UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA EN ELECTRONICA Y TELECOMUNICACIONES

"Trabajo de grado previo a la obtención del Título de Ingeniero en Electrónica y Telecomunicaciones"

TITULO DEL PROYECTO

ANALISIS COMPARATIVO DE NIVELES Y MECANISMOS DE CALIDAD DE SERVICIO PARA LA TRANSMISION DE VIDEO Y TARJETAS RFID EN LA FACULTAD DE INGENIERIA EN LA UNIVERSIDAD NACIONAL DE CHIMBORAZO

AUTORES:

ERIKA PATRICIA MEDINA GAVIDIA
CRISTIAN VINICIO PAZMIÑO JARA

Director: MSC. Anibal Llanga

Riobamba – Ecuador

2015

Los miembros del Tribunal de Graduación del proyecto de investigación de título:

ANALISIS COMPARATIVO DE NIVELES Y MECANISMOS DE CALIDAD DE SERVICIO PARA LA TRANSMISION DE VIDEO Y TARJETAS RFID EN LA FACULTAD DE INGENIERIA EN LA UNIVERSIDAD NACIONAL DE CHIMBORAZO

Presentado por:
Erika Patricia Medina Gavidia y Cristian Vinicio Pazmiño Jaray dirigida por: Msc. Anibal Llanga.

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación con fines de graduación escrito en la cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la facultad de ingeniería de la UNACH.

Para constancia de lo expuesto firman:

Ing. Carlos Peñafiel M. Eng. Presidente del Tribunal	Firma
Msc. Aníbal Llanga Director del Tema de Investigación	Firma
Ing. Fabián Gunsha Miembro del Tribunal	Firma

AUTORÍA DE LA INVESTIGACIÓN

"La responsabilidad del contenido de este Proyecto de Graduación, nos corresponde exclusivamente a: Erika Patricia Medina Gavidia, Cristian Vinicio Pazmiño Jara y del Director del Proyecto Msc. Aníbal Llanga; y el patrimonio intelectual del mismo a la Universidad Nacional de Chimborazo.

Los autores:

_____

Erika Patricia Medina Gavidia
C.I 0604179192

_____

Cristian Vinicio Pazmiño Jara
C.I 0602749319

AGRADECIMIENTO

Queremos dar gracias a Dios, por darnos la oportunidad de disfrutar la etapa universitaria y permitirnos llegar a este momento tan importante al ver culminada nuestra carrera, a nuestros padres por su apoyo en nuestra formación académica, a nuestro director de tesis Msc. Aníbal Llanga por su ayuda incondicional para guiarnos a alcanzar esta meta, y de manera especial a la Facultad de Ingeniería y a su representante Msc. Rodrigo Briones por facilitarnos el acceso a las instalaciones y darnos la apertura y confianza para el desarrollo de este proyecto.

DEDICATORIA

Dedicamos este proyecto a Dios Todopoderoso, a nuestros padres: Víctor Medina, Silvio Pazmiño, Corina Escalante y Llanett Gavidia, por su tenacidad y lucha incansable para ayudarnos frente a las circunstancias de la vida, a nuestros amigos y amigas con quienes hemos compartido gratos momentos y por brindarnos su apoyo desinteresado.

INDICE GENERAL

INDICE DE TABLAS Y FIGURAS

RESUMEN

El trabajo de investigación **"Análisis Comparativo de Niveles Y Mecanismos de Calidad de Servicio para la Transmisión de Video y Tarjetas RFID en la Facultad de Ingeniería en la Universidad Nacional de Chimborazo"** tiene como objetivo analizar los diferentes mecanismos de calidad de servicio, donde se encuentra como mejor opción para un sistema de video vigilancia la aplicación de servicios diferenciados. Para el desarrollo de la investigación se utiliza como método de investigación el método experimental y se realizó un ambiente de prueba donde se comparaban los modelos de implementación de QoS. De esta manera se implementó el sistema de video vigilancia para la Facultad de Ingeniería de la Universidad Nacional de Chimborazo, aclarando que con este sistema se prevé salvaguardar los bienes de la institución y no como un sistema de persecución o control hacia el personal administrativo, docentes y de servicio de la Facultad. Además se indica que el sistema RFID planteado al inicio de este trabajo no se implementó debido a la existencia de otro sistema de mejores características que está en pleno funcionamiento en la UNACH.

Eltrabajodeinvestigacióncontiene6 capítulos que presentan el desarrollo de la investigación de la siguiente manera:

El Capítulo I: Fundamentación Teórica, detalla la teoría usada en el estudio.

El Capítulo II: Metodología, presenta el tipo y método de investigación a realizarse, el sistema de hipótesis y la operacionalización de las variables, validación de instrumentos la población y muestra en los que se basará el trabajo.

El Capítulo III: Resultados, se valora el rendimiento de cada uno de los escenarios de prueba, tanto de la variable dependiente e independiente para llegar a la comprobación de nuestra hipótesis.

El Capítulo IV: Discusión, acerca de los resultados obtenidos.

El Capítulo V: Conclusiones y recomendaciones.

El Capítulo VI: Propuesta, donde se despliega la evolución de las alternativas y la implementación del sistema de video vigilancia IP y tarjetas RFID para el trabajo requerido.

UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERIA
CENTRO DE IDIOMAS

Licda. Lorena Gallegos 24 de diciembre del 2015

SUMMARY

The research **"Comparative Analysis of levels and quality mechanisms of service for the video transmission and RFID cards in the Engineering Faculty at the National University of Chimborazo"** its aim is to analyze the different quality mechanisms of service, where the best option for a video surveillance system the application of differentiated services. For the development of the research was used the experimental method and a test environment was performed in which the implementation model QoS were compared. In this way, the video surveillance system for the Faculty of Engineering of the National University of Chimborazo was implemented clarifying that with this system we will safeguard the university property of the institution and not as a system of persecution or control at the administrative staff, teachers and service to the university. It is further stated that the RFID system proposed at the beginning of this work was not implemented due to the existence of another system which has better features and also because it is fully operational at UNACH.

The research covers six chapters that show the development of research as follows:

Chapter I: Theoretical Foundation, details the theory used in the study.

Chapter II: Methodology illustrates the type and method of investigation to be done, the system of hypotheses and operationalization of variables, validation of instruments in population and shows that the work was based.

Chapter III: Results, the performance is assessed of each of the test states, dependent and independent variable, to reach checking our hypothesis.

Chapter IV: Discussion about the results.

Chapter V: Conclusions and recommendations.

Chapter VI: Proposal, where the development of alternatives and the implementation of IP video surveillance system and RFID cards for the required work is displayed.

INTRODUCCIÓN

Los sistemas informáticos actualmente se basan en una red de datos, la cual debe ser capaz de soportar cada vez más una amplia gama de aplicaciones. El protocolo de Internet (IP), que ha sido utilizado en estas redes durante las tres últimas décadas para el intercambio de información entre los diferentes ordenadores, ha terminado imponiéndose como el protocolo más usado.

Actualmente el desarrollo de estas redes de datos se está enfocando hacia la provisión de Calidad de Servicio (QoS), la cual se requiere para permitir asegurar determinadas características de calidad en la transmisión de información. El objetivo es determinar la arquitectura a emplearse y evitar que la congestión de determinados nodos de la red afecte a algunas aplicaciones que requieran un especial caudal o retardo, como pueden ser las aplicaciones de video-vigilancia-IP. Gracias al indiscutible avance en la tecnología de las telecomunicaciones hoy en día se puede conseguir un sin número de sistemas que nos permitan garantizar la seguridad e integridad de las personas como la seguridad física de bienes.

En la actualidad es sumamente necesaria la protección de los recursos adquiridos por una empresa o institución, lo cual ha llevado a la sociedad a buscar los mejores equipos y sistemas tecnológicos para salvaguardar dichos bienes adquiridos. Por tal motivo en la Facultad de Ingeniería de la Universidad Nacional de Chimborazo, es menester tener un sistema propio donde se pueda vigilar y precautelar los equipos, bienes y enceres y porque no precautelar la integridad de los individuos que trabajan, estudian y visitan la Facultad de Ingeniería.

Debido a esta necesidad el presente trabajo investigativo hace un estudio de los mecanismos de calidad de servicio, para proceder a la instalación la red de video vigilancia IP, haciendo un análisis de la calidad de servicio para dotar a dicha red

la robustez y confiabilidad necesaria que garantice el funcionamiento de esta, y además que no llegue a interferir con su normal funcionamiento.

I FUNDAMENTACIÓN TEÓRICA

1.1 INTRODUCCION

En el presente tema de investigación se hace referencia a un sistema de video vigilancia IP, por lo tanto es necesario conocer acerca de toda la teoría alrededor de una red de video vigilancia y más cuando en la actualidad las redes se utilizan para el envío de diferentes clases de paquetes y de tráfico ya sea datos, voz o video se necesita garantizar que todos estos paquetes sean llevados a su destino por lo tanto se analizará de manera rápida toda la teoría alrededor de una red de cámaras que se caracterizará por ser confiable, escalable y segura.

1.2 SISTEMAS DE VIGILANCIA IP

1.2.1 CARACTERÍSTICAS

Un sistema de vigilancia con cámaras IP, debe tener las mismas características de una red robusta sobre todo cuando este sistema va a ser instalado para ayudar a la seguridad del personal docente, administrativo, estudiantil y salvaguardar los inmuebles de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo.

Las características principales son:

- Escalable: que tenga la posibilidad de incrementar el número de cámaras a medida de las necesidades de la institución:
- Garantiza la visualización de las imágenes en tiempo real.
- Debe ser una red fácil de administrar.
- Puede soportar el tráfico de diferentes tipos de paquetes.

- Debe tener la posibilidad de guardar los eventos grabados para su posterior revisión.
- Visualización de todas las cámaras instaladas.

1.2.2 CÁMARAS DE RED

Una cámara de red incorpora su propio miniordenador, lo que le permite emitir vídeo por sí misma. Además de comprimir el vídeo y enviarlo, según su modelo puede tener una gran variedad defunciones.

- Activación mediante movimiento de la imagen.
- Activación a través de otros sensores.
- Posibilidad de guardar y emitir los momentos anteriores a un evento.
- Utilización de diferente cantidad de fotogramas según la importancia de la secuencia para conservar ancho de banda.
- Actualización de las funciones por software.(CALDERON RIOS , 2012)

Las cámaras IP permiten ver en tiempo real que está pasando en un lugar, aunque esté a cientos de kilómetros de distancia. Son cámaras de video de gran calidad que tienen incluido un ordenador, a través de él se conecta directamente al Internet.(SANCHEZ, 2015)

Una cámara IP(o una cámara de red) es un dispositivo que contiene:

- Una cámara de vídeo de gran calidad, que capta las imágenes.
- Un chip de compresión que prepara las imágenes para ser transmitidas por la red.
- Un ordenador que se conecta por sí mismo a la red.

Los últimos avances han hecho posible conectar cámaras directamente a una red de ordenadores basada en el protocolo IP. La tecnología de las cámaras de red

permite al usuario tener una cámara en una localización y ver el vídeo en tiempo real desde otro lugar a través de la red o de Internet.
Una cámara de red tiene su propia dirección IP y características propias de ordenador para gestionar la comunicación en la red. Todo lo que se precisa para la visualización de las imágenes a través de la red se encuentra dentro de la misma unidad.

1.2.3 VIDEO VIGILANCIAIP

El vídeo no es nada más que la reproducción en forma secuencial de imágenes, que al verse con una determinada velocidad y continuidad dan la sensación al ojo humano de apreciar el movimiento natural.(LARRIBA GARCÍA , 2009)
Entre las necesidades que la transmisión de video-IP requiere tenemos:

- Requiere un ancho de Banda (384Kps-6Mbps)
- Flujo Variable
- Admite hasta un 2% de pérdidas de paquetes
- Sensitiva al retardo (delay) (- 150 ms)
- Sensitiva al Jitter (- 30ms)

El avance hacia sistemas de vídeo abiertos, combinado con los beneficios de las imágenes digitales a través de una red IP y cámaras de red, constituye un medio de vigilancia y monitorización remota mucho más efectivo que los conseguidos hasta el momento. El vídeo IP ofrece todo lo que el vídeo analógico proporciona, además de una amplia gama de funciones y características innovadoras que sólo son posibles con la tecnología digital.(ALMORA MORALES)

1.2.4 VISIÓNATIEMPOREAL

A diferencia de las cámaras web, las cámaras IP no necesitan un computador para enviar las imagines a través del Internet, ya que estas se pueden conectar a un punto de la red, a través switch o un punto de acceso. Las cámaras IP poseen su

propia dirección IP que las identifica en el entorno de red. Gracias a esto cada cámara IP puede transmitir video usando el Internet como medio a cientos de kilómetros de distancia, lo que faculta el monitoreo y vigilancia remota a tiempo real. El acceso a estas imágenes está totalmente restringido: sólo las personas autorizadas pueden verlas.(FIALLOS PROAÑO, 2011)

1.3 MEDIOSDECONEXIÓN

1.3.1 MEDIOSGUIADOS

Los medios de transmisión guiados están constituidos por un cable que se encarga de la conducción (o guiado) de las señales desde un extremo al otro. Las principales características de los medios guiados son el tipo de conductor utilizado, la velocidad máxima de transmisión, las distancias máximas que puede ofrecer entre repetidores, la inmunidad frente a la interferencia electromagnética, la facilidad de instalación y la capacidad de soportar diferentes tecnologías de nivel de enlace.

La velocidad de transmisión depende directamente de la distancia entre los terminales, y de si el medio se utiliza para realizar un enlace punto a punto o un enlace multipunto. Debido a esto los diferentes medios de transmisión tendrán diferentes velocidades de conexión que se adaptarán a utilizaciones dispares.(ROJO MENDOZA, 2012)

A continuación se mencionara las características principales de los medios guiados comúnmente usados:

1.3.1.1 ELPARTRENZADO

Consiste en un par de hilos de cobre conductores cruzados entre sí, con el objetivo de reducir el ruido de diafonía. A mayor número de cruces por unidad de longitud, mejor comportamiento ante el problema de diafonía.

Existen dos tipos de par trenzado:

-Protegido: Shielded Twisted Pair (STP)

-No protegido: Unshielded Twisted Pair (UTP)

El UTP son las siglas de Unshielded Twisted Pair. Es un cable de pares trenzado y sin recubrimiento metálico externo, de modo que es sensible a las interferencias. Es importante guardar la numeración de los pares, ya que de lo contrario el efecto del trenzado no será eficaz disminuyendo sensiblemente o incluso impidiendo la capacidad de transmisión. Es un cable barato, flexible y sencillo de instalar.

En el casodelasredesseempleaUTPCat.5cat.5e o Cat.6para transmisión de datos. ConsiguiendovelocidadesdevarioscentenaresdeMbps.Unejemplodeesteuso loconstituyenlasredes10/100/1000BASE-T.((TIA) & (EIA), 2014)

Tabla 1. Características de los Medios Guiados
Fuente: El autor

CUADRO COMPARATIVO ENTRE MEDIOS GUIADOS			
Medio de Transmisión	**Razón total de datos**	**Ancho de Banda**	**Separación entre Repetidores**
Par Trenzado	4Mbps	3 Mhz	2 a 10 km
Cable Coaxial	500 Mbps	350 Mhz	1 a 10 km
Fibra Óptica	2Gbps	2 Ghz	10 a 100 km

Cabe destacar que hay una gran cantidad de cables de diferentes características que tienen diversas utilidades en el mundo de las comunicaciones.

1.4 QoS (QUALITYOFSERVICE)

"Es la capacidad de la red de proporcionar un mejor servicio al tráfico seleccionado"
(INTER-AMERICAN TELECOMMUNICATION COMMISSION, 2010)

La Calidad de Servicio ayuda a mejorar y a dar prioridades al tráfico que según el administrador, considere más importante para la red. Las características de Calidad de Servicio son:

- Prioriza tráfico de modo tal que las aplicaciones no-críticas para la operación de la empresa no ralenticen o entorpezcan el tráfico que corresponde a aplicaciones críticas para el negocio de la empresa.
- Prioriza tráfico para asegurar que tráfico indeseable en la red no sobrecargue el uso de ancho de banda.
- Preservar el ancho de banda dilatando el reenvío de información no crítica para la empresa.

1.4.1 INTRODUCCIÓN

Dado que distintas aplicaciones como, por ejemplo, teléfono, correo electrónico y video vigilancia, pueden utilizar la misma red IP, es necesario controlar el uso compartido de los recursos de la red para satisfacer los requisitos de cada servicio. Una solución es hacer que los enrutadores y los conmutadores de red funcionen de maneras distintas para cada tipo de servicio (voz, datos y vídeo) del tráfico de la red. Al utilizar la Calidad de servicio (QoS), distintas aplicaciones de red pueden coexistir en la misma red sin consumir cada una el ancho de banda de las otras.

El término Calidad de servicio hace referencia a una cantidad de tecnologías, como DSCP (Differentiated Service Codepoint), que pueden identificar el tipo de datos que contiene un paquete y dividirlos paquetes en clases de tráfico para priorizar su reenvío. Las ventajas principales de una red sensible a la QoS son la priorización del tráfico para permitir que flujos importantes se gestionen antes que flujos con menor prioridad, y una mayor fiabilidad de la red, ya que se controla la cantidad de ancho de banda que puede utilizar cada aplicación y, por lo tanto, la competencia entre aplicaciones en el uso del ancho de banda. El tráfico, que se considera crítico y requiere una latencia baja, es un caso típico en el que la QoS puede garantizar respuestas rápidas a solicitudes de

movimiento.(GARCIA MATA, 2010)

1.4.2 MODELOS DE IMPLEMENTACIÓN DE QOS

Calidad de Servicio (QoS) es un requerimiento creciente en las redes actuales. La presencia de tráfico de VoIP y crecientemente de video o multicast en la misma infraestructura que se utiliza para el tráfico de datos requiere de la implementación de QoS a fin de asegurar una correcta prestación de cada uno de los servicios.

(GEROMETTA, MODELO DE IMPLEMENTACION DE QOS, 2010)

En la actualidad hay 3 modelos de aplicación de calidad de servicios para redes de datos:

1.4.2.1 BEST-EFFORT

No se discrimina ningún tipo de tráfico y se brinda el mejor soporte posible desde la infraestructura. Es el modelo aplicado en Internet, y el que aplica por defecto toda red que no tiene políticas explícitamente definidas. No garantiza ningún tratamiento o recurso específico a ningún flujo de información. Todo paquete es tratado de igual forma; no hay tratamiento preferencial.

Las principales características del modelo son:

- Altamente escalable.
- No requiere mecanismos o configuraciones especiales.
- No garantiza recursos ni diferencia ningún tipo de servicio.(GEROMETTA, MODELO DE IMPLEMENTACION DE QOS, 2010)

1.4.2.2 INTSERV

Servicios Integrados o IntServ constituyen una arquitectura cuyo cometido es gestionar los recursos necesarios para garantizar calidad de servicio (QoS) en una red de computadores. El concepto que los servicios integrados proponen para cumplir con su cometido, requiere de una nueva arquitectura de protocolos que es difícilmente escalable.

Dentro de la arquitectura de servicios integrados, podrían distinguirse las siguientes funciones principales:

1. Control de admisión
2. Enrutamiento
3. Disciplina del servicio
4. Descarte de paquetes

Control de admisión: Para esto hay implementado un protocolo de reserva de recursos denominado RSVP (ReServation Protocol).

Enrutamiento: Los routers se basarán en la QoS de cada flujo de datos para enrutar los paquetes. Para ello los paquetes serán clasificados por flujos. Una vez clasificados pasarán por un organizador que dictará el modo en que se envían los paquetes. Los paquetes serán enviados a una de las colas con QoS, o bien, si no se ha especificado QoS alguna, serán enviados a la cola por defecto asociada al servicio Best Effort.

Disciplina de servicio: Se podría considerar como disciplina de servicio al modo de funcionamiento con el que trabajarán las colas para llevar a cabo la mencionada diferenciación atendiendo a la QoS de los flujos.

Descarte de paquetes: Con el fin de evitar colapsos en las redes de comunicación se realizan controles de congestión. A continuación se introducirán tres métodos para realizar control de congestión mediante descarte de paquetes.

- Tail drop: Descarta los paquetes recién llegados con el fin de no llenar las colas.
- QoS: Descarta los paquetes con menos calidad de servicio.
- RED (Random Early Detection): Descarta continua y aleatoriamente paquetes de una manera controlada, así se estará tratando la congestión de la red antes de que se produzca. Es uno de los más utilizados.(IBM REDBOOKS, 2006)

Las características principales de IntServ:

- Negocia condiciones específicas de calidad de servicio antes de que se inicie la comunicación propiamente dicha.
- Una vez hecha la reserva, la aplicación cuenta con los recursos reservados más allá de la situación de tráfico de la red.
- Puede adecuarse a demandas específicas y diferentes de cada tipo de tráfico o aplicación.
- La reserva de recursos se realiza para cada flujo de información en particular. No se reservan recursos en función de la aplicación genéricamente.
- Cuando se asocia a desarrollos de telefonía IP, da una aproximación orientada a la conexión para este tipo de servicios. Cada dispositivo a lo largo de la ruta configura y mantiene la operación de cada comunicación individualmente.
- Utiliza los servicios de RSVP (Resource Reservation Protocol).
- No es escalable en grandes redes o implementaciones muy complejas.(GEROMETTA, MODELO DE IMPLEMENTACION DE QOS, 2010)

1.4.2.3 DIFFSERV

La infraestructura de la red es la que reconoce los diferentes tipos de tráfico y aplica políticas diferenciadas para cada clase de tráfico. Es más escalable y flexible en su implementación. Modelo de implementación de recursos garantizados de modo genérico y no por flujos o sesiones. Permite garantizar diferentes condiciones de servicio para diferentes tipos de tráfico, de modo escalable y efectivo, a través de toda la red.

- No requiere señalización previa.
- No permite garantizar condiciones de tráfico extremo a extremo.
- Es muy flexible y escalable.
- Divide el tráfico en clases en función de los requerimientos de la organización.

- Cada paquete recibe el tratamiento que se ha definido para la clase a la cual ese paquete pertenece.
- A cada clase se le puede asignar un diferente nivel de servicio y con ello diferentes recursos.
- La asignación de recursos se hace salto por salto en cada dispositivo de la red y no para una ruta específica.
- El mecanismo de implementación es relativamente complejo. (GEROMETTA, MODELO DE IMPLEMENTACION DE QOS, 2010)

1.4.3 CONCEPTO DE DIFFSERV (DIFFERENTIATED SERVICES)

La propuesta de este modelo es garantizar la mayor QoS en las redes IP de gran tamaño como lo es Internet, añadiendo la facilidad de implementación y el bajo costo ya que no hay necesidad de implementar grandes cambios en la estructura de las redes actuales. Los DiffServ son un conjunto de tecnologías por medio de las cuales los proveedores de servicios de red pueden ofrecer distintos niveles de QoS para diferentes clientes y tráfico de información.

Se basan en la división del tráfico en diferentes clases y en la asignación de prioridades a los paquetes, llamando a este proceso tratamiento diferenciado delos paquetes IP en los routers. Las características de los paquetes se pueden especificar en términos cuantitativos o estadísticos del rendimiento, de la demora, de la inestabilidad, y/o de la pérdida, o de otro modo se puede especificar en términos de alguna prioridad relativa del acceso a los recursos de la red. Este modelo sigue una estrategia que facilita la estabilidad y el despliegue en las redes, ya que no necesita que en todos los nodos de la red tengan implementado este tipo de arquitectura.

Con el marcado de paquetes que proponen los DiffServ hace que los paquetes que pertenezcan a una misma clase reciban un mismo trato por parte de la red. Cuanto mayor sea la prioridad o el ancho de banda asignado a la clase, mejor

será el trato que reciba el paquete.

La diferenciación de servicios se lleva a cabo mediante la definición de comportamientos específicos para cada clase de tráfico entre dispositivos de interconexión, a este hecho se le conoce como PHB (Per Hop Behavior-Comportamiento por Salto). En este modelo se introduce el concepto de PHB, el cual define cuánto tráfico le corresponde a un paquete en particular. En las cabeceras de los paquetes IP, el PHB no es indicado como tal, sino que se maneja mediante los valores del campo DSCP (Differentiated Services Code Point – Punto de Codificación de Servicios Diferenciados) (GARCIA REYES, 2007)

1.4.3.1 FUNCIONESDELAARQUITECTURADIFFSERV

En la Arquitectura de Servicios Diferenciados se realizan las siguientes funciones:

- Clasificación y Agregación de Tráfico.

Marcación del tráfico a nivel de capa 3 mediante el campo DS (DiffServ) que redefine a ToS en datagramas IP, y que pretende unificar los campos similaresenIPv4eIPv6.

- Clasificación y marcación de los paquetes para que reciban cierto tratamiento por salto de la ruta (no extremo-a-extremo).

La clasificación, marcación, políticas y acondicionamiento del tráfico solo se realizan en los nodos frontera. (FIALLOS PROAÑO, 2011)

1.4.3.2 OPERACIÓNDELAARQUITECTURADIFFSERV

En DiffServ, los paquetes son clasificados sólo en el dispositivo de acceso a la red. Dentro de la red, el tipo de procesamiento que reciban los paquetes depende del encabezado. En la Figura (1) se puede observar la operación de DiffServ.

