

 UNIVERSIDAD
SEÑOR DE SIPÁN

**FACULTAD DE INGENIERÍA, ARQUITECTURA Y
URBANISMO**

**ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA
DE SISTEMAS**

TESIS

**ANÁLISIS COMPARATIVO DE PROTOCOLOS DE
COMUNICACIÓN DE REDES PARA UN SISTEMA
DE VIDEOVIGILANCIA**

**PARA OPTAR EL TÍTULO PROFESIONAL DE
INGENIERO DE SISTEMAS**

Autor:

Bach. Huertas Honores Victor Manuel

Asesor:

Mg. Tuesta Monteza, Victor Alexci

Línea de Investigación:

Tecnologías de la Información

Pimentel, Perú

2018

**ANÁLISIS COMPARATIVO DE PROTOCOLOS DE COMUNICACIÓN DE
REDES PARA UN SISTEMA DE VIDEOVIGILANCIA**

Aprobación de la Tesis

**Ing. Fuentes Adrianzén Denny
Presidente del Jurado de Tesis**

**Ing. Mejía Cabrera Heber Iván
Secretario del jurado de Tesis**

**Ing. Bruno Sarmiento José
Vocal del Jurado de Tesis**

**Pimentel, Perú
2018**



INFORMACIÓN GENERAL

1.1 Título del Informe de Investigación:

“ANÁLISIS COMPARATIVO DE PROTOCOLOS DE COMUNICACIÓN DE REDES PARA UN SISTEMA DE VIDEOVIGILANCIA”

1.2 Línea de Investigación:

Tecnologías de la Información

1.3 Autor:

Huertas Honores Victor Manuel

1.4 Asesor Metodólogo:

Mg. Tuesta Monteza, Victor Alexci

1.5 Tipo y diseño de investigación.

Tipo tecnológica – Aplicada, Cuasi Experimental

1.6 Facultad y Escuela Académico Profesional:

Facultad de Ingeniería, Arquitectura y Urbanismo
Escuela Profesional de Ingeniería de Sistemas

1.7 Periodo: 2018-II

1.8 Fecha de inicio y término del proyecto:

Julio – Diciembre 2018

1.9 Firma de los autores del proyecto:

Huertas Honores Victor Manuel
AUTOR

1.10 Aprobado:

Mg. Tuesta Monteza, Victor Alexci
ASESOR DE INVESTIGACION

1.11 Fecha de Presentación:

Diciembre del 2018



DEDICATORIA

A Mi Madre

Dedico esta tesis con mucho amor y admiración a mi madre que está en el cielo, y en el tiempo que la tuve a mi lado se esmeró con su buen ejemplo y grandiosos amor, para cosechar este fruto de mi formación profesional y de mi personalidad.

A Mis Hermanos

Ya que siempre ellos fueron mi guía y ejemplo a seguir.

A Mi Esposa e Hijas

A mi amada esposa, por su apoyo y ánimo que me brinda día a día para alcanzar nuevas metas. A mis adoradas hijas Karen, Gianella, Dayanne, y a mi adorado Emmanuel a quienes siempre cuidaré para verlos hechos personas capaces y que puedan valerse por sí mismos.

VICTOR MANUEL



AGRADECIMIENTO

A Dios por iluminarnos siempre y permitirme seguir en el camino del bien, por darnos la oportunidad que con nuestra vida profesional acompañemos y ayudemos a nuestros semejantes. Y a la Virgen María por acogernos siempre bajo su manto y tenerla como ejemplo para nuestra vida.

A la Universidad Señor de Sipán, nuestra Alma Mater por todo lo que nos brinda.

A Mi Asesor Mg. Ing. Victor A. Tuesta Monteza, por su acertada orientación y motivación constante, por su amistad bajo un clima de confianza y respeto.

VICTOR MANUEL



ÍNDICE

| | |
|--|----|
| I. INTRODUCCION..... | 6 |
| 1.1. Realidad Problemática | 6 |
| 1.2. Trabajos Previos de la Investigación | 15 |
| 1.3. Bases Teóricas – Científicas (Trabajos Relacionados al Tema)..... | 18 |
| Variable Independiente: Protocolos de Comunicación..... | 18 |
| 1.3.1. Concepto:..... | 18 |
| 1.3.1.1. Protocolo UDP:..... | 19 |
| 1.3.1.2. Protocolo TCP | 22 |
| 1.3.1.3. Protocolo RSTP | 24 |
| 1.3.1.4. Protocolo PPPoE..... | 26 |
| 1.3.1.5. Protocolo DCCP | 26 |
| 1.3.1.6. CCTV DIGITAL | 27 |
| 1.3.1.7. CCTV HIBRIDO | 28 |
| 1.3.2. CARACTERISTICAS DE CAMARAS IP: | 29 |
| 1.3.2.1. Cámara IP | 29 |
| 1.3.2.2. Tipos de Cámaras | 30 |
| 1.3.3. Concepto:..... | 41 |
| 1.4. Formulación del Problema | 42 |
| 1.5. Justificación de la Investigación | 42 |
| 1.6. Hipótesis | 42 |
| 1.6.1. Variables | 42 |
| 1.7. Objetivos de la investigación..... | 43 |
| 1.7.1. Objetivo General..... | 43 |
| 1.7.2. Objetivos Específicos | 43 |
| 1.8. Caso de Estudio..... | 45 |
| 1.9. Escenario de Pruebas | 46 |



| | |
|--|----|
| Diseño físico propuesto | 49 |
| 1.10. Estudio de Viabilidad del Proyecto | 62 |
| 1.10.1. Costos de Implementación para la Analizar Protocolos de Comunicación 62 | |
| 1.10.2. Flujo de caja proyectada | 64 |
| 1.10.3. Análisis de rentabilidad | 65 |
| 1.10.3.1. Valor Actual Neto (VAN) | 65 |
| II. MATERIALES Y METODOS | 70 |
| 2.1. Tipo de Investigación | 70 |
| 2.1.1. Según su Propósito | 70 |
| 2.1.2. Según el diseño de investigación..... | 70 |
| 2.2. Material de Estudio – Población y Muestra..... | 70 |
| 2.2.1. Población | 70 |
| 2.2.2. Muestra..... | 70 |
| 2.2.3. Diseño de Contrastación..... | 70 |
| 2.3. Métodos, Técnicas e Instrumentos | 73 |
| 2.3.1. Métodos de Investigación | 73 |
| 2.3.2. Técnicas e Instrumentos de Recolección | 73 |
| 2.4. Procedimientos para la Recolección de Datos..... | 74 |
| 2.4.1. Plan de análisis estadístico de datos..... | 74 |
| 2.4.1.1. Números de pérdidas de paquetes | 74 |
| 2.5. Criterios de Rigor Científico.- | 74 |
| 2.6. Selección del Protocolo | 75 |
| III. ANALISIS DE RESULTADOS..... | 76 |
| IV. ANALISIS DE RESULTADOS..... | 83 |
| 4.1. PROPUESTA DE INVESTIGACION..... | 83 |
| 4.2. EVALUACIÓN DE DESEMPEÑO DE SIMULACIÓN | 83 |
| 4.2.1. Parámetros de Simulación:..... | 84 |



| | |
|---|-----------|
| 4.2.2. Métricas de Evaluación: | 84 |
| 4.2.3. Resultados de simulación | 85 |
| 4.2.4. Evaluaciones Comparativas | 88 |
| CONCLUSIONES | 93 |
| Referencias Bibliográficas | 94 |



INDICE DE FIGURAS

Figura 1: Gráfico que muestra el tráfico de Internet en Estados Unidos, se puede ver que9

Figura 2: Proceso 3- Way handshake que se realiza en cada conexión TCP.Fuente Serverfault.com..... 9

Figura3: Flujo de paquetes TCP en Wireshark, Fuente: Universidad Federico Santa María 10

Figura4: Características de UDP 21

Figura5: Datagrama UDP 22

Figura6: Servicios UTP 24

Figura 7: Sistemas de CCTV Digital 28

Figura 8: Sistema CCTV Híbrido 28

Figura 9: Partes de una Cámara de Red 29

Figura 10: Cámaras de red Fijas 32

Figura 11: Cámaras IP Domo Fija..... 33

Figura 12: Cámara Domo PTZ..... 35

Figura 13: Grabador AXIS Camera Station S1148 37

Figura 14: NVR o E (Power Over Ethernet)..... 39

Figura15: Alimentación a Través de POE 39

Figura 16: Topología Lógica 48

Figura 17: Topología Física 48

Figura 18 Topología Física 49

Figura 19..... 51

Figura 20 Topología de la red..... 52

Figura 21: Diseño Físico de la red de la Municipalidad Distrital de Víctor Larco Trujillo 53

Figura22: Distribución de las cámaras en todo el Distrito de Víctor Larco..... 54

Figura23: (a) Evolución de la ventana de congestión en TCP. (b) Evolución de la ventana de transmisión en TCP. 56

Figura 24: Funcionamiento del Protocolo TCP 58

Figura25: Reensamble de Datos 59

Figura26: Protocolo UDP 60

Figura27: Cabecera de Protocolo UDP 61

Figura28: Reensamble de Datos 62

Figura29: Diagrama de Tiempo 65



| | |
|---|----|
| Figura30: Análisis de Rendimiento (a) | 80 |
| Figura31: Pérdida de Paquetes (b)..... | 80 |
| Figura32: Retraso (c)..... | 81 |
| Figura33: Jitter (d)..... | 81 |
| Figura34: Retrasos promedio de extremo a extremo en el Caso Uno con diferentes protocolos | 87 |
| Figura35: Porcentaje de Efectividad de Paquetes Recibidos usando diferentes protocolos | 88 |
| Figura36: Pérdidas de Datos Consecutivos usando diferentes protocolos..... | 90 |
| Figura37: Máximo número de pérdidas | 91 |



INDICE DE TABLAS

| | |
|---|-----------|
| Tabla 1: Requisitos de algunas aplicaciones de red seleccionadas | 13 |
| Tabla 2: <i>Velocidades de diferentes medios de transmisión</i> | 40 |
| Tabla 3: Elaboración de Ranking de Protocolos seleccionado los cuales se elegirán los dos primeros | 44 |
| Tabla 4: Costo de Inversión del Proyecto de Simulación..... | 64 |
| Tabla 5: Flujo e caja..... | 64 |
| Tabla 7: Calculo del TIR..... | 68 |
| Tabla 8: Operacionalización de Variable | 72 |
| Tabla 9: Matriz de Selección de Protocolo..... | 75 |
| Tabla 10: Criterios de la encuesta | 75 |
| Tabla 11: Parámetros de valores | 77 |
| Tabla 12: Parámetros de valores | 84 |
| Tabla 13: Retraso promedio de extremo a extremo en caso de que se use un protocolo diferente | 86 |
| Tabla 14: Porcentaje de Paquetes de Datos Efectivo con diferentes protocolos | 87 |
| Tabla 15: Pérdidas consecutivas de datos efectivos con diferentes protocolos. | 89 |
| Tabla 16: Máximo número de pérdida de datos consecutivos..... | 90 |



RESUMEN

El objetivo de la presente tesis está enfocado en el estudio de los diferentes protocolos de redes en los sistemas de videovigilancia con el fin de establecer los principales aspectos a tener en cuenta en la implementación de esta arquitectura de red. Sin embargo, los dispositivos de video existentes han sido implementados durante muchos años por diferentes proveedores en los cuales las cámaras de red de videovigilancia soportan distintos protocolos. Para integrar estos dispositivos heterogéneos, la gestión centralizada servidor (CMS) y sus clientes necesitan una arquitectura especializada para tratar con diferentes tipos de codificaciones de medios y protocolos de conexión, etc. Para la elección del protocolo UDP fue necesario probar los diferentes protocolos existentes.

Por el momento, el tráfico de video y las telecomunicaciones crecen bajo la expansión de LTE, que se considera como la tecnología de acceso de motivación real de la red 4G en cámaras de video vigilancia. Durante el despliegue de LTE, varios protocolos de transporte son aconsejados y ampliamente experimentados, por ejemplo, TCP, HTTP, RTPS y UDP que pueden ejecutarse de manera diferente en redes 4G sujetas a los escenarios de red y configuraciones de parámetros. Aunque el despliegue de LTE se mejora rápidamente, hay una falta de evaluación del rendimiento de sus protocolos. Por lo tanto, se requiere un escrutinio generalizado para la evaluación del funcionamiento de numerosos protocolos para aplicaciones de alta gama, como multimedia. Adoptando estas aplicaciones con las restricciones flexibles de la calidad del servicio con un mejor uso de los recursos son una tarea desafiante. En esta tesis, los resultados de salida de Se analizan diferentes protocolos de transporte para aplicaciones de transmisión multimedia, por ejemplo, video, mediante simulaciones no tan extensas. El rendimiento de una transmisión de video MPEG-4 se evalúa usando GNS-3. Las medidas de rendimiento utilizadas son retraso, jitter, rendimiento, y pérdida de paquetes. Estas métricas se evalúan en la estación base a través de los protocolos TCP y UDP sobre cámaras de videovigilancia 4G-LTE. Los resultados obtenidos muestran que

UDP realiza el mejor rendimiento con la minimización de retraso y jitter en comparación con TCP.

Palabra Clave: Protocolo, Videovigilancia, Cámara en red

ABSTRACT

The objective of this thesis is focusing on the study of different network protocols in video surveillance systems in order to establish the main aspects to be taken into account in the implementation of this network architecture. However, existing video devices have been implemented for many years by different providers in which the video surveillance network cameras support different protocols. To integrate these heterogeneous devices, the centralized server management (CMS) and its clients need a specialized architecture to deal with different types of media encodings and connection protocols, etc. For the choice of the UDP protocol it was necessary to test the different existing protocols.

At the moment, video traffic and telecommunications are growing under the expansion of LTE, which is considered as the real motivational access technology of the 4G network in video surveillance cameras. During the deployment of LTE, several transport protocols are advised and widely experienced, for example, TCP, HTTP, RTPS and UDP that can be executed differently in 4G networks subject to network scenarios and parameter settings. Although the deployment of LTE is rapidly improving, there is a lack of evaluation of the performance of its protocols. Therefore, a generalized scrutiny is required for the evaluation of the operation of numerous protocols for high-end applications, such as multimedia. Adopting these applications with flexible restrictions on quality of service with better use of resources is a challenging task. In this thesis, the output results of different transport protocols are analyzed for multimedia transmission applications, for example, video, through not so extensive simulations. The performance of an MPEG-4 video transmission is evaluated using GNS-3. The performance measures used are delay, jitter, performance, and packet loss. These metrics are evaluated in the base station through the TCP and UDP protocols on 4G-LTE video surveillance cameras. The results obtained show that UDP performs the best performance with the minimization of delay and jitter compared to TCP.

Key Words: Protocol, Video surveillance, Network camera

INTRODUCCIÓN

Los sistemas de seguridad están conformado por equipos como servidores de red, cámaras, discos duros interconectados entre sí que permitan la monitorización de un entorno de trabajo.

En la actualidad en Perú los sistemas de vigilancia se despliegan siguiendo un plan para la seguridad tanto ciudadana como para los bienes de cualquier entorno de trabajo ya sea empresarial o comercial, en la mayoría usados de los casos como un complemento a la vigilancia por factor humano. Aun se siguen usando en algunas empresas los sistemas analógicos que fueron con los que se inició este sistema.

Es importante resaltar que, en nuestro país especialmente en la Libertad la delincuencia se ha incrementado de forma alarmante principalmente en la ciudad de Trujillo, en los últimos años siendo la falta de sistemas de vigilancia un factor significativo. Es por esto, que la seguridad hoy en día es una prioridad para entidades públicas y privadas que buscan principalmente que los sistemas de vigilancia sean los más eficientes posibles, económicos, y de despliegue rápido.

En la actualidad existen dos conceptos que se están desarrollando ampliamente en el área de las comunicaciones: la tecnología de información y la seguridad, encontrándose los dos en proceso de convergencia. Estos dos desarrollos han creado el interés de soluciones basadas en la utilización de una red IP, pasando así de lo analógico a lo digital, y dando como solución un sistema de vigilancia IP que ha surgido como una alternativa a los VCRs y DVRs antiguos.

En el presente trabajo se desarrolló la implementación de un sistema de vigilancia usando una red muy difundida como es la red IP, y la transmisión de datos vía la red guiada para los laboratorios de cómputo de una empresa educativa privada.

Además este estudio servirá para la posterior implementación en cualquier otra aplicación que se requiera. Si bien la implementación de Long Term Evolution (LTE) se realiza rápidamente, existe una falta de evaluación del rendimiento de sus protocolos.

(Kohler E, 2009) “Por lo tanto, una evaluación amplia es indispensable para la evaluación del rendimiento de varios trajes de protocolo para gama alta aplicaciones como multimedia, etc. Los comportamientos desafiantes de los tres protocolos de transporte mencionados para la transmisión de aplicaciones multimedia deben enfatizar los aspectos positivos y negativos de su performances”.

(Sarabjot Singh, 2010) “Como resultado, en el desarrollo de las comunicaciones inalámbricas, el tráfico de la red se está incrementando, particularmente con el aumento en el número de nodos de red. Long Term Evolution (LTE) ofrece una mayor velocidad de transmisión y cumple con el crecimiento en la demandas de transmisión multimedia”

(J., 1981) “Durante las pruebas de la transmisión de videovigilancia, cuatro protocolos de la capa de transporte son los más lentos ampliamente revisados, como (TCP)”

(Shukla S, 2013) “En la era actual de las telecomunicaciones, el tráfico de video está creciendo rápidamente y simultáneamente con el avance de Long Term Evolution (LTE), que es famoso por la verdadera tecnología de acceso fundamental de Redes 4G”

CAPÍTULO I: PROBLEMA DE INVESTIGACION

I. INTRODUCCION

1.1. Realidad Problemática

En la actualidad el mundo está pasando en una transición de tráfico de datos convencionales a la transmisión de datos convergentes (datos, voz y video), El Perú no es ajeno a este cambio tecnológico, uno de los factores que permitió este cambio es los diferentes proyectos de video vigilancia en las ciudades debido al crecimiento de la delincuencia, esto originó un crecimiento exponencial del tráfico de video en la red, esta realidad implica un análisis correcto de los protocolos que permiten una transmisión eficiente del emergente tráfico de la red, no existen estudios detallados del manejo de protocolos orientados al video realizados en base a nuestra realidad aun teniendo en cuenta que las redes de videovigilancia han cobrado un papel muy relevante, tanto en el mundo industrial como en el ámbito social.

En muchos casos, los protocolos de comunicación de cámaras no han sido analizados formalmente con el fin de hacer un estudio exhaustivo y riguroso de los mismos para garantizar su coherencia.

El uso de métodos formales que nos permitan hacer este análisis riguroso es un paso importante en el uso de estos protocolos, ya que permiten realizar simulaciones previas a la instalación de este tipo de redes de tráfico de video. En un artículo realizado por CISCO de título Tutorial de calidad de servicio de video en el cual se considera que la red de transporte de video debe cumplir con unos estándares en latencia no mayor de 150 – 300ms, pérdida no mayor del 0.5% y jitter no mayor de 50ms (CISCO, 2017); según este artículo de CISCO habla de capa 3 (capa red) pero no incluye la capa 4 que es referente para el desarrollo de esta tesis.

(SHARHUDIN, ALUBADY, & KAMIL, 2016), “Rendimiento simulado de los protocolos TCP, SCTP, DCCP y UDP sobre red 4G”

“Los autores: Shahrudin Awang Nor, Raaid Alubady y Wisam Abduladeem Kamil nos informan que como resultado del desarrollo de las comunicaciones

inalámbricas, el tráfico de red se está incrementando, en particular, con el aumento en el número de nodos de red. Evolución a largo plazo (Long Term Evolution – LTE¹) ofrece una mayor velocidad de transmisión y satisface las crecientes demandas de transmisión multimedia. En la era actual de las telecomunicaciones, el tráfico de video está creciendo rápidamente y simultáneamente con el avance de LTE, que es famoso por la verdadera tecnología de acceso fundamental de las redes 4G. Durante el despliegue de LTE, los cuatro protocolos de la capa de transporte son los más recomendados y revisados, denominado Transmission Control Protocol (TCP), Stream Control Transmission Protocol (SCTP), Protocolo de control de congestión de datagramas (DCCP) y Protocolo de datagramas de usuario (UDP). La tasa de transmisión es motivada considerablemente por el rendimiento de los protocolos de transporte, que se utiliza en los escenarios de redes inalámbricas.

Si bien la implementación de LTE se acelera rápidamente, hay una falta de evaluación de desempeño de sus protocolos.

Por lo tanto, una evaluación amplia es indispensable para la evaluación del rendimiento de varios protocolos para aplicaciones de gama alta, como multimedia, etc. Los comportamientos desafiantes de los cuatro protocolos de transporte mencionados para la transmisión de aplicaciones multimedia necesitan enfatizar los aspectos positivos y negativos de sus actuaciones. Los informes de comparación actuales no reflejan el rendimiento de los protocolos TCP, SCTP, DCCP y UDP para el transporte de videos bajo las redes de acceso LTE. El mejor protocolo de transporte para la transmisión de datos de video ni siquiera está ilustrado debido a las inferencias en conflicto. Por lo tanto, presentar una investigación importante del rendimiento de los protocolos mencionados para el entorno LTE puede ayudar a los investigadores y académicos a seleccionar el protocolo preciso para la transmisión de aplicaciones de video.”

(Maria, 2018) “La revolución del contenido multimedia de pies a cabeza”

¹ LTE Responde a las siglas Long Term Evolution (evolución a largo plazo) y hace referencia a la tecnología de banda ancha inalámbrica que sirve para la transmisión de datos con la finalidad de dar acceso a Internet a los dispositivos móviles.

“Debido a que Netflix requiere una conexión a internet, prácticamente todos los dispositivos conectados a internet, pueden ejecutar esta aplicación, tales como SmartTV, SmartPhones, Tablets, Computadores. Dicha compatibilidad hace el sistema muy escalable, debido a que permite dar abasto a muchos dispositivos con conexión a internet.”

“Sobre la base de las consideraciones anteriores, se reporta que en horarios “picos”, Netflix llega a ocupar sobre el 30% del tráfico de internet en Estados Unidos, lo cual demuestran el gran impacto que tienen este tipo de aplicaciones sobre la sociedad de consumo de entretenimiento (Ver Figura 1).

Dentro de la capa de transporte, encontraran que, para que la aplicación no tenga que “esperar” esta utiliza el protocolo TCP, esto es debido a que tiene un mejor control de congestión y utiliza un método adecuado para la retransmisión de paquetes, establece el 3-Way handshake (ver figura 2), de hecho es posible ver muchos paquetes TCP a la hora de realizar la conexión (Ver Gráfico 3) y el buffer de video. Este protocolo es mucho más robusto que el protocolo **UDP**, en efecto, podría generarse la inquietud de pensar que Netflix utiliza el protocolo UDP, pero no es así. Esto debido a que, Netflix busca entregar un servicio de calidad, el cual no tenga cortes ni saltos intermedios, es por esto que se decide utilizar **TCP**, protocolo que asegura la fiable entrega de los paquetes. Esto explicaría por qué existe un tiempo de espera antes de poder ver contenido multimedia en Netflix, y es debido a que se genera un buffer de tamaño definido, el que almacena los paquetes de video que aún no han sido reproducidos, y que se encuentran en cola para su reproducción, esto es bastante cómodo, ya que permite aprovechar al máximo el protocolo **TCP**, y ajustarse a la característica de la red (velocidad de enlace).

Cabe señalar que en la **capa de red** implementa protocolos ya existentes, como lo son el protocolo **IP**, y el **ARP**, encontrando la ruta más óptima para poder dirigir los paquetes. El protocolo **ARP**, es el encargado de enviar los paquetes entre las direcciones IP de origen y destino.

La **capa de enlace**, toma los paquetes de datos y los empaqueta en tramas, además busca el método apropiado de transmisión, se utiliza principalmente el protocolo **Ethernet II** . Finalmente la **capa física**, utiliza medios de transmisión bastante estándares, como lo son: 802.11 : Wi-Fi y 802.3 : Ethernet.”

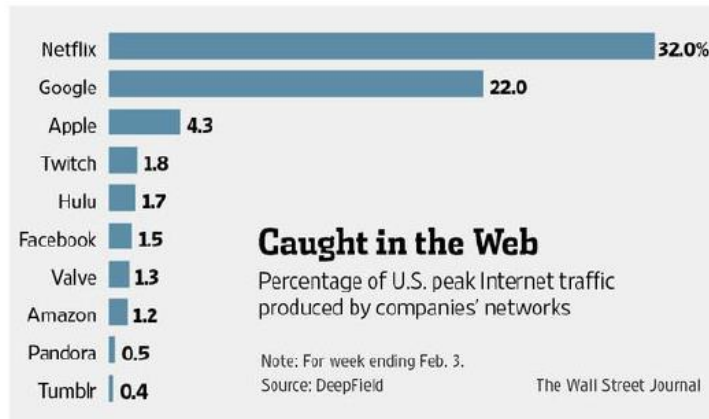


Figura 1: Gráfico que muestra el tráfico de Internet en Estados Unidos, se puede ver que Netflix lidera con un tráfico del 32%, fuente The Wall Street Journal

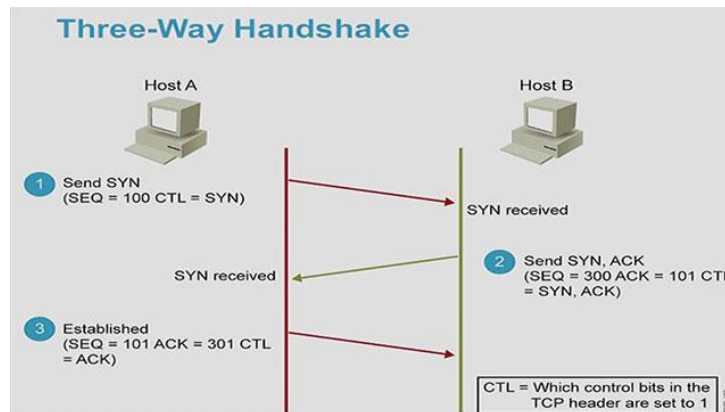


Figura 2: Proceso 3- Way handshake que se realiza en cada conexión TCP. Fuente Serverfault.com

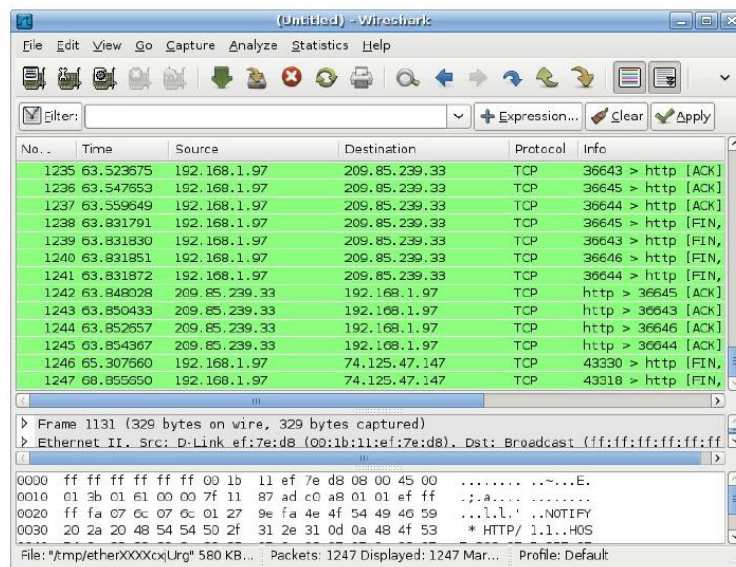


Figura3: Flujo de paquetes TCP en Wireshark, Fuente: Universidad Federico Santa María

(Claveria) “La Realidad Actual del Streaming de Video”

“El proceso de difusión en continuidad consiste en uno o más medios multiplexados en un cliente en tiempo real, usando una red con un determinado ancho de. En el proceso de streaming NO hay ningún fichero que se descarga al ordenador del cliente, sino que el medio se transcribe conforme se está recibiendo, y a su vez el medio se recoge a la velocidad adecuada para su transcripción. Esto contrasta con las descargas progresivas, en las que el fichero sí queda descargado en disco y además se recibe a la mayor velocidad posible, con el fin de terminar el proceso de descarga lo antes posible. En un proceso de streaming estándar de audio y vídeo sincronizado, las peticiones de servicio por parte de los clientes se pueden manejar utilizando el protocolo RTSP (RealTime Streaming Protocol). Este protocolo se encarga de controlar el stream de contenido multimedia en dos direcciones, de forma que los clientes pueden pedir al servidor hacer cosas como rebobinar la película, saltar al siguiente capítulo, etc. Esto se puede conseguir con streaming ya que el medio no se descarga linealmente sino que se reproduce conforme se obtiene, y se permiten saltos en la reproducción, consiguiendo un acceso aleatorio al medio, incluso en saltos hacia delante. Por otra parte, los datos del medio (el stream que

contiene típicamente audio y vídeo sincronizados) se pueden transportar usando el protocolo estándar RTP (Real-Time Transport Protocol), que es un protocolo de transporte que permite la transmisión de información multimedia en tiempo real sobre cualquier tipo de red (aunque su uso más habitual es sobre redes IP usando el protocolo UDP).

