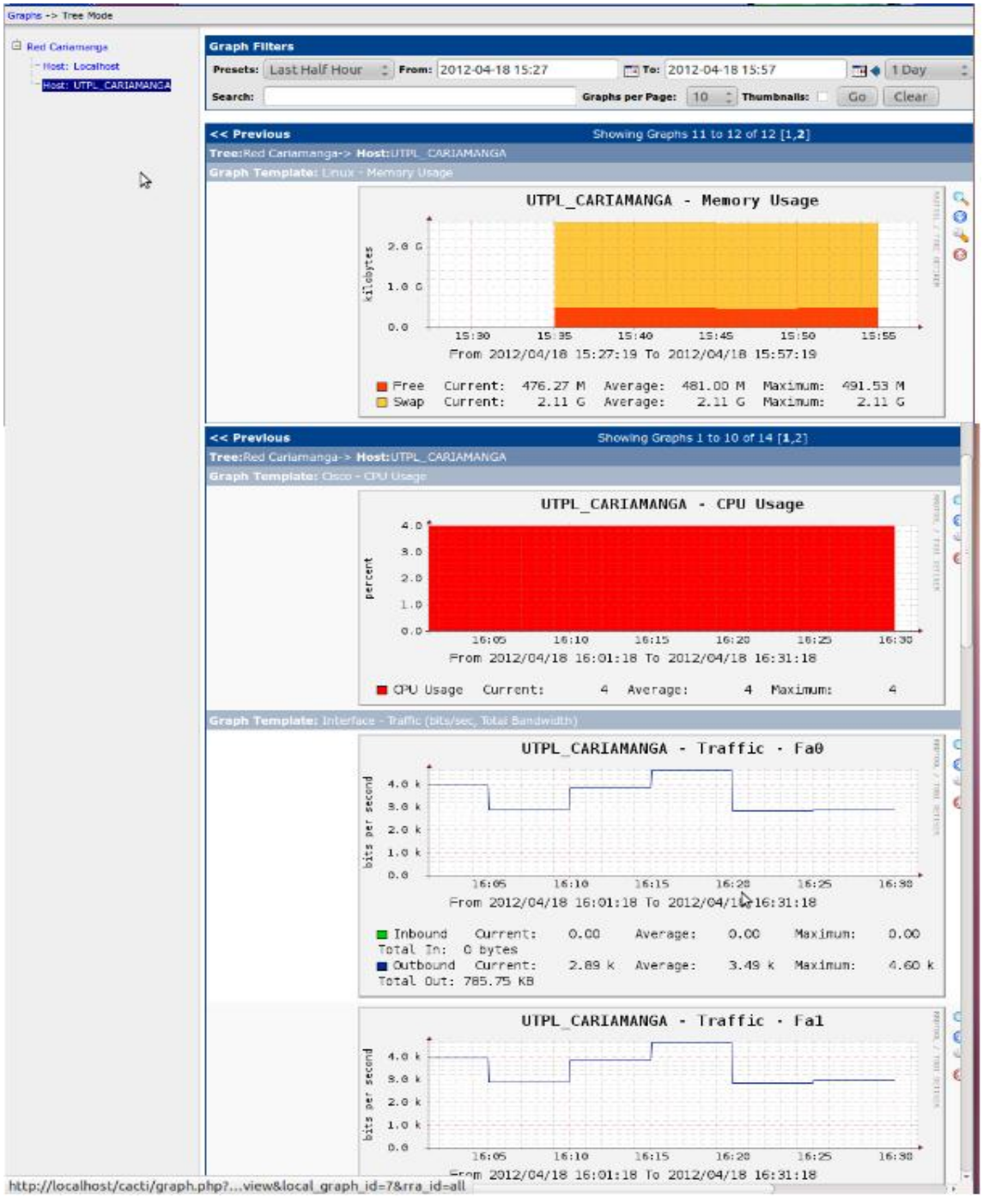


Figura a.3. 15. Memoria usada, carga, respuesta del ping y el porcentaje de procesos.

Figura a.3. 16. Tráfico de las Interfaces del Router.

Con toda esta información brindada, por el Sistema de monitoreo Cacti, podemos darnos cuenta con facilidad, cuando se utiliza mayor ancho de banda, en un determinado tiempo, así como las caídas de la red. Toda esta información corresponde a las interfaces que posee el router monitoreado.

A.3.3.7. Algunas soluciones para resolver fallas en la red.

Luego de haber visto los reportes de los equipos de red monitoreados y dadas las alarmas que se envían cuando se suscita un problema, se ha visto la necesidad de presentar algunas alternativas de solución, mismas que se mencionan a continuación.

- Cuando la utilización de la memoria de los servidores superen el 70 % de su capacidad, se deben analizar los procesos que corren en el servidor, para determinar cuáles realmente son necesarios y cuales solamente están consumiendo recursos, para que aquellos que no están siendo utilizados o no son indispensable se los elimine o en su defecto detenerlos para disminuir, la carga de utilización de la memoria.

Otra alternativa ante este problema sería ampliar la memoria RAM.

- Cuando la utilización del disco duro supera el 85% de su capacidad. Se recomienda añadir un disco duro de más capacidad que el que posee en la actualidad, o un disco secundario. Otra alternativa sería sacar respaldo, de los datos que contiene el disco, en un disco duro externo, con la finalidad de que el disco duro en uso siempre tenga el espacio suficiente, para almacenar.

Realizar procesos comunes, como eliminar archivos temporales.

- Perdida de conectividad de los equipos de red. Para tratar de dar solución al problema, se debe comprobar los cables que corresponden a la conexión final, los conectores bien ponchados, realizar un tester al cable, ya que algunas fallas suelen presentarse a nivel de la capa física.

  Realizar pruebas de conectividad, como ping, tracert o traceroute o un get manual del agente snmp si se diera el caso.

  Verificar si no han existido cambios en el direccionamiento IP de un determinado dispositivo.

- Cuando la falla se presenta se debe tratar de aislar el problema para que el resto de la red no se vea afectada, no se debe olvidar de documentar el problema y la solución de forma detallada, para ello se recomienda utilizar el formato propuesto para el informe de fallas.

- Una recomendación importante para evitar fallas, es el realizar el mantenimiento periódico de los equipos de red.

- Si el ancho de banda utilizado, es casi igual al ancho de banda contratado, todos los días, es momento de contratar mayor ancho de banda, ya que los requerimientos sobrepasan el ancho de banda disponible.

Anexo 4

A.4.1. Configuración del Agente SNMP en Windows 7.

Indicamos la configuración del servicio SNMP en Windows 7, debido a que un servidor de monitoreo tiene instalado este sistema operativo.

1. Dentro del Panel de Control, nos ubicamos en programas, una vez ahí ingresamos en programas y características, en donde damos un click en activar o desactivar las características de Windows.

2. Nuevamente nos ubicamos en panel de control y buscamos servicios locales, observémoslo claramente en la figura a.4.1.

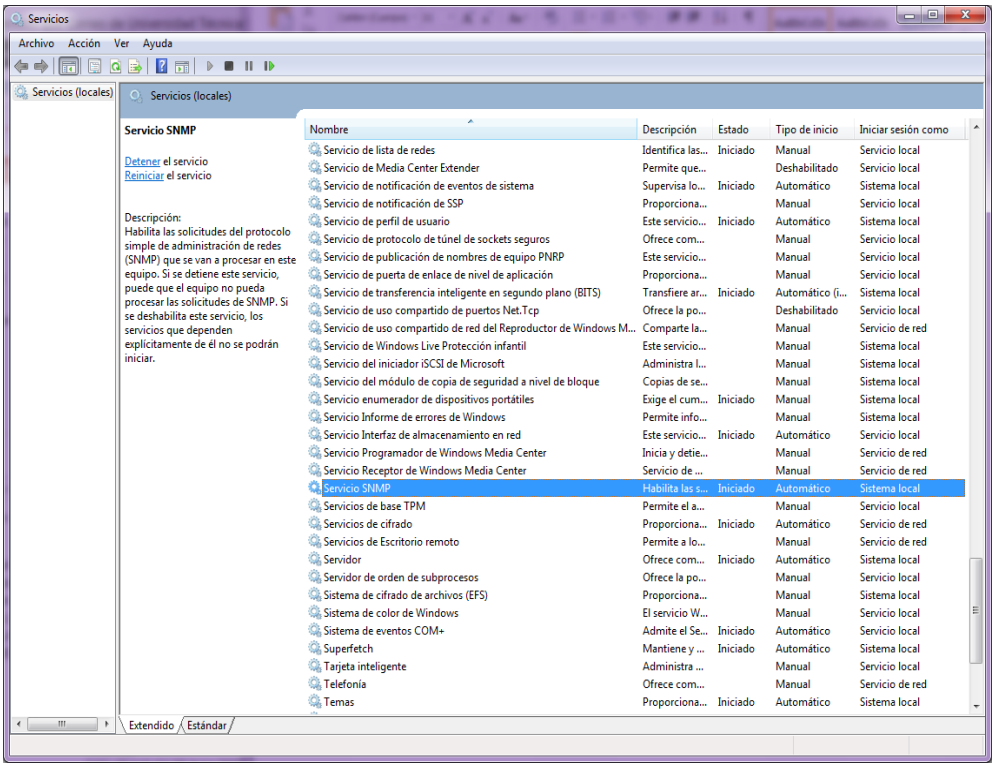


Figura a.4. 1. Iniciar el Servicio SNMP.

3. Nos ubicarnos en Servicios de SNMP, damos en click derecho para reiniciar el servicio y nuevamente damos click derecho en propiedades, y nos ubicamos en la pestaña de seguridad. Las propiedades del servicio SNMP los podemos observar en la figura a.4.2.

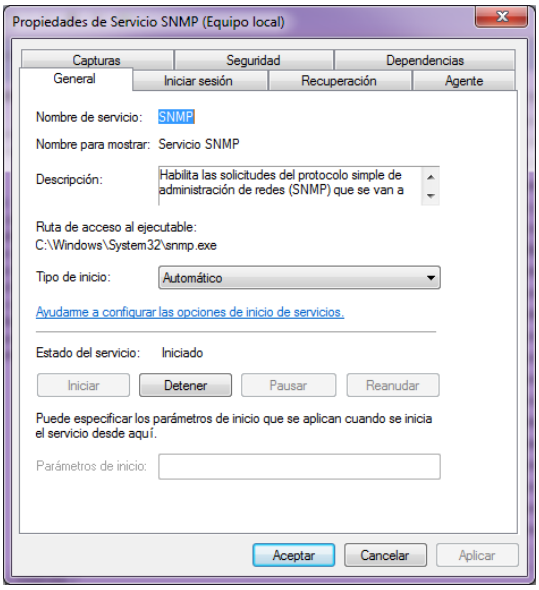


Figura a.4. 2. Propiedades de Servicio SNMP.

