Evaluación y Análisis del Desempeño de redes Inalámbricas WI-FI con Servicios de Seguridad Propiciados por IPSec. Caso de Estudio: Red Inalámbrica de la Universidad del Cauca

Diego Mauricio Puerto Rojas

Jorge Andrés Zarama Benavides

Director: Mag. Francisco Javier Terán Cuarán

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones

Departamento de Telecomunicaciones

Popayán, Marzo de 2012

Evaluación y Análisis del Desempeño de redes Inalámbricas WI-FI con Servicios de Seguridad Propiciados por IPSec. Caso de Estudio: Red Inalámbrica de la Universidad del Cauca

Trabajo de Grado presentado como requisito para obtener el título de Ingeniero en Electrónica y Telecomunicaciones

Diego Mauricio Puerto Rojas

Jorge Andrés Zarama Benavides

Director: Mag. Francisco Javier Terán Cuarán

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones

Departamento de Telecomunicaciones

Popayán, Marzo de 2012

Contenido

Índice de Tablas

Índice de Figuras

LISTA DE ACRÓNIMOS

ACK	*Acknowledgement*, Acuse de Recibo
AES	*Advanced Encryption Standard*, Estándar de Cifrado Avanzado
AH	*Authentication Header,* Cabecera de Autenticación
AP	*Access Point*, Punto de Acceso
BITS	*Bump In The Stack*, Puesto en la Pila
BITW	*Bump In The Wire*, Puesto en el Cable
CCK	*Complementary Code Keying,* Modulación por Código Complementario
CSMA/CA	*Carrier Sense Multiple Access with Collision Avoidance***,** Acceso Múltiple por Detección de Portadora con Evasión de Colisiones
DES	*Data Encryption Standard,* Estándar de cifrado de datos
D-ITG	*Distributed Internet Traffic Generator*, Generador de Tráfico Distribuido de Internet
DOI	*Domain of Interpretation*, Dominio de interpretación
DSCP	*Differentiated Services Code Point,* Punto de Código de Servicios Diferenciado
DSS	*Digital Signature Standard*, Estándar de Firma Digital
DSSS	*Direct Sequence Spread Spectrum,* Espectro Ensanchado por Secuencia Directa
DTE	*Data Terminal Equipment,* Equipo Terminal de Datos
ESP	*Encapsulating Security Payload*, Carga de seguridad Encapsulada
FIET	Facultad de Ingeniería Electrónica y Telecomunicaciones
HMAC	*Hashed Message Authentication Codes,* Códigos de Autenticación de Mensaje Hash
IEEE	*Institute of Electrical and Electronics Engineers*, Instituto de Ingenieros Eléctricos y Electrónicos

IETF	*Internet Engineering Task Force,* Grupo de Trabajo de Ingeniería en Internet
IKE	*Internet Key Exchange*, Intercambio de Claves en Internet
IPDV	*One-way Packet Delay Variation,* Variación de Retardo en un Sentido
IPET	Instituto de Postgrados de Ingeniería Electrónica y Telecomunicaciones
IPLR	*IP Packet Loss Ratio,* Tasa de Pérdida de Paquetes
IPPM	*IP Performance Metrics*, Grupo de Trabajo de Métricas de Desempeño IP
IPSEC	*Internet Protocol Security,* Seguridad para el Protocolo de Internet
IPTD	*Mean One-way Delay*, Retardo Medio en un Sentido
ISAKMP	*Internet Security Association and Key Management Protocol*, Protocolo de Asociaciones de Seguridad de Internet y de Gestión de Claves
ISP	Internet Service Provider, Proveedor de Servicios de Internet
ITU	*International Telecommunication Union*, Unión Internacional de Telecomunicaciones
ITU-T	*The ITU Telecommunication Standardization*, Sector de Estandarización de Telecomunicaciones de la ITU
LAN	*Local Area Network*, Red de Área Local
MD5	*Message Digest*, Resumen de Mensaje
MTU	*Maximum Transfer Unit*, Unidad Máxima de Transferencia
NAT	*Network Address Translation,* Traducción de Dirección de Red
NP	*Network Performance*, Desempeño de Red
NSA	*National Security Agency,* Agencia Nacional de Seguridad
NTP	*Network Time Protocol*, Protocolo de Tiempo de Red
ODFM	*Orthogonal Frequency Division Multiplexing,* Multiplexación por División de Frecuencias Ortogonales
OSI	*Open System Interconnection*, Interconexión de Sistemas Abiertos
PAD	*Pairs Authorization Database,* Base de Datos de Autorización de Pares
PDV	*Packet Delay Variation*, Variación de Retardo de Paquetes
QoS	*Quality of Service*, Calidad de Servicio
RDSI	Red Digital de Servicios Integrados

RFC	*Request For Comments,* Petición De Comentarios
RSA	Rivest, Shamir y Adleman
SA	*Security Association*, Asociación de Seguridad
SAD	*Security Associations Database*, Bases de Datos de Asociaciones de Seguridad
SPD	*Security Policy Database*, Base de datos de Políticas de Seguridad
SG	*Security Gateway*, Pasarela de Seguridad
SKEME	*Versatile Secure Key Exchange Mechanism for Internet,* Mecanismo Versátil y Seguro de Intercambio de Claves de Internet
SPI	*Security Parameter Index*, Índice de Parámetro de Seguridad
TCP	*Transmission Control Protocol*, Protocolo de Control de Transmisión
TTL	*Time to Live*, Tiempo de Vida
UDP	*User Datagram Protocol*, Protocolo de Datagrama de Usuario
UTC	*Coordinated Universal Time*, Tiempo Universal Coordinado
UTP	*Unshielded Twisted Pair*, Par Trenzado no Blindado
WEP	*Wired Equivalent Privacy*, Privacidad Equivalente a Cableado
WPA	*Wi-Fi Protected Access*, Acceso Wi-Fi Protegido
WPA2	*Wi-Fi Protected Access 2*, Acceso Wi-Fi Protegido 2
WI-FI	*Wireless Fidelity*, Fidelidad Inalámbrica
WLAN	*Wireless Local Area Network*, Red de Area Local Inalámbrica

1. CONCEPTOS FUNDAMENTALES DEL FUNCIONAMIENTO DE IPSEC, DE AIGORITMOS DE AUTENTICACIÓN Y CIFRADO, DE REDES INALÁMBRICAS WI-FI Y DE LA INFRASTRUCTURA DE LA RED DE INFORMACIÓN DE LA UNIVERSIDAD DEL CAUCA

1.1 IPSEC: IP SECURITY

1.1.1 Introducción. IPSec se define como un conjunto o *suite* de protocolos, los cuales están basados en mecanismos de autenticación y cifrado, cuyo fin es proteger la información a nivel del protocolo IP (nivel 3 del modelo OSI), brindado de esta manera, protección tanto a la información manejada en este nivel como a la información en los niveles superiores.

Básicamente IPSec crea fronteras en las interfaces de los sistemas de información, brindándole un tratamiento especial a la información que las atraviesa. En este contexto los paquetes de información a nivel 3 (datagramas IP) se seleccionan para uno de los tres modos de procesamiento IP los cuales son:

- Aplicación de los servicios de seguridad para los datagramas IP.
- Permitir el paso a los datagramas IP sin seguridad.
- Descartar los datagramas IP.

1.1.2 Servicios de Seguridad Propiciados por IPSec. IPSec es una arquitectura diseñada para proporcionar seguridad inter-operable, de alta calidad, basada en criptografía tanto para IPv4 como para IPv6 [1]. El conjunto de servicios de seguridad tal como se definen en el glosario de seguridad de Internet [2], [3] es:

- **Control de acceso:** es un servicio de seguridad que impide el uso no autorizado de un recurso, incluyendo la prevención del uso de recursos en forma no autorizada.

- **Integridad sin conexión:** es un servicio que detecta la modificación de un datagrama IP individual, sin considerar el orden de los datagramas cuando estos llegan.

- **Autenticación del origen de los datos:** es un servicio de seguridad que verifica la identidad de origen de los datos. Este servicio usualmente trabaja en conjunto con el servicio de integridad sin conexión.

- **Confidencialidad:** es un servicio de seguridad que protege los datos de la exposición (divulgación) no autorizada.

- **Encriptación:** La encriptación es un mecanismo de seguridad usado para transformar datos desde una forma inteligible (texto plano) en una forma ininteligible (texto cifrado), para proporcionar confidencialidad.

El servicio de **no repudio** no es prestado explícitamente por IPSec, sin embargo, este puede ser implementado al utilizar algoritmos de encriptación de firma digital como RSA. El no repudio es un servicio que tiene como finalidad evitar la falsa negación de una entidad de estar involucrada en una comunicación.

El objetivo de IPSec es implementar uno o varios de estos servicios de seguridad dependiendo de las necesidades existentes en una organización o sistema informático. Para el cumplimiento de este objetivo, IPSec se soporta en el uso de sus dos protocolos de seguridad los cuales son Cabecera de Autenticación o **AH** y Encapsulamiento de Seguridad de la Carga Útil o **ESP**. AH puede ofrecer los servicios de integridad sin conexión, autenticación del origen de los datos y protección anti-repetición [4], [5], mientras que ESP ofrece los mismos servicios de AH además del servicio adicional de confidencialidad de los datos (Encriptación) [6], [7].

Los protocolos utilizados por IPSec están diseñados para ser independientes del algoritmo, esto permite utilizar cualquier grupo de algoritmos sin afectar las demás partes de la implementación, además IPSec es inter-operable lo que permite que los usuarios, host y otros componentes de la red que no empleen estos mecanismos de seguridad para la protección del tráfico no se vean afectados. El uso de estos algoritmos, en conjunto con la protección del tráfico de IPSec y los protocolos de manejo de claves, están constituidos para permitir el desarrollo de aplicaciones, sistemas y tecnología criptográfica de seguridad de alta calidad en la capa IP [1].

1.1.3 Visión General de IPSec. Para poder tener una visión general de IPSec se deben entender los conceptos de las partes que componen esta arquitectura, las

cuales son: Implementación, Asociaciones de Seguridad, Bases de Datos de Seguridad, Protocolos de Seguridad, Manejo de Claves, Algoritmos de Autenticación y Cifrado, entre otros. Información más detallada sobre esta arquitectura no es objetivo de este proyecto y puede ser consultada en sus respectivos RFCs [2], [3], [8].

1.1.3.1 Implementación de IPSec. IPSec puede ser implementado de varias formas [2]: en un host, en un enrutador, o en un cortafuegos. Algunos ejemplos frecuentes son:

- Integrar IPSec en una implementación nativa IP. Se debe tener acceso al código fuente IP y puede ser aplicada tanto en hosts como en una pasarela de seguridad (SG).

- "Puesto-en-la-Pila" (BITS), IPSec se implementa "por debajo" de una implementación existente de una pila IP, entre el IP nativo y los drivers locales de la red. El acceso al código fuente para la pila IP no es requerido en este contexto. Este método es apropiado para los sistemas antiguos y cuando se adopta se emplea generalmente en hosts.

- El uso de un procesador criptográfico externo es una característica de diseño común de los sistemas de seguridad de red usados por los militares, y en algunos sistemas comerciales. A estos sistemas algunas veces se los refiere como implementaciones "Puesto-en-el-cable" (BITW). Tales implementaciones se pueden diseñar para asistir a un host o una SG (o a ambos). El dispositivo BITW generalmente tiene una IP direccionable. Cuando asiste a un único host, puede resultar análogo a una implementación BITS, pero en un enrutador o en un cortafuegos debe funcionar como una SG.

1.1.3.2 Asociaciones de Seguridad (SA). Una Asociación de Seguridad o Security Association como lo define la arquitectura, es una conexión unidireccional (simplex) que ofrece servicios de seguridad al tráfico transportado por esta. AH y ESP ejecutan los servicios de seguridad ofrecidos por una SA, pero no ambos; dado el caso que un determinado tipo de tráfico requiera el uso de AH y ESP se utilizaran dos o más SAs para poder transportarlo. De esta manera, para poder

establecer una comunicación entre dos hosts o dos SG se requiere del uso de dos o más SAs.

Según la tercera versión de IPSec [3], una SA se puede identificar unívocamente por el campo SPI (Índice de Parámetro de Seguridad), pero dado que la mayoría de las implementaciones están construidas basándose en la segunda versión, en esta, una SA queda identificada por un trio que consiste en: un SPI, una dirección IP de destino, y un identificador de protocolo de seguridad (50 para AH o 51 para ESP).

Las SAs pueden trabajar de dos modos: Transporte y Túnel. Una SA en modo transporte es una conexión entre dos host. En IPv4, la cabecera del protocolo de seguridad en modo transporte se ubica inmediatamente después de la cabecera IP y algunas opciones, y antes de los protocolos de niveles superiores (por ejemplo UDP o TCP). En IPv6, la cabecera de seguridad se ubica después de la cabecera IP y las extensiones de esta, pero se podría ubicar antes o después de las opciones de destino, y antes de los protocolos de nivel superior. Una SA en modo túnel es en pocas palabras una SA aplicada a un túnel IP. Cualquier caso que implique el uso de una SG, donde esta sea el fin del túnel IP, se debe trabajar con SAs en modo túnel. Una SA en modo túnel implica el uso de una cabecera IP externa que especifica el inicio y el fin del túnel IPSec, además del uso de la cabecera interna IP que define las direcciones de origen y destino originales. La cabecera del protocolo de seguridad se ubica después de la cabecera IP externa y antes de la cabecera IP interna.

Una SA básicamente es una gestión que se hace para poder cumplir con una política de seguridad para el tráfico que cruza la frontera IPSec. Con el fin de cumplir con este objetivo y lograr características de interoperabilidad IPSec cuenta con bases de datos que tienen la función de especificar y gestionar los servicios ofrecidos a los datagramas IP. La última versión de IPSec cuenta con tres bases de Datos aunque las versiones anteriores utilizan solamente dos.

1.1.3.3 Bases de Datos de Políticas de Seguridad (SPD). Básicamente las SPD especifican las políticas que determinan el tratamiento del tráfico entrante o saliente en una interfaz de un host, Security Gateway o una implementación IPSec en BITS o BITW. De esta manera se debe consultar la SPD durante todo el procesamiento del tráfico entrante y saliente incluyendo el tráfico al cual no se le deba aplicar servicios de seguridad. Cuando un tráfico requiera servicios de

seguridad la SPD debe especificar los servicios de seguridad que se proporcionaran, los protocolos que se emplearán, algoritmos a utilizar, etc.

La SPD está dividida lógicamente en tres partes SPD-S (*secure traffic*), SPD-O (*outbound*) y SPD-I (*inbound*). SDP-S contiene todas las entradas para el tráfico al cual se le aplicarán servicios de seguridad propiciados por IPSec, SPD-O contiene todas las entradas para el tráfico saliente que debe ser descartado o enviado sin seguridad, y SPD-I es aplicada al tráfico de entrada que debe ser pasado sin protección o descartado, si una entrada de tráfico no coincide con ninguna SPD este tráfico deberá ser descartado.

1.1.3.4 Selectores. Una SA puede tener mayor o menor modularidad dependiendo de los selectores utilizados para definir el grupo de tráfico para la SA. Por ejemplo al implementar IPSec entre dos host (o entre dos SG), todo el tráfico entre estos puede ser transportado por una simple SA y ofrecer servicios de seguridad uniforme. Este mismo tráfico podría ser transportado por múltiples SAs dependiendo de los selectores utilizados. Para el ejemplo, uno de estos selectores podría ser la aplicación que está inyectando el tráfico; este selector está definido por los campos siguiente *protocolo* y el *puerto* en la cabecera de los Datagramas IP, en este caso para cada aplicación se utilizaría una SA distinta y la seguridad tendría mayor granularidad.

Los siguientes parámetros del selector deben ser soportados por la gestión de SA para facilitar el control de la granularidad de SA:

- Dirección IP destino (IPv4 o IPv6).
- Dirección IP destino (IPv4 o IPv6).
- Nombre. Hay dos casos: Identificación de Usuario y Nombre del Sistema.
- Nivel de Sensibilidad de los Datos.
- Protocolo de la Capa Transporte.
- Puertos de Origen y Destino.

1.1.3.5 Bases de Datos de Asociaciones de Seguridad (SAD). En la SAD se indexan los datos necesarios para la aplicación de IPSec en una parte de la comunicación y para retirar la protección IPSec en el otro extremo y de esta forma obtener información de usuario para comprobar que los valores de los selectores en un paquete de entrada concuerden con aquellos registrados en una SA.

Algunos de los principales datos registrados por una SAD son: SPI, contador del número de secuencia, ventana de anti repetición, algoritmo de autenticación usado con AH, algoritmos usados con ESP (cifrado, integridad o combinados) y valores relacionados como llaves y modos IV; tiempos de vida de las SA (en bytes o tiempo), opciones de desfragmentación y de tratamiento de DSCP [9].

1.1.3.6 Bases de Datos Autorización de Pares (PAD). Esta base de datos solo esta especificada en la tercera versión de la arquitectura y cumple la función de servir de vínculo entre la SPD y un protocolo de gestión de asociaciones de seguridad. Básicamente le presta funciones a las partes comunicantes en los procesos de seguridad; algunas de estas funciones son la identificación de pares o grupos autorizados para comunicarse, especificar el protocolo de gestión de claves (IKEv1, IKEv2), proveer los datos de autentificación (contraseñas, firma digital, etc.), entre otras.

1.1.4 Protocolos de Seguridad

1.1.4.1 Cabecera de Autenticación (AH). Este protocolo proporciona los servicios de seguridad de integridad sin conexión, autenticación del origen de los datos y como servicio adicional el de protección anti-repeticiones. Este último servicio es opcional y puede ser utilizado por el receptor cuando la SA así lo haya establecido. AH proporciona autenticación a las partes de la cabecera IP que se les pueda brindar este servicio (partes no mutables), así como a la información de los protocolos de capas superiores, por esta razón AH proporciona una protección “por partes”.

1.1.4.2 Encapsulamiento de Seguridad de la Carga Útil (ESP). El protocolo ESP es utilizado para brindar los servicios de seguridad de confidencialidad, autentificación del origen de los datos, integridad sin conexión, anti-repetición y confidencialidad limitada a flujo de tráfico. El conjunto de servicios que se utilicen en una comunicación depende de la Asociación de Seguridad. Como los servicios de autentificación de los datos y la integridad sin conexión están unidos de ahora en adelante se les denominara “autenticación”. En ESP el servicio de autenticación es opcional y el servicio de confidencialidad es obligatorio.

La principal diferencia que se puede encontrar entre AH y ESP es la cobertura, ya que ESP no puede autenticar los campos de la cabecera IP que no estén encapsulados por él; sin embargo si solo se necesita la autenticación de cabeceras de nivel superior es preferible utilizar ESP ya que como fue nombrado anteriormente este protocolo brinda el servicio de encriptación.

1.1.5 Gestión de Claves y Asociaciones de Seguridad. Los protocolos de AH y ESP son independientes de las técnicas de gestión de asociaciones de seguridad, aunque algunos servicios ofrecidos por estos protocolos (por ejemplo el servicio de anti-repetición) requieren gestión automática de las SAs.

La tercera versión de IPSec [3] utiliza IKEv2, las anteriores versiones son compatibles con ISAKMP (*Internet Security Association and Key Management Protocol*) y con IKEv1.

1.1.5.1 Protocolo de Gestión de Claves y Asociaciones de Seguridad en Internet (ISAKMP). ISAKMP utiliza conceptos de seguridad necesarios para el establecimiento de asociaciones de seguridad y claves criptográficas en el entorno de Internet. Este protocolo ofrece herramientas de generación de claves y de mitigación de amenazas (como por ejemplo, degeneración de servicio y ataques de reenvío), las cuales permiten a ISAKMP entablar y mantener comunicaciones seguras para protocolos de seguridad en un entorno de Internet. Para el caso de IPSec, este protocolo permite la negociación, establecimiento, modificación y cancelación de las Asociaciones de Seguridad.

ISAKMP difiere de otros protocolos de intercambios de claves debido a que separa las funciones de las gestiones de SAs de las de intercambio de claves; esto con el objetivo de facilitar una migración progresiva hacia mejores mecanismos y algoritmos.

La documentación sobre las fases de negociación, mecanismos de autenticación e intercambio de claves de este protocolo no son tema de estudio de este proyecto y pueden ser consultados en [10].

1.1.5.2 Internet Key Exchange (IKE)

- **IKE-v1.** Mientras ISAKMP proporciona un marco para la autenticación y el intercambio de claves, sin definirlo, IKEv1 define un protocolo de intercambio de claves que básicamente es una combinación de Oakley, SKEME e ISAKMP para la obtención de información de autenticación y claves [11].

Oakley describe una serie de intercambios de claves, llamados "modos", y detalla los servicios proporcionados por cada uno de ellos. SKEME describe una técnica de intercambio de claves que proporcionan anonimato, repudiabilidad, y renovación rápida de claves. El propósito de este protocolo híbrido es negociar y proporcionar el material autentificado para las SAs en un modo protegido.

Información más detallada sobre el funcionamiento de este protocolo no es objetivo de este proyecto y puede encontrarse en el RFC 2409 [11].

- **IKE-v2.** La segunda versión de IKE no es interoperable con la primera y fue realizada con el fin de definir completamente el protocolo, incorporando los contenidos de lo que eran previamente documentos separados como ISAKMP, IKE, el DOI (Interpretación de Dominio de Internet) [12], Traducción Transversal de Direcciones de Red (NAT-Transversal), Autenticación Heredada, Adquisición de Direcciones Remotas y Autenticación Extendible; también, se buscó simplificar IKE remplazando todos los intercambios iniciales con un solo tipo de intercambio [9].

Información más detallada sobre el funcionamiento de este protocolo puede ser encontrada en el RFC 4306 [13].

1.2 ALGORITMOS DE AUTENTICACIÓN Y CIFRADO

1.2.1 Introducción. Los algoritmos de autenticación y de cifrado son un componente esencial en la arquitectura de IPSec, ya que son estos, los que soportan cada uno de los servicios de seguridad que ofrece esta suite. La descripción que se hace a continuación contiene conceptos muy generales sobre

estos algoritmos y los términos relacionados con estos. Para un conocimiento más profundo de este tema en el contexto de seguridad, se recomienda la lectura de [1], [9].

1.2.2 Criptografía. La palabra criptografía proviene de dos palabras griegas "krypto" que significa oculto, y "logos" que significa estudio; en el contexto del presente proyecto una definición adecuada podría ser: "El arte de escribir con clave secreta o de un modo enigmático" [14]. Obviamente la criptografía hace años dejo de ser un arte para convertirse en un conjunto de técnicas que tratan sobre la protección de la información. Habitualmente se emplea este término para agrupar tanto la criptografía como el criptoanálisis.

Por otro lado, el cifrado es el proceso por el cual un mensaje de texto plano o legible se convierte en un mensaje ilegible o texto cifrado.

1.2.3 Cifrado Simétrico o Privado. En este tipo de cifrado tanto el emisor como el receptor del mensaje deben conocer la clave, con esta clave se pueden cifrar y descifrar los mensajes. Sus principales ventajas son:

- Longitud de clave relativamente reducida.
- Necesitan menos recursos computacionales que algoritmos asimétricos.
- Un cálculo de clave no requiere que cada parte sepa quién inicio el intercambio.
- Requiere menos ancho de banda que los algoritmos asimétricos.

Sus principales desventajas son:

- La simetría en el protocolo de administración de claves puede producir vulnerabilidad a ataques de tipo reflexión (*reflection attacks*).
- La clave es generada en un lado de la comunicación, si no se confía en este extremo, este método no sirve.

1.2.3.1 Cifrado en Bloque. La mayoría de los algoritmos simétricos se apoyan en conceptos de confusión que básicamente tratan de ocultar la relación entre el texto claro, el texto cifrado y la clave; y de difusión que tratan de repartir la influencia de cada unidad de información del mensaje original lo más posible en el mensaje

cifrado. Estos conceptos se combinan para dar lugar a los Cifrados de Producto [1].

Los principales algoritmos basados en cifrado en bloque son:

- **Triple DES.** Surge como mejora de DES, en 1988 se demostró que un ataque por fuerza bruta puede obtener la información en texto plano de DES. La debilidad se centra en el reducido tamaño de la clave, por lo cual, en 3DES se aumentó la clave a 192 bits, implementando DES en fila tres veces.

- **AES (*Advanced Encryption Standard*).** Es el algoritmo más utilizado por sistemas y personas en el mundo entero gracias a que sus procesos de selección, revisión y estudio se han efectuado en forma pública y abierta [15]. Este sistema de cifrado por bloques tiene un tamaño de bloque fijo de 128 bits y tamaños de llave de 128, 192 o 256 bits.

1.2.4 Cifrado Asimétrico. También conocido como cifrado de clave pública ya que cuenta con dos claves para la encriptación, de esta forma, se utiliza una clave para cifrar el mensaje (clave pública) y otra para descifrarlo (clave privada). Las claves públicas se reparten a las entidades con las cuales se desea establecer un canal seguro y los mensajes recibidos solo pueden ser descifrados con la clave privada. La importancia de este cifrado es el hecho de que existe una relación matemática entre estas dos claves, pero no se puede obtener una a partir de la otra.

El principal algoritmo utilizado por IPSec basado en cifrado asimétrico es el ICDH (Intercambio de Claves Diffie-Hellman*)* el cual es un esquema que permite a las partes comunicantes derivar una *clave* común sin la necesidad de establecer previamente una clave secreta entre ellas, todo a través de un canal inseguro.

1.2.5 Funciones de resumen o hash. Un paso importante en el establecimiento de una comunicación de red segura es la autenticación de la entidad en el otro extremo de la comunicación. En este contexto el término “autenticación” se debe entender como cualquier método que permita comprobar de manera segura alguna característica sobre un objeto, esta característica puede ser: su origen, su integridad, su identidad, etc.

Las funciones de resumen o hash generan un valor de resumen (hash) de algún flujo de datos, como una clave de manejo o sesión. Con el uso de estos algoritmos, las modificaciones que se le hagan a un flujo de datos pueden ser detectadas fácilmente, ya que si este hecho se produce, los valores de hash que se obtienen tanto en el emisor como en el receptor van a ser distintos.

Los principales algoritmos basados en funciones de resumen o hash son [16]:

- **Message Digest (MD5).** Algoritmo diseñado por Ron Rivest, el cual produce resúmenes o firmas de 128 bits, a partir de bloques de 512 bits del mensaje original. El mensaje original es rellenado hasta tanto se cumpla que la longitud de este sea 64 bits inferior a un múltiplo de 512. Este alargamiento se lleva a cabo añadiendo un "uno" seguido de tantos "ceros" como sea necesario. De esta forma se tiene el mensaje como un número entero de bloques de 512 bits.

