**UNIVERSIDAD TECNOLOGICA DE BOLIVAR**

**ESPECIALIZACION EN TELECOMUNICACIONES**

# ESTUDIO PARA MEJORAR LA EFICIENCIA DE LA RED DE DATOS CORPORATIVA DE LA FUNDACIÓN UNIVERSITARIA TECNOLOGICO COMFENALCO MEDIANTE SU RENOVACIÓN TECNOLÓGICA.

**AUTORES**

**DILIA ESTER TORRES CANTILLO**
**JUAN HAROLD SILVA MIRANDA**

**CARTAGENA OCTUBRE 14 DE 2011**

# TABLA DE CONTENIDO


*1 INTRODUCCION ..... 5*

*2 OBJETIVOS ..... 6*

**2.1 Objetivo general ..... 6**

**2.2 Objetivos específicos ..... 6**

*3 MARCO TEORICO ..... 7*

*4 DIAGNOSTICO ..... 12*

**4.1 Misión ..... 12**

**4.2 Visión ..... 12**

**4.3 La división de Tecnologías de información y comunicaciones ..... 13**

*4.3.1 Misión ..... 13*

*4.3.2 Visión ..... 13*

4.3.3 Objetivo ..... 13

*4.3.4 Organigrama ..... 13*

**4.4 Organigrama de la institución ..... 14**

**4.5 Inventario de hardware ..... 14**

*4.5.1 Equipos usuarios administrativos ..... 14*

**4.6 Inventario de software ..... 15**

**4.7 Estructura física de la red ..... 15**

*4.7.1 Servidores ..... 15*

*4.7.2 Diagrama actual de red ..... 19*

**4.8 Muestreo y aplicación de encuestas al usuario final ..... 20**

**4.9 Análisis de tráfico ..... 23**

*4.9.1 Trafico detectado en la red ..... 23*

*4.9.2 Diagrama de internet ..... 27*

*4.9.3 Análisis de cargas ..... 27*

*4.9.4 Equipos activos ..... 31*

*4.9.5 Enlace inalámbrico entre las dos sedes ..... 31*

**4.10 Recomendaciones a partir del análisis de tráfico ..... 33**

*5 DISEÑO FISICO DE LA RED ..... 34*

*6 DISEÑO LOGICO DE LA RED ..... 38*

**6.1 Segmentación de Broadcast ..... 39**

*6.1.1 Vlan de Gestion ..... 39*

*6.1.2 Vlan de VoIP ..... 39*

*6.1.3 Vlan dependencias Administrativas* ..... 40

**6.2 Descripción distribución lógica para cada switch ..... 40**

*6.2.1 Switch Rectoría: Cisco 2960. 24 puertos* ..... 40

*6.2.2 Switches 4° piso: Flexstack. 2 switches Cisco 2960. 96 puertos en total.* ..... 40

*6.2.3 Switch derecho: Cisco 2960. 24 puertos* ..... 40

*6.2.4 Switch Colonia china. Cisco 2960. 24 puertos* ..... 41

*6.2.5 Switches sala de profesores y decanatura. 2 switches Cisco de 24 puertos cada uno.* ..... 41

*6.2.6 Switches sede Zaragocilla: 2 switch de acceso 2960 de 48 puertos cada uno.* ..... 41

**6.3 Switch de Distribución : switch Cisco 4507R+E ..... 42**

**6.4 Comunidad SNMP ..... 44**

***7 CONSIDERACIONES FINALES ..... 46***

***8 ANEXOS ..... 47***

***9. INDICE DE TABLAS ..... 48***

***10. INDICE DE FIGURAS ..... 49***

***11. BIBLIOGRAFIA ..... 50***

## AGRADECIMIENTOS

Mis más sinceros agradecimientos para los amigos incondicionales que durante todo este año y medio me brindaron su apoyo, en especial a aquellos que con su paciencia orientaron el camino de la construcción de este trabajo que más que un requisito se constituyó en una escuela por todos los conocimientos que interioricé.

Gracias a mi esposo y a mis hijos por todo el tiempo que deje de compartir con ellos para dedicarme a estudiar y por ese amor tan grande que a diario me profesan. Los frutos de este esfuerzo los dedico a ellos.

# ESTUDIO PARA MEJORAR LA EFICIENCIA DE LA RED CORPORATIVA DE LA FUNDACIÓN UNIVERSITARIA TECNOLOGICO COMFENALCO MEDIANTE SU RENOVACIÓN TECNOLÓGICA.

## 1 INTRODUCCION

El crecimiento acelerado que a diario experimentan la ciencia y la tecnología hace que las instituciones de educación superior propendan por disponer de los medios y tecnología de comunicación que le permita mantenerse a la vanguardia de los tiempos optimizando de esta forma el trabajo de que desempeña su equipo humano.

Por esta razón se plantea la renovación de la red corporativa existente en la Fundación Universitaria Tecnológico Comfenalco, dada la importancia que reviste para los actores de esta empresa contar con alta disponibilidad de servicios compartidos, procurando la integración entre las aplicaciones de voz y datos sin descuidar la priorización y seguridad que este proceso debe llevar implícito.

El diseño lógico propuesto se fundamenta en el modelo de tres capas estando el core en manos del ISP mientras que las capas de distribución y acceso constituyen grupos funcionales dentro de la empresa. Los protocolos utilizados se ajustan a las particularidades del diseño planteado en este documento.

# 2 OBJETIVOS

## 2.1 Objetivo general

Realizar un estudio que permita mejorar la eficiencia de la red corporativa de la Fundación Universitaria Tecnológico Comfenalco mediante su renovación tecnológica.

## 2.2 Objetivos específicos

- Proveer una solución adecuada para la comunidad administrativa de la institución, que hacen uso de los servicios de la red a través de la integración de nuevos servicios.

- Optimizar la planificación del soporte técnico al contar con una plataforma de red dinámica de fácil gestión que permita la identificación y rápida resolución de problemas en la infraestructura de red de La Fundación Universitaria.

- Diseñar un modelo de red de tres capas: acceso, Distribución y Core, partiendo del estudio del flujo de información y utilizando estrategias y metodologías que permitan optimizar el esquema tradicional teniendo en cuenta la escalabilidad de la red corporativa.

# 3 MARCO TEORICO

Para construir correctamente una interconexión de redes que pueda dar una respuesta eficaz a las necesidades de los usuarios, se utiliza un modelo jerárquico de tres capas que permita organizar el flujo del tráfico.

La jerarquía tiene muchos beneficios en el diseño de las redes y nos ayuda a hacerlas más predecibles. En esencia, definimos funciones dentro de cada capa, ya que las redes grandes pueden ser extremadamente complejas e incluir múltiples protocolos y tecnologías; así, el diseño nos ayuda a tener un modelo fácilmente manejable y configurable [1].

Las capas y sus funciones típicas son:

- La capa de **Acceso** (access layer): Conmutación (switching); controla a los usuarios y el acceso de grupos de trabajo (workgroup access) o los recursos de internetwork. Los recursos más utilizados por los usuarios deben ser ubicados localmente, pero el tráfico de servicios remotos es manejado aquí. Entre sus funciones están la continuación de control de acceso y políticas, creación de dominios de colisión separados (segmentación), conectividad de grupos de trabajo en la capa de distribución (workgroup connectivity). En esta capa se lleva a cabo la conmutación Ethernet (Ethernet switching), DDR y ruteo estático (el dinámico es parte de la capa de distribución).

- La capa de **Distribución** (distribution layer): Enrutamiento (routing); también llamada *workgroup layer*, y es el medio de comunicación entre la capa de acceso y el Core. Las funciones de esta capa son proveer ruteo, filtrado,

[1] Tomado de http://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red

acceso a la red WAN y determinar que paquetes deben llegar al Core. Además, determina cuál es la manera más rápida de responder a los requerimientos de red, por ejemplo, cómo traer un archivo desde un servidor.

Aquí además se implementan las políticas de red, por ejemplo: ruteo, access-list, filtrado de paquetes, cola de espera (queuing), se implementa la seguridad y políticas de red (traducciones NAT y firewalls), la redistribución entre protocolos de ruteo (incluyendo rutas estáticas), ruteo entre VLANs y otras funciones de grupo de trabajo, se definen dominios de broadcast y multicast. Debemos evitar que se hagan funciones en esta capa que son exclusivas de otras capas.

- La capa de **Núcleo** (core layer): Backbone; es literalmente el núcleo de la red, su única función es *switchear* tráfico tan rápido como sea posible y se encarga de llevar grandes cantidades de tráfico de manera confiable y veloz, por lo que la **latencia** y la **velocidad** son factores importantes en esta capa.

  El tráfico que transporta es común a la mayoría de los usuarios, pero el tráfico se procesa en la capa de distribución que a su vez envía las solicitudes al core si es necesario. En caso de falla se afecta a todos los usuarios, por lo que la tolerancia a fallas es importante.

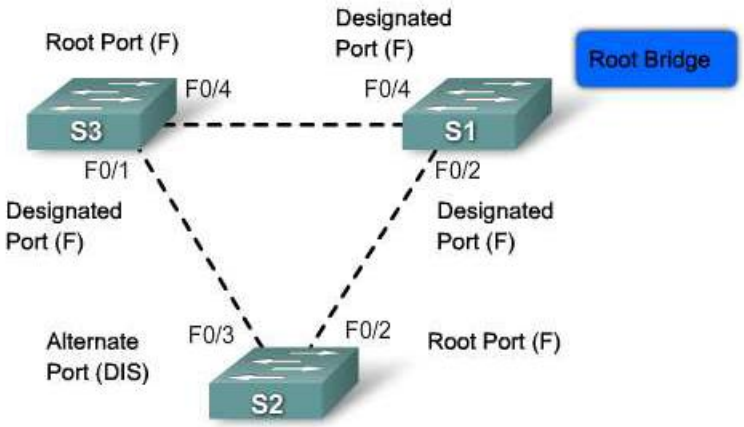
  Además, dada la importancia de la velocidad, el core no hace funciones que puedan aumentar la latencia, como access-list, ruteo interVLAN, filtrado de paquetes, ni tampoco workgroup access. Se debe evitar a toda costa aumentar el número de dispositivos en el *Core* (no agregar routers), si la capacidad del Core es insuficiente, debemos considerar aumentos a la

plataforma actual (upgrades) antes que expansiones con equipo nuevo[2].

Los protocolos de comunicaciones desempeñan un papel importante a nivel de funcionalidad de cualquier modelo de red. Para garantizar el rendimiento y disponibilidad de los servicios de red en la Fundación Universitaria, se trabajará con los protocolos ERSH y RSTP.

RSTP (IEEE 802.1w) es una evolución de estándar 802.1D.

Figura 1.Protocolo RSTP




Características de RSTP:

- Es el protocolo preferido para evitar bucles de capa 2 en un entorno de red conmutada.
- Mantiene la compatibilidad retrospectiva.
- Puede confirmar de manera activa que un puerto puede sufrir una transición segura al estado de enviar sin depender de ninguna configuración de temporizadores[3].

[2] Tomado de http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Introduccion.aspx

El RSTP requiere una conexión full-duplex de punto a punto entre los switches para alcanzar la velocidad de reconfiguración más rápida. La reconfiguración de Spanning Tree mediante RSTP se produce en menos de 1 segundo, mientras que con STP demoraba hasta 50 segundos.

Para acelerar el proceso de cálculo, RSTP reduce la cantidad de estados de puerto a tres: descarte, aprendizaje y envío. El estado de descarte es similar a tres de los estados del STP original: bloqueo, escucha y desactivación. RSTP también presenta el concepto de topología activa. Todos los puertos que no estén en estado de descarte se consideran parte de la topografía activa y pasan de inmediato al estado de reenvío.

El manejo de las Vlan en el modelo se hará a partir del protocolo VTP (Vlan trunking protocol) que opera en los modos servidor, cliente y transparente.

**Servidor**: Debe haber al menos un Servidor. Desde él se pueden crear, eliminar o modificar VLANs.

**Cliente**: Desde la CLI no se pueden crear, eliminar o modificar VLANs.

**Transparente**: Desde él no se puede crear, eliminar o modificar VLANs (que afecten a los demás switches), las VLANs que se creen en el switch mediante CLI serán sólo locales para este switch. No procesa las actualizaciones VTP recibidas, sólo las reenvía a los switches vecinos.

Los administradores cambian la configuración de las VLANs en el switch en modo servidor, después de que se realiza algún cambio, estos son distribuidos a todos los demás dispositivos en el dominio VTP a través de los enlaces que permiten el Trunk. Los dispositivos que operan en modo transparente no aplican las configuraciones VLAN que reciben, ni envían las suyas a otros dispositivos, sin embargo los

[3] Inc. Cisco System. Academia de Networking de Cisco System, Guia del segundo año CCNA 3 y 4.

dispositivos en modo transparente que usan la versión 2 del protocolo VTP enviarán la información que reciban (publicaciones VTP) a otros dispositivos a los que estén conectados, actualmente (año 2009) dichas publicaciones se envían cada 5 minutos.

Los dispositivos que operen en modo cliente, automáticamente aplicarán la configuración que reciban del dominio VTP, en el modo cliente NO se podrán crear VLAN, sino que sólo podrá aplicar la información que reciba de las publicaciones VTP.

Las configuraciones VTP en una red son controladas por un número de revisión. Si el número de revisión de una actualización recibida por un switch en modo cliente o servidor es más alto que la revisión anterior, entonces se aplicará la nueva configuración. De lo contrario se ignoran los cambios recibidos. Cuando se añaden nuevos dispositivos a un dominio VTP, se debe resetear los números de revisión de todo el dominio VTP para evitar conflictos. Se recomienda tener mucho cuidado al usar VTP cuando haya cambios de topología ya sean lógicos o físicos.

Realmente no es necesario resetear todos los números de revisión del dominio. Sólo hay que asegurarse de que los switches nuevos que se agregen al dominio VTP tengan números de revisión más bajos que los que están configurados en la red. Si no fuese así, bastaría con eliminar el nombre del dominio del switch que se agrega. Esa operación vuelve a poner a cero su contador de revisión.

