ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN SISTEMAS

"ANÁLISIS DE TÉCNICAS DE ENCOLAMIENTO DIRIGIDO A QoS EN TRANSMISIÓN DE VIDEO. CASO PRÁCTICO: DESARROLLO DE VIDEO-VIGILANCIA-IP EN LA ESPOCH-DESITEL"

TESIS DE GRADO

Previa Obtención del Título de:

INGENIERO EN SISTEMAS INFORMÁTICOS

Presentado Por:

MENTOR IVAN POVEDA CACERES

JORGE RODRIGO PONTON BALDEON

RIOBAMBA – ECUADOR

- 2008 -

A Dios, porque ser dignos de sus bendiciones, siempre estuvo con nosotros, permitiéndonos llegar a alcanzar esta meta importante en nuestras vidas

Al Ing. Diego Ávila, Ing. Alberto Arellano, Ing. Byron Vaca; quienes nos brindaron todo el apoyo necesario para que la presente tesis llegará a culminar con éxito

El presente trabajo realizado con mucha paciencia y esmero, dedicamos a DIOS y a nuestras familias; en especial a nuestros padres y hermanos por su comprensión y amor brindado durante toda nuestra vida.

Iván y Jorge

NOMBRE	FIRMA	FECHA
Dr. Romeo Rodríguez **DECANO FACULTAD DE** **INFORMÁTICA Y ELECTRÓNICA**	……	……
Ing. Iván Menes **DIRECTOR ESCUELA DE** **INGENIERÍA EN SISTEMAS**	……	……
Ing. Diego Ávila **DIRECTOR DE TESIS**	……	……
Ing. Alberto Arellano **MIEMBRO DEL TRIBUNAL**	……	……
Ing. Byron Vaca **MIEMBRO DEL TRIBUNAL**	……	……
Lcdo. Carlos Rodríguez **DIRECTOR CENTRO DE** **DOCUMENTACIÓN**	……	……

NOTA DE LA TESIS: ……

“Nosotros: Iván Poveda y Jorge Portón somos responsables de las ideas, doctrinas y resultados expuestos en esta tesis; y, el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO”.

……..

Iván Poveda

……..

Jorge Portón

ÍNDICE GENERAL

CAPÍTULO II

FORMATOS DE COMPRESION EN VIDEO-VIGILANCIA-IP

CAPÍTULO III

CONFIGURACION Y ANALISIS DE LAS TECNICAS DE ENCOLAMIENTO, FORMATOS DE COMPRESION

ÍNDICE DE ABREVIATURAS

QoS: Quality of Service – Calidad de Servicio

IntServ: Servicios Integrados

RSPV: Protocolo de Reserva de Recursos

ESPOCH: Escuela Superior Politécnica de Chimborazo

DiffServ: Servicios Diferenciados

CS: Class selector – Selector de Clases.

FIFO: First In – First Out – Primero en Entrar Primero en Salir

IP: Internet Protocol – Protocolo de Internet

JPEG: Joint Photographic Experts Group– Grupo de Expertos En Fotografía

Motion-JPEG: Grupo de Expertos En Fotografía para movimiento

ÍNDICE DE FIGURAS

CAPITULO I

CAPITULO II

CAPITULO III

ÍNDICE DE TABLAS

CAPITULO I

CAPITULO III

ÍNDICE DE ANEXOS

INTRODUCCIÓN

La gran difusión de las redes IP así como el desarrollo de nuevos servicios fundamentalmente multimedia que sobre estas redes convergen hacen necesario implementar mecanismos que permitan dar al tráfico un trato diferenciado. Estos mecanismos son inherentemente necesarios a la red cuando esta ofrece servicios de tiempo real.

La presente Tesis tiene como objetivo realizar un Análisis de técnicas de encolamiento dirigido a QoS en transmisión de video. Caso Práctico: Desarrollo de Video-Vigilancia-IP en la ESPOCH-DESITEL

Las técnicas de encolamiento permiten dar diferentes aproximaciones al problema de encolamiento de los paquetes en el router dirigidos a distribuir de manera equitativa entre los diferentes flujos la capacidad de un enlace compartido. El encolamiento de paquetes se enmarca dentro del conjunto de métodos y mecanismos de cola que proveen a ciertas aplicaciones o protocolos con determinadas prioridades sobre el resto del tráfico en la red.

El resultado de la investigación reside en aplicar una o varias formas de encolamiento y así brindar QoS para la transmisión de video, asi como determinar que mecanismo de compresión de video es el que mejor se adapta al desarrollo de video-vigilancia-IP en la ESPOCH-DESITEL.

La tesis esta dividida en cuatro capítulos, donde el objetivo principal de cada uno de ellos es:

1. Estudio de las técnicas de encolamiento.

   Donde se revisan primeramente los diversos modelos que implementan Calidad de Servicio con sus características; Así como toda la teoría referente a cada uno las técnicas de encolamiento, su fundamento, funcionalidad y características.

2. Estudio de los formatos de compresión de video.

   En el cual se estudia cada uno de los formatos de compresión, su funcionamiento y aplicabilidad y se establece las generalidades de de los sistemas de video vigilancia-IP.

3. Configuración y análisis de las técnicas de encolamiento, formatos de compresión de video-IP,

   Se realizan las configuraciones para implementar las diversas técnicas de encolado en el router para obtener resultados que permitan su análisis y comparación; Así también se caracterizan los formatos de compresión con motivo de un análisis comparativo, además de análisis sobre la infraestructura de video-vigilancia-IP y el impacto que pueda causar sobre la red de la ESPOCH

4. Desarrollo de un Prototipo de sistema de video-vigilancia-IP

   Donde se realizan todas las actividades involucradas en la ingeniería de Software para la construcción del prototipo.

CAPÍTULO I

CALIDAD DE SERVICIO (QoS) Y ENCOLAMIENTO EN REDES IP

1.1. Introducción

Los sistemas informáticos actualmente se basan en una red de datos, la cual debe ser capaz de soportar una cada vez más 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 evitar que la congestión de determinados nodos de la red afecte a algunas aplicaciones que requieran un especial caudal o retardo, como pueden ser aplicaciones de video-vigilancia-IP.

1.2. Parámetros que definen la QoS

La calidad de servicio consiste en la capacidad de la red para reservar algunos de los recursos disponibles para un tráfico concreto con la intención de proporcionar un determinado servicio.

Sería muy fácil dar calidad de servicio si las redes nunca se congestionaran, pero para ello habría que sobredimensionar todos los enlaces, cosa no siempre posible. Por tanto, para dar calidad de servicio en gran escala y en redes con posibilidades de congestión, es preciso tener mecanismos que permitan dar al tráfico un trato diferenciado acorde con el SLA (Service Level Agreement). De todas formas, aunque el estado de congestión pueda ser una decisión de compromiso entre sobredimensionamiento y saturación, una situación permanente de congestión es inabordable y su única solución es el sobredimensionamiento. Es decir, los mecanismos de calidad de servicio son inútiles en una red saturada permanentemente como podemos ver en la figura (figura I.1)

Figura I.1 Funcionalidades de Evolución del rendimiento de una red en función de la carga o tráfico ofrecido

Los parámetros que definen la calidad de un servicio son 4 parámetros: ancho de banda, retraso temporal, variación de retraso (o jitter) y probabilidad de error (o pérdida de paquetes o fiabilidad).

1.2.1. Ancho de banda

En las redes de ordenadores, el ancho de banda a menudo se utiliza como sinónimo para la tasa de transferencia de datos - la cantidad de datos que se puedan llevar de un punto a otro en un período dado (generalmente un segundo). Esta clase de ancho de banda se expresa generalmente en bits (de datos) por segundo (bps). En ocasiones, se expresa como bytes por segundo (Bps). Un módem que funciona a 57.600 bps tiene dos veces el ancho de banda de un módem que funcione a 28.800 bps.

En general, una conexión con ancho de banda alto es aquella que puede llevar la suficiente información como para sostener la sucesión de imágenes en una presentación de video.

Debe recordarse que una comunicación consiste generalmente en una sucesión de conexiones, cada una con su propio ancho de banda. Si una de estas conexiones es mucho más lenta que el resto actuará como cuello de botella enlentenciendo la comunicación.

La clave para que un servicio multimedia distribuido sobre una red sea efectivo es disponer del ancho de banda adecuado. Las conexiones de ancho de banda reducido basadas en módems no pueden soportar el tipo de video en tiempo real y el audio que hacen atractiva al usuario una aplicación multimedia. Las velocidades necesarias para ofrecer multimedia de una mínima calidad para una aplicación típica, van desde un

límite mínimo de 128 Kbit/s a varios Mbit/s en aplicaciones de cierta calidad. Con todo, las aplicaciones que soportan audio y video de alta calidad precisan velocidades de transmisión más altas.

1.2.2. Retraso temporal

Retraso Temporal (o Time-Delay) es un concepto ya conocido en el área de procesamiento adoptivo de señales. Si se retrasa la entrada de la señal por una unidad de tiempo y se deja que la red reciba ambas (la señal actual y la retrasada) al mismo tiempo, obtenemos una simple red de retraso temporal. El diseño de la red refleja la dependencia que se asume existe entre las entradas actuales y las previas.

Los datos transmitidos sobre una red como Internet sufren retraso temporal causado por el retraso de encolamiento, el retraso de procesamiento, el retraso de transmisión en los interruptores y el retraso de propagación en las conexiones. El retraso de encolamiento define el tiempo que un paquete espera en el búfer de un interruptor hasta que se transmite en la próxima conexión. Por lo tanto su valor varía con la carga de la red. El retraso de la propagación depende de la distancia física debido a la velocidad de la luz. El retraso de encolamiento representa la mayor parte del retraso total de la comunicación.

El retraso temporal, como un parámetro de QoS, representa el tiempo medio requerido por un paquete para viajar de un emisor a un receptor.

1.2.3. Variación de retraso (jitter)

Un componente crucial del retraso temporal son los retrasos arbitrarios de encolamiento en los dispositivos de la red. Debido a estos retrasos variantes dentro de la red, el tiempo desde la generación de un paquete hasta que se recibe, puede fluctuar de un paquete a otro. Este fenómeno se llama variabilidad instantánea o jitter. El jitter es la variación en la latencia en una ruta de conexión.

Se puede calcular el jitter enviando y recibiendo paquetes consecutivos. Como se muestra en la (figura II.16), dos paquetes se están enviando de un remitente a un contestador.

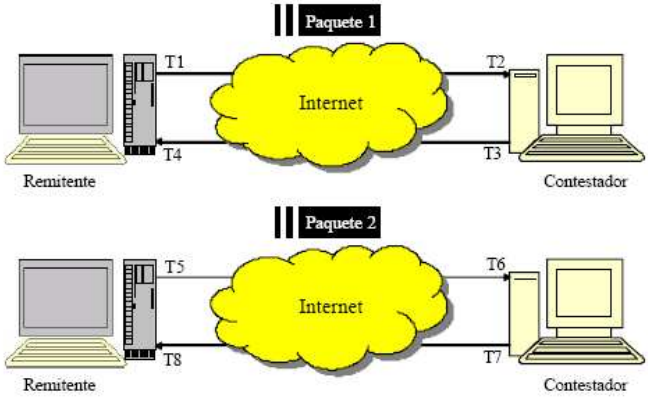


Figura I. 2 variaciones del retraso

1.2.4. Probabilidad de error (o pérdida de paquetes o fiabilidad)

Probablemente la preocupación más grande de los sistemas de interacción remota basados en Internet es el comportamiento no determinista del sistema que resultaría

durante la pérdida de paquetes o la caída total de la comunicación entre los sitios del sistema.

La pérdida de paquetes se origina por exceder la capacidad de la red causando que un dispositivo de la red deje caer un paquete. Este parámetro depende de la carga de la red y el mecanismo de encolamiento utilizado en el nodo de la red.

Una posibilidad para prevenir la pérdida de paquetes está implementada en TCP. En este protocolo, cuando se descubre una pérdida de paquetes, se pide un reenvío por el receptor. Esto produce una latencia más alta con el protocolo TCP comparándolo con el UDP, por eso existe una compensación entre porción de pérdida de paquetes y el retraso temporal. Generalmente, el parámetro del retraso temporal es más crucial que la pérdida de paquetes.

1.3. Mecanismos que implementan Calidad de Servicio

El protocolo TCP/IP no ofrece Calidad de Servicio en forma nativa dado que su funcionamiento es Best-Effort (Mejor Esfuerzo) de esta manera la red realizará el máximo esfuerzo para entregar los paquetes, pero sin garantías y sin ningún recurso asignado a algún tipo de paquetes.

Con la aparición de aplicaciones multimedia con requisitos de tiempo real (telefonía, videoconferencia, etc.) este modelo no es válido y se ha visto la necesidad de dotar a las redes de calidad de servicio.

Durante los últimos años han surgido variados métodos para establecer QoS en equipamientos de redes. Algoritmos avanzados de manejos de cola, modeladores de

tráfico (traffic shaping), y mecanismos de filtrado mediante listas de acceso (access-list), han hecho que el proceso de elegir una estrategia de QoS sea más delicado.

Cada red puede tomar ventaja de distintos aspectos en implementaciones de QoS para obtener una mayor eficiencia, ya sea para redes de pequeñas corporaciones, empresas o proveedores de servicios de Internet. Existen dos modelos en los que se divide el despliegue de calidad de servicio:

1.3.1. Servicios Integrados (IntServ)

IntServ (rfc 1633), provee a las aplicaciones de un nivel garantizado de servicio, negociando parámetros de red, de extremo a extremo.

Al mantener sesiones de extremo a extremo la aplicación solicita el nivel de servicio necesario para ella con el fin de operar apropiadamente, y se basa en la QoS para que se reserven los recursos de red necesarios antes de que la aplicación comience a operar. Estas reservaciones se mantienen en pie hasta que la aplicación termina o hasta que el ancho de banda requerido por ésta sobrepase el límite reservado para dicha aplicación.

En la arquitectura IntServ ocupa un papel fundamental el concepto de flujo. Entendemos por flujo un tráfico continuo de datagramas relacionados entre sí que se produce como consecuencia de una acción del usuario y que requiere una misma Calidad de Servicio. Un flujo es unidireccional y es la entidad más pequeña a la que puede aplicarse una determinada Calidad de Servicio. Los flujos pueden agruparse en clases; todos los flujos de una misma clase reciben la misma calidad de servicio.

En IPv4 los flujos se identifican por las direcciones de origen y destino, el puerto de origen y destino (a nivel de transporte) y el protocolo de transporte utilizado (TCP o UDP). En IPv6 la identificación puede hacerse de la misma forma que en IPv4, o alternativamente por las direcciones de origen y destino y el valor del campo Etiqueta de Flujo. Aunque el campo Etiqueta de Flujo en IPv6 se definió con este objetivo la funcionalidad aún no se ha implementado en la práctica.

En la arquitectura IntServ se definen tres tipos de servicio:

- *Servicio Garantizado*: garantiza un caudal mínimo y un retardo máximo. Cada router del trayecto debe ofrecer las garantías solicitadas, aunque a veces esto no es posible por las características del medio físico (por ejemplo en Ethernet compartida).

- *Servicio de Carga Controlada*: este servicio debe ofrecer una calidad comparable a la de una red de datagramas poco cargada, es decir en general un buen tiempo de respuesta, pero sin garantías estrictas. Eventualmente se pueden producir retardos grandes.

- *Servicio Best Effort*: este servicio no tiene ninguna garantía.

Figura I.3 Reparto de recursos en IntServ

1.3.1.1. Procedimiento de IntServ:

- Antes de enviar datos → petición servicio

En este modelo, una aplicación realiza una petición de una clase de servicio específica a la red, antes de comenzar a enviar información.

- Señalización explicita → Clase de servicio

La petición se realiza mediante una señalización explicita, de modo que la aplicación informa a la red del perfil o características de su tráfico, y pide una clase particular de servicio que pueda satisfacer sus requerimientos, tanto de ancho de banda como de retraso.

- La red confirma la petición.

La aplicación queda a la espera de enviar la información hasta recibir la confirmación de la petición por parte de la red.

- La red realiza control de admisión.

La red realiza un control de admisión, en función de la petición realizada por la aplicación y los recursos disponibles en la red.

- La red guarda información de estado.

La red mantiene información del estado de sí misma por flujos, mirando la clasificación, normas, y el algoritmo de cola en cada estado.

1.3.1.2. El Protocolo de reserva de recursos (RSPV)

El mecanismo más importante para llevar a cabo el modelo IntServ es el llamado RSVP (rfc 2205) Resource Reservation Protocol, que puede ser utilizado por las aplicaciones para enviar los requerimientos de QoS al router.

El protocolo de reserva de recursos crea y mantiene un estado específico para cada flujo de información tanto en los nodos finales como en los nodos intermedios por los que pasan las conexiones.

La clave de RSVP es reservar recursos en cada nodo por donde transitarán los paquetes o flujos de datos.

Cuando la aplicación realiza la petición de una clase de servicio específica a la red, el RSVP es el que transporta la información sobre *caracterización del tráfico y requerimientos de los recursos*, por lo que cada nodo a lo largo del camino puede determinar si se puede aceptar o no una nueva solicitud de reserva. De esta manera el protocolo de establecimiento de la reserva debe seguir los cambios en la topología de la red en el tiempo.

RSVP está basado en una aproximación iniciada por el receptor y está diseñado para trabajar con IP Multicast. RSVP permite diferentes tipos de estilos de reserva y usa la aproximación del *soft state* para seguir los cambios de las rutas.

RSVP produjo una euforia inicial (1996-1997) que luego dió paso a la decepción. La razón principal fueron problemas de *escalabilidad* debidos a la necesidad de mantener *información de estado en cada router de cada flujo.* Esto hace inviable usar RSVP en grandes redes, por ejemplo en el 'core' de Internet.

1.3.2. Servicios Diferenciados (DiffServ)

Una aproximación para otorgar calidad de servicio es diferenciar entre el conjunto de paquetes que circulan por la red.

El modelo DiffServ (basados en la clasificación y marcado) tiene como objetivo tratar a los paquetes de manera diferente, tomando la decisión de cómo procesarlo dependiendo del contenido del encabezado del paquete. Y si existen similitudes entre diferentes paquetes, es posible clasificar los paquetes en grupos y tomar decisiones de cómo procesar los paquetes dependiendo del grupo al que pertenezca un paquete.

Este mecanismo se logra reservando ciertos bits en el encabezado del paquete (de hecho el campo de tipo de servicio del protocolo Ipv4 estaba reservado para este propósito) y definir en él, el tipo de servicio que se le debe aplicar al paquete de acuerdo a las políticas que se hayan especificado para ese propósito.

1.3.2.1. Dominio de los Servicios Diferenciados.

Un dominio DS (DiffServ) es un conjunto de nodos DS que operan con una política de provisionamiento de servicios común y con un conjunto de tratamiento de paquetes implementados en cada nodo. En este Dominio se pueden distinguir dos tipos de nodos o dispositivos tal como observamos en la figura I.4. Los dispositivos Frontera que hacen la clasificación y el marcado del tráfico y los dispositivos Internos que se encargan de evitar la congestión.

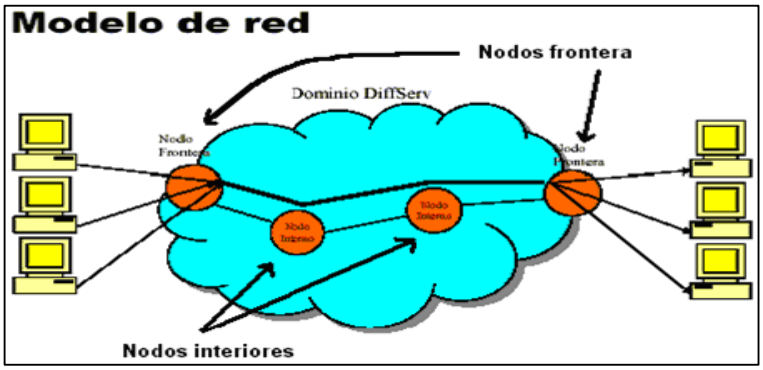


Figura I.4 Servicios diferenciados, basado en nodos frontera y nodos internos.

El esquema de servicios diferenciados especifica las funciones que se tienen que realizar en los nodos de ingreso a la red y en los nodos internos de la red. Los nodos

de acceso a la red se encargan de la clasificación y de especificar el contenido del campo DS (Differentiate Service). Los nodos interiores se encargan del reenvío de los paquetes dependiendo del contenido del campo DS.

La clasificación que se haga del paquete, queda especificada en el contenido del campo ToS del encabezado del paquete IP.

1.3.2.2. El campo Differentiated Services Code Point (DSCP)

Para realizar el marcado de los paquetes se pueden utilizar varias técnicas, pero la más extendida y estandarizada es utilizar los DSCP (Differentiated Service Code Point).

Originalmente, para el protocolo IPv4 se diseñó el campo ToS (Type of Service) de ocho bits para capacitar el marcado de paquetes con un nivel de servicio requerido. Esta definición no se utilizó mayormente debido a la ambigüedad de su significado, por lo que más tarde se convirtió en el denominado campo DSCP (Differentiated Services Code Point). Este campo sí tuvo una aceptación global y se asumió una interpretación estándar que permitió a las redes planificar metodologías basándose en ésta. Tal fue el éxito de esta nueva definición, que fue incluida para ofrecer las mismas ventajas en el protocolo IPv6 en el denominado campo TC (Traffic Class).

<table>
<tr><td>Version</td><td>Lon.Cab.</td><td>TOS</td><td colspan="4">Longitud total</td></tr>
<tr><td colspan="3">Identificación</td><td>X</td><td>DF</td><td>MF</td><td>Desplazamiento fragmento</td></tr>
<tr><td>Tiempo de vida</td><td colspan="2">Protocolo</td><td colspan="4">Checksum</td></tr>
<tr><td colspan="7">Dirección de origen</td></tr>
<tr><td colspan="7">Dirección de destino</td></tr>
<tr><td colspan="7">Opciones</td></tr>
</table>

(a)

Version	Lon.Cab.	DS	Longitud total			
Identificación			X	DF	MF	Desplazamiento fragmento
Tiempo de vida	Protocolo	Checksum				
Dirección de origen						
Dirección de destino						
Opciones						

(b)

Figura I.5 (a) Cabecera IPV4 antes de DiffServ. (b) Cabecera IPV4 con DiffServ

Los primeros 6 bits son utilizados como parte del código mientras que los últimos dos bits deben ser ignorados (para aplicaciones futuras) por los nodos que tengan implementado DiffServ. La estructura del campo DS se muestra en la tabla I.1.

0	1	2	3	4	5	6	7
DSCP						SU	

Tabla I.1.- Campo ToS del protocolo IPV4

Donde DSCP = DiffServ Code Point

SU = Sin uso

De esta manera DiffServ utiliza la combinación de los bits del campo DSCP para marcar el tipo de servicio que luego será usado para conducir el paquete hacia una cola especifica o tratamiento en el dispositivo por el cual circule el paquete. Cada una de las 64 (2^6) posibles combinaciones puede significar una forma diferente de tratar los

paquetes por parte de los nodos medulares. A cada una de estas posibles formas de tratar al paquete se le llama "**Per Hop Behavior**" **(PHB**) tratamiento por salto.

En DiffServ, se definen *clases de servicio*, cada flujo particular de datos es agrupado en un tipo de clase, donde son tratados idénticamente.

Una vez que existe la capacidad de marcar los paquetes utilizando DSCP, es necesario proveer del tratamiento apropiado para cada una de estas clases. El conjunto de paquetes con el mismo valor DSCP circulando hacia una dirección determinada, es llamado **Behavior Aggregate** (**BA**) agregado de trafico. Es así cómo múltiples aplicaciones/ fuentes pueden pertenecer al mismo BA. El PHB se refiere a la programación, encolamiento, limitación y modelamiento del comportamiento de un nodo, basado en el BA perteneciente del paquete.

Los enrutadores internos sólo están interesados del comportamiento por salto (PHB), marcado en la cabecera del paquete. Esta arquitectura permite a DiffServ rendir mucho mejor en ambientes de bajo ancho de banda, y provee de un mayor potencial que una arquitectura IntServ.

1.3.2.3. Funciones de los nodos en DiffServ

Podemos distinguir dos tipos de nodos: Los Frontera que se encargan básicamente de la clasificación y marcado del tráfico y los Internos encargados de evitar la congestión.

1.3.2.3.1. Nodos Frontera

Los nodos Frontera (figura I.6) de la red realizan una serie de acciones a los paquetes que son recibidos por parte de los usuarios:

- Clasificación
- Control de la tasa (rate control)
- Medición (metering)
- Marcado (marking)

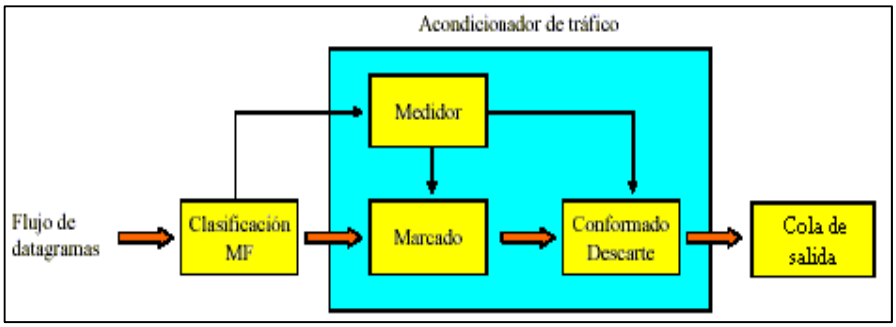


Figura I.6 Arquitectura de un nodo Frontera

Básicamente podemos referirnos a dos tareas principales:

- **Clasificación.**

Existen dos tipos básicos de clasificadores: Behavior Agrégate (BA) y los MultiField (MF) múltiple campo . Un clasificador BA selecciona los paquetes únicamente en base al código DSCP de la cabecera IP. Los clasificadores BA se utilizan generalmente cuando el campo DSCP ya esta activado (o marcado), antes de llegar a los clasificadores.

Los clasificadores MF utilizan una combinación de uno o más campos de la quíntupla (dirección origen, dirección destino, puerto origen, puerto destino, e identificador de protocolo) de la cabecera IP del paquete para realizar la clasificación. Puede utilizarse el soporte de políticas de reserva de los clientes. Por ejemplo:

- Marcar los paquetes en base al tipo de aplicación (numero de puertos) como TELNET o FTP.
- Marcar los paquetes en base a unas direcciones origen/destino en particular, o en los prefijos de red, como trafico de CEO o algún servidor de misión critica.
- Marcar los paquetes en base a t-tupla que determina un flujo de aplicación, como un stream de video.

La otra fase clave en el nodo frontera es el marcado de tráfico.

- **Marcado (marking)**

Los marcadores son los encargados de poner en el campo DSCP un determinado valor, añadiendo así un paquete a una determinada clase de envío (BA). Los marcadores pueden actuar sobre paquetes que no se han marcado todavía o remarcar paquetes ya marcados previamente. El marcado puede ocurrir en diferentes situaciones y lugares. Si la red del cliente soporta el marcado de servicios diferenciados los paquetes pueden marcarse por las aplicaciones o por el encaminador de primer nivel de la LAN. Los nodos limítrofes del proveedor de servicio también pueden marcar los paquetes en representación de los clientes. Todos estos marcados se suelen asociar con un clasificador MF.

El marcado es también una de las acciones que se puede tomar contra los paquetes no conformes a un perfil de tráfico. Cuando un flujo de tráfico pasa por un medidor, algunos paquetes pueden marcarse con un valor de DSCP especial para indicar que no son conformes. Si la red experimenta algún tipo de congestión, estos paquetes serian los primeros en drenarse.

1.3.2.4. Comportamiento por salto “Per Hop Behavior” (PHB)

El PHB (rfc 2475) se refiere a la programación, encolamiento, limitación y modelamiento del comportamiento de un nodo, basado en el BA al que pertenece el del paquete.

Después que se ha seteado el campo DSCP de un trafico, le corresponderá luego un tratamiento especifico en cada nodo de la red. Este tratamiento específico que se le brinda a cada clase de tráfico se llama en DiffServ PHB (Per Hop Behavior).

Los PHBs normalmente se implementan por medio de un manejador de buffer y una disciplina de servicio. Aunque muchos PHBs están estrechamente asociados a ciertas disciplinas (como el Weith Fair Queve), se pretende que la definición del PHB sea una descripción genérica de los tratamientos de envió mas que una implementación concreta.

1.3.2.5. Tipos de Servicio en DiffServ

Actualmente DiffServ implementa 4 tipos de servicio:

- comportamiento por omisión (Default Behavior)
- Selector de clase

- Tránsito expedito (Expedited forwarding)
- Tránsito asegurado (Assured forwarding)

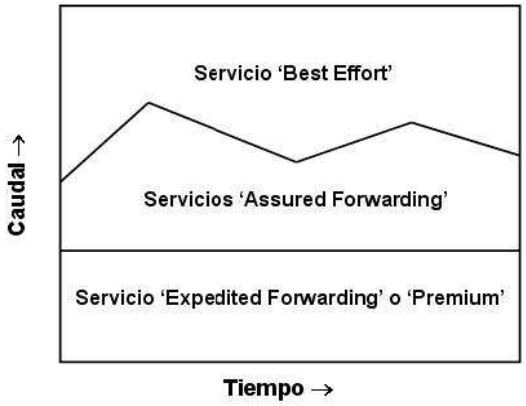


Figura I.7 Reparto de recursos en DiffServ

1.3.2.5.1. Comportamiento por omisión (o mejor esfuerzo).

Este comportamiento (rfc 2474) equivale a un servicio de mejor esfuerzo (por ej. la congestión y pérdida son completamente descontroladas). Es el comportamiento que todas las redes que implementen DiffServ deben de incorporar.

Todos los paquetes que no tengan especificado un comportamiento, utilizan el servicio de mejor esfuerzo para moverse a través de la red. El código que representa el comportamiento por omisión en el DSCP es el '000000'. Este servicio se caracteriza por tener a cero los tres primeros bits del DSCP. En este caso los dos bits restantes pueden utilizarse para marcar una prioridad, dentro del grupo 'best effort'. En este servicio no se ofrece ningún tipo de garantías.

1.3.2.5.2. Seleccionador de clase (CS PHB).

Este Tratamiento (rfc 2474) define hasta ocho clases distintas (Tabla I.2). El formato del código especifica los primeros 3 bits del DSCP. Los tres primero bits representan un número del 0 al 7. El número de menor valor representa una prioridad menor (los tres primeros bits son cero, por omisión o de mejor esfuerzo) mientras que un número mayor representa una prioridad mayor. No es necesario que un nodo (puede ser un nodo interno) soporte las ocho clases. Puede agrupar las clases para soportar por ejemplo 2 prioridades. Los códigos con número 1 al 3 pueden representar una prioridad baja, mientras que los códigos con los números del 4 al 7 representan una prioridad alta. De esta forma, el nodo sigue siendo compatible con la especificación DiffServ, aún sin tener ocho clases definidas.

Clase	Código
0	000000
1	001000
2	010000
3	011000
4	100000
5	101000
6	110000
7	111000

Tabla I.2 Códigos para el selector de clase

1.3.2.5.3. Tránsito expedito (Expedited forwarding)

La finalidad de este PHB (rfc 2598) es la de proveer enlaces de alta calidad, con respecto a retardo y pérdidas. EF PHB, elemento clave de DiffServ, proporciona este servicio a través de una pérdida baja, una baja latencia y un bajo jitter, así como un servicio asegurado de ancho de banda. EF puede ser utilizado para proveer enlaces que simulen enlaces dedicados. El valor del subcampo DSCP relacionado con este servicio es '101110'.

EF puede implementarse usando PQ. Cuando se implementa en una red DiffServ, EF PHB proporciona una linea virtual, o un servicio premium. Sin embargo, para una eficiencia óptima, EF debe ser reservado para únicamente las aplicaciones más críticas, puesto que en situaciones de congestión de tráfico, no es factible tratar todo o gran parte del tráfico con alta prioridad.

1.3.2.5.4. Tránsito asegurado (Assured forwarding).

Este servicio (rfc 2597) asegura un trato preferente, pero no garantiza caudales, retardos, etc. Se definen cuatro clases posibles (AF1, AF2, AF3, AF4) pudiéndose asignar a cada clase una cantidad de recursos en los routers (ancho de banda, espacio en buffers, etc.). La clase se indica en los tres primeros bits del DSCP. Para cada clase se definen tres categorías de descarte de paquetes (probabilidad alta, media y baja) que se especifican en los dos bits siguientes (cuarto y quinto). Es importante señalar que no es necesario implementar los tres niveles de descarte. Si el operador de la red, no espera que existan muchas condiciones de congestión, el número de niveles de descarte se puede compactar a dos.

Existen por tanto 12 valores de DSCP diferentes asociados con este tipo de servicio, que son:

	Precedencia de descarte		
Clase	Baja	Media	Alta
4	10001	10010	10011
3	01101	01110	01111
2	01001	01010	01011
1	00101	00110	00111

Tabla I.3 Códigos DSCP recomendados para AF.

1.4. 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 “manejo de congestión” es un término general usado para nombrar los distintos tipos de estrategia de encolamiento (en un dispositivo) que se utilizan para manejar situaciones donde la demanda de ancho de banda solicitada por las aplicaciones excede el ancho de banda total de la red, controlando la inyección de tráfico a la red, para que ciertos flujos tengan prioridad sobre otros.

El encolamiento permite establecer una prioridad al forwarding 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 ése puerto.

Las colas de espera juegan un papel fundamental, ya que entre mayor tiempo pasen los paquetes en la cola de espera, mayor será el tiempo total de comunicación.

La congestión en un interfaz de salida se produce cuando éste no puede enviar paquetes al medio físico tan rápidamente como le llegan procedentes de interfaces de entrada en un router.

CISCO define que un interfaz está congestionado cuando se alcanza un 75% de tiempo de uso. Por defecto, y si no se aplica QoS, cada interfaz tiene una única cola de salida y se gestiona con una estrategia FIFO.

Una vez que los paquetes son enviados a las interfaces de salida que les corresponden, los mismos pasan al proceso de scheduling o encolamiento.

Para el control de la congestión, el dispositivo establece en el interfaz varias colas donde se colocarán los paquetes dependiendo de sus prioridades. El router planificará, según distintos algoritmos, como emplear estas colas para evitar la congestión.

Un conmutador LAN que opere con múltiples colas de tráfico posibilita la priorización de los paquetes. El tráfico de alta prioridad puede pasar a través del conmutador sin ser retardado por el tráfico de baja prioridad, asegurando así la calidad de las comunicaciones sensibles al tiempo, como la voz y el vídeo, con independencia del nivel de sobrecarga de la red. Para ello, el conmutador debe tener al menos dos colas por puerto. Aunque un número mayor de colas podría optimizar aún más el rendimiento, es improbable que en un entorno LAN se precisen más de cuatro. A medida que cada paquete llega al conmutador, se introduce en la cola apropiada dependiendo de su nivel de prioridad. El conmutador envía entonces los paquetes de cada cola según este criterio.

Existen diferentes mecanismos de encolamiento basados en algoritmos que van desde los mas simples hasta los sumamente complejos.

Cada mecanismo de encolamiento tiene sus ventajas y desventajas, así como escenarios dónde es más recomendable aplicar ese mecanismo en particular; la elección del mecanismo de encolamiento a utilizar depende de lo que se quiera lograr.

1.4.1. Encolado First In – First Out (FIFO)

Es el tipo más simple de encolamiento, se basa en el siguiente concepto: el primer paquete en entrar a la interfaz, es el primero en salir

En su forma más sencilla, el mecanismo de cola FIFO (Figura I.8) , se encarga de almacenar paquetes cuando hay congestión en la red, y a enviarlos cuando tiene la posibilidad, manteniendo el orden de llegada, es decir, que no ofrece ninguna prioridad de unos paquetes sobre otros.

Es adecuado para interfaces de alta velocidad, sin embargo, no para bajas, ya que FIFO es capaz de manejar cantidades limitadas de ráfagas de datos. Si llegan más paquetes cuando la cola está llena, éstos son descartados. No tiene mecanismos de diferenciación de paquetes.

La mayoría de routers implementan colas de tipo (FIFO) con descarte “trasero” (tail drop). Esto significa que primer paquete en alcanzar el router es el primero colocado en la cola para ser entregado a la red sin realizar ninguna consideración sobre el desempeño de la misma ni de las métricas actuales del flujo al que pertenece dicho paquete. Dado que en ocasiones el router recibe paquetes más rápido de lo que los puede retransmitir, los debe almacenar en la cola. Descarte trasero significa que cuando se presenta congestión en la red, la cola se llena y los paquetes que continúan llegando son descartados. Por defecto, un router se basa en FIFO, Cisco lo utiliza por defecto en enlaces superiores a T1 (1.5 Mbps)

Este algoritmo, al igual que ocurre con el resto de mecanismo de cola, tiene como limitación la capacidad de su buffer en momentos de congestión. Es el método más rápido.

Hoy en día se necesitan algoritmos más sofisticados, que permiten diferenciar entre distintos tipos de paquete, por lo que este método está cayendo en desuso.

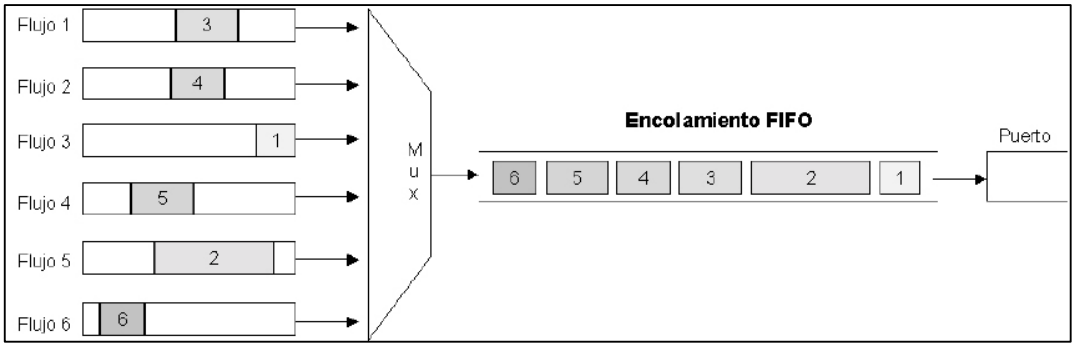


Figura I.8 Esquema del funcionamiento de FIFO

1.4.2. Encolado Priority Queuing (PQ)

El Encolamiento de Prioridad (PQ), asegura que el tráfico importante reciba un servicio rápido en cada punto de la red, donde este mecanismo esté presente.

PQ que se caracteriza por definir 4 tipos de colas con prioridad (Figura I.9) ***high, medium, normal*** y ***low***, de forma que mientras queden paquetes en la cola high no se atienden los paquetes de medium y así sucesivamente.

En ocasiones esta configuración puede crear inanición, debido a que el tráfico clasificado como *PQ high* puede llegar a consumir todo el ancho de banda disponible. Además, cabe resaltar que su disciplina es estática y no se adapta a los cambios en la red. Los tamaños respectivamente de las diferentes colas por defecto son 20, 40, 60 y 80 paquetes respectivamente y la cola por defecto para tráfico no clasificado (o marcado) es nivel *normal*.

El modo de configuración en los routers de Cisco es *priority-list*, haciendo clasificación en base al protocolo (y puertos, ej *priority-list 4 protocol ip medium TCP 23*) o a la interfaz de entrada (ej, *priority-list 4 interface fa0/0 high*). utilizada por los protocolos de tiempo real.

En la gestión de colas siempre que haya información en una cola de más prioridad se enviará antes que la de colas de menos prioridad. Si una cola de menor prioridad está siendo atendida, y un paquete ingresa a una cola de mayor prioridad, ésta es atendida inmediatamente. Este mecanismo se ajusta a condiciones donde existe un tráfico importante, pero puede causar la total falta de atención de colas de menor prioridad (starvation).

La prioridad de los paquetes puede diferenciarse por diversos medios, como: el protocolo de red, el interfaz del router por el que llegue el paquete, el tamaño del paquete y la dirección de origen o destino.

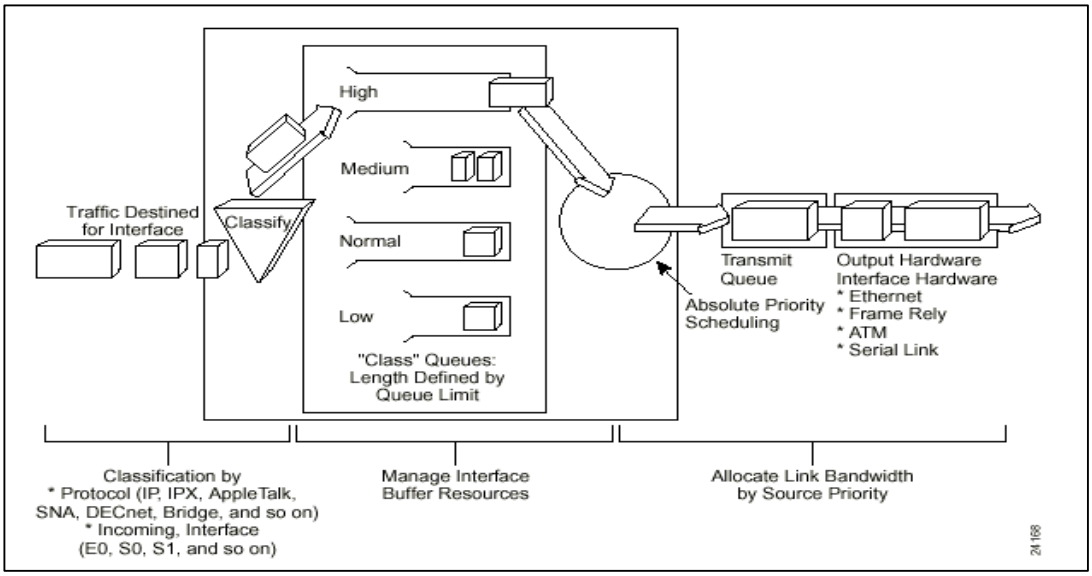


Figura I.9 Esquema del funcionamiento de PQ

Inconveniente: Este método es estático y no se adapta a los requerimientos de la red. Además, puede crear inanición, es decir dejar fuera de servicio a tráfico menos prioritario. Sin embargo al trafico prioritario ofrece garantías totales.

1.4.3. Encolado Custom Queuing (CQ)

Para evadir la rigidez de PQ, se opta por utilizar Encolamiento Personalizado (CQ). La gestión de colas CQ permite especificar qué porcentaje de ancho de banda se dedica a cada tipo de tráfico.

CQ fue diseñado para permitir que varias aplicaciones compartieran la red, y que además tuvieran asignado un ancho de banda mínimo garantizado, y unas garantías aceptables en cuanto a los retrasos

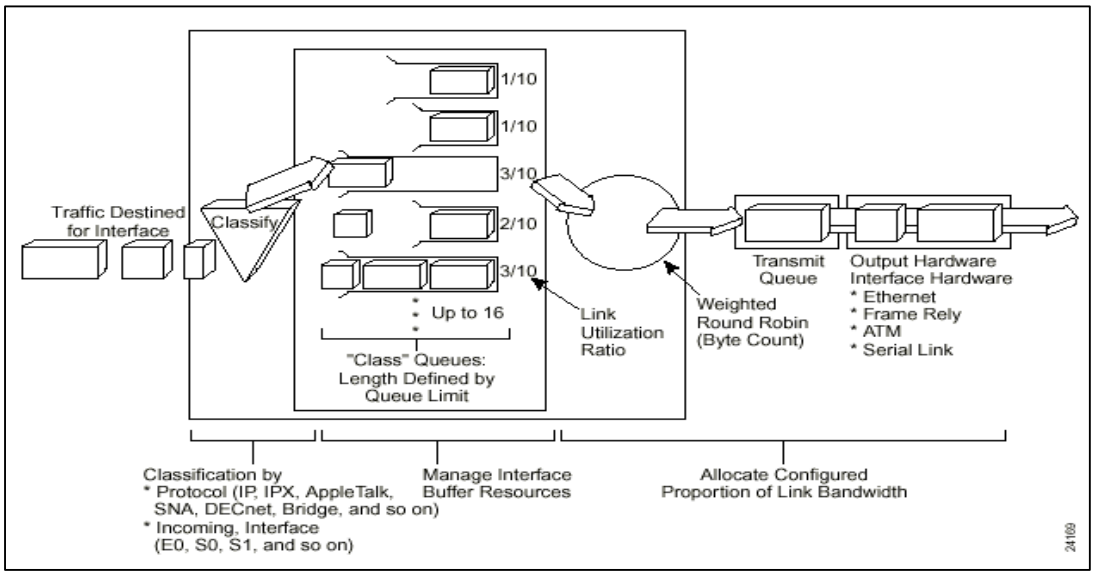
Permite al administrador priorizar el tráfico sin los efectos laterales de inanición de las colas de baja prioridad, especificando el número de paquetes o bytes que deben ser atendidos para cada cola. Se pueden crear hasta 16 colas para categorizar el tráfico, donde cada cola es atendida al estilo Round-Robin. CQ ofrece un mecanismo más refinado de encolamiento, pero no asegura una prioridad absoluta como PQ. Se utiliza CQ para proveer a tráficos particulares de un ancho de banda garantizado en un punto de posible congestión, asegurando para este tráfico una porción fija del ancho de banda y permitiendo al resto del tráfico utilizar los recursos disponibles.

Con CQ la cola 0 está asociada sólo a funciones del sistema (routing, keepalives) y se atiende siempre primero, todas las colas se atienden según Round Robin, con quantos definidos en bytes y que por defecto queda definido en 1500 bytes. La cola

por defecto para tráfico no marcado es la 1. El modo de configuración en los routers de Cisco es *queue-list*, haciendo clasificación en base al protocolo (y puertos, ej *queue-list 4 protocol ip 1 TCP 23*) o a la interfaz de entrada (ej, *queue-list 4 interface fa0/0 2*). El tamaño de cada una de estas colas es de 20 paquetes, pero se puede modificar.

En este método el acho de banda debe de ser compartido proporcionalmente entre las aplicaciones, sin dejar tráfico fuera de servicio. CQ no da garantías estrictas.

La desventaja de este método consiste en que no se ajusta el tamaño de los buffers en forma dinámica por lo que no se adapta a las condiciones variables del tráfico más allá de que cada cola aprovecha ancho de banda adicional en el caso de que otras colas no posean tráfico o el tráfico esta por debajo del mínimo garantizado.



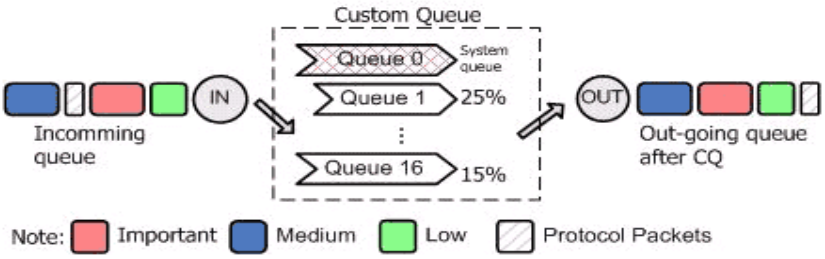


Figura I.10 Esquema del funcionamiento de CQ

1.4.4. Encolado Weighted Fair Queuing (WFQ)

El encolado por peso justo o encolado inteligente (WFQ) es óptimo en situaciones en las que se desea proveer un tiempo de respuesta razonable a todos los usuarios de la red sin agregar demasiado ancho de banda. Detecta qué tipos de flujos de datos existen y los clasifica en más interactivos y menos interactivos, de forma que el flujo interactivo será enviado antes que el no interactivo. Consiste en gestionar los diferentes flujos o sesiones en colas independientes, buscando un reparto equitativo o justo (fair), priorizando aquellas de menor volumen, las cuales asocia como más sensibles al retardo como VOIP y Telnet, y penalizando aquellas sesiones más grandes, dado que no las asocia con aplicaciones de tiempo real, como FTP

WFQ es una de las principales técnicas de encolamiento de cisco (Figura I.11). Es un algoritmo de encolamiento basado en el flujo que realiza dos tareas simultáneamente. Programa el tráfico interactivo al frente de la cola para reducir el tiempo de respuesta, y comparte equitativamente el ancho de banda remanente entre flujos de gran ancho de banda. WFQ asegura que las colas no mueran de inanición por falta de ancho de banda, y que el tráfico tenga un servicio predecible. Los flujos trafico de bajo volumen (que comprende la parte mas importante del trafico) reciben un servicio preferencial, transmitiendo toda su carga en el momento oportuno.

Los flujos de tráfico de alto volumen comparten entre ellos la capacidad remanente proporcionalmente. WFQ está diseñado para minimizar los esfuerzos de configuración y adaptarse automáticamente a las condiciones de cambio del tráfico en las redes. De hecho, WFQ realiza un buen trabajo en la mayoría de las aplicaciones que han sido implementadas con el modo de encolamiento por defecto en interfaces seriales configuradas para correr a la velocidad de una línea E1 (2.5Mbps) o menor.

