ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

ESCUELA DE POSTGRADO Y EDUCACIÓN CONTÍNUA

MAESTRÍA EN INTERCONECTIVIDAD DE REDES

TESIS DE GRADO

ANÁLISIS DE LA TÉCNICA "PACKET CLASSIFICATION" Y SU APLICACIÓN EN LA PROVISIÓN DE QoS EN LA TRANSMISIÓN DE VOIP EN IPV4 E IPV6

Presentado por: *Barragán Torres René Alfonso*

Director de Tesis: *Ingeniero Washington Luna*

Abril 2013

Aprobación del documento por los Miembros del Tribunal

Ing. Ms.C. Fernando Proaño

DIRECTOR DE LA EPEC

Ing. Washington Luna: M.Sc.

DIRECTOR DE TESIS

Ing. Eduardo Villa: M.Sc.

MIEMBRO

Ing. Alberto Arellano: M.Sc.

MIEMBRO

INDICE

LISTA DE CUADROS

LISTA DE FIGURAS

ÍNDICE DE ABREVIATURAS

PC: Packet Classification

IPV4: Protocolo de Internet Versión 4

IPV6: Protocolo de Internet Versión 6

QoS: Calidad de Servicio

LACNIC: Registro de direcciones de internet para América Latina y el Caribe

VOIP: Voz Sobre Protocolo de Internet

IP: Protocolo de Internet

D-ITG: Distributed Internet Traffic Generator

RFc: Referencias

RFC: Petición de Comentarios

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos

DEDICATORIA

La dedicatoria de este proyecto de investigación es para mis Padres a quienes les amo mucho, siempre han sido el apoyo en mis buenas y malas decisiones, a mis primos Fernando y Shirley, a Juan Fernando y María Gracia que son el alma de cada uno de mis días, a mis hermanos, familiares y profesores que me supieron ayudar.

AGRADECIMIENTO

Mi agradecimiento es hacia Dios, mis padres y familia ya que siempre supieron guiarme por el sendero de los buenos modales, la honestidad y la persistencia para poder culminar mis estudios y la confianza entregada en cada paso de mi vida. Un agradecimiento muy especial a Fernando y Shirley quienes con su ejemplo de familia hicieron que no me pierda entre tantos inconvenientes que ocurrieron en mi vida, ya son los pilares fundamentales de mi existencia. A mi prima Violeta, a mis profesores y tutor de tesis ya que sin ellos no habría culminado esta investigación.

RESUMEN

La presente investigación tiene como objetivo analizar la técnica “Packet Classification” y su aplicación en la provisión de Calidad de Servicio en la transmisión de VOIP en redes IPV4 e IPV6 haciendo uso de los equipos CISCO en los Laboratorios de la Academia CISCO de la Escuela Superior Politécnica de Chimborazo.

Los métodos usados para este trabajo fueron: Científico para determinar la relación existente entre los escenarios planteados logrando de esta manera la comprobación de la hipótesis. También se empleo el método Deductivo que permitió realizar el análisis de los mecanismos de QoS aplicado al tráfico de VOIP en IPV4 e IPV6 ya que se estudiaron desde una definición y características generales hacia los detalles más particulares. Los materiales utilizados fueron: Software D-ITG, IOS CISCO c2801.adviipservicesk9-mz.124-8a.bin, Software DIAGNOS.I Versión I, Algoritmo para VOIP af31 y el Códec G.711.

De la tabulación y recolección de resultados se obtuvo una mejora en el Jitter utilizando la técnica “Packet Classification”. Esto produjo una mejor calidad de servicio al transmitir tráfico de VOIP. Por lo que se concluye que la aplicación de la Técnica Packet Classification provee una adecuada calidad de servicio para VOIP en redes IPV4 e IPV6. Se creó una guía para la implementación de la técnica citada para redes de VOIP en IPV4 e IPV6.

Se recomienda utilizar un nivel de 50 para manejar la prioridad de las políticas de entrada, ya que brindo una mejora en el Jitter en IPV4 e IPV6.

SUMMARY

This research aims to analyze the technique "Packet Classification" and its application in the provision of Quality of Service in VoIP transmission in IPV4 and IPV6 networks using CISCO equipment in the laboratories of the CISCO Academy at the Polytechnic University of Chimborazo.

The methods used for this work were: Scientist to determine the relationship between the proposed scenarios thus achieving the hypothesis testing. Also, the deductive method that allowed for the analysis of QoS mechanisms applied to VoIP traffic in IPV4 and IPV6 as studied from a definition and general characteristics to more specific details was used. The materials used were: D-ITG Software, CISCO IOS c2801.adviipservicesk9-mz.124-8a.bin, DIAGNOS.I Software Version I, Algorithm for VOIP af31 and G.711 codec.

From tabulation and result collection, an improvement in the jitter using the technique "Packet Classification" was obtained. This produced a better quality of service to transmit VOIP traffic. As conclusion, the Packet Classification Technique provides an adequate quality of service for VOIP IPV4 and IPV6 networks. It was created a guide to the implementation of the above technique to VOIP networks IPV4 and IPV6.

It is recommended the use of level 50 to handle the priority input policy, since it showed a better improvement in the jitter in IPV4 and IPV6.

CAPITULO I

1.1 INTRODUCCIÓN

Planteamiento del Problema

La clasificación de paquetes se ha convertido en uno de los cuellos de botella para el funcionamiento eficaz de las modernas redes multimedia. El crecimiento de la demanda de ancho de banda por parte de los usuarios, que no sólo hacen uso de servicios más exigentes sino que utilizan las facilidades de comunicación de forma más intensiva, no puede ser satisfecho de manera sostenible incrementando los recursos de transmisión. En este escenario se ha tornado imprescindible el dotar a las redes de telecomunicación con técnicas que permitan controlar el performance (Quality of Service, QoS) de una manera técnica y económicamente viable.

El tráfico que circula en la red no es clasificado, es decir las diferentes aplicaciones generan paquetes y todos estos paquetes viajan a través de la red sin importar su nivel de prioridad, por lo que no es lo mismo transmitir un paquete de datos como de voz, es por esta razón que se hace necesaria la investigación de la técnica de QoS “Packet Classification”. La clasificación de paquetes proporciona un medio por el cual los paquetes generados por una aplicación pueden ser clasificados y priorizados posteriormente, antes de ser enviados a través de una red.

La técnica “Packet Classification” es el mecanismo por el cual el control del tráfico determina el flujo de los paquetes, y por lo tanto, el tratamiento que recibe el paquete. Una vez que el paquete ha sido clasificado como perteneciente a un determinado flujo, el programador de paquetes QoS es capaz tratar el paquete de acuerdo con los parámetros que se estime convenientes.

Como se puede visualizar esta técnica con el protocolo IPV4 ya no se la podrá implantar

ya que el protocolo está a punto de colapsar, según varias organizaciones lo ratifican, para lo cual se ha desarrollado un nuevo protocolo que suplirá al actual que predomina en la red es decir IPV4, este nuevo protocolo es IPV6, el mismo que ya no está en fase de diseño y experimentación. Todas las ventajas que introduce este nuevo protocolo (espacio virtualmente ilimitado de direcciones, seguridad a nivel de red, movilidad, multicas, etcétera) aparecen disponibles ante un mundo que todavía no deja de sorprenderse por el impacto de una tecnología, IPV4, que fue concebida allá por los años 60 con unos objetivos muy distintos de aquellos a los cuales sirve en la actualidad.

La mayoría de sistemas operativos están preparados para el nuevo protocolo y la emigración al mismo no debería suponer problemas al usuario final. No obstante, desde el punto de vista del profesional existe aún cierto recelo a la introducción de esta nueva tecnología.

El uso de internet para lograr una comunicación de voz ya no es novedad por el uso de la VOIP la cual tendrá que adaptarse a este nuevo protocolo como lo es el IPV6, pero para lograr una calidad en la implantación se debe hablar de mecanismos de QoS como “Packet Classification”, que serán los que determinen la calidad de la llamada.

En esta investigación se realizará un estudio de la técnica “Packet Classification” en IPV6 aplicado al tráfico de VOIP, en el cual se define los siguientes problemas:

La escasez de direcciones IPV4 trae la necesidad de migrar a IPV6 por lo cual la VOIP debe estar preparada para este nuevo protocolo.

La falta de priorización de tráfico en las redes IPV6 podría limitar el uso de las aplicaciones en tiempo real como lo es la VOIP

La baja calidad de la llamada podría ser uno de los principales inconvenientes que afronte la VOIP, si no existe un adecuado tratamiento de los paquetes de voz.

En la actualidad las implantaciones de VOIP se lo realiza con el protocolo IPV4, muchos centros de diferentes países se encuentran migrando sus sistemas a IPV6 según lo dice LACNIC [1].

Como se puede visualizar países como México, Costa Rica, Venezuela, Chile, Brasil y el mismo Ecuador entre otros, ya se encuentran implementando el protocolo IPV6 es por esta razón que se determina que la implantación de IPV6 es ya un hecho, si se desea continuar comunicándose haciendo uso de la VOIP se debería seguir estudiando la técnica "Packet Classification" aplicado al tráfico de VOIP. En la figura I.1 se puede visualizar los datos de LACNIC:

Organización	País/ Región	Estado de Implementación de IPv6			Detalles
		IPv6 ya implementado	*Actualmente implementando*	*Con planes de implementación*	
RIU - Red Interconexión Universitaria	Argentina		X		Desplegar
ET Latinoamérica	Argentina	X			Desplegar
RedCLARA	América Latina	X			Desplegar
ICE - Institute Costarricense de Electricidad y Telecomunicaciones	Costa Rica	X			Desplegar
Telecom Argentina S.A.	Argentina		X		Desplegar
SMITCOMS	Antillas Neerlandesas			X	Desplegar
Global Crossing	América Latina y Caribe	X			Desplegar
CENIT	Venezuela	X			Desplegar
Universidad Tecnica Federico Santa Maria (UTFSM)	Chile	X			Desplegar
Dualtec	Brasil	X			Desplegar
CTD	Chile	X			Desplegar
NIC Chile	Chile	X			Desplegar
NipCable de Brasil Telecom LTDA	Brasil	X			Desplegar
TRICOM	Republica Dominicana	X			Desplegar
Universidad Técnica Particular de Loja	Ecuador	X			Desplegar
NAP.EC	Ecuador	X			Desplegar
Cooperativa Telefónica de Villa Gobernador Gálvez Limitada (TelVGG)	Argentina	X			Desplegar
ETB S.A. ESP	Colombia		X		Desplegar
IPLAN	Argentina		X		Desplegar
RENATA	Colombia	X			Desplegar
Google	Global	X			Desplegar
Youtube	Global via Google Network	X			Desplegar
Universidad APEC	República Dominicana		X		Desplegar
Universidad Nacional Autonoma de Mexico (UNAM)	México	X	X		Desplegar

Figura I.1: Implementación de IPV6 en América
Fuente: http://portalIPV6.lacnic.net/es/quienes-est-n-implementando-IPV6-en-la-regi-n

En el análisis se podrá visualizar la técnica “Packet Classification” aplicada al tráfico de VOIP, con lo cual se realizará correctas y necesarias implantaciones de la VOIP sobre el protocolo IPV4 e IPV6 que tarde o temprano estará implantado en la totalidad de sistemas de cada país.

La relación presente entre el tráfico de VOIP y la técnica “Packet Classification” está claramente establecida ya que sin un correcto control del flujo de paquetes de VOIP la llamada podría entrecortarse y no hacer posible la comprensión del mensaje.

El estudio de la técnica “Packet Classification” en IPV4 e IPV6 aplicado al tráfico de VOIP, se lo realizará mediante la configuración de switch cisco en la Academia Cisco en la Escuela Superior Politécnica de Chimborazo, haciendo uso del software Asterisk mediante un ambiente de pruebas aplicando y no implementando la técnica “Packet Classification”.

1.2 Justificación

La importancia de este trabajo de investigación radica que en la actualidad no existe una correcta administración de los paquetes IP que generan los diferentes tipos de aplicaciones como la VOIP. En el futuro la implantación de VOIP sobre redes IPV4 e IPV6 van a quedar obsoletas si no se estudia adecuadas técnicas de QoS como “Packet Classification” para de esta manera asegurar la calidad de servicio QoS en la VOIP en el protocolo IPV4 e IPV6.

Mediante el estudio de la técnica “Packet Classification” se podrá obtener una mejora en el audio de la VOIP para el protocolo IPV4 e IPV6, que a futuro será el protocolo que

predominará en el medio.

Para lo anteriormente expuesto se implementará un escenario de pruebas en el cual se transmitirá tráfico de VOIP en IPV4 e IPV6 sin aplicar “Packet Classification” y otro escenario aplicando “Packet Classification”.

El escenario es el siguiente:

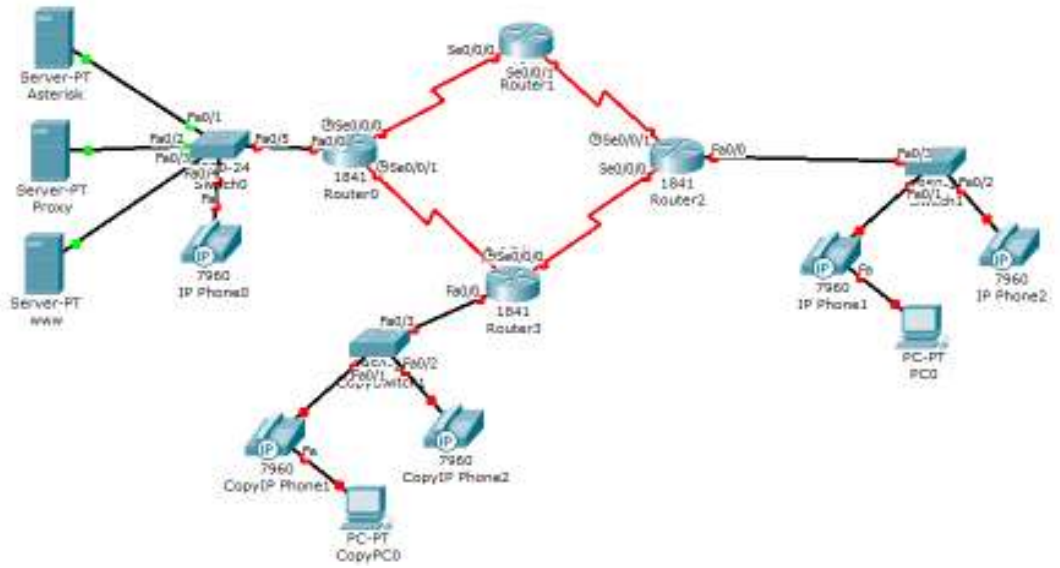


Figura I.2: Escenario de prueba para la técnica “Packet Classification” en IPV4 e IPV6 para el tráfico de VOIP
Fuente: Autor

Las pruebas se las realizara según los siguientes escenarios:

Primer escenario aplicando la técnica “Packet Classification” en IPV4

Segundo escenario no aplicando la técnica “Packet Classification” en IPV4.

Tercer escenario aplicando la técnica “Packet Classification” en IPV6

Cuarto escenario no aplicando la técnica “Packet Classification” en IPV6

1.3. Objetivos

1.3.1. Objetivo General

Analizar la técnica “Packet Classification” y su aplicación en la provisión de QoS en la transmisión de VOIP en IPV4 e IPV6

1.3.2. Objetivos Específicos

- Analizar la técnica “Packet Classification” en IPV4 e IPV6 para determinar la factibilidad de su aplicación en la transmisión de tráfico de VOIP.
- Diseñar un ambiente de pruebas para verificar la técnica “Packet Classification” en IPV4 e IPV6 en la trasmisión de VOIP
- Proponer una guía de implementación de la técnica “Packet Classification” en IPV6 para la transmisión del tráfico de VOIP.

1.4 Hipótesis

La aplicación de la técnica “Packet Classification” en la transmisión de VOIP proveerá una adecuada calidad de servicio en redes IPV4 e IPV6

Tipo: Causa Efecto

1.5 Operacionalización Conceptual

Tabla I.I: Operacionalización Conceptual de Variables

Variable	Tipo	Concepto
Técnica “Packet Classification” en la trasmisión de VOIP en IPV6 e IPV4	Independiente	Clasificación de tramas de red dependiendo de la aplicación que las genero las tramas
Performance en redes	Dependiente	Asegurar

IPV6 e IPV4		determinadas características de calidad en la transmisión de Información

Autor: René Barragán
Fuente: ESPOCH

1.6 Operacionalización Metodológica

Tabla I.II: Operacionalización Metodológica de Variables

VARIABLE	CATEGORIA/DIMENSION	INDICADORES	TÉCNICAS	FUENTE DE VERIFICACIÓN/INSTRUMENTOS
Técnica Packet Classification	Normal	Mapas de Políticas	Observación y recopilación de la información	Internet Libros Revistas Documentos RFC`s
		Niveles de Prioridad		
Performance	Normal	Jitter(ms)	Observación Pruebas	D-ITG
		Ancho de Banda		
		Delay		
		Tiempo Total		

Autor: René Barragán
Fuente: ESPOCH

CAPITULO II

Revisión de Literatura

En este capítulo se hará una revisión de los conceptos claves de las tecnologías utilizadas para la realización de este trabajo de investigación.

2.1 IPV6

2.1.1 Que es IPV6

El Protocolo de Internet version 6 (IPV6) (En español: Protocolo de Internet versión 6) es una versión del protocolo Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol version 4 (IPV4) RFC 791, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.

Diseñado por Steve Deering de Xerox PARC y Craig Mudge, IPV6 está destinado a sustituir a IPV4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. El nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles sus direcciones propias y permanentes.

A principios de 2010, quedaban menos del 10% de IPs sin asignar.1 En la semana del 3 de febrero del 2011, la IANA (Agencia Internacional de Asignación de Números de Internet, por sus siglas en inglés) entregó el último bloque de direcciones disponibles (33 millones) a la organización encargada de asignar IPs en Asia, un mercado que está en auge y no tardará en consumirlas todas.

IPV4 posibilita 4.294.967.296 (232) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos a cada

vehículo, teléfono, PDA, etcétera. En cambio, IPV6 admite 340.282.366.920.938.463.463.374.607.431.768.211.456 (2128 o 340 sextillones de direcciones) —cerca de 6,7 × 1017 (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de La Tierra.

2.1.2 Conceptos de IPV6

Según WIKIPEDIA **[2]** El Internet Protocol versión 6 (IPV6) (en español: *Protocolo de Internet versión 6*) es una versión del protocolo Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol versión 4 (IPV4) RFC 791, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.

Según Alessandro Porro **[9]** IPV6 es una versión protocolar diseñada para reemplazar a Internet Protocol versión 4 (IPV4); edición que actualmente está implementada en la gran mayoría de los dispositivos que acceden a Internet. Ahora, si bien el surgimiento de IPV6 se debe a necesidades de tipo estructural, al colapso de las direcciones IP existentes, su creación dio pie a la inclusión de novedades que hoy resultan interesantes; y que a su vez abren un enorme universo de posibilidades para trabajar en la red.