El VTP permite a un administrador de red configurar un switch de modo que propagará las configuraciones de la VLAN hacia los otros switches en la red. El switch se puede configurar en la función de servidor del VTP o de cliente del VTP. El VTP sólo aprende sobre las VLAN de rango normal (ID de VLAN 1 a 1005). Las VLAN de rango extendido (ID mayor a 1005) no son admitidas por el VTP. El VTP guarda las configuraciones de la VLAN en la base de datos de la VLAN, denominada vlan.dat.

El VTP permite al administrador de red realizar cambios en un switch que está configurado como servidor del VTP. Básicamente, el servidor del VTP distribuye y sincroniza la información de la VLAN a los switches habilitados por el VTP a través de la red conmutada, lo que minimiza los problemas causados por las

configuraciones incorrectas y las inconsistencias en las configuraciones. El VTP guarda las configuraciones de la VLAN en la base de datos de la VLAN denominada vlan.dat. Para que dos equipos que utilizan VTP puedan compartir información sobre VLAN, es necesario que pertenezcan al mismo dominio.

# 4 DIAGNOSTICO

La Fundación Universitaria Tecnológico Comfenalco es una institución de Educación Superior de carácter universitario reconocida por el Ministerio de Educación Nacional.

Inició actividades académicas al servicio de la educación colombiana en 1984. El Tecnológico Comfenalco es una respuesta que tradicionalmente ha tenido la Caja de Compensación Familiar hacía el problema educativo de la región. Por ello creó esta institución sin ánimo de lucro, para prestar el servicio de Educación Superior conforme a las normas legales vigentes.

## 4.1 Misión

Somos una Institución de educación superior con personal altamente comprometido que forma personas integrales con cultura investigadora, innovadora y emprendedora, capaces de transformar e impactar positivamente el sistema social.

## 4.2 Visión

La Fundación Universitaria Tecnológico Comfenalco en el 2019 será una institución de calidad reconocida por su modelo en formación progresiva, con un excelente equipo humano aportando soluciones para el desarrollo de Cartagena, la Región y el País.

## 4.3 La división de Tecnologías de información y comunicaciones

### *4.3.1* M*isión*

Ser el soporte de los procesos académicos y administrativos de la institución. Garantizando a través de tecnología de punta y personal calificado la disponibilidad, confiabilidad e integridad de la información.

### *4.3.2 Visión*

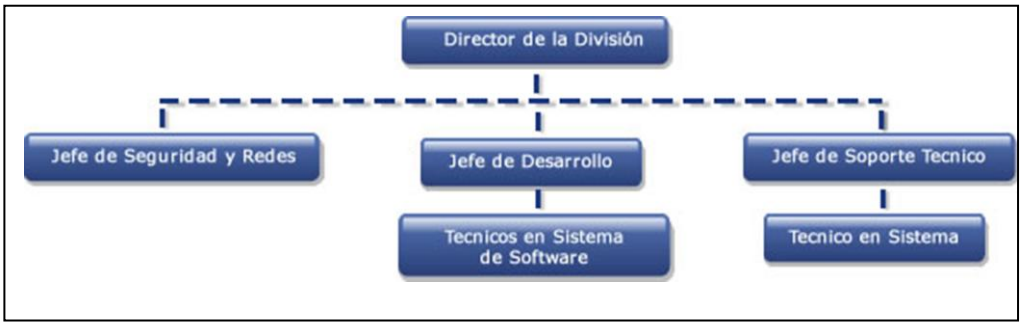
En el año 2012 la División de tecnologías de la información y comunicaciones tendrá las herramientas computacionales implementadas que permitirán a la institución tener automatizados todos sus procesos.

### 4.3.3 Objetivo

Gestionar los recursos tecnológicos para contribuir con el alcance de los objetivos institucionales.

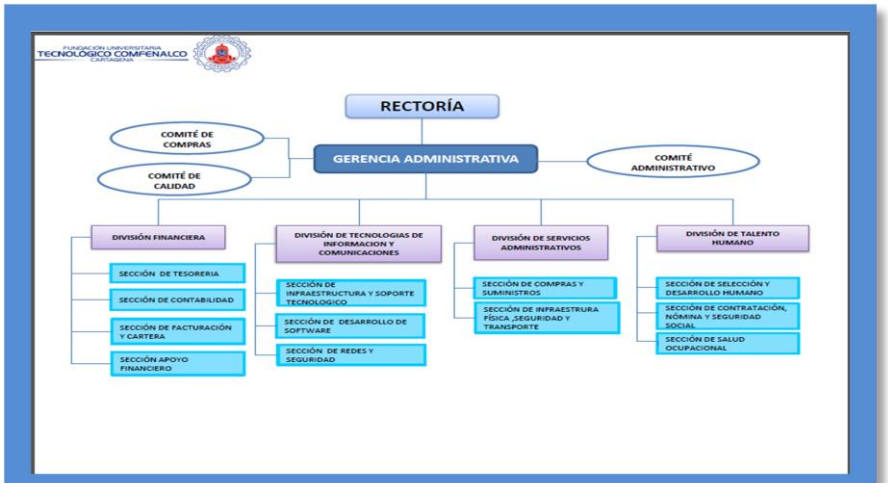
### *4.3.4 Organigrama*

Figura 2. Organigrama Division Tecnologias de Informacion y comunicaciones



## 4.4 Organigrama de la institución

Figura 3. Organigrama FUTCO




La división de tecnologías de la información y comunicaciones está formada por tres secciones a saber: infraestructura y soporte tecnológico, desarrollo de software y la sección de redes y seguridad. Cada una de ellas tiene un jefe de sección que se responsabiliza por el cumplimiento de las metas propuestas para su área y a su vez dependen directamente del director de la división. La gerencia administrativa es el ente que a nivel de gestión y planeación supervisa las labores que ejecuta la división de tecnologías de la información y comunicaciones.

## 4.5 Inventario de hardware

### *4.5.1 Equipos usuarios administrativos*

Tabla 1. Inventario equipos red FUTCO

| *Tipo de Usuario* | *Inventario Equipos* |
|---|---|
| Administrativos sede España | 156 |
| Administrativos Zaragocilla | 54 |
| **Total** | 210 |

## 4.6 Inventario de software

Se presenta como anexo 1.

## 4.7 Estructura física de la red

La arquitectura de comunicación (LAN ) de la Fundación Universitaria Tecnológico Comfenalco utiliza básicamente cable UTP categoría 6A, Fibra Óptica, Switches capa (3), Routers, Firewall, servidores y Antenas de Radio enlace; la normativa que se maneja es la T568B, con velocidades de 10 Mbps - 100 Mbps – 1000 Mbps. La topología de red implementada es la topología Árbol, además se cuenta con un Backbone que va desde el Data Center hasta un piso superior del edificio. La red LAN del Tecnológico se encuentra dividida en dos subredes, Área Administrativa y la Académica, esto se hace mediante un Switch Core Cat4500 E-Series 7-Slot Chassis de capa 3 y 4 de 48 y 24 puertos.

La red de voz esta soportada por cable UTP categoría 6 y es administrada por una central telefónica PBX digital-análoga marca Panasonic la cual está conectada por un equipo de cómputo donde se gestiona y se configura las extensiones, grupo, tiempo etc.

El servicio de Internet es suministrado por dos proveedores, Telefónica Telecom con un canal dedicado 1:1 de 4 Mbps y Columbus con un canal de 10 Mbps. Para proporcionar el servicio de Internet a la sede de Zaragocilla se utiliza un Radio Enlace, las señales son enviadas a través de antenas ubicadas en zonas altas tanto de la sede principal (sede España) como en la sede Zaragocilla para lograr una buena línea de vista. Para aterrizar este enlace se usa cable UTP categoría 5A que se interconecta a un Switch 3Com 4500G capa 3 de 24 puertos, este tiene configurado Vlans para segmentar la información tanto para el área administrativa como para el área académica.

### *4.7.1 Servidores*

Los servidores se encuentran ubicados en el cuarto de comunicaciones de la Fundación Universitaria Tecnológico Comfenalco, estos presta servicios como: Web tecnológico Comfenalco, Plataforma virtual, Conexiones Cartagena, Exchange Server, Portal Institucional (SharePoint), Dhcp Académico, Dhcp Administrativo, Servido de Almacenamiento, Synersis, Proxy académico, Proxy Administrativo, DNS, Antivirus, ERP, Nomina entre otros.

En los servidores están instalados los siguiente sistemas operativos: Linux Centos 5,1, Windows 2003 Server R2, Windows 2008 Server, Linux Red hat 9, donde se administra y se gestiona todo los recursos y servicios que la institución ofrece.

Citando las marcas correspondientes a los servidores de la institución, podemos mencionar:

- ✓ 2 HP Blade System C3000 Enclousure, con 11 servidores
- ✓ HP Storage works P2000
- ✓ DELL: se cuenta con los siguientes modelos (PowerEdge R200, PowerEdge 2950, PowerVault MD1000, Proliant ML350 G4, PowerEdge 1600SC, PowerEdge 600SC, entre otros).

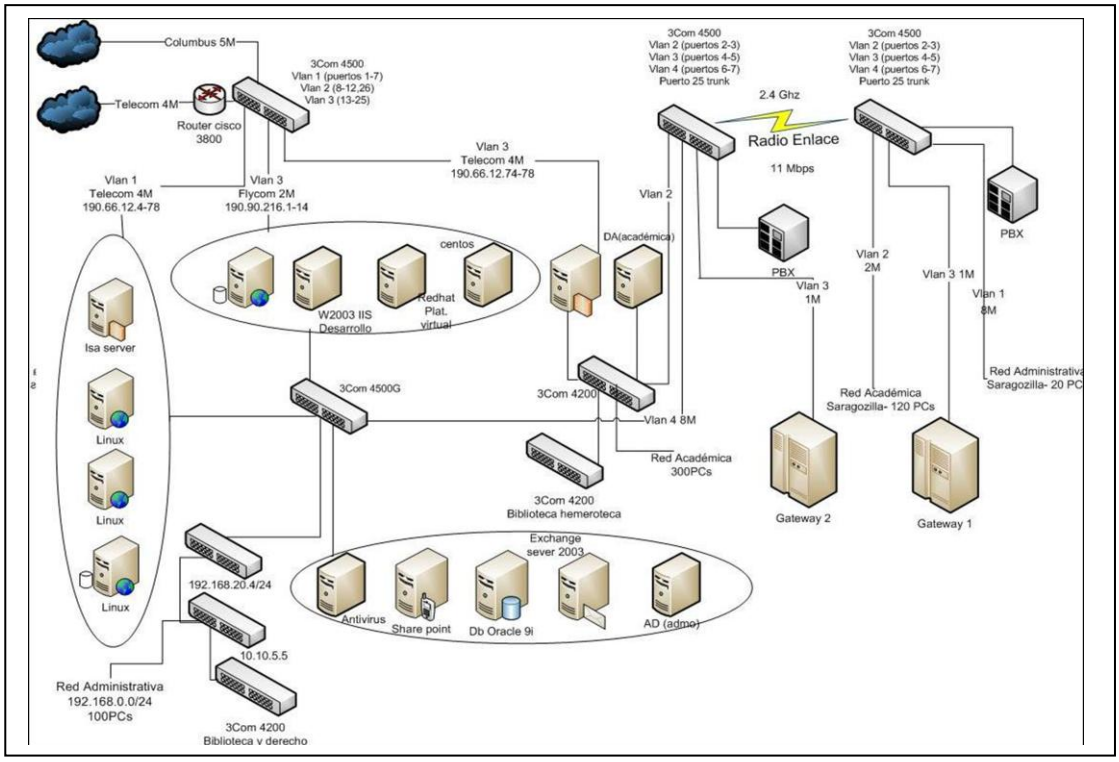
Tabla 2. Descripción de servidores

| Servidor | Ip | Aplicaciones | Servicio |
|---|---|---|---|
| Web | | pagina web institucional; Funciona bajo Linux y servidor Apache | Web |
| Amsys /Itachi | | Software de manejo académico, manejo de inscripciones, matriculas, registro de notas, novedades académicas, volantes de pagos, Instalado sobre plataformas Windows 2008 R2, desarrollado en java , utiliza como contenedor apache tomcat 6 | apache tomcat |
| Portal | | Servicio diseñado para manejo de portal de calidad institucional, bajo ambiente Windows y desarrollado en SharePoint | SharePoint/ Sql Server |
| Plataforma Virtual | | Software para soporte tecnológico virtual a estudiantes y docentes basado en moodle , sobre sistema operativo Linux | Moodel |
| Directorio Activo | | Manejo de usuarios y políticas, funciona sobre Windows 2008 R2 | |
| Servidor DHCP | | Asignación dinámica de Ip para los usuarios administrativos | |
| Servidor DNS | | Dns interno para resolución de nombres de equipos complemento para directorio activo | |
| Directorio Activo /DNS secundario | | Respaldo para Directorio Activo y Dns, Instalados bajo Windows 2008 R2 | |
| Directorio Activo - Academia/dns primario | | Manejo de usuarios y políticas, funciona sobre Windows 2008 R2 | |
| Base de Datos Oracle | | Servidor de Dbase de Datos para las aplicaciones,(Erp Administrativo, software académico Amsys e Itachi), Funciona Bajo sistema operativo Linux | Oracle 11G |

| Servidor | Ip | Aplicaciones | Servicio |
|---|---|---|---|
| Base de Datos Oracle (Pruebas) | | Servidor de base de datos de pruebas y respaldo | Oracle 11G |
| Aplicaciones | | Servidor de Aplicaciones Erp, contiene los ejecutables , Funciona bajo sistema operativo Windows 2008 St. R2 | |
| Aplicaciones Web | | Servidor de aplicaciones Web, para software de pruebas de personalidad 16pf, registro de horas docente, registro de notas | 16PF, |
| Gestion Documental | | Aplicativo para manejo de Archivo de documentos digitales, Funciona bajo Sistema operativo Windows 2008 R2, y base de datos Sql Server 2008 | |
| Aplicativo de Biblioteca SIABUC | | Programa para el manejo de Prestamos, reservas e inventario de libros, Bajo plataforma Windows 2008 st R2 y base de datos Postgres | |
| Desarrollo de Aplicativo ERP Web | | Desarrollo de aplicaciones Web, utilizando java para desarrollo, base de datos Oracle 11G R2/ sistema operativo Windows 2008 St. R2 | Java /Oracle 11G |
| Consola Antivirus | | Manejo y Control de Clientes Antivirus / Funciona Bajo Plataforma Windows 2008 St R2 | |
| proyecto Proservicios | | Servidor para desarrollo de Software de Nominas, Funciona bajo ambiente Linux, base de datos Postgres, herramienta de Desarrollo Java | |
| Synersis | | Software Administrativo Finaciero y académico, bajo ambiente Windows server 2003 St R2 / base de datos Oracle 9i | |
| | | | |

### *4.7.2 Diagrama actual de red*

Figura 4. Diseño actual de la red FUTCO




La red institucional, posee 2 canales de internet con diferentes proveedores (Columbus network 5MB y Telecom 4MB), estas conexiones llegan a un switch principal 3com 4500G configurado con 3 VLAN (aplicaciones WEB, Servidores de aplicación y Proxy), las dos sedes son comunicadas con un radio enlace que provee una velocidad de 11 Mbps por los cuales viajan las 3 VLAN configuradas como troncales (incluida aquí la voz por medio de Gateway) interconectado por switches 3com 4500G.