WFQ asigna una ponderación a cada flujo de forma que determina el orden de transito en la cola de paquetes, divide el ancho de banda a través de las colas de trafico basadas en pesos. (WFQ se asegura de que todo el tráfico sea atendido, dado su peso). Es eficiente en el sentido que usaría todo el ancho de banda disponible para transmitir el tráfico de los flujos de baja prioridad en caso de que en ese momento no exista tráfico en los flujos de alta prioridad. WFQ reserva para cada sesión, espacio hasta 64 paquetes y si se excede se descartan y sólo se vuelven a aceptar en el caso que la ocupación descienda al 25%. WFQ se considera una disciplina adaptativa al estado de la red y las características del tráfico. WFQ no es escalable al requerir recursos adicionales en la clasificación y manipulación dinámica de las colas por tanto no funciona bien en routers backbone.

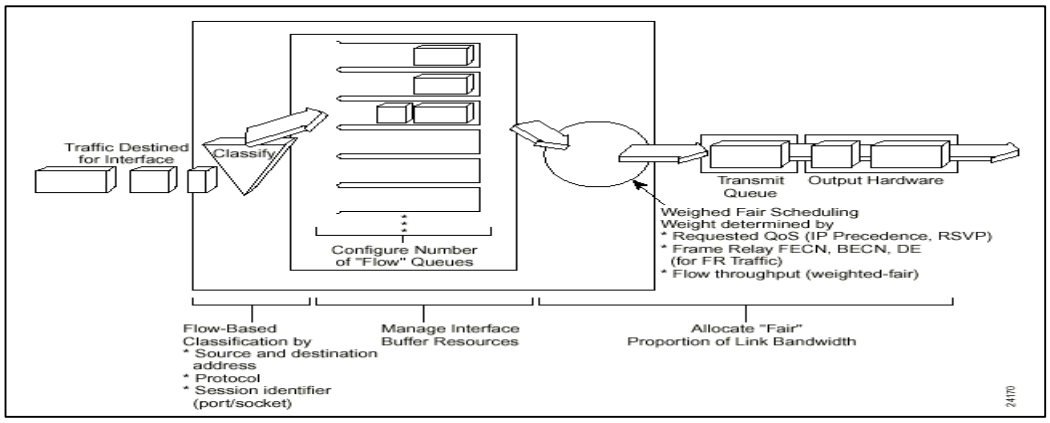


Figura I.11 Esquema del funcionamiento de WFQ

1.4.5. Encolado Class Based Weighted Fair Queuing (CBWFQ)

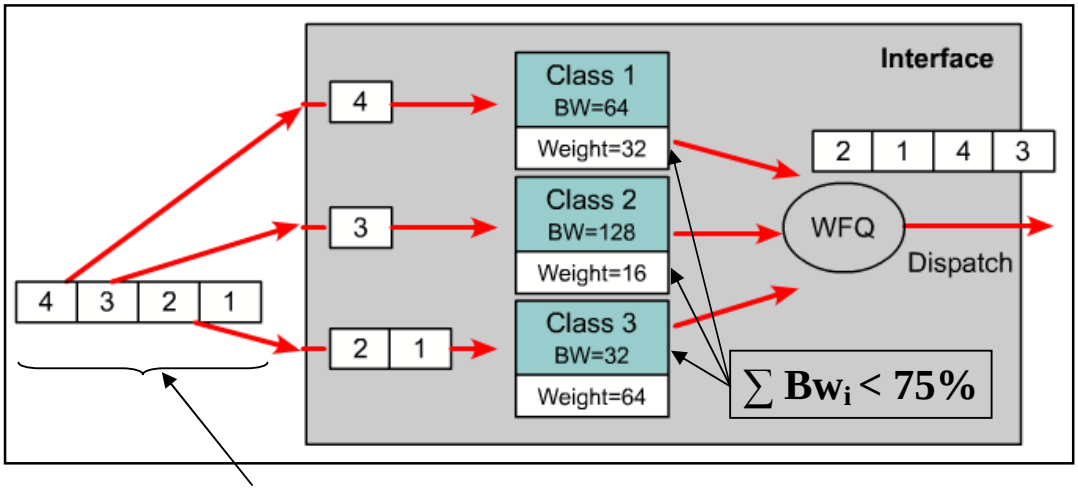
El encolado justo basado en clases (CBWFQ) es una extensión de WFQ para brindar soporte de clases de tráfico definidas por el usuario. Para CBWFQ, se definen clases de tráfico basadas en criterios de coincidencias que incluyen protocolos, listas de control de acceso (ACLs), e interfaces de entrada.

WFQ tiene algunas limitaciones de escalamiento, ya que la implementación del algoritmo se ve afectada a medida que el tráfico por enlace aumenta; colapsa debido a la cantidad numerosa de flujos que analizar. CBWFQ fue desarrollada para evitar estas limitaciones, tomando el algoritmo de WFQ y expandiéndolo, permitiendo la creación de clases definidas por el usuario, que permiten un mayor control sobre las colas de tráfico y asignación del ancho de banda. Algunas veces es necesario garantizar una determinada tasa de transmisión para cierto tipo de tráfico, lo cual no es posible mediante WFQ, pero sí con CBWFQ. Las clases que son posibles implementar con CBWFQ pueden ser determinadas según protocolo ACL, valor DSCP, o interfaz

de ingreso. Cada clase posee una cola separada, y todos los paquetes que cumplen el criterio definido para una clase en particular son asignados a dicha cola. Una vez que se establecen los criterios para las clases, es posible determinar cómo los paquetes pertenecientes a dicha clase serán manejados. Si una clase no utiliza su porción de ancho de banda, otras pueden hacerlo. Se pueden configurar específicamente el ancho de banda y límite de paquetes máximos (o profundidad de cola) para cada clase. El peso asignado a la cola de la clase es determinado mediante el ancho de banda asignado a dicha clase.

La diferencia fundamental con respecto a WFQ, es que con CBWFQ la implementación es más ajustada, ya que se puede especificar directamente la cantidad de ancho de banda que quiere asignar a cada clase. Otra ventaja es que con esta técnica hay mayor granularidad y escalamiento para clases de servicio, alcanzándose a configurar hasta 64 clases de servicios diferentes.

Las dos técnicas últimas analizadas (WFQ — CBWFQ) corresponden a algoritmos que ofrecen una distribución de ancho de banda en forma equitativa, basadas en colas personalizadas. Ambas por si solas no alcanzan a ofrecer QoS para requerimientos en tiempo real, por la razón indicada deben implementarse en conjunto con otras herramientas que facilitan la priorización. WFQ requiere Prioridad IP RTP, en tanto que CB-VVFQ usa técnicas adicionales como LLQ.



- Los paquetes llegan clasificados, ya no tenemos en cuenta los flujos independientes, solo la clase.

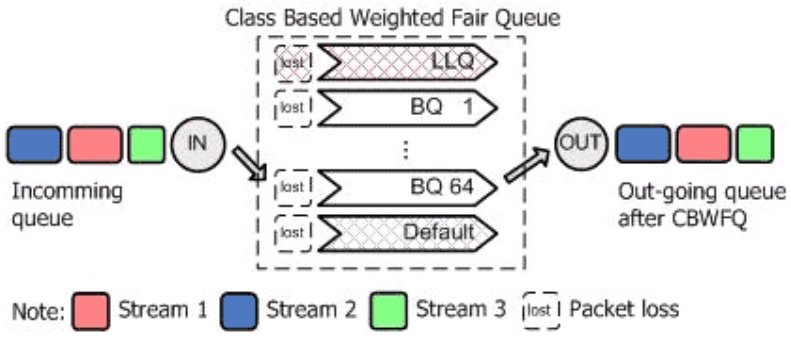


Figura I.12 Esquema del funcionamiento de CBWFQ

Las clases utilizadas en CBWFQ pueden asociarse a:

- Flujos (direcciones origen-destino, protocolo, puertos)
- Prioridades (campo DS differentiated service, otras etiquetas)
- Interfaces de entrada/salida
- VLAN

Estas clases se implementan filtrando el tráfico con filtros en los routers. Este proceso se llama clasificación de tráfico, que puede ir acompañado a su vez con proceso de

marcado de paquetes. El servicio recibido en función de esta clasificación se asocia a la política de servicio.

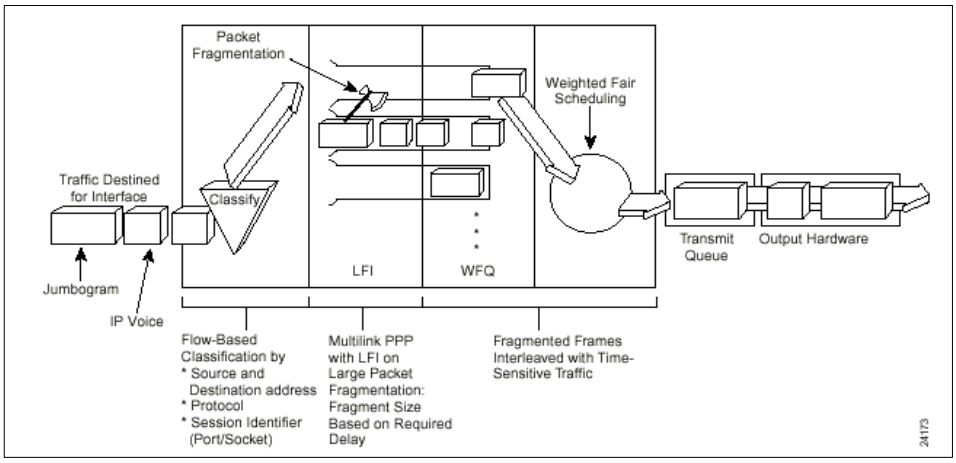
1.4.6. Link Fragment and Interleaving (LFI)

Aunque la técnica Fragmentación e intercalado (LFI) no pertenece a las de encolamiento sino más bien a las de Acondicionamiento de Trafico, es importante destacarla, ya que mediante la misma se puede brindar calidad de servicio a determinado tráfico.

El retardo de los paquetes no es exclusivo en los buffers de los nodos. El retardo que sufren los paquetes debido a la serialización es un tema muy importante a considerar, sobre todo uando los nodos usan interfaces de baja velocidad y tramitan tráficos sensibles al retardo.

Si el tamaño de los paquetes de datos no es analizado y acondicionado con anterioridad a su ingreso a los buffers, estos inevitablemente retrazarán al resto de tráficos que presionan por salir a través de las interfaces seriales, y su vuelve una condición muy crítica cuando de por medio hay tráficos que no admiten retardos como la voz y la multimedia.

La fragmentación e intercalado es una técnica usada en enlaces de baja velocidad para asegurar que los paquetes de tráfico prioritario no sufran un retardo excesivo. Se logra fragmentando los paquetes de datos e intercalado entre ellos los paquetes de prioridad (Figura I.!3). En general el objetivo debe ser no permitir retados de serialización más allá de los tiempos mínimos requeridos por los paquetes de prioridad.



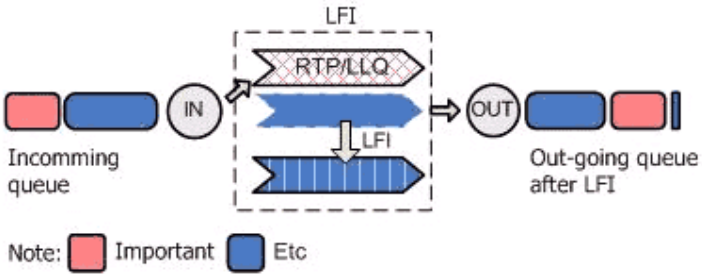


Figura I.13 Esquema del funcionamiento de LFI

Los paquetes de prioridad no se deben fragmentar.

1.4.7. WRED (Weighted Random Early Detection)

La Detección Aleatoria Anticipada basada en pesos (WRED) pertenece a las técnicas de prevención de la congestión, para ello monitorean la carga de tráfico en un esfuerzo por anticiparse y prevenir posibles focos de congestión que pudieran darse en los cuellos de botella de la red. El método consiste básicamente en descartar paquetes antes de que se llegue a una congestión del tráfico, situación conocida como

administración activa de la profundidad de la cola de la interfaz. Hay dos formas de descartar el tráfico:

• Tail Drop. Es la respuesta por defecto de todo sistema a la congestión, descartar paquetes sin tomar en cuanta el tipo de tráfico.
• Random Early Detection.

WRED es la evolución del la técnica RED por lo explicaremos en que cosiste esta:

Es una forma de administración activa de la cola. En lugar de esperar pasivamente hasta que los buffers descarten el tráfico, RED descarta aleatoriamente y en forma progresiva paquetes en cuanto detecta una tendencia a la congestión (detección anticipada aleatoria). La probabilidad y velocidad de descarte de los paquetes aumenta con el grado de ocupación de la cola (profundidad de cola). En respuesta a este aumento de descarte de paquetes por parte del receptor, el emisor reduce la tasa de envío hasta tanto se recupera la profundidad de la cola. Al utilizar un algoritmo de descarte aleatorio, que no toma en cuenta la prioridad del tráfico, no ofrece posibilidades de QoS para tráficos en tiempo real, caso Video IP

WRED Weighted Random Early Detection

Weighted RED (figura I.14) asocia la probabilidad de descarte al tipo de tráfico, evitando de esta manera que se descarte paquetes de mayor prioridad. El objetivo básico es que los paquetes de mayor prioridad tengan la menor probabilidad de descarte.

WRED combina RED con IP Precedente y DSCP, y permite el descarte de paquetes en forma selectiva con base en clases de servicio. El tráfico con una reserva RSVP es tratado por encima del valor más alto de prioridad de IP. WRED al permitir la clasificación de tráfico en clases de servicio y administra la profundidad de cola de todos los tipos de tráficos, proporciona una velocidad de descarte mayor para el tráfico menos prioritario.

WRED es útil principalmente cuando la mayoría de tráfico es TCP. Al descartar tráfico no prioritario al azar y tempranamente, el emisor regula el tamaño de la ventana

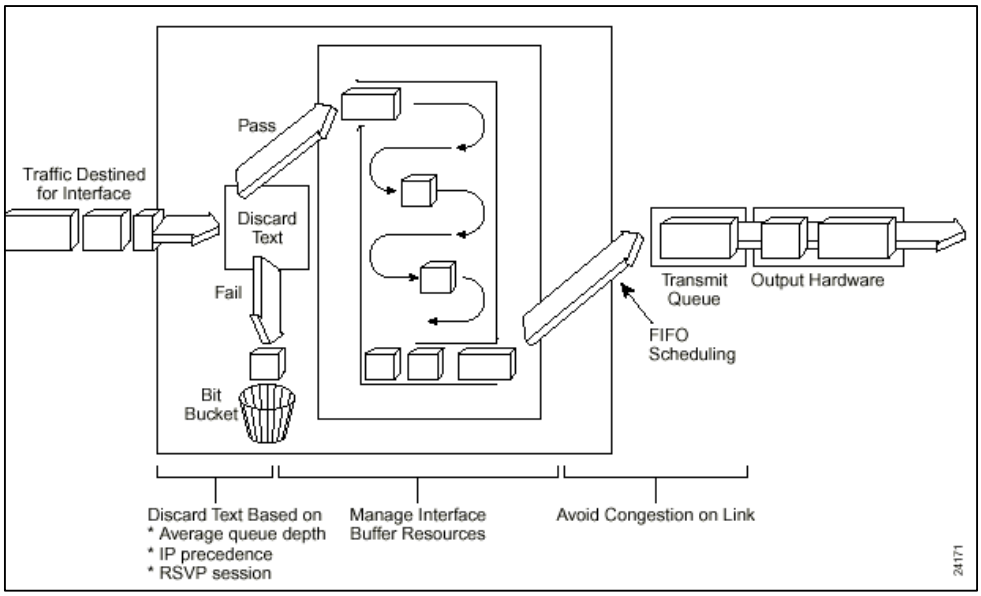


Figura I.14 Esquema del funcionamiento de WRED

CAPÍTULO II

FORMATOS DE COMPRESION EN VIDEO-VIGILANCIA-IP

2.1. Introducción

La digitalización de diferentes medios visuales ha posibilitando el acceso directo a la información y una riqueza de presentación de contenidos (información en general) muy superior a la información textual. Incluso el concepto de Hypertexto, como una forma de acceso interactivo a la información textual, queda obsoleto, apareciendo el concepto de Hypermedia, donde la información ya es de tipo multimedia (texto, images, gráficos y vídeo). Se presenta entonces el concepto de vídeo interactivo (objeto vídeo), permitiendo la interactividad y navegación dentro del propio medio y su integración dentro de entornos Multimedia.

A pesar de los grandes avances en tecnología digital, el uso del vídeo digital todavía está seriamente limitado por dos razones principales:

1) el gran tamaño de información digital que supone el almacenamiento de imagen en movimiento de alta calidad (aunque recientemente esta limitación disminuye gracias a la aparición de nuevas técnicas y estándares de compresión/descompresión, como MPEG y H.261).

2) la falta de sistemas viables para gestionar dicha información, ofreciendo una organización efectiva y una recuperación selectiva de la información. Donde en los últimos años, se han empezado a desarrollar tecnologías y sistemas muy innovadores, con grandes perspectivas de éxito y aceptación, que plantean de un modo realista la utilización del vídeo digital de una forma auténticamente interactiva dentro de nuevos entornos informáticos.

Desde la introducción de los sistemas de vídeo vigilancia analógicos a principios de los años 70, las ventas de sistemas de CCTV (circuito cerrado de TV) para ayudar en la investigación criminal y de seguridad han ido aumentando año tras año.

Tradicionalmente, estos sistemas han sido cerrados y han contado con funcionalidades bastante limitadas. Hoy, los sistemas de **video vigilancia digitales** han demostrado numerosas ventajas frente los analógicos: accesibilidad remota a imágenes de vídeo en directo, escalabilidad, almacenamiento mejorado, potencial de integración y muchos otros.

2.2. Video-Vigilancia- IP

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.

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 perdidas 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.

El vídeo IP, a menudo conocido como vigilancia IP para determinadas aplicaciones en el ámbito de la vigilancia en seguridad y la monitorización remota, es un sistema que ofrece a los usuarios la posibilidad ver en vídeo a través de una red IP (LAN/WAN/Internet).

Los componentes de un sistema de video-vigilancia-IP son:

2.2.1. Cámaras de 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.

Una cámara de red puede describirse como una cámara y un ordenador combinados (Figura II.), Se conecta directamente a la red como cualquier otro dispositivo y en el caso de cámaras más sofisticadas software propio para servidor Web, servidor FTP, cliente FTP y cliente de correo electrónico, también incluye entradas para alarmas y salida de relé. Las cámaras de red más avanzadas también pueden equiparse con muchas otras funciones de valor añadido como son la detección de movimiento y la salida de vídeo analógico.

El componente cámara de la cámara de red captura la imagen, que puede ser descrita como luz de diferentes longitudes de onda, y la transforma en señales eléctricas. Estas señales son entonces convertidas del formato analógico al digital y son transferidas al componente ordenador donde la imagen se comprime y se envía a través de la red.

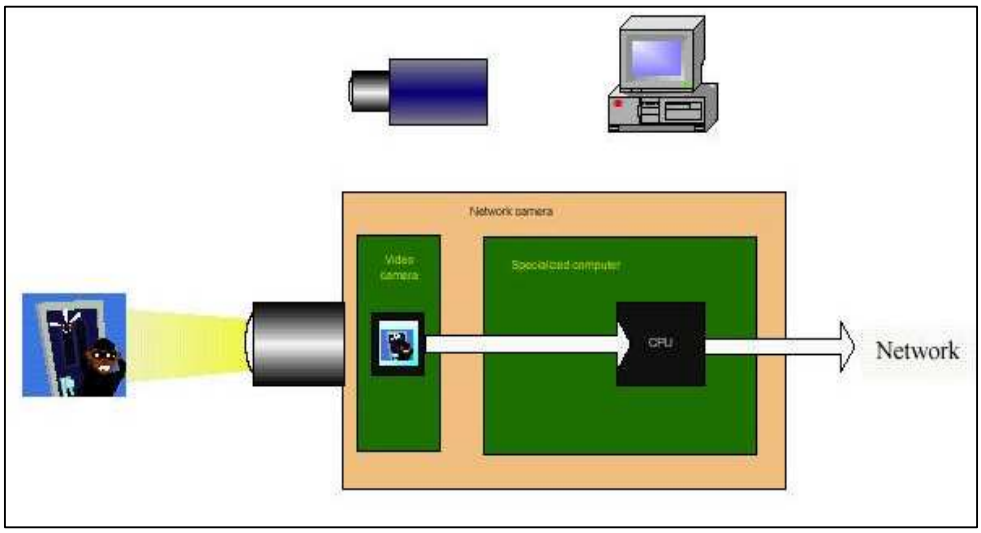


Figura II.15- Función general de la cámara de red

Examinemos más en profundidad los componentes de la cámara de red.

La lente de la cámara enfoca la imagen en el sensor de imagen (CCD). Antes de llegar al sensor la imagen pasa por el filtro óptico que elimina cualquier luz infrarroja de forma que se muestren los colores correctos. El sensor de imagen convierte la imagen, que está compuesta por información lumínica, en señales eléctricas. Estas señales eléctricas se encuentran ya en un formato que puede ser comprimido y transferido a través de redes.

Las funciones de cámara gestionan la exposición (el nivel de luz de la imagen), el equilibrio de blancos (el ajuste de los niveles de color), la nitidez de la imagen y otros aspectos de la calidad de la imagen. Estas funciones las llevan a cabo el controlador

de cámara y el chip de compresión de vídeo, La imagen digital se comprime en una imagen que contiene menos datos para permitir una transferencia más eficiente a través de la red.

La conexión Ethernet de la cámara la proporciona un segundo chip, una solución optimizada para la conexión de periféricos a la red. Este segundo chip incluye una CPU de 32 bits, conectividad Ethernet 10/100 MBps, funcionalidad de Acceso Directo a Memoria (DMA) y una amplia variedad de interfaces de entrada y salida. La CPU, y la memoria flash y DRAM representan los “cerebros” o funciones de ordenador de la cámara y están específicamente diseñados para su aplicación en redes. Juntos, gestionan la comunicación con la red.

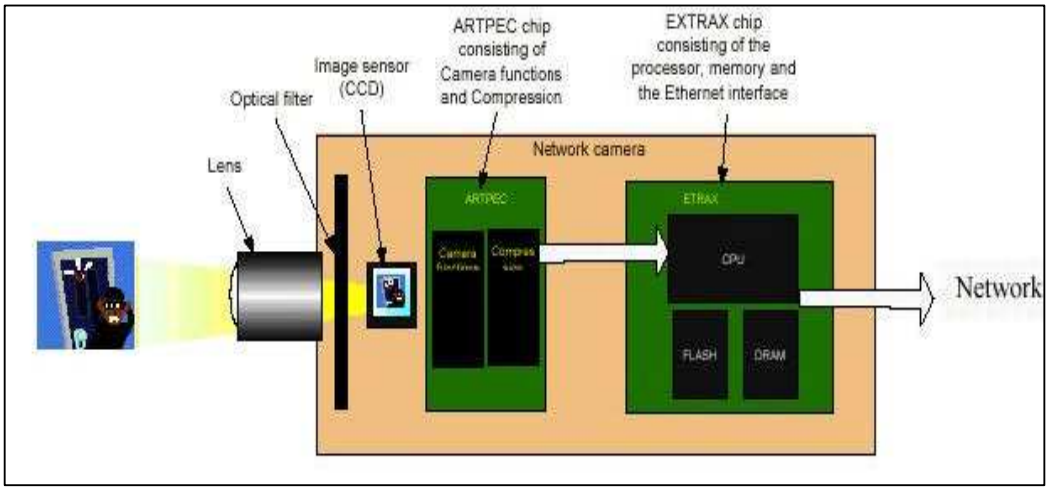


Figura II.16 Detalle del funcionamiento de la cámara de red

2.2.2. Red de transferencia

Si un edificio está equipado con una red IP, entonces ya cuenta con la infraestructura necesaria para incorporar las cámaras de red. Una cámara de red realiza la mayoría de las funciones que lleva a cabo una cámara analógica estándar de circuito cerrado, pero proporciona más funcionalidades a un precio notablemente inferior. Dado que las cámaras de red se conectan directamente a la red existente a través de un puerto Ethernet, las empresas pueden ahorrar cantidades considerables de dinero al no precisar en sus instalaciones un cableado coaxial adicional como necesitan las cámaras analógicas.

Un sistema de vídeo en red utiliza como red troncal (backbone) para el transporte de información redes LAN/MAN/WAN/Internet (Figura II.3) en vez de las líneas punto a punto dedicadas que se utilizan en los sistemas de vídeo analógicos. Muchos negocios ya usan redes informáticas para una amplia cantidad de funciones. La tecnología de vídeo en red utiliza y amplía esta misma infraestructura para la monitorización remota y local.

Cuando se dispone de ordenadores, ya no se necesita ningún equipamiento adicional para ver las imágenes de la cámara de red. Las imágenes pueden verse de una forma muy sencilla desde un navegador web y, en soluciones de seguridad más complejas, con la ayuda de un software dedicado.

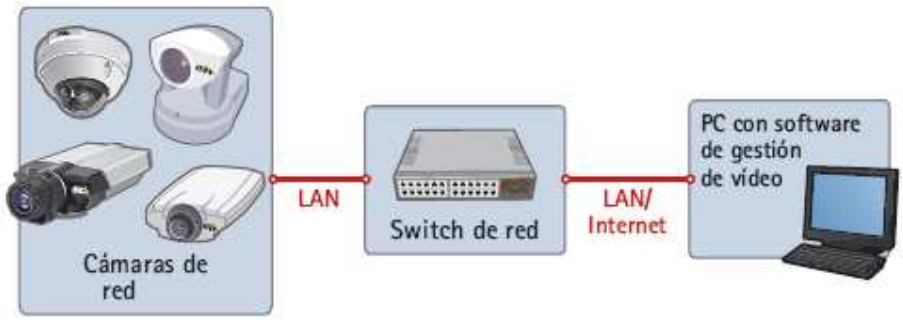


Figura II.17 video –IP sobre la infraestructura de red.

Si la instalación cuenta además con cámaras analógicas, la adición de un servidor de video puede hacer que las imágenes estén disponibles en cualquier localización que fuera necesaria.

La comunicación entre la videocámara IP y el ordenador puede ser directa –mediante un cable UTP estándar– o remota a través del router de una red local o de una conexión a Internet.

La tecnología de vídeo en red tiene la capacidad de proporcionar un mayor nivel de integración con otras funciones y servicios, lo que lo convierte en un sistema en continuo desarrollo. El uso de protocolos y redes estándares abiertos para la comunicación permiten una sencilla integración de sistemas con equipamiento de una amplia variedad de fabricantes.

Además que permite obtener múltiples ventajas adicionales:

- Acceso remoto a imágenes utilizando la red IP, lo que elimina la necesidad de monitores de seguridad dedicados en una oficina central.
- Fácil integración con otros sistemas y aplicaciones.

- Menor TCO (Total cost of ownership, o coste total de propiedad) al aprovechar infraestructuras de red y equipos existentes.
- Crea un sistema preparado para el futuro.

2.2.3. Software de Gestión.

Aunque el vídeo se puede visualizar directamente desde un navegador web normal sin la necesidad de software dedicado, se recomienda usar una aplicación de software en combinación con las cámaras. Este software puede ofrecer al usuario opciones de visualización más flexibles así como la posibilidad de almacenar y gestionar el vídeo.

El software puede ser una solución autónoma para un único PC o una aplicación cliente/servidor más avanzada que proporcione soporte a múltiples usuarios simultáneos (Figura II.18). En algunos casos el usuario final quiere seleccionar el software para implementar el soporte a múltiples sistemas como el de vídeo y el control de accesos.

Seleccionar el paquete de software que permita unir los objetivos de la aplicación y del sistema es una de las claves en el diseño de un sistema útil y eficiente.

Figura II.18 Ejemplo de software de gestión de video.

2.3. Formatos de Compresión para video-IP

La digitalización y transmisión sin comprimir de una señal de vídeo exige anchos de banda prohibitivos incluso hoy en día. Por ejemplo, pensemos que para transmitir una simple señal VGA, con 640 x 480 pixeles, a 25 fotogramas por segundo y dedicando 8 bits para codificar cada una de los tres componentes de color (RGB o rojo, verde y azul), se exigiría un ancho de banda de 640 x 480 x 25 x 24 = 184.32 Mbps, tasa binaria que satura con mucho la velocidad primaria de muchas redes. Pero gracias a la utilización de las técnicas de compresión de video para la transmisión se ha podido reducir la utilización a un ancho de banda de 1.5 Mbps aproximadamente, dependiendo de la técnica utilizada.

En los últimos años, los sistemas de vídeo-vigilancia han evolucionado a pasos agigantados. Estos sistemas han pasado de la captura y transmisión video en forma

analógica, hasta el uso de técnicas que permiten capturar video en forma digital y transmitirlo con esquemas distribuidos sobre infraestructuras IP. Al transmitir flujos de video sobre IP, éste puede ser almacenado en lugares remotos. Además, existe la posibilidad de acceder al los dispositivos de captura desde cualquier parte de la red.

El mayor inconveniente de la transmisión de vídeo por la red IP, es el ancho de banda necesario y la necesidad de calidad de servicio extremo a extremo. En el caso de redes inalámbricas, esta limitación viene dada por el ancho de banda de la propia tecnología. Por todo ello, es imprescindible usar algoritmos de compresión de video que consuman poco ancho de banda y ocupen menor espacio de almacenamiento en disco. En la actualidad coexisten varias técnicas de codificación. Algunas de estas técnicas están basadas en la compresión espacial de las imágenes (por ejemplo, Motion-JPEG), otras se basan en la compresión temporal de las secuencias de video analizando la variación del movimiento entre una imagen y la siguiente (por ejemplo, H.261 y H.263). El objetivo de estas técnicas es conseguir mayores ratios de compresión a la vez que se intenta conseguir buena calidad de imagen.

Existe una gama muy diversa de aplicaciones para video que tienen condiciones ó características muy diversas de funcionamiento. Las aplicaciones para comunicación por video pueden ser comunicaciones extremo a extremo, multicast y de difusión.

El video puede estar precodificado (almacenado) ó puede ser codificado en tiempo real (videoteléfono interactivo ó video-vigilancia). Los canales de comunicación para video pueden ser estáticos ó dinámicos, de paquetes conmutados ó de circuitos conmutados. Estos canales de transmisión para video pueden tener transmisiones con una tasa de bits constante ó variable y pueden también, soportar alguna forma de calidad de servicio (QoS) ó pueden proveer solamente el soporte de “mejor esfuerzo”.

Las propiedades específicas de una aplicación de comunicaciones por video determina fuertemente el diseño del sistema.

2.3.1. El video Afluente

Un sistema de video afluente es aquel que codifica el contenido visual y lo transmite en forma de ristras sobre una red de datos (alámbrica ó inalámbrica) donde uno ó más receptores pueden acceder, decodificar y desplegar el video hacia los usuarios en tiempo real.

Dado que el video sin comprimir demanda un gran ancho de banda, la necesidad de una compresión eficiente es de gran importancia en este tipo de aplicaciones.

La compresión de video se lleva acabo explotando las similitudes ó redundancias que existen en una señal de video típica. Por ejemplo, imágenes consecutivas en una secuencia de video presentan una redundancia temporal, ya que generalmente contienen los mismos objetos en movimiento entre las imágenes. Dentro de una sola imagen, existe la redundancia espacial, dado que las amplitudes de intensidad de la vecindad de píxeles están frecuentemente correlacionadas. De la misma manera, los componentes de color: rojo, verde y azul está correlacionados. Otro objetivo de la compresión es reducir lo irrelevante de la señal de video. Esto es, solamente codificar características del video que son perceptualmente importantes y no utilizar bits en información que es irrelevante.

Cada uno de los gráficos o imágenes individuales de la secuencia es un frame. El número de frames por segundo (fps) se conoce como el ratio de frames (frame rate).

Para que el movimiento sea suave el número de frames por segundo tiene que ser superior a 16. El vídeo se basa en el fenómeno de la persistencia: en cuanto la frecuencia está entorno a 16 cuadros/imágenes por segundo, percibimos sensación de continuidad.

Analizaremos algunos conceptos importantes en la compresión de video:

2.3.2. Compresión Espacial

La compresión espacial se relaciona con las similitudes entre píxeles adyacentes en áreas planas de la imagen y en frecuencias espaciales.

Consiste en explotar la redundancia espacial y la del color para comprimir la imagen. Las intensidades de los píxeles vecindarios en una imagen, generalmente son muy similares y la mayoría de su energía se concentra en las bajas frecuencias

A la imagen original capturada luego dividirla en macro bloques y a cada uno dividirlo en un número determinado de pixels para luego determinar su similitud (Figura II.19)

Figura II.19 Explorar la similitud de pixels adyacentes

Luego de dividir los bloques en un numero de pixels se aplica la transformada discreta del coseno DTC para de esta manera obtener una matriz de números reales a la cual se pueda aplicar un centrado ha cero para obtener los bits redundantes y puedan ser suprimidos para la transmisión.

2.3.3. Compresión Temporal

La redundancia temporal es extraída usando similitudes entre imágenes sucesivas. Tanto como sea posible, la imagen actual es estimada a partir de imágenes recientemente enviadas. Cuando se usa esta técnica, solo se necesita enviar la diferencia entre la imagen estimada y la actual. La imagen diferencia es entonces sujeta a codificación espacial.

La redundancia temporal puede ser explotada realizando codificación Inter, es decir, trasmitiendo solo la diferencia de imágenes.

2.3.4. Explicación de un sistema de Vídeo-IP

Antes de abordar la cuestión que nos interesa debemos realizar un pequeño análisis para comprender mejor los procesos de grabación y almacenamiento digital. En un sistema de vídeo IP hay múltiples procesos ejecutándose simultáneamente. Nos centraremos sólo en alguno de los más importantes relacionados con la compresión:

Codificación: El proceso que se realiza en la cámara de red o el servidor de vídeo que codifica (digitaliza y comprime) la señal de vídeo analógico de manera que pueda transmitirse a través de la red.

Transmisión IP: Transmisión sobre una red de datos basada en el protocolo IP, inalámbrica o con cableado, desde una fuente a hardware variado de grabación o visualización (por ejemplo un servidor de PC's).

Grabación: Datos transferidos a discos duros estándar conectados a un dispositivo de almacenamiento como puede ser un servidor, NAS (Network Attached Server) o SAN (Storage Area Network).

Decodificación: El vídeo codificado debe ser traducido, o decodificado, con el fin de ser visualizado/monitorizado. Este proceso se realiza en un PC o en otro sistema decodificador que se emplee para visualizar el vídeo.

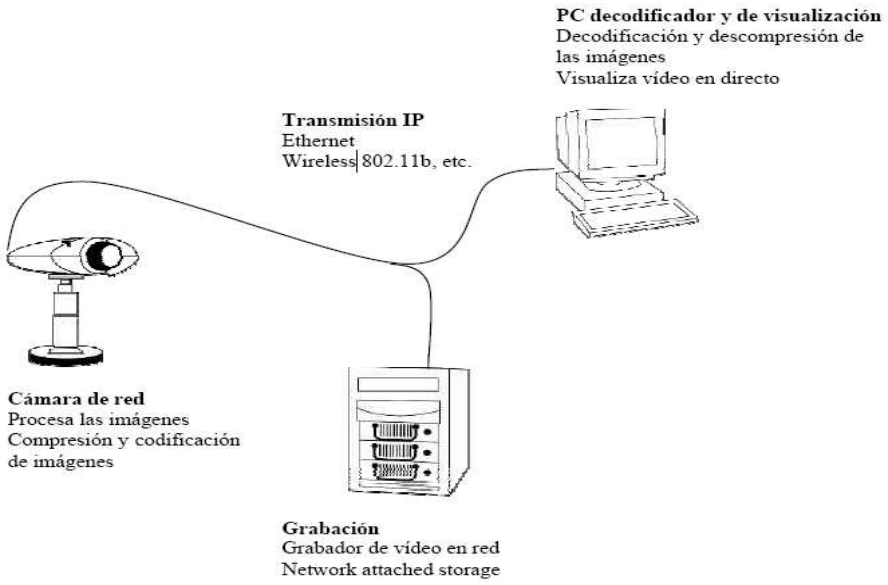


Figura II. 20 Ejemplo de un sistema de vídeo en red

Ahora revisaremos los formatos de compresión estandarizados:

2.3.5. Formato de compresión JPEG

JPEG es un conocido método de compresión, que fue originalmente estandarizado a mediados de los años 80 en un proceso iniciado por el Joint Photographic Experts Group.

La compresión JPEG utiliza solamente una compresión espacial que puede realizarse a diferentes niveles definidos por el usuario y que determinan cuanto tiene que comprimirse una imagen. El nivel de compresión seleccionado tiene una relación directa con la calidad de imagen obtenida. Además del nivel de compresión la escena de la imagen en sí misma también tiene un impacto en el nivel de compresión resultante. Mientras que un muro blanco, por ejemplo, puede producir un fichero de imagen relativamente pequeño (y aceptar un mayor nivel de compresión), el mismo nivel de compresión aplicado a una escena compleja y patronizada producirá un fichero de mayor tamaño y con un nivel de compresión menor.

Las dos imágenes (Figura II.21) ilustran el nivel de compresión frente a la calidad de la imagen para una escena dada a dos niveles de compresión diferentes

(a)

(b)

a) Nivel de compresión “bajo”
Ratio de compresión 1:16
6% del tamaño original del fichero
No hay degradación visible en la calidad de la imagen

b) Nivel de compresión “alto”
Ratio de compresión 1:96
1% del tamaño original del fichero
Calidad de imagen claramente degradada

Figura II.21 Niveles de compresión para JPEG

2.3.6. Formato de compresión M-JPEG

En Motion-JPEG, al igual que una cámara fotográfica digital, una cámara de red captura imágenes individuales y las comprime en formato JPEG. La cámara de red puede capturar y comprimir las imágenes, por ejemplo 30 imágenes individuales por segundo (30 ips), y después hacerlas disponibles como un flujo continuo de imágenes sobre una red a una estación de visualización. Se denomina a este método como Motion JPEG o M-JPEG.

Dado que cada imagen individual es una imagen JPEG comprimida todas tendrán garantizada la misma calidad, determinada por el nivel de compresión definido en la cámara de red o el servidor de vídeo en red.

2.3.7. Formato de compresión MPEG

Una de las técnicas de vídeo y audio más conocidas es el estándar denominado MPEG (Motion Picture Experts Groups) iniciado a finales de los años 80.

Descrito de forma sencilla, el principio básico de MPEG es comparar entre dos imágenes para que puedan ser transmitidas a través de la red, y usar la primera imagen como imagen de referencia (denominada I-frame), enviando tan solo las partes

de las siguientes imágenes (denominadas B y P –frames) que difieren de la imagen original. La estación de visualización de red reconstruirá todas las imágenes basándose en la imagen de referencia y en los “datos diferentes” contenidos en los B- y P- frames.

Una secuencia típica de I -, B- y P-frames puede tener un aspecto similar a la (figura II.22). Hay que tener en cuenta que un P-frame puede solo referenciar a un I - o P-frame anterior, mientras que un B-frame puede referenciar tanto a I - o P-frames anteriores y posteriores.

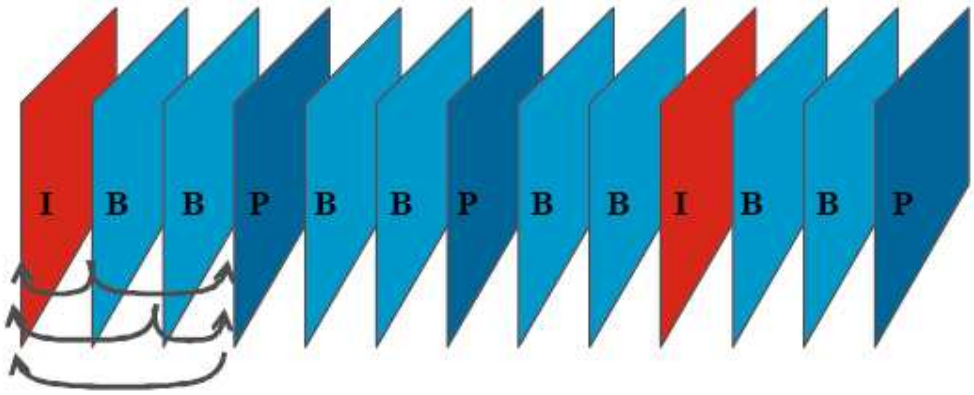


Figura II.22 Transmisión de frames en MPEG

MPEG es de hecho bastante más complejo que lo indicado anteriormente, e incluye parámetros como la predicción de movimiento en una escena y la identificación de objetos que son técnicas o herramientas que utiliza MPEG. Además, diferentes aplicaciones pueden hacer uso de herramientas diferentes, por ejemplo comparar una aplicación de vigilancia en tiempo real con una película de animación. Existe un número de estándares MPEG diferentes: MPEG-1, MPEG-2 y MPEG-4, que se comentarán a continuación.

2.3.7.1. MPEG-1

El estándar MPEG-1, ISO/IEC 11172, fue presentado en 1993 y está dirigido a aplicaciones de almacenamiento de vídeo digital en CD's. Por esta circunstancia, la mayoría de los codificadores y decodificadores MPEG-1 precisan un ancho de banda de aproximadamente 1.5 Mbit/segundo a resolución CIF (352x288 píxeles). Para MPEG-1 el objetivo es mantener el consumo de ancho de banda relativamente constante aunque varíe la calidad de la imagen, que es típicamente comparable a la calidad del vídeo VHS. El número de imágenes por segundo (ips) en MPEG-1 está bloqueado a 25 ips.

2.3.7.2. MPEG-2

MPEG-2, ISO/IEC 11172, fue aprobado en 1994 como estándar y fue diseñado para vídeo digital de alta calidad (DVD), TV digital de alta definición (HDTV), medios de almacenamiento interactivo (ISM), retransmisión de vídeo digital (Digital Vídeo Broadcasting, DVB) y Televisión por cable (CATV). El proyecto MPEG-2 se centró en ampliar la técnica de compresión MPEG-1 para cubrir imágenes más grandes y de mayor calidad en detrimento de un nivel de compresión menor y un consumo de ancho de banda mayor. MPEG-2 también proporciona herramientas adicionales para mejorar la calidad del vídeo consumiendo el mismo ancho de banda, con lo que se producen imágenes de muy alta calidad cuando lo comparamos con otras tecnologías de compresión. El ratio de imágenes por segundo está bloqueado a 25 (PAL)/30 (NTSC) ips. al igual que en MPEG-1.

2.3.7.3. MPEG-4

El estándar MPEG-4 fue aprobado en 2000 y es uno de los desarrollos principales de MPEG- 2.

Como uno de los desarrollos principales de MPEG-2, MPEG-4 incorpora muchas más herramientas para reducir el ancho de banda preciso en la transmisión para ajustar una cierta calidad de imagen a una determinada aplicación o escena de la imagen. Además el ratio de imágenes por segundo no está bloqueado a 25 ips.

Es importante destacar, no obstante, que la mayoría de las herramientas para reducir el número de bits que se transmiten son sólo relevantes para las aplicaciones en tiempo no real. Esto es debido a que alguna de las nuevas herramientas necesitan tanta potencia de proceso que el tiempo total de codificación/decodificación (por ejemplo la latencia) lo hace impracticable para otras aplicaciones que no sean la codificación de películas, codificación de películas de animación y similares. De hecho, la mayoría de las herramientas en MPEG-4 que pueden ser usadas en aplicaciones en tiempo real son las mismas herramientas que están disponibles en MPEG-1 y MPEG-2.

Otra mejora de MPEG-4 es el amplio número de perfiles y niveles de perfiles que cubren una variedad más amplia de aplicaciones desde todo lo relacionado con transmisiones con poco ancho de banda para dispositivos móviles a aplicaciones con una calidad extremadamente amplia y demandas casi ilimitadas de ancho de banda. La realización de películas de animación es sólo un ejemplo de esto.

2.3.8. Formato de compresión H261

H.261 es un estándar de codificación de vídeo diseñado por la International Telecommunication Union (ITU) en 1990 para transmitir vídeo sobre lineas ISDN a bitrates entre 40kbits/s y 2Mbits/s.

Fue el primer estándar de codificación de vídeo llevado a la práctica, y aunque fuera pionero y muy mejorable, todos los subsecuentes estándares de codificación de vídeo internacionales (desde MPEG-1 hasta incluso H.264) se han basado en su diseño.

Adicionalmente, los métodos de desarrollo colaborativo del estándar conforman los básicos del proceso de estandarización hoy en día.

Diseñado para videoconferencia, aunque también se utilizan para cámaras de red, este estándar ofrece un gran ratio de imágenes. Sin embargo, la calidad de las imágenes es baja. Este estándar normalmente proporcionan resoluciones de imagen de hasta 352x288 pixeles. Ya que la resolución disponible es bastante limitada, los productos nuevos tienden a no utilizar este estándar.

Las aplicaciones de videoconferencia generalmente transmiten imágenes de cabeza y hombros de gente con movimiento limitado y un fondo estático, por eso H.261 es adecuado para estas aplicaciones.

Las mejoras introducidas en los estándares subsiguientes han resultado en mejoras significantes en la compresión con respecto a H.261, de forma que H.261 ahora está obsoleto, aunque sigue manteniéndose compatibilidad con él en ciertos sistemas de Video-conferencia y para ciertos tipos de vídeo en Internet.

En cualquier caso, H.261 conforma un hito histórico en el campo de la codificación de vídeo.

2.3.9. Formato de compresión H263

H.263 es un codec de vídeo originalmente diseñado por ITU-T en 1995/1996 como una solución de codificación que requiere un bitrate bajo, en un principio, para vídeoconferencia.

Fue desarrollado como una mejora evolutiva basada en la experiencia obtenida del desarrollo de H.261, MPEG-1 y MPEG-2. Sustituye a H.261 ya que ofrece una mejora con respecto a este codec para cualquier bitrate.

Más adelante fue mejorado en proyectos conocidos como H.263v2 o H.263v3.

La mayoría del vídeo flash (como el utilizado en YouTube, Google vídeo, MySpace) es codificado en este formato. Utiliza el algoritmo de control de bitrate TMN8.

La técnica de compresión H.263 se centra en una transmisión de vídeo con una tasa de bits fija. La desventaja de tener una tasa de bits fija es que cuando un objeto se mueve, la calidad de la imagen disminuye. H.263 fue originalmente diseñado para aplicaciones de videoconferencia y no para aplicaciones de vigilancia donde los detalles son más importantes que una tasa de bits fija.

CAPÍTULO III

CONFIGURACION Y ANALISIS DE LAS TECNICAS DE ENCOLAMIENTO, FORMATOS DE COMPRESION.

3.1. Introducción

Se trata de la configuración y análisis de las técnicas de encolado y el escenario practico actual con una exploración de los parámetros que permitan obtener datos cuantitativos para valorar los resultados y así establecer comparativos de dichas técnicas. Así como un análisis teórico sobre los formatos de compresión de video.

Los aspectos de comparación pueden ser variados y muy amplios, por lo que habrá que acotar de alguna manera el ámbito de la tesis. Nos centraremos característicamente en aquellos parámetros que estén orientados a aplicaciones en tiempo real.

3.2. Configuración y Análisis de las técnicas de encolamiento

El mecanismo de calidad de servicio se refiere a la habilidad en 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.

Con lo estudiado en el capitulo I nuestro objetivo siguiente es configurar las técnicas de encolamiento en un escenario de prueba donde podamos analizar cada una de ellas para así determinar comparativas entre los mismos que permitan determinar cual se ajusta de mejor manera a nuestra necesidad de brindar preferencia de trafico al videoIP.

3.3.1. Parámetros de medición

Hemos tomado en cuenta los parámetros que definen globalmente la calidad de servicio para escoger el que se adecue a nuestro escenario y que a su vez nos permita interpretar el resultado: Siendo este parámetro cuantitativo el tiempo que se demora desde que se envía el paquete hasta que se recibe, conocido como retraso.

Además incorporamos un parámetro cualitativo que será la calidad de la imagen percibida por el usuario.