- **Secure Hash Algorithm (SHA-1).** Este algoritmo fue desarrollado por la NSA (Agencia Nacional de Seguridad de USA), para ser incluido en el estándar DSS (Digital Signature Standard). Produce firmas de 160 bits, a partir de bloques de 512 bits del mensaje original. Este algoritmo es similar a MD5 ya que se inicializa igual a este añadiendo al final del mensaje un "uno" seguido de tantos "ceros" como sean necesarios hasta completar 448 bits en el último bloque. A diferencia de MD5, SHA-1 emplea cinco registros de 32 bits en lugar de cuatro.

- **SHA-2.** Es una función criptográfica hash diseñada por la NSA y publicada en 2001. SHA-2 consta de cuatro funciones hash con bloques de 224, 256, 384, 512 bits. Este algoritmo fue diseñado con el objetivo de superar las debilidades que aquejaban a su predecesor (SHA-1).

- **Hashed Message Authentication Codes (HMAC).** Es un algoritmo que consiste en aplicar una función resumen a la combinación de unos datos de entrada y una clave secreta, la cual es solo conocida por el emisor y el receptor. Como resultado se obtiene una cadena de caracteres que se conoce como extracto. De esta manera el resultado de la función resumen depende no solamente de la información de entrada sino también de una clave secreta, aumentando así el nivel de seguridad.

1.3 REDES INALÁMBRICAS WI-FI

1.3.1 Introducción. Para la definición de las redes de área local (LAN), la IEEE publica un conjunto de estándares de obligatorio cumplimiento para el caso de desarrollo de productos de red, con el fin de garantizar interoperabilidad entre los distintos fabricantes. Uno de estos estándares es el 802, incluyendo el 802.3 para redes cableadas y el 802.11 para redes inalámbricas.

1.3.2 Redes inalámbricas 802.11 (Wi-Fi). Este estándar fue definido en 1997 y define las redes de área local inalámbricas (WLAN) que operan en el espectro de 2.4 y 5 GHz. Originalmente este estándar aseguraba la interoperabilidad entre equipos de comunicación dentro de cada una de las tecnologías inalámbricas, pero no entre estas. Desde entonces, muchas especificaciones han sido definidas dentro del estándar 802.11, que definen distintas velocidades de transmisión [17].

En la Tabla 1.1 [17] se muestran las distintas especificaciones con sus características más importantes.

Tabla 1.1 Especificaciones que certifica Wi-Fi

Estándar	Frecuencia	Técnica de Modulación	Tasa de Transición nominal	Descripción
802.11ª	5 GHz	ODFM	54 Mbps	12 Canales no solapados. No ofrece QoS
802.11b	2.4 GHz	CCK, DSSS	11 Mbps	14 Canales solapados
802.11g	2.4 GHz	OFDM, CCK, DSSS	54 Mbps	14 Canales solapados, compatibilidad con 802.11b

Tabla 1.1 (Continuación)

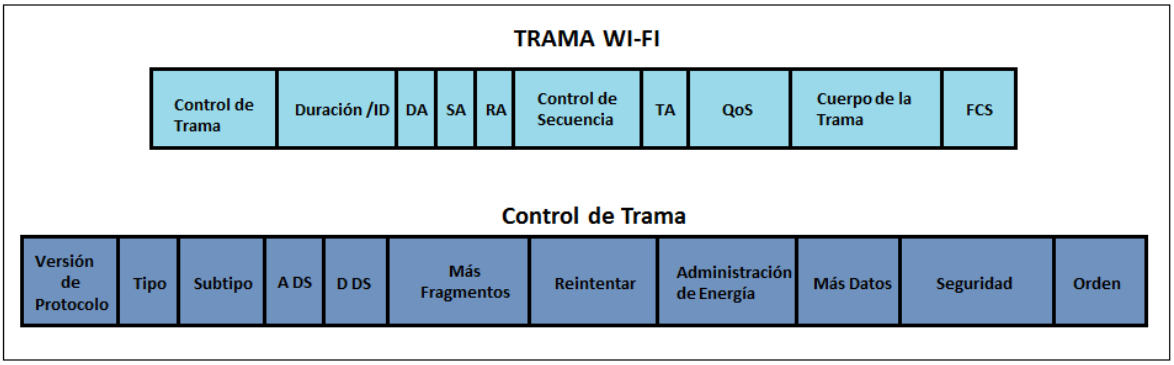
Estándar	Frecuencia	Técnica de Modulación	Tasa de Transición nominal	Descripción
802.11n	2.4 GHz 5 GHz	OFDM	54 – 600 Mbps	Mejora los estándares anteriores agregando MIMO que aprovecha transmisores múltiples para aumentar el rendimiento mediante multiplexación espacial

1.3.2.1 Trama Wi-Fi (802.11). Las LAN inalámbricas comparten un origen similar con las LAN Ethernet; sin embargo, hay diferencias importantes entre ellas (ver Tabla 1.2). Cuando se trabaja en ambientes inalámbricos, el entorno requiere consideraciones especiales. No existe una conexión física disponible, de esta forma existen muchos factores externos que pueden interferir en la transferencia de datos y se hace difícil controlar el acceso. El estándar para Wi-Fi incorpora controladores para superar estas dificultades.

Tabla 1.2 Diferencias entre Wi-Fi y Ethernet

Característica	802.11 LAN Inalámbrica	802.3 LAN Ethernet
Capa Física	Radiofrecuencia	Cable
Acceso al Medio	Prevención de Colisión	Detección de Colisiones
Disponibilidad	Cualquiera con una Radio NIC en el Rango de un Punto de Acceso	Se Requiere Conexión por Cable
Interferencia de Señal	Si	Irrelevante
Regulación	Estándar IEEE	Estándar IEEE

Figura 1.1 Trama Wi-Fi - 802.11



Wi-Fi es un sistema por contención que maneja un proceso de acceso múltiple por detección de portadora con evitación de colisiones (CSMA/CA). CSMA/CA especifica un procedimiento de postergación aleatorio para todos los nodos que están esperando transmitir. La oportunidad más probable para la contención del medio es el momento en que el medio está disponible.

Las redes 802.11 también utilizan Acuse de recibo de enlace de datos para confirmar que una trama se recibió con éxito. Si la estación transmisora no detecta la trama de reconocimiento, ya sea porque la trama de datos original o el reconocimiento no se recibieron intactos, se retransmite la trama. Este reconocimiento explícito supera la interferencia y otros problemas relacionados con la radio.

La trama 802.11 se muestra en la Figura 1.1. Esta trama contiene los siguientes campos:

- **Control de trama:** tipo de trama (tramas de datos, tramas de control o tramas administrativas), dentro del control de trama se encuentran los campos:
  - **Campo de versión del protocolo:** la versión de la trama 802.11 en uso.
  - **Campos tipo y subtipo:** identifica una de las tres funciones de la trama: control, datos y administración.
  - **Campo A DS:** establecido en 1 en las tramas de datos destinadas al sistema de distribución (dispositivos en la estructura inalámbrica).
  - **Campo Desde DS:** establecido en 1 en tramas de datos que salen del sistema de distribución.

  - **Campo Más fragmentos:** establecido en 1 para tramas que tienen otro fragmento.
  - **Campo Reintentar:** establecido en 1 si la trama es una retransmisión de una trama anterior.
  - **Campo Administración de energía:** establecido en 1 para indicar que un nodo estará en el modo ahorro de energía.
  - **Campo Más datos:** establecido en 1 para indicar a un nodo en el modo ahorro de energía que más tramas se guardan en la memoria del búfer de ese nodo.
  - **Campo Seguridad:** Define el tipo de seguridad a utilizar durante la comunicación. Este puede ser: WEP, WPA o WPA2.
  - **Campo Orden:** establecido en 1 en una trama de tipo datos que utiliza la clase de servicio Estrictamente ordenada (no requiere reordenamiento).
- **Campo Duración/ID:** según el tipo de trama, representa el tiempo, en microsegundos, requerido para transmitir la trama o una identidad de asociación (AID) para la estación que transmitió la trama.
- **Campo Dirección de destino (DA):** la dirección MAC del nodo de destino final en la red.
- **Campo Dirección de origen (SA):** la dirección MAC del nodo que inició la trama.
- **Campo Dirección del receptor (RA):** la dirección MAC que identifica al dispositivo inalámbrico que es el receptor inmediato de la trama.
- **Campo Dirección del transmisor (TA):** la dirección MAC que identifica al dispositivo inalámbrico que transmitió la trama.
- **Campo Control de calidad de servicio (QoS):** Define el tipo de ACK a utilizar en la comunicación y la prioridad de usuario de la trama.
- **Campo Número de secuencia:** indica el número de secuencia asignado a la trama; las tramas retransmitidas se identifican por números de secuencia duplicados.
- **Campo Número de fragmento:** indica el número de cada fragmento de la trama.
- **Campo Cuerpo de la trama:** contiene la información que se está transportando; para tramas de datos, generalmente un paquete IP.
- **Campo FCS:** contiene una verificación por redundancia cíclica (CRC) de 32 bits de la trama.

1.3.3 Infraestructura de la Red de Datos de la Universidad del Cauca. La Universidad del Cauca está dividida físicamente en las siguientes dependencias: Ingenierías, Artes, IPET, Medicina, Educación, El Carmen, Santo Domingo, Ciencias Contables, Las Guacas y Vicerrectoría de Investigaciones. En la Figura 1.2 se observa la topología de red y las conexiones físicas entre las respectivas dependencias.

La red de datos de la Universidad del Cauca está constituida fundamentalmente por una LAN extendida, la cual está basada en los estándares para redes de área local de la IEEE 802.3ab y 802.3z. Esta red posee una topología física de doble estrella, cuyos centros principales se encuentran ubicados en los edificios del IPET y de El Carmen. Todas las dependencias se interconectan con estos centros a través de un backbone de fibra óptica monomodo y multimodo. De igual forma aquellas dependencias que cuentan con dos o más edificios se interconectan entre sí por medio de fibra óptica.

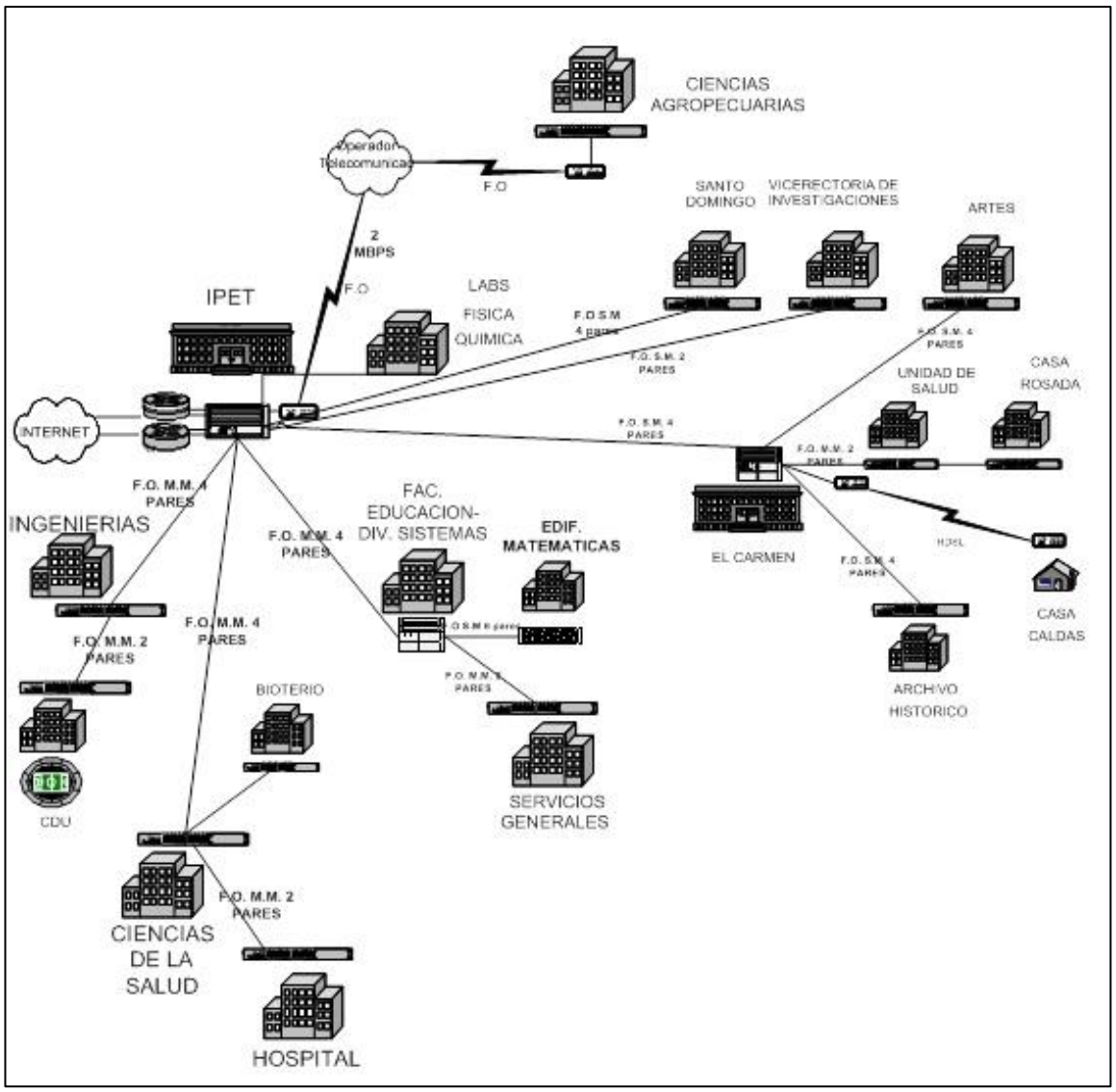
Aquellas sedes de la Universidad que están aisladas geográficamente tales como: Consultorio Jurídico, Ciencias Agropecuarias, Centro de salud Alfonso López y Santander de Quilichao se conectan a través del operador de comunicaciones por medio de canales dedicados de 2Mbps.

Todos los edificios de la universidad cuentan con un sistema de cableado estructurado que se basa en cable de par trenzado no-apantallado (Unshielded Twisted Pair - UTP) Categoría 5, categoría 6 y categoría 6ª. De igual manera cada edificio cuenta por lo menos con un centro principal de cableado estructurado (CC1), y en aquellos edificios en los cuales las distancias se hacen muy grandes se cuenta con centros secundarios de cableado (CC2, CC3, etc…). Estos centros secundarios se interconectan con el centro principal de cableado, con el fin de que los puntos de red abarquen la totalidad de puestos de trabajo dentro de la estructura.

Los puntos de red conectan estaciones de trabajo, impresoras y servidores a los equipos de transmisión de la red (switches de acceso y distribución).

La velocidad de transmisión con la que cuenta la red de datos en todas sus áreas (*Core*, Distribución y Acceso) actualmente es de 1Gbps, sin embargo, pronto se migrara a 10 Gbps en los enlaces principales.

Figura 1.2 Infraestructura de la red de datos de la Universidad del Cauca



1.3.3.1 Enlaces de Internet. La red de datos de la Universidad del Cauca cuenta en la actualidad[1] con 2 enlaces permanentes, uno principal y el otro secundario, que le brindan un total de 156 Mbps de acceso a Internet. El enlace principal es suministrado por la empresa EMTEL, con la cual se contrata un servicio de 91 Mbps, mientras que el enlace secundario es soportado por la empresa ETB (Empresa de Telecomunicaciones de Bogotá), con la cual se contrata un servicio de 65 Mbps.

[1] Fecha: Enero de 2012

1.3.3.2 Infraestructura cableada. La infraestructura de los equipos de red de la Red de Datos de la Universidad del Cauca se divide en tres áreas fundamentales las cuales son: core, distribución y acceso.

- *Core*: El core de la red de datos consiste en un Switch Cisco Catalyst 6509-E que brinda conexiones Ethernet y Gigabit Ethernet en sus puertos de cobre y fibra, y conexiones 10 Gigabit Ethernet en sus módulos de fibra.

- Distribución: Esta área de la red está compuesta por switches Cisco Catalyst 3750G que brindan conexiones Gigabit Ethernet a los equipos de acceso.

- Acceso: Este último segmento de la red está compuesto por switches Cisco 2950 y 2960G, los cuales suministran velocidades de acceso de 100Mbps y 1Gbps a los usuarios finales de la red.

1.3.3.3 Infraestructura inalámbrica. La Red de Datos de la Universidad del Cauca cuenta con una infraestructura inalámbrica basada en el sistema ***Mobile Edge*** **de Aruba**[2], el cual brinda una cobertura inalámbrica Wi-Fi dentro de cada uno de los edificios del campus universitario permitiéndole a los usuarios que así lo deseen, acceder de manera inalámbrica a todos los recursos que brinda la universidad. Este sistema trabaja con un rango amplio de APs (Puntos de Acceso) 802.11 a, b y g, tanto para interiores como para exteriores.

Los sistemas Mobile Edge de Aruba se basan en tres componentes:

- **Sistema Aruba OS:** Este software es el encargado de toda la inteligencia dentro del sistema Mobile Edge.

- **Controladores de Movilidad:** Son los equipos centrales dentro del sistema Mobile Edge. Estos equipos son los encargados de la distribución de datos dentro del sistema, así como de la gestión y el control de todos los APs relacionados con los mismos.

[2] Para mayor información visite: http://www.arubanetworks.com/

- **Access Points controlados:** Son los equipos encargados de llevar todo el tráfico generado por los usuarios finales hacia los Controladores de Movilidad, sobre redes LAN, WAN o Internet.

El controlador de movilidad con el que cuenta la Universidad del Cauca es el Aruba 3200 (ver Figura 1.3), el cual tiene una capacidad de 64 APs de campo y maneja puertos 10,100,1000 BASE-T. Los APs Aruba desplegados dentro del campus universitario son los siguientes: AP 60, AP 61, AP 121 y AP 125 (ver Figura 1.4); su distribución dentro del campus universitario se muestra en la Tabla 1.3. En la tabla 1.4, se muestra las principales características de los APs antes nombrados.

Tabla 1.3 Distribución de APs dentro de la red de la Universidad del Cauca

Sector	Numero de APs	Sectores/Oficinas que cubre
Sector de Educación	2	División de Sistemas
		Red de Datos
		Área de Equipos
		División de Comunicaciones
Sector Santo Domingo	4	Rectoría
		Paraninfo
		División Financiera
		División Recursos Humanos
		Prensa
		Secretaria General
		Vicerrectoría Académica
		Facultad de Derecho
		Vicerrectoría Administrativa
		Planeación
Sala Virtual	1	Sala Virtual
Instituto de postgrados en Ingeniería Electrónica y Telecomunicaciones	4	Facultad de Ingeniería Electrónica
		IPET
Instituto de postgrados en Ingeniería Civil	4	Facultad de Ingeniería Civil
		IPIC
Instituto de postgrados en Derecho y Contaduría	4	Casa Rosada

Tabla 1.3 (Continuación)

Sector	Numero de APs	Sectores/Oficinas que cubre
Facultad de Medicina	4	1er, 2do y 3er piso Facultad de Medicina
Bibliotecas	7	Biblioteca El Carmen
		Biblioteca Central
		Biblioteca Ciencias de la Salud
Derecho	6	Facultad de Derecho
Artes	2	Patio principal Artes
		Oficina profesores
Facultad de Ciencias Contables Económicas y Administrativas	6	Primer piso oficinas
		Segundo piso salones
		Tercer piso salones
		Cuarto piso salones

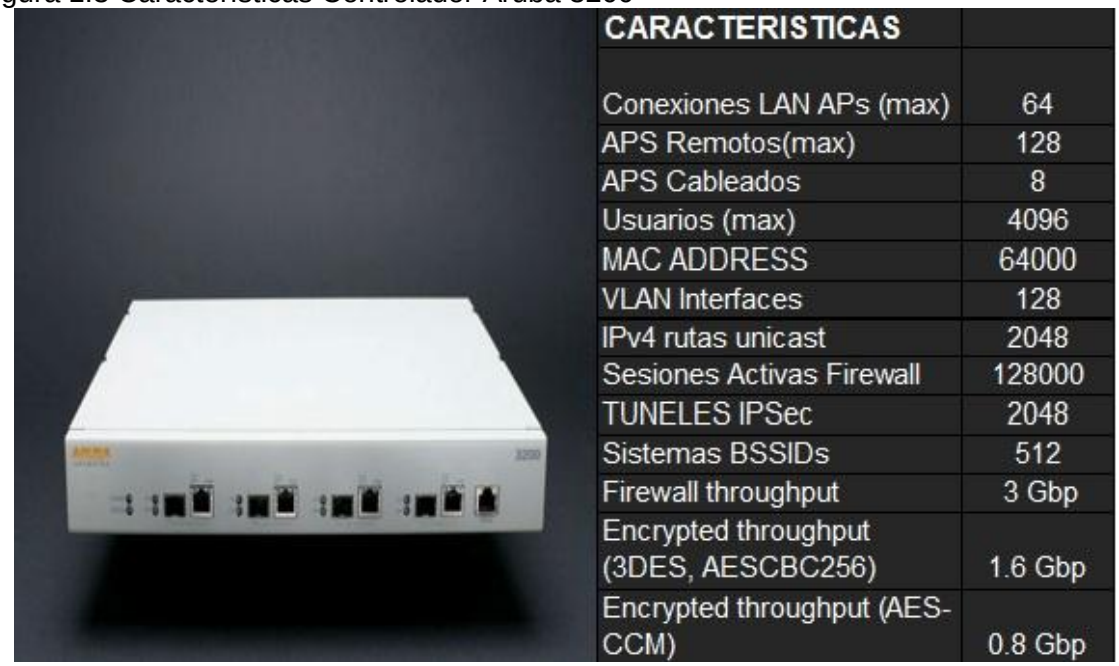
Tabla 1.4 Principales características Puntos de Acceso Aruba

Punto de Acceso	**APs 60-61**	**AP 121**	**AP 125**
Radios	Radio Única ConFigurable para 802.11a/b/g	Radio Única ConFigurable para Soportar 2,4GHz o 5GHz	Radio Dual ConFigurable para Bandas de 2,4 GHz y 5GHz
Gestión de RF	ARM-Adaptive Radio Management	ARM-Adaptive Radio Management	ARM-Adaptive Radio Management
Frecuencias de Trabajo	(5,15GHz - 5,950 GHz) (2,4GHz - 2,5 GHz)	(5,15GHz - 5,950 GHz) (2,4GHz - 2,5 GHz)	(5,15GHz - 5,950 GHz) (2,4GHz - 2,5 GHz)
Antena	doble dipolo integrado, omnidireccional, multibanda	triple dipolo omnidireccional MIMO con diversidad espacial	triple dipolo omnidireccional MIMO con diversidad espacial

Tabla 1.4 (Continuación)

Punto de Acceso	**APs 60-61**	**AP 121**	**AP 125**
Ganancia de Antena	(2,4 GHz-2,5 GHz / 2,8 dBi) - (5,150 GHz-5,350 GHz / 3,9 dBi) (5,950 GHz / 4,0 dBi)	(2,4 GHz-2,5 GHz / 3,2 dBi) - (5,150 GHz-5,350 GHz / 5,2 dBi)	(2,4 GHz-2,5 GHz / 3,2 dBi) - (5,150 GHz-5,350 GHz / 5,2 dBi)

Figura 1.3 Características Controlador Aruba 3200



CARACTERISTICAS	
Conexiones LAN APs (max)	64
APS Remotos(max)	128
APS Cableados	8
Usuarios (max)	4096
MAC ADDRESS	64000
VLAN Interfaces	128
IPv4 rutas unicast	2048
Sesiones Activas Firewall	128000
TUNELES IPSec	2048
Sistemas BSSIDs	512
Firewall throughput	3 Gbp
Encrypted throughput (3DES, AESCBC256)	1.6 Gbp
Encrypted throughput (AES-CCM)	0.8 Gbp

http://www.arubanetworks.com/pdf/products/DS_A3000.pdf

Figura 1.4 Puntos de Acceso Aruba

http://www.arubanetworks.com/products/access-points

2. PARÁMETROS PARA LA EVALUACIÓN DEL DESEMPEÑO DE REDES IP

2.1 DESEMPEÑO DE UNA RED

En la actualidad las redes IP están creciendo de una manera exponencial y con estas, los servicios que en ellas se ofrecen. Este hecho, sumado a que los usuarios finales de estas redes son cada día más exigentes, hace necesario que estas sean evaluadas de manera constante y permanente con el fin de poder obtener conclusiones claras, acerca del comportamiento en términos de desempeño que estas presenten. Medir el desempeño de Internet es difícil, sin embargo, se hace necesario si se requiere censar y cuantificar la percepción que puedan tener los administradores y usuarios de red acerca de este.

Visto de esta manera el problema se centra en qué y cómo medir este desempeño para verificar acuerdos que permitan el cumplimiento de los Acuerdos de Nivel de Servicio (SLA's), la facturación de servicios, la gestión de recursos, etc. Esto ha generado un desarrollo académico tanto en IETF con el grupo de trabajo IPPM y la ITU con el grupo de estudio número 12 (SG 12 - *Study Group 12*) con el fin de establecer un marco, una metodología y una terminología común para la medición del desempeño de una red IP.

2.1.1 Definición de Parámetros o Métricas. En la búsqueda de los parámetros o métricas (término utilizado en los RFCs por la IETF) generales de red, se observa que estos pueden ser definidos desde la Calidad de Servicio (QoS) o desde la Calidad de funcionamiento de la red (NP). La QoS según la recomendación de la ITU-T E.800 se define como "efecto global de las calidades de funcionamiento de un servicio que determinan el grado de satisfacción de un usuario al utilizar dicho servicio" [18], esta definición muestra un carácter subjetivo, es decir, que se debe tener en cuenta la opinión de usuarios que perciben el funcionamiento de los sistemas. La NP se mide en términos de parámetros significativos para el proveedor de red, estos parámetros brindan información que sirve para el diseño, configuración, explotación y mantenimiento de los sistemas de información, es independiente de los terminales y de la actuación de los usuarios [19].

El presente trabajo de grado busca obtener datos útiles para los administradores de red, particularmente los de la red de información de la Universidad del Cauca y no para los usuarios finales. Desde este punto de vista la evaluación realizada en

este proyecto se centra en la calidad de funcionamiento de la red que comúnmente se conoce como “desempeño” y no en la calidad del servicio.

Para poder identificar y organizar los posibles parámetros de calidad de funcionamiento de la red, la recomendación ITU-T I.350 “*Aspectos Generales de Calidad de Servicios y de Calidad de Funcionamiento en las Redes Digitales Incluidas las Redes Digitales de Servicios de Servicios Integrados*” [19], ofrece un método sistemático que consiste en una matriz 3x3. En esta matriz las columnas identifican criterios básicos que describen la calidad de funcionamiento de esta forma:

- Velocidad: Básicamente es una descripción del tiempo que es utilizado para realizar algún tipo de función aunque esta función se realice o no con la precisión deseada.

