

**FASE 6  
EVALUAR EL PROYECTO**

**DIPLOMADO DE PROFUNDIZACIÓN EN REDES DE NUEVA GENERACIÓN**

**Realizado por:**

Diego Alejandro Granados Brand – 1115916214  
Carlos Hernando Salazar Vallejo – 98512376  
Juan Camilo Pulgarin Salazar - 8175302  
Jorge Cano Parra – 71318529

**Fecha:**

Diciembre 12

**Tutor:**

Omar Trejo



UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA

2018

## **Introducción**

Después de definir y planificar paso a paso el proyecto definido para el semestre, consolidamos en el presente trabajo los puntos que busca evidenciar que el desarrollo propuesto funciona correctamente.

Inicialmente se hace una conceptualización de los temas más importantes que aportaron en el desarrollo de los siguientes puntos en los cuales nos apoyamos en el uso de herramientas como simuladores, evidenciando así el funcionamiento correcto.

El trabajo en equipo fue fundamental para obtener los resultados que se describen en el presente trabajo.

## **Objetivo General**

Implementación de los servicios de voz y calidad de servicio para una red NGN que permite la red para la comunicación entre la ciudad de Bogotá y Cali.

## **Objetivos específicos**

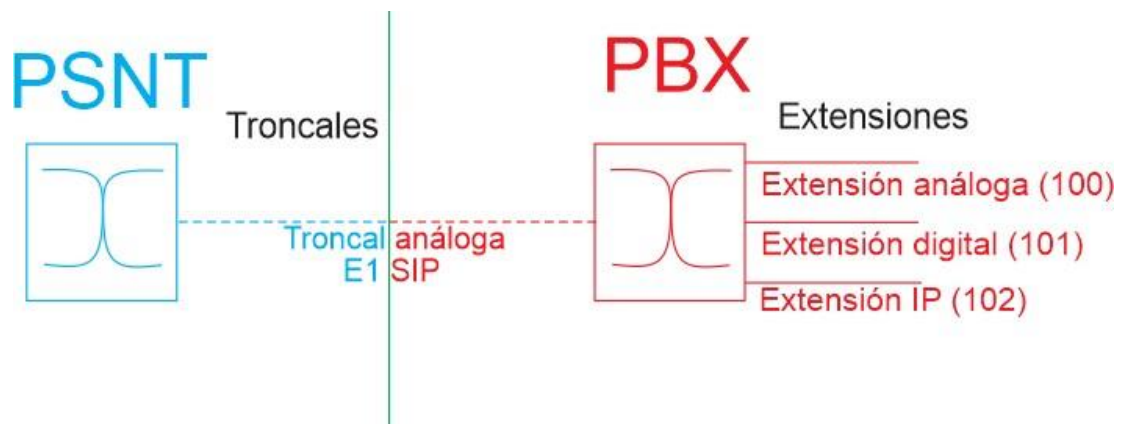
- Explicar cómo funciona una PBX y los protocolos HTTP, RTP y MPLS
- Identificar la importancia de IPV6
- Implementa El servicio IPTV entre las dos ciudades y el plan de calidad
- Explica una red IPv4/IPv6 con soporte MPLS para las dos ciudades.

# CONTENIDO

## 1. Explique cómo funciona una PBX.

PBX: Son las siglas en inglés de “Private Branch Exchange”, la cual es una red telefónica privada utilizada dentro de una empresa. Es central telefónica conectada directamente a la red pública de telefonía por medio de líneas troncales para gestionar además de las llamadas internas, las entrantes y salientes con autonomía sobre cualquier otra central telefónica. Este dispositivo generalmente pertenece a la empresa que lo tiene instalado y no a la compañía telefónica. Un PBX se refiere al dispositivo que actúa como una ramificación de la red primaria pública de teléfonos, por lo que los usuarios no se comunican directamente al exterior mediante líneas telefónicas convencionales, sino que al estar el PBX directamente conectado a la RTC (red telefónica pública), será esta misma la que enrute la llamada hasta su destino final mediante enlaces unificados de transporte de voz llamados líneas troncales

Aquí tenemos la red telefónica pública conmutada que nos provee de una línea al PBX; estas líneas son troncales que pueden ser analógicas, E1 o SIP y el PBX provee de extensiones. En el ejemplo tenemos 3: 100 de tipo analógico, 101 de tipo digital y 102 de tipo IP.



Si en un establecimiento como una empresa el jefe (extensión 100) quiere hablar con su secretaria (extensión 101) sin una PBX, el jefe y la secretaria tendrían que tener cada uno una línea telefónica con el PSNT donde se cobra por minuto.

Una PBX permite conectar la llamada sin llegar al PSNT permitiéndose llamadas ilimitadas y gratuitas entre las extensiones.

La línea troncal permite hacer llamadas al exterior y todos comparten las líneas externas. 20 o 30 líneas pueden ser compartidas por 200 o 300 personas, pensando en que es poco probable que salgan 200 llamadas a la vez, por eso el número de líneas limita el número de llamadas externas simultáneas y hay que tener en cuenta esto al implementar este sistema, ver la necesidad del cliente.

## 2. Que se debe tener en cuenta para implementar el servicio IPTV.

La arquitectura de telecomunicaciones para una plataforma IPTV (modelo de solución de CISCO) que debe disponer un operador para la prestación del servicio de IPTV constituida por los siguientes componentes:

- Cabecera: Es la responsable por la codificación, el cifrado y la inyección de los canales de televisión en forma de paquetes de datos IP en multicast.
- Plataforma de video en demanda: Encargada de atender y almacenar las solicitudes de los usuarios en forma de datos IP unicast.
- Portal interactivo: Permite a los usuarios navegar dentro de los diferentes servicios IPTV (en particular, permite navegar el catálogo de productos en demanda).
- Red de transporte: Red responsable por el transporte de paquetes (unicast/multicast) IP. Gateway
- residencial: pieza de equipo en el hogar del suscriptor que termina el enlace de acceso desde la red de transporte.

Dependiendo de la arquitectura de la red del prestador del servicio, se pueden considerar dos arquitecturas básicas para el servidor de entrega de contenidos encaminadas al despliegue de IPTV: una centralizada y la otra distribuida.

En la arquitectura centralizada, todos los contenidos están almacenados en servidores centralizados, y, por tanto, no es necesario contar con un sistema de distribución de contenidos

Las exigencias de los equipos para el uso de IPTV en SD con estos códecs son:

DSLAM IP

- Funcionalidad IGMP O IGMP Proxy
- Velocidad de conmutación de canales multicast menor a 2 segundos.
- Facilidad de incrementar las interfaces de red
- Manejo y mapeo de VLAN
- Priorización de tráfico

#### DSLAM ATM

- Debe soportar multicast con funcionalidad IGMP Snooping
- Velocidad de conmutación de canales adecuada.
- Facilidad de incremento de sus interfaces
- Debe controlar cuales canales multicast envía al modem ADSL.

#### Modem ADSL

- Priorización del tráfico en función de PVC O de PVLAN.
- Disponer de varios puertos Ethernet.
- Verificar que la distancia máxima del lazo de línea no exceda los 3 kilómetros de radio del NAM.

#### Equipo de Cabecera

- Permitir la recepción de señales provenientes de satélites o de emisores locales.
- Codificar señales de audio y video para la protección de contenidos
- Conformación de los flujos digitales como CBR.
- Insertar propaganda y sobre impresos
- Multiplexar las señales digitales en un único flujo IP/GbE CBR para ser distribuido en la red de acceso y transporte IP del operador que oferta el servicio
- Posibilidad de presentación de una Mosaico de canales o de la facilidad Picture in Picture.
- Envío de la factura electrónica de programación a los canales de BTV.
- Posibilitar el monitoreo remoto del servidor de video.
- Empleo de interfaces de red GbE.