De esta forma quedan definidos dos canales de comunicación entre los clientes y el servidor de streaming: Un canal para el control de sesión (RTSP) y un canal para la transmisión de la información.(RTP/UDP/TCP)”

(Kurose James F, 2010) “Redes de Computadores un Enfoque Descendente”

“Internet puede verse como una infraestructura que proporciona servicios a aplicaciones distribuidas que se ejecutan en sistemas terminales. Idealmente, desearíamos que los servicios de Internet pudieran transportar tantos datos como quisiéramos entre cualesquiera dos sistemas terminales de forma instantánea y sin que tuviera lugar ninguna pérdida de datos. Evidentemente, en la realidad, este objetivo es inalcanzable, ya que necesariamente las redes de computadoras tienen que restringir su **tasa de transferencia** (la cantidad de datos por segundo que pueden transmitir) entre sistemas terminales, introducir retardos entre los sistemas terminales y perder paquetes. Por una parte, es lamentable que las leyes físicas introduzcan retardos y pérdidas, así como que restrinjan las tasas de transferencia, pero, por otra parte, puesto que las redes de computadoras presentan estos problemas, existen muchas cuestiones interesantes relacionadas con cómo abordarlos.”

(Kurose James F, 2010) “Tasa de Transferencia”

“Un protocolo de la capa de transporte podría proporcionar, una tasa de transferencia disponible garantizada a una cierta velocidad especificada. Con un servicio así, la aplicación podría solicitar una tasa de transferencia garantizada de r bits/segundo y el protocolo de transporte podría entonces garantizar que la tasa de transferencia disponible sea siempre al menos de r bits/segundo. Un servicio que ofreciera una tasa de transferencia

garantizada resultaría atractivo para muchas aplicaciones. Por ejemplo, si una aplicación de telefonía por Internet codifica voz a 32 kbps, tendrá que enviar datos a la red y tendrá que entregar los datos a la aplicación receptora a esa velocidad. Si el protocolo de transporte no puede proporcionar esa tasa de transferencia, la aplicación tendrá que realizar la codificación a una velocidad menor (y recibir a una tasa de transferencia adecuada como para mantener esa velocidad de codificación más lenta) o bien tendrá que renunciar, puesto que recibir a la mitad de la tasa de transferencia necesaria no tiene ninguna utilidad para esta aplicación de telefonía por Internet. Las aplicaciones con requisitos de tasa de transferencia se conocen como **aplicaciones sensibles al ancho de banda**. Muchas aplicaciones multimedia actuales son sensibles al ancho de banda, pero algunas de ellas pueden emplear técnicas de codificación adaptativa para realizar la codificación a una velocidad que se adapte a la tasa de transferencia disponible actualmente.

Mientras que las aplicaciones sensibles al ancho de banda tienen que cumplir requisitos específicos para la tasa de transferencia, las **aplicaciones elásticas** pueden hacer uso de la tasa de transferencia, mucha o poca, que haya disponible. El correo electrónico, la transferencia de archivos y las transferencias web son todas ellas aplicaciones elásticas. Por supuesto, cuanto mayor sea la tasa de transferencia, mejor.”

(Kurose James F, 2010) “Temporización”

“Un protocolo de la capa de transporte también puede proporcionar garantías de temporización.

Al igual que con las tasas de transferencia garantizadas, las garantías de temporización también pueden darse de diversas formas. Un ejemplo de garantía podría ser que cada bit que el emisor empuja por su socket llegue al socket del receptor en no más de 100 milisegundos.

Un servicio así sería atractivo para las aplicaciones interactivas en tiempo real, como la telefonía por Internet, los entornos virtuales, la teleconferencia y los juegos multijugador, todas las cuales requieren restricciones de

temporización muy estrictas sobre la entrega de datos para ser efectivas. Por ejemplo, los retardos largos en la telefonía por Internet tienden a dar lugar a pausas antinaturales en una conversación; en un juego multijugador o en un entorno de videoconferencia, un retardo largo entre la realización de una acción y la visualización de la respuesta del entorno (por ejemplo, de otro jugador que se encuentra en el otro extremo de una conexión extremo a extremo) hace que la aplicación parezca menos realista. En las aplicaciones que no se ejecutan en tiempo real, siempre es preferible un retardo pequeño que grande, pero no se aplican restricciones estrictas a los retardos extremo a extremo.”

(Kurose James F, 2010) “Servicios de transporte proporcionados por Internet”

Servicios TCP

El modelo de servicio TCP incluye un servicio orientado a la conexión y un servicio de transferencia de datos fiable. Cuando una aplicación invoca TCP como su protocolo de transporte, la aplicación recibe estos dos servicios de TCP.

| Aplicación | Pérdida de datos | Ancho de banda | Sensible al tiempo |
|---|--------------------------|--|-------------------------|
| Transferencia de archivos | Sin pérdidas | Elástica | No |
| Corre electrónico | Sin pérdidas | Elástica | No |
| Documentos web | Sin pérdidas | Elástica | No |
| Telefonía por Internet/ Videoconferencia | Tolerante a las pérdidas | Audio: unos pocos kbps–1 Mbps Vídeo: 10 kbps–5 Mbps | Sí: décimas de segundo |
| Audio/vídeo almacenado | Tolerante a las pérdidas | Como el anterior | Sí: unos pocos segundos |
| Juegos interactivos | Tolerante a las pérdidas | Unos pocos kbps–10 kbps | Sí: decimas de segundos |
| Mensajería instantánea | Sin pérdidas | Elástica | Sí y no |

Tabla 1: Requisitos de algunas aplicaciones de red seleccionadas

SERVICIO ORIENTADO A LA CONEXIÓN. TCP hace que el cliente y el servidor intercambien la información de control de la capa de transporte entre sí antes de que empiecen a fluir los mensajes del nivel de aplicación. Este procedimiento denominado de negociación, de reconocimiento o de establecimiento de la conexión alerta al cliente y al servidor, permitiéndoles prepararse para el intercambio de paquetes. Después de esta fase de negociación, se dice que existe una conexión TCP entre los sockets de los dos procesos. La conexión es una conexión full-duplex ya que los dos procesos pueden enviarse mensajes entre sí a través de la conexión al mismo tiempo. Una vez que la aplicación ha terminado de enviar mensajes, es necesario desactivar la conexión. Se dice que es un servicio “orientado a la conexión” en lugar de un servicio de “conexión” porque los dos procesos están conectados de una forma muy laxa.

SERVICIO DE TRANSFERENCIA DE DATOS FIABLE. Los procesos de comunicación pueden confiar en TCP para entregar todos los datos enviados sin errores y en el orden correcto. Cuando un lado de la aplicación pasa un flujo de bytes a un socket, puede contar con TCP para entregar el mismo flujo de bytes al socket receptor sin pérdida ni duplicación de bytes.

TCP también incluye un mecanismo de control de congestión, que es un servicio para mejorar el funcionamiento general de Internet, más que para el beneficio directo de los procesos que se comunican. Este mecanismo de control de congestión de TCP regula el proceso emisor (cliente o servidor) cuando la red está congestionada entre el emisor y el receptor.

El control de congestión de TCP también intenta limitar cada conexión TCP para que utilice una cuota equitativa de ancho de banda de la red. La regulación de la velocidad de transmisión puede tener efectos muy dañinos sobre las aplicaciones de audio y de vídeo en tiempo real, que tienen unos requisitos mínimos de tasa de transferencia. Además, las aplicaciones en tiempo real son tolerantes a las pérdidas y no necesitan un servicio de transporte completamente fiable. Por estas razones, los desarrolladores de aplicaciones en tiempo real a menudo deciden ejecutar sus aplicaciones utilizando el protocolo UDP en lugar de TCP.

Servicios UDP

UDP es un protocolo de transporte ligero simple que proporciona unos servicios mínimos y no está orientado a la conexión, por lo que no tiene lugar un procedimiento de negociación antes de que los dos procesos comiencen a comunicarse. UDP proporciona un servicio de transferencia de datos no fiable; Kurose James F, Keith W, Rosses explican, cuando un proceso envía un mensaje a un socket UDP, el protocolo UDP no ofrece ninguna garantía de que el mensaje vaya a llegar al proceso receptor. Además, los mensajes que sí llegan al proceso receptor pueden hacerlo de manera desordenada. UDP no incluye tampoco un mecanismo de control de congestión, por lo que el lado emisor de UDP puede introducir datos en la capa inferior (la capa de red) a la velocidad que le parezca. (Sin embargo, debe observar que la tasa de transferencia extremo a extremo real puede ser menor que esta velocidad a causa del ancho de banda limitado de los enlaces intervinientes o a causa de la congestión.) Puesto que las aplicaciones en tiempo real a menudo pueden tolerar ciertas pérdidas pero requieren una velocidad mínima para ser efectivas, los desarrolladores de estas aplicaciones en ocasiones deciden ejecutarlas usando UDP, soslayando los mecanismos de control de congestión y la sobrecarga de gestión de los paquetes TCP. Por otro lado, dado que muchos cortafuegos están configurados para bloquear casi todos los tipos de tráfico UDP, los diseñadores están decidiendo cada vez más frecuentemente ejecutar las aplicaciones multimedia en tiempo real sobre TCP.

1.2. Trabajos Previos de la Investigación

(Farahnaz Naeimipoor, 2015) “Evaluación del rendimiento de los protocolos de difusión de video sobre redes vehiculares”

“La difusión de video sobre Vehicular Ad hoc Network (VANETs²) es necesaria para implementación de servicios útiles y cruciales sobre vehículos redes. Sin embargo, hay muchos desafíos que necesitan ser superado con el fin de cumplir con todos los requisitos de transmisión de video.”

En este estudio, los autores analizaron el rendimiento de los distintos protocolos de encaminamiento en una red VANET en entornos urbanos, en los que se tuvieron en cuenta los retardo (Delay), paquetes perdidos (Drop) y la tasa de transferencia efectiva (Troughput), Permitiendo determinara el comportamiento de cada unos de estos indicadores según protocolo.

(Marion Souil, 2014) “Un nuevo protocolo (Medium Access Control- MAC) adaptable con soporte QoS o calidad de servicio (quality of service-QoS) para redes de sensores inalámbricos heterogéneos”

“Los autores, propusieron AMPH o Protocolo heterogéneo para redes de sensores inalámbricos (Protocol for Heterogeneous wireless sensor networks AMPH), un nuevo MAC adaptativo, protocolo para redes de sensores inalámbricos heterogéneos con diferenciación de servicio, alto rendimiento y soporte QoS. Los resultados de validación han demostrado que el comportamiento híbrido de AMPH supera los protocolos basados en contención como CSMA/CA o acceso múltiple por detección de portadora y prevención de colisiones (del inglés Carrier Sense Multiple Access with Collision Avoidance - CSMA/CA), es un protocolo que opera en la capa de enlace de datos (Capa 2) del modelo OSI o interconexión de sistemas abiertos (Open System Interconnection- OSI).”

En los marcos de las observaciones anteriores Este equipo de investigadores proponen un nuevo protocolo que permitirán en términos de utilización del canal, latencia y confiabilidad”

² VANETs. red ad-hoc vehicular es un tipo de red de comunicación que utiliza a los vehículos como nodos de la red. Dado el reducido alcance del canal de comunicación, la conectividad se establece de forma esporádica.

(Shahrudin Awang Nora, 2017) “Rendimiento simulado de protocolos TCP o Protocolo de control de transmisión, (Transmission Control Protocol - TCP), SCTP o Protocolo de transmisión de control de flujo, (Stream Control Transmission Protocol -SCTP), DCCP Protocolo de control de congestión de datagramas (Datagram Congestion Control Protocol- DCCP) y UDP o Protocolo de datagrama de usuario (User Datagram Protocol - UDP) sobre 4G network”

“La transmisiones de video necesita más ancho de banda y alta calidad de comunicación. El principal contribución en términos de la calidad de la comunicación es el desarrollo de la tecnología LTE, que ayuda en el rendimiento del aumento datos y la disminución de latencia.”

Los autores recomiendan que se debería optar por TCP, de lo contrario, DCCP es la mejor opción con un mejor rendimiento en la transmisión de video MPEG-4 en el entorno LTE.

(Xiaoyan Wang, 2014) “Protocolo para Redes Ad Hoc Inalámbricas”

“En este documento, los autores han propuesto una novedosa codificación de red protocolo cooperativo, a saber NCAC-MAC o protocolo de cooperación cooperativa compatible con codificación de red - control de acceso al medio, (network coding aware cooperative- Medium Access Control- NCAC-MAC) (Protocolo de Capa Física), para redes ad hoc inalámbricas. Introduciendo NCAC-MAC, las ventajas de NC y CC pueden ser explotado de manera satisfactoria en redes punto a punto”

Los autores refieren que el protocolo NCAC-MAC, serviría mucho para transmisión ya que muchos nodos vecinos en la red están transmitiendo en cada instante y para eso proponen un nuevo protocolo NCAC-MAC basado en MAC.

(Jianchao Ji1, 2015) “Protocolo de investigación en cápsula espacial”

“Los autores muestran resultados que la red Ad hoc posee rendimiento estable de la red solo si el nodo en movimiento se mueve lento. Uso de un sistema de red Ad hoc en la cápsula de satélite hace que el sistema de comunicación por cápsula satelital sea más confiable y mucho más seguro”

De acuerdo a la investigación Ji1, nos dice que el movimiento en una capsula espacial debe de ser lento para tener una performance, lo que pareciera a los investigadores que esto es un trabajo a futuro que se debe de tener en cuenta.

1.3. Bases Teóricas – Científicas (Trabajos Relacionados al Tema)

Variable Independiente: Protocolos de Comunicación

1.3.1. Concepto:

Un protocolo es un conjunto de normas. Los protocolos de Internet son conjuntos de reglas que inspeccionan la comunicación dentro de una red y entre los hosts que lo conforman. Las especificaciones de protocolo definen el formato de los mensajes que se intercambian.

(JORDI, y otros, 2008) “Estructura De Redes De Computadoras”

“Con los protocolos de red se pretende la intercomunicación de NIC’s situadas en máquinas diferentes. Entendemos por tarjetas de red a un sistema informático, ubicado dentro de una capa de un modelo de red como OSI”

De acuerdo a los autores los protocolos pretenden unificar diferentes sistemas para que se puedan entender y desarrollar las aplicaciones para las que fueron hechas.

(CISCO, 2018) “En lugar de crear sistemas exclusivos e independientes para la prestación de cada nuevo servicio, toda la industria de redes ha adoptado un marco de desarrollo que permite a los diseñadores comprender y mantener las plataformas de red actuales. Al mismo tiempo, este marco se está utilizando para facilitar el desarrollo de nuevas tecnologías para satisfacer las necesidades de comunicación y las futuras mejoras tecnológicas.”

Un aspecto fundamental de este marco de desarrollo es el uso de modelos generalmente aceptados que describen las reglas y funciones de la red.

1.3.1.1. Protocolo UDP:

(Bova, 1999) “Sin embargo, los investigadores han propuesto varias metodologías de diseño para utilizar los contenidos libres de errores de paquetes de red corruptos como UDP-Lite, UDP confiable y UDP completo”

(CISCO, 2018) “Si bien las características de confiabilidad TCP permiten una comunicación más robusta entre las aplicaciones, también representan una carga adicional y pueden causar retrasos en la transmisión. Existe una relación de compromiso entre el valor de confiabilidad y la carga que esto implica para los recursos de red.”

(CISCO, 2018) “Agregar gastos generales para garantizar la confiabilidad de algunas aplicaciones podría reducir la utilidad de la aplicación e incluso ser dañino. En estos casos, UDP es un mejor protocolo de transporte.”

(CISCO, 2018) “UDP proporciona las funciones básicas para proporcionar segmentos de datos entre las aplicaciones apropiadas, con muy poca sobrecarga y revisión de datos. UDP se conoce como protocolo de entrega de esfuerzo máximo.”

(CISCO, 2018) “En el contexto de las redes, la entrega del esfuerzo máximo se denomina "poco confiable" porque no hay confirmación de que los datos se han recibido en el destino. Con UDP, ningún proceso de capa de transporte informa al remitente si la transmisión fue exitosa.”

(TANENBAUM, 2003) “Redes de Computadoras”

“La suite de protocolos de Internet soporta un protocolo no orientado a la conexión que es Protocolo de Datagrama de Usuario”

Lo dicho por Tanenbaum sobre el protocolo UDP es que este no protocolo es un protocolo no orientado a la conexión

(CISCO, 2018) “Las redes nos están conectando más y más. Las personas se comunican en línea desde cualquier lugar. Las conversaciones en el aula continúan durante las sesiones de chat de mensajería instantánea y las discusiones en línea continúan en la ubicación del estudio. Todos los días, se desarrollan nuevos servicios para aprovechar la red”

(CISCO, 2018) “UDP se considera un protocolo de transporte de esfuerzo máximo. UDP es un protocolo de transporte liviano que ofrece la misma segmentación y reensamblaje de datos que TCP, pero sin la confiabilidad y el control de la transmisión TCP. UDP es un protocolo tan simple que generalmente se describe en términos de lo que no hace en relación con TCP.”

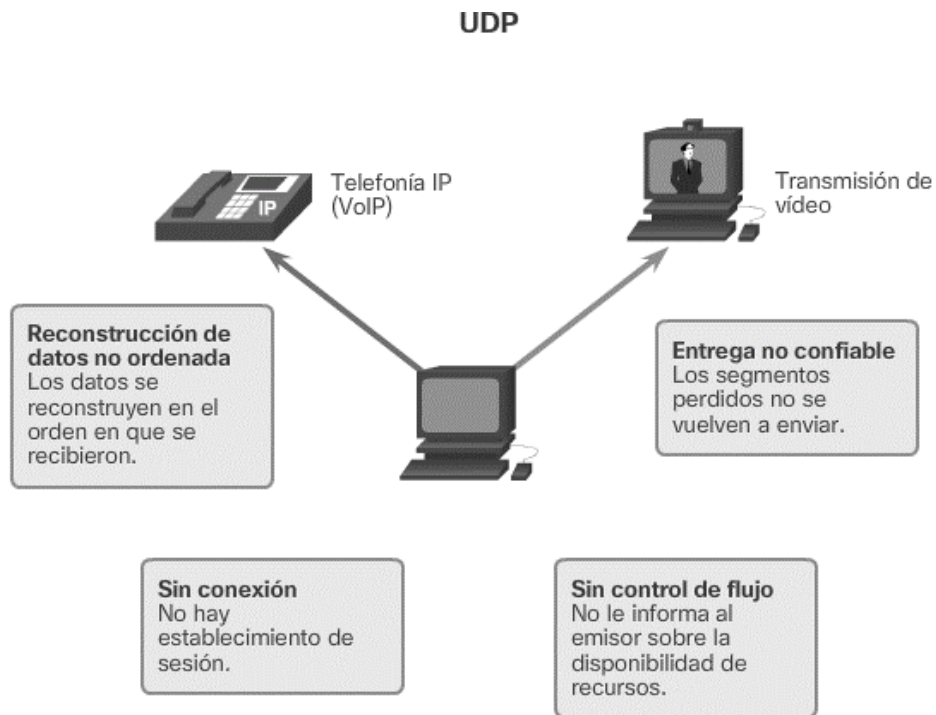


Figura4: Características de UDP
Fuente CISCO Networking

(CISCO, 2018) “UDP es un protocolo sin estado de información, lo que significa que ni el cliente ni el servidor deben monitorear el estado de la sesión de comunicación. Si se requiere confiabilidad cuando se utiliza UDP como protocolo de transporte, debe ser administrado por la aplicación.”

(CISCO, 2018) “Uno de los requisitos más importantes para el video en vivo y la voz en la red es que los datos viajan rápidamente. Las aplicaciones de video y voz en vivo pueden tolerar la pérdida de datos con un efecto mínimo o imperceptible y adaptarse perfectamente a UDP.”

(CISCO, 2018) “Los fragmentos de comunicación en UDP se llaman datagramas, como se muestra en la figura. El protocolo de capa de transporte envía estos datagramas con el máximo esfuerzo. UDP tiene una sobrecarga mínima de 8 bytes.”

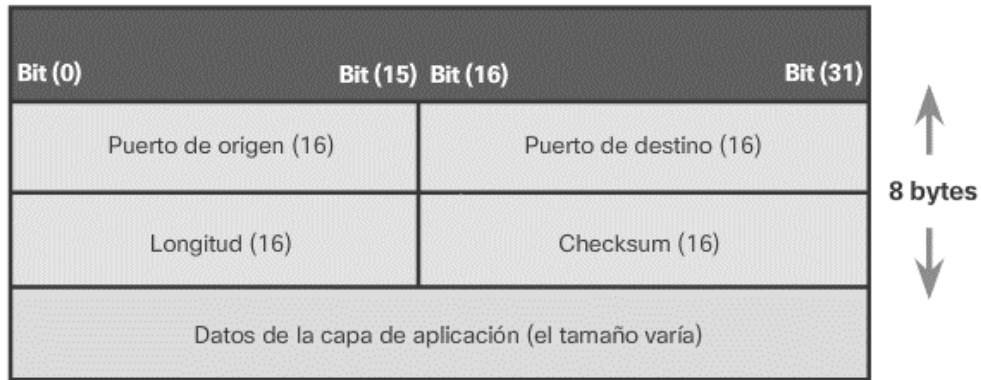


Figura5: Datagrama UDP
Fuente CISCO Networking

En lo dicho por los autores líneas arriba ellos deducen que el protocolo UDP es un protocolo rápido pero que tienen pérdidas, de paquetes en su transmisión, no entrega acuse de recibo, y no reensambla los paquetes, los entrega conforme van llegando.

1.3.1.2. Protocolo TCP

(TANENBAUM, 2003) “Redes de Computadoras”

“TCP se diseñó especialmente para proporcionar un flujo de byte, La función del protocolo de transporte TCP es similar al envío de paquetes de los que se hace un seguimiento de origen a destino. Si se divide un pedido de envío en varios paquetes, el cliente puede revisar en línea el orden de la entrega” El autor nos da a entender que el protocolo TCP es el que permite regenerar los paquetes perdidos y enviarlos nuevamente, además de enviarlos en forma secuencial.

(CISCO, 2018) “La función de protocolo de transporte TCP es similar a enviar paquetes seguidos de origen a destino. Si una orden de envío se divide en varios paquetes, el cliente puede ver la orden de entrega en línea.”

(CISCO, 2018) “Con TCP, hay tres operaciones básicas de confiabilidad:

- Numeración y seguimiento de segmentos de datos enviados a un host específico desde una aplicación específica
- Reconocimiento de los datos recibidos
- Retransmisión de datos sin reconocimiento después de un tiempo”

(CISCO, 2018) “Para comprender las diferencias entre TCP y UDP, es importante comprender cómo cada protocolo implementa características de confiabilidad específicas y cómo siguen las conversaciones. Además de admitir funciones básicas de segmentación y reensamblado de datos, el protocolo TCP, como se muestra en la figura 3, también brinda otros servicios.”

(CISCO, 2018) “En un establecimiento de una sesión, TCP es un protocolo orientado a la conexión. Un protocolo orientado a la conexión es un protocolo que negocia y establece una conexión permanente (o una sesión) entre los dispositivos fuente y destino antes de transferir el tráfico.

(CISCO, 2018) “Al configurar una reunión, los dispositivos negocian la cantidad de tráfico que se puede transmitir en un momento dado, y la comunicación de datos entre ellos se puede manejar con cuidado”

(CISCO, 2018) “En la entrega confiable, en términos de redes, fiabilidad significa garantizar que cada segmento enviado por el origen llegue a su destino. Por varias razones, es posible que un segmento se dañe por completo o se pierda cuando se transmite a través de la red.”

(CISCO, 2018) “Entrega en el mismo orden, los datos pueden llegar en el orden equivocado porque las redes pueden proporcionar múltiples rutas con diferentes velocidades de datos. Al numerar y secuenciar los segmentos, TCP puede garantizar su reensamblaje en el orden correcto.”

(CISCO, 2018) “Control de flujo, los hosts de red tienen recursos limitados, como memoria o potencia de procesamiento. Cuando TCP advierte que estos recursos están sobrecargados, puede solicitarle a la aplicación de envío que reduzca la velocidad del flujo de datos. “

(CISCO, 2018) “Esto se hace mediante TCP, que regula la cantidad de datos transmitidos por el origen. El control de flujo puede evitar tener que retransmitir datos cuando se exceden los recursos del host de destino.”