La sede principal ubicada en el barrio España cuenta con switches 4500, 4500G 3com, 4200 marca 3com, Next, Hubs 3com, planet y Encore. Los conmutadores 4500 son de Nivel 3 y los 4200 3com, planet y Next son de nivel 2.

El acceso a la red pública se recibe a través de 2 operadores: TELECOM (4Mbps) vía router Cisco 3800 y COLUMBUS (5Mbps). Ambos enlaces físicos se integran a la plataforma de comunicaciones de la institución a través de 2 switches 3com 4500 que se conectan en cascada con los 4 switches principales de la capa de núcleo de la red.

La interconexión de los 4 switches de la capa de núcleo ubicados en el centro principal de cableado se hizo en cascada a través de interfaces de Gigabit.

La sede principal se interconecta a la sede Zaragocilla ubicada a 870 Metros aproximadamente, a través de un enlace de radio en la banda de los 2.4Ghz implementado con equipos tipo indoor marca Linksys serie WAP54G basados en el estándar 802.11g.

## 4.8 Muestreo y aplicación de encuestas al usuario final

Partiendo de la importancia de la percepción del usuario final acerca del rendimiento de la red, en este caso el cuerpo administrativo de la Fundación Universitaria, se elaboró una encuesta (anexo 2) cuyo objetivo es determinar el nivel de satisfacción de los funcionarios de la institución en cuanto al aspecto anteriormente citado y conocer además las expectativas que tienen al respecto de la utilización de servicios adicionales a los ya existentes que complementen y optimicen la labor realizada por cada uno de ellos desde su lugar de trabajo

Consideramos de gran importancia antes de entrar en el detalle de la operacionalizacion de la encuesta de satisfacción**,** presentar una pequeña fundamentación teórica que contextualice el trabajo realizado en esta etapa.

**Población**, una población es el total de las observaciones concebibles de un tipo particular.

**Muestra**, es un número limitado de observaciones de una población, elegidos de tal modo que permita que todas las observaciones posibles tengan la misma probabilidad de presentarse.

**Individuo**: Es cada uno de los integrantes de la población o muestra en los que se estudiarán las características de interés determinadas por los objetivos del estudio. Normalmente, el número de individuos de la muestra se representa con la letra **n** y el número de sujetos de la población por la **N**.

Tras la definición de las características de la población a través de los criterios de inclusión y exclusión, se ha de decidir si se estudia a toda la población o en caso que ésta sea demasiado grande a un número de sujetos representativo, que no han de ser ni pocos ni demasiados, sino simplemente los necesarios.

El tamaño de la muestra está condicionado por los objetivos del estudio, que determinarán su diseño, las variables a considerar y el método planteado.

El tamaño de la muestra depende de tres aspectos:

1) Error permitido
2) Nivel de confianza estimado
3) Carácter finito o infinito de la población.

La fórmula general para determinar el tamaño de la muestra cuando la población es finita es la siguiente:

Para poblaciones finitas (menos de 100,000 habitantes)

$$n = \frac{Z^2 * P * Q * N}{E^2 (N-1) + Z^2 * P * Q}$$

Nomenclatura:

n = Número de elementos de la muestra

N = Número de elementos de la población o universo

P/Q = Probabilidades con las que se presenta el fenómeno.

Z2 = Valor crítico correspondiente al nivel de confianza elegido; siempre se opera con valor zeta 2, luego Z = 2.

E = Margen de error permitido (determinado por el responsable del estudio).

Cuando el valor de P y de Q sean desconocidos o cuando la encuesta abarque diferentes aspectos en los que estos valores pueden ser desiguales, es conveniente tomar el caso más adecuado, es decir, aquel que necesite el máximo tamaño de la muestra, lo cual ocurre para P = Q = 50, luego, P = 50 y Q = 50.

Atendiendo a lo anteriormente expuesto, se aplicó inicialmente una prueba piloto a 15 funcionarios de la institución para partir de esto, determinar el tamaño de la muestra de acuerdo con el nivel de confianza deseado.

Como resultado de este proceso, se seleccionó un tamaño de muestra de 66 empleados administrativos lo cual nos dá un nivel de confianza del 95% con un error máximo permisible del 10%.

Los resultados de la encuesta tabulada se muestran en el Anexo 3.

Partiendo de los resultados observados y del análisis grafico de los mismos, es posible concluir lo siguiente:

- La mayor parte de la población administrativa coincide en que el servicio prestado por la red es Regular, lo cual supone la implementación de estrategias que optimicen el servicio prestado a los usuarios de la misma.
- Los tiempos de respuesta percibidos por la mayoría de los usuarios de la red, son calificados como regulares.
- Los servicios ofrecidos por la red que experimentan mayor demanda son el correo electrónico, software de notas y financiero, software de horas plataforma virtual.
- Dentro de los servicios adicionales que se pueden ofrecer a través de la red de comunicaciones, los usuarios se inclinan por la telefonía Ip y las aplicaciones web.

Además de la encuesta anterior, se elaboró una encuesta técnica para ser aplicada al administrador de la red, con la cual se pretende levantar información relevante al respecto de la disponibilidad, servicios y anomalías existentes en la infraestructura de red de la Fundación Universitaria. Anexo 4.

Partiendo de la información recolectada en la encuesta técnica, podemos sacar las conclusiones a continuación detalladas:

- El diseño de la red no se ciñe al modelo jerárquico de tres capas lo que le resta beneficios tales como, el ser un modelo fácilmente entendible que permita gestionar de manera sencilla y eficaz la aplicación de configuraciones determinadas. De la misma forma el modelo actual carece de bondades que faciliten la labor de mantenimiento de la red. Por otro lado el manejar un diseño plano limita la escalabilidad de la red, característica importante en este caso si tomamos en consideración que hablamos de una institución educativa en permanente crecimiento.

- Existen problemas de disponibilidad en la red así como también de otras serie de anomalías tales como: congestión, saturación por broadcast (en alto nivel), colisiones, retardos y jitter, lo cual entorpece las funciones coyunturales que se desarrollan en la universidad a diario, no solo a nivel de funcionarios administrativos sino también de aquellos que pertenecen al área académica. De otro lado esto imposibilita la implementación de servicios como VoIP y videoconferencia.

- No existe un sistema de gestión de fallas proactivo que permita la detección oportuna y recuperación de los problemas que se presenten en la red, lo cual se refleja en tiempos de respuesta inadecuados ante situaciones críticas como la no disponibilidad de un servicio.

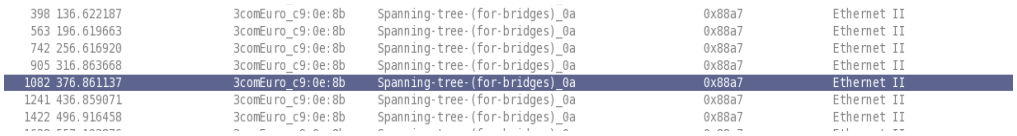
## 4.9 Análisis de tráfico

Para llevar a cabo el análisis de tráfico utilizamos como herramienta Wireshark que es una multiplataforma de **análisis de red,** producto de la evolución de **Ethereal**. Funciona al igual que otros sniffer pero, tiene como valor agregado el manejo de un **entorno gráfico** además de manejar una interfaz amigable al usuario y de fácil comprensión.

### *4.9.1 Trafico detectado en la red*

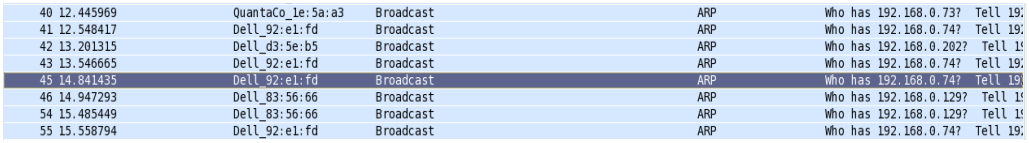
A continuación relacionamos el tráfico detectado en la red corporativa de la fundación universitaria:

**Trafico 0x88a7**



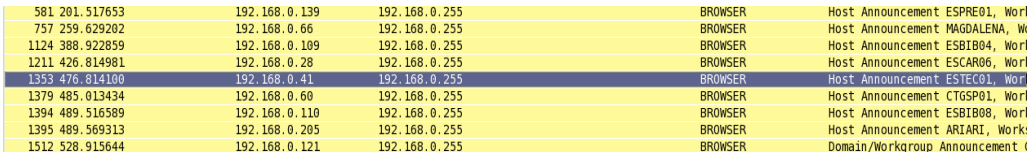
| | | | | | |
|---|---|---|---|---|---|
| 398 | 136.622187 | 3comEuro_c9:0e:8b | Spanning-tree-(for-bridges)_0a | 0x88a7 | Ethernet II |
| 563 | 196.619663 | 3comEuro_c9:0e:8b | Spanning-tree-(for-bridges)_0a | 0x88a7 | Ethernet II |
| 742 | 256.616920 | 3comEuro_c9:0e:8b | Spanning-tree-(for-bridges)_0a | 0x88a7 | Ethernet II |
| 905 | 316.863668 | 3comEuro_c9:0e:8b | Spanning-tree-(for-bridges)_0a | 0x88a7 | Ethernet II |
| 1082 | 376.861137 | 3comEuro_c9:0e:8b | Spanning-tree-(for-bridges)_0a | 0x88a7 | Ethernet II |
| 1241 | 436.859071 | 3comEuro_c9:0e:8b | Spanning-tree-(for-bridges)_0a | 0x88a7 | Ethernet II |
| 1422 | 496.916458 | 3comEuro_c9:0e:8b | Spanning-tree-(for-bridges)_0a | 0x88a7 | Ethernet II |

**Trafico Arp**



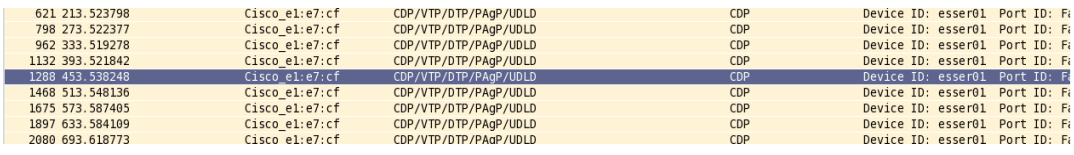
| | | | | | |
|---|---|---|---|---|---|
| 40 | 12.445969 | QuantaCo_1e:5a:a3 | Broadcast | ARP | Who has 192.168.0.73? Tell 192 |
| 41 | 12.548417 | Dell_92:e1:fd | Broadcast | ARP | Who has 192.168.0.74? Tell 192 |
| 42 | 13.201315 | Dell_d3:5e:b5 | Broadcast | ARP | Who has 192.168.0.202? Tell 19 |
| 43 | 13.546665 | Dell_92:e1:fd | Broadcast | ARP | Who has 192.168.0.74? Tell 192 |
| 45 | 14.841435 | Dell_92:e1:fd | Broadcast | ARP | Who has 192.168.0.74? Tell 192 |
| 46 | 14.947293 | Dell_83:56:66 | Broadcast | ARP | Who has 192.168.0.129? Tell 19 |
| 54 | 15.485449 | Dell_83:56:66 | Broadcast | ARP | Who has 192.168.0.129? Tell 19 |
| 55 | 15.558794 | Dell_92:e1:fd | Broadcast | ARP | Who has 192.168.0.74? Tell 192 |

**Tráfico Browser**



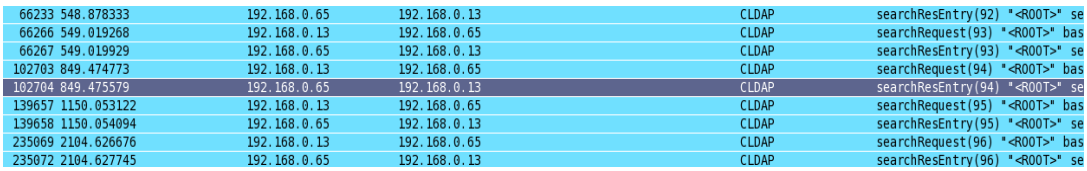
| | | | | | |
|---|---|---|---|---|---|
| 581 | 201.517653 | 192.168.0.139 | 192.168.0.255 | BROWSER | Host Announcement ESPRE01, Worl |
| 757 | 259.629202 | 192.168.0.66 | 192.168.0.255 | BROWSER | Host Announcement MAGDALENA, W |
| 1124 | 388.922859 | 192.168.0.109 | 192.168.0.255 | BROWSER | Host Announcement ESBIB04, Worl |
| 1211 | 426.814981 | 192.168.0.28 | 192.168.0.255 | BROWSER | Host Announcement ESCAR06, Worl |
| 1353 | 476.814100 | 192.168.0.41 | 192.168.0.255 | BROWSER | Host Announcement ESTEC01, Wor |
| 1379 | 485.013434 | 192.168.0.60 | 192.168.0.255 | BROWSER | Host Announcement CTGSP01, Worl |
| 1394 | 489.516589 | 192.168.0.110 | 192.168.0.255 | BROWSER | Host Announcement ESBIB08, Worl |
| 1395 | 489.569313 | 192.168.0.205 | 192.168.0.255 | BROWSER | Host Announcement ARIARI, Works |
| 1512 | 528.915644 | 192.168.0.121 | 192.168.0.255 | BROWSER | Domain/Workgroup Announcement ( |