#### Middleware

- Interoperabilidad con los STB utilizados
- Soporte a los servicios básicos BTV, EPG, VoD y servicios PPV.
- Permitir aplicaciones avanzadas como lo son el identificador de llamadas, PVR, gestión y aprovisionamiento de clientes, autoconfiguración de los STB, auditoria y trazas, gestión automatizada del contenido y creación automatizada de EPG.

- Servicio DHCP a los STB de los clientes.
- Servicios de tasación de los servicios de VoD y PPV.
- Poseer una interfaz gráfica amigable.

Para un adecuado funcionamiento de los servicios IPTV, es crítico dimensionar correctamente la red IP. La interactividad de estos servicios requiere que la velocidad de respuesta adecuadas entre 50 y 200 ms para no afectar la interactividad del usuario. Los puntos que hay que tener en cuenta en el dimensionamiento son:

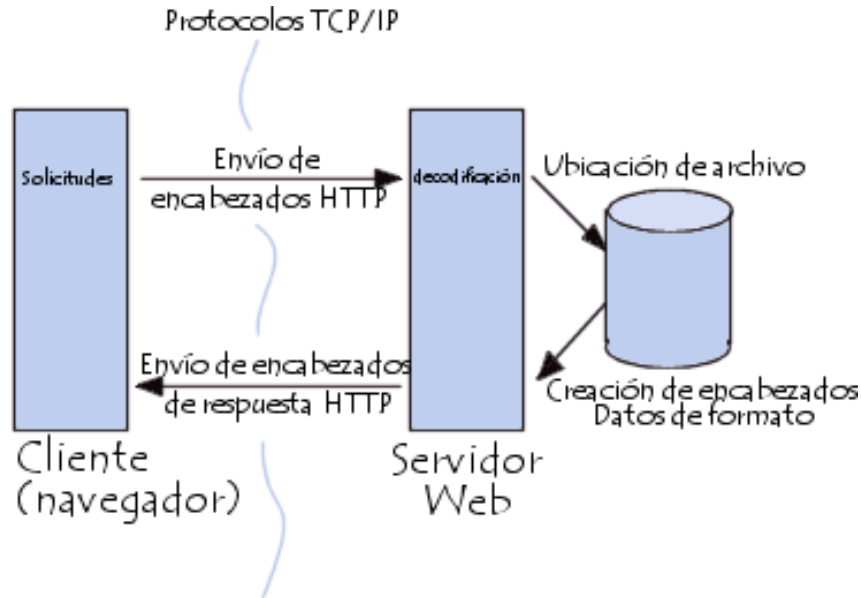
- Concurrencia de canales BTV, la cantidad de canales que pueden ser vistos simultáneamente.
- Concurrencia de usuarios de VoD, es decir cuántos usuarios están solicitando este servicio.
- Cantidad de canales HD, pues estos consumen más ancho de banda que los SD.
- Cantidad de señales que recibe un usuario simultáneamente.

### 3. Explique los protocolos HTTP, RTP y MPLS

- ✓ Protocolos HTTP: Son las siglas en inglés de HyperText Transfer Protocol (en español protocolo de transferencia de hipertexto). Es un protocolo de red (un protocolo se puede definir como un conjunto de reglas a seguir) para publicar páginas de web o HTML. HTTP es la base sobre la cual está fundamentado Internet, o la WWW.

El protocolo HTTP funciona a través de solicitudes y respuestas entre un cliente (por ejemplo, un navegador de Internet) y un servidor (por ejemplo, la computadora donde residen páginas web). A una secuencia de estas solicitudes se le conoce como sesión de HTTP.

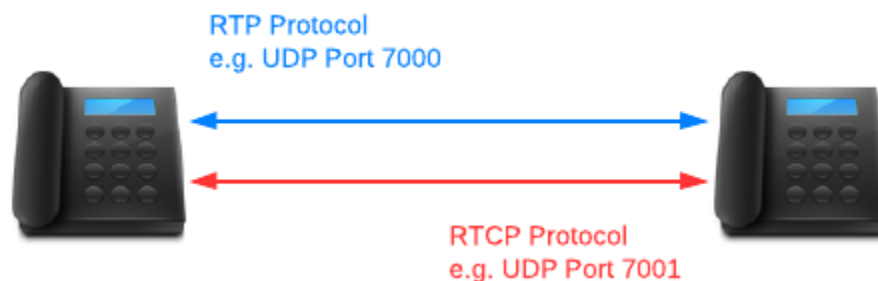
La información que el navegador de Internet está presentando en un momento dado, se identifica en la llamada “barra de navegación”, que comienza con http y se le conoce como URI (más conocido como URL).



- ✓ Protocolos RTP Significa “Real Time Transport Protocol” (Protocolo de transporte en tiempo real), y define un formato de paquete estándar para el envío de audio y video sobre Internet. Es definido en el RFC1889. Fue desarrollado por el grupo de trabajo de transporte de audio y video y fue publicado por primera vez en 1996. RTP se utiliza ampliamente en los sistemas de comunicación y entretenimiento que involucran medios de transmisión, tales como la telefonía, aplicaciones de videoconferencias, servicios de televisión y web basado en funcionalidades push-to-talk

Permite:

- ✓ Identificar el tipo de información transmitida.
- ✓ Agregarle marcadores temporales y números de secuencia a la información transmitida.
- ✓ controlar la llegada de los paquetes a destino.



- protocolos MPLS: MPLS (MultiProtocol Label Switching) es un protocolo de conmutación por etiquetas definido para funcionar sobre múltiples protocolos



como Sonet, Frame Relay, ATM, Ethernet o cualquiera sobre el que pueda funcionar PPP

Los campos de la cabecera MPLS de 4 bytes, son los siguientes:

- ✓ Label (20 bits). Es el valor actual, con sentido únicamente local, de la etiqueta MPLS. Esta etiqueta es la que determinará el próximo salto del paquete.
- ✓ CoS (3 bits). Este campo afecta a los algoritmos de descarte de paquetes y de mantenimiento de colas en los nodos intermedios, es decir, indica la QoS del paquete. Mediante este campo es posible diferenciar distintos tipos de tráfico y mejorar el rendimiento de un tipo de tráfico respecto a otros.
- ✓ Stack (1 bit). Mediante este bit se soporta una pila de etiquetas jerárquicas, es decir, indica si existen más etiquetas MPLS. Las cabeceras MPLS se comportan como si estuvieran apiladas una sobre otra, de modo que el nodo MPLS tratará siempre la que esté más alto en la pila. La posibilidad de encapsular una cabecera MPLS en otras, tiene sentido, por ejemplo, cuando se tiene una red MPLS que tiene que atravesar otra red MPLS perteneciente a un ISP u organismo administrativo externo distinto; de modo que, al terminar de atravesar esa red, se continúe trabajando con MPLS como si no existiera dicha red externa.

#### 4. Explique la importancia de IPV6

El nuevo protocolo IPv6, dispone de 340 billones de billones de billones (sextillones) de direcciones, lo que hace que la cantidad de direcciones IPv4 parezca insignificante, se ha puesto el ejemplo en que, si todo el espacio de IPv4 fuera como una pelota de golf, IPv6 tendría el tamaño del sol.

Con este mayor espacio de direcciones, IPv6 ofrece una variedad de ventajas en términos de estabilidad, flexibilidad y simplicidad en la administración de las redes. También generara una nueva ola de innovación en las aplicaciones y las ofertas de servicio ya que, termina con la necesidad de direcciones compartidas

La cantidad de direcciones disponibles en IPV6 es mucho más grande que las de IPV4:

- ✓ IPv4: 4,294,967,296 direcciones.
- ✓ IPv6: 340,282,366,920,938,463,463,374,607,431,768,211,456 direcciones.

Actualmente hay 17.6 mil millones de dispositivos conectados y se pronostica que para el 2020 habrá 50 mil millones.

## **Colaborativa**

La empresa TecnoTelecoUnad, implementará una red NGN en la cual se van a configurar los siguientes servicios:

1. Un Call Center basado en Asterisk para comunicar las ciudades de Bogotá y Cali, con capacidad para 2 troncales telefónicas 1 analógica y 1 digital.