- Precisión: Describe el grado de corrección con que se realiza la función, aunque esta puede realizarse o no con la velocidad deseada.

- Seguridad: Describe el grado de certidumbre con que se realiza la función, independiente de la velocidad o precisión.

Tabla 2.1 Calidad de funcionamiento de la RDSI de banda estrecha y de banda ancha, IP y GII

Narrow-band and Broadband ISDN, IP and GII Performance (including physical layer digital transmission performance)			
Criteria / Function	**Speed**	**Accuracy**	**Dependability**
Access	**I.352 (N-ISDN - CKT) I.354 (N-ISDN - PKT) I.358 (B-ISDN) Y.1530 (IP)**	**I.354 (N-ISDN - PKT) I.358 (B-ISDN) I.359 (N-ISDN - CKT) Y.1530 (IP)**	**I.354 (N-ISDN - PKT) I.358 (B-ISDN) I.359 (N-ISDN - CKT) Y.1530 (IP)**
Information Transfer	**I.354 (N-ISDN - PKT) I.356 (ATM) Y.1540 (IP) Y.1541 (IP)**	**G.821(CKT) G.826 (CKT) G.828 (CKT) G.829 (CKT) I.354 (N-ISDN - PKT) I.356 (ATM) I.35AAL (AAL) Y.1540 (IP) Y.1541 (IP)**	**I.354 (N-ISDN - PKT) I.356 (ATM) Y.1540 (IP) Y.1541 (IP)**

Tabla 2.1 (Continuación)

Criteria / Function	Speed	Accuracy	Dependability
Disengagement	**I.352 (N-ISDN - CKT) I.354 (N-ISDN - PKT) I.358 (B-ISDN) Y.1530 (IP)**	**I.354 (N-ISDN - PKT) I.358 (B-ISDN) I.359 (N-ISDN - CKT) Y.1530 (IP)**	**I.354 (N-ISDN - PKT) I.358 (B-ISDN) I.359 (N-ISDN - CKT) Y.1530 (IP)**

ITU-T I.350 "*Aspectos Generales de Calidad de Servicios y de Calidad de Funcionamiento en las Redes Digitales Incluidas las Redes Digitales de Servicios de Servicios Integrados*"

Cada fila de esta matriz representa una de las tres funciones básicas y distintivas de comunicación (acceso, transferencia de información de usuario y desvinculación). La evaluación realizada en este proyecto se hace en la fase de transferencia de información ya que en el caso de la ITU-T los parámetros de red se definen en las recomendaciones Y.1540 y Y.1541, donde se especifica que su alcance se encuentra en la función de comunicación de transferencia de información de usuario como se puede observar en la Tabla 2.1, además, el número de paquetes en las fases de conexión y desvinculación son muy pequeños y no afectan de manera significativa el desempeño de red. En IPSec estas fases se realizan cuando una asociación de seguridad caduca, cada 86400 segundos (24 horas) [13].

Por esta razón, no se evaluó el impacto de las diferentes configuraciones de protocolos de gestión de claves y asociaciones de seguridad utilizados por IPSec para las fases de conexión y desvinculación.

2.1.2 Métricas para el Desempeño IP. Los trabajos en la definición de los parámetros de red que desde ahora se llamaran métricas son realizados más a fondo por el grupo IPPM de la IETF en la RCF 2330, donde se definen las métricas como cantidades relacionadas con el rendimiento y fiabilidad que pueden ser correctamente cuantificadas [20]. En este RFC se hace referencia a la dificultad de la medición de algunas métricas, aunque no es permitido darle significados ambiguos.

A continuación se nombraran las características que deben cumplir este tipo de métricas para la correcta descripción de redes IP.

- Las unidades de medidas deben estar expresadas en metros y segundos aunque están permitidas las unidades relacionadas basadas en miles y milésimas.

- Cuando una unidad sea expresada como combinación de unidades, también las unidades basadas en miles y milésimas son aceptadas, pero todas las miles y milésimas deben ser agrupadas al comienzo.

- Cuando se utilizan prefijos de métricas con bits o combinaciones que incluyen bits, estos prefijos tendrán su significado métrico relacionado a 1000 y no a 1024 que es el significado convencional de almacenamiento computacional.

- Cuando se hable en términos de tiempo, este será expresado en Tiempo Universal Coordinado (UTC).

También se deben tener en cuenta los siguientes criterios para la definición de una métrica:

- La métrica debe ser concreta y bien definida.

- La metodología para obtener una métrica debe tener la propiedad de ser repetible: Si la metodología es usada múltiples veces bajo las mismas condiciones los resultados deben ser los mismos.

- Las métricas no deben exhibir parcialidad para redes IP implementadas con la misma tecnología.

- Las métricas deben ser útiles, tanto para usuarios como para proveedores de servicios, para comprender el desempeño de red que experimentan o proveen.

- Las métricas deben tener características de auto-consistencia, es decir que en la medición de parámetros se deben hacer mínimas suposiciones mientras se pueda.

- Se recomienda que la definición de una métrica se de en términos de tipo determinísticos, en contraposición al uso de definiciones de tipo estocásticas (probabilidades).

2.1.3 Clasificación de Métricas. La clasificación de las métricas de desempeño se hace con referencia a trabajos realizados por el grupo IPPM y es plasmada en [17]. En estos términos se pueden clasificar las métricas en:

- Métrica Individual: Hace referencia a métricas de tipo atómicas. Un ejemplo podría ser el retardo que sufre un solo paquete al ser enviado de un host a otro.

- Métrica de Muestra: Son métricas derivadas de una métrica individual y son generadas al tomar un número determinado de estas instancias individuales. Por ejemplo: se puede definir una métrica de muestra de retardo en un sentido desde un host a otro como el equivalente a una hora de mediciones, realizadas en intervalos de Poisson en un espaciamiento medio de un segundo.

- Métrica Estadística: Se refiere a métricas que son derivadas de una métrica de muestra por una función estadística aplicada a los valores de la métrica individual en la muestra. Por ejemplo: el valor medio de retardo sobre una muestra dada.

Además, las métricas se pueden clasificar en métricas analíticas y empíricas:

- Métricas Analíticas: Son aquellas métricas que son definidas bajo un marco analítico de conceptos llamado marco analítico o A-Frame, el cual tiene como objetivo principal la caracterización de las redes de internet de manera práctica y analítica, a fin de que los estudios no empíricos que se lleven a cabo por medio de análisis y simulaciones se relacionen de la mejor manera posible con el comportamiento real de este tipo de redes. Ejemplos de estas métricas son: tiempo de propagación de un enlace, ancho de banda de un enlace para paquetes de un tamaño k, número de saltos de una ruta, etc.

- Métricas Empíricas: Son aquellas métricas, que por falta de detalles dentro del marco de referencia A-Frame, no pueden ser consideradas como analíticas. Estas métricas deben cumplir estas dos propiedades:

    - Estar definidas en términos de los componentes de Internet.
    - Tiene que existir al menos un medio efectivo para medirlas.

Para cada métrica, sea analítica o empírica, existen dos tipos de composición las cuales son:

- Composición Espacial: La composición espacial hace referencia a la característica presente en algunas métricas de desempeño, que permite que estas puedan definir el comportamiento de una ruta ya sea por medio de la evaluación completa de la misma o por la evaluación de secciones más pequeñas resultado de la división de esta. Una definición de una métrica espacial debe incluir:

    - La hipótesis especifica aplicada a esta métrica.
    - Análisis de como la hipótesis podría ser incorrecta.
    - Una justificación de una posible medición incorrecta si no se divide la ruta.

- Composición Temporal: Hace referencia a la característica que pueden presentar ciertas métricas de desempeño, según la cual, puede existir una relación entre una muestra tomada en un tiempo T y otras muestras tomadas en tiempos inferiores a este de la forma $t0 < t1 <\ldots< tn < T$. Una definición de una métrica temporal debe incluir:

    - La hipótesis especifica aplicada a cada métrica.
    - Una justificación de la utilidad de la composición en términos de la exactitud que pueda llegar a alcanzarse al aplicar esta.
    - Una justificación de la utilidad de la composición en términos de la efectividad que puede llegar a alcanzarse al realizar análisis basándose en los conceptos A-Frame.

2.1.4 Definición de Métricas de Desempeño. La recomendación ITU-T Y.1543 define un grupo de métricas para caracterizar el desempeño de una red, con sus

equivalentes en la recomendación Y.1540 y su RFC correspondiente. A continuación se presentan cada una de ellas:

- **Retardo medio en un sentido (*Mean one-way delay*)**
  - *IP packet transfer delay* (IPTD) – ITU-T Y.1540
  - *A One-way Delay Metric for IPPM* - RFC 2679

- **Variación de retardo en un sentido (*One-way packet delay variation*)**
  - *End-to-end 2-point IP packet delay variation* (PDV) – ITU-T Y.1540
  - *IP Packet Delay Variation Metric for IP Performance Metrics* - RFC 3393

- **Tasa de pérdida de paquetes (*IP packet loss ratio*)**
  - *IP packet loss ratio* (IPLR) – ITU-T Y.1540
  - *A One-way Packet Loss Metric for IPPM* - RFC 2680

- **Indisponibilidad de la ruta (*Path unavailability*)**
  - Función de disponibilidad de un servicio IP – ITU-T Y.1540
  - *IPPM Metrics for Measuring Connectivity* - RFC 2678

Según lo descrito en la recomendación Y.1543 estas métricas deben medirse en un sentido y no deben estar orientados a la conexión [21], hecho que se justifica por las siguientes razones:

- El camino desde un host fuente a un host destino generalmente es distinto al camino usado en el sentido contrario (características del enrutamiento IP); de esta forma si se mide el retardo ida y vuelta es muy probable que se mida el retardo de caminos distintos.

- Los ISPs tienen políticas de calidad de servicios distintas para los enlaces de subida y bajada; de esta forma aunque los caminos sean los mismos en una medición ida y vuelta las métricas tendrían diferentes características para cada sentido de comunicación.

- El desempeño de las aplicaciones y protocolos de niveles superiores depende del desempeño en una dirección.

El *throughput* de aplicación depende de muchos parámetros incluyendo la pérdida de paquetes, el retardo de tránsito y muchos otros factores que no pueden ser controlados por el proveedor de servicios; por estas razones el *throughput* de aplicación por sí mismo no cumple con las características de las métricas para la medición del desempeño de redes IP. Adicionalmente otras métricas definidas en la recomendación ITU-T Y.1540 pueden ser útiles, sin embargo, el valor que aportan sobre las métricas nombradas arriba no justifica la complejidad adicional que requieren para especificarse, implementarse y desplegarse; esta recomendación indica que con el tiempo se puede demostrar lo contrario y de esta forma agregar otras métricas básicas para la medición Internet [22].

2.1.5 Métricas Principales

2.1.5.1 Retardo Medio en un Sentido (Mean One-Way Delay). Métrica definida según la ITU-T en la recomendación Y.1540 como la diferencia temporal *t2 – t1* para todos los paquetes exitosos y erróneos que lleguen a un DTE (*Data Terminal Equipment*), donde *t1* es el momento en que sale el paquete de la interfaz del DTE emisor y *t2* es el momento en que llega a la interfaz del receptor [23]. La IETF la define como el tiempo que trascurre entre el envío del primer bit de un paquete de prueba en el dispositivo fuente y la llegada del último bit al dispositivo de destino [24].

Es una métrica muy importante no solo por lo que representa en sí misma, sino por múltiples razones, algunas de las cuales se mencionan a continuación:

- Algunas aplicaciones no funcionan bien si el retardo supera ciertos umbrales propios de la aplicación.
- El retardo y su variación irregular hace difícil (o imposible) soportar servicios de tiempo real como telefonía y televisión IP.
- Entre más altos sean los valores de retardo, más difícil es para los protocolos de la capa de transporte sostener altos anchos de banda.
- El valor mínimo de esta métrica brinda información del retardo por propagación y el retardo de transmisión.
- Los valores de retardo por encima del mínimo indican congestión en el trayecto.

2.1.5.2 Variación de Retardo en un Sentido (One-Way Packet Delay Variation). Existen muchas formas de encontrar la variación de retardo presente en las redes IP; tanto la ITU-T como la IETF han establecido distintas especificaciones a fin de definir esta métrica. Por un lado la IETF maneja los RFC 3393 y 3550, mientras por el otro la ITU-T trabaja con las especificaciones Y.1540 y G.1020.

La variación de retardo es una métrica derivada, ya que basa su comportamiento en otra métrica fundamental (retardo en un sentido). La variación de retardo es calculada ya sea mediante la comparación sucesiva de retardos entre dos paquetes dentro de una muestra o por medio de la comparación entre cada uno de los retardos encontrados en una muestra y una referencia previamente seleccionada [25].

Dos especificaciones, las cuales son equivalentes entre si [25], han sido ampliamente aceptadas y desplegadas en la industria:

- **Inter Packet Delay Variation, IPDV (RFC 3393):** En este caso la referencia es el paquete inmediatamente anterior (teniendo en cuenta la secuencia de envío), y esta referencia es distinta para cada paquete dentro de un flujo de información. El IPDV es la diferencia entre los retardos en un sentido obtenidos para dos paquetes específicos dentro de un flujo de datos [26].

- **Packet Delay Variation, PDV (Y.1540):** En este caso una sola referencia es tomada en cuenta, la cual es seleccionada basada en criterios específicos. El criterio más usado para encontrar la referencia es el del paquete con el retardo más bajo. El PDV, por consiguiente, es la diferencia entre cada paquete de una muestra y la referencia correspondiente a esta muestra [22].

Algunas de las razones por las cuales es importante cuantificar esta métrica son las siguientes:

- Es utilizada para definir el tamaño de *buffers* para aplicaciones que requieren entregas regulares de paquetes, por ejemplo voz y video en tiempo real.

- El valor de la variación de retardo es utilizado para conocer la dinámica de las colas en los enrutadores o en las redes, donde estas variaciones de

retardo pueden estar relacionadas con los cambios en las longitudes de las colas en un vínculo dado o en una combinación de enlaces.

2.1.5.3 Tasa de Pérdida de Paquetes IP (IP Packet Lost Ratio). La recomendación ITU-T Y.1540 define esta métrica como la razón entre los paquetes enviados y los paquetes perdidos en una población de interés. Para esto se establece un tiempo, *Tmax,* que debe ser lo suficientemente grande para diferenciar un paquete retrasado de uno perdido, en la práctica este tiempo es de 10 segundos o más.

Esta métrica es en gran medida sensible a las tecnologías de acceso, anchos de banda, número de saltos y distancia; los objetivos se pueden ajustar a la ubicación final del lugar de estudio.

Esta métrica es particularmente importante por su impacto en la calidad o rendimiento de la red y para aplicaciones no elásticas de tiempo real como voz y video.

2.1.5.4 Indisponibilidad de ruta (Path Unavailability). Métrica relacionada estrechamente con la tasa de pérdida de paquetes. En la recomendación Y.1543 se especifica que una ruta se considera indisponible si hay una pérdida excesiva de paquetes (IPLR > 75%) sobre un intervalo de tiempo fijo de 5 minutos.

Adicionalmente, en el RFC 2678 se definen los parámetros para conectividad instantánea unidireccional y bidireccional que pueden ser usados para evaluar la conectividad a través del tiempo [27], similar a la función de disponibilidad del servicio de Y.1540.

2.2 REQUERIMIENTOS PARA LA MEDICIÓN DEL DESEMPEÑO

El concepto Inter-Domain QoS referenciado en [21], está diseñado para aumentar la confianza en las características de servicio que se espera para las redes de nueva generación. Una parte integral de aumentar esta confianza consiste en la medición continua de los parámetros de red. El objetivo de tomar mediciones es proporcionar información a clientes, clientes potenciales y proveedores del servicio.

La recomendación de la ITU-T Y.1543 especifica algunos requerimientos que deben cumplir las medidas de la calidad del funcionamiento:

- Todas las mediciones deben ser unidireccionales, pero se pueden hacer las mediciones en dos sentidos para estimar una calidad de funcionamiento bidireccional.

- Las medidas tomadas en cada segmento del camino pueden ser combinadas para formar métricas multi-segmento, sitio-a-sitio, borde-a-borde o terminal a terminal [21].

Además, se habla de los dos tipos de metodologías de medición: activa y pasiva.

2.2.1 Medición Activa. Para este tipo de medición se deben inyectar paquetes de prueba en ciertos dispositivos de la red, los cuales son enviados a dispositivos extractores que devuelven información al dispositivo inyector para cuantificar las métricas de desempeño.

Los principales requerimientos para los paquetes de prueba son los siguientes:

- Protocolo de nivel superior UDP-Echo.

- Utilizable para mediciones de retardo y pérdida de paquetes, de preferencia en ambas direcciones entre los dos dispositivos.

- Estar marcados con el correspondiente DSCP en la cabecera y en el payload.

- Los paquetes deben ser marcados con *time-stamp* en dispositivos de inyección y extracción.

- Preferiblemente marcados con las direcciones de origen y destino de las fuentes, para minimizar el impacto del balanceo de carga.

- Se debe tener la capacidad de indicar la confiabilidad en la sincronización de reloj.

La recomendación Y.1543 también plantea una serie de recomendaciones más profundas respecto a los procedimientos de medición:

- Para medir el retardo medio en un sentido: se deben recolectar las medidas para cada periodo de *rollup*[3], descartar las medidas de los periodos de indisponibilidad, sumar todas las medidas de retardo de paquetes exitosos y dividirla entre el número de ellos.

- Para medir la variación de retardo en un sentido se calculan los percentiles (DV90, DV99, DV99.9) y se le resta el retardo mínimo del periodo de rollup. Para QoS más estrictas debe utilizar DV99.9, para otras QoS menos exigentes se pueden utilizar percentiles más bajos.

- La tasa de pérdidas de paquetes se debe calcular con la siguiente ecuación:

$$PLR = \frac{paquetes\ perdidos + paquetes\ llegados\ despues\ del\ tiempo\ maximo\ de\ espera}{numero\ de\ paquetes\ generados}$$

La indisponibilidad de ruta la determina un IPLR > 75% en un periodo de rollup.

2.2.2 Medición Pasiva. Al utilizar este tipo de medición no se inyecta tráfico adicional a la red sino que se monitorean las métricas en dispositivos de las redes residentes o entidades de medición independiente.

Los requerimientos para este tipo de medición son los siguientes:

- Cada medición debe tener al menos direcciones de origen y destino, un tipo de QoS asociado, y tiempo exacto de inicio y finalización.
- Se debe hacer copia del tráfico analizado sin afectar el tráfico original.
- Se debe clasificar el tráfico de diferentes granularidades.
- Se deben soportar métodos probabilísticos y muestreo hash.
- Se debe realizar la operación de muestreo a la velocidad-del-cable.
- Se deben soportar métodos de muestreo basados en flujo.
- Se debería soportar muestreo antes y después de la clasificación.

[3] Rollup: Término que hace referencia al tiempo necesario para realizar una prueba de medición.

- Se debe soportar la medición del desempeño de paquetes fragmentados.
- Se debe poder medir paquetes de cualquier tamaño hasta el tamaño de MTU máximo para la ruta analizada.

Los procedimientos para una medición pasiva implican el uso de dos dispositivos de medición que extraen una copia de los datos para crear una base de datos de paquetes para su posterior análisis, a diferencia de la medición activa, en la cual las rutas pueden cambiar durante el periodo de medición.

2.2.3 Métodos de Recolección de Muestras. Para el análisis de desempeño existen dos clases de métodos para la recolección de muestras: la recolección periódica y la recolección aleatoria.

2.2.3.1 Periódica. Definido en por la IETF en el RFC 3432, en donde la toma de muestras se hace de forma periódica y se hace especialmente útil por las siguientes razones [28]:

- Se puede aplicar a mediciones activas y pasivas.
- Se simplifica el análisis en el dominio de la frecuencia.
- Las mediciones activas pueden ser configuradas para que coincidan con los flujos de datos de los medios de comunicación, de esta forma se simplifica la estimación del rendimiento de las aplicaciones.

El RFC también señala los siguientes problemas potenciales para el muestreo periódico:

- Si la métrica evaluada presenta un comportamiento periódico es probable que se esté haciendo un análisis de solo una parte del comportamiento.

- La acción misma de medir puede perturbar de alguna manera lo que se está midiendo en determinado momento.

2.2.3.2 Aleatoria. Basada en el "muestreo aditivamente aleatorio" [18], donde las muestras están separadas por intervalos independientes, generados al azar con una distribución estadística común G(t).

El muestreo aditivamente aleatorio ofrece las siguientes ventajas respecto al muestreo periódico:

- Evita efectos de sincronización.
- Evita efectos de estimación no parcial del rendimiento de la propiedad evaluada.

Las dificultades de este tipo de muestreo son:

- El análisis en frecuencia ya que las muestras no se producen en intervalos fijos como en los asumidos por la transformada de Fourier.
- En la distribución estadística G(t), el muestreo contiene segmentos predecibles.

2.3 CONSIDERACIONES DE TIEMPO

El RFC 2330 [18] hace referencia de la necesidad de cuantificar los distintos tipos de errores presentes en las evaluaciones de una determinada métrica. Para el proyecto los errores más importantes se presentan en las imperfecciones en la obtención de tiempo o imperfecciones de reloj. A continuación se nombraran los parámetros para la caracterización de los relojes.

- *Offset* de reloj: En un momento determinado se define como la diferencia entre el tiempo reportado por el reloj y el tiempo verdadero determinado por el UTC.

$$offset = T_{clock} - T_{true}$$

- Precisión de Reloj: Es un valor que define cuan cerca está el valor absoluto de *offset* de cero.

- *Sken* o asimetría de reloj: En un momento determinado es la diferencia de frecuencia entre el reloj y el tiempo verdadero.

- *Drift:* se define como la segunda derivada de *offset* de reloj con respecto al verdadero tiempo.

- Resolución de reloj: es la menor unidad para la cual el reloj es actualizado. Este valor representa el límite inferior de incertidumbre de reloj.

- Sincronización: si dos relojes están precisos uno con respecto a otro (caso ideal), se dice que estos relojes están sincronizados.

$$T_{reloj\ 1} - T_{reloj\ 2} = 0$$

El valor de los parámetros anteriormente descritos depende de manera crítica del protocolo que se utilice para la sincronización de los relojes. En el proyecto se utilizó el protocolo de tiempo de red NTP (*Network Time Protocol*).

Entre las escalas de tiempo más relevantes utilizadas para las mediciones realizadas en este proyecto se encuentra la unidad de tiempo de medición "rollup" de 5 minutos [21], estudios han revelado que este valor es consistente con los límites prácticos sobre las operaciones de la capa IP. La recomendación Y.1541 sugiere que la evaluación para el retardo, variación de retardo y la tasa de pérdida de paquetes sea de un minuto, además, se hace énfasis en la importancia de realizar las mediciones en los mismos intervalos de tiempo con las mismas condiciones.

2.4 CONSIDERACIONES DE LOS PAQUETES DE INFORMACIÓN

La IETF en el RFC 2330 lista una serie de requisitos que deben cumplir los paquetes de prueba tipo P o sondas para la medición de las métricas los cuales son:

- El tamaño indicado en la cabecera IP corresponde al tamaño de la cabecera IP más el tamaño de la carga útil.
- No se permite la fragmentación del paquete.
- Las direcciones de origen y destino deben corresponder a los host en cuestión.
- No deben contener opciones de Internet a menos que se indique explícitamente.
- Tener un valor de TTL suficiente para viajar desde el origen al destino.

- Si una cabecera de transporte está presente, este debe contener una suma de verificación y demás campos válidos.
- Si un paquete se describe como que tiene una longitud en octetos “B” donde

$$0 \leq 65535 \leq B$$

Y si B es la longitud de la carga útil en octetos, entonces B ≤ 65535 (tamaño de la cabecera IP en bytes)

Se debe tener en cuenta un tipo especial de paquete el “paquete mínimo de A hasta B” el cual debe tener las siguientes propiedades.

- El tamaño de datos del payload es 0 bytes.
- No debe contener opciones.

Aunque sería importante caracterizar todo tipo de tráfico y QoS para cada uno de ellos, esto implicaría una cantidad de mediciones grande. La recomendación de la ITU-T Y.1541 sugiere que todas las mediciones deben hacerse con un tamaño de campo de información fijo de 160 o 1500 octetos, este último tamaño se utiliza en especial para pruebas en capas inferiores como la medición de errores de bit.

2.5 HERRAMIENTAS DE MEDICIÓN

Para la selección de la herramienta que permitiera la medición de las distintas métricas para la evaluación de desempeño de forma confiable, se consideraron como criterios los conceptos anteriormente descritos. En la tabla 2.2, se realiza un listado de herramientas software que se tuvieron en cuenta para esta selección.

Tabla 2.2 Herramientas para medición del desempeño de red

Herramienta	Enlace
1. Netperf	http://www.netperf.org/netperf/
2. D-ITG	http://www.grid.unina.it/software/ITG/
3. NetStress	http://www.performancewifi.net/performance-wifi/main/NetStress.htm
4. MGEN	http://cs.itd.nrl.navy.mil/work/mgen/
5. LANforge	http://www.upname.com/domain/AnForge.org

Tabla 2.2 (Continuación)

Herramienta	Enlace
6. Network Traffic Generator	http://sourceforge.net/projects/traffic/
7. Rude & Crude	http://rude.sourceforge.net/
8. WlanTV	http://sourceforge.net/projects/wlantv/
9. Packit	http://www.packit.com/
10. Bandwidth	http://bandwidthd.sourceforge.net/
11. Netcat	http://netcat.sourceforge.net/
12. iprf	http://iperf.sourceforge.net/
13. OWAMP	http://www.internet2.edu/performance/owamp/
14. Ngrep	http://ngrep.sourceforge.net/
15. Wireshark	http://www.wireshark.org
16. Ethereal	http://www.ethereal.com/
17. Smokeping	http://oss.oetiker.ch/smokeping/
18. MRTG	http://www.mrtg.jp/en/es_es/
19. Nagios	http://www.nagios.org/
20. Rrdtool y Cacti	http://www.cacti.net/
21. NTOP	http://www.ntop.org/news.php
22. NetCPS	http://www.netchain.com/netcps/
23. Ping	http://linux.die.net/man/8/ping

Al hacer la selección de las distintas herramientas, algunas muestran limitaciones para la implementación de algunos escenarios; por otra parte, la mayoría de ellas han sido desarrolladas sin tener en cuenta lineamientos claros como un estándar por lo que las medidas realizadas no resultan confiables para la medición de métricas de desempeño de red. Por otra parte, la herramienta D-ITG permite medir los parámetros de red de forma muy precisa bajos los lineamientos de la ITU-T y la IETF. Esta herramienta tiene un módulo generador de tráfico que permite una evaluación bajo las características de diferentes tipos de tráfico como datos, video y VoIP.