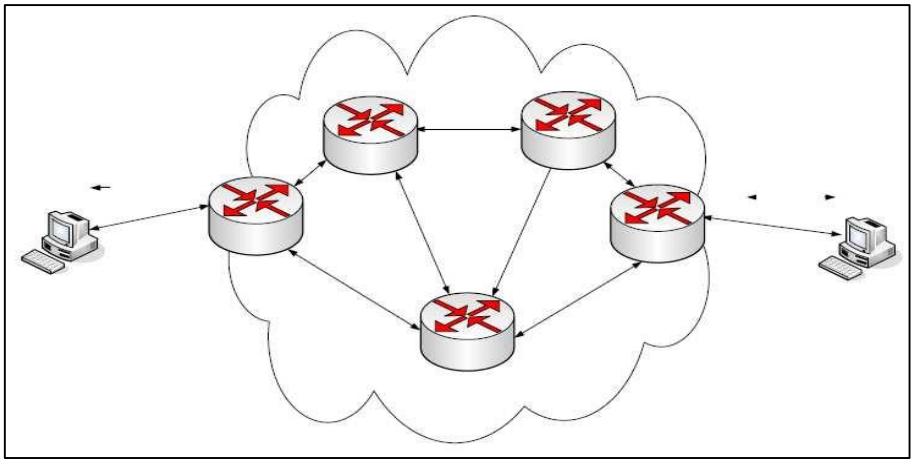


Figura 1. Dominio de Servicios Diferenciados
Fuente: El autor

Losruteadoresdebordeclasificanlospaquetesylosmarcanconlaprecedencia IP o el valor DSCP para la red DiffServ. Otros dispositivos en el núcleo que soportan Diffserv, utilizan el valor DSCP en la cabecera IP, para seleccionar un comportamiento PHB para el paquete y entregarle el tratamiento de Calidad de Servicio apropiado .La información sobre Calidad de Servicio en cada datagrama viaja en un campo de 8 bits llamado DS.

Los seis bits más significativos se llaman DSCP y a los dos menos significativos se los llama CU (Currently Unused) ya que no están definidos en la arquitectura DiffServ, pero se los utiliza para ECN (Notificación de Congestión Explícita). (FIALLOS PROAÑO, 2011)

1.4.3.3 APLICACIONESDEDIFFSERV

Dimensionar una red con DiffServ es muy complejo, ya que se deben tomar en cuenta las cargas de los enlaces, el comportamiento de las aplicaciones, el tráfico en hora pico, etc. El Servicio PHBEF puede utilizarse para VPNs (Redes Privadas Virtuales), debido a la calidad, con bajo retardo y poca pérdida de paquetes. El PHBAF puede servir para dar el llamado “Servicio Olímpico “que consiste en tres clases, oro, plata y bronce para la asignación de recursos, (oro60%, plata30% y bronce 10%). En la Tabla (2) se puede observar algunas aplicaciones con los servicios correspondientes.

Tabla 2. Ejemplo de Asignación de Clases
Fuente: El autor

Aplicación	Clase	PHB
Video	Premium	EF
Voz		
Sesiones interactivas	Oro	AF31
Telnet	Plata	AF21
HTTP		AF22
SMTP	Bronce	AF12
FTP		

1.5 AUTO QoS

Con el avance progresivo de las redes convergentes, y particularmente de algunos servicios como los de telefonía y video sobre IP, es necesario implementar el concepto de Calidad de Servicio (QoS).

Cisco marcha a la vanguardia de la introducción de estas nuevas tecnologías y propuestas. Cisco IOS implementa hoy varios métodos diferentes de implementación de QoS, Para ello Cisco ha desarrollado una nueva forma de QoS denominada AutoQoS y que tiene como propósito facilitarle al administrador de la red el seteo básico de los atributos de QoS.

En dispositivos Cisco IOS se puede configurar QoS de diferentes modos. Las 4 opciones principales son:

- Configurar QoS manualmente creando listas de acceso para identificar tráfico que luego es controlado con comandos específicos de QoS.
- Utilizar el QoS Wizard de SDM (Security Device Manager) de Cisco para crear políticas QoS predefinidas que pueden ser editadas más tarde.
- Utilizar AutoQoS para crear políticas basadas en el flujo de tráfico en tiempo real a través del router o switch.
- Utilizar AutoQoS para crear políticas predefinidas para el flujo de tráfico de VoIP a través de los dispositivos Cisco IOS.(GEROMETTA, ¿QUE ES AUTOQOS ?, 2006)

1.5.1 BENEFICIOS DE AUTOQoS

AutoQoS se encuentra disponible en los routers Cisco IOS desde la serie 2600 hasta la serie 7200 y también en la mayoría de los routers Cisco que utilizan versiones de IOS 12.2 (15) T y posteriores. AutoQoS ofrece los siguientes beneficios:

- No requiere una comprensión avanzada de QoS del mismo modo que si se desea configurar desde la línea de comandos.
- Se pueden modificar las políticas de QoS y reutilizarlas, del mismo modo que si se tratara de un template (plantilla ya definida).
- Se ahorra mucho tiempo de configuración.(GEROMETTA, ¿QUE ES AUTOQOS ?, 2006)

1.5.2 CONFIGURACIÓN DE AUTOQOS

Su configuración es muy simple y fácil, lo verdaderamente complicado es comprender qué es lo que se está configurando, modificar la configuración si es necesario, y probar lo hecho para ver si funciona como se esperaba. También es necesario tener presente no configurar AutoQoS en modo configuración global, sino en las interfaces.(GEROMETTA, ¿QUE ES AUTOQOS ?, 2006)

Tabla 3. Comandos para configuración de Auto-QoS en Switch Cisco
Fuente: El autor

COMANDOS PARA AUTOQoS		
	Comando	**Propósito**
Paso 1	**configure terminal**	Entre en el modo de configuración global.
Paso 2	**Interfaz** *Interfaz-id*	Especificar el puerto que está conectado a un dispositivo de vídeo o el puerto de enlace ascendente que está conectado a otro interruptor de confianza o router en la red interior, y entrar en el modo de configuración de interfaz.
Paso 3	**qos autos voip{cisco-phone |cisco-softphone | trust** }	Habilitar auto-QoS. Las palabras clave tienen estos significados: • **cisco-phone** - Si el puerto está conectado a un teléfono IP de Cisco, las etiquetas de calidad de servicio de los paquetes entrantes son de sólo confiar cuando se detecta el teléfono. • **cisco-softphone** - El puerto está conectado al dispositivo que ejecuta la función de Cisco Softphone. • **trust** - El puerto de enlace ascendente está conectado a un switch o router de confianza, y la clasificación de tráfico VoIP
	vídeo qos auto{cts | ip-camera}	Habilitar auto-QoS para un dispositivo de vídeo. • **cts** - Un puerto conectado a un sistema de telepresencia de Cisco. • **ip-camera** -Un puerto conectado a una cámara IP. Etiquetas de QoS de paquetes entrantes sólo son de confianza cuando se detecta el sistema.
	auto qos classify[**police**]	Habilitar auto-QoS para la clasificación. • **Police**- Policía se estableció mediante la definición de los mapas de políticas QoS y su aplicación a los puertos (QoS basada en puerto).
	auto qos trust{**cos** | **dscp**}	Habilitar auto-QoS para las interfaces de confianza. • **cos** - Clase de servicio. • **dscp** –Diferenciación de Servicios de Punto Código.
Paso 4	**Exit**	Volver al modo de configuración global.

Paso 5	**interface***interface-id*	Especifique el puerto del switch identificado como conectado a un interruptor de confianza o router, y entrar en el modo de configuración de interfaz.
Paso 6	**auto qos trust**	Habilitar auto-QoS en el puerto, y especificar que el puerto está conectado a un router o switch de confianza.
Paso 7	**End**	Vuelva al modo EXEC privilegiado.
Paso 8	**show auto qos interface***interface-id*	Verifique sus entradas. Este comando muestra el comando de auto-QoS en la interfaz en la que auto-QoS fue habilitada. Puede utilizar el **show running-config** comando EXEC privilegiado para mostrar la configuración automática de calidad de servicio y de las modificaciones de los usuarios.

1.6 PARÁMETROS DE CALIDAD DE SERVICIO

1.6.1 LATENCIA (DELAY)

"Retardo o tiempo de tránsito extremo a extremo del paquete de un flujo, es decir, el tiempo requerido por el paquete de un flujo para atravesarlos diferentes enlaces de una red" (YAGUEZ GARCIA, 2011)

Un sencillo ejemplo para entender lo de forma fácil:

Una persona navegando por Internet, esperando a que se descargue una página web, o descargando un archivo puede asumir cierta cantidad de tiempo de espera. Esto no es así en el servicio a tiempo real, sensible a la latencia o a los retardos. Si la latencia entre extremos llegase a ser muy larga por ejemplo 250ms, la calidad del servicio, en general, podría ser considerada pobre, generaría dificultades reales en el entendimiento de los participantes en la transmisión. Si en alguna parte, el uso de la red excede el ancho de banda disponible, los usuarios pueden experimentar retardo, también conocido como latencia.(FIALLOS PROAÑO, 2011)

1.6.2 JITTER (VARIACIÓN DE LA LATENCIA)

"Variación o fluctuación de la latencia o latencia variable (interpacket delay) es la diferencia de tiempo extremo a extremo en la red entre paquetes secuenciales de un mismo flujo" (YAGUEZ GARCIA, 2011)
Por ejemplo, si un paquete requiere 200 ms en atravesar toda la red hacia su destino, es decir de emisor hasta receptor, y el siguiente paquete requiere, a su vez, 250 ms para realizar el mismo viaje, el jitter será de 50 ms.

El Jitter es causado principalmente por las diferencias en los tiempos de espera en cola por los paquetes consecutivos dentro de un flujo y es la consecuencia más importante para QoS. Teniendo en cuenta que todos los sistemas de transporte presentan algo de Jitter es importante saber qué tipos especiales de tráfico especialmente en tiempo real, como la voz, transmisión de video son muy intolerantes al Jitter. Diferencias en los tiempos de llegada producen cortes en el video o la voz.(FIALLOS PROAÑO, 2011)

1.6.3 PAQUETES PERDIDOS

Como IP no es un protocolo 100% fiable, lo cual significa que en determinadas circunstancias los paquetes de datos pueden ser perdidos por la red. Esto normalmente ocurre cuando la red está especialmente congestionada. La pérdida de múltiples paquetes de un flujo y secuencia puede causar un ruido que puede llegar a ser molesto para el usuario. Para mantenerla calidad deseada, los paquetes perdidos no deberían de exceder, del entorno al 3% de todos los paquetes.

1.6.4 DISPONIBILIDADDEANCHODEBANDA

Muchas veces se relaciona únicamente a este término con la Calidad de Servicio, pues se suele pensar que basta con incrementar el ancho de banda para mejorar las prestaciones de una red, lo que en un principio puede ser verdad, pero QoS depende también de otros parámetros como se está viendo; y al aumentar el

ancho de banda innecesariamente se llega a sobre dimensionar la red, lo que implica costos innecesarios y muchas veces sin alcanzar los resultados deseados. A pesar de lo mencionado, se debe tener en cuenta que este es el parámetro técnico más importante a considerarse al momento de proporcionar calidad de servicio.

De manera general se puede definir al ancho de banda como la máxima velocidad de transferencia de datos entre dos extremos de una red. El límite lo impone la infraestructura física de los canales y los flujos que comparten algunos de los enlaces. Aunque el ancho de banda no es infinito y depende de las leyes físicas que rigen para un medio físico dado, constantemente se hacen avances en lo referente a técnicas de modulación para aprovechar de manera más eficiente dicho medio.(FIALLOS PROAÑO, 2011)

1.6.5 CONFIABILIDAD

Se concibe como la tasa media de error de la red, siendo una propiedad del sistema de transmisión en su conjunto. Diversos factores pueden afectar a la confiabilidad, como por ejemplo ruteadores mal configurados o de bajas prestaciones; exceso de tráfico, que ocasiona congestión en la red; insuficiente espacio de almacenamiento en los nodos, etc. Otro factor muy importante en el momento de considerar la confiabilidad de un sistema es el medio físico que está siendo usado, ya que hay tasas medias de error asociadas a cada uno de estos.

Si se consideran aplicaciones basadas en el protocolo de transporte TCP, este corrige las deficiencias de confiabilidad mediante retransmisiones, lo que se traduce en obligar al emisor a disminuir su velocidad de envío.

1.7 TÉCNICAS DE ENCOLAMIENTO

Existen varios niveles en los cuales se puede proveer de calidad de servicio en una red IP. Uno de ellos es el de contar con una estrategia de manejo de los paquetes en caso de congestión, o evitar que la red alcance este estado, descartando paquetes a medida que estos ingresan a la red. El encolamiento

permite establecer una prioridad al forwarding (seguimiento) de paquetes, en base a determinados parámetros establecidos según la técnica utilizada.

Sólo es necesario configurar colas en caso de que la línea esté ocasionalmente congestionada, ya que, si no está congestionada es mejor no configurarlas, y si está congestionada de manera permanente, sería necesario ampliarla.

Cuando se configuran colas, hay que dar prioridad a los protocolos interactivos.

Sólo se debería configurar colas en enlaces inferiores a 4 Mbps.

Cuando un paquete entra en un router, la lógica de ruteo selecciona su puerto de salida y su prioridad es usada para conducir el paquete a una cola específica o tratamiento específico en ese puerto.(FIALLOS PROAÑO, 2011)

1.7.1 ENCOLADO DE CLASE BASADO EN COLAS EQUITATIVAS PONDERADAS (CBWFQ)

La Clase basada en colas equitativas ponderadas CBWFQ (Class Based Weighted Fair Queuing) amplía la funcionalidad estándar de WFQ para proporcionar apoyo a las clases de tráfico definidas por el usuario. Para CBWFQ, se definen las clases de tráfico basadas en criterios de coincidencia con inclusión de protocolos, listas de control de acceso (ACL) y las interfaces de entrada. Los paquetes que cumplan los criterios de coincidencia para una clase constituyen el tráfico para esa clase. Una cola se reserva para cada clase, y el tráfico perteneciente a una clase se dirige a la cola para esa clase. (ABAD AVILA, 2014)

Una vez que una clase ha sido definida de acuerdo con los criterios de su partido, se puede asignar características. Para caracterizar una clase, se le asigna el ancho de banda, el peso, y el límite máximo de paquete. El ancho de banda asignado a una clase es el ancho de banda garantizado entregado a la clase durante la congestión.

Para caracterizar una clase, también se especifica el límite de la cola de esa clase, que es el número máximo de paquetes permitido para acumular en la cola de la clase. Los paquetes pertenecientes a una clase están sujetos a los límites de ancho de banda y la cola que caracterizan a la clase.

Si una clase predeterminada está configurada con el ancho de banda de la política-mapa comando de configuración de clase, todo el tráfico no clasificado se coloca en una sola cola y dado el tratamiento de acuerdo con el ancho de banda configurado. Si una clase predeterminada está configurada con el f de aire de cola de comandos, todo el tráfico no clasificado flujo es clasificado y dado el tratamiento de mejor esfuerzo. Si no hay ninguna clase por defecto configurada, el tráfico que no coincide con ninguna de las clases configuradas en el flujo clasificado y será tratado bajo estándar BestEffort. Una vez que un paquete es clasificado, todos los mecanismos estándar que pueden ser utilizados. (FIALLOS PROAÑO, 2011)

1.8 FORMATO DE VÍDEO EN LAS CÁMARAS DE SEGURIDAD

La codificación de vídeo sirve para convertir señales de vídeo analógico a señales de vídeo digital. Esto hace que dependiendo el tipo de codificación se optimice el tamaño de este vídeo sin perder la calidad de la imagen, sin duda esto ayuda básicamente para el caso de las cámaras de seguridad IP en :

- A mejor compresión: el vídeo se ve mejor, más fluido a través de celulares, tabletas y dispositivos móviles.
- En sitios donde el ancho de banda es bajo, la calidad de imagen será mejor, la fluidez será mayor, no se perderá la imagen de la cámara.
- A mejor formato de compresión se dejará más espacio para transmisión de otros datos como por ejemplo el sonido, datos de operación de la cámara, etc.
- A un mejor formato de compresión, el vídeo como se dijo anteriormente es más liviano, esto influye directamente sobre la cantidad de espacio que ocupa la grabación de este vídeo en un disco duro, ya sea en el servidor, computador, o en el DVR. En pocas palabras a mejor formato de compresión mayor tiempo de grabación en nuestros discos duros es decir podemos ver el vídeo de hace 3, 4, 7, 8 meses dependiendo el tamaño del disco duro.

1.8.1.1 FORMATO DE COMPRESIÓN H.264

El formato H.264 es un estándar para la compresión de vídeo, cuyo borrador final en la primera versión del estándar se completó en mayo del 2003.La intención del formato H.264/AVC fue crear un estándar capaz de proporcionar buena calidad de vídeo con tasas de bits sustancialmente más bajas que los estándares anteriores, por ejemplo, la mitad o menos que la tasa de bits de vídeo MPEG-2, H.263 o MPEG-4, esto sin aumentar la complejidad del diseño de tal manera que sería poco práctico o demasiado costoso su implementación. Un objetivo adicional es proporcionar la suficiente flexibilidad para que el formatoH.264 se aplique a una amplia variedad de aplicaciones en una amplia variedad de redes y sistemas, incluyendo las tasas de bits bajas y altas, la resolución de vídeo alta y baja, la difusión, el almacenamiento DVD, las redes de paquetes RTP/IP, y los sistemas de telefonía multimedia de la ITU.

Las principales características son:

- Uso de imágenes previamente codificadas como referencias de una manera mucho más flexible que en los formatos anteriores, permitiendo hasta 16 fotogramas de referencia o 32 campos de referencia en el caso de la codificación entrelazada.
- La compensación VBSMC (Variable block-size motion compensation) con tamaños de bloque tan grandes como 16x16 pixeles y tan pequeños como 4x4 pixeles, permiten la segmentación precisa de regiones en movimiento.
- La capacidad de usar múltiples vectores de movimiento por macro bloque, uno o dos por partición, con un máximo de 32 en el caso de un B-frame construido con 16particiones de 4x4 pixeles.
- La precisión de un cuarto de píxel para la compensación del movimiento, permite la precisa descripción de los desplazamientos de las zonas en movimiento.
- Para la crominancia, normalmente la resolución suele reducirse a la mitad tanto vertical como horizontalmente, por lo que la compensación de movimiento de la crominancia utiliza unidades de un octavo de píxel.

- Un filtro de desbloqueo in-loop que ayuda a prevenir los errores del bloqueo a otras técnicas de compresión de imagen basadas en DCT, resultando una mejor apariencia visual y mayor eficiencia de compresión.
- Una definición de NAL (Network Abstraction Layer) que permita la misma sintaxis de vídeo para ser utilizado en muchos entornos de red. Un concepto de diseño muy fundamental de H.264 es generar paquetes auto contenidos para eliminar la duplicación de la cabecera como en el HEC (Header Extension Code) de MPEG-4.Esto se logró desacoplando la información relevante para más de un tramo del flujo.
- Contar el orden de las imágenes, una característica que sirve para mantener el orden de las imágenes y los valores de las muestras en las imágenes descodificadas aisladas de la información de tiempo, permitiendo que la información de tiempo sea transportada y controlada/cambiada por separado por un sistema sin afectar el contenido de la imagen decodificada.

Estas técnicas, junto con otras varias, hacen que el H.264 sea mucho mejor que cualquier formato anterior bajo una amplia variedad de circunstancias en una amplia variedad de entornos de aplicaciones. A menudo el H.264 puede ser mejor que el MPEG-2 Video. Normalmente se obtiene la misma calidad a mitad de la tasa de bits o menos, sobre todo en la tasa de bits alta y situaciones de alta resolución.(SALAVERT CASAMORT)

II. METODOLOGIA

2.1 TIPO DE INVESTIGACION

Para este tipo de estudio se consideró que por sus características se debe tratar como estudio experimental.

2.1.1 INVESTIGACIÓN EXPERIMENTAL

La investigación experimental es el conjunto de procedimientos ordenados, metódicos y técnicos que se ejecutan para obtener la información necesaria y verídica sobre el tema a investigar y de la manera en que se lo va a resolver, manipulando una o más variables para determinar su efecto sobre otra variable llamada dependiente.

En este caso se tiene en cuenta que al variar condiciones que influyen en el buen rendimiento de una red, se generan datos y variables experimentales los cuales facilitaron la elección de cual o cuales mecanismos de QoS (Calidad de Servicio) conviene más al sistema de video vigilancia IP, dando como resultado una red robusta, garantizada y que no interfiera con la red ya instalada y en pleno funcionamiento que posee la Facultad.

Esta investigación no está asociada únicamente a establecer una comparación entre conceptos de funcionamiento, sino a establecer parámetros de comparación reales, capaces de demostrar de una manera clara el protocolo que presente mayor fiabilidad al afrontarlas demandas de calidad requeridas en la transmisión de Video IP para un sistema de seguridad y vigilancia en la facultad de Ingeniería de la UNACH.

2.2 MÉTODOS DE INVESTIGACIÓN

Se utilizaron para este proyecto los siguientes métodos de investigación:

Método científico y de observación: ya que mediante la implementación y análisis de un escenario de prueba y un escenario físico real se pretende estudiar y observar cambios en los rendimientos de los protocolos expuestos, en los parámetros a analizar y en los posibles errores al instalar la red.
Método Inductivo: A través del cual se encontró el mejor mecanismo de QoS para la red.

Se realizó las siguientes consideraciones para esta investigación:

Plantear la investigación en base al análisis de los modelos de QoS y al momento de escoger un protocolo de QoS en la implementación de sistemas de seguridad y vigilancia basados en tecnologías IP, como también el análisis de factibilidad de un Sistema RFID para control de docentes y personal administrativo.

2.3 OPERACIONALIZACION DE LAS VARIABLES

HIPOTESIS

Utilizar niveles y mecanismos de Calidad de Servicio que permitirá mejorar la transmisión de video en la implementación del sistema de control de personal a través de video y tarjetas RFID.

VARIABLE INDEPENDIENTE

El análisis de niveles y mecanismos de Calidad de Servicio.

VARIABLE DEPENDIENTE

La mejora de la transmisión de video con QoS para el sistema de video vigilancia IP.

2.3.1 OPERACIONALIZACIÓN CONCEPTUAL

Tabla 4. Operacionalización Conceptual de las variables
Fuente: El autor

VARIABLE	TIPO	DEFINICIÓN
El análisis de niveles y mecanismos de Calidad de Servicio.	Independiente	Cuantificación de la productividad de cada uno de los protocolos sometidos a estudio. Análisis y configuración de los mecanismos para tener QoS.
La mejora de la transmisión de video con QoS para el sistema de video vigilancia IP	Dependiente	Comparación de una red que posea QoS.

2.3.2 OPERACIONALIZACIÓNMETODOLÓGICA

Tabla 5. Operacionalización Metodológica
Fuente: El autor

HIPOTESIS	VARIABLES	INDICADORES	ÍNDICES	INSTRUMENTOS
Utilizar niveles y mecanismos de Calidad de Servicio que permitirá mejorar la transmisión de video en la implementación del sistema de control de personal a través de video y tarjetas RFID.	DEPENDIEN-TE La mejora de la transmisión de video con QoS para el sistema de video vigilancia IP	Paquetes transmitidos	Número de paquetes Totales	Simulaciones Pruebas Analizador de Red, Wireshark
			Paquetes Perdidos	
		Velocidad en la transmisión o trafico útil	Ancho de Banda	
		Tiempo de Transmisión	Retardo en la Transmisión	
			Jitter	
	INDEPEN-DIENTE El análisis de niveles y mecanismos de Calidad de Servicio.	Rendimiento IntServ	Comparación IntServ con BestEffort	Simulación Razonamiento
		Rendimiento DiffServ	Comparación DiffServ con BestEffort	

2.4 POBLACIÓN Y MUESTRA

La población es el conjunto de todos los elementos a ser evaluados y en el presente análisis la conformaron todos los elementos de la red de la Universidad Nacional de Chimborazo. De esta población se seleccionó una muestra de la red y del tráfico en la Facultad de Ingeniería.

2.5 PROCEDIMIENTOS GENERALES

2.5.1 ANÁLISIS DE CALIDAD DE SERVICIO

HERRAMIENTASDESOFTWARE

- Cisco Packet Tracer versión 6.2
- Analizador de Paquetes Wireshark
- Analizador de tráfico PRTG

El mecanismo de calidad de servicio se refiere a la habilidad de la red de ofrecer prioridad a unos determinados tipos de tráfico. Estos mecanismos son inherentemente necesarios a la red cuando esta ofrece servicios de tiempo real: voz IP, videoconferencia por Internet, video streaming, radio por Internet, etc.

El objetivo fue llevar a cabo un análisis profundo de lo que realmente es calidad de servicio, para que sirve y como funciona en cada una de las capas del modelo OSI y configurar las técnicas de encolamiento en un escenario de prueba donde podamos analizar cada una de ellas para así determinar cuál se ajusta de mejor manera a nuestra necesidad de brindar preferencia de trafico al video IP.

2.5.1.1 PARÁMETROS DE MEDICIÓN

Se tomó en cuenta los parámetros que definen globalmente la calidad de servicio para escoger el que se adecúe al escenario y que a su vez permitió interpretar el resultado: siendo este parámetro cuantitativo por el tiempo que se demora desde que se envía el paquete hasta que se recibe, conocido como retraso, también se consideró el ancho de banda y pérdida de paquetes. Además se incorporó un parámetro cualitativo que fue la calidad de la imagen percibida por el usuario.

ESCENARIO DE PRUEBAS

Se inició configurando un escenario de prueba, donde se configuraron los diferentes modelos de QoS para su respectivo análisis.

Donde la red de cámaras es la de la derecha de la Figura (2), PC- Camara1 y PC-Camara2 simulan las cámaras de prueba.

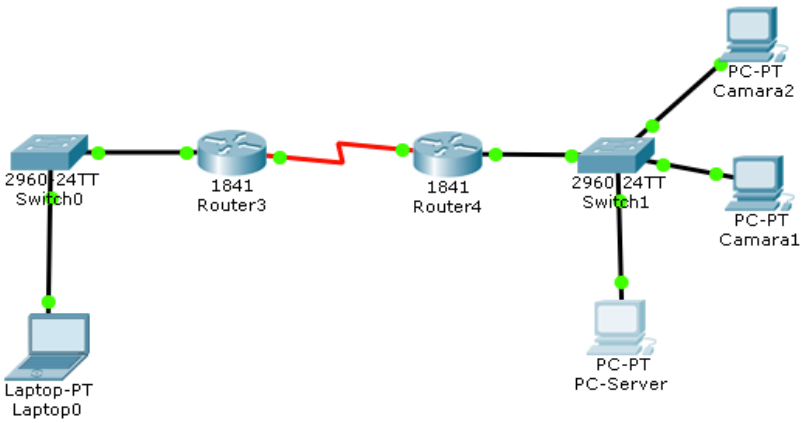


Figura 2. Escenario de prueba en Packet Tracer

Fuente: El autor

HERRAMIENTAS DE HARDWARE

El escenario de pruebas físico se llevó a cabo con Routers y Switch Cisco y con las cámaras adquiridas para la instalación. Véase ANEXO 1.