Para poder utilizar las troncales analógicas y digitales, se tendrán en cuenta las siguientes condiciones:

80 llamadas simultáneas entre la sede de Bogotá y Cali de la empresa.

El transporte de datos entre las sedes de la empresa tiene un ancho de banda de 2Mbps.

La PBX analógica en Bogotá deberá mantener el enlace troncal de 4 conexiones con el central office (C.O)

La PBX analógica en Cali deberá mantener en enlace troncal de 20 conexiones con el central office (C.O)

Partiendo de la red planteada en el trabajo anterior continuaremos con la descripción de la red a implementar, pero inicialmente debemos hacer los cálculos de los datos necesarios que se describen a continuación:

Elementos para tener presentes:

- RED ANALÓGICA: emplea el puerto FX0
- RED DIGITAL: Emplea el puerto E1
- PROTOCOLO: EIE1

Se emplea una muestra de 0,25ms, con un ancho de banda de 8kbps, obteniendo como resultado un paquete de bytes de 25

Calculamos el tiempo por una llamada:

- 25 por WAN

- Conexión punto a punto, muestra por 8
- 48 utilizan 3 protocolos

Total de la suma de las variables anteriores 48 y eso lo multiplico por la relación con minutos y posteriormente los relaciono en paquetes de bite así:

$$81*50=4050*8=32.400$$

Este dato lo multiplicamos por 80 porque en el enunciado del ejercicio nos dan como requisito que este número deben ser las llamadas en simultanea:

$$32400*80=2.592.000/2.5 \text{ ancho de banda}$$

Por lo tanto, necesitamos los 2Mbps que ya tenemos definidos, más 2,5 que acabamos de hallar en el ejercicio anterior para un total de 4,5 Mbps.

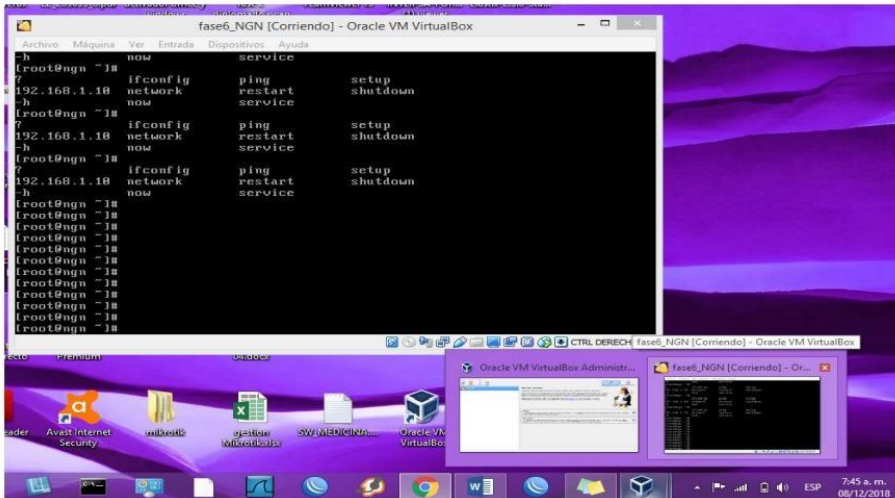
Para Bogotá emplearemos 4 puertos y para Cali como son 20 llamadas se deben digitalizar.

Con la descripción anterior calculamos los elementos necesarios para poder realizar la comunicación de las llamadas que nos describen en la guía de actividades.

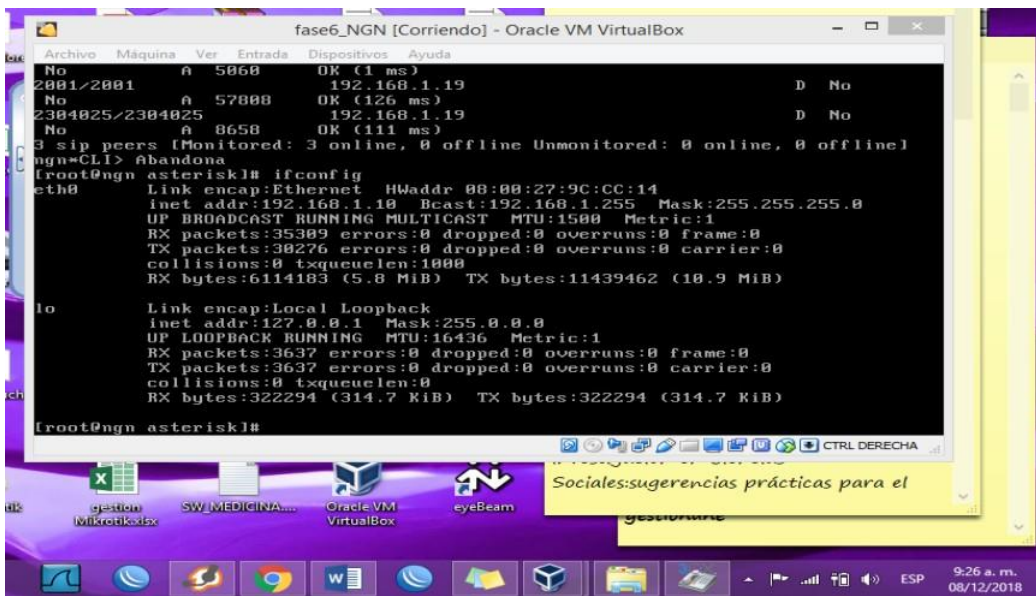
2. El servicio IPTV entre las dos ciudades el cual permitirá transferir contenidos multimedia.

Nombre de la maquina: ngn

Contraseña root: 123456

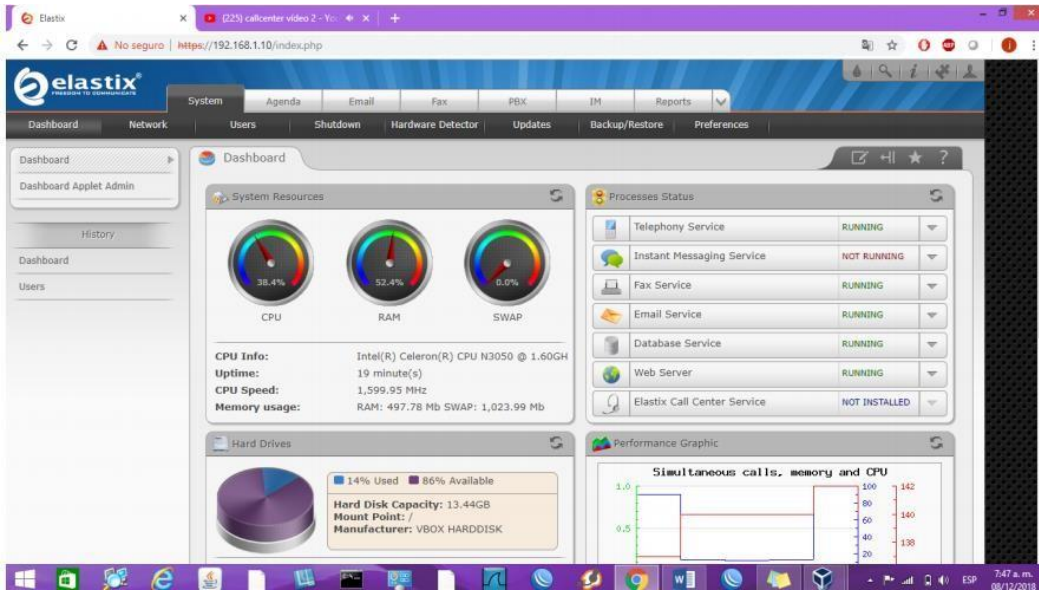


Ifconfig: interfaz configurada para nuestro caso el puerto de red para el servidor Asterisk 192.168.1.10