**Trafico CDP**



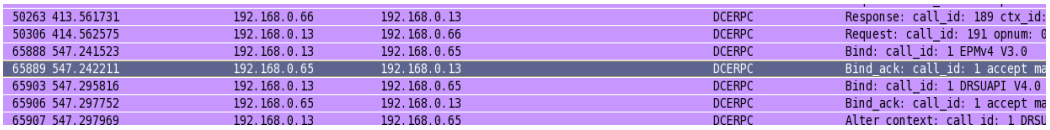
| | | | | | |
|---|---|---|---|---|---|
| 621 | 213.523798 | Cisco_e1:e7:cf | CDP/VTP/DTP/PAgP/UDLD | CDP | Device ID: esser01 Port ID: Fa |
| 798 | 273.522377 | Cisco_e1:e7:cf | CDP/VTP/DTP/PAgP/UDLD | CDP | Device ID: esser01 Port ID: Fa |
| 962 | 333.519278 | Cisco_e1:e7:cf | CDP/VTP/DTP/PAgP/UDLD | CDP | Device ID: esser01 Port ID: Fa |
| 1132 | 393.521842 | Cisco_e1:e7:cf | CDP/VTP/DTP/PAgP/UDLD | CDP | Device ID: esser01 Port ID: Fa |
| 1288 | 453.538248 | Cisco_e1:e7:cf | CDP/VTP/DTP/PAgP/UDLD | CDP | Device ID: esser01 Port ID: Fa |
| 1468 | 513.548136 | Cisco_e1:e7:cf | CDP/VTP/DTP/PAgP/UDLD | CDP | Device ID: esser01 Port ID: Fa |
| 1675 | 573.587405 | Cisco_e1:e7:cf | CDP/VTP/DTP/PAgP/UDLD | CDP | Device ID: esser01 Port ID: Fa |
| 1897 | 633.584109 | Cisco_e1:e7:cf | CDP/VTP/DTP/PAgP/UDLD | CDP | Device ID: esser01 Port ID: Fa |
| 2080 | 693.618773 | Cisco_e1:e7:cf | CDP/VTP/DTP/PAgP/UDLD | CDP | Device ID: esser01 Port ID: Fa |

**Trafico CLDAP**



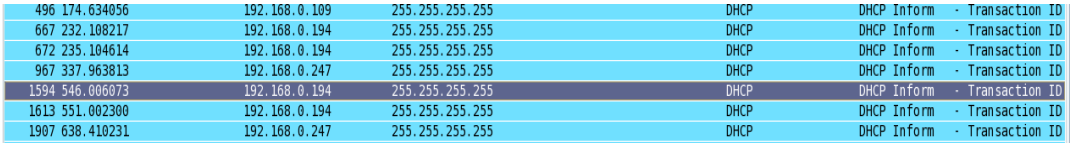
| | | | | |
|---|---|---|---|---|
| 66233 | 548.878333 | 192.168.0.65 | 192.168.0.13 | CLDAP searchResEntry(92) "<ROOT>" se |
| 66266 | 549.019268 | 192.168.0.13 | 192.168.0.65 | CLDAP searchRequest(93) "<ROOT>" bas |
| 66267 | 549.019929 | 192.168.0.65 | 192.168.0.13 | CLDAP searchResEntry(93) "<ROOT>" se |
| 102703 | 849.474773 | 192.168.0.13 | 192.168.0.65 | CLDAP searchRequest(94) "<ROOT>" bas |
| 102704 | 849.475579 | 192.168.0.65 | 192.168.0.13 | CLDAP searchResEntry(94) "<ROOT>" se |
| 139657 | 1150.053122 | 192.168.0.13 | 192.168.0.65 | CLDAP searchRequest(95) "<ROOT>" bas |
| 139658 | 1150.054094 | 192.168.0.65 | 192.168.0.13 | CLDAP searchResEntry(95) "<ROOT>" se |
| 235069 | 2104.626676 | 192.168.0.13 | 192.168.0.65 | CLDAP searchRequest(96) "<ROOT>" bas |
| 235072 | 2104.627745 | 192.168.0.65 | 192.168.0.13 | CLDAP searchResEntry(96) "<ROOT>" se |

### Tráfico DCERPC



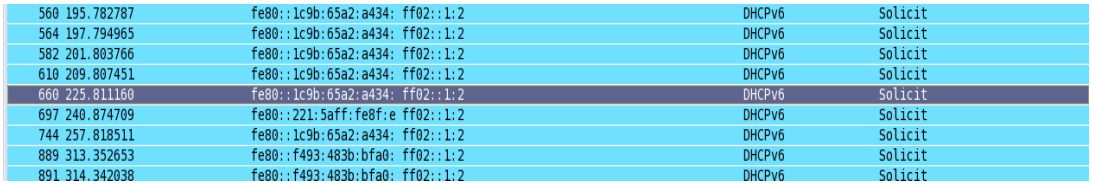
| | | | | |
|---|---|---|---|---|
| 50263 413.561731 | 192.168.0.66 | 192.168.0.13 | DCERPC | Response: call_id: 189 ctx_id: |
| 50306 414.562575 | 192.168.0.13 | 192.168.0.66 | DCERPC | Request: call_id: 191 opnum: 0 |
| 65888 547.241523 | 192.168.0.13 | 192.168.0.65 | DCERPC | Bind: call_id: 1 EPMv4 V3.0 |
| 65889 547.242211 | 192.168.0.65 | 192.168.0.13 | DCERPC | Bind_ack: call_id: 1 accept ma |
| 65903 547.295816 | 192.168.0.13 | 192.168.0.65 | DCERPC | Bind: call_id: 1 DRSUAPI V4.0 |
| 65906 547.297752 | 192.168.0.65 | 192.168.0.13 | DCERPC | Bind_ack: call_id: 1 accept ma |
| 65907 547.297969 | 192.168.0.13 | 192.168.0.65 | DCERPC | Alter context: call_id: 1 DRSU |

### Trafico DHCP



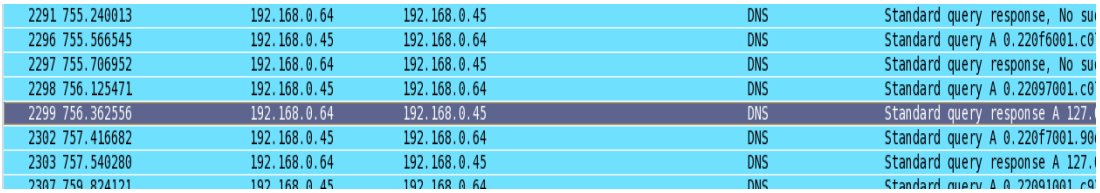
| | | | | |
|---|---|---|---|---|
| 496 174.634056 | 192.168.0.109 | 255.255.255.255 | DHCP | DHCP Inform - Transaction ID |
| 667 232.108217 | 192.168.0.194 | 255.255.255.255 | DHCP | DHCP Inform - Transaction ID |
| 672 235.104614 | 192.168.0.194 | 255.255.255.255 | DHCP | DHCP Inform - Transaction ID |
| 967 337.963813 | 192.168.0.247 | 255.255.255.255 | DHCP | DHCP Inform - Transaction ID |
| 1594 546.006073 | 192.168.0.194 | 255.255.255.255 | DHCP | DHCP Inform - Transaction ID |
| 1613 551.002300 | 192.168.0.194 | 255.255.255.255 | DHCP | DHCP Inform - Transaction ID |
| 1907 638.410231 | 192.168.0.247 | 255.255.255.255 | DHCP | DHCP Inform - Transaction ID |

### Trafico DHCP versión 6



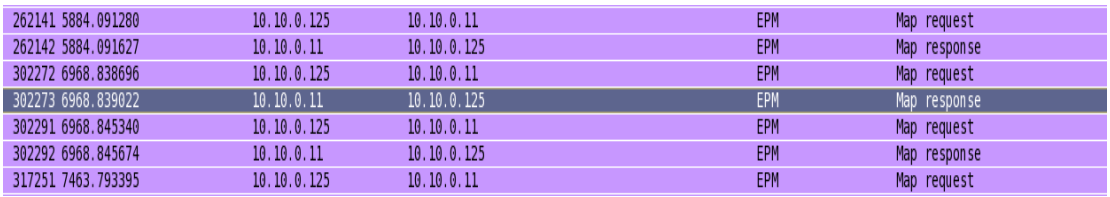
| | | | |
|---|---|---|---|
| 560 195.782787 | fe80::1c9b:65a2:a434: | ff02::1:2 | DHCPv6 | Solicit |
| 564 197.794965 | fe80::1c9b:65a2:a434: | ff02::1:2 | DHCPv6 | Solicit |
| 582 201.803766 | fe80::1c9b:65a2:a434: | ff02::1:2 | DHCPv6 | Solicit |
| 610 209.807451 | fe80::1c9b:65a2:a434: | ff02::1:2 | DHCPv6 | Solicit |
| 660 225.811160 | fe80::1c9b:65a2:a434: | ff02::1:2 | DHCPv6 | Solicit |
| 697 240.874709 | fe80::221:5aff:fe8f:e | ff02::1:2 | DHCPv6 | Solicit |
| 744 257.818511 | fe80::1c9b:65a2:a434: | ff02::1:2 | DHCPv6 | Solicit |
| 889 313.352653 | fe80::f493:483b:bfa0: | ff02::1:2 | DHCPv6 | Solicit |
| 891 314.342038 | fe80::f493:483b:bfa0: | ff02::1:2 | DHCPv6 | Solicit |

### Trafico DNS



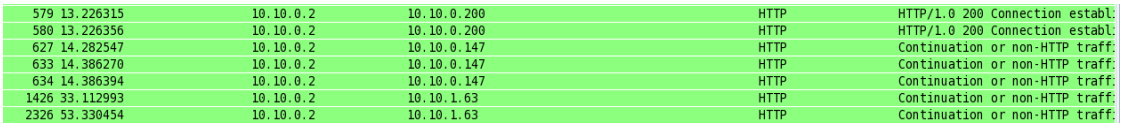
| | | | | |
|---|---|---|---|---|
| 2291 755.240013 | 192.168.0.64 | 192.168.0.45 | DNS | Standard query response, No su |
| 2296 755.566545 | 192.168.0.45 | 192.168.0.64 | DNS | Standard query A 0.220f6001.c0 |
| 2297 755.706952 | 192.168.0.64 | 192.168.0.45 | DNS | Standard query response, No su |
| 2298 756.125471 | 192.168.0.45 | 192.168.0.64 | DNS | Standard query A 0.22097001.c0 |
| 2299 756.362556 | 192.168.0.64 | 192.168.0.45 | DNS | Standard query response A 127. |
| 2302 757.416682 | 192.168.0.45 | 192.168.0.64 | DNS | Standard query A 0.220f7001.90 |
| 2303 757.540280 | 192.168.0.64 | 192.168.0.45 | DNS | Standard query response A 127. |
| 2307 759.824121 | 192.168.0.45 | 192.168.0.64 | DNS | Standard query A 0.22091001.c9 |

### Trafico EPM



| | | | | |
|---|---|---|---|---|
| 262141 5884.091280 | 10.10.0.125 | 10.10.0.11 | EPM | Map request |
| 262142 5884.091627 | 10.10.0.11 | 10.10.0.125 | EPM | Map response |
| 302272 6968.838696 | 10.10.0.125 | 10.10.0.11 | EPM | Map request |
| 302273 6968.839022 | 10.10.0.11 | 10.10.0.125 | EPM | Map response |
| 302291 6968.845340 | 10.10.0.125 | 10.10.0.11 | EPM | Map request |
| 302292 6968.845674 | 10.10.0.11 | 10.10.0.125 | EPM | Map response |
| 317251 7463.793395 | 10.10.0.125 | 10.10.0.11 | EPM | Map request |

### Trafico HTTP



| | | | | |
|---|---|---|---|---|
| 579 13.226315 | 10.10.0.2 | 10.10.0.200 | HTTP | HTTP/1.0 200 Connection establ: |
| 580 13.226356 | 10.10.0.2 | 10.10.0.200 | HTTP | HTTP/1.0 200 Connection establ: |
| 627 14.282547 | 10.10.0.2 | 10.10.0.147 | HTTP | Continuation or non-HTTP traff: |
| 633 14.386270 | 10.10.0.2 | 10.10.0.147 | HTTP | Continuation or non-HTTP traff: |
| 634 14.386394 | 10.10.0.2 | 10.10.0.147 | HTTP | Continuation or non-HTTP traff: |
| 1426 33.112993 | 10.10.0.2 | 10.10.1.63 | HTTP | Continuation or non-HTTP traff: |
| 2326 53.330454 | 10.10.0.2 | 10.10.1.63 | HTTP | Continuation or non-HTTP traff: |

## Trafico ICAP

| | | | | |
|---|---|---|---|---|
| 2549 58.239388 | 10.10.0.11 | 10.10.0.196 | ICAP | Continuation |
| 88431 1923.122650 | 10.10.0.2 | 10.10.0.223 | ICAP | Continuation |
| 88432 1923.122774 | 10.10.0.2 | 10.10.0.223 | ICAP | Continuation |
| 88433 1923.122872 | 10.10.0.2 | 10.10.0.223 | ICAP | Continuation |
| 144061 2938.259664 | 10.10.0.11 | 10.10.0.196 | ICAP | [TCP Previous segment lost] Co |
| 152120 3058.259790 | 10.10.0.11 | 10.10.0.196 | ICAP | [TCP Previous segment lost] Co |
| 189046 3718.260653 | 10.10.0.11 | 10.10.0.196 | ICAP | [TCP Previous segment lost] Co |
| 264041 5938.263782 | 10.10.0.11 | 10.10.0.196 | ICAP | [TCP Previous segment lost] Co |