En esta simulación física se usaron los siguientes equipos:

Tabla 6. Elementos a usarse en la simulación física
Fuente: El autor

CANTIDAD	EQUIPO	MODELO
2	Router	Cisco 2901
2	Switch	Catalyst 2960
1	Laptop	Dell
1	Laptop	MacBook Pro
2	Cámaras	ZKTECO

III. RESULTADOS

3.1. ANÁLISISEINTERPRETACIÓNDERESULTADOS

3.1.1. SISTEMA RFID PARA LA FACULTAD DE INGENIERIA.

En cuanto al sistema RFID propuesto en el presente proyecto de investigación, mediante un informe comparativo (ANEXO 2) se descartó, ya que en la actualidad, existe en la Facultad de Ingeniería un sistema Biométrico para el control del personal que cumple con mayores estándares de calidad y seguridad que al antes mencionado sistema RFID.
Desde este punto de vista ya no se instaló dicho sistema, tomando esta decisión gracias a la corroboración de las autoridades encargadas de la instalación y control del Sistema Biométrico.

Con lo correspondiente al análisis de los mecanismos para Calidad de Servicio QoS se puede decir que la calidad requerida en la transmisión de video de un sistema de seguridad se reflejó en la manera de apreciar los parámetros establecidos siendo estos: el retardo, jitter, ancho de banda y pérdida de paquetes. La valoración de cada uno de estos parámetros en el escenario de prueba permitió establecer esquemas de comparación confiables. Al referirse a la transmisión de video, los retardos y pérdida de paquetes deben de ser bajos, así se llega a garantizar una transmisión que cumpla eficientemente con el propósito del sistema en sí, en el caso de un sistema de seguridad implica una visualización oportuna de los acontecimientos ocurridos en el sitio.

En primer lugar se diseñó un escenario de prueba donde se simuló una conexión típica de red mediante dos routers, los cuales proporcionaron los esquemas de ruteo necesarios en los que a QoS se refiere, empezando a trabajar bajo la arquitectura Besteffort con tráfico y sin tráfico para analizar las diferencias e incidencias del mismo en las redes. Después en el mismo

escenario se procedió a cambiar los parámetros, implementando una arquitectura QoS IntServ con la cual se valoró idénticamente los parámetros antes mencionados.

Por último se modificó una vez más la arquitectura QoS, esta vez procediendo a usar DiffServ, como en el caso anterior se valoraron los parámetros mencionados.

Finalmente se realizó el análisis de las técnicas de encolamiento y el escenario práctico actual con una exploración de los parámetros que permitan obtener datos cuantitativos para valorar los resultados y así establecer comparativos de dichas técnicas, como también un análisis teórico sobre los formatos de compresión de video.

3.2. PROCESAMIENTO DE LA INFORMACION.

En el trabajo de investigación se implementó tres pruebas en un mismo escenario para lograr obtener el beneficio de cada una de los modelos usados, para la cuantificación de cada índice se utilizó un nivel de medición máxima al 100%, donde se asigna pesos a cada uno de los índices que conforman un indicador obteniendo una media aritmética porcentual de los experimentos, para luego ser comparada con el porcentaje individual de la propuesta de la investigación.

3.3. RESULTADO DE LAS PRUEBAS

En la transmisión de video los aspectos de mayor importancia al momento de definir la calidad necesaria son: la pérdida de paquetes, el retardo en la transmisión, el jítter, la técnica de encolamiento y el análisis teórico sobre los formatos de compresión de video.

Para este caso por motivo de estudio se transmitió trafico FTP conjuntamente con el tráfico de video, con la finalidad de valorar el porcentaje de mejora de QoS en cada uno de nuestros protocolos. Se consideró un enlace dedicado

para la transmisión de video, es decir un escenario en el cual no existe ningún otro tipo de tráfico, que solamente el generado por el sistema de vigilancia. En una segunda prueba se estima una red BestEffort (sin calidad de servicio) con tráfico FTP.

Al mantener estos dos escenarios, se tuvo dos puntos de vista reales, un rendimiento de un enlace dedicado a la video vigilancia IP, que es lo adecuado en el caso de estudio, y el otro escenario donde se envió el tráfico sin ningún tipo de calidad de servicio, lo que vendría a ser el caso de menor eficiencia.

3.3.1. ESCENARIO GENERAL

Como primer paso se configuró las interfaces de los routers y del protocolo de enrutamiento necesario para que funcione la red y proceder a realizar las pruebas. Cabe recalcar que esta misma configuración se realizó para las tres pruebas que son: Besteffort, InterServ y DiffServ. Con el software Packet tracer se simula el entorno donde haremos las pruebas:

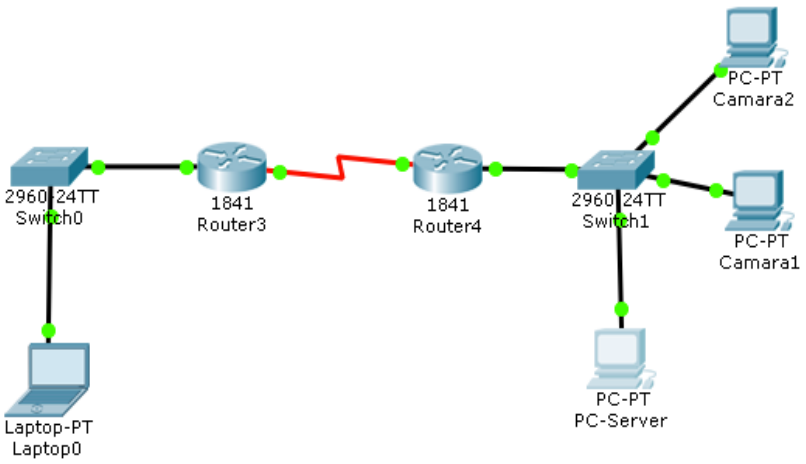


Figura 3. Escenario de prueba

Fuente: El autor

A continuación se muestra la configuración de cada uno de los routers:

Configuración de Interfaces:

Router PRINCIPAL

```
PRINCIPAL>
PRINCIPAL>enable
PRINCIPAL#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
PRINCIPAL(config)#interface fastethernet 0/0
PRINCIPAL(config-if)#ip address 192.168.1.1 255.255.255.0
PRINCIPAL(config-if)#no shutdown
PRINCIPAL(config-if)#exit
PRINCIPAL(config)#interface serial 0/1/0
PRINCIPAL(config-if)#ip address 10.0.0.1 255.0.0.0
PRINCIPAL(config-if)#clock rate 9600
PRINCIPAL(config-if)#no shutdown
PRINCIPAL(config-if)#exit
PRINCIPAL(config)#
```

Figura 4. Configuración de las interfaces en Router PRINCIPAL
Fuente: El autor

Router CAMARAS

```
Router>enable
```

Figura 5. Configuración de las interfaces Router CAMARAS

Fuente: El autor

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname CAMARAS
CAMARAS(config)#interface serial 0/1/0
CAMARAS(config-if)#ip address 10.0.0.2 255.0.0.0
CAMARAS(config-if)#no shutdown
CAMARAS(config)#interface fastethernet 0/0
CAMARAS(config-if)#ip address 192.168.153.1 255.255.255.0
CAMARAS(config-if)#no shutdown
```

Configuración del Parámetro de Ruteo:

Considerando que en esta simulación, intervienen tres tipos de redes y no existe gran número de equipos se procede a realizar un enrutamiento RIP versión 2:

Router PRINCIPAL

```
PRINCIPAL#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
PRINCIPAL(config)#router rip
PRINCIPAL(config-router)#version 2
PRINCIPAL(config-router)#network 192.168.1.0
PRINCIPAL(config-router)#network 10.0.0.0
PRINCIPAL(config-router)#end
PRINCIPAL#
%SYS-5-CONFIG_I: Configured from console by console
```

Figura 6. Configuración de Rip en Router PRINCIPAL

Fuente: El autor

Router CAMARAS

```
CAMARAS>enable
CAMARAS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CAMARAS(config)#router rip
CAMARAS(config-router)#version 2
CAMARAS(config-router)#network 192.168.153.0
CAMARAS(config-router)#network 10.0.0.0
CAMARAS(config-router)#end
CAMARAS#
%SYS-5-CONFIG_I: Configured from console by console
```

Figura 7. Configuración Rip Router CAMARAS

Fuente: El autor

En todas las pruebas realizadas se tomó como referencia el ancho de banda, el jitter, el retardo y los paquetes perdidos, donde se considera para fines de cálculo con mayor peso a los mejores atributos para la red.

3.3.1.1. PRUEBA 1

Estas pruebas se realizaron sin ningún modelo de Calidad de Servicio, los paquetes son analizados por el programa Wireshark.

- Se transmite video a través de una simulación de red WAN sin tráfico, donde no se aplicó ningún modelo de Calidad de Servicio.
- Se transmite video en una red WAN de prueba con tráfico y sin ningún modelo de Calidad de Servicio.

3.3.1.1.1. RESULTADOS DE LA PRUEBA 1 BESTEFFORT SIN TRAFICO Y CON TRÁFICO.

Después de analizar la transmisión del video enviando un total de 602 paquetes de video en la prueba sin tráfico y 500 paquetes de video en la prueba con tráfico se determinó que:

Tabla 7. Resultados obtenidos de transmisión en escenario de prueba
Fuente: El autor

PRUEBA 1	SIN TRAFICO	CON TRAFICO FTP
PAQUETES TOTALES	602	500
ANCHO DE BANDA (bits/s)	6300	3500
JITTER (ms)	160,2	236.8
RETARDO (s)	106.35	119.18
PAQUETES PERDIDOS	73	102

3.3.1.1.2. ANÁLISIS DE RESULTADOS PRUEBA 1

Como se mencionó anteriormente, se procede a dar pesos y mayores porcentajes a los parámetros que mayor calidad de servicio pueden brindar a la transmisión de video:

a) **Ancho de banda.** El ancho de banda definido para una determinada conexión a la red se reparte para gestionar las demandas de procesos

existentes en la subred. Esto se realiza según el proceso de encolamiento existente. Según la arquitectura que se utilice en la red tendremos diferentes maneras de gestionar el espacio y tiempo en el ancho de banda disponible.

Tabla 8. Asignación de porcentajes al ancho de banda resultante.
Fuente: El autor

ANCHO DE BANDA (Bits/s)		
	PRUEBA SIN TRAFICO	**PRUEBA CON TRAFICO**
RESULTADO	6300	3500
PORCENTAJE	100%	55.6%

En el análisis del ancho de banda destinado al tráfico de video IP sin ningún mecanismo de Calidad de Servicio, se determinó que como era de esperarse la prueba BestEffort sin tráfico obtiene el mayor ancho de banda para el proceso, puesto que al no existir más tráfico en la red que el de Video IP el proceso puede disponer del ancho de banda de la red.

Por otra parte el escenario BestEffort con trafico otorgó el ancho de banda más bajo en los escenarios para el tráfico de Video IP, puesto que al no tener ninguna distinción del resto del tráfico fue tratado igual que el tráfico que no necesita mayores condiciones de calidad.

b) **Jitter.** Se consideró el tiempo en que se demora un paquete en llegar a su destino, conociendo el objetivo se espera tener menor jitter en la transmisión, en este índice el porcentaje es calculado dándole un peso del 100% al menor jitter existente en la transmisión.

Tabla 9. Asignación de porcentaje al Jitter
Fuente: El autor

JITTER (ms)		
	PRUEBA SIN TRAFICO	**PRUEBA CON TRAFICO**
RESULTADO	160.2	236.8
PORCENTAJE	100%	67.65%

Tomando en cuenta que el Jitter está ligado al retardo podemos anticipar que los resultados de este indicador van a tener mucha relación con los obtenidos en la valoración del retardo.

c) **Retardo.** El retardo depende del tiempo que se demora un paquete en transmitirse, lo cual se mide en segundos**,** cabe recalcar que el porcentaje fue calculado dando un peso de 100% al número de menor de retardo, lo que podemos observar el tratamiento de los datos por cada prueba implementada.

Tabla 10. Asignación de porcentaje al Retardo
Fuente: El autor

RETARDO (s)		
	PRUEBA SIN TRAFICO	**PRUEBA CON TRAFICO**
RESULTADO	106.35	119.18
PORCENTAJE	100%	89.23%

Este aspecto pudo ser deducido por simple lógica ya que una red con tráfico sin ninguna arquitectura de QoS va a presentar un retardo considerable al momento de trasmitir nuestros datos.

d) **Paquetes totales transmitidos.** Se observó que el ambiente con mayor transmisión de paquetes de video es BestEffort sin tráfico, esto sucede porque el tráfico es exclusivo para la transmisión de video, prácticamente se tiene un enlace dedicado para el sistema de seguridad lo que resulta una transmisión mayor de paquetes.

e) **Pérdida de Paquetes.** Al analizar la calidad de servicio un factor muy importante en la transmisión de video real, es la pérdida de paquetes puesto que al tener una pérdida considerable, el video será de baja calidad y poca fluidez. En este índice se tomó en cuenta el porcentaje de paquetes perdidos por cada arquitectura implementada en relación

con los enviados, así se otorgó el peso de 100% a la arquitectura que menor porcentaje de pérdidas presentó.

Tabla 11. Asignación de porcentajes a la pérdida de paquetes
Fuente: El autor

PERDIDA DE PAQUETES		
	PRUEBA SIN TRAFICO	**PRUEBA CON TRAFICO**
PAQUETES TOTALES ENVIADOS	602	500
PAQUETES PERDIDOS	73	102
PORCENTAJE DE PAQUETES PERDIDOS	12.13 %	20.4%
PORCENTAJE	**100%**	**20.4%**

En el ambiente de simulación BestEffort sin tráfico, que representa un enlace dedicado para la transmisión de video se obtuvo la menor pérdida porcentual de paquetes en relación con el número de paquetes recibidos.

Tabla 12. Resumen de resultados Prueba 1
Fuente: El autor

PRUEBA 1	Ancho de Banda (Bytes)	%	Jitter (ms)	%	Retardo (s)	%	Paquetes Totales	%	Paquetes Perdidos	%
Escenario BestEffort sin trafico	6300	100%	160.2	100%	106.35	100%	602	83.06%	73	100.00%
Escenario BestEffort con trafico FTP	3500	55.6%	236.8	67.65%	119.18	89.23%	500	100%	102	20.4%

3.3.1.2. PRUEBA 2(INTSERV)

Se configuró en el mismo escenario usado anteriormente, pero se aplicó la configuración de IntServ:

Tabla 13. Configuración de IntServ
Fuente: El autor

Configuración del Router PRINCIPAL	**Configuración del Router CAMARAS**
<Define class map> R1#configure terminal R1(config)#class-map Gold R1(config-cmap)# match acces-group name Gold R1(config)# ip access-list extended Gold R1(config-ext-nacl)# permit tcp 192.168.153.51 0.0.0.255 any R1(config-ext-nacl)# permit tcp 192.168.1533.52 0.0.0.255 any R1(config-ext-nacl)# deny ip any any <Creating policies > R1(config-pmac-c)# bandwidth 1536 <Attaching policies to interfaces> R1(config)# interface serial 0/1/0 R1(config)# service-policy output JPG	<Define class map> R2#configure terminal R2(config)#class-map Gold R2(config-cmap)# match acces-group name Gold R2(config)# ip access-list extended Gold R2(config-ext-nacl)# permit tcp 192.168.153.51 0.0.0.255 any R2(config-ext-nacl)# permit tcp 192.168.153.52. 0.0.0.255 any R2(config-ext-nacl)# deny ip any any <Creating policies > R2(config-pmac-c)# bandwidth 1536 <Attaching policies to interfaces> R2(config)# interface serial 0/0/0 R2(config)# service-policy input JPG

3.3.1.2.1. RESULTADOS DE LA PRUEBA 2 (INTSERV)

En la segunda prueba de simulación, se varió las condiciones en el tratamiento de la información de la siguiente manera:

- Se implementó la arquitectura IntServ reservando ancho de banda en la conexión para la transmisión del tráfico de video.

Tabla 14. Resultados de análisis IntServ
Fuente: El autor

Anchode Banda (bytes)	Jitter (ms)	Retardo (s)	Paquetes Totales	Paquetes Perdidos
4200	202.8	111.22	512	97

3.3.1.3. PRUEBA 3

Se configuró en el mismo escenario usado para las pruebas 1 y 2, cambiando la configuración de DiffServ.

Tabla 15. Configuracion de DiffServ
Fuente: El autor