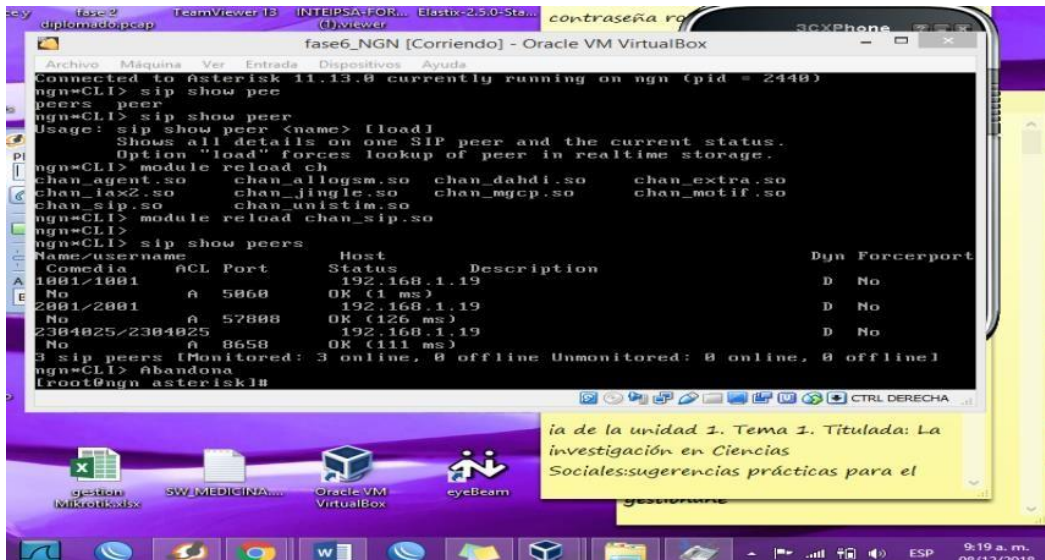
Se realiza prueba de conectividad con ping a la dirección ip configurada en el eth0 192.168.1.10





Rasterisk

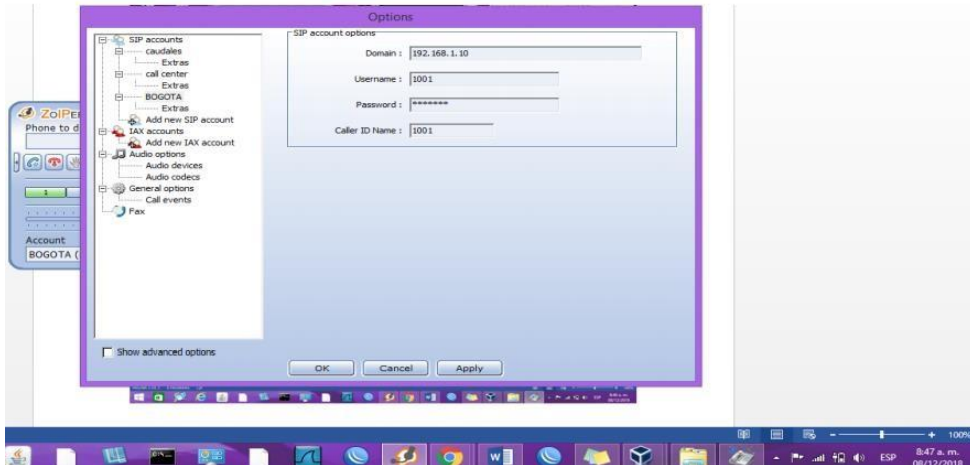
Sip show peers: estado de las cuentas creadas.