## Trafico ICMP

| | | | | |
|---|---|---|---|---|
| 263104 5910.622575 | 10.10.0.125 | 10.10.0.11 | ICMP | Destination unreachable (Port |
| 263632 5926.623171 | 10.10.0.125 | 10.10.0.11 | ICMP | Destination unreachable (Port |
| 264234 5944.622469 | 10.10.0.125 | 10.10.0.11 | ICMP | Destination unreachable (Port |
| 264965 5970.866965 | 10.10.0.11 | 10.10.0.125 | ICMP | Destination unreachable (Port |
| 265021 5972.366915 | 10.10.0.11 | 10.10.0.125 | ICMP | Destination unreachable (Port |
| 265073 5973.866873 | 10.10.0.11 | 10.10.0.125 | ICMP | Destination unreachable (Port |

## Trafico IGMP

| | | | | |
|---|---|---|---|---|
| 948 328.834282 | 192.168.3.3 | 224.0.0.1 | IGMP | V2 Membership Query, general |
| 960 333.451378 | 192.168.20.200 | 239.255.255.250 | IGMP | V2 Membership Report / Join gr |
| 1289 453.809940 | 192.168.3.3 | 224.0.0.1 | IGMP | V2 Membership Query, general |
| 1291 454.447123 | 192.168.20.200 | 239.255.255.250 | IGMP | V2 Membership Report / Join gr |
| 1687 578.786242 | 192.168.3.3 | 224.0.0.1 | IGMP | V2 Membership Query, general |
| 1705 585.442596 | 192.168.20.200 | 239.255.255.250 | IGMP | V2 Membership Report / Join gr |
| 2138 703.762679 | 192.168.3.3 | 224.0.0.1 | IGMP | V2 Membership Query, general |
| 2167 712.438161 | 192.168.20.200 | 239.255.255.250 | IGMP | V2 Membership Report / Join gr |
| 2503 828.737072 | 192.168.3.3 | 224.0.0.1 | IGMP | V2 Membership Query, general |

## Trafico IP

| | | | | |
|---|---|---|---|---|
| 63446 1372.071793 | 10.10.0.208 | 255.255.255.255 | IP | Fragmented IP protocol (proto= |
| 63575 1375.061332 | 10.10.0.208 | 255.255.255.255 | IP | Fragmented IP protocol (proto= |
| 63714 1378.046411 | 10.10.0.208 | 255.255.255.255 | IP | Fragmented IP protocol (proto= |
| 63861 1381.041782 | 10.10.0.208 | 255.255.255.255 | IP | Fragmented IP protocol (proto= |
| 82404 1789.996046 | 10.10.0.219 | 255.255.255.255 | IP | Fragmented IP protocol (proto= |
| 82540 1792.972930 | 10.10.0.219 | 255.255.255.255 | IP | Fragmented IP protocol (proto= |
| 176885 3441.776334 | 10.10.0.208 | 255.255.255.255 | IP | Fragmented IP protocol (proto= |

## Trafico LLMNR

| | | | | |
|---|---|---|---|---|
| 790 272.163112 | 192.168.0.12 | 224.0.0.252 | LLMNR | Standard query A Chicagua |
| 791 272.263187 | fe80::e9a9:e4b3:6874: | ff02::1:3 | LLMNR | Standard query A Chicagua |
| 792 272.263251 | 192.168.0.12 | 224.0.0.252 | LLMNR | Standard query A Chicagua |
| 1746 600.179697 | fe80::1c9b:65a2:a434: | ff02::1:3 | LLMNR | Standard query ANY ESSIS007 |
| 1747 600.279451 | fe80::1c9b:65a2:a434: | ff02::1:3 | LLMNR | Standard query ANY ESSIS007 |
| 1766 604.155092 | fe80::1c9b:65a2:a434: | ff02::1:3 | LLMNR | Standard query A Chicagua |
| 1767 604.257104 | fe80::1c9b:65a2:a434: | ff02::1:3 | LLMNR | Standard query A Chicagua |
| 2061 690.151878 | fe80::f493:483b:bfa0: | ff02::1:3 | LLMNR | Standard query A isatap |
| 2062 690.254007 | fe80::f493:483b:bfa0: | ff02::1:3 | LLMNR | Standard query A isatap |

## Trafico LDAP

| | | | | |
|---|---|---|---|---|
| 302315 6968.855933 | 10.10.0.11 | 10.10.0.125 | LDAP | bindResponse(79) success |
| 302316 6968.856148 | 10.10.0.125 | 10.10.0.11 | LDAP | SASL GSS-API Integrity: searchR |
| 302317 6968.856444 | 10.10.0.11 | 10.10.0.125 | LDAP | SASL GSS-API Integrity: searchR |
| 302318 6968.856586 | 10.10.0.125 | 10.10.0.11 | LDAP | SASL GSS-API Integrity: searchR |
| 302319 6968.856956 | 10.10.0.11 | 10.10.0.125 | LDAP | SASL GSS-API Integrity: searchR |
| 302320 6968.857138 | 10.10.0.125 | 10.10.0.11 | LDAP | SASL GSS-API Integrity: searchR |
| 302324 6968.858683 | 10.10.0.11 | 10.10.0.125 | LDAP | SASL GSS-API Integrity: searchR |

## Trafico LLC

| | | | | | |
|---|---|---|---|---|---|
| 251911 | 5507.995052 | IntelCor_90:cb:30 | Broadcast | LLC | S P, func=RNR, N(R)=64; DSAP Nl |
| 252696 | 5547.535631 | IntelCor_90:cb:30 | Broadcast | LLC | S P, func=RNR, N(R)=64; DSAP Nl |
| 252752 | 5550.220576 | IntelCor_90:cb:30 | Broadcast | LLC | S P, func=RNR, N(R)=64; DSAP Nl |
| 252753 | 5550.248724 | IntelCor_90:cb:30 | Broadcast | LLC | S P, func=RNR, N(R)=64; DSAP Nl |
| 253283 | 5569.446755 | IntelCor_90:cb:30 | Broadcast | LLC | S P, func=RNR, N(R)=64; DSAP Nl |
| 253679 | 5586.317593 | IntelCor_90:cb:30 | Broadcast | LLC | S P, func=RNR, N(R)=64; DSAP Nl |
| 253795 | 5592.476470 | IntelCor_90:cb:30 | Broadcast | LLC | S P, func=RNR, N(R)=64; DSAP Nl |

## Trafico NBIPX

| | | | | |
|---|---|---|---|---|
| 4179 | 94.189124 | 00000000.000ffe3ace52 | 00000000.ffffffffffff | NBIPX | Find name 104-08<20> |
| 4214 | 95.158962 | 00000000.000ffe3ace52 | 00000000.ffffffffffff | NBIPX | Find name 104-08<20> |
| 4246 | 96.033873 | 00000000.000ffe3ace52 | 00000000.ffffffffffff | NBIPX | Find name 104-08<20> |
| 4280 | 96.907848 | 00000000.000ffe3ace52 | 00000000.ffffffffffff | NBIPX | Find name 104-08<20> |
| 4509 | 101.814085 | 00000000.000ffe3ace52 | 00000000.ffffffffffff | NBIPX | Find name 104-08<20> |
| 4552 | 102.689010 | 00000000.000ffe3ace52 | 00000000.ffffffffffff | NBIPX | Find name 104-08<20> |
| 4587 | 103.565511 | 00000000.000ffe3ace52 | 00000000.ffffffffffff | NBIPX | Find name 104-08<20> |
| 4747 | 107.518730 | 00000000.000ffe3ace52 | 00000000.ffffffffffff | NBIPX | Find name 104-08<20> |

## Trafico NBNS

| | | | | | |
|---|---|---|---|---|---|
| 70 | 19.957647 | 192.168.0.124 | 192.168.0.255 | NBNS | Name query NB CHICAGUA<00> |
| 74 | 20.722062 | 192.168.0.124 | 192.168.0.255 | NBNS | Name query NB CHICAGUA<00> |
| 129 | 43.122979 | 192.168.0.152 | 192.168.0.255 | NBNS | Name query NB ZACON03<20> |
| 131 | 43.873003 | 192.168.0.152 | 192.168.0.255 | NBNS | Name query NB ZACON03<20> |
| 133 | 44.622919 | 192.168.0.152 | 192.168.0.255 | NBNS | Name query NB ZACON03<20> |
| 182 | 66.613667 | 192.168.0.124 | 192.168.0.255 | NBNS | Name query NB CHICAGUA<00> |

## Trafico SMB

| | | | | | |
|---|---|---|---|---|---|
| 15159 | 125.004552 | 192.168.0.13 | 192.168.0.90 | SMB | Write Response, FID: 0x4009, 1( |
| 15158 | 125.004518 | 192.168.0.90 | 192.168.0.13 | SMB | Write Request, FID: 0x4009, 10 |
| 15157 | 125.002159 | 192.168.0.13 | 192.168.0.90 | SMB | Write Response, FID: 0x4009, 8 |
| 15156 | 125.002129 | 192.168.0.90 | 192.168.0.13 | SMB | Write Request, FID: 0x4009, 8 I |
| 15155 | 125.000493 | 192.168.0.13 | 192.168.0.90 | SMB | Write Response, FID: 0x4009, 1( |
| 15154 | 125.000460 | 192.168.0.90 | 192.168.0.13 | SMB | Write Request, FID: 0x4009, 10 |
| 15153 | 124.998101 | 192.168.0.13 | 192.168.0.90 | SMB | Write Response, FID: 0x4009, 8 |
| 15152 | 124.998072 | 192.168.0.90 | 192.168.0.13 | SMB | Write Request, FID: 0x4009, 8 I |

## Trafico SSDP

| | | | | | |
|---|---|---|---|---|---|
| 103 | 35.248826 | 192.168.0.79 | 239.255.255.250 | SSDP | NOTIFY * HTTP/1.1 |
| 104 | 35.249798 | 192.168.0.79 | 239.255.255.250 | SSDP | NOTIFY * HTTP/1.1 |
| 105 | 35.251730 | 192.168.0.79 | 239.255.255.250 | SSDP | NOTIFY * HTTP/1.1 |
| 154 | 55.265251 | 192.168.0.79 | 239.255.255.250 | SSDP | NOTIFY * HTTP/1.1 |
| 155 | 55.266369 | 192.168.0.79 | 239.255.255.250 | SSDP | NOTIFY * HTTP/1.1 |
| 156 | 55.268539 | 192.168.0.79 | 239.255.255.250 | SSDP | NOTIFY * HTTP/1.1 |
| 157 | 55.269599 | 192.168.0.79 | 239.255.255.250 | SSDP | NOTIFY * HTTP/1.1 |

## Trafico STP

| | | | | | |
|---|---|---|---|---|---|
| 174 | 62.519300 | 3comEuro_c9:0e:8b | Spanning-tree-(for-bridges)_00 | STP | MST. Root = 32768/0/00:04:0b:6 |
| 178 | 64.529556 | 3comEuro_c9:0e:8b | Spanning-tree-(for-bridges)_00 | STP | MST. Root = 32768/0/00:04:0b:6 |
| 181 | 66.539527 | 3comEuro_c9:0e:8b | Spanning-tree-(for-bridges)_00 | STP | MST. Root = 32768/0/00:04:0b:6 |
| 187 | 68.539523 | 3comEuro_c9:0e:8b | Spanning-tree-(for-bridges)_00 | STP | MST. Root = 32768/0/00:04:0b:6 |
| 191 | 70.558970 | 3comEuro_c9:0e:8b | Spanning-tree-(for-bridges)_00 | STP | MST. Root = 32768/0/00:04:0b:6 |
| 199 | 72.569249 | 3comEuro_c9:0e:8b | Spanning-tree-(for-bridges)_00 | STP | MST. Root = 32768/0/00:04:0b:6 |
| 202 | 74.589734 | 3comEuro_c9:0e:8b | Spanning-tree-(for-bridges)_00 | STP | MST. Root = 32768/0/00:04:0b:6 |
| 210 | 76.604201 | 3comEuro_c9:0e:8b | Spanning-tree-(for-bridges)_00 | STP | MST. Root = 32768/0/00:04:0b:6 |

## Trafico TCP

| | | | | | |
|---|---|---|---|---|---|
| 540462 | 5484.586862 | 192.168.0.90 | 192.168.0.13 | TCP | [TCP segment of a reassembled F |
| 540463 | 5484.587843 | 192.168.0.90 | 192.168.0.13 | TCP | [TCP segment of a reassembled F |
| 540464 | 5484.587863 | 192.168.0.13 | 192.168.0.90 | TCP | microsoft-ds > 1028 [ACK] Seq= |
| 540467 | 5484.592999 | 192.168.0.90 | 192.168.0.13 | TCP | [TCP segment of a reassembled F |
| 540468 | 5484.593925 | 192.168.0.90 | 192.168.0.13 | TCP | [TCP segment of a reassembled F |
| 540469 | 5484.593942 | 192.168.0.13 | 192.168.0.90 | TCP | microsoft-ds > 1028 [ACK] Seq= |

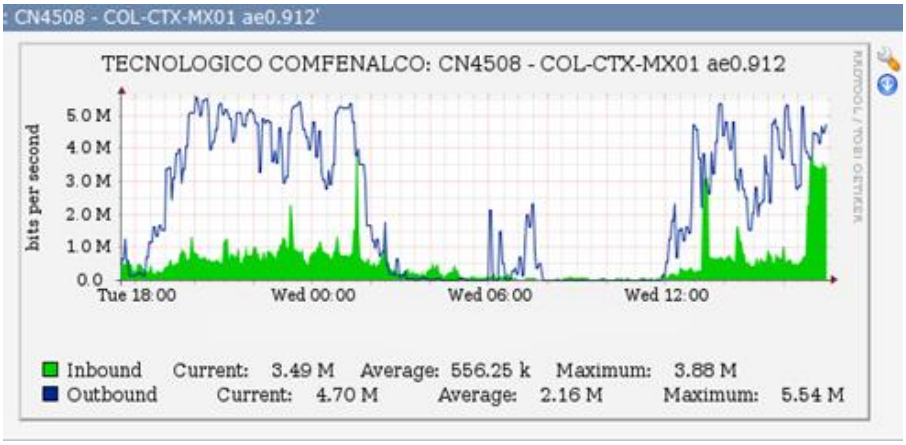
**Trafico UDP**

| | | | | |
|---|---|---|---|---|
| 85 25.462209 | 192.168.0.121 | 255.255.255.255 | UDP | Source port: neod2 Destinatio |
| 93 30.462952 | 192.168.0.121 | 255.255.255.255 | UDP | Source port: neod2 Destinatio |
| 108 35.459001 | 192.168.0.121 | 255.255.255.255 | UDP | Source port: neod2 Destinatio |
| 123 40.459698 | 192.168.0.121 | 255.255.255.255 | UDP | Source port: neod2 Destinatio |
| 134 45.471836 | 192.168.0.121 | 255.255.255.255 | UDP | Source port: neod2 Destinatio |
| 146 50.461222 | 192.168.0.121 | 255.255.255.255 | UDP | Source port: neod2 Destinatio |

### *4.9.2 Diagrama de internet*

Tal como se mencionó anteriormente, la institución cuenta con dos proveedores del servicio de internet que son Columbus y Telecom, con el primero de ellos se tiene contratado un ancho de banda de 5 Mbps y con el segundo de 4 Mbps. La grafica que muestra el consumo de internet en ambas sedes es la siguiente (figura 3):

Figura 5. Consumo de Internet




De acuerdo a lo mostrado en la gráfica podemos resaltar la aparición de unos picos altos de consumo sobrepasando los 5 Mbps, del total del ancho de banda de Columbus network, lo cual genera una disminución en el rendimiento del servicio prestado al usuario final reflejándose en tiempos de respuesta indeseados además de saturación en la red sobre todo en el horario nocturno.