```
CAMARAS(config)#interfaceserial0/0
CAMARAS(config-if)#random-detect
CAMARAS(config)#interfaceserial0/0
CAMARAS(config-if)#random-detect
exponential-weighting-constant 10
```

3.3.1.3.1. RESULTADOS DEL AMBIENTE 3

En la tercera prueba de simulación se varió las condiciones en el tratamiento de la información con DiffServ:

Tabla 16. Resultado análisis DiffServ
Fuente: El autor

Ancho de Banda (bits/s)	Jitter (ms)	Retardo (s)	Paquetes Totales	Paquetes Perdidos
4500	224.7	108.10	499	85

3.3.2. COMPARACION DEL RENDIMIENTO DE LOS PROTOCOLOS CALIDAD DE SERVICIO EN LA TRANSMISIÓN DE VIDEO IP

Para la valoración de las arquitecturas implementadas se comparó los datos obtenidos en los ambientes de simulación IntServ y DiffServ con los datos obtenidos en el escenario BestEffort con y sin tráfico en la red, (véase ANEXO 3) ya que el motivo de la investigación fue encontrar la arquitectura con mayor robustez de calidad para un sistema de seguridad basados en tecnologías IP. Para esto se dio los pesos a cada indicador e índice de valoración de acuerdo a los siguientes criterios.

- Considerando que lo más importante en una transmisión de Video IP, es la fluidez de las imágenes, se decidió darle un peso mayor al tiempo de transmisión, en el cual el Jitter es el índice que mayor porcentaje tuvo en la obtención del rendimiento.
- El segundo indicador en orden de importancia fueron los paquetes transmitidos.
- Por último el ancho de banda, donde el principal objetivo de una red implementada con alguna arquitectura QoS, es mejorar la calidad sin la necesidad de cambiar la red física para obtener un mayor ancho de banda.

Tabla 17. Pesos indicadores para valoración de rendimiento
Fuente: El autor

Pesos de los Indicadores e Índices			
Indicador	**Peso**	**Índice**	**Peso**
Tiempo de Trasmisión	50	Retardo en la transmisión	20
		Jitter	30
Paquetes Trasmitidos	30	Total Paquetes Transmitidos	10
		Paquetes Perdidos	20
Velocidad de Trasmisión	20	Ancho Banda	20

Tabla 18. Cuadro Comparativo de porcentajes de las Pruebas

Fuente: El autor

VALORACION DE RENDIMIENTO DEL PROTOCOLO			**BestEffort sin tráfico en la red**		**BestEffort con tráfico en la red**		**IntServ**		**DiffServ**	
Indicador	***Índice***	***Peso***	***%de Valoración***	***Sub Total***	***%de Valoración***	***Sub Total***	***%de Valoración***	***Sub Total***	***%de Valoración***	***Sub Total***
Paquetes Trasmitidos	Total Paquetes Transmitidos	10	83.06%	8.301	100,00%	10	97.66.%	9.77	99.8%	9.98
	Paquetes Perdidos	20	100%	20	20.4%	4.8	75.23%	15.05	85.88%	17.18
Velocidad de Trasmisión	Ancho de banda	20	100%	20	55.6%	11.12	66.7%	13.34	75%	15
Tiempo de Trasmisión	Retardo en la transmisión	20	100%	20	89.23%	17.85	95.62%	19.12	98.39%	19.68
	Jitter	30	100%	30	67.65%	20.30	78.99%	23.70	71.30%	21.39
Total		**100**		**98.301**		**64.07**		**80.98**		**83.23**

3.4. INTERPRETACIÓN DEPORCENTAJES

Tomando en cuenta que cada indicador tiene su peso entonces se desglosa cada uno de los promedios de los indicadores con la siguiente denominación:

PT= PAQUETES TOTALES

VT= VELOCIDAD DE TRANSMISION

TT= TIEMPO DE TRANSMISION

SIN CALIDAD DE SERVICIO

BestEffort sin tráfico = PT+ VT+TT= 28.30+40+30=98.30%

BestEffort con tráfico = PT+VT+TT=14.8+28.97+20.30=64.07%

Variabilidad = (BestEffortsintráfico) – (BestEffortcontráfico)

Variabilidad=98.30%-64.07%

Variabilidad= 34.23%

CON CALIDAD DE SERVICIO INTSERV

IntServ = PT+VT+TT= 24.82+32.46+23.70=80.98

CON CALIDAD DE SERVICIO DIFFSERV

DiffServ = PT+VT+TT=27.16+34.68+21.39=83.23%

Variabilidad IntServ = (IntServ)–(BestEffortcontráfico)

Variabilidad IntServ=80.98%-64.07%

VariabilidadIntServ= 16.91%

Variabilidad DiffServ = (DiffServ)–(BestEffortcontráfico)

VariabilidadDiffServ =83.23%-64.07%

VariabilidadDiffServ = 19.16%

Finalmente se llegó a concluir que la transmisión de video por IP con DiffServ, mejora la calidad de trasmisión en un 19.16 %, en comparación de IntServ en un 16.91 %.

3.5. AUTO QoS PARA MEJORAR LA CALIDAD DE SERVICIO

El análisis previamente realizado, arrojó como resultado que la mejor opción de modelo de Calidad de Servicio es DiffServ,

DiffServ presentó una ampliación en la calidad de la transmisión. Ahora es necesario saber cómo ingresar esta calidad de servicio a los equipos ya instalados en la Facultad de Ingeniería, propiamente en los switch Cisco que manejan el tráfico de esta Facultad. Para ello la marca Cisco nos presenta una alternativa más rápida y segura para la configuración de Diffserv, esto es el auto QoS.

Como ya se conoce Diffserv trabaja dando niveles o clases al tráfico para así priorizarlo.

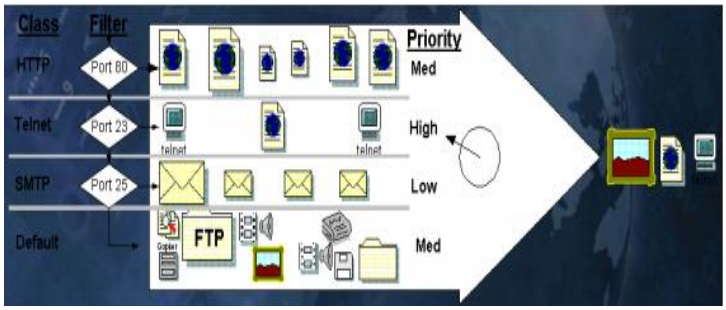


Figura 8. División de tráfico de diferentes clases en diferentes prioridades

Fuente: http://arantxa.ii.uam.es/~ferreiro/sistel2008/anexos/Diff&IntServ.pdf

Por tales motivos se consideró como mejor opción trabajar con Auto-QoS, donde dichos comandos propios de un switch CISCO, proporcionan las mejoras necesarias para el soporte de video y así garantizar el tráfico de video proveniente de las cámaras IP.

Se puede utilizar la función de auto-QoS para simplificar el despliegue de características de calidad de servicio. Auto-QoS determina el diseño de la red y permite configuraciones de QoS de manera que el interruptor puede dar prioridad a los flujos de tráfico diferente. También se utilizó los comandos del auto-QoS

para identificar los puertos que reciben tráfico de confianza. Auto-QoS realiza estas funciones:

- Detecta la presencia o ausencia de dispositivos de auto-QoS a través de interfaces de confianza condicionales.
- Se utiliza para clasificar el tráfico, para asignar etiquetas de paquetes, y para configurar las colas de entrada y salida.
- QoS está habilitado globalmente (mls QoS comando de configuración global), y otros comandos de configuración global se generan automáticamente.
- Interruptor permite la función de límite de confianza y usa el Cisco Discovery Protocol (CDP) para detectar la presencia de un dispositivo compatible.
- Vigilancia: se utiliza para determinar si un paquete está dentro o fuera de perfil y especifica la acción en el paquete.

3.6. ANALISIS DELFORMATODECOMPRESIÓNPARAVIDEO-IP

La elección de un determinado formato de compresión depende de la aplicación a la que vaya destinado. En el caso específico de video-vigilancia-IP se necesitó la utilización de un formato que no utilice mucho ancho de banda de la red, debido a que en un futuro podrían existir otros servicios que converjan sobre la misma. Así mismo el formato debe permitir una calidad de imagen aceptable para la visualización del movimiento y que a su vez el procesamiento de las imágenes no sea complejo para obtener un rendimiento óptimo en la aplicación.

Por tal motivo se escogió las cámaras IP ZKTECO que provee de todas estas características al comprimir el video en formato H.264, permitiendo una calidad de alta visualización de las imágenes con un poco consumo de ancho de banda, aunque requiera un procesamiento tanto complicado pero que no afectaría en gran medida al rendimiento del sistema.

3.7. DISCUSION

Dado que distintas aplicaciones como, por ejemplo, teléfono, correo electrónico y video vigilancia, pueden utilizar la misma red IP, es necesario controlar el uso compartido de los recursos de la red para satisfacer los requisitos de cada servicio. Una solución es hacer que los enrutadores y los conmutadores de red funcionen de maneras distintas para cada tipo de servicio (voz, datos y vídeo) del tráfico de la red. Al utilizar la Calidad de servicio (QoS) y sobre todo los Servicios Diferenciados distintas aplicaciones de red pueden coexistir en la misma sin consumir cada una el ancho de banda de las otras, sino que al usar DiffServ cada paquete marcado será tratado según la prioridad de la red.

Las ventajas principales de una red sensible a DiffServ son: la priorización del tráfico para permitir que paquetes importantes se gestionen antes que paquetes con menor prioridad, y una mayor fiabilidad de la red, ya que se controla la cantidad de ancho de banda que puede utilizar cada aplicación. El tráfico, que se considera crítico y requiere una latencia baja, es un caso típico en el que DiffServ puede garantizar respuestas rápidas a solicitudes de movimiento de paquetes.

Cabe recalcar que la red posteriormente instalada, es una red autónoma, configurada sobre una VLAN dedicada para este propósito, la video vigilancia, por lo tanto no está asociada a Internet, en caso de que el Internet falle o caiga, no afectará de ninguna manera a la red de video vigilancia, dando así más garantías y robustez a una red que debe estar 24 horas en funcionamiento.

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

La Calidad de Servicio es un parámetro muy importante que toda red convergente debe alcanzar, sin esta, la red no garantiza que todos los paquetes lleguen a su destino, o puede llegar a ser una transmisión lenta, convirtiéndose así en un problema para el usuario.

Un gran ancho de banda no es suficiente para dar la calidad de servicio que necesita una red, ya que en algún momento este puede sobrecargarse cuando haya distinto tipo de tráfico y el ancho de banda por sí solo no sabe priorizar la información que sea de mayor importancia para el usuario.

Se establece para el caso específico de video IP el Auto-QoS que es en donde mejor se ajusta los requerimientos en la transmisión de este tipo de tráfico en la red de la Facultad de Ingeniería de la UNACH.

Se determina que para poder escoger uno de los formatos de compresión de video el principal parámetro a tomar en cuenta es la cantidad de video grabado en un intervalo de tiempo, permitiendo tener más espacio en el disco disponible para la grabación de varios eventos. Para el caso del desarrollo de una aplicación de video vigilancia IP en la UNACH, la calidad que dicha aplicación requiere es la de transmisión con calidad TV, Por lo que se establece que el formato de compresión H.264 es el que deben incorporar las cámaras de red.

El sistema de video vigilancia que se instaló en la Facultad de Ingeniería, tiene todas las características de confiabilidad, robustez, y escalabilidad, gracias al proceso de configuración de Calidad de Servicio, tanto así que puede en esta misma red usarse servicios de telefonía IP o datos, siempre y cuando se sepa que

el video es prioridad en esta red.

El sistema RFID propuesto a inicios de este proyecto de investigación es totalmente innecesario, debido al uso de un Sistema Biométrico ya implementado en la Facultad, así evitamos redundancia de la información, gastos en mantenimiento, y pérdida de tiempo al momento en que el personal docente y administrativo se registra.

4.2. RECOMENDACIONES

Sedeberealizarunacorrectavaloracióndedispositivosysoftwarenecesario para la implementación delos escenarios de prueba, ya que de ellos dependerá la fiabilidad de los resultados obtenidos en los estudios.

Al momento de seleccionar el dispositivo de ruteo para la implementación se debe tomar en cuenta el tipo de IOS que soporta el switch ya que existen IOS que no soportan implementaciones de Calidad de Servicio y habrá que actualizarlos.

Se recomienda la utilización de herramientas comunes de análisis de tráfico tal como Wireshark ya que permite analizar en detalle los campos de los paquetes y presenta una interface gráfica amigable con el usuario.

En caso de que en un futuro se desee enviar por esta red otro tipo de datos, tomar en cuenta que al estar habilitada el DiffServ, se está priorizando el video al ser una red instalada y construida para este fin, y si se desea cambiar la prioridad se tendrán que ejecutar los comandos necesarios para un equipo CISCO.

Tomar muy en cuenta el crecimiento esperado de la red para la implementación de una arquitectura QoS, puesto que un cambio de arquitectura en una etapa avanzada de la vida útil de la red, podría inquirir en gastos innecesarios.

Si se desea incorporar más cámaras de red, no olvidar el formato de compresión con el cual ya se ha trabajado, para de esta manera mantener la homogeneidad en la calidad de visualización de las imágenes y no afectar al rendimiento global del sistema.

V. PROPUESTA

5.1. IMPLEMENTACION DE UN SISTEMA DE VIDEO VIGILANCIA IP EN LA FACULTAD DE INGENIERIA EN LA UNIVERSIDAD NACIONAL DE CHIMBORAZO

OBJETIVOS.

General.-

Efectuar un análisis comparativo de niveles y mecanismos de calidad de servicio para transmitir video por IP en la red de la Universidad Nacional de Chimborazo para la implementación de un sistema de video vigilancia en la Facultad de Ingeniería.

Específicos:

- Comparar niveles y mecanismos de calidad de servicio que soporten la transmisión de video en tiempo real garantizando la eficiencia y eficacia del sistema.
- Analizar las ventajas y desventajas de un sistema RFID.
- Estudiar las tecnologías de Hardware y Software para determinar los mejores equipos para el sistema de video vigilancia.
- Configurar e implementar el sistema de video vigilancia con su respectivo manual de usuario.

5.1.1. EQUIPOS Y MATERIALES

Para la instalación del sistema de video vigilancia se adquirieron los siguientes equipos, los cuales fueron donados a la Facultad de Ingeniería de la UNACH. Véase ANEXO 4.

- 10 cámaras IP marca ZKTECO con su respectivo Software de Gestión

- 1 CPU procesador Intel ® Celeron ® CPU J1800 2.41 Ghz
- 1 televisor marca TCL 32 pulgadas
- 450 m de cable UTP Cat 5e
- 100 m de cable gemelo #12
- 10 tomacorrientes
- 12 conectores rj45, 10 jacks rj45
- 30 canaletas
- 5 cajetines sobrepuestos
- 1 faceplate
- 12 tubos de silicón bison de alto rendimiento

5.1.1.1. CARACTERISTICAS

Cámaras IP marca ZKTECO

Tabla 19. Especificación Técnica de Cámara IP ZKTECO.
Fuente: El autor

Modelo	*ZKMD532*
Nombre	*1.0 MEGAPIXEL CMOS IR DOME IP CAMERA*
Sensor de Imagen	*¼ "CMOS*
Resolución de Imagen	*1280*720*
Iluminación mínima	*1 LUX (IR APAGADO), O LUX (IR PRENDIDO)*
Modo día/noche	*FILTRO AUTOMATICO PARA EL INFRAROJO*
Tipo de lentes	*3.6 mm LENTE FIJO*
Distancia Infrarrojo	*ANGULO DE PROYECCION DE 60º, DE 5-8 m*
Compresión de video	*H.264*
Resolución de video	*1280*720*
Interfaces de red	*10BASE-t/ 100BASE-tx ETHERNET*
Protocolos soportados	*TCP/IP, HTTP, TCP, UDP, ARP, SMTP, FTP, DHCP, DNS, DDNS, NTP, UPNP, P2P*
Cubierta	*METAL (ALEACION DE ALUMINIO) COLOR BLANCO*
Suministro de energía	*12V DC 1ª*
Consumo de energía	*5W*
Condiciones de trabajo	*+50º*
Peso	*1.43 Kgs*
Instalación	*MONTADO EN PARED*

Software De Gestión Zkivision

ZKivision es un software independiente bajo ZKTeco, que se centran principalmente en la oferta de productos de video vigilancia IP y soluciones innovadoras, que hecho gran diferencia y es altamente valorado por quienes han adquirido este producto. Dentro de sus principales equipos de gestión están las cámaras de megapíxeles IP, cámaras analógicas, NVR, DVR, software de cliente, software CMS y monitorear aplicaciones móviles que soportan Android, iPhone, Blackberry O dispositivos / S(ZKTECO, 2014)

La forma de uso de este Software se muestra en el Manual de Usuario. Véase ANEXO 5.

5.1.2. INSTALACION

Se procedió a realizar el levantamiento de información donde se debe constatar la ubicación correcta de los switch en cada uno de los bloques de la Facultad de Ingeniería, obteniendo la siguiente información: Véase ANEXO 6 y ANEXO 7.

Tabla 20. Ubicación de los switch usados para el sistema de video vigilancia

Fuente: El autor

SWITCH EXISTENTES EN LA FACULTAD DE INGENIERIA		
NOMBRE DEL BLOQUE O EDIFICIO	**UBICACION**	**MODELO DE SWITCH**
Bloque A	Segundo Piso: Área de Administrativos	Catalyst 3750
Bloque B	Primer Piso: Área Sala de Profesores	Catalyst 2960-S
Edificio Civil	Segundo Piso: Laboratorio de Computación	3com
Edificio Agroindustrial	Segundo Piso: Laboratorio	Catalyst 3750

Se buscó la mejor ubicación para colocar las cámaras, donde tenga la mejor visión de los principales accesos a cada uno de los Bloques.

Se trazó la trayectoria de los cables en los planos correspondientes a la infraestructura de la Facultad de Ingeniería. Véase ANEXO 8.

Con la información ya en planos se procedió a la instalación física de las cámaras y del cable UTP Cat 5e en la Facultad de Ingeniería. Véase ANEXO 9.

Tabla 21. Ubicación de cámaras
Fuente: El autor

UBICACIÓN DE CAMARAS EN LA FACULTAD DE INGENIERIA			
NUMERO DE CÁMARAS	**BLOQUE**	**SWITCH**	**PUERTOS HABILITADOS**
6	A	Catalyst 3750	16,17,18,19,20,21,22
2	B	Catalyst 2960-S	21,22,23
1	CIVIL	3COM	24
1	AGROINDUSTRIAL	Catalyst 3750	21,22,23

Para mejor control del sistema de video vigilancia se realizó la localización del computador en el Decanato de la Facultad, permaneciendo de forma definitiva en esta oficina para uso del Decano en función. Este computador actúa como servidor y es donde se instaló el Software de Gestión de cámaras. Véase ANEXO 10.

En la Facultad de Ingeniería se realizó la instalación de un sistema de video vigilancia, para ello es necesario que se haya creado una VLAN, esta VLAN es solo para el sistema de cámaras la cual tiene el siguiente dominio **192.168.153.0/24.** Al momento de instalar las cámaras, se cambian las direcciones IP que vienen por defecto a las direcciones apropiada con la VLAN destinada para el sistema de video vigilancia. Las nuevas direcciones se detallan a continuación:

Tabla 22. Nuevas direcciones para las cámaras IP
Fuente: El autor

NUEVAS DIRECCIONES IP DE LAS CÁMARAS					
Nº CAMARA	**BLOQUE**	**PISO**	**DIRECCIÓN IP ANTERIOR**	**DIRECCION IP ACTUAL**	**PUERTO HABILITADO EN SWITCH**
1	A	1er	192.168.1.30	192.168.153.51	17
2	A	1er	192.168.1.28	192.168.153.52	18
3	A	2do	192.168.1.27	192.168.153.53	19
4	A	2do	192.168.1.29	192.168.153.54	20

5	A	3er	192.168.1.24	192.168.153.55	21
6	A	3er	192.168.1.21	192.168.153.56	22
7	B	1er (acceso sala de profesores)	192.168.1.20	192.168.153.57	21
8	B	1er (acceso aulas)	192.168.1.26	192.168.153.58	22
9	CIVIL	1er	192.168.1.88	192.168.153.59	24
10	AGRO	1er	192.168.1.25	192.168.153.60	21

5.1.3. CONFIGURACION DE CALIDAD DE SERVICIO

La solución encontrada en el análisis de calidad de servicio, es aplicar Servicios diferenciados para lo cual se procedió con dicha configuración, es importante señalar que los comandos aplicados sirven únicamente para switch de la marca CISCO series desde 2600 hasta 7200.

5.1.3.1. CONFIGURACION SWITCH BLOQUE A

Crear la VLAN

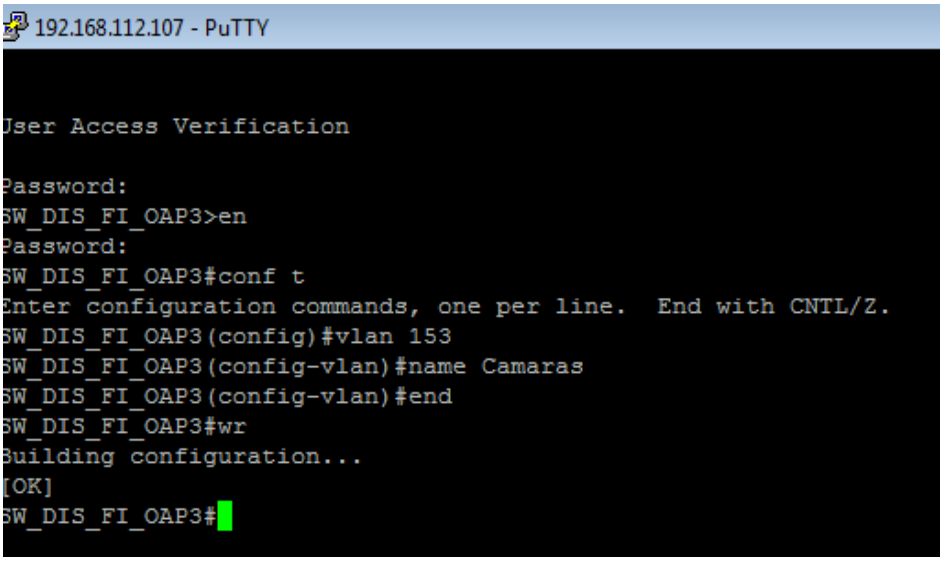


Figura 9. Configuración de VLAN Switch 3750
Fuente: El autor

```
127  USEG                             active
128  Evaluacion_Unach                 active
130  C_Directivo_Ing                  active
135  video                            active
140  VLAN0140                         active
149  RelojesDocentes                  active
150  Servidores                       active    Gi1/0/13
151  ESTADIO                          active
152  VideoSeguridad                   active
153  Camaras                          active
160  CTEAdministrativos               active
161  Videoconferencia                 active    Gi1/0/3, Gi1/0/4
170  Unidec                           active
171  UnachEvaluacion                  active
```

Figura 10. VLAN 153 activa
Fuente: El autor

Acceso a puertos para ser configurados

```
SW_AC_FI_AD1P2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_AC_FI_AD1P2(config)#inter
SW_AC_FI_AD1P2(config)#interface gi
SW_AC_FI_AD1P2(config)#interface gigabitEthernet 1/0/16
SW_AC_FI_AD1P2(config-if)#sw
SW_AC_FI_AD1P2(config-if)#switchport mode access
SW_AC_FI_AD1P2(config-if)#sw
SW_AC_FI_AD1P2(config-if)#switchport access vlan 153
SW_AC_FI_AD1P2(config-if)#no sw
SW_AC_FI_AD1P2(config-if)#no switchport voice vlan 20
SW_AC_FI_AD1P2(config-if)#end
SW_AC_FI_AD1P2#sh run
```

Figura 11. Configuración de puerto del servidor, puerto 16.
Fuente: El autor

```
SW_AC_FI_AD1P2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_AC_FI_AD1P2(config)#inter
SW_AC_FI_AD1P2(config)#interface range gi
SW_AC_FI_AD1P2(config)#interface range gigabitEthernet 1/0/17 -22
SW_AC_FI_AD1P2(config-if-range)#sw
SW_AC_FI_AD1P2(config-if-range)#switchport mode access
SW_AC_FI_AD1P2(config-if-range)#sw
SW_AC_FI_AD1P2(config-if-range)#switchport access vlan 153
SW_AC_FI_AD1P2(config-if-range)#no sw
SW_AC_FI_AD1P2(config-if-range)#no switchport voice vlan 20
SW_AC_FI_AD1P2(config-if-range)#exit
SW_AC_FI_AD1P2(config)#
```

Figura 12. Configuración de puertos de las cámaras, puertos desde 17 hasta 22.

Fuente: El autor

Configuración de QoS

```
SW_AC_FI_AD1P2(config-if-range)#auto
SW_AC_FI_AD1P2(config-if-range)#auto qo
SW_AC_FI_AD1P2(config-if-range)#auto qos video ?
  cts        Trust the QoS marking of the Cisco Telepresence System
  ip-camera  Trust the QoS marking of the Ip Video Surveillance camera

SW_AC_FI_AD1P2(config-if-range)#auto qos video ip-ca
SW_AC_FI_AD1P2(config-if-range)#auto qos video ip-camera
SW_AC_FI_AD1P2(config-if-range)#
```

Figura 13. Configuración de Auto-QoS

Fuente: El autor

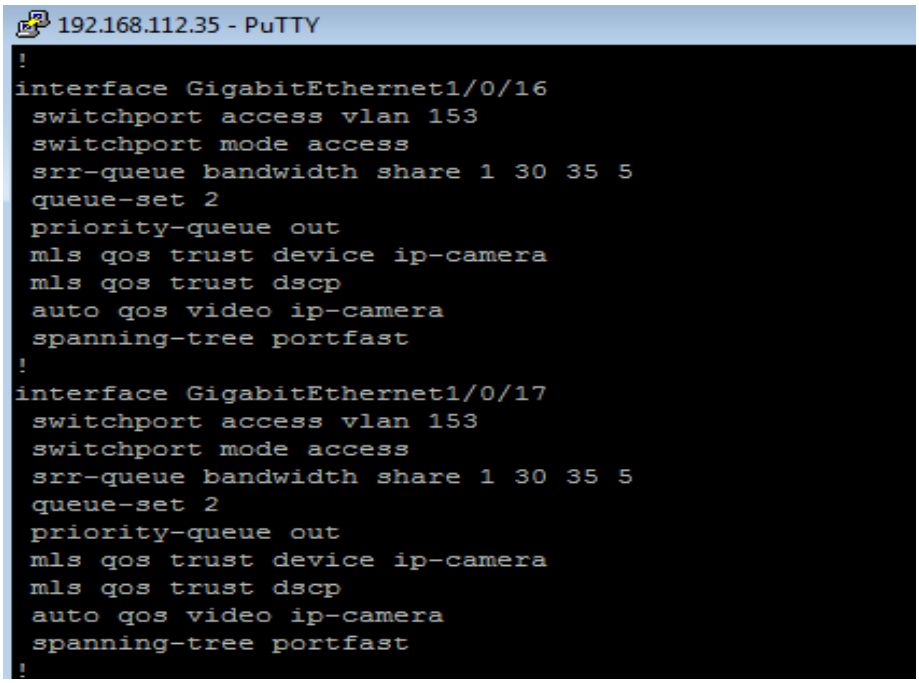


Figura 14. Comandos ejecutados al habilitar Auto-Qos
Fuente: El autor

5.1.3.2. CONFIGURACION DE SWITCH BLOQUE B

Crear la VLAN

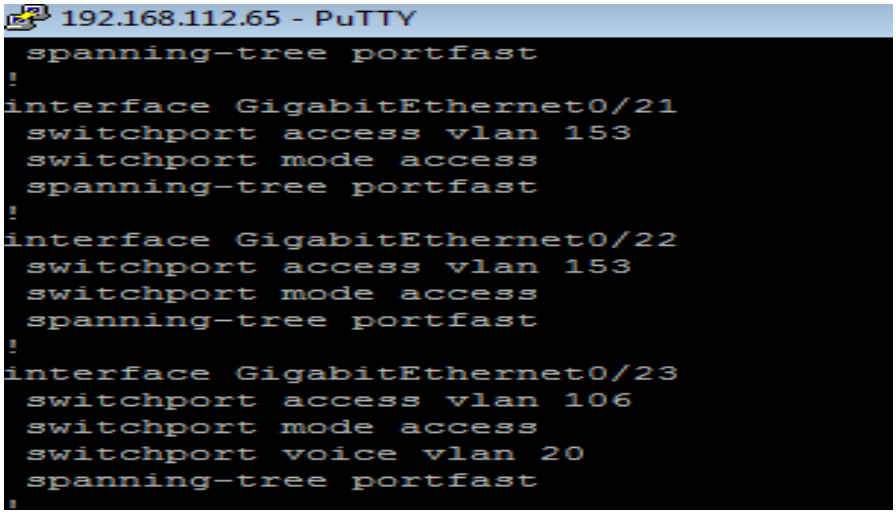


Figura 15. Configuración de VLAN switch Cisco 2960
Fuente: El autor

```
124  Wireless_Tplink                  active
127  USEG                             active
128  Evaluacion_Unach                 active
135  video                            active
150  Servidores                       active
151  ESTADIO                          active
152  VideoSeguridad                   active
153  Camaras                          active    Gi0/21, Gi0/22
160  CTEAdministrativos               active
161  Videoconferencia                 active
170  Unidec                           active
171  UnachEvaluacion                  active
172  Cisco_Wireless                   active
199  Sicoa_Unach                      active
```

Figura 16. Activación de VLAN 153 en switch catalyst 2960

Fuente: El autor

Configuración de Auto-QoS

```
192.168.112.65 - PuTTY
SW_DIS_AGR_LBP2(config-if)#SW
SW_DIS_AGR_LBP2(config-if)#SWitchport MODE
SW_DIS_AGR_LBP2(config-if)#SWitchport mode acces
SW_DIS_AGR_LBP2(config-if)#SWitchport mode access
SW_DIS_AGR_LBP2(config-if)#sw
SW_DIS_AGR_LBP2(config-if)#switchport access vlan 153
SW_DIS_AGR_LBP2(config-if)#no sq
SW_DIS_AGR_LBP2(config-if)#no sw
SW_DIS_AGR_LBP2(config-if)#no switchport voice vlan 20
SW_DIS_AGR_LBP2(config-if)#auto
SW_DIS_AGR_LBP2(config-if)#auto qos
SW_DIS_AGR_LBP2(config-if)#auto qos vide
SW_DIS_AGR_LBP2(config-if)#auto qos video ip ca
SW_DIS_AGR_LBP2(config-if)#auto qos video ?
  cts        Trust the QoS marking of the Cisco Telepresence System
  ip-camera  Trust the QoS marking of the Ip Video Surveillance camera