3.3.2. Escenario de pruebas

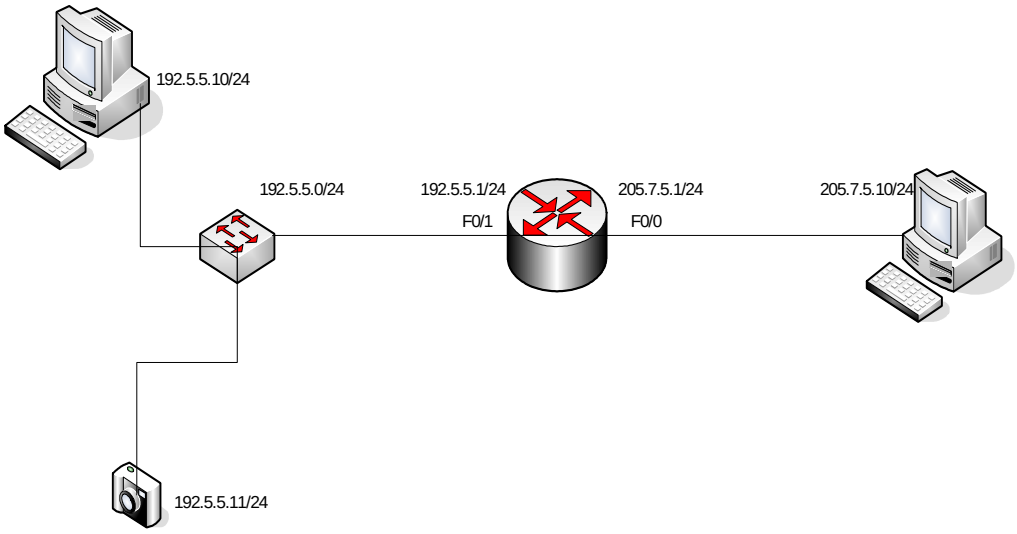


Figura III.23 Esquema del escenario de pruebas

Elementos Hardware

La maqueta muestra el escenario para las pruebas compuesto por:

- Router Cisco2811
- Switch
- Pc`s
- Cámara de red.

Elementos Software

- Capturadotes o Sniffers
- Software de prueba para la visualización de la cámara
- Consola del DOS para efectuar Pings en formato -t -l para realizar pings indefinidos y de longitud establecida en 20000.

3.3.3. Configuración de las interfaces Fastethernet en el Router

- Vamos como primer paso a borrar toda configuración previa en el Router.

```
Router>ena
Router# erase  startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
Router#
*Feb 19 15:32:15.935: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
```

- Ahora configuraremos las IP en las interfaces Fastethernet disminuyendo su velocidad a 10Mbps dandole un nombre al Router .

```
Router#configure Terminal
Router(config)#hostname VideoIP
VideoIP(config)#interface fastEthernet 0/0
VideoIP(config-if)#ip address 205.7.5.1  255.255.255.255
VideoIP(config-if)#speed 10
VideoIP(config-if)#no shutdown
VideoIP(config-if)#exit
VideoIP(config)#interface fastEthernet 0/1
VideoIP(config-if)#ip address 192.5.5.1 255.255.255.0
VideoIP(config-if)#speed 10
VideoIP(config-if)#no shutdown
VideoIP(config-if)#exit.
```

3.3.4. Configuración y pruebas con FIFO (First In First Out)

En los Interfaces con velocidades superiores a los 2.5 Mbps la técnica de encolado FIFO viene ya configurada por defecto, por lo que no es necesario especificarla en la configuración. Pero podríamos confirmar si esta presente en las interfaces mediante el comando siguiente.

VideoIP#show interfaces

En donde a más de toda la información de las interfaces Fastethernet nos muestra la técnica de encolado presente:

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/40 (size/max)

- **Pruebas con FIFO**

Para la realización de pruebas con esta técnica de encolado vamos a realizar los siguientes pasos:

Abrir 8 consola de DOS (Ver Anexo 1(a)) y en cada una de ellas ejecutar el comando Ping infinito con una longitud del paquete de 20000 y poder visualizar el tiempo de transmisión en la forma siguiente:

Ping 205 .7.5.10 – t - l 20000

AL mismo tiempo se ejecuta la transmisión del video desde el host IP 192.5.5.11 que corresponde a la cámara de red hacia la aplicación de prueba en el host IP 205.7.5.10 (Ver anexo1 (b))

En el mismo instante se efectúa una transferencia de archivo vía FTP desde el host IP 192.5.5.11 hacia el host IP 205.7.5.10.

Los resultados obtenidos con esta prueba son los siguientes

Tiempos promedio de ejecutar el comando PING = **36 milisegundos** (Ver Anexo2 (c))
Tiempo promedio de transmisión de video (tiempo promedio entre una imagen JPEG a otra JPEG capturadas con el sniffer) = **35 milisegundos** (Ver Anexo2 (d))
Tiempo promedio de la transmisión del archivo vía FTP = **93.54 segundos** (Ver Anexo2 (e))
Para obtener los valores promedio se realizaron 15 pruebas o ensayos con los tres tipos de trafico circulando por la red.

3.3.5. Configuración y pruebas con WFQ

Aunque WFQ viene configurado por defecto en enlaces inferiores a 2.5 Mbps, se puede configurar en cualquier interfase para tratar de satisfacer las necesidades de trafico prioritario, ya que mediante esta técnica se da predilección al trafico menos pesado al que WFQ asimila que son aplicaciones sensibles al retardo.

Se configura WFQ para la interface deseada de la manera siguiente

```
VideoIP(config)#interface fastEthernet 0/0
VideoIP(config-if)#fair-queue
VideoIP(config-if)#exit
```

De esta manera queda configurada la interface con WFQ, podemos ver:

VideoIP#show interfaces

.
.
.

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: weighted fair

Output queue: 0/40 (size/max)

- **Pruebas con WFQ**

Para la realización de las pruebas con WFQ se siguieron los mismos pasos establecidos con con FIFO en lo referente a la ejecución del comando Ping, Transmisión de video y la transferencia FTP. Obteniéndose los siguientes resultados:

Tiempos promedio de ejecutar el comando PING = **41 milisegundos** (Ver Anexo2 (f))
Tiempo promedio de transmisión de video (tiempo promedio entre una imagen JPEG a otra JPEG capturadas con el sniffer) = **49 milisegundos** (Ver Anexo2 (g))
Tiempo promedio de la transmisión del archivo vía FTP = **96.34** (Ver Anexo2 (f))

Para obtener los valores promedio se realizaron 15 pruebas con esta técnica de encolado con los tres tipos de tráfico circulando por la red.

3.3.6. Configuración y pruebas con PQ

Para poder configura esta técnica de encolado es necesario establecer filtros mediante los cuales se permita clasificar el trafico, esto se logra con el uso de listas de control de acceso *access-list*, para después asociarlo con cada una de los tipos de

colas definidas en PQ mediante el modo de configuración *priority-list x* , y por ultimo asociar esta disciplina x a la interfaz de salida del router en la que necesitemos:

Como se ha comprobado que la cámara utiliza el protocolo http para transmitir las imágenes vamos a clasificar como *high* al trafico HTTP, como *medium* al trafico FTP y *low* al trafico ICMP, siendo como *normal* el resto de trafico.

Realizamos la configuración de PQ en el router de la siguiente manera:

```
VideoIP(config)#access-list 111 permit tcp any any eq 80
VideoIP(config)#access-list 112 permit tcp any any eq 21
VideoIP(config)#access-list 113 permit icmp any any
```

Una vez que hemos creado las listas de control, vamos ha asociarlo a cada uno de los tipos de trafico definidos en PQ

```
VideoIP(config)#priority-list  5 protocol ip high list 111
VideoIP(config)#priority-list  5 protocol  ip medium list 112
VideoIP(config)#priority-list  5 protocol  ip low list 113
```

Finalmente asociamos la disciplina 5 a la interfsce fastEthernet 0/0

```
VideoIP(config)#interface fastEthernet0/0
VideoIP(config-if)#priority-group  5
```

Revisamos si la configuración quedo establecida

```
VideoIP#show queueing priority
Current DLCI priority queue configuration:
Current priority queue configuration:

List   Queue  Args
5      high   protocol ip         list 111
5      medium protocol ip      list 112
5      low    protocol ip         list 113
```

Revisamos si la estrategia esta configurada en la interface

VideoIP#show queueing interface fastEthernet 0/0
Interface FastEthernet0/0 queueing strategy: **priority**

- **Pruebas con PQ**

Realizamos la Transmisión de video, transferencia FTP y ejecución del comando Ping como en los casos anteriores y obtenemos los resultados siguientes:

Tiempos promedio de ejecutar el comando PING = **97 milisegundos** (Ver Anexo2 (h))
Tiempo promedio de transmisión de video (tiempo promedio entre una imagen JPEG a otra JPEG capturadas con el sniffer) = **33 milisegundos** (Ver Anexo2 (i))
Tiempo promedio de la transmisión del archivo vía FTP = **102.34 segundos** (Ver Anexo2 (h))

Para obtener los valores promedio se realizaron 15 pruebas con esta técnica de encolado con los tres tipos de tráfico circulando por la red.

3.3.7. Configuración y pruebas con CQ

CQ trata de repartir el ancho de banda entre diferentes servicios para de esta manera ser más equitativo.

Vamos a configurar CQ y lo que primero tenemos que hacer es establecer filtros para clasificar el trafico mediante access-list y luego asociarlo con cada una de las colas definidas en CQ utilizando para este propósito el modo de configuración queue-list x para luego asociar esta disciplina x a la interface de salida que necesitemos.

Establecemos los porcentajes para cada servicio de la siguiente manera:

HTTP 40%,FTP 20%, TFTP 20%, y dejando el 20% restante para otros servicios

La configuración del router es la siguiente:

```
VideoIP(config)#queue-list  1 protocol ip 1  tcp ftp
VideoIP(config)#queue-list  1 protocol ip 2 tcp tftp
VideoIP(config)#queue-list  1 default 3
```

Lo que hemos hecho es declarar una queue-list 1 la cual asigna a la cola1 el trafico FTR, a la cola 2 el trafico TFTP y por defecto a la cola 3 el resto. Lo siguiente es es asignar a la cola 4 el HTTP, para ello utilizamos el siguiente método de clasificación.

```
VideoIP(config)#access-list 114 permit tcp any any eq 80
VideoIP(config)#queue-list  1 protocol ip 4 list 114
```

Ahora debemos asignar un quanto a cada una de las colas que debe ser asignado mediante los porcentajes establecidos.

Si consideramos el cuanto por defecto que es de 1500 bytes y lo hacemos corresponder con el 20% del ancho de banda entonces tendriamos que el quanto asignado para HTTP tendra que ser de 3000 bytes es decir el doble ya que su porcentaje es 40%. Esta representación de porcentajes en cuantos se realiza de la siguiente forma.

```
VideoIP(config)#queue-list  1  queue 1 byte-count 1500
VideoIP(config)#queue-list  2  queue 1 byte-count 1500
VideoIP(config)#queue-list  3  queue 1 byte-count 1500
VideoIP(config)#queue-list  4  queue 1 byte-count 3000
```

El paso final es asignar esta configuración a la fastEthernet 0/0

```
VideoIP(config)#interface fastEthernet0/0
VideoIP(config-if)#custom-queue-list 1
```

Verificamos la configuración

```
VideoIP(config)# show queueing custom

Current custom queue configuration:

List   Queue  Args
1      3      default
1      1      protocol ip     tcp port ftp
1      2      protocol ip     tcp port tftp
1      4      protocol ip     list 114
1      4      byte-count  3000
```

- **Pruebas con CQ**

Con la configuración CQ establecida nuevamente realizamos la Transmisión de video, transferencia FTP y ejecución del comando Ping como en los casos anteriores y obtenemos los resultados siguientes:

Tiempos promedio de ejecutar el comando PING = **38 milisegundos** (Ver Anexo2 (j))

Tiempo promedio de transmisión de video (tiempo promedio entre una imagen JPEG a otra JPEG capturadas con el sniffer) = **33 milisegundos** (Ver Anexo2 (k))

Tiempo promedio de la transmisión del archivo vía FTP = **94.1 miliegundos**

Para obtener los valores promedio se realizaron 15 pruebas con esta técnica de encolado con los tres tipos de tráfico circulando por la red

3.3.8. Análisis de CBWFQ

La técnica de encolamiento CBWFQ hace referencia a la posibilidad de agrupar varios tipos de tráfico en *clases de servicio* con la finalidad de brindar el mismo tratamiento de encolado WFQ a toda la clase agrupada.

Esta técnica se enmarca en el modelo de QoS de *Servicios Diferenciado* (DiffServ) pensado para trafico proveniente del Internet donde el trafico proveniente del exterior sea clasificado en clases y marcado con una prioridad en router de entrada llamados frontera , para luego de implementar políticas internas de tratamiento de esa prioridad de ser tratado con esa prioridad en los routers internos dentro de la Intranet

En el ámbito de desarrollo y pruebas establecido para la presente tesis podemos destacar que el tráfico de videoIP se genera dentro de la Intranet y solo transitara por la misma de esta manera resulta que el pensar en la implementación del modelo DiffServ para nuestro ámbito video-vigilancia-IP interna no es necesario

Sin embargo que CBWFQ dentro de una Intranet agrupa varios tipos de tráfico en clases de servicio para luego internamente en el router interno aplicar WFQ es de suponer que en el marco de pruebas de la presente tesis CBWFQ se comporte en forma similar que simplemente WFQ. Por lo que la implementación de esta técnica arrojara valores aproximados a los de WFQ.

3.3.9. Análisis comparativo de las técnicas de encolamiento

Una ves que se ha logrado obtener resultados cuantitativos en base a los diferentes parámetros establecidos, surge la necesidad de realizar comparaciones de dichos resultados que nos permitan analizar de una manera mas clara dichos resultado.

3.2.9.1. Diagrama comparativo

Se establece el siguiente cuadro

	FIFO	WFQ	PQ	CQ	CBWFQ
PING (ms)	36	41	97	38	41
VIDEO (ms)	35	49	33	33	49
FTP (s)	93.54	96.34	102.34	94.1	96.34

Tabla III.4 Comparación de los formatos de encolamiento

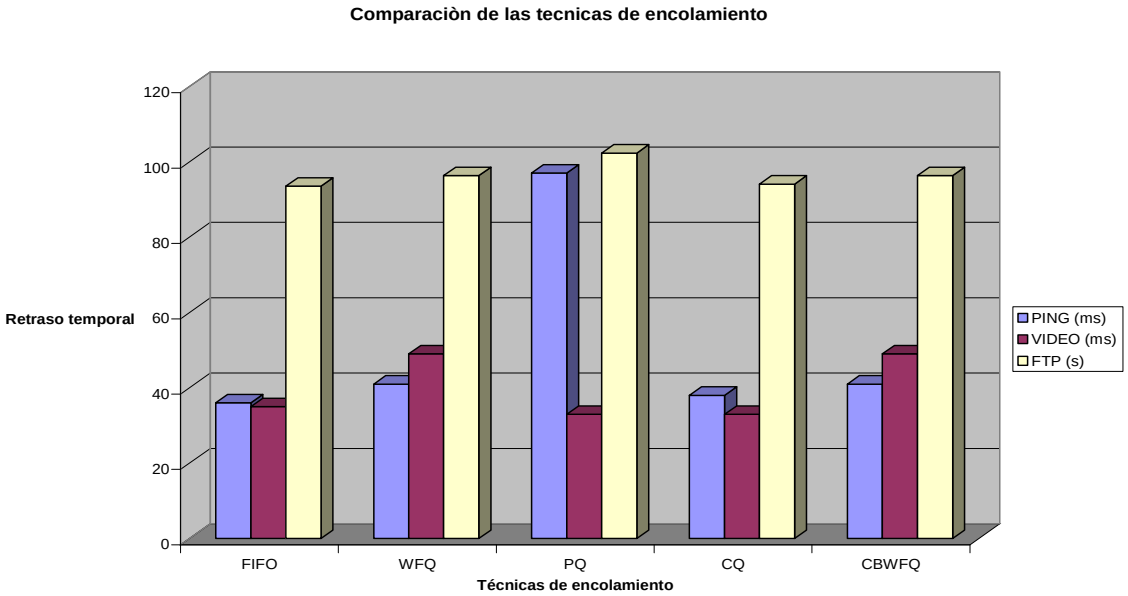


Figura III.24 Diagrama de comparación de las técnicas de encolado

Interpretación

Luego de aplicar una determinada técnica de encolamiento en el router , podemos observar que cada uno de los tipos de tráfico sufre un retrazo temporal diferente en la su transmisión lo que conlleva a interpretar que si existe una diferencia entre aplicar una determinada técnica de encolamiento u otra. Esta diferencia puede ser substancial como en el caso de PQ, donde el trafico ICMP (Ping) ha sufrido una variación considerable con respecto a las demás técnicas.

Para el caso del traficó de video-IP podemos darnos cuenta de que el retraso sufrido en PQ es menor que los demás, mientras para el los otros casos varia en una forma no considerable.

El Trafico FTP aumenta en forma considerable en PQ y para las demás técnicas aunque varia en forma estrecha.

3.2.9.2. Elección de la técnica de encolamiento para video-IP

En base a los resultados obtenidos podernos darnos cuenta de que en forma especifica para el trafico de video-IP las técnicas de encolamiento PQ y CQ son las que permiten obtener menor retraso en la transmisión de este servicio, sin embargo debemos considerar que PQ produce que trafico de otros tipos sufran un retraso mayor y en caso de un congestionamiento considerable puede llegar a crear inanición de los demás servicios.

Tomando en cuenta el ámbito de desarrollo de la tesis donde además de video-IP existen otros tipos de trafico y que en CQ se puede configurar los anchos de banda específicos para cada tipo de tráfico resulta que esta técnica de encolamiento seria la que mejor se adapte a los requerimientos de video-IP y que además pueda seguir brindando un servicio de transmisión para otros servicios.

3.3. Análisis de los formatos de compresión de video

Con base a lo estudiado en el capitulo II, Ahora nos centraremos en el estudio y caracterización de cada una de las técnicas (JPEG; M-JPEG; MPEG; H261/H263) con el objetivo final de establecer comparaciones entre las mismas que permitan obtener una visión objetiva de su avance tecnológico.

En la (figura III.25) se muestra básicamente el proceso de transmisión de video.

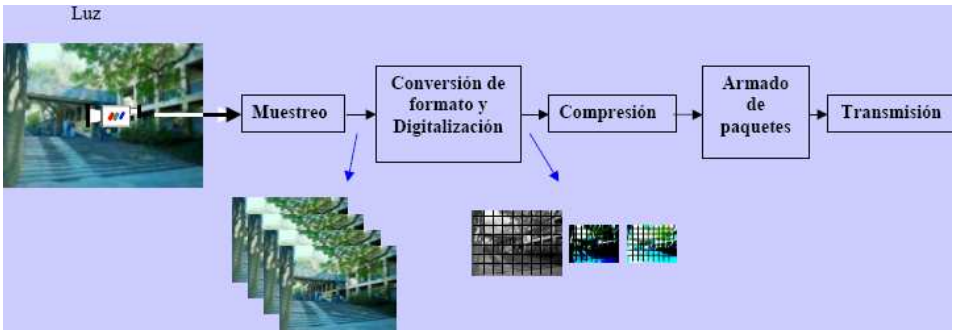


Figura III.25 Transmisión de video-IP

En donde se siguen los siguientes pasos

- Luz -> Secuencia de Imágenes -> Cambio de dominio de colores -> Compresión -> armado de paquetes -> transmisión

En la recepción se efectúa el proceso inverso

- Recepción -> reconocimiento de paquetes -> descompresión -> cambio de formato de colores ->despliegue

3.3.1. Análisis del formato de compresión JPEG

Formato desarrollado por Joint Photographic Experts Group (JPEG) para la compresión de imágenes estáticas. Utiliza básicamente una ***compresión espacial*** (figura III.26) la cual es conocida como compresión Intra Frame y la que trata de establecer la redundancia entre pixels adyacentes dentro de la imagen con el objetivo de omitir esta redundancia o similitud para de esta manera realizar la compresión de dicha imagen.

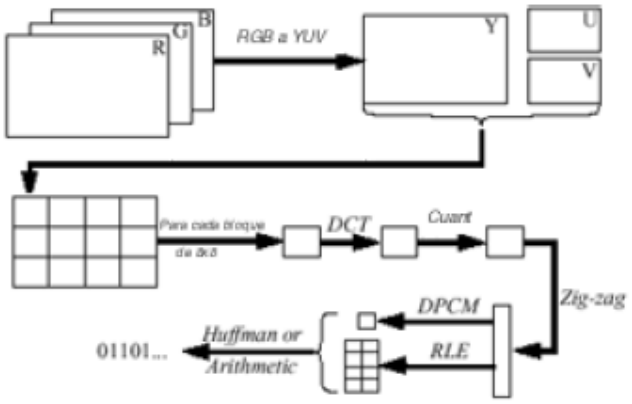


Figura III.26 Representación grafica de la compresión JPEG

3.3.1.1. Características.

- Solo compresión espacial
- Gran calidad de imagen
- Compresión simétrica
- Compresión con perdida
- Resolución estándar 320x 240 pixels
- Catálogo estándar cada bloque de 8x8
- Rangos de compresión de 100:1 teniendo su media entre 10:1 y 20:1.
- Compresión mediante DCT
- Produce archivos de gran tamaño
- Está libre de patentes
- Para aplicaciones de fotografía digital: captura, almacenamiento, transmisión, impresión, etc.

Explicaremos en forma detallada la compresión que efectúa JPEG ya que los formatos posteriores básicamente realizan la misma compresión espacial con cambios en la forma de tratar el movimiento.

1.- Después de la captura de la imagen se divide la misma en una matriz de macro broques de 8x8 (Figura III.27) para luego a cada uno de estos macro bloques volver a dividirlos en una matriz de 8x8 pixels

Figura III.27 División de la imagen en matices de 8 x8

2,. Cada uno de los pixels esta representado RGB (RedGreenBlue) es el color normal de una imagen expresada en los colores primarios para la visualizacion. YCbCr representa la misma imagen pero con valores de Luminancia y Cromancia como en la figura III.6

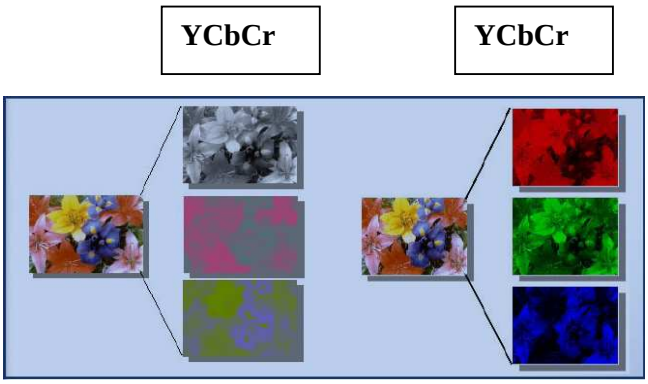


Figura III.28 Representación de RGB en YCbCr

Con las formulas siguientes se calculan los valores para YCbCr para obtener una (tabla III.28) en valores reales que representa la Luminancia y la Cromancia de cada Píxel.

Y = 0.3R + 0.6G + 0.1B

U = B – Y

V = R Y

Cb = 0.5U + 0.5

Cr = 0.625V + 0.5

Y1	Y2	Y3	Y4	Cr1	Cr2	Cb1	Cb2
Y5	Y6	Y7	Y8	Cr3	Cr4	Cb3	Cb4
Y9	Y10	Y11	Y12				
Y13	Y14	Y15	Y16				

Tabla III.5 Tabla de cada píxel en YCbCr

3.- La finalidad es obtener una matriz con valores numéricos reales para luego aplicarle a esta matriz la Transformada Discreta del Coseno (DTC), como en la (Figura III.29) con la finalidad de realizar una aproximación a cero que represente la redundancia o similitud de pixels adyacentes tanto verticalmente como horizontal.

$$\begin{bmatrix} 105 & 103 & 104 & 106 & 107 & 108 & 114 & 122 \\ 117 & 112 & 107 & 106 & 108 & 110 & 116 & 122 \\ 137 & 126 & 116 & 112 & 112 & 116 & 120 & 123 \\ 152 & 144 & 133 & 123 & 120 & 120 & 123 & 125 \\ 159 & 155 & 148 & 137 & 128 & 124 & 124 & 124 \\ 159 & 160 & 157 & 147 & 136 & 130 & 127 & 125 \\ 162 & 163 & 161 & 154 & 147 & 142 & 136 & 132 \\ 165 & 165 & 163 & 158 & 155 & 153 & 146 & 137 \end{bmatrix} \xrightarrow{\text{DTC}} \begin{bmatrix} 2 & 5 & 2 & 0 & 0 & 0 & 0 & 0 \\ -11 & -4 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Figura III.29 Aplicación de la DTC

4.- A la matriz resultante se realiza un recorrido en zig-zag (Figura III.8) para de este modo obtener un vector que luego de la codificación en binario se transmitirá solo los bits representativos de cada píxel.

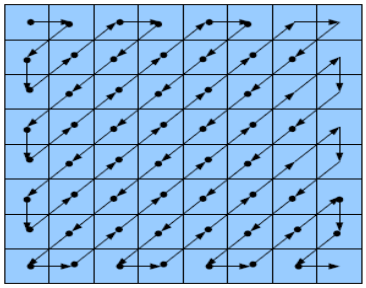


Figura III.30 Recorrido en zig-zag

Por ejemplo se obtendría solamente el vector (Tabla III.6) de bits significativos para la transmisión.

$$[2 \quad 5 \quad -11 \quad 0 \quad -4 \quad 2 \quad 0 \quad 1 \quad -2 \quad -1 \quad 0 \quad 0 \quad -1 \quad 0 \quad 0 \quad 0$$

Tabla III.6 Vector de transmisión

De esta manera se ha realizado la compresión espacial horizontal y vertical de cada píxel y consecuentemente de la imagen total.

Al ser JPEG un algoritmo simétrico, en el lado del receptor se realizaran los mismos pasos pero en sentido inverso para la reconstrucción de la imagen.

3.3.2. Análisis del formato de compresión M-PEG

Motion-JPEG Es la evolución del formato JPEG para movimiento o presentación de video, mediante el cual un dispositivo captura imágenes individuales y las comprime en formato JPEG. Luego se puede transmitir por la red para presentarlas del lado del receptor en forma de secuencia de imágenes lo cual permitirá obtener la visualización del movimiento en una estación de monitorización. Se designa a este método como Motion JPEG o M-JPEG.

Con M-JPEG, cada trama dentro del video se almacena como una imagen completa en formato JPEG (Figura III.9). Las imágenes fijas se visualizan con un alto ratio de imágenes para producir video de muy alta calidad como contrapartida produce archivos de gran tamaño.

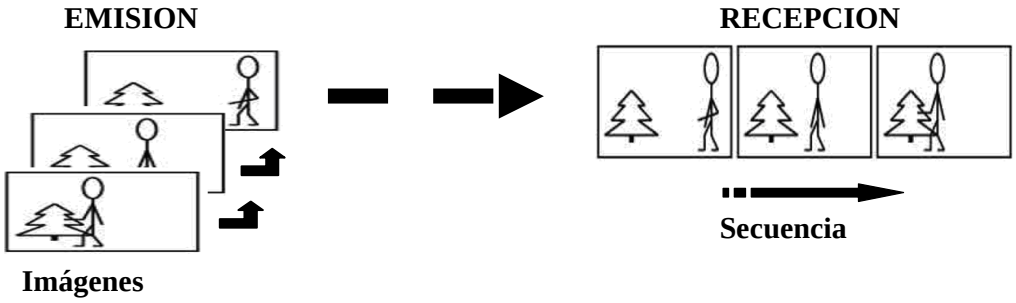


Figura III.31 Transmisión de video en M-JPEG

3.3.2.1. Características

- Solo compresión espacial
- Gran calidad de imagen
- Compresión simétrica
- Compresión con perdida
- Resolución estándar 640x 480 pixels
- Catálogo para cada bloque de ajustable básico 8x8
- Compresión de 100:1 teniendo su media entre 20:1 y 40:1.
- Compresión mediante DCT
- Transmisión de 25 ips
- Produce archivos de gran tamaño
- Utiliza mucho ancho de banda (2,5Mbps)
- Está libre de patentes
- Para aplicaciones de video digital: captura, almacenamiento, transmisión.

3.3.3. Análisis del formato de compresión MPEG

MPEG es el acrónimo de Moving Pictures Experts Group, establecido por la ISO para trabajar en compresión de video.

Utiliza la compresión espacial de JPEG e introduce un nuevo avance de compresión conocido como **compresión Temporal** que relaciona las similitudes entre imágenes sucesivas.

3.3.3.1. Características.

- Compresión espacial y Compresión temporal
- Gran calidad de imagen
- Compresión asimétrica
- Compresión con perdida
- Resolución estándar 720x576 pixels
- Catálogo para cada bloque 16X16
- Compresión de 100:1 variable en el tiempo
- Compresión mediante DCT
- Produce archivos de pequeño tamaño
- Utiliza mucho poco de banda (1.86 Mbps) como máximo
- Transmisión de 30 ips
- Está libre de patentes
- Para aplicaciones que requieren calidad de TV.

Con la compresión temporal, si una imagen esta disponible en el codificador, la siguiente imagen puede ser reconstruida enviando solo la imagen diferencia. Esta diferencia (Figura III.32) se incrementa con el movimiento, pero esto puede ser compensado con la estimación de movimiento, ya que un objeto en una imagen generalmente solo cambiará de posición, no de apariencia. Si el movimiento puede ser medido, puede ser creada una aproximación a la imagen actual, corriendo parte de la imagen previa a una nueva localidad. El proceso de movimiento es controlado por un vector que es transmitido al decodificador

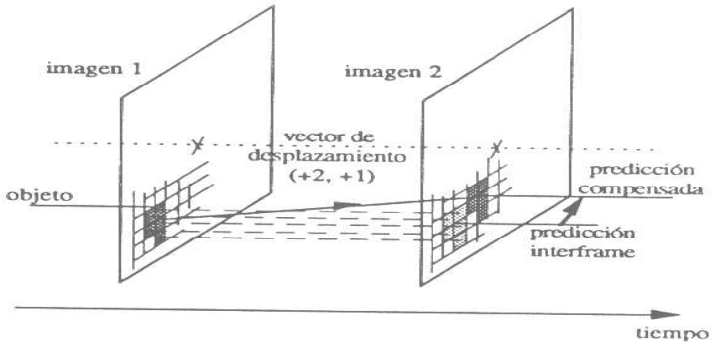


Figura II.32 Transmisión de la imagen diferencia

La imagen diferencia es una imagen mas, y puede ser codificada espacialmente después. El decodificador revierte de codificación espacial y le suma la diferencia para obtener la siguiente imagen.

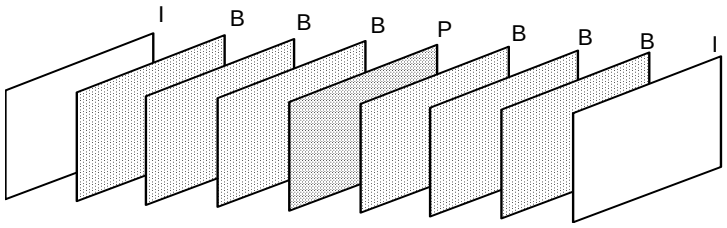


Figura III.33 Tipos de imágenes en MPEG

Existen tres tipos de imágenes en la codificación MPEG (Figura III.33); Imágenes I, imágenes P e imágenes B.

Las Imágenes I que son las imágenes de referencia obtenidas a partir de la compresión JPEG; Las Imágenes P las cuales solo se utilizan para comprimir la imagen diferencia con respecto a la imagen referencia y las imágenes B en las cuales se comprimen a partir de una anterior I o P y que solo transmiten vectores de movimiento y atenuación.

3.3.4. Análisis de los formatos de compresión H26 / H263

H261 / H263: Ambos son formatos con una tasa de compresión muy elevada, que se utilizan para lograr archivos pequeños a una calidad mínimamente aceptable, ideal para utilizar en videoconferencias y transmisiones por Internet y multimedia. Funciona de manera correcta con tamaños de ventanas pequeñas, entre los 352 x 288, y los 128 x 96 píxeles.

H261 desarrollado por International Telecommunication Union (ITU) en 1990, primer estándar de codificación de vídeo llevado a la práctica.

H261 / H263 utilizan el modelo de compresión JPEG para la compresión espacial añadiéndole además una compresión temporal pero sin predicción de movimiento por lo que ha sido utilizado en aplicaciones de videoconferencia ya generalmente transmiten imágenes de cabeza y hombros de gente con movimiento limitado y un fondo estático, por eso H.261 es adecuado para estas aplicaciones.

Estos formatos también utilizan para la transmisión el concepto de compresión temporal pero solo con tramas P para trasmitir las imágenes diferencia (Figura III.34)

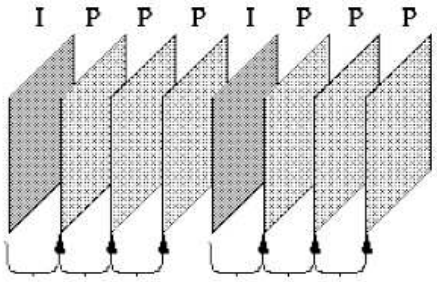


Figura III.34 Transmisión de imágenes en H261 / H263

Las mejoras introducidas en los estándares subsiguientes han resultado en mejoras significantes en la compresión con respecto a H.261, de forma que H.261 ahora está obsoleto, aunque sigue manteniéndose compatibilidad con él en ciertos sistemas de videoconferencia y para ciertos tipos de vídeo en Internet.

3.3.4.1. Características

- Compresión espacial y Compresión temporal
- Baja calidad de imagen
- Compresión asimétrica
- Compresión con perdida
- Resolución estándar 352 x 288 pixels
- Catálogo para cada bloque 16X16 para macro y 8x8 para pixels
- Compresión de 100:1
- Compresión mediante DCT
- Produce archivos de pequeño tamaño
- Utiliza mucho poco de banda (546 kbps)
- Transmisión de 20 ips
- Está libre de patentes
- Para aplicaciones de video conferencia principalmente.

3.4. Análisis comparativo de las técnicas de compresión de video

Luego del análisis de las diferentes surge la necesidad de establecer comparaciones entre dichos formatos con el objeto de establecer relaciones y diferencias tanto cualitativas como cualitativas.

Los parámetros a tomar en cuenta para dicha comparación están reaccionados con las características propias de cada modelo de compresión así tenemos:

	Tipo de Compresión	Calidad de la imagen	Simetría	Perdida	Algoritmo matemático	Tamaño de Los archivos	Patentes	Aplicaciones
JPEG	Espacial	Grande	Simétrica	Con perdida	DTC	Grande	libre	Fotografía, captura, almacenamiento, transmisión, etc.
M-JPEG	Espacial	Grande	Simétrica	Con perdida	DTC	Grande	Libre	Transmisión de video
MPEG	Espacial y temporal	Pequeña	Asimétrica	Con perdida	DTC	Pequeños	Libre	Transmisión con calidad TV
H261/H263	Espacial y temporal	Pequeña	Asimétrica	Con perdida	DTC	Pequeños	Libre	Videoconferencia

Tabla III.7 Comparación cualitativa de los formatos de compresión de video

	Tipo de resolución	Matriz	Ratio	Ancho de banda (Mbps)	Imágenes por segundo
JPEG	320X240	8X8	20:01		
M-JPEG	640X480	8X8	20:1 Y 40:1	2,5	25
MPEG	720X576	16X16	100:1 variable	1,86	30
H261/H263	352X288	8X8	100:01:00	0,546	20

Tabla III.8 Comparación cuantitativa de los formatos de compresión de video

Interpretación

En la tabla III.7 podemos ver la comparación cualitativa de las diferentes formatos de compresión en la que se exponen las similitudes y diferencias entre ellas dándonos cuenta de que existen parámetros cuantitativos como el Algoritmo Matemático y la Perdida que no varían indiferentemente de la técnica de compresión; Mientras que otros cambian de una técnica a otra, esta variación depende a Aplicación en la que se vayan a aplicar.

En la tabla III.8 se expone una comparación cuantitativa de los parámetros que asi lo permiten; En la cual hemos de darnos cuenta en forma general todos ellos cambian de una técnica a otra, esto se debe primordialmente al grado evolutivo que han tenido cada uno de ellos.

3.5. Elección del formato de compresión para video-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 necesita la utilización de un formato que no utilice mucho ancho de banda de la red ya que existen otros servicios que convergen 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 optimo en la aplicación.

Ubicándonos en el ámbito de desarrollo práctico de la aplicación de la tesis hemos considerado que el formato de compresión que mejor se ajusta a los requerimientos de video-vigilancia-IP es el MPEG, ya que permite una calidad 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.

3.6. Análisis de un sistema de video-vigilancia–IP

Dentro del ámbito de desarrollo de la tesis, ahora nos enfocaremos en analizar como incorporar el hardware necesario para video-vigilancia-IP a la infraestructura de red existente.

Luego de lo estudiado en el Capitulo II, donde se enfatiza que lo necesario para incorporar las cámaras de red es que exista una infraestructura de red establecida previamente, vamos a analizar cada uno de las consideraciones para agregar las cámaras de red esta infraestructura existe

En la situación actual, no existe un sistema de video vigilancia de ningún tipo, al cual se pueda evolucionar hacia un sistema digital. Por lo que simplemente incorporaremos las cámaras de red a un punto de conexión dentro de la LAN.

Se puede configurar la cámara de red para que reconozca una IP dinámica asignada por el DHCP para la Lan o Vlan a la que pertenezca ese punto de conexión, con lo que ya se incorpora automáticamente a ellas.

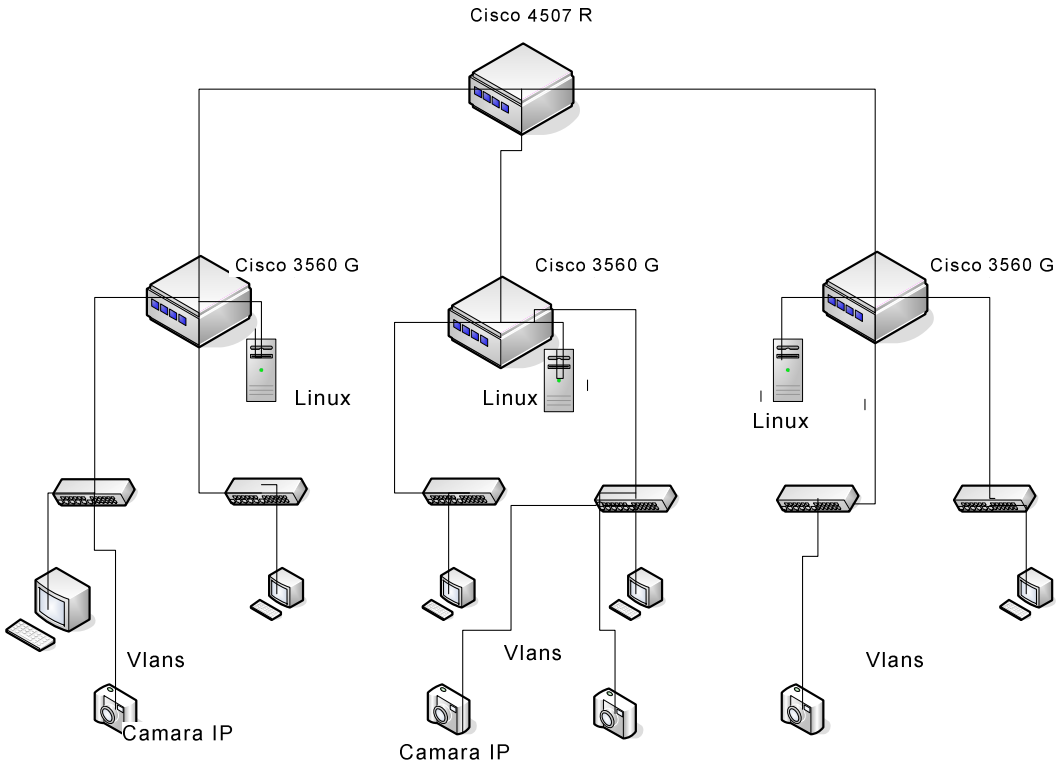


Figura III.35 Esquema lógico que incorpora cámaras de red.

Consideraciones de ancho de banda:

La transmisión de Video-IP con una cámara utiliza un ancho de banda de 0.28 Mbps como se muestra en la figura III.36. Para determinar el impacto que este tipo de tráfico producirá en forma general en la red del esquema anterior, será necesario analizar el ancho de banda disponible en cada una de las Vlans por donde se transmitirá el video-IP hasta llegar a la aplicación de visualización, de esta manera también se podrá establecer el numero de cámaras que pueden incorporarse en cada Vlan. Así podemos calcular el impacto en el ancho de banda que sufrirá la red en la implementación de video-IP de la manera siguiente:

Impacto = (ancho de banda necesario /Ancho de banda disponible) x 100%

Ancho de banda necesario = (Numero de cámaras) x (0.28 Mbps)

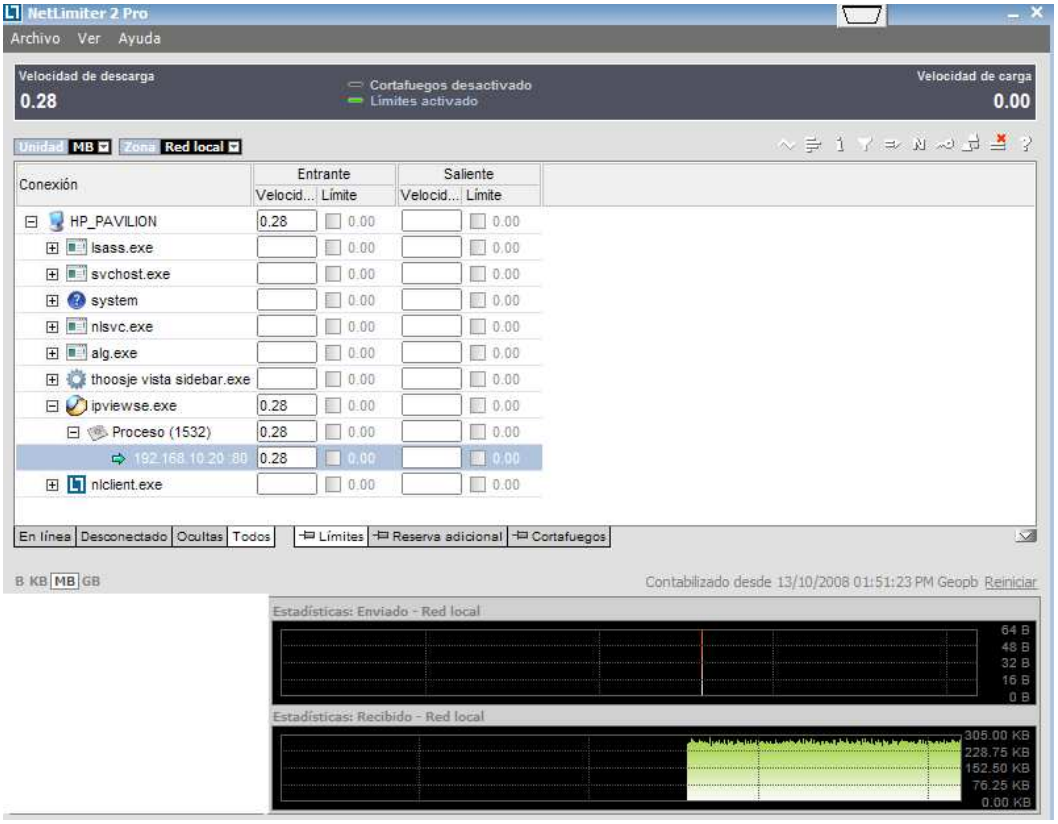


Figura III.36 Medición del ancho de banda para Video-IP.

CAPITULO IV

DESARROLLO DEL SISTEMA DE VIDEO-VIGILANCIA-IP

4.1. Introducción

Se trata del desarrollo de un sistema informático para la video-vigilancia-IP, que se caracteriza por ser software dedicado es un sistema de vídeo abierto, combinado con los beneficios de las imágenes digitales a través de la red IP de la ESPOCH y cámaras de red, constituye un medio de vigilancia y monitorización remota mucho más efectivo los sistema tradicionales Circuitos cerrados de televisión CCTV. 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.

4.2. Definición de casos de uso de formato expandido

Definimos los siguientes casos de uso:

Modulo De Administración

Caso de Uso 1: Autenticación del usuario

Actores: Administrador.

Propósito: Autentificar los usuarios.

Visión General: Autentificarse cada uno de los usuarios para acceder al sistema con diferentes propósitos ya sea de configuración o utilización del sistema

Tipo: Primario

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El Usuario solicita ingreso al sistema.	b) Solicitar nombre y contraseña.
c) El Usuario ingresa los datos para ingresar al sistema.	d) Valida nombre y contraseña.
	e) Presenta página de inicio del usuario.
f) El Usuario selecciona opción	g) Presenta información seleccionada.

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

d.3) Presenta recordatorio de clave para usuario.

Caso de Uso 2: Creación de Cuentas de Usuario.

Actores: Administrador (Iniciador).

Propósito: Crear una cuenta para cada usuario del sistema

Visión General: El Administrador crea los diferentes cuentas para usuarios según su nivel de seguridad o responsabilidad (tipo de usuario).

Tipo: Primario

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre y contraseña.
c) El Administrador ingresa sus datos.	d) Valida nombre y contraseña.
	e) Presenta página de creación Cuentas de usuario.
f) El Administrador ingresa datos de creación de Cuentas de Usuario.	g) Almacena datos en la base de datos.
h) El Administrador confirma.	i) Crear Cuenta de Usuario.

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de Uso 3: Actualización de Cuentas de Usuario

Actores: Administrador (Iniciador).

Propósito: Proponer la actualización de una Cuenta de Usuario.

Visión General: El Administrador Actualiza dada una cuenta de usuario según datos nuevos o responsabilidades.

Tipo: Primario

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre y contraseña.
c) El Administrador ingresa sus datos.	d) Valida nombre y contraseña.
	e) Presenta página de actualización Cuentas de usuario.
f) El Administrador ingresa datos de actualizar Cuentas de usuario.	g) Almacena datos en la base de datos.
h) El Administrador confirma actualización Cuentas de usuario	i) Actualiza Cuentas de usuario

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de uso 4: Eliminación de Cuentas de Usuario

Actores: Administrador (Iniciador)

Propósito: eliminar una cuenta de usuario.

.Visión General: El Administrador Elimina dada una cuenta de usuario según el criterio de suspensión de cuenta.

Tipo: Primario

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre y contraseña.
c) El Administrador ingresa sus datos.	d) Valida nombre y contraseña.
	e) Presenta página de eliminación de Cuentas de usuario
f) El Administrador ingresa datos de eliminar Cuentas de usuario.	g) elimina datos en la base de datos.
h) El Administrador confirma eliminación Cuentas de usuario	i) Elimina Cuentas de usuario

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de uso 5: Creación de unidad departamental (departamento).

Actores: Administrador (Iniciador)

Propósito: ingresar al sistema los departamentos existentes en la ESPOCH.

Visión General: El Administrador solicita ingresar al sistema un departamento (ejemplo; Desitel) con el propósito de que conste en el sistema de video vigilancia para su posterior monitorización.

Tipo: Primario.

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre y contraseña.
c) El Administrador ingresa sus datos.	d) Valida nombre y contraseña.
	e) Presenta página creación de Departamento
f) El Administrador ingresa datos de creación de departamento	g) Almacena datos en la base de datos
h) El Administrador confirma creación de Departamento	i) Creación de Departamento

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de uso 6: Actualización de unidad departamental (departamento).

Actores: Administrador (Iniciador)

Propósito: Actualizar datos de los departamentos existentes en la ESPOCH.

Visión General: El Administrador solicita actualizar los datos en el sistema de un departamento especifico (ejemplo; Desitel).

Tipo: Primario.

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre y contraseña.
c) El Administrador ingresa sus datos.	d) Valida nombre y contraseña.

	e) Presenta página Actualización de Departamento
f) El Administrador ingresa datos de actualización de departamento	g) Almacena datos en la base de datos
h) El Administrador confirma Actualización de Departamento	i) Actualiza Departamento

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de uso 7: Eliminación de unidad departamental (departamento).

Actores: Administrador (Iniciador)

Propósito: eliminar un departamento.

.Visión General: El Administrador elimina un departamento según el criterio de suspensión.

Tipo: Primario

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre y contraseña.
c) El Administrador ingresa sus datos.	d) Valida nombre y contraseña.

	e) Presenta página de eliminación de departamento
f) El Administrador ingresa datos de eliminar departamento.	g) elimina datos en la base de datos.
h) El Administrador confirma eliminación departamento	i) Elimina departamento

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de uso 8: Creación de unidad de vigilancia (Cámara)

Actores: Administrador (Iniciador)

Propósito: ingresar al sistema las cámaras de vigilancia.

Visión General: El Administrador solicita ingresar al sistema una unidad de vigilancia (cámara) a un departamento especifico (ejemplo; Desitel) con el propósito de que conste en el sistema de video vigilancia para su posterior monitorización.

Tipo: Primario.