4. Una vez ubicados en esta pestaña, damos click en agregar, tal y como lo vemos en la figura a.4.3.

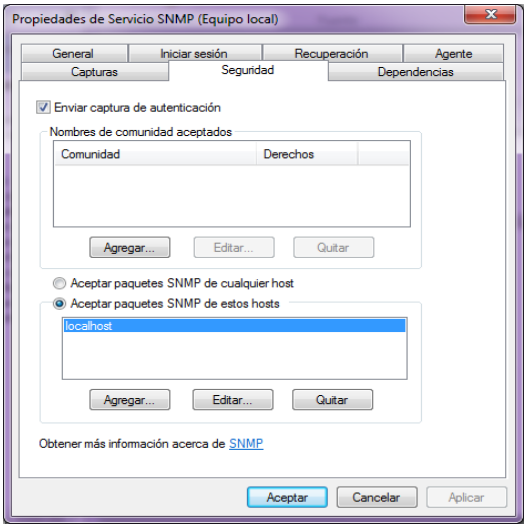


Figura a.4. 3. Agregar localhost.

5. Seleccionamos la opción de lectura y escritura y el nombre de la comunidad, tal como se muestra en la figura a.4.4.

Figura a.4. 4. Configuración del servicio SNMP.

6. Luego en la ventana activamos “Aceptar paquetes SNMP de cualquier host” y aplicar.

7. Ahora dentro de la misma ventana nos ubicamos en la pestaña Capturas, en donde debemos escribir el nombre de la comunidad y agregamos a la lista, en la misma ventana en la parte inferior en destino de capturas, damos click en agregar, y se coloca la dirección IP del servidor de monitoreo, tal como podemos apreciar en la figura a.4.5.

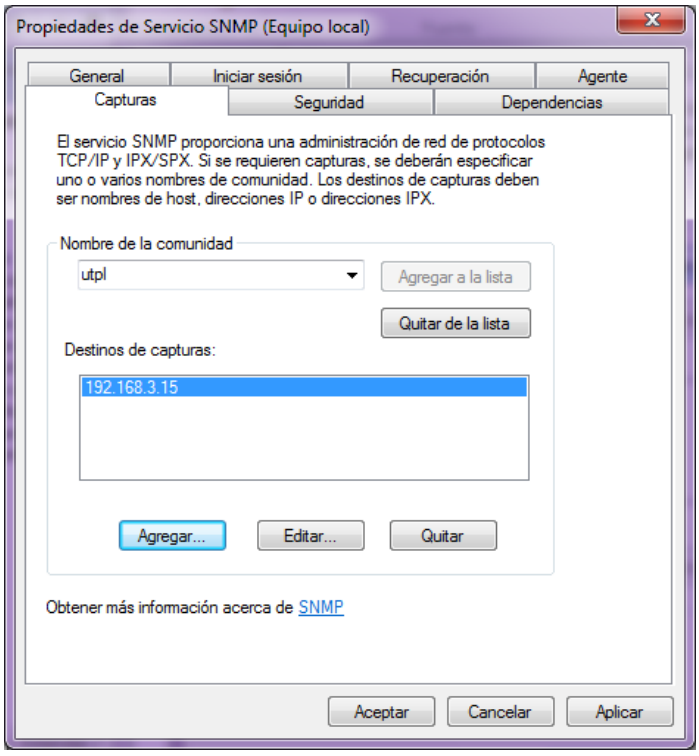


Figura a.4. 5. Configurando Propiedades de SNMP.

8. Damos click en aplicar y aceptar, finalmente reiniciamos el servicio SNMP.

A.4.2. Configuración del Agente SNMP en Ubuntu-Linux.

Para instalar SNMP en Linux, debemos seguir los siguientes comandos.

#apt-get install snmpd

Luego se debe quitar la dirección de loopback del archivo **/etc/default/snmpd,** para que el servidor de monitoreo pueda monitorear otros equipos de la red.

Una vez que hemos seguido los pasos anteriores, debemos crear la comunidad, para esto editamos el siguiente archivo.

A.4.3. Configuración de SNMP en Routers Cisco.

Habilitar y configurar la generación de traps SNMP

Router(config)# snmp-server enable traps

Definir el nombre de la comunidad

Router(config)# snmp-server comunity (nombre de la comunidad) [view nombre-vista] [ro|rw]

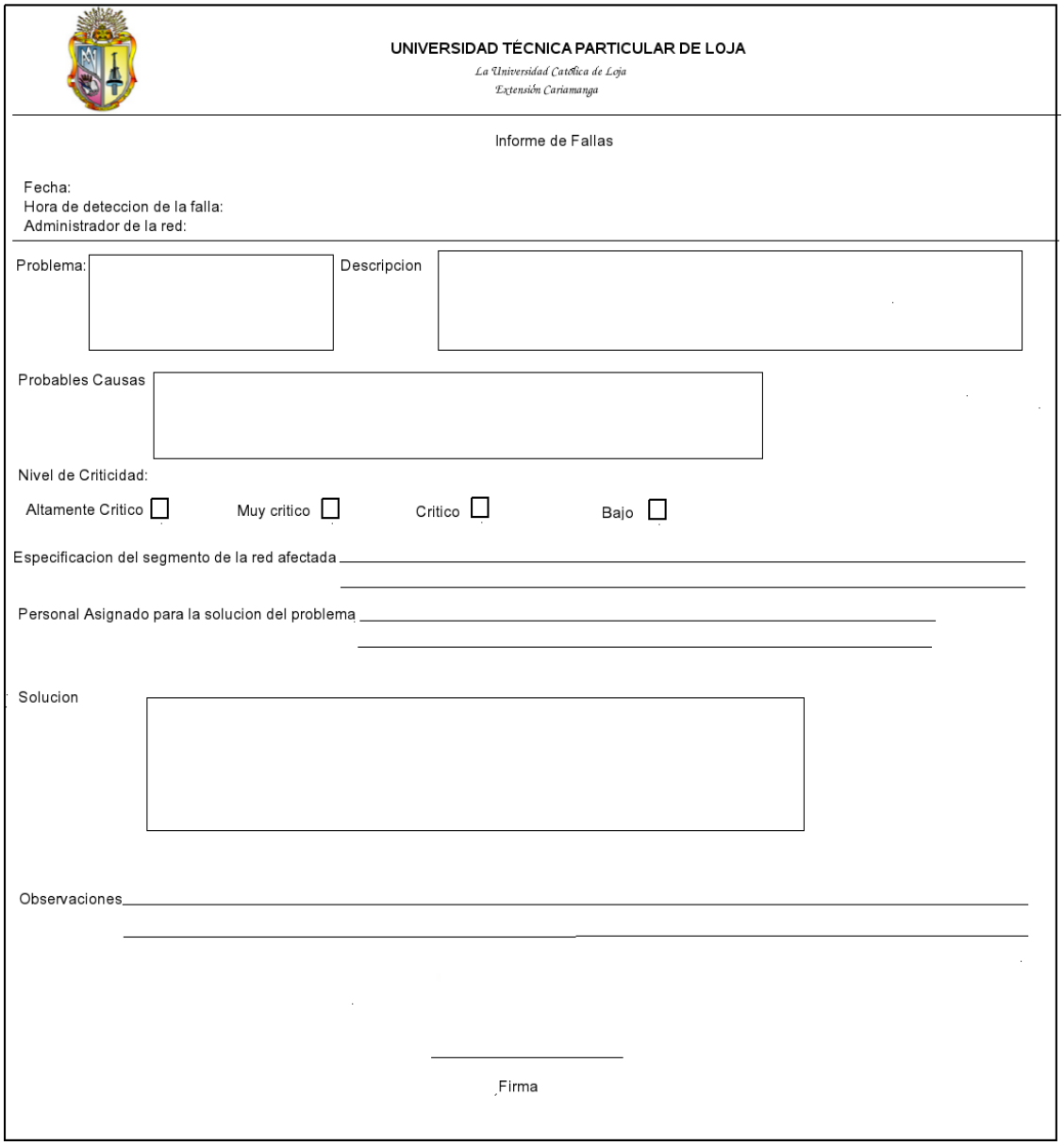
Así mismo se debe dar a la comunidad los permisos de lectura y escritura, con la finalidad de tener un mayor control sobre el equipo

Router(config)# snmp-server comunity (nombre de la comunidad) rw

Anexo 5.

A.5.1. Informe de Fallas.

Luego de haber identificado y solucionado un problema, es importante registrarlo, con la finalidad de tenerlo como respaldo y ayuda por si volviese a darse el mismo problema. La plantilla propuesta para el Informe de Fallas se muestra en la figura a.5.1. que viene a continuación.



UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

Extensión Cariamanga

Informe de Fallas

Fecha:
Hora de deteccion de la falla:
Administrador de la red:

Problema: Descripcion

Probables Causas

Nivel de Criticidad:

Altamente Critico ☐ Muy critico ☐ Critico ☐ Bajo ☐

Especificacion del segmento de la red afectada

Personal Asignado para la solucion del problema

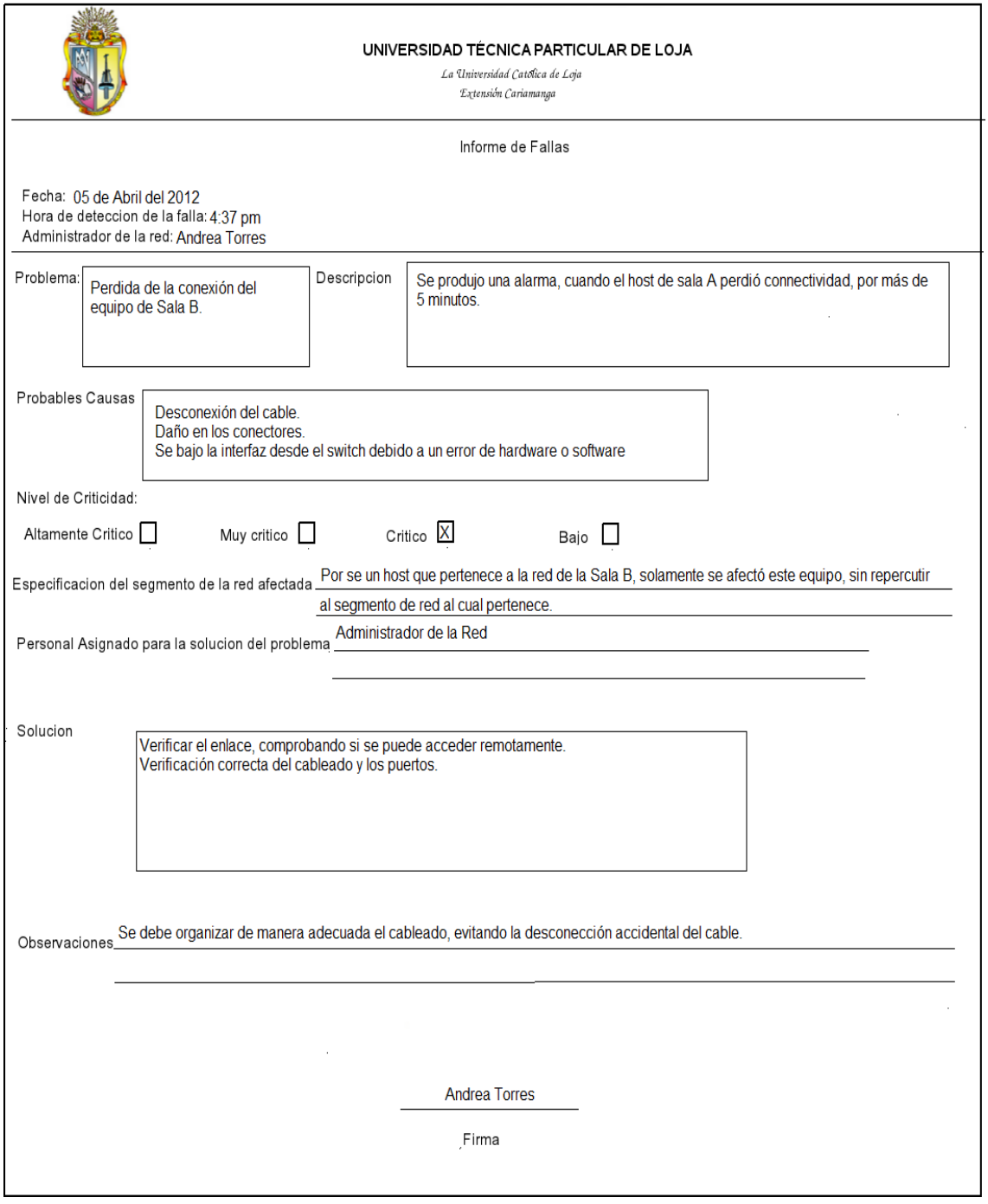
Solucion

Observaciones

Firma

Figura a.5. 1. Plantilla para la documentación de las Fallas.

Informe de fallas, ante la de caída de interfaces que se realizó en la red de datos del CUP (descrita anteriormente). Dicho informe se muestra figura a.5.2.



UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

Extensión Cariamanga

Informe de Fallas

Fecha: 05 de Abril del 2012
Hora de deteccion de la falla: 4:37 pm
Administrador de la red: Andrea Torres

Problema: Perdida de la conexión del equipo de Sala B.

Descripcion: Se produjo una alarma, cuando el host de sala A perdió connectividad, por más de 5 minutos.

Probables Causas:
Desconexión del cable.
Daño en los conectores.
Se bajo la interfaz desde el switch debido a un error de hardware o software

Nivel de Criticidad:

Altamente Critico [ ] Muy critico [ ] Critico [X] Bajo [ ]

Especificacion del segmento de la red afectada: Por se un host que pertenece a la red de la Sala B, solamente se afectó este equipo, sin repercutir al segmento de red al cual pertenece.

Personal Asignado para la solucion del problema: Administrador de la Red

Solucion:
Verificar el enlace, comprobando si se puede acceder remotamente.
Verificación correcta del cableado y los puertos.

Observaciones: Se debe organizar de manera adecuada el cableado, evitando la desconección accidental del cable.

Andrea Torres

Firma

Figura a.5. 2. Informe de falla de la prueba realizada.

Anexo 6.

A.6.1. Instalación y Configuración de los sistemas de Monitoreo.

A.6.1.1. Proceso de Configuración de WhatsUp.

La figura a.6.1, nos muestra la ventana principal del sistema donde se nos permite iniciar la identificación de los componentes de la red, a los cuales se puede se les puede hacer ping.

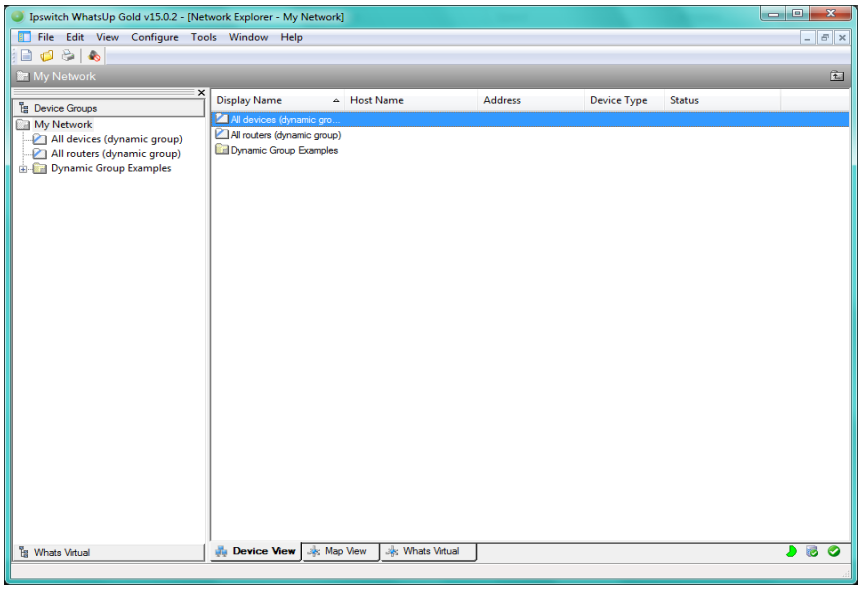


Figura a.6. 1. Ventana Principal de WhatsUp.

Una vez que ya nos encontramos en la ventana principal, procedemos a crear la topología de red, agregando los dispositivos de nuestra red que van a ser monitoreados. La figura a.6.2. nos muestra, como fueron creados los dispositivos de la red de datos del CUP.

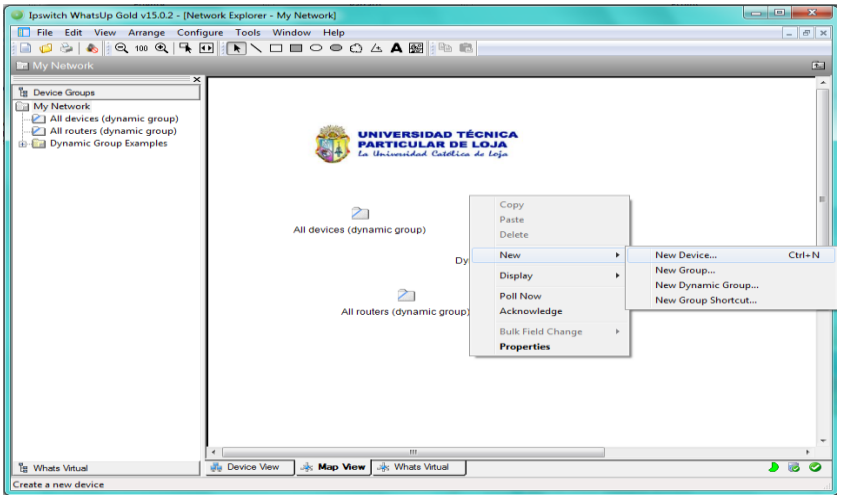


Figura a.6. 2. Agregar nuevo dispositivo.

Una vez que se ha elegido nuevo dispositivo se debe ingresar la IP correcta, WhatsUp antes de agregar un dispositivo realiza el escaneo de la red para identificarlo y luego agraegarlo,para ello dicho dispositivo debe estar encendido, cuando el dispositivo es encontrado se presenta las siguientes ventanas, como se muestra en la figura a.6.3.

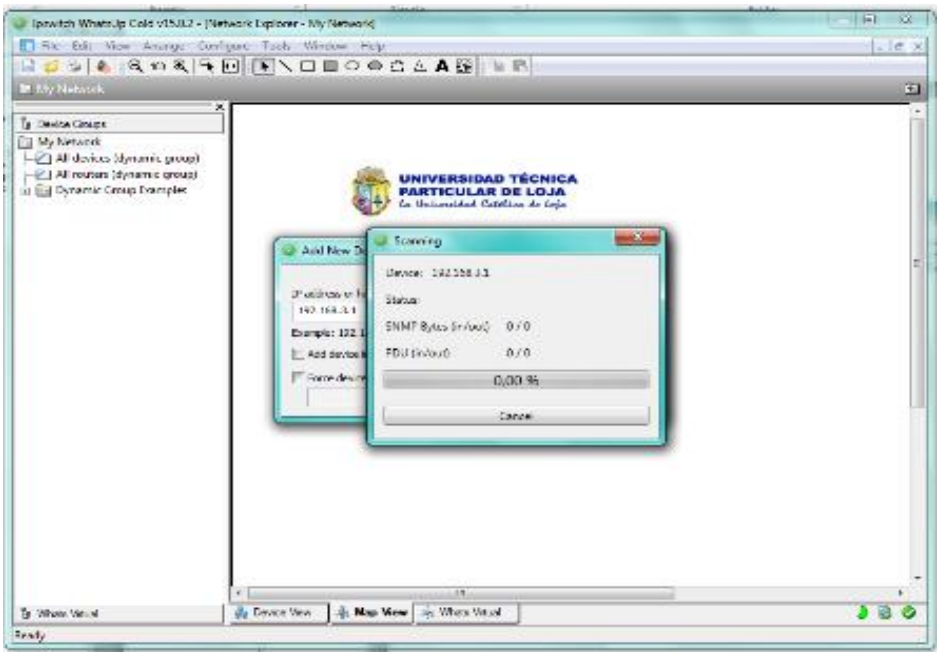


Figura a.6. 3. Escaneo del dispositivo a agregar.