Tomando en cuenta los conceptos citados se determina que el protocolo IPV6 se desarrollo por el colapso del protocolo existente IPV4, este nuevo protocolo facilitará la implementación de nuevos servicios principalmente en los nuevos dispositivos que se están sumando a la conexión de internet.

2.1.3 ¿Porqué IPV6?

Se tomo en cuenta el protocolo IPV6 ya que como es de conocimiento general el protocolo IPV4 en pocos años quedara obsoleto, además de las ventajas que ofrece este nuevo protocolo.

La voz sobre IP implementada con este nuevo protocolo promete grandes cambios, como lo indican algunos estudios realizados.

Para determinar los beneficios se implementara un escenario de pruebas que se detalló en la justificación de esta tesis.

2.1.4 Características de IPV6

Mayor espacio de direccionamiento (RFC 2373 o draft de 16/09/2002)

Las direcciones pasan de los 32 a 128 bits, o sea de 2^32 direcciones (4.294.967.296) a 2^128 direcciones (3.402823669 e38, o sea sobre 1.000 sixtillones).

Esto hace que:

Desaparezcan los problemas de direccionamiento del IPV4 actual.

No sean necesarias técnicas como el NAT para proporcionar conectividad a todos los ordenadores/dispositivos de nuestra red.

Por tanto, todos los dispositivos actuales o futuros (ordenadores, PDAs, teléfonos GPRS o UMTS, neveras, lavadoras, etc.) podrán tener conectividad completa a Internet.

2.1.5 Seguridad (RFC 2401 y RFC 2411)

Uno de los grandes problemas achacable a Internet es su falta de seguridad en su diseño base. Este es el motivo por el que han tenido que desarrollarse, por ejemplo, el SSH o SSL, protocolos a nivel de aplicación que añaden una capa de seguridad a las

conexiones que pasan a través suyo.

IPV6 incluye IPsec, que permite autenticación y encriptación del propio protocolo base, de forma que todas las aplicaciones se pueden beneficiar de ello.

IPsec también ha sido diseñado para aportar interoperabilidad y no afectar a las redes y dispositivos que no lo implementan. Resaltar también que IPsec es independiente de los algoritmos criptográficos actuales, y es capaz de adaptarse a nuevos algoritmos según éstos vayan siendo definidos y puestos en marcha

2.1.6 Autoconfiguración (RFC 2462, en español)

Al igual que ocurría con el punto anterior, en el actual IPV4 han tenido que desarrollarse protocolos a nivel de aplicación que permitiesen a los ordenadores conectados a una red asignarles su datos de conectividad al vuelo. Ejemplos son el DHCP o BootP.

IPV6 incluye esta funcionalidad en el protocolo base, la propia pila intenta autoconfigurarse y descubrir el camino de conexión a Internet (router discovery)

Movilidad (RFC 3024)

Con la movilidad (o roaming) ocurre lo mismo que en los puntos anteriores, una de las características obligatorias de IPV6 es la posibilidad de conexión y desconexión de nuestro ordenador de redes IPV6 y, por tanto, el poder viajar con él sin necesitar otra aplicación que permita que ese enchufe/desenchufe se pueda hacer directamente.

2.1.7 Diferencias con IPV4

No hay direcciones broadcast (su función es sustituida por direcciones multicast).

Los campos de las direcciones reciben nombres específicos, denominamos prefijo a la

parte de la dirección hasta el nombre indicado (incluyéndolo).

Dicho prefijo nos permite conocer donde está ubicada dicha dirección, es decir, su ruta de encaminado.

Cualquier campo puede contener sólo ceros o sólo unos, salvo que explícitamente se indique lo contrario.

Las direcciones IPV6, indistintamente de su tipo (unicast, anycast o multicast), son asignadas a interfaces, no nodos. Dado que cada interfaz pertenece a un único nodo, cualquiera de las direcciones unicast de las interfaces del nodo puede ser empleado para referirse a dicho nodo.

Todas las direcciones han de tener, al menos, una dirección unicast link-local (enlace local).

Una única interfaz puede tener también varias direcciones IPV6 de cualquier tipo o ámbito.

Al igual que en IPV4, se asocia un prefijo de subred con un enlace, y se pueden asociar múltiples prefijos de subred a un mismo tiempo

El IPV6 tiene diferencias con respecto al IPV4 tanto para los operadores de la red como para los usuarios finales. El nuevo protocolo permite la conexión de millones de dispositivos con capacidad IP, que siempre están en funcionamiento y cada uno de ellos teniendo su propia y exclusiva dirección IP. Un creciente número de retos ha sido detectado al momento de utilizar el actual Protocolo de Internet IPV4 a lo largo de los años, incluyendo la escasez de direcciones que son esenciales para los mercados emergentes del Internet, donde el número de usuarios continúa sucediéndose en crecimiento exponencial. Algunos operadores se han adaptado a esta limitación de direcciones utilizando la NAT (Network Address Translation) o Conversión de la

Dirección de Red. La NAT proporciona una solución a las aplicaciones cliente/servidor con base en el Internet, pero resulta menos apropiada para aplicaciones de colega-a-colega {“peer-to-peer”) en cuando a comunicaciones móviles, lo que siempre limita en gran manera el despliegue de servicios innovadores en la Red. Los beneficios más notables que ofrece el IPV6 tienen que ver con el enorme espacio y capacidad para direcciones IP, seguridad incorporada y características de movilidad, "plug-and-play"(conecte y haga funcionar) hasta auto-configuración de direcciones, renumeración simplificada del sitio, redes y servicios de fácil re-diseño. Estas características inherentes al IPV6 ayudarán a reducir gastos de ejecución y minimizarán la carga administrativa para las empresas. Servicios innovadores tales como una movilidad “sin costuras” en la próxima generación requiere de accesibilidad global, “de colega a colega” y seguridad de extremo-a-extremo (“end-to-end”), algo esencial para los viajeros.

2.1.8 Reservas de espacios de direccionamiento en IPV6

Existen direcciones IPV6 reservadas que no pueden utilizarse para direcciones unicast convencionales, las más importantes son:

::/128 Dirección no especificada, equivalente a 0.0.0.0 de IPV4

::1/128 Dirección de loopback, equivalente a 127.0.0.1 de IPV4

fc00::/7 ULA, equivalente a las direcciones especificadas en RFC1918 de IPV4

Se divide a su vez en dos grupos:

fc00::/8 que se debe asignar de forma centralizada a través del denominado “ULA-Central”, aunque todavía no está definido. ?

fd00::/8 que se construye generando una cadena de 40 bits aleatoria, tal como se

define en el RFC4193

ff00::/8 Direcciones multicast, equivalente al rango 224.0.0.0/4 de IPV4

fe80::/10 Direcciones link-local, equivalente al rango 169.254.0.0/16 de IPV4.

2.2 VOIP en IPV6

La telefonía IP, combina la transmisión de voz y datos simultáneamente por la misma red informática basada en protocoló IP. Esta tecnología surge como una gran alternativa a telefonía convencional, trayendo nuevos servicios para los clientes y abarcando un tema económico. Las principales características son la interoperabilidad que pueden utilizar los proveedores de servicios dentro de la misma red en el sistema actual de telefonía, además agrega una calidad de servicio con una red de alta velocidad (calidad de la voz). Entre los elementos básicos están la central IP, el Gateway IP y los diferentes teléfonos IP. Al ocupar esta tecnología basada IP, en un tiempo cercano, tendrá una limitación por el tema de la direcciones IPV4 (2^32= 4294967296 direcciones posibles), las cuales se están agotando por el uso masivo de internet. Por esto se han visto en la necesidad de crear un nuevo protocolo de IP, llamado IPV6, que no es más que la continuación de IPV4, la gran novedad de este protocolo nuevo es que las direcciones son de 128 bits (21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A , 2^128 = 3,402823669209384634633746074317 7e+38 direcciones posibles), con esto se quiere arreglar el agotamiento de la direcciones de IPV4, además posee un campo de longitud fija, con la finalidad de minimizar el tiempo necesario para procesar y encaminar los datagramas por Internet haciéndolos fijo. De esta forma se agiliza el tráfico y se suprimen opciones pocos utilizada, entre otras características. Es allí en

donde se basa, en la necesidad de complementar dos tecnologías de futuro, en donde si bien actualmente en algunas empresas se están animando a ocupar telefonía ip, todavía no están al máximo como debería ser por todos los beneficios que conlleva. Por su parte en IPV6 a nivel mundial se han hecho algunas cosas y en el mundo se están preparando para poder llevar a cabo la implementación de IPV6.

2.3 Calidad de Servicio

Que es calidad de servicio

QoS o Calidad de Servicio (Quality of Service, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

2.3.1 Definiciones de calidad de servicio

Según la Dra. María del Carmen Romero Ternero en el ITU E.800 [5], QoS es: “Efecto global de las prestaciones de un servicio que determinan el grado de satisfacción de un usuario al utilizar dicho servicio.

Según la Dra. María del Carmen Romero Ternero en el IETF RFC 2386 [5], QoS es: “Conjunto de requisitos del servicio que debe cumplir la red en el transporte de un flujo”.

Según Carlos Montaño Vanega [6] la QoS también suele ser definida como un conjunto de tecnologías que permiten a los administradores de red manejar los efectos de la congestión del tráfico usando óptimamente los diferentes recursos de la red, en lugar de ir aumentando continuamente capacidad. En este punto es necesario prestar una

atención especial al hecho de que la QoS no crea ancho de banda

Recopilando los conceptos citados QoS son parámetros para determinar la calidad de un servicio en nuestro caso específico el tráfico de paquetes en redes de datos.

2.4 Técnica Packet Classification

2.4.1 ¿Qué es la Clasificación de Paquetes?

La clasificación de paquetes: Es la creación de grupos de paquetes para así definir como tratar a ese determinado paquete. Una vez clasificado, el paquete ya es accesible para los dispositivos que gestionan la QoS a lo largo de la red. Así, mediante la clasificación de paquetes, el tráfico de la red se puede dividir en múltiples niveles o clases de servicio.

Para realizar la clasificación de paquetes Cisco emplea:

2.4.1.1 Los class-maps.

Las listas de acceso (Acces List). Con ellas se puede dividir el tráfico entrante tomando datos de la cabecera de los paquetes tales como el puerto origen o destino, la dirección IP de origen o destino, etc.

Los Traffic Conditioners, que también pueden realizar clasificaciones del tráfico según se adapte o no al contrato.

2.4.1.2 Cómo definir una clase de tráfico

El primer paso que hay que seguir para implementar una clase de tráfico es poder separar los diferentes flujos de tráfico cuando éstos alcancen el router. Para poder definir una clase de tráfico se empleará el comando **class-map**. Mediante las clases de

tráfico, se podrán separar los paquetes que lleguen al router para aplicarles un tratamiento diferenciado.

2.4.1.2.3 Configuración

La sintaxis del comando class-map es:

class-map [match-any|match-all] class-name

class-map [match-any|match-all] class-name

El comando class-map:

El comando class-map se usa para definir una clase de tráfico. Una clase de tráfico contiene principalmente tres elementos: un nombre, una serie de comandos match y una instrucción de cómo evaluar esos comandos match.

El nombre se le da dentro de la línea del comando class-map. Por ejemplo, si se introduce el comando class-map trafico_telnet mientras se configura la clase de tráfico en el CLI, la clase se llamará trafico_telnet.

El comando class-map match-all se usa cuando deben coincidir todos los criterios de selección para que un paquete entre a formar parte de la clase. El comando class-map match-any cuando sólo se debe cumplir uno de los criterios para que el paquete pertenezca a la clase.

El comando match:

Los comandos match se usan para especificar los criterios para la clasificación de los paquetes. Los paquetes se comprueban para ver si cumplen con los criterios de selección especificados por los comandos match; si un paquete cumple el criterio especificado, el paquete será considerado miembro de la clase y será encaminado de acuerdo a las especificaciones de QoS que aparecen en la service policy. Los paquetes que no cumplen alguno de los criterios de selección son clasificados como miembros

de la clase por defecto. La clase por defecto se explicará más adelante.

Dentro de la clase especificaremos los criterios de selección de los paquetes usando el comando match seguido de:

access-group access-group, el criterio de selección se hará basándose en el número de la access-control list (ACL) especificado.

mach any, con este comando todos los paquetes pasarán a formar parte de la clase.

mach class-map class-map-name, para usar una clase como política de selección. El Modular QoS CLI permite a múltiples clases de tráfico (clases de tráfico anidadas, que son denominadas también class-maps anidadas), estar configuradas como una única clase.

mach cos cos-value [cos-value cos-value cos-value], para seleccionar paquetes basándose en el marcado de Clase de Servicio de la capa de enlace de datos.

mach destination-address dirección-MAC, usará la dirección MAC destino como criterio de selección.

match input-interface interface-name, utilizará la interfaz de entrada del paquete como criterio de selección.

match ip dscp ip-dscp-value[ip-dscp-value ip-dscp-value ip-dscp-value ipdscp-value ip-dscp-value ip-dscp-value ip-dscp-value], identificará un determinado IP DSCP como criterio de selección

match ip precedence ip-precedence-value[ip-precedence-value ip-precedencevalue ip-precedence-value], ídem que el anterior pero basándose en el valor del IP Precedence del paquete.

match ip rtp starting-port-number port-range, usará el Puerto del protocolo en tiempo real (RTP) como criterio de selección.

match mpls experimental number, para usar el valor del MPLS de los paquetes como criterio de selección.

match not, se usa para prevenir que un paquete pase a formar parte de una determinada clase.

match protocol protocol, para configurar el criterio de selección de una clase basándose en el protocolo del paquete.

match QoS-group QoS-group-value, para identificar un valor especifico de QoS como criterio de selección. El valor del grupo de QoS es local al router.

match source-address mac adress, usará la dirección MAC origen como criterio de selección.

2.4.1.3 Mapas de Politicas

El comando policy-map crea la política de tráfico. El propósito de un tráfico con política es implementar funciones específicas asociadas con una clase de tráfico. La política de tráfico contiene los siguientes componentes:

- Nombre de la Política del mapa
- El tráfico anteriormente creado mapa de clase o, de forma opcional, el mapa de Clase-default

2.4.1.4 Configuración de Mapas de la Clase y Política de mapas

Iniciamos en router en modo de configuración

ROUTER#conf t

Creamos un mapa de clase para clasificar el tráfico de entrada

ROUTER(config)#class-map classEntrada

Definimos que el tráfico a clasificar sera IPV6

ROUTER(config-cmap)#match protocol IPV6

Configuramos que el mapa de clase sea para VOIP ya que el algoritmo af31 es utilizado para tráfico de VOIP

ROUTER(config-cmap)#match ip dscp af31

ROUTER(config-cmap)#exit

Creamos un mapa de clase de salida como en ejemplo anterior

ROUTER(config)#class-map classSalida

ROUTER(config-cmap)#match protocol IPV6

ROUTER(config-cmap)#match ip dscp af31

ROUTER(config-cmap)#exit

Definimos el mapa de Politica para nuestro mapa de clase inicial osea el classEntrada

ROUTER(config)#policy-map policyEntrada

ROUTER(config-pmap)#class classEntrada

Configuramos que el mapa de politica sea para VOIP

ROUTER(config-pmap-c)#set ip dscp af31

ROUTER(config-pmap-c)#exit

ROUTER(config-pmap)#exit

Creamos el mapa de politica para la salida de tráfico

ROUTER(config)#policy-map policySalida

ROUTER(config-pmap)#class classSalida

Para el mapa de politica de salida definimos nivel de prioridad 50 ya que nos interesa que si es tráfico de VOIP no se entrecorte la llamada.

ROUTER(config-pmap-c)#priority 50

ROUTER(config-pmap-c)#end

ROUTER#conf t

Y aplicamos los mapas de politicas a la interfaz del router

ROUTER(config)#int s 0/0/0

ROUTER(config-if)#service-policy input policyEntrada

ROUTER(config-if)#service-policy output policySalida

ROUTER(config-if)#exit

ROUTER(config)#int s 0/0/1

ROUTER(config-if)#service-policy input policyEntrada

ROUTER(config-if)#service-policy output policySalida

ROUTER(config-if)#exit

ROUTER(config)#int fa 0/0

ROUTER(config-if)#service-policy input policyEntrada

ROUTER(config-if)#service-policy output policySalida

ROUTER(config-if)#exit

ROUTER(config)#do wr

2.4.2 ¿Porqué la clasificación de paquetes?

Internet transporta todo tipo de tráfico y cada tipo de tráfico tiene diferentes características y requisitos. Por ejemplo, una aplicación de transferencia de ficheros requiere que alguna cantidad de datos sea transferida de forma aceptable en un tiempo determinado, mientras que la telefonía sobre Internet requiere que la mayor parte de los paquetes sean recibidos en el menor tiempo posible.

La solución para utilizar multimedia sobre IP es clasificar todo el tráfico, localizar el

prioritario para las distintas aplicaciones y realizar las reservas de recursos.

Es por esta razón que cisco desarrollo la técnica “Packet Classification”, la cual hace uso de políticas y clases de mapas que permiten a las aplicaciones configurar y dirigir en una sola infraestructura, aplicaciones multimedia y aplicaciones tradicionales.

CAPITULO III

3.1 Materiales y Métodos

En este capítulo se describe los materiales y métodos usados para el desarrollo de este análisis de investigación. Se hace referencia a aspectos como al diseño de investigación, tipo de estudio y métodos que han sido utilizados en el análisis.

3.2 Diseño de la investigación

El tipo de investigación a utilizarse es la descriptiva y de laboratorio. La investigación descriptiva ayuda a aprender las características externas del objeto de estudio, profundizar el conocimiento del objeto del problema.

La investigación de laboratorio trata de comprobar la hipótesis desarrollando experimentos.

3.3 Tipo de estudio

La investigación que se realizará es cuasi experimental, ya que se manipulan deliberadamente al menos un variable independiente para ver su efecto y relación con una y más variables dependientes, solamente que difieren de los experimentos verdaderos en el grado de seguridad o confiabilidad de poder tenerse sobre la equivalencia inicial de los grupos.

Se realizará escenario de prueba con equipos Cisco, el primer escenario aplicando la técnica “Packet Classification” en IPV4, el segundo escenario sin aplicar la técnica “Packet Classification” en IPV4, el tercer escenario aplicando la técnica “Packet Classification” en IPV6 y por último el cuarto escenario sin aplicar la técnica “Packet

Classification" en IPV6, realizando comparaciones entre los cuatro escenarios midiendo cada uno de los parámetros que determinan la calidad de Servicio (QoS).

3.4 Métodos, Técnicas e Instrumentos

Métodos

Método Científico

Debido a que se trata de un proyecto de investigación, que para obtener los resultados deseados se debe seguir un proceso.