SW_DIS_AGR_LBP2(config-if)#auto qos video ip
SW_DIS_AGR_LBP2(config-if)#auto qos video ip-camera
SW_DIS_AGR_LBP2(config-if)#end
SW_DIS_AGR_LBP2#
```

Figura 17. Configuración de Auto-Qos
Fuente: El autor

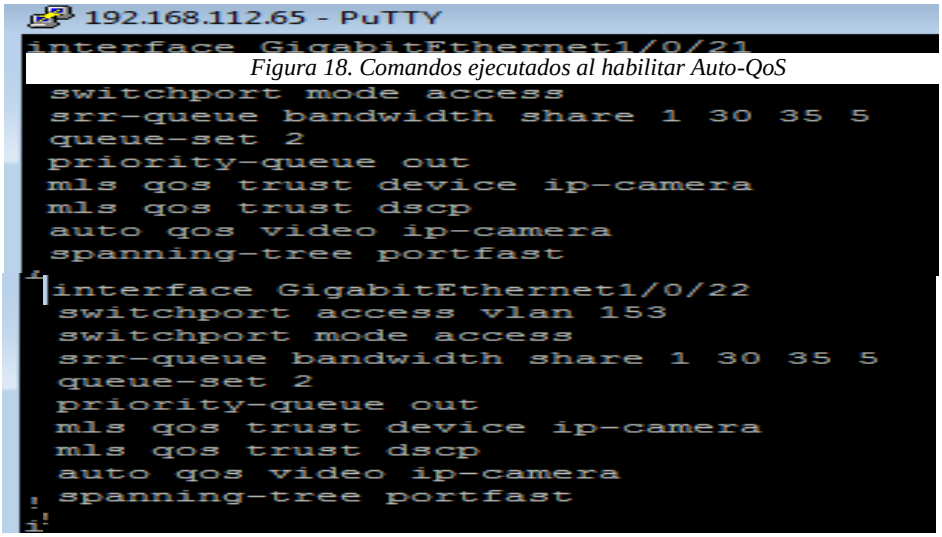


Figura 18. Comandos ejecutados al habilitar Auto-QoS

Fuente: El autor

5.1.3.3. CONFIGURACION AGROINDUSTRIAL

Configuración de Auto-QoS

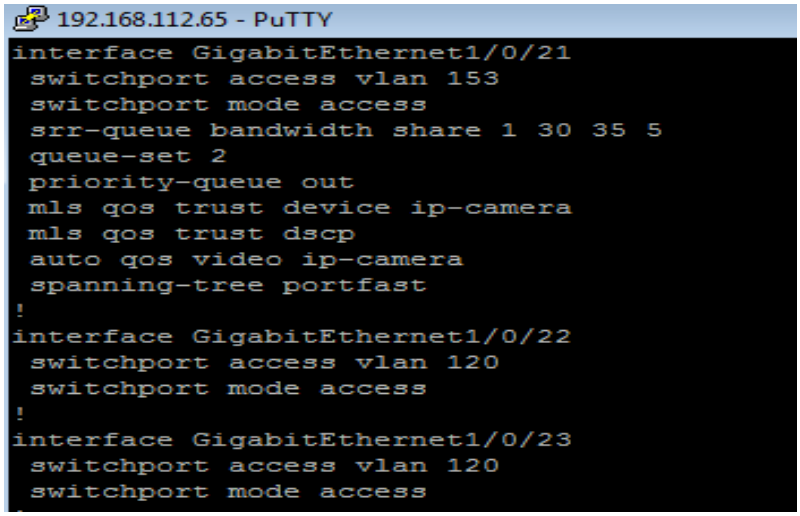


Figura 19. Configuración de Auto-QoS switch 3750 edificio de Agroindustrial

Fuente: El autor

VI BIBLIOGRAFIA

Bibliografía

CALDERON RIOS , D. (07 de 2012). *Tesis_t721ec SISTEMA DE COMUNICACIÓN Y MONITOREO PARA LA OPTIMIZACIÓN DE LA TRANSMISIÓN DE VOZ Y VIDEO VIGILANCIA CON PROTOCOLO IP EN LA UNIDAD ONCOLÓGICA SOLCA TUNGURAHUA*. Recuperado el 16 de 09 de 2015, de REPOSITORIO DIGITAL UNIVERSIDAD TECNICA DE AMBATO: http://repo.uta.edu.ec/bitstream/123456789/2371/3/Tesis_t721ec.pdf

SANCHEZ, E. (20 de 01 de 2015). *CAMARA WEB*. Recuperado el 16 de 09 de 2015, de PREZI: https://prezi.com/dsri_yawasug/camara-web/

GOMEZ CASTILLO, N. (14 de 05 de 2015). *UNA CAMARA IP ES UNA CAMARA QUE EMITE LAS IMAGENES DIRECTAMENTE*. Recuperado el 16 de 09 de 2015, de PREZI: https://prezi.com/ughdft72cydh/una-camara-ip-es-una-camara-que-emite-las-imagenes-directame/

(TIA), T. I., & (EIA), E. I. (2014). *TIA/EIA-568.*

BLANCO TIENDA, R. J. (02 de 10 de 2014). *PRACTICA 1 DE REDES: FABRICACION DE CABLES DE RED*. Recuperado el 16 de 09 de 2015, de RAFAEL BLANCO 92.

UQUILLAS LASSO, J. D. (03 de 2010). *DISEÑO DE UN ISP SOBRE ADSL PARA PRESTAR EL SERVICIO DE INTERNET Y SERVICIOS AGREGADOS DE VOZ (VOIP) Y DATOS Y ESTUDIO DE FACTIBILIDAD DE IMPLEMENTACION DEL ISP PARA LA CIUDAD DE PUERTO AYORA EN LA ISLASANTA CRUZ (GALAPAGOS).* Recuperado el 16 de 09 de 2015, de REPOSITORIO DIGITAL DE LA ESCUELA POLITECNICA NACIONAL.

GARCIA MATA, F. J. (2010). *VIDEOVIGILANCIA: CCTV USANDO VIDEOS IP*. VÉRTICE.

ALMORA MORALES, T. L. (s.f.). *SISTEMA DE CIRCUITO CERRADO PARA VIDEOVIGILANCIA BASADO EN SOFTWARE LIBRE Y ESTANDARES ABIERTOS.* Recuperado el 16 de 09 de 2015, de REPOSITORIO INSTITUCIONAL UNIVERSIDAD VERACRUZANA.

YAGUEZ GARCIA, J. (2011). *ARQUITECTURA DE REDES DE COMUNICACIONES.*

LARRIBA GARCÍA , J. C. (09 de 2009). *INTERFAZ DE TELEOPERACÓN Y CONTROL PARA PLATAFORMA ROBÓTICA MOVIL*. Recuperado el 16 de 09 de 2015, de UPM AUTONOMOUS SYSTEMS LABORATORY: http://tierra.aslab.upm.es/documents/PFC/PFC_JCLarriba.pdf

FIALLOS PROAÑO, R. R. (2011). *ANALISIS COMPARATIVOS DE PROTOCOLOS QoS USADOS EN LA IMPLEMENTACIONDE SISTEMAS DE SEGURIDAD Y VIGILANCIA BASADOS EN TECNOLOGIAS IP: CASO PRACTICO DESITEL*. Recuperado el 16 de 09 de 2015, de DSPACE ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO:

http://dspace.espoch.edu.ec/bitstream/handle/123456789/959/38T00265%20UDCTFIYE.pdf?sequence=1
ROJO MENDOZA, Y. (13 de 11 de 2012). *MEDIOS DE TRANSMISION DE DATOS*. Recuperado el 16 de 09 de 2015, de REDES DE COMPUTADORAS-BLOG: http://socializandoredes.blogspot.com/2012/11/medios-de-transmision-de-datos.html
INTER-AMERICAN TELECOMMUNICATION COMMISSION. (04 de 2010). *CALIDAD DE SERVICIO EN INTERNET*. Recuperado el 16 de 09 de 2015, de ORGANIZACION DE ESTADOS AMERICANOS: http://www.oas.org/en/citel/infocitel/2010/abril/calidad_i.asp
CEPEDA CARREÑO, K. (14 de 01 de 2014). *ESTUDIO DE FACTIBILIDAD TECNICA Y DISEÑO DE UN PROVEEDOR DE SERVICIOS DE INTERNET (ISP) INALAMBRICO DE BANDA ANCHAPARA EL CANTON BALZAR EN LA PROVINCIA DEL GUAYAS.* Recuperado el 16 de 09 de 2015, de REPOSITORIO DIGITAL INSTITUCIONAL DE LA UNIVERSIDAD CATOLICA SANTAGO DE GUAYAQUIL: http://repositorio.ucsg.edu.ec/bitstream/123456789/1708/1/T-UCSG-PRE-TEC-ITEL-31.pdf
GEROMETTA, O. (10 de 08 de 2010). *MODELO DE IMPLEMENTACION DE QOS*. Recuperado el 16 de 09 de 2015, de MIS LIBROS DE NETWORKING: http://librosnetworking.blogspot.com/2010/08/modelos-de-implementacion-de-qos.html
GARCIA REYES, T. (06 de 2007). *ANALISIS DE LOS MODELOS DE SERVICIOS DIFERENCIALES Y SERVICIOS INTEGRALES PARA BRINDAR QOS EN INTERNET.* Recuperado el 17 de 09 de 2015, de UTM UNIVERSIDAD TECNOLOGICA DE MIXTECA: http://mixteco.utm.mx/~resdi/historial/Tesis/Tesis-Thelma.pdf
ABAD AVILA, L. H. (2014). *ESTUDIO Y DISEÑO DE QOS PARA UNA RED DE INTERNET, DATOS Y VOIP*. Recuperado el 17 de 09 de 2015, de UNIVERSIDAD ISRAEL REPOSITORIO DIGITAL: http://repositorio.uisrael.edu.ec/bitstream/47000/899/1/UISRAEL%20-%20EC%20-%20SIS%20-%20378.242%20-%2057.pdf
PEREZ VEGA, C. (2006). *COMPRESION DE VIDEO, DEPEARTAMENTO DE INGENIERIA DE COMUNICACIONES.*
ZKTECO. (2014). *ZKTECO*. Recuperado el 04 de 11 de 2015, de ZKIVISION: http://www.zksoftware.rs/home.html
SALAVERT CASAMORT, A. *ALMACENAMIENTO DE LA INFORMACION DE LOS ORDENADORES.*
IBM REDBOOKS. (2006). *TCP/IP TUTORIAL Y DESCRIPCION TECNICA GENERAL.*
GEROMETTA, O. (10 de 11 de 2006). *¿QUE ES AUTOQOS ?* Obtenido de MIS LIBROS DE NETWORKING: http://librosnetworking.blogspot.com/2006/11/que-es-autoqos_10.html

VIII. ANEXOS

ANEXO 1. ESCENARIO DE PRUEBA PARA ANALISIS DE CALIDAD DE SERVICIO

ANEXO 2. INFORME COMPARATIVO ENTRE SISTEMA RFID Y SISTEMA BIOMETRICO.

INFORME COMPARATIVO TECNOLOGÍA RFID VS BIOMÉTRICA

1. ANTECEDENTES:

Este informe ha sido desarrollado debido a que en la tesis de tema "ANÁLISIS COMPARATIVO DE NIVELES Y MECANISMOS DE CALIDAD DE SERVICIO PARA LA TRANSMISION DE VIDEO Y TARJETAS RFID EN LA FACULTAD DE INGENIERIA EN LA UNIVERSIDAD NACIONAL DE CHIMBORAZO", presentado por los Señores Egresados de la Escuela de Electrónica y Telecomunicaciones, Erika Medina y Cristian Pazmiño, fue planteado el desarrollo de un sistema de control de personal con tecnología RFID teniendo en cuenta que al momento de ser planteada la tesis la Universidad Nacional de Chimborazo no contaba con ningún sistema tecnológico para el registro de docentes, pero en la actualidad y al momento de la implementación de la tesis la UNACH cuenta con un sistema biométrico en pleno funcionamiento de mejores características que el antes planteado en esta tesis, para lo cual surge la necesidad de hacer un informe técnico sobre ambos sistemas y no convertir ninguno de los dos en sistemas obsoletos y redundantes.

2 INFORMACIÓN TECNOLÓGICA:

2.1 RFID

La identificación por radio-frecuencia o RFID es un término genérico para denominar las tecnologías que utilizan ondas de radio para identificar automáticamente personas u objetos. Existen varios métodos de identificación, pero el más común es almacenar un número de serie que identifique a una persona u objeto, y quizás otra información en una etiqueta RFID, compuesta por un microchip conectado a una antena. Dicha antena permite que el chip transmita la información de identificación a un lector, el cual convierta las ondas de radio reflejadas por la etiqueta RFID en información digital que luego se puede transmitir a sistemas informáticos que puedan procesarla.

2.1.1 Funcionamiento

RFID (identificación por radiofrecuencia) es una tecnología empleada para el almacenamiento remoto y captura de datos que utiliza dispositivos denominados etiquetas, transponder o tags.

En los tags, formados por un chip y una antena, se almacena información que le da una identidad única al producto que la porta [BDEV2009].

El lector envía una serie de ondas de radiofrecuencia al tag, que éste capta a través de una pequeña antena. Estas ondas activan el microchip, que, mediante la micro antena y la radiofrecuencia, transmite al lector cuál es el código único del artículo [Implat2009].

Los datos capturados son procesados por un servidor que actualiza, en tiempo real, el sistema de gestión que se posea, generando una ventaja competitiva para el negocio [BDEV2009].

Elementos que componen un sistema RFID

Para que la tecnología RFID funcione, son necesarios tres elementos básicos: [Implat2009]

Una etiqueta electrónica, transpondedor o tag, que permite realizar la comunicación entre la etiqueta y el lector, a través de ondas de radio. En función del elemento usado existen dos tipos de etiquetas: las activas, que tienen una batería para alimentar el circuito, y las pasivas, que poseen un condensador el cual se carga con la energía emitida por el interrogador y luego utiliza dicha energía para responder.

Un lector de tags es un elemento fundamental de la RFID. No es sólo responsable de la lectura de las etiquetas por radiofrecuencia sino también de la transmisión de las informaciones contenidas en éstas hacia el nivel siguiente del sistema.

Una base de datos, la tecnología RFID facilita la recogida de multitud de datos que permiten obtener en gran detalle lo que está sucediendo. Además, estas lecturas son en general de manera automática, por este motivo es importante gestionar bien este gran volumen de datos.

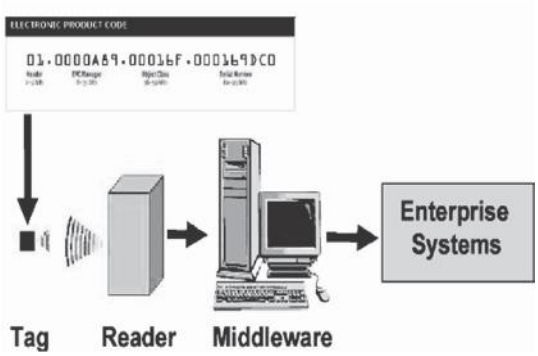


Figura 1. Elementos que componen un sistema RFID

2.1.2 Ventajas de la tecnología RFID

La tecnología RFID presenta ciertas ventajas las cuales veremos a continuación:

- Es una gran herramienta de identificación de objetos. Esta puede ser utilizada para garantizar la legitimidad de los productos y para la protección frente a falsificaciones, robos y fraudes.
- Ofrece la eliminación de errores de escrita y lectura de datos.
- Colección de datos de forma más rápida y automática además la tecnología Rfid garantiza la operación segura en ambientes severos (lugares húmedos, mojados, sucios, corrosivos, alta/baja temperatura, vibración, choques).
- Operación sin contacto y sin la necesidad de un campo visual y grande variedad de formatos y tamaños.
- Aparece como una tecnología con un bajo índice de error, proporciona una trazabilidad exacta, fiable y segura.
- Gracias a la tecnología RFID cada cliente tendrá su propia identidad en su tarjeta.

- El uso de esta tecnología en las personas puede producir resultados positivos, siempre y cuando sea regulada su utilización, bajo estricta clasificación, vigilancia y control.

2.1.3 Desventajas de la tecnología RFID

La tecnología RFID presenta ciertas desventajas las cuales veremos a continuación:

- El gran obstáculo de la tecnología RFID es el coste de los tags.
- Uno de los inconvenientes de la tecnología RFID son los altos costos de adquisición y el despliegue de los sistemas RFID.
- Costo del mantenimiento en cuanto a tarjetas incrementa al realizarse dicho mantenimiento periódicamente.
- El sistema sufre de desgaste constante y continuo debido a su emisión de Radio Frecuencia, propenso a colapsar.

2.2 BIOMÉTRICO

2.2.1 Funcionamiento

El término biometría proviene de los términos bio (vida) y metría (medida), estudia la identificación o verificación de individuos a partir de una característica física o del comportamiento de la persona. Esta tecnología se basa que cada persona es única y posee rasgos distintivos que pueden ser utilizados para identificarla.

2.2.2 Características

Las principales características que debe cumplir un sistema biométrico para la identificación de personal son:

- El desempeño: El sistema debe ser rápido, exacto y robusto al momento de identificar a un individuo.
- La aceptabilidad: El grado hasta el cual los usuarios están dispuestos a aceptar el sistema biométrico, el sistema debe proteger la integridad física de las personas y debe inspirar confianza ya que a veces en lugar deobtener información para validar un parámetro de acceso se puede estar profanando rasgos importantes del usuario.
- La fiabilidad: Esta característica refleja cuán seguro es el sistema al momento de validar la información de acceso ya que en ocasiones se puede tratar de suplantar la identidad de una persona por medio de diferentes técnicas como por ejemplo crear dedos de látex, prótesis de ojos, grabaciones de voz, copia de huella dactilar, etc.