Si el dispositivo que se quiere agregar no se encuentra encendido, no será localizable para WhastUp, razón por la cual no será posible agregarlo, cuando esto sucede se muestra un mensaje como el que podemos ver en la figura a.6.4.

Si desconocemos la dirección IP de los equipos que se encuentran en la red se puede realizar el escaneo, en donde nos pide que pongamos el rango de direcciones IP a buscar, una vez que que WhatsUp nos muestre las direcciones IP de los equipos que se encuentran activos en ese momento, podremos agregarlos sin ningún problema.

Si el dispositivo está en red, es decir encendido, directamente se presenta una ventana en donde se debe agregar algunos datos tal como se muestra en la figura a.6.5.

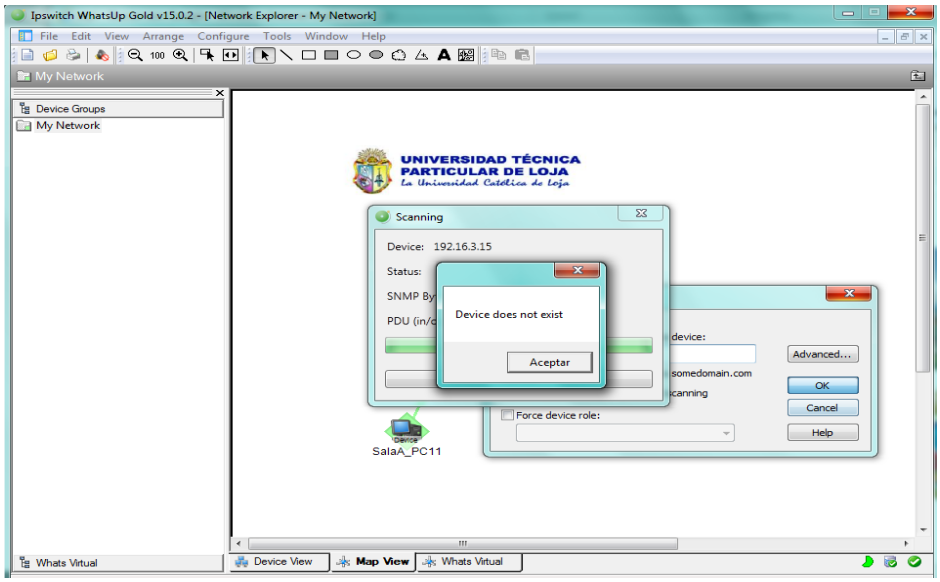


Figura a.6. 4. Dispositivo no existe.

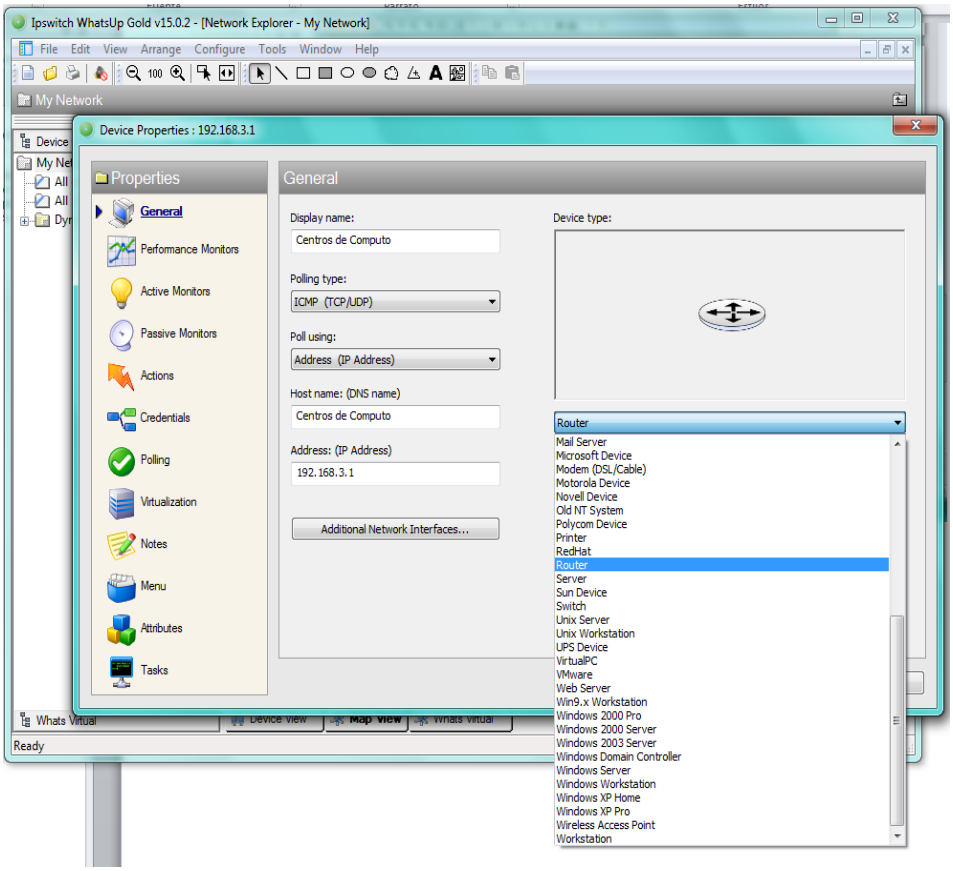


Figura a.6. 5. . Datos del dispositivo.

Una vez agregado el dispositivo se debe conectar al siguiente dispositivo al cual que se encuentra directamente conectado, como se muestra en la figura a.6.6.

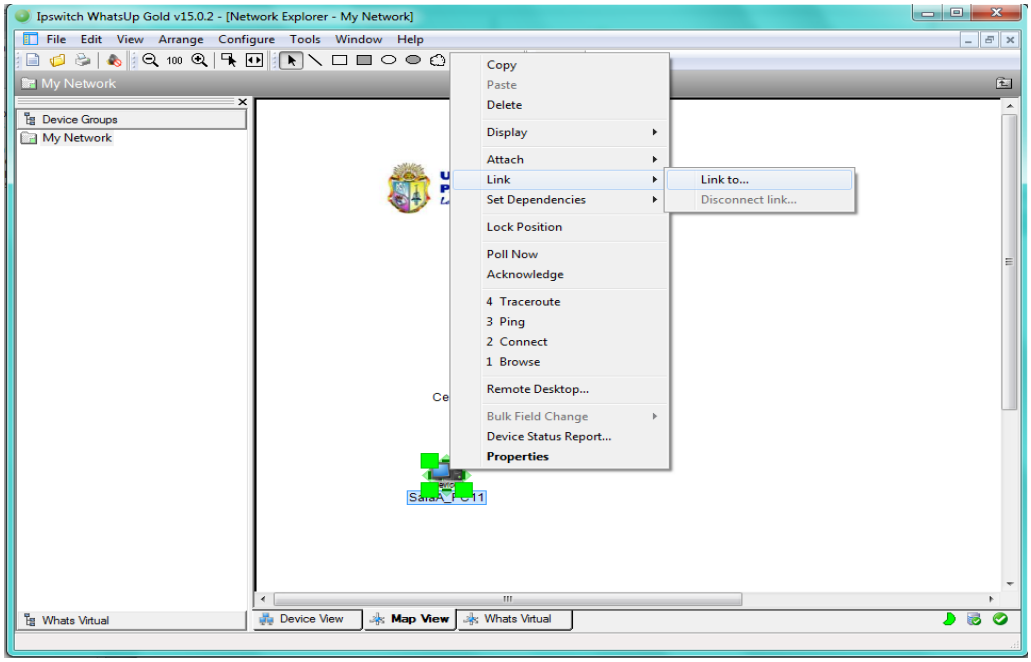


Figura a.6. 6. Conectar dispositivos.

Una vez creada toda la red a monitorear se procede a configurar los dispositivos, para obtener los datos que requerimos conocer y por ende monitorear continuamente.

El primer dato a monitorear debe ser el reporte de ping, comprobando de esta manera la conectividad. Para ello hacemos doble click en el dispositivo, y nos ubicamos en las propiedades, específicamente en la pestaña Performance Monitors, en donde se elige está opción a ser monitoreada, así como podemos observar en la figura a.6.7.

Una vez configurada esta opción podremos obtener el reporte, con este dato solicitado.

Dado que los problemas en una red de datos siempre pueden surgir, es necesario contar con un tipo de alerta, que ayude a conocer de forma rápida, que algo ha sucedido. WhatsUp proporciona algunos tipos de alerta, y para ello debemos elegir el medio de alertar, ya sea por correo electrónico, mensajes al celular, etc. En los siguientes gráficos se muestra cómo hacerlo.

Para configurar la alertas se debe ubicar en la pestaña Actions y agregamos damos click en Add, para adherir nueva acción, tal y como podemos apreciar en la figura a.6.8.

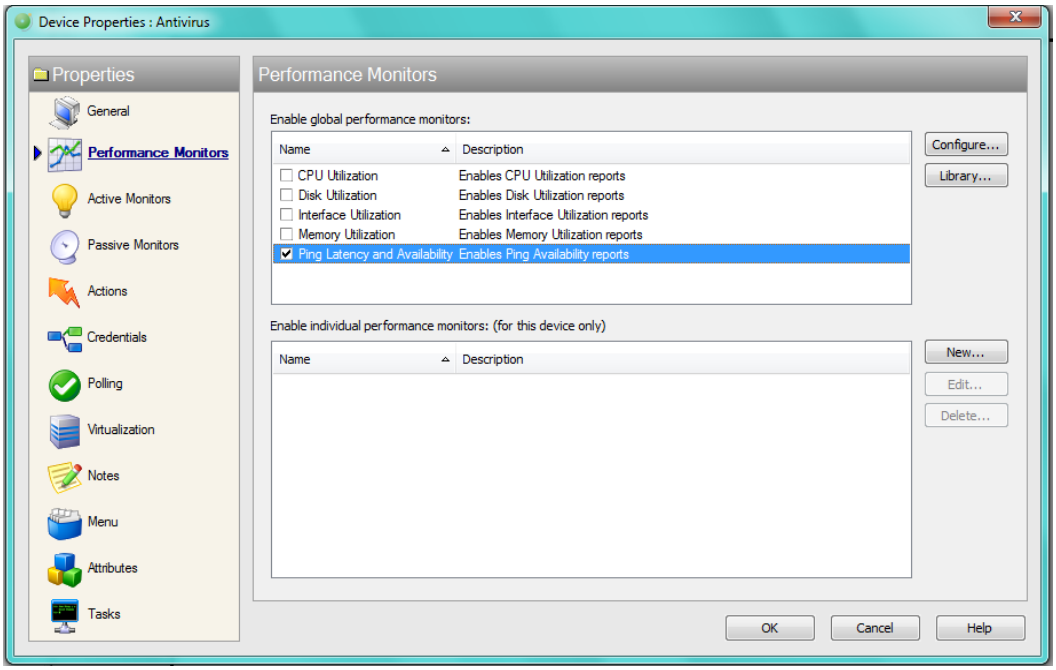


Figura a.6. 7. Ping Latency.