Método Deductivo

Método que será utilizado en el análisis de los mecanismos de QoS aplicado al tráfico de VOIP en IPV4 e IPV6 ya que se estudiará desde una definición y características generales hacia los detalles más particulares.

Método Experimental

Consiste en realizar actividades con la finalidad de comprobar, demostrar o reproducir ciertos fenómenos hechos o principios.

Método Comparativo

Su aplicación permitirá comparar los cuatro esquemas propuestos.

3.5 Técnicas

Observación

Razonamiento

Recopilación de información

Análisis

Pruebas.

3.6 Instrumentos

D-ITG

IOS Cisco c2801.adviipservicesk9-mz.124-8a.bin

Distribución Normalizada Z

DIAGNOS.I Versión I

Algoritmo para VOIP af31

Códec G.711

Internet

Libros

Estándares

RFC`s

Otros

3.7 Validación de instrumentos

Se utilizo los equipos CISCO ya que son los únicos capaces de implementar la técnica Packet Classification, al ser esta una técnica de propiedad de la empresa CISCO Systems. El algoritmo usado para estas pruebas es el AF31 que según recomendación por la IEEE en su RFC 2597 [9] ya que es uno de los algoritmos más utilizados al mantener una buena calidad de servicio. El códec usado es el G.711 ya que es uno de los más utilizados especificado por la ITU-T [10].

La validez del uso de la tecnología Cisco Systems se la ha determinado en base a la experiencia que esta empresa tiene desde 1984 y de las importantes empresas que hacen uso de los productos que esta empresa brinda, así como del IOS usado que es el

c2801.adviipservicesk9-mz.124-8a.bin, este ISO permite utilizar la técnica “Packet Classification” tanto en escenarios IPV4 e IPV6.

Para la demostración de las bondades y la mejora que brindo la técnica “Packet Classification” se utilizo el programa D-ITG, el cual fue actualizado en Agosto del 2011, la versión utilizada es la 2.8.0, este software permite inyectar trafico a modo de simulación de un escenario saturado de paquetes el cual determinará mediante sus resultados que la técnica “Packet Classification” mejorará la calidad de la transmisión de VOIP tanto en escenarios IPV4 e IPV6.

Para la demostración de la hipótesis se utilizo el software DIAGNOS.I Versión I, de propiedad de la Dra. Narcisa Salazar el cual nos permite obtener la grafica de demostración de la hipótesis haciendo uso de la distribución normalizada Z, la distribución mencionada la emplee al tener una muestra alta de paquetes generados mediante la herramienta D-ITG.

3.8 Diseño de ambientes de pruebas

IPV4

Para este escenario se utilizarán 4 routers cisco de la serie 2800 los cuales permitirán configurar vlans de voz y datos sin la inclusión de la técnica “Packet Classificatión” en IPV4, además de la utilización de los 3 switchs cisco, un servidor de VOIP Asterisk, un servidor proxy y un servidor web, además de la utilización de 4 teléfonos IP Grandstream GXP280 y varias terminales Pcs para realizar pruebas de conectividad.

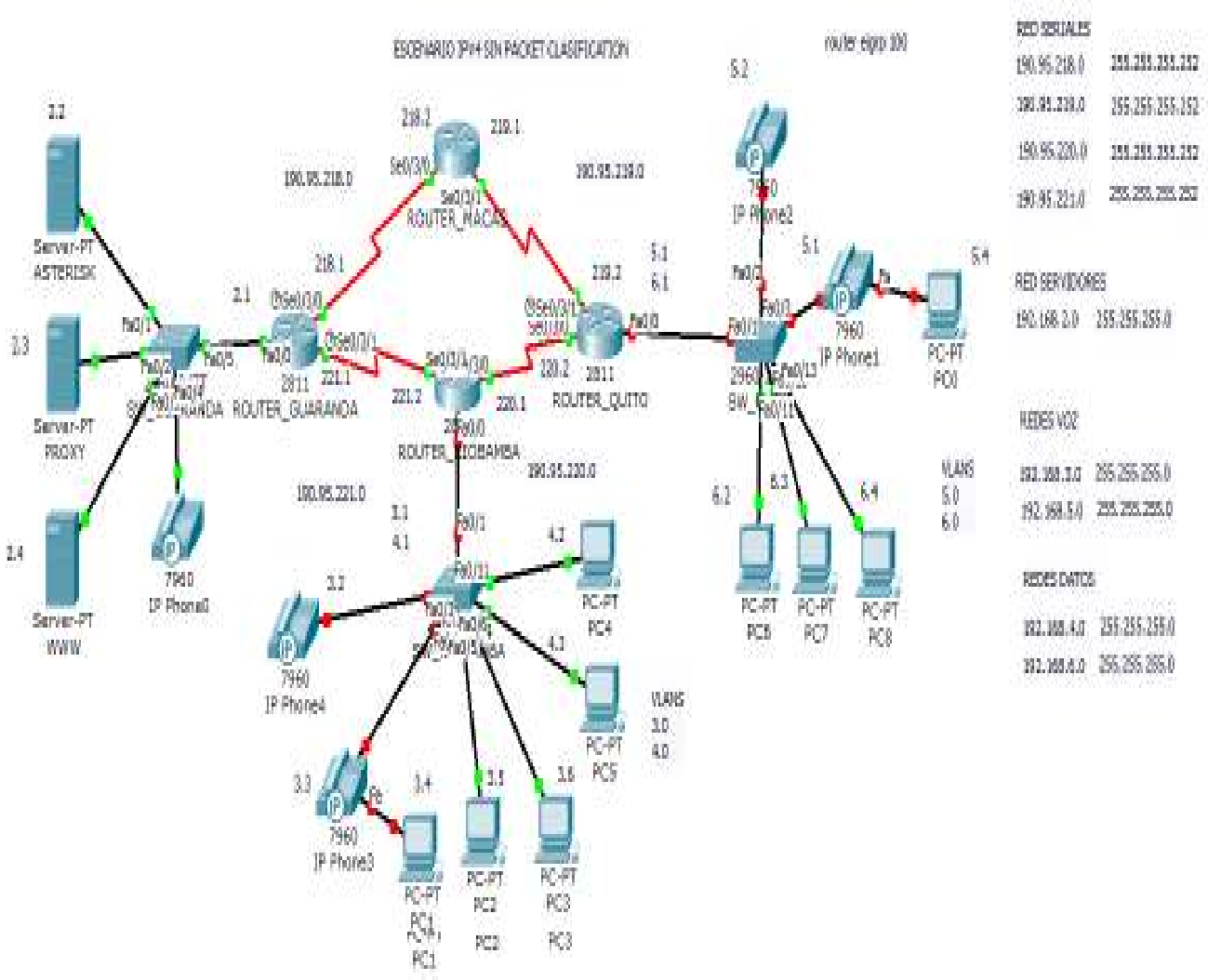


Figura III.1: Escenario de prueba para IPV4 sin “Packet Classification”.
Fuente: Autor

IPV4 CON PACKET CLASSIFICATION

Para este escenario se utilizarán 4 routers cisco de la serie 2800 los cuales permitirán configurar vlans de voz y datos con la inclusión de la técnica “Packet Classificatión” en IPV4, además de la utilización de los 3 switchs cisco, un servidor de VOIP Asterisk, un servidor proxy y un servidor web, además de la utilización de 4 teléfonos IP Grandstream GXP280 y varias terminales Pcs para realizar pruebas de conectividad.

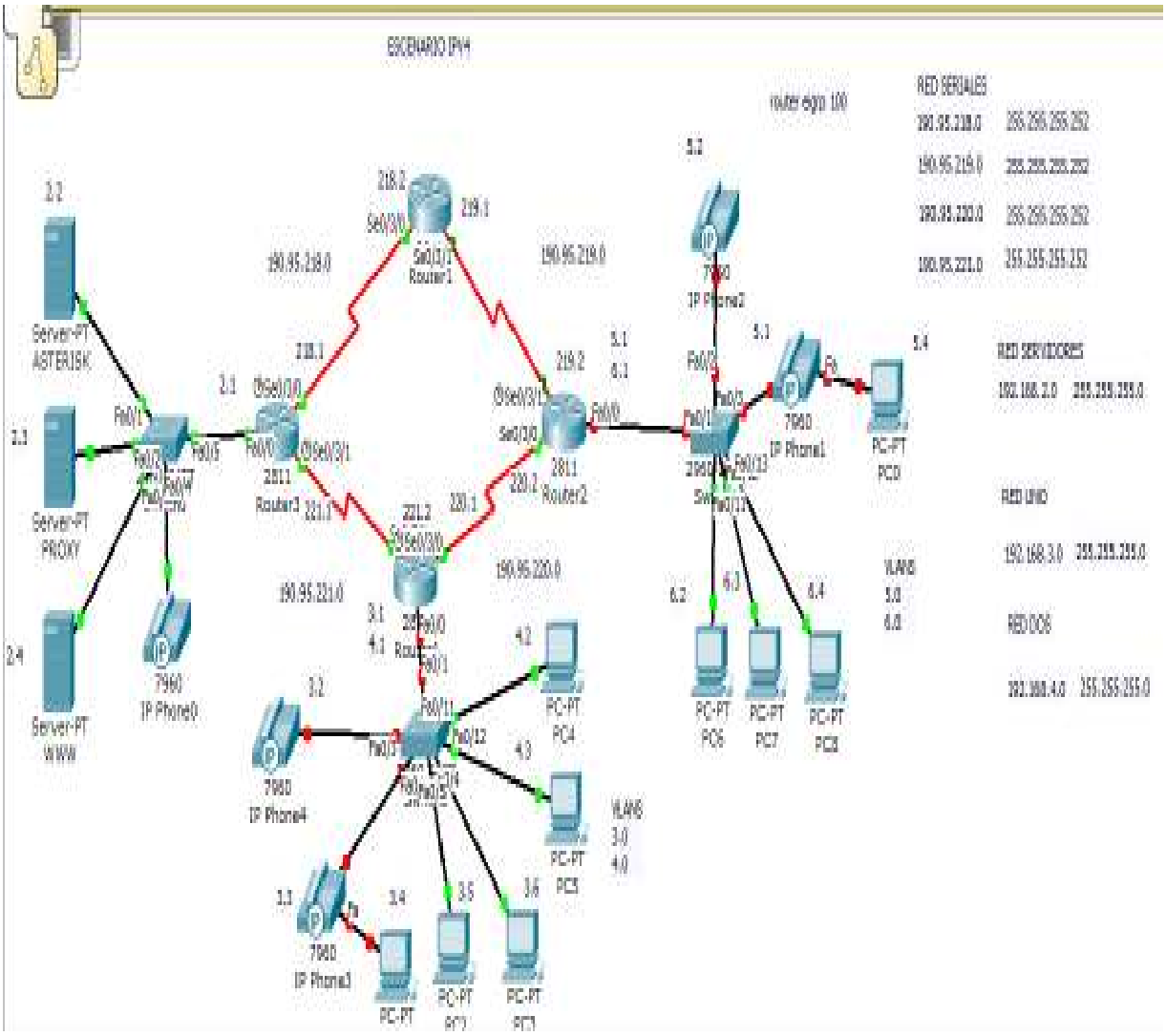


Figura III.2: Escenario de prueba para la técnica “Packet Classification” en IPV4
Fuente: Autor

IPV6

Para este escenario se utilizarán 4 routers cisco de la serie 2800 los cuales permitirán configurar la red sin la inclusión de la técnica “Packet Classificatión” en IPV6, además de la utilización de los 3 switchs cisco, un servidor de VOIP Asterisk, un servidor proxy y un servidor web, además de la utilización de 4 teléfonos IP Grandstream GXP280 y varias terminales Pcs para realizar pruebas de conectividad.

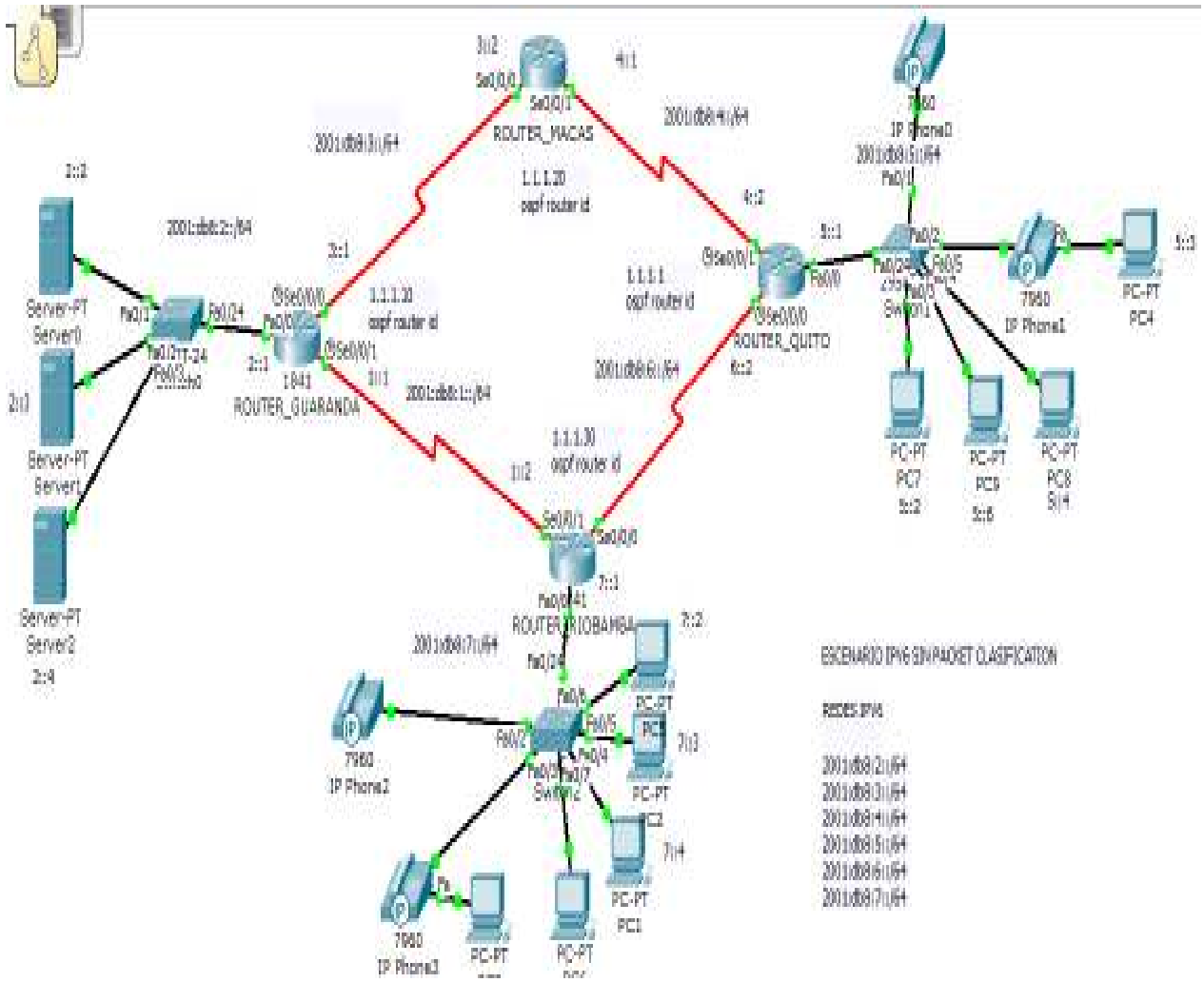


Figura III.3: Escenario de prueba para IPV6 sin la técnica “Packet Classification”.
Fuente: Autor

IPV6 CON PACKET CLASSIFICATION

Para este escenario se utilizarán 4 routers cisco de la serie 2800 los cuales permitirán configurar la red con la inclusión de la técnica “Packet Classificatión” en IPV6, además de la utilización de los 3 switchs cisco, un servidor de VOIP Asterisk, un servidor proxy y un servidor web, además de la utilización de 4 teléfonos IP Grandstream GXP280 y varias terminales Pcs para realizar pruebas de conectividad.

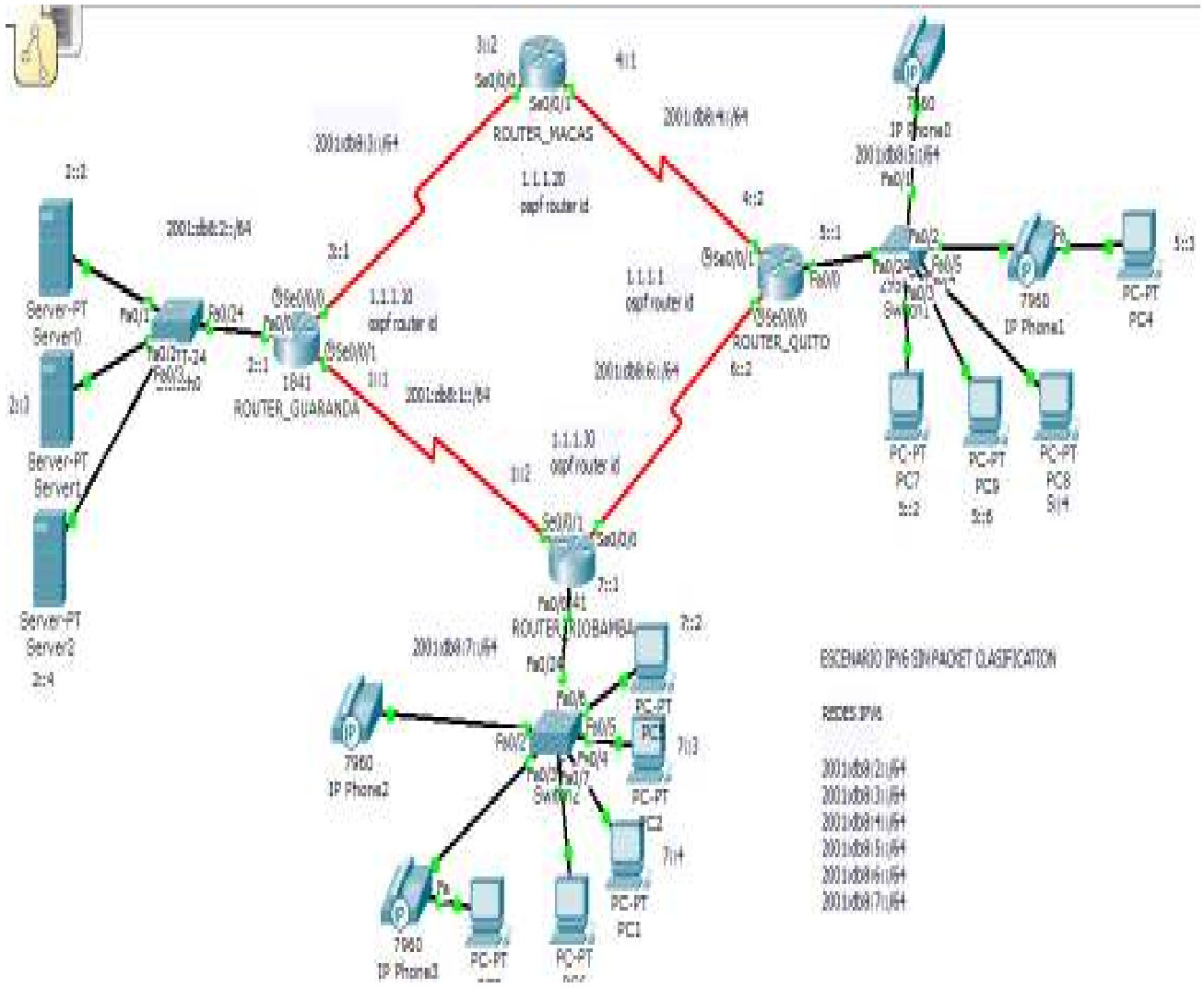


Figura III.4: Escenario de prueba para IPV6 con la técnica “Packet Classification”.
Fuente: Autor

3.9 Definición de las Variables

Para la demostración de la hipótesis planteada se utilizo las siguientes variables que a continuación se describen:

Delay

El delay de la red se define como el tiempo de tránsito que experimenta una aplicación desde el punto de ingreso al punto de egreso en una red. Este puede causar problemas en la Calidad de Servicio en aplicaciones tales como VOIP y transmisiones de fax que simplemente se retrasan y sufren condiciones de delay excesivas. Algunas aplicaciones pueden compensar ciertas cantidades de delay finitos, pero una vez que se excede cierta cantidad, la Calidad de Servicio se ve comprometida. Por ejemplo, los portales VoIP y los teléfonos brindan cierta amortiguación local para compensar los retrasos en la red.