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre y contraseña.
c) El Administrador ingresa sus datos.	d) Valida nombre y contraseña.
	e) Presenta página creación de Cámara
f) El Administrador ingresa datos de creación de Cámara	g) Almacena datos en la base de datos

h) El Administrador confirma creación de Cámara	i) Creación de Cámara

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de uso 9: Actualización de una unidad de vigilancia (Cámara).

Actores: Administrador (Iniciador)

Propósito: Actualizar datos de Cámaras existentes en un departamento.

Visión General: El Administrador solicita actualizar los datos en el sistema Cámaras existentes en un departamento (ejemplo; Desitel).

Tipo: Primario.

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre y contraseña.
c) El Administrador ingresa sus datos.	d) Valida nombre y contraseña.
	e) Presenta página Actualización de Cámara
f) El Administrador ingresa datos de actualización de Cámara	g) Almacena datos en la base de datos
h) El Administrador confirma Actualización de Cámara	i) Actualiza Cámara

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de uso 10: Eliminación de una unidad de vigilancia (Cámara).

Actores: Administrador (Iniciador)

Propósito: eliminar una Cámara.

.Visión General: El Administrador elimina una Cámara según el criterio de suspensión.

Tipo: Primario

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre y contraseña.
c) El Administrador ingresa sus datos.	d) Valida nombre y contraseña.
	e) Presenta página de eliminación de Cámara
f) El Administrador ingresa datos de eliminar Cámara.	g) elimina datos en la base de datos.
h) El Administrador confirma eliminación Cámara	i) Elimina Cámara

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Modulo De Usuario (Vigilante)

Caso de Uso 1: Monitorización de un área específica.

Actores: Vigilante (iniciador).

Propósito: Acceder a la visualización que de una cámara especifica.

Visión General: El vigilante accede al sistema para poder monitorizar lo que una cámara del sistema de vigilancia presenta como video en vivo. Para ello accede al mapa de la ESPOCH, escoge un lugar geográfico (manzana) que desea monitorizar, y escoge una cámara específica de un departamento escogido.

Tipo: Primario.

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El vigilante solicita acceder al sistema	b) Solicita su nombre y contraseña.
c) El vigilante ingresa sus datos.	d) Valida nombre y contraseña.
	e) Verifica su existencia en la Base de Datos.
f) El vigilante escoge una manzana, y accede a una cámara de un departamento escogido	g) muestra mapa de la ESPOCH. Despliega cámaras del departamento
h) El vigilante visualiza el video en vivo	i) Muestra video en vivo

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de Uso 2: Monitorización de varias cámaras a la vez de un departamento

Actores: Vigilante (iniciador).

Propósito: Acceder a la visualización de todas las cámaras de un departamento.

Visión General: El vigilante accede al sistema para poder monitorizar lo que varias cámaras de un departamento especifico presentan como video en vivo. Para ello accede al mapa de la ESPOCH, escoge un lugar geográfico (manzana) que desea monitorizar, y escoge un departamento específico.

Tipo: Primario.

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El vigilante solicita acceder al sistema	b) Solicita su nombre y contraseña.
c) El vigilante ingresa sus datos.	d) Valida nombre y contraseña.
	e) Verifica su existencia en la Base de Datos.
f) El vigilante escoge una manzana, y accede a un departamento especifico	g) muestra mapa de la ESPOCH. Despliega cámaras del departamento
h) El vigilante visualiza las cámaras del departamento	i) Muestra video en vivo de todas las cámaras del departamento.

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de Uso 3: Grabación de video

Actores: Vigilante (iniciador).

Propósito: Grabar la visualización de video.

Visión General: El vigilante accede al sistema para poder grabar lo que una o varias cámaras de un departamento específico presentan como video en vivo. Para ello accede al mapa de la ESPOCH, escoge un lugar geográfico (manzana) que desea monitorizar, y escoge un departamento específico.

Tipo: Primario.

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El vigilante solicita acceder al sistema	b) Solicita su nombre y contraseña.
c) El vigilante ingresa sus datos.	d) Valida nombre y contraseña.
	e) Verifica su existencia en la Base de Datos.
f) El vigilante escoge una manzana, y accede a un departamento especifico	g) muestra mapa de la ESPOCH. Despliega cámaras del departamento
h) El vigilante visualiza las cámaras del departamento y procede a la grabación de una o varias cámaras	i) Graba video en vivo de la o las cámaras seleccionadas en la base de datos.

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

d.3) Solo se puede grabar lo que se esta visualizando.

Caso de Uso 4: Recuperación de la Grabación de video

Actores: Vigilante (iniciador).

Propósito: visualizar una grabación de video.

Visión General: El vigilante accede al sistema para poder visualizar una grabación o captura de video, para ello accede a un archivo de grabaciones de un departamento especifico seleccionado, donde se muestran las grabaciones de todas las cámaras de dicho departamento y que se seleccionan para poder reproducir.

Tipo: Primario.

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El vigilante solicita acceder al sistema	b) Solicita su nombre y contraseña.
c) El vigilante ingresa sus datos.	d) Valida nombre y contraseña.
	e) Verifica su existencia en la Base de Datos.
f) El vigilante escoge una manzana, y accede a un departamento especifico	g) muestra solapa de grabaciones de las cámaras del departamento
h) El vigilante escoge lel archivo que desea reproducir	i) reproduce video grabado del archivo seleccionado.

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

4.3. Definir los diagramas de caso de uso y refinar los casos de uso definidos.

Modulo De Administración

Diagrama Autenticación de Usuario

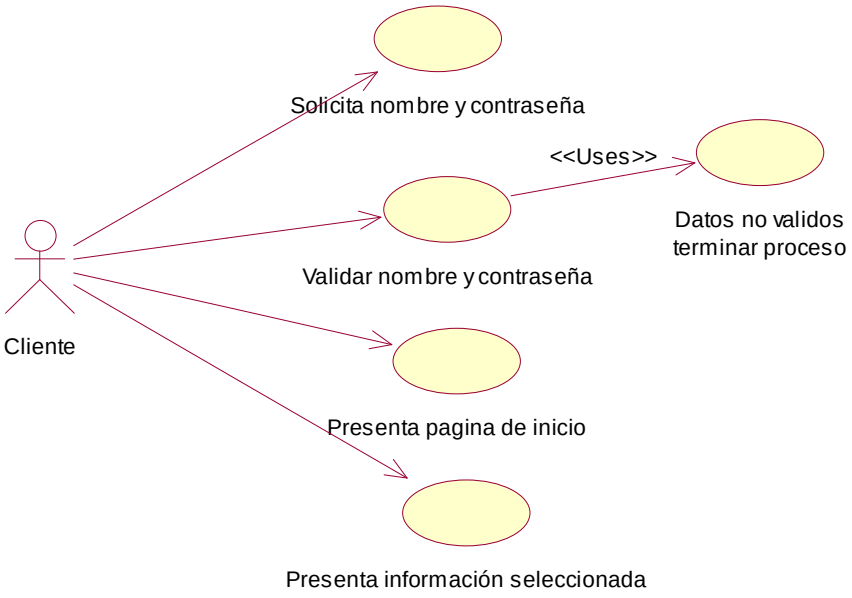


Diagrama Creación de Cuentas de Usuario.

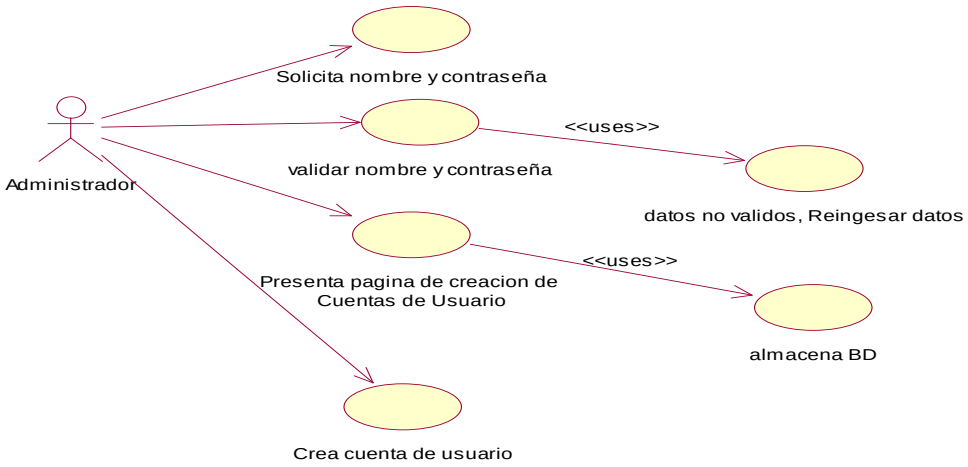


Diagrama Actualización de Cuentas de Usuario

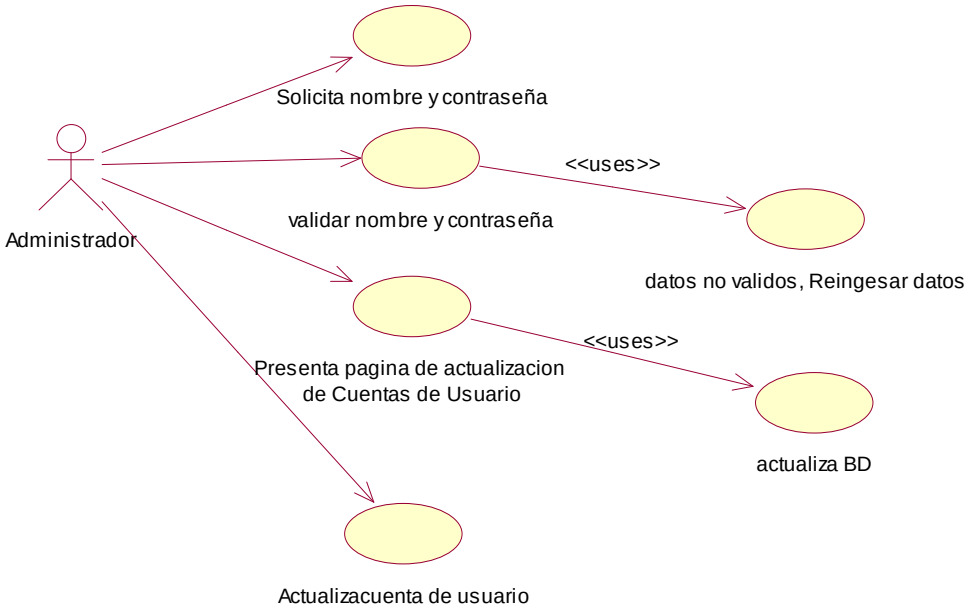


Diagrama Eliminación de Cuentas de Usuario

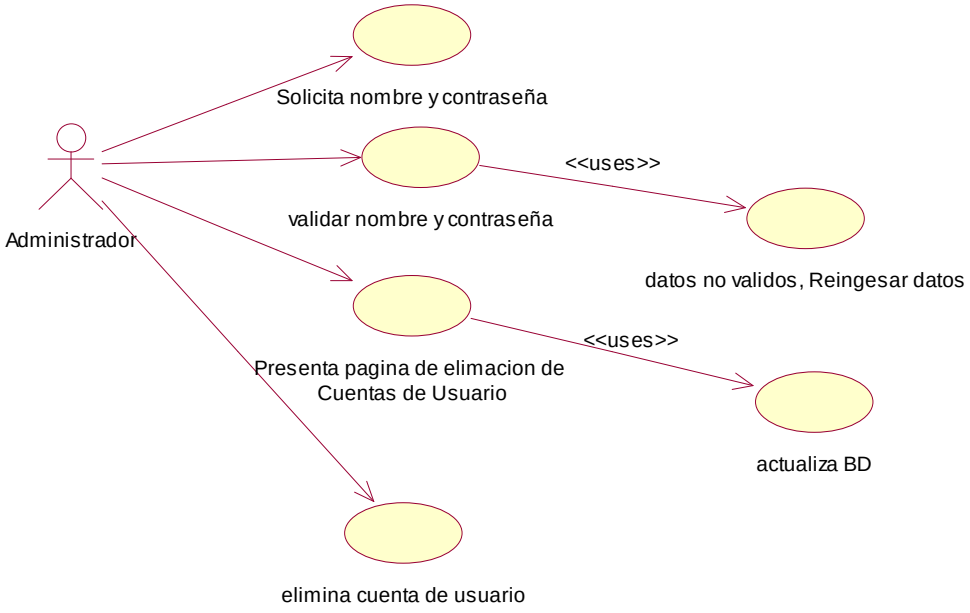


Diagrama Creación de unidad departamental (departamento).

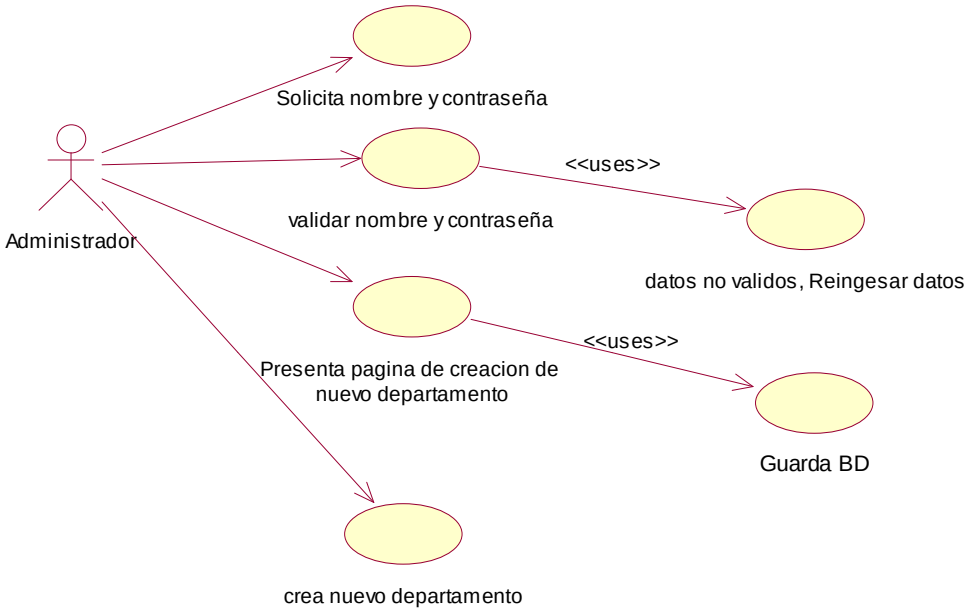


Diagrama Actualización de unidad departamental (departamento).

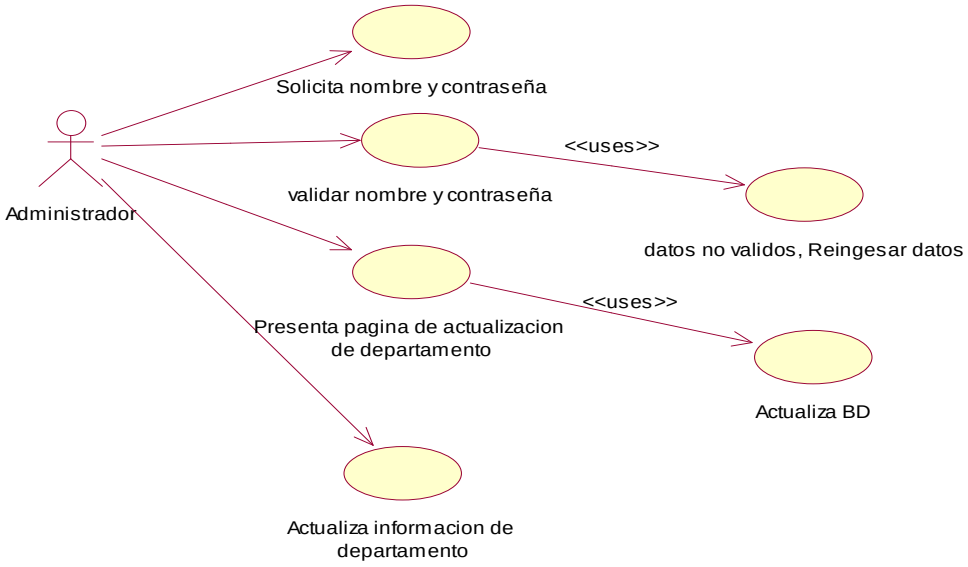


Diagrama Eliminación de unidad departamental (departamento).

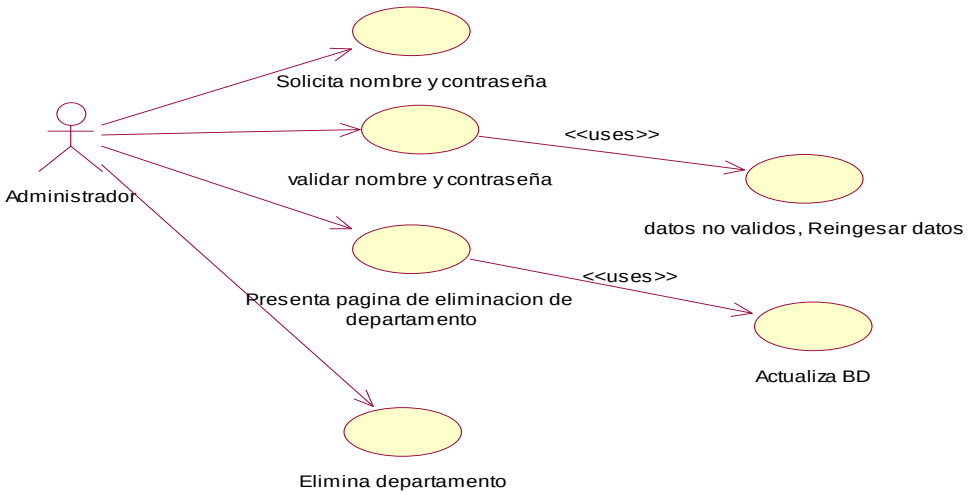


Diagrama Creación de unidad de vigilancia (Cámara)

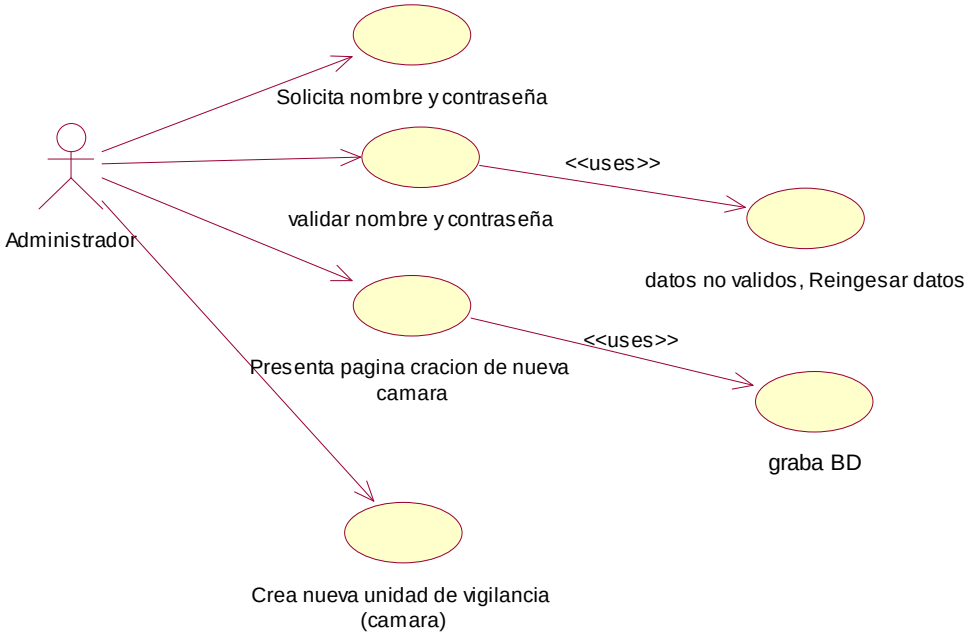


Diagrama Actualización de unidad de vigilancia (Cámara)

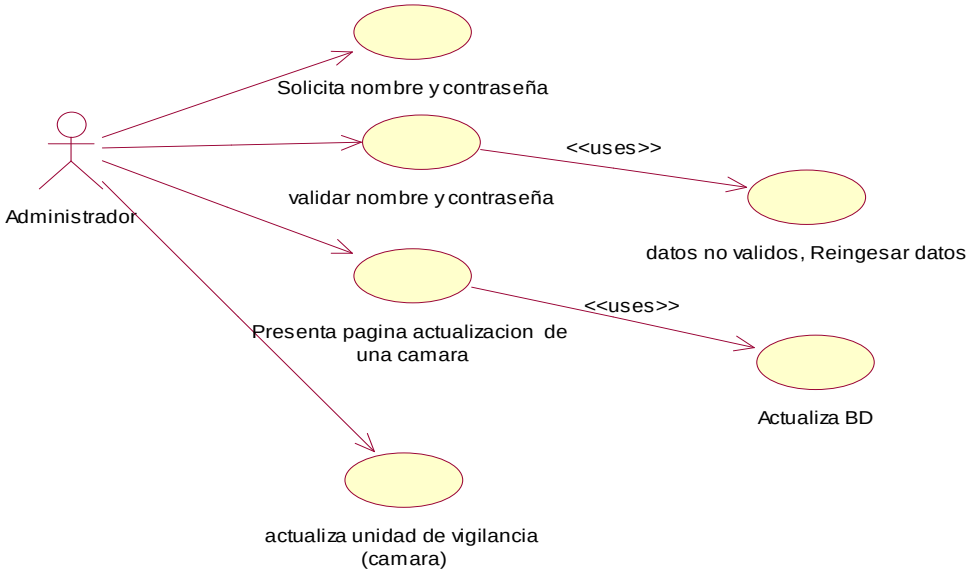
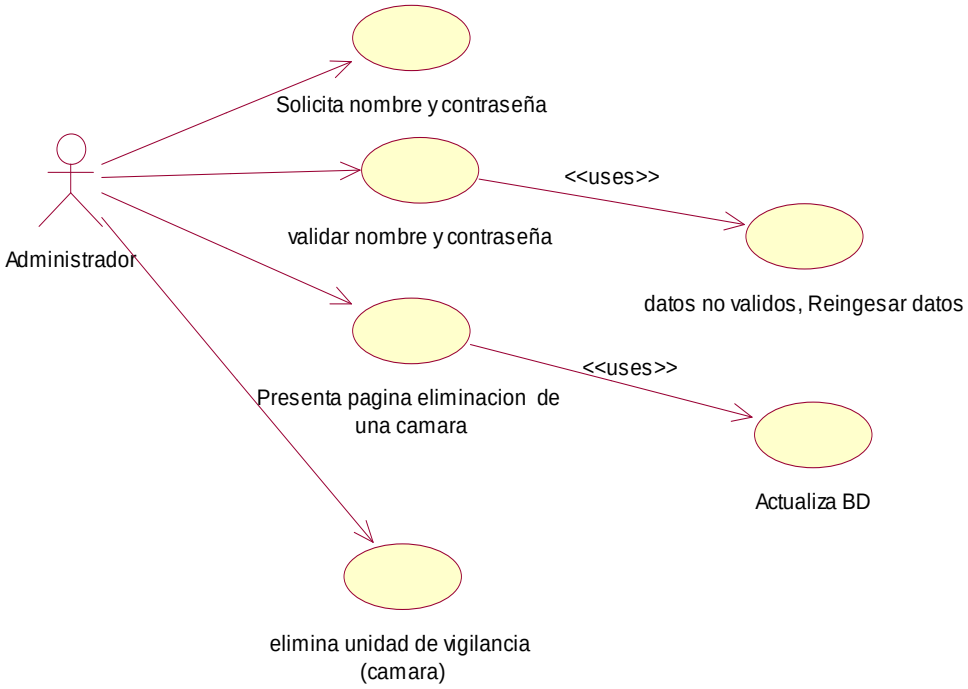


Diagrama eliminación de unidad de vigilancia (Cámara)



Modulo De Usuario (Vigilante)

Diagrama Monitorización de un área específica.

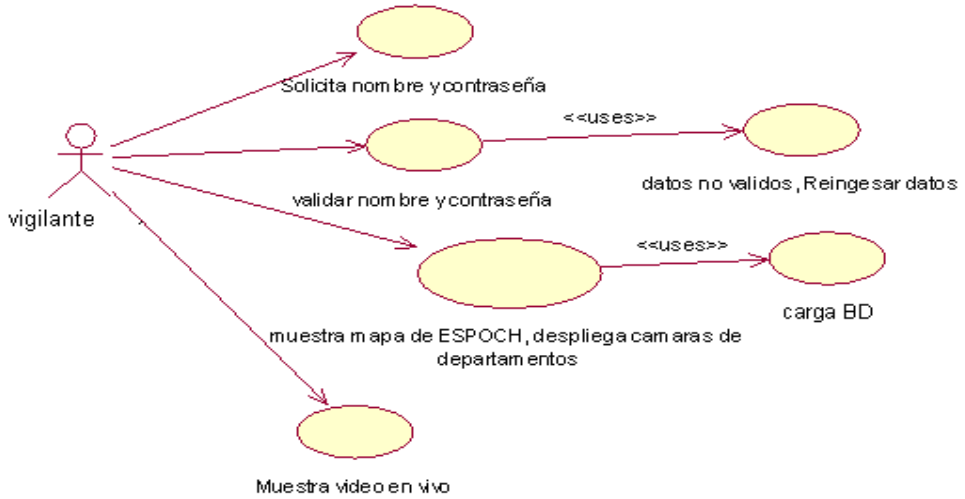


Diagrama Monitorización de varias cámaras a la vez de un departamento

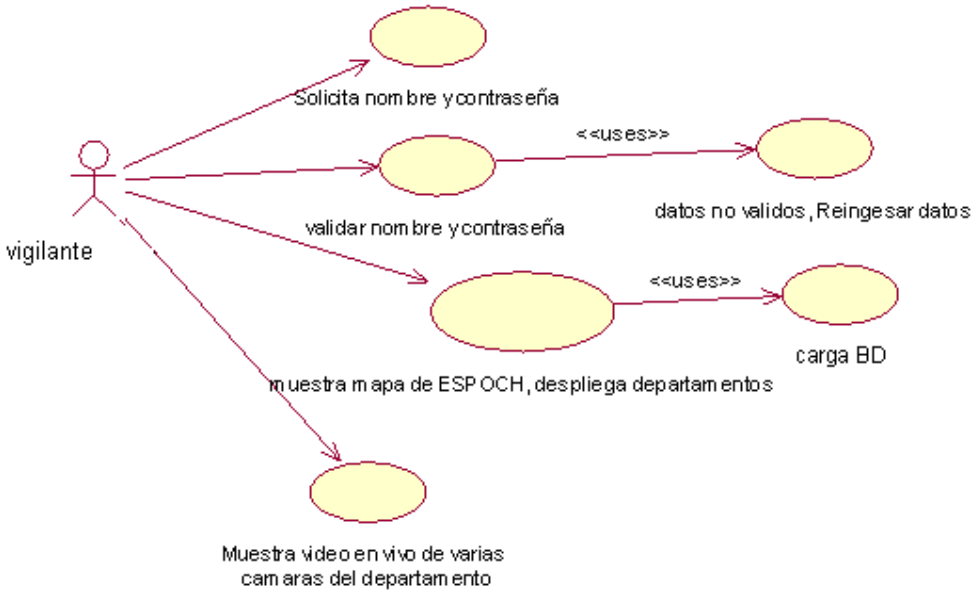


Diagrama Grabación de video

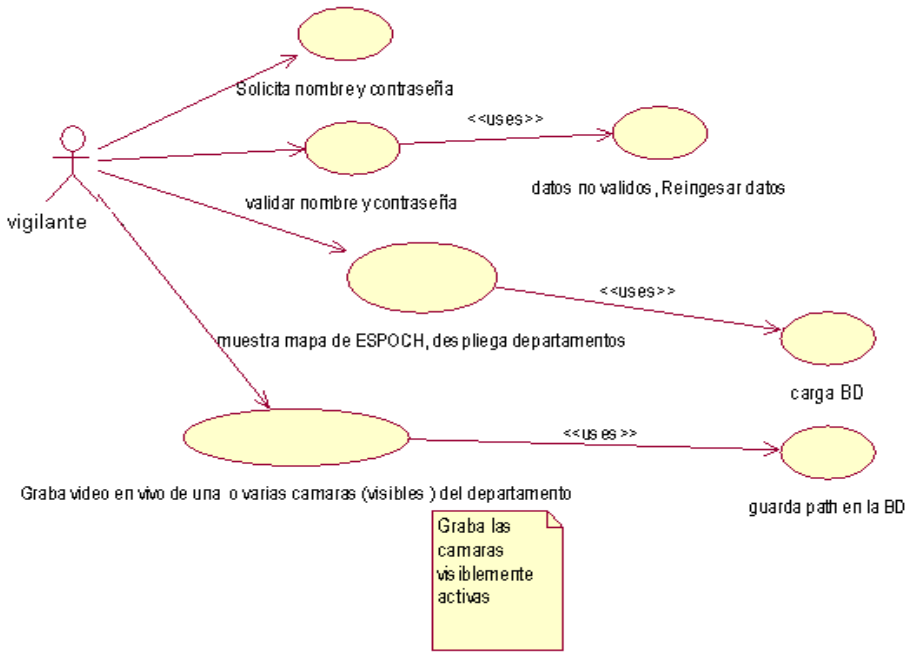
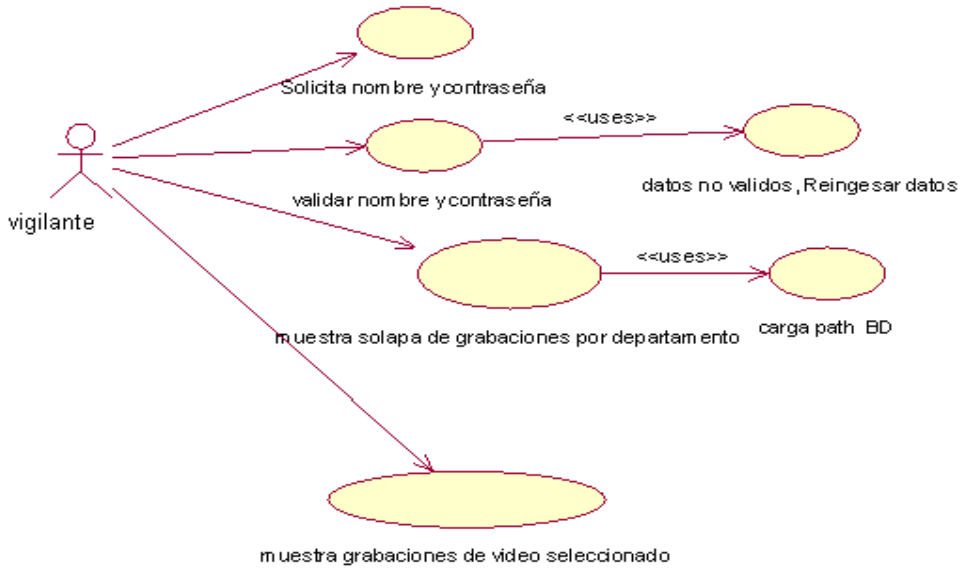
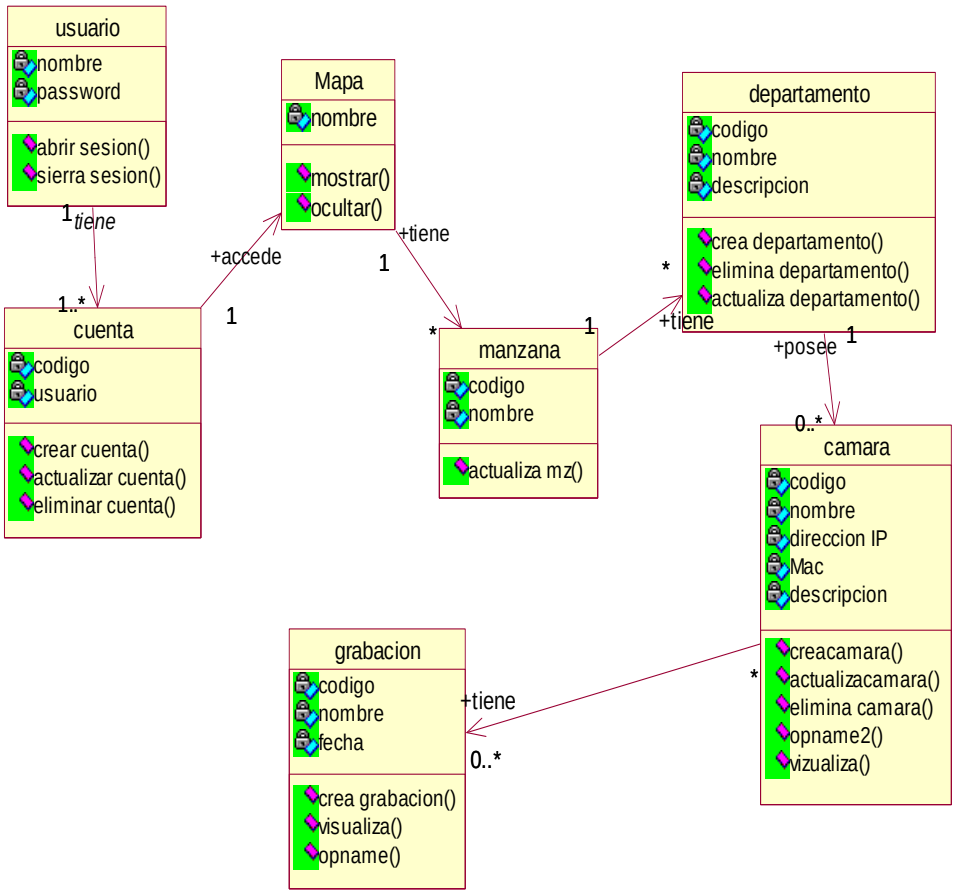


Diagrama Recuperación de la Grabación de video



4.4. Definir y refinar el diagrama clases (modelo conceptual)

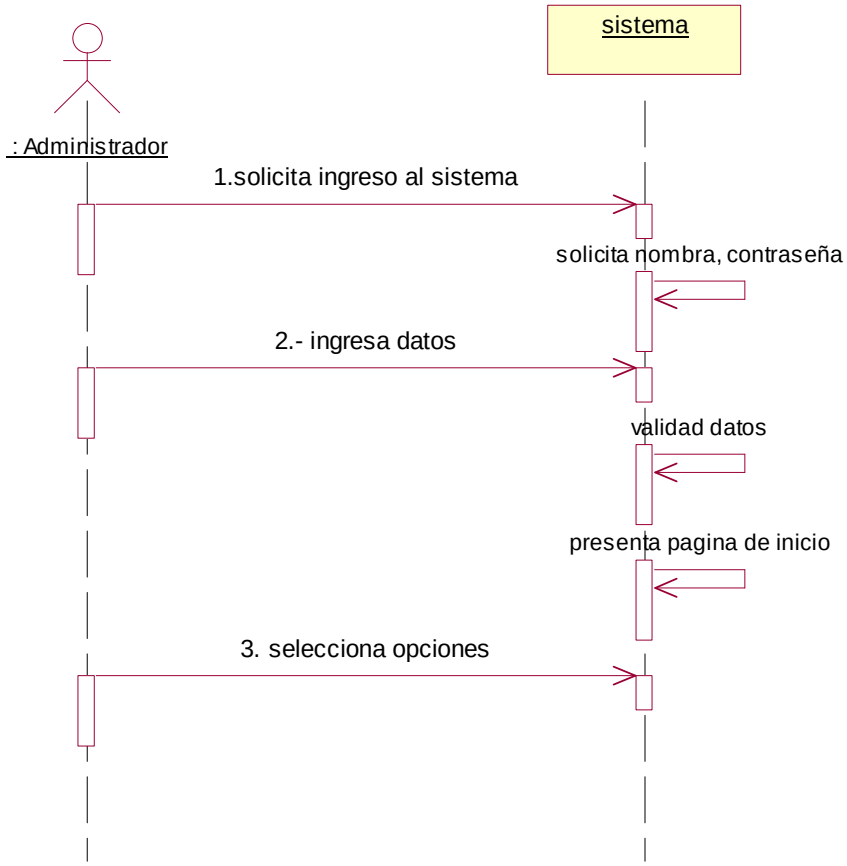


4.5. Definir y refinar el glosario de términos o diccionario de objetos.

TERMINO	CATEGORÍA	DESCRIPCIÓN
Administrador	Definición	Usuario encargado de gestionar la administración del sistema.
vigilante	Definición	Usuario que utiliza el sistema con motivos de monitorización y vigilancia.
Departamento	Definición	Cualquier Unidad departamental de la ESPOCH (ejemplo. DESITEL)
Cámara	Definición	Dispositivo electrónico de captura de video en vivo
Monitorización	Definición	Visualización del video para control
Creación de cuentas de usuario.	Caso de Uso	Crear cuentas de usuario para un acceso diferenciado sistema.
Grabación de video	Caso de Uso	Permite grabar el video que esta siendo visualizado.
Recuperación de una grabación	Caso de Uso	Ver un video que ha sido previamente grabado por una cámara
Actualización de cuentas de usuario.	Caso de Uso	Actualizar datos de un usuario.

4.6. Definir Los Diagramas De Secuencia

Diagrama Autenticación de Usuario



Modulo De Administración

Diagrama Creación de Cuentas de Usuario.

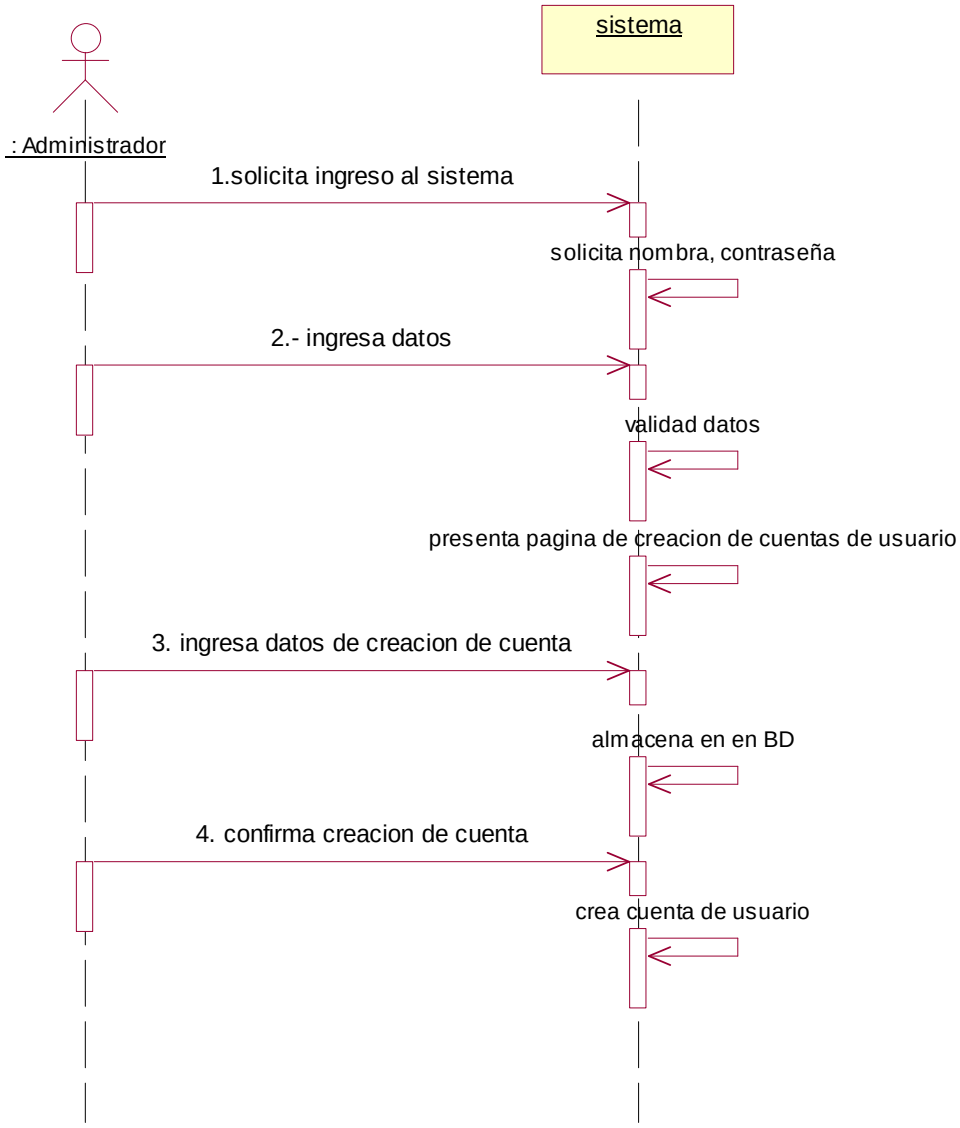


Diagrama Actualización de Cuentas de Usuario

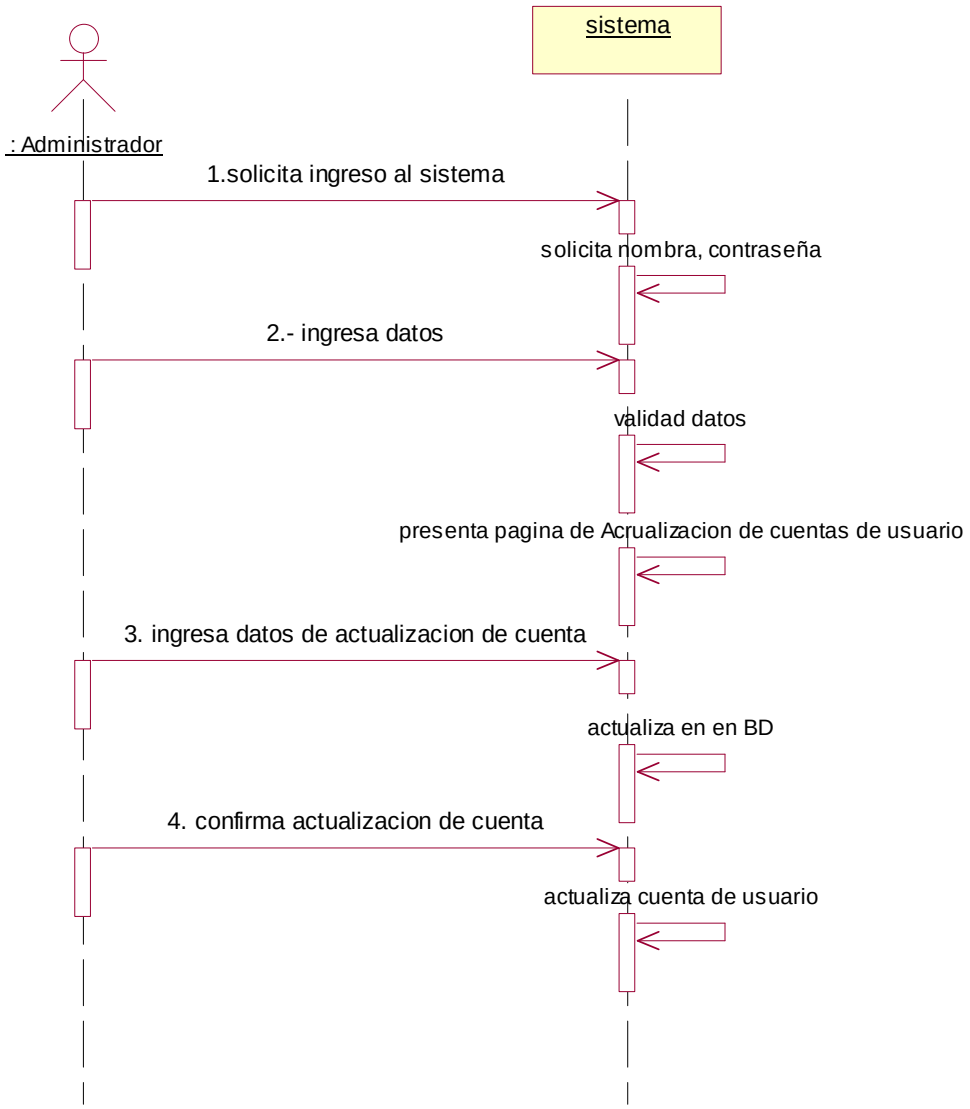


Diagrama Eliminación de Cuentas de Usuario

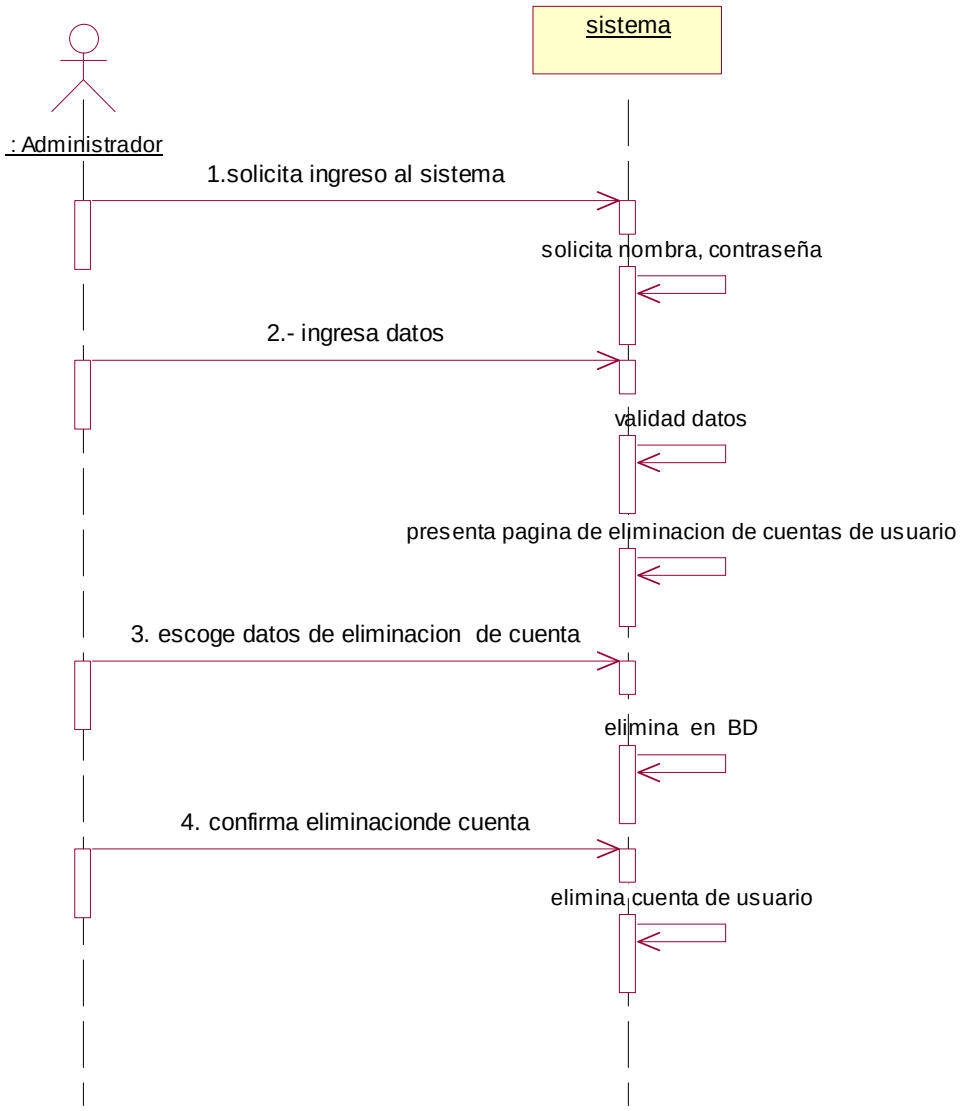


Diagrama Creación de unidad departamental (departamento).