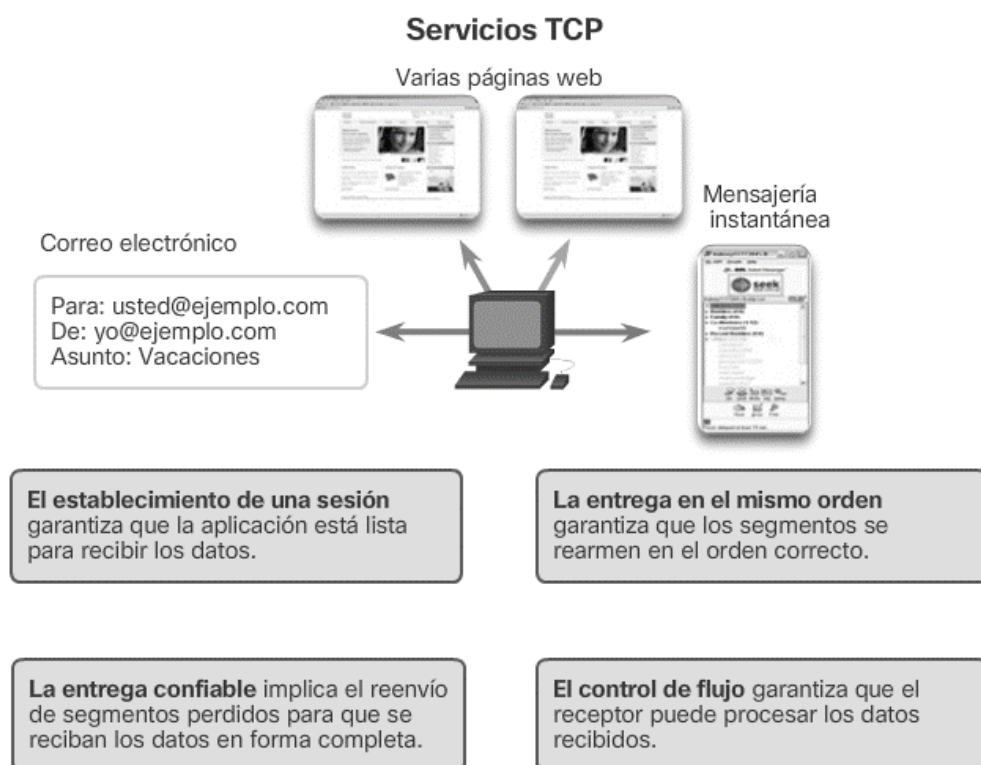


Figura6: Servicios UTP
Fuente CISCO Networking

El TCP es uno de los protocolos que permite la transferencia con confianza debido a que permite garantizar la entrega, pero con lentitud debido al tiempo que demora en garantizar la entrega, y está más orientado a la mensajería instantánea y al servicio de páginas web, pero esto no quiere decir que se le excluya de una transmisión de video.

1.3.1.3. Protocolo RSTP

(Profesores-ELO, s.f.) “RTSP es un protocolo orientado a la aplicación y no orientado a la conexión. En su lugar, el servidor RTSP ejecuta una sesión con un identificador (ID de sesión).

RTSP usa TCP para enviar datos de control del reproductor (mensajes "fuera de banda") y UDP para datos de audio y video fuera de banda (mensajes "en banda"), aunque TCP también se puede usar cuando se requiere confiabilidad para enviar paquetes que no son compatibles con UDP, para ser proporcionado.

El concepto de "en banda" y "fuera de banda" se refiere al hecho de que el protocolo puede enviar diferentes tipos de información a diferentes puertos”.

(Tenealive, s.f.) “**Protocolos y modelos de comunicación de las cámaras ip wifi de videovigilancia y domótica de Tenealive**”

“RTSP, proviene de las siglas en inglés Real Time Streaming Protocol y como su nombre indica **es un protocolo de flujos de datos en tiempo real**. Su función consiste en establecer y controlar uno o muchos flujos sincronizados de datos (pudiendo ser audio o vídeo)”, este protocolo trabaja en la capa 2 (capa de enlace) del modelo OSI (Open System Interconnection) siendo este modelo el que rige las comunicaciones en el mundo de las redes.

“RSTP se ha convertido en el protocolo preferido para prevenir bucles de capa 2 en topologías que incluyen redundancia. Además de que el 802.1w contiene mejoras, retiene compatibilidad con su antecesor 802.1D dejando algunos parámetros sin cambiar. Por ejemplo, RSTP mantiene el mismo formato de BPDU o unidad de datos de protocolo puente (bridge protocol data unit - BPDU) que STP sólo que cambia el campo de versión, el cual se le asigna el valor de 2.”

“RSTP también define el concepto de edge-port, el cual también se menciona en STP como PortFast, en donde el puerto se configura como tal cuando se sabe que nunca será conectado hacia otro switch de manera que pasa inmediatamente al estado de direccionamiento sin esperar los pasos intermedios del algoritmo –etapas de escucha y aprendizaje- los cuales consumen tiempo. Los puertos que no son edge-ports pueden ser punto a punto o compartidos. El tipo de enlace es detectado automáticamente, pero

puede ser configurado explícitamente para hacer más rápida la convergencia.”

1.3.1.4. Protocolo PPPoE

Protocolo sobre Ethernet punto a punto (Point-to-Point Protocol over Ethernet- PPPoE). Es un miembro de la suite TCP / IP de protocolos de red. PPP es una extensión de TCP / IP que agrega dos conjuntos adicionales de funcionalidad:

- a) Puede transmitir paquetes TCP / IP a través de un enlace serial
- b) Tiene seguridad de inicio de sesión

PPP que fue diseñado para comunicaciones en serie ahora se ha adaptado a Ethernet y se denomina PPP over Ethernet (PPPoE).

PPPoE mejora el tráfico de red que el protocolo TCP/IP en redes punto a punto.

(Tenealive, s.f.) **“Protocolos y modelos de comunicación de las cámaras ip wifi de videovigilancia y domótica de Tenealive”**

“Protocolo sobre ethernet punto a punto (Point-to-Point Protocol over Ethernet- PPPoE) se usa generalmente para la abastecimiento de conexiones de banda ancha mediante servicios de DSL y módem/cable. Habilita la implementación de una capa IP sobre una conexión entre dos puertos Ethernet.”

1.3.1.5. Protocolo DCCP

Las aplicaciones cambiaron cuando aparecieron aplicaciones multimedia en tiempo real. Como resultado de su confiabilidad, TCP no permite que las aplicaciones controlen la velocidad de envío. Esto produce retrasos incompatibles con el servicio que ofrecerá la aplicación. UDP permite controlar la tasa de envío, pero resulta peligroso ya que no provee control de congestión, pudiendo saturar de la red. Para resolver esta situación, el IETF ha definido el Protocolo de Control de Congestión de Datagramas (DCCP), un protocolo diseñado específicamente para soportar aplicaciones multimedia en tiempo real.

(Kohler, Handley, & Floyd, 2014) “Diseñando DCCP: control de la congestión sin fiabilidad”

“DCCP, el protocolo de control de congestión de Datagram, es un nuevo protocolo de transporte en la familia TCP / UDP que proporciona un flujo controlado por congestión de datagramas poco confiables”.

“DCCP es un protocolo de transporte mínimo de propósito general que proporciona

dos funciones principales: (1) el establecimiento, mantenimiento y desmontaje

de un flujo de paquetes no confiable y (2) control de congestión de ese flujo de paquetes.”

Su medio está: Orientado a la conexión; Transporte no confiable; Preserva límite de mensaje; entrega no ordenada; datos de comprobación; checksum tamaño 16 bits; parcial checksum; path MTU o unidad de transmisión máxima (Maximum Transmission Unit-MTU); control de congestión.

1.3.1.6. CCTV DIGITAL

La videovigilancia IP es una tecnología de vigilancia visual que combina los beneficios analógicos del circuito cerrado de televisión tradicional (circuito cerrado de televisión) con las ventajas digitales de las redes de comunicación IP (Protocolo de Internet), que permiten el monitoreo local y / o remoto de imágenes y audio. Así como el tratamiento digital de imágenes, para aplicaciones tales como reconocimiento de registro (placas de vehículos) o reconocimiento facial.

(Aslan, 2011) “Un circuito cerrado de televisión o CCTV, admite la conexión de cámaras de vídeo directamente a las redes informáticas por las que se comunican los ordenadores basados en los protocolos TCP/IP, y que ya la mayoría de las oficinas y empresas cuentan con dicho sistema para su protección.”

(Aslan, 2011) “El sistema de audio y el vídeo transmitido desde cualquier cámara de red o servidor de vídeo pueden visualizarse desde cualquier ordenador conectado a una red de área local, a través de una intranet privada o a través de Internet.”

Sin embargo, si tenemos un sistema CCTV analógico, la migración se hace muy costoso.



Figura 7: Sistemas de CCTV Digital
Fuente: Axis Communications

1.3.1.7. CCTV HIBRIDO

(Network, 2011) “Con referencia a los otros sistemas nace el CCTV mixto que es la combinación del analógico y el digital basado en IP, se adquiere todas las funcionalidades y ventajas que ofrece la tecnología digital, reduciendo costos usando laboratorios análogos.”

(Network, 2011) “Según los especialistas de redes, este sistema combina las ventajas de la tecnología analógica de circuito cerrado de televisión con la flexibilidad y facilidad de acceso proporcionados por la tecnología IP.”

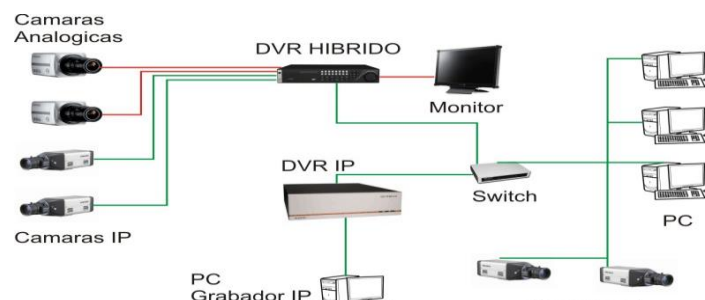


Figura 8: Sistema CCTV Híbrido
Fuente: Axis Communications

1.3.2. CARACTERISTICAS DE CAMARAS IP:

Entre los elementos más importantes que conforman una estructura de un sistema de videovigilancia se pueden enumerar a los siguientes:

1.3.2.1. Cámara IP

(Axis, Axis, 2013) “La cámara de red tiene su propia dirección IP, está directamente conectada a un dispositivo intermediario de la red. Una cámara de red proporciona servidor web, FTP File Transfer Protocol (Protocolo de transferencia de archivos) y funciones de correo electrónico.”

En el orden de las ideas anteriores, decir que las cámaras IP son host de red que tienen características similares a las de una computadora, ya que tiene una dirección IP propia, o asignada por un servidor DHCP.

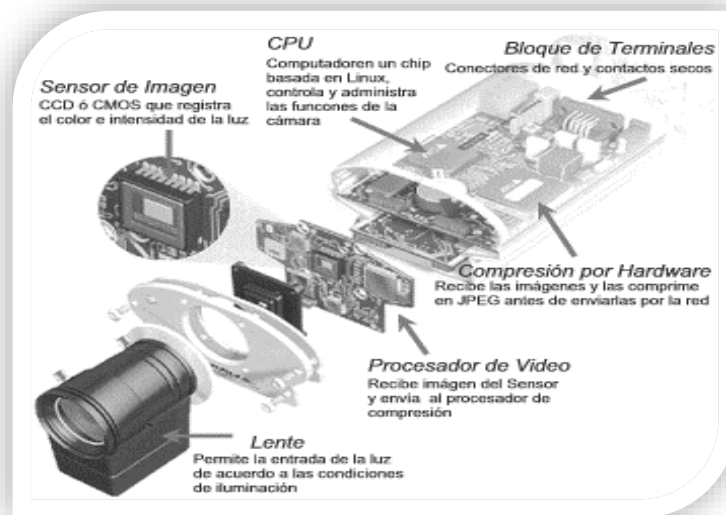


Figura 9: Partes de una Cámara de Red

Fuente: <http://comaxnet-seguritech.blogspot.com/2009/11/que-es-una-camara-ip.html>

(Teostekwebstore, 2014) “Según la revista, las cámaras de red pueden configurarse para enviar vídeo a través de una red IP para visualización y/o grabación en directo, ya sea de forma continua, en horas programadas, en un evento concreto o previa solicitud de usuarios autorizados.”

(Teostekwebstore, 2014) “Las imágenes que se capturan pueden secuenciarse con formatos como Motion JPEG, MPEG-4 o H.264 utilizando distintos protocolos de red. De la misma manera, pueden almacenarse como imágenes JPEG individuales usando FTP, correo electrónico o HTTP (Hypertext Transfer Protocol).”

Se presenta, a continuación, las características principales que debe tener una cámara así como también algunos ejemplos de cada una:

| CARACTERISTICAS PRINCIPALES QUE DEBE TENER UNA CAMARA IP | |
|---|---------------------------------|
| Lentes | Para las aplicaciones externas |
| Sensor de imagen | CCD o CMOS |
| Resolución | 640x480, 320x240 |
| Tasa de cuadro | 30, 25 o 20 cuadros por segundo |
| Formatos de video | MJPEG y/o MPEG4 |
| Audio | G.711 o formato AAC-LC |
| Software | Compatible |
| Seguridad | nombre y contraseña de usuario |

1.3.2.2. Tipos de Cámaras

Las cámaras de red, pueden clasificarse en cámaras de red fijas, domo fijas, PTZ, y domo PTZ.

Cámaras de red fijas.

(Axis, Axis, 2014) “Son cámaras que tienen un área de vista fija una vez instalada. Es la cámara tradicional en la que la dirección en la que esta direccionada son visibles.”

(Axis, Axis, 2014) “En este tipo de cámaras generalmente encontramos como la mejor opción cuando se trata de tener cámaras visibles con gabinetes en exteriores.”

“Las cámaras de caja fija de Axis envían un mensaje disuasorio claro a los delincuentes potenciales. Esto se debe a que proporcionan un ángulo de visión fijo y claramente visible que permite percibir con exactitud hacia dónde están dirigidas y posibilita la grabación de una zona definida con precisión. Las cámaras permiten una instalación rápida y sencilla para aplicaciones en interiores y exteriores. Son ideales para proteger tiendas, colegios y lugares públicos. La alimentación a través de Ethernet (IEEE 802.3af) suministra alimentación eléctrica a las cámaras a través de la red, lo que elimina la necesidad de cables de alimentación y reduce los costes de instalación.”

| CARACTERISTICAS DE CAMARAS IP MARCA AXIS | | | | |
|---|-------------------|---------------------|-------------------|---------------------|
| CARACTERISTICAS | AXIS M1124 | AXIS M1124-E | AXIS M1125 | AXIS M1125-E |
| Resolución de vídeo máx. | 1280x720 | 1280x720 | 1920x1080 | 1920x1080 |
| Iluminación/sensibilidad de luz mín. (color) | 0.25 lux | 0.25 lux | 0.25 lux | 0.25 lux |
| Tamaño de sensor en megapíxeles | 1.3 | 1.3 | 2 | 2 |
| Resolución HDTV | 720p | 720p | 1080p | 1080p |
| Lentes varifocales | ✓ | ✓ | ✓ | ✓ |
| Iris DC | ✓ | ✓ | ✓ | ✓ |

| | | | | |
|--|---|---|---|---|
| P-Iris | | | | |
| Movimiento horizontal y vertical digital | ✓ | ✓ | ✓ | ✓ |
| Zoom digital | ✓ | ✓ | ✓ | ✓ |
| Alimentación a través de Ethernet | ✓ | ✓ | ✓ | ✓ |
| Almacenamiento local | ✓ | ✓ | ✓ | ✓ |
| Funcionalidad día y noche | ✓ | ✓ | ✓ | ✓ |
| Infrarrojos integrados | ✓ | ✓ | ✓ | ✓ |
| E/S digital | ✓ | ✓ | ✓ | ✓ |
| Zipstream | ✓ | ✓ | ✓ | ✓ |



Figura 10: Cámaras de red Fijas
Fuente: Axis Communications

Cámaras de red Domo Fijas:

(Axis, Axis, 2014) “Estas cámaras son discretas por su tamaño, tienen buena resistencia por su gabinete en la manipulación.”

“La serie AXIS Q35 cuenta con domos fijos para interior y exterior de alto rendimiento y resistentes a agresiones que ofrecen una calidad de imagen excelente con una resolución de hasta 4K. El amplio rango dinámico (WDR) de las cámaras garantiza una calidad de vídeo perfectamente equilibrada en escenas con fuertes variaciones de luz, mientras que la tecnología Lightfinder permite unos resultados de imagen extraordinarios con poca luz. La serie AXIS Q35 también cuenta con la estabilización de imagen electrónica, EIS, que mejora considerablemente la calidad de vídeo y mantiene la tasa de bits baja cuando la cámara se ve sometida a vibraciones. Además, algunas cámaras cuentan con zoom óptico que puede usarse al supervisar una escena.”



Figura 11: Cámaras IP Domo Fija
Fuente: Axis Communications

| CARACTERISTICAS PRINCIPALES DE DOS MODELOS DE CAMARAS IP DE LA MARCA AXIS | | |
|---|--------------------|-------------------|
| CARACTERISTICAS | MODELOS - DOMO | |
| | AXIS Q3517-SLVE | AXIS Q3518-LVE |
| Resolución de vídeo máx. | 3072x1728 | 3840x2160 |

| | | |
|-----------------------------------|--------------|--------------|
| Tamaño de sensor en megapíxeles | 5 | 8 |
| Resolución HDTV | 1920x1080 | 1920x1080 |
| Lightfinder | ✓ | ✓ |
| Estabilización de imagen | ✓ | ✓ |
| Zoom remoto | ✓ | ✓ |
| Audio bidireccional | ✓ | ✓ |
| Entradas/salidas de alarma | 2 | 2 |
| Enfoque remoto | ✓ | ✓ |
| Alimentación a través de Ethernet | ✓ | ✓ |
| Zipstream | ✓ | ✓ |
| Tecnología WDR | Forensic WDR | Forensic WDR |
| Infrarrojos integrados | ✓ | ✓ |

Cámaras PTZ y (Axis, Axis, 2014) “este tipo de cámaras las domo PTZ. Tienen movilización en ambos ejes, acercarse o alejarse de un área o un objeto de forma manual o automática.”

“Las cámaras de red PTZ de Axis utilizan el movimiento horizontal/vertical y zoom para cubrir los dos perímetros amplios y proporcionar un excelente

nivel de detalle con una sola cámara. Una excelente calidad de imagen y la habilidad de acercar el zoom hacen posible la verificación de eventos de seguridad detectados. El resultado es una protección máxima y unos costes mínimos.”

“Las cámaras incorporan una variedad de funciones inteligentes y se pueden mover entre posiciones predefinidas y acercar el zoom automáticamente como respuesta a los eventos detectados. También pueden integrarse fácilmente en un sistema con otras cámaras.”



Figura 12: Cámara Domo PTZ
Fuente: Axis Communications

| CARACTERISTICAS PRINCIPALES DE DOS MODELOS DE CAMARAS IP DE LA MARCA AXIS | | |
|---|--------------------|--------------------|
| CARACTERISTICAS | MODELOS – DOMO PTZ | |
| | AXIS P5624-E Mk II | AXIS P5635-E Mk II |
| Resolución de vídeo máx. | 1280x720 | 1920x1080 |

| | | |
|--|-------------|-------------|
| Iluminación/sensibilidad de luz mín. (color) | 0.2 lux | 0.2 |
| Resolución HDTV | 720p | 1080p |
| Zoom óptico | 23 | 30 |
| Rango de panorámica | 360 endless | 360 endless |
| Audio bidireccional | ✓ | ✓ |
| Entradas/salidas de alarma | ✓ | 4 |
| Estabilización de imagen | ✓ | ✓ |
| Alimentación a través de Ethernet | ✓ | ✓ |
| Zipstream | ✓ | ✓ |
| Focus recall | ✓ | ✓ |

Servidor de Video

Un servidor de video son dispositivos que permiten convertir señales analógicas a digitales.



Figura 13: Grabador AXIS Camera Station S1148
Fuente: Axis Communications

“Los grabadores ofrecen un rendimiento mejorado y contiene una potente CPU que permite un rápido procesamiento de los datos. El sistema operativo se almacena en un disco de estado sólido (SSD), lo que significa que el inicio del sistema es rápido y que el sistema operativo está protegido en caso de fallo.”

“El AXIS S1148 viene pre configurado con RAID, con lo que el almacenamiento de los datos es aún más fiable gracias a la protección adicional e integrada contra pérdidas. Además, económico, con un soporte técnico in situ en el siguiente día laborable y la opción de ampliación de garantía por dos años, siempre puede confiar en la calidad, fiabilidad y soporte técnico de primera clase de Axis”

Grabador de Video en Red (NETWORK VIDEO RECORDER- NVR)

El grabador de video en red (Network Video Recorder-NVR), a diferencia del grabador de video digital (Digital Video Recorder-DVR) del caso analógico, puede no ser parte del sistema, ya que cualquier computadora en la intranet o en internet podrá acceder directamente a las cámaras y almacenar las imágenes en su propio disco duro. El NVR deberá estar presente solo si deseamos realizar simultáneamente la visualización y grabación de las

cámaras. Todas las cámaras IP suelen llevar incorporado un sistema de almacenamiento que también permite la grabación del video.

El NVR es el indicado para instalaciones profesionales. El soporte de grabación es, generalmente, un disco duro o HD (igual que el de los ordenadores, aunque de mayor resistencia). Se puede conectar al NVR un monitor Diodo Emisor de Luz (*light-emitting diode*-LED para visualizar las grabaciones, y un teclado especial para controlar el movimiento y/o zooms desde el propio grabador. El NVR puede conectarse en cualquier parte de la LAN, lo que permiten que comparta espacios con otros equipos de red equipados con climatización y un sistema de alimentación ininterrumpida (uninterruptible power supply-UPS). Para la conexión a internet requiere una IP fija, o una configuración adecuada por parte de personal informático en el caso de que la IP sea dinámica. Para instalaciones en las que se requiera almacenar una cantidad de información relativamente grande es posible la conexión de varios NVR a la red.

Un sistema NVR es un grabador basado en IP que opera independientemente.

Funciones que desempeña:

Diseñado para almacenar video digital de las cámaras IP.

Tiene un disco duro de gran mínimo de 1 terabyte de capacidad para permitir grabación por largos períodos de tiempo.

La diferencia principal entre un DVR y un NVR es que en el DVR se conectan cámaras análogas y en el NVR se conectan cámara IP.

El grabador AXIS Camera Station S1148 es una solución de grabación lista para instalar y diseñada para conseguir una vigilancia fiable en alta definición. El grabador tiene la forma de un servidor para bastidor, con la posibilidad de agregarle discos duros adicionales y una capacidad de almacenamiento de hasta 140 TB.

Esta solución fácil de instalar incluye licencias de AXIS Camera Station para instalaciones medianas, de modo que tendrá todo lo necesario para que cada instalación de cliente esté libre de problemas.

Ya se trate de fábricas, escuelas o comercios, el grabador AXIS Camera Station S1148 cumple los requisitos de una gran variedad de negocios y sectores. Resulta ideal siempre que sea necesaria una vigilancia fiable y segura.



Figura 14: NVR o E (Power Over Ethernet)

POE-Ethernet

Este tipo de alimentación permite otorgar energía al sistema de vigilancia, manteniendo el sistema en funcionamiento incluso durante cortes de corriente, generalmente cuando lo tenemos conectado a un UPS.

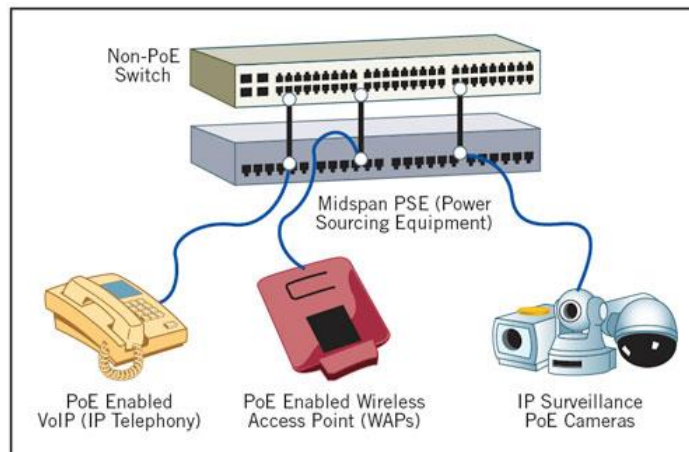


Figura15: Alimentación a Través de POE

Ancho de Banda

Es una medida que se usa para medir la velocidad de Internet. Se puede usar para referirse a capacidad o a consumo. Se mide en bits por segundo (bits/s), en kilobits por segundo (kbit/s), megabits por segundo (Mbit/s) o algún otro múltiplo. También se le conoce como ancho de banda digital o ancho de banda de red.

| VELOCIDAD DE ALGUNOS MEDIOS TÍPICOS DE TRANSMISIÓN | | |
|--|------------------------|-------------------------|
| Medios típicos | Velocidad | Distancia física máxima |
| Cable coaxial de 50 ohmios (Ethernet 10BASE2) | 10-100 Mbps | 185m |
| Cable coaxial de 50 ohmios (Ethernet 10BASE5) | 10-100 Mbps | 500m |
| Par trenzado no blindado de categoría 6 (UTP)(Ethernet 10BASE-T y 100BASE-TX) | 10 Mbps | 100m |
| Par trenzado no blindado mejorado categoría 6 (UTP) (Ethernet 10BASE-T, Fast Ethernet 100BASE-TX y 1000BASE-T) | 100 Mbps | 100m |
| Fibra óptica multimodo (62,5/125mm) 100BASE-FX, 1000BASE-SX | 100 Mbps | 2000m |
| Fibra óptica monomodo (núcleo de 9/125mm) 1000BASE-LX | 1000 Mbps (1.000 Gbps) | 3000m |
| Inalámbrico | 54Mbps | Unos 100 metros |

Tabla 2: Velocidades de diferentes medios de transmisión

Existe otro concepto importante que se debe tener en cuenta: el rendimiento.

El rendimiento generalmente se refiere al ancho de banda real medido, en un momento específico del día, usando rutas específicas de Internet, mientras se descarga un archivo específico. Desafortunadamente, por varios motivos, el rendimiento a menudo es mucho menor que el ancho de banda digital máximo posible del medio que se está usando. Algunos de los factores que determinan el rendimiento y el ancho de banda son los siguientes:

1. dispositivos de internetworking
2. tipo de datos que se transfieren
3. topología
4. cantidad de usuarios
5. computador del usuario
6. computador del servidor

Al diseñar una red, es importante tener en cuenta el ancho de banda teórico. La red no será más rápida que lo que los medios permiten.

Variable Dependiente: Prestaciones de rendimiento en la transmisión de datos en un sistema de videovigilancia.

