UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO
UNIDAD DE POSGRADO

MAESTRÍA EN CONECTIVIDAD Y REDES DE ORDENADORES

Tesis previa la obtención del Grado Académico de Magíster en Conectividad y Redes de Ordenadores

TEMA:

"LA CONECTIVIDAD EN LA RED LÓGICA Y SU INCIDENCIA EN LA GESTIÓN POR PROCESOS DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO. 2013." IMPLEMENTACIÓN DE REDES LAN VIRTUALES.

AUTOR:

STALIN DANIEL CARREÑO SANDOYA

ASESOR:

ING. BYRON WLADIMIR OVIEDO BAYAS, MSc.

QUEVEDO– LOS RIOS- ECUADOR

2015

UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO
UNIDAD DE POSGRADO

MAESTRÍA EN CONECTIVIDAD Y REDES DE ORDENADORES

Tesis previa la obtención del Grado Académico de Magíster en Conectividad y Redes de Ordenadores

TEMA:

"LA CONECTIVIDAD EN LA RED LÓGICA Y SU INCIDENCIA EN LA GESTIÓN POR PROCESOS DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO. 2013." IMPLEMENTACIÓN DE REDES LAN VIRTUALES.

AUTOR:

STALIN DANIEL CARREÑO SANDOYA

ASESOR:

ING. BYRON WLADIMIR OVIEDO BAYAS, MSc.

QUEVEDO– LOS RIOS- ECUADOR

2015

CERTIFICACIÓN

Ing. Byron Wladimir Oviedo Bayas, MSc., Docente Tutor de la Tesis, previo a la obtención del Título Académico de Magíster en Conectividad y Redes de Ordenadores

C E R T I F I C A

Que el Ing. Stalin Daniel Carreño Sandoya, ha cumplido con la elaboración de la de Tesis titulada: **"LA CONECTIVIDAD EN LA RED LÓGICA Y SU INCIDENCIA EN LA GESTIÓN POR PROCESOS DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO. 2013." IMPLEMENTACIÓN DE REDES LAN VIRTUALES.**

El mismo que está apto para la presentación y sustentación respectiva.

Ing. Byron Wladimir Oviedo Bayas, MSc.

DOCENTE- ASESOR

AUTORÍA

Los criterios ideas, comentarios, conclusiones y recomendaciones son de mi autoría, excepto aquellos referentes que se encuentran debidamente citados.

Asumo la responsabilidad por el contenido de esta investigación

Stalin Daniel Carreño Sandoya

Autor

DEDICATORIA

Para Natalie Daniela, Hilda Daniela, Stalin Manuel (+), Fausto Andrés y Nimio Stalin.

AGRADECIMIENTO

A la Universidad Técnica Estatal de Quevedo, por acogerme en su seno en toda mi formación profesional, desde el pregrado (Tecnología y la Ingeniería) brindarme la oportunidad de incrementar mi formación a través del Programa de Maestría: “CONECTIVIDAD Y REDES DE ORDENADORES”. A todos los docentes que transfirieron sus conocimientos, por sus valiosos aportes durante la escolaridad de la maestría. A mis compañeros de maestría, por compartir sus reflexiones y experiencias.

PROLOGO

En las redes Lan, se procura que estén los servicios de red siempre disponibles, dentro de estos servicios, el más importante y más usado en las instituciones de carácter público, es el Internet, ya que a través de este se accede a muchos otros servicios, y más aún que en la actualidad el Gobierno Nacional ha implementado muchas plataforma informáticas Online que permiten una gobernabilidad de las instituciones del sector gobierno, razón más que importante para disponer de una infraestructura de red robusta, segura y que tenga una alta disponibilidad para los usuarios de la misma.

La Universidad Técnica Estatal de Quevedo, al haber implementado su nueva estructura organizacional por procesos, ha requerido cambio en su estructura de red, es por esta razón que el autor del presente trabajo propone una nueva estructura de red y la implementa, considerando los procesos actuales ya en ejecución, la estructura que se implanta es la de usar redes virtuales, es decir VLANS.

El segmentar las redes en porciones más pequeñas, permiten administrar de mejor forma a sus usuarios y servicios, aislando problemas que permitan una rápida detección e inmediata corrección del mismo, sin que esto afecte el rendimiento de otras redes, es decir buscar siempre que los servicios estén disponibles, y es así que el autor cuida de que se cumplan estos requisitos y los propone en su diseño, el mismo que está en funcionamiento.

Ing. Sist. Jorge W. Saa Saltos, Msc.

CI. 1202444574
REG. SENESCYT NRO.
1014-08-843172
1006-13-86035323

RESUMEN EJECUTIVO

La Universidad Técnica Estatal de Quevedo, expidió el Estatuto de Gestión Organizacional por Procesos, el mismo que es aprobado en segunda y definitiva instancia el 24 de Enero de 2012, una vez que el Ministerio de Relaciones Laborales con fecha de Agosto 16 de 2011 emite el informe favorable para su aplicación.

Ante este cambio de estructura organizacional, se vio conveniente administrar la red de datos de tal forma que ajuste a estos cambios sin que afecte el rendimiento y sea transparente para el usuario final, dentro de las ventajas de la institución es que cuenta con una estructura de comunicaciones robusta tanto en su parte activa como pasiva que permitió realizar una estructura lógica que se ajustó a la estructura organizacional por procesos.

Se implementaron redes virtuales (VLAN) para cada sector y para cada servicio en el ámbito de las redes, es así que se crearon redes virtuales para la parte Administrativa, académica, Laboratorios de computación, así como las redes inalámbricas, con esta organización de hace más fácil llevar a cabo la administración de la red y de poder agregar servicios sin ninguna afectación a su rendimiento.

Para el acceso a Internet de cada Vlan se virtualizo los servidores, utilizando XenCenter y como plataforma de Gateway el Sistema operativo ClearOS el mismo que permitió administrar el servicio de internet y establecer seguridades en cada red virtual.

ABSTRACT

The University of Quevedo, issued the Statute Organizational Process Management, the same that is approved in second and final instance on January 24, 2012, once the Ministry of Labour Relations dated August 16, 2011 issued by the report favorable to its application.

Given this change in organizational structure, was convenient to administer the data network so that fits these changes without affecting performance and is transparent to the end user, in the benefits of the institution it is that it has a structure robust communications both active and passive part which allowed for a logical structure that is adjusted to the organizational structure processes.

Virtual networks (VLAN) for each sector and for each service in the field of networks were implemented, so that virtual networks for the administrative part, academic, computer labs and wireless networks were created, this organization ago easier to carry out the administration of the network and to add services without affecting its performance.

For Internet access each VLAN servers using XenCenter as Gateway platform ClearOS operating system that allowed it to manage Internet service and establishing securities in each virtual network is virtualized.

INDICE GENERAL

Pág.

Pág.

INDICE DE TABLAS

Pág

Pág

INDICE DE FIGURAS

Pág.

Pág.

INTRODUCCION.

Una red de área local virtual (VLAN) es una subdivisión de una red de área local en la capa de enlace de datos de la pila de protocolo TCP/IP. Se pueden crear redes VLAN para redes de área local que utilicen tecnología de nodo. Al asignar los grupos de usuarios en redes VLAN, puede mejorar la administración de red y la seguridad de toda la red local. También puede asignar interfaces del mismo sistema a redes VLAN diferentes.

Es recomendable dividir una red de área local en redes VLAN cuando se requiere que se cree una división lógica de grupos de trabajo, cuando se desee designar diferentes directivas de seguridad para los grupos de trabajo y cuando se requiera dividir los grupos de trabajo en dominios de difusión administrables.

El uso de redes VLAN reduce el tamaño de los dominios de emisión y mejora la efectividad de la red.

Ante el crecimiento de la cantidad de nodos que cuenta la red de la Universidad Técnica Estatal de Quevedo, nace la necesidad de separar los nodos en redes virtuales más pequeñas, creando grupos homogéneos en base a la nueva estructura por procesos que se está implementando en la Institución, permitiendo de esta manera una mejor administración de los servicios de red con que se cuenta, en especial el Internet, que hoy en día es una herramienta indispensable de trabajo, tanto en el ámbito académico como administrativo y se la debe de administrar de tal manera que los usuarios se encuentren satisfechos en respuesta y puedan desarrollar sus actividades institucionales sin contratiempos.

En el capítulo I, donde podemos encontrar los preliminares de la tesis y se refiere básicamente al porque de la investigación y delimitar los objetivos del trabajo a realizar.

En el capítulo II, se revisan conceptos sobre las redes, haciendo énfasis en el objeto central del proyecto de tesis, Redes Virtuales.

El capítulo III, hace referencia a la Metodología de la Investigación, en donde se mencionan los métodos y las técnicas utilizadas para llevar a cabo el desarrollo de la tesis.

En el capítulo IV, se encuentra el desarrollo de la tesis, en donde se determinan los requerimientos para la implementación de las redes virtuales.

El capítulo V, abarca las conclusiones de la implementación y las respectivas recomendaciones.

CAPITULO I.

MARCO CONTEXTUAL DE LA INVESTIGACIÓN

1.1. Ubicación y Contextualización de la Problemática.

La Universidad Técnica Estatal de Quevedo está ubicada en el Km 1 ½ Vía Santo Domingo de los Tsáchilas en el Campus Ing. Manuel Haz Álvarez, fue creada mediante Decreto Legislativo, publicado en el Registro Oficial # 674 del 1 de febrero de 1984, con las Escuelas de Ingeniería Forestal, Ingeniería Zootécnica, Ingeniería en Administración de Empresas Agropecuarias, que han venido cumpliendo un rol muy importante en el desarrollo agropecuario del País y muy especialmente en su zona de influencia.

La Universidad empieza a incursionar en las tecnologías de las redes y comunicaciones en el año de 1998, cuando mediante convenio con la Secretaria Nacional de Ciencia y Tecnología SENECYT crea la Red Ecuatoriana de Ciencia y Tecnología REICYT, en la que las universidades del país debían compartir la información científica de investigaciones, tesis de grados y demás artículos científicos para ser difundidos en la web, tecnología que estaba entrando en boga en el país; para estos propósitos el REICYT donó equipos de comunicaciones tales como servidores, módems, hubs, switches, como contraparte la universidad debía de alquilar un servicio dedicado de internet, el mismo que se lo contrato con la empresa Puntonet con un enlace de última milla vía Modem, este enlace trabajaba a una velocidad de 24 Kbps y solamente se contaba con una cantidad muy limitada de equipos que podían accesar al internet. La universidad publico ese año su primer sitio web creado con el software de diseño de sitios web NetObject Fusion, donado por el REICYT, de la misma manera entro a funcionar el servidor de correos bajo la plataforma de Lotus Notes, ambos bajo el dominio uteq.edu.ec.

Ante los cambios de gobiernos desaparece el proyecto REICYT y es así que el 13 de diciembre del 2002, el Honorable Consejo Universitario aprobó la creación del instituto de informática para aportar con el desarrollo de nuevas tecnologías con altos estándares de calidad de servicio. Además esta unidad

de servicios, presta soporte a todos los departamentos que conforman la UTEQ, así como también lo hace a la comunidad externa a la institución. El Instituto de Informática está compuesto por las secciones de: Redes y Conectividad, Mantenimiento y Soporte Técnico, Laboratorios y Servicios y Desarrollo de Software, la sección encargada de administrar los servicios de redes y sus servicios es la sección de redes y comunicaciones.

En sus inicios la Sección de Redes y Comunicaciones proveía de los servicios de red a las diferentes dependencias de la universidad mediante cable UTP categoría 5, y es en ese año que se actualiza el enlace de internet de 24 Kbps a 256 Kbps clear channel 1:1 con la empresa Porta, ya para esta época se contaba con un laboratorio de internet con diez computadoras que era utilizado por los estudiantes de las facultades de Ciencias Agrarias y Ciencias Pecuarias, posteriormente se unió la reciente creada Facultad de Ciencias Empresariales, ya para ese entonces se incrementó el ancho de banda del internet a 1024 Kbps y así mismo se adquirieron nuevos equipos de cómputo para atender a la comunidad universitaria.

Actualmente antes los cambios de leyes y de nuevos modelos de administración, la Universidad adopta un nuevo estatuto basado en la gestión por procesos, en la cual se crean nuevas dependencias, dentro de estos cambios el Instituto de Informática pasa a ser la Unidad de Gestión de las TiC´s y con el proceso de Redes y Servicios TIC's, así mismo la institución al estar sujeta a una constante evaluación y para cumplir con estándares de calidad en el año 2012 se incrementó el ancho de banda a 100 Mbps.

La Universidad cuenta en la actualidad con un backbone de fibra óptica que permite la conectividad entre las diferentes dependencias de la universidad, así mismo posee conectividad con la Finca "La María" ubicada en el cantón Mocache, donde funciona la Facultad de Ciencias Pecuarias y la Unidad de Investigación, la conectividad con el campus "Manuel Haz Álvarez" se la realiza con un enlace de radio, de la misma manera se cuenta un enlace de radio para la conexión con la Finca "La Represa"

La comunidad universitaria ha estado en constate crecimiento y es así que en este año 2013 está conformada por 272 empleados (184 con Nombramiento, 36 contratados y 52 amparados en el código del Trabajo) y 427 Docentes (245 Docentes con nombramiento y 186 Docentes por contrato), Además la institución posee una población estudiantil de 8445 estudiantes matriculados en el periodo académico 2012 – 2013.

Ante el crecimiento de la comunidad universitaria y sobre todo al cambio de administración, se requiere restructurar la red lógica de la universidad, para que uso sea más eficiente, la administración sea más sencilla y eficaz, y sobre todo permita alcanzar los estándares requeridos para futuras acreditaciones.

1.2. Situación actual de la problemática.

La Universidad Técnica Estatal de Quevedo, cuenta con un Backbone de Fibra Óptica, el mismo que está distribuido en los diferentes departamentos del Campus Manuel Haz Álvarez, se cuenta con Switches Capa 2 marca Cisco, que permite dar servicios de red a las dependencias; como Switch de Core se cuenta con un equipo de capa 3 marca Cisco.

Actualmente se cuenta con dos redes lógicas, ambas /22, es decir 1022 host en cada una. Una presta servicio a la parte administrativa y la otra a los laboratorios de cómputo que son utilizados por los estudiantes.

La cantidad de host que se utilizan en la parte administrativa hace que la administración de la red se complique, de los inconvenientes a mencionar es la duplicidad de direcciones IP y un único segmento de colisión a nivel de toda la institución.

La Universidad cuenta con el servicio de Internet, el mismo que no está segmentado, esto es un inconveniente ya que siempre habrá usuarios que consuman más ancho de banda que otros, dejando a los demás usuarios con un ancho de banda mínimo causando un inconveniente a lo que si necesitan un

ancho de banda necesario para trabajar con aplicaciones en línea como son: Esigef, Esiprem, Quipux, Iess, Talento Humano, Etc.

En la actualidad la institución cuenta con un servicio de Internet de 100 Mbps, este ancho de banda debe de ser distribuido de forma proporcional a la cantidad de usuarios por facultades y en las diferentes dependencias.

De la misma forma no se cuenta con un sistema que permita el filtrado de contenidos de la web a nivel de la red administrativa, provocando esto que se utilice el servicio de internet para actividades ajenas a las actividades institucionales.

1.3. Problema de investigación

La Universidad Técnica Estatal de Quevedo requiere restructurar su red lógica que permita una administración centralizada, eficiente, eficaz y de fácil administración, aplicando normas y estándares que rigen las redes y comunicaciones así como la de organismo gubernamentales locales y nacionales.

¿DE QUE MANERA INCIDE EL USO DE REDES VIRTUALES EN LA GESTION POR PROCESOS DE LA UTEQ?

P1: ¿Cuántas subredes lógicas se necesitarían para cubrir a todas las dependencias de la institución?

P2: ¿Qué niveles de seguridad lógica se implementará en cada subred y el acceso a cada una de ellas?

P3: ¿Cuál será la forma de compartir el servicio de Internet entre las redes lógicas?

P4: ¿Como la separación en subredes influirá las comunicaciones en la institución?

1.4. Delimitación del problema

El objeto de estudio del presente proyecto abarca a la estructura de red de la Universidad Técnica Estatal de Quevedo, la misma que al haber adoptado una nueva estructura de gestión por procesos, esta debe de adaptarse a la misma, para lo cual se propone segmentar la red en redes Lan Virtuales (Vlan's) que agrupe los procesos en segmentos de red para una mejor administración, esta estructura se la implementará utilizando los recursos con lo que ya cuenta la institución en su red de área local existente

1.5. Justificación

La Universidad Técnica Estatal de Quevedo, se encuentra en la puesta en marcha del nuevo estatuto por procesos, el mismo que reestructura a la institución para estar acorde a los cambios nacionales en base a las leyes y reglamentos expedidos por la Ley Orgánica de Educación Superior (LOES) y la Ley Orgánica del Servicio Público (LOSEP), es así que los sistemas de redes que la universidad actualmente posee deben de adaptarse a estos cambios, los mismos que deben de ser transparentes para los usuarios finales.

El uso de redes virtuales (Vlan´s), permitiría separar la red en redes más pequeñas, fáciles de administrar, evitando duplicidad de direcciones, ya que al tener una subred con un rango extenso de direcciones ipv4 pueden causar inconvenientes al administrador al asignar un grupo de direcciones, se debe de considerar la seguridad, ya al estar todos los usuarios en una misma subred cada uno de ellos podría tener acceso a los recursos compartidos de cada usuario, otro punto a considerar es el acceso a internet, actualmente la institución posee un ancho de banda de 100 Mbps el mismo que está disponible para todos los usuarios, sin restricción alguna, es decir que si un usuario de la red utiliza un gestor de descarga o un algún software del tipo Per to Per (P2P) consumiría solamente él, un gran porcentaje del ancho de banda,

y por ende dejando a los usuarios que realmente requieren el servicio con una navegación lenta.

En la actualidad la mayoría de sistemas de información se encuentran en la nube (Internet), las instituciones tanto públicas como privadas han lanzado aplicaciones para que sus usuarios las utilicen y racionalicen su tiempo al realizar transacciones mucho más rápidas, es así que la universidad utiliza las aplicaciones del Ministerio de Economía y Finanzas eSigef y eSiprem, ahora SPRYM (Subsistema Presupuestario de Remuneraciones y Nomina), para la administración presupuestaria y los pagos tantos de nóminas como de proveedores de bienes y/o servicios, de la misma manera se utiliza el sistema de gestión documental Quipux, la institución quiere llegar a una gestión cero papeles, y por lo tanto cada funcionario involucrado en los diferentes procesos debe de tener acceso a la red para atender requerimientos y/o solicitudes enviadas por el sistema. La segmentación de la red actual en subredes, permitirá una mejor administración de los servicios de red, dándole a cada segmento lo necesario para que puedan realizar las diferentes actividades institucionales, así también permitirá al administrador de la red administrarla de una forma más dinámica y eficiente. La universidad cuenta con el hardware y software necesario para llevar a cabo esta propuesta.

1.6. Cambios esperados con la investigación

Red Lan de la Universidad Técnica Estatal de Quevedo, segmentada en subredes en base a los procesos establecidos.

- Comunidad Universitaria complacida con el acceso a la red y sus servicios.
- Administrador de la red con un sistema de gestión ordenada.

1.7. Objetivos

1.7.1. Objetivo General

- Evaluar la incidencia del uso de VLANS en la gestión por procesos de la UTEQ

1.7.2. Objetivos Específicos.

- Determinar la cantidad mínima de subredes para satisfacer a los nuevos procesos.
- Diseñar un esquema de red para una fácil gestión y administración.
- Determinar el ancho de banda adecuado para que cada proceso pueda ejecutarse sin inconvenientes.

CAPÍTULO II.