2.5.1 Distributed Internet Traffic Generator (D-ITG). D-ITG es un generador de tráfico de código abierto y una herramienta para el análisis y evaluación del desempeño de redes IP, el cual basa su funcionamiento en el modelamiento de tráfico de Internet, por medio de la variación de los tiempos de partida entre

paquetes y el tamaño de los mismos [29]. A partir de una evaluación paquete por paquete del tráfico generado, la herramienta D-ITG brinda las siguientes métricas:

- Retardo medio en un sentido
- Retardo medio de ida y vuelta
- Variación de Retardo
- Tasa de pérdida de paquetes

D-ITG se basa en el modelo cliente-servidor y su arquitectura se compone de los siguientes elementos:

- **ITGSend:** Hace las veces de cliente y es el encargado de enviar los flujos de datos hacia el servidor.

- **ITGRecv:** Hace las veces de servidor y su misión es la de recibir y aceptar peticiones de comunicación por parte de los clientes.

- **ITGLog:** Este elemento actúa como servidor de registro y se encarga de recibir información tanto del cliente como del servidor.

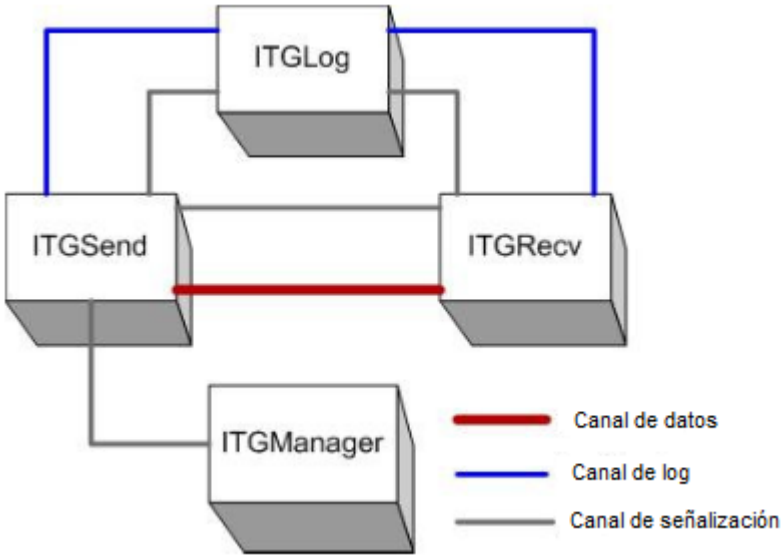
- **ITGManager:** Permite el control de sesiones de manera remota.

- **ITGDec:** Es el encargado de analizar la información recolectada en ITGLog y obtener las métricas de desempeño (Retardo medio en un sentido y de ida y vuelta, Variación de retardo, Tasa de pérdida de paquetes y *Throughput*).

- **TSP (Traffic Specification Protocol):** Es el protocolo sobre el cual se soporta la herramienta D-ITG. Sus principales funciones son:

    - Permitir la negociación entre el cliente y el servidor, acerca de que parámetros se va a usar durante las pruebas
    - Crear una conexión entre el cliente y el servidor
    - Autenticar el receptor
    - Cerrar una conexión entre el cliente y el servidor
    - Detectar eventos

Figura 2.1 Arquitectura de D-ITG.



Università degli Studi di Napoli "Federico II"

- Canal de señalización: Canal TCP utilizado por el protocolo TSP para la comunicación entre el cliente y el servidor.

Esta herramienta no cuenta con sistema propio de sincronización entre el cliente y el servidor, por lo que se hace necesario utilizar algún mecanismo externo como NTP o GPS, para obtener resultados confiables y precisos.

Las características de esta herramienta que motivaron su elección fueron las siguientes:

- Permite realizar pruebas de retardo en un sentido.
- Es de código abierto y gratuita.
- Tiene la capacidad de modelar de manera muy aproximada gran variedad de flujos de tráfico [29].
- Permite establecer conexiones tanto UDP como TCP.
- Cumple con todas las métricas de desempeño definidas en la sección 2.1.2.
- Permite establecer tiempos aleatorios de partida, lo que ayuda a evitar el análisis de comportamientos periódicos sobre redes IP.
- Define tiempos exactos para la realización de pruebas, hecho que posibilita el establecimiento del tiempo de *rollup* que se recomienda en [21].
- Soporte multiplataforma (Linux y Windows).

3. EVALUACIÓN DEL DESEMPEÑO DE LOS PROTOCOLOS DE SEGURIDAD PROPICIADOS POR IPSEC EN LA RED INALÁMBRICA WI-FI DE LA UNIVERSIDAD DEL CAUCA

3.1 INTRODUCCIÓN

Para la evaluación del desempeño de la red inalámbrica WI-FI de la Universidad del Cauca se implementaron los servicios de Integridad con Autenticación y Confidencialidad. Para la implementación del servicio de Control de Acceso se deben realizar listas de acceso para permitir solo a personas o equipos autorizado el uso de los recursos de una red, el uso de estas listas de acceso no tienen un impacto negativo en el desempeño de una red por lo que no se hizo la evaluación de este servicio.

En capítulos anteriores se especificaron los conceptos básicos del funcionamiento de IPSec y de medición del desempeño de redes IP, en este capítulo el estudio se centra en los detalles de las pruebas realizadas en los distintos escenarios.

La metodología utilizada en la realización del proyecto introduce consideraciones importantes ya que se trabaja sobre escenarios reales que no permiten la flexibilidad de los escenarios realizados en el laboratorio.

3.2 CONSIDERACIONES PARA LA REALIZACIÓN DE LAS PRUEBAS

Las siguientes consideraciones fueron tomadas en cuenta para la realización de las pruebas del presente trabajo de grado:

- El servidor para túneles IPSec utilizado en el proyecto fue OpenSwan, el cual ofrece ventajas sobre otros como el soporte multiplataforma y la posibilidad de utilizar el modo agresivo de ISAKMP que obliga la utilización de la transformada de estudio en un momento determinado. Este servidor no permite la configuración de solo-autenticación (autenticación + integridad) pero si de solo-confidencialidad; se permite la prestación de ambos servicios con el protocolo ESP utilizando algoritmos combinados.

- El protocolo de seguridad AH no fue tenido en cuenta para la realización de pruebas, ya que la última versión de IPSec da la posibilidad de no incluirlo dentro de las distintas implementaciones de esta arquitectura, argumentando que este protocolo de seguridad comparado con ESP está

quedando obsoleto [3], además, en la busca de los servidores para túneles IPSec se encontró que en sus últimas versiones no se permite la implementación del protocolo de seguridad AH.

- Los algoritmos tanto de autenticación como de cifrado fueron escogidos con base en RFC 4835 y a los algoritmos disponibles en Openswan. El RFC 4835 define los algoritmos que deben ser usados con IPSec para garantizar un mínimo grado de interoperabilidad [30].

- La implementación de escenarios con servicios de seguridad IPSec entre dos pasarelas de seguridad (SG - SG) no fue realizada principalmente por dos razones.

    - Entre dos enrutadores que prestan servicios de seguridad con IPSec, no se utilizan segmentos de red con tecnologías de acceso como Wi-Fi que es el objetivo de estudio del proyecto.

    - La red de Información de la Universidad del Cauca no cuenta con equipos que puedan implementar los servicios de seguridad de IPSec.

- Se utilizó tráfico con los parámetros definidos en las recomendaciones y los RFC de la ITU-T y la IETF respectivamente (parámetros nombrados en la sección 2). A este tipo de tráfico se lo denominará como *"Tráfico Parametrizado"* de ahora en adelante. Además del Tráfico Parametrizado se utilizaron: tráfico de datos, voIP y video; las características con las cuales se modelaron estos tráficos se basan en [29][31]. Las características para estos tipos de tráfico, se listan en la Tabla 3.1.

Tabla 3.1 Caracterización de tráficos de Internet en D-ITG

	Tráfico Parametrizado	**Video**	**VoIP**	**Datos**
Protocolo Transporte	UDP	UDP	UDP	TCP
Tamaño de paquete	160 bytes de Payload	Distribución normal con media μ = 27791 y desviación típica σ = 6254 bytes	117,5 bytes	Distribución poisson, con una media de 48 bytes

Tabla 3.1 (Continuación)

	Tráfico Parametrizado	**Video**	**VoIP**	**Datos**
Tiempo de Partida entre paquetes	Distribución Poisson con media μ = 20 paquetes por segundo	24 paquetes/s	50 paquetes/s	100 paquetes/s
Duración	5 minutos	5 minutos	5 minutos	5 minutos
Códec (solo VoIP)	No aplica	No aplica	G.711.2	No aplica

Al hacer uso de la característica de modelamiento de tráfico con VoIP en la herramienta D-ITG, no se pueden modificar las variables que determinan el tamaño de los paquetes así como tampoco el tiempo de partida entre los mismos.

- Se realizaron dos tipos de pruebas ya que se utilizó la infraestructura de una red en funcionamiento:

    - Pruebas con tráfico mínimo: realizadas en horarios en los cuales la cantidad de personas que acceden a la red de información es mínima. Los resultados de estas pruebas están consignadas en el Anexo A.

    - Pruebas con alto tráfico: realizadas en horarios en los cuales la cantidad de tráfico de la red es alta y constante. Para la realización de estas pruebas se tomó como referencia el monitoreo de la utilización de un servidor Proxy (NEXUS) de la red de información de la Universidad del Cauca durante un mes. El resultado de este monitoreo se muestra en la Figura 3.1 donde se observa el uso del servidor durante las horas del día.

Figura 3.1 Uso por horas del proxy NEXUS en el mes de agosto

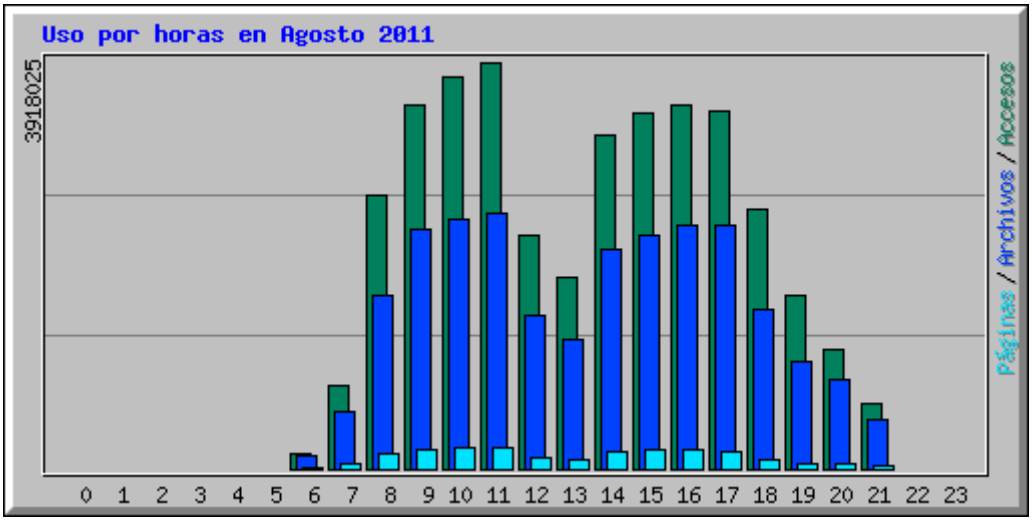


Tabla 3.2 Horarios utilizados durante las pruebas

Hora	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
1 - 5 AM	Sin Tráfico	Sin Tráfico	Sin Tráfico	Sin Tráfico	Sin Tráfico	Sin Tráfico	Sin Tráfico
9 - 11 AM	Con Tráfico	Con Tráfico	Con Tráfico				
2 - 4 PM	Con Tráfico	Con Tráfico	Con Tráfico				

Como se puede observar en la Figura 3.1, los períodos de tiempo en donde hay un tráfico alto y constante son los comprendidos entre las 9 AM hasta las 11 PM y de las 2 PM hasta las 4PM. En la Tabla 3.2 se muestran los horarios utilizados para la realización de las pruebas del presente proyecto.

- Los resultados obtenidos en algunos edificios no se tuvieron en cuenta para el análisis de las pruebas, factores como la congestión de red modifican los resultados de la pruebas impidiendo observar el comportamiento de IPSec sobre la red inalámbrica de la Universidad del Cauca. En facultades como la FIET la congestión es un parámetros crítico a la hora de realizar las pruebas; los puntos de acceso en este edifico siempre están congestionados inclusive en los horarios de bajo tráfico.

3.3 SERVICIOS DE SEGURIDAD CONSIDERADOS EN LA EVALUACIÓN

Para la realización del proyecto se consideraron los servicio de seguridad propiciado por IPSec de Autenticación + Integridad (como uno solo), y de confidencialidad. En el Capítulo 1 se mencionaron más servicios de seguridad, pero no se implementaron ya que no afectan de manera significativamente el desempeño de las redes IP [9].

3.4 MÉTRICAS DE RED A EVALUAR

En el Capítulo 2 se describieron las métricas más importantes para la evaluación del desempeño de una red IP las cuales son:

- Retardo en un sentido
- Variación de retardo en un sentido
- Tasa de pérdida de paquetes
- Indisponibilidad

La ITU-T en la recomendación Y.1543 define la indisponibilidad como un periodo de *rollup* (5 minutos) en el cual las pérdidas son mayores al 75% de total de paquetes enviados, para las pruebas realizadas en el proyecto este umbral nunca fue superado por lo que no hubo periodos de indisponibilidad y esta métrica no fue tenida en cuenta en análisis de los resultados.

Como se mencionó en la sección 2 la herramienta usada para la realización de las pruebas fue D-ITG, la cual, es una herramienta que permite la modificación de los distintos parámetros para la medición en Internet cumpliendo con los requerimientos de la ITU-T y la IETF.

El tiempo de medición para las pruebas básicas fue aproximadamente de 5 minutos cada una (tiempo de *rollup*) [21], con tiempos aleatorios de espera antes y después de cada una de ellas con el objetivo de evitar mediciones de comportamientos periódicos.

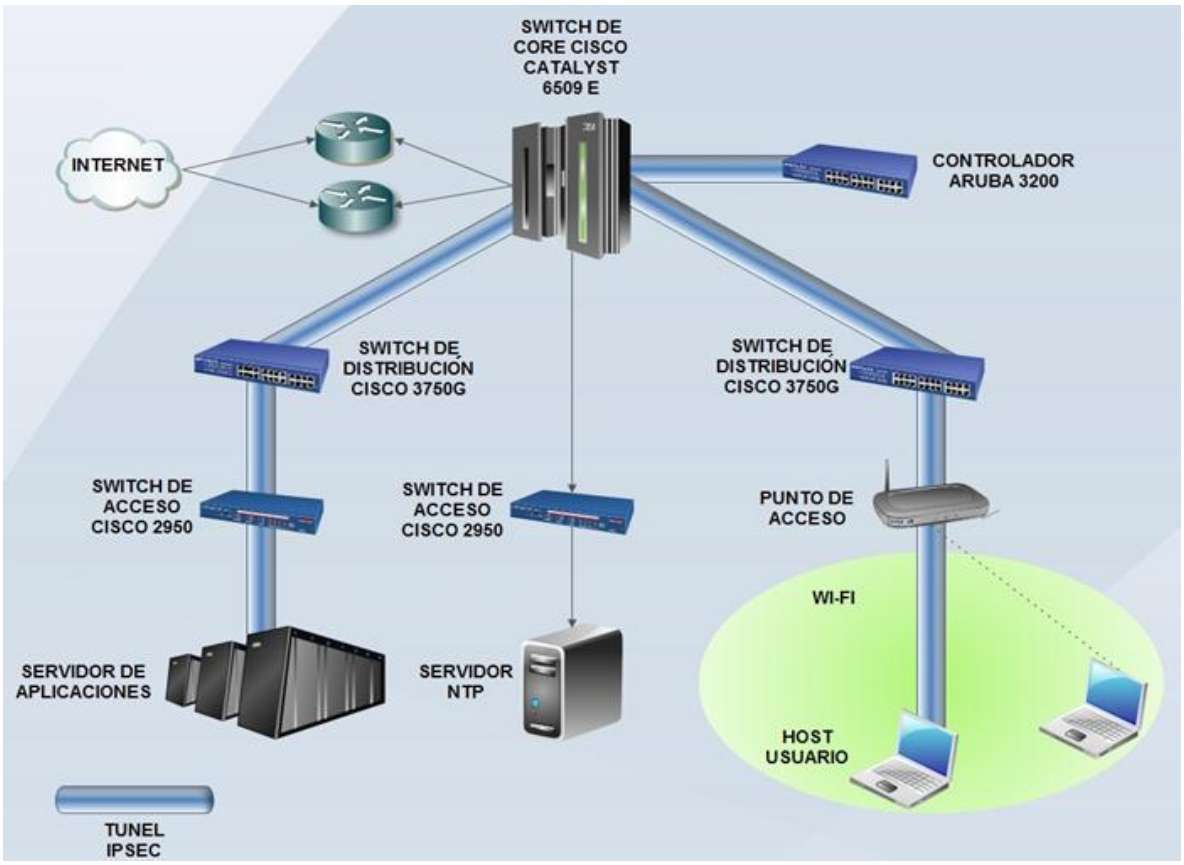
3.5 ESCENARIO DE TRABAJO

En el Capítulo 1 se muestra la estructura de la red de Información de la Universidad del Cauca donde se utilizan equipos de red para las áreas de Acceso, Distribución y *Core* de la red. En la Figura 3.2 se observa el diagrama de red para el escenario utilizado en el proyecto.

En las pruebas, el escenario físico cambió dependiendo del edificio de la Universidad del Cauca en el cual se realizaron las pruebas; de forma lógica el escenario es básicamente el mismo debido a la estructura jerárquica de red implementada en la Universidad. Se trabajó siempre con un servidor de aplicaciones conectado en el área de servidores de la red de forma cableada y un host cliente conectado de forma inalámbrica que cambio su posición dependiendo del edificio en el cual se realizaron las pruebas.

Como se puede observar en la Figura 3.2 se implementó un servidor de tiempo en Internet (NTP) ya que la herramienta D-ITG necesita estados de sincronización para proporcionar los valores de retardo y variación de retardo de manera precisa. También se puede observar en la Figura 3.2, que todo el camino entre los servidores de aplicaciones y el host cliente que se están comunicando queda protegido con un túnel IPSec.

Figura 3.2 Escenario de trabajo



Según la segunda versión de IPSec [2], existen tres posibles escenarios básicos para la implementación de esta *suite* de protocolos, los cuales son: Host a Host, Host a Pasarela de Seguridad y Pasarela de Seguridad a Pasarela de Seguridad. De estos tres escenarios se escogió y trabajó con el llamado Host a Host, debido a que actualmente la Red de Información de la Universidad del Cauca no cuenta con equipos que soporten las capacidades de una Pasarela de Seguridad, elemento indispensable para la implementación de los dos escenarios restantes.

3.6 IMPACTO DE IPSEC EN EL DESEMPEÑO DE LA RED WI-FI DE LA UNIVERSIDAD DEL CAUCA

Se realizaron las pruebas para el protocolo ESP en modo túnel y en modo transporte. Los distintos tipos de pruebas para los servicios evaluados se listan en la Tabla 3.3. Las figuras que se muestran para estas pruebas corresponden a diagramas de barras que representan los valores promedios que se obtuvieron de cada métrica en los distintos edificios del campus universitario. Para una mejor interpretación de los resultados en las distintas figuras se realizaron las siguientes convenciones:

- Para el caso del servicio de solo-confidencialidad, las barras correspondientes a las transformadas que menores incrementos presentaron para las distintas transformadas serán representadas con color amarillo.

- Para el caso de los servicios de confidencialidad más autenticación, las barras correspondientes a las transformadas que menores incrementos presentaron para las distintas transformadas serán representadas con color verde.

- Para el caso de los servicios de confidencialidad más autenticación, las barras correspondientes a las transformadas que mayores incrementos presentaron para las distintas transformadas serán representadas con color rojo.

Para las métricas de retardo y variaciones de retardo los resultados están en milisegundos y para la métrica de pérdida de paquetes los resultados se encuentran en valores porcentuales. Aquellos resultados resaltados en rojo, fueron aquellos que no se tuvieron en cuenta para la obtención de los valores promedio.

Tabla 3.3 Escenarios, servicios de seguridad evaluados, modos de IPSec y transformadas de seguridad aplicadas

	SERVICIO – PROTOCOLO	MODO	ALGORITMOS
SERVIDOR DE APLICACIONES – HOST CLIENTE	**Confidencialidad – ESP**		
		Túnel	AES
		Túnel	3DES
		Transporte	AES
		Transporte	3DES
	Autenticación + Confidencialidad – ESP		
		Túnel	AES - MD5
		Túnel	AES - SHA1
		Túnel	3DES - MD5
		Túnel	3DES - SHA1
		Transporte	AES - MD5
		Transporte	AES - SHA1
		Transporte	3DES - MD5
		Transporte	3DES - SHA1

3.6.1 Impacto de IPSec para el Tráfico Parametrizado

3.6.1.1 Retardo en un sentido para ESP en modo túnel. El edificio que menores valores de retardo presentó para la prueba con las distintas transformadas de seguridad fue la Casa Rosada donde los valores de retardo no superan los 2,7 milisegundos como se puede observar en la Tabla 3.4. Contrario a este comportamiento las pruebas realizas en el edificio de la FIET muestran los valores de retardo más altos superando los 30 milisegundos como fue el caso en el cual no se utilizó protocolo de seguridad. Los resultados obtenidos en este edificio no fueron tenidos en cuenta para el análisis del comportamiento de esta métrica ya que el punto de acceso para este edifico siempre tiene altos niveles de

tráfico inclusive para horarios nocturnos lo que podría modificar el valor de los resultados para la prueba.

Tabla 3.4 Prueba de retardo en modo túnel para tráfico parametrizado

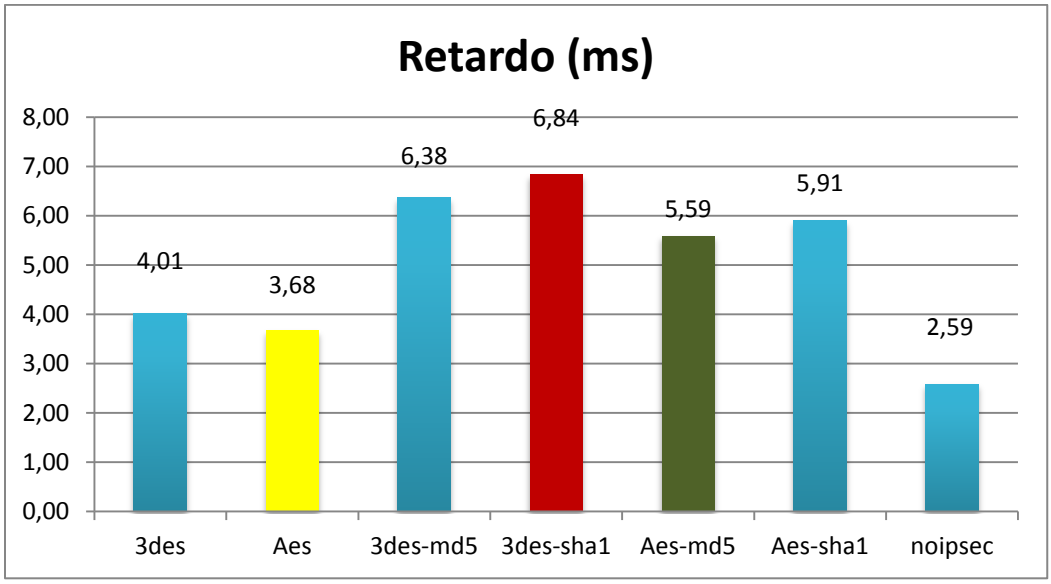
Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	3,31	7,14	0,86	5,27	2,76
Aes	3,55	5,61	1,08	5,56	2,56
3des-md5	4,89	11,63	2,14	6,22	6,18
3des-sha1	5,36	13,10	2,70	8,31	6,61
Aes-md5	4,79	8,07	1,72	5,71	6,04
Aes-sha1	4,82	9,12	2,46	6,93	6,66
Sin IPSec	2,91	4,71	0,74	3,89	0,46
Edificio / Transformada (ms)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	2,78	12,09	2,08	7,90	4,01
Aes	0,05	23,13	2,25	8,75	3,68
3des-md5	4,03	3,34	7,66	8,26	6,38
3des-sha1	5,12	11,89	4,32	9,18	6,84
Aes-md5	4,01	1,47	6,79	7,62	5,59
Aes-sha1	4,98	16,22	3,68	8,60	5,91
Sin IPSec	1,31	37,21	0,34	6,33	2,59

Esta prueba muestra resultados interesantes sobre el comportamiento de IPSec para la métrica de retardo; como se puede observar en la Figura 3.3, el resultado para el caso en cual no se implementó transformada de seguridad, muestra el valor más bajo, de esta forma se puede observar de manera más detallada el comportamiento del retardo utilizando las distintas transformadas de seguridad.

Las transformadas de seguridad que prestan los servicios de confidencialidad más autenticación son aquellas en las cuales las pruebas muestran los valores de retardo más altos, en este caso la utilización de un algoritmo de autenticación incrementa los valores de retardo en la evaluación de esta métrica. Cuando las transformadas utilizan el mismo algoritmo de cifrado, las transformadas que utilizan el algoritmo de Autenticación “md5” son las que presentan los menores valores de retardo comparadas con las transformadas de seguridad que trabajan con el algoritmo “sha1”; de forma análoga cuando las transformadas de seguridad trabajan con el mismo algoritmo de autenticación, las que utilizan el algoritmo de

cifrado "aes" son aquellas para las cuales el retardo muestra el mejor comportamiento[4].

Figura 3.3 Valores promedio de retardo en modo túnel para tráfico parametrizado



3.6.1.2 Retardo en un sentido para ESP en modo transporte. Los resultados obtenidos en los Edificios de Contaduría y la FIET no fueron tenidas en cuenta para la evaluación del comportamiento de esta métrica ya que proyectaron los resultados con mayores fluctuaciones con respecto a los valores promedios que se obtuvieron para las distintas transformadas, estas fluctuaciones en algunos casos superaron los 20 milisegundos como se puede observar en la Tabla 3.5.