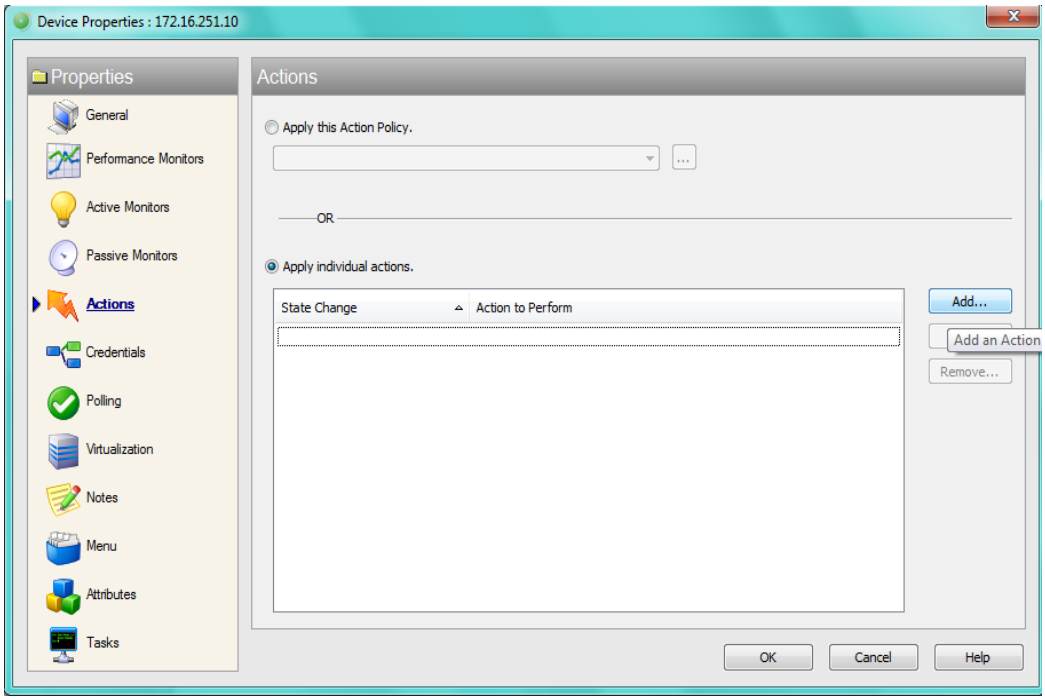


Figura a.6. 8. Agregar nueva acción.

Con lo que inmediatamente nos dice si queremos crear una nueva acción o seleccionar una desde la librería. Esta opción se la elige si es la primera vez que vamos a crear, cuando queremos agregarla a otro dispositivo ya solo debemos elegir la opción crear la acción desde la librería, este proceso se muestra en la figura a.6.9.

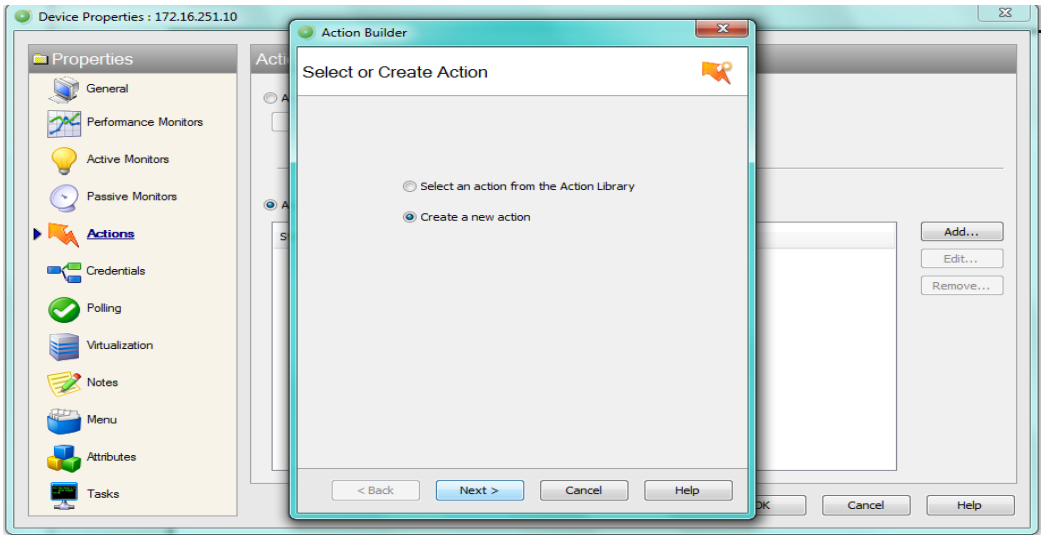


Figura a.6. 9. Crear nueva acción.

Una vez creada la acción se debe elegir el tipo de acción que se requiere crear, en nuestro caso la alarma que necesitamos se nos envíe cuando un dispositivo se apaga, es a través de correo electrónico, y para ello elegimos la opción mencionada. La selección del tipo de alarma se muestra en la figura a.6.10.

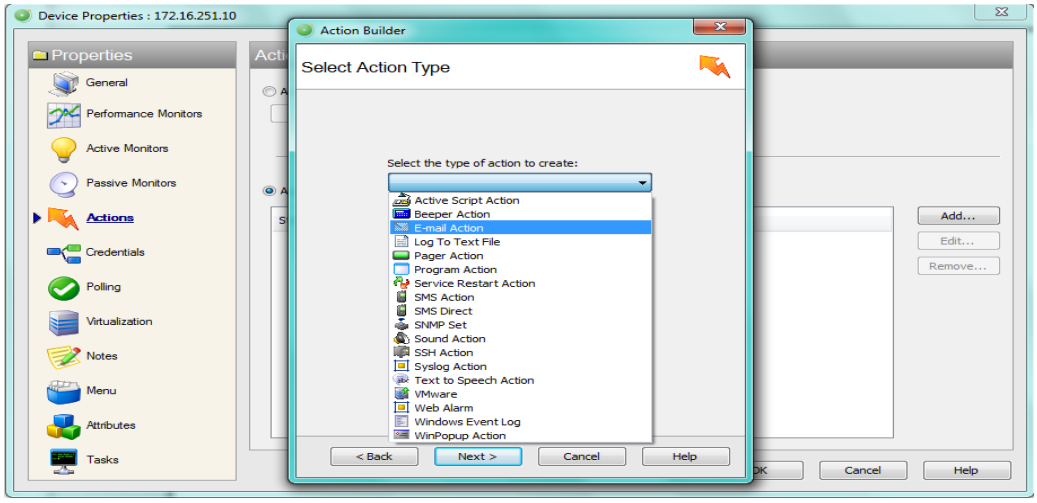


Figura a.6. 10. Seleccionar el tipo de alarma.

Una vez seleccionado el tipo de alarma, se debe ingresar los datos: el nombre de la acción, el servidor SMTP y por supuesto la dirección del correo electrónica de la persona que administra la red, para que le sean enviadas las alertas, podemos observar este proceso en la figura a.6.11.

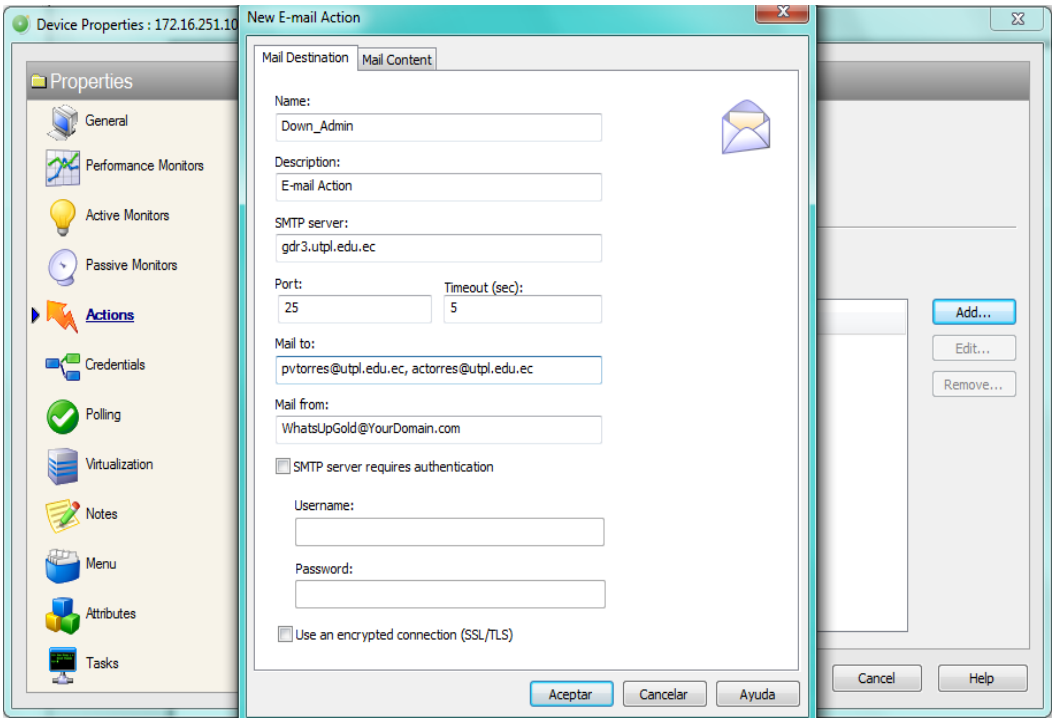


Figura a.6. 11. Agregar los datos a la acción elegida.

Luego de esto se deben crear las credenciales SNMP con la finalidad de poder recolectar más datos, para ellos nos ubicamos en las propiedades del dispositivo, en la pestaña de Credenciales, como lo apreciamos en la figura a.6.12.