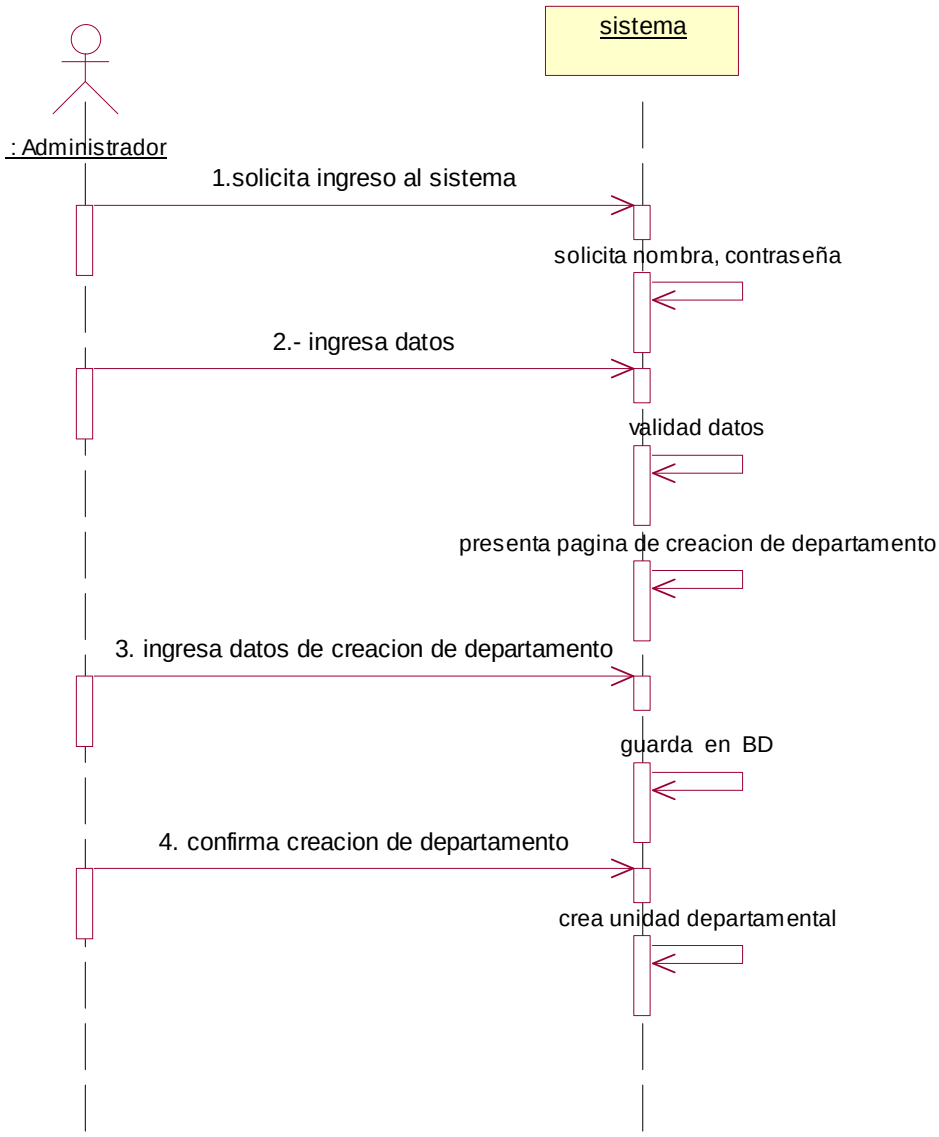


Diagrama Actualización de unidad departamental (departamento).

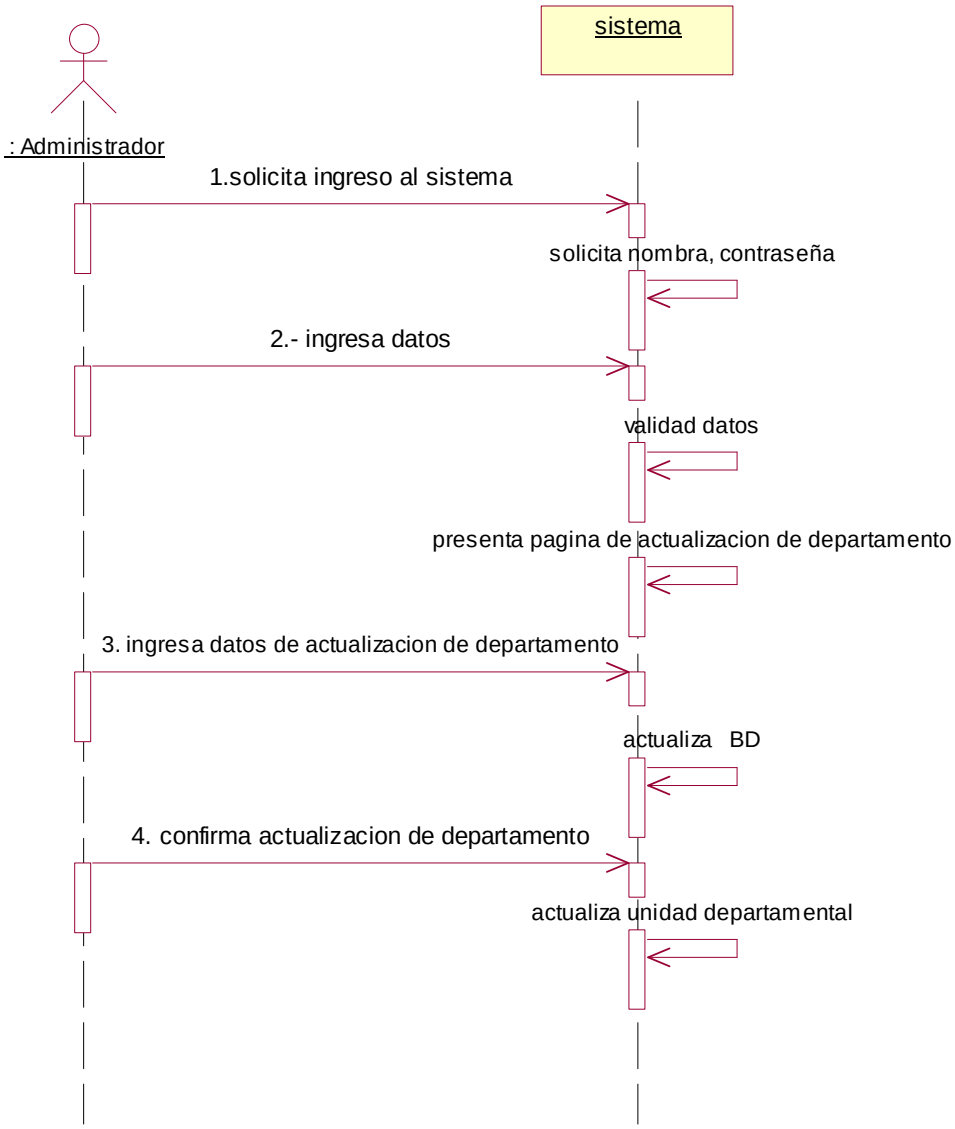


Diagrama Eliminación de unidad departamental (departamento).

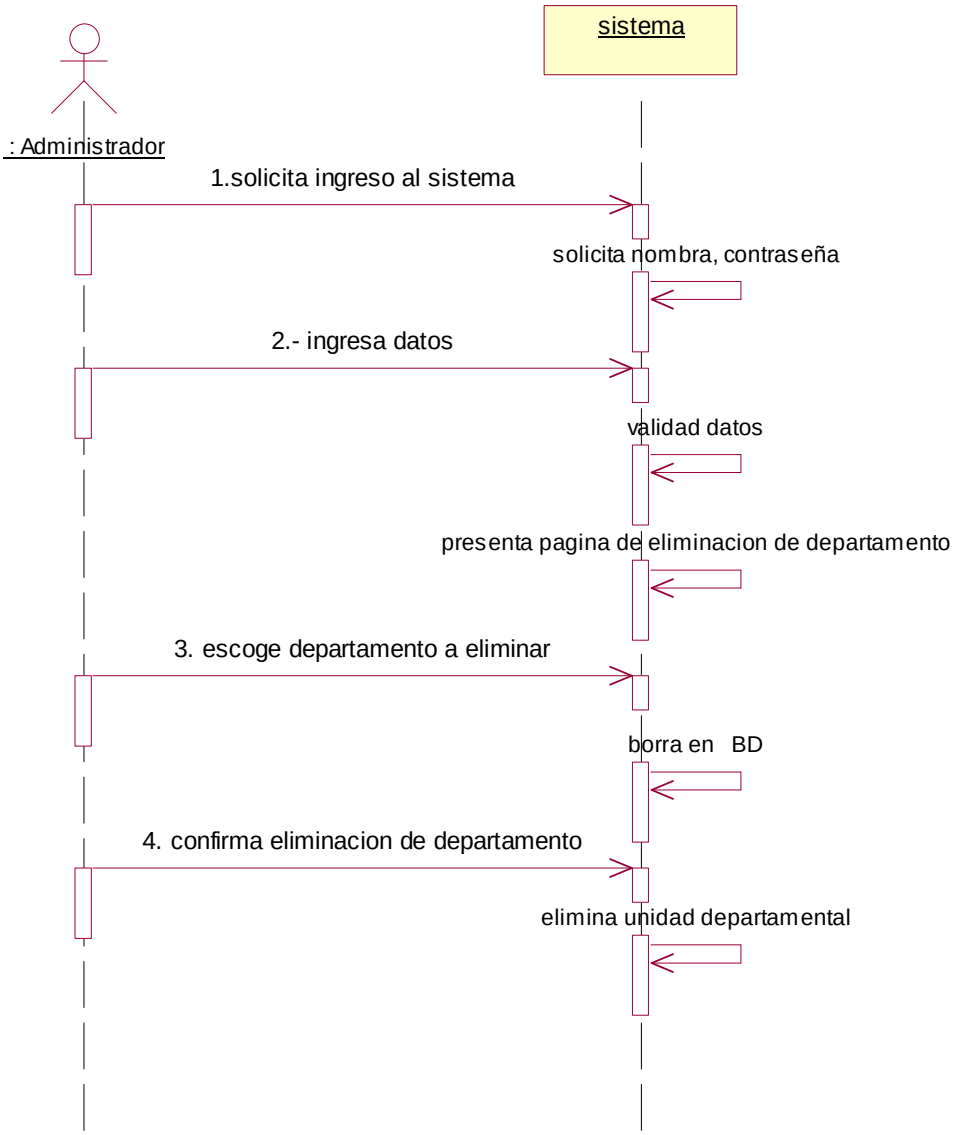


Diagrama Creación de unidad de vigilancia (Cámara)

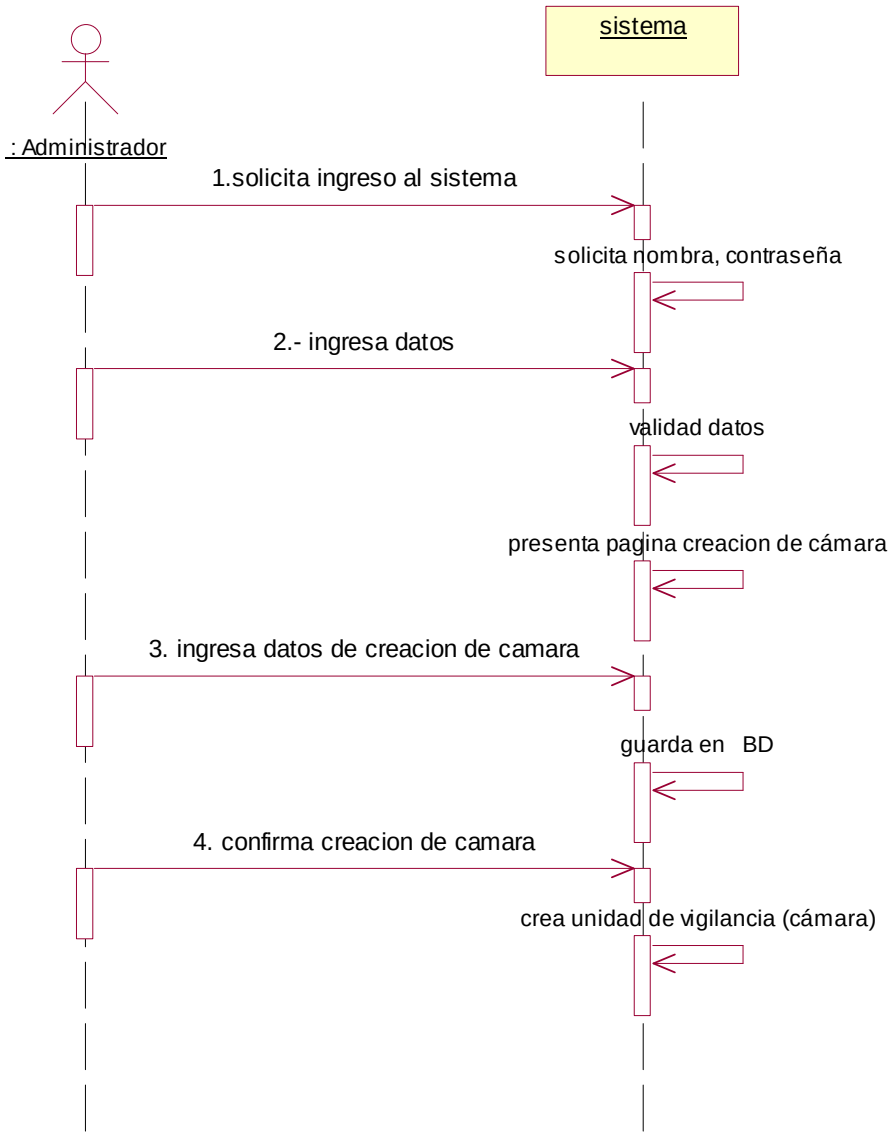


Diagrama Actualización de una unidad de vigilancia (Cámara).

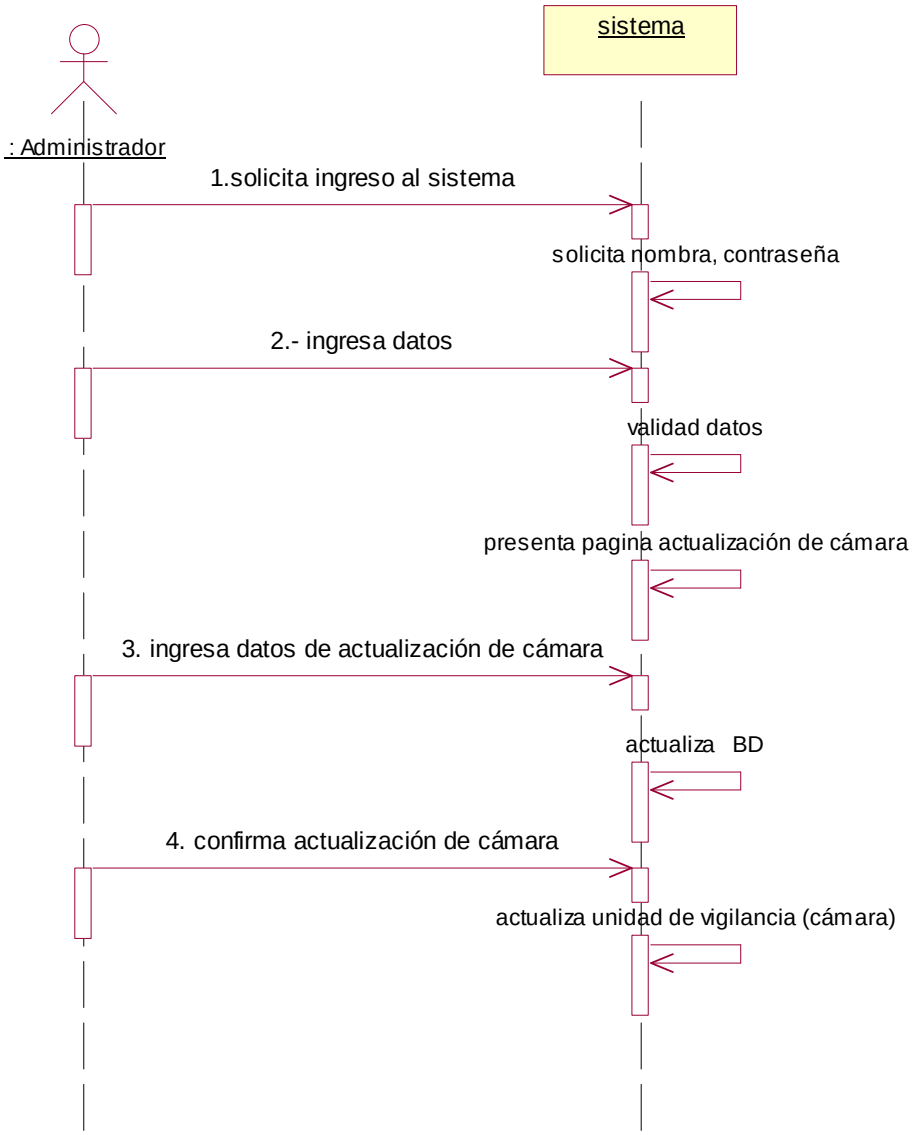
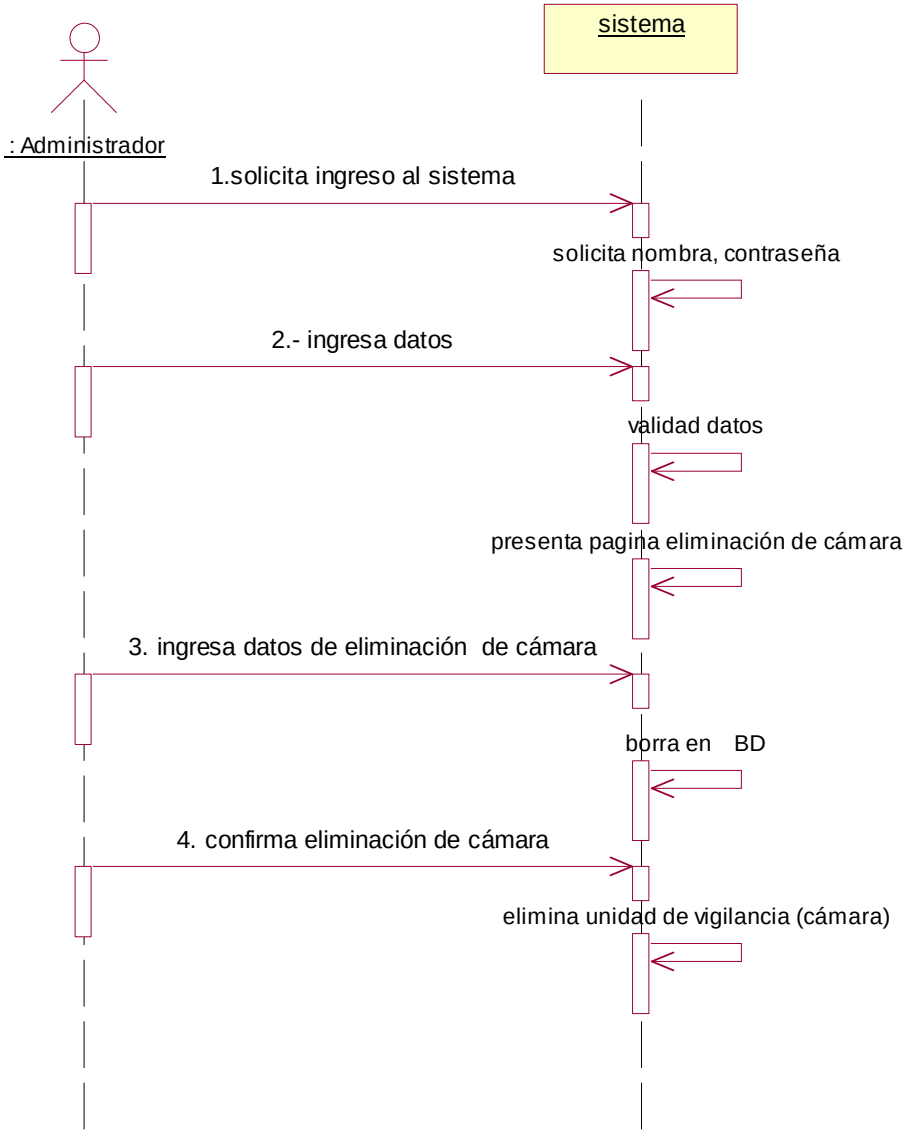


Diagrama Eliminación de una unidad de vigilancia (Cámara).



Modulo De Usuario (Vigilante)

Diagrama Monitorización de un área específica.

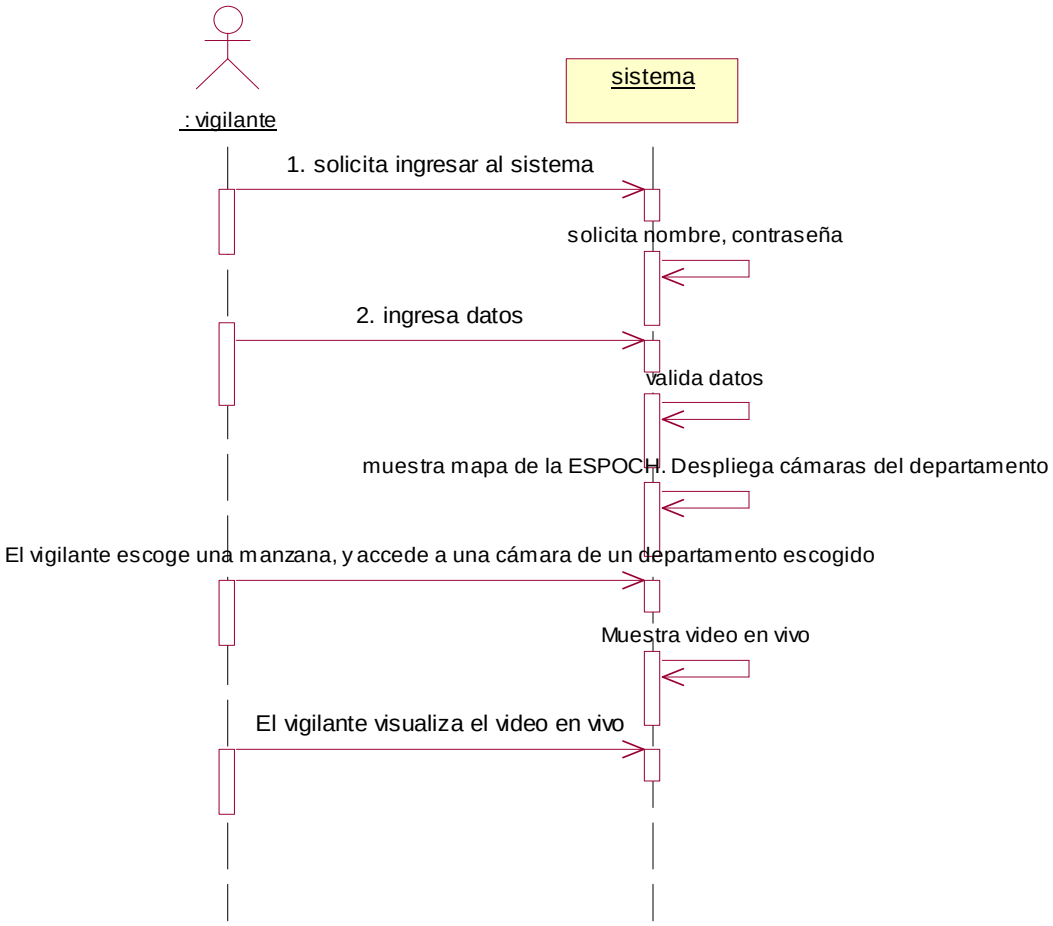


Diagrama Monitorización de varias cámaras a la vez de un departamento

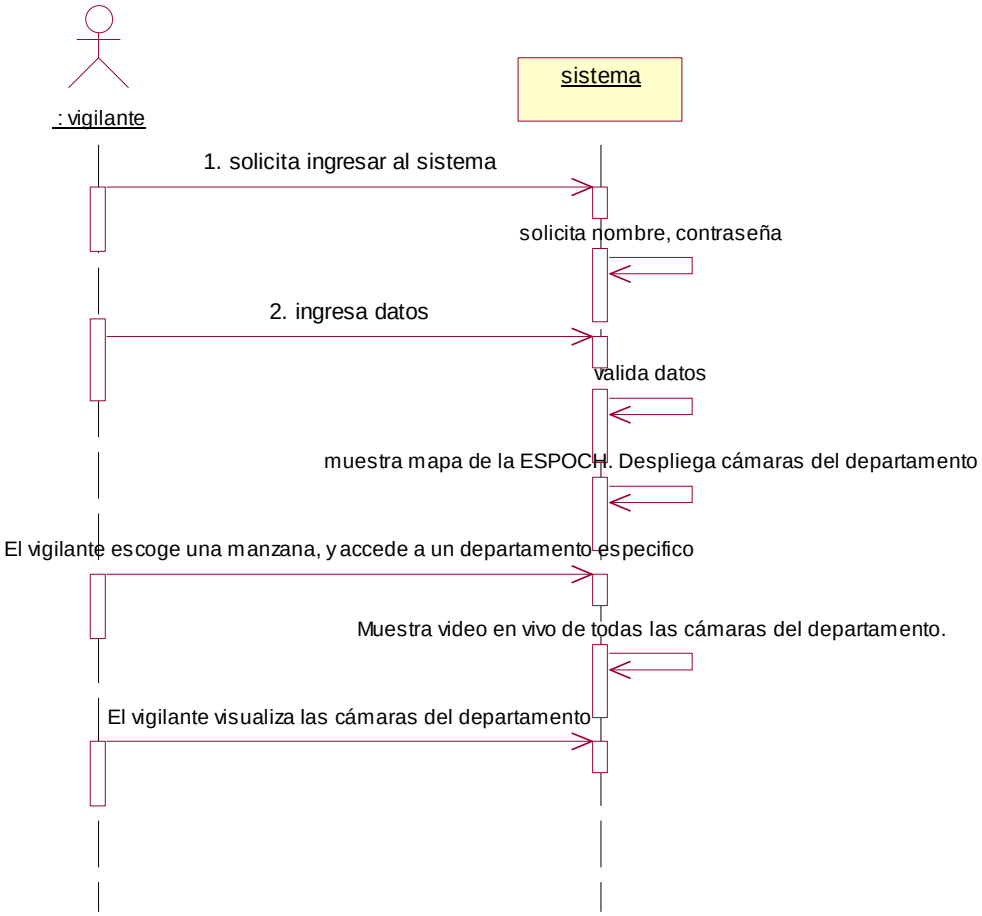


Diagrama Grabación de video

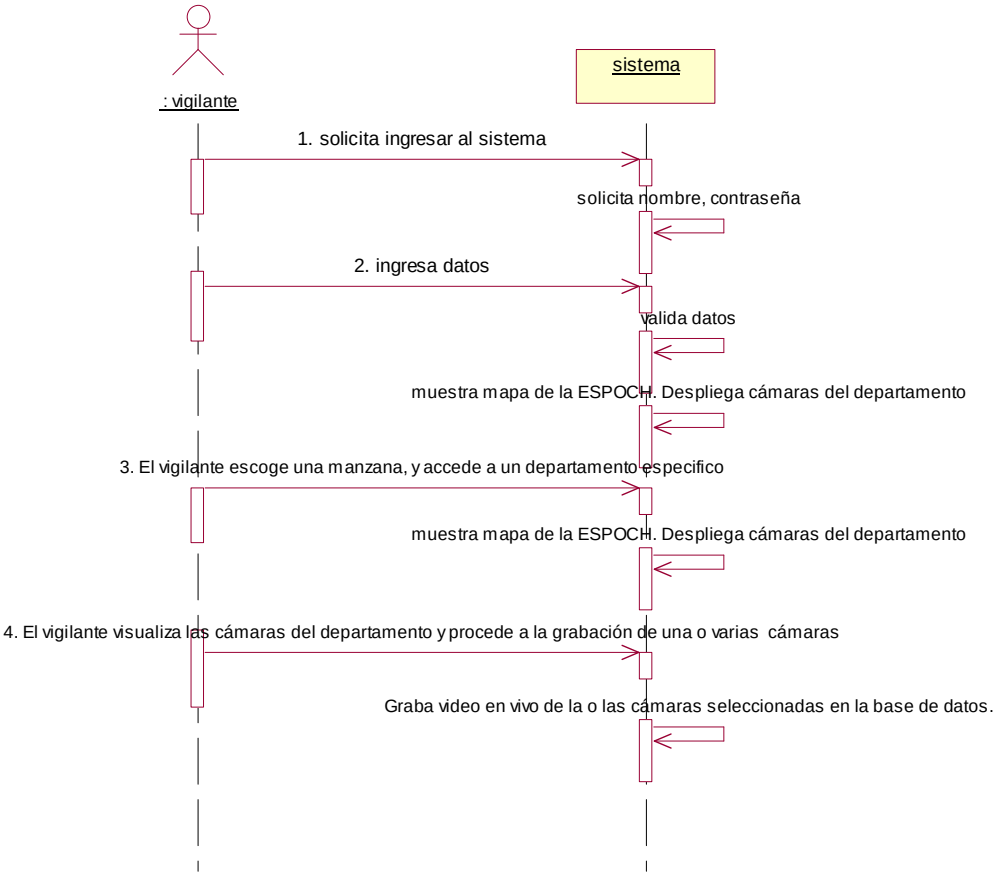
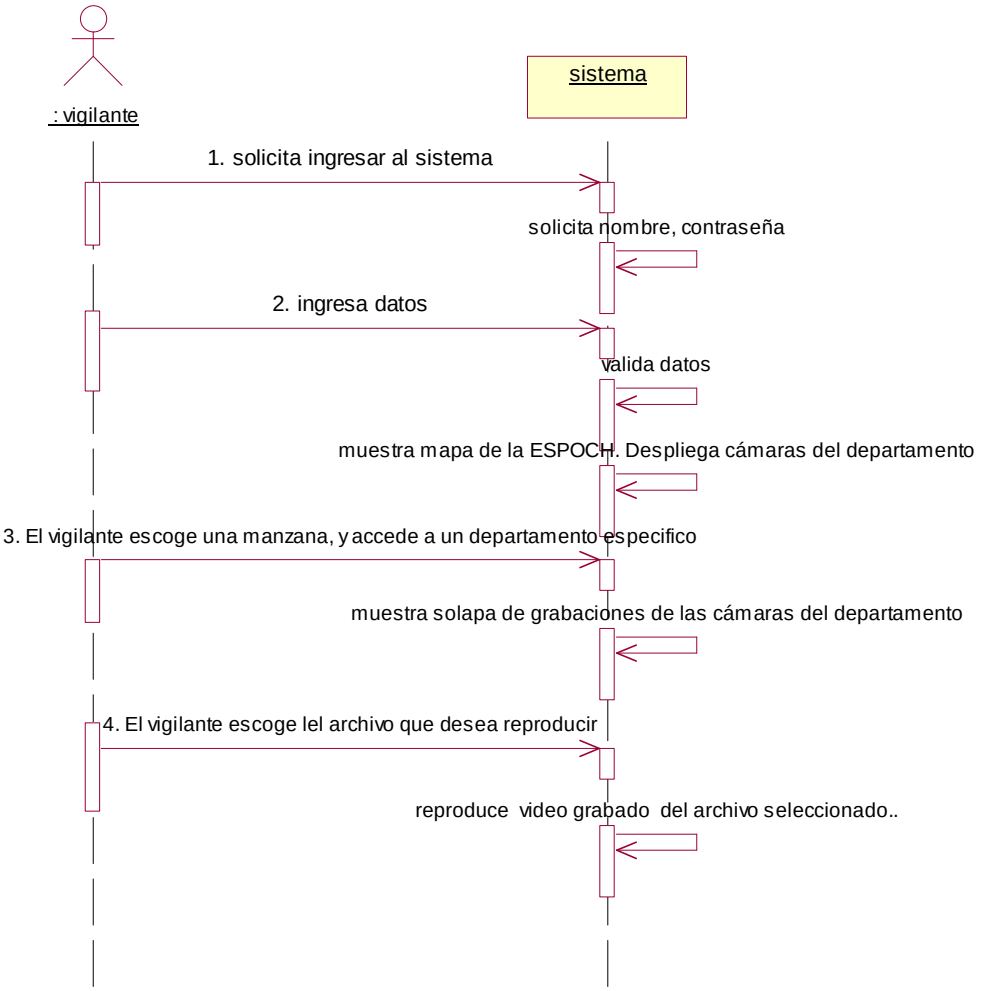


Diagrama Recuperación de la Grabación de video



4.7. Definir Los Contratos De Operación

Nombre	Autenticación del usuario.
Responsabilidades	Autenticación del usuario que requiere acceso al sistema.
Referencias Cruzadas	CU. CU2, Administrador.
Casos de Uso	Autenticación del usuario.
Notas	
Excepciones	Cualquier autenticada persona puede acceder al uso del servicio.
Salida	
Precondición	Personas en espera de creación de cuentas de usuario.
Poscondición	cuenta fue creado para acceder al uso.

Nombre	Creación de Cuentas de Usuario.
Responsabilidades	Crear una cuenta para cada usuario del sistema
Referencias Cruzadas	CU. CU3, Administrador.
Casos de Uso	Creación de Cuentas de Usuario.
Notas	
Excepciones	Solo administrador puede acceder a crear el servicio.
Salida	
Precondición	Personas en espera de ser creada cuenta.
Poscondición	Cuenta creada para acceder al uso.

Nombre	Actualización de Cuentas de Usuario
Responsabilidades	Proponer la actualización de una Cuenta de Usuario
Referencias Cruzadas	CU. CU4, Administrador.
Casos de Uso	Actualización de Cuentas de Usuario
Notas	
Excepciones	Solo administrador puede acceder a actualizar el servicio.
Salida	
Precondición	Personas en espera de ser actualizada su cuenta..
Poscondición	Cuenta actualizada para acceder al uso.

Nombre	Eliminación de Cuentas de Usuario.
Responsabilidades	eliminar una cuenta de usuario
Referencias Cruzadas	CU. CU5, Administrador.
Casos de Uso	Eliminación de Cuentas de Usuario
Notas	
Excepciones	Solo administrador puede acceder a eliminar la cuenta
Salida	
Precondición	Personas en espera de eliminada.
Poscondición	Usuario eliminado.

Nombre	Creación de unidad departamental (departamento).
Responsabilidades	ingresar al sistema los departamentos existentes en la ESPOCH
Referencias Cruzadas	CU. CU1, Administrador.
Casos de Uso	Creación de unidad departamental (departamento).
Notas	
Excepciones	Solo administrador puede acceder a crear un departamento
Salida	
Precondición	No existe el departamento
Poscondición	Departamento creado.

Nombre	Actualización de unidad departamental (departamento).
Responsabilidades	Actualizar datos de los departamentos existentes en la ESPOCH.
Referencias Cruzadas	CU. CU1, administrador.
Casos de Uso	Actualización de unidad departamental (departamento).
Excepciones	Solo administrador puede acceder a actualizar un departamento
Salida	
Precondición	El departamento debe haber sido creado

Poscondición	Se actualiza los datos del departamento

Nombre	Eliminación de unidad departamental (departamento).
Responsabilidades	Eliminar un departamento
Referencias Cruzadas	CU. CU2, administrador
Casos de Uso	Eliminación de unidad departamental (departamento).
Salidas	
Excepciones	Solo administrador puede acceder a eliminar un departamento
Precondición	El departamento debe existir
Poscondición	El departamento es eliminado

Nombre	Creación de unidad de vigilancia (Cámara)
Responsabilidades	Ingresar al sistema las cámaras de vigilancia.
Referencias Cruzadas	CU, CU1, administrador
Casos de Uso	Creación de unidad de vigilancia (Cámara)
Notas	
Excepciones	Solo administrador puede acceder crear una camara
Precondición	Debe existir el departamento
Poscondición	Cámara ingresada al sistema

Nombre	Actualización de una unidad de vigilancia (Cámara)
Responsabilidades	Actualizar datos de Cámaras existentes en un departamento.
Referencias Cruzadas	CU, CU1, Cliente.
Casos de Uso	Actualización de una unidad de vigilancia (Cámara).
Notas	
Excepciones	Solo administrador puede acceder actualizar una cámara
Precondición	La cámara debe constar en el sistema
Poscondición	Se actualiza la información de la cámara

Nombre	Eliminación de una unidad de vigilancia (Cámara).
Responsabilidades	Eliminar una Cámara del sistema
Referencias Cruzadas	CU, CU2, Administrador
Casos de Uso	Eliminación de una unidad de vigilancia (Cámara).
Notas	
Excepciones	Solo administrador puede acceder eliminar una cámara
Precondición	Existir la cámara en el sistema
Poscondición	Cámara borrada del sistema

Nombre	Monitorización de un área específica.
Responsabilidades	Acceder a la visualización que de una cámara especifica.
Referencias Cruzadas	CU, CU3, vigilante
Casos de Uso	Monitorización de un área específica.
Notas	
Excepciones	Cualquier usuario puede acceder al servicio
Precondición	Existir la cámara en el sistema
Poscondición	Visualización de video en vivo

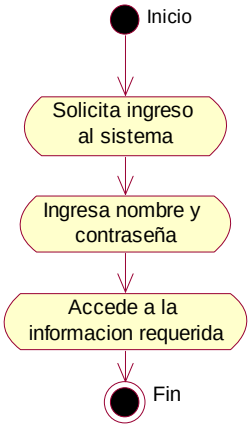
Nombre	Monitorización de varias cámaras a la vez de un departamento
Responsabilidades	Acceder a la visualización de todas las cámaras de un departamento.
Referencias Cruzadas	CU, CU3, vigilante
Casos de Uso	Monitorización de varias cámaras a la vez de un departamento
Notas	
Excepciones	
Precondición	Existir las cámaras en el sistema
Poscondición	Visualización de video en vivo

Nombre	Grabación de video
Responsabilidades	Grabar la visualización de video.
Referencias Cruzadas	CU, CU6, vigilante
Casos de Uso	Grabación de video
Notas	
Excepciones	Solo se puede grabar el video que se esta visualizando
Precondición	Existir la visualización de video
Poscondición	Video grabado.

Nombre	Recuperación de la Grabación de video
Responsabilidades	Visualizar una grabación de video.
Referencias Cruzadas	CU, CU4, vigilante
Casos de Uso	Recuperación de la Grabación de video
Notas	
Excepciones	Cualquier usuario puede reproducir una grabación
Precondición	Existir el archivo de video de video
Poscondición	Video visualizado.

4.8. Definir El Diagrama De Calles

Diagrama Autenticación de Usuario



Modulo De Administración

Diagrama Creación de Cuentas de Usuario.

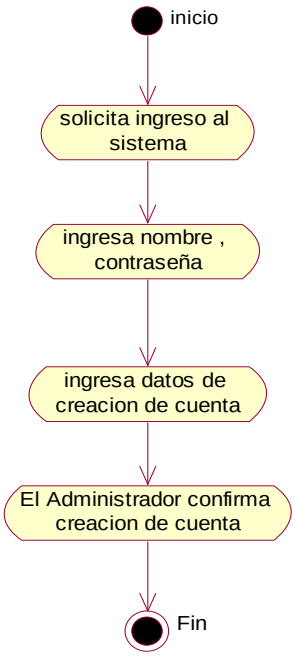


Diagrama Actualización de Cuentas de Usuario

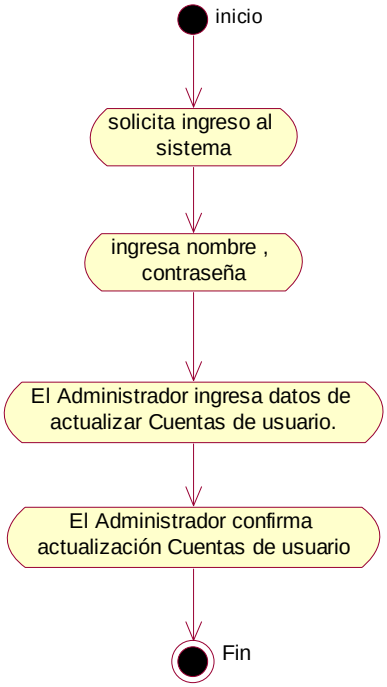


Diagrama Eliminación de Cuentas de Usuario

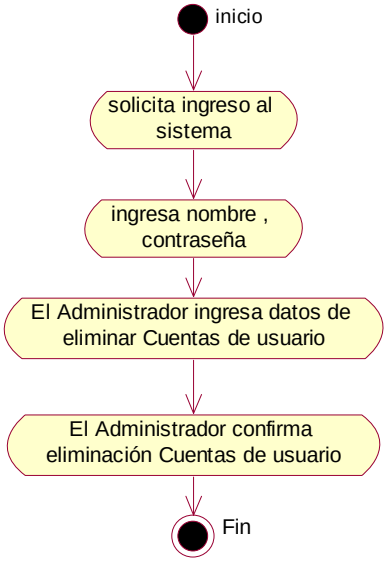


Diagrama Creación de unidad departamental (departamento).

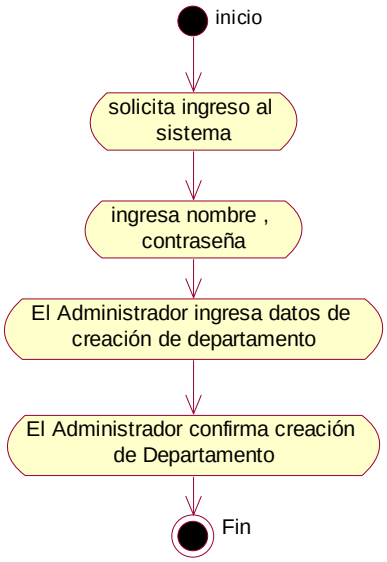


Diagrama Actualización de unidad departamental (departamento).

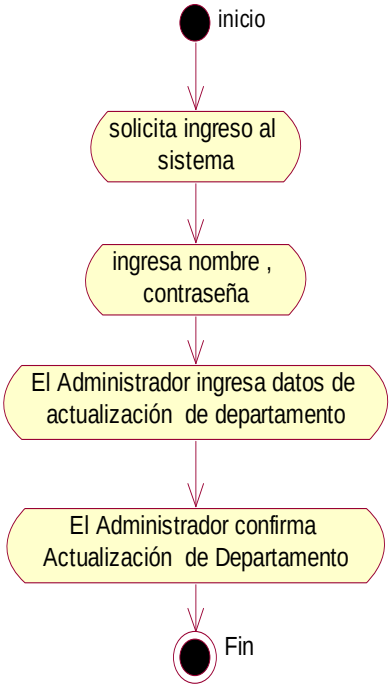


Diagrama Eliminación de unidad departamental (departamento).

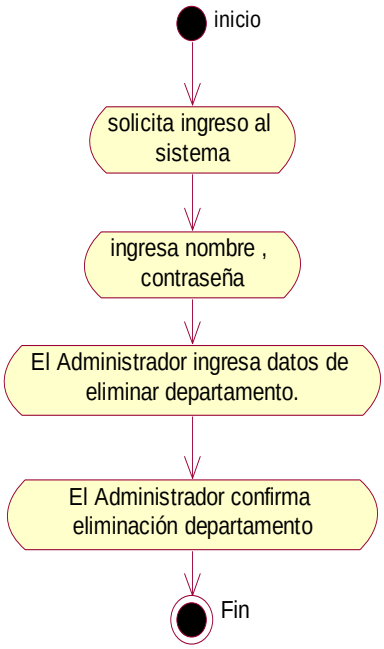


Diagrama Creación de unidad de vigilancia (Cámara)

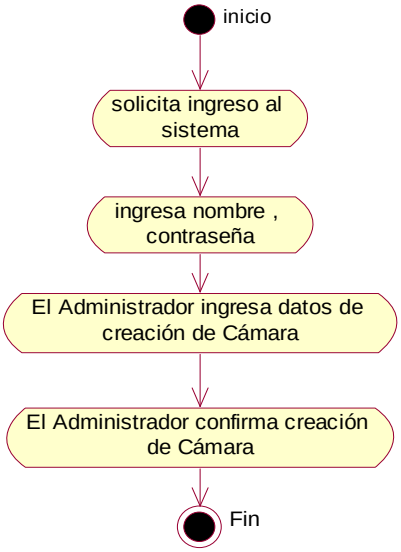


Diagrama Actualización de una unidad de vigilancia (Cámara).

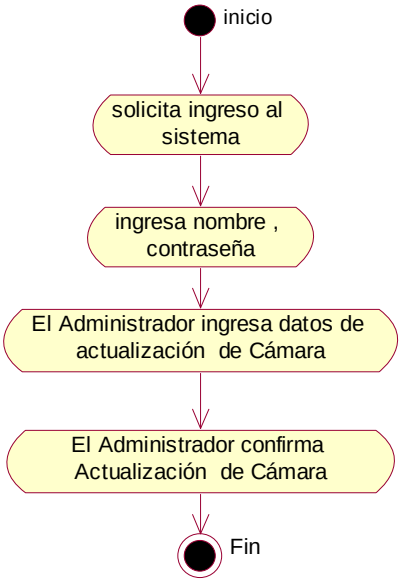
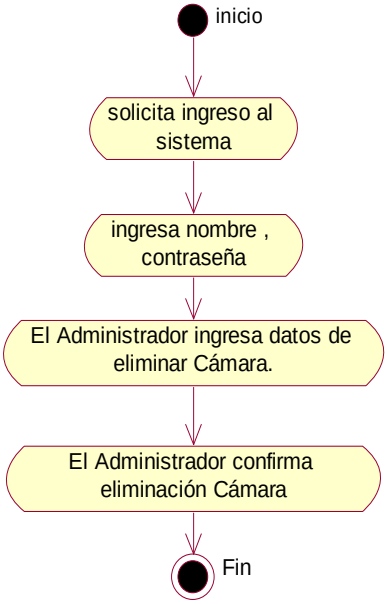


Diagrama Eliminación de una unidad de vigilancia (Cámara).



Modulo De Usuario (Vigilante)

Diagrama Monitorización de un área específica.

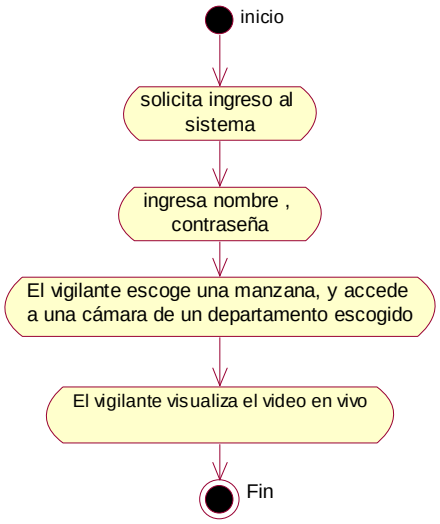


Diagrama Monitorización de varias cámaras a la vez de un departamento

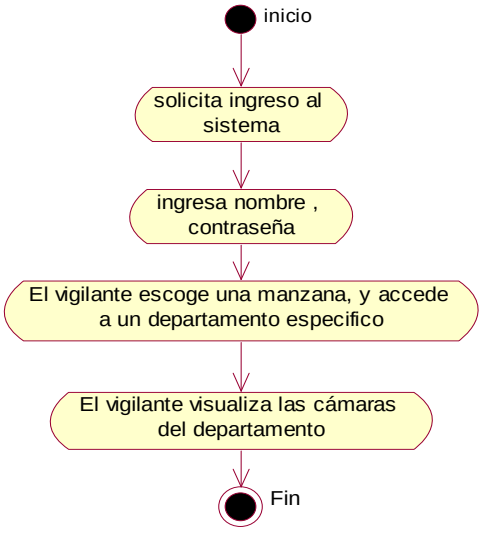


Diagrama Grabación de video

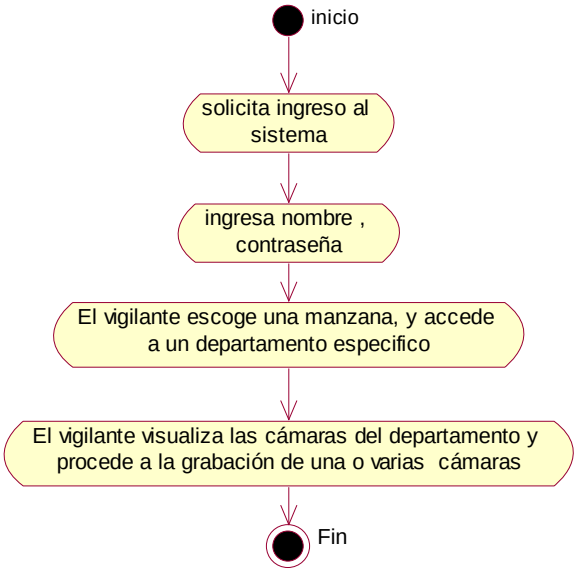
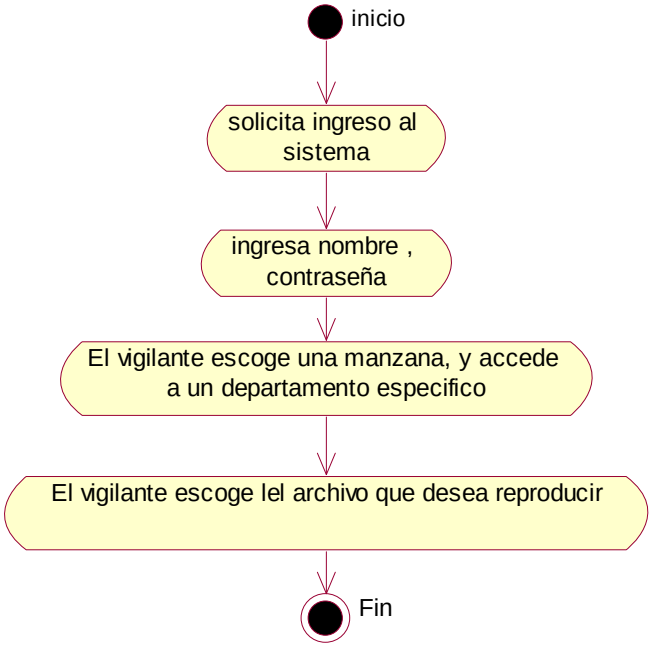


Diagrama Recuperación de la Grabación de video



4.9. Definir los diagramas de caso de uso reales

Definimos los siguientes casos de uso:

Modulo de administración

Caso de Uso 1: Autenticación del usuario

Actores: Administrador.

