



**UNIVERSIDAD INDUSTRIAL DE SANTANDER**  
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES  
Perfecta Combinación entre Energía e Intelecto

---

**ADMINISTRACIÓN Y GESTIÓN DE LOS SERVIDORES DEL SISTEMA DE ToIP  
DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER.  
PROCEDIMIENTOS Y DOCUMENTACIÓN.**

**DANIEL ALEJANDRO BERNAL YHAMÁ**

**UNIVERSIDAD INDUSTRIAL DE SANTANDER  
FACULTAD DE INGENIERÍAS FÍSICO-MECÁNICAS  
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE  
TELECOMUNICACIONES  
BUCARAMANGA**

**2010**



**UNIVERSIDAD INDUSTRIAL DE SANTANDER**  
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES  
Perfecta Combinación entre Energía e Intelecto

---

**ADMINISTRACIÓN Y GESTIÓN DE LOS SERVIDORES DEL SISTEMA DE ToIP  
DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER.  
PROCEDIMIENTOS Y DOCUMENTACIÓN.**

**DANIEL ALEJANDRO BERNAL YHAMÁ**

**Proyecto de grado para optar al título de Ingeniero Electrónico.**

**Directora:**

**ANA BEATRIZ RAMÍREZ SILVA, M.SC.**

**Codirectores:**

**BENJAMÍN PICO MERCHÁN, ING.**

**JOSÉ AMAYA PALACIO, M.I.E**

**UNIVERSIDAD INDUSTRIAL DE SANTANDER  
FACULTAD DE INGENIERÍAS FÍSICO-MECÁNICAS  
ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE  
TELECOMUNICACIONES**

**BUCARAMANGA**

**2010**



*A mis padres **Edilberto** y **Carmen Stella** y a mi hermano **Juan Nicolás** por todo su apoyo, amor, esfuerzo y motivación durante toda esta etapa de mi vida.*

*Daniel Bernal*

## **AGRADECIMIENTOS**

A MIE. José Alejandro Amaya Palacio, por la oportunidad y el gran apoyo incondicional brindado que hizo posible el desarrollo de este proyecto.

A Ing. Benjamín Pico Merchán, por su asesoría y dedicación a la hora efectuar las respectivas revisiones de la documentación entregada, así mismo la disposición de resolver dudas y complementar la información existente.

A MsC. Ana Beatriz Ramirez, por su orientación y valiosos consejos durante la revisión de la versión final de este documento.

A Ing. Antonio Marín, por su disposición para la solución de dudas y suministro de información.

A los profesores MsC. Gilberto Arenas, PhD. Sofía Pinzón, PhD. Julio Cesar Carrillo, Msc. Jorge Villamizar Morales, demás profesores y administrativos de la Escuela de Matemáticas, por su confianza, paciencia y apoyo incondicional durante el desarrollo de este proyecto y de toda la carrera.

A Alejandra, mis amigos y mi familia quienes fueron mi soporte durante todo este proceso.

## TABLA DE CONTENIDO

<b>1</b>	<b>INTRODUCCIÓN.....</b>	<b>17</b>
<b>2</b>	<b>MARCO TEÓRICO.....</b>	<b>19</b>
2.1	<i>Red De Área Local (Local Area Network- LAN).....</i>	<i>19</i>
2.1.1	Dispositivos Asociados .....	20
2.1.1.1	Switches o Conmutadores .....	20
2.1.1.1.1	Características de los Switches .....	20
2.1.1.1.2	LAN Virtuales (VLANs) .....	21
2.1.1.2	Routers o Enrutadores .....	21
2.1.1.3	Servidores.....	21
2.2	<i>Telefonía IP (ToIP) y Voz IP (VoIP).....</i>	<i>22</i>
2.2.1	El Estándar VoIP (H323) .....	23
2.2.2	Elementos de Una red VoIP .....	24
2.2.3	QoS - <i>Quality of Service</i> .....	26
2.2.4	PoE – <i>Power Over Ethernet</i> .....	27
<b>3</b>	<b>CONFIGURACIÓN DE LOS SERVIDORES DEL CAMPUS PRINCIPAL DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER. ....</b>	<b>28</b>
3.1	<i>Gabinetes del sistema de Telefonía IP .....</i>	<i>29</i>
3.1.1	Gabinete de VoIP .....	30
3.1.2	Gabinete de Conexiones .....	32

3.2	<i>Configuración de equipos que conforman el gabinete de VoIP</i> .....	34
3.2.1	Configuración Servidores de Voz .....	35
3.2.1.1	Características Técnicas y condiciones ambientales.....	37
3.2.1.2	Procesador .....	37
3.2.1.3	Almacenamiento y memoria RAM.....	38
3.2.1.4	Sistema Operativo.....	39
3.2.1.5	Configuración de Conexiones Servidores S8730.....	39
3.2.1.5.1	Sistema de Redundancia dúplex .....	40
3.2.1.5.2	Configuración de red servidores s8730.....	43
3.2.1.5.3	Enrutamiento de red .....	48
3.2.1.6	Configuración de interconexión con demás servidores que conforman el sistema. 48	
3.2.1.7	Interfaces de configuración de los servidores de voz. ....	50
3.2.1.7.1	Interface Web.....	50
3.2.1.7.2	Interface <i>Communication Manager 5.0</i> .....	51
3.2.1.7.3	Configuración usando protocolo SSH.....	52
3.2.2	Configuración de Gateways .....	53
3.2.2.1	Configuración de componentes que conforman los <i>Gateways</i> .....	55
3.2.2.1.1	Tarjetas <i>IP Server Interface (IPSI) TN2312BP</i> .....	56
3.2.2.1.2	Tarjetas Mepro, C-lan y Val. ....	58
3.2.2.1.3	Otras Tarjetas instaladas.....	62
3.2.2.2	Conexiones de la parte posterior de los <i>Media Gateways G650</i> .....	64

3.2.3	Switch de red.....	66
3.2.4	Configuración Servidor protocolo SIP .....	68
3.2.4.1	Características Técnicas y condiciones ambientales.....	70
3.2.4.2	Configuración de red Servidor S8500 .....	71
3.2.4.3	Sistema Operativo.....	73
3.2.4.4	Interconexión con el Servidor de Voz. ....	74
3.2.5	Descripción Módems .....	76
3.2.6	Descripción del Tarificador Dalí Enterprise.....	76
3.2.6.1	Características Técnicas y condiciones ambientales.....	77
3.2.6.2	Configuración de red Servidor .....	78
3.2.6.3	Interconexión con el Servidor de Voz .....	79
3.2.7	Descripción del servidor que presta el servicio de Intuity Audix.....	81
3.2.7.1	Características Técnicas y condiciones ambientales.....	83
3.2.7.2	Configuración de red Servidor .....	84
3.2.7.3	Interconexión con el Servidor de Voz .....	85
<b>4</b>	<b>EVALUACIÓN, ANÁLISIS DE CONEXIONES Y DE CONFIGURACIÓN .....</b>	<b>87</b>
4.1	<i>Servidores de Voz AVAYA S8730 .....</i>	<i>87</i>
4.2	<i>Media Gateways G650.....</i>	<i>88</i>
4.3	<i>Servidor de protocolo SIP AVAYA S8500 .....</i>	<i>96</i>
4.4	<i>Servidor de Tarificación y Mensajería Unificada.....</i>	<i>96</i>
<b>5</b>	<b>PROPUESTA DE PROCEDIMIENTO PARA LA CONFIGURACIÓN E INSTALACIÓN DE EQUIPOS ACTIVOS ADICIONALES.....</b>	<b>97</b>

<b>5.1</b>	<b><i>Configuración de nuevos switches</i></b> .....	<b>98</b>
5.1.1	<b>Configuración básica</b> .....	98
5.1.1.1	Primeros pasos .....	99
5.1.1.2	Habilitar servicio SSH .....	101
5.1.1.3	Definir contraseña para SSH y Consola .....	101
5.1.1.4	Definir Fecha y hora, nombre del sistema, VLANs y servidor de log .....	102
5.1.1.5	Definir IP de administración a través de interface Ethernet y rutas de red. .....	105
5.1.1.6	Activación de QoS .....	105
5.1.1.7	Configuración de puertos como híbridos.....	107
5.1.1.8	Configuración de puerto para enlace de fibra óptica .....	108
5.1.2	<b>Configuración conexión entre switches de tipo clúster</b> .....	109
5.1.2.1	Procedimiento para configurar los Switches miembros.....	110
5.1.2.2	Procedimiento para configurar el Switch administrador del clúster.....	112
5.2	<b><i>Cambios en la configuración de los servidores para nuevos switches</i></b> .....	<b>115</b>
<b>6</b>	<b>CONCLUSIONES Y RECOMENDACIONES</b> .....	<b>116</b>
<b>7</b>	<b>RECOMENDACIONES TECNICAS</b> .....	<b>117</b>
<b>8</b>	<b>BIBLIOGRAFÍA</b> .....	<b>118</b>

## LISTA DE TABLAS

Tabla 3.1 Lista de componentes que conforman el Gabinete de telefonía IP.....	31
Tabla 3.2 Descripción física servidores AVAYA S8730 .....	36
Tabla 3.3 Rangos de operación y características técnicas básicas. ....	37
Tabla 3.4 Sistema de particionado de discos .....	38
Tabla 3.5 Conexiones de red asociadas a la duplicación por medio de red UTP. .	41
Tabla 3.6 Estado tarjeta DAL-2 terminal SSH servidor primario .....	42
Tabla 3.7 Estado tarjeta DAL-2 terminal SSH servidor secundario.....	43
Tabla 3.8 Configuración de red Servidores S8730 .....	44
Tabla 3.9 Puertos abiertos del servidor activo usando escaneo de puertos desde otro servidor. ....	47
Tabla 3.10 Tabla de enrutamiento de red .....	48
Tabla 3.11 Descripción física <i>Media Gateway G650</i> . ....	55
Tabla 3.12 Componentes principales del Media Gateway G650 .....	56
Tabla 3.13 Componentes adicionales Media Gateway G650 .....	56
Tabla 3.14 direcciones IP tarjetas IPSI conectadas a la CNA (Control Netwok A)	57
Tabla 3.15 Direcciones IP red corporativa UIS tarjetas C-LAN, MEDPRO y VAL..	60
Tabla 3.16 Puertos abiertos Tarjetas CLAN .....	61
Tabla 3.17 Puertos abiertos Tarjeta VAL .....	62
Tabla 3.18 Puertos de Instalación de DS1 TN2464CP .....	63
Tabla 3.19 Puertos de Instalación de TN293CP .....	64
Tabla 3.20 Puertos de Instalación de TN771DP .....	64
Tabla 3.21 Puertos de Instalación de TN747B .....	64

Tabla 3.22 Descripción física Switch 3COM 4500G 48 puertos .....	68
Tabla 3.23 Rangos de operación y características técnicas básicas. ....	70
Tabla 3.24 Servidor SIP S8500.....	71
Tabla 3.25 Configuración de red servidor S8500.....	73
Tabla 3.26 Puertos abiertos del Servidor SIP usando escaneo de puertos desde otro servidor.....	73
Tabla 3.27 Rangos de operación y características técnicas básicas. ....	78
Tabla 3.28 Interfaz de red servidor Tarificador Dalí Enterprise.....	78
Tabla 3.29 Puertos abiertos de red del servidor Dalí Enterprise.....	79
Tabla 3.30 Rangos de operación y características técnicas básicas. ....	84
Tabla 3.31 Características físicas servidor S3210R .....	84
Tabla 3.32 Configuración de red servidor S3210.....	84
Tabla 3.33 Puertos abiertos del servidor usando escaneo de puertos desde otro servidor.....	85
Tabla 4.1 Configuración de interfaces de red Servidores S8730 con esquema de duplicación de alta disponibilidad propuesta.....	91
Tabla 4.2 Direcciones IP red corporativa UIS tarjetas C-LAN, MEDPRO y VAL con sistema de alta confiabilidad.....	92
Tabla 5.1 VLANs de Voz configuradas en campus de la Universidad. ....	103

## LISTA DE FIGURAS

Figura 2.1 Elementos de una red VoIP .....	25
Figura 3.1 Foto del Gabinete de servidores de VoIP de la Universidad Industrial de Santander .....	31
Figura 3.2 Rack de cableado .....	33
Figura 3.3 Diagrama de conexiones de servidores y equipos anexos al sistema de telefonía IP.....	35
Figura 3.4 Foto servidores S8730 Campus UIS.....	36
Figura 3.5 Diagrama de conexiones de red .....	40
Figura 3.6 Diagrama configuración de interfaces de red servidores S8730.....	45
Figura 3.7 resultado del comando <code>list node-names</code> usando <i>Communication Manager</i> en el Servidor de Voz.....	49
Figura 3.8 Vista de sistema de configuración Web. ....	51
Figura 3.9 Vista del sistema de configuración usando CM 5.0. ....	52
Figura 3.10 Vista del sistema de consola usando Putty a través del protocolo SSH. ....	53
Figura 3.11 Comando <code>list cabinet</code> en CM 5 .....	54
Figura 3.12 <i>Media Gateway G650</i> .....	55
Figura 3.13 Tarjeta IPSI instalada en <i>MediaGatewayG650</i> . ....	57
Figura 3.14 <code>list ipserver-interface</code> en <i>Communication Manager</i> .....	58
Figura 3.15 Comando <code>ip-inferface all</code> .....	59
Figura 3.16 Foto de conexiones posteriores de los <i>Media Gateways G650</i> . ....	65
Figura 3.17 Foto Swich 3COM 4500G 24 puertos instalado actualmente. ....	66

Figura 3.18 Diagrama de puertos utilizados en el Switch 3COM 4500G. ....67

Figura 3.19 Puertos asignados a las VLAN 14 y 114.....68

Figura 3.20 Foto Servidor SIP AVAYA S8500 .....69

Figura 3.21 Diagrama de Interfaces de red Servidor SIP AVAYA S8500 .....72

Figura 3.22 Configuración Web en Servidor SIP para lograr interconexión con Servidor de Voz. ....75

Figura 3.23 Foto Dos Módems Externos USB *Multitech*.....76

Figura 3.24 Foto Servidor *Dalí Enterprise* HP DL380 G5 Series. ....77

Figura 3.25 Comando `change system-parameters cdr` en CM 5.0 .....80

Figura 3.26 Comando `chane ip-services` en CM 5.0 .....81

Figura 3.27 Foto Servidor S3210R que presta el servicio de Intuity AUDIX. ....82

Figura 3.28 Comando `display node-names audix`.....85

Figura 3.29 Configuración `hunt-group 1` .....86

Figura 4.1 Propuesta de interconexión de servidores del sistema de ToIP para el campus UIS. ....89

Figura 4.2 Configuración de Identidad AVAYA S8730.....93

Figura 4.3 Configuración de Interfaces de red AVAYA S8730.....94

Figura 5.1 Diagrama de conexión usando el puerto de consola. ....100

Figura 5.2 Configuración de puerto Rs232 en Hyperterminal. ....101

Figura 5.3 Configuración de Switches en Clúster un administrador y dos miembros. ....110

## RESUMEN

**TITULO:** ADMINISTRACIÓN Y GESTIÓN DE LOS SERVIDORES DEL SISTEMA DE ToIP DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER. PROCEDIMIENTOS Y DOCUMENTACIÓN\*.

**AUTOR:** BERNAL YHAMÁ, Daniel Alejandro\*\*.

**Palabras clave:** Avaya, ToIP, VoIP, Red de voz, Servidores, LAN UIS.

### Resumen

En este trabajo se documentan los principales parámetros de configuración de los servidores involucrados en los servicios de ToIP, de una forma clara y detallada. Mostrando al lector un panorama que le permita entender el funcionamiento del sistema y la función que cada equipo cumple dentro del sistema de ToIP, con el objetivo principal de permitir su administración, pues uno de los principales requisitos para tomar el control completo de un sistema es conocerlo de la mejor forma. Con lo cual hasta el momento la Universidad Industrial de Santander no contaba.