Una vez elegida la opción de SNMP, WhatsUp nos arrojará una nueva ventana en donde podemos crear una nueva credencial, tal como se muestra en la figura a.6.13.

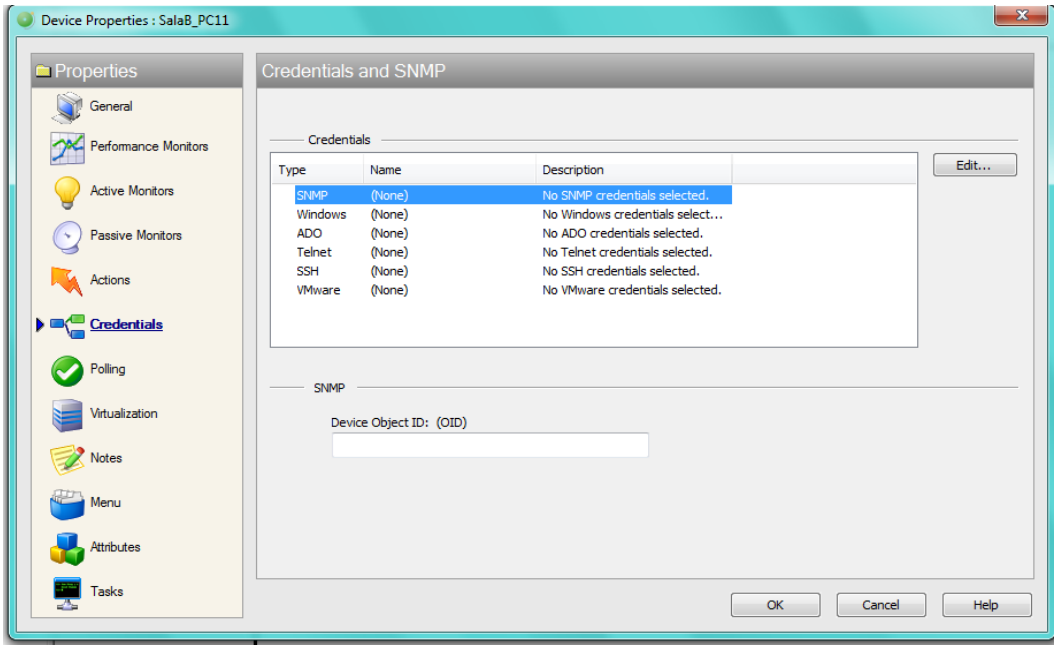


Figura a.6. 12. Credenciales.

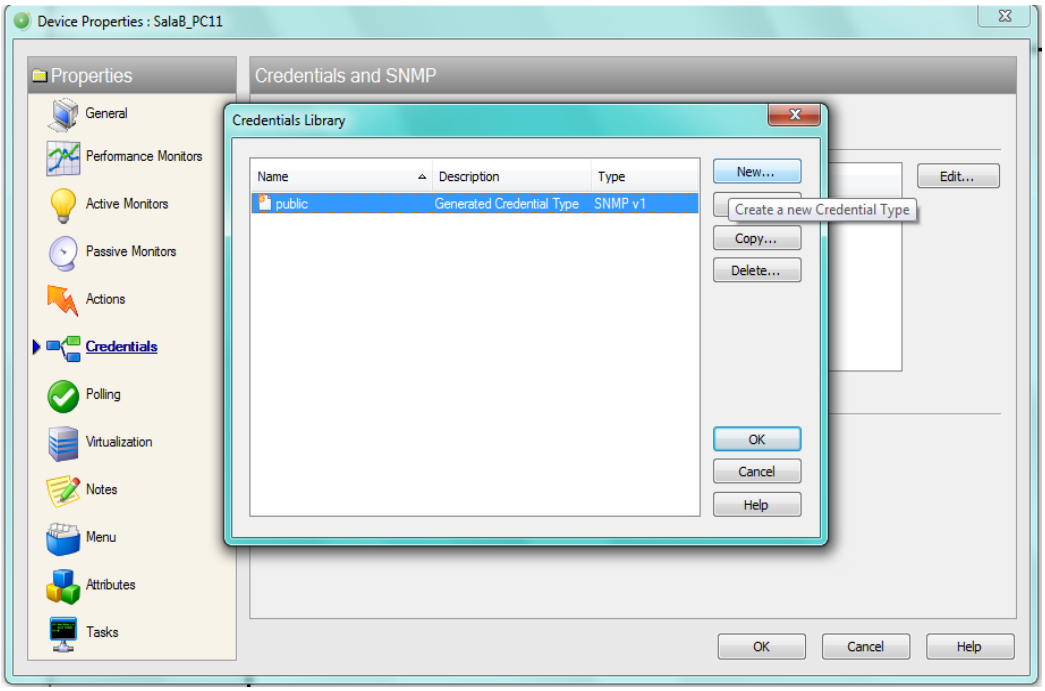


Figura a.6. 13. Crear nueva Credencial.

En este caso elegiremos la versión de la credencial SNMP v1, tal y como se demuestra en la figura a.6.14.

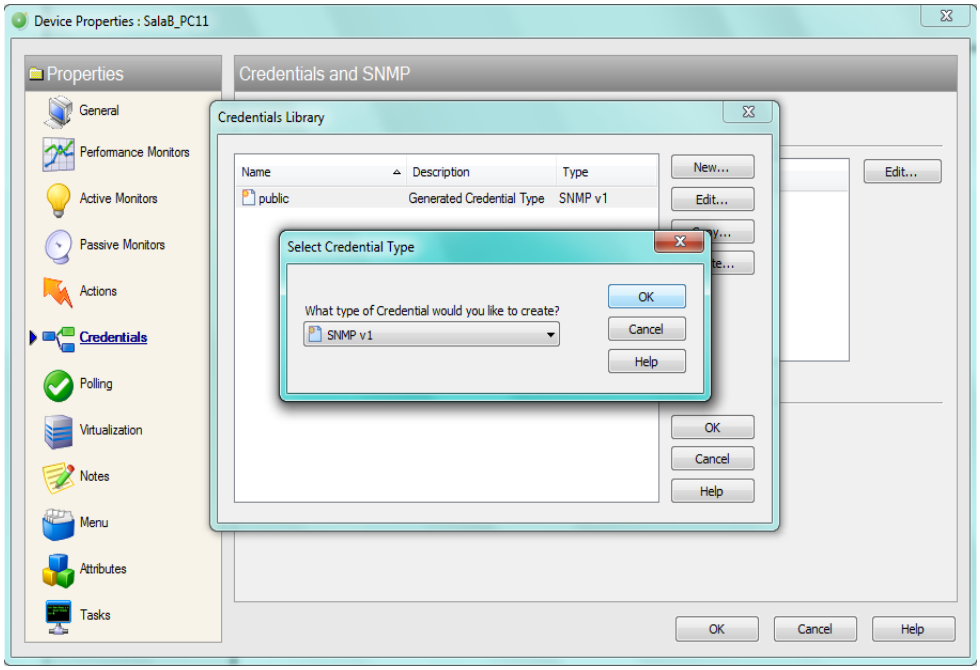


Figura a.6. 14. Elegir la versión de la credencial.

Una vez elegida la versión de la credencial, se debe escribir el nombre de la comunidad. En este caso se ha puesto como nombre de la comunidad las siglas de la institución. Como podemos apreciar en la siguiente figura a.6.15.

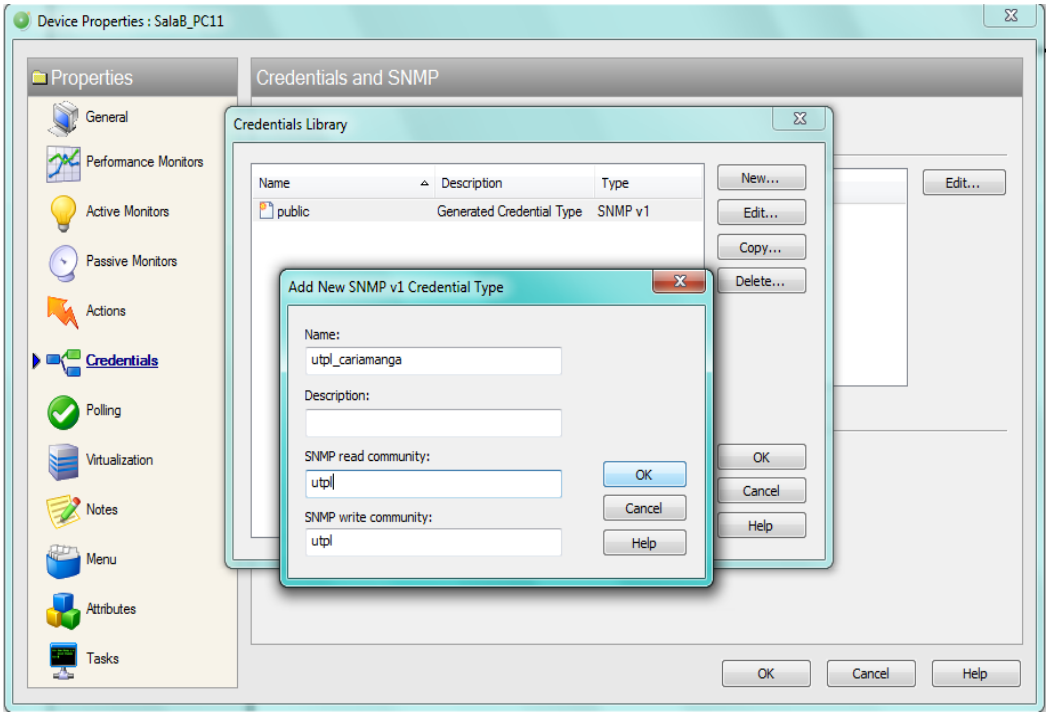


Figura a.6. 15. Identificar a la comunidad.

Una vez configurado el WhatsUp, para que nos arroje los datos requeridos, se debe habilitar el SNMP en cada uno de los equipos a ser monitoreados.

Proceso de configuración del Cacti.

Para objeto de nuestro estudio, al sistema de monitoreo Cacti, se lo instaló en Linux Ubuntu, y para ello seguimos los siguientes pasos. Cabe recalcar que para no tener problemas con el software a instalar, es necesario actualizar el Sistema con el siguiente comando:

Apt-get update

Luego ejecutamos los siguientes comandos:

sudo apt-get install tasksel

Iniciamos instalamos LAMP.

sudo apt-get install lamp-server^

Durante la instalación de LAMP, nos pedirá que le ingresemos contraseña para root mysql.