MARCO TEÓRICO

1.8. Fundamentación conceptual

1.8.1. Redes de Comunicaciones

Conjunto de enlaces de comunicaciones dispuestos de manera que es posible el envío de mensajes mediante su paso a través de muchos de aquéllos, con el fin de comunicar a un emisor y un receptor. Hay que observar que dentro de la definición de red de comunicaciones no se especifica qué hay en el extremo de los enlaces. Eso dependerá del tipo de red: ordenadores, teléfonos fijos o móviles, etc. Lo cual se debe al hecho de que el concepto de red de comunicaciones en realidad se remonta al siglo XIX, con inventos como el telégrafo o el teléfono. En contraposición, la aparición de los primeros ordenadores programables es bastante posterior, un siglo más tarde.

Aun así, es precisamente la aparición de los ordenadores lo que conforma el punto de partida de la explosión de las redes de comunicaciones. Aparece el fenómeno de la convergencia digital: la fusión gradual entre las tecnologías de comunicaciones y los ordenadores de manera que se genera un nuevo entorno en el que es posible intercambiar información entre diferentes tipos de dispositivos. Una vez cualquier dispositivo basado en procesador adquiere la capacidad de comunicarse con otros, las posibilidades se multiplican. Llegado al punto en que dos partes, como pueden ser dos ordenadores, se tienen que comunicar entre sí de manera autónoma, se hace imprescindible un protocolo de comunicaciones.

Un protocolo de comunicaciones es el conjunto de normas que definen el formato y el orden de los mensajes intercambiados entre dos o más entidades que se comunican entre sí, así como el conjunto de acciones que se toman durante la transmisión y la recepción de estos mensajes.

En realidad, siempre que dos entidades se quieren comunicar entre sí tienen que establecer un protocolo. Una analogía muy sencilla de esta definición es la comunicación que podrían tener dos personas con walkie-talkies. A fin de que la comunicación sea fluida hay que seguir dos normas: cuando se quiere ceder

el turno de palabra se dice la palabra “cambio” y cuando se quiere cerrar la conversación se dice “cambio y cierro”. Eso en sí es un protocolo de comunicaciones, aunque muy sencillo.

Con el fin de categorizar las redes de comunicaciones, hay diferentes sistemas: por el área de alcance, por el tipo de conexión, por la manera como se interconectan los diferentes dispositivos, por el tipo de servicios provistos, etc.

Como hilo inicial conductor, se utilizará la división por área de alcance:

• Red de área personal (PAN, Personal Area Network).

• Red de área local (LAN, Local Area Network).

• Red de área metropolitana (MAN, Metropolitan Area Network).

• Red de área extensa (WAN, Wide Area Network) (Arnedo Moreno, 2013).

LAN (Red de Área Local)

El término LAN (Local Area Network o red de área local) se aplica a una red de datos cuando los dispositivos unidos en dicha red se encuentran ubicados en un área geográfica limitada. Las distancias entre dispositivos conectados a una red de área local pueden variar entre unos pocos metros hasta varios cientos de metros o incluso kilómetros. En este caso, lo importante es que toda la infraestructura que forma la red pertenezca a una misma unidad organizativa, por ejemplo, una empresa, institución educativa, organismo público. Se han desarrollado tecnologías específicas para implementar este tipo de redes, por ello, otro criterio habitual de identificación de una red LAN es el uso de una tecnología específica para redes LAN. Los estándares actuales de redes LAN son Ethernet y Wi-Fi (Moreno Pérez & Santos González, 2014).

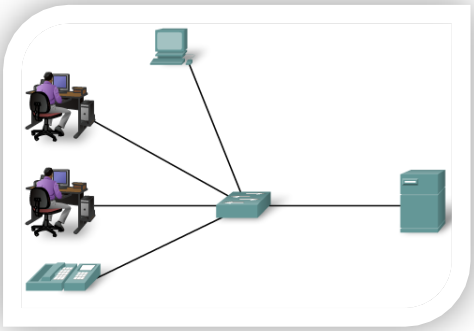


Figura 1. Red de Área Local
Fuente: Cisco CCNA 1

MAN (Red de Área Metropolitana)

Red de área metropolitana (Metropolitan Area Network o MAN): generalmente, una MAN está confinada dentro de una misma ciudad y se haya sujeta a regulaciones locales. Puede constar de varios recursos públicos o privados, como el sistema de telefonía local, sistemas de microondas locales o cables enterrados de fibra óptica. Una empresa local construye y mantiene la red, y la pone a disposición del público. Puede conectar sus redes a la MAN y utilizarla para transferir información entre redes de otras ubicaciones de la empresa dentro del área metropolitana (Molina Robles, 2014).

Figura 2. Red de Area Metropolitana
Fuente: http://redes-man-unerg.blogspot.com/2008/05/redes-man.html

WAN (Red de Área Extensa)

El término WAN (Wide Area Network o red de área extensa) se aplica realmente a la infraestructura que permite la conexión de redes o dispositivos ubicados en diferentes zonas geográficas sin límite de distancia. En resumidas

cuentas, todo lo que no sean infraestructuras pertenecientes a redes LAN serán redes WAN. Una característica muy significativa en este tipo de redes es el uso de las infraestructuras proporcionadas por los operadores de telecomunicación cuyo ámbito de actuación esté dentro de las zonas que cubren este tipo de redes. Existen tecnologías específicas para redes WAN, como Frame Relay, ATM, xDSL, etc. Es necesario destacar la expresión “sin límite de distancia”, es decir, se puede utilizar una red WAN para unir dispositivos (o redes) dentro de, por ejemplo, la misma ciudad. O se podría utilizar una red WAN para unir dispositivos (o redes) separados miles de kilómetros (Moreno Pérez & Santos González, 2014).

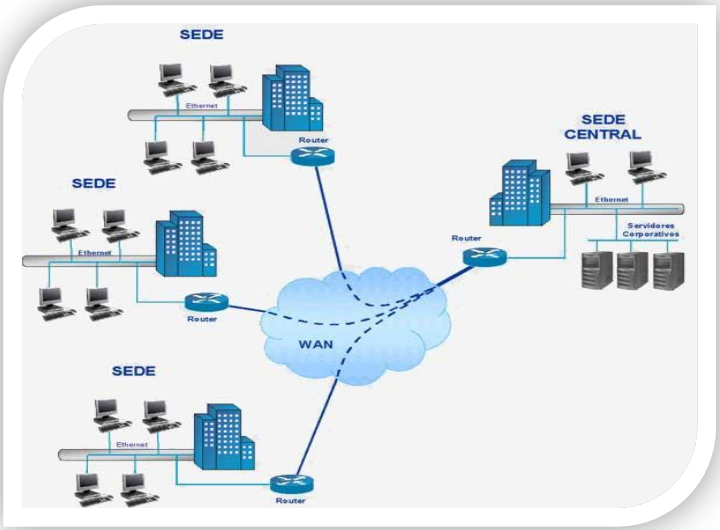


Figura 3. Red de Área Extensa
Fuente: http://galeon.com/redes5b/tipo.html

PAN (Red de Área Personal)

Son redes cuyos equipos terminales están situados en un radio de pocos metros y están destinadas a uso personal, por ejemplo, cuando dos usuarios se conectan con una PSP para jugar en red o cuando un móvil se conecta a otro vía bluetooth para enviarle fotografías (Castaño Ribes & López Fernández, 2013) .

Figura 4. Red de Área Personal
Fuente: https://camiesco11.files.wordpress.com/2010/03/dispositivosbluetooth.jpg

1.8.2. Internet

Internet es una Red informática que conecta los ordenadores de todo el mundo permitiendo compartir información a todos los que forman parte de ella a través de una simple conexión telefónica. Existen otras redes que conectan varios ordenadores entre sí (las llamadas Intranet) pero Internet, popularmente conocida como “Red de Redes” por englobar todas estas Intranet dentro de sí misma, ha revolucionado las comunicaciones al conseguir que usuarios conectados en cualquier parte del mundo puedan obtener información sobre cualquier tema, enviar mensajes, transferirse archivos, etc., en cuestión de segundos incluso desde un punto a otro del planeta (Cruz Herradón, 2013).

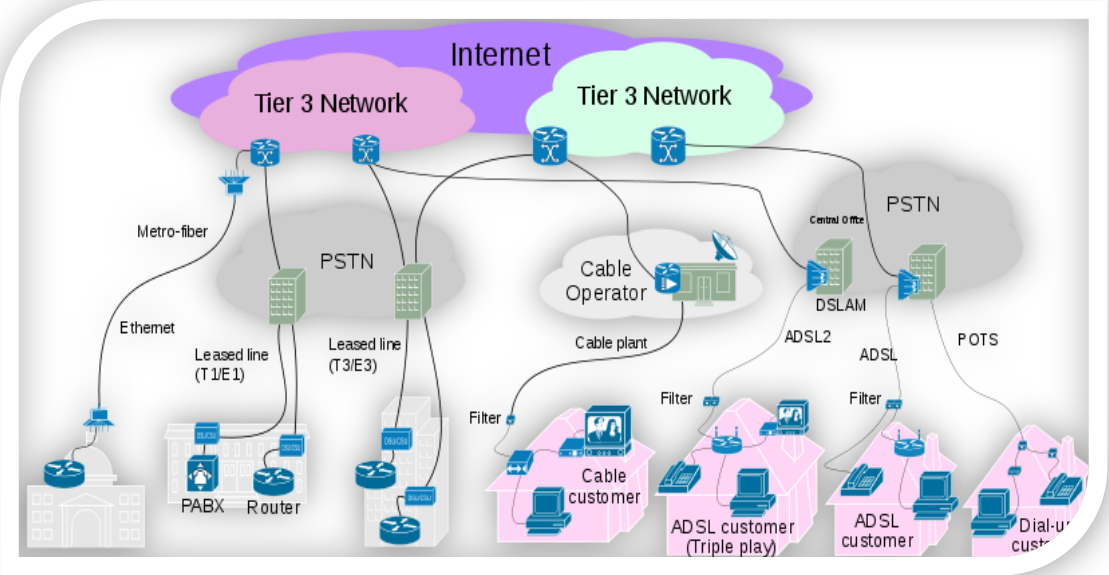


Figura 5. Esquema del Acceso al Internet
Fuente: http://commons.wikimedia.org/wiki/File:Internet_Connectivity_Access_layer.svg

1.8.3. Ethernet

Ethernet es la red de norma IEEE 802.3, que utiliza el protocolo de acceso al medio CSMA/CD en el que las estaciones están permanentemente a la escucha del canal y, cuando lo encuentran libre de señal, efectúan sus transmisiones. Esto puede llevar a una colisión que hará que las estaciones suspendan sus transmisiones, esperen un tiempo aleatorio, transmitan una trama de aviso (jam frame) y vuelvan a intentarlo. Si dos nodos en el mismo dominio de colisión se sitúan muy alejados, es posible que no puedan detectar si se produce una colisión y no procederán a la retransmisión de los datos. El problema en la detección se produce porque hay un retardo en la propagación de la señal eléctrica por los cables, que se incrementa con la longitud del cable y con la velocidad de transmisión. Esta es la razón por la que la longitud de los segmentos Ethernet no puede ser tan grande como se desee.

Cualquier estación conectada a una red IEEE 802.3 debe poseer una tarjeta de red que cumpla con este estándar y con los componentes electrónicos y el

software adecuado para la generación y recepción de tramas. La tarjeta o adaptador de red se encarga de verificar las tramas que le llegan desde el canal, así como de ensamblar los datos de información dándoles la forma de una trama, detectar los posibles errores en destino, etc. La tarjeta también es la encargada de negociar los recursos que necesita con el sistema operativo del ordenador en que se instala (Abad Domingo, 2013).

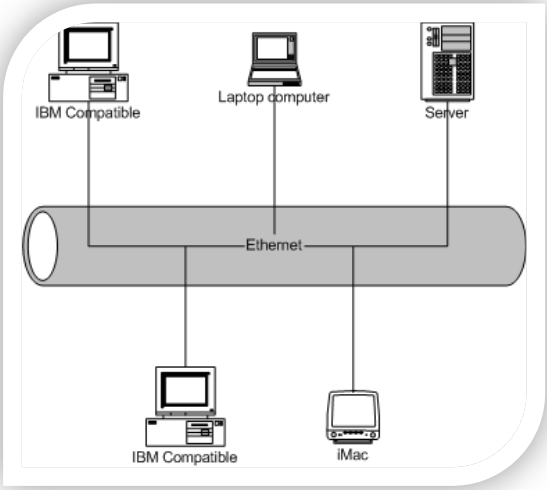


Figura 6. Red Ethernet
Fuente: http://en.wikipedia.org/wiki/File:Ethernet.png

1.8.4. WiFi

Si bien la conexión de computadoras mediante ondas de radio o luz infrarroja está siendo investigada intensamente en la actualidad, una de las tecnologías más prometedoras y preferidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. Las redes inalámbricas facilitan el trabajo en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos (Cedano Olvera, Rubio González, & Vega Gutiérrez, 2014).

Principales ventajas

- Permiten la movilidad de usuarios y dispositivos: los usuarios pueden desplazarse con sus dispositivos inalámbricos a lo largo de toda la zona de cobertura de la WLAN sin perder la conexión.

- Menor coste: el hecho de necesitar muy pocos cables, o incluso ninguno si la red es pequeña, junto con el bajo coste de los componentes de la WLAN hacen que la instalación resulte muy económica.

- Menor tiempo de instalación: es más rápida porque no se tienen que instalar cables, canalizaciones, rosetas, etc.

Principales inconvenientes

- Sensibilidad a las interferencias electromagnéticas y a la presencia de otras WLAN: la presencia de interferencias electromagnéticas y de otras WLAN que operen con frecuencias próximas a las de la nuestra puede influir negativamente en el rendimiento de la misma.

- Si en una zona aumenta el número de dispositivos, el rendimiento en dicha zona disminuye: en una misma zona e instante solo puede existir una transmisión para nuestra WLAN, pues sería como si todos los dispositivos de la zona estuvieran conectados a un mismo hub. Esto no ocurre en las redes cableadas basadas en switches.

- Velocidades de transmisión generalmente inferiores: aunque cada vez surgen tecnologías más veloces, todavía no se ha llegado a igualar la velocidad que ofrecen los medios cableados.

- Mayores requerimientos de seguridad: dado que no hace falta acceder físicamente a las WLAN para atacarlas, necesitan mayor seguridad.

El estándar IEEE 802.11 define una arquitectura de red que establece las bases de funcionamiento de las WLAN (WiFi). Para ello define un conjunto de componentes físicos y lógicos, dos modos de operación y toda una colección de protocolos y especificaciones agrupados en dos capas: la física o PHY y la de control de acceso al medio o MAC. Estas capas regulan los aspectos de las

capas físicas y de enlace, respectivamente, de la pila de protocolos OSI. El estándar, además, guarda compatibilidad en todo momento con las redes de área local IEEE 802.3 y Ethernet, de tal forma que una red WLAN se puede integrar dentro de una LAN Ethernet convencional (Castaño Ribes & López Fernández, 2013).

Figura 7. Red WiFi
Fuente: http://www.howstuffworks.com/wireless-network.htm

1.8.5. Medios Físicos

1.8.5.1. Cable de cobre de par trenzado

El par trenzado consiste en dos alambres de cobre recubiertos por una cobertura plástica. Estos alambres recubiertos se encuentran trenzados entre ellos, enroscados uno al otro.

Cada cable tiene su propia carga eléctrica, que genera interferencia, y al trenzar un cable con el otro, cada cable anula la inducción eléctrica de la contraparte. Al trenzar los cables, logramos reducir significativamente el nivel de interferencia entre ellos, lo cual aumenta la calidad de transmisión del medio.

Existen dos categorías de cables de par trenzado. El cable UTP significa Unshielded Twisted Pair (Par trenzado sin protección). El cable STP significa Shielded Twisted Pair (Par trenzado con escudo). Ambos tienen ocho hilos, es decir, cuatro pares.

El cable UTP es el más comúnmente utilizado. Se ha transformado en un estándar de facto en las redes LAN de todo tipo. Su escudo tiene un recubrimiento externo general, que contiene cuatro pares trenzados con distintos colores, que nos servirán para armarlo y establecer conectividad de red. Este armado requiere una combinación de posiciones específicas de cada hilo (Katz, 2013).

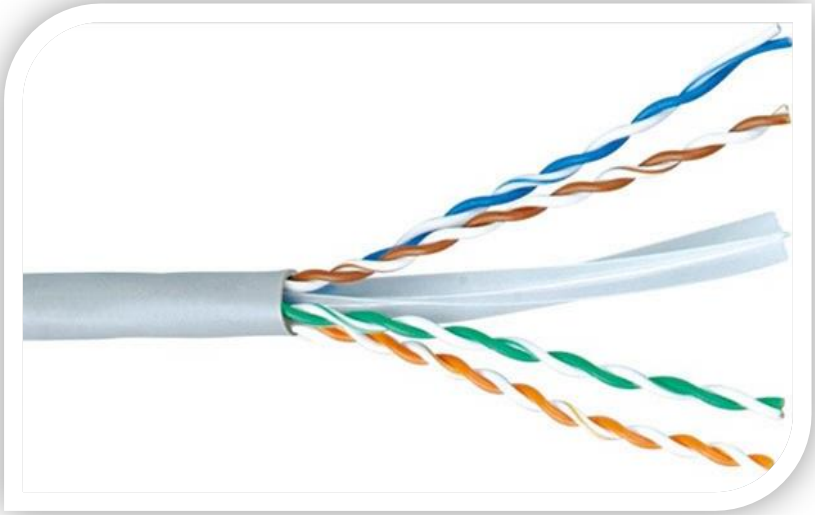


Figura 8. Cable UTP
Fuente: http://coisasuteis.net/es/cables-y-accesorios/16-cabo-de-rede-utp-solido-cat-5e.html

1.8.5.2. Fibra óptica

La fibra óptica es el medio de transmisión que permite enviar información a mayor velocidad (10 Gbps), mayor distancia (40 km) y sin tener que preocuparse de las interferencias externas. Aun así, su utilización no se ha extendido todo lo que se podría esperar por dos motivos: los altos precios y la

mayor dificultad en la instalación. El funcionamiento de la fibra óptica se basa en la emisión de un haz de luz sobre una fibra de vidrio. Esta fibra de vidrio está recubierta por revestimientos aislantes que la protegen del exterior y le dan firmeza.

Las fibras ópticas deben cumplir las especificaciones de las normas EN 60793 y EN 60194. Las principales características que determinan el tipo de fibra óptica son:

- Diámetro del núcleo de vidrio.
- Longitud de onda de la luz que viaja por el vidrio.

Según la primera característica se distinguen dos tipos de fibras: multimodo y monomodo.

Las fibras multimodo son aquellas que el diámetro del núcleo de fibra de vidrio es de 50 o 62,5 µm. Esta distancia permite que el haz de luz tenga más de un recorrido óptico (modo) posible cuando viaja por el vidrio. Esta característica hace que las fibras de este tipo tengan más pérdidas (debidas a la atenuación de los rebotes, distorsión). Normalmente se utilizan LEDs para la emisión del haz de luz, aunque a partir de 622 Mbps es necesario utilizar un láser de emisión por superficie de cavidad vertical (VCSEL). Si se quiere utilizar este tipo de láser se deberá instalar fibra adecuada para ello y entonces será posible llegar hasta velocidades de 10 Gbps. Hay que tener en cuenta que la fibra multimodo es más cara pero que los equipos electrónicos son mucho más baratos que en el caso de la fibra monomodo. Con este tipo de fibra se puede transmitir a dos longitudes de onda diferentes: 850 y 1.300 nm.

Habitualmente, la cubierta exterior de las fibras multimodo es de color naranja, ya que así se define en la recomendación TIA/EIA-598-B.