Jitter

El jitter es la medida de variación de delay entre paquetes consecutivos en un determinado flujo de tráfico. Genera un efecto importante sobre las aplicaciones sensibles al delay en tiempo real, como voz y video, que deben recibir paquetes en una tasa relativamente constante, con un delay fijo entre los paquetes consecutivos. A medida que varía la tasa de delay, el jitter impacta sobre el rendimiento de la aplicación. Una cantidad mínima de jitter puede ser aceptable, pero a medida que éste se incrementa, esa aplicación puede terminar siendo inútil. Algunas aplicaciones, como portales de voz y teléfonos IP, pueden compensar una cantidad finita de jitter; pero como las aplicaciones de voz necesitan que el audio trabaje a una tasa constante, si el próximo paquete no llega dentro del tiempo de playback, la aplicación volverá a reproducir el paquete de voz anterior hasta que llegue el próximo paquete de voz. Sin embargo, si el paquete siguiente se retrasa demasiado, simplemente se descarta al llegar, lo cual implica una menor cantidad de audio distorsionado. Todas las redes

presentan cierta cantidad de jitter debido a la variabilidad de delay que presenta cada nodo de la red mientras llegan los paquetes. De todos modos, siempre que el jitter esté controlado, se puede mantener la Calidad de Servicio.

Tiempo Total

El tiempo total es el tiempo empleado en enviar todos los paquetes generados durante la prueba realizada en cada escenario.

Ancho de Banda

El ancho de banda es la diferencia de frecuencias del espectro electromagnético.

AB= fmax - fmin

AB = Ancho de Banda

fmax= frecuencia máxima

fmin= frecuencia mínima

CAPITULO IV

Resultados y Discusión

Los resultados y discusión de las pruebas realizadas tanto para los escenarios en IPV4 e IPV6 y de los comandos utilizados en la aplicación D-ITG se describirán a continuación.

4.1 Pruebas realizadas para IPV4

4.1.1 Comandos utilizados mediante la herramienta D-ITG sin Packet Classification Implementado en los Routers CISCO 2800.

a) Iniciar archivo log en el origen que permitirá guardar los resultados con el siguiente comando detallado en el paso 1, el parámetro –l se lo necesita para especificar que es un archivo log. El comando ITDRecv es el receptor de tráfico de la plataforma D-ITG.

   1. ITDRecv -l recv_log_file_IPV4_sinp25oct

b) Iniciar el archivo log en el destino con el siguiente comando detallado en el paso 2 que permitirá guardar los resultados, el parámetro –l se lo necesita para especificar que es un archivo log. El comando ITDRecv es el receptor de tráfico de la plataforma D-ITG.

   2. ITDRecv -l recv_log_file_IPV4_sinp25oct

c) Iniciar el envío de tráfico desde la dirección 192.168.5.1 que es la maquina en la cual se ejecuta el comando hacia la dirección 192.168.5.2, para iniciar el envío de trafico se utiliza el comando ITDSend que es un generador de tráfico de la plataforma D-ITG, el parámetro -a es el comando para especificar la dirección de destino, el parámetro –i se lo utiliza para determinar por la interfaz que será enviado el tráfico, el parámetro -T es para especificar qué tipo de tráfico será

transmitido que en nuestro caso será UDP, el parámetro -b se utiliza para establecer que son Servicios Diferenciados, el parámetro -t es utilizado para determinar el tiempo que durará la transmisión de los paquetes está configurado en milisegundos –l es para especificar en qué lugar se guardaran los logs que en este caso será en la dirección de destino 192.168.5.2 el comando VoIP se lo utiliza para especificar que será un tráfico de VOIP, el parámetro –x se lo utiliza para determinar con que códec se enviará el tráfico en nuestro caso se utilizo el códec G.711.1.

3. **ITDSend -a 192.168.5.2 -i eth0 -T UDP -b 184 -t 300000 -l 192.168.5.2 VoIP -x G.711.1**

d) Finalizar el envío de tráfico mediante la combinación de la teclas ctrl+c en el destino.

4. **Para con ctrl+c el ITDRecv en el destino**

e) Finalizar la recepción de datos en el archivo log de origen mediante la combinación de la teclas ctrl+c en el origen.

5. **Para con ctrl+c el ITDRecv en el origen**

f) Visualizar los resultados mediante la utilización del comando ITGDec haciendo uso del archivo log recv_log_file_IPV4_sinp25oct obtenido en la computadora cuya dirección fue 192.168.5.2

6. Iniciar en el destino el ./ITGDec recv_log_file_IPV4_sinp25oct

Resultados con D-ITG IPV4 sin PC

Tabla IV.III: Resultados obtenidos con la herramienta D-ITG en IPV4 sin PC

Variables	Cantidad	Unidad de Medida
Tiempo Total	299.992.927	S
Total de Paquetes	30000	Unidad
Delay Promedio	11.009.699	S
Promedio Jitter	0.000155	S
Desviacion Estándar del Delay	0.016083	S
Ancho de Banda	73.601.735	Kbit/s

Autor: René Barragán
Fuente: ESPOCH

4.1.2 Comandos utilizados mediante la herramienta D-ITG con Packet Classification Implementado en los Routers CISCO 2800.

Para la explicación de la funcionalidad de los comandos por favor revisar la sección 4.1.1

1. Iniciar el ITDRecv -l recv_log_file_IPV4_conp25oct

2. Iniciar el el Destino ITDRecv -l recv_log_file_IPV4_conp25oct

3. Iniciar el ITDSend -a 192.168.5.2 -i eth0 -T UDP -b 184 -t 300000 -l 192.168.5.2 VoIP -x G.711.1

4. Para con ctrl+c el ITDRecv en el destino

5. Para con ctrl+c el ITDRecv en el origen

6. Iniciar en el destino el ./ITGDec recv_log_file_IPV4_conp25oct

Resultados con D-ITG IPV4 con PC

Tabla IV.IIII: Resultados obtenidos con la herramienta D-ITG en IPV4 con PC

Variables	Cantidad	Unidad de Medida
Tiempo Total	299.954249	s
Total de Paquetes	30000	Unidad
Delay Promedio	11.035750	s
Promedio Jitter	0.000118	s
Desviacion Estándar del Delay	0.010955	s
Ancho de Banda	73.611226	Kbit/s

Autor: René Barragán
Fuente: ESPOCH

4.1.3 Resultados Gráficos

Tiempo Total

Tabla IV.V: Resultados Tiempo Total y Total de Paquetes en IPV4 con PC

	SIN PC IPV4	CON PC IPV4
Tiempo Total	299,992927	299,9542

Fuente: Resultados programa D-ITG

De las pruebas realizadas se obtuvo la siguiente comparación Gráfica del Tiempo Total entre IPV4 con Packet Classification e IPV4 sin Packet Classificacion como se muestra en la figura IV.1

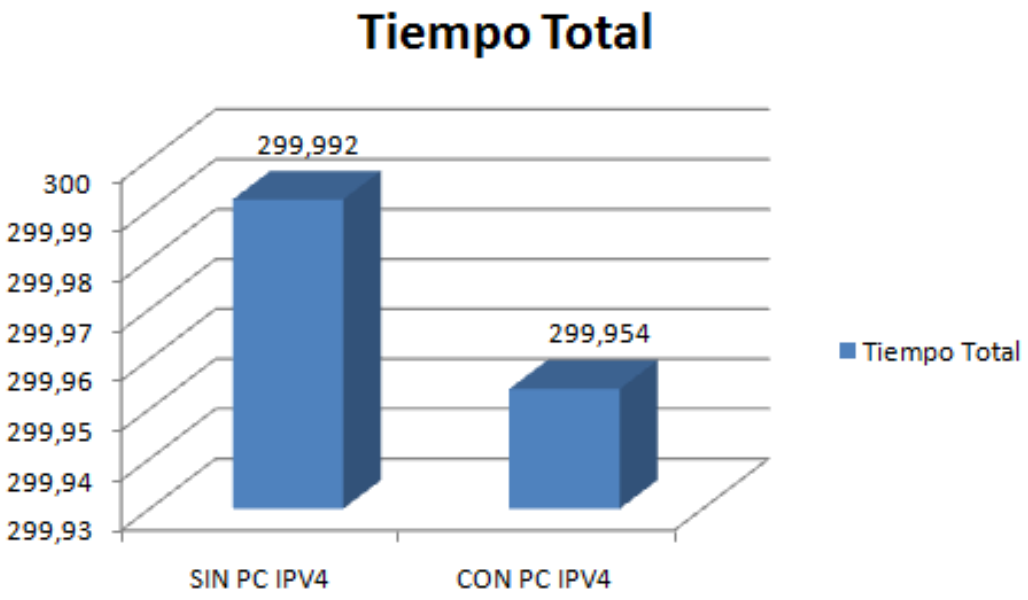


Figura IV.1: Tiempo Total en segundos aplicando y sin aplicar la técnica Packet Classification en IPV4
Fuente: Tabulación resultados programa D-ITG

Delay

Tabla IV.VI: Resultados Delay en IPV4 con PC

	SIN PC IPV4	CON PC IPV4
Delay Minimo	10,9994	11,029447
	SIN PC IPV4	CON PC IPV4
Delay Máximo	11,0489	11,076817
	SIN PC IPV4	CON PC IPV4
Delay Promedio	11,0097	11,3575

Fuente: Resultados programa D-ITG

De las pruebas realizadas se obtuvo la siguiente comparación Gráfica del Delay Minimo entre IPV4 con Packet Classification e IPV4 sin Packet Classificacion como se muestra en la figura IV.2

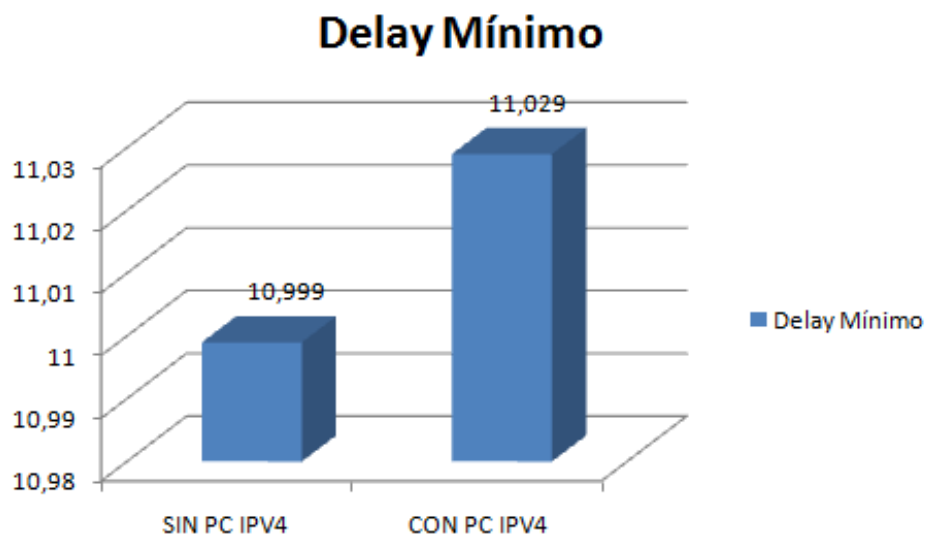


Figura IV.2: Delay Mínimo en segundos aplicando y sin aplicar la técnica Packet Classification en IPV4

Fuente: Tabulación resultados programa D-ITG

De las pruebas realizadas se obtuvo la siguiente comparación Gráfica del Delay Máximo entre IPV4 con Packet Classification e IPV4 sin Packet Classificacion como se muestra en la figura IV.3

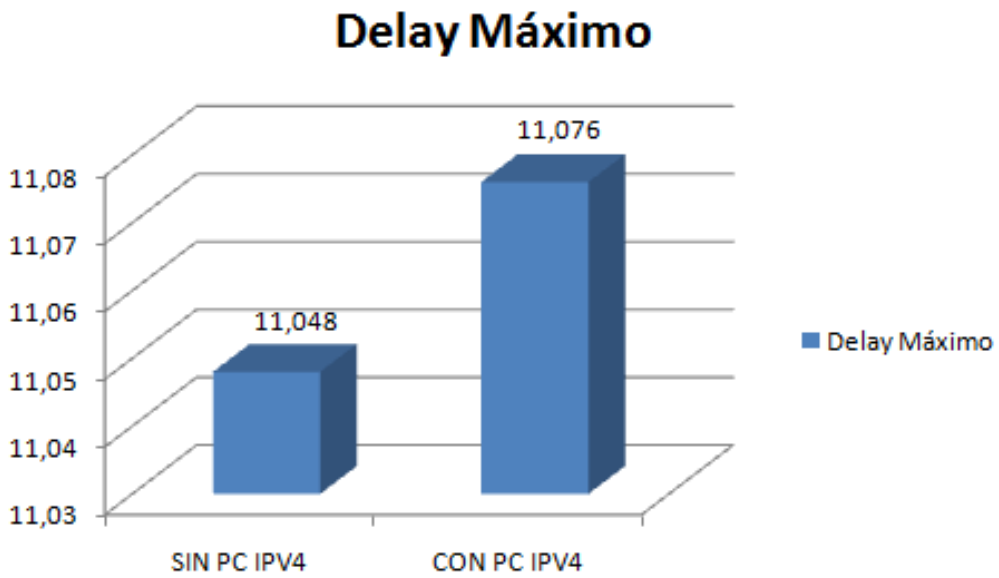


Figura IV.3: Máximo Delay en segundos aplicando y sin aplicar la técnica Packet Classification en IPV4

Fuente: Tabulación resultados programa D-ITG.

De las pruebas realizadas se obtuvo la siguiente comparación Gráfica del Delay Promedio entre IPV4 con Packet Classification e IPV4 sin Packet Classificacion como se muestra en la figura IV.4

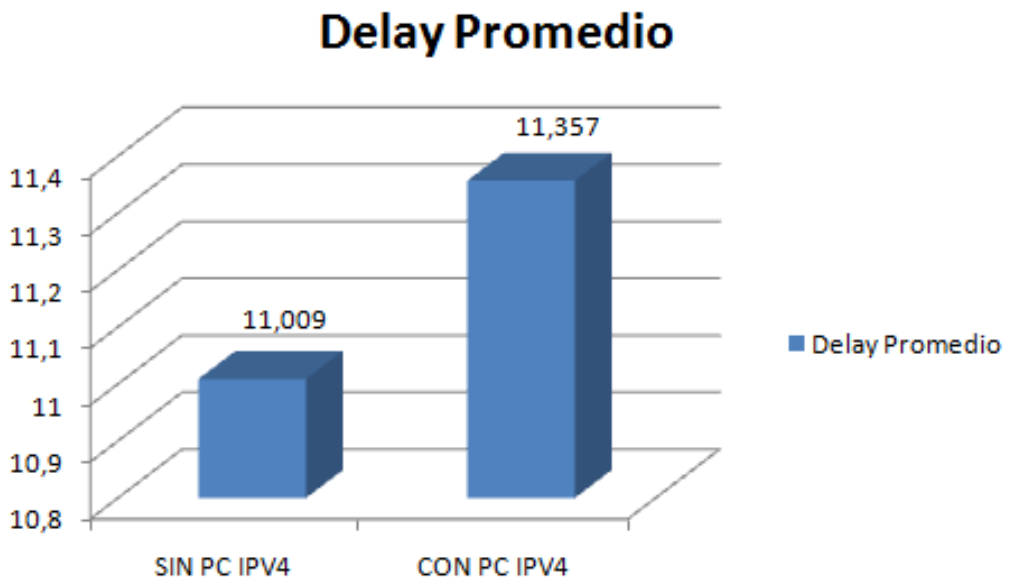


Figura IV.4: Delay Promedio en segundos aplicando y sin aplicar la técnica Packet Classification en IPV4
Fuente: Tabulación resultados programa D-ITG.

Jitter

Tabla IV.VII: Resultados Jitter en IPV4 con PC

	SIN PC IPV4	CON PC IPV4
Jitter Promedio	0,00016	0,000118

Fuente: Resultados programa D-ITG

De las pruebas realizadas se obtuvo la siguiente comparación Gráfica del Jitter Promedio entre IPV4 con Packet Classification e IPV4 sin Packet Classificacion como se muestra en la figura IV.5

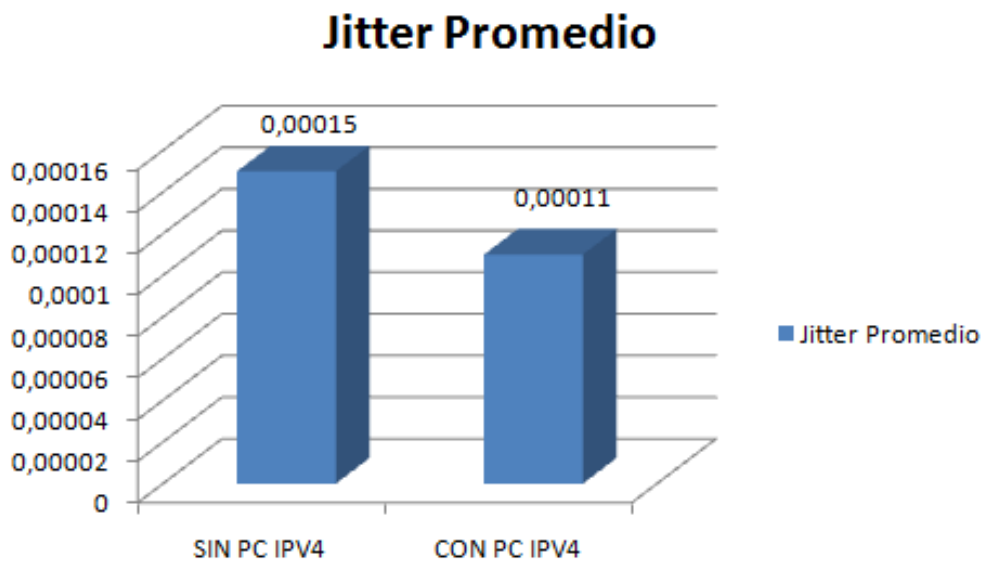


Figura IV.5: Jitter Promedio en segundos aplicando y sin aplicar la técnica Packet Classification en IPV4
Fuente: Tabulación resultados programa D-ITG.