1.3.3. Concepto:

(Juan B. Riera García, 1986) “La transmisión de datos, la transmisión de datos digitales y la comunicación de datos digitales es la transmisión de datos de datos a un canal de comunicación común a un servidor de telefonía móvil. Modelos de alambroón, fibra óptica, canales de comunicación inalterables y almacenamiento de medios”

(CISCO, 2018) “Para algunas aplicaciones, los segmentos deben llegar en un orden específico para responder correctamente. Además, todos los datos son aceptados por todos. En ambos casos, use TCP como el protocolo de transporte. Los desarrolladores de aplicaciones deben seleccionar el tipo de protocolo de transporte apropiado en función de las necesidades de la aplicación”

(ECURED, 2018) “Transmisión de información que consiste en el movimiento de información codificada, de un punto a uno o más puntos, mediante señales eléctricas, ópticas, electrónicas o electromagnéticas.”

1.4. Formulación del Problema

¿Cuál será el protocolo de comunicación de capa de Transporte que presenta mejores prestaciones de rendimiento en la transmisión de datos en un sistema de videovigilancia?

1.5. Justificación de la Investigación

Pertenencia: Está enmarcada dentro de la línea de investigación de Tecnologías de la información de la Escuela profesional de ingeniería de sistemas, de la USS, y se aporta un conocimiento sobre el rendimiento de los protocolos de comunicación de redes en entornos de video vigilancia.

Pertinencia: El protocolo elegido en este casos, ayudara a que los usuarios, de casa, escuelas, municipalidades puedan elegir un protocolo adecuado para la transmisión de videovigilancia en vivo.

Viabilidad: La viabilidad técnica y económica es asequible ya que no se incrementaría en los costos de presupuestos ya que los protocolos están incluidos en los sistemas operativos y los equipos vienen implementados para los principales protocolos que existen como son el UDP, TCP, IP, DCCP, AODV, OLSR y BATMAN.

1.6. Hipótesis

El protocolo UDP de la capa de Transporte OSI/TCP es el que presenta mejores prestaciones de rendimiento en la transmisión de datos en un sistema de videovigilancia.

1.6.1. Variables

a) Variable Independiente

Protocolos de comunicación de redes.

b) Variable Dependiente.

Prestaciones de rendimiento en la transmisión de datos en un sistema de videovigilancia.

1.7. Objetivos de la investigación

1.7.1. Objetivo General

Realizar un análisis comparativo de protocolos de comunicación de redes UDP y TCP para un sistema de videovigilancia, la elección de la muestra fue elegida por conveniencia.

1.7.2. Objetivos Específicos

1. Seleccionar los protocolos de comunicación de redes.
2. Implementar los protocolos de comunicación de redes.
3. Analizar los resultados.

(Pelaez Salvador, 2018). “En vista de que existen distintos protocolos para capa del modelo, debemos centrarnos en aquellos que nos sirvan para transmitir contenido multimedia, más específicamente audio y video”.

Por consiguiente, los protocolos necesarios son los siguientes:

| Ranking Mejores 10 Protocolos para Videovigilancia IP | | |
|---|------------------|----------------------|
| Posición | Nombre Protocolo | Capa en la que Opera |
| 1 | UDP | Transporte |
| 2 | TCP | Transporte |
| 3 | RTP | Sesión/Transporte |
| 4 | RTCP | Sesión/Transporte |
| 5 | RTSP | Sesión |
| 6 | FTP | Aplicación |
| 7 | HTTP | Aplicación |
| 8 | SMTP | Aplicación |
| 9 | DCCP | Transporte |
| 10 | BATMAN | Internet |

Tabla 3: Elaboración de Ranking de Protocolos seleccionado los cuales se elegirán los dos primeros
Fuente. Elaboración Propia

1. **UDP:** (CISCO, 2018)“Proporciona las funciones básicas para proporcionar segmentos de datos entre las aplicaciones apropiadas, con muy poca sobrecarga y revisión de datos. UDP se conoce como protocolo de entrega de esfuerzo máximo.”
2. **TCP:** (CISCO, 2018) “Se considera un protocolo de transporte de datos completo y confiable que garantiza que el sistema de transferencia de datos sea compatible. El protocolo TCP es similar al envío en varios paquetes, el cliente puede revisar en línea el orden de la entrega.”
3. **RTP:** (H Schulzrinne, 2003)(Real-Time Transport Protocol) Funciona sobre el protocolo UDP. Utiliza un canal para audio y un canal para video. La transmisión de estos datagramas no es garantizada pues solo se verifica el envío. Funciona con unicast, pero también puede funcionar con multicast.
4. **RTCP:** (H Schulzrinne, 2003) Funciona sobre el protocolo UDP. Se verifica periódicamente los datos enviados en tiempo real. La transmisión de estos datagramas es garantizada, pero en ocasiones tardía. Funciona con unicast y también con multicast.
5. **RTSP:** (H Schulzrinne, 2003) Funciona sobre el protocolo UDP. Transmisión de datos multimedia de manera segura para múltiples usuarios. Control de sesión y localización de medios.
6. **FTP:** (*File Transfer Protocol*) es, como su nombre indica, otro protocolo de transferencia de datos basado en la estructura cliente-servidor. Este protocolo **determina cómo se deben transmitir estos archivos a través de una red TC/IP**, de manera que no sólo hace

posible esta transferencia de datos, sino que también **garantiza la independencia de los sistemas del equipo cliente y del servidor.**

7. **HTTP:** (*Hiper Text Transfer Protocol*), de transferencia de texto, cumple 26 años en 2016. Desarrollado por el World Wide Web Consortium y la Internet Engineering Task Force, **su principal objetivo es la transferencia de archivos entre un cliente, por ejemplo un navegador web, y un servidor, como puede ser un ordenador**, siguiendo el esquema de cliente-servidor. **Es el protocolo usado en cada transacción de la World Wide Web (WWW), donde es el protocolo más utilizado**, haciendo que la información de las páginas web pueda verse en los navegadores. La información obtenida a través de estas transacciones se denomina cookies y queda guardada en el servidor. **Está pensado para recuperar información y realizar búsquedas indexadas.** Además de la transferencia de textos HTML, permite hacer lo mismo con otros archivos de varios formatos.

8. **SMTP:** (*Simple Mail Transport Protocol*) está presente en el intercambio de correos electrónicos entre diferentes ordenadores de manera fiable y eficiente. **Funciona en línea y mediante una conexión punto a punto.** Este protocolo **tiene la función de enviar el correo electrónico, la entrega del mensaje**, a la vez que define una serie de **normas** para el envío del correo, necesarias para estandarizar la comunicación.

9. **DCCP:** Funciona sobre el protocolo TCP. Transmisión de datos multimedia similar al protocolo RTCP. Ofrece control de congestión y reenvío de paquetes perdidos.

1.8. Caso de Estudio

La Municipalidad Distrital de Víctor Larco desea implementar una red de videovigilancia acorde con la tecnología de vanguardia en el mundo moderno.

Ante la inseguridad ciudadana existente el Alcalde Distrital tomo la decisión de implementar un sistema de video vigilancia para así mejorar la seguridad ciudadana.

Al respecto detallo que la infraestructura tecnológica comprende de al menos 80 cámaras de video vigilancia, modelo Domo PTZ, 50 cámaras fijas para reconocimiento de placas y 19 para el reconocimiento de rostros. A éstas se suman las 9 instaladas en el 2015, teniendo un total de 78 video cámaras.

“Con la implementación de esta central de cámaras de seguridad, Víctor Larco se convierte en el primer distrito, de todo el norte del país, en contar con un control de vigilancia constante que identifique actos delictivos a un tiempo real, para poder combatir la delincuencia y actos antisociales”.

Asimismo la meta de la municipalidad es hacer de Víctor Larco, un distrito moderno y seguro para que los moradores de los diferentes sectores puedan transitar tranquilamente por las calles, sin temor a ser asaltados.

Se eligió esta institución gubernamental por ser la mas adecuada para la puesta en marcha de los protocolo ya que sus cámaras estaban usando el protocolo automático, el protocolo TCP, por esa razón es que se hizo pruebas en dos cámaras del sector de “Clínica Fátima”

1.9. Escenario de Pruebas

Para el escenario de Pruebas se usó el formato de la metodología Top Down de CISCO el cual nos proporciona cuatro fases las que se explicaran a continuación.

Fase I. Análisis

En esta fase se analizaron que protocolos se deberían usar para el estudio de los protocolos, el cual se determinó por conveniencia que deberían ser los protocolos TCP y UDP.

Fase II. Diseño Lógico

En las pruebas de laboratorios, se usaron Software como GNS-3, Packet Tracer y Virtual Box, ya que permiten configurar routers, Switches, incluso los sistemas operativos de computadoras. Se pudieron poner máquinas virtuales usando software virtual box, funcionales (por ejemplo de servidores). De esta forma, se tuvieron laboratorios virtuales para hacer pruebas en los ordenadores. Se pudieron probar de manera virtual, sin necesidad de hacerlo en producción, cómo responderían cambios de configuración en equipos en la red real. Pueden planear cambios en la red y visualizar lo que implicarían, configurar red privada virtual (virtual private network-VPNs, virtual local área network-VLANs).

Es compatible con muchos equipos y sistemas operativos. Es decir pueden emular routers Cisco, Juniper, Mikrotik..., pueden poner equipos Mac, PC, Linux, servidores, redes de área local inalámbricas (wireless lan área network-WLANs). Y se probaran todas las topologías de red con sólo un par de clics. Sin riesgos.

La mayoría de los usuarios no necesita direcciones IP estáticas. Por lo general, es importante tener una cuando un dispositivo o sitio web externo necesita recordar direcciones IP. Un ejemplo de ello son las VPN y otras soluciones de acceso remoto que confían (incluyen en una lista blanca) en determinadas IP por motivos de seguridad.

Se usó IP estáticas para las cámaras para la identificación de los nodos en los distintos puntos del distrito.

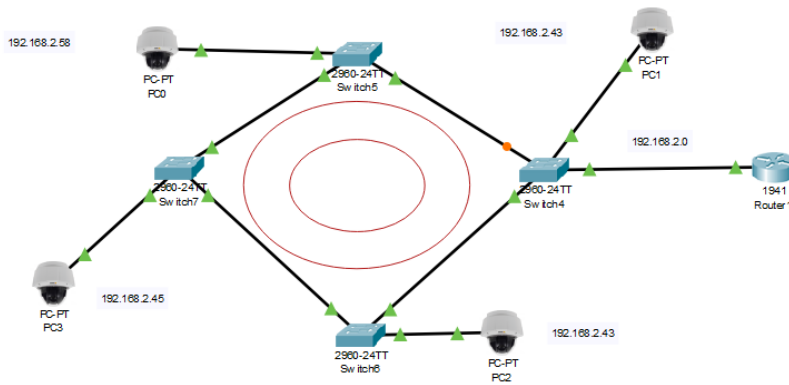


Figura 16: Topología Lógica
Elaboración Propia

Como tenemos una topología en anillo, si falla cualquiera de las tres líneas serie los routers rápidamente activarán la ruta indirecta para restablecer la comunicación entre las redes que hayan quedado aisladas.

Fase III. Diseño Físico

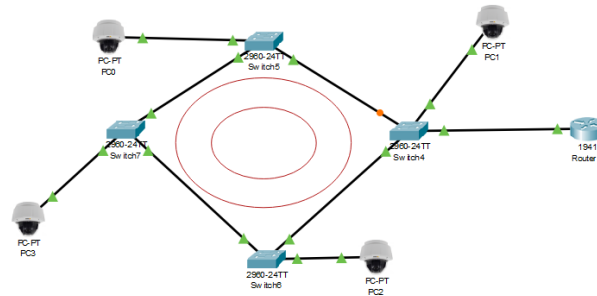


Figura 17: Topología Física
Elaboración Propia

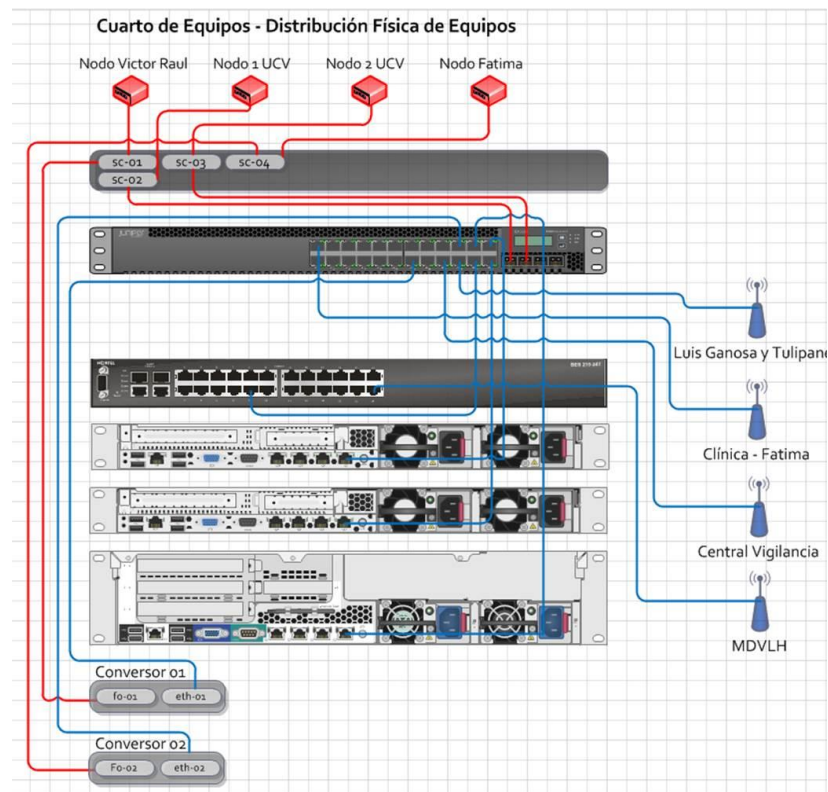


Figura 18 Topología Física
Fuente Municipalidad Victor Larco

Diseño físico propuesto

Los medios que se usaron fueron los guiados (cableado), por razones de facilidad para el estudio de los protocolos incluidos en la cámara de seguridad en la práctica de laboratorio.

Para la implementación de la topología se tuvo que adquirir cable UTP cat 6, conectores RJ45 de la categoría 6, la norma que se uso es la norma 568-B, se hicieron las pruebas usando una cámara de video vigilancia IP TredNet, una computadora, un switch y un Router de la marca CISCO, para las pruebas.

A. TIPO DE MEDIO:

- a. UTP: Categoría 6

- b. Dispositivos finales con patch Cord
- c. Estándar TIA 568 B

B. DISPOSITIVOS

- a. 1 cámaras IP
- b. 1 Modelo Cloud Inalámbrica TV-IP751W
- c. 1 Monitor: Televisor Smart 42 " samsung.
- d. 1 Servidor Dell PowerEdge 2950 Server
- e. 1.5 TB disco duro 16 GB ram.WD Purple
- f. 1 Switch cisco catalys 2960 24 puertos.
- g. 1 Router Router Cisco 870w.

En la topología propuesta por CISCO el servidor de medios de videovigilancia es el componente central de la solución, que proporciona la colección y enrutamiento de video desde cámaras IP a espectadores u otros servidores de medios. El sistema es capaz de correr en un único servidor físico o distribuido a través de la red, escalando para manejar miles de cámaras y usuarios. La Figura16 muestra cómo las cámaras IP o los codificadores envían un flujo de video único al Servidor de Medios. Los Media Server es responsable de distribuir transmisiones de video en vivo y archivadas a los espectadores simultáneamente a través de una red IP.

Para la visualización de archivos, el servidor de medios recibe el video de la cámara IP o el codificador continuamente (como configurado según la configuración del archivo) y solo envía secuencias de video al espectador cuando se lo solicita. En entornos con sucursales remotas, esto se vuelve

muy eficiente ya que el tráfico solo necesita atravesar la red cuando lo solicitan los espectadores remotos. El tráfico de la sucursal permanece localizado y no tiene que atravesar conexiones de área amplia a menos que sea solicitado por otros usuarios.

En la Figura16 se muestra que protocolo usaría las cámaras de Video y que protocolo usaría los clientes.

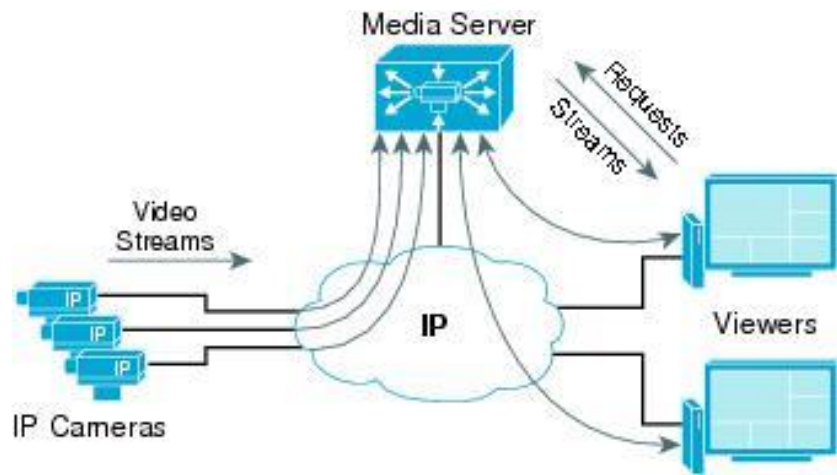


Figura 19
Fuente: CISCO Networking

En la topología propuesta por CISCO el servidor de medios de videovigilancia es el componente central de la solución, que proporciona la colección y enrutamiento de video desde cámaras IP a espectadores u otros servidores de medios. El sistema es capaz de correr en un único servidor físico o distribuido a través de la red, escalando para manejar miles de cámaras y usuarios

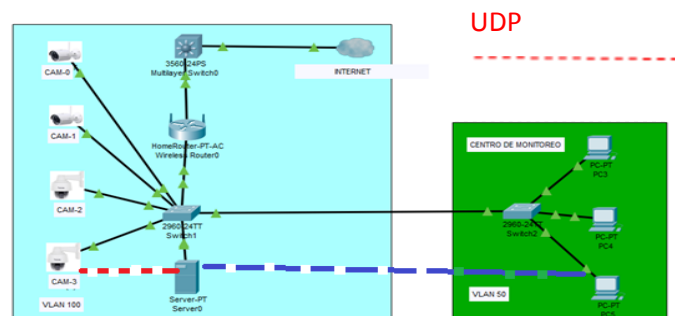


Figura 20 Topología de la red
Fuente: Elaboración Propia

Se aplicó la topología de CISCO Top Down que es la más adecuada para una red host en este caso de cámaras IP, es una topología en la que importa el caudal del ancho de banda que circula por la red

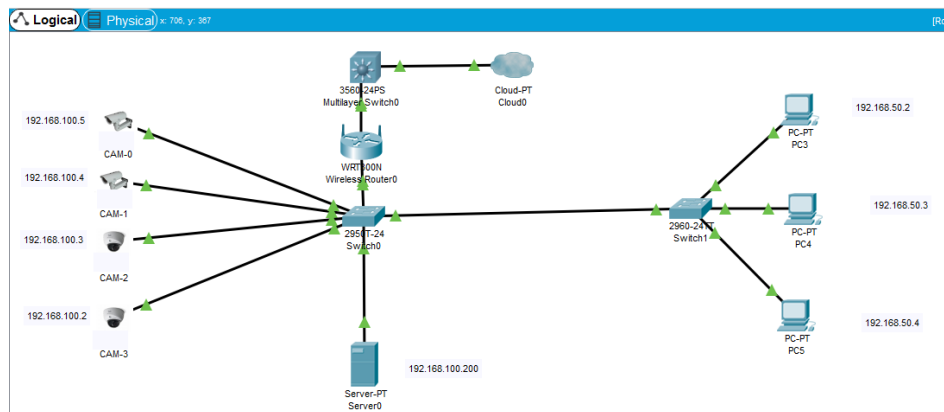


Figura 17: Topología Lógica
Fuente: Elaboración propia

En la topología física se usaron dos redes una para las cámaras y otra red para los observadores (vigilantes de red).

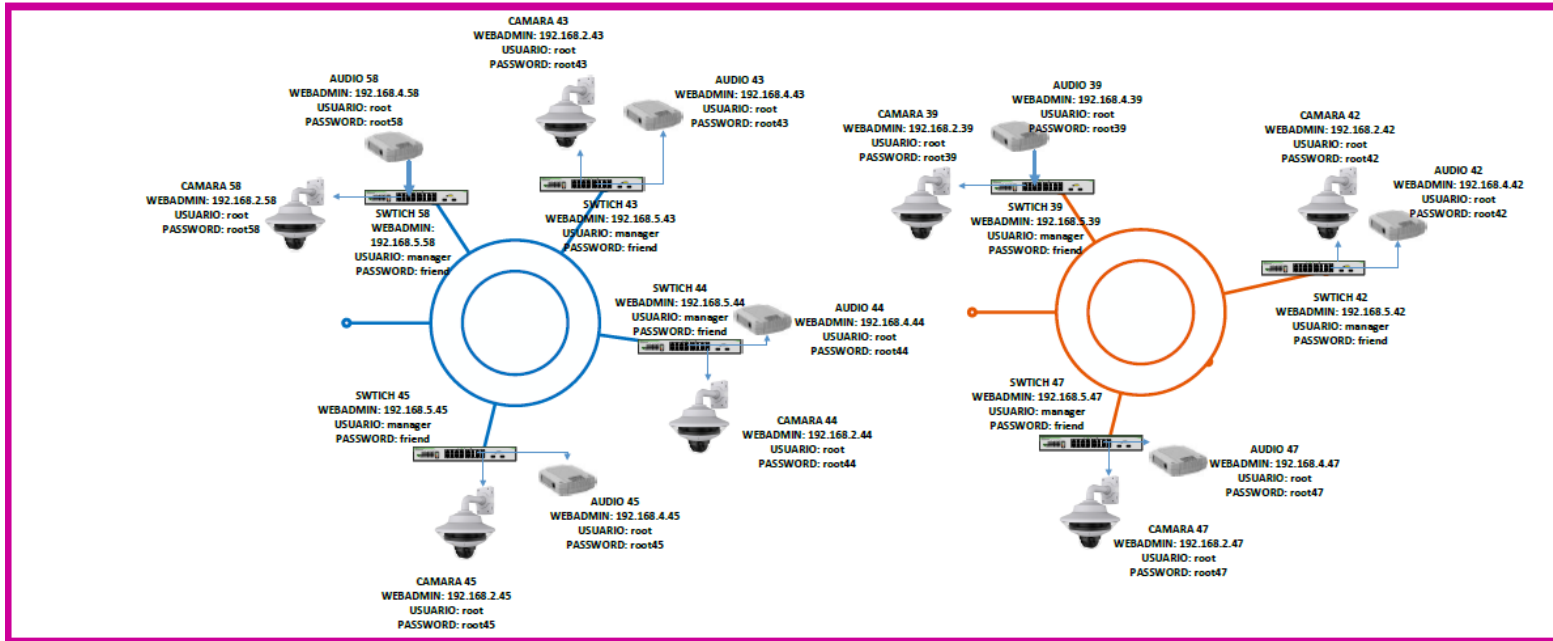


Figura 21: Diseño Físico de la red de la Municipalidad Distrital de Victor Larco Trujillo

Fuente: Municipalidad Distrital de Victor Larco

En la Grafica 21 se estableció la topología Anillo por los distintos puntos que se instalaron las centrales vistos en la figura 18 como Luis Ganoza y Tulipanes, Clinica fatima, Central Vigilancia y Municipalidad, toda la red esta implementada con Fibra Óptica Multimodo

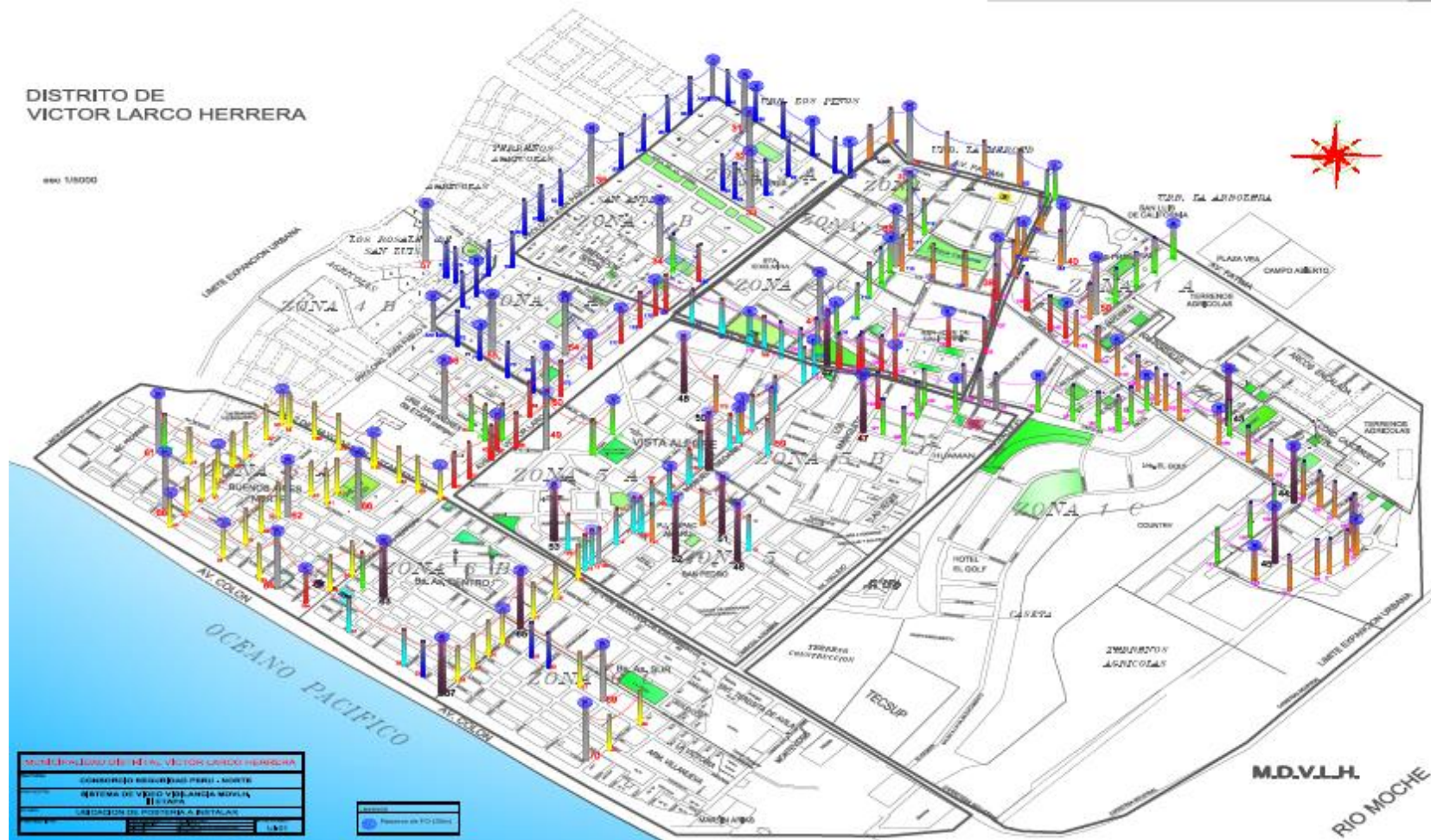


Figura22: Distribución de las cámaras en todo el Distrito de Victor Larco
Fuente: Municipalidad Distrital e Victor Larco

FUNDAMENTOS DE TCP

(Postel, 1981) “TCP es el principal protocolo de transporte en Internet. Es un protocolo orientado a conexión, encargado de proporcionar una comunicación fiable extremo a extremo en una red de paquetes, para lo cual emplea las facilidades que le proporciona la capa de red, habitualmente IP. TCP no asume ningún tipo de fiabilidad en la capa de red, por lo que incluyen mecanismos para proporcionar una transmisión con éxito. El otro gran objetivo de TCP, además de la fiabilidad, es el de realizar un control de flujo, para evitar congestionar la red, y en caso de que haya congestión, ayudar a reducirla.”