2.2.3 Tipos de sistemas biométricos

En la actualidad se cuenta con un sin número de sistemas biométricos, estos se clasifican de la siguiente manera:

1. Por su Tecnología: La tecnología biométrica es el desarrollo de aplicaciones (sistemas biométricos) que permiten llevar a cabo de manera automatizada la identificación y verificación de la identidad de los

individuos. A continuación se describen de manera general las tecnologías biométricas con más presencia en el mercado.

- Reconocimiento de Huella Dactilar
- Reconocimiento de Iris y Retina
- Reconocimiento de la Geometría de la mano
- Reconocimiento de Firma escrita
- Reconocimiento de Voz

2. Por su uso: Según información proporcionada por el International Biometric Group, las tecnologías biométricas más utilizadas entre el año 2007 y 2013 fueron las siguientes: el reconocimiento de huellas dactilares (con un 54.2%), geometría de la mano (con un 13.5%), el escaneo de Iris y retina (con un 12%), el reconocimiento facial (con un 9.4%), el reconocimiento de voz (con un 6.2%), el análisis de firma escrita (con un 3.6%) y otras tecnologías (con un 1.1%).

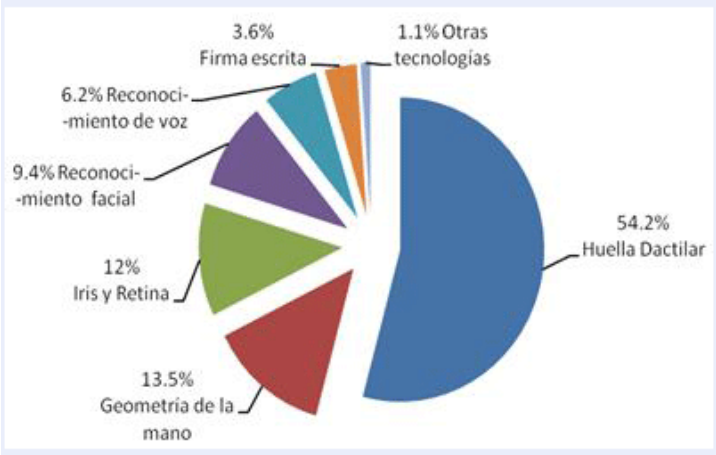


Figura 2. Porcentaje de tecnologías biométricas más utilizadas

Como la instalación de dicho sistema está instalado en la Universidad Nacional de Chimborazo, se va a profundizar acerca de los tipos de Biométricos existentes en la institución.

En la Universidad Nacional de Chimborazo se cuenta con un biométrico capaz de reconocer rostro y huellas dactilares, a continuación una explicación de las características de cada uno de ellos:

2.2.3.1 Rostro: Este sistema de reconocimiento es el más dable ya que el rostro es la manera directa para identificar familiares, amigos o conocidos. Los métodos utilizados en el reconocimiento de rostros van desde la correlación estadística de la geometría y forma de la cara, hasta el uso de redes neuronales que funcionan en el cerebro humano.

2.2.3.2 Huellas digitales: Gracias a que los patrones de las huella digitales son únicos y se mantienen durante la vida de la persona, ésta es la primera técnica que se viene a la mente y de hecho es un método utilizado en diversos proyectos de muchos países para la construcción de bases de datos de huellas digitales para

control y por otro lado la incorporación de la tecnología en diminutos aparatos tales como teléfonos móviles, ordenadores portátiles, teclados, tarjetas bancarias, armas de fuego, entre otros.
En la siguiente tabla se pueden resumir las diferentes características de los sistemas biométricos.

CARACTERISTICAS DE TECNOLOGIA BIOMETRICA		
	Huellas dactilares	**Cara**
Fiabilidad	Alta	Alta
Facilidad deuso	Alta	Alta
Prevención deataques	Alta	Media
Aceptación	Media	Muy alta
Estabilidad	Alta	Media

Tabla 1 . Características de tecnologías biométricas

2.2.4 Ventajas de la tecnología Biométrica:

Las ventajas que presentan el sistema biométrico instalado en la Facultad de Ingeniería en la Universidad Nacional de Chimborazo son:

- Como principal ventaja de la biometría es que es más cómoda y segura que los sistemastradicionales como las contraseñas, llaves, o tarjetas.
- No se puede perder y/o transferir ya que el elemento de identificación es una parte de nosotros mismos y no undispositivo externo. (Tarjetas, llaves, etc).
- No hay coste de mantenimiento. Al no haber ningún dispositivo externo de identificación, no hayque renovarlo cada cierto tiempo por caducidad, desperfecto, robo o pérdida.
- No se puede olvidar. Al no haber ninguna contraseña, no puede ser olvidada.

2.2.5 Desventajas de la tecnología Biométrica

- Si se usa el rostro de una persona para acceder a un sistema y se puede replicar con el uso de una fotografía, no sólo también se tendrá acceso, sino que, aunque se detecte dicho acceso, difícilmente podrá ser reemplazado. Si alguien roba un patrón biométrico, éste permanece robado de por vida, ya que no puede ser reemplazado, pues rostro solo tenemos uno.
- Es posible utilizar un dedo de silicona con la huella de una persona para acceder al sistema, si el equipo biométrico no es garantizado fácilmente puede ser vulnerado de esta manera.
- Alto costo del equipo biométrico.
- El software de reconocimiento de huellas dactilares sólo lee una sección del dedo de una persona que es propenso al error. Reposicionar manualmente los dedos para obtener la lectura correcta puede llevar mucho tiempo.

3. CUADRO COMPARATIVO DE TECNOLOGIAS

	Biométrico	**RFID**
Modificación de Datos	No Modificable	Modificable
Seguridad de Datos	Altamente seguro	Rango de baja a alta seguridad
Cantidad típica de datos (byte)	Ninguno	Alrededor de 64 KBytes
Costo	Ninguno	Medio (Unos 2 $ por targeta)
Costo suceptible a pérdida	No (Sin costo)	Si (2 $ por tarjeta)
Desgaste	Indefinido	Ninguno
Distancia de lectura	Contacto Directo	Del orden de 0.3 metro
Interfaz	Contacto	Sin barreras aunque puede haber interferencias
Susceptible a laSuciedad/líquidos	Ninguno	Ninguno
Influencia en ladirección y posición	MuyAlto	Ninguno
Suplantación de personal	No	Si
Identificación de Rostro	Si	No
Capacidad de Usuarios	50000	500
Puerto USB para extracción de datos	Si	Si
Tiempo de Identificación	</= 2 segundos	</=2 segundos

Tabla 2. Cuadro comparativo en Sistema Biométrico vs Sistema RFID

4. CONCLUSIONES

Después de analizar ambas tecnologías, la tecnología RFID y la tecnología Biométrica se puede concluir que:

- Para aplicar cualquiera de estas dos tecnologías se requiere de una inversión pero al momento de su funcionamiento y mantenimiento, se

puede comprobar que la tecnología biométrica tiene una gran ventaja frente a la tecnología RFID ya que con la tecnología biométrica no se hace uso de tarjetas y no se corre el riesgo de que en caso de pérdida se tenga que adquirir nuevas tarjetas.

- En cuanto a modificación de datos la tecnología Biométrica presenta la ventaja de mayor seguridad ya que una huella dactilar es única en cada individuo y es intransferible, mientras que una tarjeta para el lector RFID es fácilmente transferible entre el personal y propensa a pérdida.
- En cuanto al desgaste del sistema, tratándose de tecnología, ambas tecnologías tendrán su tiempo de vida útil, pero en comparación huella dactilar a tarjeta de lectura se conoce que una huella dactilar tiene un tiempo indefinido de uso al no tratarse de equipo electrónico, mientras que una tarjeta RFID tiene un tiempo definido de uso.
- La tecnología Biométrica que dispone la Universidad Nacional de Chimborazo es al contacto, debido a su registro por huella dactilar y además posee el registro por rostro con esto garantiza la autentificación de personalidad, en cambio con una tecnología RFID carece de esta ventaja a pesar de poder ser detectada a cierta distancia.
- El sistema Biométrico no se ve afectado por interferencia de frecuencias o por sistemas radiantes ajenos a este, lo que no sucede con la tecnología RFID que al ser un sistema que irradia frecuencia para la lectura de las tarjetas, en algún momento podrá verse afectado por algún tipo de frecuencia externa al sistema, el cual introduciría datos erróneos haciéndolo un sistema no confiable.
- Al referirse a la capacidad de usuarios, el sistema Biométrico es ampliamente superior al sistema RFID en una relación de 1000 a 1.

5. BIBLIOGRAFIA

UNAM – Facultad de Ingeniería. Biometría Informática. Recuperado de: http://redyseguridad.fip.unam.mx/proyectos/biometria/clasificacionsistemas/clasificaciontipo.html

RFID pasaporte electrónico. (Octubre 13, 2005). Ventajas y desventajas del rfid. Recuperado de: http://anita315.blogspot.com/2005/10/ventajas-y-desventajas-del-rfid.html

Manual Técnico, A TIEMPO Sistema de Comunicación, Reloj Biométrico Biosystem Stylus 980. Recuperado de: http://www.atiempo.com.ec/productos/sistemas_biometricos/

Con las conclusiones extraídas del informe comparativo entre la tecnología biométrica y la tecnología RFID se ha tomado la determinación de no aplicar un sistema con tecnología RFID en la Facultad de Ingeniería de la Universidad Nacional de Chimborazo, debido a que esta Institución cuenta con un sistema Biométrico en pleno funcionamiento y cumpliendo el trabajo que en un principio fue planteado como parte del control de personal en esta tesis. Se concluye que no es necesario un sistema RFID en la actualidad ya que se constituiría en un sistema redundante, de menor seguridad, mayor costo de mantenimiento, menor confiabilidad y sobre todo se trata de un sistema de menores características técnicas y tecnológicas frente al que el actualmente está implementado.

Para lo cual corrobora y respalda esta información:

Ing. Carlos Coloma M.
Director del Departamento de Administración de Talento Humano

Msc. Aníbal Llanga
Tutor de tesis Sistema

Msc. Rodrigo Briones
Decano de la Facultad de Ingeniería De la Universidad Nacional de Chimborazo

UNIVERSIDAD NACIONAL DE CHIMBORAZO
DEPARTAMENTO DE ADMINISTRACIÓN DEL TALENTO HUMANO
Ext.: 1141 - 1142

Riobamba, 23 de noviembre del 2015
Oficio. No. 2550-DATH-UNACH

Ingeniero
Rodrigo Briones
DECANO DE LA FACULTAD DE INGENIERÍA
Presente.-

De mi consideración:

Luego de expresarles un saludo cordial, el suscrito Director del Departamento de Administración del Talento Humano de la Universidad Nacional de Chimborazo, Ing. Carlos Coloma M.

CERTIFICA QUE: Los relojes biométricos de la Institución están en pleno funcionamiento para el registro del control de asistencia del Personal Docente, Administrativo y de Servicio.

Es todo cuanto puedo certificar en honor a la verdad, facultando a la interesada hacer uso del presente, como estime conveniente.

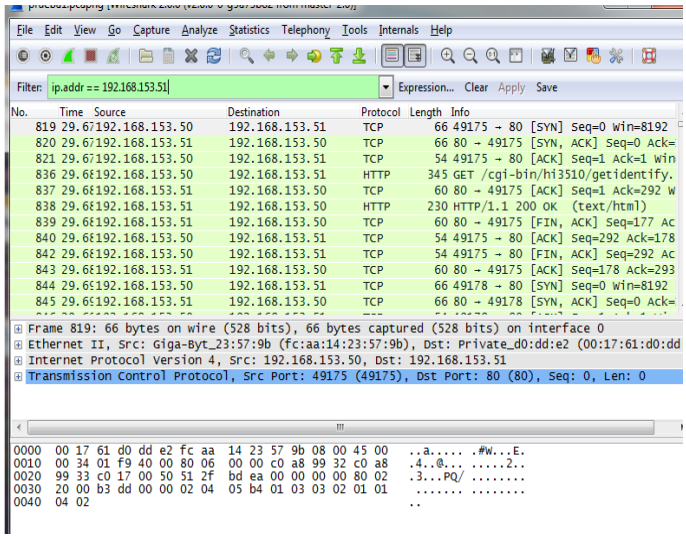
Atentamente,

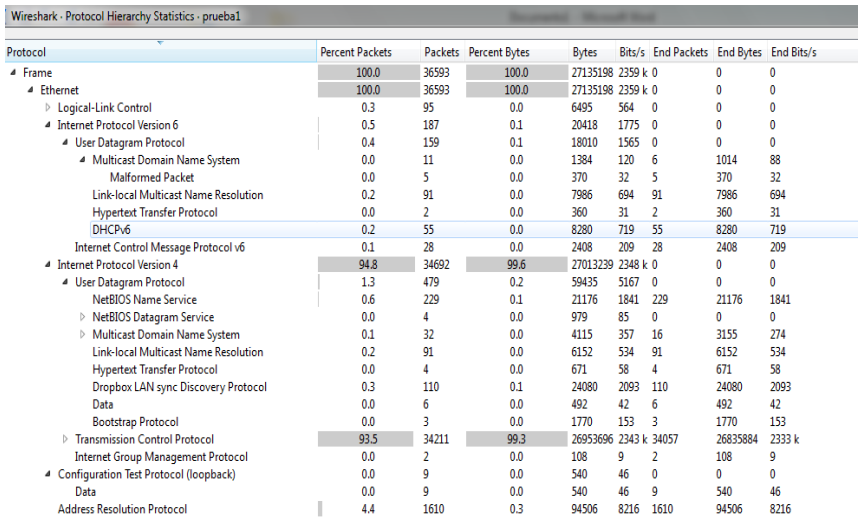
Ing. Carlos Coloma M.
DIRECTOR DEL DEPARTAMENTO
DE ADMINISTRACIÓN DE TALENTO HUMANO

C.c: Archivo
Elab por: Silvia Toala

ANEXO 3. RECOLECCION DE DATOS EN ESCENARIO DE PRUEBA.

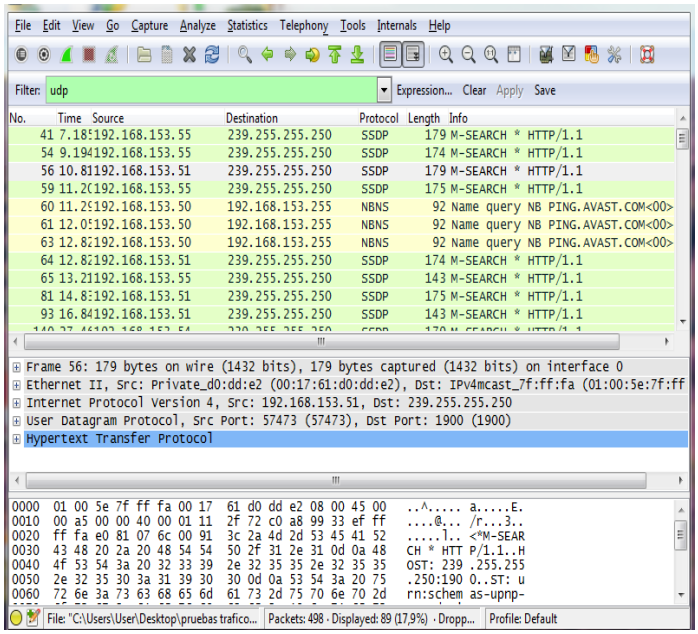
ANÁLISIS DE PAQUETES SIN TRAFICO-WIRESHARK

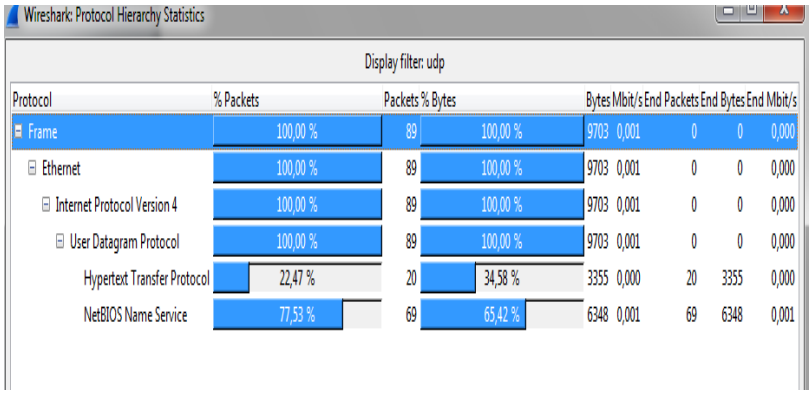




Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	36593	100.0	27135198	2359 k	0	0	0
Ethernet	100.0	36593	100.0	27135198	2359 k	0	0	0
Logical-Link Control	0.3	95	0.0	6495	564	0	0	0
Internet Protocol Version 6	0.5	187	0.1	20418	1775	0	0	0
User Datagram Protocol	0.4	159	0.1	18010	1565	0	0	0
Multicast Domain Name System	0.0	11	0.0	1384	120	6	1014	88
Malformed Packet	0.0	5	0.0	370	32	5	370	32
Link-local Multicast Name Resolution	0.2	91	0.0	7986	694	91	7986	694
Hypertext Transfer Protocol	0.0	2	0.0	360	31	2	360	31
DHCPv6	0.2	55	0.0	8280	719	55	8280	719
Internet Control Message Protocol v6	0.1	28	0.0	2408	209	28	2408	209
Internet Protocol Version 4	94.8	34692	99.6	27013239	2348 k	0	0	0
User Datagram Protocol	1.3	479	0.2	59435	5167	0	0	0
NetBIOS Name Service	0.6	229	0.1	21176	1841	229	21176	1841
NetBIOS Datagram Service	0.0	4	0.0	979	85	0	0	0
Multicast Domain Name System	0.1	32	0.0	4115	357	16	3155	274
Link-local Multicast Name Resolution	0.2	91	0.0	6152	534	91	6152	534
Hypertext Transfer Protocol	0.0	4	0.0	671	58	4	671	58
Dropbox LAN sync Discovery Protocol	0.3	110	0.1	24080	2093	110	24080	2093
Data	0.0	6	0.0	492	42	6	492	42
Bootstrap Protocol	0.0	3	0.0	1770	153	3	1770	153
Transmission Control Protocol	93.5	34211	99.3	26953696	2343 k	34057	26835884	2333 k
Internet Group Management Protocol	0.0	2	0.0	108	9	2	108	9
Configuration Test Protocol (loopback)	0.0	9	0.0	540	46	0	0	0
Data	0.0	9	0.0	540	46	9	540	46
Address Resolution Protocol	4.4	1610	0.3	94506	8216	1610	94506	8216

ANALISIS DE PAQUETES CON DIFFSERV





ANEXO 4. ACTA DE DONACION DE EQUIPOS A LA FACULTAD DE INGENIERIA DE LA UNACH