Por el contrario, las fibras monomodo son aquellas que tienen un diámetro más pequeño del núcleo, ente 8,3 y 10 µm. Este diámetro obliga al haz de luz a recorrer un camino concreto por el vidrio, sólo hay un único modo. Esta característica hace que este tipo de fibras tenga menores pérdidas (se pueden

alcanzar mayores distancias) y que se deba utilizar un láser para la emisión del haz de luz. Con este tipo de fibra se pueden transmitir a dos longitudes de onda: 1.310 y 1.550 nm. Para diferenciar este tipo de fibras, habitualmente, la cubierta exterior de las fibras monomodo es de color amarillo, ya que así se define en la recomendación TIA/EIA-598-B (Cadenas Sanchez & Zaballos Diego, 2011).

Figura 8. Cable de Fibra óptica
Fuente: http://rebeskua.blogspot.com/2012/02/que-es-es-un-medio-de-transmision.html

1.8.5.3. Canales de radio terrestres

El conjunto de todas las posibles longitudes de onda (o frecuencias) constituye el llamado espectro electromagnético. Este espectro se divide en bandas en función de la frecuencia. El rango de frecuencias utilizadas en telecomunicaciones va desde los 3 kHz hasta alrededor de los 300 GHz. A este rango se le conoce como espectro de radiofrecuencia y abarca las siguientes bandas:

Ondas de radio. Son fáciles de generar, pueden viajar largas distancias, penetran en los edificios sin problemas y viajan en todas direcciones desde la fuente emisora. El rango de frecuencias que cubre va desde las frecuencias más bajas, alrededor de los 10 kHz, hasta frecuencias en torno a los 300 MHz. Existen dos tipos de ondas de radio:

Ondas de radio de baja frecuencia: se caracterizan por que en su recorrido siguen la curvatura de la Tierra y pueden atravesar con facilidad los edificios. Sin embargo, su ancho de banda solo permite velocidades de transmisión bajas.

Ondas de radio de alta frecuencia: estas ondas tienden a ser absorbidas por la Tierra, por lo que deben ser enviadas a la ionosfera, donde son reflejadas y devueltas de nuevo, con lo que se consigue transmitir a largas distancias.

Microondas. Además de su aplicación en hornos, las microondas permiten transmisiones tanto terrestres como con satélites. Sus frecuencias están comprendidas entre 300 MHz y 300 Ghz. A diferencia de las ondas de radio, las microondas no atraviesan bien los obstáculos, de forma que es necesario situar antenas repetidoras cuando queremos realizar comunicaciones a largas distancias. En el caso de las comunicaciones por satélite, hay que tener en cuenta que siempre existe un pequeño retardo en las transmisiones debido a que la señal tarda aproximadamente 0,3 segundos en llegar y volver. Para algunas aplicaciones de envío y recepción de datos, este tiempo de espera puede resultar inaceptable.

Ondas infrarrojas. Este tipo de ondas se utiliza para la comunicación de corto alcance, en controles remotos de televisores, y en general de dispositivos electrónicos. También es posible encontrar un puerto de comunicación infrarroja en los ordenadores portátiles. Estos controles son relativamente direccionales, baratos y fáciles de construir, pero tienen un inconveniente importante: no atraviesan los objetos sólidos. Este inconveniente también resulta a veces una ventaja en el sentido de que ofrecen más seguridad, precisamente porque la comunicación no atraviesa las paredes de un edificio. Además, el uso de frecuencias en la banda de los infrarrojos no está regulado por las administraciones como ocurre con otras bandas de frecuencia.

La mayor parte de las comunicaciones en redes telemáticas inalámbricas se llevan a cabo en la banda de las microondas (Santos González, 2014).

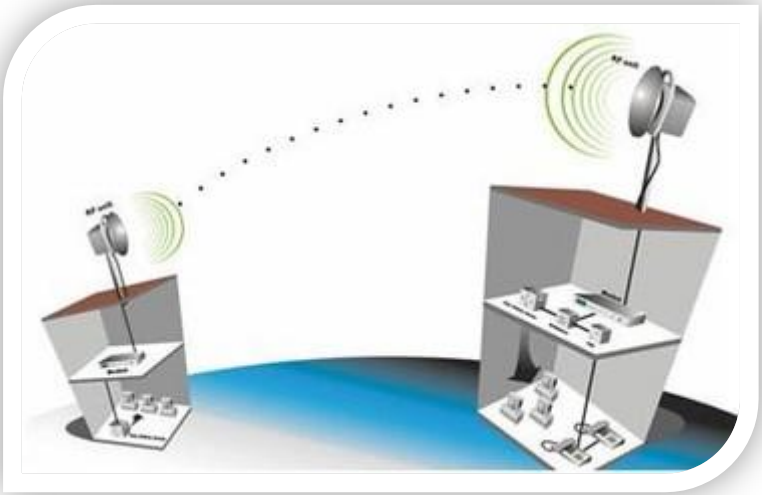


Figura 9. Enlaces de Radio
Fuente: http://coisasuteis.net/es/cables-y-accesorios/16-cabo-de-rede-utp-solido-cat-5e.html

1.8.6. Protocolos y Estándares de Red.

En la década de los setenta los ordenadores empezaron a disminuir considerablemente de precio y de tamaño. Ya no se disponía de un solo ordenador para toda una organización, sino que empezaban a coexistir varios en una misma sala. Como los recursos eran caros, pronto empezaron a surgir iniciativas que proponían interconectar las máquinas y compartir dichos recursos. Nacieron así las redes locales.

Protocolos de comunicaciones. Aparecieron entonces los primeros fabricantes de componentes de red a gran escala. Estos fabricantes tuvieron que determinar las normas y procedimientos que utilizarían en sus componentes de red, definiendo así los primeros protocolos de comunicaciones.

Un protocolo de comunicaciones es un conjunto de normas y procedimientos que los diseñadores de una red eligen o establecen para que los distintos componentes de esa red los utilicen.

Estándares de red. Al principio, cada fabricante utilizaba sus propios protocolos de comunicaciones, de tal forma que sus componentes no eran compatibles con los del resto de fabricantes. Esto obligaba a los clientes a comprar toda la red al mismo fabricante y, dada la gran inversión que suponía, era impensable cambiar de fabricante una vez implantada una red. Sin embargo, aunque dicho comportamiento pudiera parecer ventajoso para los fabricantes, no lo era del todo. Por ejemplo, los nuevos productos más competitivos no siempre tenían éxito, ya que, no siendo compatibles con los de otros fabricantes, al cliente le resultaba excesivamente caro cambiar toda la infraestructura de red para poder disponer de ellos. Por eso no pasó mucho tiempo antes de que los fabricantes empezaran a unir esfuerzos y aparecieran los primeros estándares para redes.

Un estándar es un modelo o patrón que se propone para que distintos fabricantes lo sigan y fabriquen componentes compatibles entre sí. Los estándares pueden proceder de una iniciativa propia de las empresas, estándares de facto, o de un organismo oficial, estándares de iure.

Por un lado, empezaron a establecerse algunas alianzas entre fabricantes y algunos protocolos empezaron a convertirse en estándares de facto. Por el otro, algunas instituciones autónomas y organismos nacionales e internacionales de estandarización comenzaron a elaborar y a publicar recomendaciones y estándares de iure a los cuales podían adherirse, si querían, los fabricantes.

1.8.7. Arquitecturas de red basadas en capas.

Los primeros ingenieros de comunicaciones se dieron cuenta de que el proceso de comunicación entre computadoras se podía dividir en capas, y de que abordar cada una de estas capas por separado facilitaba enormemente la tarea de diseño de protocolos y estándares para redes. Una arquitectura de red basada en capas consiste en la división en capas de los distintos aspectos que regulan el proceso de comunicación entre las computadoras de una red. Al ocuparse cada una de las capas de ciertos aspectos concretos del proceso de comunicación, se libera de tales aspectos al resto de las capas, simplificando así el diseño de la red (Castaño Ribes & López Fernández, 2013).

1.8.8. Modelo de Referencia OSI

Este modelo fue creado por la Organización Internacional para la Estandarización (ISO), a fines de la década de 1970, con el propósito de unificar el modo en el cual diferentes entidades a lo largo del mundo caracterizaran las comunicaciones en una red desde el punto de vista del diseño. De esta manera, todos los componentes que conforman una red, al igual que sus modos de operación y sus características pueden ser categorizadas equitativamente, sin importar sus detalles específicos. El modelo en sí es simplemente un diseño de arquitectura gráfica que segmenta a cada componente de red en diferentes capas. Mediante esta subdivisión conceptual es posible englobar y agrupar a los objetos correspondientes a cada capa y a sus comportamientos, según una lista de reglas y características únicas e iguales entre componentes de igual nivel (Katz, 2013).

El modelo OSI define siete capas, con sus respectivas funciones:

Física. Realiza la transmisión de los bits en el medio de transmisión físico. Tiene relación con los mecanismos de acceso al medio físico y los temas

eléctricos de las señales transmitidas, como ser la potencia a utilizar, así como con los aspectos mecánicos de las conexiones. Especifica las características del medio de transmisión. Estos temas los hemos analizado en el capítulo anterior.

Enlace de datos. Transfiere datos (en forma de tramas) a través del medio de transmisión físico. Se encarga de las funciones de sincronización, control de flujo y detección y corrección de errores. Si varios nodos comparten el medio de transmisión, se encarga del control de acceso al medio (MAC), el cual estudiaremos más adelante en este mismo capítulo.

Red. Realiza el enrutamiento de los paquetes desde el origen hasta el destino entre redes homogéneas o heterogéneas y determina cómo se mueven por la red. También ejecuta un control del flujo. Representa el límite entre las funciones de la red (ésta y sus dos capas inferiores) y las del usuario.

Transporte. Se encarga de la transferencia de datos entre el origen y el destino, brindando servicios de seguridad, esquemas de control de flujo entre ambos puntos y sistemas de detección y corrección de errores.

Sesión. Realiza el control de la comunicación entre las aplicaciones en el origen y el destino. Abre, administra, mantiene y cierra las conexiones o sesiones de las aplicaciones y se encarga de la recuperación.

Presentación. Se encarga del manejo de la sintaxis y la semántica de los datos transmitidos. Se hacen traducciones si fueran necesarias para representar datos que el usuario pueda entender.

Aplicación. Representa el punto de ingreso al modelo de capas. Pueden ser los protocolos de transferencia de archivos, correo electrónico, chat, etc. Un ejemplo clásico es el protocolo HTTP (Hypertext Transfer Protocol – Protocolo

de transferencia de hipertexto), mediante el cual desde el navegador Web se solicita una página determinada (Hillar, 2009).

Figura 10. Modelo OSI
Fuente: http://es.wikipedia.org/wiki/Modelo_OSI

1.8.9. VLANS

La configuración de una red de área local típica depende, en gran manera, de la infraestructura física de sus conexiones. Así pues, la agrupación de usuarios se hace según su situación física, su conexión a un determinado concentrador o conmutador y su cableado correspondiente. Si el dispositivo que interconecta los diferentes concentradores es un encaminador (Router), éste proporcionará segmentación y evitará que el tráfico de difusión (Broadcast) pase de una red a otra.

En cambio, si el dispositivo que interconecta los diferentes concentradores es un conmutador, éste no podrá evitar que el tráfico de difusión pase de un segmento a otro. Además, este tipo de segmentación no permite agrupar a los usuarios según el tipo de tarea que hacen, el departamento al cual pertenecen o el ancho de banda que necesitan.

Una VLAN crea un dominio de difusión único que no está restringido a un segmento físico. Así pues, el tráfico de difusión no se propaga entre las LAN virtuales. Por lo tanto, para que dos usuarios de VLAN diferentes se puedan comunicar entre ellos, será necesario que un encaminador interconecte las dos VLAN. Dos usuarios que estén conectados al mismo conmutador y que pertenezcan a VLAN diferentes no se podrán comunicar entre ellos mientras no haya un encaminador entre las dos VLAN. Es importante destacar que la implementación de VLAN se hace mediante software instalado en los conmutadores. Consiguientemente, cada fabricante implementa su versión para la creación y gestión de VLAN.

Es importante destacar que la implementación de VLAN se hace mediante software instalado en los conmutadores. Consiguientemente, cada fabricante implementa su versión para la creación y gestión de VLAN (Íñigo Griera, Barceló Ordinas, & Cerdà Alabern, 2008).

Una VLAN es un método que crea una red lógica dentro de una red física. De este modo se consigue que la información que se genera dentro de cada una de las redes virtuales solo sea recibida por hosts de la propia red lógica y no por toda la red física.

1.8.10. Características de las VLAN

La característica principal de las redes virtuales es que reducen el costo real y administrativo de la generación de la red, ya que se configuran mediante software y no mediante hardware. Ya no es necesario colocar un router cada

vez que se genera un nuevo dominio de difusión sino que, por medio de conmutadores de precio más reducido, se consigue el mismo efecto. Otras características reseñables de las redes virtuales son:

Aumento de la eficiencia del ancho de banda: al tener un mayor control sobre los dominios de difusión, la cantidad de paquetes que circula por la red es menor y, por tanto, el uso del ancho de banda es más eficiente, elevándose el rendimiento general de toda la red.

Mejoras en la seguridad de la red: el hecho de separar la red en grupos que no pueden compartir información entre sí supone una mejora de la seguridad. Además se puede conseguir que los servidores no sean vistos por todos los hosts, lo que evita despistes a la hora de configurar la seguridad global de la red.

Aumento de la flexibilidad de la red: varios hosts conectados al mismo conmutador pueden pertenecer a distintas VLAN y, a su vez, hosts de distintos conmutadores pueden pertenecer a la misma VLAN. Esto aumenta la flexibilidad de segmentación y organización de toda la red y hace que los traslados o cambios en la red no sean traumáticos.

Aumento de escalabilidad de la red: es más fácil aumentar una red previamente segmentada con VLAN, dadas sus ventajas en ancho de banda, seguridad y flexibilidad (Castaño Ribes & López Fernández, 2013).

1.8.11. Clases de VLAN

Mediante VLAN podemos disponer de una red conmutada que está segmentada lógicamente según las aplicaciones, los protocolos y las funciones de los usuarios, sin que importe dónde están situados físicamente estos usuarios. Así pues, podríamos definir que cada puerto de un conmutador forma parte de una VLAN distinta, si es necesario. Las VLAN se pueden clasificar

según la forma de asignación de los puertos de un conmutador a una VLAN. Sin embargo, otra manera de clasificar las VLAN dependerá del tipo de información que utilice el conmutador para agrupar los dispositivos de una manera lógica. A continuación analizaremos las diferentes VLAN, que se pueden clasificar en los tipos siguientes:

- VLAN estáticas o dinámicas
- VLAN basadas en el puerto o en el protocolo

1.8.12. VLAN Estáticas y Dinámicas

En una VLAN estática los puertos de un conmutador se asignan estáticamente a una VLAN determinada. Así pues, la configuración sólo cambiará si el administrador de red cambia un puerto de una VLAN a otra. En caso contrario, esta configuración se mantendrá fija. Este tipo de VLAN comporta un control muy grande del administrador, pero es fácil de configurar, monitorizar y gestionar. Esto se debe a que es el administrador el que tiene el control total.

La asignación automática del puerto a las VLAN dinámicas puede depender de las direcciones de nivel de enlace, de las direcciones lógicas o bien del tipo de protocolo de los paquetes.

1.8.13. VLAN Basadas en Puertos o en el Protocolo

Es decir, a cada VLAN le corresponderá toda una serie de puertos determinados. En el fondo, tendremos que entender que se trata de una VLAN estática, como la estudiada anteriormente. Cuando hablamos de VLAN basada en el protocolo, el conmutador clasificará el tráfico recibido según el tipo de protocolo del paquete de nivel de red. En el caso de VLAN basadas en el protocolo la información

Este tipo de VLAN requiere menos administración en caso de que un usuario cambie de situación geográfica, ya que no es necesario definir para cada puerto su asignación de VLAN. Sin embargo, hay que disponer de una base de datos actualizada con todos los usuarios y el criterio de asignación de VLAN elegido.

1.8.14. Protocolo IEEE 802.1Q

El conmutador es el dispositivo encargado de filtrar y permitir el paso de las tramas según los criterios de VLAN y, además, tiene que compartir esta información con otros conmutadores y encaminadores de la red. Si tenemos a usuarios de una misma VLAN conectados a diferentes conmutadores, será necesario que éstos se pasen información entre ellos y que conozcan a qué VLAN pertenecen las tramas que conmutan. Se puede dar el caso de que un usuario conectado a un conmutador envíe tramas a otro usuario de la misma VLAN que cuelga de otro conmutador. Además, recordemos que las tramas de difusión llegan a todos los miembros de una VLAN. Por lo tanto, un conmutador deberá reconocer y asociar las tramas que recibe con la VLAN correspondiente. La técnica de identificación de tramas asigna un identificador determinado para cada trama. Esta técnica introduce un identificador en la cabecera de la trama de nivel de enlace. Este identificador se transmite para la red troncal y es examinado por los diferentes conmutadores y encaminadores que atraviesa. Cuando la trama está a punto de salir de la red troncal, el conmutador elimina este identificador, con el objetivo de que no llegue hasta la estación de destino.

Cualquier puerto, por defecto, siempre es access port y, por lo tanto, únicamente puede pertenecer a una sola VLAN. En cambio, un trunk port permitirá la interconexión de conmutadores y, consiguientemente, tendrá que

pertenecer a todas las VLAN de las cuales transmita tramas. En un trunk port, la información viajará acompañada con la etiqueta de la VLAN correspondiente.

En cambio, las tramas que salen de un puerto de acceso siempre estarán sin marcar (untagged) y esto significa que no llevarán información especial con respecto a qué VLAN en particular pertenecen. Los trunk ports se utilizan usualmente para interconectar diferentes conmutadores, sin tener en cuenta a qué VLAN pertenecen las tramas intercambiadas (Íñigo Griera, Barceló Ordinas, & Cerdà Alabern, 2008).

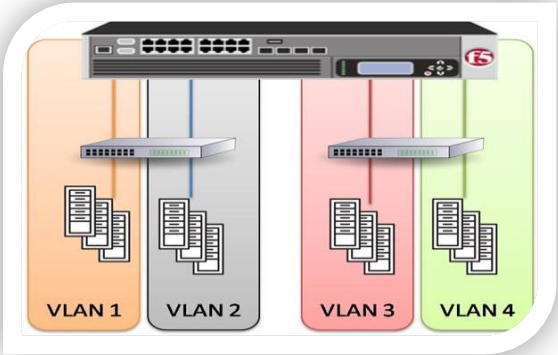


Figura 11. VLANS
Fuente: https://devcentral.f5.com/blogs/us/virtualization-how-to-isolate-application-traffic

1.8.15. Gestión por Procesos

Las organizaciones son tan eficientes como lo son sus procesos. La mayoría de las empresas han tomado conciencia de esto y se plantean cómo mejorarlos y evitar algunos males habituales como: bajo rendimiento, poco enfoque al cliente, barreras departamentales, subprocesos inútiles debido a la falta de visión global del proceso, etc.

Un proceso puede ser definido como un conjunto de actividades interrelacionadas entre sí que, a partir de una o varias entradas de materiales o información, dan lugar a una o varias salidas también de materiales o información con valor añadido.

En otras palabras, un proceso es la manera en la que se hacen las cosas en la empresa. Ejemplos de procesos son el de producción y entrega de bienes y/o servicios, el de gestión comercial, el de desarrollo de la visión estrategia, el de desarrollo de producto, estos procesos deben estar correctamente gestionados empleando distintas herramientas de la gestión de procesos.