(M. Duke, 2006) “La principal referencia de TCP son las distintas RFCs (Request For Comments) que describen el protocolo TCP y los algoritmos que emplea, que se encuentran recopiladas en la RFC 4614”

y la RFC 5783, que describe la historia del control de congestión en las RFCs [179]. Sin embargo, a pesar de que comportamiento de TCP esta especificado en las RFCs, no hay un TCP “estándar”, sino que existen versiones de TCP que emplean los distintos algoritmos para el control de la congestión descritos en las distintas RFCs. Incluso cada sistema operativo tiene su propia implementación de TCP, que escoge los mecanismos de control de flujo, congestión que cree convenientes.

(R. Stevens, 1994) “En esta sección se realiza un recorrido por los fundamentos de TCP necesarios para entender su dinámica, que será clave para entender su comportamiento posteriormente en redes OBS. Para profundizar en los detalles de TCP, además de las RFC, una buena referencia didáctica es el libro de Stevens.”

Control de flujo y congestión

TCP envía la información en partes, denominadas segmentos, que son asentidos por el receptor mediante un mensaje ACK. Cada segmento esta

numerado, para posibilitar su ordenamiento en el destino y detectar posibles pérdidas.

Para realizar la tarea de control de flujo, TCP emplea un mecanismo de ventana deslizante. El tamaño de la ventana de transmisión determina cuantos datos pueden estar en tránsito, cuantos bytes pueden haber sido enviados por el transmisor sin que aún se haya recibido su asentimiento. Cuando se tienen en tránsito tanta cantidad de datos como indica la ventana de transmisión, el emisor deja de enviar nuevos segmentos. Cada vez que se recibe un asentimiento, y si el valor de la ventana de transmisión lo permite, TCP transmite nuevos datos. El valor de la ventana de transmisión se determina por el mínimo de dos límites, uno que esta impuesto por el receptor, e indica el tamaño del buffer de recepción disponible, para evitar saturar el receptor, y otro impuesto por el propio emisor, denominado ventana de congestión, que tiene el objetivo de evitar el envío de mas datos que los que la red soporta (Figura 17).

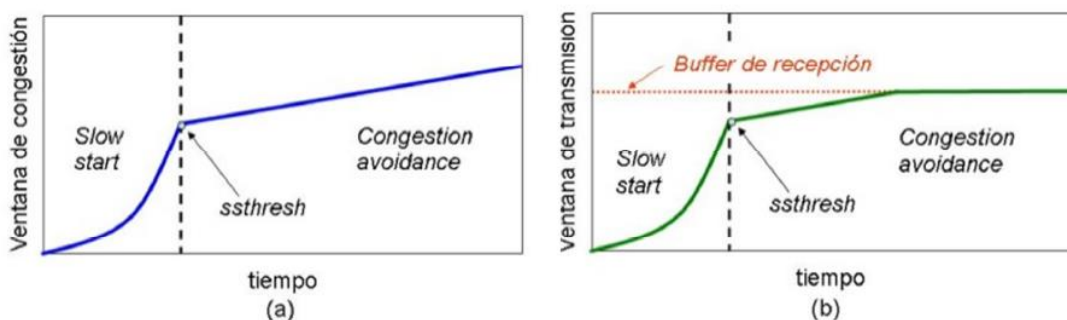


Figura23: (a) Evolución de la ventana de congestión en TCP. (b) Evolución de la ventana de transmisión en TCP.

Fuente: https://es.wikipedia.org/wiki/Protocolo_de_control_de_transmision

TCP tiene varias fases en la transmisión, en las que el valor de la ventana de congestión varía de una manera diferente. TCP inicia la comunicación probando la red, enviando un mensaje, solo segmento, y establece el tamaño de la ventana de congestión (cwnd) en un segmento.

Después de la fase de inicio lento, la ventana aumenta linealmente en la fase denominada evitación de congestión para no saturar la red. En la Figura 16b observe la evolución de la ventana de transmisión, que, como se mencionó, es el mínimo entre la ventana de relieve y el tamaño del búfer



de recepción, Por lo tanto, el valor de la ventana de transmisión proporciona una indicación de la velocidad de transmisión de TCP en todo momento, ya que se transmite en ausencia de errores durante un RTT (Tiempo de viaje de ida y vuelta). Tanto segmentos como especifica la ventana de transferencia. El RTT se define como el tiempo que transcurre se envía un segmento hasta que llega la aprobación que confirma su llegada correcta. Por lo tanto, la relación entre la velocidad de transmisión $X(t)$ expresada en segmentos por segundo y la ventana de transmisión $W(t)$ en términos de segmentos se muestra en (Ecuacion-1).

$$X(t) = \frac{W(t)}{RTT}$$

Ecuación 1

(Jain, 2003.)“De esta forma, el rendimiento máximo de TCP viene dado por la ecuación (2), donde W_{max} es el tamaño máximo que puede alcanzar la ventana de transmisión.”

$$X_{max} = \frac{W_{max}}{RTT}$$

Ecuación 2

Mecanismos De Fiabilidad TCP

(Duke, Branden, Blanton, & Eddy, 2006) “TCP es un protocolo de transporte que garantiza la fiabilidad de la transmisión. Con tal Finalmente, hay una serie de mecanismos para hacer frente a la pérdida de Segmentos A lo largo de la historia del TCP, nuevos métodos de Recuperación de la pérdida de segmentos [178]. En los párrafos siguientes se describirá en Detalle cada uno de los diferentes mecanismos.”



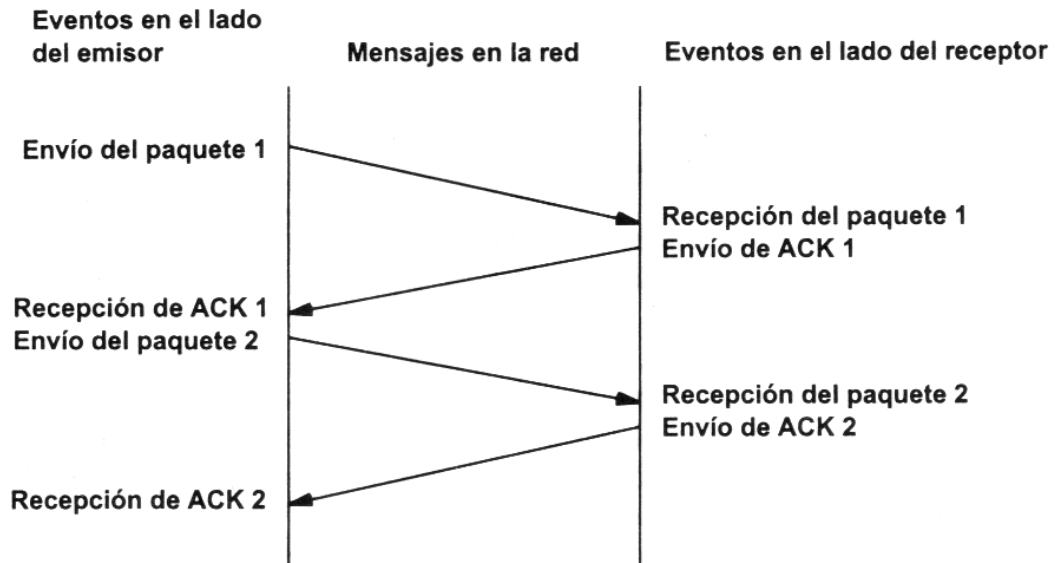


Figura 24: Funcionamiento del Protocolo TCP

Fuente: https://es.wikipedia.org/wiki/Protocolo_de_control_de_transmisión

Administración de las sesiones TCP

Cuando los servicios envían datos utilizando TCP, los segmentos pueden llegar a destinos desordenados. Para que el receptor comprenda el mensaje original, los datos en estos segmentos se reensamblan en el orden original. Para lograr esto, se asignan números de secuencia en el encabezado de cada paquete.

Todos los segmentos que llegan con números de secuencia no contiguos se mantienen para su procesamiento posterior. Luego, se procesan los segmentos cuando llegan con los bytes perdidos.



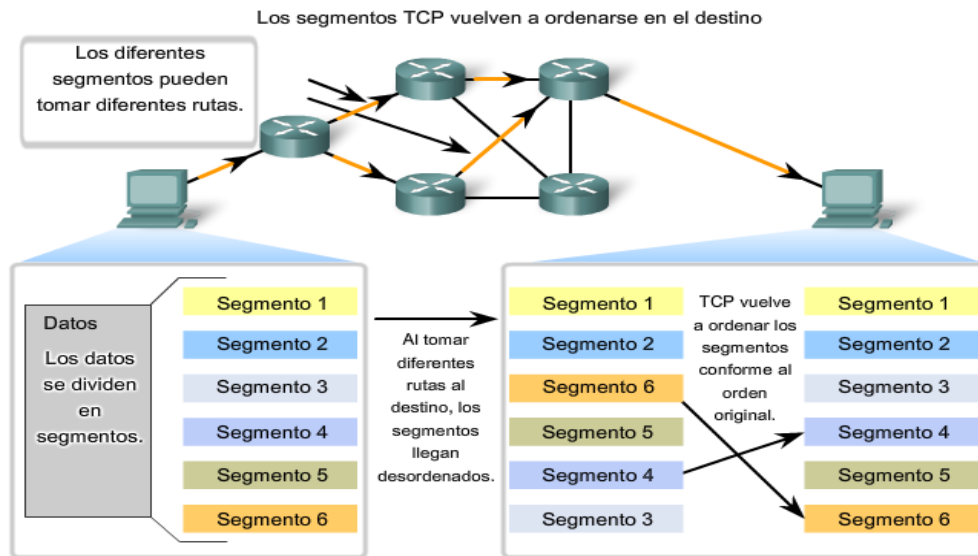


Figura25: Reensamble de Datos
Fuente: CISCO Networking-CCNA1 R&S

FUNDAMENTO UDP

(CISCO, 2018) “UDP (Protocol de Datagrama de Usuario) es un protocolo simple que proporciona las funciones básicas de la capa de transporte. Tiene una sobrecarga mucho menor que TCP porque no está orientada a la conexión y no proporciona mecanismos sofisticados para la retransmisión, la secuenciación y el flujo de control.”

(CISCO, 2018) “Esto no significa que las aplicaciones que usan UDP no siempre son poco confiables. Solo significa que estas funciones no están cubiertas por el protocolo de la capa de transporte y deben implementarse por separado si es necesario.

Aunque la cantidad total de tráfico UDP que se puede encontrar en una red típica es relativamente baja, los protocolos de capa de aplicación más importantes que usan UDP incluyen:”

- Sistema de nombres de dominio (DNS)
- Protocolo simple de administración de red (SNMP, Simple Network Management Protocol)
- Protocolo de configuración dinámica de host (DHCP)
- Protocolo de información de enrutamiento (RIP)

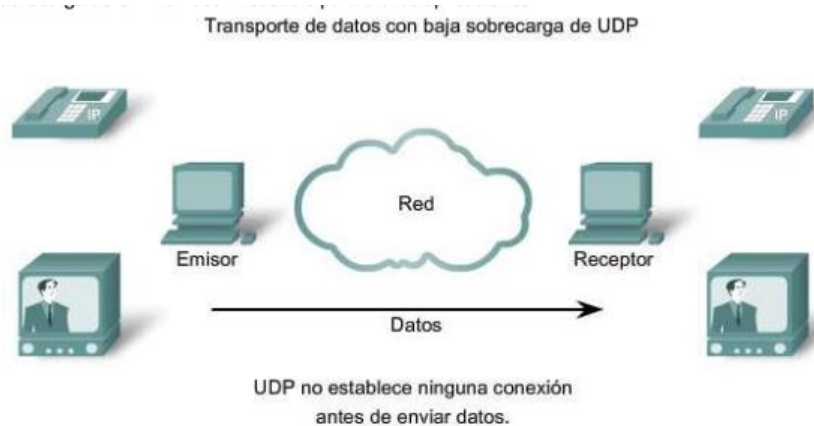


- Protocolo de transferencia de archivos trivial (TFTP)
- Juegos en línea

(CISCO, 2018) “Algunas aplicaciones como juegos en línea o VoIP toleran la pérdida de algunos datos. Cuando estas aplicaciones utilizan TCP, experimentan largos retrasos porque TCP detecta y retransmite la pérdida de datos. Estos retrasos serían más perjudiciales para la aplicación que las pequeñas pérdidas de datos.”

(CISCO, 2018) “Algunas aplicaciones, por ejemplo. DNS, simplemente vuelva a intentar la solicitud si no reciben una respuesta y, por lo tanto, no requieren TCP para garantizar la entrega del mensaje.

La baja sobrecarga del UDP hace que sea deseable para estas aplicaciones.”



UDP suministra transporte de datos con baja sobrecarga debido a que posee un encabezado de datagrama pequeño sin tráfico de administración de red.

Figura26: Protocolo UDP

Fuente: **Fuente: CISCO Networking-CCNA1 R&S**

Las principales características técnicas del protocolo UDP son:

- Es un protocolo mínimo de nivel de transporte orientado a mensajes (*datagramas*) documentado en el RFC 768 de la IETF.
- Proporciona una sencilla interfaz entre la capa de red y la capa de aplicación.



- No otorga garantías para la entrega de sus mensajes.
- Se utiliza, por ejemplo, cuando se necesita transmitir voz o vídeo y resulta más importante transmitir con velocidad que garantizar el hecho de que lleguen absolutamente todos los bytes.

La cabecera del protocolo UDP se muestra a continuación:

| + | Bits 0 - 15 | 16 - 31 |
|----|----------------------|----------------------|
| 0 | Puerto origen | Puerto destino |
| 32 | Longitud del Mensaje | Suma de verificación |
| 64 | Datos | |

Figura27: Cabecera de Protocolo UDP

Fuente: <http://personales.upv.es/rmartin/tcpip/cap02s11.html>

Reensamblaje De Datagrama De UDP

Debido a que UDP funciona sin conexión, las sesiones no se establecen antes de la comunicación, como es el caso de TCP. Se dice que UDP está basado en transacciones. En otras palabras, si una aplicación tiene datos para enviar, simplemente los envía.

Muchas aplicaciones que utilizan UDP envían pequeñas cantidades de datos que pueden ocupar un segmento. Sin embargo, algunas aplicaciones envían grandes cantidades de datos que deben dividirse en varios segmentos. La PDU de UDP se conoce como datagrama, aunque los términos segmento y datagrama a veces se usan indistintamente para describir una PDU de la capa de transporte.

Cuando se envían múltiples datagramas a un destino, pueden tomar diferentes rutas y llegar en el orden incorrecto. UDP no rastrea los números de secuencia como TCP lo hace. UDP no puede reordenar los datagramas en el orden de transmisión. Mira la foto



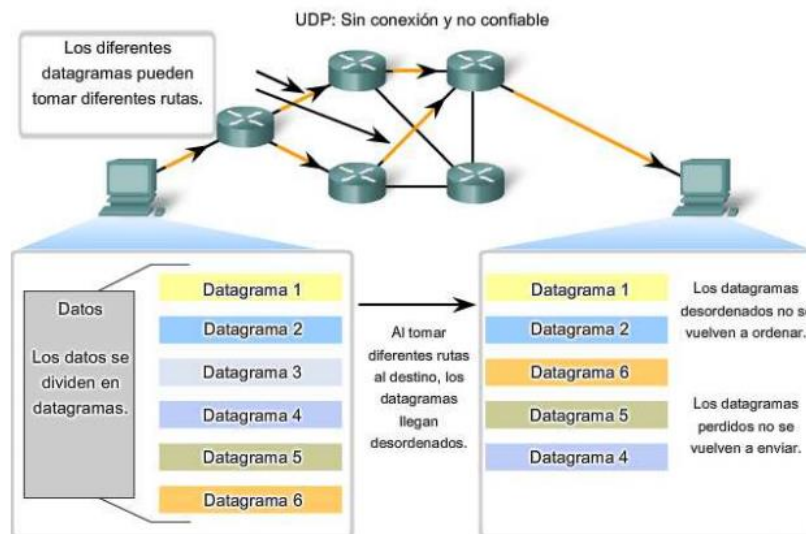


Figura28: Reensamble de Datos
Fuente: Fuente: CISCO Networking-CCNA1 R&S

Procesos y requerimientos del servidor UDP.

Al igual que en las aplicaciones basadas en TCP, a los números de puerto conocidos o registrados se les asignan aplicaciones de servidor basadas en UDP. Cuando estas aplicaciones o procesos se ejecutan, aceptan los datos que corresponden al número de puerto asignado. Cuando UDP recibe un datagrama destinado a uno de estos puertos, envía los datos de la aplicación a la aplicación correspondiente en función de su número de puerto.

1.10. Estudio de Viabilidad del Proyecto

1.10.1. Costos de Implementación para la Analizar Protocolos de Comunicación

Para el cálculo del costo de la implementación para el análisis de Protocolos de Comunicación de un Sistema de Videovigilancia, se tomó en cuenta los paquetes adicionales que deben adquirirse para el proyecto de estudio, a continuación se detalla lo que se requieren con respecto a materiales de oficina, hardware y software para el presente proyecto.



| | INVERSION |
|--|-------------------|
| Materiales de oficina (Papel Bond A4, Lapicero, etc) | S/. 12.00 |
| Recarga de tinta negra | S/. 10.00 |
| MATERIALES E INSUMOS | S/. 22.00 |
| Duo Movistar (Internet 8M + Telefonía fija) | |
| USB | S/. 107.00 |
| SERVICIOS TECNOLOGICOS | S/. 107.00 |
| Pasajes | S/. 80.00 |
| llamadas, viáticos | S/. 70.00 |
| PASAJES Y VIATICOS | S/. 150.00 |
| Servidor Dell PowerEdge 2950 Server 1.5 TB disco duro 16 GB RAM | S/. 9,586.00 |
| Cámara Cloud inalámbrica TrendNet TV-IP751WC | S/. 199.00 |
| Conector RJ45 Cat 6 (4 Unidades) | S/. 4.00 |
| Cable UTP Cat. 6e AMP (6 Mts.) | S/. 10.00 |
| Ponchos de conectores RJ45 | S/. 20.00 |
| Switch cisco Catalys 2960 24 puertos | S/. 3,640.00 |
| Televisor Smart 42 " Samsung | S/. 1,500.00 |
| Rack para televisor | S/. 120.00 |
| | S/. |
| HARDWARE DE IMPLEMENTACION | 15,079.00 |
| Soporte Técnico (Colaboradores) | S/.0.00 |
| Jefe de proyecto | S/. 0.00 |
| HONORARIOS | S/. 0.00 |
| Impresora HP F2180 | S/. 225.00 |
| Silla | S/. 35.00 |
| Escritorio | S/. 150.00 |



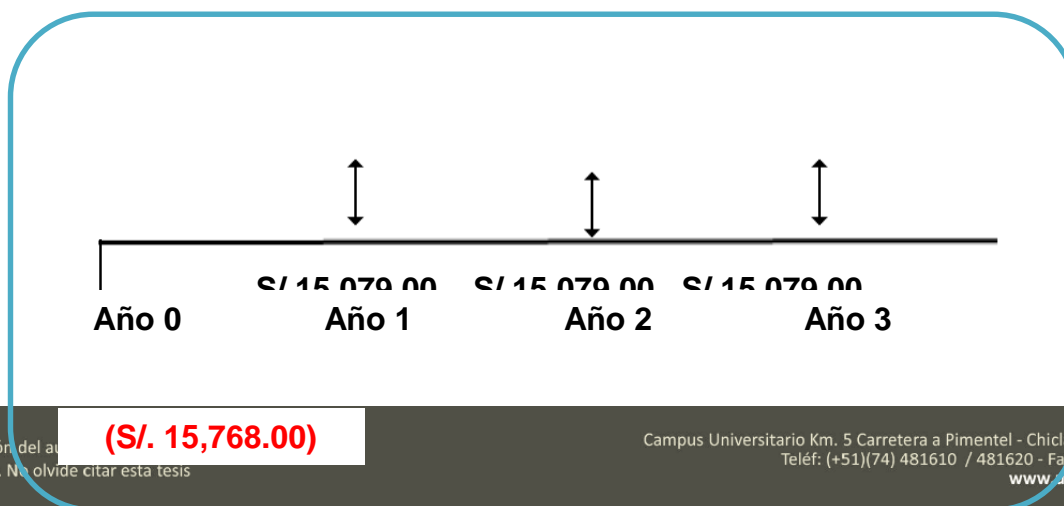
| | |
|-------------------------|----------------------|
| EQUIPOS Y BIENES | S/. 410.00 |
| TOTAL | S/. 15,768.00 |

Tabla 4: Costo de Inversión del Proyecto de Simulación
Fuente: *Elaboración propia*

1.10.2. Flujo de caja proyectada

| AÑO | | AÑO 0 | AÑO 1 | AÑO 2 | AÑO 3 |
|-----------------------------|-------------------------------------|-----------------|---------------|---------------|---------------|
| | Materiales e insumos | S/. 22.00 | S/. 0.00 | S/. 0.00 | S/. 0.00 |
| | Servicios tecnológicos | S/. 107.00 | S/. 107.00 | S/. 107.00 | S/. 107.00 |
| | Pasajes y viáticos | S/. 150.00 | S/. 0.00 | S/. 0.00 | S/. 0.00 |
| | Hardware de implementación | S/. 15,079.00 | S/. 0.00 | S/. 0.00 | S/. 0.00 |
| | Honorarios | S/. 0.00 | S/. 0.00 | S/. 0.00 | S/. 0.00 |
| | Equipos y bienes | S/. 410.00 | S/. 0.00 | S/. 0.00 | S/. 0.00 |
| COSTO OPERACION | | S/. 15,768.00 | S/. 107.00 | S/. 107.00 | S/. 107.00 |
| | Número de clientes | 0 | 1 | 1 | 1 |
| | Costo de Implementación del sistema | S/. 15,079.00 | S/. 15,079.00 | S/. 15,079.00 | S/. 15,079.00 |
| TOTAL BENEFICIOS | | S/. 0.00 | S/. 15,079.00 | S/. 15,079.00 | S/. 15,079.00 |
| Flujo Anual de Caja: | | S/. - 15,768.00 | S/. 14,972.00 | S/. 14,972.00 | S/. 14,972.00 |

Tabla 5: Flujo e caja
Fuente: *Elaboración propia*



-S/. 107.00 -S/. 107.00 -S/. 107.00

Figura29: Diagrama de Tiempo
Fuente: Elaboración Propia

1.10.3. Análisis de rentabilidad

Los criterios de rentabilidad que se utilizarán para demostrar que el los protocolos seleccionados son factibles en cualquier proyectos de instalación de un sistema de videovigilancia por lo tanto es factible económicamente son:

- Valor Actual Neto (VAN).
- Relación Beneficio – Costo (B/C).
- Tasa Interna de Retorno (TIR).

Se realizarán los cálculos utilizando una tasa activa en moneda nacional de 18%.

1.10.3.1. Valor Actual Neto (VAN)

El Valor Actual Neto de la alternativa propuesta está dado por la diferencia del Valor Presente de los Beneficios (VPb) y el Valor Presente de los Costos (VPc), durante el Horizonte de evaluación.

Si el VAN resulta negativo, no conviene ya que significa que el valor actual de los costos supera a los beneficios, o también que el Capital invertido no rinde beneficios suficientes para hacer frente a los costos. Si el VAN es positivo conviene realizar el proyecto. Si es cero o cercano a cero es indiferente invertir o no en el proyecto.

El VAN refleja el Valor Total Actualizado de los beneficios o pérdidas netas que el proyecto es capaz de generar; o lo que es lo mismo, el valor total de los beneficios netos que se dejaría de obtener en caso de no realizarse el proyecto.

Los cálculos son los siguientes:



$$VAN = -I_0 + \sum_{t=1}^n \frac{BN}{(1+r)^t}$$

Dónde:

- **n:** Vida útil del proyecto = 3 años
- **Io:** Inversión del proyecto = 15,768.00
- **BN:** Beneficio Neto = 15,079.00
- **r:** Tasa Anual de Interés de 11% según Banco de Crédito del Perú. (13 de Julio del 2018)

Reemplazando, tenemos:

$$VAN = -15,768.00 + \sum_{t=1}^3 \frac{15,079.00}{(1+0.11)^t} + \frac{15,079.00}{(1+0.11)^2} + \frac{15,079.00}{(1+0.11)^3}$$

$$VAN = -15,768.00 + 13,584.68 + 12,238.45 + 11,025.63$$

$$VAN = 21,080.77$$

$$VAN > 0$$

Interpretación: Se logrará un beneficio a mediano plazo de S/.21,080.77 sobre la inversión.

a. Costo de Beneficio – Costo

Es un indicador que permite establecer si se debe o no realizar la inversión, viendo que la razón sea mayor a la unidad, entonces los beneficios son mayores que los costos. Resultando de dividir la sumatoria de los beneficios actualizados entre la sumatoria de los costos actualizados que son generados en la vida útil del proyecto.

Los cálculos son los siguientes:

$$\frac{B}{C} = \frac{VAB}{VAC}$$

Dónde:

- **VAB:** Valor Actual Beneficio



- **VAC:** Valor Actual Costo

▪ **Hallar Valor Actual Beneficio:**

$$VAB = \sum_{t=1}^n \frac{B}{(1+r)^t}$$

$$B = 15,079.00$$

$$VAB = \sum_{t=1}^n \frac{15,079.00}{(1+0.11)^1} + \frac{15,079.00}{(1+0.11)^2} + \frac{15,079.00}{(1+0.11)^3}$$

$$VAB = 13,584.68 + 12,238.45 + 11,025.63$$

$$VAB = 36,848.77$$

▪ **Hallar Valor Actual Costo:**

$$VAC = I_0 + \sum_{t=1}^n \frac{C}{(1+r)^t}$$

$$C = 107.00$$

$$VAC = 15,768.00 + \sum_{t=1}^n \frac{107.00}{(1+0.11)^1} + \frac{107.00}{(1+0.11)^2} + \frac{107.00}{(1+0.11)^3}$$

$$VAC = 15,768.00 + 96.4 + 86.84 + 78.24$$

$$VAC = 16,029.43$$

▪ **Hallamos el B/c (Beneficio/Costo)**

$$\frac{B}{C} = \frac{VAB}{VAC}$$

Reemplazando:



$$\frac{B}{C} = \frac{36,848.77}{16,029.43} = 2.3$$

Interpretación: Por cada sol que se invierte obtendremos de ganancia 2.3 soles

b. Calculo de la Tasa Interna de Retorno (TIR)

Representa la tasa de rendimiento a la cual el proyecto se hace indiferente, cuando el VAN igual a cero. Es la tasa de descuento que iguala el valor actual de los beneficios y el valor actual de los costos.

$$0 = -I_0 + \sum_{t=1}^n \frac{BN}{(1 + TIR)^t}$$

TIR = 11%, Donde TIR > 11%; El 11% es la tasa de interés a plazo fijo dado por el Banco de Crédito del Perú.