### *4.9.3 Análisis de cargas*

El análisis de tráfico se realizó en las sedes España y Zaragocilla. La muestra para recolección de tráfico fue del 60% e incluyó al 90 % de los servidores ubicados en la sede principal y al 99% de los equipos activos administrables.

La sede principal ubicada en el barrio España cuenta con switches 4500, 4500G 3com, 4200 marca 3com, Next, Hubs 3com, planet y Encore. Los conmutadores 4500 son de Nivel 3 y los 4200 3com, planet y Next son de nivel 2.

Los grupos administrativo y académico se encuentran asociados a una VLAN diferente cada uno (vlan 2, Vlan 4), adicionalmente existe una VLAN (vlan 3) usada para transportar tráfico de unas pasarelas voz (ATA) entre las dos sedes.

El acceso a la red pública se recibe a través de 2 operadores: TELECOM (4Mbps) vía router Cisco 3800 y COLUMBUS (5Mbps). Ambos enlaces físicos se integran a la plataforma de comunicaciones de la institución a través de 2 switches 3com 4500 que se conectan en cascada con los 4 switches principales de la capa de núcleo de la red.

En la sede España, se cuenta con 100 estaciones de trabajo Dell que hacen parte del grupo administrativo, 30 estaciones adicionales ubicadas en la biblioteca y en el área de derecho.

La sede principal se interconecta a la sede Zaragocilla ubicada a 870 Metros aproximadamente, a través de un enlace de radio en la banda de los 2.4Ghz implementado con equipos tipo indoor marca Linksys serie WAP54G basados en el estándar 802.11g.

En la sede Zaragocilla se cuenta con 20 estaciones de trabajo marca Dell que hacen parte del grupo administrativo y con 120 estaciones de trabajo ubicadas en las salas de informática que hacen parte del grupo académico.

Tabla 3. Índice de tráfico promedio

| | | | |
|---|---|---|---|
| Avg Frame | 64 | Frame s/s | Sube a 96 |
| Avg Size | 374 | Bytes | |
| Trafico WS: | 23.936 | Bytes/seg | |
| #WS*SW1 | 24 | puertos | |

De acuerdo con el grafico anterior observamos que el trafico promedio por estación de trabajo en este grupo es de 23,936 Bytes / segundo equivalente a 191,488 bits/segundo. Nótese que tanto el número de tramas promedio como el tamaño de las mismas varían con respecto al trafico académico, incluso varían entre sí para el tráfico administrativo y de los servidores. La respuesta a este comportamiento se debe a que los PAYLOAD tanto de ethernet como de muchos protocolos de capa superior son variables.

Siendo que la sede principal cuenta con 100 estaciones de trabajo más 30 ubicadas en biblioteca:

Tabla 4. Medición de tráfico

| Sede principal España | | | |
|---|---|---|---|
| #Ws | 130 | | |
| #Frames Sede /s | 8320 | Frames/seg | |
| #Bytes Sede /s | 4.779.540.480 | Bytes/seg | 4.8 GBps |
| #bits Sede /s | 38.236.323.840 | bits/seg | 38.3 Gbps |

Considerando que los conmutadores 3com tienen capacidades de conmutación de 128Gbps (4500G) y 8.8 Gbps (4500/4200) y teniendo en cuenta que los servidores se encuentran directamente conectados a un 4500G pero las estaciones que consumen sus recursos se encuentran conectadas 4500 Fast ethernet y 4200, puede afirmarse que el tráfico generado excede en 29,5 Gbps, la capacidad de la plataforma de conmutación de la serie 4200 y 4500 fastEthernet en situaciones de alto tráfico.

Aunque el conmutador 4500G 3com tiene capacidad de conmutar 128Gbps, el resto de los switches que posee la institución, lo hace a 8.8Gbps generando la saturación de las colas (memoria), incrementando el tiempo de cpu al 95% lo que se refleja en la pérdida de tramas y paquetes que de incluir segmentos TCP incrementan los niveles de congestión debido a la retransmisión de los mismos como parte de la implementación confiable del protocolo.

En condiciones de distribución de tráfico normalizado, la capacidad de canal requerida se distribuye entre los switches generando necesidades de 7.1 Gbps conmutables por los switches de la sede principal, tal como puede apreciarse en la siguiente tabla:

Tabla 5. Capacidad de canal requerida

| Sede principal España | | |
|---|---|---|
| #Sw | 5 | unidades |
| Trafico x Sw | 7.059.013.632 | 7.1 Gbps |
| | | |
| | | |

Para la sede Zaragocilla los resultados son los detallados a continuación:

Tabla 6. Índice de tráfico promedio Zaragocilla

| Sede Zaragocilla | | | |
|---|---|---|---|
| #Ws | 20 | | |
| #Frames Sede/s | 1.280 | frames s/s | |
| #Bytes sedes/s | 478.720 | Byte s/s | |
| #bits sede/s | 3.829.760 | bist/s | 3.8 Mbps |

Las 20 estaciones asociadas a la Vlan Administrativa generan 1.280 Tramas por segundo con un tamaño promedio de 374 Bytes para una capacidad de canal requerida de 3.830 Mbps.

Considerando esta situación podría afirmarse que la capacidad de conmutación de los switches de esta sede es aceptable con relación a las necesidades de trafico de las estaciones de trabajo, en situaciones en las cuales casi el 100% de los usuarios soliciten/usen recursos de forma concurrente. No obstante, la presencia de Hubs incrementa el tráfico innecesariamente y permite la aparición de colisiones en situaciones de acceso concurrente.

En condiciones de tráfico distribuido, la capacidad de conmutación estaría dada por la información de la siguiente tabla:

Tabla 7. Capacidad de conmutación

| Sede Zaragocilla | | |
|---|---|---|
| # sw/hubs | 1 | unidades |
| trafico x sw | 3.829.760 | 3,8 Mbps |
| #hubs | 0 | unidades |
| # sw | 1 | unidades |

El tráfico del segmento administrativo puede clasificarse de la siguiente forma:

Tabla 8. Trafico Administrativo

| | | |
|---|---|---|
| ARP/Broadcast | 25,0% | |
| IP | 73,0% | |
| TCP en IP | 62,8% | |
| NetBIOS en UDP | 10,2% | |
| Otros | 2,0% | |
| Total | **100,0%** | |
| | | |
| Trafico Total | 38.240.153.600 | 38.3Gbps |
| Broadcast Zarag. | 957.440 | 1.4 Mbps |
| Broadcast Espa. | 9.559.080.960 | 9.5 Gbps |
| Broadcast Total | 9.560.038.400 | 9.6 Gbps |
| Trafic No Broad Zar. | 2.872.320 | 2.8Mbps |

Puede apreciarse que el 25% del tráfico es de Broadcast, siendo de 1.4Mbps en la sede zaragocilla y de 9.5Gbps en la sede España en condiciones de alto tráfico. Considerando esta situación puede obtenerse que los requerimientos de trafico Unicast son de 28.6 Gbps (considerando las respuestas de los servidores a los clientes en Zaragocilla e incluyendo trafico innecesario unicast como CDP,STP,IPv6, etc.

### *4.9.4 Equipos activos*

Tabla 9. Equipos activos

| EQUIPOS ACTIVOS | | | |
|---|---|---|---|
| SWITCHES | | | |
| FABRICANTE | 3COM | 4500G/4500/4200 | |
| VERSION OS | v3.03.00556 | | |
| FLASH | 8196 | Kb | |
| DRAM | 64 | MB | |
| QUEUE | 0-7 | ROUND ROBIN | |
| CAPACIDAD DE SWICHING | 128Gbps/8.8Gpbs | | |
| INTERCONEXION | Cascada | | |
| | | | |
| COMPORTAMIENTO CON TRAFICO | | | |
| Memoria Usada | 38% | 3114,48 | kb |
| Memoria Disponible | 62% | 5081,52 | kb |
| Tamaño CAM | 298 DIR. MAC | | |
| Tramas descarte prom. | 37% | 15,91 | Tramas |
| Tramas Entregadas Éxito | 63% | 27,09 | Tramas |

Se observa que en condiciones de no congestión, el porcentaje de memoria principal usada es del 38% (para tareas del sistema operativo) y que le promedio de tramas descartadas es del 37% (bastante altas para condiciones normales). El porcentaje de uso de las colas gira alrededor del 90% en situaciones de alto tráfico para los switches 4500 fast Ethernet, 4200 3com y superior para NEXT y Planet.

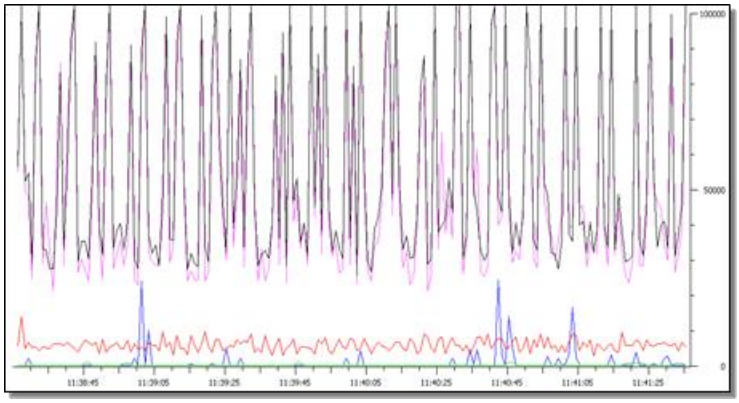
### *4.9.5 Enlace inalámbrico entre las dos sedes*

Tabla 10. Equipos Wireless

| **Equipos Wireless** | | | |
|---|---|---|---|
| Linksys Wap54G | 13 dbm | -84 dBm | |
| Estandar | 802.11 g | 54Mpbs | indoor |
| Antenas | Grilla | 24 dbi | |

Los equipos utilizados para interconectar ambas sedes son tipo INDOOR (No para soluciones inalámbricas a la intemperie) de manera que la exposición a temperaturas elevadas genera ruido térmico como efecto negativo para las comunicaciones. Incluso el hardware pobre de estos equipos genera retardo de procesamiento, que se ve reflejado en la una pobre calidad de experiencia de uso del servicio por parte de los usuarios. Adicionalmente, aunque el estándar 802.11G defina operación a 54Mbps como valor teórico, la capacidad de canal real es de 30Mbps promedio. La situación se empeora debido a que los equipos están operando como bridges permitiendo que todo el tráfico de Broadcast de ambas sedes se propague por el enlace generando un incremento exponencial en los requerimientos de capacidad de canal que inducen a caídas periódicas de la solución.

Figura 6. Trafico Broadcast



En el grafico anterior se observa que el tráfico de broadcast (En color Negro), supera en muchas situaciones los 10000 paquetes.

## 4.10 Recomendaciones a partir del análisis de tráfico

Las sugerencias a continuación relacionadas, apuntan mejorar el nivel de rendimiento en la red corporativa asi como también la disponibilidad de la misma, atendiendo a las falencias detectadas durante el análisis de tráfico:

- Se propone hacer un diseño de tipo jerárquico, que facilite implementación, gestión y escalamiento de la red.
- Se propone segmentar la red administrativa en Vlans facilitándose el trabajo en grupos lógicos. Además de lo anteriormente citado, la segmentación implica el control de tráfico de broadcast lo cual reduce el consumo de capacidad de canal.
- Se propone Eliminar los hubs y switches nos administrables presentes en la red debido al problema creciente a nivel de broadcast.
- Implementar políticas de acceso a internet en el servidor proxy que restrinjan la utilización de recursos de alto consumo siempre y cuando no hagan parte de las herramientas de trabajo de los usuarios.
- Proponer la compra de equipos activos administrables que permitan monitorear el tráfico a partir de agentes SNMP.

# 5 DISEÑO FISICO DE LA RED

Se propone el uso de Switch multicapa para implementar la distribución en la red, entendiendo como Switches multicapas aquellos con la capacidad genérica de usar información de diferentes capas de protocolo como parte del proceso de conmutación de datos (switching) y enrutamiento avanzado.

Considerando buenas prácticas de diseño se plantea entonces el esquema para la actualización de la Red de LA FUNDACION UNIVERSITARIA TECNOLOGICO COMFENALCO basado en Switches de acceso de la nueva serie 2960S que poseen alternativamente conexiones a 10 Gbps que permitirá interconectarse con el Switch de distribución de la red (4507R E).