Propósito**:** Autentificar los usuarios.

Visión General: Autentificarse cada uno de los usuarios para acceder al sistema con diferentes propósitos ya sea de configuración o utilización del sistema

Tipo: Primario

Curso Típico de Eventos:

ACCIONES DEL ACTOR	**RESPUESTA DEL SISTEMA**
a) El Usuario solicita ingreso al sistema.	b) Solicitar nombre (varchar50) y contraseña (varchar10).
c) El Usuario ingresa los datos en los textbox para ingresar al sistema.	d) Valida nombre y contraseña.
	e) Presenta página de inicio del usuario.
f) El Usuario selecciona opción	g) Presenta información seleccionada.

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

d.3) Presenta recordatorio de clave para usuario.

Caso de Uso 2: Creación de Cuentas de Usuario.

Actores: Administrador (Iniciador).

Propósito: Crear una cuenta para cada usuario del sistema

Visión General: El Administrador crea las diferentes cuentas para usuarios según su nivel de seguridad o responsabilidad (tipo de usuario).

Tipo: Primario

Curso Típico de Eventos:

ACCIONES DEL ACTOR	**RESPUESTA DEL SISTEMA**
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre (varchar50) y contraseña (varchar10).
c) El Usuario ingresa los datos en los textbox para ingresar al sistema.	d) Valida nombre y contraseña.
	e) Presenta página (pantalla) de creación Cuentas de usuario.
f) El Administrador ingresa datos en los text box de creación de Cuentas de Usuario.	g) Almacena datos en la base de datos.
h) El Administrador confirma mediante un button.	i) Crear Cuenta de Usuario.

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de Uso 3: Actualización de Cuentas de Usuario

Actores: Administrador (Iniciador).

Propósito: Proponer la actualización de una Cuenta de Usuario.

Visión General: El Administrador Actualiza dada una cuenta de usuario según datos nuevos o responsabilidades.

Tipo: Primario

Curso Típico de Eventos:

ACCIONES DEL ACTOR	**RESPUESTA DEL SISTEMA**
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre (varchar50) y contraseña (varchar10).
c) El Usuario ingresa los datos en los textbox	d) Valida nombre y contraseña.

para ingresar al sistema .	
	e) Presenta página (pantalla) de actualización Cuentas de usuario.
f) El Administrador ingresa datos en los textbosx de actualizar Cuentas de usuario.	g) Almacena datos en la base de datos.
h) El Administrador confirma actualización Cuentas de usuario mediante un button	i) Actualiza Cuentas de usuario

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de uso 4: Eliminación de Cuentas de Usuario

Actores: Administrador (Iniciador)

Propósito: eliminar una cuenta de usuario.

.Visión General: El Administrador Elimina dada una cuenta de usuario según el criterio de suspensión de cuenta.

Tipo: Primario

Curso Típico de Eventos:

ACCIONES DEL ACTOR	**RESPUESTA DEL SISTEMA**
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre (varchar50) y contraseña (varchar10).
c) El Administrador ingresa sus datos en los textbox.	d) Valida nombre y contraseña.
	e) Presenta página (pantalla) de eliminación de Cuentas de usuario
f) El Administrador ingresa datos en los textbox de eliminar Cuentas de usuario.	g) elimina datos en la base de datos.
h) El Administrador confirma eliminación Cuentas de usuario button	i) Elimina Cuentas de usuario

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de uso 5: Creación de unidad departamental (departamento).

Actores: Administrador (Iniciador)

Propósito: ingresar al sistema los departamentos existentes en la ESPOCH.

Visión General: El Administrador solicita ingresar al sistema un departamento (ejemplo; Desitel) con el propósito de que conste en el sistema de video vigilancia para su posterior monitorización.

Tipo: Primario.

Curso Típico de Eventos:

ACCIONES DEL ACTOR	**RESPUESTA DEL SISTEMA**
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre (varchar50) y contraseña (varchar10).
c) El Administrador ingresa sus datos en los textbox.	d) Valida nombre y contraseña.
	e) Presenta página (pantalla) creación de Departamento
f) El Administrador ingresa datos en los textbox de creación de departamento	g) Almacena datos en la base de datos
h) El Administrador confirma creación de Departamento mediante un button	i) Creación de Departamento

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de uso 6: Actualización de unidad departamental (departamento).

Actores: Administrador (Iniciador)

Propósito: Actualizar datos de los departamentos existentes en la ESPOCH.

Visión General: El Administrador solicita actualizar los datos en el sistema de un departamento especifico (ejemplo; Desitel).

Tipo: Primario.

Curso Típico de Eventos**:**

ACCIONES DEL ACTOR	**RESPUESTA DEL SISTEMA**
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre (varchar50) y contraseña (varchar10).
c) El Administrador ingresa sus datos en los textbox.	d) Valida nombre y contraseña.
	e) Presenta página (pantalla) Actualización de Departamento
f) El Administrador ingresa datos en los textbox de actualización de departamento mediante un button	g) Almacena datos en la base de datos
h) El Administrador confirma Actualización de Departamento mediante un button	i) Actualiza Departamento

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de uso 7: Eliminación de unidad departamental (departamento).

Actores: Administrador (Iniciador)

Propósito: eliminar un departamento.

.Visión General: El Administrador elimina un departamento según el criterio de suspensión.

Tipo: Primario

Curso Típico de Eventos:

ACCIONES DEL ACTOR	**RESPUESTA DEL SISTEMA**
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre (varchar50) y contraseña (varchar10).
c) El Administrador ingresa sus datos en los textbox.	d) Valida nombre y contraseña.
	e) Presenta página (pantalla) de eliminación de departamento
f) El Administrador ingresa datos en los textbox de eliminar departamento.	g) Elimina datos en la base de datos.
h) El Administrador confirma eliminación departamento mediante un button	i) Elimina departamento

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de uso 8: Creación de unidad de vigilancia (Cámara)

Actores: Administrador (Iniciador)

Propósito: ingresar al sistema las cámaras de vigilancia.

Visión General: El Administrador solicita ingresar al sistema una unidad de vigilancia (cámara) a un departamento específico (ejemplo; Desitel) con el propósito de que conste en el sistema de video vigilancia para su posterior monitorización.

Tipo: Primario.

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre (varchar50) y contraseña (varchar10).
c) El Administrador ingresa sus datos en los textbox. .	d) Valida nombre y contraseña.
	e) Presenta página (pantalla) creación de Cámara
f) El Administrador ingresa datos en los textbox de creación de Cámara	g) Almacena datos en la base de datos
h) El Administrador confirma creación de Cámara mediante un button	i) Creación de Cámara

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de uso 9: Actualización de una unidad de vigilancia (Cámara).

Actores: Administrador (Iniciador)

Propósito: Actualizar datos de Cámaras existentes en un departamento.

Visión General: El Administrador solicita actualizar los datos en el sistema Cámaras existentes en un departamento (ejemplo; Desitel).

Tipo: Primario.

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre (varchar50) y contraseña (varchar10).
c) El Administrador ingresa sus datos en los textbox. .	d) Valida nombre y contraseña.
	e) Presenta página (pantalla) Actualización de Cámara
f) El Administrador ingresa datos en los textbox de actualización de Cámara	g) Almacena datos en la base de datos
h) El Administrador confirma Actualización	i) Actualiza Cámara

de Cámara mediante un button	

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de uso 10: Eliminación de una unidad de vigilancia (Cámara).

Actores: Administrador (Iniciador)

Propósito: eliminar una Cámara.

.Visión General: El Administrador elimina una Cámara según el criterio de suspensión.

Tipo: Primario

Curso Típico de Eventos:

ACCIONES DEL ACTOR	**RESPUESTA DEL SISTEMA**
a) El Administrador solicita ingresar al sistema.	b) Solicitar nombre (varchar50) y contraseña (varchar10).
c) El Administrador ingresa sus datos en los textbox.	d) Valida nombre y contraseña.
	e) Presenta página (pantalla) de eliminación de Cámara
f) El Administrador ingresa datos en los textbox de eliminar Cámara.	g) Elimina datos en la base de datos.
h) El Administrador confirma eliminación Cámara mediante un button	i) Elimina Cámara

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

MODULO DE USUARIO (VIGILANTE)

Caso de Uso 1: Monitorización de un área específica.

Actores: Vigilante (iniciador).

Propósito: Acceder a la visualización que de una cámara especifica.

Visión General: El vigilante accede al sistema para poder monitorizar lo que una cámara del sistema de vigilancia presenta como video en vivo. Para ello accede al mapa de la ESPOCH, escoge un lugar geográfico (manzana) que desea monitorizar, y escoge una cámara específica de un departamento escogido.

Tipo: Primario.

Curso Típico de Eventos:

ACCIONES DEL ACTOR	**RESPUESTA DEL SISTEMA**
a) El vigilante solicita acceder al sistema	b) Solicitar nombre (varchar50) y contraseña (varchar10).
c) El vigilante ingresa sus datos en los textbox.	d) Valida nombre y contraseña.
	e) Verifica su existencia en la Base de Datos.
f) El vigilante escoge una manzana mediante la selección de un nodo , y accede a una cámara de un departamento nodo hijo escogido	g) muestra mapa de la ESPOCH (pantalla). Despliega cámaras del departamento
h) El vigilante visualiza el video en un display panel en vivo	i) Muestra video en vivo display panel

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de Uso 2: Monitorización de varias cámaras a la vez de un departamento

Actores: Vigilante (iniciador).

Propósito: Acceder a la visualización de todas las cámaras de un departamento.

Visión General: El vigilante accede al sistema para poder monitorizar lo que varias cámaras de un departamento especifico presentan como video en vivo. Para ello accede al mapa de la ESPOCH, escoge un lugar geográfico (manzana) que desea monitorizar, y escoge un departamento específico.

Tipo: Primario.

Curso Típico de Eventos**:**

ACCIONES DEL ACTOR	**RESPUESTA DEL SISTEMA**
a) El vigilante solicita acceder al sistema	b) Solicitar nombre (varchar50) y contraseña (varchar10).
c) El vigilante ingresa sus datos en los textbox.	d) Valida nombre y contraseña.
	e) Verifica su existencia en la Base de Datos.
f) El vigilante escoge una manzana mediante la selección de un nodo , y accede a una cámara de un departamento nodo hijo escogido	g) muestra mapa de la ESPOCH. (pantalla) Despliega cámaras del departamento
h) El vigilante visualiza las cámaras del departamento en displays de 4 en 4	i) Muestra video en vivo en display panel de todas las cámaras del departamento.

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

Caso de Uso 3: Grabación de video

Actores: Vigilante (iniciador).

Propósito: Grabar la visualización de video.

Visión General: El vigilante accede al sistema para poder grabar lo que una o varias cámaras de un departamento específico presentan como video en vivo. Para ello accede al mapa de la ESPOCH, escoge un lugar geográfico (manzana) que desea monitorizar, y escoge un departamento específico.

Tipo: Primario.

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El vigilante solicita acceder al sistema	b) Solicitar nombre (varchar50) y contraseña (varchar10).
c) El vigilante ingresa sus datos en los textbox.	d) Valida nombre y contraseña.
	e) Verifica su existencia en la Base de Datos.
f) El vigilante escoge una manzana mediante la selección de un nodo , y accede a una cámara de un departamento nodo hijo escogido	g) muestra mapa de la ESPOCH. (pantalla) Despliega cámaras del departamento
h) El vigilante visualiza las cámaras del departamento y procede a la grabación de una o varias cámaras mediante un button de grabación	i) Graba video en vivo de la o las cámaras seleccionadas en la base de datos.

Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

d.3) Solo se puede grabar lo que se esta visualizando.

Caso de Uso 4: Recuperación de la Grabación de video

Actores: Vigilante (iniciador).

Propósito: visualizar una grabación de video.

Visión General: El vigilante accede al sistema para poder visualizar una grabación o captura de video, para ello accede a un archivo de grabaciones de un departamento especifico seleccionado, donde se muestran las grabaciones de todas las cámaras de dicho departamento y que se seleccionan para poder reproducir.

Tipo: Primario.

Curso Típico de Eventos:

ACCIONES DEL ACTOR	RESPUESTA DEL SISTEMA
a) El vigilante solicita acceder al sistema	b) Solicitar nombre (varchar50) y contraseña (varchar10).
c) El vigilante ingresa sus datos en los textbox.	d) Valida nombre y contraseña.
	e) Verifica su existencia en la Base de Datos.
f) El vigilante escoge una manzana mediante la selección de un nodo , y accede a una cámara de un departamento nodo hijo escogido	g) muestra solapa (pantalla) de grabaciones de las cámaras del departamento
h) El vigilante escoge el archivo de un listview que desea reproducir	i) reproduce video grabado del archivo seleccionado en un display panel.

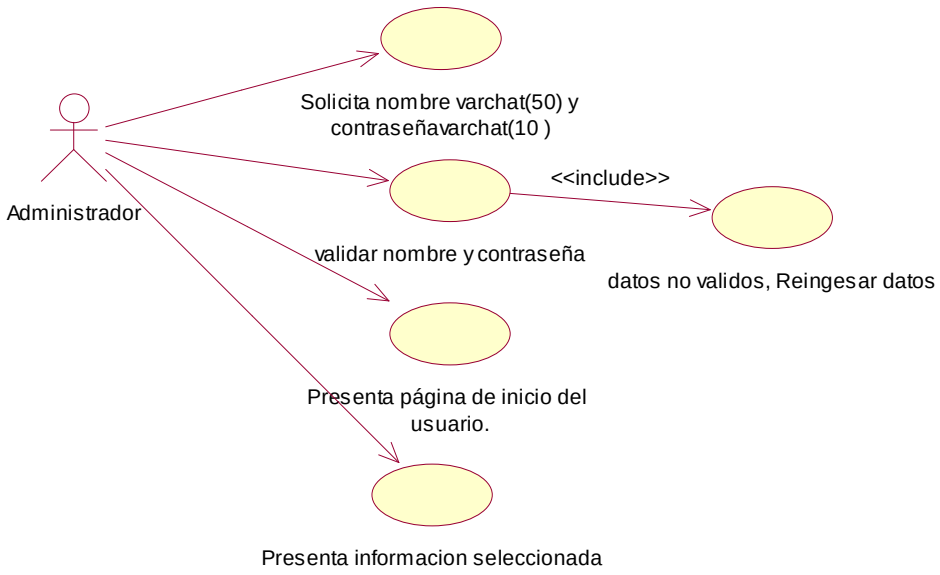
Curso Alternativo de Eventos:

d.1) Datos no válidos terminar proceso

d.2) Ingrese nuevamente su nombre y contraseña.

4.10. Definir los diagramas de Casos de Uso reales

Diagrama Autenticación de Usuario



Modulo De Administración

Diagrama Creación de Cuentas de Usuario.

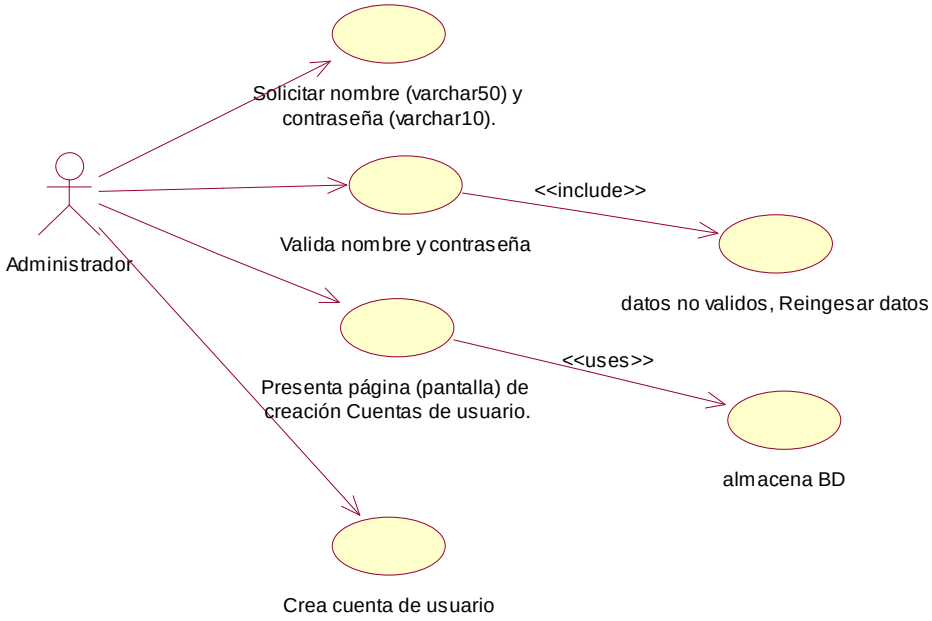


Diagrama Actualización de Cuentas de Usuario

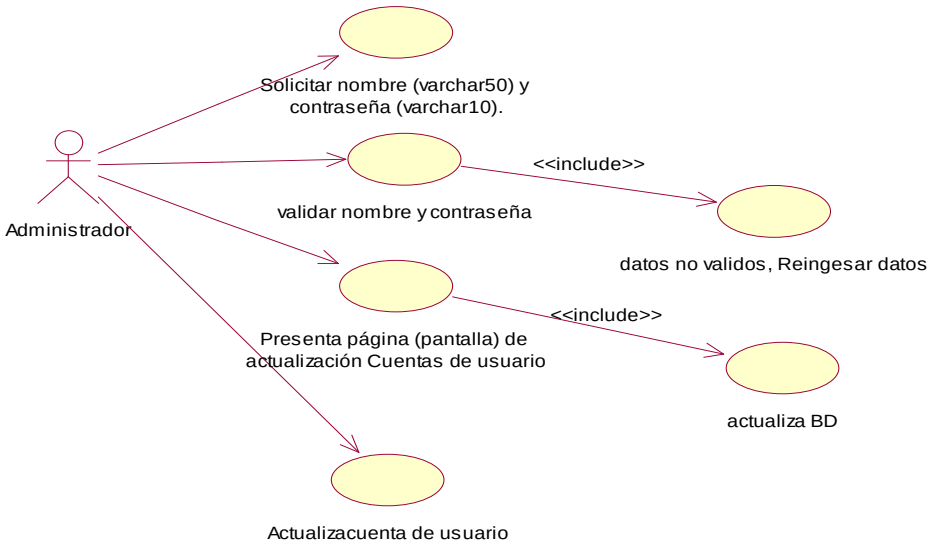


Diagrama Eliminación de Cuentas de Usuario

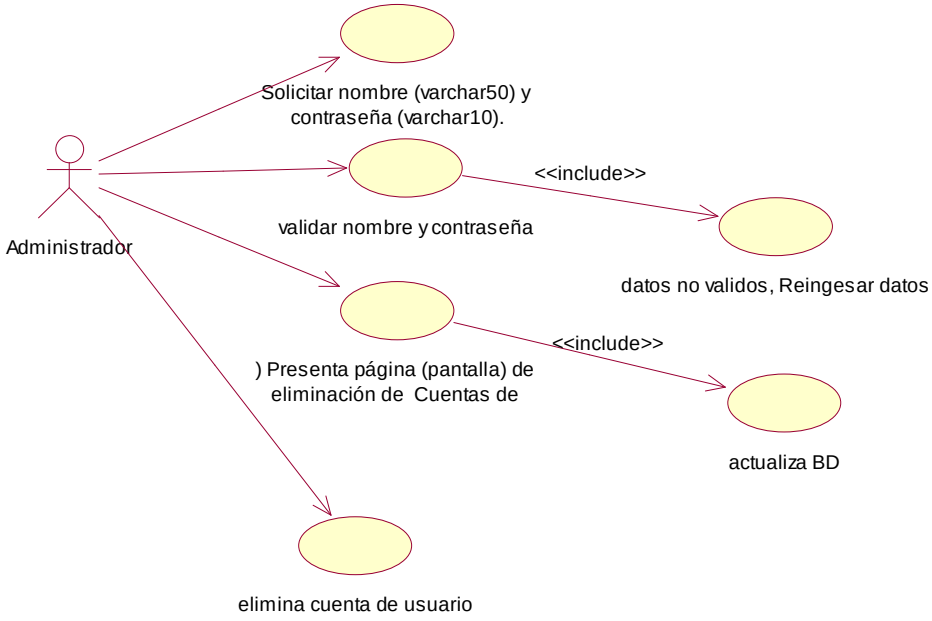


Diagrama Creación de unidad departamental (departamento).

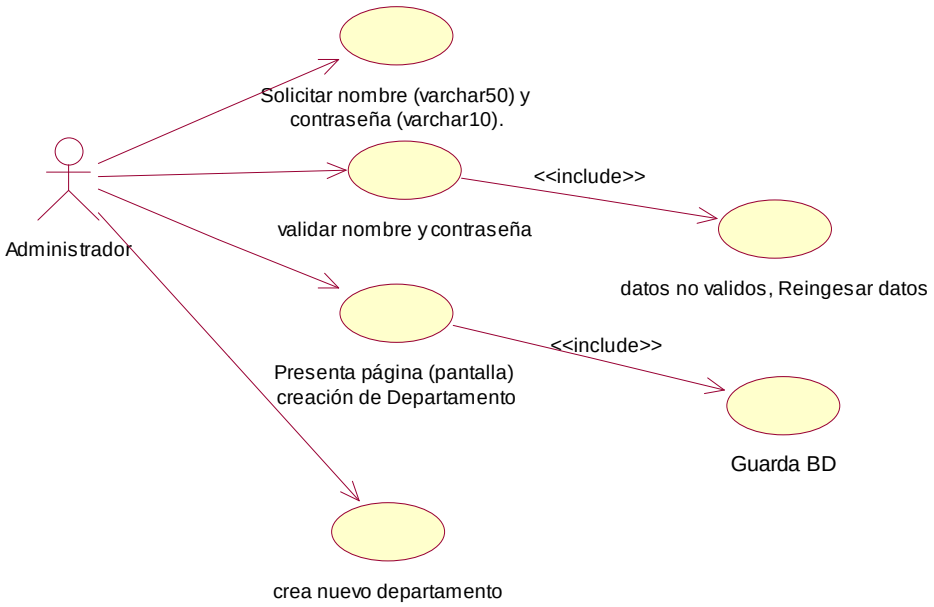


Diagrama Actualización de unidad departamental (departamento).

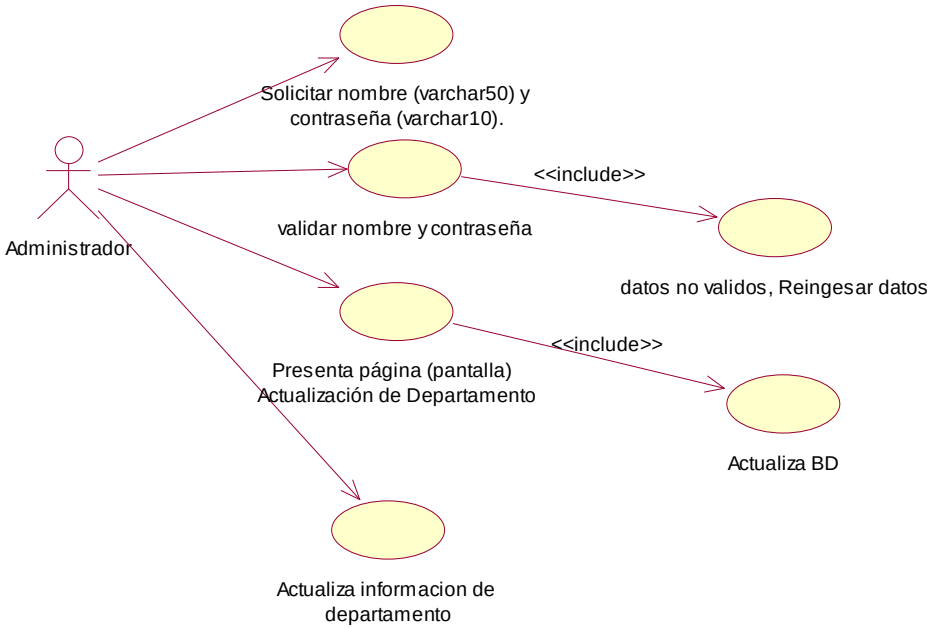


Diagrama Eliminación de unidad departamental (departamento).

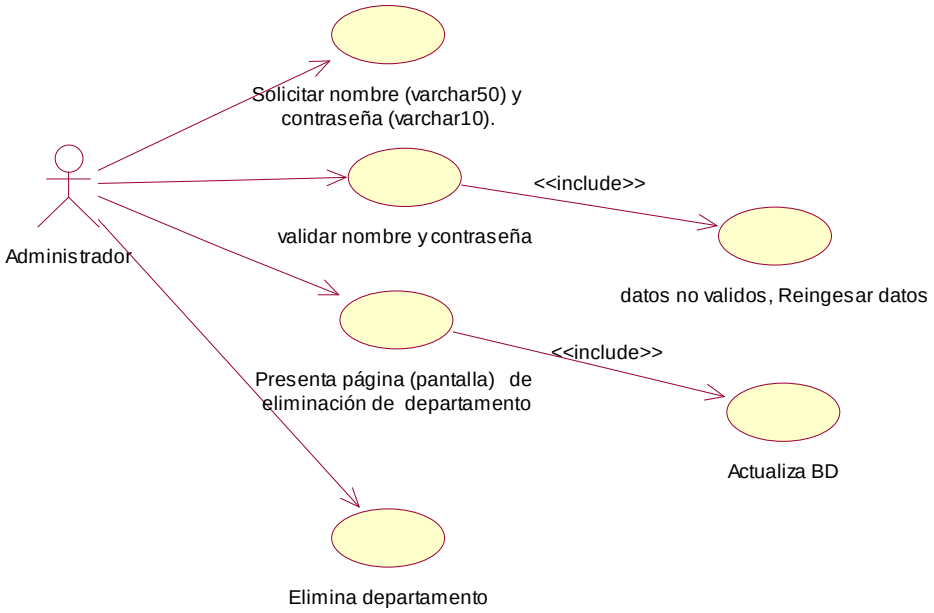


Diagrama Creación de unidad de vigilancia (Cámara)

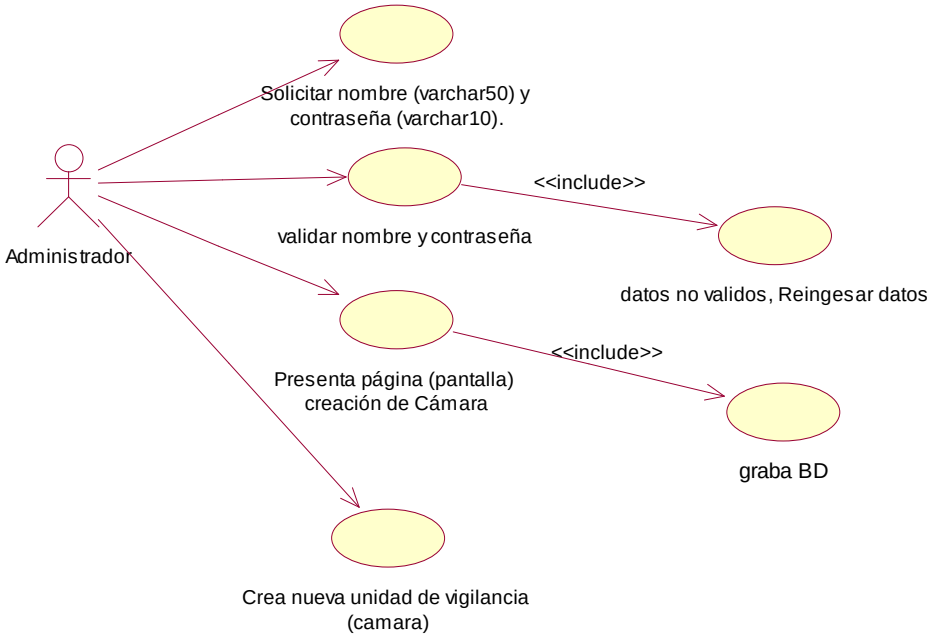


Diagrama Actualización de una unidad de vigilancia (Cámara).

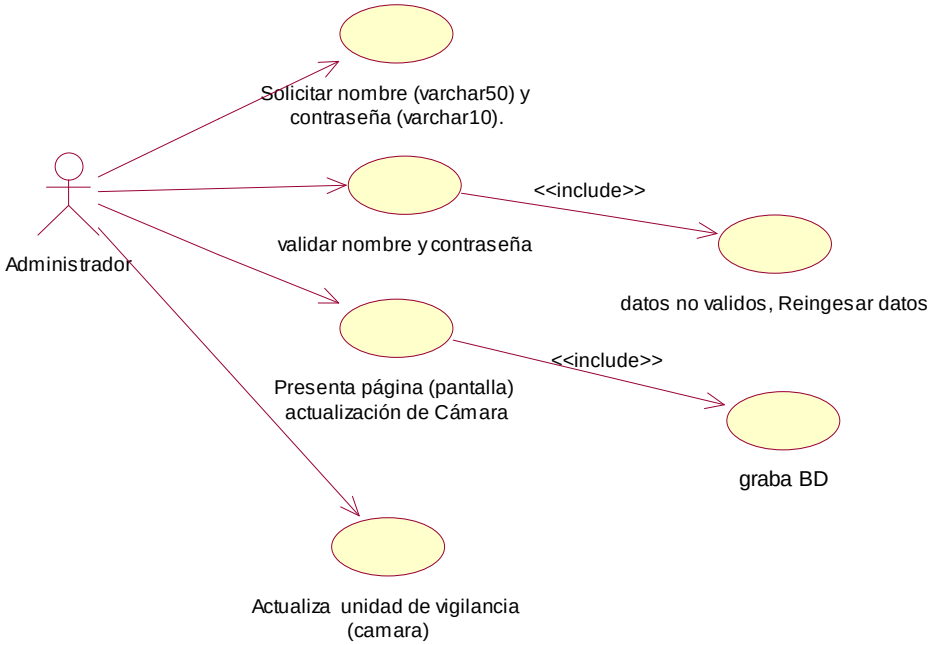
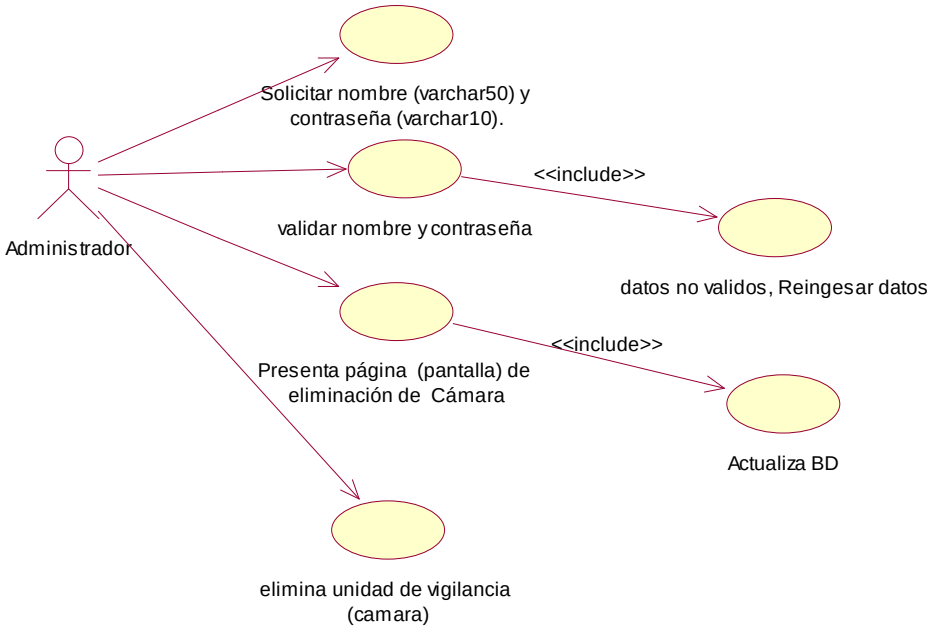


Diagrama Eliminación de una unidad de vigilancia (Cámara).



MODULO DE USUARIO (VIGILANTE)

Diagrama Monitorización de un área específica.

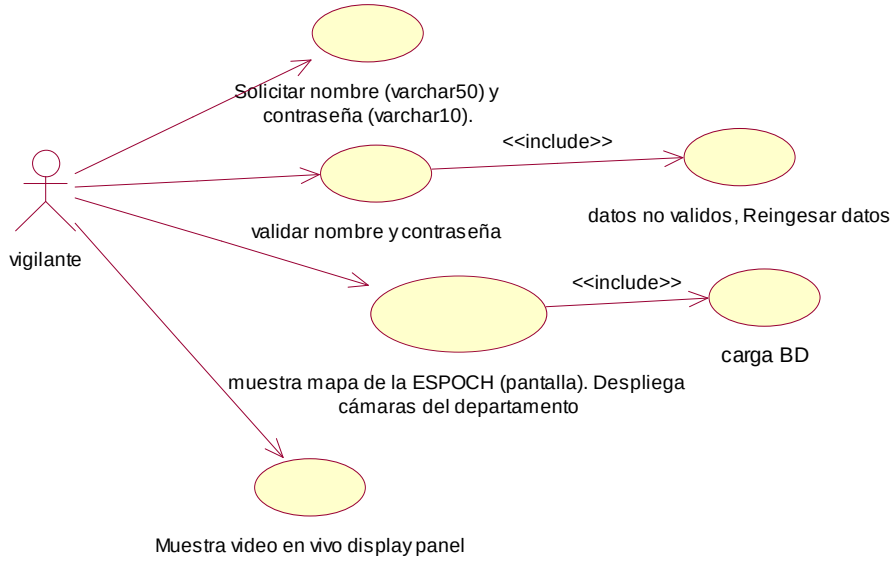


Diagrama Monitorización de varias cámaras a la vez de un departamento

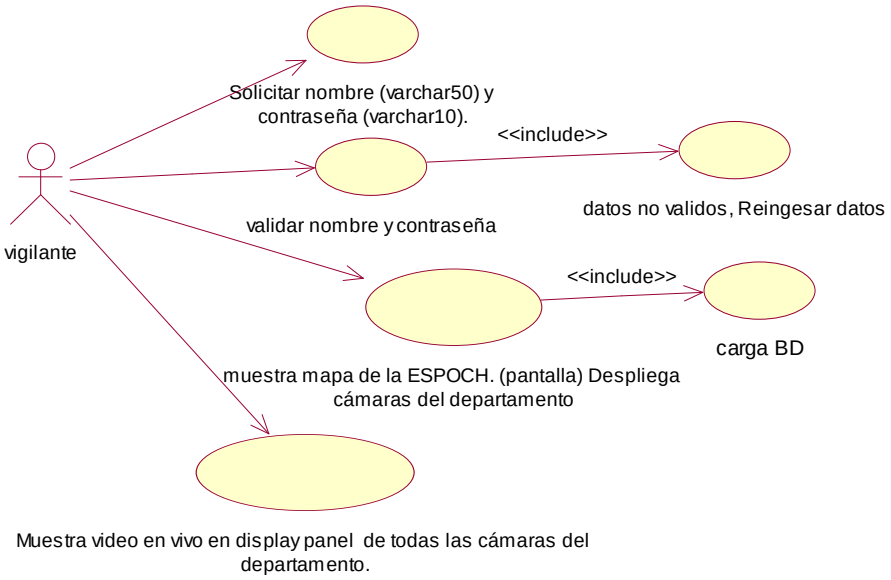


Diagrama Grabación de video

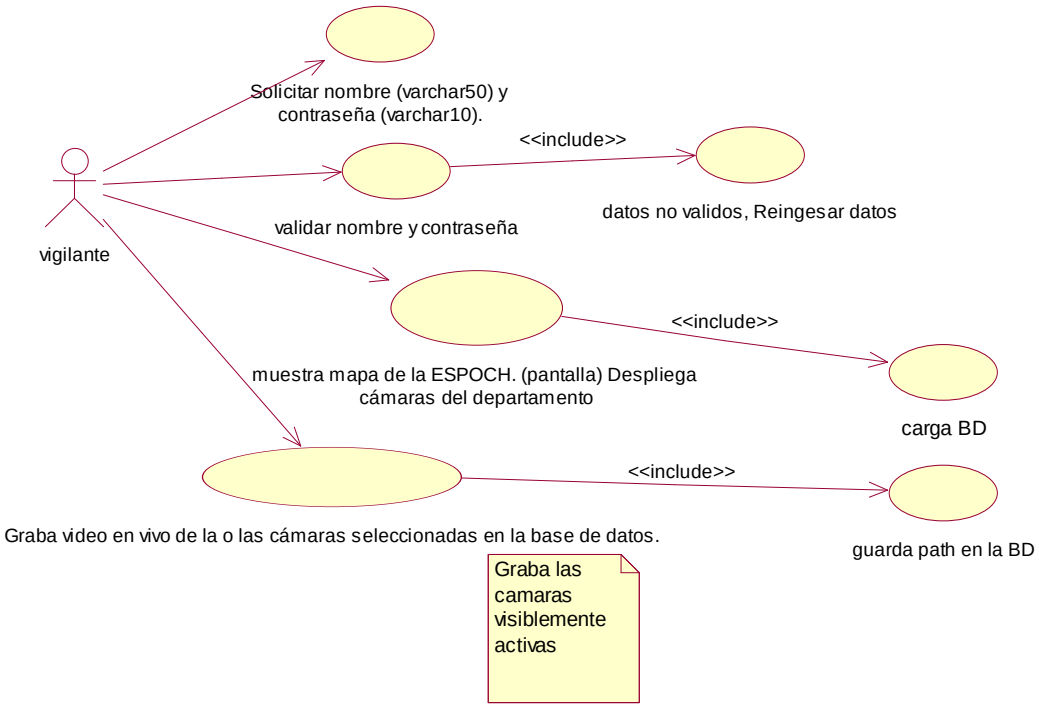
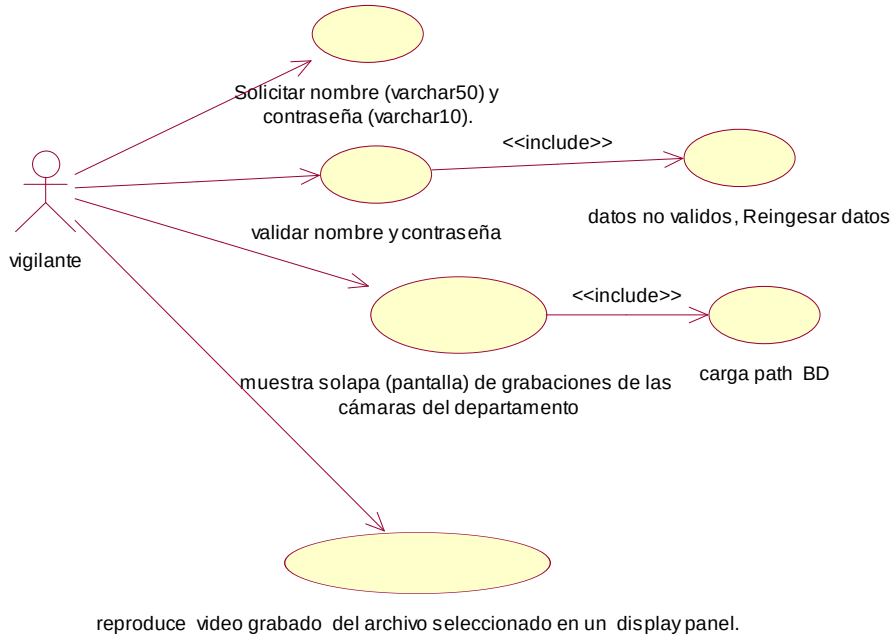


Diagrama Recuperación de la Grabación de video



4.11. Definir la interfaz de usuario

El objetivo debe ser diseñar interfaces que ayuden a los usuarios y negocios a proporcionar y obtener información del sistema que necesiten, cumpliendo los siguientes objetivos:

1. Efectividad lograda por medio de diseño de interfaces que permitan a los usuarios a acceder el sistema en una forma que sea congruente con sus necesidades individuales.

2. Efectividad mostrada por medio de interfaces que aumenten la velocidad de la captura de datos y reduzca errores.

3. Demostrar consideración al usuario diseñando interfaces adecuadas y que el sistema les proporcione la retroalimentación adecuada.

4. Productividad mostrada por su adecuación a los principios ergonómicos establecidos en el diseño de interfaces y espacios de trabajo para los usuarios.

Componentes de la interfaz de usuario

La interfaz de usuario tiene dos componentes principales:

El lenguaje de presentación, que es la parte de la computadora al usuario de la transacción.

El lenguaje de acción, que caracteriza la parte usuario a computadora.

Ambos conceptos juntos cubren la forma y contenido del término Interfaz de Usuario.

4.12. Definir los diagramas de interacción.

Los Diagramas de Interacción muestran el intercambio de mensajes entre instancias del modelo de clases para cumplir las post-condiciones establecidas en un contrato.

Hay dos clases de Diagramas de Interacción:

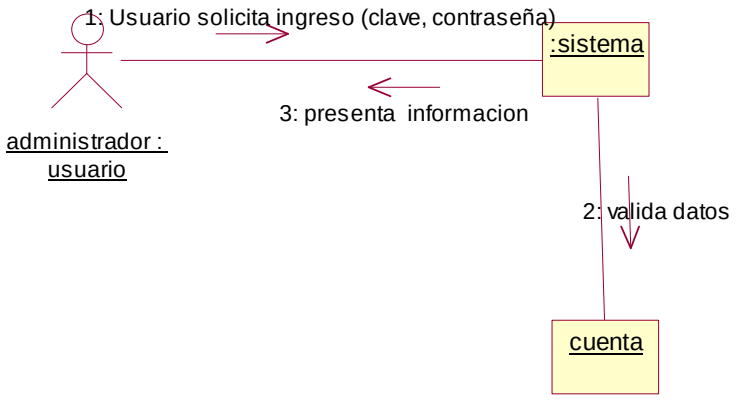
1. Diagramas de Colaboración.
2. Diagramas de Secuencia.

La creación de los Diagramas de Colaboración de un sistema es una de las actividades más importantes en el desarrollo orientado a objetos, pues al construirlos se toman decisiones claves acerca del funcionamiento del futuro sistema. La creación de estos diagramas, por tanto, debería ocupar un porcentaje significativo en el esfuerzo dedicado al proyecto entero.

El Diagrama de Colaboración modela la interacción entre los objetos de un Caso de Uso. Los objetos están conectados por enlaces (links) en los cuales se representan los mensajes enviados acompañados de una flecha que indica su dirección. El Diagrama de Colaboración ofrece una mejor visión del escenario cuando el analista está intentando comprender la participación de un objeto en el sistema.

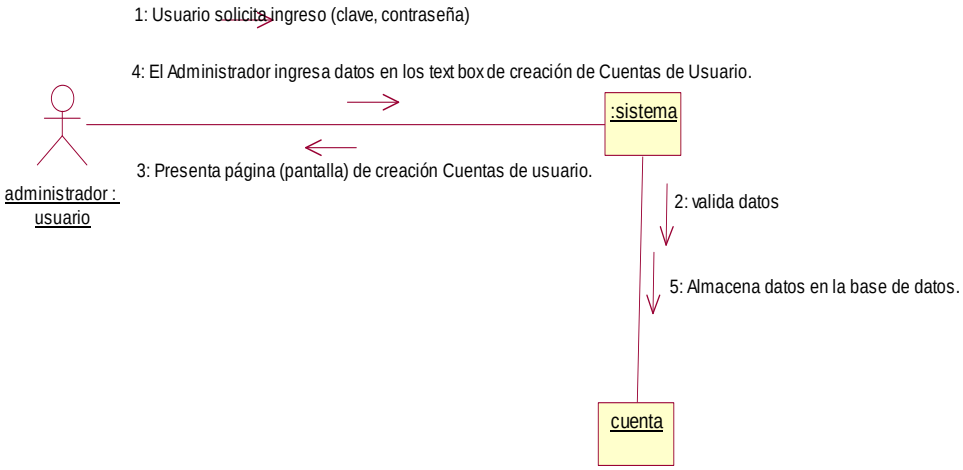
Diagramas de colaboración

Autenticación del usuario

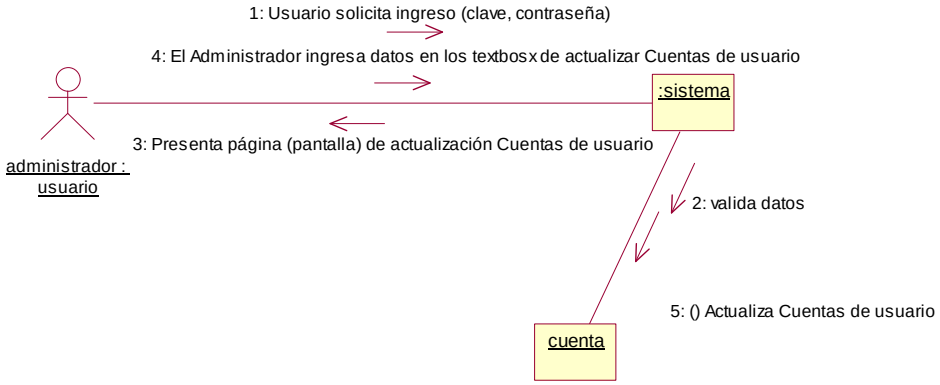


Modulo de administración

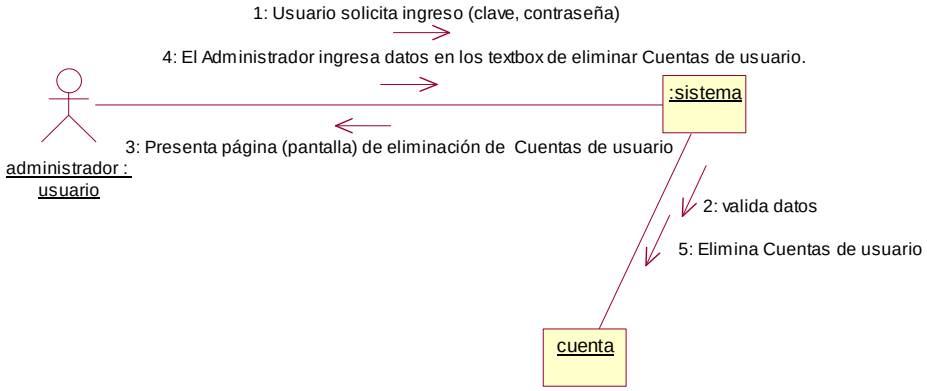
Creación de Cuentas de Usuario.



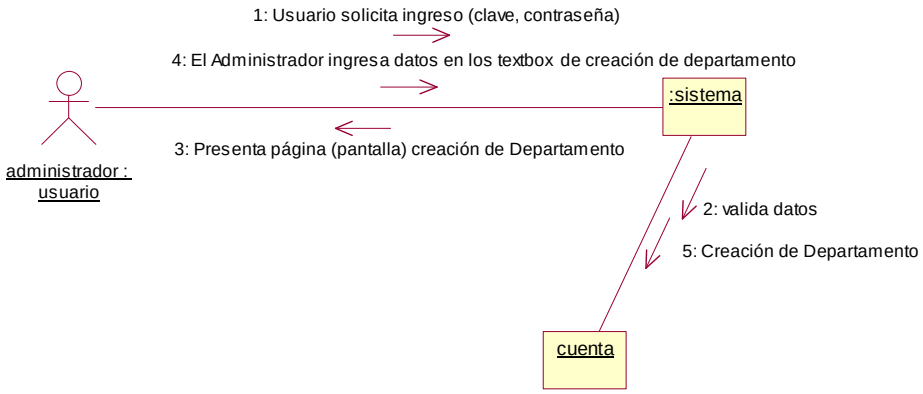
Actualización de Cuentas de Usuario



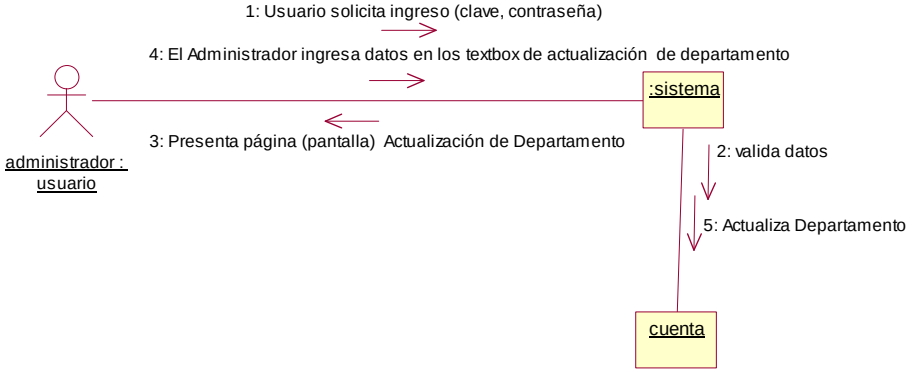
Eliminación de Cuentas de Usuario



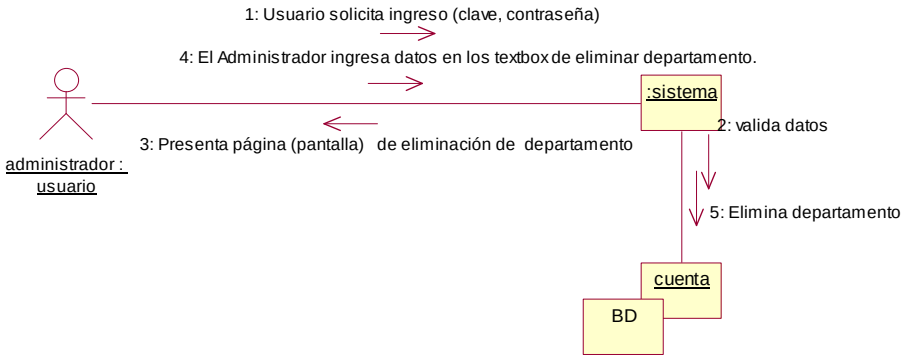
Creación de unidad departamental (departamento).