Este informe se encuentra dividido en tres grandes capítulos con el objetivo de cumplir con los objetivos establecidos al inicio de este proyecto. En el primero (Cap. 3) se realiza la descripción de hardware y software del sistema orientado a los equipos que administran el sistema de VoIP con la finalidad de instruir al lector sobre los parámetros de configuración del sistema instalado y buscando mostrar un panorama del sistema de interconexión existente entre los equipos que conforman el sistema de VoIP.

En la segunda parte (Cap. 4) con base en la documentación recopilada y la investigación realizada sobre el sistema, se realiza un análisis de las conexiones del sistema y se proponen procedimientos y algunas modificaciones a la instalación que podrían mejorar la estabilidad y las prestaciones.

En la tercera parte (Cap. 5) se documentan y explican los procedimientos realizados para instalar nuevos equipos al sistema de VoIP orientado a Switches con base en la retroalimentación de la DSI (División de Servicios de Información), y finalmente se ofrecen recomendaciones (Cap. 6 y 7) con base en el estudio realizado durante este trabajo el cual se espera cumpla con sus expectativas.

---

\* Proyecto de grado.

\*\* Facultad de Ingenierías Físico-Mecánicas, Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones. Directora Ana Beatriz Ramírez. Coodirectores MPE José Amaya Palacio, Ing. Benjamín Pico Merchán.

## **ABSTRACT**

**TITLE:** ADMINISTRATION AND MANAGEMENT ToIP SYSTEM OF UNIVERSIDAD INDUSTRIAL DE SANTANDER. PROCEDURES AND DOCUMENTATION.\*

**AUTHOR:** BERNAL YHAMÁ, Daniel Alejandro.\*\*

**KEYWORDS:** Avaya, ToIP, VoIP, Network, Servers, LAN UIS.

### **Abstract**

This paper documents the main settings of the servers involved in ToIP services, in a clear and detailed way. Showing the reader an overview that allows you to understand the functioning of the system and the role that each device meets in ToIP system, with the main objective of allowing his administration, as one of the main requirements to take complete control of a system is know the best way. Thus far the Universidad Industrial de Santander did not count.

This report is divided into three main chapters in order to meet the objectives set at the beginning of this project. In the first (Chapter. 3) the author describe the system hardware and software devices designed to manage the VoIP system in order to educate the reader about the settings of the installed system and trying to show an overview of the system interconnection between the servers that make up the VoIP system.

In the second part (Chapter 4) based on the documentation collected and research conducted on the system, an analysis of the connections of the system and procedures are proposed and some modifications to the facility that could improve the stability and performance .

In the third part (Chapter 5) are documented and explained the procedures performed to install new equipment to the VoIP system aimed at Switches based on feedback from the DSI (Information Services Division), and finally offer recommendations (Chapter 6 and 7) based in the study during this work which is expected to meet its expectations.

---

\* Graduate Thesis Project

\*\* Physics Mechanical Engineering Faculty. Electric, Electronic and Telecommunications School. Director Msc. Ana Beatriz Ramirez. Co-directors. MPE Jose Alejandro Amaya Palacio, Ing. Benjamin Pico Merchan.

## 1 INTRODUCCIÓN

Desde la invención del teléfono por Alexander Graham Bell a finales del siglo XIX, los sistemas de telefonía no han cambiado substancialmente. Hay que reconocer que la telefonía móvil ha causado una revolución, sin embargo, para empresas y oficinas la telefonía tradicional sigue en operación.

Diversas mejoras se han desarrollado como la marcación por tonos DTMF (*Dual-tone multi-frequency signaling*) y la identificación de llamadas. Aún así la funcionalidad básica es la misma.

A finales de los noventa investigadores, tanto orientados a fines educativos como a soluciones comerciales, se interesaron seriamente en transportar voz y video a través de redes públicas y privadas operando en el protocolo IP (*Internet Protocol*). La tecnología que se desarrolló es lo que ahora se conoce como Telefonía IP y es, en términos sencillos, el proceso de fragmentar el audio y el video en paquetes<sup>1</sup> pequeños, transmitirlos por la red en cuestión y desfragmentarlos durante la recepción de tal manera que dos personas puedan comunicarse.

Actualmente la ToIP (*Telephony over IP*) ha logrado un gran auge debido al incremento del ancho de banda mundial, la optimización de los equipos de red para el soporte de nuevas tecnologías y el desarrollo de software más robusto, lo que la permitido un crecimiento en la implementación de este nuevo sistema en reemplazo de las plantas telefonicas analogicas.

---

<sup>1</sup> Un paquete de datos es una unidad fundamental de transporte de información y está generalmente compuesto de tres elementos: una cabecera, el área de datos, y la cola.

Ante esto la Universidad Industrial de Santander en su preocupación de mantenerse acorde con crecimiento tecnológico mundial realiza la migración a este nuevo sistema de telefonía buscando la convergencia de la red e integrar todas las sedes regionales con el fin de eliminar los problemas existentes hasta entonces de comunicación, reducir los costos de servicio a nivel global, así como también ampliar la capacidad, cobertura y gama de servicios ofrecidos teniendo en cuenta el gran crecimiento de la universidad en los últimos años.

Luego de instalado el sistema, es de gran importancia para la Universidad Industrial de Santander que se cuente con información y documentación concreta de la configuración (hardware y Software) de los servidores instalados orientado a VoIP, con el fin de una futura ampliación de la cobertura del servicio de telefonía, o la reconfiguración de algún equipo por pérdida de su configuración (daño, robo, etc.), o la necesidad futura de integración de nuevos servicios por ser esta una solución con gran posibilidad de escalabilidad e integración.

Por lo cual en este documento luego de un proceso arduo de investigación y documentación se explica de forma instructiva el funcionamiento y sistema de conexiones orientado a servidores del sistema de VoIP con objeto de dar a conocer un panorama detallado del sistema instalado en la Universidad para permitir su futura administración y control.

Este informe se encuentra dividido en tres grandes capítulos con el objetivo de cumplir con los objetivos establecidos al inicio de este proyecto. En el primero (Cap. 3) se realiza la descripción de hardware y software del sistema orientado a los equipos que administran el sistema de VoIP con la finalidad de instruir al lector sobre los parámetros de configuración del sistema instalado y buscando mostrar un panorama del sistema de interconexión existente entre los equipos que conforman el sistema de VoIP.

En la segunda parte (Cap. 4) con base en la documentación recopilada y la investigación realizada sobre el sistema, se realiza un análisis de las conexiones del sistema y se proponen procedimientos y algunas modificaciones a la instalación que podrían mejorar la estabilidad y las prestaciones.

En la tercera parte (Cap. 5) se documentan y explican los procedimientos realizados para instalar nuevos equipos al sistema de VoIP orientado a Switches con base en la retroalimentación de la DSI, y finalmente se ofrecen recomendaciones (Cap. 6 y 7) con base en el estudio realizado durante este trabajo que se espera cumpla con sus expectativas.

## 2 MARCO TEÓRICO

Con el fin de realizar un análisis y estudio estructurado y concreto conceptualmente se requiere una base teórica, que argumente los objetivos del proyecto y explique los diversos protocolos, estándares y tecnologías estudiadas durante el desarrollo de la práctica empresarial orientada al campo de configuración y administración de redes y servidores.

### 2.1 Red De Área Local (*Local Area Network- LAN*)

Una red de área local se puede definir como un tipo de red privada que permite la interconexión entre un conjunto de terminales o equipos informáticos, por lo general computadores personales, para transmitir datos a gran velocidad en un entorno geográfico restringido [1].

Las propiedades básicas que caracterizan una red de área local son las siguientes:

- Permite la interconexión de dispositivos heterogéneos.
- Contribuye al incremento de la velocidad de transferencia de datos.

- Su empleo está restringido a zonas geográficas poco extensas, tales como campus universitarios departamentos de empresas etc.
- Se caracteriza por su facilidad de instalación y flexibilidad de reubicación de equipos y terminales.

Existen varias tecnologías de capa de enlace de datos disponibles para redes LAN. Entre estas se encuentran Ethernet, *Token Ring*, *Token Bus*, *FDDI (Fiber Distributed Data Interface)* principalmente.

Entre estas Ethernet es la que ha logrado posicionarse como la solución de redes de área local más utilizada, y la solución utilizada por la Universidad.

### **2.1.1 Dispositivos Asociados**

Las redes LAN combinan diferentes tipos de dispositivos entre los que se encuentran *Hubs*, *Bridges* (puentes), *Switches* y enrutadores. Algunos de ellos como los *Switches* y los enrutadores permiten ser administrados de forma compleja para que tomen decisiones con los paquetes de datos que circulan a través de ellos.

#### **2.1.1.1 Switches o Conmutadores**

Los *Switches* son dispositivos de alta capacidad. A diferencia de lo *Hubs* en ellos no se debe competir por el acceso al medio, cada puerto tiene asignados sus propios recursos independientemente del número de estaciones conectadas o el tráfico generado por ellas.

Son dispositivos que permiten enlazar segmentos Ethernet.

##### **2.1.1.1.1 Características de los Switches**

Los *switches* pueden tener un software de administración que permite recolectar y visualizar estadísticas de la red, además permite configurar diversas opciones como es el habilitar el uso de ciertos protocolos con el fin de optimizar su funcionamiento de acuerdo al propósito en la red y a los servicios que este ofrece.

### **2.1.1.1.2 LAN Virtuales (VLANs)**

La configuración de VLANs es una característica adicional que pueden ofrecer ciertas gamas de switches, para agrupar el flujo de tráfico dentro de estos.

En términos generales las VLANs tiene una característica bastante importante y es que permite la interconexión de terminales ubicadas en distintos segmentos de red físicos como si se encontraran dentro de la misma LAN.

Una VLAN consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo conmutador, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina [2].

### **2.1.1.2 Routers o Enrutadores**

El enrutador es el componente de hardware básico para interconectar redes heterogéneas.

Un enrutador puede interconectar LANs una LAN con un ISP<sup>1</sup> etc. Además cuando un enrutador interconecta dos redes de la misma categoría, estas no necesariamente deben usar la misma tecnología. [2]

### **2.1.1.3 Servidores**

El Servidor es un computador o dispositivo que se encarga de la administración de los recursos de la red. También se puede denominar como una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de

---

1 ISP: Internet Service provider.

archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final. Este es el significado original del término. Es posible que un ordenador cumpla simultáneamente las funciones de cliente y de servidor. [3]

## 2.2 Telefonía IP (ToIP) y Voz IP (VoIP)

Voz sobre Protocolo de Internet, también llamado Voz sobre IP, VoIP, VoIP (por sus siglas en inglés), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP. Esto significa que se envía la señal de voz en forma digital en paquetes en lugar de enviarla (en forma digital o analógica) a través de circuitos utilizables sólo para telefonía como una compañía telefónica convencional o PSTN (acrónimo de Public Switched Telephone Network, Red Telefónica Pública Conmutada).

Los Protocolos que son usados para llevar las señales de voz sobre la red IP son comúnmente referidos como protocolos de Voz sobre IP o protocolos IP. Pueden ser vistos como implementaciones comerciales de la "Red experimental de Protocolo de Voz" (1973), desarrollada por ARPANET.

El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo redes de área local (LAN).

Es muy importante diferenciar entre Voz sobre IP (VoIP) y Telefonía sobre IP.

- VoIP es el conjunto de normas, dispositivos, protocolos, en definitiva la tecnología que permite la transmisión de la voz sobre el protocolo IP.
- Telefonía sobre IP es el conjunto de nuevas funcionalidades de la telefonía, es decir, en lo que se convierte la telefonía tradicional debido a los servicios que finalmente se pueden llegar a ofrecer gracias a poder portar la voz sobre el protocolo IP en redes de datos. [2]

### 2.2.1 El Estándar VoIP (H323)

Definido en 1996 por la UIT (Unión Internacional de Telecomunicaciones) proporciona a los diversos fabricantes una serie de normas con el fin de que puedan evolucionar en conjunto.

El VoIP/H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación: [4]

#### **Direccionamiento:**

RAS (*Registration, Admission and Status*). Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través de el Gatekeeper.

DNS (*Domain Name Service*). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS

#### **Señalización:**

Q.931 Señalización inicial de llamada

H.225 Control de llamada: señalización, registro y admisión, y paquetización / sincronización del *stream* (flujo) de voz

H.245 Protocolo de control para especificar mensajes de apertura y cierre de canales para *streams* de voz.

#### **Compresión de Voz:**

Requeridos: G.711 y G.723

Opcionales: G.728, G.729 y G.722

#### **Transmisión de Voz:**

UDP<sup>1</sup>. La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.

RTP (*Real Time Protocol*). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

#### **Control de la Transmisión:**

RTCP (*Real Time Control Protocol*). Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

### **2.2.2 Elementos de Una red VoIP**

Actualmente se puede partir de una serie de elementos ya disponibles en el mercado y que, según diferentes diseños, permiten construir las aplicaciones VoIP. Estos elementos son:

- Teléfonos IP.
- Adaptadores para PC.
- Hubs Telefónicos.
- Gateways (pasarelas RTC / IP).
- Gatekeeper.
- Unidades de audio conferencia múltiple. (MCU Voz)
- Servicios de Directorio.

---

<sup>1</sup> *User Datagram Protocol (UDP)* es un protocolo del nivel de transporte basado en el intercambio de datagramas.

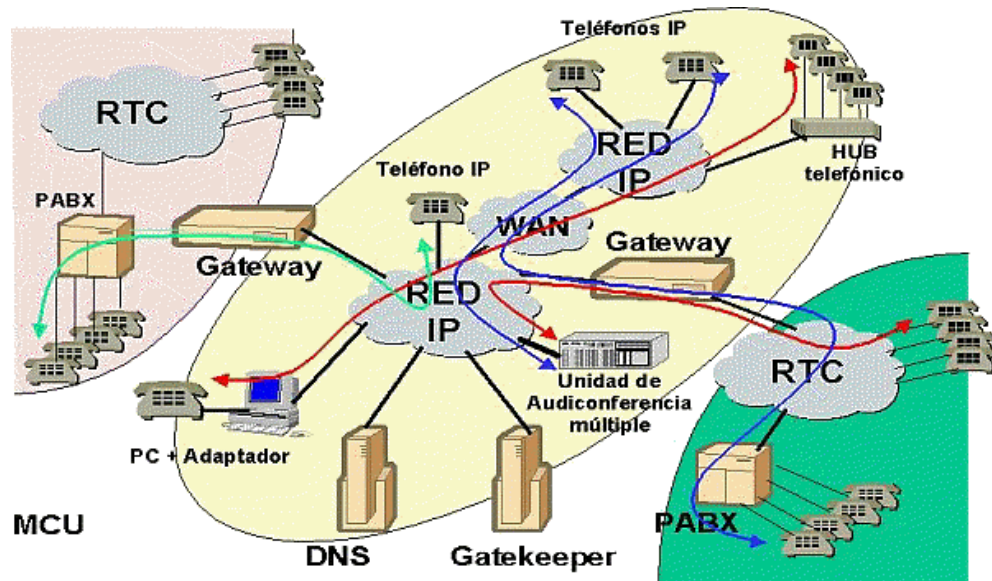


Figura 2.1 Elementos de una red VoIP<sup>1</sup>

Las funciones de los distintos elementos son fácilmente entendibles a la vista de la Figura 2.1, si bien merece la pena recalcar algunas ideas.

El Gatekeeper<sup>2</sup> es un elemento opcional en la red, pero cuando está presente, todos los demás elementos que contacten dicha red deben hacer uso de aquel. Su función es la de gestión y control de los recursos de la red, de manera que no se produzcan situaciones de saturación de la misma.

El Gateway es un elemento esencial en la mayoría de las redes pues su misión es la de enlazar la red VoIP con la red telefónica analógica o RDSI. Se puede considerar al Gateway como una caja que por un lado tiene un interface LAN y por el otro dispone de varias interfaces de conexión analógicas.

<sup>1</sup> Figura tomada de Gonzales, Gustavo, Vásquez, Javier, "Sistema de Contact Center Basado en Telefonía IP". Tesis de Especialización en Telecomunicaciones. UIS, E3T, 2001.

<sup>2</sup> El gatekeeper es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323 y Gateways.