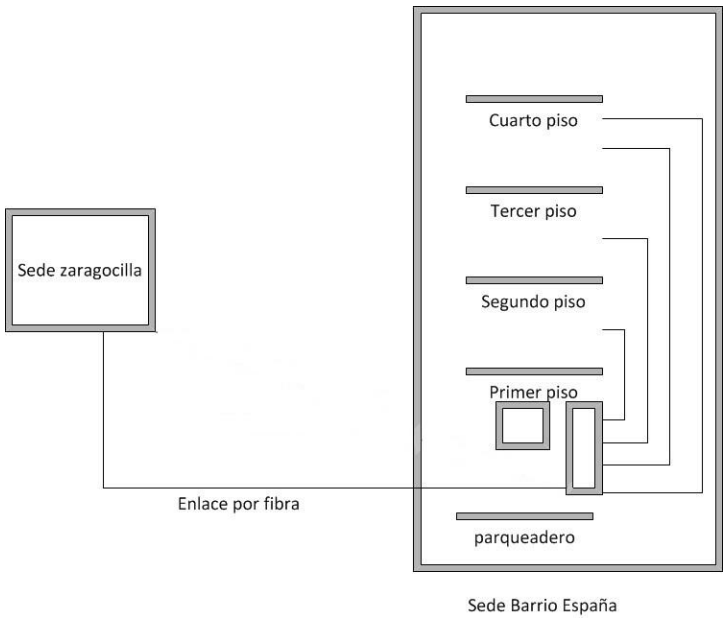
La función del núcleo o Core está directamente asociada al proveedor del servicio es decir el ISP que maneja la conectividad de la red corporativa con el exterior (Wan).

Para la segmentación de dominios de colisión y funcionalidades de capa de acceso confiable a la red, la recomendación es el uso de Switches de la nueva serie de Switches Cisco 2960S Estos nuevos Switches 2960S poseen además una gran funcionalidad como es el APILAMIENTO de hasta 4 unidades con el fin de verse como si fuera 1 solo equipo de 192 puertos, mejorando las capacidades y el desempeño operativo de la red de LA FUNDACION UNIVERSITARIA TECNOLOGICO COMFENALCO. Igualmente permiten realizar conexiones a 1Gbit (hasta 4 puertos) asegurando altas velocidades de transferencia de datos.

El Switch Cisco de la serie 4507R E que usaremos para cumplir la función de distribución, tiene capacidad de 7 slots (Bahias para insertar tarjetas de conexiones y servicios), una supervisora 6E Lite (Tarjeta administradora de la plataforma) una alternativa de redundancia para alta disponibilidad, que garantiza conectividad en alto desempeño (cuenta además con 2 slot 10G o 4 Ptos 1Gb por módulo TwinGig), fuentes de poder redundante de 1300 W (alimentación eléctrica), cuatro (4) tarjeta de 48 puertos 10/100/1000 sobre cobre una de las cuales posee alimentación Power over Ethernet Plus para equipos a 1GB PoE, preparando la infraestructura para tecnologías de alto consumo de recursos y de seguridad. Con esta alternativa se ofrece una escalabilidad mejorada y capacidades de enrutamiento mejoradas con inspección de protocolos.

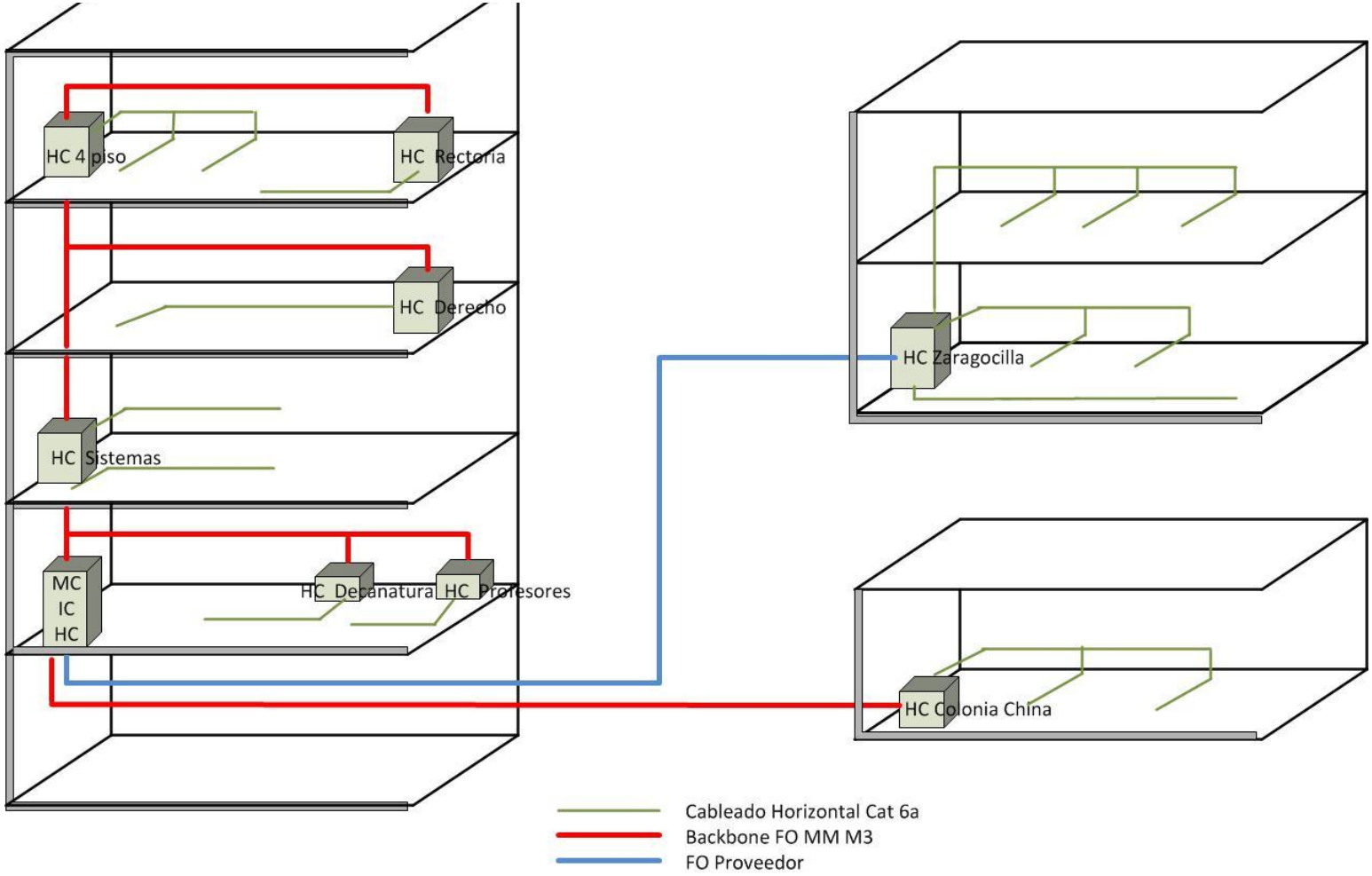
De acuerdo a lo anteriormente expuesto, se propone el siguiente esquema general para el diseño físico de la red:

Figura 7. Esquema general propuesto red Futco



## DISEÑO FISICO RED CORPORATIVA

Figura. 8. Diseño físico propuesto red Futco. Ver anexo 5

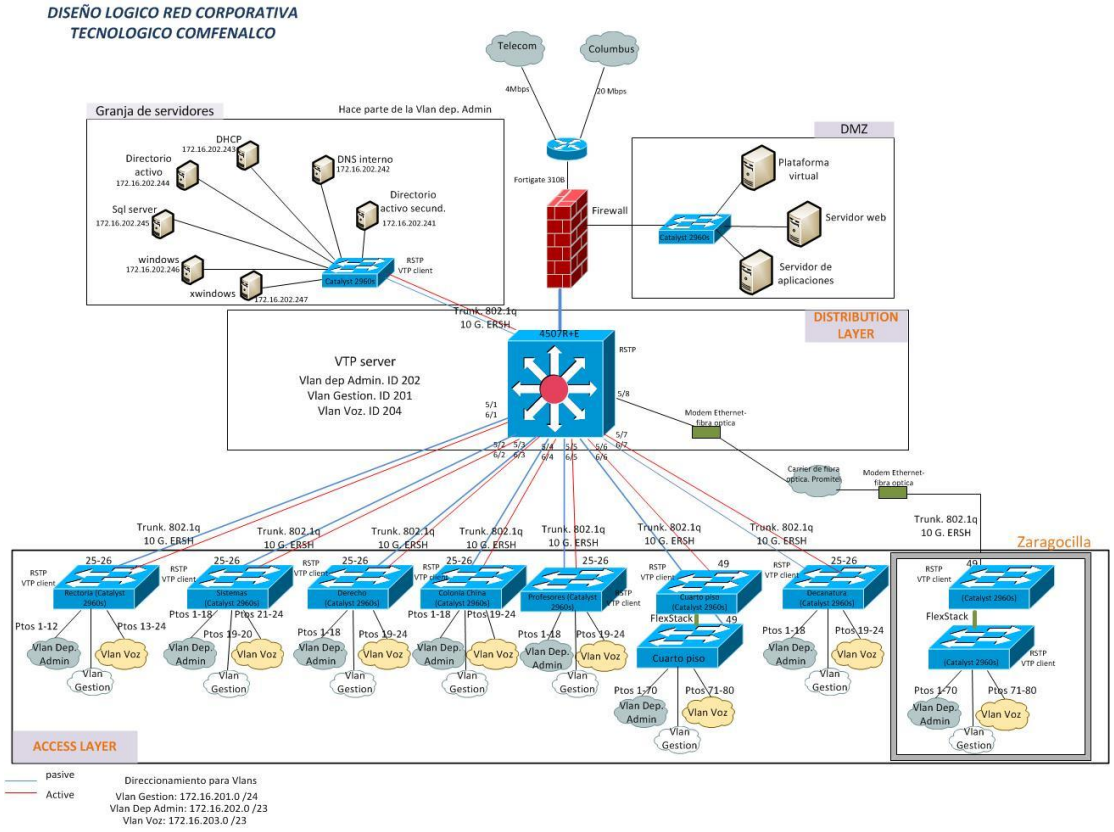


El switch de distribución 4507R+E cumple con la función de filtrar e identificar los flujos de información que circulan por la red utilizando para ello políticas tales como filtrado basado en puertos, rutas estáticas, seguridad y calidad de servicio.

Los switches 2960 conforman la **capa de acceso** cumpliendo con la función de proveer conectividad, acceso local de usuario a la red de LA FUNDACION UNIVERSITARIA TECNOLOGICO COMFENALCO y a sus servicios tecnológicos integrales.

# 6 DISEÑO LOGICO DE LA RED

Figura 9. Diseño Lógico propuesto Red Futco. Ver anexo 5



## 6.1 Segmentación de Broadcast

El rendimiento de la red es un factor determinante en la productividad de la Universidad y una de las estrategias que contribuye al excelente rendimiento de la red es la división de los grandes dominios de broadcast, en dominios más pequeños con el uso de las VLAN. Los dominios de broadcast más pequeños limitan el número de dispositivos que participan en los broadcasts y permiten que los dispositivos se separen en agrupaciones funcionales.

Una VLAN (acrónimo de Virtual LAN, 'Red de Área Local Virtual') es un método para crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del Dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa, servicios, etc.) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un Switch Multicapa).

En el anexo 6 se detalla el direccionamiento para una de las siguientes Vlans:

- Vlan de gestión ID 201
- Vlan dependencias Administrativas ID 202
- Vlan de VoIP ID 204

### *6.1.1 Vlan de Gestion*

Esta vlan, se utiliza para asignar la configuración de cada uno de los dispositivos de forma remota, lo que incluye monitoreo de los mismos.

Direccionamiento IP: 172.16.201.0/24
Gateway: 172.16.201.10

### *6.1.2 Vlan de VoIP*

Permite gestionar los servicios de telefonía sobre protocolo IP a los diferentes usuarios de la red.

Direccionamiento IP: 172.16.204.0/23
Gateway: 172.16.204.10

### *6.1.3 Vlan dependencias Administrativas*

Gestiona los servicios que los usuarios necesitan para el desempeño de sus labores diarias.

Direccionamiento IP: 172.16.202.0/23
Gateway: 172.16.202.50

## 6.2 Descripción distribución lógica para cada switch

### *6.2.1 Switch Rectoría: Cisco 2960. 24 puertos*

Puertos 25 y 26: puertos troncales. Conexión por fibra óptica
Puertos 1-12: se usan para conectar a los usuarios de la Vlan Dependencias administrativas. ID de Vlan 202
Puertos 13-24: usados para dar servicio de telefonía IP. Id de Vlan 204.
Hace distribución a los puertos 5/1 y 6/1

### *6.2.2 Switches 4° piso: Flexstack. 2 switches Cisco 2960. 96 puertos en total.*

Puertos 49 ambos switches: puertos troncales. Conexión por fibra óptica.
Puertos 1-48 y 50-70: se usan para conectar a los usuarios de la Vlan Dependencias administrativas. ID de Vlan 202
Puertos 71-80 : usados para dar servicio de telefonía IP. Id de Vlan 204.
Hace distribución a los puertos 5/6 y 6/6

### *6.2.3 Switch derecho: Cisco 2960. 24 puertos*

Puertos 25 y 26: puertos troncales. Conexión por fibra óptica
Puertos 1-18: se usan para conectar a los usuarios de la Vlan Dependencias administrativas. ID de Vlan 202
Puertos 19-24: usados para dar servicio de telefonía IP. Id de Vlan 204.
Hace distribución a los puertos 5/3 y 6/3

### *6.2.4 Switch Colonia china. Cisco 2960. 24 puertos*

Puertos 25 y 26: puertos troncales. Conexión por fibra óptica
Puertos 1-18: se usan para conectar a los usuarios de la Vlan Dependencias administrativas. ID de Vlan 202
Puertos 19-24: usados para dar servicio de telefonía IP. Id de Vlan 204.
Hace distribución a los puertos 5/4 y 6/4

### *6.2.5 Switches sala de profesores y decanatura. 2 switches Cisco de 24 puertos cada uno.*

Puertos 25 y 26: puertos troncales en ambos switches. Conexión por fibra óptica
Puertos 1-18 en ambos switches: se usan para conectar a los usuarios de la Vlan Dependencias administrativas. ID de Vlan 202
Puertos 19-24 en ambos switches: usados para dar servicio de telefonía IP. Id de Vlan 204.
Switch sala de profesores: Hace distribución a los puertos 5/5 y 6/5
Switch sala de decanatura: Hace distribución a los puertos 5/7 y 6/7

### *6.2.6 Switch sistemas*

Puertos 25 y 26: puertos troncales. Conexión por fibra óptica
Puertos 1-18: se usan para conectar a los usuarios de la Vlan Dependencias administrativas. ID de Vlan 202
Puertos 19 y 20: usados para realizar la gestión de la red
Puertos 21-24: usados para dar servicio de telefonía IP. Id de Vlan 204.
Hace distribución a los puertos 5/2 y 6/2

### *6.2.7 Switches sede Zaragocilla: 2 switch de acceso 2960 de 48 puertos cada uno.*

Puertos 1-35 de switch 1 y switch2: se usan para conectar a los usuarios de la Vlan Dependencias administrativas. ID de Vlan 202.
Puertos 36-40 en switch 1 y switch2: usados para dar servicio de telefonía IP. Id de Vlan 204.
Hace distribución a los puertos 5/8

La conexion entre los dos switches de acceso se da a través de un modulo Flex Stack. La conexión de los switches de acceso de la sede Zaragocilla con el switch de distribución ubicado en la sede España se dá por fibra óptica contratada con un proveedor externo (canal Lan to Lan).