Tabla 3.5 Prueba de retardo en modo transporte para tráfico parametrizado

Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	5,43	2,98	2,83	9,88	3,65
Aes	4,94	2,49	2,78	3,34	2,94
3des-md5	6,35	5,75	2,24	13,59	4,03
3des-sha1	6,32	5,55	3,73	4,15	3,93
Aes-md5	6,51	4,86	3,84	31,10	4,52

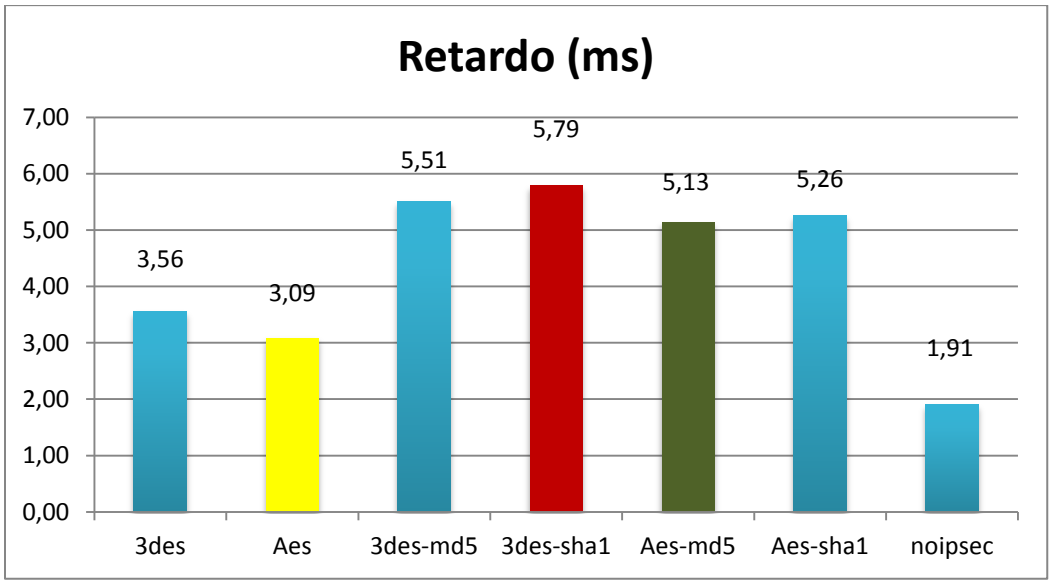
[4] Mejor comportamiento: Se habla de mejor comportamiento cuando las distintas métricas exhiben valores bajos en los resultados para las distintas pruebas.

Tabla 3.5 (Continuación)

Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
Aes-sha1	6,20	2,93	3,46	9,38	3,88
Sin IPSec	3,68	0,88	1,00	11,18	2,15
Edificio / Transformada (ms)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	2,38	2,88	2,87	4,77	3,56
Aes	2,76	2,58	1,78	3,92	3,09
3des-md5	4,13	10,64	3,12	5,97	5,51
3des-sha1	4,20	2,37	3,83	6,00	5,79
Aes-md5	2,69	20,41	3,38	3,15	5,13
Aes-sha1	3,32	2,92	3,86	6,18	5,26
Sin IPSec	1,16	8,66	1,02	3,44	1,91

En la Figura 3.4, se observa que al utilizar el algoritmo “md5” para prestar el servicio de autenticación, las transformadas muestran menores valores de retardos comparadas con aquellas que utilizan “sha1”; de forma análoga cuando se utiliza el algoritmo “aes” para brindar el servicio de confidencialidad, las transformadas muestran un mejor comportamiento comparadas con aquellas que utilizan el algoritmo “3des”.

Figura 3.4 Valores promedio de retardo en modo túnel para tráfico parametrizado



Comparando los resultados de esta prueba con la realizada para medir retardo con el protocolo de seguridad ESP en modo túnel (véase el numeral 3.6.1.1), se observa una gran similitud en el comportamiento para los dos modos de operación del protocolo de seguridad; la diferencia entre los dos modos de operación son solo 20 bytes de más en la cabecera del paquete IP para el modo túnel por lo que este tipo de comportamientos fue el esperado.

3.6.1.3 Variación de retardo para ESP en modo túnel. Los valores de los resultados para las distintas transformadas de seguridad en el edificio de la FIET no fueron tenidos en cuenta para este análisis ya que sus valores tienen grandes fluctuación con respecto a los valores promedios obtenidos para la prueba como se observa en la Tabla 3.6. Mientras los valores promedios oscilan alrededor de 1 milisegundo, los resultados obtenidos para el edificio de la FIET superan algunas veces los 7 milisegundos como ocurrió en el caso para el cual no se utilizó el protocolo de seguridad.

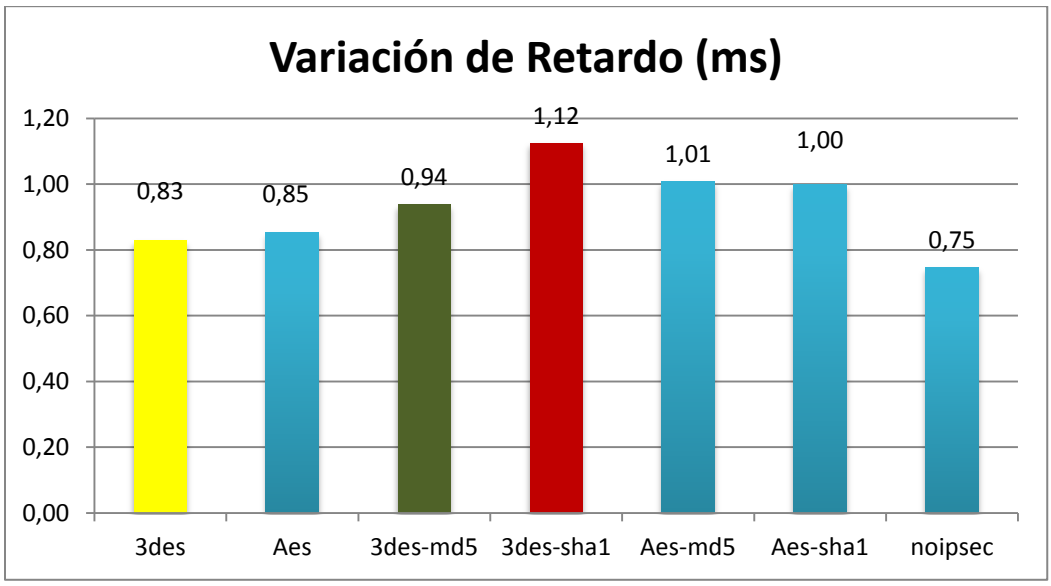
Tabla 3.6 Prueba de variación de retardo en modo túnel para tráfico parametrizado

Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	0,4	0,83	0,32	1	0,34
Aes	0,49	0,83	0,37	1,03	0,34
3des-md5	0,49	1,28	0,5	1,32	0,41
3des-sha1	0,94	1,6	0,7	1,48	0,67
Aes-md5	0,65	1,37	0,4	1,26	0,61
Aes-sha1	0,6	1,56	0,51	1,44	0,45
Sin IPSec	0,48	0,92	0,27	1,02	0,31
Edificio / Transformada (ms)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	0,87	3,65	0,49	2,38	0,83
Aes	1,06	4,46	1,9	0,82	0,85
3des-md5	0,43	0,9	1,54	1,54	0,94
3des-sha1	1,31	6,43	0,81	1,5	1,12
Aes-md5	0,42	2,58	2,49	0,87	1,01
Aes-sha1	0,69	5,27	1,6	1,14	1
Sin IPSec	0,81	7.02	1,06	1,1	0,75

Los valores de variación de retardo incrementan su valor promedio cuando se utiliza el servicio de seguridad de confidencialidad más autenticación, de esta forma se observa en la Figura 3.5 que las transformadas que tienen algún protocolo de autenticación son aquellas en las cuales la variación de retardo muestra el peor comportamiento.

Comparando esta prueba con la realizada para cuantificar la métrica de retardo para ESP en modo túnel (véase el numeral 3.6.1.1), se evidencia una relación entre las dos métricas ya que las transformadas que mayores retardos presentan también son aquellas que presentan las mayores variaciones de retardo.

Figura 3.5 Valores promedio de variación de retardo en modo túnel para tráfico parametrizado



Cuando se implementa el servicio de seguridad de confidencialidad más autenticación y se utiliza el mismo algoritmo de cifrado, las transformadas que utilizan el algoritmo “md5” para prestar el servicio de autenticación muestran los menores valores de variación de retardo comparadas con aquellas que utilizan “sha1” para prestar este servicio.

3.6.1.4 Variación de retardo para ESP en modo transporte. Como se puede observar en la Tabla 3.7. Los valores obtenidos para variación de retardo en los

edificios de Contaduría y la FIET superan notablemente los valores promedio obtenidos para las distintas transformadas por lo que no fueron tenidos en cuenta para el análisis de esta prueba. Para la evaluación de retardo para ESP en modo transporte (véase numeral 3.6.1.2) se presentó el mismo problema con los valores obtenidos en los edificios antes nombrados, este hecho evidencia la fuerte relación que existe entre las métricas de retardo y variación de retardo.

Tabla 3.7 Prueba de variación de retardo en modo transporte tráfico parametrizado

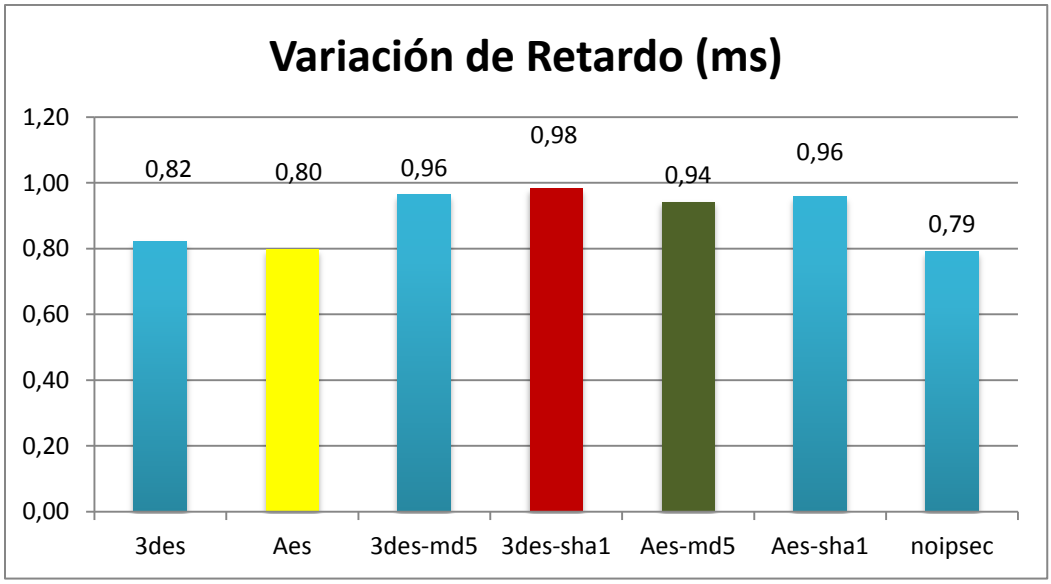
Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	1,17	0,59	0,68	0,67	0,90
Aes	0,77	0,31	0,85	1,31	0,53
3des-md5	1,06	1,12	1,17	4,60	0,31
3des-sha1	1,30	0,82	1,05	1,72	0,83
Aes-md5	0,64	1,02	0,64	6.05	0,56
Aes-sha1	1,19	0,75	0,74	0,52	0,72
Sin IPSec	1,02	0,46	0,72	2,30	0,91
Edificio / Transformada (ms)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	0,53	0,90	0,45	1,43	0,82
Aes	0,84	0,74	0,68	1,61	0,80
3des-md5	0,62	3.45	1,46	1,00	0,96
3des-sha1	0,77	0,93	0,90	1,21	0,98
Aes-md5	0,77	5.65	0,67	2,30	0,94
Aes-sha1	1,06	0,48	0,98	1,26	0,96
Sin IPSec	0,78	3,83	0,60	1,05	0,79

Como se observa en la Figura 3.6, las transformadas que menores valores de variación de retardo presentan son aquellas que prestan el servicio de solo-confidencialidad; de estas transformadas la que utiliza el algoritmo de cifrado “aes” es aquella para la cual la métrica de variación de retardo muestra el mejor comportamiento.

Cuando se presta el servicio de seguridad de confidencialidad más autenticación, independientemente del algoritmo de cifrado que se esté utilizando, las transformadas que utilizan el algoritmo de autenticación “md5” son aquellas para las cuales la variación de retardo muestra el mejor comportamiento. De forma análoga cuando se compara las transformadas que trabajan con el mismo

algoritmo de autenticación, las transformadas que utilizan el algoritmo de cifrado "aes" son aquellas para las cuales la variación de retardo muestra los menores valores en los resultados.

Figura 3.6 Valores promedio de variación de retardo en modo transporte para tráfico parametrizado



3.6.1.5 Pérdida de paquetes para ESP en modo túnel. Como se puede observar en la Tabla 3.8, los valores promedio para esta prueba muestran porcentajes de pérdida de paquetes entre 0.52% y 0.58%. De esta forma los valores para la prueba están en su mayoría dentro de este rango de puntos porcentuales. En el caso de los porcentajes de pérdida de paquetes obtenidos en el edifico del IPET, estos superan en algunos casos los 4 puntos porcentuales, estas anomalías en los resultados obligaron a no tenerlos en cuenta para el análisis de esta prueba.

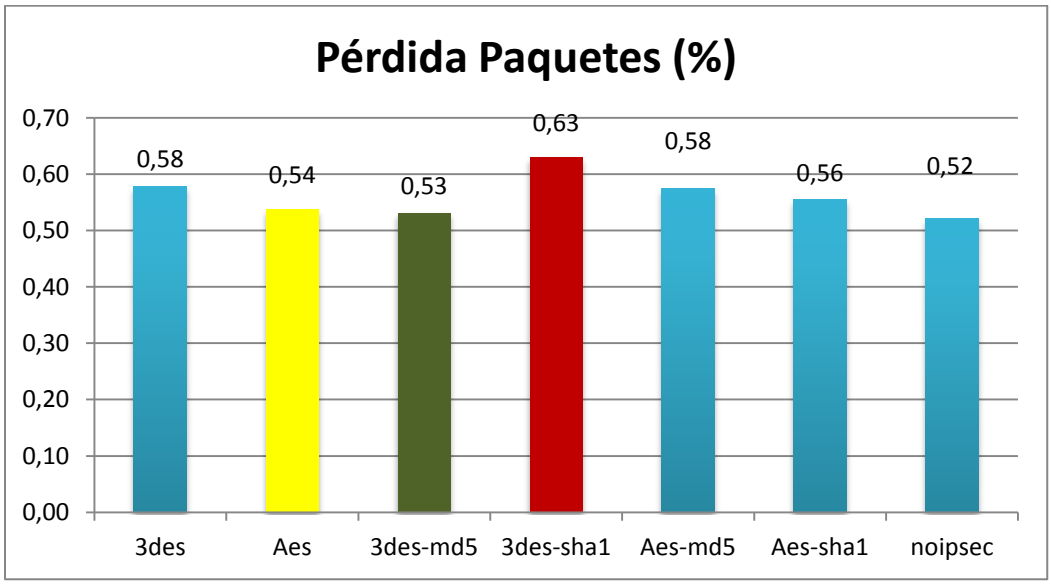
Tabla 3.8 Prueba de pérdida de paquetes en modo túnel para tráfico parametrizado

Edificio / Transformada (%)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	0,49	0,61	0,49	0,69	0,53
Aes	0,37	0,56	0,53	0,61	0,53
3des-md5	0,39	0,65	0,51	0,58	0,65
3des-sha1	0,62	0,65	0,53	0,60	0,55

Tabla 3.8 (Continuación)

Edificio / Transformada (%)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
Aes-md5	0,46	0,56	0,51	0,79	0,48
Aes-sha1	0,68	0,49	0,53	0,77	0,46
Sin IPSec	0,95	0,44	0,54	0,64	0,49
Edificio / Transformada (%)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	0,53	0,76	0,63	0,53	0,58
Aes	0,56	0,70	4,00	0,56	0,55
3des-md5	0,53	0,41	1,37	0,53	0,53
3des-sha1	0,76	0,57	0,53	0,76	0,63
Aes-md5	0,60	0,60	1,09	0,60	0,58
Aes-sha1	0,51	0,49	4,53	0,51	0,56
Sin IPSec	0,49	0,13	2,72	0,49	0,52

Figura 3.7 Valores promedio de pérdida de paquetes en modo túnel para tráfico parametrizado



Como se observa en la Figura 3.7 los porcentajes promedios para la métrica de paquetes perdidos no muestran grandes fluctuaciones en los valores de los resultados para las distintas transformadas y el valor para el caso en el cual no se utilizó transformada de seguridad. A pesar de este comportamiento la transformada que presentó los porcentaje más altos de paquetes perdidos fue

aquella que utiliza los algoritmos de cifrado y autenticación “3des-sha1“; para esta transformada las métricas utilizadas para medir el desempeño de red siempre muestran el peor comportamiento. Se puede afirmar que la combinación de estos algoritmos en una transformada siempre es la que más impacta de forma negativa el desempeño de la red, cuando se utiliza el protocolo ESP para brindar servicios de seguridad.

3.6.1.6 Pérdida de paquetes para ESP en modo transporte. En la Tabla 3.9 se observa que los valores de porcentajes para la métrica de pérdida de paquetes en su mayoría no superan el 1%; esto quiere decir que por cada 5000 paquetes con los cuales se realiza la evaluación de cada transformada de seguridad, se pierden menos de 5 paquetes. Para el caso de los edificios de contaduría y la FIET, para algunas transformadas de seguridad las pérdidas de paquetes superan el 4% esta es la razón para no tener en cuenta estos valores para el análisis en esta prueba.

Tabla 3.9 Prueba de pérdida de paquetes en modo transporte tráfico parametrizado

Edificio / Transformada (%)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	0,92	0,18	0,62	3,87	0,59
Aes	0,18	1,04	0,68	0,81	0,50
3des-md5	0,11	0,58	0,64	1,30	0,25
3des-sha1	0,84	0,75	0,20	0,50	0,42
Aes-md5	1,38	0,19	0,39	0,78	0,38
Aes-sha1	1,34	0,51	0,47	4,26	0,28
Sin IPSec	0,65	0,24	0,50	1,17	0,49
Edificio / Transformada (%)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	0,39	0,48	0,32	0,83	0,55
Aes	0,36	3,53	0,39	0,57	0,53
3des-md5	0,62	0,49	0,77	1,32	0,61
3des-sha1	0,64	0,12	1,26	0,22	0,62
Aes-md5	0,39	4,63	0,60	0,81	0,59
Aes-sha1	0,57	1,31	0,58	0,27	0,57
Sin IPSec	0,45	1,01	0,43	0,71	0,50

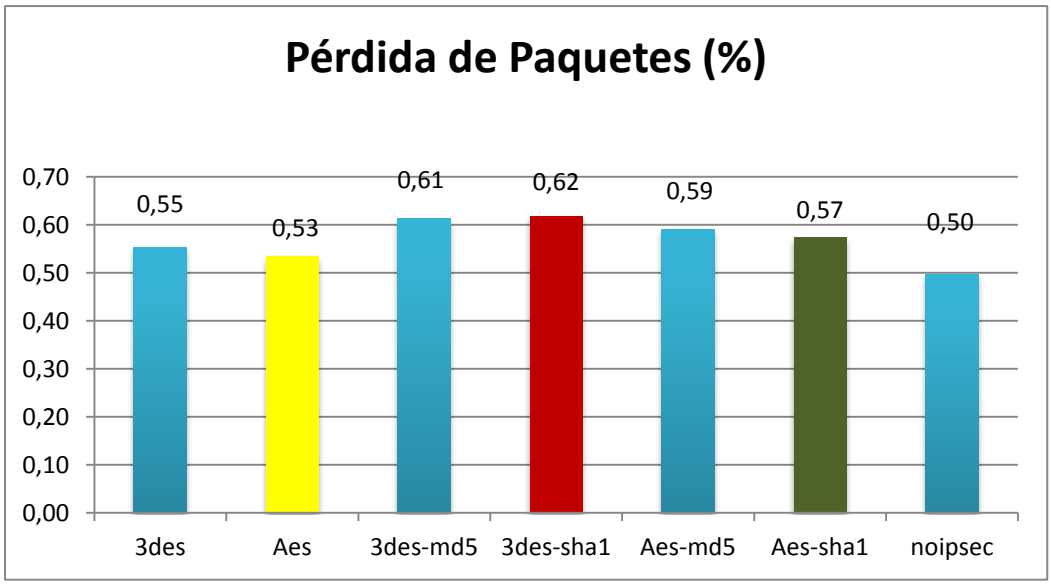
Como se observa en la Figura 3.8 las transformadas que prestan el servicio de seguridad de solo-confidencialidad son aquellas para las cuales los porcentajes de

pérdidas muestran los valores más bajos, comparadas con las transformadas que prestan los servicios de confidencialidad más autenticación.

Para el servicio de confidencialidad más autenticación, las transformadas que utilizan el algoritmo de cifrado “aes”, son aquellas para las cuales la métrica de pérdida de paquetes muestra el mejor comportamiento.

Aunque se observa un comportamiento coherente en los resultados para esta prueba comparados con los obtenidos para medir el desempeño de la red con otras métricas, la mayor fluctuación para estos resultados esta entre el 0.62% que fue el resultado obtenido cuando se utilizó la transformada con los algoritmos “3des-sha1” y el 0.5 % para el caso en el cual no se utilizó el protocolo de seguridad. Analizando estos resultados se observa que esta fluctuación es del orden de los 0.11 puntos porcentuales, de esta forma se infiere que las transformadas de seguridad no alteran significativamente el comportamiento de la métrica de paquetes perdidos para esta prueba.

Figura 3.8 Valores promedio de pérdida de paquetes en modo transporte para tráfico parametrizado



3.6.2 Impacto de IPSec sobre el tráfico de Datos. Para el tráfico de datos se estableció el protocolo TCP para hacer la marca en el campo de “protocolo de nivel superior” en el datagrama IP. Al realizar este tipo de marca, durante las

pruebas nunca se presentaron pérdidas de paquetes, por esta razón la métrica de pérdida de paquetes no fue incluida en el análisis para este tipo de tráfico.

3.6.2.1 Retardo en un sentido para ESP en modo túnel. Como ocurrió en algunas pruebas para la evaluación del desempeño para las que no se tuvieron en cuenta algunos resultados (véase el numeral 3.6.1), para esta prueba los resultados obtenidos en los edificios de Contaduría, la FIET y el IPET no se consideraron para la realización del análisis. Se observa en la Tabla 3.10, que mientras los valores promedios para las distintas transformadas no superan los 23 milisegundos, para estos edificios algunos valores superan los 200 milisegundos; estas grandes fluctuaciones son el motivo para descartar los valores obtenidos en estos edificios. El caso contrario de observa en el edificio de la Casa rosada donde el retardo muestra los valores más bajos para esta prueba.

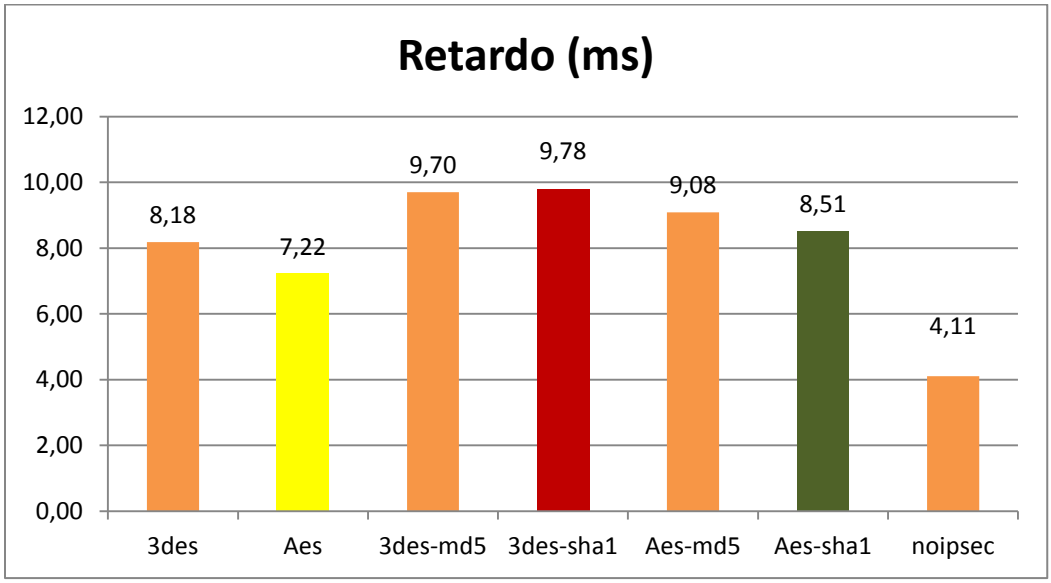
Tabla 3.10 Prueba de retardo en modo túnel para datos

Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	1,67	2,70	2,41	174,08	8,96
Aes	0,86	3,54	0,79	245,45	8,69
3des-md5	2,77	10,03	1,70	2,24	12,55
3des-sha1	2,18	10,69	1,26	253,77	12,26
Aes-md5	2,20	6,48	0,58	265,58	12,46
Aes-sha1	2,89	6,29	1,78	206,46	11,93
Sin IPSec	0,56	2,78	3,41	475,91	7,42
Edificio / Transformada (ms)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	21,70	214,23	4,41	11,67	8,18
Aes	19,34	85,47	27,94	10,13	7,22
3des-md5	19,45	12,84	2,55	11,73	9,70
3des-sha1	21,01	17,27	34,13	11,27	9,78
Aes-md5	20,68	30,18	5,41	12,11	9,08
Aes-sha1	18,39	32,91	240,67	15,42	8,51
Sin IPSec	0,60	293,43	0,83	9,88	4,11

En la Figura 3.9 se observa que el caso en el que no se utiliza IPSec es aquel que menor valor promedio de retardo presenta reiterando el hecho que la utilización del protocolo de seguridad impacta de forma negativa el desempeño de la red. Las

transformadas de seguridad que prestan el servicio de solo-confidencialidad son las que menores valores de retardo presentan, de estas, aquella que utiliza el algoritmo de cifrado “aes” es aquella que tiene el mejor comportamiento para esta prueba.