Luego ejecutamos los siguientes comandos.

sudo apt-get install php5 php5-gd php5-mysql

Ahora si iniciamos la instalación del Cacti con el siguiente comando

sudo apt-get install cacti-spine

Luego se desplegará una ventana en la que debemos elegir Apache 2.

Así mismo debemos configurar la base de datos, e ingresar una contraseña.
Una vez instalado el Cacti se debe comprobar que todas las librerías estén instaladas, para lo cual nos debemos dirigir a la pestaña Settinngs en Paths. La correcta configuración se muestra en la siguiente figura a.6.16.

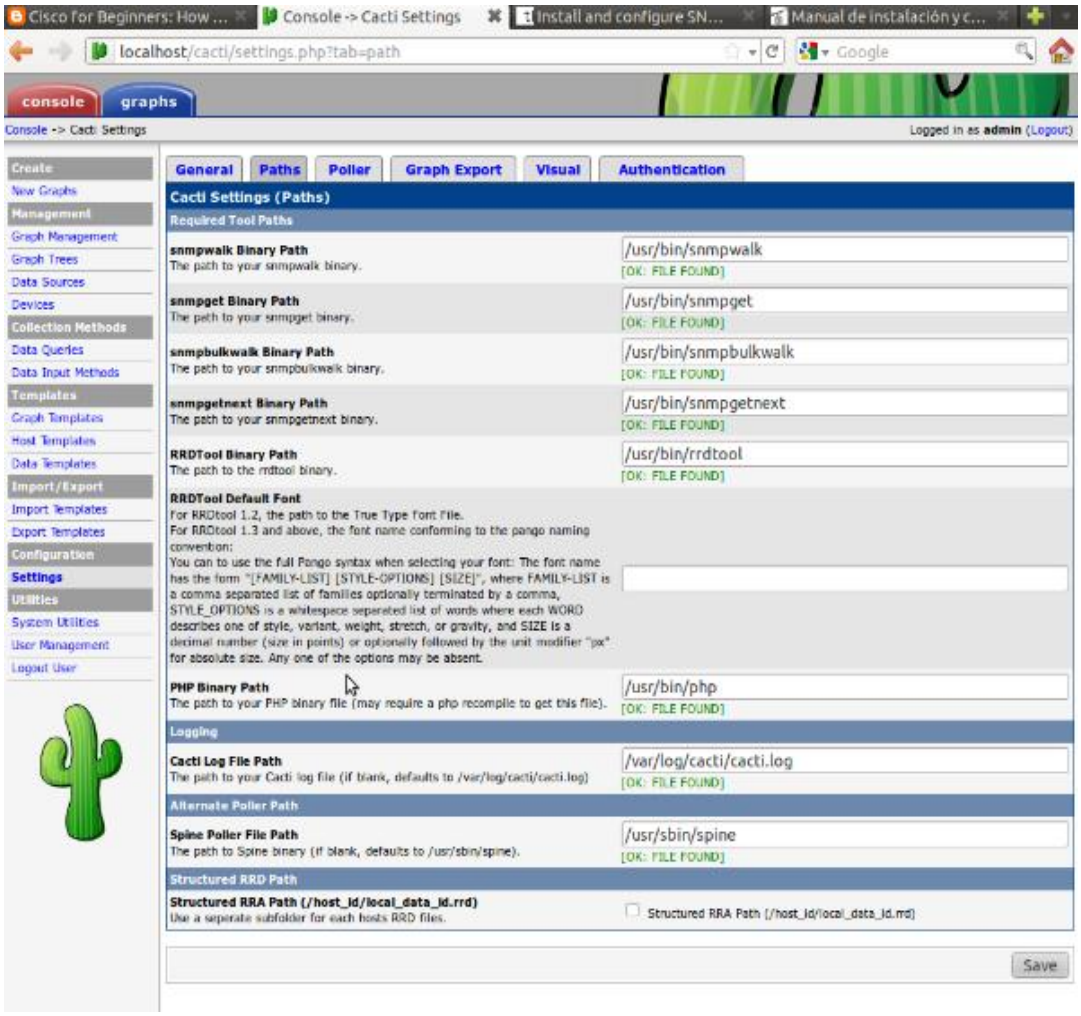


Figura a.6. 16. Settings.

Una vez verificada la ubicación de las librerías, es necesario ubicarnos en Poller y elegir el tipo de poller, en nuestro caso elegimos el spine, como se muestra en la siguiente figura a.6.17.

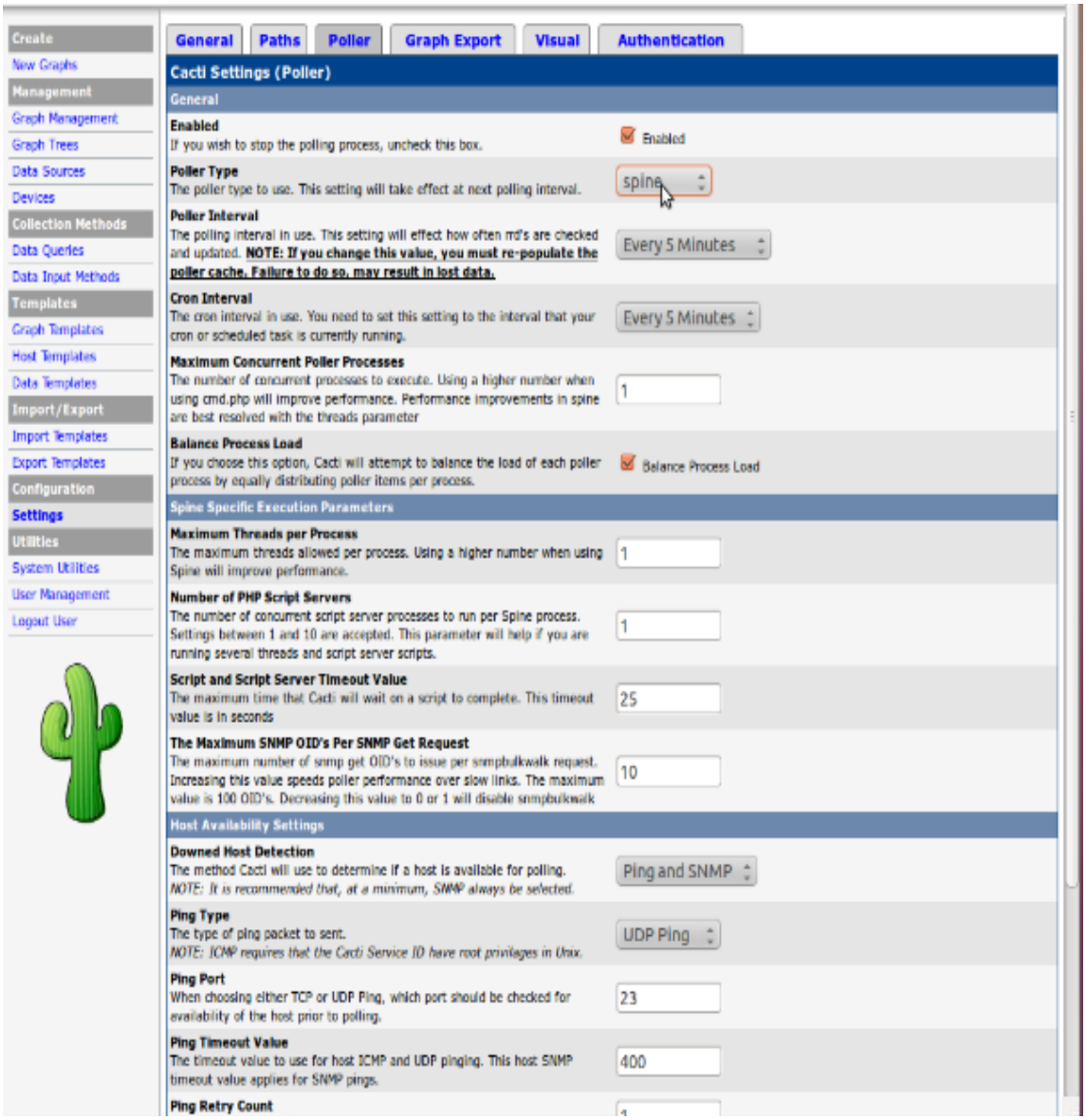


Figura a.6. 17. Elegir el Poller Spine.

Una vez realizados los pasos anteriormente expuestos se agregan los dispositivos que se requieren monitorear, en nuestro caso el router, en donde además elegimos la versión Snmp que configuramos anteriormente en el router. Una vez agregado debe presentarnos la información correspondiente, tal y como se muestra en la figura a.6.18.