2. El servicio IPTV entre las dos ciudades el cual permitirá transferir contenidos multimedia.

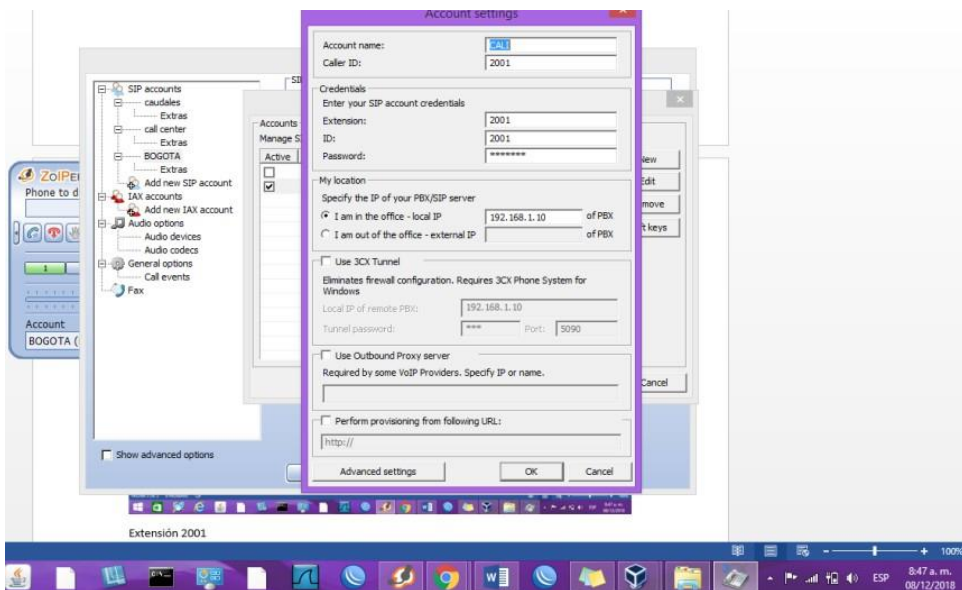
Extensión 1001

Secret abc1001



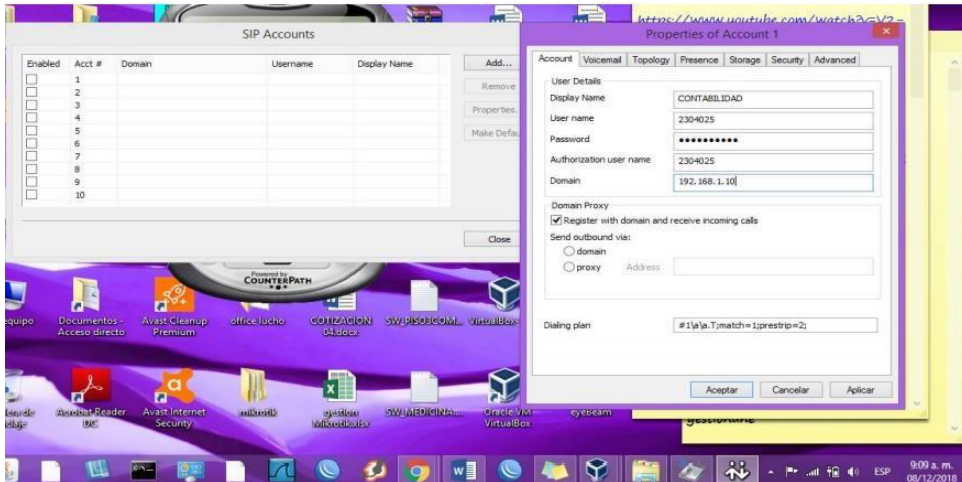
Extensión 2001

Secret abc2001

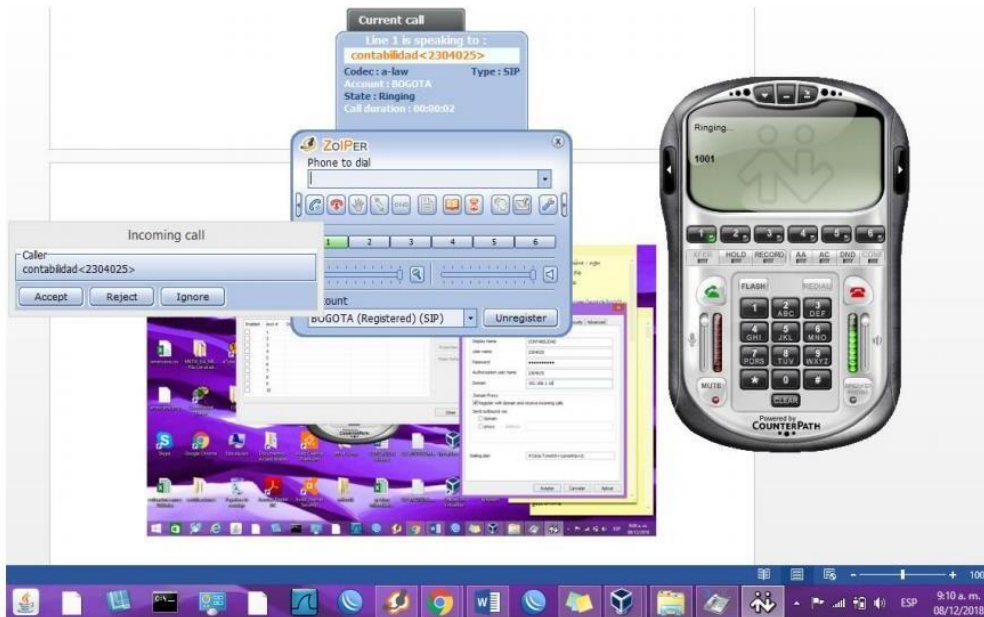


CONTABILIDAD 2304025

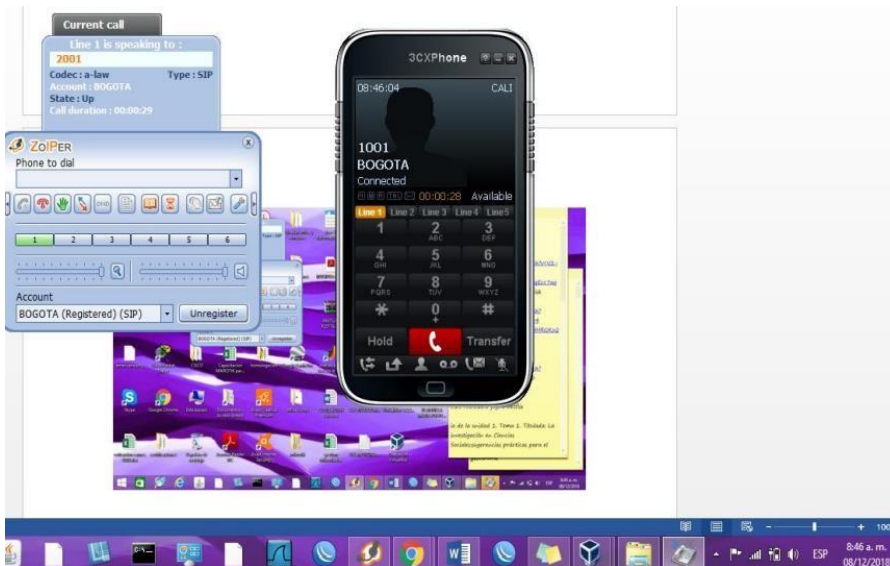
Secret abc2304025



Pruebas de llamadas entre las cuentas creadas.





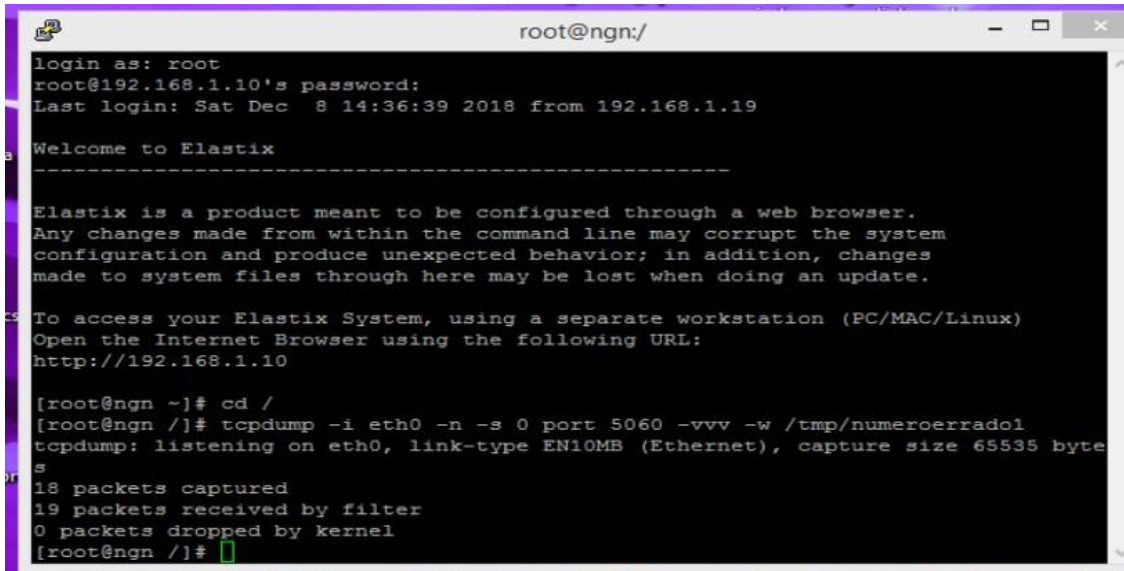


2.2 Realice el respectivo análisis del protocolo SIP

## ANALISIS LLAMADAS

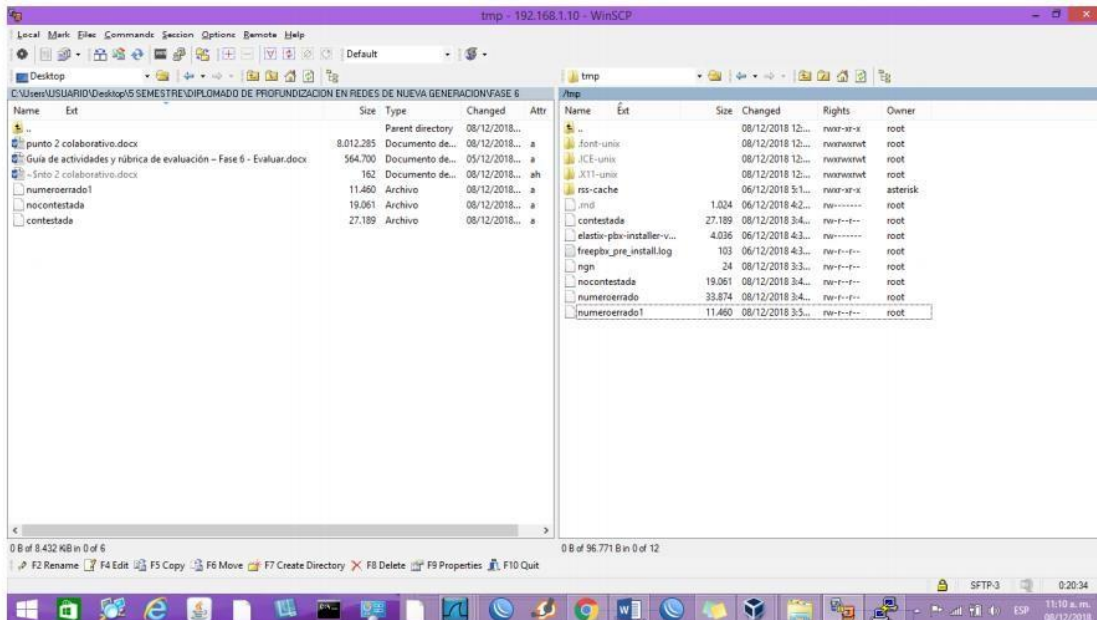
Para correr la captura de paquetes desde el Asterisk utilizo:

```
tcpdump -i eth0 -n -s 0 port 5060 -vvv -w /tmp/(nombre del archivo)
```



```
root@ngn:/  
login as: root  
root@192.168.1.10's password:  
Last login: Sat Dec 8 14:36:39 2018 from 192.168.1.19  
  
Welcome to Elastix  
-----  
  
Elastix is a product meant to be configured through a web browser.  
Any changes made from within the command line may corrupt the system  
configuration and produce unexpected behavior; in addition, changes  
made to system files through here may be lost when doing an update.  
  
To access your Elastix System, using a separate workstation (PC/MAC/Linux)  
Open the Internet Browser using the following URL:  
http://192.168.1.10  
  
[root@ngn ~]# cd /  
[root@ngn /]# tcpdump -i eth0 -n -s 0 port 5060 -vvv -w /tmp/numeroerrado1  
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 byte  
s  
18 packets captured  
19 packets received by filter  
0 packets dropped by kernel  
[root@ngn /]#
```