La incorporación de las nuevas tecnologías de la información permite redefinir los procesos alcanzando grados de eficacia y eficiencia inimaginables hace unos años. Las organizaciones que sean capaces de descubrir estas posibilidades e implantarlas correctamente, conseguirán ventajas competitivas debido a la disminución de costes y el aumento de flexibilidad frente a los requerimientos de los clientes.

La Gestión de Procesos coexiste con la administración funcional, asignando "propietarios" a los procesos clave, haciendo posible una gestión interfuncional generadora de valor para el cliente y que, por tanto, procura su satisfacción. Determina qué procesos necesitan ser mejorados o rediseñados, establece prioridades y provee de un contexto para iniciar y mantener planes de mejora que permitan alcanzar objetivos establecidos. Hace posible la comprensión del modo en que están configurados los procesos de negocio, de sus fortalezas y debilidades.

Un modelo de gestión integrado debe presentar una visión globalizada y orientada al Cliente tanto interno como externo según postulados de Calidad Total y de ser posible según principios basados en modelos de excelencia empresarial.

No estaremos hablando realmente de un Sistema de Gestión Integrado hasta que no sistematizar todos los procesos claves y relevantes que intervienen en la empresa (Angel Maldonado, 2011).

1.8.16. Conceptos Básicos en la Gestión por Procesos

Otros términos relacionados con la Gestión por Procesos, y que son necesarios tener en cuenta para facilitar su identificación, selección y definición posterior son los siguientes:

Proceso: Conjunto de actividades organizadas para conseguir un fin, desde la producción de un objeto o prestación de un servicio hasta la realización de cualquier actividad interna (ejemplo: elaboración de una factura). Los objetivos clave del negocio dependen de procesos de negocio interfuncionales eficaces, y, sin embargo, estos procesos no se gestionan. El resultado es que los procesos de negocio se convierten en ineficaces e ineficientes, lo que hace necesario adoptar un método de gestión por procesos.

Conjunto de recursos y actividades interrelacionados que transforman elementos de entrada en elementos de salida. Los recursos pueden incluir personal, finanzas, instalaciones, equipos, técnicas y métodos.

Proceso relevante: es una secuencia de actividades orientadas a generar un valor añadido sobre una entrada, para conseguir un resultado que satisfaga plenamente los objetivos, las estrategias de una organización y los requerimientos del cliente. Una de las características principales que normalmente intervienen en los procesos relevantes es que estos son interfuncionales, siendo capaces de cruzar verticalmente y horizontalmente la organización.

Proceso clave: Son aquellos procesos extraídos de los procesos relevantes que inciden de manera significativa en los objetivos estratégicos y son críticos para el éxito del negocio.

Subprocesos: son partes bien definidas en un proceso. Su identificación puede resultar útil para aislar los problemas que pueden presentarse y posibilitar diferentes tratamientos dentro de un mismo proceso.

Sistema: Estructura organizativa, procedimientos, procesos y recursos necesarios para implantar una gestión determinada, como por ejemplo la gestión de la calidad, la gestión del medio ambiente o la gestión de la prevención de riesgos laborales. Normalmente están basados en una norma de reconocimiento internacional que tiene como finalidad servir de herramienta de gestión en el aseguramiento de los procesos.

Procedimiento: forma específica de llevar a cabo una actividad. En muchos casos los procedimientos se expresan en documentos que contienen el objeto y el campo de aplicación de una actividad; que debe hacerse y quien debe hacerlo; cuando, donde y como se debe llevar a cabo; que materiales, equipos y documentos deben utilizarse; y como debe controlarse y registrarse.

Actividad: es la suma de tareas, normalmente se agrupan en un procedimiento para facilitar su gestión. La secuencia ordenada de actividades da como resultado un subproceso o un proceso. Normalmente se desarrolla en un departamento o función.

Proyecto: suele ser una serie de actividades encaminadas a la consecución de un objetivo, con un principio y final claramente definidos. La diferencia fundamental con los procesos y procedimientos estriba en la no repetitividad de los proyectos.

Indicador: es un dato o conjunto de datos que ayudan a medir objetivamente la evolución de un proceso o de una actividad (Angel Maldonado, 2011).

1.8.17. Beneficios de la Gestión por Procesos

Los procesos han de estar bien definidos en función de las metas y objetivos comunes que involucran a todos, en el mejoramiento continuo que tendrá siempre presente la satisfacción de los usuarios. Como consecuencia de que

las organizaciones desarrollan sus actividades en un entorno complejo e inestable, los procesos en general son sometidos a continuos cambios para que puedan adaptarse al medio, permitiendo obtener la máxima rentabilidad (Moreira Delgado, 2009).

1.9. Fundamentación legal

En los derechos del buen vivir **Sección octava: Ciencia, tecnología, innovación y saberes ancestrales**, articulo 385, garantiza el desarrollo de tecnologías e innovaciones que eleven la eficiencia de la productividad, mejorando la calidad de vida

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.
2. Recuperar, fortalecer y potenciar los saberes ancestrales.
3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

En la ley Orgánica de Educación Superior (LOES) vigente, en el capítulo 3, articulo 13, literal b que indica sobre los principios de la educación superior, en la cual garantiza Promover la creación, desarrollo, transmisión y difusión de la ciencia, la técnica, la tecnología y la cultura

Art.13.- Funciones del Sistema de Educación Superior.- Son Funciones del sistema de Educación Superior:

a) Garantizar el derecho a la educación superior mediante la docencia, la investigación y su vinculación con la sociedad, y asegurar crecientes niveles de calidad. excelencia académica y pertinencia

b) Promover la creación, desarrollo, transmisión y difusión de la ciencia, la técnica, la tecnología y la cultura;

c) Formar académicos, científicos y profesionales responsables, éticos y solidarios, comprometidos con la sociedad, debidamente preparados para que sean capaces de generar y aplicar sus conocimientos y métodos científicos, así como la creación y promoción cultural y artística:

d) Fortalecer el ejercicio y desarrollo de la docencia y la investigación científica en todos los niveles y modalidades del sistema:

e) Evaluar, acreditar y categorizar a las instituciones del Sistema de Educación Superior, sus programas y carreras, y garantizar independencia y ética en el proceso.

f) Garantizar el respeto a la autonomía universitaria responsable;

g) Garantizar el cogobierno en las instituciones universitarias y politécnicas;

h) Promover el ingreso del personal docente y administrativo, en base a concursos públicos previstos en la Constitución; i) Incrementar y diversificar las oportunidades de actualización y perfeccionamiento profesional para los actores del sistema;

i) Incrementar y diversificar las oportunidades de actualización y perfeccionamiento profesional para los actores del sistema;

j) Garantizar las facilidades y condiciones necesarias para que las personas con discapacidad puedan ejercer el derecho a desarrollar actividad, potencialidades y habilidades:

k) Promover mecanismos asociativos con otras instituciones de educación superior, así como con unidades académicas de otros países, para el estudio. análisis, investigación y planteamiento de soluciones de problemas nacionales, regionales, continentales y mundiales:

l) Promover y fortalecer el desarrollo de las lenguas. culturas y sabidurías ancestrales de los pueblos y nacionalidades del Ecuador en el marco de la interculturalidad:

m) Promover el respeto de los derechos de la naturaleza, la preservación de un ambiente sano y una educación y cultura ecológica;

n) Garantizar la producción de pensamiento y conocimiento articulado con el pensamiento universal; y.
o) Brindar niveles óptimos de calidad en la formación y en la investigación.

En el Estatuto Orgánico de La universidad Técnica Estatal de Quevedo, en su art 8, inciso 3, hace referencia a los fines de la institución, nos indica que la UTEQ, fomentará las investigaciones que ayuden a satisfacer necesidades, y una de esta es el control de acceso del parque automotor en los predios universitario

Art.8.- Los fines de la Universidad Técnica Estatal de Quevedo, son los siguientes:

1. Desarrollo del talento humano en concordancia con los principios y valores institucionales, para que, comprendiendo la realidad del Ecuador y del mundo, pueda enfrentarla en forma crítica, contribuyendo eficazmente a la construcción de una sociedad justa y solidaria.
2. Acceso a la educación superior a todos los estratos sociales, sin discriminación, para contribuir al mejoramiento de la calidad de vida de la población.
3. Desarrollo de la investigación científica y técnica orientada a solucionar los problemas de la sociedad ecuatoriana, tendiente a mejorar la productividad, la competitividad, el manejo sustentable de los recursos naturales, y a satisfacer las necesidades básicas de la población más vulnerable del Ecuador.
4. Fortalecimiento de la relación con todos los sectores de la sociedad, difundiendo su misión y visión, promocionando el conocimiento, la interculturalidad, práctica de principios y valores, integración y conservación del ambiente.
5. Fomento del intercambio de ciencia y tecnología, con instituciones de reconocido prestigio nacional e internacional.

6. Formación de profesionales, que por sus conocimientos científicos, tecnológicos, valores éticos y morales y el cultivo de su talento creador, contribuyan eficazmente al bienestar de la colectividad.

CAPÍTULO III.

METODOLOGÍA DE INVESTIGACIÓN

3.1. Métodos utilizados en la investigación

Para la realización del presente trabajo se utilizaron diferentes métodos de investigación:

- Método analítico: Utilizado para analizar los diferentes escenarios de redes lógicas y su desempeño en la transmisión de información a través de estas para cada uno de los procesos de la UTEQ, además de utilizarlo para definir qué equipos se ajustan de mejor manera a la administración de las Vlans.

- Método deductivo: Se lo utilizo para estudiar probables escenarios de aplicación de las Vlans, dependiendo de los servicios de red a utilizarse.

3.2. Pasos del desarrollo de la Investigación.

Para el desarrollo del presente trabajo, se realizó un inventario de equipos de comunicación con lo que cuenta la universidad, para determinar cuales se ajustan para llevar a cabo la creación de Vlans, exclusivamente los equipos que trabajen a nivel de capa dos. Así también obtener el mapa de procesos para identificarlos y proponer un escenario para cada uno de ellos.

Con la recopilación de la información mencionada, se realizaron pruebas en ambiente de laboratorios para determinar el rendimiento de las mismas aplicando configuraciones y determinar la más óptima.

3.3. Construcción metodológica del objeto de Investigación

La investigación se realizó en el campus “Ing. Manuel Haz Álvarez” ubicado en el Km 1/2 de la vía a Santo Domingo, cantón Quevedo, provincia de Los Ríos. En las diferentes edificaciones tanto de áreas administrativas como facultades.

3.4. Elaboración del Marco Teórico

Se utilizó la investigación a través de fuentes bibliográficas de varios autores, para contar con amplia bibliografía. La información recopilada permitió conocer varias alternativas en lo referente a Redes Virtuales y llevar a cabo una propuesta que se ajuste a las necesidades de la Institución.

3.5. Recolección de Información Empírica

Para la realización del trabajo fue necesario obtener información de las características del hardware de red de la Universidad, en especial los Switches que forman parte de la red, y determinar cuáles cumplían con los requerimientos para aplicar redes virtuales.

3.6. Descripción de la Información Obtenida.

La UTEQ cuenta con una infraestructura de red bastante sólida, ya que su principal medio de transmisión en la fibra óptica, formando este medio parte del backbone principal que permite llegar a cada una de las edificaciones de la institución, además se cuenta con Switches de la marca Cisco, modelo Catalyst 2960, estos equipos se ajustan de manera idónea para realizar una administración con redes virtuales, ya que trabajan a nivel de capa 2.

Para determinar con cuantas redes virtuales podemos trabajar se revisó el mapa de procesos de la institución para proponer una solución que se ajuste a los requerimientos de comunicación de la institución.

3.7. Análisis e Interpretación de Resultados

Los pruebas y configuraciones se las realizo a nivel de laboratorio en donde se aplicaron diferentes escenarios y determinar el comportamiento de la red, tanto

en tiempos de respuesta como en tiempos de convergencia, y de velocidades de respuestas a los cambios realizados, estas configuraciones son transparentes a los usuarios finales, ya que ellos perciben las redes de comunicaciones en las velocidades en que puedan realizar sus tareas cotidianas.

Para tener una mejor perspectiva de la red con sus componentes y servicios se utilizó software exclusivo de Cisco, marca de los equipos a nivel de Switch, ya que este nos permite observar el comportamiento de las redes virtuales y de su paso a cada equipo de comunicación.

3.8. Construcción del Informe de Investigación

El informe de la investigación se elaboró teniendo en cuenta el relevamiento previo de la información, con los resultados obtenidos en las pruebas de laboratorio se llegó a un análisis para emitir criterios sobre la mejor alternativa, apoyados en la teoría recopilada en el marco teórico y en los mapas de procesos de la UTEQ, para llegar a dar conclusiones y recomendaciones que se ajusten a los requerimientos institucionales.

CAPÍTULO IV.

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS EN RELACIÓN CON LA HIPÓTESIS DE LA INVESTIGACIÓN

4.1. Hipótesis

4.1.1. Hipótesis General

La implementación de redes virtuales incidirá positivamente en la administración de las redes y sus servicios en la gestión por procesos de la UTEQ.

4.1.2. Operacionalizacion de las Variables

Tipo de Variable	Definición	Dimensión de la Variable	Indicador
Variable Independiente REDES VIRTUALES	Red de área local que agrupa un conjunto de equipos de manera lógica y no física.	Velocidad de acceso	Velocidad en Mbps Paquetes perdidos
Variable Dependiente ADMINISTRACIÓN DE REDES	Conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.	Eficiencia	Velocidad de Subida(Mbps/S) Velocidad de Bajada (Mbps/S) Cantidad de paquetes perdidos. Nro. De Vulnerabilidades.

4.2. Ubicación y descripción de la información empírica

La universidad Técnica Estatal de Quevedo, aprueba el Estatuto Orgánico de Gestión Organizacional por Procesos en segunda y definitiva instancia por el Consejo Universitario mediante resolución segunda de fecha 24 de enero del 2012, en razón del informe favorable Ministerio de Relaciones Laborales, según resolución NO. SVRE-2770

En el mismo se define la nueva estructura organizacional por procesos, determinando los procesos y el organigrama estructural.

Mapa de Procesos:

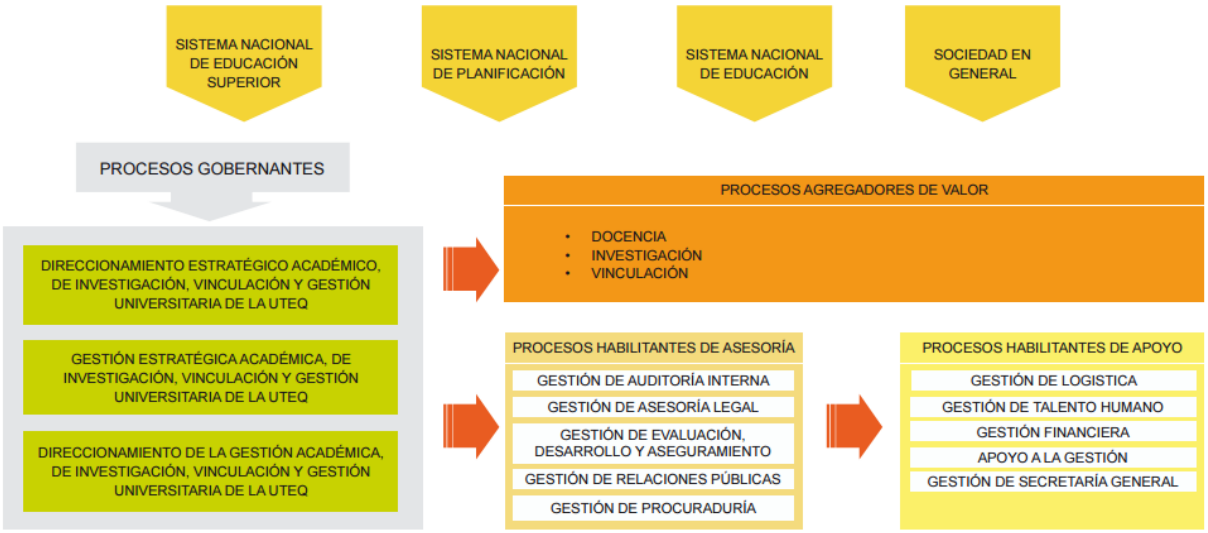


Figura 12. Mapa de Procesos de la UTEQ
Tomado del Estatuto Orgánico de Gestión Organizacional por Procesos

Organigrama estructural:

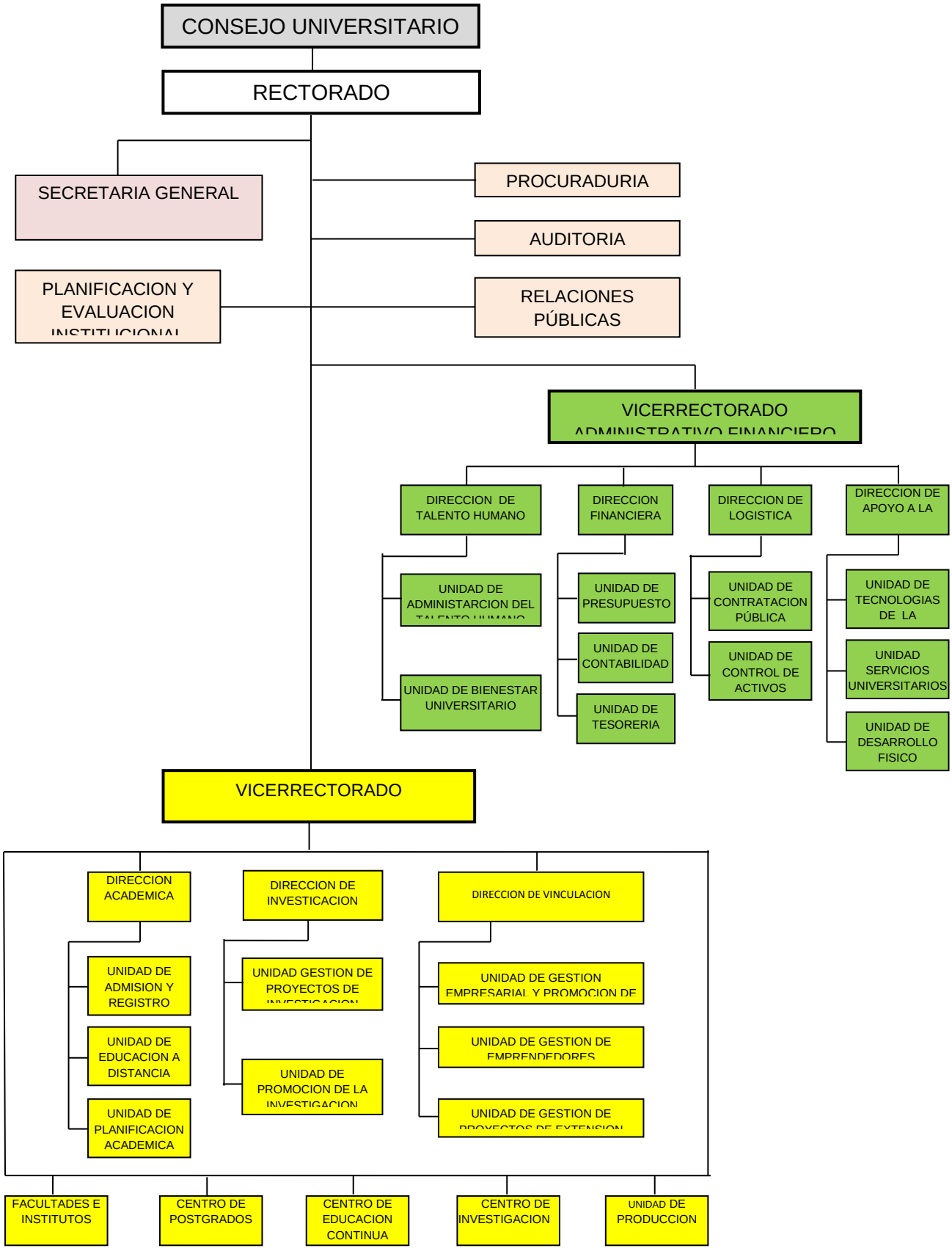


Figura 13. Organigrama Estructural de la UTEQ
Tomado del Estatuto Orgánico de Gestión Organizacional por Procesos

4.2.1. Equipos de Comunicación utilizados por la UTEQ

Los equipos utilizados en la infraestructura de la UTEQ son:

- Equipos de Última milla
- Equipos del Backbone
- Servidores

4.2.1.1. Equipos de Última milla

Son los provistos por el proveedor del servicio de Internet (ISP) y cuenta con un enlace de fibra óptica desde la central del ISP hasta el cuarto de comunicaciones de la UTEQ, usando un router Cisco 2800 con un módulo de fibra óptica para la respectiva conexión.