Los distintos elementos pueden residir en plataformas físicas separada, o es posible encontrarse con varios elementos conviviendo en la misma plataforma. De este modo es bastante habitual encontrar juntos Gatekeeper y Gateway. También hay que tener presente que se ha implementado las funciones de Gateway en el router en los dispositivos actuales.

Un aspecto importante a reseñar es el de los retardos en la transmisión de la voz. Hay que tener en cuenta que la voz no es muy tolerante con estos. De hecho, si el retardo introducido por la red es de más de 150 milisegundos, resulta casi imposible tener una conversación fluida. Debido a que las redes de área local no están preparadas en principio para este tipo de tráfico, el problema puede parecer grave. Hay que tener en cuenta que los paquetes IP son de longitud variable y el tráfico de datos suele ser a ráfagas. Para intentar obviar situaciones en las que la voz se pierde porque tenemos una ráfaga de datos en la red, se ha ideado el protocolo RSVP (*Protocolo de Reserva de Recursos*), cuya principal función es trocear los paquetes de datos grandes y dar prioridad a los paquetes de voz cuando hay una congestión en un *router*. Si bien este protocolo ayudará considerablemente al tráfico multimedia por la red, hay que tener en cuenta que RSVP no garantiza una calidad de servicio como ocurre en redes avanzadas tales como ATM (*Asynchronous Transfer Mode*) que proporcionan QoS de forma estándar.

### **2.2.3 QoS - *Quality of Service***

Se refiere a las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (*throughput*). Calidad de servicio es la capacidad de dar un buen servicio bajo los siguientes criterios:

- La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda al transmitir menos información.
- Compresión de cabeceras aplicando los estándares RTP/RTCP.

- Priorización de los paquetes que requieran menor latencia. Las tendencias actuales son:
  - CQ (*Custom Queuing*) (Sánchez J.M., VoIP'99): Asigna un porcentaje del ancho de banda disponible.
  - PQ (*Priority Queuing*) (Sánchez J.M., VoIP'99): Establece prioridad en las colas.
  - WFQ (*Weight Fair Queuing*) (Sánchez J.M., VoIP'99): Se asigna la prioridad al tráfico de menos carga.
- *DiffServ*: Evita tablas de encaminados intermedios y establece decisiones de rutas por paquete.
- La implantación de IPv6 que proporciona mayor espacio de direccionamiento y la posibilidad de *tunneling*.

#### 2.2.4 PoE – *Power Over Ethernet*

Es una tecnología que permite la alimentación eléctrica de dispositivos de red a través de un cable UTP / STP en una red Ethernet. PoE se rige según el estándar IEEE 802.3af y abre grandes posibilidades a la hora de dar alimentación a dispositivos tales como cámaras de seguridad, teléfonos o puntos de acceso inalámbricos.

Actualmente existen en el mercado varios dispositivos de red como switches o hubs que soportan esta tecnología. Para implementar PoE en una red que no se dispone de dispositivos que la soporten directamente se usa una unidad base (con conectores RJ45 de entrada y de salida) con un adaptador de alimentación para recoger la electricidad y una unidad terminal (también con conectores RJ45) con un cable de alimentación para que el dispositivo final obtenga la energía necesaria para su funcionamiento. [2]

### **3 CONFIGURACIÓN DE LOS SERVIDORES DEL CAMPUS PRINCIPAL DE LA UNIVERSIDAD INDUSTRIAL DE SANTANDER.**

En el presente capítulo se presenta la descripción de la configuración actual del sistema y sus respectivas funciones orientado a los servidores y equipos encargados de prestar el servicio de ToIP teniendo en cuenta que el proyecto tiene como objetivo fundamental documentar el proceso de configuración y administración de los servidores que soportan este servicio.

Debido a la cantidad de documentación existente sobre procedimientos de configuración [5] [6] [7], el proyecto de grado [8] desarrollado alrededor de estos temas y buscando aportar la mayor cantidad de información útil a la Universidad. Este capítulo busca explicar detalladamente los principales parámetros de instalación de los servidores y mostrar información que quizás no se encuentra plasmada de forma detallada en la documentación existente y que se considera es de gran relevancia a la hora de asumir la administración de un sistema de esta magnitud.

El desarrollo del capítulo se inicia realizando una descripción del lugar donde se encuentran los servidores y equipos del sistema destacando las características ambientales y de seguridad.

Luego se realiza una descripción básica de los diferentes gabinetes que se encuentran en este lugar destinados albergar al sistema de ToIP y finalmente se presenta una descripción detallada de la configuración de los equipos orientados a servicios de ToIP intentando explicar su función e importancia dentro del sistema, con el objeto de dar al lector un panorama claro de la configuración de estos equipos como complemento a la documentación existente y provista por el fabricante.

Hay que aclarar que en este trabajo se presentan los parámetros de configuración principales como son características de hardware y configuración de conexiones actuales, realizando especial énfasis en los servidores de voz y *Gateways* que son

los principales implicados en la prestación de los servicios de ToIP al campus principal de la Universidad. Se abordará en menor detalle la configuración usando la plataforma CM (*Communication Manager*) debido a que esta información ya fue documentada en otro proyecto de grado [8] y existen extensos manuales de procedimiento muy claros acerca de esta temática<sup>1</sup>.

### 3.1 Gabinetes del sistema de Telefonía IP

En esta sección se describen las condiciones ambientales y de seguridad del lugar en donde se encuentran los equipos que conforman el núcleo del sistema de ToIP. Hay que tener presente que toda la infraestructura descrita en este capítulo está instalada en el edificio llamado CENTIC (Centro de tecnologías de la información) de la Universidad Industrial de Santander en una sala diseñada para mantener dichos equipos en condiciones tanto ambientales como de seguridad ideales, con la finalidad de garantizar operatividad del sistema.

La sala cuenta entre otras con las siguientes condiciones:

- Protección contra incendios.
- Control ambiental, tanto de temperatura como de humedad, la temperatura se mantiene constante en un rango de 16 a 18 grados centígrados usando un aire acondicionado de precisión marca DATA AIRE.
- Ventilación tanto vertical como horizontal lo cual garantiza una temperatura homogénea en toda la sala de servidores.
- Seguridad y acceso controlado con registro.
- Cámaras de seguridad.

---

<sup>1</sup> Ver Bibliografía.

- Los cables se encuentran perfectamente identificados, y se encuentran cableados por piso falso.
- La sala se encuentra alimentada por UPS de tipo Online y planta eléctrica de contingencia lo cual garantiza un suministro eléctrico estable y sin interrupciones.

La Universidad Industrial de Santander cuenta con dos gabinetes de 52U<sup>1</sup> de altura en donde están instalados y organizados todos los equipos; en el primero llamado gabinete de VoIP se encuentran todos los servidores y equipos de red que conforman el núcleo del sistema, y el segundo llamado Gabinete de conexiones se encuentra todo el cableado del sistema.

### 3.1.1 Gabinete de VoIP

Como se observa en la Figura 3.1, dentro del primer gabinete la solución de comunicaciones consta de los siguientes componentes los cuales serán descritos detalladamente más adelante:

Item	Referencia	Descripción
Modem	MultiTech MultiModemUSB	Modem de administración remota Servidor S8730-2
Modem	MultiTech MultiModemUSB	Modem de administración remota Servidor S8730-1
Modem	MultiTech MultiModemUSB	Modem de administración remota Servidor SIP
Servidor	S8730	Servidor de Voz principal primario
Servidor	S8730	Servidor de Voz Principal Secundario
Switch	3COM 4500G 48 Puertos	Switch de red
Servidor	AVAYA S8500/dell 1950	Servidor de protocolo SIP
Servidor	AVAYA S3210	Servidor de Mensajería Intuity Audix
Servidor	HP DL380 G5	Servidor Tarifador E-Dalí
Media Gateway	G650	Media Gateway 1
Media Gateway	G650	Media Gateway 2
Media Gateway	G650	Media Gateway 3
Lector SD	SD card 128MB	Memoria SD para S8730

<sup>1</sup> Se refiere a distancia entre cada guía horizontal o "estante" de un rack. Todos los equipos deben adaptar su altura a un múltiplo de dicha unidad. 1U equivale a 4,5 cm.

Lector SD	SD card 128MB	Memoria SD para S8730
Lector SD	SD card 128MB	Memoria SD para S8500

Tabla 3.1 Lista de componentes que conforman el Gabinete de telefonía IP.

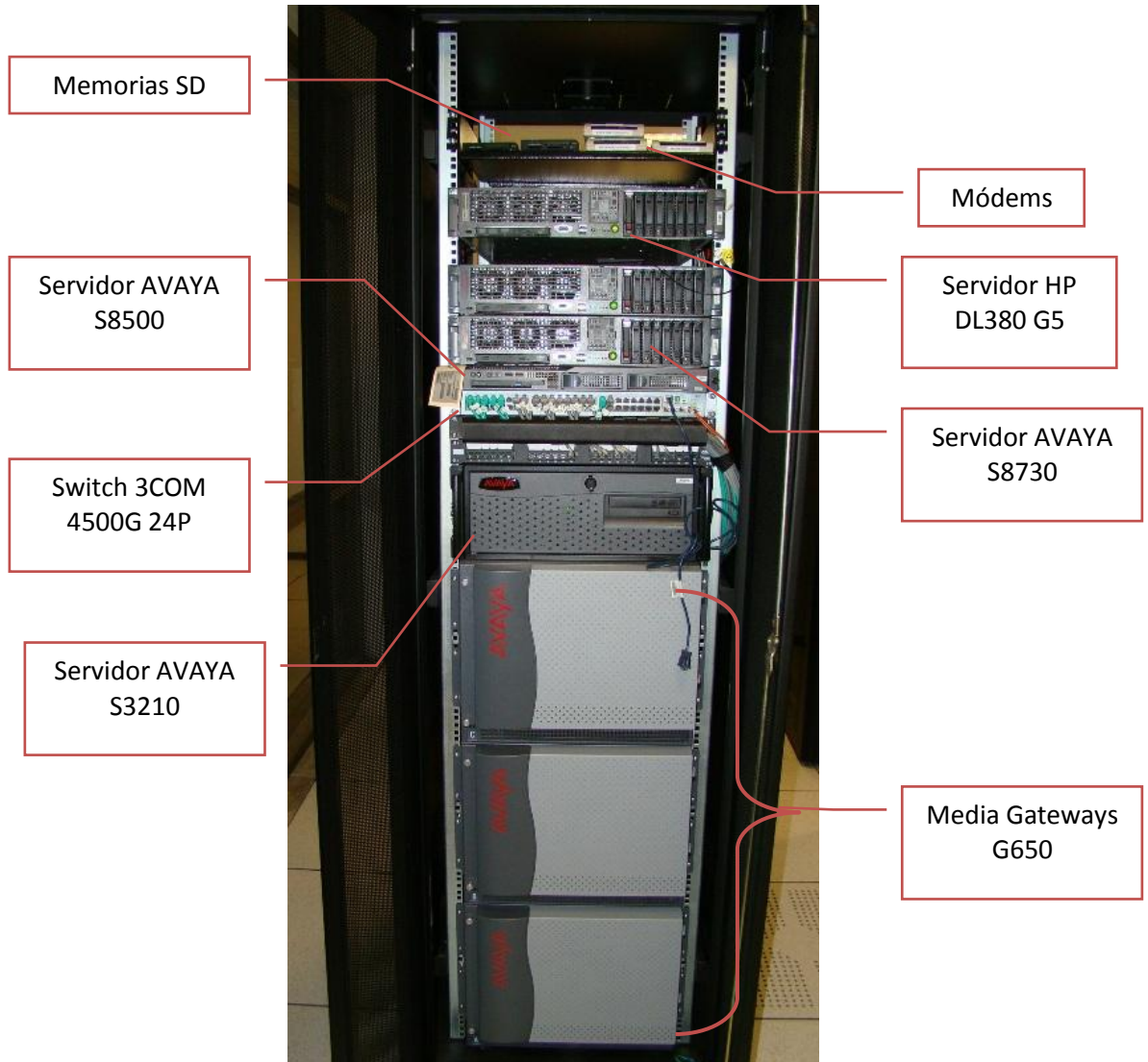


Figura 3.1 Foto del Gabinete de servidores de VoIP de la Universidad Industrial de Santander<sup>1</sup>

<sup>1</sup> Imagen tomada por el autor con autorización de la DSI.

Los equipos relacionados en la Tabla 3.1 conforman el rack principal del sistema, dado que es aquí donde se coordinan y administran todas las operaciones del servicio de ToIP. En el numeral 3.2 se explica la configuración detallada de cada uno de estos haciendo especial énfasis en los equipos encargados de prestar el servicio de ToIP, y mostrando al lector la configuración necesaria para establecer la comunicación tanto en hardware como en software de los demás equipos con estos.

### 3.1.2 Gabinete de Conexiones

Para el cableado proveniente del rack de VoIP que lleva las conexiones para las extensiones y troncales análogas que se describirán más adelante se destina el segundo rack llamado Rack de conexiones como se observa en la Figura 3.2 el cual contiene los *patch panels* que permiten terminar el cableado proveniente de los Gateways.

En este rack están instaladas también las regletas que permiten llevar el cableado de extensiones y líneas hasta el cuarto de telefonía actual y desde ahí a los diferentes edificios. Las conexiones desde los Gateways hacia el cuarto de telefonía se hacen mediante 5 cables telefónicos de 25 pares terminados en Conectores *Telco Amphenol* cada uno. [8]



Figura 3.2 Rack de cableado<sup>1</sup>

Para las conexiones de las siete líneas digitales (RDSI) se utilizan cables mini-coaxiales terminados en conectores BNC.

El cable de todas las conexiones es UTP categoría 5E existiendo enlaces de categoría 6 y 7 de acuerdo con las normas de TIA/EIA-568-B para este tipo de cableado.

---

<sup>1</sup> Foto tomada por el autor con autorización de la DSI.

### 3.2 Configuración de equipos que conforman el gabinete de VoIP

En la presente sección se realiza la descripción de la configuración de los equipos que conforman el gabinete de VoIP de la Universidad el cual está compuesto por diversos equipos como se menciona en la sección 3.1.1. En la Figura 3.3 se muestra un diagrama general de conexiones de red con objeto de introducir al lector en el funcionamiento del sistema el cual está conformado por un Servidor de Voz el cual coordina y administra todos los recursos del sistema, un Servidor de Tarificación el cual permite llevar estadísticas de uso de los servicios que el sistema presta a la comunidad UIS, un Servidor SIP (Protocolo de Inicio de Sesiones) el cual permite el uso de equipos y software compatible con este protocolo, un Servidor de Mensajería el cual permite la integración de correo de voz entre otras funciones, un switch de red el cual permite realizar las conexiones a la red de todos los equipos del rack de VoIP, tres Gateways los cuales permiten entre otras la conexión del sistema de telefonía IP con la red telefónica conmutada pública (PSTN o *Public Switched Telephone Network*); hay que tener claro que todos estos equipos están conectados por dos líneas de fibra óptica al switch principal de la Universidad el cual concentra la WAN de las sedes regionales.

Además se resalta la red de control CNA en color azul y la red corporativa LAN-WAN las cuales serán descritas más adelante.

Hay que tener presente que de los equipos existentes en el gabinete de VoIP hay dos que son fundamentales para el funcionamiento del sistema por lo cual el proceso de documentación es principalmente dedicado a ellos, los cuales son los servidores de Voz y los Gateways, los demás servidores y equipos se encargan de prestar servicios complementarios no esenciales pero anexos al sistema, esto quiere decir que dependen de estos equipos para su funcionamiento por lo cual serán documentados de forma más superficial por no hacer parte del objetivo esencial de este proyecto.