Desviación Estándar

Tabla IV.VIII: Resultados Desviación Estandar en IPV4 con PC

	SIN PC IPV4	CON PC IPV4
Desviación Estandar	0,016083	0,010955

Fuente: Resultados programa D-ITG

De las pruebas realizadas se obtuvo la siguiente comparación Gráfica de la Desviación Estandar entre IPV4 con Packet Classification e IPV4 sin Packet Classificacion como se muestra en la figura IV.6

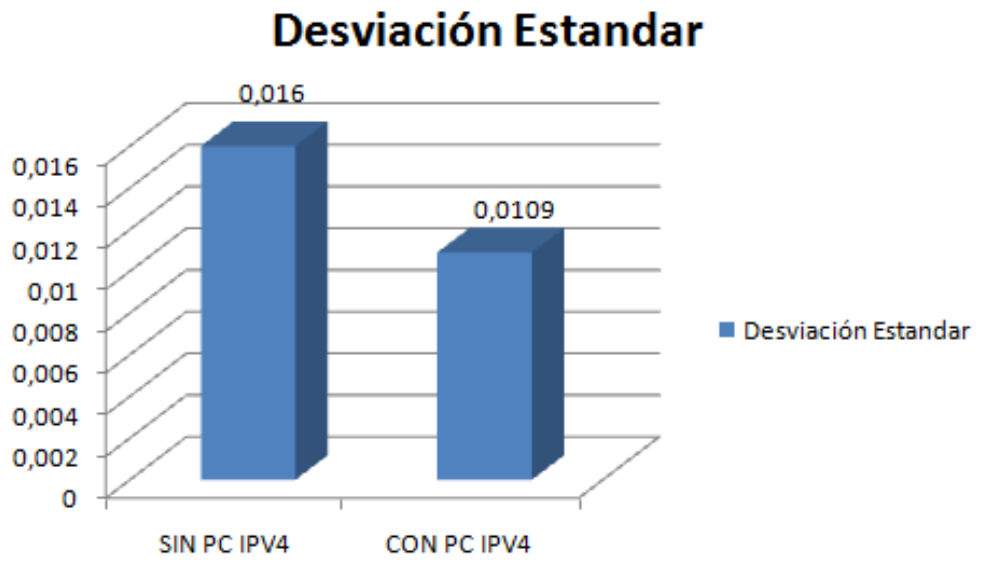


Figura IV.6: Desviación Estándar en segundos aplicando y sin aplicar la técnica Packet Classification en IPV4
Fuente: Tabulación resultados programa D-ITG.

Ancho de Banda

Tabla IV.VIX: Resultados Ancho de Banda en IPV4 con PC

	SIN PC IPV4	CON PC IPV4
Ancho de Banda	73,6017	73,611226

Fuente: Resultados programa D-ITG

De las pruebas realizadas se obtuvo la siguiente comparación Gráfica del Ancho de Banda entre IPV4 con Packet Classification e IPV4 sin Packet Classificacion como se muestra en la figura IV.7

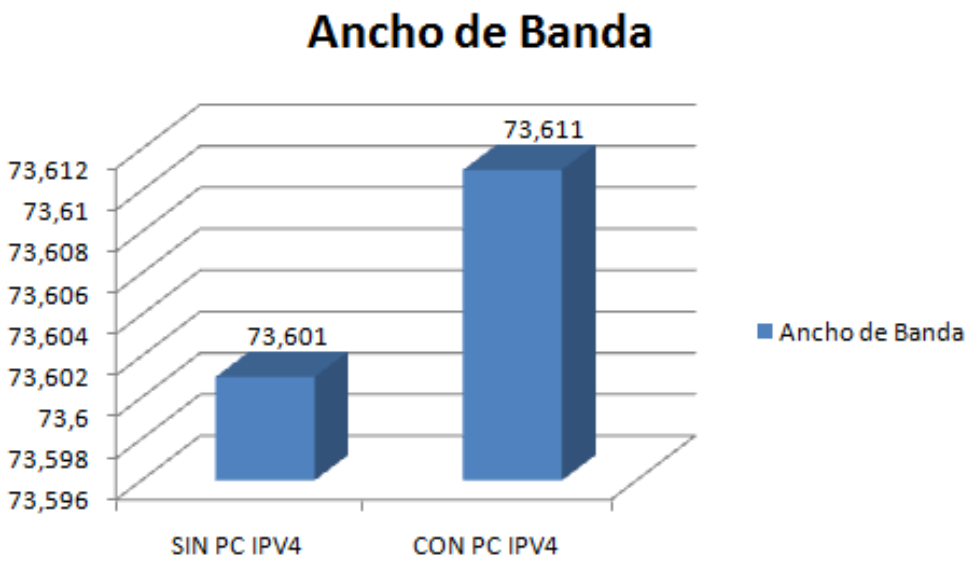


Figura IV.7: Ancho de Banda Promedio en Kbits/s aplicando y sin aplicar la técnica Packet Classification en IPV4
Fuente: Tabulación resultados programa D-ITG.

4.2 Pruebas realizadas para IPV6

4.2.1 Comandos utilizados mediante la herramienta D-ITG sin Packet Classification Implementado en los Routers CISCO 2800.

Para la explicación de la funcionalidad de los comandos por favor revisar la sección 4.1.1

1. Iniciar el ITDRecv -l recv_log_IPV6sinp25oct

2. Iniciar el el Destino ITDRecv -l recv_log_IPV6sinp25oct

3. iniciar el ITDSend -a 2001:db8:5::2 -i eth0 -T UDP -b 184 -t 300000 -l 2001:db8:5::2 VoIP -x G.711.1

4. Para con ctrl+c el ITDRecv en el destino

5. Para con ctrl+c el ITDRecv en el origen

6. Iniciar en el destino el ./ITGDec recv_log_file_IPV6sinp25oct

Resultados con D-ITG IPV6 sin PC

Tabla IV.X: Resultados obtenidos con la herramienta D-ITG en IPV6 sin PC

Variables	Cantidad	Unidad de Medida
Tiempo Total	300.026939	s
Total de Paketes	30000	Unidad
Delay Promedio	11.390611	s
Promedio Jitter	0.000090	s
Desviacion Estándar del Delay	0.015689	s
Ancho de Banda	73.593392	Kbit/s

Autor: René Barragán
Fuente: ESPOCH

4.2.2 Comandos utilizados mediante la herramienta D-ITG con Packet Classification Implementado en los Routers CISCO 2800.

Para la explicación de la funcionalidad de los comandos por favor revisar la sección 4.1.1

1. Iniciar el ITDRecv -l recv_log_IPV6conp25oct

2. Iniciar el el Destino ITDRecv -l recv_log_IPV6conp25oct

3. iniciar el ITDSend -a 2001:db8:5::2 -i eth0 -T UDP -b 184 -t 300000 -l 2001:db8:5::2 VoIP -x G.711.1

4. Para con ctrl+c el ITDRecv en el destino

5. Para con ctrl+c el ITDRecv en el origen

6. Iniciar en el destino el ./ITGDec recv_log_file_IPV6conp25oct

Resultados con D-ITG IPV6 con PC

Tabla IV.XI: Resultados obtenidos con la herramienta D-ITG en IPV6 con PC

Variables	Cantidad	Unidad de Medida
Tiempo Total	299.997339	s
Total de Paketes	30000	Unidad
Delay Promedio	11.352798	s
Promedio Jitter	0.000073	s
Desviacion Estándar del Delay	0.001641	s
Ancho de Banda	73.600653	Kbit/s

Autor: René Barragán
Fuente: ESPOCH

4.2.3 Resultados Gráficos

Tiempo Total

Tabla IV.XII: Resultados Tiempo Total y Total de Paquetes en IPV6 con PC y sin PC

	SIN PC IPV6	CON PC IPV6
Tiempo Total	300,026939	299,997339

Fuente: Resultados programa D-ITG

De las pruebas realizadas se obtuvo la siguiente comparación Gráfica del Tiempo Total empleado al transmitir tráfico de VOIP entre IPV6 con Packet Classification e IPV6 sin Packet Classificacion como se muestra en la figura IV.8

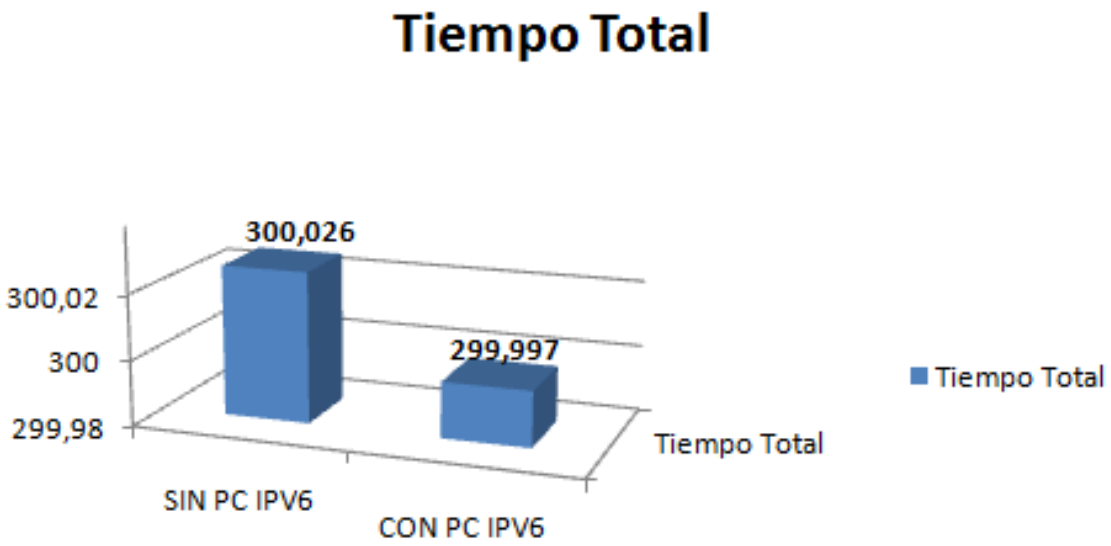


Figura IV.8: Tiempo Total en segundos aplicando y sin aplicar la técnica Packet Classification en IPV6
Fuente: Tabulación resultados programa D-ITG.

Delay

Tabla IV.XIII: Resultados Delay en IPV6 con PC

	SIN PC IPV6	CON PC IPV6
Delay Mínimo	11,376852	11,349484
	SIN PC IPV6	CON PC IPV6
Delay Máximo	11,414412	11,356785
	SIN PC IPV6	CON PC IPV6
Delay Promedio	11,390611	11,352798
	SIN PC IPV6	CON PC IPV6

Fuente: Resultados programa D-ITG

De las pruebas realizadas se obtuvo la siguiente comparación Gráfica del Delay Mínimo entre IPV6 con Packet Classification e IPV6 sin Packet Classificacion como se muestra en la figura IV.9

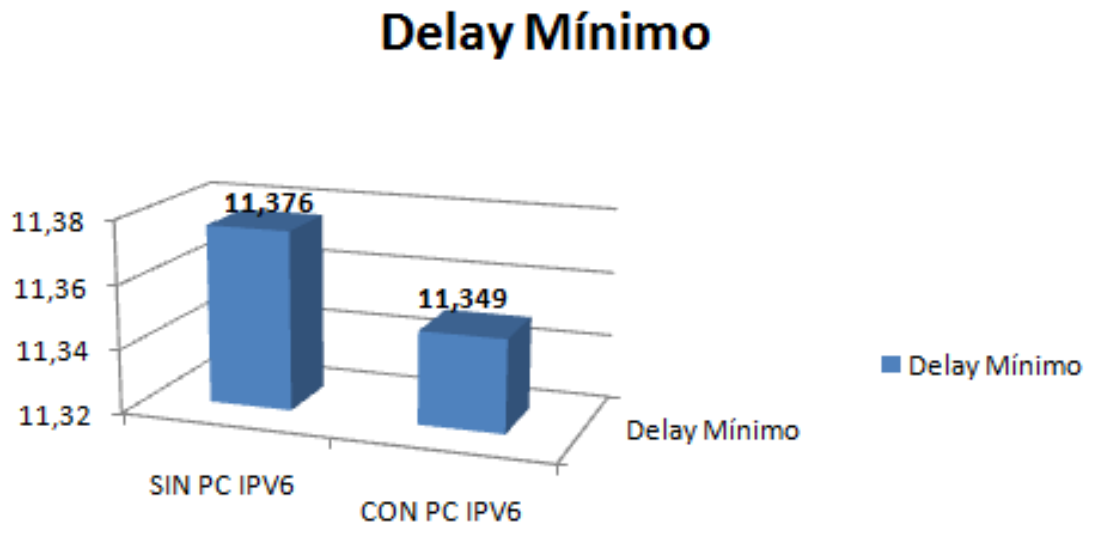


Figura IV.9: Delay Mínimo en segundos aplicando y sin aplicar la técnica Packet Classification en IPV6
Fuente: Tabulación resultados programa D-ITG.

De las pruebas realizadas se obtuvo la siguiente comparación Gráfica del Delay Máximo entre IPV6 con Packet Classification e IPV6 sin Packet Classificacion como se muestra en la figura IV.10

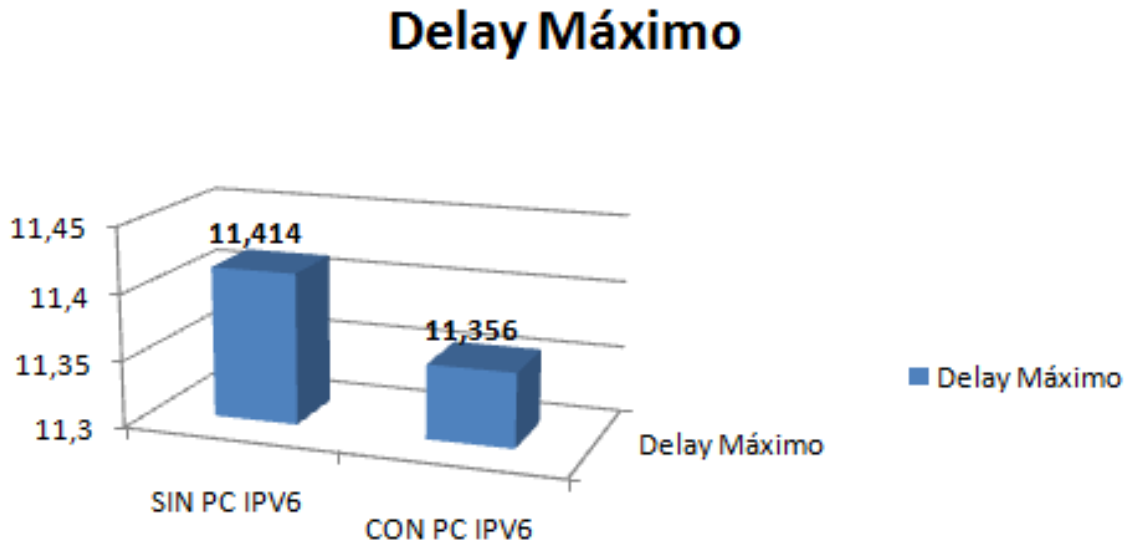


Figura IV.10: Máximo Delay en segundos aplicando y sin aplicar la técnica Packet Classification en IPV6
Fuente: Tabulación resultados programa D-ITG.

De las pruebas realizadas se obtuvo la siguiente comparación Gráfica del Delay Promedio entre IPV6 con Packet Classification e IPV6 sin Packet Classificacion como se muestra en la figura IV.11

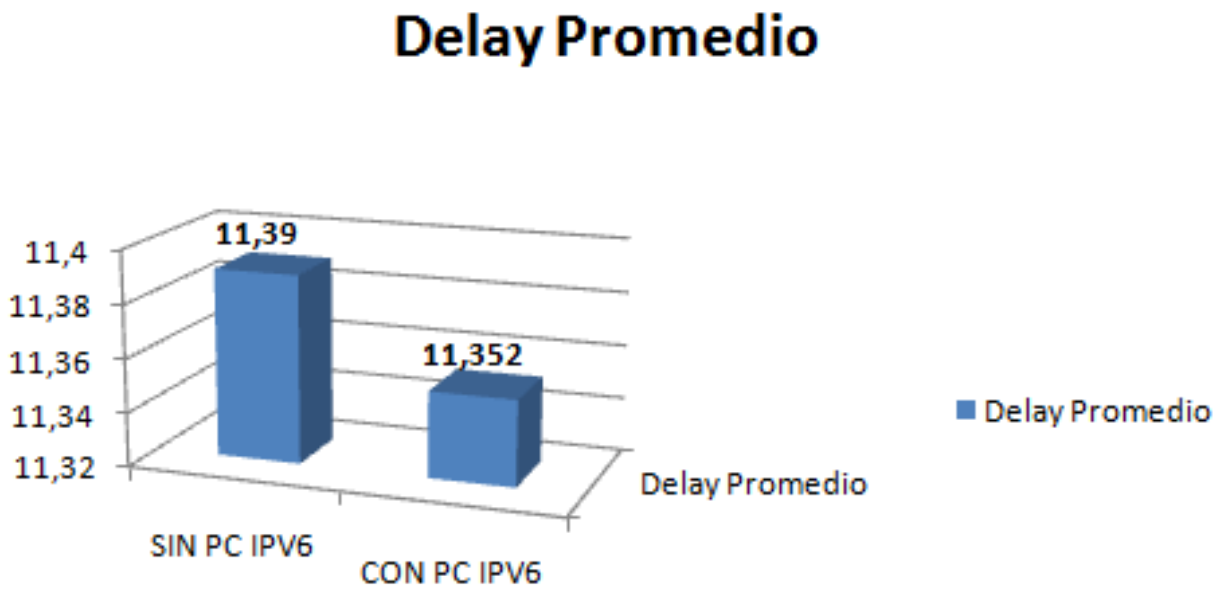


Figura IV.11: Delay Promedio en segundos aplicando y sin aplicar la técnica Packet Classification en IPV6
Fuente: Tabulación resultados programa D-ITG.