4.2.1.2. Equipos del backbone

La Universidad Técnica Estatal de Quevedo, cuenta con un Backbone de Fibra óptica, el mismo que permite llevar las comunicaciones a las diferentes edificaciones de la institución y por ende a cada una de las dependencias,

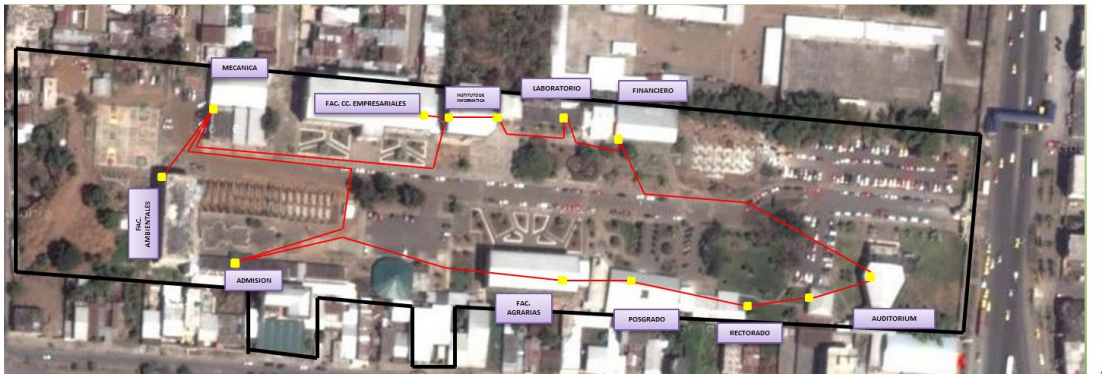


Figura 14. Backbone de Fibra óptica de la UTEQ

En la imagen, tomada del Google Maps, se observa el campus “Manuel Haz Álvarez”, las líneas en rojo es el tendido de fibra óptica que forma parte de la troncal principal de comunicaciones, el cable de fibra óptica esta tendido de manera aérea, y aparentemente pareciera una topología en anillo, sin

embargo es una topología en estrella, como se puede observar en la imagen a continuación:

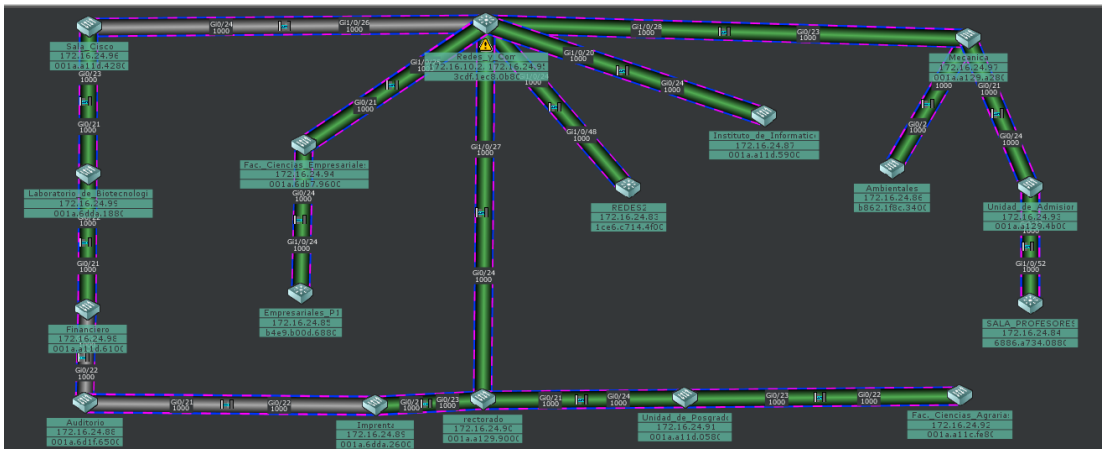


Figura 15. Topología del Backbone de la UTEQ

Esta imagen obtenida del Software de Cisco Network Assistant, permite visualizar la topología real de la red de la UTEQ, dentro de los equipos de comunicación se cuenta con un Switch de Core de la marca Cisco Modelo Catalyst 3750

Figura 16. Switch de Core, Cisco Catalyst 3750

Este equipo de capa 3 es el “corazón” de la red, es el que almacena la información de las Redes Virtuales, Vlans, a través del protocolo VTP (VLAN Trunking Protocol), en modo servidor.

También se cuenta con los switches Cisco Catalyst 2960G que sirven como switchs de distribución.

Figura 17. Switch de Distribución, Cisco Catalyst 2960G

Estos equipos se encuentran en cada dependencia donde llega el cable de fibra óptica, estos equipos se caracterizan por su robustez y durabilidad.

Dentro de los niveles de acceso se cuenta con una gama de switchs Cisco Small Business SG300

Figura 18. Switch de Acceso, Cisco Small Business SG300

También se tiene switchs de otras marcas que trabajan a nivel de capa dos.

La Universidad Técnica Estatal de Quevedo recibe el Internet de su proveedor de servicio de Internet, y este llega a un Firewall de marca Cisco, modelo ASA 5520.

Figura 19. Firewall de la UTEQ, Cisco Asa 5520

Este equipo es el encargado de proveer los servicios de Internet a toda la Universidad, así como dar seguridades tanto a la Red Interna como a la red de servidores que proveen servicios a la comunidad Universitaria.

El cuarto de equipos cuenta con sistema de energía ininterrumpida, pasando por un UPS de 120 Kva que en caso de un corte del suministro eléctrico este

los mantiene operando, contando también con un generador a diésel que permite mantener el suministro de energía de manera continua, razón por lo cual el “corazón” principal de la red se mantiene operativo los 24 horas del día, 7 días a la semana, los 365 días del año.

Se cuenta además con un dispositivo que permite administrar las redes inalámbricas, el mismo que unifica las comunicaciones dando facilidades y versatilidad en las configuraciones, este dispositivo es un Wireless Lan Controller, de Marca Cisco modelo 2500.

Figura 20. Controlador Inalámbrico, Cisco 2500 Serie

Este dispositivo funciona con los Access Point de la misma marca modelo AiroNet 2700.

Figura 21. Puntos de Acceso Inalámbricos, Cisco AiroNet 2700**.**

4.2.1.3. Servidores

Los equipos utilizados como servidores de DNS, DHCP, RADIUS, MySql, etc. Son HP e Intel, con el sistema operativo instalado dependiendo de la funciones que estos realizan, de los que se encuentran el Windows Server y Linux Centos.

Figura 22. Servidores de la UTEQ, HP Proliant 360 G7

Figura 23. Servidores de la UTEQ, Intel Xeon, Modelo SR1625UR

Estos servidores cuentan con procesadores Intel Xeon, doce gigas de memoria Ram, 4 discos duros de 500 Gb que permiten crear una configuración en array 1+0, doble fuente de poder y cuatro interfaces GigaBit Ethernet, todos son para montaje en Rack de cuatro parantes.

4.3. Discusión de la información obtenida en relación a la hipótesis.

4.3.1. Creación de Redes Virtuales

La UTEQ tiene una infraestructura de comunicaciones robusta en donde se maneja un modelo jerárquico (Núcleo – Distribución – Acceso) por lo que la aplicación de las Vlan's son totalmente factibles, es así que se determinó el uso de cuatro redes virtuales, agrupados de la siguiente manera

Administrativos: Agrupa al personal administrativo que labora en oficinas, también se puede acceder a través de la red inalámbrica, pero registrando previamente la dirección MAC del dispositivo por el cual se van a conectar a

dicha red. A continuación se presenta la cantidad de Usuarios por cada proceso.

Cuadro 1. Cantidad de Usuarios por Procesos. Administrativos

Procesos	**Nro. Usuarios**
RECTORADO	3
SECRETARIA GENERAL	3
PLANIFICACION Y EVALUACION INSTITUCIONAL	10
PROCURADURIA	3
AUDITORIA INTERNA	2
RELACIONES PUBLICAS	2
VICERRECTORADO ADMINISTRATIVO FINANCIERO	3
Dirección de Talento Humano	1
Unidad de Administración del Talento Humano	6
Unidad de Bienestar Universitario	4
Dirección Financiera	2
Unidad de Presupuesto	2
Unidad de Contabilidad	4
Unidad de Tesorería	2
Dirección de Logística	1
Unidad de contratación Pública	3
Unidad de Control de Activos	3
Dirección de Apoyo a la Gestión	1
Unidad de Tecnologías de la Información	14
Unidad de Servicios Universitarios	5
Unidad de Desarrollo Físico	4
TOTAL DE USUARIOS	**78**

Fuente: Unidad de Tics

Además a esta red de conectaran las coordinaciones de carrera y demás docentes que realicen labores administrativas en sus respectivas Facultades.

Cuadro 2. Cantidad de Usuarios por Procesos. Docentes con funciones Administrativas.

Coordinaciones	**Nro. Usuarios**
FACULTAD DE CIENCIAS AMBIENTALES	
Decano	2
Carrera de Gestión Ambiental	2
Carrera de Eco Turismo	2
Carrera de Forestal	2
FACULTAD DE CIENCIAS AGRARIAS	
Decano	2
Carrera de Ingeniería Agronómica	2
Carrera de Admin. Empresas Agropecuarias	2
FACULTAD DE DERECHO	

Decano	1
Coordinador Jurídica	2
FACULTAD DE CIENCIAS EMPRESARIALES	
Decano	2
Subdecano	2
Coordinador carrera Marketing	4
Coordinador carrera Administración Financiera	4
Coordinador carrera Economía	4
Coordinador carrera Contabilidad y Auditoria	4
Coordinador de carrera de Gestión Empresarial	4
FACULTAD DE CIENCIAS DE LA INGENIERIA	
Decano	2
Subdecano	2
Coordinador carrera de Telemática	2
Coordinador carrera de Ing. Sistemas	3
Coordinador carrera Ing. Agroindustrial	2
Coordinador carrera Ing. Mecánica	2
UNIDAD DE ESTUDIOS A DISTANCIA	
Director	2
Subdirector	2
Coordinador carrera Secretariado Ejecutivo	2
Coordinador carrera Sistemas	3
Coordinador carrera agropecuaria	4
Coordinador carrera marketing	3
Coordinador carrera contabilidad y auditoria	3
Coordinador carrera Gestión Pública y Municipal	2
Coordinador carrera Enfermería	2
Coordinador carrera Industrial	2
TOTAL	**79**

Fuente: Unidad de Tics

Docentes: Agrupa a los académicos cuya conexión se la realiza a través de los computadores que se encuentran en los cubículos de acompañamiento docentes.

Cuadro 3. Cantidad de Usuarios por Procesos. Docentes

DESCRIPCION CUBICULOS	**CANTIDAD**
FACULTAD DE CIENCIAS EMPRESARIALES	76
FACULTAD DE CIENCIAS AGRARIAS	30
FACULTAD DE CIENCIAS AMBIENTALES	35
FACULTAD DE CIENCIAS DE LA INGENIERIA	50
UNIDAD DE ESTUDIOS A DISTANCIA	40
TOTAL DE CUBICULOS	**231**

Fuente: Unidad de Tics

Laboratorios: Esta red Virtual agrupa los laboratorios de cómputo a servicio de la comunidad Universitaria, esta red tiene limitaciones en cuanto al ancho de banda.

Cuadro 4. Número de Laboratorios UTEQ.

DESCRIPCION LABORATORIOS	CANTIDAD
UNIDAD DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN	260
FACULTAD DE CIENCIAS EMPRESARIALES	80
FACULTAD DE CIENCIAS AGRARIAS	40
FACULTAD DE CIENCIAS AMBIENTALES	20
FACULTAD DE CIENCIAS DE LA INGENIERIA	20
UNIDAD DE ESTUDIOS A DISTANCIA	20
TOTAL DE EQUIPOS	**440**

Fuente: Unidad de Tics

Wireless: Esta red lógica sirve para que los estudiantes y docentes, de manera especial, puedan acceder al Internet a través de la red Inalámbrica WiFi-UTEQ y Docentes respectivamente.

Cuadro 5. Número de Docentes y Estudiantes UTEQ.

DESCRIPCION	CANTIDAD
Docentes (2014-2015)	**344**
Estudiantes (2014 - 2015)	**7.694**

Fuente: Sistema Académico - Sicau

4.3.2. Direccionamiento IP de Redes Virtuales

Se determinó las direcciones IP por cada VLAN de la siguiente manera:

Administrativo.

Para esta red se determinó que existe un requerimiento de 157 host, por lo que para determinar qué dirección IP vamos a utilizar usamos la fórmula 2^M – 2, donde M es el número de bits disponibles en la porción de host y -2 porque la primer y ultima dirección IP de la subred no se utilizan por pertenecer a la dirección de red y broadcast.

Entonces:

2^7 = 128 - 2 = 126 host

Si utilizamos 7 bits de la porción de host nos da un total de 126 host, lo que obviamente no satisface el requerimiento mínimo para esta red virtual, por lo que se utilizará un bit más de la porción de host siendo:

2^8= 256 -2 = 254 host

Se asignara la siguiente dirección de red clase C privada.

Cuadro 6. Direccionamiento IP para red de Administrativo.

RED	MASCARA	PRIMERA IP	ULTIMA IP	NRO. HOST
192.168.100.0	255.255.255.0	192.168.100.1	192.168.100.254	254

En el Switch de Core se crea la Vlan Administrativo el identificador Nro. 7

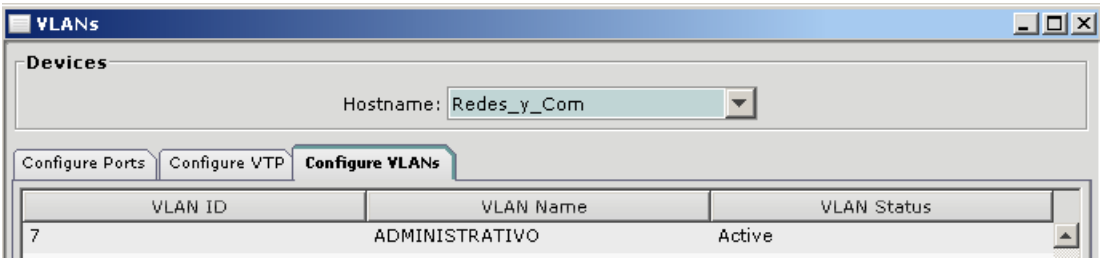


Figura 24. Creación de Vlan Administrativo

Para la administración de esta Vlan se colocó un servidor con sistema operativo ClearOS Community, en mismo que ejecuta los servicios de DHCP que será el encargado de administrar las direcciones IP, Web Proxy, Control de Contenidos y Antivirus, así mismo será el encargado de enrutar esta red al Internet y demás servicios de red.

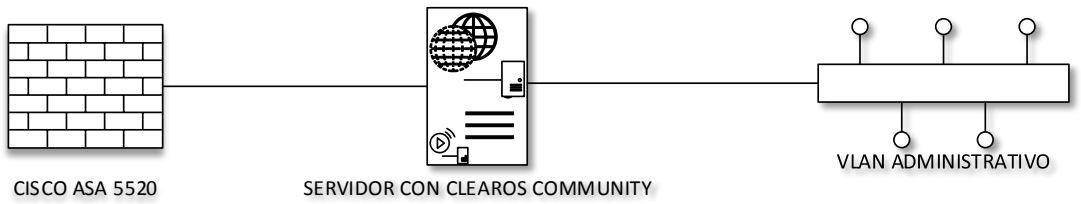


Figura 25. Diagrama de conexión de la Vlan Administrativo.

Docentes

Para esta red se determinó la cantidad de cubículos de acompañamiento Docente, dando un requerimiento mínimo de 231 host, aplicando el mismo análisis de la vlan anterior tenemos que:

2^8= 256 -2 = 254 host

Se asignara la siguiente dirección de red clase C privada.

Cuadro 7. Direccionamiento IP para red de Docente.

RED	MASCARA	PRIMERA IP	ULTIMA IP	NRO. HOST
192.168.102.0	255.255.255.0	192.168.102.1	192.168.102.254	254

Esta Vlan se la asigna con el identificador nro. 6 y descripción Docente

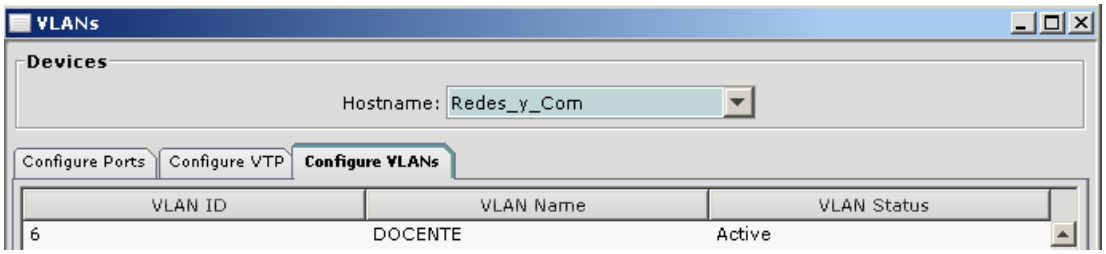


Figura 26. Creación de Vlan Docente

De igual forma para administrar las direcciones IP y, para proveer de Internet y de los servicios de red se instala un servidor con ClearOS Community

Figura 27. Diagrama de conexión de la Vlan Docente

Laboratorios.

Para esta red se determinó la cantidad de máquinas que existen en los diferentes laboratorios de la UTEQ, dándonos un requerimiento mínimo de 440 host, entonces:

2^9= 512 -2 = 510 host

Se asignara la siguiente dirección de red clase B privada.

Cuadro 8. Direccionamiento IP para red de Laboratorios.

RED	MASCARA	PRIMERA IP	ULTIMA IP	NRO. HOST
172.16.250.0	255.255.254.0	172.16.250.1	172.16.251.254	510

Esta Vlan se la asigna con el identificador nro. 2 y descripción Laboratorios

Figura 28. Creación de Vlan Laboratorios

Para esta Vlan se usara un servidor con ClearOs Community para la administración de las direcciones IP, Seguridades y para el acceso al Internet y demás servicios de red.

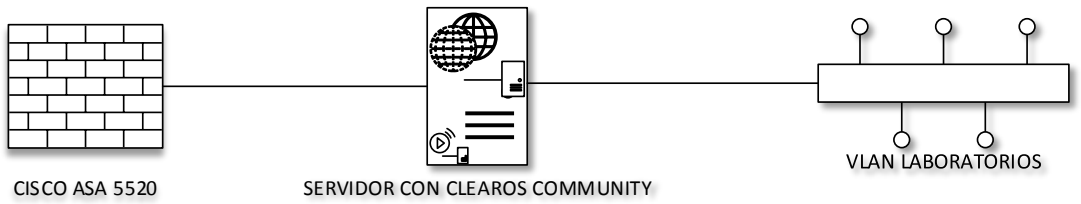


Figura 29. Diagrama de conexión de la Vlan Laboratorios

Redes Wireless

Con respecto a las redes inalámbricas, el direccionamiento se lo realizo en base a la capacidad de conexión de los equipos inalámbricos por lo que se determinó utilizar dos subredes clase C, de prefijo /24, es decir 254 host.