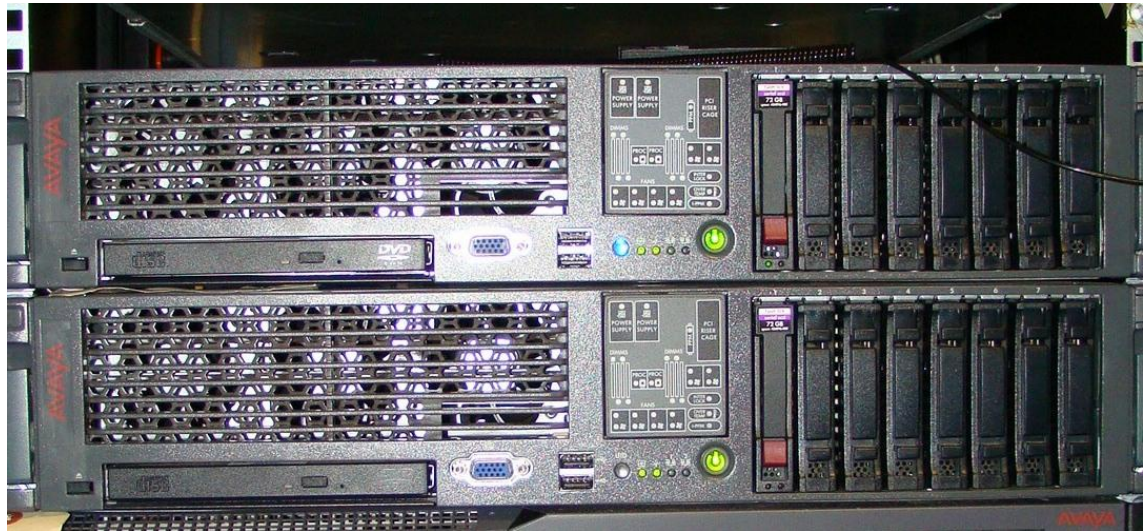


Figura 3.4 Foto servidores S8730 Campus UIS<sup>1</sup>.

Para cumplir la función de Servidor de Voz en el campus principal se encuentran instalados dos servidores AVAYA S8730 los cuales se encargan de coordinar todos los demás equipos anexos al Rack del sistema de ToIP, además de administrar y establecer políticas de seguridad en la autenticación y el direccionamiento del tráfico de todas las extensiones de la Universidad.

Estos dos servidores se encuentran dispuestos en modo redundante en modo de confiabilidad Duplex por Hardware (véase Sección 3.2.1.5.1), en un gabinete de 19 pulgadas, quiere decir que a nivel operativo equivale a un único equipo activo.

Físicamente cada servidor cuenta con las características descritas a continuación:

Equipo	Peso(Kg)	Dimensiones (Cm)	Unidades
S8730	27	8.6 x 45 x 66	2

Tabla 3.2 Descripción física servidores AVAYA S8730

<sup>1</sup> Foto tomada por el autor con permiso de la DSI.

### 3.2.1.1 Características Técnicas y condiciones ambientales

Cada servidor cuenta con las siguientes características técnicas y condiciones ambientales de operación:

Parámetro	Descripción
Temperatura ambiente de operación	50°F to 95°F (10°C to 35°C)
Humedad (operativo)	10% to 90% (Sin condensación)
Tensión de alimentación	100 to 132 VAC
Frecuencia Tensión de entrada	60 Hz
Corriente alimentación	10 A at 100 VAC
Potencia	960 W at 120V AC input
BTUs por hora	2500
Potencia en Standby	850 W at 120V AC input
Potencia pico máxima	400 W
Microprocesador	1 Dual Core Rev. "F" AMD
Memoria	2.5GB
Unidades (SCSI)	Disco duro: 72 GB, 10.000 RPM
	CD-ROM/DVD-ROM: 24x Max.
	Disquete 1.44MB
DLA2 Duplicación por hardware	Activado
Tarjeta de red	3 Puertos 100/1000GB Ethernet
Funciones Integradas	2 Puertos 100/1000Gb Ethernet
	Interfaz ILO
	Conector para teclado
	Conector para Mouse
	4 puertos USB
	Conector de video

Tabla 3.3 Rangos de operación y características técnicas básicas.

### 3.2.1.2 Procesador

Los servidores S8730 cuentan con un procesador *Dual-Core AMD Opteron(tm) 2216 stepping 03*, el cual únicamente realiza tareas de coordinación de todo el sistema de VoIP como se pudo observar ejecutando el comando “top” en una terminal SSH a diferentes horas del día donde el uso del procesador no excedía el 15%, pues todo el procesamiento complejo de comunicaciones, uso de codecs,

compresión y descompresión de audio, codificación, digitalización, lo realizan las unidades Gateways, las tarjetas que lo componen y el Servidor SIP S8500, equipos que serán descritos más adelante.

### 3.2.1.3 Almacenamiento y memoria RAM.

Los servidores S8730 cuentan con 4 gigas de memoria DDR2, además cada servidor S8730 cuenta con un disco duro de SAS<sup>1</sup> de 72GB para el almacenamiento de la información y configuración e instalación del sistema operativo, este se encuentra instalado en la primera bahía del servidor.

<b>SERVIDOR 1</b>					
<b>Filesystem</b>	<b>1K-blocks</b>	<b>Used</b>	<b>Available</b>	<b>Use%</b>	<b>Mounted on</b>
/dev/cciss/sda1	17377004	873316	15620984	6%	/
/dev/cciss/sda6	17377004	879184	15615116	6%	/root2
/dev/cciss/sda5	34750004	1927240	31057556	6%	/var

<b>SERVIDOR2</b>					
<b>Filesystem</b>	<b>1K-blocks</b>	<b>Used</b>	<b>Available</b>	<b>Use%</b>	<b>Mounted on</b>
/dev/cciss/sda1	17377004	874196	15620104	6%	/
/dev/cciss/sda6	17377004	879164	15615136	6%	/root2
/dev/cciss/sda5	34750004	1271356	31713440	4%	/var

Tabla 3.4 Sistema de particionado de discos

En la Tabla 3.4 se observa los sistemas de archivos creados en ambos servidores de manera idéntica, así como sus respectivos puntos de montaje, el tamaño total, el disponible y el ocupado por partición, estos datos son obtenidos de la línea de comandos de Linux usando el comando `df` (Véase Sección 3.2.1.7).

<sup>1</sup> Serial Attached SCSI o SAS, es una interfaz de transferencia de datos en serie, sucesor del SCSI (*Small Computer System Interface*) paralelo, aunque sigue utilizando comandos SCSI.

Hay que agregar que los servidores S8730 cuentan con un sistema de memoria Flash de uso corporativo<sup>1</sup> de 128 MB como se observa en la Figura 3.1 conectada a un puerto USB, en la cual el sistema se encarga de realizar temporalmente todas las operaciones de escritura y modificaciones realizadas en el sistema con objeto de evitar que las operaciones de escritura se realicen de forma continua aumentando el rendimiento de lectura y minimizando los posibles errores que se pueden producir en el sistema de archivos o en la base de datos por estar realizando operaciones simultáneas de lectura y escritura.

Según configuración verificada en el servidor usando el comando `display system-parameters maintenance` en CM esta operación se realiza una vez al día en el periodo comprendido entre las 10 pm y las 6 am de forma automática, el comando que se encarga de ejecutar esta tarea de modo manual se llama `save Translation`.

#### **3.2.1.4 Sistema Operativo**

Cada servidor posee instalada la distribución de Linux RedHat 3.4.3-9.EL4 la cual se encuentra diseñada y optimizada con soporte de hardware embebido en el Kernel del sistema, esto con el objetivo específico de garantizar la máxima estabilidad y rendimiento del sistema de telefonía IP ejecutando el software *AVAYA Communication Manager 5.0*.

#### **3.2.1.5 Configuración de Conexiones Servidores S8730**

La configuración de las conexiones del servidor AVAYA S8730 se explica a continuación y se divide en sistema de redundancia, y las conexiones de red.

---

<sup>1</sup> De alta durabilidad diseñada para millones de operaciones de escritura y lectura y garantizada de por vida.

### 3.2.1.5.1 Sistema de Redundancia dúplex

Los servidores S8730 se encuentran conectados por medio de un sistema de redundancia dúplex, el cual consta de una interfaz de red en ambos servidores conectada por medio de un cable de red UTP cruzado y de un sistema de duplicación de memoria por hardware usando un enlace de fibra óptica.

En la Figura 3.5 se puede observar la configuración del actual sistema de redundancia instalado en los servidores S8730 de la Universidad además de las diferentes interfaces de red que los servidores utilizan para prestar los servicios de telefonía IP e interconectarse con los demás equipos encargados de administrar el sistema.

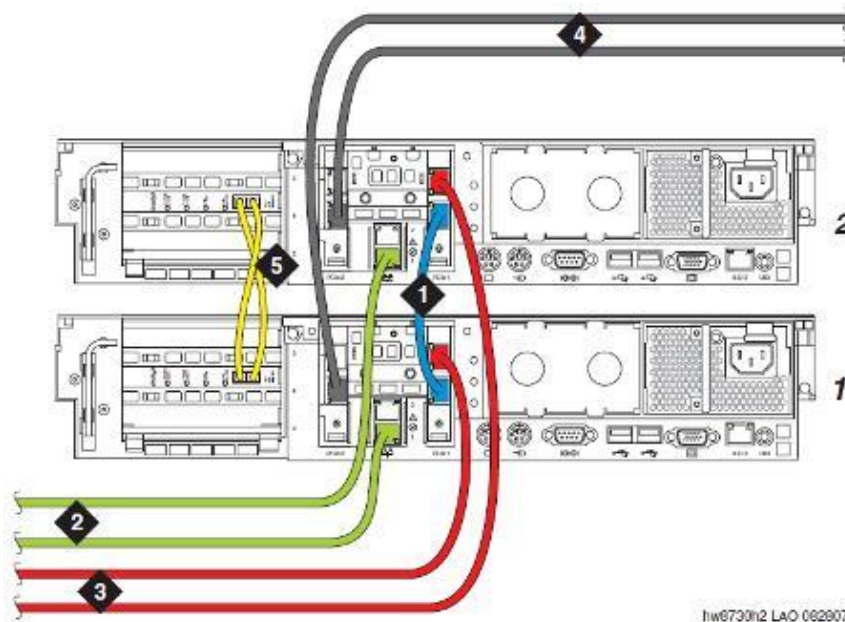


Figura 3.5 Diagrama de conexiones de red<sup>1</sup>

1. eth2 – Interfaz de duplicación <sup>2</sup>

<sup>1</sup> Imagen tomada de **Sims, Jamie**. Jaymzworld. [En línea] Technical Manager, Avaya Inc. [http://jaymzworld.com/wiki/Server\\_ports\\_and\\_IP\\_addresses](http://jaymzworld.com/wiki/Server_ports_and_IP_addresses).

<sup>2</sup> Eth corresponde al nombre del dispositivo establecido por Linux para nombrar las diferentes interfaces de red.

2. eth0 - CNA (interfaz de control LAN privada)
3. eth3 - CNB (Interfaz de control LAN privada)
4. eth4 – Interfaz de conexión con red LAN institucional.
5. Cable de duplicación de fibra óptica.

La interfaz de red que interconecta mutuamente los dos servidores corresponde a Eth2 y existe con el objeto de mantener en constante sincronismo la información almacenada en los discos duros locales y se establece por medio del uso de un cable UTP cruzado.

Protocolo	Servidor Local:puerto	Servidor Remoto:Puerto	Estado	Servidor
tcp	VozUIS-1-dup:12080	VozUIS-2-dup:58185	ESTABLISHED	Primario
tcp	VozUIS-2-dup:58185	VozUIS-1-dup:12080	ESTABLISHED	Secundario

Tabla 3.5 Conexiones de red asociadas a la duplicación por medio de red UTP.

Como se puede observar en la Tabla 3.5 en cada uno de los servidores se encuentra un proceso ejecutándose en el sistema operativo con el objeto de mantener en constante sincronismo la información y establecer una conexión del servidor primario con el servidor secundario y viceversa.

En la tabla también se observa el tipo de protocolo y los puertos de red utilizados para la transferencia de la información.

Los servidores S8730 cuentan con un sistema avanzado de replicación de memoria para garantizar alta disponibilidad y minimizar la posible pérdida de datos al ocurrir una falla, aunque la duplicación por software usando conexión de red UTP únicamente es bastante útil y eficaz. Para ambientes de producción y de gran congestión de usuarios es insuficiente, pues el rendimiento se reduce y termina por convertirse en un cuello de botella para el sistema [5] , por lo cual se recomienda un sistema de duplicación adicional dedicado a la memoria RAM del sistema que se ejecute en tiempo real, de forma independiente y tenga la capacidad de procesar gran cantidad de información sin elevar el consumo de recursos del servidor.

La solución instalada para la Universidad Industrial de Santander corresponde a un sistema por hardware y tiene como objetivo replicar la información de la

memoria de intercambio del sistema operativo y se encuentra implementado por medio del uso de una tarjeta de expansión referencia AVAYA DAL2 la cual es instalada en cada uno de los servidores S8730 y permite que toda la información de la memoria RAM<sup>1</sup> del servidor activo sea procesada por la tarjeta y transmitida por medio de un enlace de fibra óptica de alta velocidad al servidor secundario en tiempo real y de forma independiente, con objeto de mantener en constante sincronismo la memoria RAM de los dos servidores y reducir el riesgo de pérdida de información en el momento de una falla.

Al usar el comando `cat /proc/mdd` usando una terminal SSH en el servidor activo se despliega la siguiente información:

This DAL-2 card is ACTIVE
Error Reg = 00200000
Status Reg = 40010037
Signal detected from SERDES
The optical interface is in sync.
The card memory is 512 MB.
The PCI bus is 64 bits at 133 MHz.

Tabla 3.6 Estado tarjeta DAL-2 terminal SSH servidor primario

De la cual se puede observar que el estado actual de la tarjeta es activo y que cuenta con una memoria de 512MB para la transferencia y el procesado de la información.

Escribiendo el mismo comando en el servidor secundario en estado standby encontramos lo siguiente:

This DAL-2 card is STANDBY
Error Reg = 00000000
Status Reg = 40010037
Signal detected from SERDES
The optical interface is in sync.

<sup>1</sup> Random Access Memory: Memoria de acceso aleatorio

The card memory is 512 MB.
The PCI bus is 64 bits at 133 MHz.

Tabla 3.7 Estado tarjeta DAL-2 terminal SSH servidor secundario

De lo cual se obtiene que la tarjeta DAL-2 esté en estado STANDBY debido a que la tarjeta no está realizando el procesamiento de la información de la memoria RAM y solo está en sincronismo con el servidor primario recibiendo la información que éste le envía.

Finalmente hay que recordar que cada uno de los servidores cuenta con 4 GB de memoria RAM y 512MB de memoria Swap.

### **3.2.1.5.2 Configuración de red servidores s8730**

Los servidores S8730 cuentan con 5 interfaces de red físicas y 3 virtuales para permitir la conectividad con los diversos equipos que conforman el núcleo del sistema.

Las interfaces virtuales son creadas en Linux con el objetivo de permitir asignar a una única tarjeta de red 2 direcciones IP de manera simultánea. En la Tabla 3.8 se observa ETH0:0, ETH3:0 y ETH4:0 las cuales corresponden a alias de red de las interfaces ETH0, ETH3 y ETH4, estos alias se crean únicamente en el servidor marcado como primario y apuntan a las interfaces principales de este, lo que permite que a pesar de que el servidor primario salga de servicio y el secundario tenga que convertirse en primario siempre la conectividad hacia los servidores desde la red se mantenga.

Esto quiere decir que si el servidor 1 cambia a modo inactivo (sale de servicio) y servidor 2 debe entrar a estado activo el software de AVAYA activará en Linux las interfaces ETH0:0, ETH3:0 y ETH4:0 (alias de red) en el servidor secundario, con los mismos IP que contaba el servidor 1 pero dependientes de las interfaces ETH0, ETH3 y ETH4 del servidor 2, logrando con esto un cambio transparente para el usuario final o para los equipos que se conectan directamente a los servidores S8730.

Como se observa en la Figura 3.7 actualmente ETH0:0 cuenta con el IP 172.18.20.10 el cual es alias de ETH0 con IP 172.18.20.11, si servidor 1 saliera de servicio la configuración de ETH0:0 para el servidor 2 seria el mismo IP 172.18.20.10 pero alias de ETH0 con IP 172.18.20.12, y como el sistema cuenta con replicación en tiempo real el sistema continuaría funcionando normalmente sin efectos negativos para el usuario.

En la Tabla 3.8 se resume la configuración de las interfaces de red existentes en los servidores.