Jitter

Tabla IV.XIV: Resultados Jitter en IPV6 con PC

	SIN PC IPV6	CON PC IPV6
Jitter Promedio	0,000090	0,000073

Fuente: Resultados programa D-ITG

De las pruebas realizadas se obtuvo la siguiente comparación Gráfica del Jitter Promedio entre IPV6 con Packet Classification e IPV6 sin Packet Classificacion como se muestra en la figura IV.12

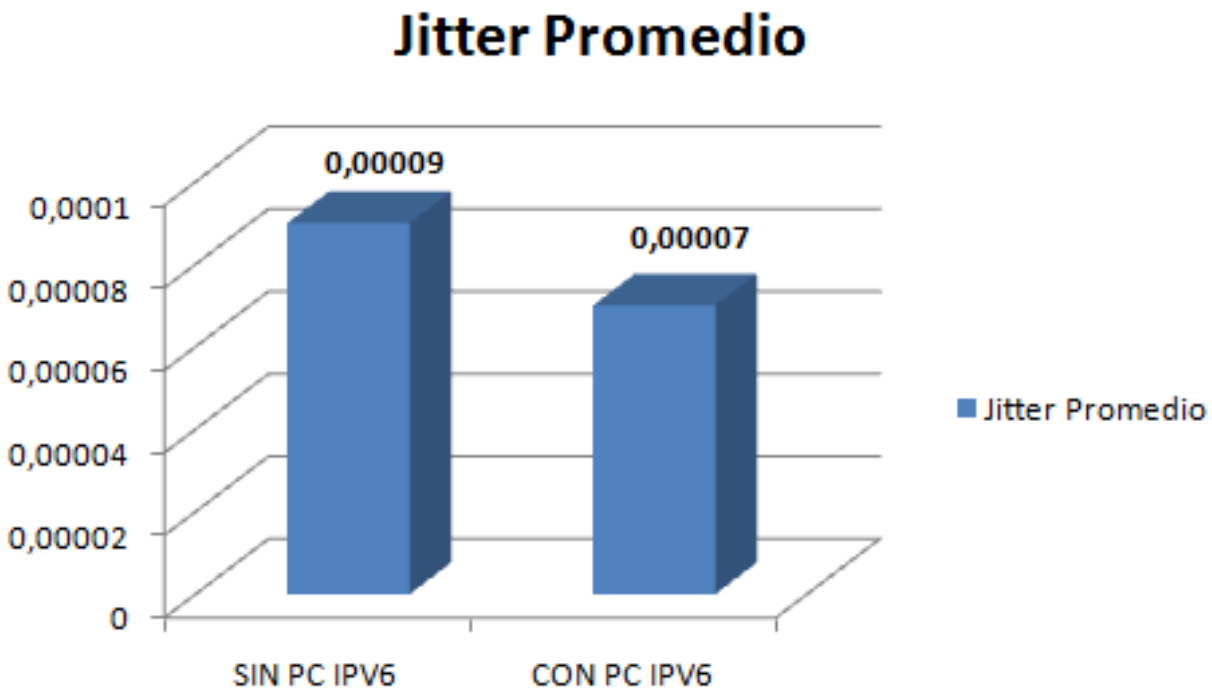


Figura IV.12: Jitter Promedio en segundos aplicando y sin aplicar la técnica Packet Classification en IPV6
Fuente: Tabulación resultados programa D-ITG.

Desviación Estándar

Tabla IV.XV: Resultados Desviación Estándar en IPV6 con PC

	SIN PC IPV6	CON PC IPV6
Desviación Estandar	0,015689	0,001641

Fuente: Resultados programa D-ITG

De las pruebas realizadas se obtuvo la siguiente comparación Gráfica de la Desviación Estandar del Delay entre IPV6 con Packet Classification e IPV6 sin Packet Classificacion como se muestra en la figura IV.13

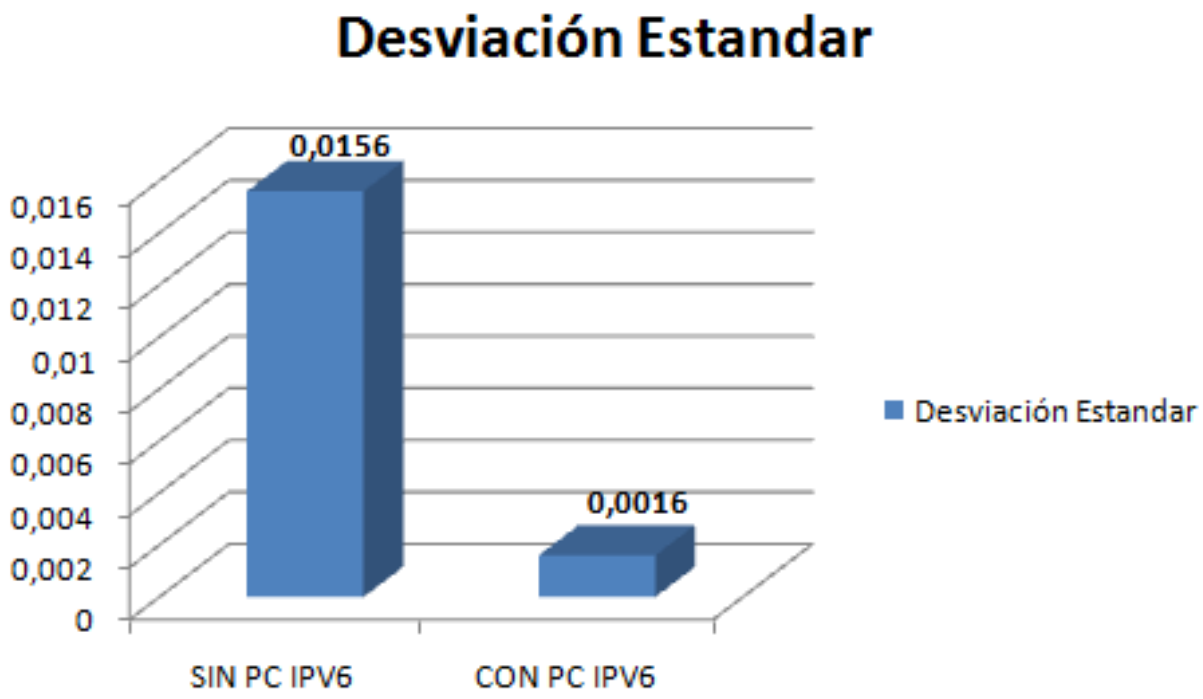


Figura IV.13: Desviación Estándar en segundos aplicando y sin aplicar la técnica Packet Classification en IPV6
Fuente: Tabulación resultados programa D-ITG.

Ancho de Banda

Tabla IV.XVI: Resultados Ancho de Banda en IPV6 con PC

	SIN PC IPV6	CON PC IPV6
Ancho de Banda	73,593392	73,600653

Fuente: Resultados programa D-ITG

De las pruebas realizadas se obtuvo la siguiente comparación Gráfica del Ancho de Banda utilizado entre IPV6 con Packet Classification e IPV6 sin Packet Classificacion como se muestra en la figura IV.14

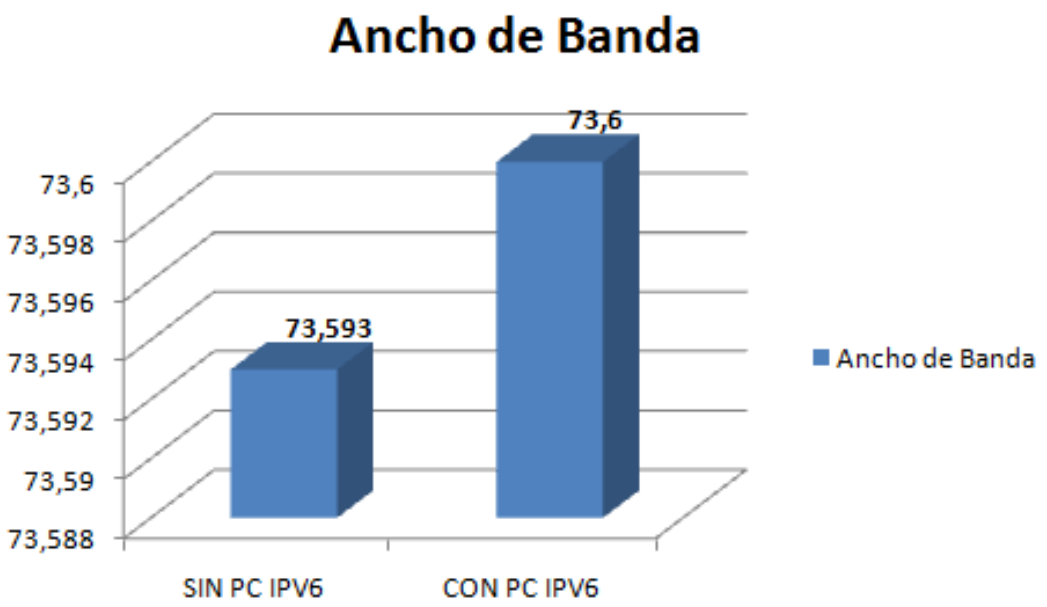


Figura IV.14: Ancho de Banda Promedio en segundos aplicando y sin aplicar la técnica Packet Classification en IPV6
Fuente: Tabulación resultados programa D-ITG.

4.3 Comprobación de la hipótesis

Para la comprobación de la hipótesis se va a realizar:

Muestra

La muestra que se utilizo fueron los cuatro escenarios planteados:

IPV4 sin Packet Classification

IPV4 con Packet Classification

IPV6 sin Packet Classification

IPV6 con Packet Classification

Para cada escenario se enviaron 30000 paquetes, los mismos que representaron la muestra escogida para la demostración de la hipótesis planteada. Esto se lo realizo en base al documento: Conceptos y Elementos Básicos de Tráfico en Telecomunicaciones [11], ya que en este documento se afirma que una llamada de VOZ dura aproximadamente 1 segundo, y tomando como base que cada paquete representa una

llamada, tendríamos lo siguiente:

1 llamada = 1 Segundo

1 llamada = 1 paquete

1 paquete = 1 Segundo

30000 paquetes = 8.33 horas

Y al tomar en cuenta que la jornada laboral de un día en Ecuador es de ocho horas se utilizó 30000 paquetes para determinar la eficacia de la aplicación de la técnica Packet Classification en un día normal de actividades, utilizando el programa D-ITG para lograr esta simulación de llamadas.

4.4 Estudio comparativo de los resultados

En este punto se detalla la tabla IV.XVII en la cual se muestran los valores generales obtenidos en las pruebas realizadas para los 4 escenarios.

Tabla IV.XVII: Resultados para los cuatro escenarios

	IPV4 SIN PK	IPV4 CON PK	IPV6 SIN PK	IPV6 CON PK	
Variables	**Cantidad**	**Cantidad**	**Cantidad**	**Cantidad**	**Unidad de Medida**
Tiempo Total	299.992	299.954	300.026	299.997	s
Total de Paquetes	30000	30000	30000	30000	Unidad
Delay Promedio	11.009	11.035	11.390	11.352	s
Promedio Jitter	0.00015	0.00011	0.00009	0.00007	s
Desviacion Estándar del Delay	0.0160	0.0109	0.0156	0.0016	s
Ancho de Banda	73.601	73.611	73.593	73.600	Kbit/s

Autor: René Barragán
Fuente: ESPOCH

Como se puede visualizar el tiempo total empleado para transmitir 30000 paquetes en IPV4 sin la utilización de la técnica “Packet Classification” es mayor al tiempo total empleando la técnica “Packet Classification”. Lo cual mejora la calidad de audio debido a una más fácil comprensión del mensaje en un menor tiempo.

De la misma manera el tiempo del Jitter en la transmisión de 30000 paquetes utilizando la técnica “Packet Classification” mejoro produciendo una mejor calidad de servicio al transmitir tráfico de VOIP. Visto en los cuatro escenarios.

Por el contrario el Delay promedio en el escenario de IPV4 implementando la técnica Packet Classification aumentó frente al escenario sin la técnica Packet Classification, pero en el escenario de IPV6 la variable Delay tuvo un descenso frente al escenario de IPV6 sin la técnica Packet Classification.

4.5 Demostración de la Hipótesis

4.5.1 Demostración de la Hipótesis para IPV4

Para la demostración de la Hipótesis se ha tomado la variable “Delay” junto con la Distribución normal Z.

Hipótesis: La aplicación de la técnica “Packet Classification” en la transmisión de VOIP proveerá una adecuada calidad de servicio en redes IPV4

H0 = La aplicación de la técnica “Packet Classification” en la transmisión de VOIP proveerá una igual calidad de servicio en redes IPV4

H1 = La aplicación de la técnica “Packet Classification” en la transmisión de VOIP proveerá una diferente calidad de servicio en redes IPV4

H0 = SINPKIPV4 = CONPKIPV4

H1 = SINPKIPV4 <> CONPKIPV4

n = 30000 paquetes

Datos IPV4 sin Packet Classification

n = 30000

Media = Uxs = 11.009699

Desv.Estand. = Ss = 0.016083

Datos IPV4 con Packet Classification

n = 30000

Media = Uxc = 11.035750

Desv.Estand.= Sc = 0.010955

Error Estándar = 5 %

Calculo de la Desviación Estándar X1-X2

$$S_{\bar{x}_1-\bar{x}_2} = \sqrt{\frac{Ss^2}{n} + \frac{Sc^2}{n}}$$

$$S_{\bar{x}_1-\bar{x}_2} = \sqrt{\frac{(0.016083)^2}{30000} + \frac{(0.010955)^2}{30000}}$$

$$S_{\bar{x}_1-\bar{x}_2} = \sqrt{0{,}0000000086220963 + 0{,}0000000004}$$

$$S_{\bar{x}_1-\bar{x}_2} = \sqrt{0{,}0000000012622}$$

$$S_{\bar{x}_1-\bar{x}_2} = 0.0000112349$$

Cálculo de Z

$$Z = \frac{\bar{x}_1 - \bar{x}_2}{S_{\bar{x}_1-\bar{x}_2}}$$

$$Z = \frac{11.009699 - 11.035750}{0.0000112349}$$

$$Z = \frac{-0.026051}{0.0000112349}$$

$$Z = -231.87$$

De los cálculos realizados para la obtención de la demostración de la hipótesis se obtuvo los siguientes resultados plasmados en la figura IV.15

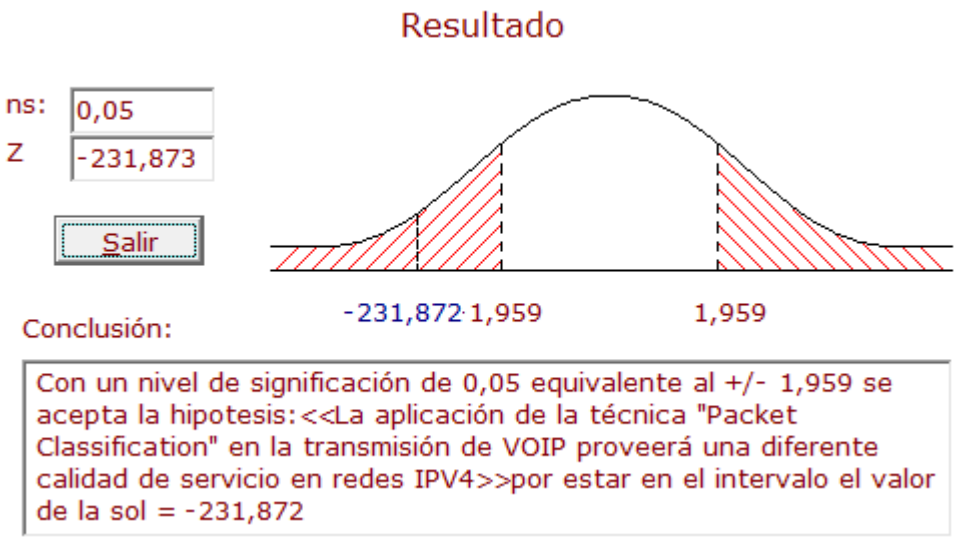


Figura IV.15: Demostración de la hipótesis para IPV4
Fuente: Programa DIAGNOS.I Versión I

Basándonos en el gráfico de demostración de la hipótesis representado en la figura IV. 15 con un nivel de significación de 0.05 equivalente al +/- 1,959 se acepta la hipótesis alternativa “La aplicación de la técnica “Packet Classification” en la transmisión de VOIP proveerá una diferente calidad de servicio en redes IPV4”, por encontrarse el valor de Z en la cola izquierda se concluye que:

“La aplicación de la técnica “Packet Classification” en la transmisión de VOIP proveerá una adecuada calidad de servicio en redes IPV4.

4.5.2 Demostración de la Hipótesis para IPV6

Para la demostración de la Hipótesis se ha tomado la variable “Delay” junto con la Distribución normal Z y la teoría de la Hipótesis.