Luego con el programa winScp comparto la captura realizada desde el Asterisk hacia el escritorio de Windows, en el cual se encuentra el wireshark utilizado para el respectivo análisis



Mediante las opciones telephony – VoIP calls – flow, se puede evidenciar la

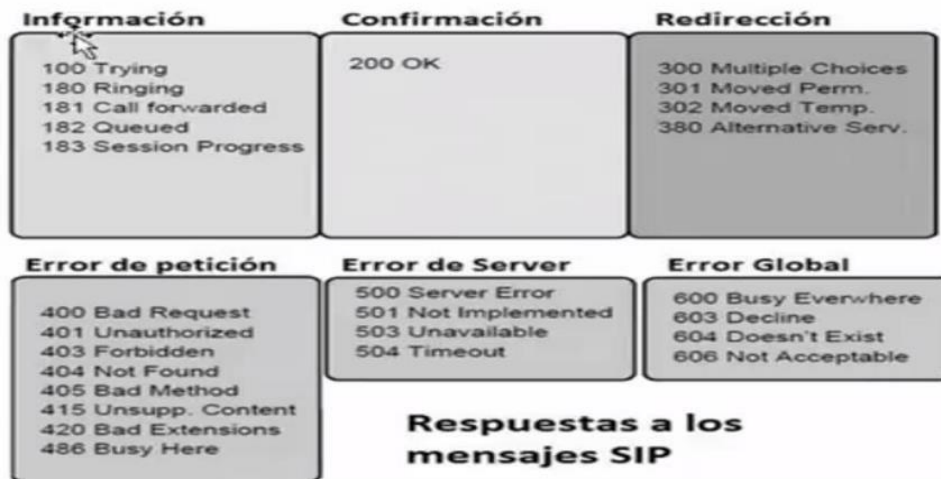
secuencia de la llamada.

Udp es el protocolo por defecto por el cual trabaja la capa de transporte para SIP. Puerto 5060 por defecto para SIP.

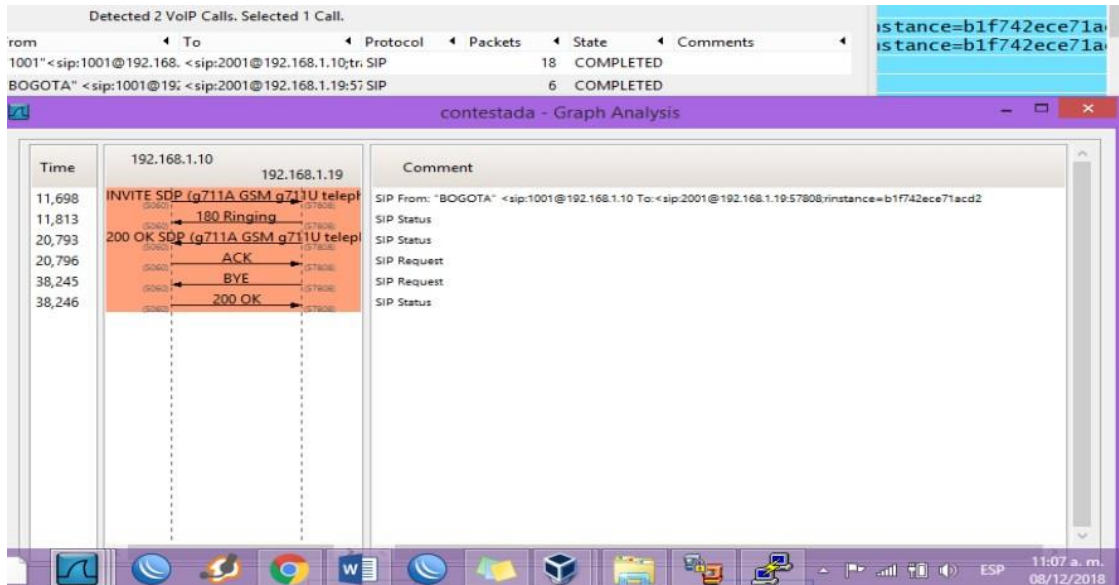
Al momento de establecer la sesión SIP se podrán visualizar una serie de mensajes que nos permiten determinar estado de la sesión, entre los más representativos se pueden encontrar:

- ✓ INVITE – mensaje enviado de una cuenta a otra con la cual se pretende establecer la sesión y a su vez contiene información con la ip origen, destino y tipo de datos.
- ✓ ACK – este mensaje se da para la confirmación del inicio de sesión entre las cuentas SIP que se intentan comunicar.
- ✓ OPTION – este se relaciona con una solicitud de información de una de las cuentas hacia la otra.
- ✓ BYE – este mensaje se envía para dar por terminada la sesión que se encuentra establecida previamente, puede ser utilizado por cualquiera de las cuentas.
- ✓ CANCEL – este permite cancelar una petición que se encuentre en curso.

Por demás se tienen una serie códigos agrupados en bloques así:



Llamada contestada



Se envía el mensaje Invite para el inicio sesión desde la cuenta 1001 con ip 192.168.1.10 a la cuenta SIP 2001 con ip 192.168.1.19, utilizando como puerto de origen 5060 y destino 57808

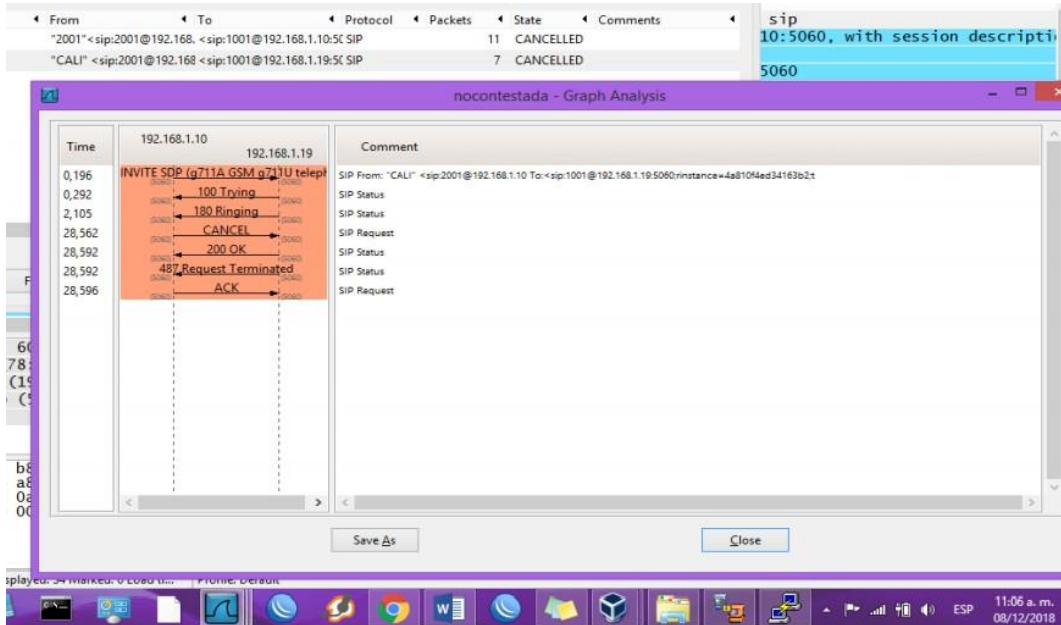
- ✓ La cuenta 2001 le informa a 1001 mediante un mensaje 180 de timbrado que le llego el invite.
- ✓ Desde 2001 se confirma mediante un mensaje 200 que se encuentra listo para el inicio de sesión.
- ✓ Nuevamente desde 1001 con esta información recibida se inicia la sesión

ENTRE las 2 cuentas mediante un ACK.