ACTA DE DONACIÓN PRIVADA:

PRIMERA.- COMPARECIENTES.- *a los 24 días del mes de diciembre del año 2015. Comparecen a la presente celebración* ***DE DONACIÓN****, por una parte, en calidad de donantes los señores:* ***CRISTIAN VINICIO PAZMIÑO JARA,*** *ecuatoriano, portador de la cédula de ciudadanía 0602749319 , mayor de edad, de estado civil soltero y la señorita* ***ERIKA PATRICIA MEDINA GAVIDIA,*** *portadora de la cédula de ciudadanía No. 0604179192; y por otra parte el señor* ***RODRIGO ALFONSO BRIONES,*** *portador de la cédula de ciudadanía 0600902860; en calidad de* ***DECANO DE LA FACULTAD DE INGENIERÍA*** *por sus propios derechos, por ellos formada, legalmente capaces para contratar y obligarse.*

SEGUNDA.- ANTECEDENTES.- *a) Los señores:* ***CRISTIAN VINICIO PAZMIÑO JARA y ERIKA PATRICIA MEDINA GAVIDIA,*** *están realizando y ejecutando la tesis de grado previa a la obtención del título de ingenieros en* ***ELECTRÓNICA Y TELECOMUNICACIONES,*** *al tratarse de la ejecución de la tesis se adquirieron ciertos equipos y aparatos que son propietarios los comparecientes en esta cláusula, que se detallan a continuación:*

1. *. Un televisor marca TCL, modelo L32T3540 de 32 pulgadas, con un valor de 330$.*

2. *. Un CPU serie CS513GNC01 con un valor de 800$*

3. *. Diez cámaras marca ZKTECO, modelo ZKMD532,con un valor de 160$ por unidad, con las siguientes series:*

   9192104310026
   9192104310038
   9192104310018
   9192104310045
   9192104310022
   9192104310032
   9192104310029
   9192104310066
   9192104310005
   9192104310025

Total del valor de equipos:2730 dólares americanos

4. *. Cuatrocientos metros de cable UTP categoría 5e*

5. *. Cien metros de cable gemelo #12*

TERCERA.- DONACIÓN.- *Con los antecedentes expuestos, que forman parte esencial e integrante de la presente acta de* ***DONACIÓN*** *y en mérito de los derechos y títulos invocados, los señores* ***CRISTIAN VINICIO PAZMIÑO JARA y ERIKA PATRICIA MEDINA GAVIDIA,*** *por sus propios derechos, de una forma voluntaria y bajo ninguna presión de alguna clase,* ***DONAN,*** *a favor de la* ***FACULTAD DE INGENIERIA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO*** *en calidad de decano de la misma al* ***MSC. RODRIGO ALFONSO BRIONES,*** *portador de la cédula de ciudadanía 0600902860, todos y cada uno de los equipos detallados en la cláusula segunda de la presente acta.*

CUARTA.- TRANSFERENCIA DE DOMINIO.- *Los donantes transfieren a favor del donatario el dominio y posesión de los bienes descrito anteriormente.*

QUINTA.- ACEPTACIÓN.- *el donatario en calidad de representante de la facultad de ingeniería, acepta la presente* ***DONACIÓN*** *en toda y cada una de las partes manifestando el testimonio de agradecimiento a los donantes antes mencionados, quienes a su vez se dan por notificados con esta aceptación.*

Para constancia de la presente acta de donación privada firman las partes por triplicado.

CRISTIAN VINICIO PAZMIÑO JARA
CI: 0602749319
DONANTE

ERIKA PATRICIA MEDINA GAVIDIA
CI: 0604179192.
DONANTE

RODRIGO ALFONSO BRIONES
DECANO DE LA FACULTAD DE INGENIERÍA
C.I: 0600902860
DONATARIO

UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERIA
SECRETARIA DECANATO
24 DIC 2015
Recibido Por: 10h15

ANEXO 5. MANUAL DE USUARIO PARA SOFTWARE DE CAMARAS ZKTECO.

Función

ZKiVision software de cliente es una pieza de software de red de vigilancia de vídeo proporcionado por ZK Tecnología de forma gratuita. Es compatible con múltiples funciones tales como monitoreo, grabación en vídeo, y la vinculación de alarma de múltiples cámaras IP a través de la LAN e Internet.
A medida que el dispositivo de video vigilancia es complejo, se recomienda encarecidamente leer el manual del usuario correspondiente antes del primer uso de este software y confirmar que el dispositivo puede ser visitado por el navegador en la LAN e Internet. Este documento describe cómo utilizar el software de cliente ZKiVision para la video vigilancia.

Entorno de funcionamiento

Sistema operativo: Windows / Windows XP / Windows / Windows Vista / Windows 7 (32 bits) 2000 2003. Se recomienda Windows XP.
Se recomienda Pentium Inter 4 o superior, 2.6 GHz o superior: CPU.

Adaptador de vídeo: Resolución de 1024 x 768 píxeles o superior. Mínimo de memoria de 256 MB, se recomienda ATI (AMD) adaptador de vídeo con la memoria 1G o superior.
Memoria: capacidad mínima de 1 GB. Se recomienda 2G o superior.

Disco duro: capacidad libre mínima de 80 GB (dependiendo del número de dispositivos y configuración de vídeo).
Como mejor ordenador puede traer un mejor efecto de la vigilancia, se recomienda utilizar un ordenador mejor para la vigilancia de vídeo.

Procedimiento para el Uso de ZKiVision

Antes de utilizar, haga lo siguiente:

Realizar la planificación e instalación de todas las cámaras IP utilizadas para la vigilancia.

Cambie las direcciones IP y los puertos de las cámaras IP a través del software de búsqueda.

Acceder a la cámara IP desde el navegador y establecer el nombre de usuario, contraseña, el modo de disparo de alarma (alarma externa o la detección de movimiento), y hora del sistema para estas cámaras IP.
Si tiene intención de acceder a estas cámaras IP a través de Internet, configurar los nombres de dominio dinámicos para ellos y realizar la asignación de puertos en los routers correspondientes.
La siguiente toma el súper usuario como ejemplo para describir el uso del software. Los procedimientos de operación varían con los usuarios de las distintas autoridades de operación. Los usuarios sólo tienen que operar los elementos que se muestran en la interfaz de la operación siguiendo el procedimiento de abajo.
Ejecutar este software de cliente.

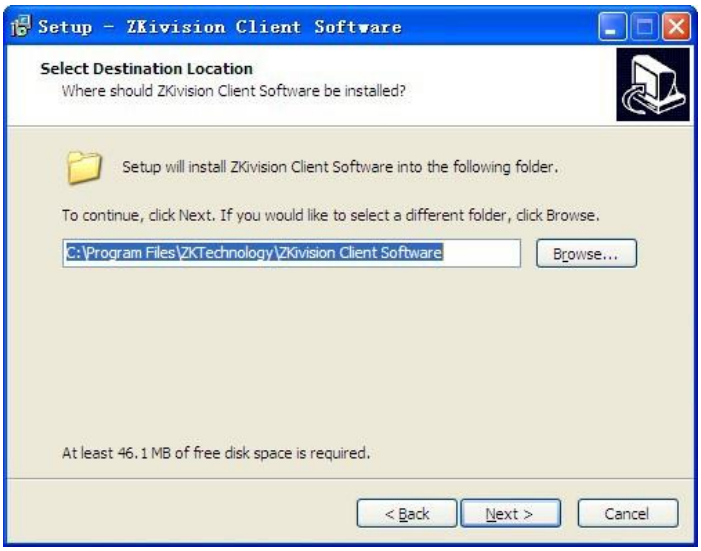
Inicie sesión en el sistema como superusuario ("Admin" y su contraseña predeterminada "123456") y cambiar la contraseña por defecto.
Buscar y añadir dispositivos al sistema.

Modificar los parámetros del dispositivo (incluyendo la información del dispositivo y los parámetros de red). Flujo de código Set.
Conjunto de armado (configuración de vinculación de alarma y gestión de almacenamiento). Vista previa de la imagen.
Usuarios Set (asignar las autoridades).

Convenciones

Para simplificar la descripción en este manual, se hacen las siguientes convenciones: software de vigilancia de vídeo en red se llama el software / sistema para abreviar.
Haga clic indica clic izquierdo del botón del ratón.

Doble click indica doble clic izquierdo del botón del ratón. Haz clic derecho indica haz clic con el botón derecho del ratón. Algunas de las figuras de este manual son sólo para referencia.



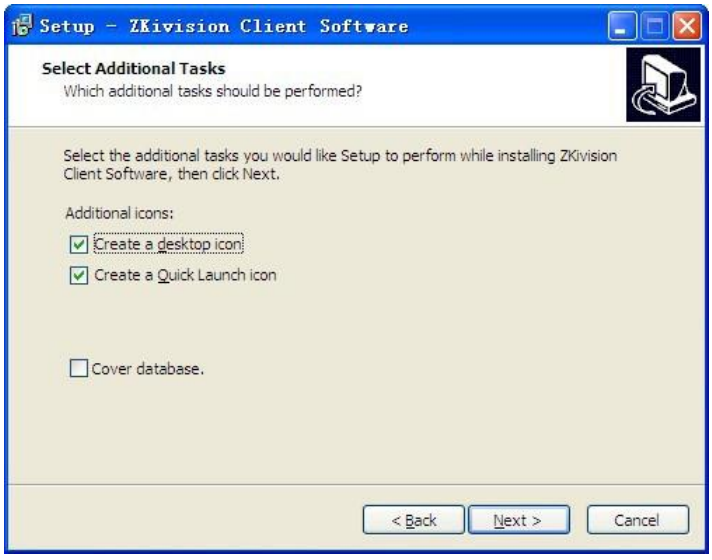
Instalación y Remoción

Instalación

Paso 1: Inserte el CD de entrega-adjunto en la unidad de CD. Haga doble clic en el paquete de instalación ZKiVision Cliente Software.exe. Elija el idioma de instalación, haga clic en Aceptar para continuar.
Paso 2: Haga clic en Siguiente cuando la interfaz de asistente de instalación aparece.

Paso 3: Establezca la ruta de instalación. La ruta predeterminada es C: \ Archivos de programa \ ZKTechnology \ ZKiVision Client Software \. Haga clic en Siguiente.

Paso 4: Confirmar la instalación es correcta y haga clic en Siguiente para esperar a la finalización de la instalación. Haga clic en Finalizar para salir.



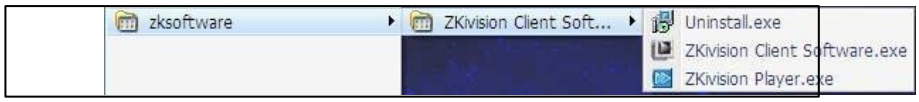
Nota: Si ya existe la carpeta de instalación, habrá un cuadro de mensaje aparece. Si desea instalar en la carpeta existido, habrá una selección de "base de datos de la cubierta" adicional. Selecciónelo para utilizarlo nueva base de datos, o utilizar la base de datos original.
Paso 5: Para la reconfiguración, por favor haga clic en Atrás, haga clic en Instalar para comenzar el proceso de instalación.

Paso 5: Una vez finalizada la instalación, haga clic en Finalizar para salir.

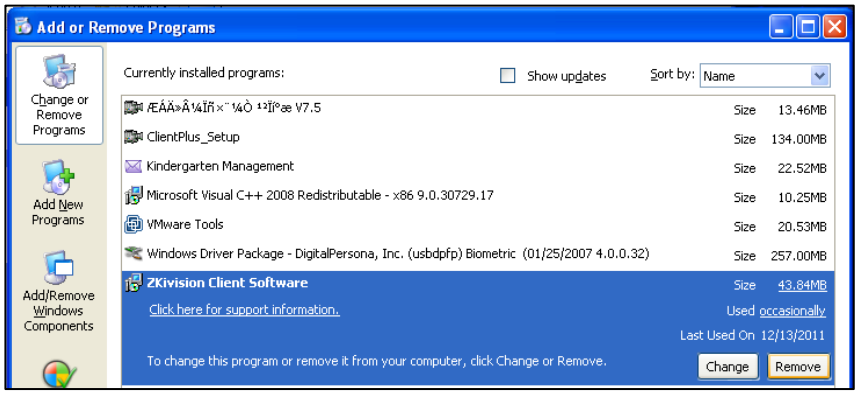
Remoción

Si no necesita usar más, puede eliminarlo en las siguientes dos maneras. Cierre todos los programas relacionados antes de la eliminación.

Modo 1: Seleccione Inicio> Todos los programas> ZKTechnology> ZKiVision Client Software> Desinstalar para eliminar documentos relacionados.



Modo 2: Abra el panel de control del sistema y seleccione ZKiVision Software de Cliente. Haga clic en Eliminar para eliminar documentos relacionados.



Nota: 1. Los dos modos anteriores no están disponibles para la eliminación de todos los documentos. Eliminación de los documentos relacionados en el directorio de instalación es necesario.
2. Cuando el software se desinstala, se mantendrá la base de datos y la configuración del usuario.

Guía de inicio rápido

Por medio de los siguientes procedimientos, puede realizar un ajuste rápido en el software de cliente.

1 Instale el software cliente y el icono del cliente de Monitor se muestra en el escritorio.

2 Haga doble clic en el icono del cliente Monitor para entrar en el sistema.
3 Elija Configuración> Administración de dispositivos> Buscar. Haga clic para mostrar la búsqueda interfaz.

4 Haga clic en Buscar en los dispositivos para buscar todos los dispositivos de cámaras producidas por nuestra empresa en la LAN.

5 Seleccione la cámara en la lista de búsqueda. Cambie la información del dispositivo a distancia (como la dirección y el dispositivo de puerto IP) en esta interfaz.
6 En la lista de búsqueda, seleccione una o más cámaras o marcar la casilla Seleccionar todo para seleccionar todas las cámaras.

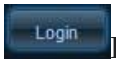
7 Haga clic en Aceptar para terminar de agregar cámaras al sistema.

8 Seleccione el canal de cámara en la lista de dispositivos en la interfaz de búsqueda modificar la información del dispositivo local (nombres de dispositivos y nombres de usuario). Se reparte el dispositivo.
9 Introduzca la interfaz de Vista previa. Haga doble clic en el canal de la cámara en la lista de dispositivos o arrastre el canal a la célula de vista previa para conectar el dispositivo. A continuación, el vídeo se puede previsualizar.
10 Seleccione Vídeo en el menú contextual o haga clic en para iniciar la grabación en vídeo.
11 Para más información de otras funciones como la configuración del usuario, la reproducción de vídeo, y la configuración de acoplamiento de la alarma, ver 5 Configuración.

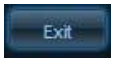
Entrada/salida

En esta página, usted puede conmutar de usuario a usuario y modificar la contraseña de usuario.

USER Seleccione el nombre de usuario para el sistema de inicio de sesión.
Password Introduzca la contraseña de usuario.



Haga clic en Inicio de sesión para iniciar sesión en el sistema después de seleccionar el nombre de usuario y escriba la contraseña.

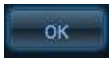


Haga clic en Salir para salir de la interfaz de inicio de sesión.

Haga clic en Modificar P.W. después de seleccionar un nombre de usuario existente para modificar la contraseña.
Contraseña antigua Escriba la contraseña antigua.

Nuevo tipo de contraseña en la nueva contraseña.

Confirmar Tipo contraseña en la nueva contraseña.

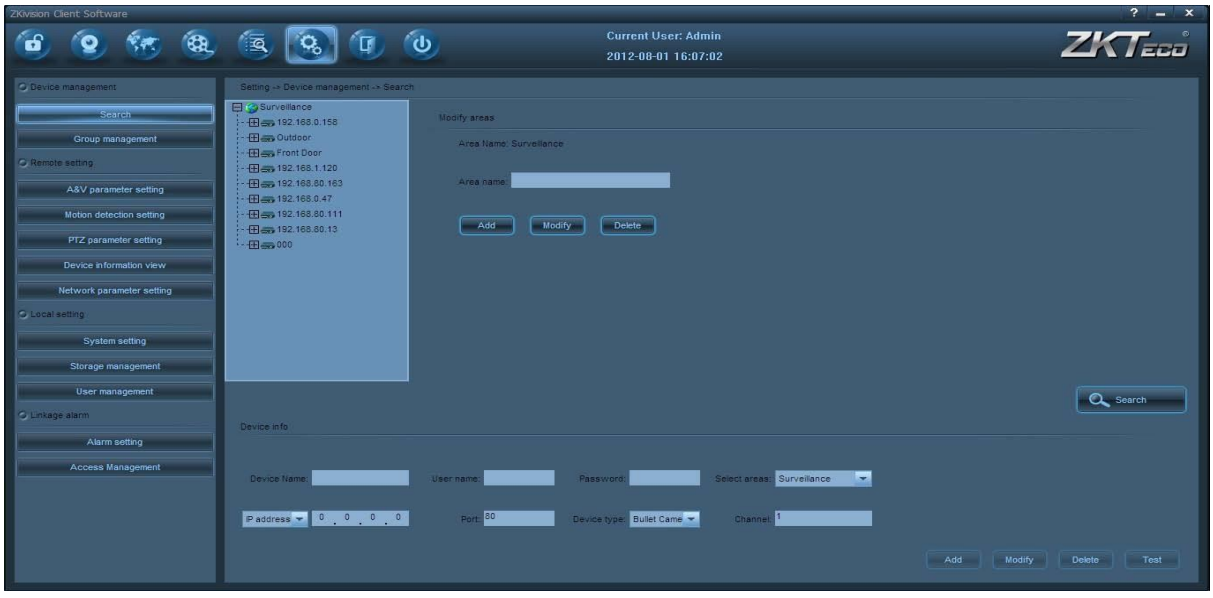


Haga clic en Aceptar para enviar la nueva contraseña.

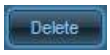
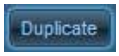
Haga clic en Eliminar para cancelar esta operación.

Nota: Superusuario Administrador existe en el sistema por defecto y la contraseña predeterminada es "123456".
Este superusuario no se puede borrar, y su nivel de usuario no se puede modificar

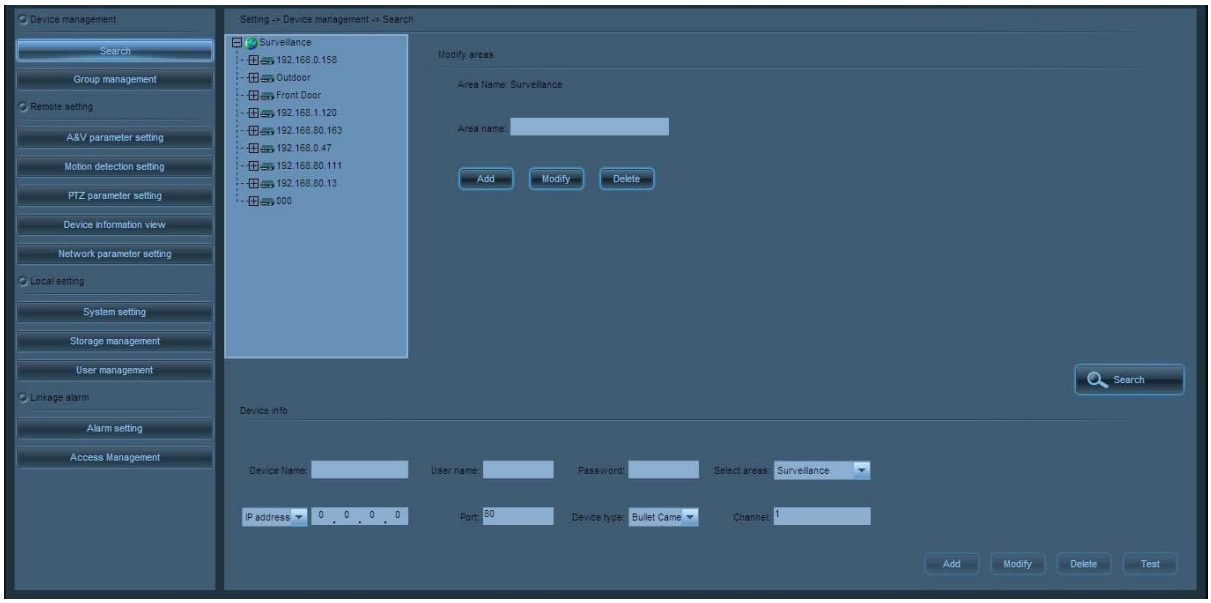
Ajustes



El menú Ajustes contiene 12 submenús y permite la configuración de múltiples dispositivos (por ejemplo, las cámaras IP).