Cuadro 9. Direccionamiento IP para red Wifi-UTEQ.

RED	MASCARA	PRIMERA IP	ULTIMA IP	NRO. HOST
192.168.104.0	255.255.255.0	192.168.104.1	192.168.104.254	254

Cuadro 10. Direccionamiento IP para red Docentes Inalámbrica

RED	MASCARA	PRIMERA IP	ULTIMA IP	NRO. HOST
192.168.106.0	255.255.255.0	192.168.106.1	192.168.106.254	254

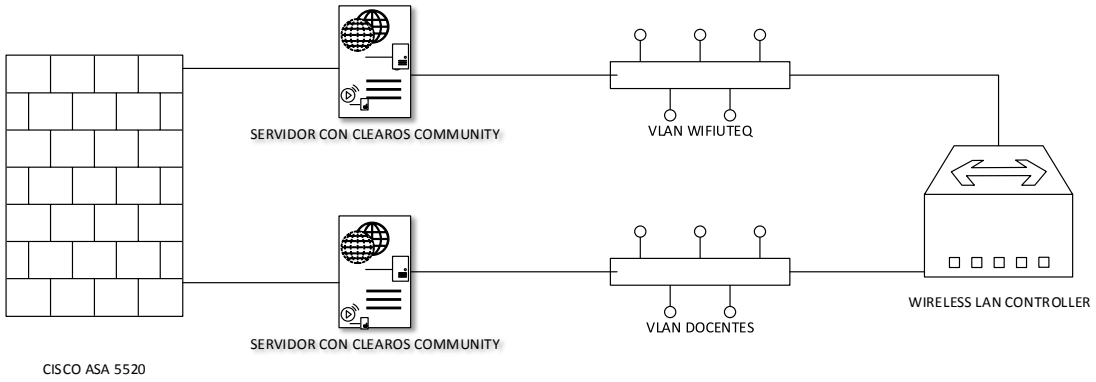


Figura 30. Diagrama de conexión de la Vlan Inalámbricas

4.3.2. Seguridad y políticas a implementarse

Las políticas generales a implementarse en las Vlans son:

- Todos los computadores en la Vlan podrán acceder a los servicios de correo electrónico y servicio web.

- Se permite el tráfico de todos los dispositivos a los servidores de red ubicados en la DMZ e INSIDE por los puertos TCP 80, 8080, 21,3128, 10000 y UDP 53.

- El tráfico entre Vlans no está permitido

- Todos los usuarios de la red solo accederán al servicio de Internet mediante el servidor que se implementara como Gateway, en la que se activaran: AntiPhishing, AntiVirus, Filtro de Contenido y un Web Proxy.

- En la Vlan Administrativo los dispositivos serán configurados con una dirección IP estática dentro del servidor de DHCP la misma que será validada mediante la dirección MAC del equipo.

- Los usuarios de las Vlan Wireless, al momento de conectarse se entregará una dirección IP dinámica mediante DHCP, e ingresando su usuario y contraseña a través de un portal cautivo y validado mediante radius.

Todas las Vlans tendrán configuradas en el Gateway un Anti Phishing y un Anti virus que permitirán darle mayor seguridad a sus usuarios, así como un control de contenidos que evitará que se ingrese a sitios indeseados y consumir ancho de banda.

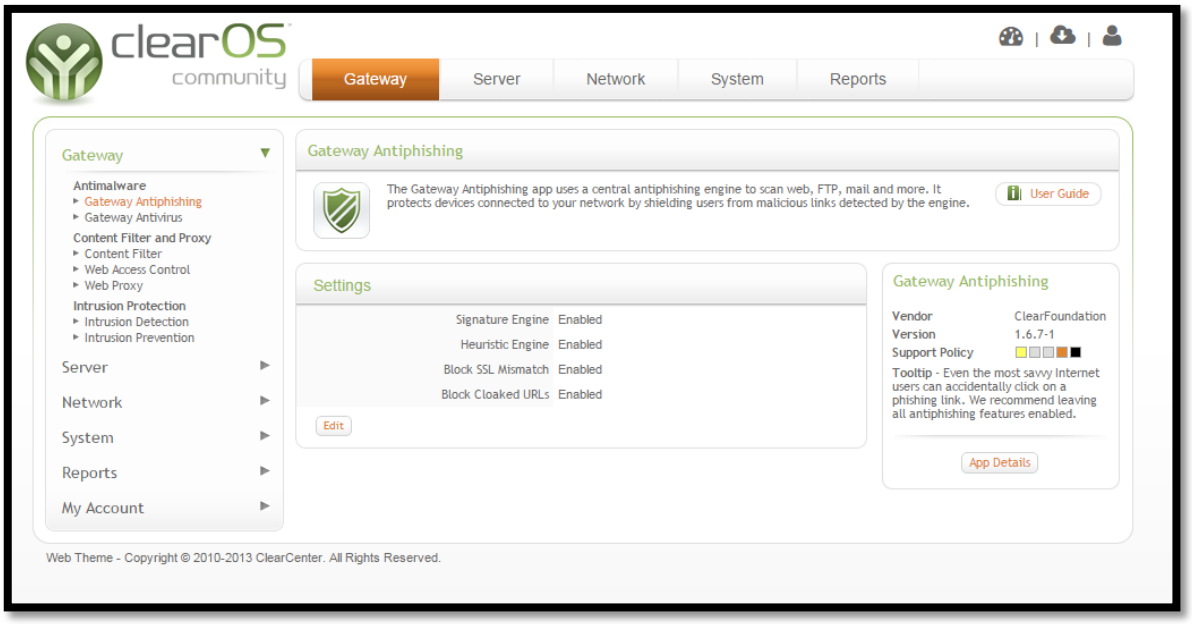


Figura 31. Ventana de configuración de motor de AntiPhishing

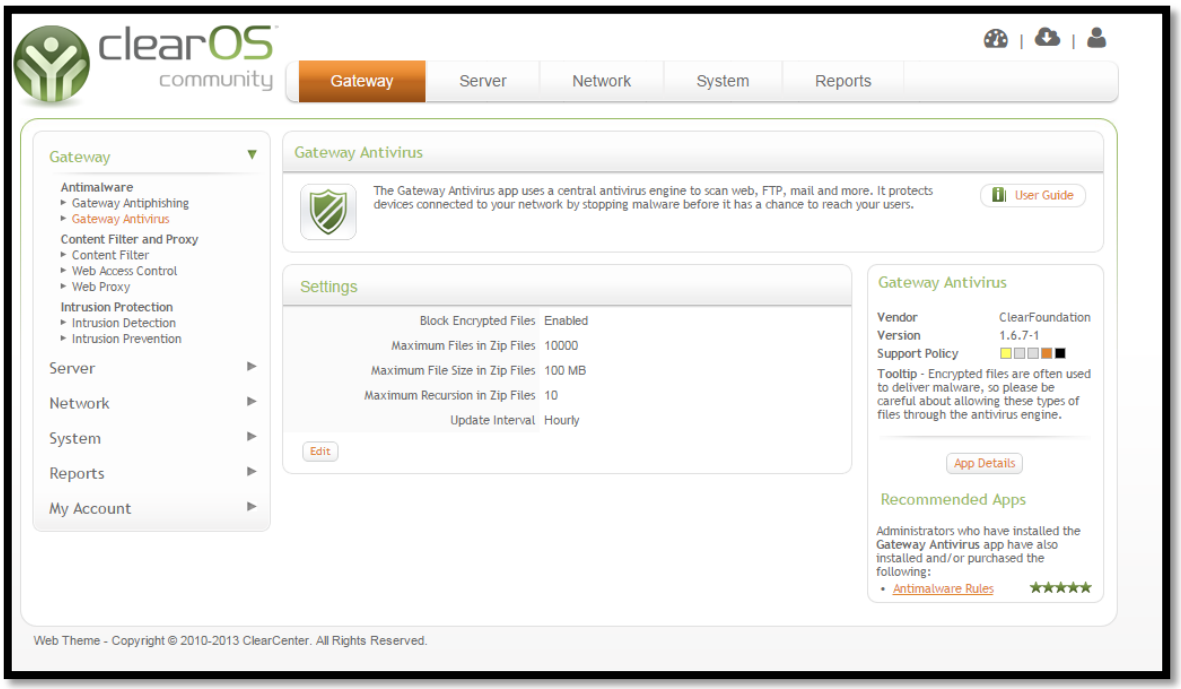


Figura 32. Ventana de configuración de motor de AntiVirus

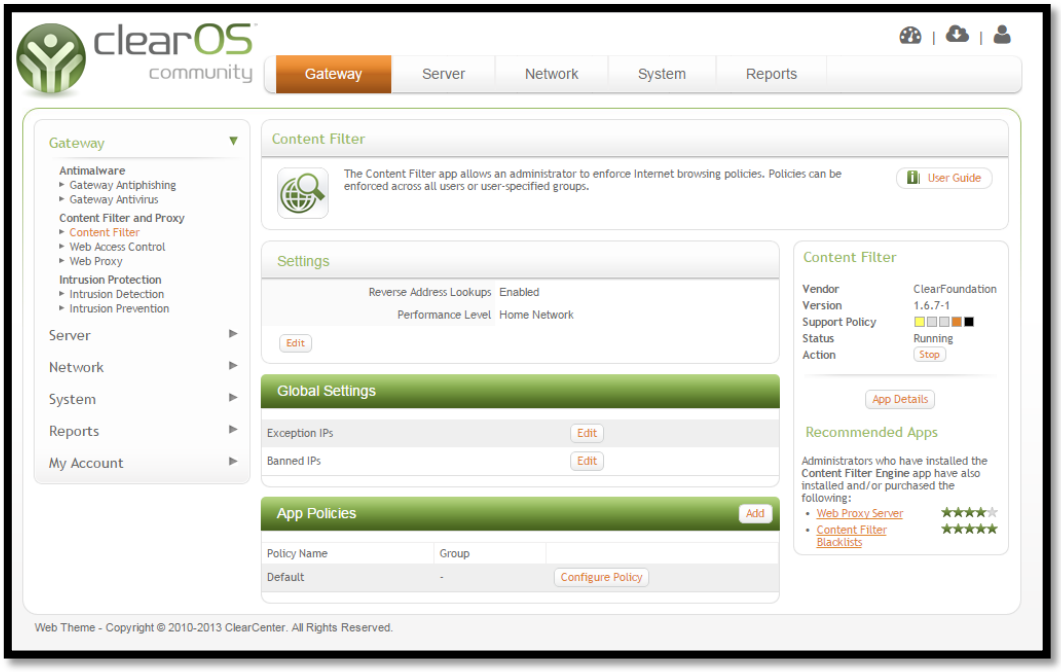


Figura 33. Ventana de configuración del Filtro de Contenidos

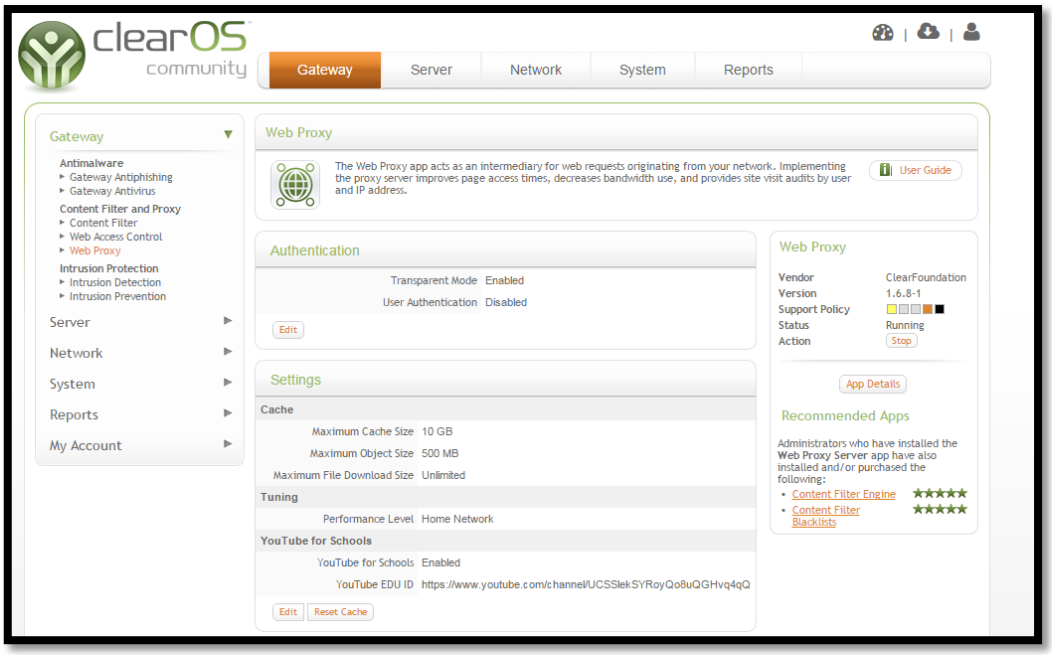


Figura 34. Ventana de configuración del Web Proxy

4.3.3. Estimación del Ancho de Banda para Vlans

Para estimar el ancho de banda para las Vlans se realizó una muestra del tráfico para determinar el flujo datos que se transmiten por la red y obtener valores referenciales para aplicar reglas de segmentación del ancho de

banda. Este muestreo se lo realizo durante una semana de labores normales dentro de la Institución, de lo cual se obtuvieron los siguientes valores:

Cuadro 10. Estimación Ancho de Banda Vlans Administrativo

Aplicación	**Usuarios**	**Datos (Kbps)**	**Capacidad (Kbps)**
Sistema Financiero Olympo	11	36	396
Sistema de Control de Personal	11	36	396
Sistema de Gestión Documental	78	56	4368
Sistema Académico SICAU	79	56	4424
Correo Electrónico	157	56	8792
Navegación	157	56	8792
TOTAL		**296**	**27.168**

Fuente: Unidad de Tics

Cuadro 11. Estimación Ancho de Banda Vlans Docentes

Aplicación	**Usuarios**	**Datos (Kbps)**	**Capacidad (Kbps)**
Sistema Académico SICAU	157	56	8792
Sistema Académico SAKAI	157	56	8792
Correo Electrónico	157	56	8792
Navegación	157	56	8792
TOTAL		**224**	**35.168**

Fuente: Unidad de Tics

Cuadro 12. Estimación Ancho de Banda Vlans Wifi-UTEQ

Aplicación	**Usuarios**	**Datos (Kbps)**	**Capacidad (Kbps)**
Sistema Académico SICAU	100	56	5600
Sistema Académico SAKAI	100	56	5600
Correo Electrónico	100	56	5600
Navegación	100	56	5600
TOTAL		**224**	**22.400**

Fuente: Unidad de Tics

Para determinar el ancho de banda para la Vlan Wifi-UTEQ, se consideró en base al tráfico obtenido un estimado de 100 usuarios concurrentes, ya que si se observa el Cuadro 5 existen un total de 7.694 estudiantes, sin embargo esto no significa que este número de alumnos van a querer conectarse al mismo tiempo.

Cuadro 13. Estimación Ancho de Banda Vlans Laboratorios

Aplicación	**Usuarios**	**Datos (Kbps)**	**Capacidad (Kbps)**
Sistema Académico SICAU	80	56	4480
Sistema Académico SAKAI	80	56	4480
Correo Electrónico	80	56	4480
Navegación	80	56	4480
TOTAL		**480**	**17.920**

Fuente: Unidad de Tics

En la Vlans para los Laboratorios se estimó que se conectaran 80 usuarios de manera concurrente, esto significa en horas en la que los laboratorios estén siendo usados a un 100% de su capacidad.

Cuadro 14. Estimación Ancho de Banda Vlans Wifi-Docentes

Aplicación	**Usuarios**	**Datos (Kbps)**	**Capacidad (Kbps)**
Sistema Académico SICAU	50	56	2800
Sistema Académico SAKAI	50	56	2800
Correo Electrónico	50	56	2800
Navegación	50	56	2800
TOTAL		**480**	**11.200**

Fuente: Unidad de Tics

Para establecer el ancho de banda en la red Wireless para los docentes se consideraron 50 usuarios simultáneos.

Mediante las estimaciones del Ancho de Banda de cada Vlans, expresadas en Kbps, se determina que el ancho de banda necesario para cada red es la siguiente,

Cuadro 15. Ancho de Banda Vlans

VLAN	ANCHO DE BANDA (Mbps)
Administrativo	20
Docente	30
Laboratorios	20
Wifi-UTEQ	20
Wifi-Docentes	10
TOTAL	**100**

Fuente: Unidad de Tics

El ancho de banda con que cuenta la UTEQ para el servicio de Internet es de 100 Mbps, si se observan los cuadros anteriores, se aprecia que hay Vlans como por ejemplo la Administrativo 27.168 Kbps expresados en Mbps es 26 Mbps, y en la Docente 35.168 expresados a Mbps da 34, si se suman los anchos de banda de todas las Vlans dan un total de 110 Mbps, lo cual sobrepasa en 10 Mbps lo contratado por la institución, razón por lo cual se establece en 20 y 30 Mbps las Vlans Administrativo y Docente respectivamente.

Las configuraciones de los anchos de banda en cada Vlans se configuraran en el sistema operativo ClearOS en el apartado de Administrador de Ancho de Banda.