Calculo en Excel TIR = (valores;[estimar])

| AÑO | INVERSION |
|------------|----------------|
| 0 | -S/. 15,768.00 |
| 1 | S/. 15,079.00 |
| 2 | S/. 15,079.00 |
| 3 | S/. 15,079.00 |
| TIR | 78.94 % |

Tabla 6: Calculo del TIR

Fuente: Elaboración propia

c. Tiempo de Recuperación de la Inversión (ROI)

$$ROI = \frac{Inversión}{Beneficios}$$



$$ROI = \frac{15,768.00}{15,079.00}$$

$$ROI = 1.05$$

Interpretación: Este indicador nos dice que la inversión se recuperará en 1.05 años, lo que equivale a 1 año.

CAPÍTULO II: MATERIALES Y METODOS

II. MATERIALES Y METODOS

2.1. Tipo de Investigación

2.1.1. Según su Propósito

Investigación tecnológica – Aplicada

El estudio de comparación de dos protocolos, permitió observar el comportamientos en envío de paquetes y así elegir el adecuado para que los futuros investigadores no solo se limiten a escoger los equipos de red (cámaras de videovigilancia)J, sino también analizar el comportamiento de los protocolos que pueden soportar, los sistemas operativos donde se trabajaran

2.1.2. Según el diseño de investigación

Cuasi experimental, porque está orientado a la evaluación del impacto del tratamiento, existe una hipótesis para contrastar, existe una respuesta, no existe una asignación aleatoria de áreas.

2.2. Material de Estudio – Población y Muestra

2.2.1. Población

Está determinada por 10 protocolos. Que se encuentran en la tabla N° 025 en el anexo 01.

2.2.2. Muestra

La muestra fue determinada por conveniencia, y están conformados por dos protocolos de comunicación de redes: TCP y UDP. Que se seleccionó de acuerdo al top 10 que se encuentra en el anexo 01

2.2.3. Diseño de Contrastación

Para la contrastación de la hipótesis se utilizará el Método de comparación ya que solo hemos utilizados dos componentes como son los dos protocolos UDP y TCP



Operacionalización.

| Variable | Indicadores | Formula | Método, técnicas e instrumentos para recolección de datos. |
|---|---|---|--|
| Independiente: Protocolos de comunicación de redes. | Tipo de Licencia. Costo: Libre | $Precio = Cantidad \times Unidad$ | Análisis documental. Descripción bibliográfica, catalogación |
| Dependiente: Prestaciones de rendimiento en la transmisión de datos en un sistema de videovigilancia. | % de paquetes entregados. % de paquetes perdidos. Retraso de extremo a extremo Promedio Jitter | Rendimiento de paquetes: $Rendimiento = \frac{Cant. Paquetes Recibidos}{UltiPaqEnviado - PrimPaqEnvi.}$ Paquetes Perdidos: $PaqPerdidos = \sum PaqEnviado - \sum PaqRecibidos$ Retraso de Extremo a Extremo | Técnica de Observación: Monitorear le envió y recepción de paquetes. Monitorear Las pérdidas de paquetes Instrumentos: Fichas de observación. Lista de variables a medir (paquetes, Velocidad) |

| | | | |
|--|--|--|--|
| | | <p><i>Retraso de Extremo a Extremo</i></p> $= T_r - T_s$ <p>Promedio Jitter</p> $Prom_Jitter = \frac{Retardo_j - Retardo_i}{N}$ | |
|--|--|--|--|

Tabla 7: Operacionalización de Variable



2.3. Métodos, Técnicas e Instrumentos

(Lourdes Münch Galindo, 1990) “La Administración es el proceso cuyo objeto es la coordinación eficaz y eficiente de los recursos de un grupo social para lograr sus objetivos con la máxima productividad.”

2.3.1. Métodos de Investigación

Se procederá a recoger información referente a los análisis de los protocolos elegidos para un sistema de videovigilancia, ya sea interno o externo, incidencias antes de implementar el protocolo UDP y después de implementar el protocolo UDP, a través de pruebas con cada uno de los protocolos en diferentes tiempos y circunstancias.

Para esto se realizará lo siguiente:

Software de testeo que a partir del problema observado se analizarán los diferentes test con programas como cports, iperf, livetcpudpwatch, wireshark y GNS-3

Luego, se validarán las pruebas elaboradas por parte de un especialista en redes, para obtener su apreciación y aprobación de estas.

Una vez aprobadas los análisis, estas serán debidamente llenadas

2.3.2. Técnicas e Instrumentos de Recolección

a) Técnicas

- Observación Científica: Directa, Participante

b) Instrumentos

- Guía de Observación
- Cuestionario
- Cuaderno de Nota

2.4. Procedimientos para la Recolección de Datos

Se procederá a recoger información referente a los protocolos estudiados de diferentes autores recogidos de estudios científicos

2.4.1. Plan de análisis estadístico de datos

Esta fase se constituyó como principal y primordial para dar respuesta a las expectativas existentes en torno a la elección del protocolo apropiado en un sistema de videovigilancia. El siguiente proceso de análisis partió de un diagnóstico que permitiese determinar la necesidad o no, de usar protocolo UDP en un sistemas de videovigilancia IP. Por tal motivo se monitoreo los diferentes resultados de las pruebas hechas a los protocolos UDP y TCP. Los instrumentos aplicados a la población arrojó los siguientes resultados:

2.4.1.1. Números de pérdidas de paquetes

Las pérdidas de paquetes ocurridas durante una transmisión de videovigilancia

2.5. Criterios de Rigor Científico.-

Confiabilidad

Hipótesis H_0 : Número de latencia registrada en el protocolo UDP en comparación a los protocolos TCP es menor o igual al protocolo TCP que viene por defecto en las cámaras de videovigilancia propuesto.

$$H_0: V_a - V_p \geq 0$$

Hipótesis H_a : Número de latencia con el protocolo UDP propuesto es mayor o igual que el Número de latencia con el protocolo TCP.

$$H_a: V_a - V_p < 0$$

Validación



Los resultados serán corroborados por expertos como son los Instructores CISCO

Contrastación

La contrastación de hipótesis se realizó con el método propuesto PreTest - PostTest, que nos permite aceptar o rechazar la hipótesis. Para esto se realizó una prueba por cada indicador relacionado con el número de incidencias ocurridas en el área de laboratorios, para lo cual se emplearan las siguientes formulas:

2.6. Selección del Protocolo

En la siguiente Matriz se reconoce las respuestas del análisis de los dos protocolos estudiados (Ver Anexo 2)

| Crterios Protocolo | C1 | C2 | C3 | C4 | $\sum_{j=1}^n$ | Prioridad |
|--------------------|------|------|------|------|----------------|-----------|
| UDP | 2.67 | 3.00 | 3.33 | 3.33 | 3.08 | 1º |
| TCP | 4 | 2 | 2 | 3 | 2.75 | 2º |

Tabla 8: Matriz de Selección de Protocolo

El método de selección de la metodología es la siguiente:

Tabla 11: Criterios de la Encuesta.

C1=Rendimiento

C2=Paquetes perdidos

C3= Retraso promedio de extremo a extremo

C4=Promedio Jitter

| CRITERIO | |
|------------------|---------|
| NIVEL DE IMPACTO | PUNTAJE |
| 1.- Muy bajo | 1 |
| 2.- Bajo | 2 |
| 3.- Normal | 3 |
| 4.- Alto | 4 |

Tabla 9: Criterios de la encuesta

Fuente: Elaboración Propia



CAPÍTULO III: RESULTADOS

III. ANALISIS DE RESULTADOS

3.1 PROPUESTA DE INVESTIGACION

El desarrollo de la propuesta, se hará siguiendo las siguientes conclusiones: (Balan HV, 2007) “En la implementación del protocolo UDP en un sistema de videovigilancia IP, dos protocolos de capa de transporte son los más recomendados y ampliamente estudiados, son UDP y TCP. Aunque el despliegue de videovigilancia es rápido, hay una falta de evaluación del rendimiento de sus protocolos.”

(Balan HV, 2007) “Por lo tanto, se requiere un análisis exhaustivo para evaluar el rendimiento de los diferentes protocolos de alta aplicaciones de usuario final como aplicaciones multimedia. El comportamiento problemático de los dos protocolos en multimedia, las aplicaciones implican resaltar los pros y los contras de su desempeño.”

En este estudio, el escenario de simulación de protocolos de capa de transporte TCP, y UDP en términos de video la transmisión en el entorno de videovigilancia se verifica mediante el simulador GNS-3 y analiza el rendimiento de estos protocolos en términos de fluctuación, rendimiento, retardo y pérdida de paquetes para resaltar los impactos de variedad de los comportamientos de los protocolos de la capa de transporte para la transmisión de videovigilancia.

3.2 Evaluación de desempeño de simulación

En este estudio, GNS-3 se utiliza para la implementación de los escenarios y la evaluación de los protocolos de transporte, TCP y UDP para transmitir un flujo de video en el entorno de videovigilancia.

3.2.1 Parámetros de Simulación:

La Tabla muestra el resumen de los parámetros del modelo que se utiliza para el experimento de simulación.



| Parámetros | Descripción |
|------------------------------|--------------------------|
| Escenario de Simulación | GNS3 |
| Protocolos | TCP, UDP |
| Numero de Nodos | 10, 20 nodos |
| Numero de paquetes | 1024 bytes |
| Canal de conexión | Punto a punto |
| Tipo de dispositivo de red | Evaluación a largo plazo |
| Intervalo | 100 ms |
| Velocidad de datos del canal | 20 Mbps |
| Tiempo de Simulación | 30 seg |

Tabla 10: Parámetros de valores

3.2.2 Métricas de Evaluación:

(Wisam AK, 2015) Las medidas de evaluación de rendimiento utilizadas son:

Rendimiento: se define como la cantidad de entrega efectiva de paquetes en un canal de comunicación.

$$\text{Rendimiento: } \frac{\text{Cantidad de Paquetes Recibidos}}{\text{Ultimo Paquete Enviado} - \text{Primer Paquete Enviado}}$$

Número de pérdida de paquetes: se define como la diferencia del número total de paquetes enviados por el remitente y el número total de paquetes recibidos en el receptor.



$$Paquetes_Perdidos = \sum Paquetes_Enviados - \sum Paquetes_Recibidos$$

Retraso de extremo a extremo: Se define como el intervalo que experimentan los paquetes cuando viajan a través de varias redes de un nodo a otro.

$$Retraso_{Extremo a Extremo} = T_r - T_s$$

T_R está transmitiendo el tiempo del paquete específico, mientras que T_S es el tiempo de recepción del paquete.

Promedio Jitter: se define como la diferencia de latencia de paquete a paquete.

$$Pomedio_{Jitter} = \frac{Retardo_j - Retardo_i}{N}$$

Retardo j es el retraso del paquete actual, Retardo i es el retraso del paquete anterior, y N representa el número total de paquetes recibido durante el tiempo de simulación.

3.3 Resultados y Análisis de Clasificación Experimental

El número máximo de nodos como 10 y 20 se usa para examinar el efecto de diferentes nodos de red con un tamaño de paquete de 1,000 bytes. La figura 1a muestra la cantidad de nodos impactados para el UDP y TCP con respecto a las diferentes métricas de rendimiento.

El rendimiento en la red se refiere a la entrega exitosa de paquetes a través de un canal de comunicación. Fig. 26 (a) demuestra que el protocolo UDP tiene un valor de rendimiento razonable en el entorno de la red LTE que tiene 10 nodos de red. El escenario aquí se supone que a los 10 nodos se les enviarán los archivos de video MPEG-4 al mismo intervalo de tiempo al



nodo de la estación base. Por otra parte, la continuidad del protocolo UDP en su buen rendimiento en el entorno de la red se muestra cuando la cantidad de nodos se aumenta de 10 a 20 nodos. El resultado confirma la estabilidad de este protocolo incluso con un número creciente de transmisión de archivos de video, mientras que el aumento en una cantidad de nodos puede cambiar el efecto del protocolo.

Además, a medida que aumentan los nodos, mejora el rendimiento de la red completa. El crecimiento constante del gráfico que muestra que la red es capaz de manejar esta densidad de nodos. Para lograr el más alto rendimiento, no hay ningún cuello de botella hasta este límite de números de nodo. A medida que aumenta el número de nodos, el rendimiento crece demasiado alto. El protocolo UDP tiene un buen rendimiento que TCP debido a sus dos esquemas utilizados en ella. Estos esquemas son el control de la congestión y el control de flujo.

En el caso de paquetes con éxito incompleto en transmisión y recepción, la pérdida de paquetes ocurre al final y el video la transmisión se vuelve intermitente. Significa que la velocidad de descarga y carga puede disminuir demasiado y la pausa en la transmisión de video puede suceder. Además, se puede lograr una voz o video de mala calidad. Además, la pérdida de paquetes ocurre en el entorno de red inalámbrica más que el entorno de red de cable porque comparte el medio entre todos los nodos de red. El resultado se presenta en la figura 27 (b) donde el protocolo TCP logró el mejor resultado y el protocolo UDP fue encontrado como el peor.

Este resultado es para 10 nodos, que transmiten archivos de video al servidor al mismo tiempo. No hay tal diferencia si la cantidad de nodos aumenta de 10 a 20, respectivamente. También se muestra que el número de pérdida de paquetes aumenta cuando los nodos también aumentan. Esto sucedió porque la estación base se convirtió en el cuello de botella que se vio afectado por la densidad de los nodos en la topología de red ya que



todos los nodos enviaron paquetes al mismo tiempo a una sola estación base.

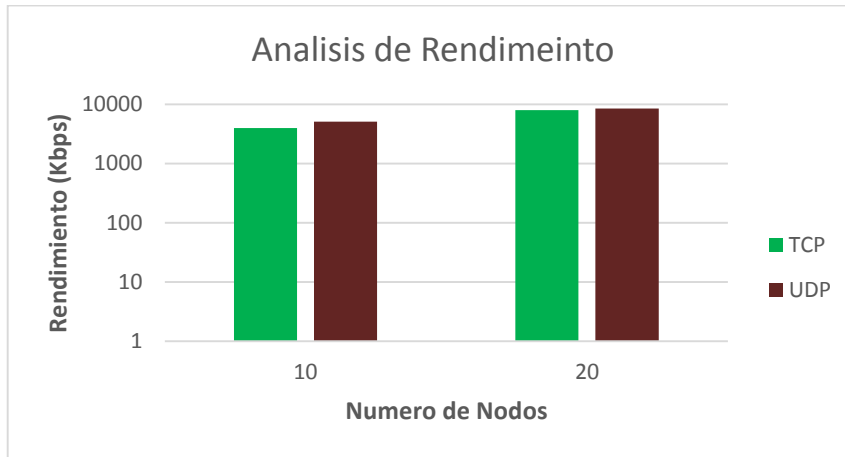


Figura30: Análisis de Rendimiento (a)
Fuente: Elaboración Propia

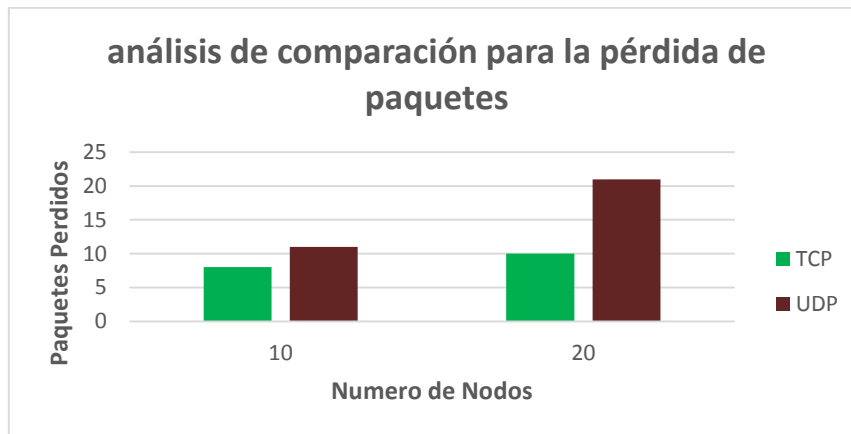


Figura31: Perdida de Paquetes (b)
Fuente: Elaboración Propia



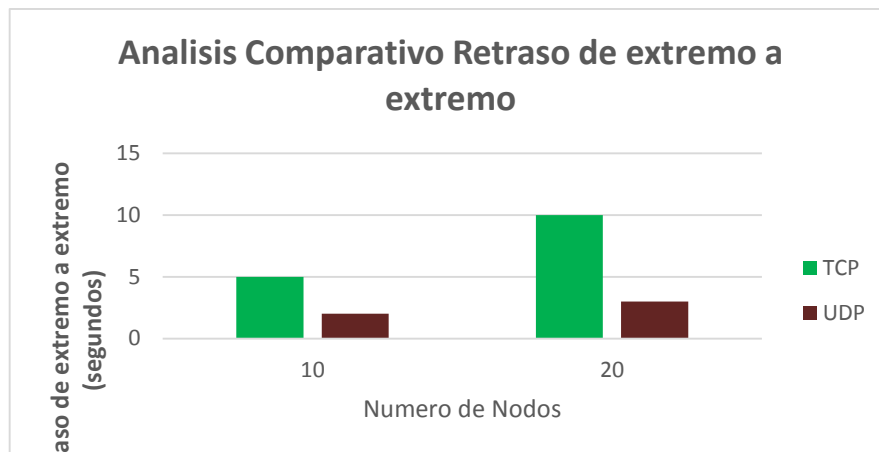


Figura32: Retraso (c)
Fuente: Elaboración Propia

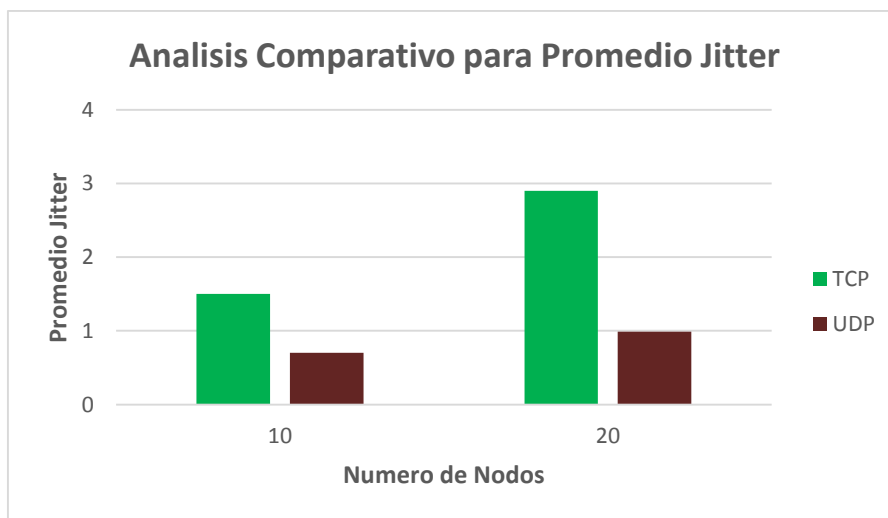


Figura33: Jitter (d)
Fuente: Elaboración Propia

Como se muestra en la Fig. 28 (c), el protocolo UDP tiene el mejor rendimiento en comparación con TCP debido al poco tiempo de retardo en comparación con otros protocolos. El protocolo TCP necesita más tiempo desde el inicio para el establecimiento de la conexión. Además, este establecimiento de conexión puede afectar la cantidad de nodos. Porque cuando se aumenta la cantidad de nodos, también se incrementará el tiempo de retardo. Este aumento se produce más en el entorno inalámbrico



que en el entorno de red cableada porque la capa de enlace de datos en la conexión inalámbrica necesita acuse de recibo (ACK), RTS / CTS y la capa tres (ACK). Del mismo modo, el entorno de redes inalámbricas usa medios compartidos diferentes al entorno de red cableada. El tiempo medio de retraso para UDP y TCP en los cuatro escenarios muestra un retraso consistentemente mayor debido a la menor circulación de datos en la red.

El protocolo TCP experimenta la mayor demora debido al esquema de control de congestión del TCP. La característica de confiabilidad del TCP usa el tiempo para que el costo de la falta de fiabilidad en UDP se mida con respecto al tiempo. Además, el UDP supera a la conexión convencional menos y los protocolos orientados a la conexión en caso de retraso. El análisis comparativo de los protocolos TCP y UDP para el escenario de 10 a 20 nodos muestra que el protocolo UDP realiza el mejor en términos de retraso de la red.

En la Fig.29 (d), el jitter se calculó variando el número de nodos. Dado que la latencia es directamente proporcional al retraso, por lo tanto, en la evaluación de UTP, la latencia aumenta con el aumento en el número de nodos de red. Mientras que UDP muestra menos valores de jitter que reflejen los mejores resultados, hasta cierto punto, en comparación con el otro protocolos. Además, se puede observar que TCP fluctúan menos que los del UDP. La razón detrás de esto es que TCP verifican la condición de la red. En caso de congestión de la red, su tasa de envío de paquetes se minimiza bastante y se supervisa hasta la condición de la red porque es mejor debido a que el jitter es comparativamente más grande que UDP.

CAPÍTULO IV: DISCUSION RESULTADOS

IV. ANALISIS DE RESULTADOS

4.1. PROPUESTA DE INVESTIGACION

El desarrollo de la propuesta, se hará siguiendo las siguientes conclusiones:

(Balan HV, 2007) “En la implementación del protocolo UDP en un sistema de videovigilancia IP, dos protocolos de capa de transporte son los más recomendados y ampliamente estudiados, son UDP y TCP. Aunque el despliegue de videovigilancia es rápido, hay una falta de evaluación del rendimiento de sus protocolos.”

(Balan HV, 2007) “Por lo tanto, se requiere un análisis exhaustivo para evaluar el rendimiento de los diferentes protocolos de alta aplicaciones de usuario final como aplicaciones multimedia. El comportamiento problemático de los dos protocolos en multimedia, las aplicaciones implican resaltar los pros y los contras de su desempeño.”

En este estudio, el escenario de simulación de protocolos de capa de transporte TCP, y UDP en términos de video la transmisión en el entorno de videovigilancia se verifica mediante el simulador GNS-3 y analiza el rendimiento de estos protocolos en términos de fluctuación, rendimiento, retardo y pérdida de paquetes para resaltar los impactos de variedad de los comportamientos de los protocolos de la capa de transporte para la transmisión de videovigilancia.

4.2. EVALUACIÓN DE DESEMPEÑO DE SIMULACIÓN

En este estudio, GNS-3 se utiliza para la implementación de los escenarios y la evaluación de los protocolos de transporte, TCP



y UDP para transmitir un flujo de video en el entorno de videovigilancia.

4.2.1. Parámetros de Simulación:

La Tabla muestra el resumen de los parámetros del modelo que se utiliza para el experimento de simulación.

| Parámetros | Descripción |
|------------------------------|--------------------------|
| Escenario de Simulación | GNS3 |
| Protocolos | TCP, UDP |
| Numero de Nodos | 10, 20 nodos |
| Numero de paquetes | 1024 bytes |
| Canal de conexión | Punto a punto |
| Tipo de dispositivo de red | Evaluación a largo plazo |
| Intervalo | 100 ms |
| Velocidad de datos del canal | 20 Mbps |
| Tiempo de Simulación | 30 seg |

**Tabla 11: Parámetros de valores
Fuente: Elaboración Propia**

4.2.2. Métricas de Evaluación:

(Wisam AK, 2015) Las medidas de evaluación de rendimiento utilizadas son:

Rendimiento: se define como la cantidad de entrega efectiva de paquetes en un canal de comunicación.

$$Rendimiento: \frac{Cantidad\ de\ Paquetes\ Recibidos}{Ultimo\ Paquete\ Enviado - Primer\ Paquete\ Enviado}$$



Número de pérdida de paquetes: se define como la diferencia del número total de paquetes enviados por el remitente y el número total de paquetes recibidos en el receptor.

Paquetes_Perdidos

$$= \sum Paquetes_Enviados - \sum Paquetes_Recibidos$$

Retraso de extremo a extremo: Se define como el intervalo que experimentan los paquetes cuando viajan a través de varias redes de un nodo a otro.

$$Retraso_{Extremo a Extremo} = T_r - T_s$$

T_R está transmitiendo el tiempo del paquete específico, mientras que T_S es el tiempo de recepción del paquete.

Promedio Jitter: se define como la diferencia de latencia de paquete a paquete.

$$Pomedio_{Jitter} = \frac{Retardo_j - Retardo_i}{N}$$

Retardo j es el retraso del paquete actual, Retardo i es el retraso del paquete anterior, y N representa el número total de paquetes recibido durante el tiempo de simulación.

4.2.3. Resultados de simulación

La simulación se hace bajo el escenario del software GNS-3 conforme se especifica en la tabla N° 07.



Se eligió GNS-3 ya que tiene la capacidad de puentear interfaces virtuales a sus dispositivos de laboratorio para una o más interfaces Ethernet físicas en su PC.

Esto nos permite que los proyectos con redes virtuales se conecten en el hardware real, tales como Router, Switches y otras computadoras (ver anexo N° 05)

La Tabla N° 14 registra los retrasos promedio de extremo a extremo para todos los archivos en los diferentes escenarios cuando se utilizan diferentes protocolos de capa de transporte. Estos los resultados también se muestran gráficamente en la Figura N° 29.

La Tabla N° 15 resume el porcentaje de paquetes de datos efectivos recibidos por el controlador en diferentes escenarios con los dos protocolos analizados (UDP – TCP). Los resultados están graficados en la Figura 30.

La Tabla N° 16 muestra números de incidencias de pérdidas consecutivas de paquetes de datos efectivos y el controlador, están graficados en la Figura 31.