Hipótesis: La aplicación de la técnica “Packet Classification” en la transmisión de VOIP proveerá una adecuada calidad de servicio en redes IPV6

H0 = La aplicación de la técnica “Packet Classification” en la transmisión de VOIP proveerá una igual calidad de servicio en redes IPV6

H1 = La aplicación de la técnica “Packet Classification” en la transmisión de VOIP proveerá una diferente calidad de servicio en redes IPV6

H0 = SINPKIPV6 = CONPKIPV6

H1 = SINPKIPV6 <> CONPKIPV6

n = 30000 paquetes

Datos IPV6 sin Packet Classification

n = 30000

Media = Uxs = 11.390611

Desv.Estand. = Ss = 0.015689

Datos IPV6 con Packet Classification

n = 30000

Media = Uxc = 11.352798

Desv.Estand.= Sc = 0.001641

Error Estándar = 5 %

Cálculo de la Desviación Estándar X1-X2

$$S_{\bar{x}_1-\bar{x}_2} = \sqrt{\frac{Ss^2}{n} + \frac{Sc^2}{n}}$$

$$S_{\bar{x}_1-\bar{x}_2} = \sqrt{\frac{(0.015689)^2}{30000} + \frac{(0.001641)^2}{30000}}$$

$$S_{\bar{x}_1-\bar{x}_2} = \sqrt{0.00000000082048 + 0.00000000008976}$$

$$S_{\bar{x}_1-\bar{x}_2} = \sqrt{0.0000000008294586}$$

$$S_{\bar{x}_1-\bar{x}_2} = 0.0000091074$$

Cálculo de Z

$$Z = \frac{\bar{x}_1 - \bar{x}_2}{S_{\bar{x}_1-\bar{x}_2}}$$

$$Z = \frac{11.390611 - 11.352798}{0.0000091074}$$

$$Z = \frac{0.037813}{0.0000091074}$$

$$Z = 415.18$$

De los cálculos realizados para la obtención de la demostración de la hipótesis se obtuvo los siguientes resultados plasmados en la figura IV.16

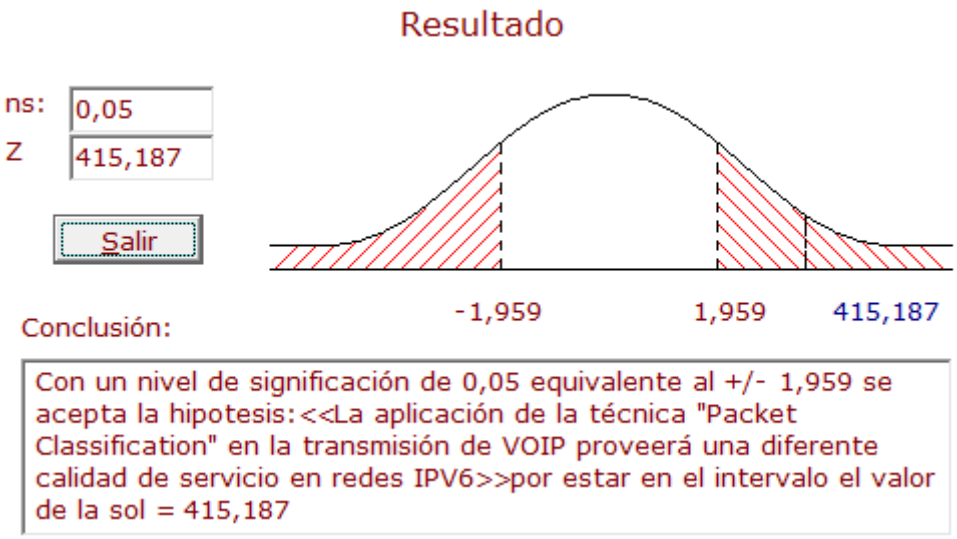


Figura IV.16: Demostración de la hipótesis para IPV6
Fuente: Programa DIAGNOS.I Versión I

Basándonos en el gráfico de demostración de la hipótesis representado en la figura IV. 16 con un nivel de significación de 0.05 equivalente al +/- 1,959 se acepta la hipótesis alternativa “La aplicación de la técnica “Packet Classification” en la transmisión de VOIP proveerá una diferente calidad de servicio en redes IPV6”, por encontrarse el valor de Z en la cola derecha se concluye que:

“La aplicación de la técnica “Packet Classification” en la transmisión de VOIP proveerá una adecuada calidad de servicio en redes IPV6.

Capitulo V

En este capítulo se sugiere una guía para la implantación de la técnica ‘‘Packet Classificatión’’ en el escenario para IPV6, para lo cual se siguió la siguiente metodología de pasos:

5 Presentación de la Propuesta

5.1 Requerimientos para la implementación

5.2 Requerimiento de los usuarios

5.3 Selección de equipos

5.4 Selección del IOS para los routers Cisco

5.5 Determinación de Mapas de Clases

5.6 Implementación de las políticas

5.7 CONFIGURACIÓN DE IPV6 CON PACKET CLASSIFICATION

5.7.1 Configuración de los ROUTERS IPV6

5.7.2 Configuración de los SWITCHS

5.7.3 Configuración por comandos de los Routers

Para de esta manera lograr una correcta implementación de la técnica detallada anteriormente.

5 Presentación de la Propuesta

5.1 Requerimientos para la implementación

Los requerimientos para la implementación de la Técnica “Packet Classification” son:

- Router Cisco 2800
    - Software: C2801.adviipservicesk9-mz.124-8a.bin
- Switch Cisco
- PCs
    - Procesador: Icore 3
    - Memoria: 2 GB
    - Disco: 500 GB
- Teléfonos IP
    - Grandstream Gxp2110
    - Firmware 1.0.3.18
- SoftPhones
- Linphone

5.2 Requerimiento de los usuarios

Conocimientos básicos sobre IPV6 e IPV4, Direccionamiento y Ruteo de Redes.

El usuario debe conocer como realizar Mapas de Clases e Implementación de Políticas para los mapas de clases, además de crear niveles de prioridad y el algoritmo af31 para VOIP.

5.3 Selección de equipos

Los equipos utilizados son:

- Router Cisco 2800
    - Software: C2801.adviipservicesk9-mz.124-8a.bin

- Switch Cisco
- PCs
    - Procesador: Icore 3
    - Memoria: 2 GB
    - Disco: 500 GB
- Teléfonos IP
    - Grandstream Gxp2110
    - Firmware 1.0.3.18
- SoftPhones
- Linphone

5.4 Selección del IOS para los routers CIsco

El IOS utilizado para la implementación de la técnica “Packet Classification” es **C2801.adviipservicesk9-mz.124-8a.bin**

5.5 Determinación de Mapas de Clases

Los mapas de clases utilizados son:

Mapa de Entrada para las interfaces

class-map ClassEntrada

match protocol IPV6 (no escribir:IPV6 para IPV4)

match ip dscp af31 (af31 por la tabla de Assured Forwarding)

Mapa de Salida para las interfaces

class-map ClassSalida

match protocol IPV6 (no escribir:IPV6 para IPV4)

match ip dscp af31 (af31 por la tabla de Assured Forwarding)

Determinación de Políticas

Política de Entrada para las interfaces

policy-map PolicyEntrada

class ClassEntrada

set ip dscp af31

Política de Salida para las interfaces

policy-map PolicySalida

class ClassSalida

priority 50

5.6 Implementación de las políticas

APLICANDO PACKET CLASSIFICATION EN IPV6

PROCESO PARA CONFIGURAR CLASS-MAP, POLICY-MAP Y APLICAR A LAS INTERFACES

ROUTER_GUARANDA#conf t

ROUTER_GUARANDA(config)#class-map classEntrada

ROUTER_GUARANDA(config-cmap)#match protocol IPV6

ROUTER_GUARANDA(config-cmap)#match ip dscp af31

ROUTER_GUARANDA(config-cmap)#exit

ROUTER_GUARANDA(config)#class-map classSalida

ROUTER_GUARANDA(config-cmap)#match protocol IPV6

ROUTER_GUARANDA(config-cmap)#match ip dscp af31

ROUTER_GUARANDA(config-cmap)#exit

ROUTER_GUARANDA(config)#policy-map policyEntrada

ROUTER_GUARANDA(config-pmap)#class classEntrada

ROUTER_GUARANDA(config-pmap-c)#set ip dscp af31

ROUTER_GUARANDA(config-pmap-c)#exit

ROUTER_GUARANDA(config-pmap)#exit

ROUTER_GUARANDA(config)#policy-map policySalida

ROUTER_GUARANDA(config-pmap)#class classSalida

ROUTER_GUARANDA(config-pmap-c)#priority 50

ROUTER_GUARANDA(config-pmap-c)#end

ROUTER_GUARANDA#conf t

ROUTER_GUARANDA(config)#int s 0/0/0

ROUTER_GUARANDA(config-if)#service-policy input policyEntrada

ROUTER_GUARANDA(config-if)#service-policy output policySalida

ROUTER_GUARANDA(config-if)#exit

ROUTER_GUARANDA(config)#int s 0/0/1

ROUTER_GUARANDA(config-if)#service-policy input policyEntrada

ROUTER_GUARANDA(config-if)#service-policy output policySalida

ROUTER_GUARANDA(config-if)#exit

ROUTER_GUARANDA(config)#int fa 0/0

ROUTER_GUARANDA(config-if)#service-policy input policyEntrada

ROUTER_GUARANDA(config-if)#service-policy output policySalida

ROUTER_GUARANDA(config-if)#exit

ROUTER_GUARANDA(config)#do wr

Implementación de una solución y configuración de equipos para IPV6

La propuesta para la implementación de “Packet Classification”, en redes IPV6, para mejorar el tráfico de VOZ IP, es la siguiente:

5.7 CONFIGURACION DE IPV6 CON PACKET CLASSIFICATION

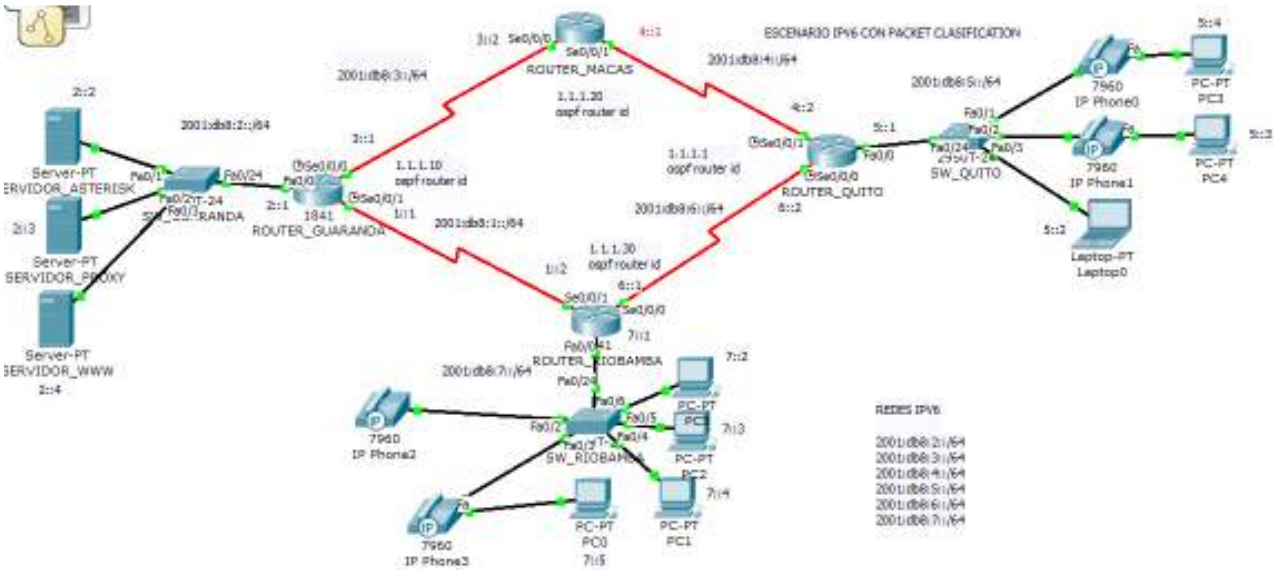


Figura IV.17: configuración IPV6 con Packet Classification

Fuente: Ing. René Barragán Torres

5.7.1 Configuración de los ROUTERS IPV6

ROUTER_GUARANDA

PUERTO	DISPOSITIVO	IP	MASCARA
F0/0	SW_GUARANDA	2001:DB8:2::1	/64
SE0/0/0	ROUTER_GUARANDA	2001:DB8:3::1	/64
SE0/0/1	ROUTER_RIOBAMBA	2001:DB8:1::1	/64

ROUTER_MACAS

PUERTO	DISPOSITIVO	IP	MASCARA
SE0/0/0	ROUTER_GUARANDA	2001:DB8:3::2	/64
SE0/0/1	ROUTER_QUITO	2001:DB8:4::1	/64

ROUTER_QUITO

PUERTO	DISPOSITIVO	IP	MASCARA
SE0/0/1	ROUTER_MACAS	2001:DB8:4::2	/64
SE0/0/0	ROUTER_RIOBAMBA	2001:DB8:6::2	/64
F0/0	SW_QUITO	2001:DB8:5::1	/64

ROUTER_RIOBAMBA

PUERTO	DISPOSITIVO	IP	MASCARA
SE0/0/1	ROUTER_GUARANDA	2001:DB8:1::2	/64
SE0/0/0	ROUTER_QUITO	2001:DB8:6::1	/64
F0/0	SW_RIOBAMBA	2001:DB8:7::1	/64

5.7.2 Configuración de los SWITCHS

SW_GUARANDA

PUERTO	PC	VLANS	IP	MASCARA	GATEWAY
F0/1	SERVIDOR_ASTERISK		2001:DB8:2::2	/64	2001:DB8:2::1
F0/2	SERVIDOR_PROXY		2001:DB8:2::3	/64	2001:DB8:2::1
F0/3	SERVIDOR_WWW		2001:DB8:2::4	/64	2001:DB8:2::1
F0/24	ROUTER_GUARANDA				

SW_RIOBAMBA

PUERTO	PC	VLANS	IP	MASCARA	GATEWAY
F0/24	ROUTER_RIOBAMBA				
F0/2	IP Phone2		2001:DB8:7::8	/64	2001:DB8:7::1
F0/3	IP Phone3		2001:DB8:7::6	/64	2001:DB8:7::
					1
F0/3	PC0		2001:DB8:7::5	/64	2001:DB8:7::1
F0/4	PC1		2001:DB8:7::4	/64	2001:DB8:7::1
F0/5	PC2		2001:DB8:7::3	/64	2001:DB8:7::1
F0/6	PC5		2001:DB8:7::2	/64	2001:DB8:7::1

SW_QUITO

PUERTO	PC	VLANS	IP	MASCARA	GATEWAY
F0/24	ROUTER_QUITO				
F0/1	IP Phone0		2001:DB8:7::6	/64	2001:DB8:5::1
F0/2	IP Phone1		2001:DB8:7::5	/64	2001:DB8:5::1
F0/1	PC3		2001:DB8:5::4	/64	2001:DB8:5::1
F0/2	PC4		2001:DB8:5::3	/64	2001:DB8:5::1
F0/3	LAPTOP0		2001:DB8:5::2	/64	2001:DB8:5::1

5.7.3 Configuracion por comandos de los Routers

Configuración ROUTER_GUARANDA

Building configuration...

Current configuration : 1424 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname ROUTER_GUARANDA

!

IPV6 unicast-routing

!

```
class-map match-all classEntrada
match protocol IPV6
match ip dscp af31
class-map match-all classSalida
match protocol IPV6
match ip dscp af31
!
policy-map policyEntrada
class classEntrada
set ip dscp af31
!
policy-map policySalida
class classSalida
priority 50
!
interface FastEthernet0/0
no ip address
service-policy input policyEntrada
service-policy output policySalida
duplex auto
speed auto
IPV6 address 2001:DB8:2::1/64
IPV6 mtu 1500
IPV6 enable
```

```
IPV6 ospf 1 area 0
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
IPV6 mtu 1500
IPV6 enable
IPV6 ospf 1 area 0
!
interface Serial0/0/0
no ip address
service-policy input policyEntrada
service-policy output policySalida
IPV6 address 2001:DB8:3::1/64
IPV6 mtu 1500
IPV6 enable
IPV6 ospf 1 area 0
clock rate 9600
!
interface Serial0/0/1
no ip address
service-policy input policyEntrada
service-policy output policySalida
```

```
IPV6 address 2001:DB8:1::1/64
IPV6 mtu 1500
IPV6 enable
IPV6 ospf 1 area 0
clock rate 9600
!
interface Vlan1
no ip address
shutdown
!
IPV6 router ospf 1
router-id 1.1.1.10
log-adjacency-changes
!
ip classless
!
no cdp run
!
line con 0
line vty 0 4
login
!
End
```

Configuración ROUTER_RIOBAMBA

Building configuration...

Current configuration : 864 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname ROUTER_RIOBAMBA

!

IPV6 unicast-routing

!

interface FastEthernet0/0

no ip address

duplex auto

speed auto

IPV6 address 2001:DB8:7::1/64

IPV6 mtu 1500

IPV6 enable

IPV6 ospf 1 area 0

!

interface FastEthernet0/1

```
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
no ip address
IPV6 address 2001:DB8:6::1/64
IPV6 mtu 1500
IPV6 enable
IPV6 ospf 1 area 0
!
interface Serial0/0/1
no ip address
IPV6 address 2001:DB8:1::2/64
IPV6 mtu 1500
IPV6 enable
IPV6 ospf 1 area 0
!
interface Vlan1
no ip address
shutdown
!
IPV6 router ospf 1
```

router-id 1.1.1.30

log-adjacency-changes

!

ip classless

!

no cdp run

!

line con 0

line vty 0 4

login

!

end

Configuración ROUTER_MACAS

Building configuration...

Current configuration : 800 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname ROUTER_MACAS

!

IPV6 unicast-routing

!

interface FastEthernet0/0

no ip address

duplex auto

speed auto

IPV6 mtu 1500

IPV6 enable

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

IPV6 mtu 1500

IPV6 enable

!

interface Serial0/0/0

no ip address

IPV6 address 2001:DB8:3::2/64

IPV6 mtu 1500

IPV6 enable

IPV6 ospf 1 area 0

!

interface Serial0/0/1

no ip address

IPV6 address 2001:DB8:4::1/64

IPV6 ospf 1 area 0

!

interface Vlan1

no ip address

shutdown

!

IPV6 router ospf 1

router-id 1.1.1.20

log-adjacency-changes

!

ip classless

!

no cdp run

!

line con 0

line vty 0 4

login

!

end

Configuración ROUTER_QUITO

Building configuration...

```
Current configuration : 881 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ROUTER_QUITO
!
IPV6 unicast-routing
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
IPV6 address 2001:DB8:5::1/64
IPV6 mtu 1500
IPV6 enable
IPV6 ospf 1 area 0
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
```

```
shutdown
!
interface Serial0/0/0
no ip address
IPV6 address 2001:DB8:6::2/64
IPV6 mtu 1500
IPV6 enable
IPV6 ospf 1 area 0
clock rate 9600
!
interface Serial0/0/1
no ip address
IPV6 address 2001:DB8:4::2/64
IPV6 mtu 1500
IPV6 enable
IPV6 ospf 1 area 0
clock rate 9600
!
interface Vlan1
no ip address
shutdown
!
IPV6 router ospf 1
router-id 1.1.1.1
```

```
log-adjacency-changes
!
ip classless
line con 0
line vty 0 4
login
end
```

Conclusiones

- Una vez analizada la técnica Packet Classification en redes IPV4 se determina que provee una diferente calidad de servicio lo cual se demostró en la sección 4.5.1, por lo que se afirma la hipótesis planteada para el escenario en IPV4.
- Una vez analizada la técnica Packet Classification en redes IPV6 se determina que provee una diferente calidad de servicio lo cual se demostró en la sección 4.5.2, por lo que se afirma la hipótesis planteada para el escenario en IPV6.
- En la implantación de la técnica Packet Classification se pudo determinar la mejor opción para la creación del diseño de los mapas de clase tanto para la entrada como para la Salida de datos, además de crear las políticas para el manejo de los mapas de clase. Cabe indicar que la política para la entrada de datos es la única que se le puede agregar niveles de prioridad, a la política para la salida de datos se le puede agregar la diferenciación de tráfico usando el reconocimiento del algoritmo af31 usado para VOIP.