## 6.3 Switch de Distribución : switch Cisco 4507R+E

El Switch Cisco de la serie 4507R E con capacidad de 7 slots (Bahías para insertar tarjetas de conexiones y servicios), tiene dos supervisoras 7E Lite (Tarjeta administradora de la plataforma) una alternativa de redundancia para alta disponibilidad, que garantiza conectividad en alto desempeño, fuentes de poder redundante de 1300 W (alimentación eléctrica), cuatro (4) tarjeta de 48 puertos 10/100/1000 sobre cobre una de las cuales posee alimentación Power over Ethernet Plus para equipos a 1GB PoE, preparando la infraestructura para tecnologías de alto consumo de recursos y de seguridad. Con esta alternativa se ofrece una mayor escalabilidad y capacidades de enrutamiento mejoradas con inspección de protocolos.

Este switch permite el filtrado de tráfico a través Backbone 10Gb entre los centros de administración de datos de LA FUNDACION UNIVERSITARIA. Como valor agregado, se maneja la configuración de la topología de la Red aprovechando la infraestructura actual que permita parámetros de configuración como la agregación de enlaces, sistemas de redundancia Capa 2 con RSTP y ERSH, para el control de loops (ciclos interminables de información entre dispositivos de red), sobre los dispositivos de red que lo soporten.

El switch de distribución maneja protocolo VTP server que permite la declaración de las Vlan que agruparan a los usuarios de la red. Estas vlan se reflejan en cada uno de los VTP client (switches de acceso) donde deben asignarse los puertos que correspondan a cada una de ellas.

Tabla 11. Descripción switches

| Nombre | Modelo | Marca | Numero de Puertos | Uplinks | FlexStack Data Stacking |
|---|---|---|---|---|---|
| SW_Distribucion | 4507 R+E | Cisco | | | |
| **SW Rectoria** | **WS-C2960S-24PD-L** | **Cisco** | **24** | **2 x 10G** | **Si** |
| SW Sistemas | WS-C2960S-24PD-L | Cisco | 24 | 3 x 10G | Si |
| **SW Derecho** | **WS-C2960S-24PD-L** | **Cisco** | **24** | **4 x 10G** | **Si** |
| SW Colonia China | WS-C2960S-24PD-L | Cisco | 24 | 5 x 10G | Si |
| **SW Profesores** | **WS-C2960S-24PD-L** | **Cisco** | **24** | **6 x 10G** | **Si** |
| SW Cuarto Piso | WS-C2960S-48FPD-L | Cisco | 48 | 7 x 10G | Si |
| **SW Cuarto Piso** | **WS-C2960S-48FPD-L** | **Cisco** | **48** | **8 x 10G** | **Si** |
| SW Decanatura | WS-C2960S-24PD-L | Cisco | 24 | 9 x 10G | Si |
| **SW Zaragocilla** | **WS-C2960S-48FPD-L** | **Cisco** | **48** | **10 x 10G** | **Si** |
| SW Zaragocilla | WS-C2960S-48FPD-L | Cisco | 48 | 11 x 10G | Si |

***Granja de servidores:*** provee los siguientes servicios a los usuarios de la red: autenticación a través de directorio activo primario y secundario, direccionamiento Ip a través del servidor DHCP, DNS interno, servidor de base de datos y servicios de Intranet.

**DMZ:** zona desmilitarizada. A través de las reglas determinadas en el firewall, da acceso a los usuarios internos al servidor de aplicaciones, servidor web y plataforma virtual. Los usuarios externos acceden a esta zona a través de la web y en este caso el firewall hace el re direccionamiento de la IP pública a una privada mediante un puerto específico.

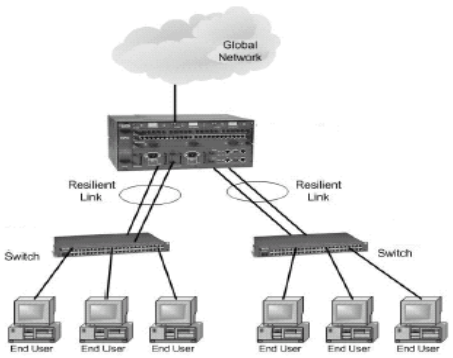
Los enlaces redundantes se manejan con el protocolo RSTP cuya función es la de monitorear el estado de todas las trayectorias:

- Si una dirección activa se cae, RSTP activa las direcciones redundantes.
- Configura de nuevo la topología de la red adecuadamente.

**ERSH** (Resilient link single home) tiene como función proteger los enlaces críticos y evitar los periodos de inactividad cuando los enlaces fallan. Consiste en un enlace principal y uno secundario que en conjunto forman un enlace resistente. Si el enlace principal falla, el secundario inmediatamente entra a cumplir el rol de principal. Este tipo de enlace puede operar entre un switch y cualquier otro dispositivo de red como un router o un servidor, proporcionando redundancia que evita fallas en la red por causa de los enlaces existentes.

Durante el funcionamiento normal, el principal puerto está habilitado y el puerto en espera está desactivado. Si el enlace principal falla, el puerto principal está desactivado y el puerto en espera está activado. Si el enlace principal entra en funcionamiento, el usuario puede volver a habilitar el puerto principal y desactivar el modo de espera.

Figura 10. Funcionamiento ERSH



## 6.4 Comunidad SNMP

SNMP (Single Network Management Protocol) es un estándar de administración de red. SNMP proporciona un método de gestión de nodos de red (Servidores, estaciones de trabajo, routers, puentes y concentradores) desde un NMS (Network Management Station).

SNMP utiliza una estructura de agentes en todos los elementos que administra. El NMS conecta con los agentes SNMP instalados en los elementos que serán administrados. Toda la información del equipo está en una base de datos MIB (Management Information Base). Esta base de datos es recogida por el agente SNMP y comunicada al NMS. SNMP puede utilizarse de varias maneras:
*Para configurar dispositivos remotos*: desde el NMS configuramos los equipos.
*Para supervisar el rendimiento de la red*: se puede hacer un seguimiento de la velocidad de la red.
*Para detectar fallos de red*: Puede llevar una alarma al NMS cuando se apague un dispositivo o cuando se detecte un error de enlace con un router.

La arquitectura de administración de red está compuesta por los siguientes elementos:

**Estación de administración (NMS):**

Es la interfaz del administrador de red en el sistema, mantiene una base de datos denominada MIB.

**Agente de administración:**

Es el proceso que corre en los dispositivos que están siendo monitoreados, routers, switches, etc. El agente SNMP responde a las solicitudes de información del sistema de administración. Cualquier equipo donde se ejecute el software de agente SNMP es un agente SNMP. El servicio SNMP responde a las solicitudes de información de uno o varios sistemas de administración. Puede configurarse para determinar qué estadísticas se están siguiendo y qué sistemas de administración están autorizados a solicitar información.

**Base de información de administración (MIB):**

Es una base de datos organizada por objetos o variables y sus atributos o valores, que contiene información del estado y es actualizada por los agentes.

A través de la MIB se tiene acceso a la información para la gestión, contenida en la memoria interna del dispositivo monitoreado. Mib es una base de datos completa y bien definida, con una estructura en árbol, adecuada para manejar diversos grupos de objetos con identificadores exclusivos para cada objeto

El objetivo de la creación de una comunidad SNMP en el Tecnológico Comfenalco es monitorear el estado de cada uno de los dispositivos networking que hacen parte de la red corporativa. En cada uno de ellos se habilitará un agente SNMP que reportará información a un equipo administrador SNMP que hará parte de la Vlan de Gestión.

Dentro de las ventajas del uso de la comunidad SNMP podemos citar:

- Estado del procesador
- Estado de buffers
- Estado de las tablas CAM
- Temperatura de los equipos
- Recepción de señales de alerta

A partir de lo anteriormente citado, el administrador de la plataforma podrá tomar decisiones oportunas que eviten al máximo la no disponibilidad de la red.

# 7 CONSIDERACIONES FINALES

Producto del desarrollo de esta monografía, presentamos las siguientes conclusiones:

- La migración del modelo de red clásico al modelo de tres capas reviste una ventaja importante para la fundación universitaria Tecnológico Comfenalco porque facilita la implementación, mantenimiento, confiabilidad y escalabilidad de la red. Todos estos factores decisivos para el funcionamiento actual y la proyección a futuro de un claustro universitario con demanda creciente a nivel local y regional.

- La redundancia debe ser entendida como una forma habitual de manejar la disponibilidad por lo cual lejos de ser vista como una inversión innecesaria de recursos debe asociarse con el salvavidas de una arquitectura de red. Protocolos como RSTP se encargan de la administración de los enlaces redundantes entre dispositivos garantizando la disponibilidad cuando se presentan fallas.

- Dentro de las principales ventajas del modelo propuesto se encuentra la administración de la infraestructura de red, proceso que abarca desde el monitoreo a los dispositivos networking, aplicación de nuevas configuraciones, monitoreo de puertos y activación de protocolos hasta el suministro de información que permita al administrador de la red la planificación de mantenimientos preventivos y correctivos según sea necesario.

- La separación de los tráficos de voz y datos brinda un componente importante a nivel de seguridad de la información así como también de calidad de servicio. Al viajar la voz y los datos por caminos separados se minimiza la el riesgo de captura de tramas de voz en caso de ataques a la red.

- La organización del modelo de red en grupos funcionales facilita el flujo de información a nivel de capa de acceso y distribución permitiendo a esta ultima proveer ruteo, filtrado, acceso a la red WAN y selección de los paquetes que deben llegar al core.

# 8 LISTA DE ANEXOS

**Anexo N° 1:** Inventario software

**Anexo N° 2:** Encuesta percepción de servicio usuario final

**Anexo N° 3:** Tabulación encuesta usuario final

**Anexo N° 4:** Encuesta técnica

**Anexo N° 5:** Diseño físico y diseño lógico de la red

**Anexo N° 6:** Direccionamiento para Vlans

# 9 INDICE DE TABLAS

**Tabla 1. Inventario equipos red FUTCO……....14**
**Tabla 2. Descripción de servidores……..17**
**Tabla 3. Índice de trafico promedio……28**
**Tabla 4. Medición de trafico……29**
**Tabla 5. Capacidad de canal requerida……29**
**Tabla 6. Índice de trafico promedio Zaragocilla……..30**
**Tabla 7. Capacidad de conmutación……..30**
**Tabla 8. Tráfico administrativo……30**
**Tabla 9. Equipos activos……31**
**Tabla 10. Equipos wireless……31**
**Tabla 11. Descripción switches……..42**

## 10 INDICE DE FIGURAS

**Figura 1. Protocolo RSTP……..9**
**Figura 2. Organigrama división de tecnologías**
**De la información y comunicaciones……..13**
**Figura 3. Organigrama FUTCO……14**
**Figura 4. Diseño actual de la red FUTCO……19**
**Figura 5. Consumo de internet……...27**
**Figura 6. Tráfico de Broadcast……32**
**Figura 7. Esquema general propuesto red FUTCO…….35**
**Figura 8. Diseño físico propuesto red FUTCO…….36**
**Figura 9. Diseño lógico propuesto red FUTCO……38**
**Figura 10. Funcionamiento ERSH…….43**

## 11 BIBLIOGRAFIA

Beltran Moura, Jose. Redes locales de Computadores. Ed. Mc Graw Hill. Mexico, 2005.

Dvrack, Jhon C. Telecomunicaciones para PC. Ed. Mc Graw Hill. Mexico, 2001.

Gibbs, Mark. Redes para todos. Ed. Prentice Hall. Mexico, 1998.

Gonzalez Says, Nestor. Comunicaciones y redes de procesamiento de datos. Ed. Mc Graw Hill. Mexico, 2008.

Tanenbaum, Andrew. Redes de ordenadores. Ed. Prentice Hall. Mexico, 2005.

Torres Nieto, Alvaro. Comunicaciones y telemática. Ed. Prentice Hall. Mexico, 2005

Glister, Ron. Construya su propia red. Ed. Prentice Hall. Mexico, 2009.

Stallings, William. Comunicaciones y redes de computadoras. Ed. Prentice Hall. Madrid, 2006.

Forouzan, Behrouz. Transmisión de datos y redes de comunicaciones. Ed. Mc Graw Hill. Mexico, 2002.

Inc. Cisco System. Academia de Networking de Cisco System, Guia del primer año CCNA 1 y 2. Cisco Press. 2000.

Inc. Cisco System. Academia de Networking de Cisco System, Guia del segundo año CCNA 3 y 4. Cisco Press. 2000.