Figura 35. Ventana de configuración para el Ancho de Banda

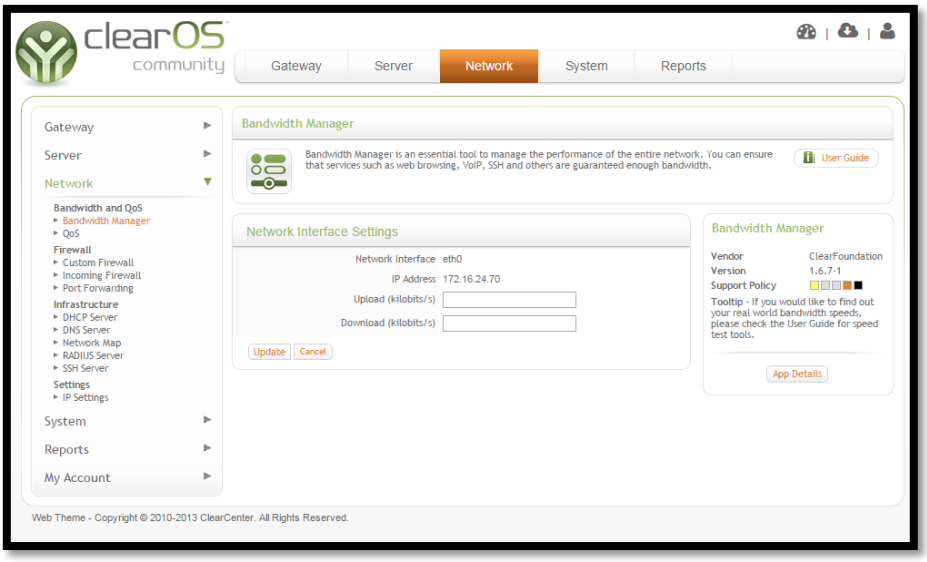


Figura 36. Configuración de la Interface de Salida al Internet (WAN)

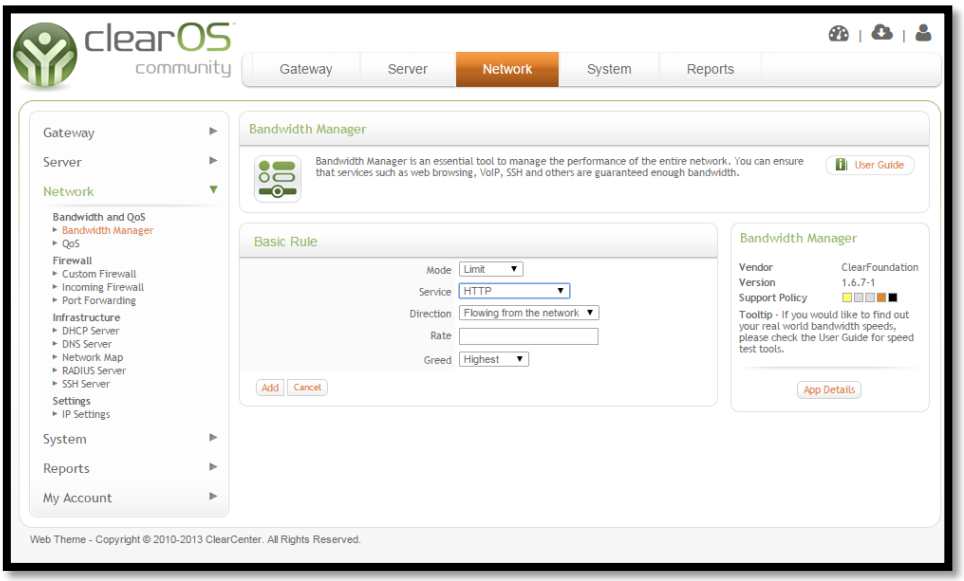


Figura 37. Configuración del AB con reglas Básicas

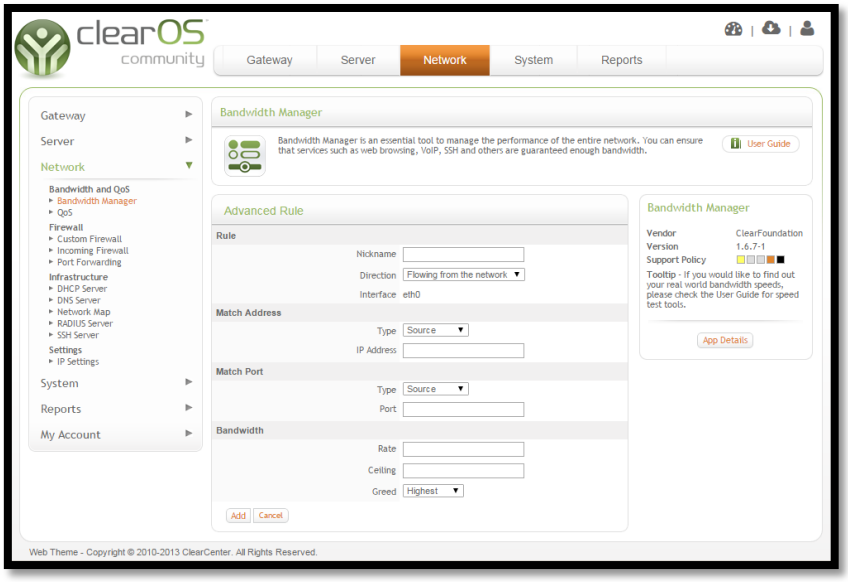


Figura 38. Configuración del AB con reglas Avanzadas

4.4. Conclusión Parcial.

En las redes lógicas Docente y Administrativo ha habido una mejor administración, ya que se ha agrupado a estos dos estamentos permitiendo un mejor control con respecto a los equipos conectados a la red, estas dos redes Lógicas, pasan a través de servidores que hacen de gateway para proveer el servicio de Internet, establecer seguridades como AntiPhishing, Antivirus, administración del anchi de banda, así también el direccionamiento IP se lo lleva a través de un servidor de direcciones dinámicas, evitando duplicación de direcciones.

La red Laboratorios se maneja de igual manera que en las dos anteriores, un Servidor que funciona como Gateway, con las mismas aplicaciones de seguridad que los anteriores, con la administración del ancho de banda, y se administran las direcciones IP de manera dinámica.

La Red Inalámbrica, cuenta con su propio servidor de acceso a internet, donde se manejan las direcciones IP de manera dinámica, cuenta con un sistema de autenticación basado en radius y mysql que en conjunto con el Wireless Lan Controller permite el acceso a los estudiantes a esta red.

CAPÍTULO V:

CONCLUSIONES GENERALES Y RECOMENDACIONES

5.1. Conclusiones.

Mediante la revisión del Estatuto Orgánico de Gestión Organizacional por procesos de la UTEQ, se pudieron determinar los nuevos procesos que forman parte de la nueva estructura de la UTEQ, y poder plasmarlos en redes más pequeñas que permitan una mejor administración, y además poder determinar los requerimientos a nivel de host para establecer un nivel de direccionamiento IP.

El ancho de banda se lo contrala a través de los servidores gateway que se encuentra en el borde de cada red, esta tarea se la realiza de manera dinámica, lo que significa que cuando varios usuarios se conecten simultáneamente, este balancee el ancho de banda, proporcionándoles equitativamente los requerimientos de comunicación.

Las Seguridades se aplican a nivel de Gateway con las aplicaciones de AntiPhishing, AntiVirus y Filtro de Contenidos para asegurar a los usuarios una red segura y confiable.

La segmentación en redes más pequeñas, ha sido beneficioso en la administración y permite llevar un mejor control del inventario de equipos y de direcciones de red.

5.2. Recomendaciones

Para que esta estructura basada en redes virtuales pueda seguir creciendo, se debe de contar siempre con equipos activos que soporten la administración de Vlans, específicamente Switchs de capa 2, por lo que es importante que cuando se realicen proyectos de Networking se consideren estos equipos.

Considerar la adquisición de un equipo de Gestión de seguridad unificada (UTM) por cuanto permite unificar la administración de seguridades y poder controlarlas.

Aumentar el ancho de banda del servicio de internet, por cuanto la universidad está en constante crecimiento, además de que en la actualidad las aplicaciones están se encuentran siempre en línea.

BIBLIOGRAFÍA.

Abad Domingo, A. (2013). Redes locales. España: McGraw-Hill España.

Angel Maldonado, J. (2011). Gestión de procesos (o gestión por procesos). España: B - EUMED.

Arnedo Moreno, J. (2013). Redes de Comunicaciones. España: Editorial UOC.

Cadenas Sanchez, X., & Zaballos Diego, A. (2011). Guía de sistemas de cableado estructurado. España: Ediciones Experiencia.

Castaño Ribes, R., & López Fernández, J. (2013). Redes Locales. España: Macmillan Iberia, S.A.

Cedano Olvera, M., Rubio González, J., & Vega Gutiérrez, A. (2014). Fundamentos de computación para ingenieros. México: Larousse - Grupo Editorial Patria.

Cruz Herradón, A. (2013). Internet y correo electrónico. España: Editorial CEP, S.L.

Hillar, G. C. (2009). Redes: diseño, actualización y reparación. Argentina: Editorial Hispano Americana HASA.

Íñigo Griera, J., Barceló Ordinas, J. M., & Cerdà Alabern, L. (2008). Estructura de redes de computadores. España: Editorial UOC.

Katz, M. (2013). Redes y seguridad. México: Alfaomega Grupo Editor.

Molina Robles, F. J. (2014). Redes Locales. España: RA-MA Editorial.

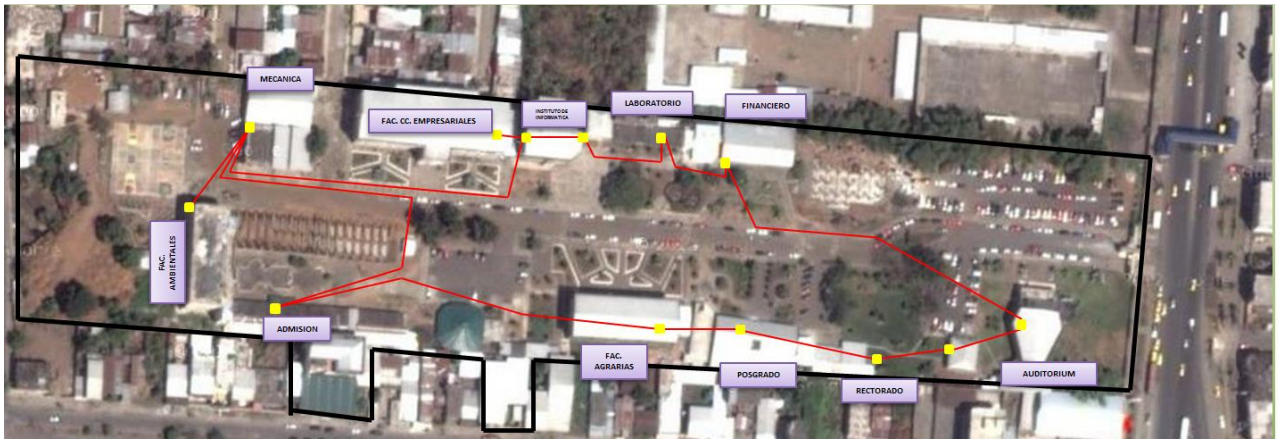
Moreira Delgado, M. (2009). Gestión por procesos y su aplicación en la organización de información de Empresa de Telecomunicaciones de Cuba, S.A. Cuba: B - Ciencias de la Información.

Moreno Pérez, J. C., & Santos González, M. (2014). Sistemas Informáticos y Redes Locales. España: RA-MA Editorial.

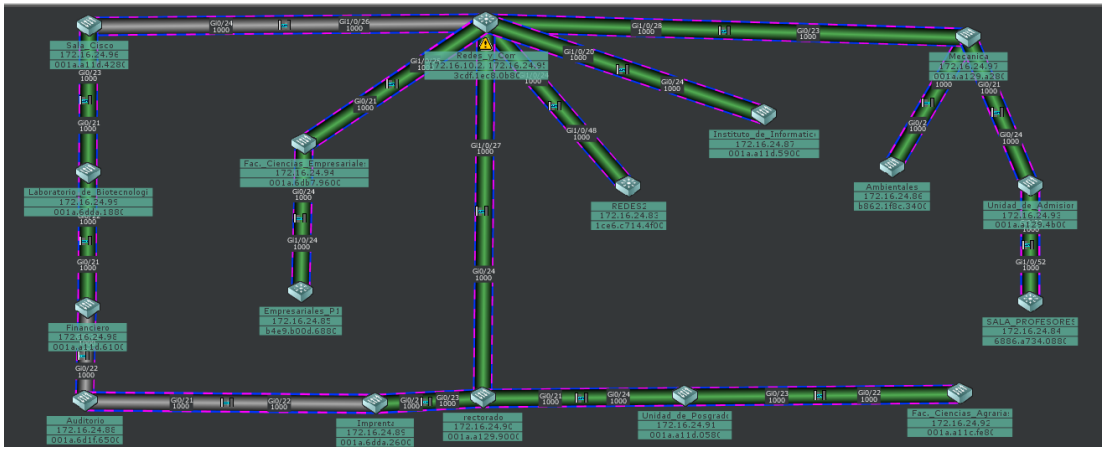
Santos González, M. (2014). Diseño de redes telemáticas. España: RA-MA Editorial.

ANEXOS

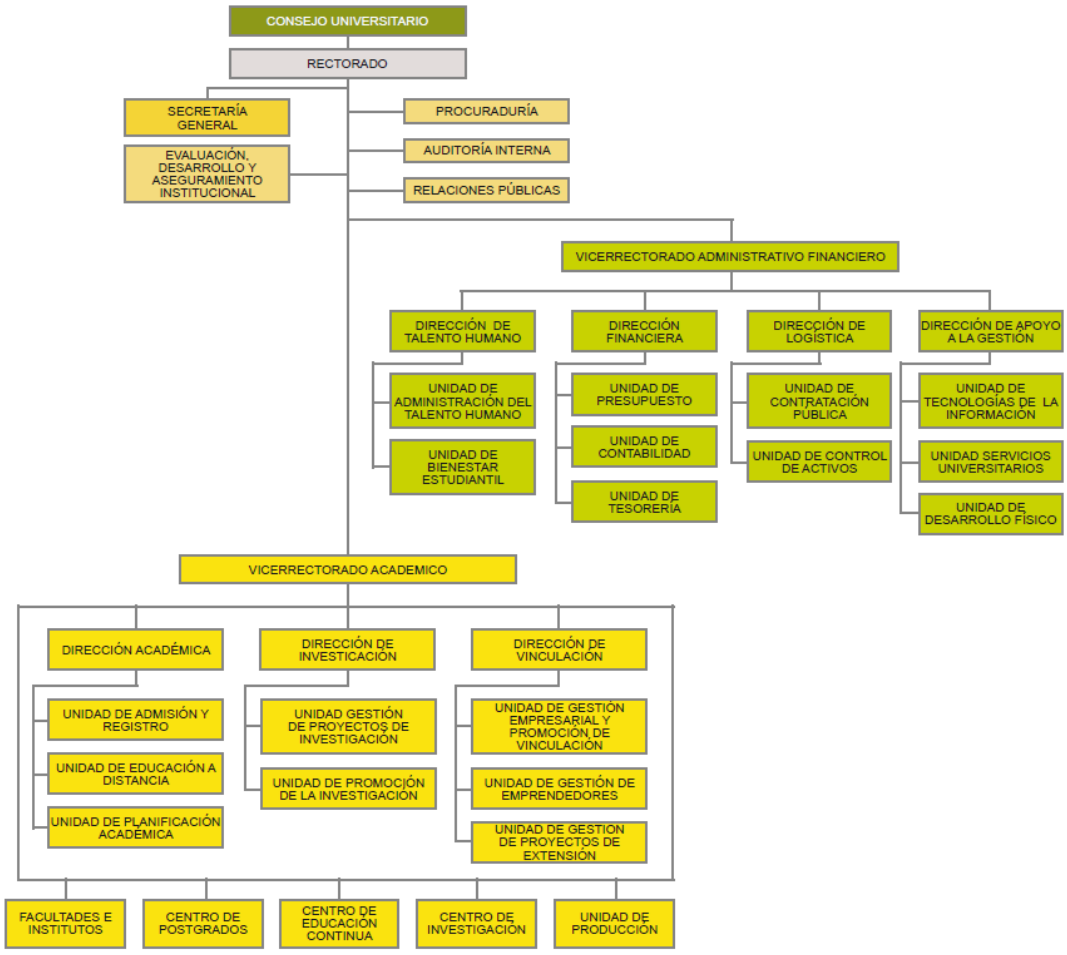
Campus “Manuel Haz Álvarez”



Backbone Principal de la Red



Estatuto Orgánico de Gestión Organizacional por Procesos
Organigrama Estructural:



Gateway Antiphishing

The Gateway Antiphishing app protects users from phishing – scam messages that attempt to extract sensitive information such as credit card numbers, passwords and personal information. For those of you who have not seen a few samples of “important messages from your bank”, you can read more about phishing.

Installation

If your system does not have this app available, you can install it via the Marketplace.

Menu

You can find this feature in the menu system at the following location:

Gateway Antimalware Gateway Antiphishing

ClearCenter Antimalware Updates

The open source ClamAV solution is the antiphishing engine used in ClearOS. This software automatically checks for updates several times a day for new antiphishing signatures. This is already included in ClearOS for free!

In addition, the ClearCenter Antimalware Updates service provides additional daily signature updates to improve the effectiveness of the antiphishing system. These signatures are compiled from third party organizations as well as internal engineering resources from ClearCenter. We keep tabs on the latest available updates and fine tune the system so you can focus on more important things.

Configuration

Antiphishing configuration is mostly a matter of fine tuning some policies based on your network needs. In the majority of cases, we recommend enabling all of the antiphishing features.

Signature Engine

Antiphishing signatures (similar to antivirus signatures) are included and maintained by the ClearOS system. The only time you should consider disabling this feature is when you find yourself with a hard to find false positive.

Heuristic Engine

The antiphishing engine uses a basic algorithm to detect phishing attempts. Though this can occasionally trigger a false positive, we recommend leaving this option enabled.

Block SSL Mismatch

A common phishing attack will use a non-secure web address to actually perform the attack, but display the web address to the user as a secure/SSL address. With this feature enabled, the antiphishing software will detect and reject this tactic.

Block Cloaked URLs

Some scammers use special encoding in web addresses (URLs) in an attempt to trick end users. Any URLs that have certain encoding characteristics will be blocked with this feature enabled.

Gateway Antivirus

The Gateway Antivirus app protects your network from viruses. The engine is used by various parts of your ClearOS system:

- Content Filter
- Mail Antivirus
- Antimalware File Scan

Installation

If your system does not have this app available, you can install it via the Marketplace.

Menu

You can find this feature in the menu system at the following location:

GatewayAntimalwareGateway Antivirus

ClearCenter Antimalware Updates

The open source ClamAV solution is the antivirus engine used in ClearOS. This software automatically checks for updates several times a day for new antivirus signatures. This is already included in ClearOS for free!

In addition, the ClearCenter Antimalware Updates service provides additional daily signature updates to improve the effectiveness of the antivirus system. These signatures are compiled from third party organizations as well as internal engineering resources from ClearCenter. We keep tabs on the latest available updates and fine tune the system so you can focus on more important things.

Configuration

Block Encrypted Files

Some file formats, including zip files, can be optionally encrypted and password protected. The antivirus system is not able to properly scan these password protected files. Since many virus writers use this technique to bypass virus checking, you may want set your network policy to completely block encrypted files.

Maximum Files in Zip Files

When the antivirus system unpacks a compressed archive (zip file), a limit on the number of files is recommended to protect the system from a potential denial of service attack. For this reason, we do not recommend setting this to unlimited.

Maximum File Size in Zip Files

The vast majority of viruses are delivered in small files. In order to preserve system resources, any file over the Maximum File Size limit will not be scanned for viruses.

Maximum Recursion in Zip Files

A zip file can contain a zip file, which contains a zip file, inside another zip file, within a zip file, etc. This technique of embedding multiple layers of zip files can be used to create a denial of service attack. Keep this setting at the default unless you have very unusual requirements.

Update Interval

The open source antivirus engine (ClamAV) in ClearOS will check for new virus signatures on a regular interval. Unless you are running on a very slow Internet connection, keep the update interval at the minimum.

Content Filter

The content filtering software blocks inappropriate websites from the end user. The software can also be used to enforce company policies; for instance, blocking personal webmail sites like Hotmail can decrease lost productivity at the office.

The filter engine uses a variety of methods including phrase matching, URL filtering and black/white lists. Although the filter works effectively 'out-of-the-box', for best results, we recommend subscribing to a service level the includes the 'Content Filter Update' service (see Services link below). By keeping your blacklist up-to-date, you will be providing your LAN with the most effective blocking solution against the 'churn' of sites that change daily.

You can find more information about the underlying technology in the Content Filtering Ins and Outs document.
If you are new to ClearOS and/or setting up a content filter policies, you may want to refer to the Guide to Setting up Web Proxy, Content Filter and Access Control Guide.

Installation

If your system does not have this app available, you can install it via the Marketplace.

Menu

You can find this feature in the menu system at the following location:

GatewayProxy and FilteringContent Filter

Content Filter Updates - Blacklists

The ClearCenter Content Filter Updates service provides regular blacklist updates to improve the effectiveness of the content filter system, including blocking HTTPS sites (e.g. https://facebook.com). These blacklists are compiled from third party organizations as well as internal engineering resources from ClearCenter. We keep tabs on the latest available updates and fine tune the system so you can focus on more important things.
The Content Filter also hooks into the Gateway Antivirus and Gateway Antiphishing engines in ClearOS. You may also want to subscribe to theAntimalware Updates service to keep your content filter running at its optimum.

Blocking HTTPS, Facebook, etc

If you need to block web sites that provide access via secure HTTP (HTTPS) - for example facebook.com - then you need to enable non-transparent mode for your web proxy / content filter setup. In transparent mode, it is not possible to properly filter secure web pages since the connection to the web server is already encrypted (and unreadable) by the time it gets to the ClearOS gateway. You can change the transparent/non-transparent mode setting from the Web Proxy app.