- ✓ Desde 2001 se finaliza la sesión con un mensaje de BYE, es decir la llamada es colgada desde la cuenta 2001.
- ✓ 1001 confirma el BYE enviado con un mensaje 200, dando por terminada la llamada.

La sesión iniciada se mantendrá por los puertos con que se inició.

Llamada no contestada.

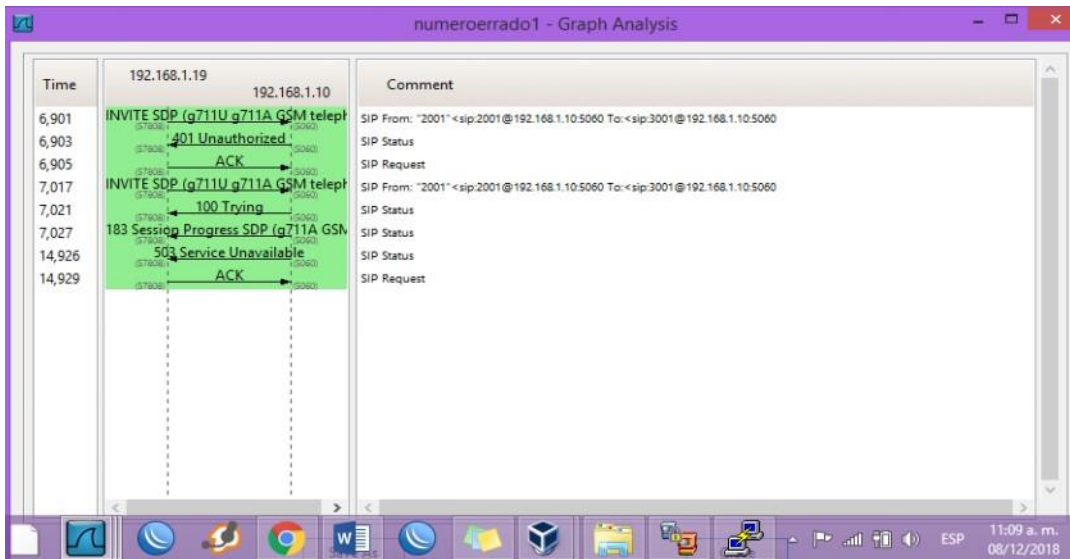


Se envía el mensaje Invite para el inicio sesión desde la cuenta 2001 (Cali) con ip 192.168.1.10 a la cuenta SIP 1001 con ip 192.168.1.19, utilizando como puerto de origen 5060.

- ✓ Se recibe respuesta de información con el código 100 de intentando.
- ✓ Se recibe respuesta de timbrando con el código 180.
- ✓ No se tiene respuesta de confirmación desde la cuenta 1001 (se esperaría un código 200)
- ✓ Por lo anterior se cuelga la llamada con un mensaje de cancelación al no establecerse la sesión.
- ✓ Se recibe mensaje de confirmación de la cancelación mediante mensaje código 200.

Mensaje de error por petición terminada sin lograr establecer la sesión.

Número errado



Se realiza el invite, pero al tener un destino desconocido o no valido se evidencia que el origen y el destino son iguales.

- ✓ Se recibe una respuesta 401 de error no autorizado.
- ✓ Envía nuevamente un ACK esperando ser confirmando el invite
- ✓ Se reenvía el invite con los mismos datos iniciales.
- ✓ Recibe una respuesta de intentado código 100.
- ✓ Igualmente, mensaje de información 183 que la sesión está en progreso, no implica que se encuentre establecida.
- ✓ Por último, recibe la información de que no es posible confirmar el inicio de sesión con un error 503.

3. Un plan de calidad de servicios QoS end-to-end, garantizando el 10% del ancho de banda total para el protocolo HTTP; para Voz RTP 15% del ancho de banda total; para Control de voz y Videoconferencia 20% del ancho de banda total.

Se nos indica que el ancho de banda será de 2Mbps. Entonces se repartirá así:

	<i>HTTP</i>	200 kbps
	<i>Voz RTP</i>	300 kbps
	<i>Voz y Video conferencia</i>	400 kbps

Las siguientes configuraciones se ejecutarán en ambos router.

Primero asignaremos el ancho de banda al protocolo RTP. Crearemos un class-map llamado voz:

```
Router(config)#class-map voz
```

Determinaremos que los paquetes a checar serán del protocolo RTP:

```
Router(config-cmap)#match protocol rtp
```

Ahora configuramos el policy-map de la clase que creamos:

```
Router(config)#policy-map voz  
Router(config-pmap)#class voz
```

Asignamos el ancho de banda de 300 Kbps y verificamos:

```
Router(config-pmap-c)#bandwidth 300  
Router(config-pmap-c)#end  
Router#  
%SYS-5-CONFIG_I: Configured from console by console  
sh run  
Building configuration...
```

Tenemos dos class-map match all, uno para RTP y otro para http. Está configurado el policy-map para voz, pero no para http; lo configuraremos ahora.

```
spanning-tree mode pvst
!  
class-map match-all voz  
  match protocol rtp  
class-map match-all http  
  match protocol http  
!  
policy-map voz  
  class voz  
    bandwidth 300  
!  
!  
!  
!  
!  
interface FastEthernet0/0  
  ip address 192.168.0.1 255.255.255.240  
  duplex auto  
  speed auto
```

Configuración policy-map Http:

```
Router#config  
Configuring from terminal, memory, or network [terminal]?  
Enter configuration commands, one per line.  End with CNTL/Z.  
Router(config)#policy-map http  
Router(config-pmap)#class http  
Router(config-pmap-c)#bandwidth 200  
Router(config-pmap-c)#end  
Router#  
%SYS-5-CONFIG_I: Configured from console by console
```

Verificamos con sh run:




```
!  
spanning-tree mode pvst  
!  
class-map match-all voz  
  match protocol rtp  
class-map match-all http  
  match protocol http  
!  
policy-map voz  
  class voz  
    bandwidth 300  
!  
policy-map http  
  class http  
    bandwidth 200  
!
```

Ahora configuraremos el ancho de banda para video:

```
Router(config)#class-map match-all video  
Router(config-cmap)#policy-map ?  
% Unrecognized command  
Router(config-cmap)#policy-map video-policy  
Router(config-pmap)#class video  
Router(config-pmap-c)#bandwidth 400
```

Verificamos las configuraciones:



The screenshot shows a window titled "Router1" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The configuration shown is as follows:

```
!  
!  
spanning-tree mode pvst  
!  
class-map match-all voz  
  match protocol rtp  
class-map match-all http  
  match protocol http  
class-map match-all video  
!  
policy-map voz  
  class voz  
    bandwidth 300  
!  
policy-map http  
  class http  
    bandwidth 200  
!  
policy-map video-policy  
  class video  
    bandwidth 400  
!  
!  
!  
--More--
```