Recomendaciones

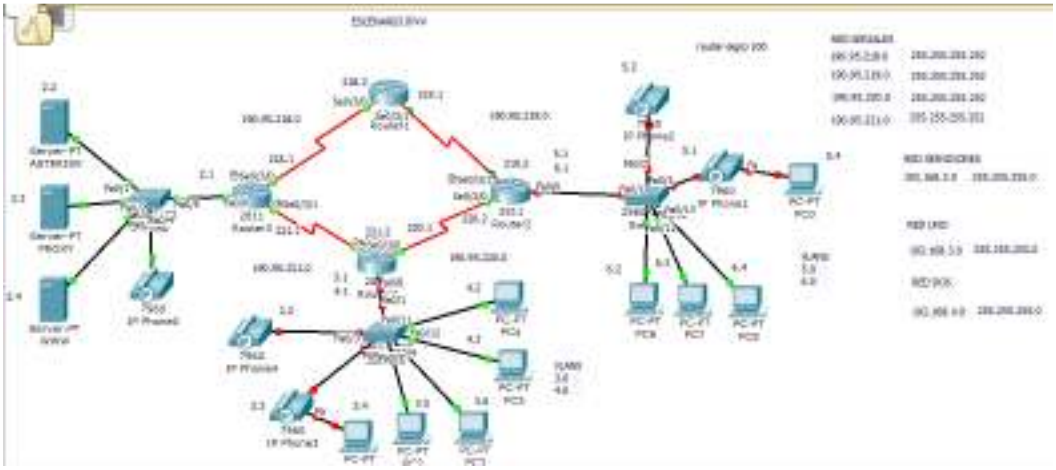
- Basado en los niveles emitidos por la ITU para llamadas de VOIP que es de 150 ms, el valor obtenido en los escenario de IPV4 e IPV6 aplicando la técnica Packet Classification para la variable jitter respectivamente es de 0.000118 y 0.00007 segundos lo cual es un valor muy por debajo al valor emitido por la ITU, por lo que se determina que la utilización de la técnica Packet Classification bajo los escenarios planteados no es recomendable ya que presenta una mejora insignificante frente a los valores publicados por la ITU para la transmisión de la VOIP.

- Si se decide implementar esta técnica para manejar el nivel de prioridad de las políticas de entrada se recomienda utilizar la prioridad 50 ya que una vez que se realizaron las pruebas brindo una mejora en el jitter tanto para el escenario en IPV4 como en el escenario de IPV6.

ANEXOS

1. Configuración de la técnica Packet Classification en IPV4

CONFIGURACION IPV4 CON PACKET CLASSIFICATION



Configuración de los ROUTERS IPV4

ROUTER_GUARANDA

PUERTO	DISPOSITIVO	IP	MASCARA
F0/0	SW_GUARANDA	192.168.2.1	255.255.255.0
SE0/3/0	ROUTER_MACAS	190.95.218.1	255.255.255.252
SE0/3/1	ROUTER_RIOBAMBA	190.95.221.1	255.255.255.252

ROUTER_MACAS

PUERTO	DISPOSITIVO	IP	MASCARA
SE0/3/0	ROUTER_GUARANDA	190.95.218.2	255.255.255.252

SE0/3/1	ROUTER_QUITO	190.95.219.1	255.255.255.252

ROUTER_QUITO

PUERTO	DISPOSITIVO	IP	MASCARA
SE0/3/1	ROUTER_MACAS	190.95.219.2	255.255.255.252
SE0/3/0	ROUTER_RIOBAMBA	190.95.220.2	255.255.255.252
F0/0	SW_QUITO	192.168.5.1	255.255.255.0
F0/0	SW_QUITO	192.168.6.1	255.255.255.0

ROUTER_RIOBAMBA

PUERTO	DISPOSITIVO	IP	MASCARA
SE0/3/1	ROUTER_GUARANDA	190.95.221.2	255.255.255.252
SE0/3/0	ROUTER_QUITO	190.95.220.1	255.255.255.252
F0/0	SW_RIOBAMBA	192.168.4.1	255.255.255.0
F0/0	SW_RIOBAMBA	192.168.3.1	255.255.255.0

Configuración de los SWITCHS

SW_GUARANDA

PUERTO	PC	VLANS	IP	MASCARA	GATEWAY
F0/1	SERVIDOR_ASTERISK	VLAN 2_SERVIDORES	192.168.2.2	255.255.255.0	192.168.2.1
F0/2	SERVIDOR_PROXY	VLAN 2_SERVIDORES	192.168.2.3	255.255.255.0	192.168.2.1
F0/3	SERVIDOR_WWW	VLAN 2_SERVIDORES	192.168.2.4	255.255.255.0	192.168.2.1
F0/4	IP Phone0	VLAN 2_SERVIDORES	192.168.2.5	255.255.255.0	192.168.2.1
F0/5	ROUTER_GUARANDA				

SW_RIOBAMBA

PUERTO	PC	VLANS	IP	MASCARA	GATEWAY
F0/1	ROUTER_RIOBAMBA				
F0/2	IP Phone4	VLAN 3_VOZ_1	192.168.3.2	255.255.255.0	192.168.3.1
F0/3	IP Phone3	VLAN 3_VOZ_1	192.168.3.3	255.255.255.0	192.168.3.1
F0/3	PC1	VLAN 3_VOZ_1	192.168.3.4	255.255.255.0	192.168.3.
					1
F0/4	PC2	VLAN	192.168.4.3	255.255.255.0	192.168.4.1

		4_DATOS_1			
F0/5	PC3	VLAN 4_DATOS_1	192.168.4.4	255.255.255.0	192.168.4.1
F0/6	PC5	VLAN 4_DATOS_1	192.168.4.5	255.255.255.0	192.168.4.1
F0/7	PC4	VLAN 4_DATOS_1	192.168.4.6	255.255.255.0	192.168.4.1

SW_QUITO

PUERTO	PC	VLANS	IP	MASCARA	GATEWAY
F0/1	ROUTER_QUITO				
F0/2	IP Phone2	VLAN 5_VOZ_1	192.168.5.2	255.255.255.0	192.168.5.1
F0/3	IP Phone1	VLAN 5_VOZ_1	192.168.5.3	255.255.255.0	192.168.5.1
F0/3	PC0	VLAN 5_VOZ_1	192.168.5.4	255.255.255.0	192.168.5.1
F0/4	PC6	VLAN 6_DATOS_1	192.168.6.2	255.255.255.0	192.168.6.1
F0/5	PC7	VLAN 6_DATOS_1	192.168.6.3	255.255.255.0	192.168.6.1
F0/6	PC8	VLAN 6_DATOS_1	192.168.6.4	255.255.255.0	192.168.6.1

CONFIGURACION IPV4 CON PACKET CLASSIFICATION

Configuración ROUTER_GUARANDA

Building configuration...

Current configuration : 1250 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname ROUTER_GUARANDA

!

class-map match-all classSalida

match ip dscp af31

class-map match-all classEntrada

match ip dscp af31

!

policy-map policyEntrada

class classEntrada

set ip dscp af31

!

policy-map policySalida

```
class classSalida
priority 50
!
interface FastEthernet0/0
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/3/0
ip address 190.95.218.1 255.255.255.252
service-policy input policyEntrada
service-policy output policySalida
clock rate 128000
!
interface Serial0/3/1
ip address 190.95.221.1 255.255.255.252
service-policy input policyEntrada
service-policy output policySalida
```

```
clock rate 128000
!
interface Vlan1
no ip address
shutdown
!
router eigrp 100
network 190.95.0.0
network 192.168.2.0
auto-summary
!
router ospf 1
log-adjacency-changes
network 190.95.221.0 0.0.0.3 area 1
network 190.95.218.0 0.0.0.3 area 1
network 192.168.2.0 0.0.0.3 area 1
!
ip classless
!
no cdp run
!
line con 0
line vty 0 4
login
```

!

end

Configuración ROUTER_RIOBAMBA

Building configuration...

Current configuration : 1409 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname ROUTER_RIOBAMBA

!

class-map match-all classEntrada

match ip dscp af31

class-map match-all classSalida

match ip dscp af31

!

policy-map policyEntrada

class classEntrada

set ip dscp af31

!

policy-map policySalida

```
class classSalida
priority 50
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.1
encapsulation dot1Q 3
ip address 192.168.3.1 255.255.255.0
!
interface FastEthernet0/0.2
encapsulation dot1Q 4
ip address 192.168.4.1 255.255.255.0
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/3/0
ip address 190.95.220.1 255.255.255.252
```

```
service-policy input policyEntrada
service-policy output policySalida
clock rate 128000
!
interface Serial0/3/1
ip address 190.95.221.2 255.255.255.252
service-policy input policyEntrada
service-policy output policySalida
!
interface Vlan1
no ip address
shutdown
!
router eigrp 100
network 190.95.0.0
auto-summary
!
router ospf 1
log-adjacency-changes
network 190.95.221.0 0.0.0.3 area 1
network 190.95.220.0 0.0.0.3 area 1
network 192.168.3.0 0.0.0.255 area 1
network 192.168.4.0 0.0.0.255 area 1
!
```

ip classless

!

no cdp run

!

line con 0

line vty 0 4

login

!

end

Configuración ROUTER_MACAS

Building configuration...

Current configuration : 1113 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname ROUTER_MACAS

!

class-map match-all class1

match ip dscp af31

class-map match-all classSalida

```
match ip dscp af31
!
policy-map policy1
class class1
set ip dscp af31
!
policy-map policySalida
class classSalida
priority 50
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/3/0
ip address 190.95.218.2 255.255.255.252
```

```
service-policy input policy1
service-policy output policySalida
!
interface Serial0/3/1
ip address 190.95.219.1 255.255.255.252
service-policy input policy1
service-policy output policySalida
!
interface Vlan1
no ip address
shutdown
!
router eigrp 100
network 190.95.0.0
auto-summary
!
router ospf 1
log-adjacency-changes
network 190.95.218.0 0.0.0.255 area 1
network 190.95.219.0 0.0.0.255 area 1
!
ip classless
!
no cdp run
```

!

line con 0

line vty 0 4

login

!

end

Configuración ROUTER_QUITO

Building configuration...

Current configuration : 1408 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname ROUTER_QUITO

!

class-map match-all classEntrada

match ip dscp af31

class-map match-all classSalida

match ip dscp af31

!

```
policy-map policyEntrada
class classEntrada
set ip dscp af31
!
policy-map policySalida
class classSalida
priority 50
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.1
encapsulation dot1Q 5
ip address 192.168.5.1 255.255.255.0
!
interface FastEthernet0/0.2
encapsulation dot1Q 6
ip address 192.168.6.1 255.255.255.0
!
interface FastEthernet0/1
no ip address
duplex auto
```

```
speed auto
shutdown
!
interface Serial0/3/0
ip address 190.95.220.2 255.255.255.252
service-policy input policyEntrada
service-policy output policySalida
!
interface Serial0/3/1
ip address 190.95.219.2 255.255.255.252
service-policy input policyEntrada
service-policy output policySalida
clock rate 128000
!
interface Vlan1
no ip address
shutdown
!
router eigrp 100
network 190.95.0.0
auto-summary
!
router ospf 1
log-adjacency-changes
```

network 190.95.219.0 0.0.0.255 area 1

network 190.95.220.0 0.0.0.3 area 1

network 192.168.5.0 0.0.0.255 area 1

network 192.168.6.0 0.0.0.255 area 1

!

ip classless

!

no cdp run

!

line con 0

line vty 0 4

login

!

End

2. Datos obtenidos de los escenarios de IPV4 e IPV6 con el software D-ITG

Anexos D-ITG

Resultados con D-ITG IPV4 sin PC

```
[root@localhost bin]# ./ITGDec recv_log_file_IPV4_sinp25oct

ITGDec version 2.8.0-rc1 (r457:458)

Compile-time options:

/------------------------------------------------------------

Flow number: 1

From 192.168.2.2:46045

To    192.168.5.2:8999

------------------------------------------------------------

Total time               =    299.992927 s

Total packets            =         30000

Minimum delay            =     10.999400 s

Maximum delay            =     11.048926 s

Average delay            =     11.009699 s

Average jitter           =      0.000155 s

Delay standard deviation =      0.016083 s

Bytes received           =       2760000

Average bitrate          =     73.601735 Kbit/s

Average packet rate      =    100.002358 pkt/s

Packets dropped          =             0 (0.00 %)

Average loss-burst size  =      0.000000 pkt
```

```
------------------------------------------------------------


____________________________________________________________

**********  TOTAL RESULTS   **********

____________________________________________________________

Number of flows          =            1
Total time               =   299.992927 s
Total packets            =        30000
Minimum delay            =    10.999400 s
Maximum delay            =    11.048926 s
Average delay            =    11.009699 s
Average jitter           =     0.000155 s
Delay standard deviation =     0.016083 s
Bytes received           =      2760000
Average bitrate          =    73.601735 Kbit/s
Average packet rate      =   100.002358 pkt/s
Packets dropped          =            0 (0.00 %)
Average loss-burst size  =            0 pkt
Error lines              =            0

------------------------------------------------------------
```

Resultados con D-ITG IPV4 con PC

```
[root@localhost bin]# ./ITGDec recv_log_file_IPV4_conp25oct

ITGDec version 2.8.0-rc1 (r457:458)
```

```
Compile-time options:

/-------------------------------------------------------------

Flow number: 1

From 192.168.2.2:50994

To    192.168.5.2:8999

-------------------------------------------------------------

Total time                =    299.954249 s

Total packets             =         30000

Minimum delay             =     11.029447 s

Maximum delay             =     11.076817 s

Average delay             =     11.035750 s

Average jitter            =      0.000118 s

Delay standard deviation =      0.010955 s

Bytes received            =       2760000

Average bitrate           =     73.611226 Kbit/s

Average packet rate       =    100.015253 pkt/s

Packets dropped           =             0 (0.00 %)

Average loss-burst size   =      0.000000 pkt

-------------------------------------------------------------


_____________________________________________________________

***************  TOTAL RESULTS   ******************

_____________________________________________________________
```

```
Number of flows          =            1
Total time               =   299.954249 s
Total packets            =        30000
Minimum delay            =    11.029447 s
Maximum delay            =    11.076817 s
Average delay            =    11.035750 s
Average jitter           =     0.000118 s
Delay standard deviation =     0.010955 s
Bytes received           =      2760000
Average bitrate          =    73.611226 Kbit/s
Average packet rate      =   100.015253 pkt/s
Packets dropped          =            0 (0.00 %)
Average loss-burst size  =            0 pkt
Error lines              =            0
```

Resultados con D-ITG IPV6 sin PC

```
[root@localhost bin]# ./ITGDec recv_log_file_IPV6sinp25oct
ITGDec version 2.8.0-rc1 (r457:458)
Compile-time options:
/------------------------------------------------------------
Flow number: 1
From 2001:db8:2::2:55893
To    2001:db8:5::2:8999
```

```
------------------------------------------------------------

Total time                =    300.026939 s

Total packets             =         30000

Minimum delay             =     11.376852 s

Maximum delay             =     11.414412 s

Average delay             =     11.390611 s

Average jitter            =      0.000090 s

Delay standard deviation =      0.015689 s

Bytes received            =       2760000

Average bitrate           =     73.593392 Kbit/s

Average packet rate       =     99.991021 pkt/s

Packets dropped           =             0 (0.00 %)

Average loss-burst size   =      0.000000 pkt

------------------------------------------------------------


____________________________________________________________

****************  TOTAL RESULTS   ******************

____________________________________________________________

Number of flows           =             1

Total time                =    300.026939 s

Total packets             =         30000

Minimum delay             =     11.376852 s

Maximum delay             =     11.414412 s
```

```
Average delay            =     11.390611 s
Average jitter           =      0.000090 s
Delay standard deviation =      0.015689 s
Bytes received           =       2760000
Average bitrate          =     73.593392 Kbit/s
Average packet rate      =     99.991021 pkt/s
Packets dropped          =             0 (0.00 %)
Average loss-burst size  =             0 pkt
Error lines              =             0
-------------------------------------------------------------
```

Resultados con D-ITG IPV6 con PC

```
root@localhost bin]# ./ITGDec recv_log_file_IPV6conp25oct
ITGDec version 2.8.0-rc1 (r457:458)
Compile-time options:
/-------------------------------------------------------------
Flow number: 1
From 2001:db8:2::2:34577
To    2001:db8:5::2:8999
-------------------------------------------------------------
Total time               =    299.997339 s
Total packets            =         30000
Minimum delay            =     11.349484 s
Maximum delay            =     11.356785 s
```

```
Average delay            =     11.352798 s
Average jitter           =      0.000073 s
Delay standard deviation =      0.001641 s
Bytes received           =       2760000
Average bitrate          =     73.600653 Kbit/s
Average packet rate      =    100.000887 pkt/s
Packets dropped          =             0 (0.00 %)
Average loss-burst size  =      0.000000 pkt
-------------------------------------------------------------


_____________________________________________________________

****************  TOTAL RESULTS   ******************

_____________________________________________________________

Number of flows          =             1
Total time               =    299.997339 s
Total packets            =         30000
Minimum delay            =     11.349484 s
Maximum delay            =     11.356785 s
Average delay            =     11.352798 s
Average jitter           =      0.000073 s
Delay standard deviation =      0.001641 s
Bytes received           =       2760000
Average bitrate          =     73.600653 Kbit/s
```

```
Average packet rate      =    100.000887 pkt/s

Packets dropped          =             0 (0.00 %)

Average loss-burst size  =             0 pkt

Error lines              =             0
```

CAPITULO 3

1.- Algoritmo para VOIP AF31

http://tools.ietf.org/html/rfc2597

02 de Abril de 2013

2.- Códec G711

http://es.wikipedia.org/wiki/Voz_sobre_Protocolo_de_Internet

02 de Abril de 2013

CAPITULO 4

3.- Conceptos y Elementos Básicos de Tráfico en Telecomunicaciones.

http://departamento.pucp.edu.pe/ingenieria/images/documentos/seccion_telecomunicaciones/Capitulo%205%20Modelos%20de%20Trafico.pdf

08 de abril de 2013

CAPITULO 2

4.- Configuring Class Maps and Policy Maps

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A1/configuration/administration/guide/mapolcy.pdf

06 de junio de 2011

CAPITULO 1

5.- Foro Latinoamericano de IPV6 – FLIP6

http://lacnic.net/documentos/lacnicxv/Presentacion%20_FLIP6.pdf

18 de Mayo del 2011

CAPITULO 2

6.- IPV6

http://es.wikipedia.org/wiki/IPV6

18 de Mayo del 2011

7.- Programa de Doctorado Informática Industrial 2009-2010

http://es.scribd.com/doc/48158880/SMARD-0910-QoS-1

18 de Mayo del 2011

8.- Protocolos de Calidad de Servicio

http://es.scribd.com/doc/49332259/Protocolos-QoS-v4-0

18 de Mayo del 2011

9.- QUÉ ES LA DESVIACIÓN ESTÁNDAR Y COMO INTERPRETARLA

http://tradingcenter.wordpress.com/2009/11/11/que-es-la-desviacion-estandar-y-como-interpretarla-1/

23 de octubre de 2012

10.- TELEFONIA IP

http://www.slideshare.net/ces1227/conceptos-vo-ip

18 de Mayo del 2011

11.- Voz Sobre IP

http://www.slideshare.net/danielayc/voip-315486

18 de Mayo del 2011