Actualización de unidad departamental (departamento)



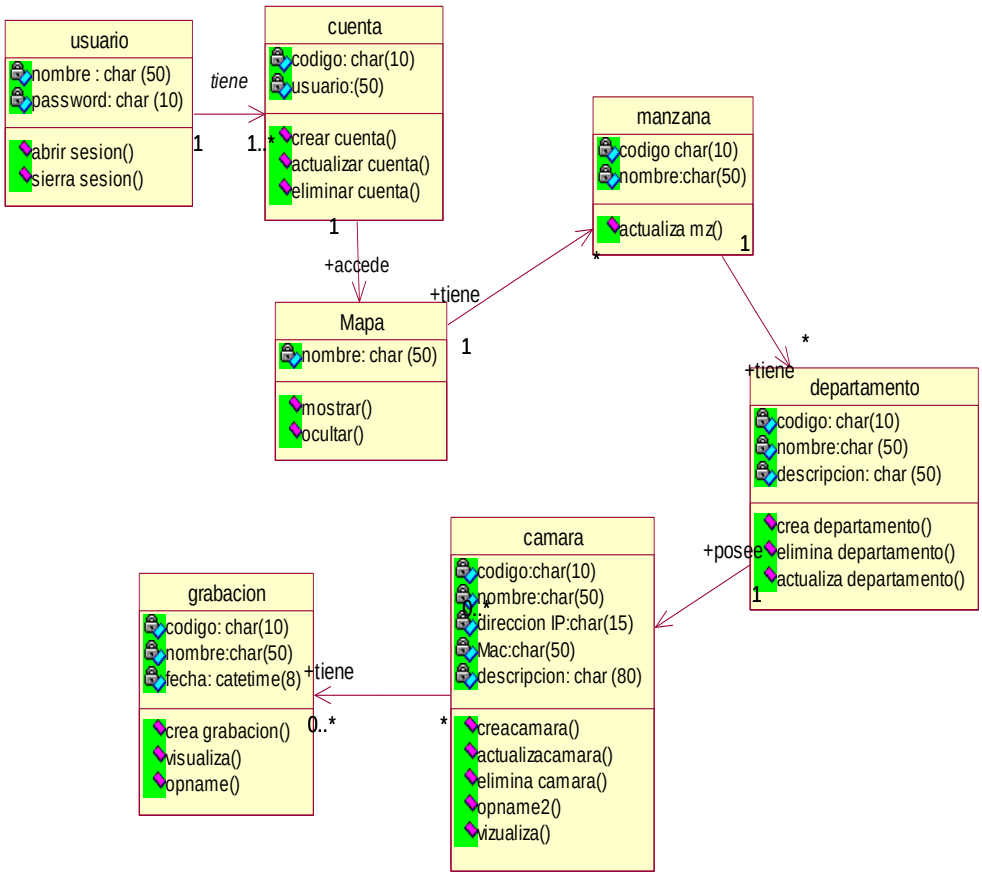
Eliminación de unidad departamental (departamento).



4.13. Diagrama de clases del diseño

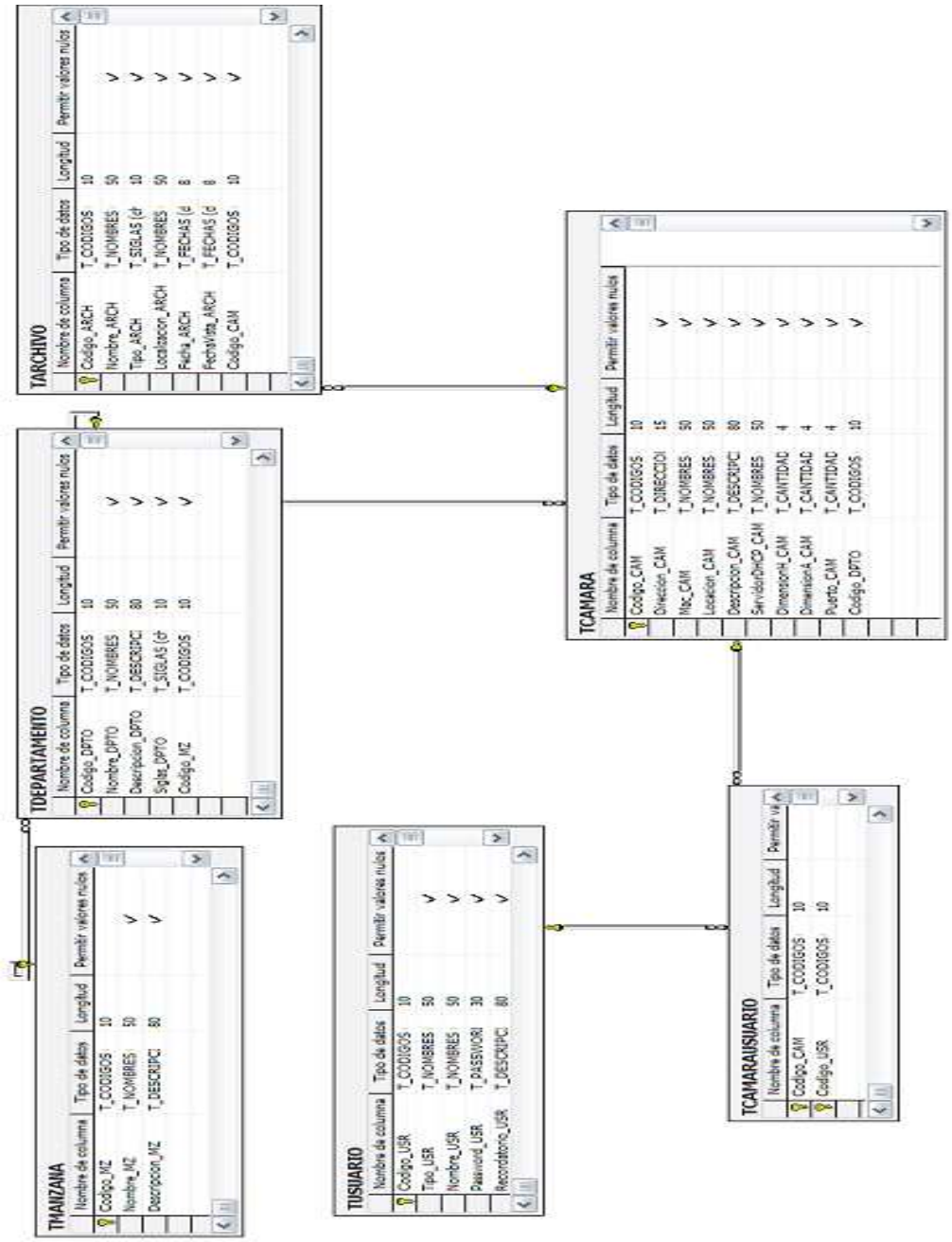
Un Diagrama de Clases de Diseño muestra la especificación para las clases software de una aplicación.

A diferencia del Modelo Conceptual, un Diagrama de Clases de Diseño muestra definiciones de entidades software más que conceptos del mundo real.



4.14. Definir el esquema de la base de datos.

Del diagrama de clases se debe evolucionar al modelo relacional para definir el diseño físico de la base de datos. Mientras no se desarrollen DBMS que manipulen objetos, todo el esfuerzo del AOO y del DOO no se optimiza cuando se regresa al modelo relacional.



4.15. Refinar el modelo físico y la arquitectura del sistema

Existen dos tipos de diagramas que sirven para modelar los aspectos físicos de un sistema orientado a objetos:

- Diagramas de Componentes
- Diagramas de Despliegue

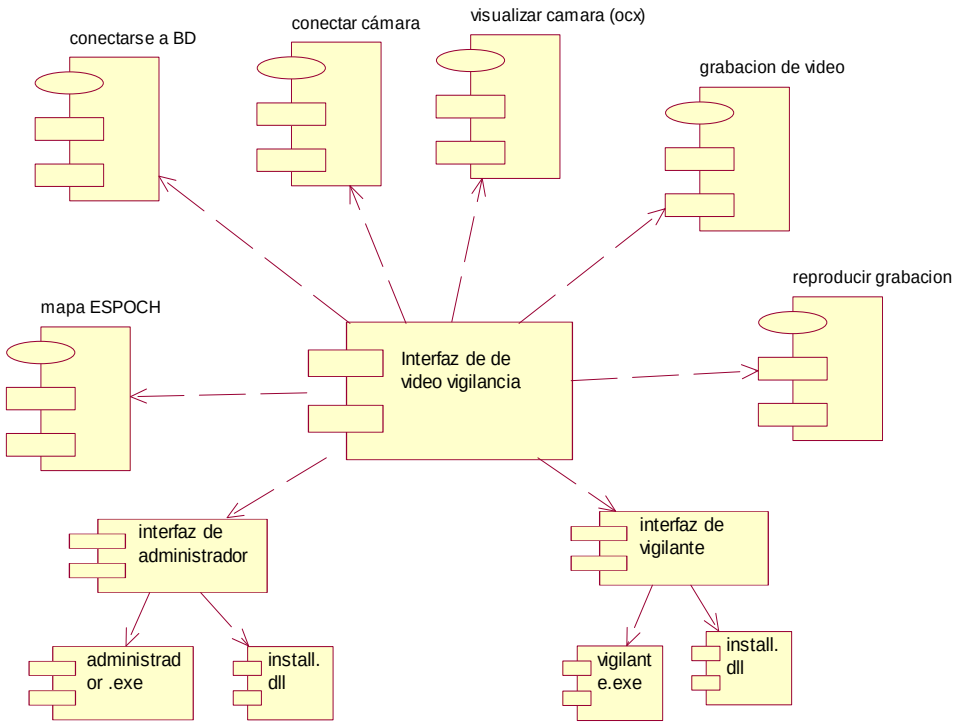
Seguidamente veremos para qué sirve cada uno de ellos y cual es su representación gráfica.

Diagramas de Componentes

Los componentes pertenecen al mundo físico, es decir, representan un bloque de construcción al modelar aspectos físicos de un sistema.

Una característica básica de un componente es que “debe definir una abstracción precisa con una interfaz bien definida, y permitiendo reemplazar fácilmente los componentes más viejos con otros más nuevos y compatibles.”

Cada componente debe tener un nombre que lo distinga de los demás. Al igual que las clases los componentes pueden enriquecerse con compartimentos adicionales que muestran sus detalles.

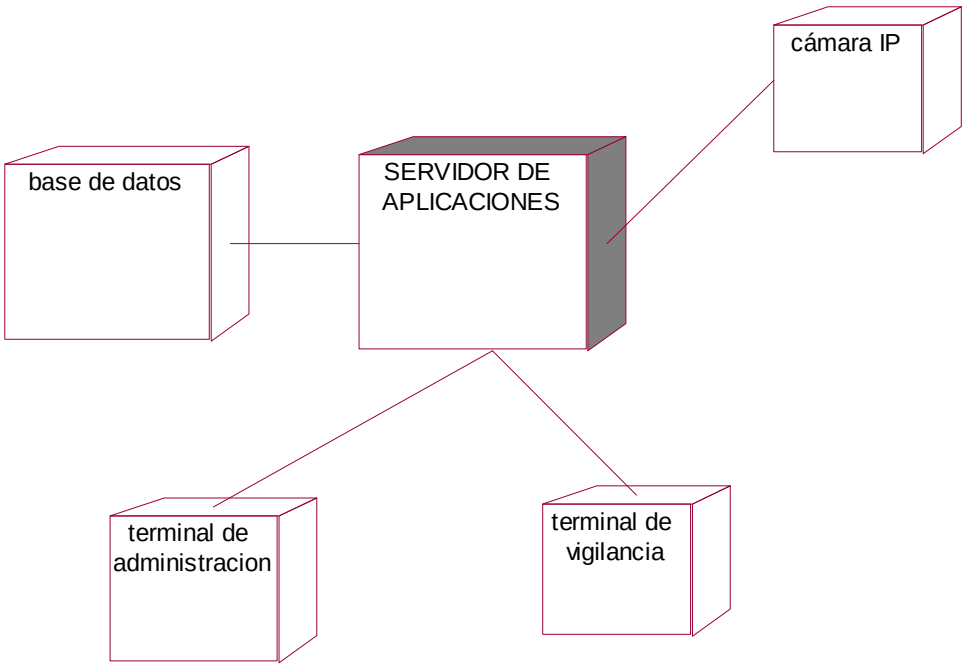


Diagramas de Despliegue

Nodos

Al igual que los componentes los nodos pertenecen al mundo material. Vamos a definir un nodo como un elemento físico, que existe en tiempo de ejecución y representa un recurso computacional que generalmente tiene alguna memoria y, a menudo, capacidad de procesamiento.

Los nodos sirven para modelar la topología del hardware sobre el que se ejecuta el sistema. Un nodo representa normalmente un procesador o un dispositivo sobre el que se pueden desplegar los componentes. Un nodo debe tener un nombre asignado que lo distinga del resto de nodos.


cámara IP
base de datos
SERVIDOR DE APLICACIONES
terminal de administracion
terminal de vigilancia

CONCLUSIONES

1) Al poder comparar las diferentes técnicas de encolamiento en base al parámetro de retraso temporal, se ha logrado establecer que existe una diferencia en la manera como gestionan el trafico cada una de ellas. Pese a que todas estas técnicas de encolamiento tratan de brindar una Calidad de Servicio a un trafico determinado , se establece que para el caso especifico de video-IP la disciplina de encolamiento Custom Queueing (CQ) es la que mejor se ajusta a los requerimientos en la transmisión de este tipo de trafico en la red de la ESPOCH-DESITEL.

2) Se determina que para poder escoger uno de los formatos de compresión de video el principal parámetro a tomar en cuenta en la comparación, es hacia que tipo de aplicación (*Aplicación orientada*) esta dirigida la compresión . Para el caso del desarrollo de una aplicación de video-vigilancia-IP en la ESPOCH, la calidad que dicha aplicación requiere es la de *Transmisión con calidad TV* . Por lo que se establece que el formato de compresión **MPEG** es el que deben incorporar las cámaras de red.

3) Para incorporar un sistema de cámaras de red orientadas a un sistema de video-vigilancia–IP se necesita que exista una infraestructura de red previamente establecida y funcional. En el caso de la ESPOCH-DESITEL al contar con una infraestructura de red totalmente eficaz y moderna dicha integracion resulta totalmente viable.

4) El desarrollo del sistema software para Video-vigilancia-IP permite la visualización del video en vivo y la gestión de los recursos propios del sistema, constituyendo así una herramienta clave y método de apoyo en la vigilancia remota de sitios estratégicos para los cuales el factor seguridad sea necesario dentro de la infraestructura de la ESPOCH-DESITEL.

5) El impacto que un sistema de video-vigilancia-IP pueda tener sobre la red ESPOCH-DESITEL, dependerá primordialmente del ancho de banda disponible en dicha red. Este impacto no deberá superar el 60%, ya que hay que considerar los varios tipos de servicios y aplicaciones que sobre la red de la ESPOCH-DESITEL convergen y que necesitan un ancho de banda suficiente.

RECOMENDACIONES

1) De aceptar los equipos en producción técnicas de encolamiento se debería configurarlos con el propósito de brindar un trato diferenciado a ciertos tipos de tráfico de ser necesario.

2) Tomar en cuenta que al incorporar cámaras de red se debe considerar el formato de compresión con el cual trabajan, para de esta manera mantener al homogeneidad en la calidad de visualización de las imágenes y no afectar el rendimiento global del sistema.

3) Incorporar el sistema de video-vigilancia-IP a los múltiples servicios que sobre la infraestructura de red convergen, para de esta manera contar con una herramienta de monitorización que ayude a vigilancia y control.

4) Antes de pensar en incorporar un sistema de video-vigilancia-IP se debe considerar aspectos propios de la red como anchos de banda y equipamiento de dispositivos que permitan convergencia del servicio de video-IP en la red institucional..

RESUMEN

La presente tesis determina mediante estudios comparativos, qué técnica de encolamiento y formato de compresión de video tienen un desempeño óptimo en la transmisión de Video-IP sobre la red de la ESPOCH-DESITEL, para el desarrollo de un sistema software de video-vigilancia-IP.

Esta tesis se realizó mediante la utilización hardware de tecnología *Cisco* que provee de los routers, tecnología *Genius* en las cámaras IP y la infraestructura de red de la institución. En cuanto al software se utilizó tecnología *Borland* en la plataforma de desarrollo. Con todo esto se estableció un escenario, en el que se transmite video en vivo por la red y se realizan las pruebas con cada una de las técnicas de encolamiento a estudiar.

Para obtener los resultados en el estudio comparativo de las técnicas de encolamiento, se determinó como parámetro principal el *retrazo temporal* en milisegundos que sufre la transmisión de video-IP, por lo que se establece que la técnica **Custom Queuing (CQ)** es la que permite un mejor manejo de la congestión. En el caso de la elección del formato de compresión para la transmisión de video-IP el parámetro que determina dicha elección es la *Aplicación orientada,* es decir hacia qué tipo de aplicación se dirige la compresión del video, siendo el formato **MPEG** el que permite una compresión y calidad de imagen optimas. Con lo anterior se pudo desarrollar un sistema Software de video-vigilancia-IP que permite la visualización del video y administración de los recursos de todos los elementos incorporados a dicho sistema.

Se alcanzó el objetivo propuesto recomendándose que para la implementación del sistema se considere la evolución hacia entornos Web.

SUMMARY

The present thesis determines by means of comparative studies, how technical of encolamiento and format of video compression they have a good acting in the transmission of Video-IP on the net of the ESPOCH-DESITEL, for the development of a system software of video-surveillance-IP.

This thesis was carried out by means of the use hardware of technology Chaos that provides of the routers, technology Genius in the cameras IP and the infrastructure of net of the institution. As for the software technology Borland was used in the development platform. With all this a scenario settled down, in which live video is transmitted by the net and they are carried out the tests with each one from the encolamiento techniques to study.

To obtain the results in the comparative study of the encolamiento techniques, it was determined as main parameter the temporary retrazo in milisegundos that suffers the transmission of video-IP, for what settles down that the technical Custom Queuing (CQ) it is the one that allows a better handling of the congestion. In the case of the election of the compression format for the transmission of video-IP the parameter that determines this election is the guided Application, that is to say he/she goes the compression of the video toward what application type, being the format MPEG the one that allows a compression and good image quality. With the above-mentioned you could develop a system Software of video-surveillance-IP that allows the visualization of the video and administration of the resources from all the incorporate elements to this system.

The proposed objective was reached being recommended that it is considered the evolution toward environments Web for the implementation of the system.

GLOSARIO

Formato de compresión.

Estándar que permite comprimir video tratando de obtener un archivo de menor tamaño que el original y manteniendo la calidad

Encolamiento

Forma en la se pueden ordenar los paquetes de un determinado trafico en la salida de un router

Interfaces

Elementos hardware del router que permite la interconexión con la red.

Codificación

Técnica mediante la cual se puede digitalizar y comprimir una señal de video analógico en señal digital.

Video Afluente

Video que se transmite en forma continúa a través de una red de datos.

Software de Gestión

Software que permite administrar los recursos de un sistema de video-vigilancia-IP, así como visualizar la captura de las cámaras.

Transferencia

Envío de video desde la cámara hacia el software de gestión

BIBLIOGRAFIA

BIBLIOGRAFÍA DE INTERNET.

Calidad de servicio

http://www.it.uc3m.es/cgarcia/articulos/cita2002_diffserv.pdf
(2007-07-23)

http://iie.fing.edu.uy/ense/asign/perfredes/trabajos/trabajos_2003/diffserv/Trabajo%20Final.pdf
(2007-07-24)

Formatos de compresión de video

http://www.videoedicion.org/manuales/compresion/compresion.htm
(2007-12-08)

http://iie.fing.edu.uy/ense/asign/codif/material/monografias/2002-01.pdf
(2006-12-15)

http://www.digitalfotored.com/videodigital/compresionmpg.htm
(2007-12-19)

http://www.axis.com/products/video/about_networkvideo/compression.es.htm
(2008-09-25)

http://www.voxdata.com.ar/voxcompresionvideo.html
(2008-01-01)

http://es.wikipedia.org/wiki/MJPEG
(2008-01-01)

http://www.indigovision.com/files/international/IP-Cameras%20-%20Apr06-Spanish-Revised.pdf
(2008-01-01)

Técnicas de encolamiento

http://www.ciscopress.com/articles/article.asp?p=352991&seqNum=7&rl=1
(2007-08-14)

http://www.acm.org/crossroads/espanol/xrds7-5/july2001.html#floyd2
(2007-09-22)

http://www.inf.utfsm.cl/~jcanas/ramos/SistemasCom/Apuntes/tema4-1.pdf
(2007-09-25)

http://telcom2006.fing.edu.uy/trabajos/mvdtelcom-010.pdf
(2007-09-25)

http://support.microsoft.com/kb/233039/es
(2007-10-10)

http://www-2.dc.uba.ar/materias/tc/downloads/diapositivas/congestion-Peterson-en-castellano.ppt
(2007-11-05)

http://www.frc.utn.edu.ar/jar2006/docs/Papers/025-jar06.pdf
(2007-11-05)

Video-IP

http://www.axis.com/products/video/software/index.htm
(2007-07-14)

ANEXOS

Anexo 1. Encuesta al personal de seguridad de la ESPOCH

Personal de seguridad de la ESPOCH

Nombre:
Fecha:

1. Existe un sistema de vigilancia remota en la ESPOCH

   ……
   ……
   ……

2. Existen areas en las cuales es preciso un monitoreo permanente

   ……
   ……
   ……

3. Cree que el sistema actual de vigilancia personal es confiable

SI	
NO	

   ……
   ……..

4. Cree usted que se deveria desarrollar un sistema de video vigilancia remota

SI	
NO	

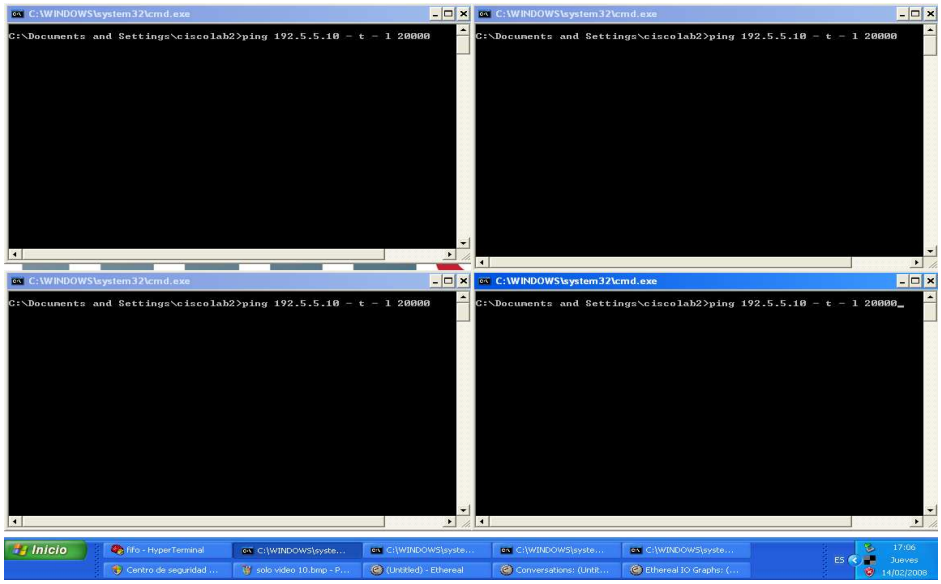
5. Se mejoraria el sistema actual de vigilancia si se desarrollara un sistema de video vigilancvia remota

SI	
NO	

6. Cuales son la areas o ubicaciones en las que se deberia implementar la video vigilancia remota

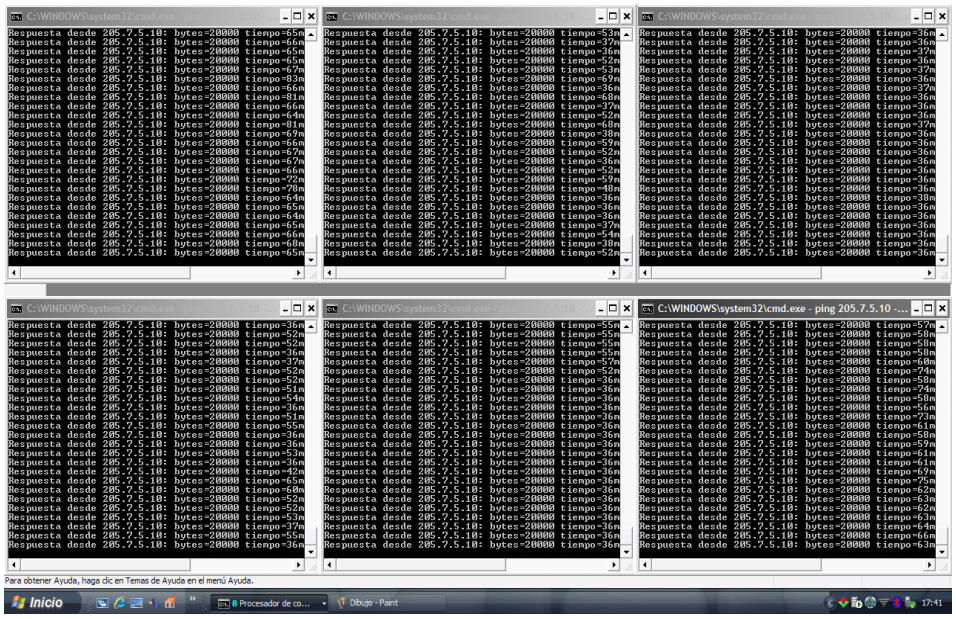
   ……
   ……

Anexo 2. Capturas de tiempos de retraso en las técnicas de encolamiento.

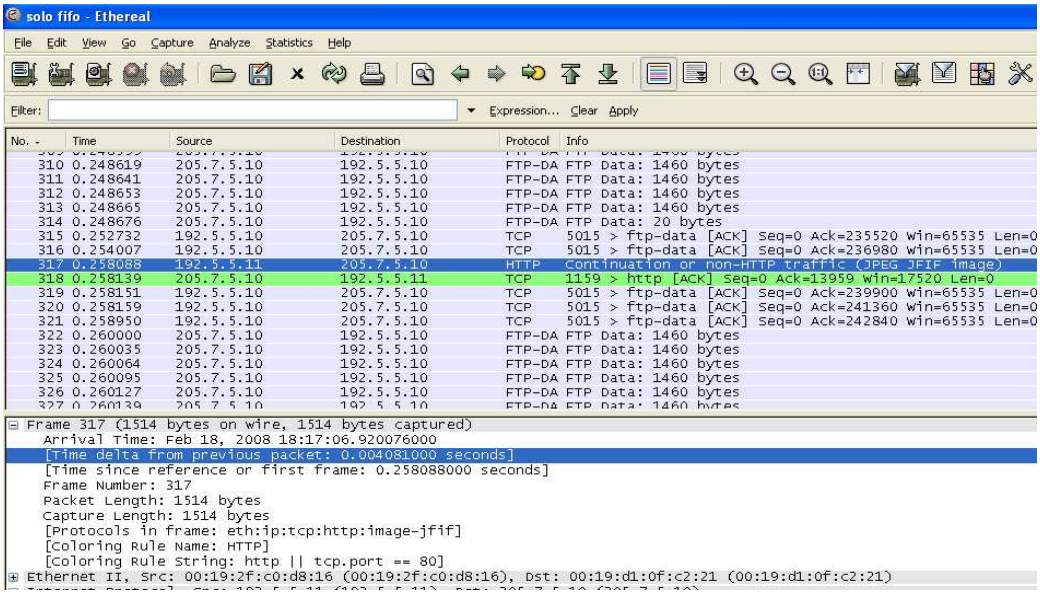


(a)

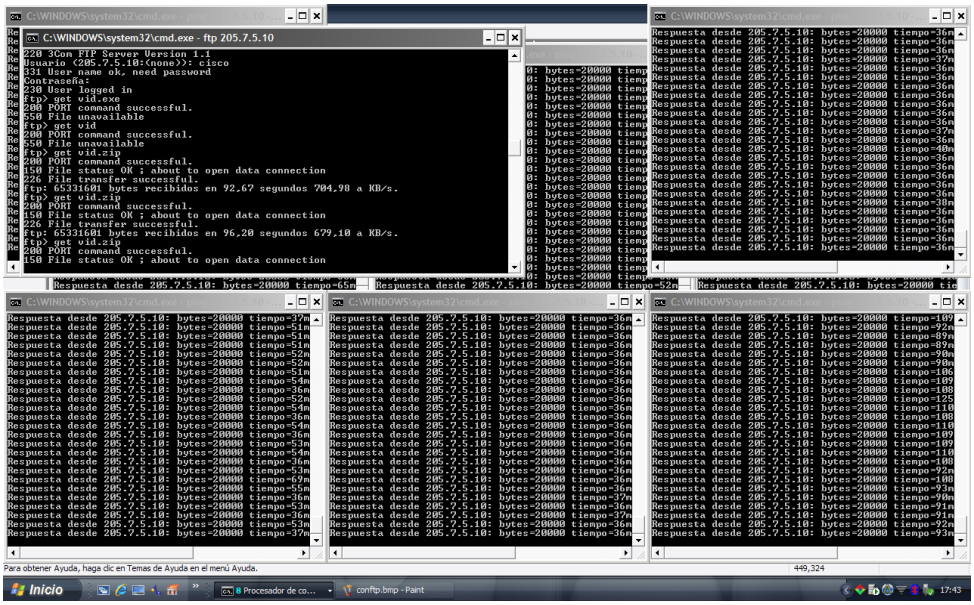
(b)


Respuesta desde 205.7.5.10: bytes=20000 tiempo=65m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=53m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=36m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=36m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=55m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=57m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=58m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=74m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=58m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=56m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=73m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=61m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=59m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=61m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=61m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=69m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=75m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=62m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=63m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=62m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=63m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=64m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=66m
Respuesta desde 205.7.5.10: bytes=20000 tiempo=63m
Para obtener Ayuda, haga clic en Temas de Ayuda en el menú Ayuda.
Inicio
Procesador de co...
Dibujo - Paint
17:41

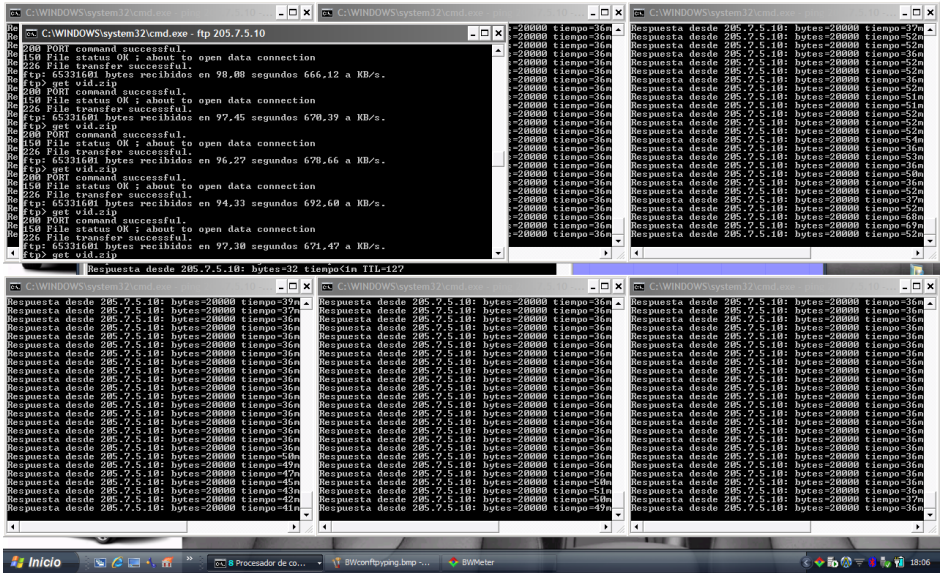
(c)


solo fifo - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
310 0.248619 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
311 0.248641 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
312 0.248653 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
313 0.248665 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
314 0.248676 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 20 bytes
315 0.252732 192.5.5.10 205.7.5.10 TCP 5015 > ftp-data [ACK] Seq=0 Ack=235520 Win=65535 Len=0
316 0.254007 192.5.5.10 205.7.5.10 TCP 5015 > ftp-data [ACK] Seq=0 Ack=236980 Win=65535 Len=0
317 0.258088 192.5.5.11 205.7.5.10 HTTP Continuation or non-HTTP traffic (JPEG JFIF image)
318 0.258139 205.7.5.10 192.5.5.11 TCP 1159 > http [ACK] Seq=0 Ack=13959 Win=17520 Len=0
319 0.258151 192.5.5.10 205.7.5.10 TCP 5015 > ftp-data [ACK] Seq=0 Ack=239900 Win=65535 Len=0
320 0.258159 192.5.5.10 205.7.5.10 TCP 5015 > ftp-data [ACK] Seq=0 Ack=241360 Win=65535 Len=0
321 0.258950 192.5.5.10 205.7.5.10 TCP 5015 > ftp-data [ACK] Seq=0 Ack=242840 Win=65535 Len=0
322 0.260000 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
323 0.260035 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
324 0.260064 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
325 0.260095 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
326 0.260127 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
Frame 317 (1514 bytes on wire, 1514 bytes captured)
Arrival Time: Feb 18, 2008 18:17:06.920076000
[Time delta from previous packet: 0.004081000 seconds]
[Time since reference or first frame: 0.258088000 seconds]
Frame Number: 317
Packet Length: 1514 bytes
Capture Length: 1514 bytes
[Protocols in frame: eth:ip:tcp:http:image-jfif]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80]
Ethernet II, Src: 00:19:2f:c0:d8:16 (00:19:2f:c0:d8:16), Dst: 00:19:d1:0f:c2:21 (00:19:d1:0f:c2:21)

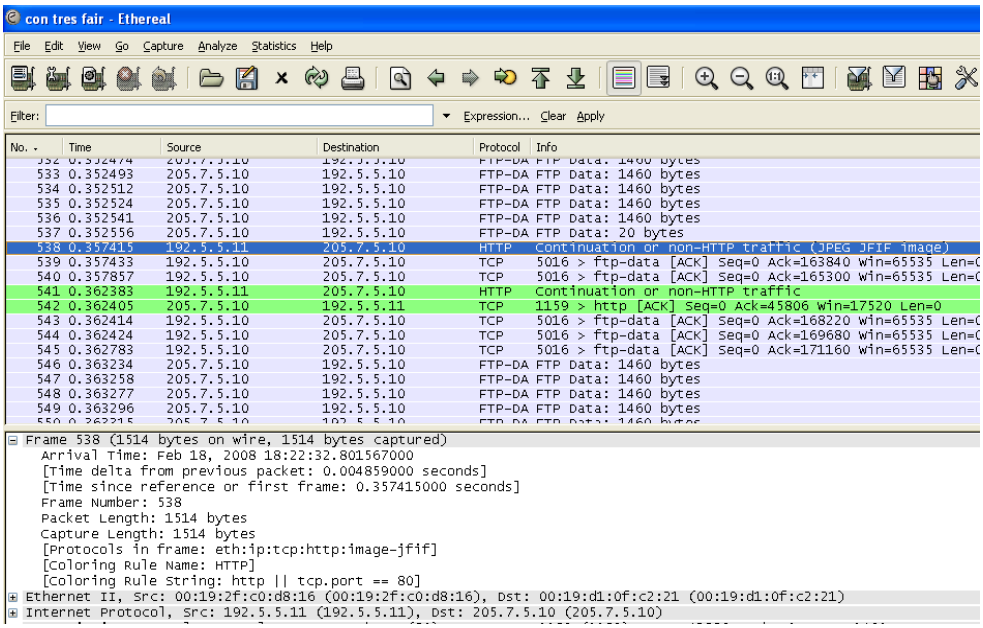
(d)


C:\WINDOWS\system32\cmd.exe - ftp 205.7.5.10
220 3Com FTP Server Version 1.1
Usuario (205.7.5.10:(none)): cisco
331 User name ok, need password
Contraseña:
230 User logged in
ftp> get vid.exe
200 PORT command successful.
550 File unavailable
ftp> get vid
200 PORT command successful.
550 File unavailable
ftp> get vid.zip
200 PORT command successful.
150 File status OK ; about to open data connection
226 File transfer successful.
ftp: 65331601 bytes recibidos en 92,67 segundos 704,98 a KB/s.
ftp> get vid.zip
200 PORT command successful.
150 File status OK ; about to open data connection
226 File transfer successful.
ftp: 65331601 bytes recibidos en 96,20 segundos 679,10 a KB/s.
ftp> get vid.zip
200 PORT command successful.
150 File status OK ; about to open data connection
Respuesta desde 205.7.5.10: bytes=20000 tiempo=36m
Para obtener Ayuda, haga clic en Temas de Ayuda en el menú Ayuda.
Inicio
conftp.bmp - Paint

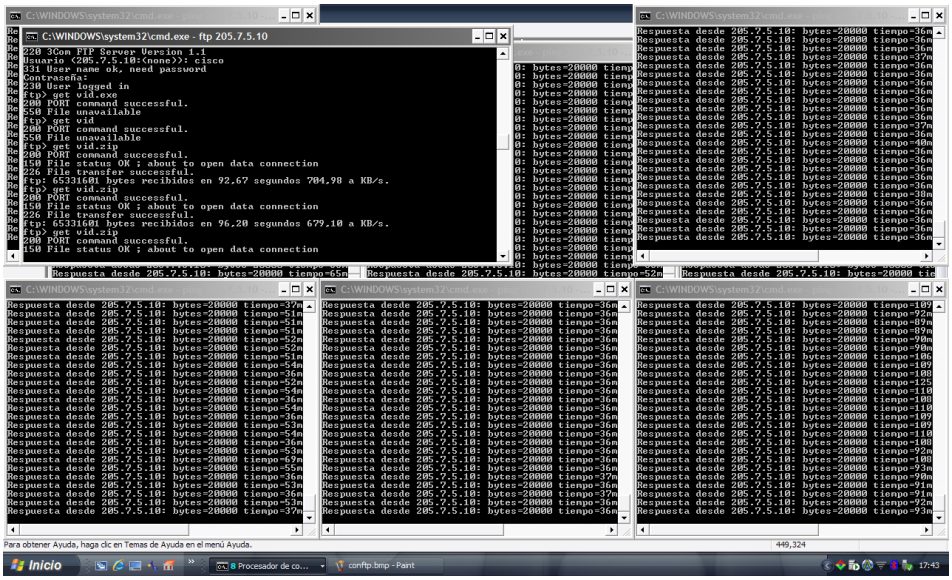
(e)


C:\WINDOWS\system32\cmd.exe - ftp 205.7.5.10
200 PORT command successful.
150 File status OK ; about to open data connection
226 File transfer successful.
ftp: 65331601 bytes recibidos en 98,08 segundos 666,12 a KB/s.
ftp> get vid.zip
200 PORT command successful.
150 File status OK ; about to open data connection
226 File transfer successful.
ftp: 65331601 bytes recibidos en 97,45 segundos 670,39 a KB/s.
ftp> get vid.zip
200 PORT command successful.
150 File status OK ; about to open data connection
226 File transfer successful.
ftp: 65331601 bytes recibidos en 96,27 segundos 678,66 a KB/s.
ftp> get vid.zip
200 PORT command successful.
150 File status OK ; about to open data connection
226 File transfer successful.
ftp: 65331601 bytes recibidos en 94,33 segundos 692,60 a KB/s.
ftp> get vid.zip
200 PORT command successful.
150 File status OK ; about to open data connection
226 File transfer successful.
ftp: 65331601 bytes recibidos en 97,30 segundos 671,47 a KB/s.
ftp> get vid.zip
Respuesta desde 205.7.5.10: bytes=32 tiempo<1m TTL=127
Inicio
BWconftpping.bmp -...
BWMeter

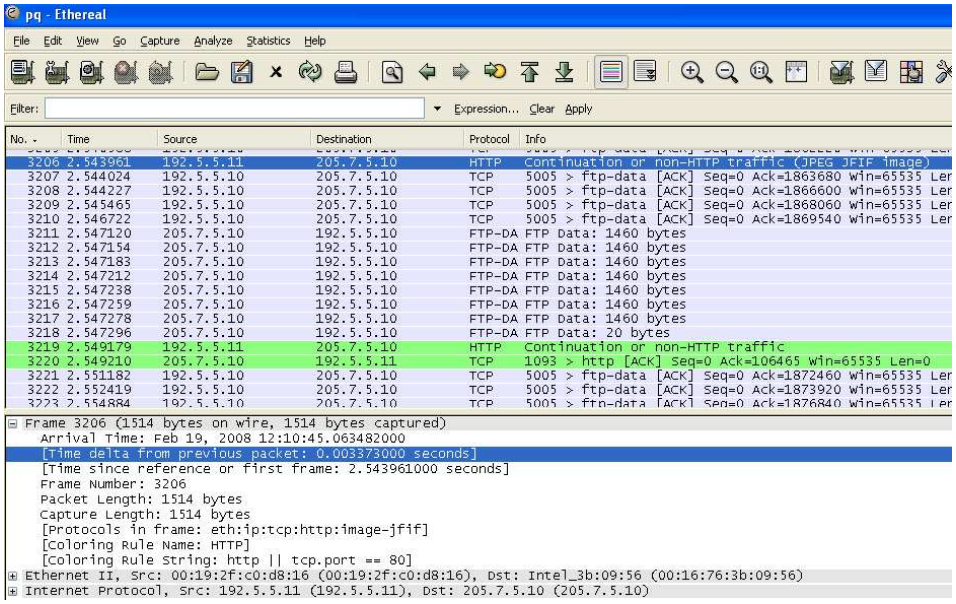
(f)


con tres fair - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
533 0.352493 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
534 0.352512 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
535 0.352524 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
536 0.352541 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
537 0.352556 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 20 bytes
538 0.357415 192.5.5.11 205.7.5.10 HTTP Continuation or non-HTTP traffic (JPEG JFIF image)
539 0.357433 192.5.5.10 205.7.5.10 TCP 5016 > ftp-data [ACK] Seq=0 Ack=163840 Win=65535 Len=0
540 0.357857 192.5.5.10 205.7.5.10 TCP 5016 > ftp-data [ACK] Seq=0 Ack=165300 Win=65535 Len=0
541 0.362383 192.5.5.11 205.7.5.10 HTTP Continuation or non-HTTP traffic
542 0.362405 205.7.5.10 192.5.5.11 TCP 1159 > http [ACK] Seq=0 Ack=45806 Win=17520 Len=0
543 0.362414 192.5.5.10 205.7.5.10 TCP 5016 > ftp-data [ACK] Seq=0 Ack=168220 Win=65535 Len=0
544 0.362424 192.5.5.10 205.7.5.10 TCP 5016 > ftp-data [ACK] Seq=0 Ack=169680 Win=65535 Len=0
545 0.362783 192.5.5.10 205.7.5.10 TCP 5016 > ftp-data [ACK] Seq=0 Ack=171160 Win=65535 Len=0
546 0.363234 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
547 0.363258 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
548 0.363277 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
549 0.363296 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
Frame 538 (1514 bytes on wire, 1514 bytes captured)
Arrival Time: Feb 18, 2008 18:22:32.801567000
[Time delta from previous packet: 0.004859000 seconds]
[Time since reference or first frame: 0.357415000 seconds]
Frame Number: 538
Packet Length: 1514 bytes
Capture Length: 1514 bytes
[Protocols in frame: eth:ip:tcp:http:image-jfif]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80]
Ethernet II, Src: 00:19:2f:c0:d8:16 (00:19:2f:c0:d8:16), Dst: 00:19:d1:0f:c2:21 (00:19:d1:0f:c2:21)
Internet Protocol, Src: 192.5.5.11 (192.5.5.11), Dst: 205.7.5.10 (205.7.5.10)

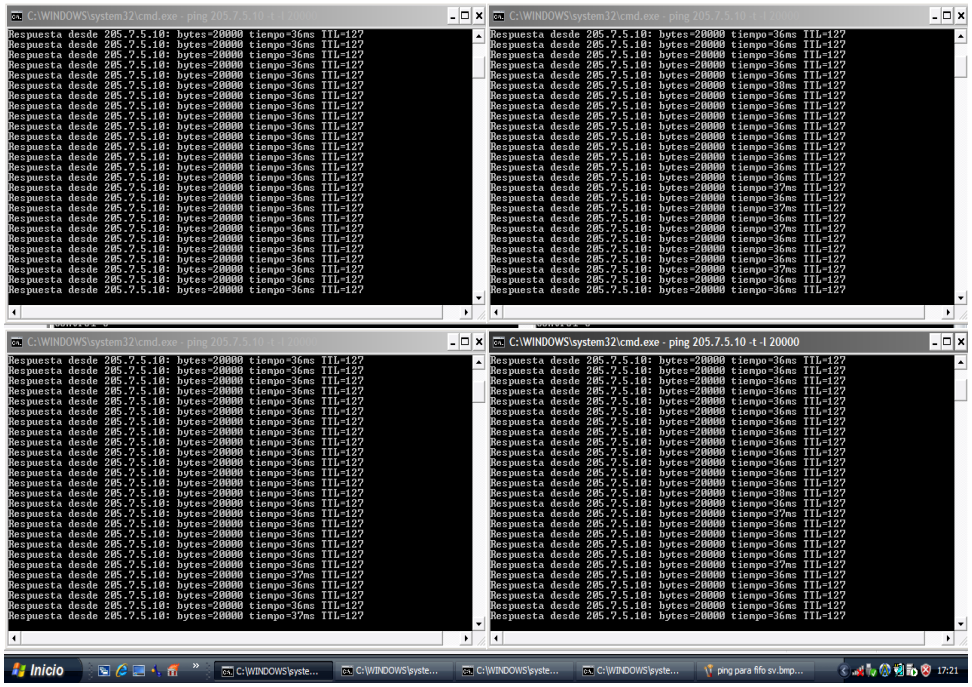
(g)


C:\WINDOWS\system32\cmd.exe - ftp 205.7.5.10
220 3Com FTP Server Version 1.1
Usuario (205.7.5.10:(none)): cisco
331 User name ok, need password
Contraseña:
230 User logged in
ftp> get vid.exe
200 PORT command successful.
550 File unavailable
ftp> get vid
200 PORT command successful.
550 File unavailable
ftp> get vid.zip
200 PORT command successful.
150 File status OK ; about to open data connection
226 File transfer successful.
ftp: 6533168l bytes recibidos en 92,67 segundos 704,98 a KB/s.
ftp> get vid.zip
200 PORT command successful.
150 File status OK ; about to open data connection
226 File transfer successful.
ftp: 6533168l bytes recibidos en 96,20 segundos 679,10 a KB/s.
ftp> get vid.zip
200 PORT command successful.
150 File status OK ; about to open data connection
Respuesta desde 205.7.5.10: bytes=20000 tiempo=36m
Para obtener Ayuda, haga clic en Temas de Ayuda en el menú Ayuda.
Inicio
conftp.bmp - Paint

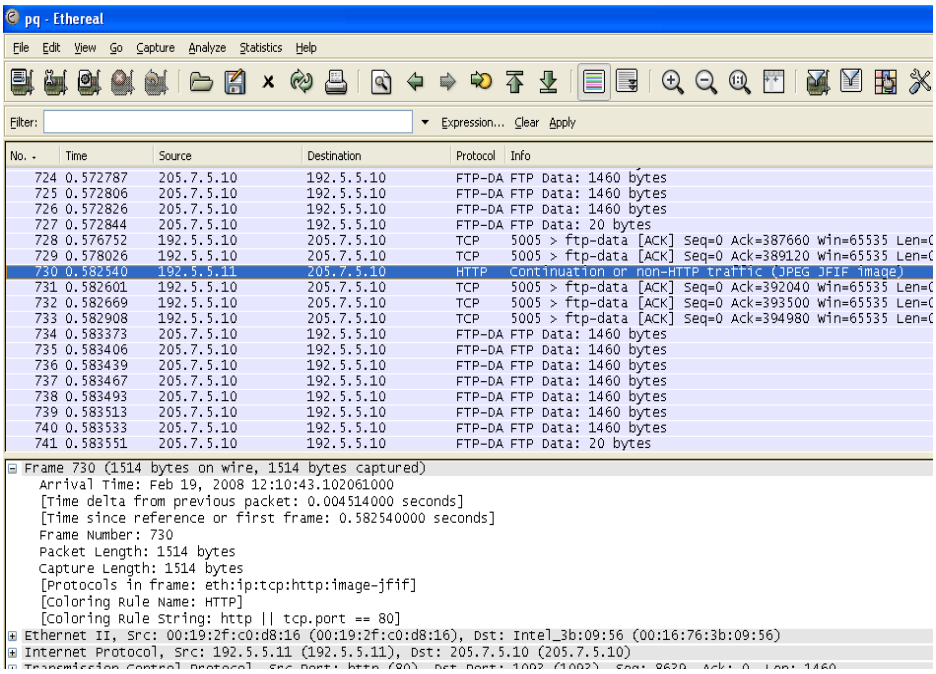
(h)


pq - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. - Time Source Destination Protocol Info
3206 2.543961 192.5.5.11 205.7.5.10 HTTP Continuation or non-HTTP traffic (JPEG JFIF image)
3207 2.544024 192.5.5.10 205.7.5.10 TCP 5005 > ftp-data [ACK] Seq=0 Ack=1863680 Win=65535 Len
3208 2.544227 192.5.5.10 205.7.5.10 TCP 5005 > ftp-data [ACK] Seq=0 Ack=1866600 Win=65535 Len
3209 2.545465 192.5.5.10 205.7.5.10 TCP 5005 > ftp-data [ACK] Seq=0 Ack=1868060 Win=65535 Len
3210 2.546722 192.5.5.10 205.7.5.10 TCP 5005 > ftp-data [ACK] Seq=0 Ack=1869540 Win=65535 Len
3211 2.547120 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
3212 2.547154 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
3213 2.547183 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
3214 2.547212 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
3215 2.547238 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
3216 2.547259 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
3217 2.547278 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
3218 2.547296 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 20 bytes
3219 2.549179 192.5.5.11 205.7.5.10 HTTP Continuation or non-HTTP traffic
3220 2.549210 205.7.5.10 192.5.5.11 TCP 1093 > http [ACK] Seq=0 Ack=106465 Win=65535 Len=0
3221 2.551182 192.5.5.10 205.7.5.10 TCP 5005 > ftp-data [ACK] Seq=0 Ack=1872460 Win=65535 Len
3222 2.552419 192.5.5.10 205.7.5.10 TCP 5005 > ftp-data [ACK] Seq=0 Ack=1873920 Win=65535 Len
Frame 3206 (1514 bytes on wire, 1514 bytes captured)
Arrival Time: Feb 19, 2008 12:10:45.063482000
[Time delta from previous packet: 0.003373000 seconds]
[Time since reference or first frame: 2.543961000 seconds]
Frame Number: 3206
Packet Length: 1514 bytes
Capture Length: 1514 bytes
[Protocols in frame: eth:ip:tcp:http:image-jfif]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80]
Ethernet II, Src: 00:19:2f:c0:d8:16 (00:19:2f:c0:d8:16), Dst: Intel_3b:09:56 (00:16:76:3b:09:56)
Internet Protocol, Src: 192.5.5.11 (192.5.5.11), Dst: 205.7.5.10 (205.7.5.10)

(i)


C:\WINDOWS\system32\cmd.exe - ping 205.7.5.10 -t -l 20000
Respuesta desde 205.7.5.10: bytes=20000 tiempo=36ms TTL=127
Inicio

(j)


pq - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
724 0.572787 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
725 0.572806 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
726 0.572826 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
727 0.572844 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 20 bytes
728 0.576752 192.5.5.10 205.7.5.10 TCP 5005 > ftp-data [ACK] Seq=0 Ack=387660 Win=65535 Len=0
729 0.578026 192.5.5.10 205.7.5.10 TCP 5005 > ftp-data [ACK] Seq=0 Ack=389120 Win=65535 Len=0
730 0.582540 192.5.5.11 205.7.5.10 HTTP Continuation or non-HTTP traffic (JPEG JFIF image)
731 0.582601 192.5.5.10 205.7.5.10 TCP 5005 > ftp-data [ACK] Seq=0 Ack=392040 Win=65535 Len=0
732 0.582669 192.5.5.10 205.7.5.10 TCP 5005 > ftp-data [ACK] Seq=0 Ack=393500 Win=65535 Len=0
733 0.582908 192.5.5.10 205.7.5.10 TCP 5005 > ftp-data [ACK] Seq=0 Ack=394980 Win=65535 Len=0
734 0.583373 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
735 0.583406 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
736 0.583439 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
737 0.583467 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
738 0.583493 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
739 0.583513 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
740 0.583533 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 1460 bytes
741 0.583551 205.7.5.10 192.5.5.10 FTP-DA FTP Data: 20 bytes
Frame 730 (1514 bytes on wire, 1514 bytes captured)
Arrival Time: Feb 19, 2008 12:10:43.102061000
[Time delta from previous packet: 0.004514000 seconds]
[Time since reference or first frame: 0.582540000 seconds]
Frame Number: 730
Packet Length: 1514 bytes
Capture Length: 1514 bytes
[Protocols in frame: eth:ip:tcp:http:image-jfif]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80]
Ethernet II, Src: 00:19:2f:c0:d8:16 (00:19:2f:c0:d8:16), Dst: Intel_3b:09:56 (00:16:76:3b:09:56)
Internet Protocol, Src: 192.5.5.11 (192.5.5.11), Dst: 205.7.5.10 (205.7.5.10)

(k)

Anexo 3. MANUAL DE USUARIO

SWIP ®
Sistema de Video Vigilancia IP

Manual de Usuario

1. VISIÓN GENERAL

1.1. ¿Qué es SWIP?