La Tabla N° 17 enumera el número máximo de pérdidas de datos consecutivas en cada escenario

| Escenarios | Promedio de Perdidas de Extremo a Extremo (Milisegundos) | |
|------------|--|-----------|
| | UDP | TCP |
| 1 | 10.061991 | 12.291061 |
| 2 | 10.085596 | 16.319366 |
| 3 | 10.055195 | 18.127047 |
| 4 | 10.070746 | 19.050467 |
| 5 | 10.057896 | 20.709423 |
| 6 | 10.06588 | 22.270711 |
| 7 | 10.040047 | 23.382781 |
| 8 | 10.064531 | 23.346436 |
| 9 | 10.081729 | 24.231340 |
| 10 | 10.064618 | 30.518884 |
| 11 | 10.089902 | 37.585497 |

Tabla 12: Retraso promedio de extremo a extremo en caso de que se use un protocolo diferente

Fuente: Elaboración Propia



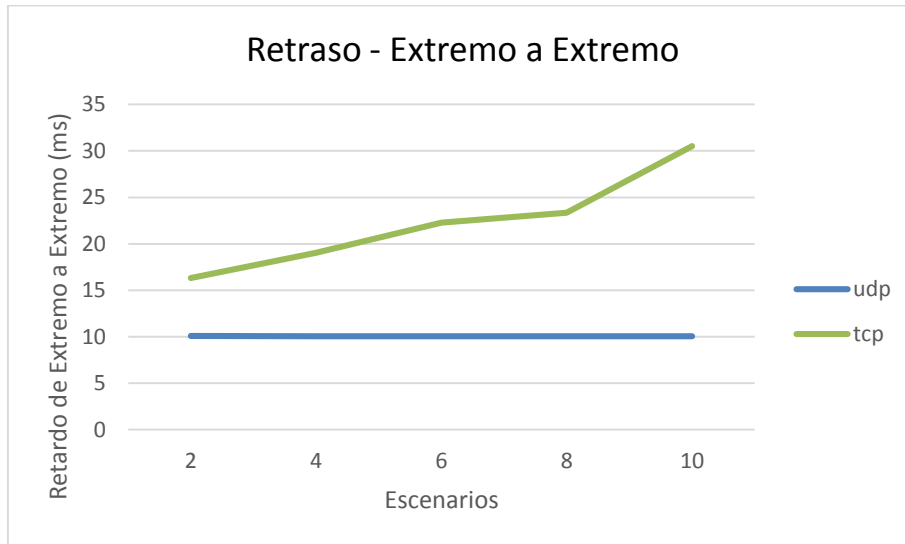


Figura34: Retrasos promedio de extremo a extremo en el Caso Uno con diferentes protocolos

Fuente: Elaboración Propia

| Escenarios | % de Paquetes de Datos Efectivo | |
|------------|---------------------------------|---------|
| | UDP | TCP |
| 1 | 99.867% | 99.8% |
| 2 | 98.933% | 97.933% |
| 3 | 98.133% | 96.933% |
| 4 | 98.533% | 96.677% |
| 5 | 96.933% | 95.333% |
| 6 | 97.133% | 94.6% |
| 7 | 97.2% | 94% |
| 8 | 97.133% | 93.733% |
| 9 | 96.933% | 93.467% |
| 10 | 94.333% | 90.2% |
| 11 | 92.467% | 90.933% |

Tabla 13: Porcentaje de Paquetes de Datos Efectivo con diferentes protocolos

Fuente: Elaboración Propia



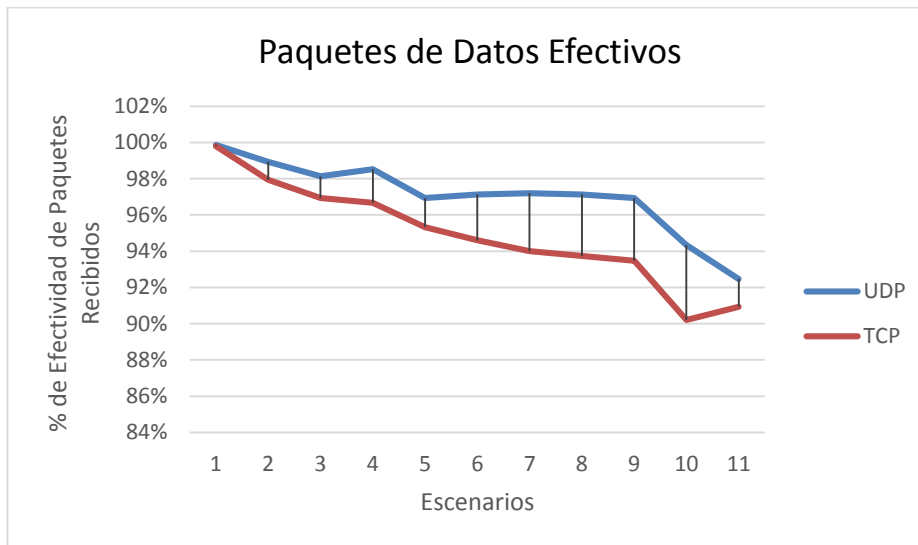


Figura35: Porcentaje de Efectividad de Paquetes Recibidos usando diferentes protocolos
Fuente: Elaboración Propia

4.2.4. Evaluaciones Comparativas

Cuando observamos el retardo promedio de extremo a extremo (Tabla N° 14 e FiguraN° 29), todo está a favor de una conexión UDP, produce el retardo promedio más pequeño que el protocolo, TCP.

| Escenarios | Número de incidencias consecutivas de pérdidas de datos efectivos | |
|------------|---|-----|
| | UDP | TCP |
| 1 | 0 | 0 |
| 2 | 11 | 11 |
| 3 | 15 | 14 |
| 4 | 19 | 18 |
| 5 | 13 | 14 |
| 6 | 15 | 17 |
| 7 | 18 | 20 |



| | | |
|----|----|----|
| 8 | 16 | 17 |
| 9 | 20 | 22 |
| 10 | 36 | 37 |
| 11 | 49 | 46 |

Tabla 14: Pérdidas consecutivas de datos efectivos con diferentes protocolos.

Fuente: Elaboración Propia

Quando se usó UDP, los retrasos promedio bajo esta cantidad de tráfico se limitaron en 10.07 milisegundos, independientemente de la condición del canal.

En cuanto a UTP, los retrasos promedio son solo un poco más largos que los retrasos promedio proporcionados por UDP, con un límite superior de 22.53 milisegundos. También se puede ver en la Figura 20, para UDP o UTP, que los retrasos promedio son casi constantes a medida que la condición de la red empeora. Pequeños y deterministas retrasos son deseables para aplicaciones en tiempo real. De acuerdo con estos resultados de simulación, UDP es adecuado para la comunicación en tiempo real en términos de demora de extremo a extremo.



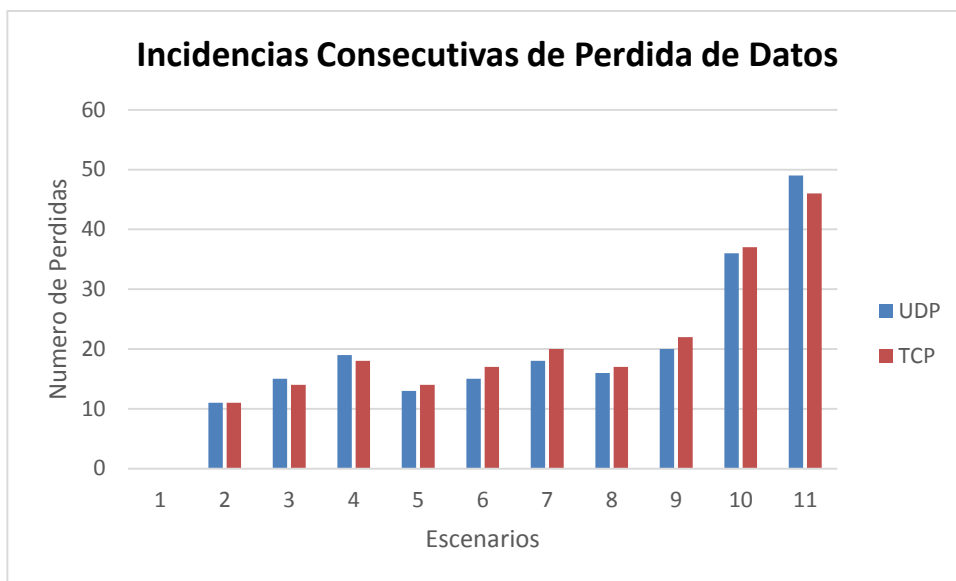


Figura36: Perdidas de Datos Consecutivos usando diferentes protocolos
Fuente: Elaboración Propia

| Escenarios | Máximo número de perdida de datos consecutivos | |
|------------|--|-----|
| | UDP | TCP |
| 1 | 0 | 0 |
| 2 | 3 | 3 |
| 3 | 3 | 3 |
| 4 | 3 | 4 |
| 5 | 3 | 4 |
| 6 | 3 | 3 |
| 7 | 3 | 4 |
| 8 | 3 | 3 |
| 9 | 3 | 3 |
| 10 | 3 | 3 |
| 11 | 4 | 4 |

Tabla 15: Máximo número de perdida de datos consecutivos
Fuente: Elaboración Propia



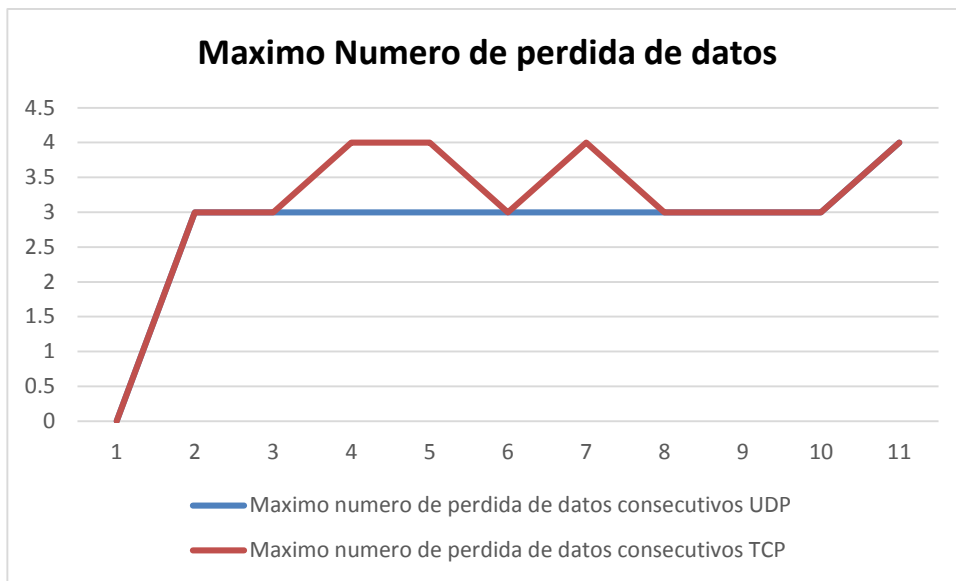


Figura37: Máximo número de pérdidas
Fuente: Elaboración Propia

La razón por la que TCP no puede funcionar bien es debido a su interminable retransmisión esquema. Un paquete será retransmitido hasta que su ACK correspondiente llegue a la remitente. La retransmisión repetida conduce a largos retrasos de extremo a extremo. En el caso de un error de canal, la retransmisión se produce con más frecuencia que en una condición de canal normal.

La diferencia de retardo entre un paquete transferido exitosamente en un paso y un paquete retransmitido varias veces puede ser muy obvio. Por lo tanto, tanto el retardo promedio de punta a punta y la fluctuación de fase para TCP produjeron valores comparativamente grandes. UDP se distingue en términos de su latencia de transmisión. Sin embargo, cuando viene a la fiabilidad de la transmisión, el rendimiento de UDP se degrada. La columna UDP en la Tabla 5.4 muestra que la pérdida de



paquetes comienza a crecer sin límite como condición de la red empeora. CRETP también introduce abandonos debido a su esquema de retransmisión condicional. Los paquetes de datos eliminados contabilizados para CRETP incluyen paquetes que fallaron para llegar al receptor y los paquetes probados como inefectivos. Sin embargo, los números de abandono fueron más pequeños en comparación con los proporcionados por UDP.

UDP proporciona el menor promedio de demora de extremo a extremo en todos los escenarios, mientras que TCP introduce retrasos mayores debido a su algoritmo de retransmisión. Para ambos UDP y TCP, la latencia de transmisión es pequeña y relativamente determinista.

Sin embargo, en términos de fiabilidad de transmisión, UDP no tiene control de errores de transmisión, esto hace que este protocolo sea el peor de los dos protocolos en algunos casos. TCP produce la comunicación más confiable ya que el número de paquetes caídos es menor más de la mitad de los UDP en la mayoría de los escenarios y la ocurrencia de abandono consecutivo también es mucho menos frecuente. La retransmisión condicional de UDP mejora significativamente la comunicación Fiabilidad manteniendo retrasos pequeños y relativamente deterministas.

El estudio comparativo del rendimiento de estos protocolos demuestra que UDP satisface mejor los requisitos de puntualidad de los datos, así como la fiabilidad de la transmisión para Aplicaciones en tiempo real en una NCS (sistema de convergencia de red) con redes inalámbricas que son vulnerables a errores.



CAPÍTULO V: CONCLUSIONES

CONCLUSIONES

Del estudio realizado se determinó que la selección del Protocolo UDP para la transmisión de videovigilancia y cualquier otro tipo de video transmitido, ha permitido mejorar la transmisión de video en vivo especialmente en las entidades gubernamentales ya que permitiría en su centro de monitoreo tener una eficaz, transmisión en vivo.

La transmisión de datos en el entorno Streaming, en los que los protocolos TCP, HTTP, RTP y UDP se estudian en diferentes métricas de rendimiento, como, retraso, pérdida de paquetes, rendimiento y jitter. La simulación muestra que UDP supera a otros protocolos en términos de rendimiento, jitter y retraso. Por otro lado, TCP da una mayor tasa de entrega de paquetes y un recuento mínimo de pérdida de paquetes debido a su característica orientada a la conexión. Al final, para aplicaciones multimedia donde la pérdida de paquetes es difícil de manejar, los



desarrolladores deberían optar por TCP, de lo contrario, UDP es la mejor opción con un mejor rendimiento en la transmisión de video MPEG-4 en el entorno de red. La implementación de protocolos en las cámaras de videovigilancia IP de las marcas comerciales se hace de manera de configuración del software de la misma cámara IP, lo que no es necesario de un software o algoritmo adicional.

BIBLIOGRAFIA

Referencias Bibliográficas

- 21, P. (7 de 11 de 2013). Regulan uso de cámaras de videovigilancia. (P. 21, Ed.) *Peru 21*. Obtenido de <https://peru21.pe/lima/regulan-camaras-videovigilancia-131815>
- Acuña Gamboa, M. E. (2013). *Propuesta de un sistema de video vigilancia para la seguridad del pabellón de ingeniería Campus Upao-Trujillo*. UPAO, La Libertad, Trujillo.
- Almeria, P. C. (2011). http://www.pitalmeria.es/public/static/files/110201d2_ppt_pitav6.pdf. Recuperado el ENERO de 2014, de http://www.pitalmeria.es/public/static/files/110201d2_ppt_pitav6.pdf: http://www.pitalmeria.es/public/static/files/110201d2_ppt_pitav6.pdf
- Alvarez Romero, E. D., & Acuña Gamboa, M. E. (2013). *PROPUESTA DE UN SISTEMA DE VIDEO VIGILANCIA PARA LA SEGURIDAD DEL PABELLON*



DE INGENIERIA CAMPUS UPAO-TRUJILLO. UNiversidad Privada Antenor Orrego, La Libertad. Trujillo: UPAO.

Al-Zoubi, H. R. (2013). Video Coding and Routing in Wireless Video Sensor Networks. *ELSEVIER*. Recuperado el 2018, de www.elsevier.com

Aslan. (01 de 2011). <http://www.aslan.es/boletin18/ralco.shtml>. Recuperado el 03 de 2014

Av-Test. (05 de 06 de 2017). <https://www.av-test.org/es/noticias/seguridad-de-camaras-ip-ver-y-ser-visto/>. (ITSitio, Editor, ITSitio, Productor, & ITSitio) Recuperado el 25 de 06 de 2018, de <https://www.av-test.org/es/noticias/seguridad-de-camaras-ip-ver-y-ser-visto/>.

Axis. (10 de 11 de 2013). *Axis*. Obtenido de Axis: <https://www.axis.com/es-ar/learning/web-articles/technical-guide-to-network-video/network-cameras>

Axis. (2013). *AXIS*. Recuperado el 01 de 2018, de http://www.axis.com/es/products/video/about_networkvideo/evolution.htm

AXIS. (01 de 2013). http://www.axis.com/es/products/video/about_networkvideo/environmental_protection.htm. Recuperado el 01 de 2014, de http://www.axis.com/es/products/video/about_networkvideo/environmental_protection.htm:

http://www.axis.com/es/products/video/about_networkvideo/environmental_protection.htm

AXIS. (01 de 2013). http://www.axis.com/es/products/video/about_networkvideo/environmental_protection.htm. Recuperado el 01 de 2014, de http://www.axis.com/es/products/video/about_networkvideo/environmental_protection.htm:

http://www.axis.com/es/products/video/about_networkvideo/environmental_protection.htm

AXIS. (2013). http://www.axis.com/es/products/video/about_networkvideo/evolution.htm.

Recuperado el 01 de 2014, de



- http://www.axis.com/es/products/video/about_networkvideo/evolution.htm:
http://www.axis.com/es/products/video/about_networkvideo/evolution.htm
- Axis. (15 de 02 de 2014). Axis. (Axis, Editor) Obtenido de Axis:
<https://www.axis.com/es-pe/learning/web-articles/technical-guide-to-network-video/types-of-network-cameras>
- Axis. (01 de 2014). <http://www.axis.com>. Recuperado el 01 de 2014, de
http://www.axis.com/es/products/video/about_networkvideo/image_sensors.htm:
http://www.axis.com/es/products/video/about_networkvideo/image_sensors.htm
- AXIS. (01 de 2014). <http://www.axis.com/es/>. Recuperado el 03 de 2014
- AXIS. (08 de Marzo de 2014).
http://www.axis.com/es/products/video/about_networkvideo/evolution.htm.
 Recuperado el 08 de Marzo de 2014, de
http://www.axis.com/es/products/video/about_networkvideo/evolution.htm:
http://www.axis.com/es/products/video/about_networkvideo/evolution.htm
- AXIS. (01 de 2014).
http://www.axis.com/es/products/video/about_networkvideo/image_sensors.htm.
 Recuperado el 01 de 2014, de
http://www.axis.com/es/products/video/about_networkvideo/image_sensors.htm:
http://www.axis.com/es/products/video/about_networkvideo/image_sensors.htm
- AXIS. (01 de 2014).
http://www.axis.com/es/products/video/about_networkvideo/light_sensitivity.htm.
 Recuperado el 01 de 2014
- AXIS PROCESAMIENTO DE IMAGEN. (01 de 2013).
http://www.axis.com/es/products/video/about_networkvideo/image_processing.htm.
 Recuperado el 01 de 2014, de
http://www.axis.com/es/products/video/about_networkvideo/image_processing.htm:



- http://www.axis.com/es/products/video/about_networkvideo/image_processing.htm
- AXIS PROTECCION AMBIENTAL. (01 de 2013).
http://www.axis.com/es/products/video/about_networkvideo/environmental_protection.htm. Recuperado el 01 de 2014, de http://www.axis.com/es/products/video/about_networkvideo/environmental_protection.htm:
http://www.axis.com/es/products/video/about_networkvideo/environmental_protection.htm
- AXIS PROXIM. (01 de 2003).
http://www.casadomo.com/images/CASADOMO/media/content/axis_vigilancia_ip_inalambrica.pdf. Recuperado el 01 de 2014, de http://www.casadomo.com/images/CASADOMO/media/content/axis_vigilancia_ip_inalambrica.pdf:
http://www.casadomo.com/images/CASADOMO/media/content/axis_vigilancia_ip_inalambrica.pdf
- AXIS-2014. (s.f.).
http://www.axis.com/es/products/video/about_networkvideo/light_sensitivity.htm. Obtenido de http://www.axis.com/es/products/video/about_networkvideo/light_sensitivity.htm:
http://www.axis.com/es/products/video/about_networkvideo/light_sensitivity.htm
- Balan HV, E. L. (2007). *Evaluación experimental de la calidad de voz sobre el protocolo de control de congestión de datagramas*.
- Bernal, F. A. (2013). *SISTEMA DE VIDEOVIGILANCIA PARA LA CIUDAD DE MÉXICO*. INSTITUTO POLITÉCNICO NACIONAL, MÉXICO D.F., MÉXICO D.F.; INSTITUTO POLITÉCNICO NACIONAL.
- Bosch. (08 de 03 de 2014). <http://www.dym-sa.com.ar/documentos/mopu.pdf>. Recuperado el 08 de 03 de 2014, de <http://www.dym-sa.com.ar/documentos/mopu.pdf>: <http://www.dym-sa.com.ar/documentos/mopu.pdf>



- Bova, T. a. (1999). *PROTOCOLO UDP CONFIABLE*.
Cali. (2014). Lanza plan nacional de cámaras y videovigilancia en Colombia. *El Tiempo*, 1.
- Castillo, P. (2013). *Deterioro en Laboratorio Cisco*. Trujillo: Propia.
- CAVOUKIAN, A. (01 de 01 de 2007).
<http://www.ipc.on.ca/images/Resources/video-e.pdf>. Recuperado el 08 de 03 de 2014, de <http://www.ipc.on.ca/images/Resources/video-e.pdf>:
<http://www.ipc.on.ca/images/Resources/video-e.pdf>
- CBOS. HENRY MANOLO, C. C. (Marzo de 2010).
<http://repositorio.espe.edu.ec/handle/21000/4383>. Recuperado el 23 de 01 de 2014, de <http://repositorio.espe.edu.ec/handle/21000/4383>
- Chauca Miguel, E. (2013). *SISTEMA DE GESTIÓN CLINICA WEB PARA MEJORAR LA ADMINISTRACIÓN DE LA CLINICA COBAC*. TRUJILLO.
- Chavez Irazabal, W. (2014). Educación a Distancia y las Nuevas Tecnologías IP. (UNMSM, Ed.) *ELECTRÓNICA - UNMSM*, 42-47.
- CHAVEZ SANCHEZ, E. J. (2013). *REDISEÑO DE LA RED INALÁMBRICA METROPOLITANA Y LOCAL PARA MEJORAR LOS SERVICIOS DE COMUNICACIONES Y ADMINISTRACION EN EL GRUPO EDUCATIVO LEONARDO DA VINCI*. TRUJILLO.
- CHEE, B. y. (2004). Digital Security Sentries. *InfoWorld*, "<http://books.google.de/books?id=6TkEAAAAMBAJ&lpg=PA39&dq=%22axis%20communications%22&pg=PA38#v=onepage&q&f=false>", 38-41.
- Chu, D., Chun-hua, J., Zong-bo, H., & Wei, J. (2013). El diseño e implementación del sistema de videovigilancia basado en H.264, SIP, RTP / RTCP y RTSP. *Sixth International Symposium on Computational Intelligence and Design*.
- CISCO. (15 de 08 de 2018). Protocolos de Transporte. *CCNA Router y Switch*.
- Comercio, E. (18 de 02 de 2014). Miraflores tiene 505 comercios con sistemas de videovigilancia. *Miraflores tiene 505 comercios con sistemas de videovigilancia*, pág. Central. Recuperado el 10 de 01 de 2015, de <https://elcomercio.pe/lima/miraflores-505-comercios-sistemas-videovigilancia-294763>



- COMMUNICATIONS, A. (2014).
http://www.axis.com/es/files/brochure/bc_ipsurv_54774_210x280_en_1401_lo.pdf. Recuperado el 24 de Enero de 2014, de http://www.axis.com/es/files/brochure/bc_ipsurv_54774_210x280_en_1401_lo.pdf:
http://www.axis.com/es/products/video/camera/networkCam_literature.htm
- Constantino, P. V. (25 de Enero de 2014).
<http://personales.unican.es/perezvr/pdf/Compresion%20de%20video.pdf>.
 Recuperado el 25 de Enero de 2014, de <http://personales.unican.es/perezvr/pdf/Compresion%20de%20video.pdf>:
<http://personales.unican.es/perezvr/pdf/Compresion%20de%20video.pdf>
- Correo, D. (01 de 03 de 2017). Trujillo: Instalan 28 cámaras de videovigilancia en el distrito de Moche. *Trujillo: Instalan 28 cámaras de videovigilancia en el distrito de Moche*, pág. Centrales.
- Costa, G. (29 de 06 de 2015). ¿Sirven las cámaras de videovigilancia? ¿Sirven las cámaras de videovigilancia?, por Gino Costa, pág. Centrales. Obtenido de <https://elcomercio.pe/lima/sirven-camaras-videovigilancia-gino-costa-169341>
- (2013). *Diseño de un sistema de televigilancia sobre IP para el edificio CRAI de la Escuela Politécnica Superior de Gandia*. UNIVERSIDAD POLITECNICA DE VALENCIA, Valencia. Valencia: UNIVERSIDAD POLITECNICA DE VALENCIA.
- dlink. (10 de Febrero de 2014). <http://www.dlinkla.com/>. Recuperado el 10 de Febrero de 2014, de <http://www.dlinkla.com/>: <http://www.dlinkla.com/ip-surveillance>
- Duke, Branden, Blanton, & Eddy. (2006). A Roadmap for Transmission Control. *RFC 4614*.
- ECURED. (2018). Transmision de Datos. *ECURED*. Recuperado el 10 de 08 de 2018
- EDIMAX. (23 de Enero de 2014). <http://www.edimax.com/>. Recuperado el 23 de Enero de 2014, de <http://www.edimax.com/>:
http://www.edimax.com/en/produce_list.php?pl1_id=27&pl2_id=



- Fahad Taha AL-Dhief a, Naseer Sabri b, & S. Foua. (2017). A review of forest fire surveillance technologies: Mobile ad-hoc network. *ScienceDirect*.
- Farahnaz Naeimipoor, C. R. (2015). Evaluación del rendimiento de los protocolos de difusión de video sobre redes vehiculares. *IEEE International*.
- FERNANDO RAÚL, R. M. (Enero de 2011). <http://tesis.pucp.edu.pe/repositorio/>. Recuperado el 25 de 01 de 2014, de <http://tesis.pucp.edu.pe/repositorio/>: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/890/REY_MANRIQUE_FERNANDO_CCTV_IP_INALAMBRICA.pdf?sequence=1
- Flores, W. I. (2015). *LEVANTAR LA INFORMACIÓN Y MEJORAR EL PROCESO DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE HARDWARE Y SOFTWARE DE LA UNIVERSIDAD DE GUAYAQUIL*. UNIVERSIDAD DE GUAYAQUIL, Guayaquil. Guayaquil: UNIVERSIDAD DE GUAYAQUIL.
- Gang Qi, L. Z. (2017). *Communication Protocol with Network Coding in Long-chain Wireless Sensor Network*. Guilin,, Guilin,, China: Guilin University of Electronic Technology,.
- Genner Vinicio, P. O. (2013). *IMPLEMENTACIÓN DE EQUIPOS DE MONITOREO Y SEGURIDAD BASADO EN CÁMARAS IP EN EL ALMACÉN LINDÓN GARCÍA REPRESENTACIONES DEL CANTÓN TOSAGUA*. ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ, Calceta. Calceta: ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ. Obtenido de <http://repositorio.espam.edu.ec/bitstream/42000/82/1/TESIS%20JENNIFER%20VILLAVICENCIO%20Y%20GENNER%20PALADINES.pdf>
- Gino Francisco, C. S. (29 de 06 de 2015). ¿Sirven las cámaras de videovigilancia? *El Comercio*, pág. 10. Obtenido de <https://elcomercio.pe/lima/sirven-camaras-videovigilancia-gino-costa-169341>
- GRANADOS, F. J. (Marzo de 2010). *METODOLOGÍA PARA LA CREACIÓN Y ADMINISTRACION DE CENTROS DE COMPUTO EDUCATIVOS*. MEXICO DF. Recuperado el 20 de Enero de 2014
- H Schulzrinne, S. C. (2003). *A transporte de protocolos para aplicaciones en tiempo real*.