Interfaz	IP Servidor 1	IP Servidor 2	Descripción	Estado
Eth0	172.18.20.11	172.18.20.12	Interfaz de control CNA red privada	Activa
Eth0:0	172.18.20.10		Interfaz activa CNA	Activa
Eth1	192.11.13.6	192.11.13.6	Interfaz de Servicios	Inactiva
Eth2	192.11.13.13	192.11.13.14	conexión de duplicación de servidores	Activa
Eth3	198.152.254.201	198.152.254.202	Interface de control CNB	Inactiva
Eth3:0	198.152.254.200		Interfaz activa CNB	Inactiva
Eth4	192.168.14.11	192.168.14.12	Interfaz de conexión con LAN Institucional	Activa
Eth4:0	192.168.14.10		Interfaz activa LAN Institucional	Activa

Tabla 3.8 Configuración de red Servidores S8730

En la Figura 3.6 se muestra un enfoque más amplio y claro de la configuración de red de los servidores de la Universidad, en ella se pueden observar claramente las diferentes interfaces de red enumeradas en la Tabla 3.8 y se encuentra señalada la red de control A (CNA) la cual se refiere a la subred privada destinada exclusivamente a interconectar los Gateways (véase sección 3.2.2) y los servidores S8730.

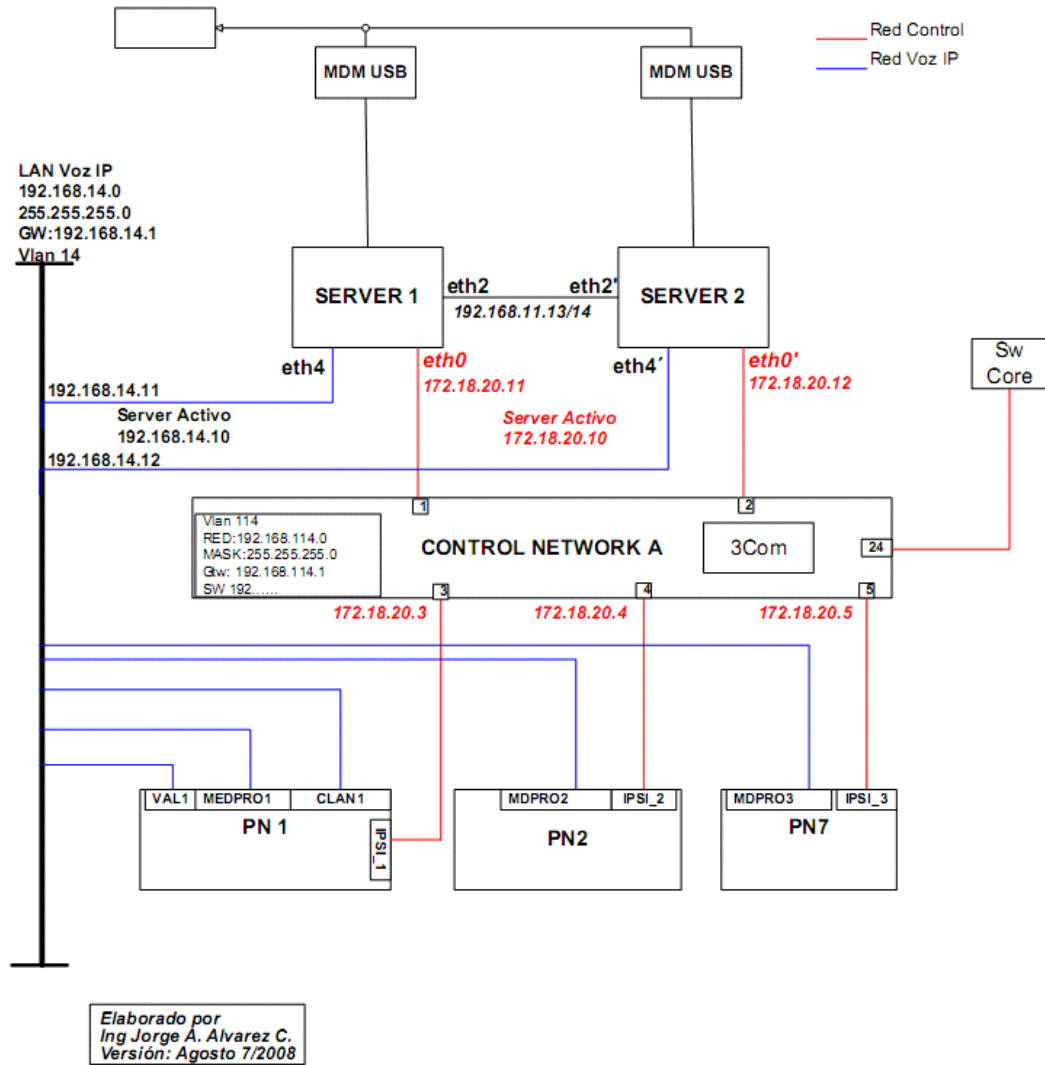


Figura 3.6 Diagrama configuración de interfaces de red servidores S8730<sup>1</sup>.

A continuación se detallará la descripción de cada una de la interfaces de red mencionadas anteriormente incluso las que en este momento se encuentran inactivas debido a que es importante conocer a profundidad estas conexiones pues permitirán realizar modificaciones futuras a la configuración de red del sistema, como se propone en el capítulo 4.

<sup>1</sup> Imagen Cortesía de Assenda S.A empresa encargada del diseño e instalación del sistema de VoIP de la Universidad.

## **Eth0**

Interfaz de red conectada a la red de control CNA<sup>1</sup> la cual corresponde a una red privada conectada al Switch 3COM como se muestra en la Figura 3.6, donde se encuentran conectadas las tarjetas IPSI (TN2312BP, IP server Interface) las cuales son la interfaz de comunicación entre los servidores S8730 y los Gateways, además son responsables del control del enrutado de llamadas y mensajes que van desde la red LAN institucional hacia los servidores. Para mayor información remitirse a Tarjetas IP Server Interface (IPSI) TN2312BP en la pagina 56.

## **Eth1 (inactiva)**

Corresponde a la interfaz de servicio del sistema y solo es utilizada en momentos en que la administración remota no es posible o en los primeros pasos de instalación del servidor.

## **Eth2**

Corresponde a la interfaz de red encargada de la duplicación de información de los discos duros de los servidores; como se explicó anteriormente existe una aplicación y unos puertos de red asociados para cumplir con este fin.

## **Eth3 (inactiva)**

Corresponde a una interfaz de red disponible para futuras ampliaciones del sistema o para la instalación de un sistema de redundancia más avanzado en el cual existan Media Gateways de contingencia y por lo tanto existan 2 redes de control como se propone en el capítulo 4.2.

---

<sup>1</sup> Control Network Interface A: Red de control A

## Eth4

Es la interfaz de red que se encuentra conectada a la red LAN institucional de la Universidad, quiere decir que es accesible desde cualquier punto de red de la universidad además esta permite la administración remota del sistema por medio de protocolos como SSH, Web, Communicator Manager, Web seguro (véase sección 3.2.1.7). Por lo cual es la interfaz que presenta mayor riesgo de seguridad para el sistema pues existen 5000 equipos aproximadamente con acceso directo a ella. Es por esto que desde otro servidor de la Universidad se ejecutó un escáner de puertos usando el comando de Linux `nmap -p1-65535 192.168.14.101` con objeto de verificar la seguridad del sistema en la interfaz Eth4. Los resultados del comando se muestran en la Tabla 3.9, el comando `nmap` con los modificadores usados busca puertos abiertos escaneando desde el puerto 1 al 65535 al IP 192.168.14.10 el cual corresponde al IP del servidor activo.

Puerto	Estado	Servicio
22/tcp	open	SSH
80/tcp	open	http
81/tcp	open	hosts2-ns
411/tcp	open	rmt
443/tcp	open	https
5022/tcp	open	Com-M
21874/tcp	open	unknown

Tabla 3.9 Puertos abiertos del servidor activo usando escaneo de puertos desde otro servidor.

De la lista mostrada se destacan puertos como el 22 que corresponde a la terminal de Linux SSH usada para documentar gran parte de este informe, el puerto 80 y 443 que corresponden al servidor Web el cual permite administrar el sistema de

---

<sup>1</sup> *Nmap es una herramienta GNU diseñada para explorar y para realizar auditorías de seguridad en una red.*

modo grafico y el puerto 5022 el cual corresponde al servicio *Communication Manager* a través una conexión encriptada usando el protocolo SSH.

Como se puede observar en la Tabla 3.9 no existen puertos que ofrezcan servicios de ToIP como se esperaría. Lo anterior se debe a que por robustez del sistema a pesar de que este servicio es coordinado por él, éste es ofrecido a través de una tarjeta instalada en los Gateways que serán descritos en la sección 3.2.2, con el objetivo de liberar al servidor de tareas y permitir manejar el trafico de llamadas de la Universidad sin problemas.

### 3.2.1.5.3 Enrutamiento de red

Continuando con la configuración de red, en la Tabla 3.10 se muestra la tabla de rutas de red usada por los servidores para direccionar los paquetes de red a través de las diferentes interfaces de red.

Kernel IP routing table							
Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
192.11.13.12	*	255.255.255.252	U	0	0	0	eth2
192.11.13.4	*	255.255.255.252	U	0	0	0	eth1
172.18.20.0	*	255.255.255.0	U	0	0	0	eth0
192.168.14.0	*	255.255.255.0	U	0	0	0	eth4
198.152.254.0	*	255.255.255.0	U	0	0	0	eth3
169.254.0.0	*	255.255.0.0	U	0	0	0	eth4
default	192.168.14.1	0.0.0.0	UG	0	0	0	eth4

Tabla 3.10 Tabla de enrutamiento de red

### 3.2.1.6 Configuración de interconexión con demás servidores que conforman el sistema.

Como fue mencionado al principio de este capítulo, el Servidor de Voz es quien coordina y administra los recursos del sistema de ToIP, es por esto que en él deben estar configurados todos los equipos que hacen parte o prestan servicios a este sistema. A pesar de que el objetivo principal de este proyecto no es mostrar la configuración usando *CM* en este caso se considera importante destacar que

para poder prestar sus servicios al sistema de ToIP, los diferentes servidores y equipos deben encontrarse registrados en el servidor principal de voz; es por esto que en la Figura 3.7 se observa no solo los servidores que hacen parte del rack de VoIP del campus principal sino los servidores distribuidos en las sedes regionales y las tarjetas que hacen parte de los Gateways, las cuales serán descritas en la siguiente sección.

```
list node-names Page 1
```

NODE NAMES		
Type	Name	IP Address
AUDIX	audix	192.168.14.15
IP	CLAN1	192.168.14.2
IP	CLAN2	192.168.14.3
IP	CLAN3	192.168.14.4
IP	DALI	192.168.14.16
IP	MEDPRO1	192.168.14.5
IP	MEDPRO2	192.168.14.6
IP	MEDPRO3	192.168.14.7
IP	SESBarbosa	192.168.55.10
IP	SESGuati	192.168.12.10
IP	SESSalud	192.168.7.10
IP	SIP-SERVER	192.168.14.20
IP	TK-IP-BARBOSA	192.168.55.10
IP	TK-IP-BARRANCAB	192.168.13.10
IP	TK-IP-BUCARICA	192.168.10.10
IP	TK-IP-GUATIGUAR	192.168.12.10
IP	TK-IP-MALAGA	192.168.52.10
IP	TK-IP-SALUD	192.168.7.10
IP	TK-IP-SOCORRO	192.168.49.10
IP	VAL1	192.168.14.8
IP	dali2	192.168.38.123
IP	default	0.0.0.0
IP	procr	192.168.14.11

Figura 3.7 resultado del comando `list node-names` usando *Communication Manager* en el Servidor de Voz.

De la lista se destaca el servidor que presta el servicio de mensajería unificada el cual se encuentra registrado como de tipo AUDIX esto debido a que es el Servidor de Voz quien debe re-direccionar las llamadas a este nodo cuando sea necesario. Un ejemplo de ese caso es cuando se llama a un usuario y este no contesta, o se realiza desde el teléfono una consulta de buzón de voz, este

servidor será descrito de forma más detallada en la sección 3.2.7. Adicionalmente en la sección 3.2.6.3 encontrará los parámetros de configuración del servidor Dalí y en la sección 3.2.4.4 los parámetros de configuración del Servidor SIP.

### **3.2.1.7 Interfaces de configuración de los servidores de voz.**

Los servidores cuentan con diferentes formas de permitir su administración; aunque existe documentación detallada sobre estos temas es de importancia en este trabajo mostrar la función de cada una de ellas dado que es fundamental conocer esta información en el momento de administrar el sistema

#### **3.2.1.7.1 Interface Web**

Esta interface es de gran utilidad para la configuración del sistema pues permite de forma grafica configurar gran parte de los parámetros básicos requeridos por el servidor, incluye asistentes de configuración para instalar el servidor además permite realizar diagnósticos, crear cuentas de usuario en el sistema, verificar alarmas, intercambiar los servidores activos, apagar el servidor, realizar copias de seguridad, actualizar software, entre otras, opciones orientadas al mantenimiento, monitoreo y administración del sistema. En la Figura 3.8 se muestra una vista previa de este entorno de configuración el cual es accesible desde un navegador web al sitio <https://192.168.14.10> desde la red LAN de la Universidad.

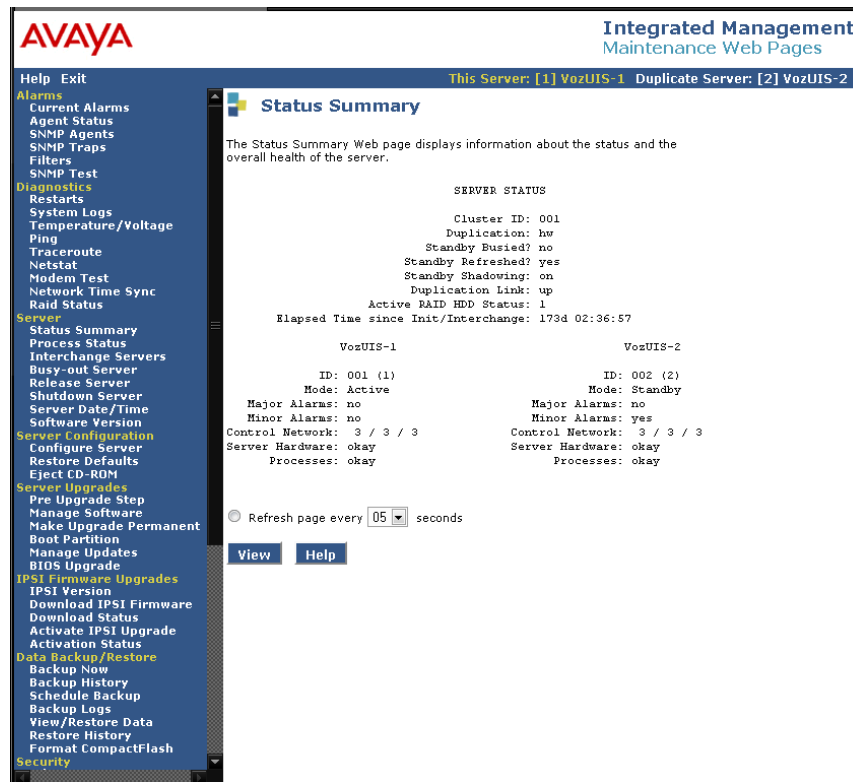


Figura 3.8 Vista de sistema de configuración Web.

Hay que agregar también que esta interface está disponible a través de una conexión a la interface Eth1 en cualquiera de los dos servidores S8730, usando un cable UTP y un computador para establecer esta conexión al sitio <https://192.168.13.6>

### 3.2.1.7.2 Interface *Communication Manager 5.0*

El ASA (*Avaya Site Administration*) como se le conoce normalmente, es un emulador de terminal que permite administrar de forma remota el servidor del *Communication Manager* (CM) y el servidor del correo de voz AUDIX descrito en el capítulo 3.2.7. Este sistema también permite modificar parámetros de configuración y existen extensos manuales sobre su uso (ver bibliografía), además de manuales diseñados para la universidad por otro proyecto de grado [8].