Operaciones comunes y funciones icono en el menú Configuración
Selección de cámara: Seleccione un canal en la lista de dispositivos, haga clic en el nombre del canal. Conexión de la cámara: Conecte una cámara haciendo doble clic en el nombre del canal en la lista de dispositivos.

Icono	Función descriptiva
	Añadir dispositivos / áreas / grupos / preajustes de cámara / rutas de cruceros / usuarios
	Guardar parámetros modificados o cambiar a la modificación del estado.
	Eliminar dispositivos / áreas / grupos / preajustes de cámara / rutas de cruceros / usuarios existentes
	Sincronizar los parámetros modificados con el dispositivo remoto.
	Restaurar los parámetros a sus valores en el último ahorro.
	Restaurar parámetros a sus valores predeterminados
	Prueba si el dispositivo se puede conectar correctamente
	Guardar la información modificada a base de datos local
	Cancelar la modificación
	Copie la configuración a otros dispositivos

Buscar



Información De Área

Nombre de área El nombre de la zona de nivel superior de la zona elegida actualmente.
Nombre del área Las áreas que se pueden establecer.

Local Información Del Dispositivo

Nombre del dispositivo nombre del dispositivo que aparece en el software. Después de que el nombre del dispositivo está activado, la lista de dispositivos muestra sólo el nombre del dispositivo en lugar de la dirección IP del dispositivo.

Nombre de usuario El nombre de usuario que utiliza para visitar el dispositivo front-end. El dispositivo no puede conectarse con éxito a menos que introduzca un nombre de usuario correcto.

Contraseña La contraseña que se utiliza para acceder al dispositivo de front-end, y el dispositivo no se puede conectar con éxito a menos que introduzca una contraseña correcta.

Área El área en la que el dispositivo pertenece.
Dirección IP / nombre de dominio El dispositivo no puede conectarse con éxito a menos que la IP del dispositivo y el nombre de dominio son consistentes con la del dispositivo remoto.

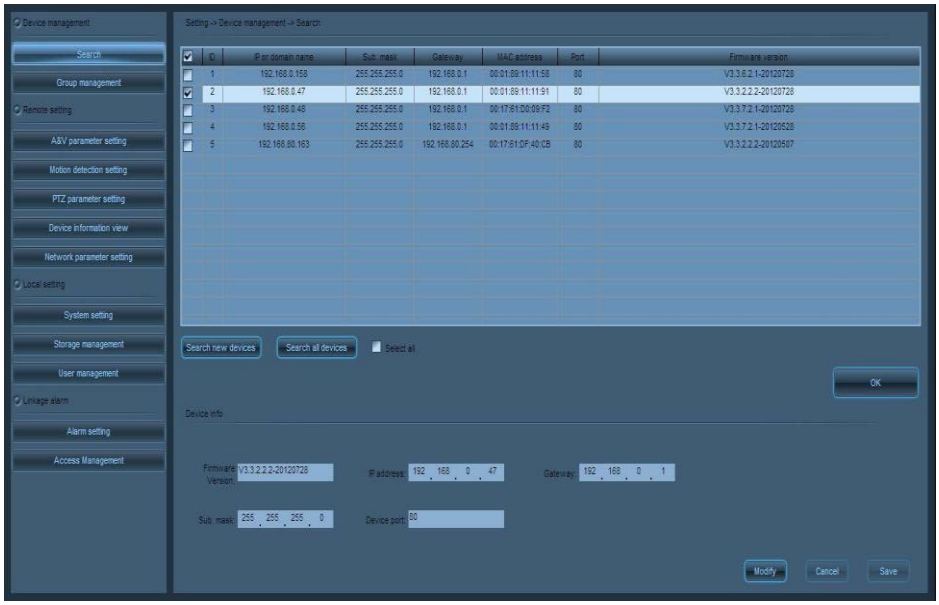
Puerto puerto de comunicación del dispositivo. El dispositivo no se puede conectar con éxito a menos que el puerto de comunicación del dispositivo es consistente con que en el dispositivo remoto.

Tipo de dispositivo de cámara tipo bala o una cámara domo.

Canal Actualmente sólo un canal de la cámara está disponible.
Nota: 1. Hay al Pueden añadirse la mayoría de 128 áreas.
2. Una vez finalizada la búsqueda de dispositivos, la cámara no puede cintas de vídeo o captura de imágenes a menos que se añade a una zona. Un dispositivo sin particiones no se puede utilizar.

Buscar dispositivo

Haga clic en Buscar para mostrar la interfaz de búsqueda:



Buscar en todos los dispositivos a través de la LAN.

Buscar nuevos dispositivos a través de la LAN.

Seleccionar todos los dispositivos en la lista de búsqueda.

Información Remota Del Dispositivo

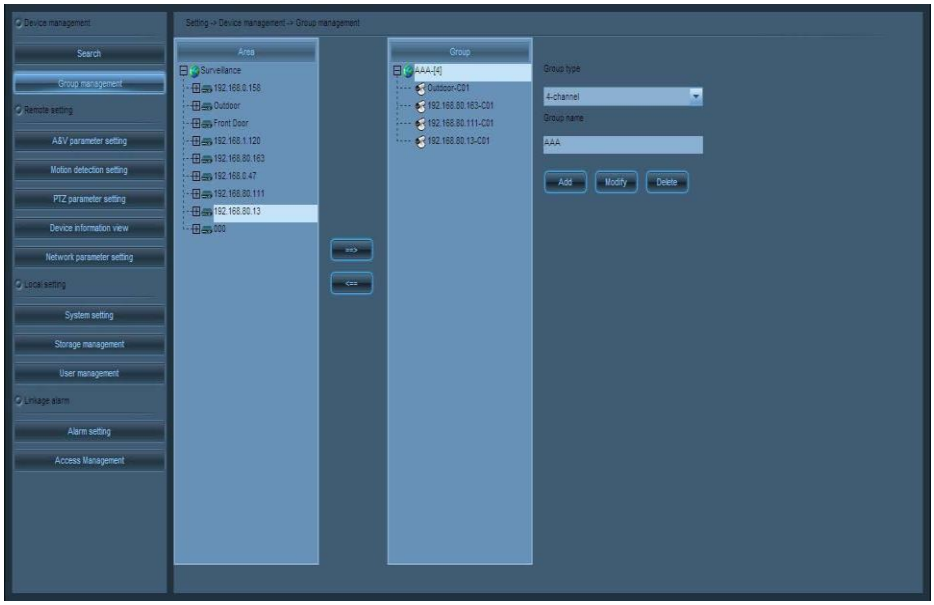
Versión de firmware La versión del firmware del dispositivo.
Dirección IP La dirección IP predeterminada es 192.168.1.88. Puede ser modificado según sea necesario.
Puerta de enlace La puerta de enlace predeterminada es 192.168.1.1. Es necesario que se restablezca si el dispositivo y el PC no están en el mismo segmento de red.
Máscara de subred La máscara de subred por defecto es 192.168.1.88. Puede ser modificado según sea necesario.
Puerto del dispositivo El número de puerto dispositivo es 80 por defecto. Para modificarlo, por favor póngase en contacto con los administradores de la red o los

profesionales de la red. La cámara se reiniciará después del puerto se modifica con éxito.

Administrador de contraseña Para modificar la dirección IP, puerta de enlace, máscara de subred o puerto, una contraseña de administrador correcta debe introducirse.

Haz clic OK aquí para volver a la interfaz superior.

Dirección del Grupo



Tipo de grupo Elegir tipo de grupo (de acuerdo a las cantidades de imagen), incluyendo las imágenes individuales, 4-imagen, 6-imagen, 8-imagen, 9-imagen o 16-imagen.

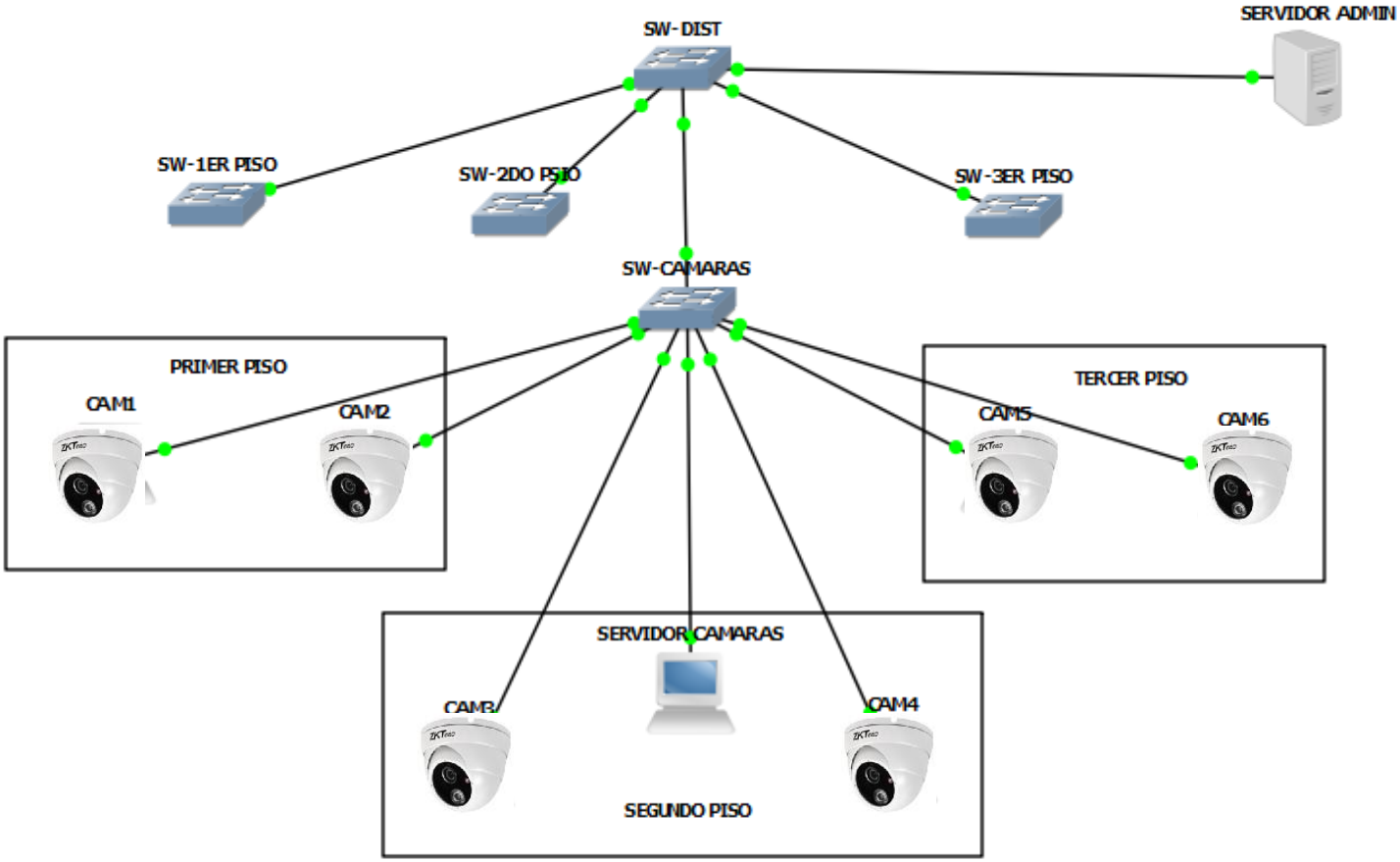
Nombre del grupo Establecer nombres de grupo

==> En la lista de dispositivos, seleccione el dispositivo que se agrupan. En la lista de grupos, haga clic en el grupo al que se añadirá a. Haga ==> para añadir el dispositivo a este grupo.

<== En la lista de grupos, seleccione el dispositivo que se elimina y, a continuación, haga clic para eliminar el dispositivo de este grupo.

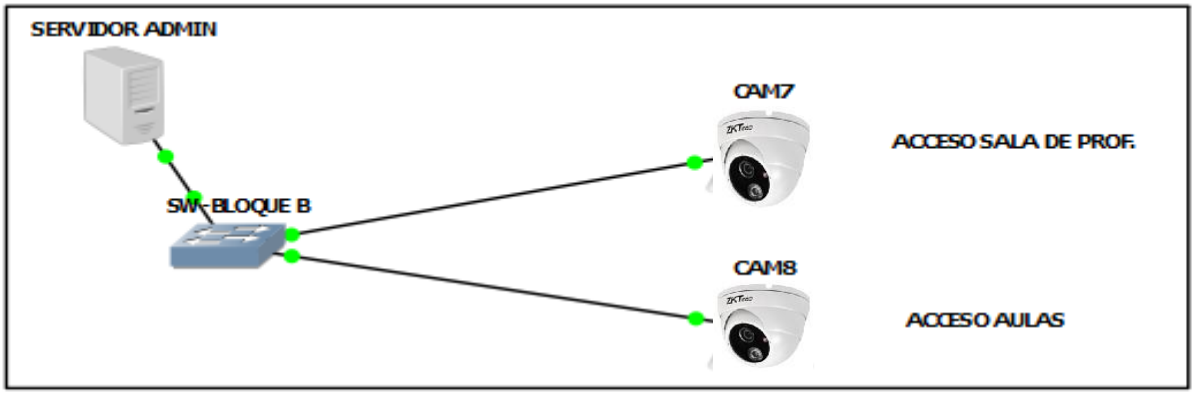
ANEXO 6. DIAGRAMAS DE RED

DIAGRAMA BLOQUE A



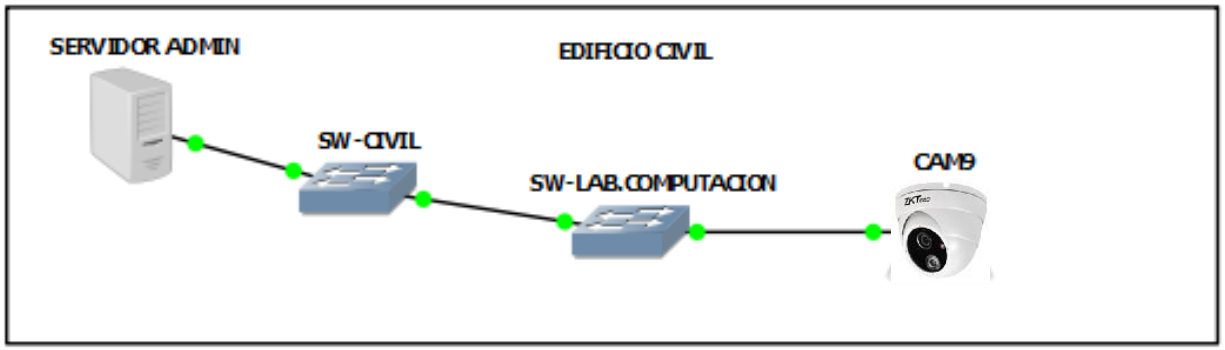
BLOQUE A FACULTAD DE INGENIERIA					
NOMBRE DEL EQUIPO	**MARCA-SERIE**	**UBICACIÓN**	**DIRECCION IP**	**PUERTOS**	
				DISPONIBLES	**# DE PUERTO CONECTADO**
SERVIDOR ADMIN	----------	CTE	----------	----------	----------
SW-DIST	CISCO 3750	Tercer piso sala de equipos	----------	24 Puertos	----------
SW-1ER PISO	CISCO 2960	Primer piso centro de idiomas	----------	24 Puertos	----------
SW-2DO PISO	CISCO 2960	Segundo piso Rack en secretarias	----------	24 Puertos	----------
SW-3ER PISO	CISCO 2960	Tercer piso laboratorio principal	----------	24 puertos	----------
SW-CAMARAS	CISCO 3750	Segundo piso Rack en secretarias	VLAN 153	16,17,18,19,20,21,22	----------
SERVIDOR	CPU	Segundo piso oficina de Decanato	192.168.153.50	----------	16
CAM1	ZKTECO	Primer piso puerta de ingreso principal	192.168.153.51	----------	17
CAM2	ZKTECO	Primer piso puerta posterior	192.168.153.52	----------	18
CAM3	ZKTECO	Segundo piso acceso a secretarias	192.168.153.53	----------	19
CAM4	ZKTECO	Segundo piso acceso auditorio	192.168.153.54	----------	20
CAM5	ZKTECO	Tercer piso acceso a laboratorio de electrónica	192.168.153.55	----------	21
CAM6	ZKTECO	Tercer piso acceso a laboratorios de computación	192.158.153.56	----------	22

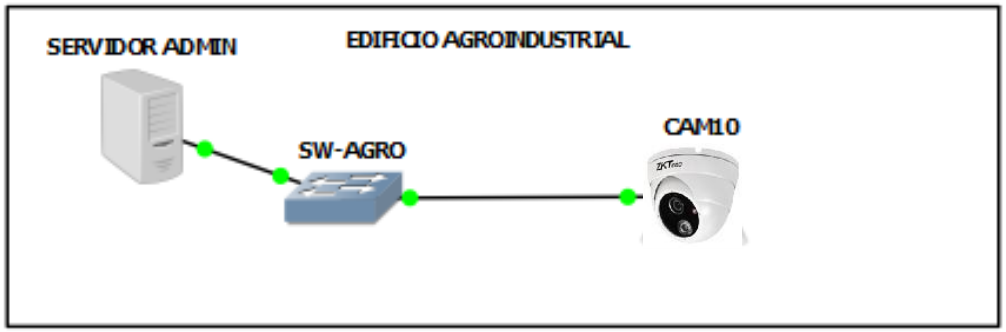
DIAGRAMA BLOQUE B



BLOQUE B FACULTAD DE INGENIERIA					
NOMBRE DEL EQUIPO	**MARCA-SERIE**	**UBICACION**	**DIRECCION IP**	**PUERTOS**	
				DISPONIBLES	**# DE PUERTO CONECTADO**
SERVIDOR ADMIN	----------	CTE	----------	----------	----------
SW-BLOQUE B	CISCO 2960	Rack sala de profesores	VLAN 153	24 PUERTOS	----------
CAM7	ZKTECO	Primer piso bloque B acceso a sala de profesores	192.168.153.57	……..	21
CAM8	ZKTECO	Primer piso bloque B acceso a aulas	192.158.153.58	……..	22

DIAGRAMA EDIFICIOS CIVIL Y AGROINDUSTRIAL





EDIFICIO CIVIL					
NOMBRE DEL EQUIPO	**MARCA-SERIE**	**UBICACION**	**DIRECCION IP**	**PUERTOS**	
				DISPONIBLES	**# DE PUERTO CONECTADO**
SW-CIVIL	CISCO 2960	Rack laboratorio segundo piso. Switch de distribución	----------	24 Puertos	…….
SW-LAB. COMPUTACION	3COM	Rack laboratorio de computación (actualmente aula) segundo piso.	VLAN 153	…….	Puerto 24 de SW_CIVIL
CAM9	ZKTECO	Primer piso entrada al edificio	192.168.153.59	……..	24
EDIFICIO AGROINDUSTRIAL					
SW-AGRO	CISCO 3750	Rack laboratorio segundo piso	VLAN 153	24 Puertos	…….
CAM8	ZKTECO	Primer piso entrada al edificio	192.158.153.60	……	21

ANEXO 7. EDIFICIOS DONDE ESTAN UBICADAS LAS CAMARAS DEL SISTEMA DE VIDEO VIGILANCIA.

BLOQUE A FACULTAD DE INGENIERIA

BLOQUE B FACULTAD DE INGENIERIA (ACCESO SALA DE PROFESORES

BLOQUE B FACULTAD DE INGENIERIA (ACCESO AULAS)

EDIFICIOS AGROINDUSTRIAL Y CIVIL

ANEXO 8. PLANOS DE LA UBICACIÓN DE LOS EQUIPOS DEL SISTEMA DE VIDEO VIGILANCIA IP.

UNIVERSIDAD NACIONAL DE CHIMBORAZO

DESCRIPCION: FACULTAD DE INGENIERIA
DEPENDENCIA: AULAS, PLANTA BAJA, BLOQUE "A"

SIMBOLOGIA

INSTALACIONES SISTEMA DE CAMARAS FACULTAD DE INGENIERIA

SW	SWITCH		CABLE UTP CAT e5
	DUCTO CABLEADO	UTP X?	NUMERO DE CABLES
	CAMARAS		

PLANTA BAJA

ESC. 1 : 300

UNIVERSIDAD NACIONAL DE CHIMBORAZO

DESCRIPCION: *FACULTAD DE INGENIERIA*
DEPENDENCIA: *ADMINISTRATIVO, PRIMERA PLANTA ALTA*

SIMBOLOGIA

INSTALACIONES SISTEMA DE CAMARAS FACULTAD DE INGENIERIA

SW	SWITCH	----------	CABLE UTP CAT e5
	DUCTO CABLEADO	UTP X?	NUMERO DE CABLES
	CAMARAS		

PRIMERA PLANTA ALTA

ESC. *1 : 300*

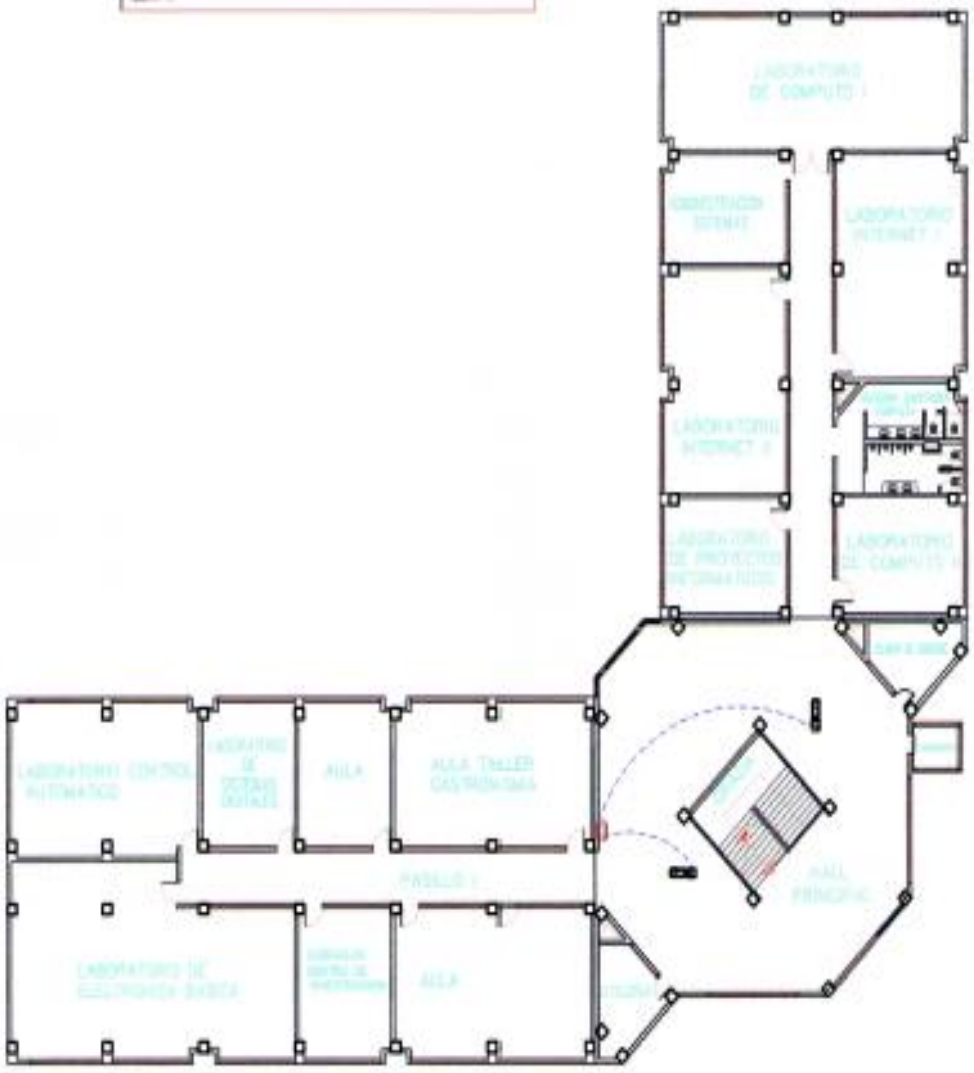
UNIVERSIDAD NACIONAL DE CHIMBORAZO

DESCRIPCION: *FACULTAD DE INGENIERIA*
DEPENDENCIA: *LABORATORIOS, SEGUNDA PLANTA ALTA*

SIMBOLOGIA

INSTALACIONES SISTEMA DE CAMARAS FACULTAD DE INGENIERIA

	SWITCH		CABLE UTP CAT e5
	DUCTO CABLEADO	UTPX?	NUMERO DE CABLES
	CAMARAS		



SEGUNDA PLANTA ALTA

ESC. 1 : 300

UNIVERSIDAD NACIONAL DE CHIMBORAZO

DESCRIPCION: FACULTAD DE INGENIERIA
DEPENDENCIA: BLOQUE B, AULAS Y LABORATORIOS, PLANTA BAJA

SIMBOLOGIA

INSTALACIONES SISTEMA DE CAMARAS FACULTAD DE INGENIERIA

	SWITCH		CABLE UTP CAT e5
	DUCTO CABLEADO	UTP X?	NUMERO DE CABLES
	CAMARAS		

PLANTA BAJA

ESC. 1 : 350

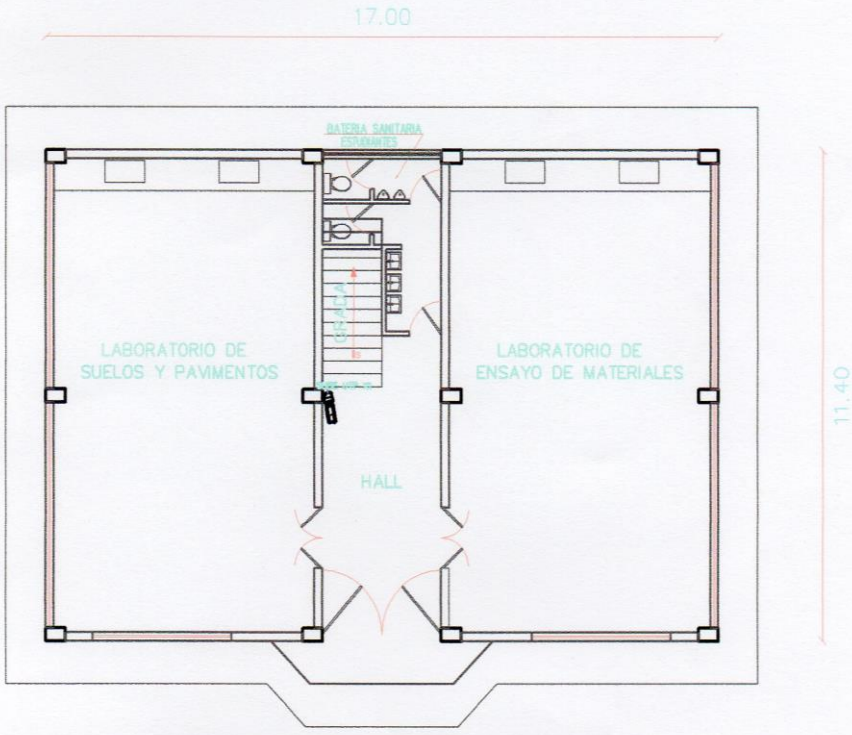
UNIVERSIDAD NACIONAL DE CHIMBORAZO

DESCRIPCION: *FACULTAD DE INGENIERIA*
DEPENDENCIA: *LABORATORIOS DE INGENIERIA CIVIL, PRIMERA PLANTA*

SIMBOLOGIA

INSTALACIONES SISTEMA DE CAMARAS FACULTAD DE INGENIERIA

SW	SWITCH	---------	CABLE UTP CAT e5
	DUCTO CABLEADO	UTP X?	NUMERO DE CABLES
	CAMARAS		



PLANTA BAJA

ESC. *1 : 150*

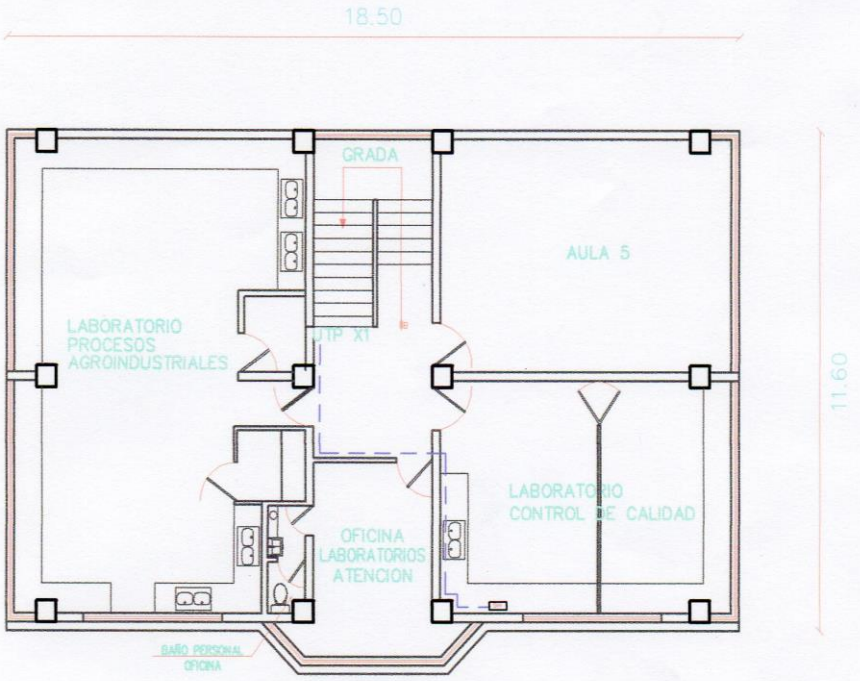
UNIVERSIDAD NACIONAL DE CHIMBORAZO

DESCRIPCION: *FACULTAD DE INGENIERIA*
DEPENDENCIA: *BLOQUE DE AULAS-LABORATORIOS, PRIMERA PLANTA ALTA*

SIMBOLOGIA

INSTALACIONES SISTEMA DE CAMARAS FACULTAD DE INGENIERIA

SW	SWITCH	--------	CABLE UTP CAT e5
	DUCTO CABLEADO	UTP X?	NUMERO DE CABLES
	CAMARAS		



PRIMERA PLANTA ALTA

ESC. *1 : 150*

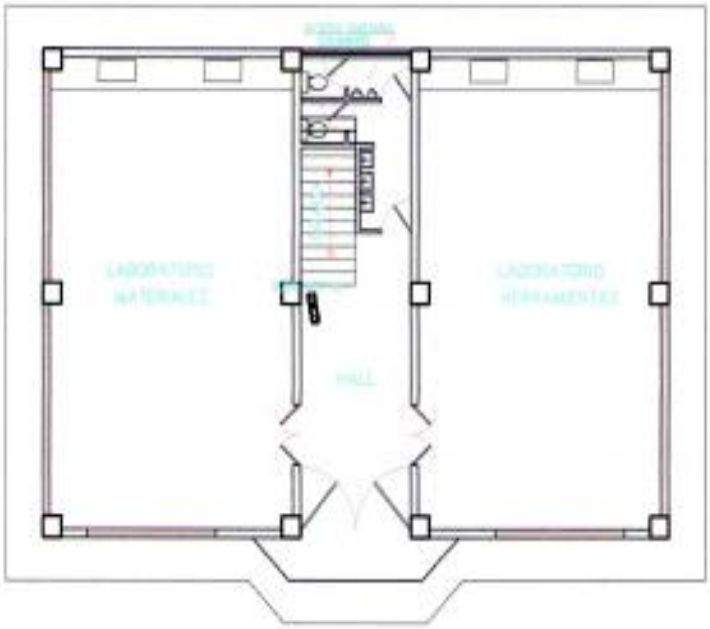
UNIVERSIDAD NACIONAL DE CHIMBORAZO

DESCRIPCION: *FACULTAD DE INGENIERIA*
DEPENDENCIA: *BLOQUE DE LABORATORIOS, PLANTA BAJA*

SIMBOLOGIA

INSTALACIONES SISTEMA DE CAMARAS FACULTAD DE INGENIERIA

	SWITCH		CABLE UTP CAT e5
	DUCTO CABLEADO	UTP X?	NUMERO DE CABLES
	CAMARAS		



PLANTA BAJA

ESC. *1 : 150*

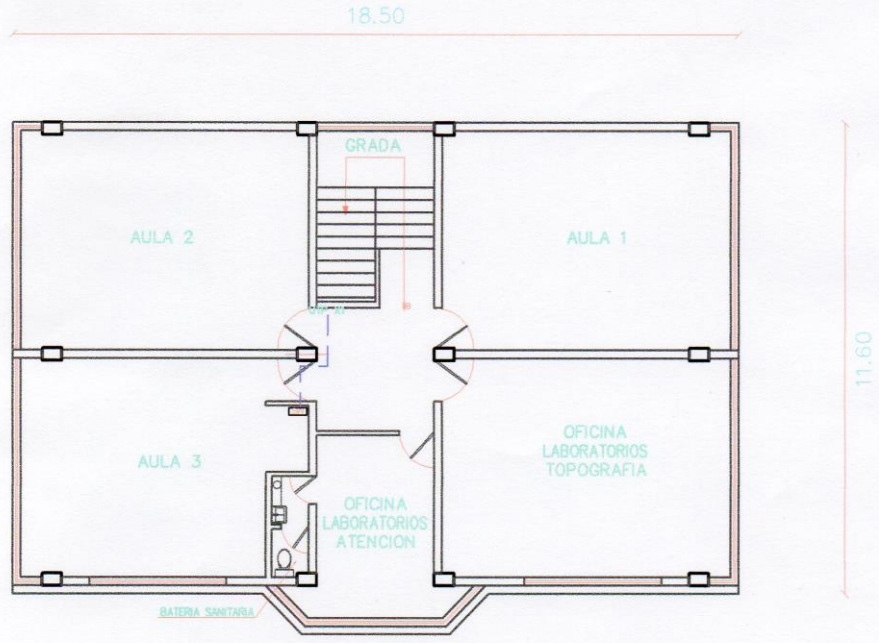
UNIVERSIDAD NACIONAL DE CHIMBORAZO

DESCRIPCION: *FACULTAD DE INGENIERIA*
DEPENDENCIA: *LABORATORIOS DE INGENIERIA CIVIL, SEGUNDA PLANTA*

SIMBOLOGIA

INSTALACIONES SISTEMA DE CAMARAS FACULTAD DE INGENIERIA

SW	SWITCH	---------	CABLE UTP CAT e5
	DUCTO CABLEADO	UTP X?	NUMERO DE CABLES
	CAMARAS		



PLANTA ALTA

ESC. *1 : 150*

ANEXO 9. INSTALACION DE LAS CAMARAS DEL SISTEMA DE VIDEO VIGILANCIA

FACULTAD DE INGENIERIA BLOQUE A

Primer piso - BIOMÉTRICOS

Primer piso - PUERTA POSTERIOR

Segundo piso – ADMINISTRATIVOS

Segundo piso – AUDIOVISUALES

Tercer piso- LABORATORIOS ELECTRONICA

Tercer piso – LABORATORIOS COMPUTACION

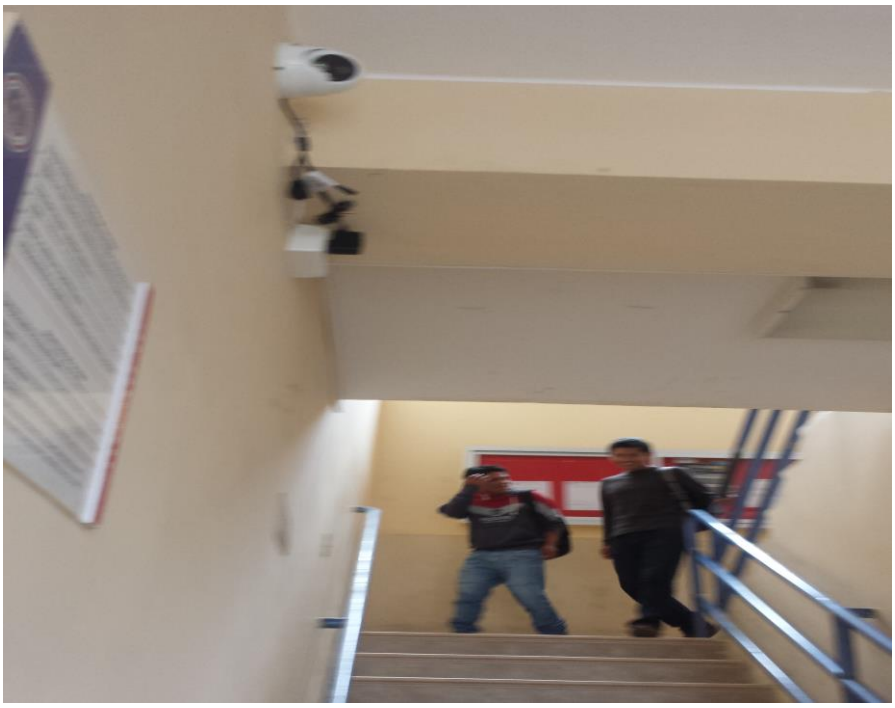
FACULTAD DE INGENIERIA BLOQUE B

Acceso a aulas

Acceso a Sala de profesores

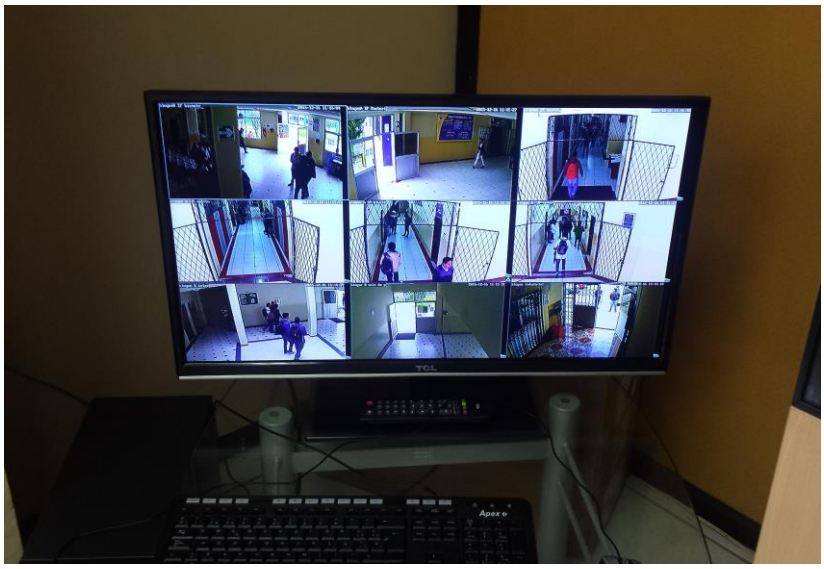
FACULTAD DE INGENIERIA EDIFICIO AGROINDUSTRIAL

FACULTAD DE INGENIERIA EDIFICIO CIVIL



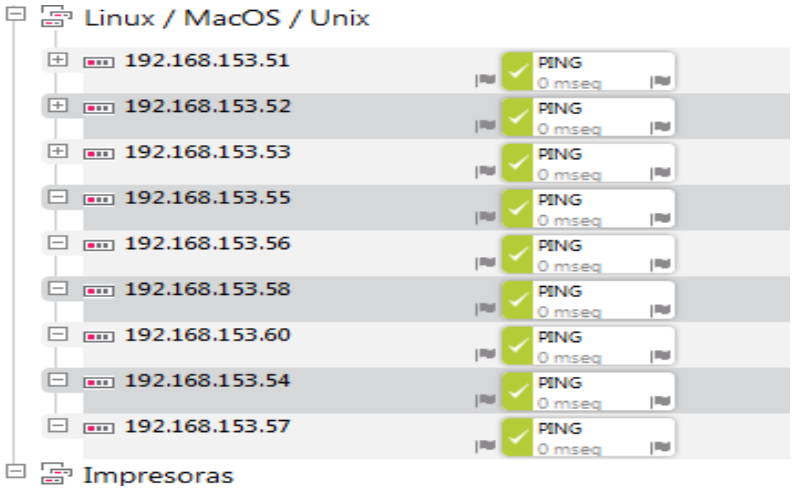
ANEXO 10. UBICACIÓN DE EQUIPO SERVIDOR (CPU Y TELEVISOR)

Oficina de Decanato

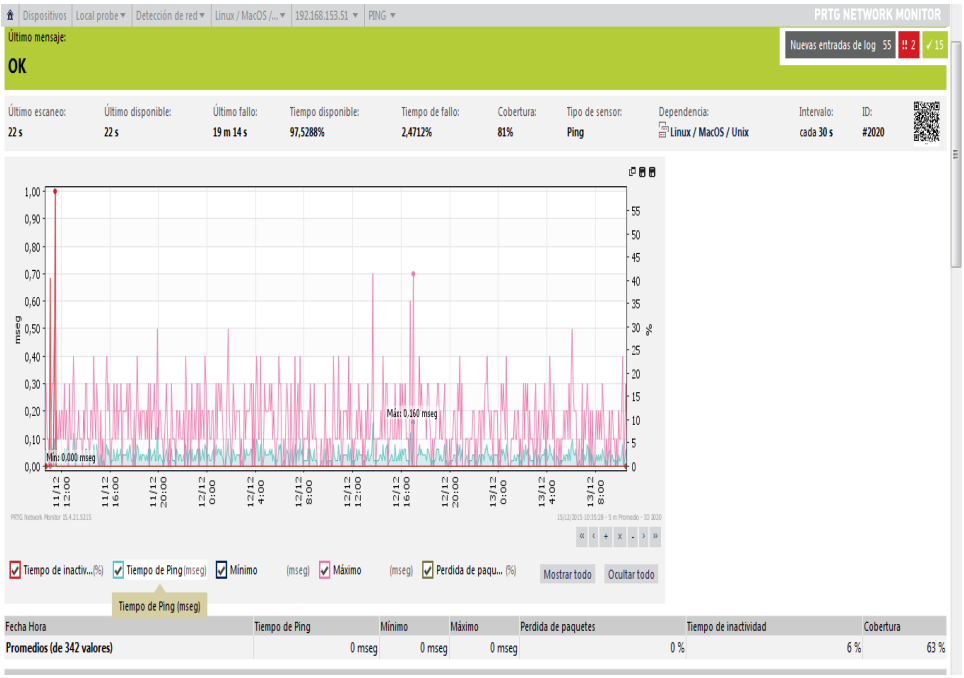


ANEXO 11. TRAFICO DE LA RED DEL SISTEMA DE VIDEO VIGILANCIA EN FUNCIONAMIENTO

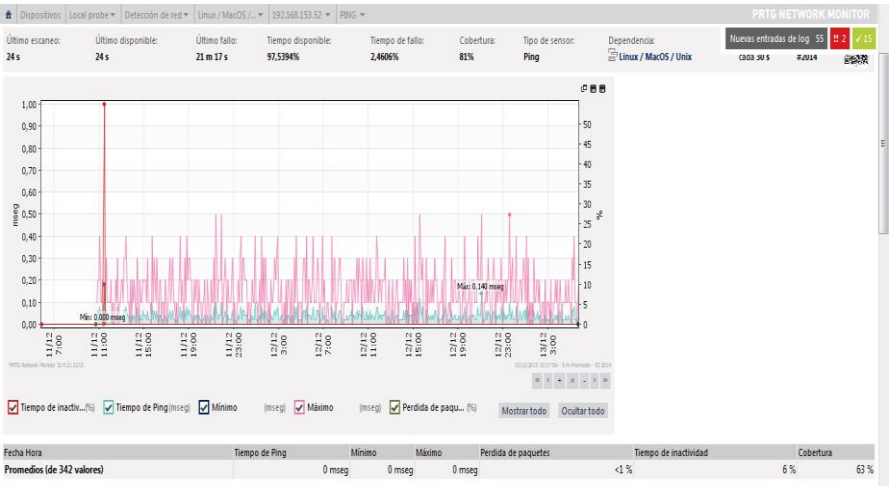
CAMARAS ACTIVAS



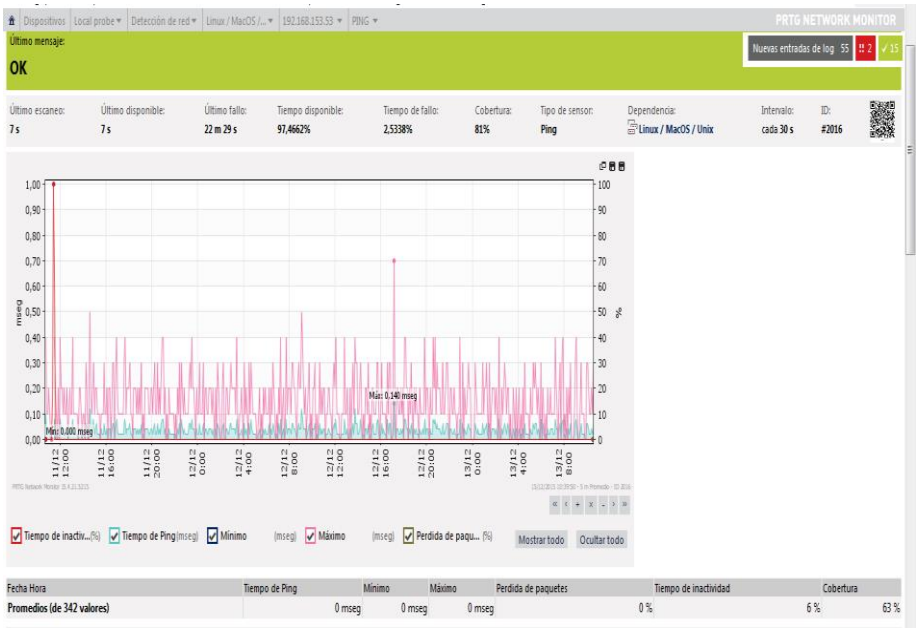
CAMARA BLOQUE A- PRIMER PISO-BIOMETRICOS 192.168.153.51



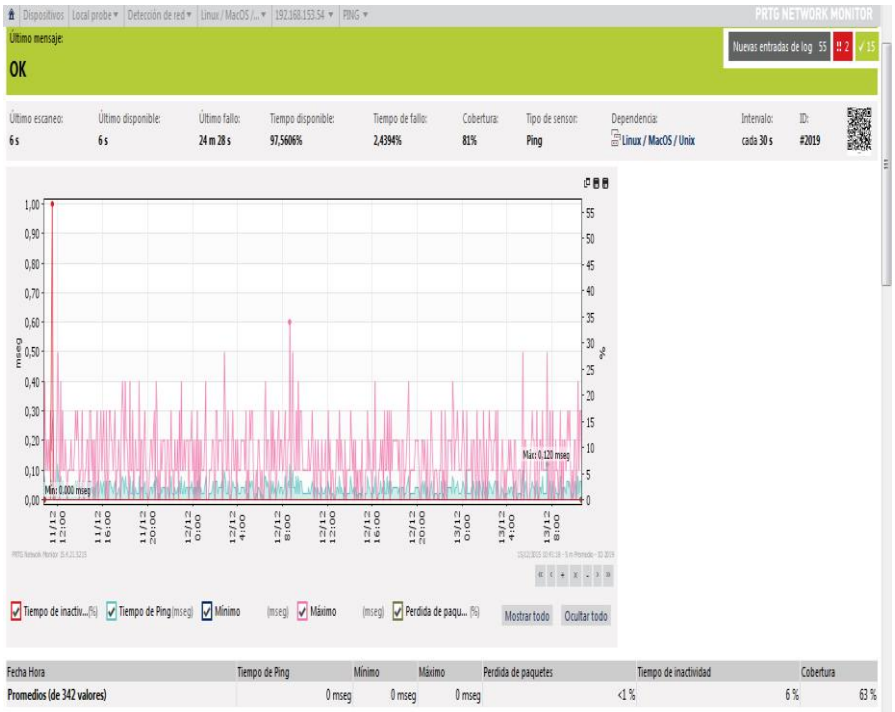
CAMARA BLOQUE A- PRIMER PISO-BIOMETRICOS 192.168.153.52



CAMARA BLOQUE A- PRIMER PISO-BIOMETRICOS 192.168.153.53



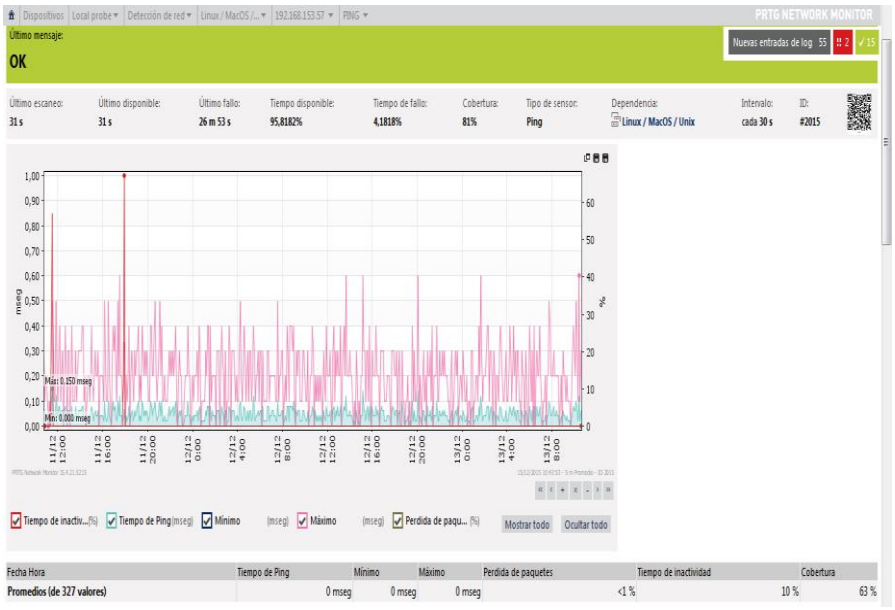
CAMARA BLOQUE A- PRIMER PISO-BIOMETRICOS 192.168.153.54



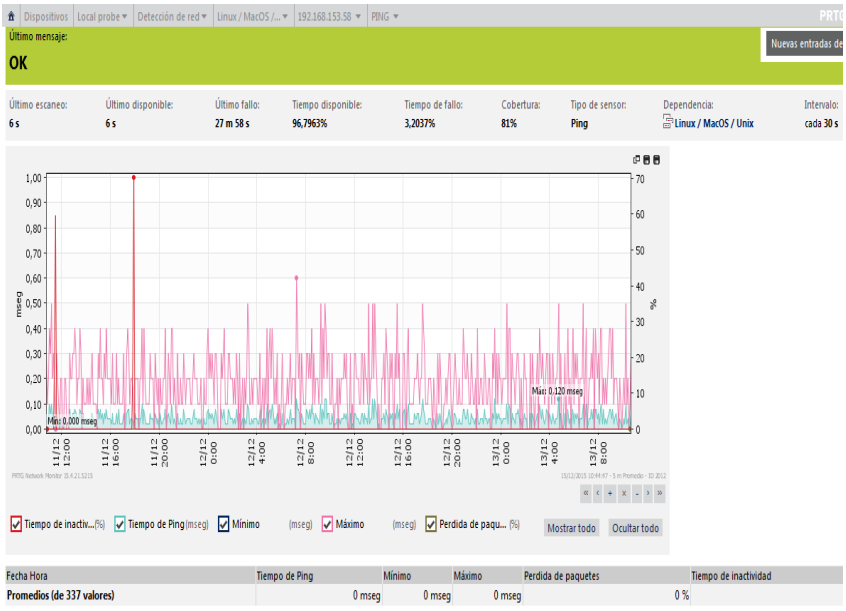
CAMARA BLOQUE A- PRIMER PISO-BIOMETRICOS 192.168.153.55

CAMARA BLOQUE A- PRIMER PISO-BIOMETRICOS 192.168.153.56

CAMARA BLOQUE A- PRIMER PISO-BIOMETRICOS 192.168.153.57



CAMARA BLOQUE A- PRIMER PISO-BIOMETRICOS 192.168.153.58



CAMARA BLOQUE A- PRIMER PISO-BIOMETRICOS 192.168.153.59

CAMARA BLOQUE A- PRIMER PISO-BIOMETRICOS 192.168.153.60