- Huerta, M. G. (12 de Noviembre de 2010). *Administración centralizada de Redes WLAN*. Lima. Recuperado el 25 de Enero de 2014, de <http://tesis.pucp.edu.pe/repositorio/handle/123456789/1727>
- Huerta, P. A. (2007). *ANÁLISIS CRÍTICO DEL RÉGIMEN JURÍDICO DE VIDEOVIGILANCIA*. Universidad de Chile, Santiago. Santiago: Universidad de Chile. Recuperado el 15 de 11 de 2013, de http://repositorio.uchile.cl/bitstream/handle/2250/114682/de-palacios_p.pdf?sequence=4
- Indra Company. (01 de 01 de 2009). <http://www.indracompany.com/sectores/transporte-y- trafico/nuestra-oferta/4143/4133/sistema-integrado-de-seguridad-iss>. Recuperado el 08 de Marzo de 2014, de <http://www.indracompany.com/sectores/transporte-y- trafico/nuestra-oferta/4143/4133/sistema-integrado-de-seguridad-iss>
- IRIS, A. T. (01 de 2013). http://www.axis.com/es/products/video/camera/about_cameras/iris.htm. Recuperado el 01 de 2014, de http://www.axis.com/es/products/video/camera/about_cameras/iris.htm
- J., P. (1981). Transmission Control Protocol. *RFC: 793*.
- Jain, M. H. (2003.). *High Performance TCP/IP Networking: Concepts, Issues, and Solutions*. Prentice-Hall, .
- JEW, R. y. (2008). Remote Surveillance from the ground up. *securityinfowatch*, 36-42.
- Jianchao Ji1, M. L. (2015). Protocolo de investigación en cápsula espacial en Capa de red . *IEEE*.
- Jin-yong, L., Wen-jie, D., Shuo, Z., & Dan-yan, L. (2015). Investigación del protocolo de comunicación de red. *IEEE*.
- JORDI, I., JOSE MARIA , B., LLORDEN, C., ENRIC, P., JAUME, A., & GIOMAR, C. (2008). *ESTRUCTURA DE REDES DE COMPUTADORAS*. BARCELONA: UOC.



- Juan B. Riera García, A. A. (1986). *Teleinformática y redes de computadores*. Recuperado el 2018
- Kapoor, A., & Moh, M. (2015). Implementación y Evaluación del Protocolo DFF para. *DRCN*.
- Kohler E, H. M. (2009). *Datagram Congestion Control Protocol*.
- Kohler, E., Handley, M., & Floyd, S. (2014). Designing DCCP: Congestion Control Without Reliability. *science direct*.
- Kohler, Handley, & Floyd. (2014). Designing DCCP: Congestion Control Without Reliability. *ScienseDirect*.
- Kolb, J. J. (2017). <http://jkolb.com.br/28641-2/>. Obtenido de <http://jkolb.com.br/28641-2/>.
- Lourdes Münch Galindo, J. G. (1990). *Fundamentos de administracion*. Mexico DF: Trillas, 1990 (5a. reimp.1995).
- M. Duke, R. B. (2006). A Roadmap for Transmission Control Protocol (TCP) Specification Documents. *RFC 4614*.
- Magazine, D. A. (21 de 01 de 2012). <https://www.digitalavmagazine.com/2013/01/21/los-minoristas-usan-la-videovigilancia-ip-para-la-prevencion-de-perdidas-con-vistas-a-mejorar-el-rendimiento-del-negocio/>. (D. A. Magazine, Editor) Recuperado el 2014, de www.digitalavmagazine.com: <https://www.digitalavmagazine.com/2013/01/21/los-minoristas-usan-la-videovigilancia-ip-para-la-prevencion-de-perdidas-con-vistas-a-mejorar-el-rendimiento-del-negocio/>
- Manrique, F. R. (2011). *DISEÑO DE UN SISTEMA DE CCTV BASADO EN RED IP*. Pontificia Universidad Católica el Peru, Lima. Lima: Pontificia Universidad Católica el Peru.
- Marco Antonio, S. M. (2005). *DISEÑO DE UNA RED DE VIDEO VIGILANCIA REMOTA*. Universidad Nacional de Ingeniería, LIma. Lima: Universidad Nacional de Ingeniería. Obtenido de <http://cybertesis.uni.edu.pe/handle/uni/10525>
- Mardoqueo, D. L. (2015). *Herramientas Cloud Computing y su impacto en la Gestion de Procesos Comerciales de la Empresa Corpomedica Cia. Ltda*.



- Universidad Politecnica Salesiana Sede Quito, Quito. Quito: Universidad Politecnica Salesiana Sede Quito.
- Marion Souil, T. R. (2014). Un nuevo protocolo MAC adaptable con soporte QoS para redes de sensores inalámbricos heterogéneos.
- Martí, S. M. (2013). *Diseño de un sistema de televigilancia sobre IP para el edificio CRAI de la Escuela*. UNIVERSIDAD POLITECNICA DE VALENCIA, Valencia. Gandia: UNIVERSIDAD POLITECNICA DE VALENCIA.
- Merit LILIN, S.-S. (08 de Marzo de 2014). <http://www.meritlilin.com/es/solutions.asp>. Recuperado el 08 de Marzo de 2014, de <http://www.meritlilin.com/es/solutions.asp>: <http://www.meritlilin.com/es/solutions.asp>
- Municipalidad Distrital De Surquillo. (2013). *ORDENANZA QUE ESTABLECE LA OBLIGATORIEDAD DE IMPLEMENTAR LA INSTALACIÓN DE UN SISTEMA*. MUNICIPALIDAD DISTRITAL DE SURQUILLO, Lima. Lima: MUNICIPALIDAD DISTRITAL DE SURQUILLO. Recuperado el 25 de 01 de 2014
- Namuche, G. V. (2013). *DISEÑO DE UN SISTEMA DE VIDEO-MONITOREO IP PARA LA SALA DE MANUFACTURA DEL CENTRO DE TECNOLOGÍAS AVANZADAS DE MANUFACTURA*. PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ, PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ. Lima: PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ.
- Navarro., A. (2010). La imparable evolución de la Videovigilancia IP. *Network World From IDG*. Recuperado el 15 de 01 de 2014, de <http://www.networkworld.es/convergencia/la-imparable-evolucion-de-la-videovigilancia-ip>
- Network, R. (03 de 2011). <http://www.ralco-networks.com/>. Recuperado el 03 de 2015
- NETWORK, R. (24 de Enero de 2014). www.ralco-networks.co. Recuperado el 24 de Enero de 2014, de <http://www.ralco-networks.com/index.php>
- NINA, J. C. (2014). *DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE VIDEO VIGILANCIA Y CONTROL DE ASISTENCIA BIOMÉTRICO DE LA EMPRESA AUTOACCESORIOS LOS GEMELOS S.A.C. DE LA CIUDAD*



- DE JULIACA. UNIVERSIDAD NACIONAL DEL ALTIPLANO PUNO, Puno.
Puno: UNIVERSIDAD NACIONAL DEL ALTIPLANO PUNO.
- Nor, S. A., Alubady, R., & Kamil, W. A. (2016). *Rendimiento simulado de los protocolos TCP, SCTP, DCCP y UDP*.
- Orozco, M. y. (01 de 2014). <http://www.maorsa.com.mx/comoelegircctv.pdf>. Recuperado el 01 de 2014, de <http://www.maorsa.com.mx/comoelegircctv.pdf>: <http://www.maorsa.com.mx/comoelegircctv.pdf>
- Oscar Enrique, M. J. (Octubre de 2013). <http://tesis.pucp.edu.pe/repositorio/handle/123456789/5000>. Recuperado el 23 de Enero de 2014, de <http://tesis.pucp.edu.pe/repositorio/handle/123456789/5000>: <http://tesis.pucp.edu.pe/repositorio/handle/123456789/5000>
- Pedro, S. S. (Enero de 2014). <http://www.monografias.com/trabajos100/informe-administracion-centro-procesamiento-datos/informe-administracion-centro-procesamiento-datos.shtml>. Recuperado el Enero de 2014, de Monografias: <http://www.monografias.com/trabajos100/informe-administracion-centro-procesamiento-datos/informe-administracion-centro-procesamiento-datos.shtml>
- Pelaez Salvador, J. (01 de 09 de 2018). Diseño de un sistema de video vigilancia IP para la Corte Superior de Justicia - La Libertad. Trujillo, La Libertad, Perú.
- Pelaéz Salvador, J. A. (2013). *Diseño de un sistema de video vigilancia IP para la Corte Superior de Justicia - La Libertad*. Universidad Privada del Norte. Trujillo: Universidad Privada del Norte.
- Perez, E. H. (15 de 01 de 2010). *Tecnologías y Redes de Trasmision de Datos*. Limusa. Obtenido de <http://gelopinformatica.blogspot.com/p/1.html>
- Peru, R. P. (10 de 12 de 2013). Trujillo: Instalarán 128 cámaras de videovigilancia en seis distritos. *Radio Programas del Peru*. Recuperado el 22 de 01 de 2014
- Ping Wang, C. Z. (2016). Un protocolo de gestión WAN TR069 para redes de sensores inalámbricos WIA-PA. *IEEE org*.
- Portinari, B. (18 de 01 de 2017). La instalación de cámaras en un instituto reabre el debate sobre su uso. *La instalación de cámaras en un instituto reabre el*



debate sobre su uso, pág. Central. Obtenido de https://elpais.com/elpais/2017/01/13/mamas_papas/1484295654_015542.html

Postel, J. (1981). Transmission Control Protocol. *RFC 793*.

R. Stevens. (1994). *TCP/IP Illustrated*.

Ralco-Networks. (15 de 01 de 2017). <http://www.ralco-networks.com/infraestructuras-inalambricas-para-videovigilancia/>. (Ralco-Networks, Editor, Ralco-Networks, Productor, & Ralco-Networks) Recuperado el 28 de 06 de 2018, de <http://www.ralco-networks.com/infraestructuras-inalambricas-para-videovigilancia/>

REY MANRIQUE, F. R. (Enero de 2011). <http://tesis.pucp.edu.pe/repositorio/handle/123456789/7/browse?value=Rey+Manrique,+Fernando+Ra%C3%BAI&type=author>. Recuperado el Enero de 2014, de <http://tesis.pucp.edu.pe/repositorio/handle/123456789/890>

Ricci, I. F. (08 de Marzo de 2014). <http://es.scribd.com/doc/3081866/Administracion-de-Centros-de-Computo>. Recuperado el 08 de Marzo de 2014, de <http://es.scribd.com/doc/3081866/Administracion-de-Centros-de-Computo>

Rivas Cruz, J. A. (2011). *Implementacion de Sistema de Seguridad con videovigilancia y software libre*. Intituto Politecnico Nacional, Mexico DF. Mexico DF: Intituto Politecnico Nacional. Obtenido de <https://tesis.ipn.mx/bitstream/handle/123456789/11622/3.pdf?sequence=1&isAllowed=y>

Sarabjot Singh, O. O. (2010). Video Capacity and QoE Enhancements over LTE. *IEEE*.

Shahrudin Awang Nora, *. R. (2017). Rendimiento simulado de protocolos TCP, SCTP, DCCP y UDP over 4G network. *Procedia Computer Science*.

Shukla S, K. V. (2013). Comparative Study of 1G, 2G, 3G and 4G. *Articulo Cientifico*.



- Sonia, S. G. (2011). *http://repositorio.utm.edu.ec/bitstream/123456789/2487/1/FEBRERO_18_2_011manuales.pdf*. Recuperado el 20 de 01 de 2014, de *http://repositorio.utm.edu.ec/bitstream/123456789/2487/1/FEBRERO_18_2_011manuales.pdf*: Gina Leonor
- SYRSOLUCIONES. (08 de Marzo de 2014). *http://www.syrsoluciones.com/index.php/cctv*. Recuperado el 08 de Marzo de 2014, de *http://www.syrsoluciones.com/index.php/cctv*: *http://www.syrsoluciones.com/index.php/cctv*
- SYSCOM. (2014). *http://www.syscomcctv.com.mx/que_es_cctv.htm*. Recuperado el 2014, de *http://www.syscomcctv.com.mx/que_es_cctv.htm*
- TANENBAUM, A. S. (2003). *REDES DE COMPUTADORAS*. NAULCAPAN DE JUAREZ: PEARSON.
- Tecnoseguro. (20 de 06 de 2018). *www.tecnoseguro.com*. (www.tecnoseguro.com, Editor, & www.tecnoseguro.com, Productor) Recuperado el 25 de Junio de 2018, de *www.tecnoseguro.com*: *https://www.tecnoseguro.com/noticias/cctv/centro-comercial-colombia-modelo-seguridad-axis*
- Tenealive. (s.f.). *http://tenealive.com*. Obtenido de tenealive: *http://tenealive.com/protocolos-y-modelos-de-comunicaci%C3%B3n-de-las-c%C3%A1maras-ip-wifi-de-videovigilancia-y-dom%C3%B3tica-de-teneali*
- Teostekwebstore. (03 de 10 de 2014). ¿Qué es una cámara de red o cámara IP? *teostekwebstore*. Recuperado el 3 de 10 de 2014, de *http://www.teostekwebstore.com/securtek/que-es-una-camara-ip*
- Torres, C. (01 de Enero de 2005). *http://www.emb.cl/gerencia/articulo.mvc?xid=2549*. Recuperado el 25 de Enero de 2014, de *http://www.emb.cl/gerencia/articulo.mvc?xid=2549*
- TTCS. (08 de Marzo de 2014). *http://www.ttcs.es/faqs/que-es-un-circuito-cerrado-de-television-cctv.html*. Recuperado el 08 de Marzo de 2014, de *http://www.ttcs.es/faqs/que-es-un-circuito-cerrado-de-television-cctv.html*: *http://www.ttcs.es/faqs/que-es-un-circuito-cerrado-de-television-cctv.html*



- VILLALOBOS, H. A. (Abril de 2009). *PLAN DE GESTION DEL ALCANCE, TIEMPO Y COSTO PARA LA IMPLEMENTACION DE UN CENTRO DE CÓMPUTO EN UNA PLANTA DE MANUFACTURA*. TESIS, UNIVERSIDAD PARA LA COOPERACION INTERNACIONA, San Jose de Costa Rica. Recuperado el 20 de Enero de 2015
- Vox, D. M. (2007). Recuperado el 2014, de <http://es.thefreedictionary.com/incidencia>:
<http://es.thefreedictionary.com/incidencia>
- Vox., D. M. (2007). *2007 Larousse Editorial, S.L.* Recuperado el 2014, de <http://es.thefreedictionary.com/incidencia>:
<http://es.thefreedictionary.com/incidencia>
- WIKIPEDIA. (2014).
http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n.
Recuperado el 2014, de http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n:
http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n
- Wisam AK, N. S. (2015). *Evaluación del rendimiento del tráfico TCP, UDP y DCCP sobre la red 4G*.
- WOLF, L. C. (1999). Electronic Networking Applications and Policy. *Internet Research*, 49-57.
- Xiaoyan Wang. (2014). Protocolo para Redes Ad Hoc Inalámbricas. *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*.
- Yansong Jennifer Ren, L. O. (2012). Precisión de una huella dactilar de video tolerante a pérdida de alto nivel para Autenticación de Vigilancia. *International Conference on Pattern Recognition*.
- Yi Gu1, M. K. (2014). Diseño e Implementación del Sistema de Cámara de Vigilancia Basado en UPnP para la Seguridad del Hogar.
- Zhang, L., Okamawari, T., & Fujii, T. (s.f.). *Evaluación del desempeño de TCP y UDP durante la transferencia de LTE*.



ANEXOS
ANEXO N° 01
RANKING DE PROTOCOLOS

| Ranking Mejores 10 Protocolos para Videovigilancia IP | | |
|--|-------------------------|-----------------------------|
| Posición | Nombre Protocolo | Capa en la que Opera |
| 1 | UDP | Transporte |
| 2 | TCP | Transporte |
| 3 | RTP | Sesión/Transporte |
| 4 | RTCP | Sesión/Transporte |
| 5 | RTSP | Sesión |
| 6 | FTP | Aplicación |
| 7 | HTTP | Aplicación |
| 8 | SMTP | Aplicación |
| 9 | DCCP | Transporte |
| 10 | BATMAN | Internet |



ANEXO N° 02

**FORMATO DE ENCUESTA PARA SELECCIÓN DE PROTOCOLO PARA EL
DESARROLLO DE LA RED DE VIDEOVIGILANCIA IP**

A. DATOS PERSONALES

Apellidos _____ y _____ Nombres: _____

Titulo y/o Grado: _____

Especialidad: _____

Centro Laboral: _____

Cargo/Ocupación: _____

Ingresar en una escala de 1 al 4 el grado de importancia de cada criterio para determinar si es una buena alternativa en cuanto a la performance y experiencia en el uso de los protocolos para un sistema de videovigilancia vía streaming.



| Criterios Protocolos | Rendimiento | Paquetes perdidos | Retraso de Extremo a Extremo | Promedio Jitter | Promedio |
|-------------------------|-------------|-------------------|------------------------------|-----------------|----------|
| UDP | | | | | |
| TCP | | | | | |

ANEXO N° 03

Evidencia de la evaluación del protocolo UDP y TCP con el Sniffer de Red LiveTcpUdpWatch

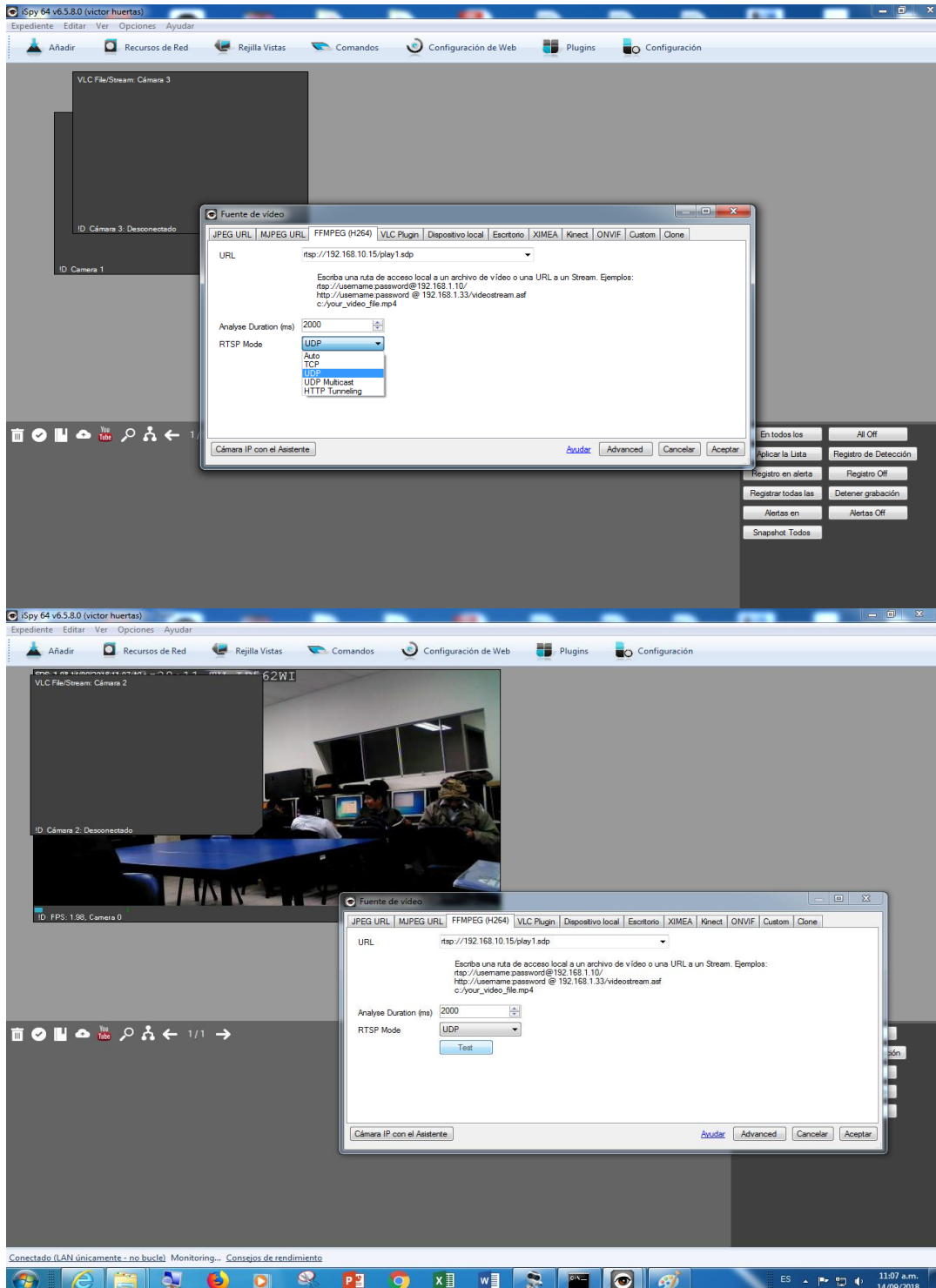


| ID de Proceso | Nombre | Dirección Remota | Protocolo | Dirección Local | Puerto Local | Puerto Remo... | Nombre del ... | Bytes Recibidos | Bytes Enviados | Paquetes |
|---------------|-------------|---|-----------|-----------------|--------------|----------------|----------------|-----------------|----------------|----------|
| 1208 | svchost.exe | 192.168.137.101 [Senati-PC.mshome.net] | UDP IPv4 | 224.0.0.252 | 5355 | 53029 | | 44 | | 2 |
| 1208 | svchost.exe | 192.168.137.101 [Senati-PC.mshome.net] | UDP IPv4 | 224.0.0.252 | 5355 | 65147 | | 44 | | 2 |
| 1208 | svchost.exe | 192.168.137.101 [Senati-PC.mshome.net] | UDP IPv4 | 224.0.0.252 | 5355 | 62507 | | 44 | | 2 |
| 1208 | svchost.exe | 192.168.137.101 [Senati-PC.mshome.net] | UDP IPv4 | 224.0.0.252 | 5355 | 49909 | | 44 | | 2 |
| 2432 | svchost.exe | 192.168.137.102 [TV-IP562W.mshome.net] | UDP IPv4 | 239.255.255.250 | 1900 | 42535 | | 137 | | 1 |
| 2432 | svchost.exe | 192.168.137.102 [TV-IP562W.mshome.net] | UDP IPv4 | 192.168.137.1 | 1900 | 42535 | | | 469 | |
| 2432 | svchost.exe | 192.168.137.102 [TV-IP562W.mshome.net] | UDP IPv4 | 239.255.255.250 | 1900 | 55646 | | 1,342 | | 3 |
| 2432 | svchost.exe | 192.168.137.102 [TV-IP562W.mshome.net] | UDP IPv4 | 239.255.255.250 | 1900 | 35778 | | 481 | | 1 |
| 2432 | svchost.exe | 192.168.137.102 [TV-IP562W.mshome.net] | UDP IPv4 | 239.255.255.250 | 1900 | 38750 | | 1,342 | | 3 |
| 2432 | svchost.exe | 192.168.137.102 [TV-IP562W.mshome.net] | UDP IPv4 | 239.255.255.250 | 1900 | 41631 | | 481 | | 1 |
| 4 | | 192.168.137.103 [Senati.mshome.net] | UDP IPv4 | 192.168.137.255 | 138 | 138 | netbios-dgm | 3,864 | | 20 |
| 2432 | svchost.exe | 192.168.137.103 [Senati.mshome.net] | UDP IPv4 | 239.255.255.250 | 1900 | 1900 | ssdp | 31,625 | | 66 |
| 4 | | 192.168.137.103 [Senati.mshome.net] | UDP IPv4 | 192.168.137.255 | 137 | 137 | netbios-ns | 994 | | 17 |
| 1208 | svchost.exe | 192.168.137.103 [Senati.mshome.net] | UDP IPv4 | 224.0.0.252 | 5355 | 63927 | | 44 | | 2 |
| 1208 | svchost.exe | 192.168.137.103 [Senati.mshome.net] | UDP IPv4 | 224.0.0.252 | 5355 | 50738 | | 44 | | 2 |
| 1208 | svchost.exe | 192.168.137.103 [Senati.mshome.net] | UDP IPv4 | 224.0.0.252 | 5355 | 59192 | | 44 | | 2 |
| 1208 | svchost.exe | 192.168.137.103 [Senati.mshome.net] | UDP IPv4 | 224.0.0.252 | 5355 | 62704 | | 44 | | 2 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 63981 | | 62 | | 2 |
| 4 | | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 192.168.137.255 | 137 | 137 | netbios-ns | 11,968 | | 230 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 57487 | | 48 | | 2 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 54355 | | 62 | | 2 |
| 640 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 255.255.255.255 | 67 | 68 | bootpc | 2,700 | | 9 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 59353 | | 44 | | 2 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 63797 | | 48 | | 2 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 55873 | | 48 | | 2 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 57418 | | 48 | | 2 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 65119 | | 48 | | 2 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 57702 | | 66 | | 2 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 62741 | | 66 | | 2 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 49226 | | 48 | | 2 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 60804 | | 40 | | 2 |
| 640 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 192.168.137.1 | 53 | 54622 | | 49 | 49 | 1 |
| 640 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 192.168.137.1 | 53 | 57343 | | 49 | 49 | 1 |
| 640 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 192.168.137.1 | 53 | 57846 | | 49 | 49 | 1 |
| 640 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 192.168.137.1 | 53 | 59740 | | 43 | 1,568 | 1 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 64079 | | 40 | | 2 |
| 640 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 192.168.137.1 | 53 | 55278 | | 33 | 33 | 1 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 61520 | | 44 | | 2 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 63559 | | 40 | | 2 |
| 4 | | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 192.168.137.255 | 138 | 138 | netbios-dgm | 201 | | 1 |
| 2432 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 239.255.255.250 | 1900 | 60915 | | 798 | | 6 |
| 2432 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 192.168.137.1 | 1900 | 60915 | | | 2,814 | |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 62187 | | 44 | | 2 |
| 1208 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 224.0.0.252 | 5355 | 55812 | | 66 | | 2 |
| 640 | svchost.exe | 192.168.137.104 [android-c4a4fcc2d61a1b4.msho...] | UDP IPv4 | 192.168.137.1 | 67 | 68 | bootpc | 600 | | 2 |

ANEXO N° 04

Capturas de Pantalla de la cámara de video Vigilancia TrendNet usando el protocolo UDP para la transmisión





ANEXO N° 05



Capturas de Pantalla del Software GNS-3