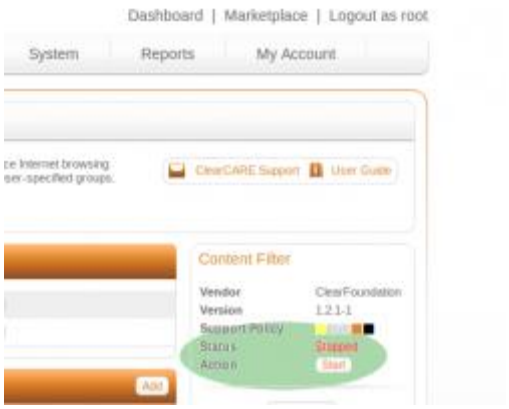
As an alternative, if you know the IP or IP range that you would like to block, you can block connections to a particular site using the Incoming Firewall and the Egress Firewall. The user will not see a helpful warning page with this alternative method, just a failed connection message in their web browser.
By design, the HTTPS protocol encrypts the payload to ensure the web browser and HTTPS server have a secure channel. This is what makes it possible to do online banking, for example. An HTTPS page cannot be scanned for keywords or other content.

However, HTTPS addresses/URLs are not encrypted. If filtering HTTPS sites is important, then the regularly updated blacklists from the Content Filter Updates paid app are recommended.

Configuration

The web-based administration tool gives you access to a number of configuration settings. The filter must be run in parallel with the Web Proxyserver.

Enable/Disable Service



The content filter service is enabled when both the content filter service is running and the proxy server. To determine if these services are running, look to the App Status bar on the right-hand-side of the web-based interface. You will find a status field along with start/stop controls to toggle the service.

Global Settings

The global settings apply to all users, regardless of the content filter group being applied to the user browsing websites from the Local Area Network (LAN). In fact, the settings explicitly exempt or ban a device on theLAN from using the proxy/content filter service. A device is identified by its source IP address.

If you are using global exemption or banned IP addresses, it is good practice to ensure these systems are assigned static IP addresses.

Group Policies

Group policy settings allow an administrator to 'fine-tune' how the content filter applies policies to different users. To do this, group policies (not to be confused with Windows AD Group Policy) are created and configured. Users are assigned to a group which dictates what policies are enforced on their browsing habits.

The content filter engine supports up to 9 different group policies - each of which can be configured to the administrators preference.

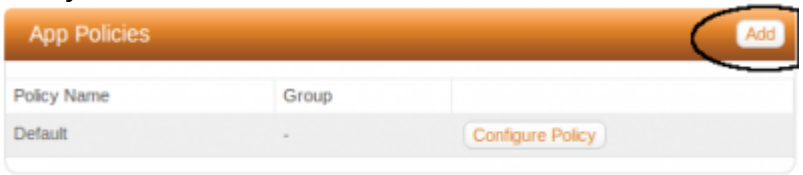
Be descriptive in naming your group policies. For example, a school might have policies named for the types of individuals that might be accessing the Internet from the school - Support Staff, Teachers, Students, Parents, Visitors etc.

When you first configure the content filter engine, one group policy is already created - named “Default”. By default, this group policy applies to all users. If a user is assigned a content filter group policy, these settings will supersede the default group policy.

The Default Group Policy cannot be deleted, nor can the default setting of 'allusers' be modified. You can (and should) modify the settings of this group to comply with the desired filtration of any user not falling into a higher up policy.

Adding a Group Policy

As previously mentioned, up to 9 (including the Default Policy) group policies can be created for the content filter. To add a policy, click Add in the Group Policy table list.



The only configuration setting to be made after you create a group policy is to assign an actual group to it. Users can be assigned to groups - this is how the filter will apply specific settings.

Filtering based on device IP addresses is not currently supported via webconfig.

Editing a Group Policy

Once you have added a group policy (or if you need to edit the default policy) it is time to edit/configure it.

Click on the “Configure Policy” link next to the group policy you wish to edit. You will see a summary of parameters/categories to edit, similar to that in the screenshot below.

General Settings

Sensitivity Level

The sensitivity level is an arbitrary scale that allows 'coarse' adjustment of the phrase filter sensitivity. Increasing the sensitivity level means that fewer bad phrases/words will cause the filter to block the page.

PICS Level

An Internet standard for rating web content. This setting will prove to be of minor significance as sites self-administrate this parameter. As a general rule, the recommendation is to disable this setting.

Reporting Level

Several options are available to customize what a user sees when the filter blocks a page:

- Stealth Mode - Site is not blocked…User's IP and site is logged
- Access Denied - User's browser will receive an 'Access Denied' in place of the web page.
- Short Report - A short error message 'bubble' will be displayed like the one below
- Full Report - Same as above, but the weighted limit and actual value will be displayed (useful for fine-tuning the system).
- Custom Report - Uses the customizable HTML template

Block IP Domains

Used to prevent users from circumnavigating the URL-based portion of the filter by using IP addresses instead of URL's. Pages will still be filtered based on the other filtering mechanisms: weightedphrases, mime types, file extensions etc.

Blanket Block

Most restrictive setting. All sites will be blocked with the exception of those listed in the exempt list. Useful for kiosks/public terminals where a browser is used to access a company site etc.

Blacklists

The content filter system uses black lists to block specific web sites. You can fine tune your content filter black lists by specifying which lists to use. Note that these lists are updated weekly by the Content Filter Update Service if you have subscribed to that service.

Phrase Lists

The content filter system uses phrase lists to calculate a score for every web page. You can fine tune your content filter scoring by specifying which phrase lists to use.

In general you will want the phrase lists you select here to correspond with the blacklists you are using. At a minimum you will want to include theproxies phrase list to prevent your users from bypassing the filter.
Note that more weighted phrases activated for the content filter mean that the filter will take more time to look at each page. It is recommended that if you are using a low powered server, you limit the number of weighted phrase lists you use and instead use more blacklists.

MIME Types

MIME types instruct a browser to utilize certain applications in order to display content encoding. Security exploits in the applications themselves can be used to infiltrate a computer. MIME types checked in the “Banned MIME Types” form will not be allowed to pass through the firewall and to the computer making the request on the LAN, providing a more secure environment.

File Extensions

Banning specific file extensions is a useful tool for limiting content available to users on the LAN. It can also greatly decrease the chances of users unwittingly downloading and running 'arbitrary' code downloaded from the Internet which could potentially contain viruses, spyware of other malicious code.

By checking a box next to an extension, you are disallowing filtered users from accessing this file type. If you wish an extension to be blocked and it is not listed in the available list, add it to the list using the “Add a new extension type” form.

Banned Sites

Sites entered in the “Banned Site List” will be banned, regardless of the site's content, or whether the site is on one of the blacklists.

Gray Sites

Sites entered in the “Grey Site List” will not be blocked by the blacklists but will still be checked for content. For example, you may have the newsblacklist enabled to prevent people from wasting time during the business day. However, you may have also decided to allow just BBC news. If you add bbc.co.uk to the exception list, all web pages will be allowed. If you add bbc.co.uk to the greylist, then most pages will pass through just fine, butthis mildly racy page and other might get blocked by the phrase list system.

Exception Sites

Sites entered in the “Exempt Site List” will be allowed, regardless of the site's content. Use this form if content on a site triggers a 'false positive' that you wish to override.

Bandwidth Manager

The bandwidth manager is used to shape or prioritize incoming and outgoing network traffic. You can limit and prioritize bandwidth based on IP address, IP address ranges and ports.

Installation

If your system does not have this app available, you can install it via the Marketplace.

Menu

You can find this feature in the menu system at the following location:

NetworkBandwidth and QoSBandwidth

Best Practices

Before getting started with the bandwidth configuration, it is important to know about best practices. There are two ways to approach bandwidth management:

- Limit low priority traffic in an effort to improve speeds for high priority traffic
- Reserve bandwidth for high priority traffic which will shuffle low priority traffic aside

It is impossible to predetermine what types of traffic will be low priority, but typically quite easy to identify important traffic (VoIP being an obvious one). Therefore, reserving bandwidth for high priority traffic is the best way to proceed with bandwidth management.

Configuration

External Interface Upload/Download Settings

The upstream and downstream rates for your external (Internet) interfaces must be specified in order to optimize the underlying bandwidth engine. If you set these values below your actual upload/download rates, then you will find your bandwidth capped by these lower values.

We recommend the SpeedTest.net online tool for measuring actual bandwidth. Please perform these tests when network traffic is low (off hours) and without a web proxy running.

If you are on a connection with a large asymmetrical ratio (e.g. 25 MB download, but only 1 MB upload), you may need to adjust your upload value to a higher value.

Add Bandwidth Rule

The basic Add Bandwidth Rule provides a simple way to specify bandwidth rules on your system. If you need more fine grained control over your bandwidth rules, see the next section: Add Advanced Rule.

Mode

There are two types of bandwidth modes available.

- Limit - clamps the bandwidth at a maximum rate
- Reserve - guarantees the specified bandwidth

With reserve mode enabled, the system will guarantee the minimum bandwidth and use more if it is available. When all the bandwidth that has been reserved/limited is in use, then the system will share the bandwidth proportionately.

Service

The network service, e.g. web traffic.

Direction

You must specify the direction of the bandwidth flow.

- Flowing to your network – a user on your LAN downloading a file over the web.
- Flowing from your network – a user on your LAN uploading a file via a peer-to-peer network.
- Flowing to your system – inbound mail going to the mail server running on your system.
- Flowing from your system – outbound mail from the system's mail server getting delivered to various locations on the Internet.

Rate

The bandwidth rate to reserve/limit in kilobits per second.

Greed

The greed level tells the bandwidth manager how to handle any extra available bandwidth on your network. Consider the following example:

- A 1000 kbps connection to the Internet
- 200 kbps reserved for web traffic, low greed
- 300 kbps reserved for mail traffic, high greed
- 500 kbps unallocated

If both mail and web traffic require 900 kbps each, mail traffic will get its full 300 kbps allotment, plus the majority (but not all) of the unallocated 500 kbps since the bandwidth rule is greedy. Web traffic will be guaranteed its 200 kbps, but will only get a small portion of the unallocated bandwidth.

Add Advanced Rule

Understanding the many options in the advanced bandwidth rules can be tricky. Please take a look at some of the examples in the next section for helpful hints.

Nickname

An easy to remember name to remind you of the purpose of the bandwidth rule.

IP Address/Range

The IP address parameter can contain:

- A single IP address
- A IP address range
- nothing

If this field is left blank, then the bandwidth rule will be used by all IP addresses will.

When specifying an IP address range with a starting and ending IP (for example, 192.168.1.100 to 192.168.1.200), each of the individual IP addresses will be assigned the configured rule. For example, the following bandwidth rule would clamp downloads from every workstation on 192.168.1.254 to a maximum of 100 kbps:

- IP Address Range - Destination - 192.168.1.1 : 192.168.1.254
- Direction - Download
- Rate - 100 kbps
- Ceiling - 100 kbps

An alternative bandwidth range can be specified using [Network Notationnetwork/netmask]]. In this case, the range of IP addresses are treated as a single bandwidth rule. For example, the following bandwidth rule would clamp downloads for 192.168.1.x to a maximum of 500 kbps:

- IP Address Range - Destination - 192.168.1.0/24
- Direction - Download
- Rate - 500 kbps
- Ceiling - 500 kbps

If only one person on the 192.168.1.0/24 network was downloading, the would get the 500 kbps. If two people were downloading, they would share the 500 kbps.

Direction

The direction of the network packet flow that you desire.

- Flowing to your network – a user on your LAN downloading a file over the web.
- Flowing from your network – a user on your LAN uploading a file via a peer-to-peer network.

Match Address

You can specify a matching address for an advanced rule. For example, if you want to limit traffic going to the LAN IP address of 192.168.1.100, you would specify this rule as a Destination type with IP 192.168.1.100.

If the IP is left empty, then all IPs will be affected.

Match Port

You can specify a matching port for an advanced rule. For example, if you would like to limit all download web traffic to your LAN, you would specify this rule as a Source type with port 80.

If the port is left empty, then all ports will be affected.

Rate

The upload/download speed to reserve (guarantee) for the service.

Ceiling

The maximum upload/download speed allowed for the service. If you would like the rule to use all available bandwidth, leave this field blank. If you set rate and ceiling to the same value, then you will be clamping bandwidth uploads at the ceiling rate.

Greed

The greed level tells the bandwidth manager how to handle any extra available bandwidth on your network. Consider the following example:

- A 1000 kbps connection to the Internet
- 200 kbps reserved for web traffic, low greed
- 300 kbps reserved for mail traffic, high greed
- 500 kbps unallocated

If both mail and web traffic require 900 kbps each, mail traffic will get its full 300 kbps allotment, plus the majority (but not all) of the unallocated 500 kbps since the bandwidth rule is greedy. Web traffic will be guaranteed its 200 kbps, but will only get a small portion of the unallocated bandwidth.

Web Proxy Gotchas

Having a web proxy configured either on a ClearOS gateway or some other local proxy server complicates matters. As soon as a web request is made via the proxy, the source IP address for the request is lost. In other words, configuring bandwidth rules using an IP address on your local network will not have an effect for any traffic going through the proxy. See the examples for ways to limit bandwidth to your proxy server.

Examples

Unless otherwise specified, fields should be left blank or with defaults.

Limit Web Proxy Downloads to 300 kbps

If you have the web proxy enabled for your network, you can limit how much bandwidth can be used for web downloads. A Basic Rule is used for limiting the speed of web downloads:

- Type: Basic
- Service: HTTP
- Direction: Flowing to the system
- Rate: 300 kbps
- Greed: Low

If you run your proxy in non-transparent or WPAD mode, you can also limit secure web traffic (HTTPS). Add a similar rule, but with HTTPS instead of HTTP:

- Type: Basic
- Service: HTTPS
- Direction: Flowing to the system
- Rate: 300 kbps
- Greed: Low

If you run your proxy in transparent mode, HTTPS traffic does not pass through the proxy. In this case, you want to limit HTTPS flows to your network:

- Type: Basic
- Service: HTTPS
- Direction: Flowing to the network
- Rate: 300 kbps
- Greed: Low

Limit Web Downloads to Workstation 192.168.1.100 to 200 kbps

Do you have a user on your network that hogs the network with downloads and video streams via a web browser? You can clamp this user to a slower speed using the following example:

- Type: Advanced
- Nickname: web_hog
- Direction: Flowing to the network
- Match Address: Destination - 192.168.1.100
- Match Port: Source - 80
- Rate: 200 kbps
- Ceiling: 200 kbps
- Greed: Medium

If you need to limit all traffic going to 192.168.1.100, remove the Match Port rule (leave it blank).

Limit Uploads from Workstation 192.168.1.100 to 200 kbps

This type of rule is useful for limiting peer-to-peer uploads for a specific user on your network.

- Type: Advanced
- Nickname: upload_hog
- Direction: Flowing from the network
- Match Address: Source - 192.168.1.100
- Rate: 200 kbps
- Ceiling: 200 kbps
- Greed: Medium

Limit Downloads from Internet Host 1.2.3.4 to 250 kbps

Software updates (for example antivirus signature updates) on desktop systems can choke a network, especially when all the systems perform the update at the same time. The following example shows how to limit downloads from 1.2.3.4 to 250 kbps (even if your Internet connection is idle).

- Type: Advanced
- Nickname: slow_sw_updates
- Direction: Flowing to the network
- Match Address: Source - 1.2.3.4
- Rate: 250 kbps
- Ceiling: 250 kbps
- Greed: Lowest

Reserve Bandwidth to/from a VoIP/SIP Provider

If you have a SIP provider for your VoIP system, you will want to reserve bandwidth for this traffic. You will need to provide two bandwidth rules – one for traffic from your provider, and one for traffic to your provider.

Traffic from SIP Provider

- Type: Advanced
- Nickname: from_sip
- Direction: Flowing to the network
- Match Address: Source - 1.2.3.4
- Rate: 800 kbps
- Greed: Highest

Traffic to SIP Provider

- Type: Advanced
- Nickname: to_sip
- Direction: Flowing from the network
- Match Address: Destination - 1.2.3.4
- Rate: 800 kbps
- Greed: Highest

Limit Bandwidth on a Specific LAN

If you have a segmented LAN network, you may want to limit bandwidth on a low priority LAN (for example, a guest wireless network). Here is an example for a limiting LAN 192.168.10.0/24 to 1000 kbps. To limit downloads from end users on the LAN:

- Type: Advanced
- Nickname: lan_10_downloads
- Direction: Flowing to the network
- Match Address: Destination - 192.168.10.0/24
- Rate: 1000 kbps
- Ceiling: 1000 kbps
- Greed: Medium

To limit uploads from end users on the LAN:

- Type: Advanced
- Nickname: lan_10_uploads
- Direction: Flowing from the network
- Match Address: Source - 192.168.10.0/24
- Rate: 1000 kbps
- Ceiling: 1000 kbps
- Greed: Medium

Units - kbit/s, kbps, Mbps, and Other Confusing Notation

Depending on where you are and who you are talking too, there are different measurement units used for bandwidth. Here are some tips to help with converting from one unit to another – capitalization is important:

Conversion tips:

- Mega is 1000 times larger than kilo
- A byte is 8 times larger than a bit

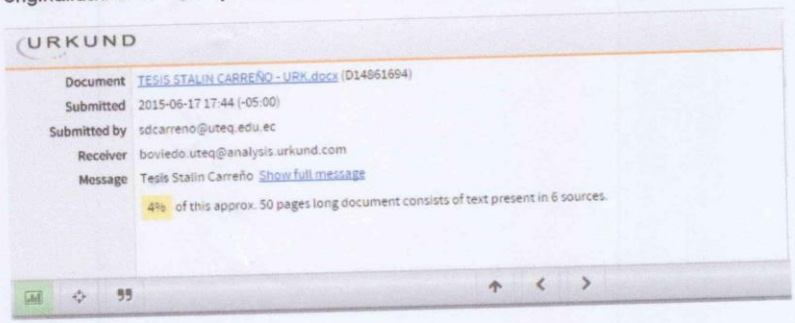
Examples:

- 1 Megabit per second is approximately 1000 kilobits per second
- 1 Megabyte per second is approximately 8000 kilobits per second

Universidad Técnica Estatal de Quevedo
.edu.ec La primera Universidad Agropecuaria del País

Quevedo, Junio 18 de 2015

Yo, Ing. Byron Oviedo Bayas, certifico que el documento final de la tesis titulada **"LA CONECTIVIDAD EN LA RED LOGICA Y SU INCIDENCIA EN LA GESTIÓN POR PROCESOS DE LA UNIVERSIDAD TECNICA ESTATAL DE QUEVEDO. 2013." IMPLEMENTACION DE REDES LAN VIRTUALES.** Elaborada por **STALIN DANIEL CARREÑO SANDOYA** egresado de la Maestria en Conectividad y Redes de Ordenadores, previo a la obtención del título de Magister cumple con los componentes que exige el Reglamento General de Grados y Títulos de la Universidad Técnica Estatal de Quevedo e incluye el informe del URKUND el cual avala los niveles de originalidad en un 96% y de copia del 4% del trabajo investigativo.


URKUND

Document	TESIS STALIN CARREÑO - URK.docx (D14861694)
Submitted	2015-06-17 17:44 (-05:00)
Submitted by	sdcarreno@uteq.edu.ec
Receiver	boviedo.uteq@analysis.urkund.com
Message	Tesis Stalin Carreño Show full message

4% of this approx. 50 pages long document consists of text present in 6 sources.

Atentamente;

Ing. Byron Oviedo Bayas, MSc.
DIRECTOR DE TESIS