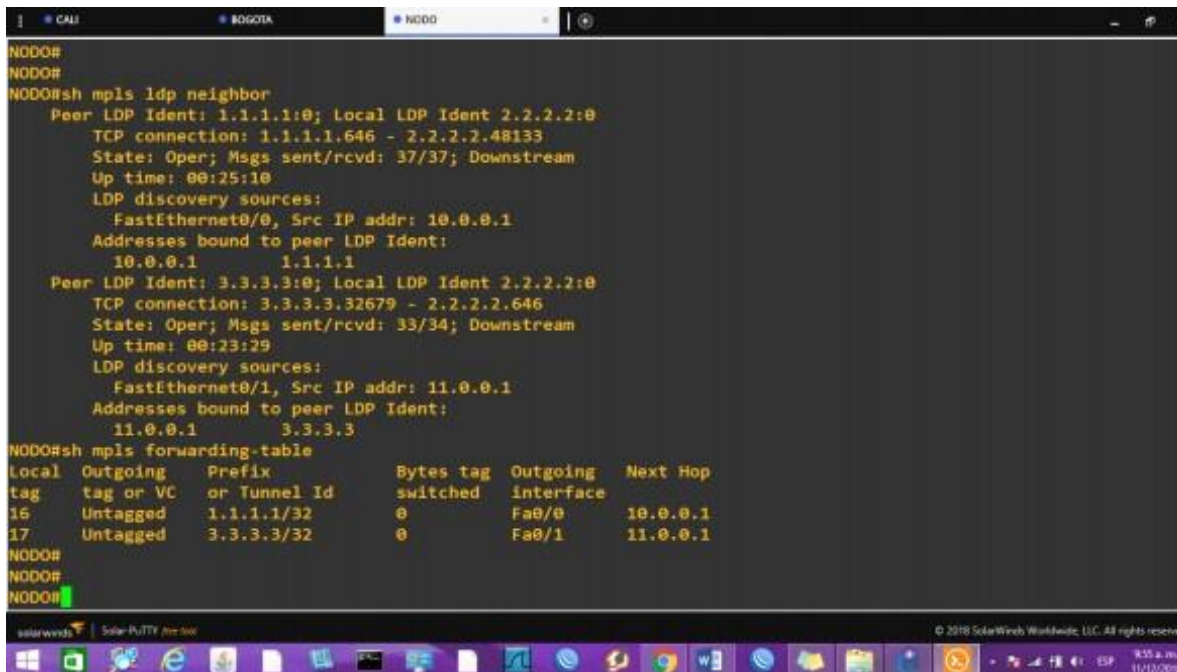


mensajes enviados y recibidos.

sh mpls ldp neighbor

sh mpls forwarding-table

```
NODO#
NODO#
NODO#sh mpls ldp neighbor
  Peer LDP Ident: 1.1.1.1:0; Local LDP Ident 2.2.2.2:0
  TCP connection: 1.1.1.1.646 - 2.2.2.2.48133
  State: Oper; Msgs sent/rcvd: 37/37; Downstream
  Up time: 00:25:10
  LDP discovery sources:
    FastEthernet0/0, Src IP addr: 10.0.0.1
  Addresses bound to peer LDP Ident:
    10.0.0.1      1.1.1.1
  Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 2.2.2.2:0
  TCP connection: 3.3.3.3.32679 - 2.2.2.2.646
  State: Oper; Msgs sent/rcvd: 33/34; Downstream
  Up time: 00:23:29
  LDP discovery sources:
    FastEthernet0/1, Src IP addr: 11.0.0.1
  Addresses bound to peer LDP Ident:
    11.0.0.1      3.3.3.3
NODO#sh mpls forwarding-table
Local  Outgoing  Prefix          Bytes tag  Outgoing     Next Hop
tag    tag or VC  or Tunnel Id    switched  interface
16     Untagged  1.1.1.1/32      0         Fa0/0        10.0.0.1
17     Untagged  3.3.3.3/32      0         Fa0/1        11.0.0.1
NODO#
NODO#
NODO#
```



```
BOGOTA(config-if)#
*Mar 1 00:40:46.251: %LDP-5-NBRCHG: LDP Neighbor 2.2.2.2:0 (1) is UP
BOGOTA(config-if)#^Z
BOGOTA#wr
*Mar 1 00:42:44.543: %SYS-5-CONFIG_I: Configured from console by console
BOGOTA#wr
Building configuration...
[OK]
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#sh mpls ldp neighbor
Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 1.1.1.1:0
TCP connection: 2.2.2.2-48133 - 1.1.1.1-646
State: Oper; Msgs sent/rcvd: 45/45; Downstream
Up time: 00:32:21
LDP discovery sources:
FastEthernet0/0, Src IP addr: 10.0.0.2
Addresses bound to peer LDP Ident:
10.0.0.2 11.0.0.2 2.2.2.2
BOGOTA#sh mpls forwarding-table
Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface interface
16 Untagged 2.2.2.2/32 0 Fa0/0 10.0.0.2
17 17 3.3.3.3/32 0 Fa0/0 10.0.0.2
18 Pop tag 11.0.0.0/24 0 Fa0/0 10.0.0.2
BOGOTA#
```

```
CALI(config-if)#
CALI(config-if)#
CALI(config-if)#
CALI(config-if)#^Z
CALI#wr
Building configuration...
*Mar 1 00:41:05.071: %SYS-5-CONFIG_I: Configured from console by console[OK]
CALI#
CALI#sh mpls ldp neighbor
Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 3.3.3.3:0
TCP connection: 2.2.2.2-646 - 3.3.3.3-32679
State: Oper; Msgs sent/rcvd: 45/44; Downstream
Up time: 00:32:45
LDP discovery sources:
FastEthernet0/0, Src IP addr: 11.0.0.2
Addresses bound to peer LDP Ident:
10.0.0.2 11.0.0.2 2.2.2.2
CALI#sh mpls forwarding-table
Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface interface
16 16 1.1.1.1/32 0 Fa0/0 11.0.0.2
17 Untagged 2.2.2.2/32 0 Fa0/0 11.0.0.2
18 Pop tag 10.0.0.0/24 0 Fa0/0 11.0.0.2
CALI#
CALI#
CALI#
```

## CONCLUSIONES

- Con el apoyo de los diferentes simuladores se pudo simular las llamadas cuando se logra conectar la llamada, cuando no y cuando se marcan los números errados.
- Es importante resaltar que el componente numérico y las formulaciones correctas permiten la configuración de los router y demás equipos necesarios, conociendo cuántas llamadas está en capacidad la red de soportar.
- El desarrollo del presente trabajo nos permite como estudiantes del diplomado acercarnos a situaciones reales que se pueden definir en nuestras vidas y en nuestros trabajos.
- Se logra mediante un análisis detallado de los protocolos como estos pueden ayudar en la implementación, mantenimiento y correctivos que se presentan en una red.

## BIBLIOGRAFÍA

- 3CX. (s.f.). ¿Qué es RTP – Real Time Transport Protocol? Obtenido de <https://www.3cx.es/voip-sip/rtp/>
- Cázarez., E. (18 de marzo de 2017). La importancia de adoptar IPv6. Obtenido de <https://transferencia.tec.mx/2017/03/18/la-importancia-de-adoptar-ipv6/>
- ccm.net/. (17 de enero de 2018). El protocolo HTTP. Obtenido de <https://es.ccm.net/contents/264-el-protocolo-http>
- <http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=27&docID=10609053&tm=1488707071091> MPLS (MultiProtocol Label Switching), tomado el 6 de noviembre del siguiente link: [https://es.wikipedia.org/wiki/Multiprotocol\\_Label\\_Switching](https://es.wikipedia.org/wiki/Multiprotocol_Label_Switching)
- PVX, tomada del siguiente link el 25 de noviembre del siguiente link: <http://elastixtech.com/fundamentos-de-telefonía/pbx-central-telefonica/>
- IPTV tomado del siguiente enlace: CISCO, Cisco end to end Solutions for IPTV [en línea] 2007. [citado en 2013] Disponible en internet: <http://www.cisco.com/en/US/solutions/>
- Protocolo HTTP: <https://developer.mozilla.org/es/docs/Web/HTTP/Overview>
- Protocolo RTP: <https://es.ccm.net/contents/278-protocolos-rtp-rtcp>
- Protocolo MPLS: [https://www.tlm.unavarra.es/~daniel/docencia/rba/rba06\\_07/trabajos/resumes/gr14-MPLSEnLinux.pdf](https://www.tlm.unavarra.es/~daniel/docencia/rba/rba06_07/trabajos/resumes/gr14-MPLSEnLinux.pdf)
- IPV6: tomado el 27 de noviembre del siguiente enlace: <https://prezi.com/xcyghifqhuub/importancia-de-ipv6/>