Figura 3.9 Valores promedio de retardo en modo túnel para datos



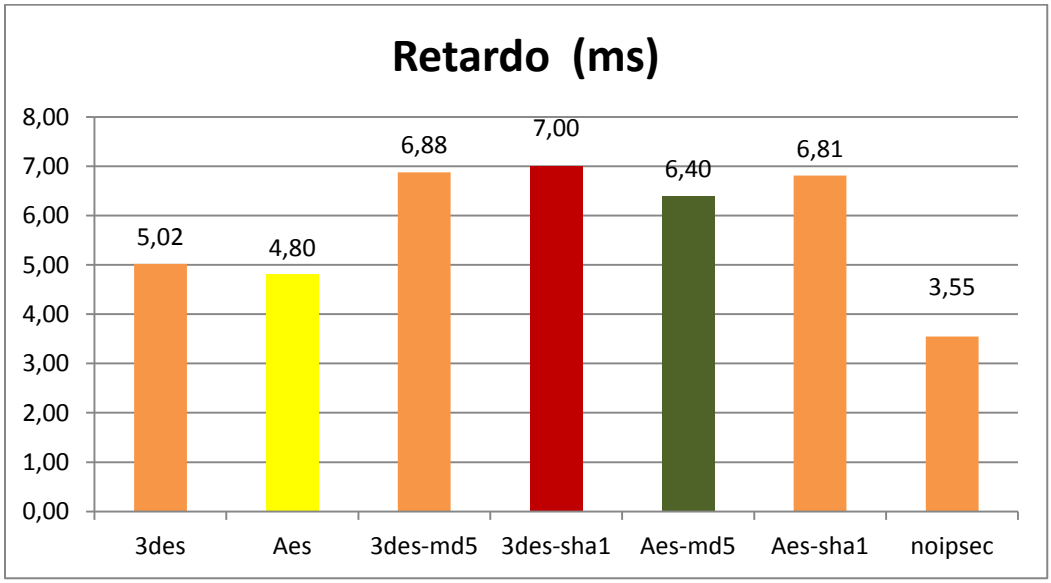
Para el servicio de seguridad de confidencialidad más autenticación, las transformadas de seguridad que trabajan con “aes” como algoritmo de cifrado son aquellas que presentan los menores valores de retardo independiente de algoritmo de autenticación que se utilice.

3.6.2.2 Retardo para ESP en modo transporte. En la Tabla 3.11 se observan valores promedio para la prueba que oscilan entre los 4 y los 8 milisegundos; para los edificios de Contaduría y la FIET se destacan resultados por encima de 200 milisegundos para algunas transformadas; como ha sido una constante para este tipo de resultados que fluctúan muy por encima de los valores promedio, los resultados obtenidos en estos edificios no fueron tenidos en cuenta para el análisis de esta métrica.

Tabla 3.11 Prueba de retardo en modo transporte para datos

Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	2,04	5,08	2,79	35,85	7,33
Aes	2,34	4,01	1,27	45,47	5,16
3des-md5	2,56	8,06	2,64	203,9	8,64
3des-sha1	2,45	9,71	3,28	8,78	8,23
Aes-md5	1,57	9,86	2,66	7,92	6,35
Aes-sha1	2,82	8,22	4,71	19,39	7,85
Sin IPSec	1,04	0,26	2,11	13,39	4,70
Edificio / Transformada (ms)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	6,08	24,61	3,79	8,05	5,02
Aes	7,82	14,95	4,41	8,61	4,80
3des-md5	13,39	46,65	4,51	7,65	6,88
3des-sha1	12,72	21,52	5,23	7,40	7,00
Aes-md5	11,06	8,56	4,79	8,49	6,40
Aes-sha1	11,32	233,84	5,39	7,35	6,81
Sin IPSec	7,07	34,9	2,31	7,36	3,55

Figura 3.10 Valores promedio de retardo en modo transporte para datos



La transformada que menores valores de retardo mostró fue las que presto el servicio de seguridad de solo-confidencialidad con el algoritmo “aes”; de igual

manera cuando se utiliza este algoritmo para prestar el servicio de confidencialidad más autenticación las transformadas mostraron los menores valores de retardo como se observa en la Figura 3.10

Para el servicio de confidencialidad más autenticación, cuando se compara el comportamiento de los algoritmos de autenticación utilizando el mismo algoritmo de cifrado, se evidencia un mejor comportamiento para las transformadas que utilizan el algoritmo “md5” para brindar el servicio de autenticación.

3.6.2.3 Variación de retardo para ESP en modo túnel. Como se puede observar los resultados de la Tabla 3.12, y comparándolos con la prueba realizada para medir retardo para ESP en modo túnel (véase el numeral 3.6.2.1) se evidencia una estrecha relación entre estas dos métricas (retardo y variación de retardo). Para que esta relación se hiciera evidente, se suprimieron los resultados de los edificios de Contaduría, la FIET y el IPET ya que al observar los valores promedios de la Tabla 3.12 estos nunca superan los 1,6 milisegundo mientras que para los edificios antes mencionados, algunos resultados sufren grandes fluctuaciones mostrando resultados que superan los 10 milisegundos.

Tabla 3.12 Prueba de variación de retardo en modo túnel para datos

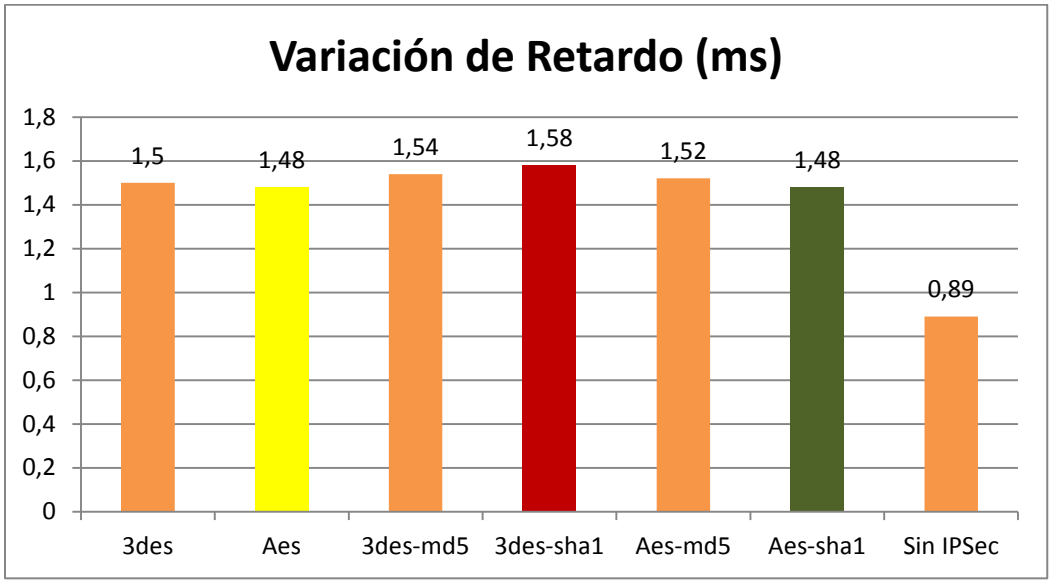
Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	0,68	0,58	0,64	6,45	1,41
Aes	0,7	0,68	0,63	15,72	1,34
3des-md5	0,44	0,59	0,71	1,27	0,96
3des-sha1	0,76	0,78	0,69	11,84	1,59
Aes-md5	0,68	0,64	0,63	12,60	1,37
Aes-sha1	0,74	0,78	0,78	9,38	1,29
Sin IPSec	0,60	0,68	0,55	18,39	1,23
Edificio / Transformada (ms)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	4,47	12,89	2,95	1,20	1,50
Aes	4,37	7,98	5,44	1,19	1,48
3des-md5	7,14	3,45	0,76	1,48	1,54
3des-sha1	4,35	3,31	2,53	1,29	1,58
Aes-md5	4,16	3,08	6,54	1,63	1,52
Aes-sha1	3,96	4,25	1,26	1,34	1,48

Tabla 3.12 (Continuación)

Edificio / Transformada (ms)	Educación	FIET	IPET	Salud	PROMEDIO
Sin IPSec	1,20	11,81	10,65	1,12	0,89

Como se observa en la Figura 3.11, cuando se presta el servicio de confidencialidad más autenticación las métricas que trabajan con el algoritmo de cifrado “aes” son aquellas que menores valores de variación de retardo exhiben, de forma análoga cuando se presta el servicio de solo-confidencialidad la transformada que trabaja con el algoritmo de cifrado “aes” es aquella que mejor comportamiento presenta.

Figura 3.11 Valores promedio de variación de retardo en modo túnel para datos



De acuerdo a estos resultados se evidencia que independiente del servicio de seguridad prestado por IPSec para el tráfico de datos, el mejor comportamiento para la variación de retardo lo muestran las transformadas que utilizan el algoritmo de cifrado “aes” para prestar el servicio de confidencialidad.

3.6.2.4 Variación de retardo para ESP en modo transporte. En la Tabla 3.13 se observa que las facultades de Contaduría y la FIET muestran valores de retardo más altos comparados con los valores promedios encontrados para esta prueba.

Las pequeñas fluctuaciones entre los resultados para las distintas transformadas de seguridad no permiten realizar un análisis coherente si se tiene en cuenta estos resultados, por este motivo estos fueron excluidos para el análisis de esta prueba.

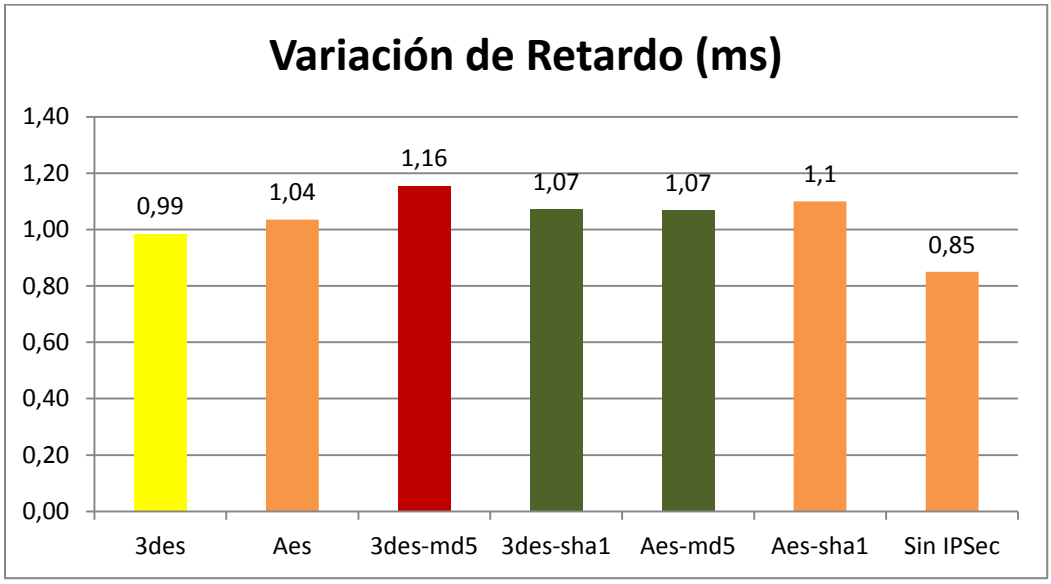
Tabla 3.13 Prueba de variación de retardo en modo transporte para datos

Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	0,62	1,15	1,01	3,21	1,07
Aes	0,70	0,84	1,02	2,49	0,81
3des-md5	0,78	1,08	0,78	15,54	1,13
3des-sha1	1,04	1,43	0,92	2,23	0,93
Aes-md5	0,67	0,86	0,90	1,34	0,85
Aes-sha1	1,15	0,98	0,78	3,88	0,63
Sin IPSec	0,61	0,29	0,97	2,00	0,77
Edificio / Transformada (ms)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	1,24	2,15	0,72	1,09	0,99
Aes	1,33	1,74	1,20	1,35	1,04
3des-md5	2,54	3,57	0,93	0,85	1,16
3des-sha1	3,13	2,31	0,52	0,57	1,07
Aes-md5	2,13	0,83	1,07	1,00	1,07
Aes-sha1	2,50	14,41	0,79	0,85	1,10
Sin IPSec	1,82	1,72	0,72	0,78	0,85

En la Figura 3.12 se observa que los valores de variación de retardo para las transformadas que prestan el servicio de solo-confidencialidad no tienen grandes fluctuaciones entre ellas, de esta forma no se logra observar una diferencia entre las transformadas que brindan este servicio.

Para las transformadas que prestan el servicio de confidencialidad más autenticación, aquellas que trabajan con el algoritmo de autenticación “aes” son para las cuales la métrica de variación de retardo muestra un mejor comportamiento.

Figura 3.12 Valores promedio de variación de retardo en modo transporte para datos



3.6.3 Impacto de IPSec sobre el tráfico de Video.

3.6.3.1 Retardo en un sentido para ESP en modo túnel. Como se observa en la los resultados de la Tabla 3.14, cuando se realiza la evaluación para tráfico de video, la métrica de retardo presenta el peor comportamiento incluso para el caso en el cual no se utilizó protocolo de seguridad; se observa que la red inalámbrica de la Universidad del Cauca muestra una mayor caída en el desempeño para este tipo de tráfico.

En la Figura 3.13 se observa que los valores promedios de la prueba realizada fluctúan entre los 29 y los 41 milisegundos aproximadamente. Para los edificios de contaduría y la FIET estos valores superan los 200 milisegundos en algunos resultados, esta fue la razón para no tenerlos cuenta para promediar los resultados ya que no permitían hacer una análisis coherente de las distintas transformadas de seguridad.

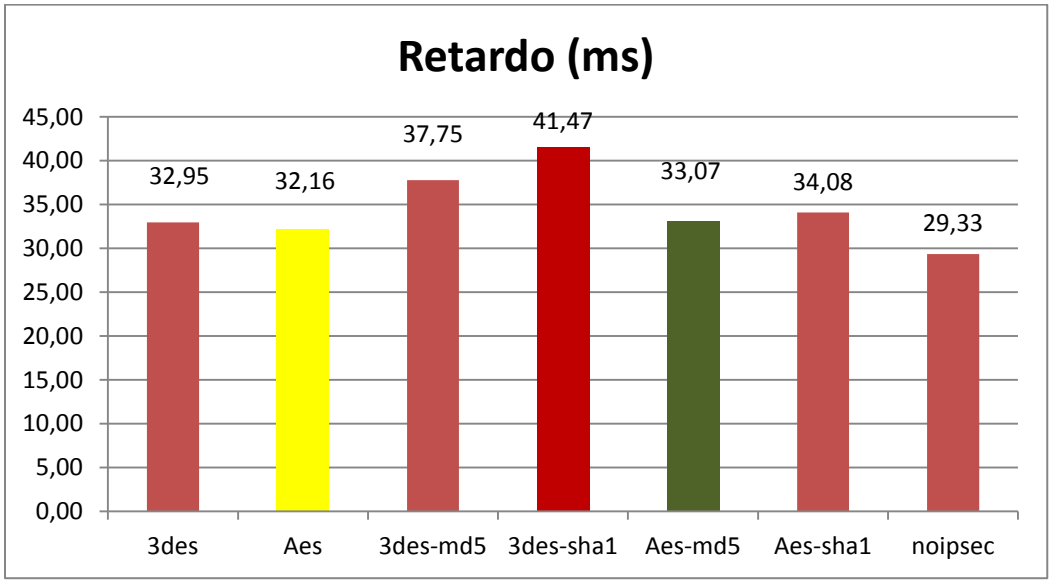
Tabla 3.14 Prueba de retardo en modo túnel para video

Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	29,13	32,34	31,35	239,22	33,81

Tabla 3.14 (Continuación)

Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
Aes	28,52	31,28	30,06	205,75	35,26
3des-md5	34,87	37,18	36,65	209,44	44,8
3des-sha1	34,83	42,61	37,82	217,71	49,81
Aes-md5	27,84	33,6	31,46	203,6	38,61
Aes-sha1	27,9	33,74	32,42	36,73	38,33
Sin IPSec	27,25	28,27	31,75	452,39	32,82
Edificio / Transformada (ms)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	27,42	19,23	45,43	31,13	32,95
Aes	28,28	34,53	37,52	34,23	32,16
3des-md5	34,84	49,84	36,84	39,04	37,75
3des-sha1	36,61	38,43	47,32	41,27	41,47
Aes-md5	31,91	27,44	32,86	35,19	33,07
Aes-sha1	35,19	25,63	30,53	40,47	34,08
Sin IPSec	28,89	236,19	27,02	29,31	29,33

Figura 3.13 Valores promedio de retardo en modo túnel para video



Como es una constante en el comportamiento del retardo para los distintos servicios de seguridad propiciados por IPSec, las transformadas de seguridad que

prestan el servicio de solo-confidencialidad son aquellas que muestran los valores de retardo más bajos comparados con los que presentan las transformadas que prestan el servicio de confidencialidad más autenticación.

Como es un comportamiento típico para la mayoría de las pruebas realizadas para medir la métrica de desempeño, las transformadas que utilizan el algoritmo de cifrado “aes” para brindar el servicio de confidencialidad son aquellas que mejor comportamiento presentan frente a las transformadas que utilizan “3des” para prestar este servicio.

3.6.3.2 Retardo para ESP en modo transporte. Los resultados que se obtuvieron en los edificios de Contaduría y la FIET fueron los que mostraron mayores variaciones con respecto a los promedios consignados para esta prueba en la Tabla 3.15. En estos edificios los retardos alcanzaron valores por encima de los 150 milisegundos muy por encima de los valores promedio para las distintas transformadas de seguridad que no superaron los 40 milisegundos, este fue el motivo para no tener en cuenta estos resultados en el análisis del comportamiento de esta métrica.

Tabla 3.15 Prueba de retardo en modo transporte para video

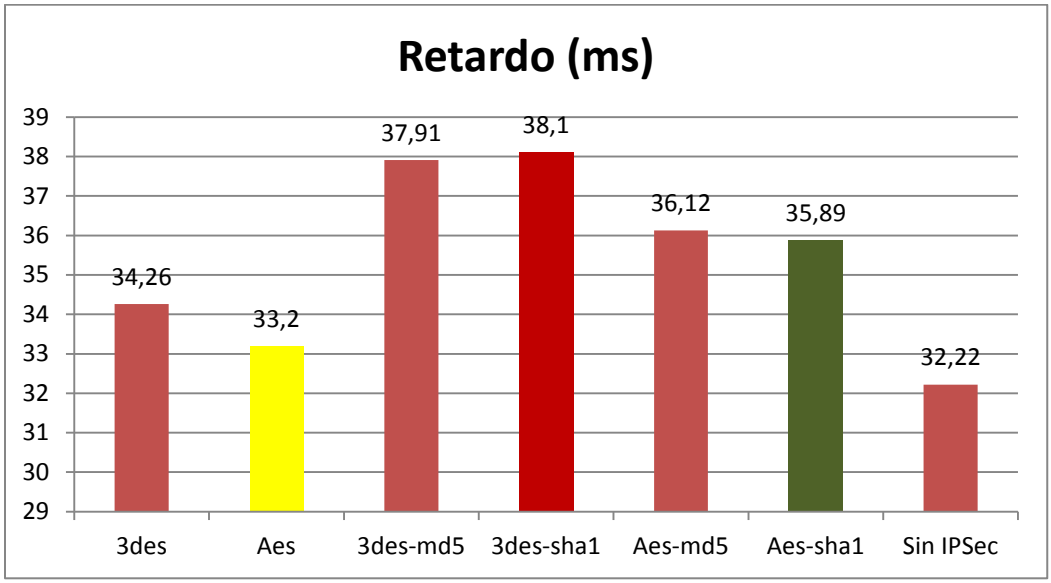
Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	28,49	35,58	31,98	128,79	38,73
Aes	28,81	35,09	32,53	84,30	34,35
3des-md5	32,22	41,52	34,00	36,78	42,15
3des-sha1	33,17	39,96	34,17	39,05	40,15
Aes-md5	31,18	35,94	34,81	56,94	40,95
Aes-sha1	30,11	38,65	32,17	93,00	39,79
Sin IPSec	26,38	33,52	32,03	152,54	38,62
Edificio / Transformada (ms)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	31,58	115,4	34,74	38,72	34,26
Aes	31,53	37,53	31,89	38,20	33,20
3des-md5	35,89	45,19	38,19	41,38	37,91
3des-sha1	36,96	352,77	38,67	43,61	38,10
Aes-md5	33,25	277,78	37,20	39,54	36,12
Aes-sha1	35,27	37,57	35,05	40,19	35,89

Tabla 3.15 (Continuación)

Edificio / Transformada (ms)	Educación	FIET	IPET	Salud	PROMEDIO
Sin IPSec	29,22	41,39	31,12	34,69	32,22

Para el servicio de solo-confidencialidad la transformada que utiliza “aes” como algoritmo de cifrado siempre muestra un mejor comportamiento para la métrica de retardo, como se puede ver en la Figura 3.14. Para las transformadas que prestan el servicio de confidencialidad más autenticación cuando se utiliza el mismo algoritmo de cifrado y se cambia el algoritmo de autenticación, las transformadas que utilizan “md5” son aquellas que mejor comportamiento presentan; si se compara esta prueba con las realizadas para evaluar el desempeño (véase el numeral 3.6) se observa una similitud en el comportamiento para las distintas transformadas de seguridad.

Figura 3.14 Valores promedio de retardo en modo transporte para video



3.6.3.3 Variación de retardo para ESP en modo túnel. Cuando se realiza el análisis de la variación retardo para el tráfico de video, se observa una relación con los resultados de la prueba para medir el retardo con el protocolo ESP en modo túnel (véase el numeral 3.6.3.1); como ocurrió en esa prueba los valores obtenidos para los edificio de Contaduría y la FIET no fueron tenidos en cuenta

para esta evaluación. Como se observa en la Tabla 3.16, los valores de los resultados obtenidos en estos edificios superan de forma significativa los valores promedios calculados para las distintas transformadas de seguridad.

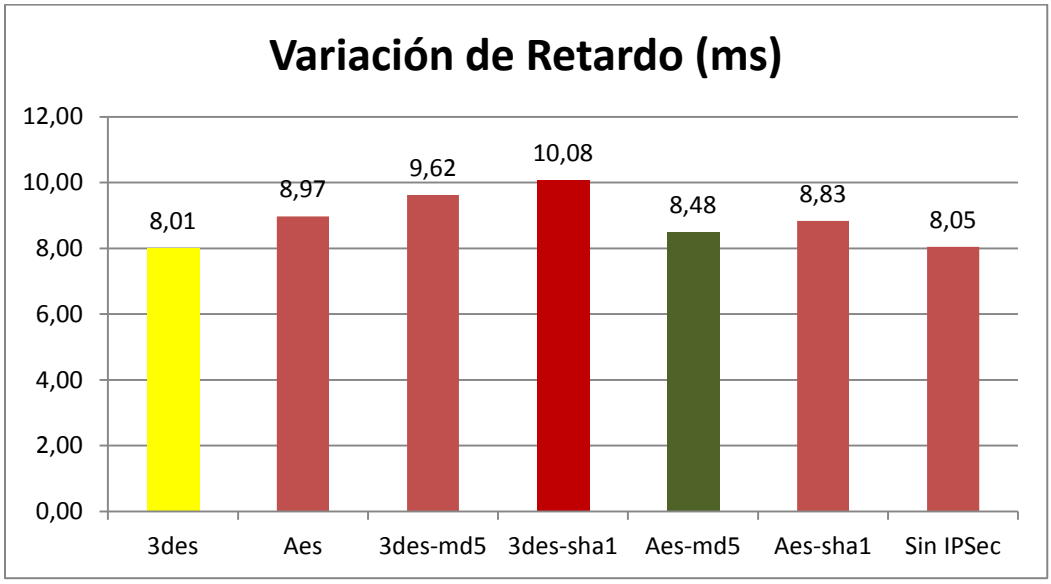
Tabla 3.16 Prueba de variación de retardo en modo túnel para video

Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	7,56	7,64	7,56	58,35	7,72
Aes	8,24	8,45	8,21	50,8	8
3des-md5	9,78	9,78	9,84	54,24	9,67
3des-sha1	9,85	9,73	9,9	58,92	10,86
Aes-md5	8,37	7,84	8,32	54,31	8,23
Aes-sha1	8,39	9,68	8,47	9,33	8,26
Sin IPSec	7,89	8,14	7,76	63,18	7,94
Edificio / Transformada (ms)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	7,59	8,16	11,68	6,32	8,01
Aes	8,33	13,63	10,9	10,64	8,97
3des-md5	9,49	12,29	9,64	9,01	9,62
3des-sha1	9,86	11,35	12,6	7,74	10,08
Aes-md5	8,36	8,4	8,89	9,38	8,48
Aes-sha1	8,63	8,82	8,43	9,97	8,83
Sin IPSec	8,27	83,48	8,2	8,16	8,05

Como se observa en la Figura 3.15, para el servicio de solo-autenticación la transformada que trabaja con el algoritmo de cifrado “3des” es la que menores valores de retardo presenta frente a la transformada que trabaja con el algoritmo “aes”.

Para el servicio de confidencialidad más autenticación, las transformadas que trabajan con el algoritmo de cifrado “aes” son aquellas con las cuales la variación de retardo muestra su mejor comportamiento. Cuando se realiza una comparación entre transformadas que trabajan con el mismo algoritmo de cifrado, aquellas que trabajan con el algoritmo de autenticación “md5” son aquellas para las cuales la métrica de estudio muestra su mejor comportamiento.

Figura 3.15 Valores promedio de variación de retardo en modo túnel para video



3.6.3.4 Variación de retardo para ESP en modo transporte. Como se observa en la Tabla 3.17, los valores para los edificios de Contaduría y la FIET muestran grandes fluctuaciones comparados con los valores promedio encontrados para la prueba; mientras para las diferentes transformadas la mayoría de los valores no superan los 10 milisegundos, en estos edificios se encuentran valores para transformadas que superan los 20 milisegundos. Fluctuaciones de 10 milisegundos son muy grandes para este tipo de métrica por lo que los valores para los edificios antes nombrados no se tienen en cuenta para el análisis de esta prueba.