Su uso se orienta a creación de extensiones, configuración de Gateways, troncales, tarjetas, nodos, estaciones, extensiones y todo lo relacionado a las conexiones del sistema.

En la Figura 3.9 se puede observar una captura de pantalla del sistema de administración.

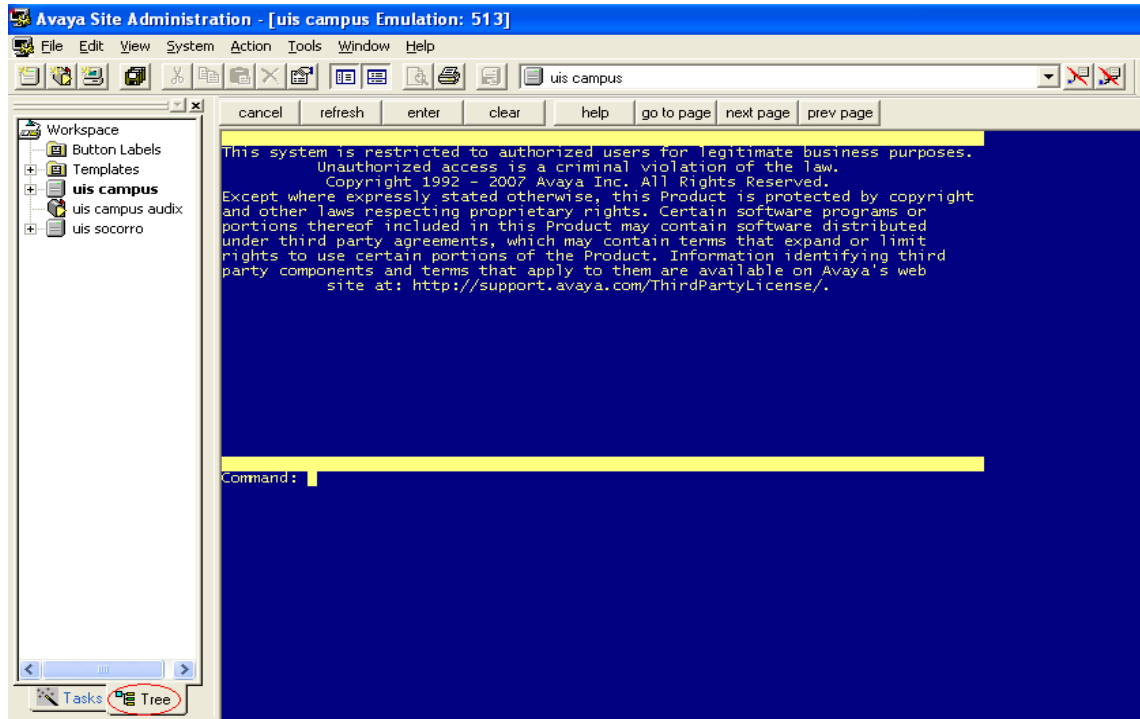


Figura 3.9 Vista del sistema de configuración usando CM 5.0.

### 3.2.1.7.3 Configuración usando protocolo SSH

El sistema instalado en la universidad se encuentra instalado en Linux el cual ha sido optimizado para garantizar la supervivencia del sistema e integra el uso del protocolo SSH el cual habilita la posibilidad de usar la emulación de una terminal cliente remota para conectarse al servidor y realizar procesos de administración avanzados relacionados con el estado de las conexiones de red, consulta de procesos activos, verificación de sistema de archivos e incluso desde esta acceder a la terminal del CM mencionada anteriormente. En la Figura 3.10 se muestra un

ejemplo de la terminal usando un cliente emulador de terminal llamado Putty de uso libre.



Figura 3.10 Vista del sistema de consola usando Putty<sup>1</sup> a través del protocolo SSH.

### 3.2.2 Configuración de Gateways

El sistema de ToIP cuenta con tres *Media Gateways G650* los cuales son elementos de hardware modulares apilables, se encuentran administrados por los servidores AVAYA S8730 y tienen la función de:

- Interconectar diferentes tipos de redes entre los cuales tenemos las diferentes troncales digitales, los nodos, los canales dedicados con las regionales de la Universidad, la red privada y la red de control.
- Supresión de eco.
- Control y señalización de llamadas
- Inserción del tono de las líneas digitales.

<sup>1</sup> Putty es un Software emulador de terminal con licencia MIT de uso libre y descargable desde: <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

- Conversión entre los teléfonos TDM y el protocolo de *streaming* (RTP).

Además de considerarse la puerta de enlace de los servidores S8730 independiza tareas en diversos dispositivos de hardware divididos en tarjetas y módulos lo que permite optimizar el rendimiento del sistema y una mayor robustez por lo cual AVAYA lo ubica en su catalogo de productos como un equipo de misión crítica.

Desde la consola de CM se pueden observar los gabinetes instalados y activos en el sistema usando el comando `list cabinet` y su resultado se observa en la Figura 3.11 donde PN (Port Network) se refiere al canal de comunicación creado entre una tarjeta IPSI y el Servidor de Voz, el cual es un concepto bastante útil cuando una sola tarjeta IPSI administra varios Media Gateways para este caso se puede observar que existe 3 PN, las cuales son PN 01, PN 02 y PN 03 lo que equivale a una tarjeta IPSI por Gateway instalado.

```
list cabinet
CABINET REPORT
No  Layout/   Rack/      Loc  A    B    C    D    E
   Room     Floor      Building
1   G650
2   G650
3   G650
1   PN 01
1   PN 02
1   PN 03
```

Figura 3.11 Comando `list cabinet` en CM 5

Físicamente los *Gateways* instalados en la Universidad lucen como se observa en la Figura 3.12, además cada *Media Gateway G650* está montado en un Rack estándar de 19" (48 cms) y es alimentado mediante potencia a.c. 120 Voltios, con un consumo de potencia de 500 watios (8 amperios).

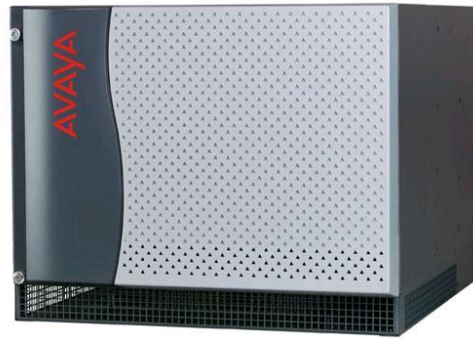


Figura 3.12 *Media Gateway G650*

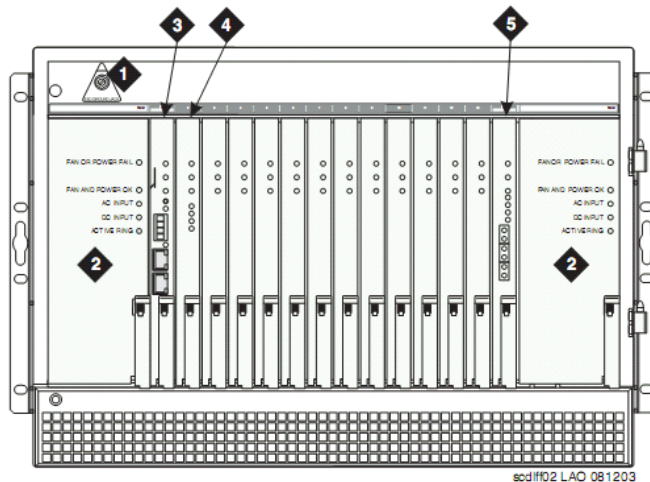
Para complementar la descripción física se anexan las dimensiones y el peso del equipo.

Equipo	Peso(Kg)	Dimensiones (Cm)	Unidades
Media Gateway 650	18	8.8x43x43	3

Tabla 3.11 Descripción física *Media Gateway G650*.

### 3.2.2.1 Configuración de componentes que conforman los Gateways

Los *Media Gateways* constan de 14 ranuras o slots cada uno, con el objeto de alojar las tarjetas necesarias para el funcionamiento del sistema y permitir implementación de nuevas funciones.



Numero	Componente
--------	------------

1	Banda de descarga ESD
2	Fuente de Poder de 655A
3	Tarjeta IPSI ( <i>IP Server Interface</i> ) Ref. TN2312BP RHS
4	Tarjeta CLAN ( <i>Control Lan Circuit Pack</i> ) Ref. TN799DP
5	Tarjeta MEPRO ( <i>IP Media Processor</i> ) Ref. TN2602AP

Tabla 3.12 Componentes principales del Media Gateway G650

En la Tabla 3.12 se describe los componentes principales de cada uno de los *Media Gateway G650*; hay que recordar que el sistema de VOIP de la Universidad Campus principal cuenta con 3 de estos para soportar el tráfico generado.

Además existen tarjetas adicionales instaladas en *los Media Gateways* las cuales implementan servicios agregados al sistema de telefonía IP las cuales se enumeran en la Tabla 3.13.

Cantidad	Componente
1	Tarjeta <i>Voice Announcements over LAN</i> (VAL) TN2501AP
7	Interfaz DS1 TN2464CP
5	Tarjeta TN793CP para líneas Analógicas
1	Tarjeta de mantenimiento y prueba TN771DP
3	Tarjeta de troncales digitales TN747B

Tabla 3.13 Componentes adicionales Media Gateway G650

A continuación se describe cada una de las tarjetas enumeradas en las tablas anteriores.

### 3.2.2.1.1 Tarjetas *IP Server Interface* (IPSI) TN2312BP



Figura 3.13 Tarjeta IPSI instalada en MediaGatewayG650<sup>1</sup>.

La universidad cuenta con 3 tarjetas IPSI, una tarjeta IPSI por cada *Media Gateway G650* instalado en configuración sin contingencia. Hay que aclarar que existe la configuración de duplicación de alta confiabilidad la cual ofrece duplicidad de *Media Gateway G650* y por lo tanto de tarjetas IPSI con el objeto de garantizar una mayor estabilidad al sistema, la cual es una propuesta incluida en este documento a la cual se dedicará el capítulo 4.2.

Las tarjetas IPSI proveen transporte de mensajes de control enviados entre el servidor S8730 y los Media Gateways G650 usando una red privada llamada Red de control (CN) denotada por las letras A y B cuando existen redes de control de contingencia, en este caso sólo se hará referencia a Red de control A.

Por otro lado además se encargan de señalar los paquetes de datos usando multiplexación TDM, e integra una interfaz Ethernet para conectividad de servicio técnico y posibilita la conexión a la tarjeta TN771DP EPN la cual permite monitoreo y diagnostico de mantenimiento del rack.

NOMBRE	IP
IPSI1	172.18.20.3
IPSI2	172.18.20.4
IPSI3	172.18.20.5

Tabla 3.14 direcciones IP tarjetas IPSI conectadas a la CNA (Control Network A)

En la Tabla 3.14 se resumen las direcciones IP en la red privada de control A de las tarjetas IPSI instaladas en el sistema. Más sin embargo haciendo uso del *Comunicator Manager (CM)* se puede extraer mas información de la configuración, usando el comando `list ipserver-interface` como se puede observar en la Figura 3.14.

<sup>1</sup> Imagen de tarjeta IPSI equivalente a la instalada mostrada para referencia tomada de: <https://www.ezylan.com/hinh/TN2312BP.jpg>

```

list ipserver-interface
his system is restricted to authorized users for legitimate business purposes.
      IP SERVER INTERFACE INFORMATION

Port Pri/  Primary/      Primary/      Primary/      State Of
Ntwk Sec  Secondary     Secondary     Secondary     Serv  Control Health
Num  Bd Loc  IP Address    Host Name     DHCP ID  State  State  C P E G
-----
  1   1A01  172.18.20.3   172.18.20.3   ipsi-A01a  IN    actv-aa 0.0.0.0
  2   2A01  172.18.20.4   172.18.20.4   ipsi-A02a  IN    actv-aa 0.0.0.0
  3   3A01  172.18.20.5   172.18.20.5   ipsi-A03a  IN    actv-aa 0.0.0.0
  
```

Figura 3.14 list ipserver-interface en Communication Manager

Esto permite determinar además de la dirección IP, el número del Slot utilizado en cada media Gateway y el número de *Media Gateway* al que se encuentra conectado. Por estándar del fabricante se exige que las tarjetas IPSI siempre sean instaladas en el primer puerto de los *Media Gateways*.

Cada IPSI tiene 2 puertos 10/100 BaseT Ethernet como se observa en la Figura 3.13 para propósito de administración vía Telnet<sup>1</sup> y ejecutar tareas como establecer la dirección IP y configuración de puerta de enlace y hacer pruebas de diagnostico como, ping, traceroute, netstat, etc. En la sección 4.2 se explican algunos de estos procedimientos ver bibliografía para más detalles.

### 3.2.2.1.2 Tarjetas Mepro, C-lan y Val.

El servidor S8730 como fue descrito, se encuentra conectado y administra los *Media Gateways* a través de las tarjetas IPSI, más sin embargo estas tarjetas no son accesibles desde la red local de la universidad debido a que no cuentan con una interfaz de conexión pública<sup>2</sup> y como fue explicado anteriormente estas tienen

---

<sup>1</sup> *TELEcommunication NETWORK*: es el nombre de un protocolo de red que sirve para acceder mediante una red a otra máquina para manejarla remotamente.

<sup>2</sup> Se refiere a la red LAN institucional de la Universidad Industrial de Santander, la cual está conformada aproximadamente por 4500 equipos de cómputo y telefonía.

principalmente la función de establecer la conexión entre los servidores S8730 y los gabinetes *Media Gateways G650*, los cuales prestan servicios a la red corporativa de la UIS a través de las tarjetas CLAN, MEPRO, y VAL. En la Figura 3.15 se muestran los datos de conexión y configuración de dichas tarjetas desde la consola de administración de los servidores S8730.

```
list ip-interface all
```

IP INTERFACES									
ON	Type	Slot	Code	Sfx	Node Name/ IP-Address	Subnet Mask	Gateway Address	Net Rgn	VLAN
y	C-LAN	01A02	TN799	D	CLAN1 192.168.14.2	255.255.255.0	192.168.14.1	1	n
y	C-LAN	02A02	TN799	D	CLAN2 192.168.14.3	255.255.255.0	192.168.14.1	2	n
y	C-LAN	03A02	TN799	D	CLAN3 192.168.14.4	255.255.255.0	192.168.14.1	3	n
y	MEDPRO	01A14	TN2602		MEDPRO1 192.168.14.5	255.255.255.0	192.168.14.1	1	n
y	MEDPRO	02A14	TN2602		MEDPRO2 192.168.14.6	255.255.255.0	192.168.14.1	1	n
y	MEDPRO	03A14	TN2602		MEDPRO3 192.168.14.7	255.255.255.0	192.168.14.1	1	n
y	VAL	01A04	TN2501		VAL1 192.168.14.8	255.255.255.0	192.168.14.1		n

```
Command successfully completed
Command:
```

Figura 3.15 Comando ip-inferface all

En la Figura 3.15 hay información bastante importante referente al slot de las tarjetas instaladas, dado que es necesario para procesos de configuración, hay que agregar que este indica la ubicación completa en el sistema de *Gateways*; por ejemplo para la primera tarjeta C-LAN de la lista el código del slot 01A02, corresponde a lo siguiente: “01” quiere decir que la tarjeta se encuentra ubicada en el primer *Port Network* registrado que para este caso específico es equivalente al primer *Media Gateway* de abajo hacia arriba en el rack de VoIP pues existe instalada una tarjeta IPSI por cada *Media Gateway*; “A” que corresponde al primer canal del *Port Network* como se explico anteriormente eso sería útil si una tarjeta IPSI administrara varios *Media Gateways* pues en este caso si la misma tarjeta

administrara 2 o más marcaria al segundo y tercer canal con la letra B y C es por esto que en la lista siempre se observa la letra A. Y finalmente “02” corresponde al número del puerto de izquierda a derecha en el Media Gateway G650.

Con respecto a las direcciones IP se pueden resumir en la siguiente tabla, la cual representa los IP de la red LAN institucional que se encuentran asignados; a continuación se describe la función de cada una de ellas en el sistema de telefonía IP.