SWIP Sistema de Video Vigilancia IP, es un prototipo que fue implementado para apoyar las labores de vigilancia del departamento de Guardianía de la Escuela Superior Politécnica de Chimborazo- DESITEL.

Este sistema aprovecha la infraestructura existente tanto hardware como software reduciendo al máximo los costos de una posible implantación y perfeccionamiento del sistema; su propósito es demostrar el desempeño de un nuevo servicio como es el video IP sobre la Intranet de la Espoch, el cual funcionará en forma paralela con los servicios existentes.

SWIP ha sido diseñado como un sistema dedicado y al régimen de la institución politécnica, posee una interfaz muy fácil de navegación, componentes de reproducción y grabación de video simples e intuitivos, así como asistentes para registro de dispositivos (cámaras IP) y sus posibles actualizaciones y eliminaciones ajustables a la necesidad del usuario.

Es un sistema desarrollado bajo arquitectura Cliente/Servidor Multicapa que posee una robusta base de datos para la organización de información del Sistema de Video Vigilancia IP

Dentro de los beneficios que el sistema brindará se sustenta la posibilidad de una seguridad sólida por parte de los departamentos conectados a la red. Mejoras en los aspectos de productividad, confiabilidad, seguridad y en sí todas las características que proporcionan la automatización.

2. VISIÓN DEL PRODUCTO

2.1. Ámbito descriptivo

SWIP constituye un elemento estratégico para el apoyo a la vigilancia y seguridad dentro de un ambiente institucional como lo es la ESPOCH. Como resultado de los procesos de video vigilancia describimos los siguientes puntos:

- Incrementar el nivel de vigilancia de acuerdo a la permanencia y disponibilidad de dispositivos de video.

- Optimizar las funciones del personal de guardianía a través de vigilancia desatendida (grabación de video vigilancia)

- Prevenir los procesos seguridad del personal de guardianía a través de la vigilancia remota que ofrece el sistema.

2.2. Perspectiva del producto

El Producto es construido con componentes de exploración bajo el estándar de Windows proporcionando de ésta forma una interfaz muy sencilla e intuitiva, su diseño lo hace fácil de manejar incluso para usuarios inexpertos y no posee demasiadas ventanas para petición d e datos de usuario.

3. REQUISITOS DEL SISTEMA

Los requisitos mínimos de hardware o del sistema de cómputo y de software de Sistema Operativo para un desempeño normal de la aplicación son los siguientes:

3.1. Requisitos hardware

Sistema Cliente:

Procesador Pentium IV de 1.2 GHz
Memoria RAM 512Mb
Disco Duro de 80 Gb
Tarjeta de Red 10/100
CD-Rom 48x
Teclado, Mouse genéricos

Sistema Servidor:

Procesador Pentium IV de 2,6Gb o superior
Memoria RAM de 1Gb
Disco Duro de 500Gb
Tarjeta de Red 10/100
CD-Rom 48x
Teclado, Mouse genéricos

3.2. Requisitos software

Sistema Cliente:

Sistema Operativo Windows 98 o superior
Protocolos TCP/IP
Componente XPlug OCX

Sistema Servidor:

Sistema Operativo Windows XP, 2003 Server o superior
Service Pack II
Servicio de Componentes Com+

Protocolos TCP/IP

4. INSTALACIÓN DEL SISTEMA

4.1. Instalación del sistema de base de datos

a. Inserte el CD de Microsoft SQL Server 2000
b. Seleccione **Componentes de SQL Server 2000**
c. En el siguiente menú seleccione la opción de **Instalar Servidor de base de Datos**
d. A continuación presione el botón siguiente del asistente de instalación
e. En las opciones de nombre del equipo seleccione **Equipo local** y a continuación presione el botón siguiente
f. En las opciones de selección de instalación, escoja **Crear una nueva instancia de SQL Server o instalar herramientas cliente**, y posteriormente presionamos el botón siguiente del asistente de instalación.
g. En la ventana de información del usuario aparecerá los datos por defecto que se ingresó en el momento de instalación del sistema; es importante que no cambie estos datos ya que se utilizará la autenticación del sistema local (en este caso del servidor).
h. A continuación, se presenta el contrato de instalación del software, presione siguiente para continuar con la instalación.
i. En la ventana de definición de instalación que aparece a continuación en el asistente, seleccione la opción de **Herramientas cliente y servidor** para posteriormente presionar el botón siguiente.
j. En la ventana de **Nombre de instalación**, asegúrese de que está seleccionada la casilla **Predeterminada,** para posteriormente presionar el botón siguiente del asistente
k. A continuación aparece la ventana de **Tipo de instalación** en la cual solicita esta información. Seleccionamos la opción **Típica** y seguidamente presionamos el botón siguiente de la ventana del asistente.
l. En la ventana de **Cuentas de servicio** seleccionamos la opción como se muestra en la figura: Utilizar la misma cuenta para cada servicio**.** Iniciar

automáticamente el servicio de SQL Server. Y, en el apartado de Configuración del servicio seleccionamos: Utilizar la cuenta del sistema local; finalmente presionamos el botón siguiente para continuar con la instalación

m. En la siguiente ventana del asistente seleccionamos **Modo de autenticación de Windows** y presionamos el botón siguiente.
n. En la ventana de iniciar la copia de archivos presionamos siguiente.
o. Para terminar, luego de algunos minutos en los cuales se realiza el copiado de los archivos necesarios para la aplicación, el asistente muestra una ventana que indica la finalización del proceso de instalación y procedemos a presionar el botón finalizar.

4.2. Instalación del sistema SWIP

a. Insertamos el CD de Instalación de SWIP
b. Presionamos el botón **Next** en el asistente de instalación del sistema
c. Presionamos **Next** en la ventana de información del usuario
d. Presionamos **Next** en la ventana de Directorio de destino que es la dirección en donde se va a instalar los archivos necesarios de la aplicación y, para que por defecto sea: “C:\Archivos de Programa\Sistemas\SWIP” ya que es importante tener en cuenta esta dirección para configuraciones posteriores.
e. Presionamos el botón **Next** del asistente de instalación para que seleccione el grupo de programas o carpeta de programas por defecto del sistema.
f. Click principal en el botón Next del asistente para iniciar la copia de archivos
g. Finalmente hacemos click principal en el botón finish para cerrar el asistente de instalación

4.3. Creación de la base de datos SWIP

a. Abrir el administrador corporativo, haciendo click principal en inicio-Todos posprogramas-Microsoft SQL Server-Administrador corporativo. Como se muestra en la figura.

b. En el administrador corporativo, desplegamos el árbol de componentes y seleccionamos dentro del servidor local la carpeta **Base de datos** haciendo click secundario en la misma.
c. En el menú emergente seleccionamos la opción **Todas las tareas** y en el submenú, la opción **Adjuntar base de datos,** luego de esto aparecerá una ventana como se muestra en la gráfica siguiente:
d. En dicha ventana seleccionamos el archivo de Base de Datos del Sistema, el cual se anexa en el momento de la instalación del sistema SWIP. El archivo está con la siguiente dirección:
   C:\Archivos de programa\Sistemas\SWIP_Data.MDF
e. Luego de seleccionar el archivo en dicha dirección observamos los archivos anexados de base de datos; presionamos el botón aceptar para que se efectúe el proceso de adjuntar la base de datos del sistema SWIP
f. Finalmente se adjunta la base de datos y aparece una ventana de información del proceso realizado.
g. Como se muestra en la gráfica, la base de datos de SWIP, ya está dentro de la consola del **administrador** corporativo de SQL

4.4. Creación del Proxy para los sistemas clientes

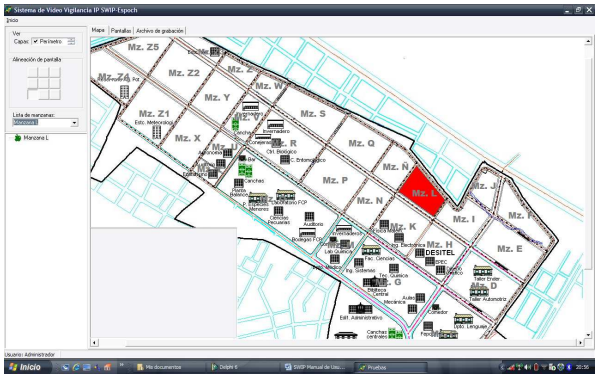
Abrir el servicio de componentes del Servidor

a. Hacemos click en inicio-Panel de control y posteriormente ubicamos el ícono de Herramientas administrativas y, servicios de componentes.
b. Al abrir el servicio de componentes, despliegue el árbol hasta localizar la carpeta de **Aplicaciones Com +**, click secundario en esta carpeta, seleccionamos la opción **Nuevo** y en el submenú **Aplicación.**
c. En el asistente para nuevos componentes presionamos siguiente y a continuación seleccionamos la opción crear una aplicación vacía.
d. A continuación ingresamos un nuevo nombre para la nueva aplicación y en tipo de activación seleccionamos la opción de Aplicación del servidor.
e. Para establecer la identidad de la aplicación, en **Cuenta** seleccionamos la opción **Usuario interactivo: usuario con sesión iniciada actualmente.**
f. Luego procedemos a finalizar el asistente de creación de componentes
g. A continuación procedemos a generar un nuevo componente seleccionando la carpeta **Componentes** del componente **Com_SWIP**, haciendo click secundario y en el menú emergente escogemos la opción **Nuevo** y en el submenú **Componente.**

h. En el asistente que aparecerá a continuación para la instalación de componentes Com+ seleccionamos la opción instalar nuevos componentes.
i. Buscamos los archivos necesarios para la instalación de componentes.

5. ENTORNO DEL FORMULARIO PRINCIPAL

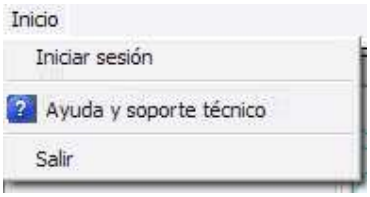
El formulario principal del sistema SWIP está diseñado mediante una interfaz SDI (Interfaz Simple de documento) el cual permite que se ejecute una sola aplicación del mismo tipo a la vez.



Estructura del Menú Principal

Para poder desarrollar las tareas más comunes del sistema se debe conocer al detalle todas las opciones del menú que nos ofrece el entorno, para ello tenemos dos tipos de menú los cuales no se presenta de forma simultáneas, es decir que existe un menú para cuando no está ninguna sesión abierta y existe otro menú muy diferente para cuando una sesión está activa.

El menú para cuando no está ninguna sesión abierta es el siguiente

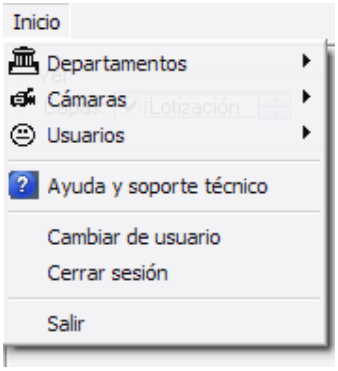


Iniciar sesión.- Esta opción genera un formulario para el acceso al sistema mediante un inicio de sesión el cual pide un nombre de usuario y una contraseña.

Ayuda y soporte Técnico.- Es una opción que muestra ayuda en línea e información del sistema.

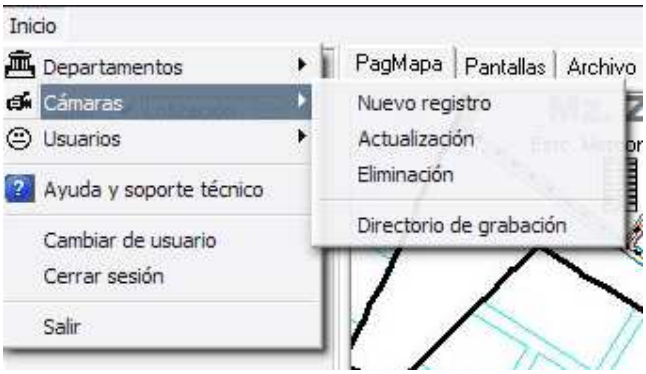
Salir.- Es la opción general de salir del sistema SWIP, al seleccionar esta opción se abre un mensaje de confirmación o cancelación con el cual abandona la aplicación o cancela dicha acción.

El menú para cuando una sesión está abierta es el siguiente

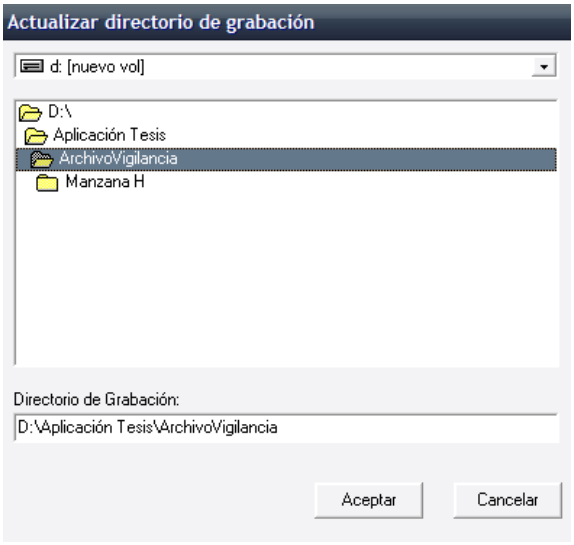


Departamentos.- Esta opción del menú, abre a su vez un submenú, el cual permite realizar procesos con los Departamentos registrados en la base de datos del sistema SWIP, es decir que podemos agregar un nuevo registro, Actualizar uno existente o eliminarlo.

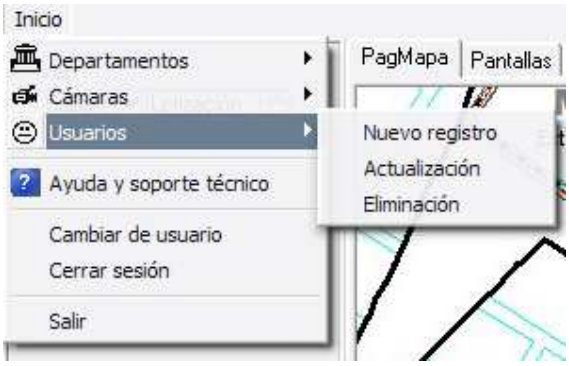
Cámaras.- Similar a la opción anterior, es decir que agrega, actualiza o elimina un registro de cámara en este caso para la base de datos del sistema.
Cabe mencionar que posee una opción adicional que es **Directorio de grabación.** Al hacer click en esta opción se muestra una ventana que permite actualizar el directorio de grabación



Directorio de grabación.- Esta opción muestra la ventana que se muestra a continuación y permite informar y/o actualizar el directorio en donde se almacenan los archivos grabados de las cámaras de vigilancia.



Usuarios.- La opción es similar a las primeras (Departamentos y cámaras), y muestra un submenú para registrar, actualizar o eliminar un usuario del sistema.



Cambiar de usuario.- Esta opción permite ejecutar dos procesos en el sistema. El primero desactiva todas las opciones, haciendo que el sistema cierre la sesión existente; El segundo proceso hace que se muestre la ventana de autenticación de usuario el cual permite iniciar una sesión luego de haber autentificado los datos.

Cerrar sesión.- Esta opción solamente desactiva todas las opciones del sistema y cierra la sesión actual.

6. ENTORNO DEL FORMULARIO DE AUTENTICACIÓN

El formulario de autenticación es la interfaz utilizada para iniciar una sesión y para que se puedan activar las opciones del sistema SWIP.

El formulario se muestra de dos formas:

a) la primera muestra el formulario con sus campos definidos como se muestra en la gráfica, y esta se presenta cuando se va a iniciar una sesión

1. **Usuario.-** Campo siempre visible, es una caja de texto donde el usuario ingresa su nombre
2. **Contraseña.-** Campo siempre visible, es un componente en el que se ingresa la contraseña

3. **Botones Aceptar y Cancelar.-** Como su nombre lo indica son botones para aceptar el acceso al sistema o cancelarlo si se desea.

4. **reintentar y recordatorio.-** Son dos links, el primero: *reintentar.-* sirve para intentar de nuevo autentificarse al pinchar este link las entradas de **Usuario** y **Contraseña** se borran automáticamente para que el usuario trate de autentificarse nuevamente.
   recordatorio.- muestra los componentes necesarios para ingresar datos para mostrar el recordatorio del usuario. Es decir que muestra un segundo modelo del formulario de autenticación el cual vamos a detallar a continuación en el item b)

b) La segunda muestra el formulario solicitando datos al usuario para recordar su contraseña y esta se muestra cuando el usuario ingreso mal sus datos de autenticación

1. **Tipo.-** Muestra la lista de tipos de usuario, debe elegir uno y a continuación; **Usuario.-** En éste componente se ingresa el nombre de usuario como uno de los datos para mostrar su recordatorio

2. **Su recordatorio es:** Después de ésta etiqueta se muestra el texto de recordatorio que el usuario ingresó en el registro de usuarios.

3. **Cancelar.-** Al presionar éste botón se cierra el formulario de acceso al sistema.

4. **Mostrar recordatorio.-** Luego de llenar los campos necesarios en el formulario y, al presionar éste vínculo, se muestra el texto de recordatorio después de la etiqueta descrita en el Item 2.

7. ABRIR EL SISTEMA SWIP

Cuando se instala una aplicación en el sistema, el instalador deposita un acceso directo en la carpeta grupo de programas del menú inicio. El sistema SWIP no es una excepción ya que cumple los mismos estándares, de ésta forma se puede acceder al sistema de la misma forma que se accede a otros programas instalados.

7.1. Ejecutar la aplicación

Para ejecutar la aplicación se debe seguir la siguiente secuencia:
Inicio-Todos los programas-Sistemas-SWIP

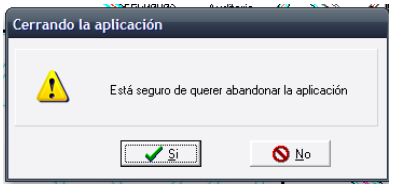
7.2. Abrir una sesión

Luego de iniciado el sistema seleccione **Inicio** del menú principal y a continuación escoja la opción **Iniciar sesión**

Una vez que haya escogido esta opción aparecerá el **Formulario de autenticación,** para una mejor referencia remítase a **Entorno del Formulario de Autenticación**

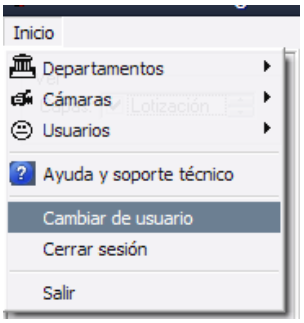
8. CERRAR EL SISTEMA SWIP

Al igual que toda aplicación instalada en el sistema, SWIP se puede cerrar haciendo click en el botón de cerrar la ventana; esto provoca que las sesiones abiertas se cierren automáticamente y que las grabaciones actuales en ese momento se detengan, por lo cual antes de cerrar el sistema aparece un formulario de confirmación del sistema como el que se muestra en la gráfica siguiente.



8.1. Cambiar de Usuario

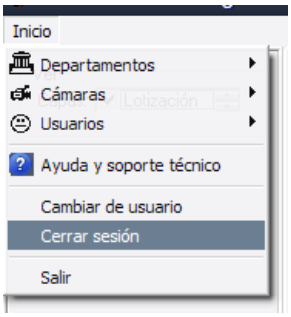
Para cambiar de usuario seleccione la siguiente secuencia en el menú principal: **Inicio-Cambiar de usuario**



Al seleccionar esta opción se ejecutan dos procesos; remítase al Item **Cambiar de usuario** en el apartado de Estructura del menú principal en **ENTORNO DEL FORMULARIO PRINCIPAL** del tema 5 de éste manual

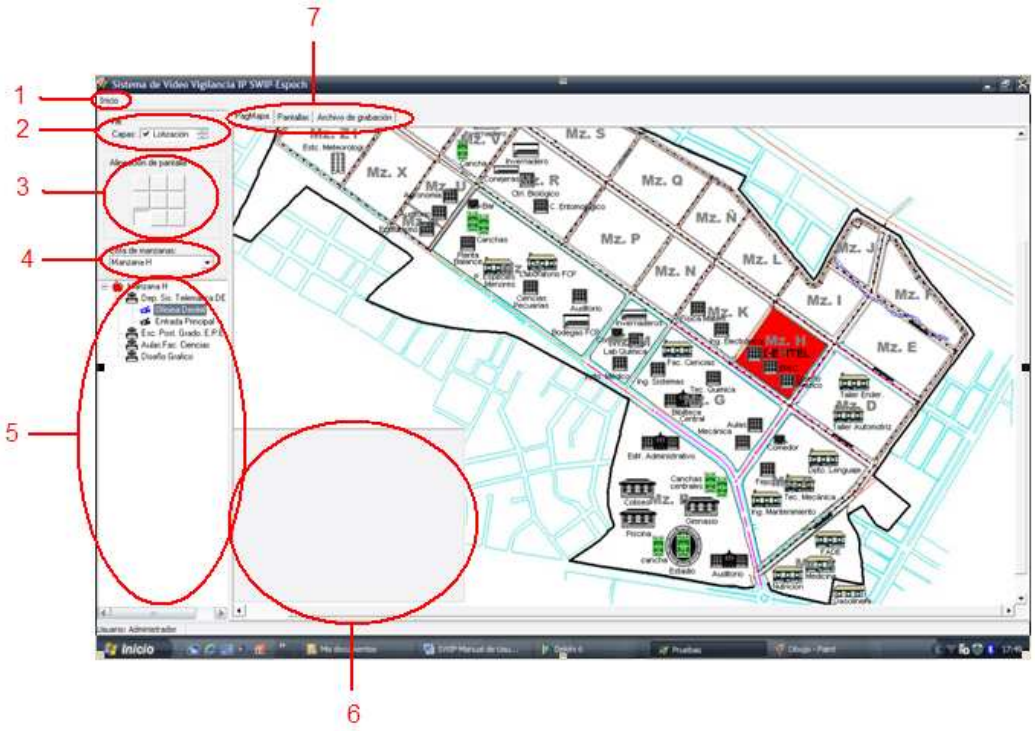
8.2. Cerrar sesión

Esta opción permite cerrar una sesión deshabilitando de esta forma las opciones del sistema, para cerrar una sesión seleccione la siguiente secuencia en el menú principal del sistema: **Inicio-Cerrar sesión**

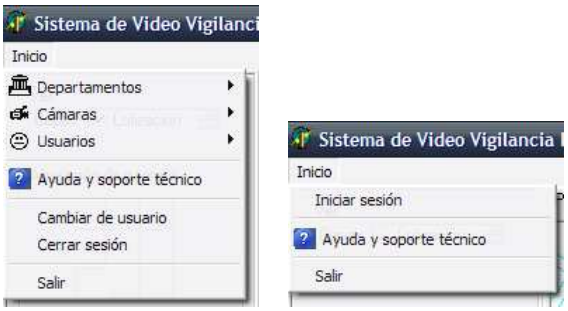


9. FUNCIONES DE NAVEGACIÓN

El sistema SWIP posee componentes de navegación y despliega la información de forma ordenada y controlada para lo cual vamos a describir todas las funciones de navegación.

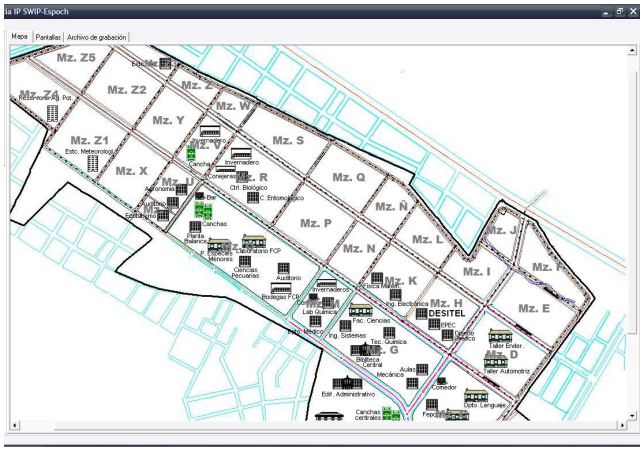


1. **Menú principal del sistema:** El menú principal se muestra de dos formas: la primera está presente cuando ninguna sesión está presente y la segunda forma se muestra cuando una sesión está activa como se muestra en las gráfica a continuación



2. **Capas:** Este componente es capaz de controlar las capas que tiene el mapa del sistema de navegación. Las capas contenidas se describen a continuación:

   Mapa completo con todas las capas



3. **Alineación de pantalla:** Este componente muestra en que posición se localiza la pantalla de la cámara dentro del mapa cabe mencionar que éste componente está visible sólo si una cámara se selecciona en el árbol de componentes, para que el usuario pueda colocarlo en un lugar donde no obstruya la visión de un determinado punto del mapa

   Posee los siguientes valores:

   Superior

   - Izquierda
   - Centro
   - Derecha

   Medio

   - Izquierda
   - Centro
   - Derecha

   Inferior

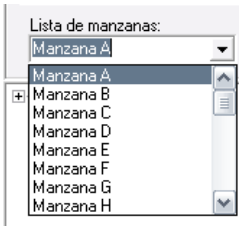
   - Izquierda

Centro

Derecha

Por defecto se muestra la alineación Inferior izquierda

4. **Lista de manzanas:** Este componente muestra la lista de manzanas que posee el sistema, trabaja conjuntamente con el mapa ya que si se escoge una manzana determinada el mapa resalta esa área de la manzana

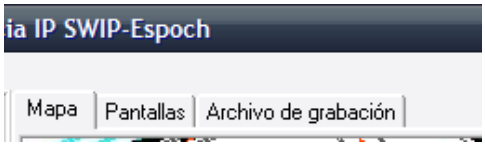


5. **Árbol de componentes:** Este componente muestra los elementos de organización hasta llegar a una localización determinada de una cámara lo cual supone que está registrada en el sistema.

6. **Pantalla de Video sobre el mapa:** Muestra la pantalla que se mostrará en el momento de navegar sobre el mapa si una cámara

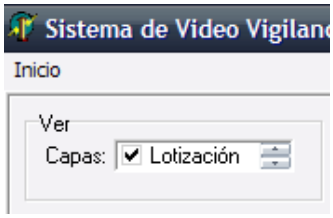
está seleccionada, es decir que es un componente visible sólo si una cámara está seleccionada.

7. **Páginas de Navegación:** Este componente es un contenedor de tres páginas que muestran información de la siguiente manera:



9.1. Mostrar capas del mapa de navegación

Las capas del mapa de navegación se muestran como se especificó en el componente de Ver capas; Este componente es muy importante y sobre el cual se ejecutan varios procesos de navegación por lo que es configurable solo para usuarios de nivel administrador



Las capas disponibles son:

Lotización

Estructuras

Etiquetas

Perímetro

Sobre las funciones que hacen cada una de estas ya se especifico en el apartado Anterior.

9.2. Alineación de pantalla

Esta función ubica la pantalla en un lugar específico del mapa, e un conjunto de nueve botones los cuales hacen este proceso, por defecto la alineación está dado en la parte inferior izquierda (donde inicialmente no obstruye la visibilidad del mapa).

9.3. Navegación de árbol

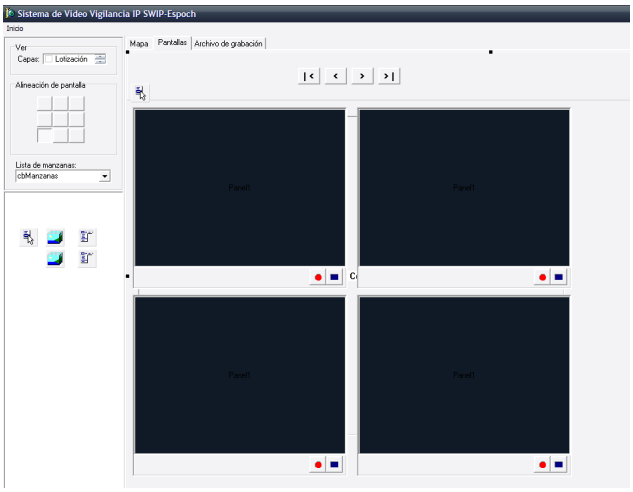
Para esta función se ha programado un árbol de componentes el cual es muy familiarizado al explorador de Windows a través de directorios y carpetas.

9.4. Navegación de mapa

Las funciones de navegación de mapa esta dado por capas de imágenes que resalta la manzana cuando es seleccionada desde su correspondiente etiqueta, es necesario mencionar que no se puede seleccionar dos áreas distintas a la vez ya que la navegación es hacia un solo punto.

9.5. Navegación de pantallas

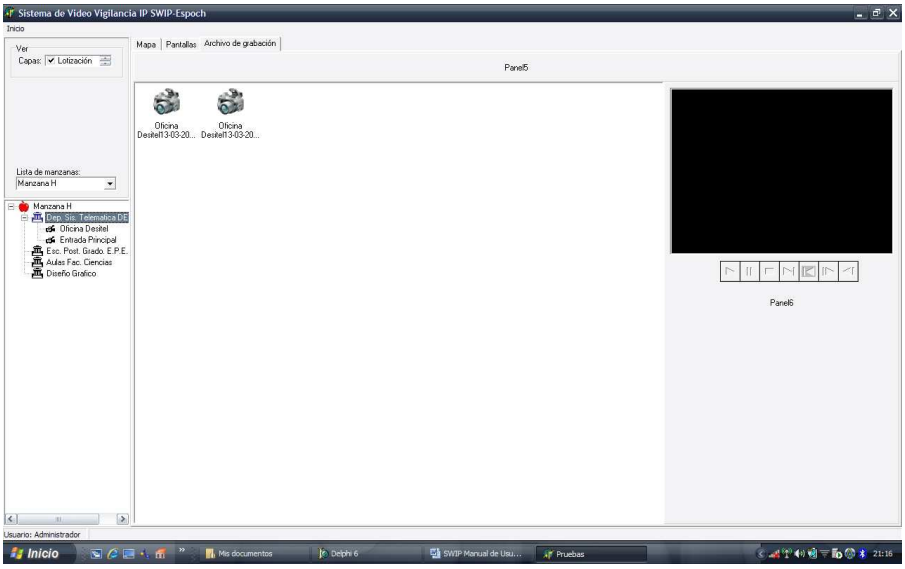
La navegación de pantallas se muestra en una configuración de pantalla de 800x600 por lo que se han especificado una cantidad de cuatro pantallas a la ves de forma simultánea para una visibilidad óptima, estas pantallas muestran las cámaras que pertenecen a un mismo departamento ya que para su navegación coherente es necesario presentar información ordenada



9.6. Navegación de archivos

Las funciones de navegación de archivos esta vinculada con la shell del sistema operativo es de cir que al crear un archivo de grabación y almacenarlo

en el disco duro, este se muestra en nuestra pantalla de navegación dada por el directorio de grabación previamente configurado



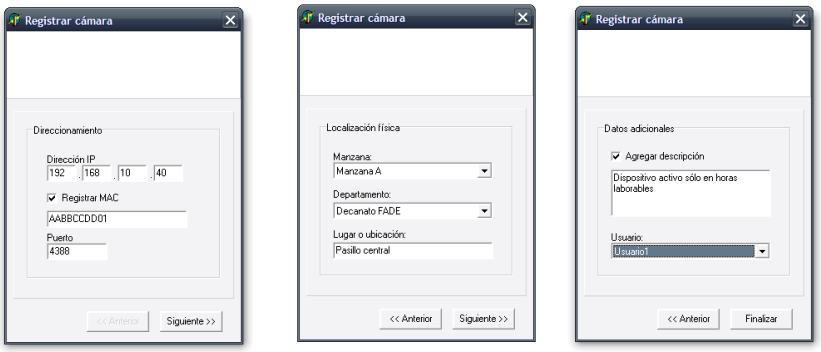
10. DISPOSITIVOS DE VIGILANCIA (CÁMARAS) EN EL SISTEMA

10.1. Registrar una cámara

Para realizar este proceso existe dos formas: la primera es desde el menú principal, si escogemos esta opción se nota que en el asistente para el ingreso se debe ingresar todos los campos y para ello seguimos la siguiente secuencia en el menú principal del sistema:

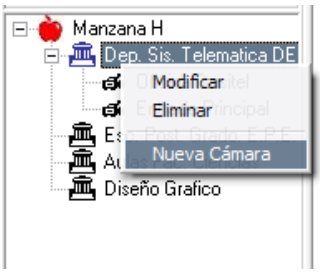
Inicio-Cámaras-Nuevo registro como se muestra en grafica que está a continuación

Luego de de acceder a ésta opción aparecerá el asistente de registro de una cámara nueva en el sistema y, luego de rellenar los campos necesarios y de forma correcta se finaliza el asistente; el las gráficas que se muestran a continuación esta el asistente en el registro de una cámara:

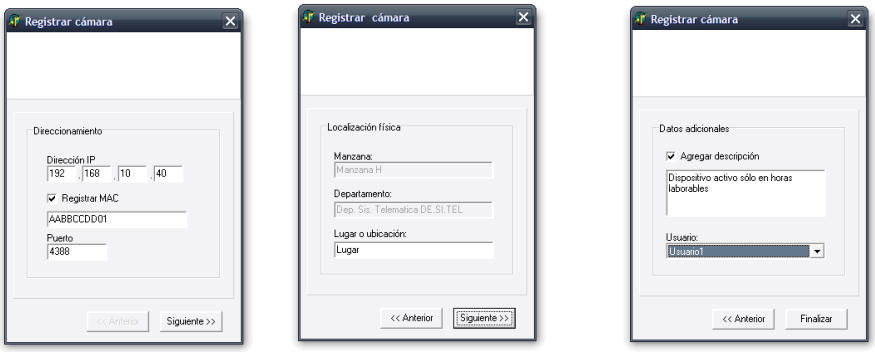


La segunda forma es a través del árbol de componentes, si usted escoge esta alternativa los campos del asistente en la segunda ficha son rellenados automáticamente por los componentes y los datos que éstos proporcionan. Para ello seguimos la siguiente secuencia en el árbol de componentes:

Nodo(Escogemos un nodo Departamento o elemento de nivel 2**)-Click secundario- Nueva Cámara**



Al hacer esto el asistente tiene una secuencia en las fichas como se muestra a continuación:

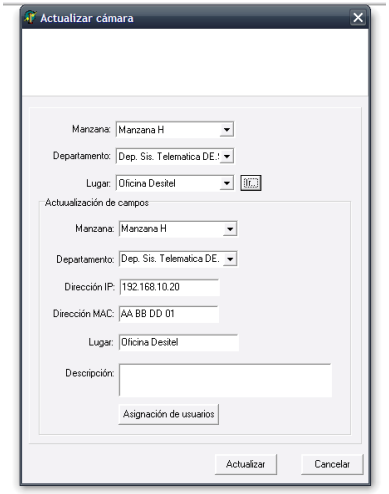


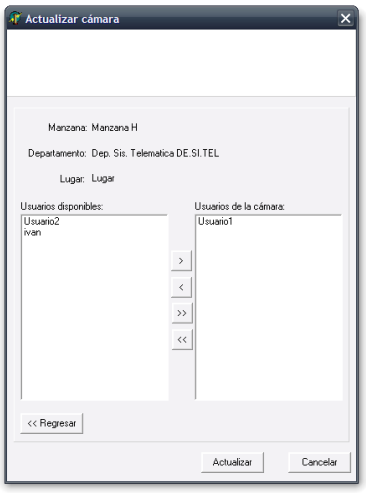
Si se fija en la grafica anterior, la ficha del centro muestra que los campos de **Manzana** y **Departamento** están previamente llenados y deshabilitados

10.2. Actualizar una cámara

De forma similar al ingreso, existen dos formas de ejecutar este proceso, vamos a analizar la primera; seguimos la siguiente secuencia en el menú principal:

Inicio-Cámaras-Actualización, luego de ello se muestra el asistente para actualizar cámara en el cual se actualiza sus campos y se puede asignar usuarios en la siguiente ficha del asistente cuando presionamos el botón **Asignación de usuarios**





10.3. Eliminar una cámara

Para ejecutar éste proceso seguimos la siguiente secuencia en el menú del sistema:

Inicio-Cámaras-Eliminación como se muestra en la gráfica siguiente:

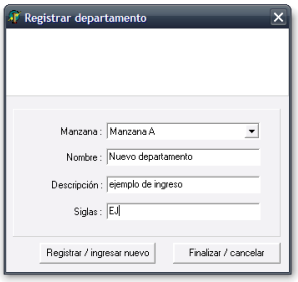
11. ELEMENTOS DE ORGANIZACIÓN EN EL SISTEMA

11.1. Registrar un departamento

Para ello seguimos la siguiente secuencia de comandos:

Inicio-Departamentos-Nuevo registro.

Luego de lo cual aparece el asistente para registro de departamentos

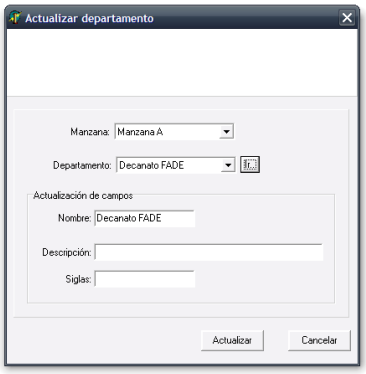


11.2. Actualizar un departamento

Para ello seguimos la siguiente secuencia de comandos:

Inicio-Departamentos-Actualización.

Luego del cual aparece el asistente para actualización de departamentos



11.3. Eliminar un departamento

Este proceso se ejecuta realizando la siguiente secuencia en el menú del sistema:
Inicio-Departamentos-Eliminación

Cuando ejecutamos este proceso el sistema nos pide una confirmación para seguir adelante con la eliminación.

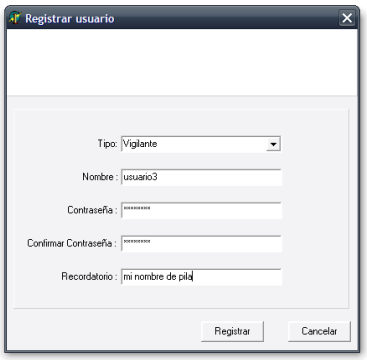
12. USUARIOS EN EL SISTEMA

12.1. Registrar un usuario

Para registrar un usuario se debe seguir la siguiente secuencia en el menú del sistema

Inicio-Usuarios-Nuevo registro

Luego de ello aparece el asistente para registro de usuarios

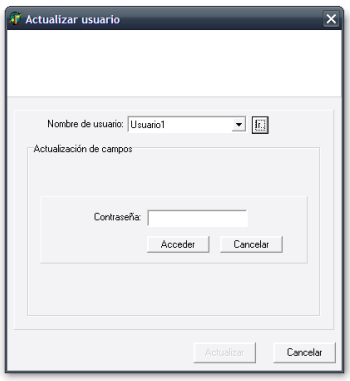


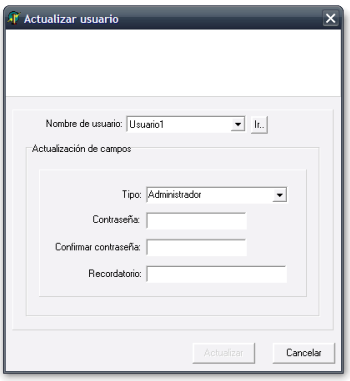
12.2. Actualizar un usuario

Para realizar este proceso se sigue la siguiente secuencia en el menú del sistema:

Inicio-Usuarios-Actualización

Luego del cual se muestra el asisten de actualización de usuarios





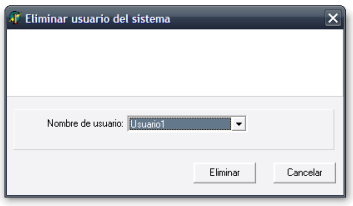
En la primera ficha se puede autentificar y en la segunda modificar la cuenta

12.3. Eliminar un usuario

Para efectuar este proceso debe seguir la siguiente secuencia en el menú del sistema:

Inicio-Usuarios-Eliminación

Luego de ello se puede realizar la eliminación desde el asistente



Anexo 4. MANUAL TECNICO

SWIP ®
Sistema de Video Vigilancia IP

Manual Técnico

1. Introducción

A continuación se detallan las generalidades, características y aspectos importantes para la instalación ejecución e implementación del de video-Vigilancia.IP

2. Ambientes de Operación

Detallamos los elementos que debe incorporar el sistema de video-Vigilancia-IP para su funcionamiento óptimo.

2.1. Elementos Hardware

En cuanto a elementos hardware se deberá disponer de:

Cámara de red (cámara IP)

- Compresión de video MPEG

Un equipo con características:

- Procesador Intel Pentium IV 3.6 GHz
- Disco Duro de 80 GB
- Memoria de 256 MB
- CD – Room de 52xLG
- Monitor 14'' SANSUNG

- Teclado Genérico multimedia
- Mouse PS2
- Case ATX

Requerimientos Adicionales

Importantes para la correcta funcionalidad de los sistema que integra.

- Tarjeta de red 10/100

2.2. Elementos Software

Los elementos software necesario para la instalación son:

Sistema Operativo

- En general el Sistema debe poder ejecutarse sobre el sistema operativo Windows XP Se recomienda realizar la instalación del service spack 2 ya que la instalación de los programas requeridos es mucho más simple.

Componente de Video Afluente

Se debe instalar el componente OCX para la aceleración de video

Base de Datos

El Sistema de video-vigilancia-IP requiere de la instalación de un servidor de bases de datos SQL- SERVER 200 para almacenar la información generada por el sistema. Este servidor puede utilizarse para otras aplicaciones.

Funcionalidad

a.- Módulo Administrador.

b.- Módulo Vigilancia (usuario normal)

c.- Módulo grabación

2.3 Funciones del producto.

Módulo Administrador.-

- Gestionar cuentas
- Asignar permisos.
- Crear usuarios.
- Configuración acceso al sistema por cuentas de usuario.
- Configuración de departamentos
- Configuración de cámaras
- Monitorización de video

Módulo Vigilancia.-

- Monitorización de video en vivo
- Grabación de video en vivo
- Recuperación de video grabado

Navegabilidad

El sistema de navegación puede ser combinando el modelo de árbol con un sistema de mapa sensitivo que permite escoger un departamento para luego ubicarnos en una determinada cámara o grupo de cámaras a visualizar

ESPECIFICACIONES DE USUARIO

a.- Interfaces de Usuario.

Las interfaces del usuario están constituidas esencialmente por las ventanas, cuadros de diálogo, gráficos, hipertexto, etc., el propósito es crear un software con características de un programa visual y didáctico en cierto punto, dando lugar a los siguientes requerimientos que debe cumplir:

- Ayuda en Línea (Guía de Ayuda).
- Menús Interactivos (Cajas de diálogo y respuestas del sistema).
- Presentación de Mensajes de Error.
- Gráficos.
- Hypertexto.

ELEMENTOS DE FUNCIONALIDAD

- *Barra de Herramientas*
- *Botones de Radio*
- *Caja de Diálogo*
- *Hipertexto*
- *Menú.*

CARACTERÍSTICAS DE LOS USUARIOS

El paquete de software está diseñado para personas que conozcan como mínimo el funcionamiento de Windows. Ya que de otra forma no lo van

a poder emplear debido al acceso, el programa una vez inicializado se lo podrá manejar por cuanto es sencillo e intuitivo