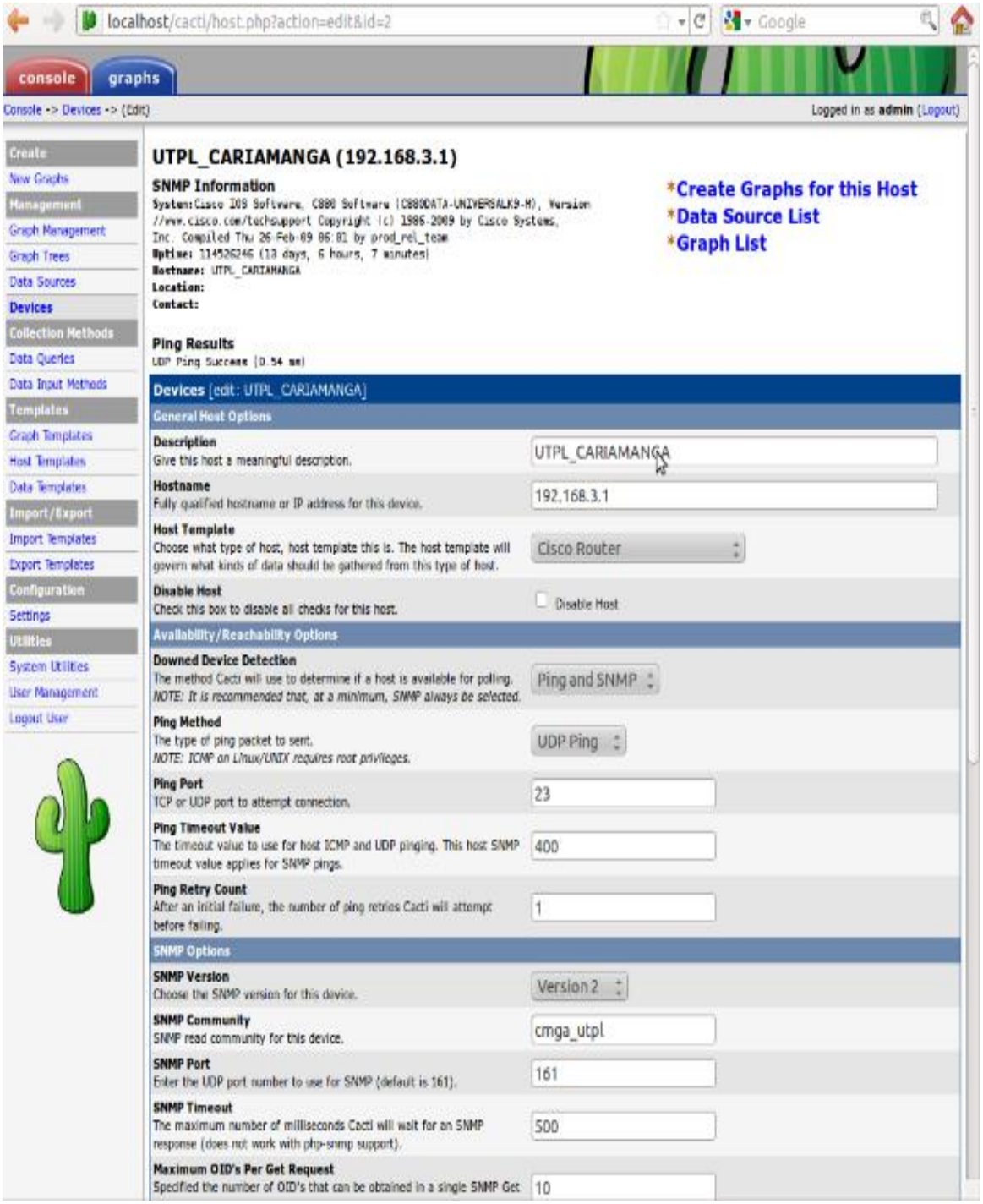


Figura a.6. 18. Información del Router Agregado.

Una vez guardada la configuración del router, podemos crear los gráficos con la información que se desea monitorear, en nuestro caso elegimos todas las interfaces del router, como se muestra en la figura a.6.19.

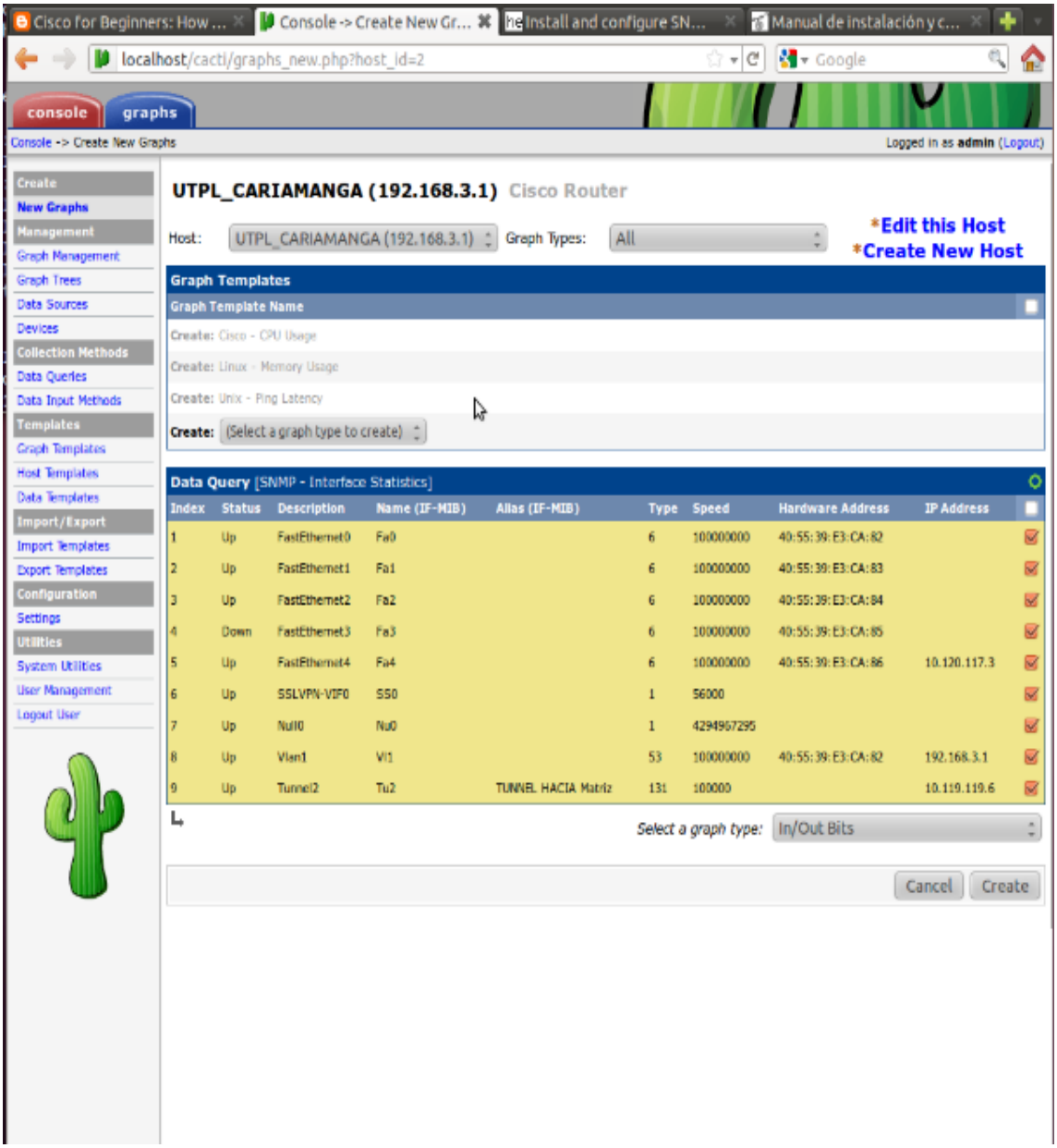


Figura a.6. 19. Creación de gráficos del Router.

La creación correcta de los gráficos nos muestra el siguiente resultado, reflejado en la figura a.6.20.

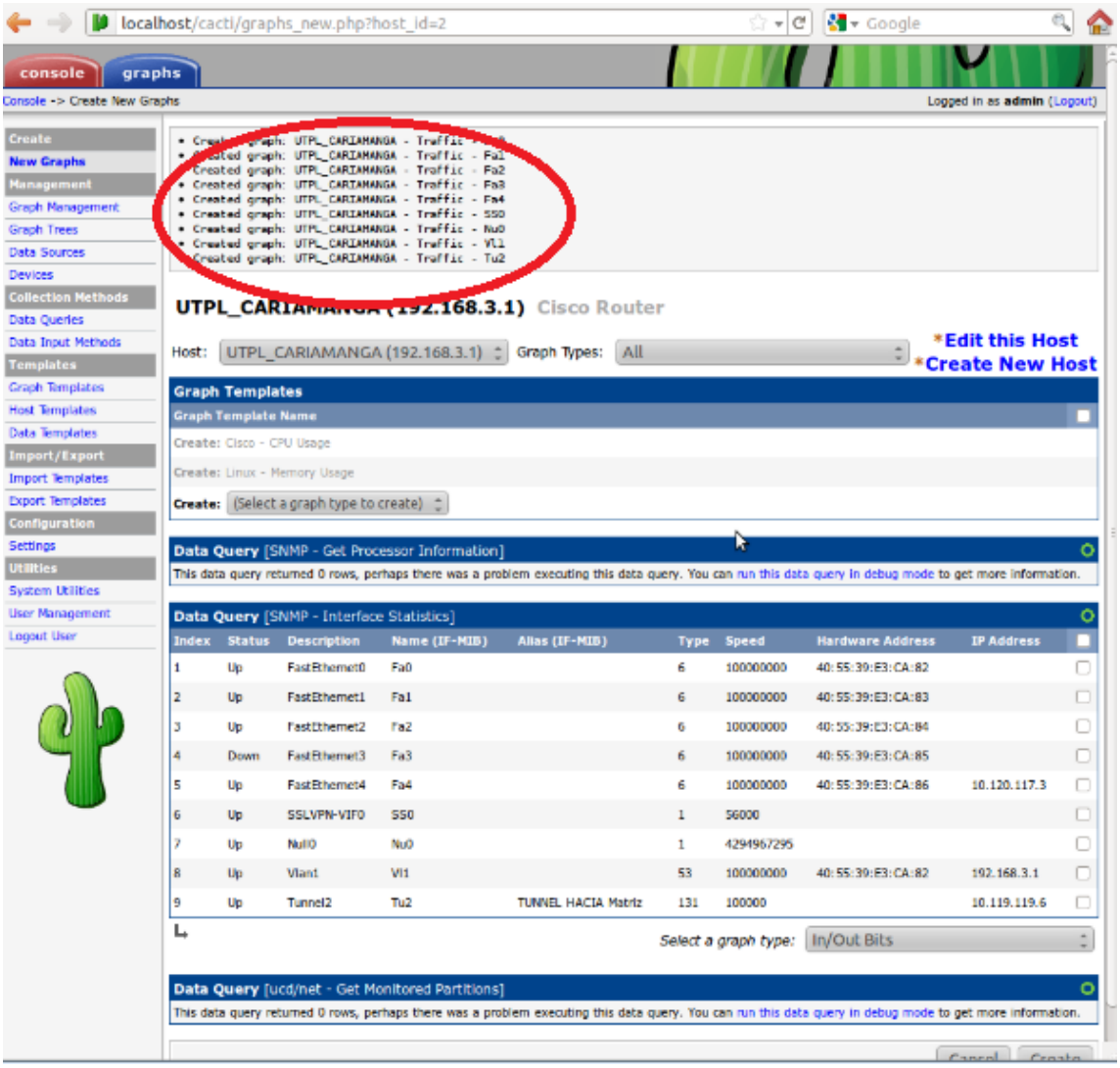


Figura a.6. 20. La creación correcta de los gráficos.

Una vez creado el dispositivo, seleccionado las gráficas de la información que se requiere monitorear, lo que resta es esperar 5 minutos, para que el Cacti no presente dicha información.