Tabla 3.17 Prueba de variación de retardo en modo transporte para video

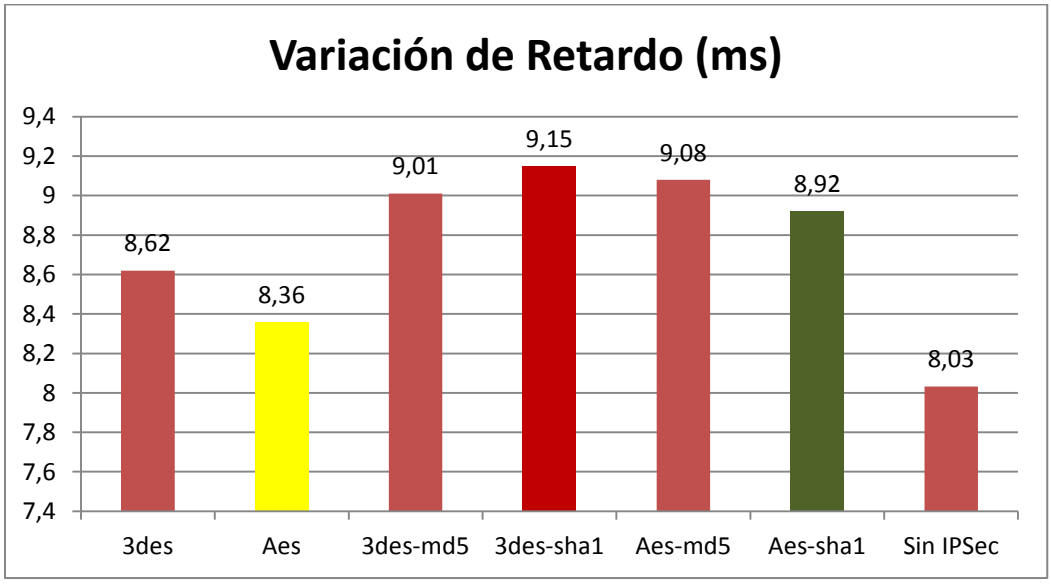
Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	8,49	8,20	8,92	21,7	9,08
Aes	7,73	8,36	8,68	15,27	8,48
3des-md5	8,13	8,13	9,20	7,59	9,46
3des-sha1	10,51	9,38	8,55	9,57	7,54
Aes-md5	9,53	8,09	10,48	13,47	10,38
Aes-sha1	8,05	9,34	8,15	19,98	8,92
Sin IPSec	8,24	8,17	8,14	23,54	7,14

Tabla 3.17 (Continuación)

Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	7,94	22,55	8,53	9,67	8,62
Aes	9,80	10,11	8,38	8,81	8,36
3des-md5	8,84	9,64	9,99	9,32	9,01
3des-sha1	7,52	53,01	11,25	9,27	9,15
Aes-md5	7,51	38,56	8,05	9,54	9,08
Aes-sha1	8,29	5,47	10,08	9,61	8,92
Sin IPSec	7,62	8,86	8,22	8,70	8,03

Como se puede observar en la Figura 3.16, los resultados de la prueba muestran un valor un mínimo de variación de retardo de 8,03 milisegundos cuando no se utilizó protocolo de seguridad y un valor máximo de 9,15 milisegundos cuando se utilizó la transformada de seguridad con los algoritmos de autenticación y cifrado "3des-sha1". Analizando este tipo de comportamiento se infiere que la métrica de variación de retardo no fue impactada de forma considerable por la utilización del protocolo de seguridad; se observa que no existen grandes diferencias entre las distintas transformadas de seguridad y el caso en el cual no se utilizó protocolo de seguridad.

Figura 3.16 Valores promedio de variación de retardo en modo transporte para video



A pesar de observarse pequeñas fluctuaciones entre los resultados para las distintas transformadas de seguridad, los valores de estos resultados se encuentran cercanos a los 10 milisegundos que es un valor alto para esta métrica comparada con otros resultados de las pruebas realizadas en el proyecto. De esta forma el tráfico de video es aquel para el cual la variación de retardo muestra su peor comportamiento comparado con los demás tipos de tráfico evaluados para el proyecto.

3.6.3.5 Pérdida de paquetes para ESP modo túnel. Como se observa en la Tabla 3.18, los resultados obtenidos en los edificios de Contaduría y la FIET para el caso en el cual no se utilizó protocolo de seguridad fluctúan de forma marcada comparados los valores obtenidos para las demás transformadas de seguridad, por este motivo los resultados obtenidos para estos edificios no fueron tenidos en cuenta para el análisis de esta prueba.

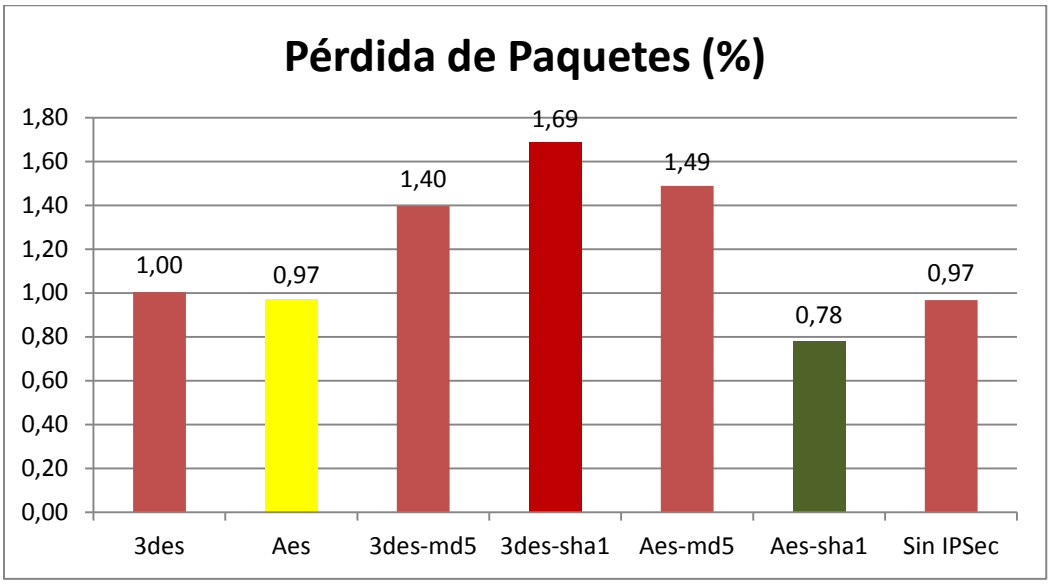
Tabla 3.18 Prueba de pérdida de paquetes en modo túnel para video

Edificio / Transformada (%)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	2,15	0,58	1,44	2,59	0,60
Aes	0,99	0,48	2,57	0,40	0,51
3des-md5	2,21	0,63	1,21	0,84	0,49
3des-sha1	2,31	1,53	2,06	1,55	1,18
Aes-md5	2,32	0,48	2,36	1,01	0,53
Aes-sha1	0,74	0,83	0,44	1,56	0,56
Sin IPSec	0,83	1,87	0,57	6,18	0,47
Edificio / Transformada (%)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	0,58	0,76	1,28	0,40	1,00
Aes	1,15	4,58	0,75	0,36	0,97
3des-md5	1,49	1,56	1,28	1,65	1,4
3des-sha1	1,78	1,85	0,49	2,45	1,69
Aes-md5	1,38	0,51	1,53	1,82	1,49
Aes-sha1	1,71	0,44	0,69	0,47	0,78
Sin IPSec	1,51	56,95	1,07	0,45	0,97

La transformada que utiliza los algoritmos de cifrado y autenticación “aes-sha1” es aquella para la cual la métrica de pérdida de paquetes mostró el mejor

comportamiento para esta prueba. Como se observa en la Figura 3.17 el porcentaje de pérdida de paquetes que presenta esta métrica está por debajo inclusive del valor mostrado en el caso en el cual no se utilizó protocolo de seguridad, este comportamiento es atípico comparado con el mostrado por las pruebas realizadas en el proyecto.

Figura 3.17 Valores promedio de pérdida de paquetes en modo túnel para video



Comparando los resultados de la métrica de las transformadas que prestan el servicio de solo-confidencialidad con el resultado del caso para el cual no se utiliza protocolo de seguridad, no se observan grandes fluctuaciones en los valores de los resultados. Analizado este comportamiento se infiere que la utilización de transformadas de seguridad para prestar el servicio de solo-confidencialidad sobre el tráfico de video no afecta de forma significativa la métrica de pérdida de paquetes.

3.6.3.6 Pérdida de paquetes para ESP en modo transporte. Como se observa en la Tabla 3.19, los resultados obtenidos en los edificios de Contaduría y la FIET no fueron tenidos en cuenta. Cuando se compara los valores de los resultados para las distintas transformadas en cada uno de estos edificios se observan grandes fluctuaciones entre estos resultados; este fenómeno impide observar el

comportamiento que pueda mostrar la métrica de "pérdida de paquetes" cuando se utiliza el protocolo de seguridad ESP.

Tabla 3.19 Prueba de pérdida de paquetes en modo transporte para video

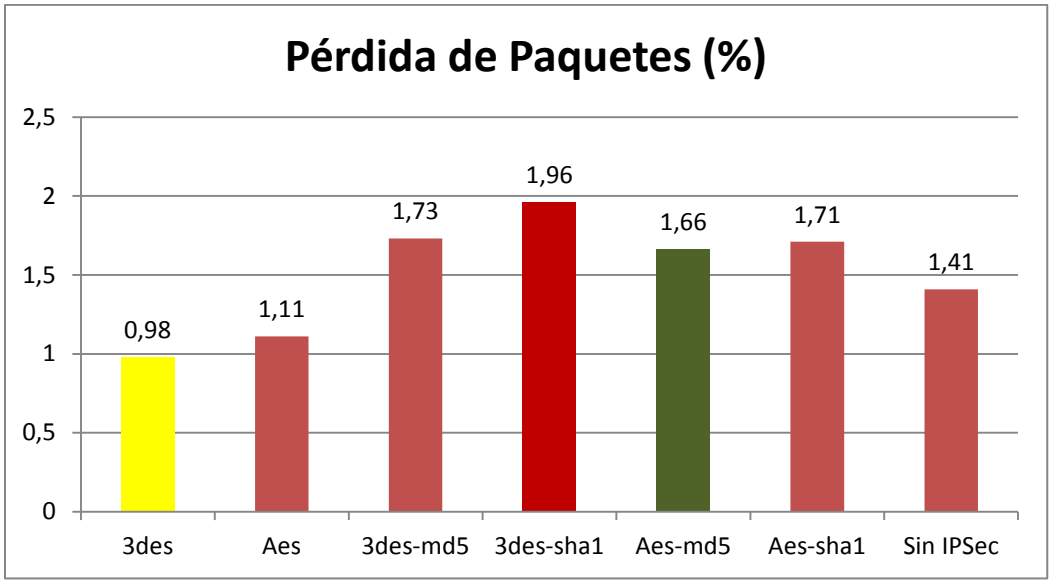
Edificio / Transformada (%)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	0,7	0,52	0,87	0,57	0,66
Aes	0,79	0,49	1,11	20,32	0,58
3des-md5	1,88	0,76	1,11	1,57	1,18
3des-sha1	2,44	1,06	1,41	1,84	1,6
Aes-md5	2,41	1,08	1,46	1,66	0,43
Aes-sha1	2,74	1,37	1,72	0,49	0,98
Sin IPSec	0,52	1,55	1,31	0,35	0,82
Edificio / Transformada (%)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	2,42	2,59	0,47	1,23	0,98
Aes	2,98	1,28	0,52	1,31	1,11
3des-md5	2,81	8,06	2,05	2,35	1,73
3des-sha1	2,68	0,69	2,29	2,25	1,96
Aes-md5	2,17	1,83	1,62	2,45	1,66
Aes-sha1	2,71	5,82	0,97	1,49	1,71
Sin IPSec	1,85	3,24	0,55	2,49	1,41

Las transformadas que prestan el servicio de solo-confidencialidad son aquellas que menores valores de porcentajes de pérdidas presentan acercándose al resultado obtenido para caso en el cual no se utilizó protocolo de seguridad como se puede observar en la Figura 3.18.

Cuando se presta el servicio de confidencialidad más autenticación si se compara las transformadas que trabajan con el mismo protocolo de cifrado, aquellas que utilizan el algoritmo de autenticación "md5" son aquellas que mejor comportamiento presentan; de forma análoga si se comparan las transformadas que trabajan con el mismo protocolo de autenticación, las que trabajan con el algoritmo de cifrado "3des" son las que muestran el mejor comportamiento. Analizando este comportamiento se infiere que para el tráfico de video independiente del tipo de seguridad prestado, los algoritmos de autenticaron y

cifrado para los cuales las transformadas de seguridad muestran su mejor comportamiento son “md5” y “3des”.

Figura 3.18 Valores promedio de pérdida de paquetes en modo transporte para video



3.6.4 Impacto de IPSec sobre el tráfico de VoIP

3.6.4.1 Retardo en un sentido para ESP en modo túnel. Para el análisis de esta prueba, no se tuvieron en cuenta los valores de los resultados obtenidos en los edificios de Contaduría, Salud y la FIET. Como se observa en la Tabla 3.20, los valores de retardo promedio están por debajo de los 6 milisegundos, mientras que los valores obtenidos en estos edificios superan los 100 milisegundos para algunas transformadas.

Tabla 3.20 Prueba de retardo en modo túnel para VoIP

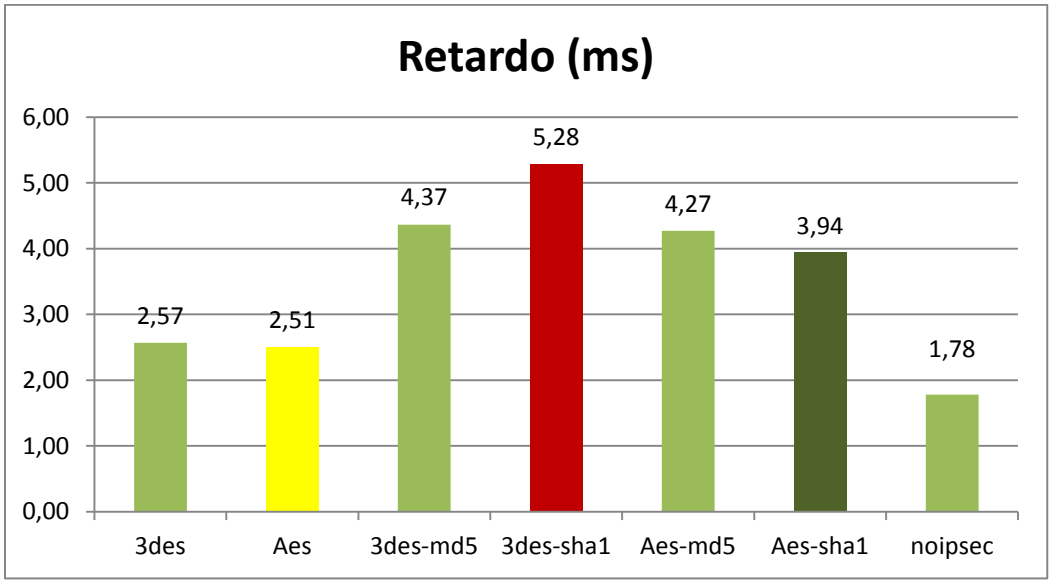
Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	3,46	6,47	0,72	19,89	2,61
Aes	3,19	4,44	0,78	118,03	4,24
3des-md5	5,26	7,90	0,76	400,43	6,42
3des-sha1	4,69	12,36	1,70	225,25	7,00

Tabla 3.20 (Continuación)

Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
Aes-md5	4,53	7,75	1,99	2,69	5,94
Aes-sha1	4,06	7,79	1,19	0,50	5,19
Sin IPSec	2,51	4,58	0,56	300,07	2,48
Edificio / Transformada (ms)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	1,06	19,17	1,10	7,01	2,57
Aes	1,69	3,32	0,70	166,72	2,51
3des-md5	3,05	2,03	2,82	2,86	4,37
3des-sha1	3,83	2,59	2,10	15,40	5,28
Aes-md5	3,92	7,79	1,50	1,59	4,27
Aes-sha1	4,08	1,77	1,32	3,57	3,94
Sin IPSec	0,33	1060,55	0,22	6,25	1,78

Como se observa en la Figura 3.19, cuando se presta el servicio confidencialidad más autenticación, las transformadas que utilizan el algoritmo de autenticación “aes” son aquellas que muestran el mejor comportamiento. Cuando se presta el servicio de solo-confidencialidad no se observan grandes diferencias entre las transformadas.

Figura 3.19 Valores promedio de retardo en modo túnel para VoIP



Cuando se compara el valor obtenido para el caso en el cual no se utilizó protocolo de seguridad con el valor del resultado para la transformada que presta el servicio de solo-confidencialidad que utiliza el algoritmo de cifrado "aes" la cual fue aquella que menor valor de retardo mostró para este servicio, la diferencia entre estos dos valores es 0.73 milisegundos. De igual manera, si se compara el valor de retardo para la transformada que presta el servicio de confidencialidad más autenticación que menos afecto esta métrica (aes-sha1) con el valor del resultado del caso en el que no se utilizó la transformada de seguridad, la diferencia entre estos valores es de 2.16 milisegundos; en estos términos queda en evidencia que para el tráfico de voz la métrica de retardo muestra un mayor impacto negativo en el desempeño cuando se utilizan algoritmos de autenticación en las transformadas de seguridad.

3.6.4.2 Retardo en un sentido para ESP en modo transporte. Como se observa en la Tabla 3.21, los valores para las transformadas de seguridad en los edificios de Contaduría y la FIET muestran grandes valores de retardo, en algunos casos por encima de los 50 milisegundos; si se compara estos valores con los valores promedios calculados para esta prueba, se observa que estos están muy por encima por lo que no se tuvo en cuenta los resultados en estos edificios para el análisis de esta prueba.

Tabla 3.21 Prueba de retardo en modo transporte para VoIP

Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	3,93	3,24	2,19	31,36	3,08
Aes	3,62	3,88	1,22	34,47	3,68
3des-md5	7,73	5,37	3,23	5,91	4,89
3des-sha1	5,73	6,39	3,73	8,29	5,04
Aes-md5	6,33	5,22	5,47	7,17	5,41
Aes-sha1	6,30	6,23	4,33	59,63	6,33
Sin IPSec	2,45	2,97	2,03	6,54	1,05
Edificio / Transformada (ms)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	4,53	3,64	2,37	6,49	3,23
Aes	4,12	21,75	1,94	6,15	3,08
3des-md5	5,52	4,50	4,3	8,33	5,17
3des-sha1	6,87	94,63	4,14	10,43	6,92
Aes-md5	6,39	31,27	4,98	10,06	5,63

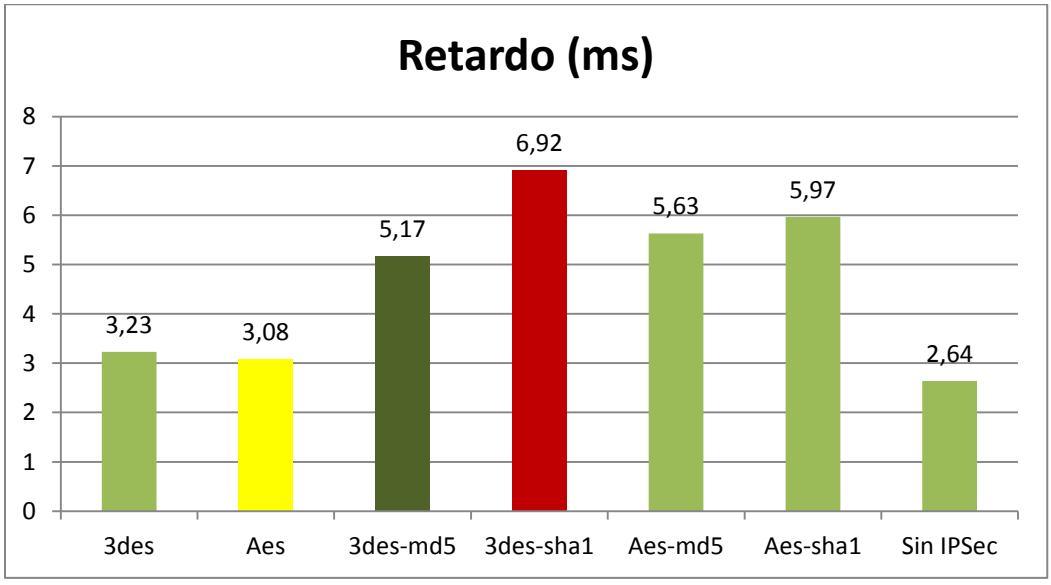
Tabla 3.21 (Continuación)

Edificio / Transformada (ms)	Educación	FIET	IPET	Salud	PROMEDIO
Aes-sha1	7,21	4,91	5,46	10,71	5,97
Sin IPSec	4,11	4,02	1,69	5,72	2,64

Como se puede observar en la Figura 3.20, los valores de los resultados obtenidos con las transformadas que prestan el servicio de solo-confidencialidad no muestran una diferencia importante entre ellas; para este caso la transformada que trabaja con “aes” como algoritmo de cifrado muestra un mejor comportamiento para la métrica de retardo.

El peor comportamiento de la métrica de retardo para esta prueba se presenta cuando se utilizan transformadas de seguridad que prestan el servicio de autenticación más cifrado, la transformada de seguridad con la combinación de algoritmos “3des-sha1” muestra el valor más alto de retardo que supera en más de 4 milisegundos al valor de retardo del caso en el cual no se utilizó protocolo de seguridad. De esta forma queda evidenciado el hecho que las transformadas que utilizan algoritmos para prestar el servicio de autenticación, son aquellas con las cuales el retardo muestra su peor comportamiento para el tráfico de voz.

Figura 3.20 Valores promedio de retardo en modo transporte para VoIP



3.6.4.2 Variación de retardo para ESP en modo túnel. Como se observa en la Tabla 3.22, los resultados promedios para variación de retardo para esta prueba están por debajo de los 0.6 milisegundos. Este umbral de retardo es superado de forma significativa por los valores de los resultados obtenidos en los edificios de Contaduría, la FIET, y de Salud; por esta razón al realizar un análisis del comportamiento de la métrica de variación de retardo para las distintas transformadas de seguridad no se tuvieron en cuenta los resultados obtenidos en estos edificios.

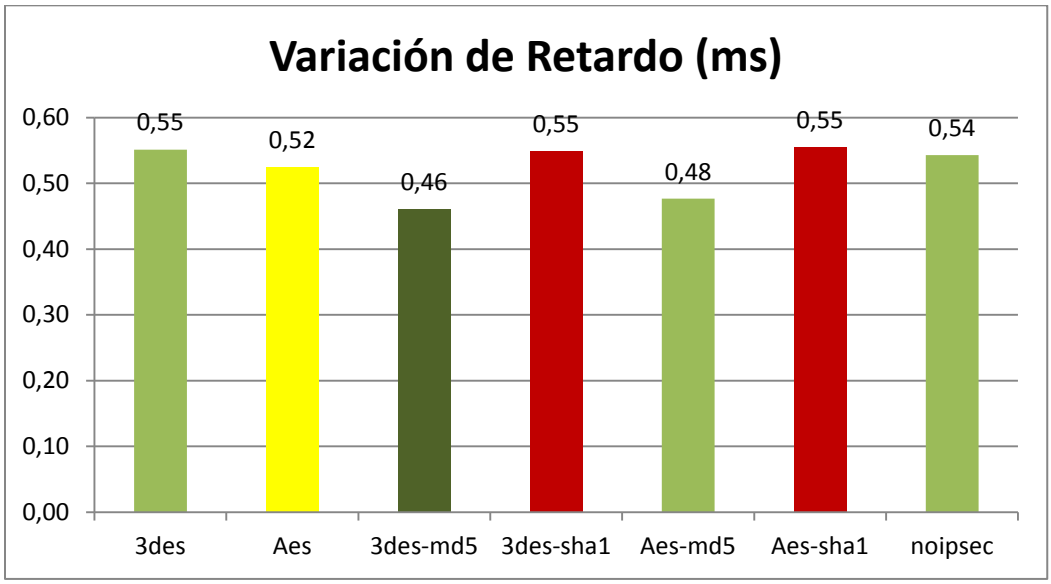
Tabla 3.22 Prueba de variación de retardo en modo túnel para VoIP

Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	0,51	1,02	0,3	2,62	0,49
Aes	0,47	0,88	0,35	7,16	0,72
3des-md5	0,44	0,58	0,29	20,49	0,53
3des-sha1	0,45	1,18	0,34	14,91	0,39
Aes-md5	0,45	0,84	0,32	3,49	0,39
Aes-sha1	0,46	1,06	0,35	1,17	0,55
Sin IPSec	0,51	0,86	0,35	7,86	0,37
Edificio / Transformada (ms)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	0,38	2,5	0,61	0,61	0,55
Aes	0,4	5,88	0,32	0,74	0,52
3des-md5	0,37	1,74	0,55	12,48	0,46
3des-sha1	0,41	3,44	0,52	0,69	0,55
Aes-md5	0,3	1,04	0,55	2,63	0,48
Aes-sha1	0,39	2,97	0,51	21,43	0,55
Sin IPSec	0,43	21,14	0,75	1,71	0,54

A partir de la Figura 3.21 y analizando el comportamiento de la variación de retardo para el tráfico de voz, se observa que los valores promedios para las distintas métricas no sufren grandes fluctuaciones para las distintas transformadas comparadas con el resultado del caso en el cual no se utilizó transformada de seguridad. En estos términos, los valores obtenidos para esta prueba no permiten observar un comportamiento que relacione la métrica de variación de retardo con las distintas transformadas de seguridad de IPSec; en otras palabras no se observa un impacto de las distintas transformadas de seguridad sobre la métrica

de variación de retardo cuando se transporta tráfico de voz en la red inalámbrica del caso de estudio.

Figura 3.21 Valores promedio de variación de retardo en modo túnel para VoIP



3.6.4.4 Variación de retardo para ESP en modo transporte. Como se observa en la Tabla 3.23, los valores de variación retardo promedio obtenidos para las distintas transformadas no superan el milisegundo para esta prueba. Para los edificios de Contaduría y la FIET los resultados para algunas transformadas superan notablemente los valores promedios y en algunos casos estos valores superan los 4 milisegundos; en los puntos de acceso ubicados en estos edificios no es posible controlar los niveles de congestión ni siquiera para los horarios nocturnos de prueba lo que introduce grandes fluctuaciones en los resultados que obligaron a no tenerlos en cuenta para el análisis del comportamiento de la métrica.