NOMBRE	IP
CLAN1	192.168.14.2
CLAN2	192.168.14.3
CLAN3	192.168.14.4
MEDPRO1	192.168.14.5
MEDPRO2	192.168.14.6
MEDPRO3	192.168.14.7
VAL1	192.168.14.8

Tabla 3.15 Direcciones IP red corporativa UIS tarjetas C-LAN, MEDPRO y VAL.

**a. Tarjetas IP *Media Processor* (MEPRO) TN2302AP**

Se consideran el componente *Gateway* en la estructura de un sistema de VoIP, estas tarjetas se encargan de proveer el soporte para los códecs definidos para ser utilizados por el protocolo H.323. Su principal función es la de proporcionar y procesar el audio del *Media Gateway* para los diferentes canales de voz es decir realizar la conversión entre VoIP y TDM (Multiplexación por división de tiempo) cuando una estación del sistema de VoIP desea acceder a la red de telefonía pública conmutada (PSTN).

Permiten otras funciones como cancelación de eco, supresión de ruido, recepción de señales de fax, módems, detección de tonos DTMF y conferencia.

Dentro de los codecs de audio soportados se encuentran los siguientes:

- G.711 (mu-law o a-law, 64Kbps);

- G.723.1 (6.3Kbps o 5.3Kbps audio);
- G.729A (8Kbps audio), 729, 729B, y 729AB

Se realizaron diversas pruebas usando herramientas de red como *nmap* y no se encontraron puertos abiertos en la interfaz de red conectada a la LAN institucional de estas tarjetas.

### **b. Tarjetas Control LAN (C-LAN) TN799DP**

Es el *Gatekeeper* del sistema de ToIP, esta es una de las tarjetas más importantes del *Media Gateway* puesto que tiene como función proporcionar conectividad TCP/IP entre la red privada de control CNA y la red LAN Institucional, además permite establecer enlaces de VoIP por medio del protocolo H.323 entre las estaciones en el campus de la Universidad; cada tarjeta tiene una capacidad de 500 sockets (Estaciones conectadas) , esto quiere decir que los teléfonos H.323 realizan su conexión al sistema de telefonía IP a través de estas tarjetas y ellas a su vez a los servidores de voz.

Además permite el control de las llamadas para las terminales IP, es decir realiza el direccionamiento de la llamada y lo verifica a diferencia de la tarjeta MEPRO que se encarga de proporcionar los códecs de comprensión para establecer las llamadas.

Por ser una tarjeta que presta servicios en la red LAN Institucional se ejecutó un escaneo de puertos a los IPs de las tarjetas para verificar las condiciones de seguridad y se encontró lo siguiente:

IP	PUERTO	ESTADO	SERVICIO
192.168.14.2	1720/tcp	Open	H.323/Q.931
192.168.14.3	1720/tcp	Open	H.323/Q.931
192.168.14.4	1720/tcp	Open	H.323/Q.931

Tabla 3.16 Puertos abiertos Tarjetas CLAN

De lo cual se concluye que únicamente se tiene activo el servicio H.323 el cual es encriptado y utiliza autenticación por medio del protocolo H.235 y algoritmos de envío de datos como es el *Diffie-Hellman*, lo cual garantiza condiciones de seguridad optimas para la prestación del servicio.

**c. Tarjeta *Voice Announcements over LAN (VAL) TN2501AP***

Esta tarjeta se encarga de los anuncios de audio del sistema sobre LAN, tiene la capacidad de almacenar hasta 1 hora de audio para anuncios, usando un bus TDM, 33 puertos y la capacidad de subir actualizaciones de firmware y archivos de anuncios en formato .wav a través del protocolo FTP.

Siguiendo con el procedimiento se verifica la interface de red usando la herramienta *nmap*, a continuación se muestra un escaneo de puertos para el IP 192.168.14.8

PUERTO	ESTADO	SERVICIO
21/tcp	open	ftp

Tabla 3.17 Puertos abiertos Tarjeta VAL

De lo cual se concluye que la tarjeta VAL tiene configurado únicamente el puerto por defecto para el protocolo FTP (21) el cual a pesar de no ser un protocolo encriptado, no se considera riesgoso pues aquí solo se puede acceder a los anuncios del sistema y además este cuenta con autenticación y log de errores.

**3.2.2.1.3 Otras Tarjetas instaladas**

En la siguiente sección se describirán las tarjetas TN2464CP, TN793CP, TN771DP, TN747B las cuales tienen funciones importantes en la conectividad de Media Gateways pero solo serán descritas brevemente debido a que no hacen parte del objetivo de este proyecto.

**a. Interfaz DS1 TN2464CP**

Este dispositivo permite introducir troncales digitales a nuestro conmutador a través de una línea de servicios digitales ISDN se encuentran instaladas en los siguientes sockets de los Media Gateways

<b>Tarjeta</b>	<b>M. Gateway</b>	<b>Puerto</b>
DS1 TN2464CP	1	11
DS1 TN2464CP	1	12
DS1 TN2464CP	1	13
DS1 TN2464CP	2	12
DS1 TN2464CP	2	13
DS1 TN2464CP	3	12
DS1 TN2464CP	3	13

Tabla 3.18 Puertos de Instalación de DS1 TN2464CP

**b. Tarjeta TN793CP para líneas Analógicas**

Esta tarjeta de líneas análogas cuenta con 24 puertos y soporta las siguientes características:

- Teléfonos con identificador de llamadas
- Fax
- Llamadas por pulsos (DTMF)
- Tiempo de flash programable
- Llamada en espera
- Contestador automático entre otros.

Se encuentran instaladas en los siguientes sockets de los *Media Gateways*

<b>Tarjeta</b>	<b>M. Gateway</b>	<b>Puerto</b>
TN793CP	1	5
TN793CP	2	3
TN793CP	2	4

TN793CP	3	3
TN793CP	3	4

Tabla 3.19 Puertos de Instalación de TN293CP

**c. Tarjeta de mantenimiento y prueba TN771DP**

Se encarga de realizar tareas de mantenimiento; su función es la de diagnosticar y corregir fallas en el bus de paquetes, se encuentra instalada en los siguientes sockets de los *Media Gateways*.

Tarjeta	M. Gateway	Puerto
TN771DP	1	3

Tabla 3.20 Puertos de Instalación de TN771DP

**d. Tarjeta de troncales digitales TN747B**

Tarjeta de troncales digitales que soporta hasta 8 troncales de conexión la cual permite enrutar e interconectar el trafico del campus principal con las sedes regionales de la Universidad, se encuentran instaladas en los siguientes sockets de los *Media Gateways*.

Tarjeta	M. Gateway	Puerto
TN747B	1	10
TN747B	3	10
TN747B	2	10

Tabla 3.21 Puertos de Instalación de TN747B

**3.2.2.2 Conexiones de la parte posterior de los *Media Gateways* G650**

Para complementar la documentación de lo mencionado anteriormente, en la siguiente figura se muestran las conexiones posteriores actuales de los *Media Gateways* G650 de la Universidad.

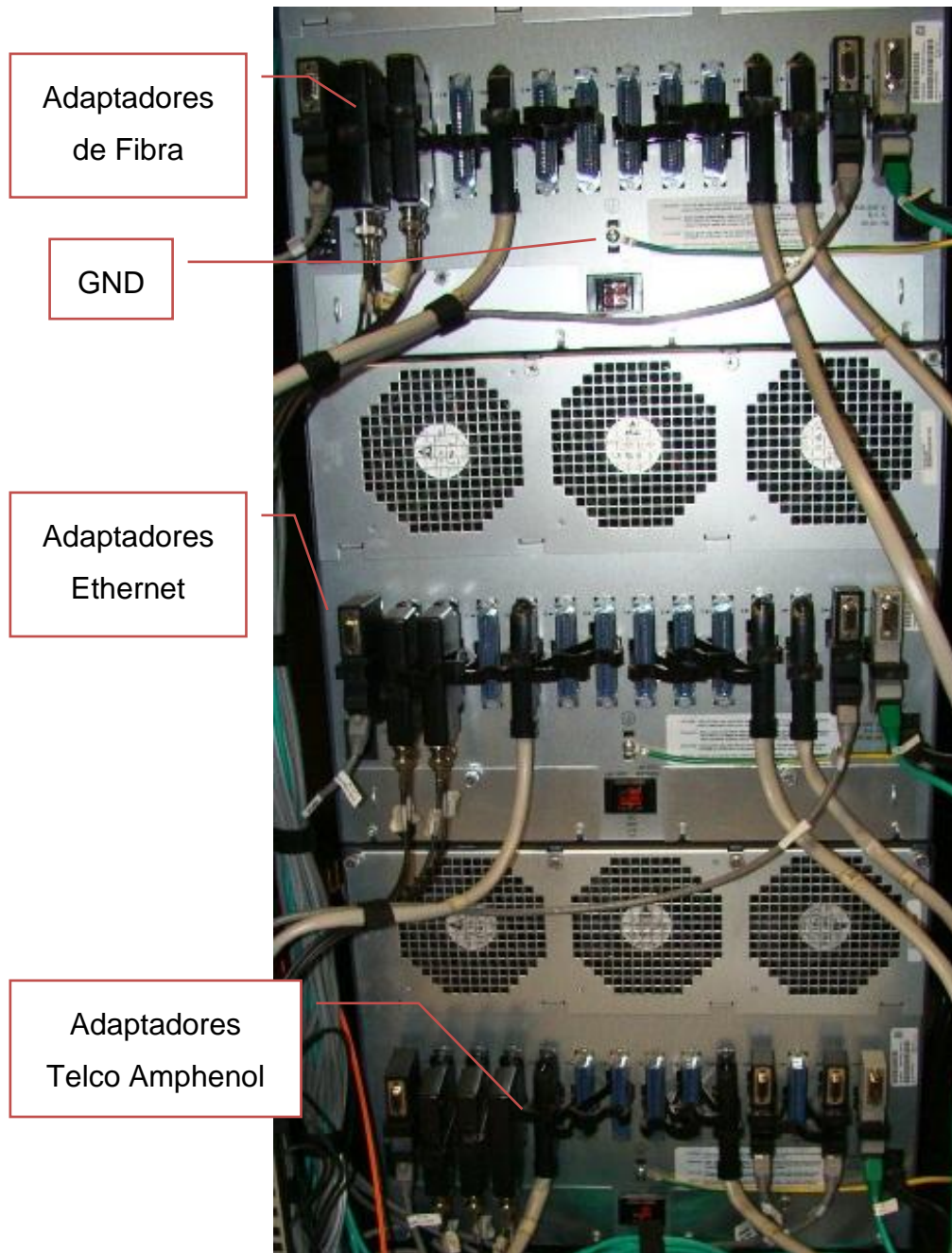


Figura 3.16 Foto de conexiones posteriores de los *Media Gateways G650*<sup>1</sup>.

<sup>1</sup> Foto tomada por el autor con autorización de la DSI.

En ella se pueden observar los conectores *Telco Amphenol*, las líneas de fibra óptica y los adaptadores de Ethernet RJ45 conectados a las tarjetas que hacen parte de los *Gateways* descritos anteriormente.

### 3.2.3 Switch de red.



Figura 3.17 Foto Switch 3COM 4500G 24 puertos instalado actualmente<sup>1</sup>.

La universidad cuenta con un Switch de red marca 3COM 4500G de 48 Puertos dispuesto con el objetivo general de centralizar las conexiones de todos los dispositivos del rack de VOIP, a nivel específico el equipo se encarga de permitir el tráfico de las señales de la red de control A (CNA) la cual conforma el núcleo del sistema pues interconecta los servidores S8730 con los Media Gateway G650, también se encarga de permitir la interconexión de los equipos de VoIP con la red WAN de la universidad a través de los dos enlaces de fibra óptica que hay entre el Switch 3COM y el Switch principal Extreme Network BD 8806 de la Universidad.

El Switch 3COM cuenta con características específicas con la finalidad de cumplir con los requisitos exigidos por el sistema de ToIP de AVAYA por lo cual se encuentra configurado con soporte de protocolos como son Qos (*Quality of service*) y VLANs, pues el sistema requiere una latencia máxima de 50 ms y pérdidas de paquetes inferiores al 0.2% para las conexiones de red internas con objeto de evitar fallas de comunicación y pérdida de calidad en las comunicaciones de Voz IP.

---

<sup>1</sup> Foto tomada por el autor con autorización de la DSI.

Con respecto al soporte de VLANs hay que aclarar que estas se crean con el objetivo de independizar el tráfico de voz, del de datos de la universidad. A nivel de configuración del switch también se crean con el objetivo de independizar dos subredes en el mismo equipo, en este caso específico la existencia de la red de control (Red privada) y la subred publica perteneciente a la LAN Institucional.

Para visualizar esta información se ingresa a la página de administración del Switch la cual corresponde a <http://192.168.5.130> de la cual se puede extraer la siguiente figura.

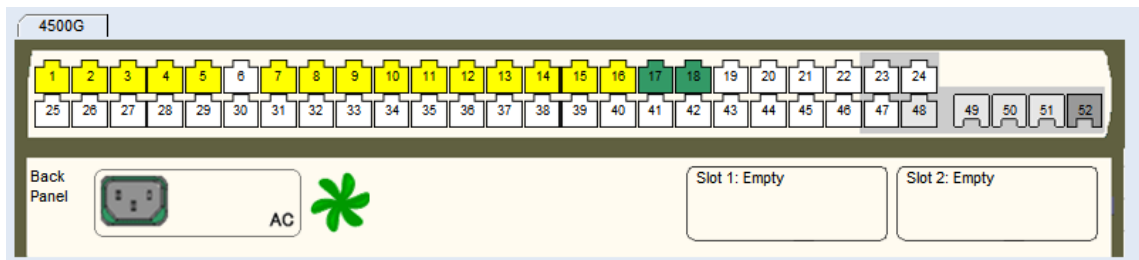
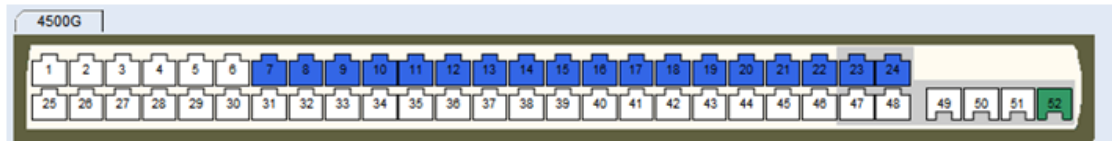


Figura 3.18 Diagrama de puertos utilizados en el Switch 3COM 4500G.

En la cual se puede observar el puerto 52 el cual corresponde al conector de fibra óptica SFP 1000 BaseSX además en color amarillo y verde los puertos activos en el switch los cuales se dividen en dos grupos los que corresponden a la red pública (Institucional) y los que corresponden a la red privada de control A, conocer los puertos activos para cada VLAN creada es importante porque permite realizar cambios en las conexiones sin afectar la conectividad de los equipos.

En la Figura 3.19 se representa la configuración de puertos del switch para las dos VLANS configuradas correspondientes a la VLAN 114 la cual representa la subred con rango IP 192.168.14.0/24 y la VLAN 14 la cual conforma la red de control A y representa la subred con rango IP 172.18.20.0/24.

PUERTOS VLAN 114



PUERTOS VLAN 14

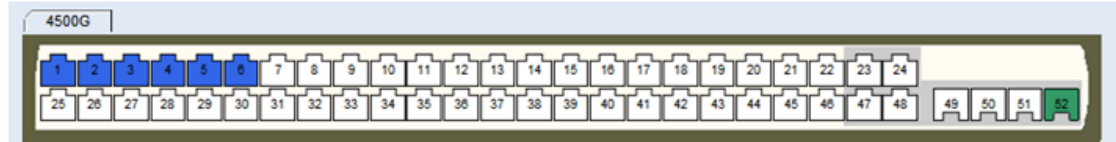


Figura 3.19 Puertos asignados a las VLAN 14 y 114.

Como se puede observar se encuentran demarcados en color azul los puertos asignados para cada VLAN lo cual es importante tener en cuenta a la hora de realizar alguna modificación en las conexiones del switch como se mencionó anteriormente.