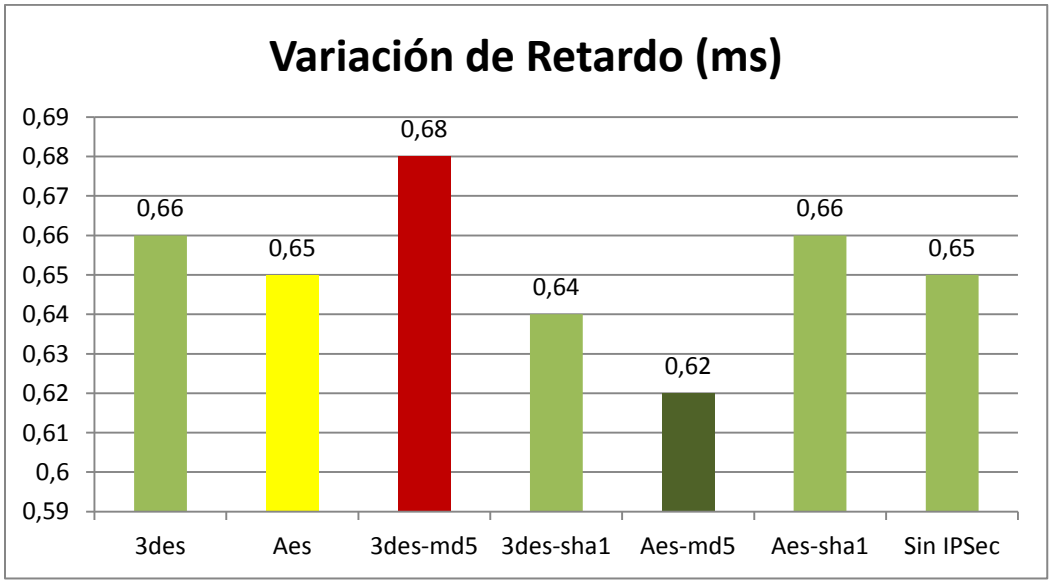
Tabla 3.23 Prueba de variación de retardo en modo transporte para VoIP

Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	0,77	0,52	0,61	3,89	0,45
Aes	0,60	0,71	0,38	3,78	0,55
3des-md5	0,61	0,54	0,56	0,57	1,30

Tabla 3.23 (Continuación)

Edificio / Transformada (ms)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des-sha1	0,78	0,65	0,61	0,78	0,46
Aes-md5	0,52	0,70	0,59	0,67	0,55
Aes-sha1	0,73	0,62	0,61	4,44	0,42
Sin IPSec	0,48	0,62	0,63	0,83	0,42
Edificio / Transformada (ms)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	0,75	0,37	0,58	0,97	0,66
Aes	0,72	2,11	0,45	1,17	0,65
3des-md5	0,44	0,91	0,62	0,66	0,68
3des-sha1	0,68	8,71	0,62	0,67	0,64
Aes-md5	0,47	2,31	0,62	0,87	0,62
Aes-sha1	0,56	0,64	0,88	0,77	0,66
Sin IPSec	0,70	0,61	0,41	0,98	0,65

Figura 3.22 Valores promedio de variación de retardo en modo transporte para VoIP



Como se observa en la Figura 3.22, los valores de retardo para los resultados de esta prueba oscilan entre 0.62 y 0.68 milisegundos lo que ubica el valor de los resultados de las distintas transformadas de seguridad en un rango de 0.06 milisegundos. Comparando estos valores con el obtenido para el caso en el cual no se utilizó protocolo de seguridad (0.65 milisegundos), los valores de variación

de retardo para las distintas transformadas no muestran un patrón de comportamiento para esta métrica en función de las distintas transformadas de seguridad que prestan los servicios de seguridad propiciados por IPSec.

3.6.4.5 Pérdida de paquetes para ESP en modo túnel. Los valores porcentuales de paquetes perdidos para los edificios están en su mayoría por debajo del 0.5 % como se observa en la Tabla 3.24. Este tipo de comportamiento no se presentó en los edificios de Contaduría, la FIET y Salud donde el resultado para algunas transformadas de seguridad supera el 4%, estas grandes fluctuaciones no permiten un análisis coherente de la métrica y no fueron tenidos para esta prueba.

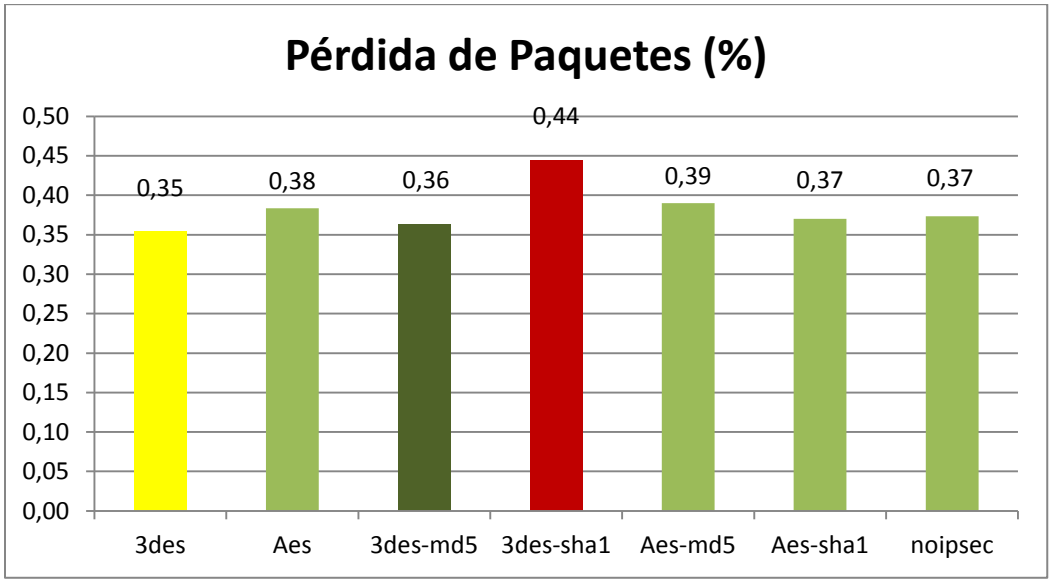
Tabla 3.24 Prueba de pérdida de paquetes en modo túnel para VoIP

Edificio / Transformada (%)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	0,21	0,38	0,37	0,31	0,35
Aes	0,19	0,53	0,39	0,55	0,37
3des-md5	0,19	0,4	0,37	3,33	0,37
3des-sha1	0,22	0,21	0,37	22,23	0,35
Aes-md5	0,5	0,21	0,37	0,59	0,37
Aes-sha1	0,2	0,39	0,37	0,52	0,48
Sin IPSec	0,19	0,37	0,39	0,63	0,44
Edificio / Transformada (%)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	0,38	1,41	0,43	0,31	0,35
Aes	0,37	2,51	0,45	0,41	0,38
3des-md5	0,37	0,94	0,48	0,92	0,36
3des-sha1	0,36	2,49	0,43	1,17	0,44
Aes-md5	0,39	0,5	0,5	5,46	0,39
Aes-sha1	0,39	0,81	0,39	1,48	0,37
Sin IPSec	0,38	4,65	0,47	1,39	0,37

Como se observa en la Figura 3.23, los porcentajes de pérdidas de paquetes más altos resultan cuando se trabaja con la transformada de seguridad que utiliza los algoritmos de autenticación y cifrado “3des-sha1”. Los valores de los resultados de las demás transformadas de seguridad comparadas con el resultado para el caso en el cual no se utilizó protocolo de seguridad no muestran grandes fluctuaciones.

Al analizar estos resultados no se logra observar el impacto negativo que tiene el uso del protocolo de seguridad sobre la métrica de paquetes perdidos para el tráfico de voz.

Figura 3.23 Valores promedio de pérdida de paquetes en modo túnel para VoIP



3.6.4.6 Pérdida de paquetes para ESP en modo transporte. Como es una constante para las pruebas realizadas en el proyecto, los resultados en los edificios de Contaduría y la FIET muestran grandes fluctuaciones con respecto a los valores promedios calculados como se observa en la Tabla 3.25. Esta es la razón para no tener en cuenta estos resultados en el análisis de las prueba ya que estos valores no permiten observar de forma adecuada el comportamiento de la métrica.

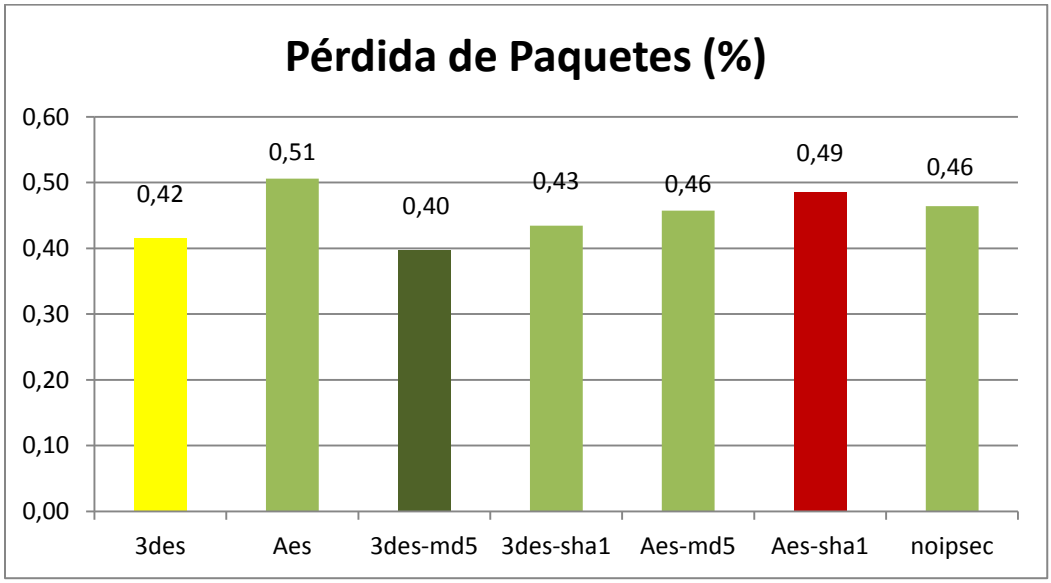
Tabla 3.25 Prueba de pérdida de paquetes en modo transporte para VoIP

Edificio / Transformada (%)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
3des	0,47	0,35	0,52	0,45	0,21
Aes	0,91	0,64	0,44	0,36	0,39
3des-md5	0,34	0,29	0,31	0,26	0,41
3des-sha1	0,41	0,41	0,46	0,47	0,35
Aes-md5	0,39	0,39	0,39	5,44	0,54

Tabla 3.25 (Continuación)

Edificio / Transformada (%)	Artes	Carmen	Casa Rosada	Contaduría	Derecho
Aes-sha1	0,51	0,51	0,59	0,52	0,32
Sin IPSec	0,45	0,45	0,37	0,35	0,43
Edificio / Transformada (%)	**Educación**	**FIET**	**IPET**	**Salud**	**PROMEDIO**
3des	0,51	0,48	0,64	0,21	0,42
Aes	0,49	0,76	0,28	0,39	0,51
3des-md5	0,46	4,56	0,56	0,41	0,40
3des-sha1	0,55	0,42	0,41	0,45	0,43
Aes-md5	0,46	0,83	0,39	0,64	0,46
Aes-sha1	0,64	5,54	0,41	0,42	0,49
Sin IPSec	0,57	0,74	0,45	0,53	0,46

Figura 3.24 Valores promedio de pérdida de paquetes en modo transporte para VoIP



Como se observa en la Figura 3.24, el porcentaje de pérdida de paquetes para el caso en el cual no se utilizó protocolo de seguridad es del 0.46%; la transformada que mayor porcentaje de pérdidas presentó fue aquella que trabaja con el algoritmo de cifrado “aes” con el 0.51% de los paquetes perdidos siendo la diferencia entre estos valores apenas de 0.05 puntos porcentuales. De esta forma se evidencia que los valores porcentuales para pérdida de paquetes no reflejan un

comportamiento que relacione esta métrica con las diferentes transformadas de seguridad.

3.7 SÍNTESIS DEL IMPACTO DE IPSEC SOBRE EL DESEMPEÑO DE LA RED INALÁMBRICA DE LA UNIVERSIDAD DEL CAUCA AL UTILIZAR LOS DISTINTOS TIPOS DE TRÁFICOS

Para poder observar de manera adecuada el impacto que tienen las distintas transformadas de seguridad del protocolo ESP en la red inalámbrica de la Universidad del Cauca con los distintos tipos de tráfico se realizaron una serie de tablas con celdas de colores donde se utilizó la siguiente convención:

- El color rojo representa mayores incrementos en los valores de los resultados para las distintas transformadas de seguridad.
- El color verde representa menores incrementos en los valores de los resultados para las distintas transformadas de seguridad.
- El color amarillo representa incrementos medios en los valores de los resultados para las distintas transformadas de seguridad.

3.7.1 Tráfico Parametrizado

3.7.1.1 Servicio de solo-confidencialidad. Como se puede observar en la tabla 3.26, para la prestación del servicio de solo-confidencialidad, la transformada que trabajó con el algoritmo de autenticación “aes” mostró los menores incrementos para las métricas de retardo y pérdida de paquetes; para el caso de la métrica de variación de retardo no se observaron variaciones significativas entre las dos transformadas.

Tabla 3.26 Síntesis del Impacto de IPSec para el servicio de solo-confidencialidad

Parámetros	3DES	AES
Retardo		
Variación de Retardo		
Pérdida de Paquetes		

3.7.1.2 Servicios de confidencialidad más autenticación. Como se puede observar en la tabla 3.27, cuando se prestaron los servicios de confidencialidad más autenticación, las transformadas que trabajaron con el algoritmo de autenticación “md5” fueron aquellas que menor impacto tuvieron sobre las distintas métricas de medición del desempeño.

Tabla 3.27 Síntesis del Impacto de IPSec para el servicio de confidencialidad más autenticación

Parámetros	3DES-MD5	3DES-SHA1	AES-MD5	AES-SHA1
Retardo				
Variación de Retardo				
Pérdida de Paquetes				

3.7.2 Tráfico de Datos

3.7.2.1 Servicio de solo-confidencialidad. Como se puede observar en la tabla 3.28, para la prestación del servicio de solo-confidencialidad, la transformada que trabajó con el algoritmo de autenticación “aes” mostró los menores incrementos para la métrica de retardo; para el caso de la métrica de variación de retardo no se observaron variaciones significativas entre las dos transformadas.

Tabla 3.28 Síntesis del Impacto de IPSec para el servicio de solo-confidencialidad

Parámetros	3DES	AES
Retardo		
Variación de Retardo		

3.7.2.2 Servicios de confidencialidad más autenticación. Como se puede observar en la tabla 3.29, cuando se prestaron los servicios de confidencialidad más autenticación, las transformadas que trabajaron con algoritmo de cifrado “aes” fueron aquellas que menor impacto tuvieron sobre las distintas métricas de medición del desempeño.

Tabla 3.29 Síntesis del Impacto de IPSec para el servicio de confidencialidad más autenticación

Parámetros	3DES-MD5	3DES-SHA1	AES-MD5	AES-SHA1
Retardo				
Variación de Retardo				

3.7.3 Tráfico de Video

3.7.3.1 Servicio de solo-confidencialidad. Como se puede observar en la tabla 3.30, para la prestación del servicio de solo-confidencialidad, la transformada que trabajó con el algoritmo de autenticación “aes” mostró los menores incrementos para la métrica de retardo; para el caso de las métricas de variación de retardo y pérdida de paquetes no se observaron variaciones significativas entre las dos transformadas.

Tabla 3.30 Síntesis del Impacto de IPSec para el servicio de solo-confidencialidad

Parámetros	3DES	AES
Retardo		
Variación de Retardo		
Pérdida de Paquetes		

3.7.3.2 Servicios de confidencialidad más autenticación. Como se puede observar en la tabla 3.31, cuando se prestaron los servicios de confidencialidad más autenticación, las transformadas que trabajaron con algoritmo de cifrado “aes” fueron aquellas que menor impacto tuvieron sobre las distintas métricas de medición del desempeño.

Tabla 3.31 Síntesis del Impacto de IPSec para el servicio de confidencialidad más autenticación.

Parámetros	3DES-MD5	3DES-SHA1	AES-MD5	AES-SHA1
Retardo				
Variación de Retardo				
Pérdida de Paquetes				

3.7.4 Tráfico de VoIP

3.7.4.1 Servicio de solo-confidencialidad. Como se puede observar en la tabla 3.32, para la prestación del servicio de solo-confidencialidad, la transformada que trabajó con el algoritmo de autenticación “aes” presentó los menores incrementos para las métricas de retardo y variación de retardo; para el caso de la métrica de pérdida de paquetes, la transformada que trabajó con el algoritmo “3des” fue aquella que menores incrementos presentó para el tráfico de voz.

Tabla 3.32 Síntesis del Impacto de IPSec para el servicio de solo-confidencialidad

Parámetros	3DES	AES
Retardo		
Variación de Retardo		
Pérdida de Paquetes		

3.7.4.2 Servicios de confidencialidad más autenticación. Como se puede observar en la tabla 3.33, cuando se prestaron los servicios de confidencialidad más autenticación, las transformadas que trabajaron con las combinaciones de algoritmos “3des-md5” y “aes-sha1” fueron aquellas para las cuales el retardo presentó menores incrementos; para el caso de la métrica de variación de retardo, la transformada que menores incrementos presentó fue aquella que trabajo con los algoritmos “aes-md5”. Las transformadas que trabajaron con el algoritmo de autenticación “md5” fueron aquellas que menores incrementos presentaron para la métrica de pérdida de paquetes.

Tabla 3.33 Síntesis del Impacto de IPSec para el servicio de confidencialidad más autenticación.

Parámetros	3DES-MD5	3DES-SHA1	AES-MD5	AES-SHA1
Retardo				
Variación de Retardo				
Pérdida de Paquetes				

3.8 PROPUESTA DE SEGURIDAD PARA LA RED INALÁMBRICA DE LA UNIVERSIDAD DEL CAUCA

Para implementar servicios de seguridad propiciados por IPSec haciendo uso de la red inalámbrica de la Universidad del Cauca y teniendo en cuenta los resultados obtenidos durante la realización del proyecto se presentan las siguientes recomendaciones:

- Para implementar el servicio de solo-confidencialidad, se recomienda trabajar con la transformada de seguridad que utilice el algoritmo de cifrado “aes”.

- Para implementar los servicios de confidencialidad más autenticación, se recomienda trabajar con la transformada que utilice la combinación de algoritmos “aes-md5”.

Las recomendaciones que se hicieron anteriormente solo tienen en cuenta el impacto que tienen las distintas transformadas de seguridad en el desempeño de las redes que hacen uso de la tecnología de acceso Wi-Fi. Las vulnerabilidades de seguridad de las distintas transformadas no son objeto de este estudio por lo cual no fueron tenidas en cuenta en la presente propuesta.

4. CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS

En el trabajo de grado se alcanzaron los objetivos propuestos, de esta forma se recopila la información necesaria para la implementación de IPSec en la red inalámbrica Wi-FI de la Universidad del Cauca teniendo en cuenta el impacto que pueda tener la utilización de esta arquitectura para la protección de la información a nivel IP. Por otro lado el trabajo de grado se constituye como una guía de gran utilidad para generar nuevos procesos de investigación y desarrollo en el área de seguridad de redes. De igual manera la información consignada en el proyecto es necesaria para la implementación del proyecto de seguridad para la protección de los servicios críticos de la Universidad del Cauca.

4.1 CONCLUSIONES

- La implementación del servicio de autenticación tiene un mayor impacto negativo en el desempeño de la red que la implementación del servicio de confidencialidad.

- Cuando IPSec con su protocolo de seguridad ESP presta el servicio de confidencialidad, el uso del algoritmo de cifrado “aes” en las transformadas de seguridad, permite un mejor desempeño en las redes inalámbricas Wi-Fi.

- Cuando IPSec con su protocolo de seguridad ESP presta el servicio de autenticación, el uso del algoritmo de autenticación “md5” en las transformadas de seguridad, permite un mejor desempeño en las redes inalámbricas Wi-Fi.

- Cuando IPSec con su protocolo de seguridad ESP presta los servicios de confidencialidad más autenticación, el uso de la combinación de algoritmos de cifrado y autenticación “aes-md5” en las transformadas de seguridad, permiten un mejor desempeño en las redes inalámbricas Wi-Fi.

4.2 RECOMENDACIONES

Para realizar el estudio del impacto en el desempeño de la red inalámbrica de la Universidad del Cauca al implementar servicios de seguridad propiciados por IPSec, son necesarios una serie de recomendaciones que facilitan la obtención y el análisis de los resultados. Estas son:

- Cuando se realiza las pruebas en horarios diurnos, parámetros como los niveles de congestión impactan la red de tal forma, que al implementar los servicios de seguridad no se logra observar de forma óptima el impacto que estos puedan tener sobre el desempeño de la red; por esta razón se recomienda hacer las pruebas en horarios nocturnos para minimizar los niveles de tráfico.

- En trabajos anteriores [9] se utilizó la herramienta “OWAMP” de la IETF para medir el desempeño de red. Se debe tener en cuenta que la herramienta no funciona bien cuando se trabaja con enrutamiento por VLAN´s como es el caso de la red de información de la Universidad del Cauca. La herramienta D-ITG es una buena alternativa de solución a este problema ya que además de medir las métricas de desempeño, tiene un módulo generador que permite la implementación distintos tipos de tráfico.

4.3 TRABAJOS FUTUROS

A través del cumplimiento de los objetivos del trabajo de grado, fue posible identificar nuevas investigaciones concernientes al impacto de IPSec sobre el desempeño de las redes inalámbricas:

- Analizar el desempeño de las distintas transformadas de seguridad teniendo en cuenta las vulnerabilidades que estas puedan tener.

- Implementar los servicios de seguridad propiciados por IPSec en los servidores que prestan los servicios críticos en la red de información de la Universidad del Cauca.

REFERENCIAS BIBLIOGRÁFICAS

[1] H. L. Francisconi, *IPsec en Ambientes IPv4 e IPv6*. Mendoza, Argentina: Carril Godoy Cruz 2801, 2005.

[2] S. Kent y R. Atkinson, *Security Architecture for the Internet Protocol*, IETF RFC 2401, Noviembre 1998. [En línea]. Disponible: http://www.ietf.org/rfc/rfc2401.txt.

[3] S. Kent y K. Seo, *Security Architecture for the Internet Protocol*, IETF RFC 4301, Diciembre 2005. [En línea]. Disponible: http://tools.ietf.org/rfc/rfc4301.txt.

[4] S. Kent y R. Atkinson, *IP Authentication Header,* IETF RFC 2402, Noviembre 1998. [En línea]. Disponible: http://tools.ietf.org/rfc/rfc2402.txt.

[5] S. Kent, *IP Authentication Header,* IETF RFC 4302, Diciembre 2005. [En línea]. Disponible: http://www.ietf.org/rfc/rfc4302.txt.

[6] S. Kent y R. Atkinson, *IP Encapsulating Security Payload (ESP),* IETF RFC 2406, Noviembre1998. [En línea]. Disponible: http://www.ietf.org/rfc/rfc2406.txt.

[7] S. Kent, *IP Encapsulating Security Payload (ESP),* IETF RFC 4303, Diciembre 2005. [En línea]. Disponible: http://www.ietf.org/rfc/rfc4303.txt.

[8] R. Atkinson, *Security Architecture for the Internet Protocol,* IETF RFC 1825, Agosto1995. [En línea]. Disponible: http://www.ietf.org/rfc/rfc1825.txt.

[9] I. C. Álvarez y J. P. Hoyos, "*Evaluación del Desempeño de las Redes IP con Servicios de Seguridad Propiciados por IPSec"*, Tesis de Pregrado, Facultad de Ingeniería Electrónica y Telecomunicaciones, Universidad del Cauca, Popayán, 2010.

[10] D. Maughan, M. Schertler, M. Schneider y J. Turner, *Internet Security Association and Key Management Protocol (ISAKMP),* IETF RFC 2408, Noviembre 1998. [En línea]. Disponible: http://www.ietf.org/rfc/rfc2408.txt.

[11] D. Harkins y D. Carrel, *The Internet Key Exchange (IKE),* IETF RFC 2409, Noviembre 1998. [En línea]. Disponible: http://www.ietf.org/rfc/rfc2409.txt.

[12] C. Kaufman, *Internet Key Exchange (IKEv2) Protocol,* IETF RFC 4306, Diciembre 2005. [En línea]. Disponible: http://www.ietf.org/rfc/rfc4306.txt.

[13] D. Piper, *The Internet IP Security Domain of Interpretation for ISAKMP,* IETF RFC 2407, Noviembre 1998. [En línea]. Disponible: http://www.ietf.org/rfc/rfc2407.txt.

[14] "Criptografía", Diccionario de la Real Academia Española – Vigésima segunda edición. [En línea]. Disponible: http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=criptografia.

[15] A. Biryukov y D. Khovratovich, "Related-key Cryptanalysis of the Full AES-192 and AES-256", Universidad de Luxemburgo, Luxemburgo, 2009.

[16] H. V. Tilborg y S. Jajodia, *Encyclopedia of Criptography and Security*, Segunda edición, Nueva York, USA: Springer, 2005.

[17] "Estándares inalámbricos (Pasado, presente y futuro de las redes wireless)", Xnet. [En línea].Disponible: http://www.x-net.es/tecnologia/wireless.pdf

[18] Recomendación *ITU-T E.800*, *Telephone Network and ISDN Quality of Service, Network Management and Traffic Engineering: Terms and Definitions Related to Quality of Service and Network Performance Including Dependability*, International Telecommunication Union, 1995.

[19] Recomendacion *ITU-T I.350*, *Integrated Services Digital Network (ISND) Overall Network Aspects and Functions: General Aspects of Quality of Service and Network Performance in Digital Networks, Including ISDNs*, International Telecommunication Union, 1993.

[20] V. Paxson, G. Almes, J. Mahdavi y M. Mathis, *Framework for IP Performance Metrics,* IETF RFC 2330, Mayo 1998. [En línea]. Disponible: http://www.ietf.org/rfc/rfc2330.txt.

[21] Recomendacion *ITU-T Y.1543*, *Measurements in IP networks for inter-domain performance assessment,* International Telecommunication Union, 2007.

[22] Recomendacion *ITU-T Y.1540*, *Internet protocol data communication service – IP packet transfer and availability performance parameters,* International Telecommunication Union, 2007.

[23] Recomendación *ITU-T Y.1541*, Network performance objectives for IP-based services, International Telecommunication Union, 2002.

[24] G. Almes, S. Kalidindi y M. Zekauskas, *A One-way Delay Metric for IPPM,* IETF RFC 2679, Septiembre 1999. [En línea]. Disponible: http://www.ietf.org/rfc/rfc2679.txt.

[25] A. Morton y B. Claise, *Packet Delay Variation Applicability Statement,* IETF RFC 5481, Marzo 2009. [En línea]. Disponible: http://www.ietf.org/rfc/rfc5481.txt.

[26] C. Demichelis y P. Chimento*, IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)*, IETF RFC 3393, Noviembre 2002. [En línea]. Disponible: http://www.ietf.org/rfc/rfc3393.txt.

[27] J. Mahdavi y V. Paxson, *IPPM Metrics for Measuring Connectivity*, IETF RFC 2678, Septiembre 1999. [En línea]. Disponible: http://www.ietf.org/rfc/rfc2678.txt.

[28] V. Raisanen, G. Grotefeld y A. Morton, *Network performance measurement with periodic streams*, IETF RFC 3432, Noviembre 2002. [En línea]. Disponible: http://www.ietf.org/rfc/rfc3432.txt.

[29] A. Botta, A. Dainotti, A. Pescapè, *"Multi-protocol and multi-platform traffic generation and measurement*", INFOCOM 2007 DEMO Session, May 2007, Anchorage (Alaska, USA).

[30] V. Manral, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*, IETF RFC 4835, Abril 2007. [En línea]. Disponible: http://tools.ietf.org/rfc/rfc4835.txt.

[31] W. Willinger y M.W.Garrett “Analysis, modeling,and generation of self similar VBR video traffic”, 1994.