Para finalizar la documentación del switch se anexa la descripción física la cual es la siguiente:

Equipo	Peso(Kg)	Dimensiones (Cm)	Unidades
Switch 3COM 4500G	4	4.3 x 44 x 30	1

Tabla 3.22 Descripción física Switch 3COM 4500G 48 puertos

Hay que agregar que en este trabajo, en el Capítulo 5 se describen procedimientos para realizar la configuración de este Switch y los que se encuentran a nivel de campus principal en la universidad.

### 3.2.4 Configuración Servidor protocolo SIP



Figura 3.20 Foto Servidor SIP AVAYA S8500<sup>1</sup>

El protocolo SIP se encuentra a cargo del servidor AVAYA S8500 el cual está diseñado para brindar gran variedad de servicios entre ellos el de ser Servidor de Voz IP para entornos de producción más pequeños que el S8730, pues este no cuenta con opciones de alta confiabilidad contra fallas como son redundancia de discos, memoria, etc.

En el caso específico de la Universidad Industrial de Santander este se encarga de prestar el servicio de telefonía usando el protocolo SIP<sup>2</sup>, el cual permite ampliar el rango de equipos de telefonía que pueden ser conectados e incrementa la gama de servicios que el sistema de ToIP puede ofrecer, ya que el SIP además de ser libre, admite su uso en equipos de escritorio, portátiles, ultra portátiles, celulares y otros equipos de comunicación en redes locales e inalámbricas dentro o fuera del Campus<sup>3</sup> de la Universidad que tengan las capacidades de usar este protocolo y/o instalar una aplicación de software cliente (Softphone) compatible con este protocolo; dentro de estos se resalta el software libre X-lite, y los teléfonos Wifi de AVAYA.

Además se destaca que este servidor se encuentra configurado como cliente del servidor S8730 pues depende de él para la asignación de recursos (extensiones, permisos y privilegios de los usuarios), de tal forma que se considera un traductor de protocolo del H323 al SIP, por lo cual a pesar de que el sistema de licenciamiento SIP es libre, en este caso se encuentra restringido por las capacidades de licenciamiento establecidas en el Servidor S8730 para el protocolo H323 adquirido por la Universidad.

Hay que tener presente que el servidor AVAYA S8500 corresponde internamente al equipo fabricado por la compañía *IBM referencia e-server mSeries 306*, esto

---

<sup>1</sup> Foto tomada por el autor con autorización de la DSI.

<sup>2</sup> Protocolo de Inicio de Sesiones.

<sup>3</sup> Usando una VPN (*Virtual Private Network*), para permitir dicha conexión.

debido a que hay que recordar que AVAYA no es una empresa especializada en hardware de servidores y se apoya de compañías con experiencia en este campo para soportar esta gama de productos y ofrecer soporte.

### 3.2.4.1 Características Técnicas y condiciones ambientales

El servidor cuenta con las siguientes características técnicas y condiciones ambientales de operación:

Parámetro	Descripción
Temperatura ambiente de operación	50°F to 95°F (10°C to 35°C)
Humedad (operativo)	8% al 80% (Sin condensación)
Tension de alimentación	100 a 132 VAC
Frecuencia Tension de entrada	60 Hz
Corriente alimentación	10 A at 100 VAC
Potencia	370 W at 120V AC input
BTUs por hora	512
Microprocesador	Intel Pentium IV 3.2 GHZ
Memoria	1 GB
Unidades (SCSI y SATA)	80 GB 7200 RPM
	CD-ROM/DVD-ROM: 24x Max.
	Disquete 1.44MB
Tarjeta de red	2 Puertos 100/1000Gb Ethernet
	Conector para teclado
	Conector para Mouse
	4 puertos USB
	Conector de video

Tabla 3.23 Rangos de operación y características técnicas básicas.

En cuanto a características de hardware el servidor AVAYA S8500 está equipado con un procesador Pentium 4 de 3.2 Ghz y para almacenar el sistema operativo tiene instalado un único disco duro SATA de 80GB además posee 1Gb de memoria RAM dispuesta en dos tarjetas DDR de 512 MB.

El servidor S8500 no cuenta con sistemas de redundancia instalados sin embargo integra un sistema implementado por software llamado Disco RAM, el cual consiste en una parte de memoria RAM usada como partición física la cual le permite al equipo continuar funcionando normalmente durante máximo 72 horas en caso de que el disco duro presente alguna falla.

Además posee las siguientes dimensiones y peso:

Equipo	Peso(Kg)	Dimensiones (Cm)	Unidades
Servidor S8510	18	4.3 x 48.3x 26	1

Tabla 3.24 Servidor SIP S8500

### 3.2.4.2 Configuración de red Servidor S8500

El servidor S8500 cuenta con 4 interfaces de red físicas para permitir la conectividad con los diversos equipos que conforman el núcleo del sistema.

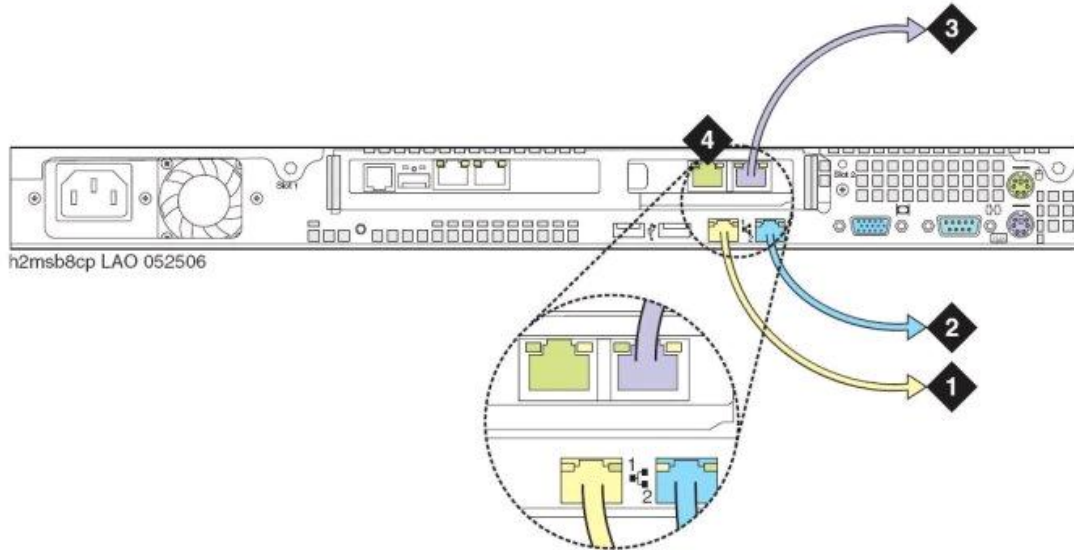


Figura 3.21 Diagrama de Interfaces de red Servidor SIP AVAYA S8500<sup>1</sup>

1. eth0 — Interfaz conectada a la red LAN Institucional.
2. eth1 —Interfaz de servicio para conexión con equipo de administración.
3. eth3 — No utilizada en este entorno.
4. eth4 — No Utilizada en este entorno.
5. Eth2 – No mostrada en la figura

A continuación se explicará cada una de ellas:

### **Eth 0**

Interfaz conectada a la red LAN institucional en donde provee los servicios de SIP.

### **Eth1 (inactiva)**

Corresponde la interfaz de servicio del sistema y solo es utilizada en momentos en que la administración remota no es posible o en los primeros pasos de instalación del servidor véase [7].

### **Eth2 (no Usada)**

Corresponde a una interfaz de red provista por la tarjeta de administración SAMP la cual tiene como finalidad permitir diagnostico, monitorear alarmas, tomar control del equipo incluso además esta tarjeta cuenta con alimentación independiente lo que permite encender el equipo y apagar el equipo de forma remota, este sistema no está activado en esta configuración.

---

<sup>1</sup> Sims, Jamie. Jaymzworld. [En línea] Technical Manager, Avaya Inc. [Citado el: 6 de 5 de 2010.] [http://jaymzworld.com/wiki/Server\\_ports\\_and\\_IP\\_addresses](http://jaymzworld.com/wiki/Server_ports_and_IP_addresses).

### Eth3 y Eth4 (inactiva)

Corresponden a una interfaz de red disponible para futuras ampliaciones del sistema o para la instalación de un sistema de redundancia más avanzado.

De lo anterior se resume que el servidor solo cuenta con una interface de red activa y una con la finalidad de realizar la instalación inicial del sistema. Los datos de IP se muestran en la siguiente tabla:

Interfaz	IP	Descripción	Estado
Eth0	192.168.14.20	Interfaz de red conectada a red Institucional	Activa
Eth1	192.11.13.6	Interfaz de Servicios	Inactiva

Tabla 3.25 Configuración de red servidor S8500

Por ser un servidor que se encuentra conectado a la red LAN Institucional, se usa la herramienta nmap en busca de puertos abiertos desde el puerto 1 al 65535 al IP 192.168.14.20 el cual corresponde al IP del Servidor SIP; los resultados se observan en la Tabla 3.26.

PUERTO	ESTADO	SERVICIO
80/tcp	open	http
443/tcp	open	https
5060/tcp	open	sip

Tabla 3.26 Puertos abiertos del Servidor SIP usando escaneo de puertos desde otro servidor.

De la lista mostrada se destacan el puerto 80 y 443 que corresponden al servicio Web el cual permite administrar el sistema de modo grafico y el puerto 5060 el cual corresponde al servicio SIP al cual se conectan *softphones*.

#### 3.2.4.3 Sistema Operativo

El servidor posee instalada la distribución de *Linux RedHat* la cual se encuentra optimizada con soporte de hardware embebido en el *Kernel* del sistema lo que

garantiza estabilidad y rendimiento durante la ejecución de los servicios SIP usando el software SES 5.1.

### 3.2.4.4 Interconexión con el Servidor de Voz.

Como se mencionó al principio de esta sección, el Servidor SIP AVAYA S8500 cumple la función de traductor de protocolo del H.323 ofrecido por el sistema de ToIP al protocolo SIP, para realizar esto el Servidor SIP debe encontrarse en sincronismo con el Servidor Voz. A continuación se presentan algunos parámetros interesantes referente a esta configuración, en este caso el Servidor SIP debe autenticarse en el Servidor de Voz para a obtener la información de la base de datos de extensiones y políticas de usuarios.

Por lo cual debe configurarse usando la interfaz WEB como se muestra a continuación.

#### Add Communication Manager Server Interface

Communication Manager Server Interface Name*	Voz - UIS
Host	192.168.14.20 <span style="font-size: 0.8em;">▼</span>
<b>SIP Trunk</b>	
SIP Trunk Link Type	<input type="radio"/> TCP <input checked="" type="radio"/> TLS
SIP Trunk IP Address*	192.168.14.2
<b>Communication Manager Server</b>	
Communication Manager Server Admin Address* (see Help)	192.168.14.10
Communication Manager Server Admin Port*	5022
Communication Manager Server Admin Login*	dadmin
Communication Manager Server Admin Password*	••••••
Communication Manager Server Admin Password Confirm*	••••••
<b>SMS Connection Type</b>	<input checked="" type="radio"/> SSH <input type="radio"/> Telnet <input type="radio"/> Not Available

Note: If the Communication Manager Serve changed,changing connection type to SSH connection type to Telnet will change adm

Fields marked \* are required.

Add

Figura 3.22 Configuración Web en Servidor SIP para lograr interconexión con Servidor de Voz.

De la Figura 3.22 se resalta el IP del host que corresponde al IP del sistema SIP, la troncal SIP la cual es la que se encarga de realizar el enlace de las extensiones H.323, y la PSTN con las extensiones SIP, también se configura el enlace con la base de datos del CM en el Servidor de Voz, para esto se configura el IP activo del servidor, y los datos de cuenta administrador para permitir al sistema SIP contar con los privilegios necesarios al establecer conexión directa con el Servidor de Voz.

Finalmente, en el Servidor de Voz debe existir el nodo configurado apuntando al IP del Servidor SIP como se puede observar en la Figura 3.7 para permitir redireccionar las llamadas cuando sea necesario, esto quiere decir cuando el Servidor de Voz detecta que la extensión a donde se dirige la llamada es de tipo SIP y no H323.

El objetivo de este capítulo es explicar el modo en que el Servidor SIP y el Servidor de Voz establecen conexión con objeto de cumplir con sus funciones, para procedimientos de configuración más avanzados consultar [7] donde se muestran todos los parámetros de configuración del Servidor SIP.

### 3.2.5 Descripción Módems



Figura 3.23 Foto Dos Módems Externos USB *Multitech*<sup>1</sup>.

Cada uno de los servidores AVAYA S8730 y S8500 se encuentran conectados adicionalmente a una línea telefónica analógica independiente al sistema de ToIP por medio de un Modem USB *Multitech* referencia *MultiModemUSB* con el objeto de permitir mantenimientos y diagnósticos remotos, el modem se encuentra configurado de tal forma que el servidor contesta las llamadas entrantes y permite al usuario remoto el acceso a una terminal de comandos previa autenticación para administrar el sistema.

La configuración de estos dispositivos se realiza automáticamente en los respectivos servidores luego de ser conectados a uno de los puertos USB disponibles por lo que no hay parámetros para mostrar.

### 3.2.6 Descripción del Tarifificador Dalí Enterprise

---

<sup>1</sup> Foto tomada con autorización de la DSI.



Figura 3.24 Foto Servidor *Dalí Enterprise* HP DL380 G5 Series<sup>1</sup>.

Este servicio se encuentra instalado en un servidor HP DL380 G5 Series, el cual se encarga de prestar el servicio de control y tarificación de las llamadas al sistema de VoIP a través de un software llamado *DALI ENTERPRISE*.

Este software desarrollado por CALLTECH, se encuentra instalado sobre plataforma Windows 2003 server, y su función consiste en permitir monitorear el tráfico de la red enfocado a registrar los diferentes consumos de llamadas de voz IP por parte de las estaciones, con objeto de hacer ajustes, evaluar el funcionamiento del sistema y además de llevar un registro de seguridad de las llamadas realizadas. Este es quizás el único servidor del rack de VoIP instalado sobre el sistema operativo Windows.

Actualmente el servidor cuenta con soporte con CALLTECH por 4 años en cuanto a software y soporte de 3 años de garantía para hardware con HP.

### 3.2.6.1 Características Técnicas y condiciones ambientales

El servidor cuenta con las siguientes características técnicas y condiciones ambientales de operación:

Parámetro	Descripción
Temperatura ambiente de operación	50°F to 95°F (10°C to 35°C)
Humedad (operativo)	8% al 80% (Sin condensación)
Tensión de alimentación	100 a 132 VAC
Frecuencia Tensión de entrada	60 Hz

<sup>1</sup> Foto tomada con autorización de la DSI.

Corriente alimentación	10 A at 100 VAC
Potencia	370 W at 120V AC input
BTUs por hora	600
Microprocesador	Quad-Core Xeon E5405 / 2 GH
Memoria	1 GB
Unidades (SCSI y SATA)	72GB 10K RPM SAS SFF
	CD-ROM/DVD-ROM: 24x Max.
	Disquete 1.44MB
Tarjeta de red	
	2 Puertos 100/1000Gb Ethernet
	Conector para teclado
	Conector para Mouse
	4 puertos USB
	Conector de video

Tabla 3.27 Rangos de operación y características técnicas básicas.

### 3.2.6.2 Configuración de red Servidor

Este servidor solo cuenta con una única interface de red para prestar sus servicios al sistema de ToIP, la configuración puede observarse en la siguiente tabla:

Interfaz	IP	Descripción	Estado
Eth0	192.168.14.16	Interfaz de red conectada a red Institucional	Activa

Tabla 3.28 Interfaz de red servidor Tarifador Dalí Enterprise

Esta interfaz tiene como objetivo permitir la conectividad del sistema con la red corporativa de la Universidad y prestar los servicios descritos al inicio de esta sección. Por seguridad se realiza un análisis de puertos para verificar los servicios adicionales que pueda estar prestando este equipo. Los resultados se muestran a continuación.

PUERTO	ESTADO	SERVICIO
80/tcp	open	http
135/tcp	open	msrpc
139/tcp	open	netbios-ssn

445/tcp	open	microsoft-ds
1025/tcp	open	NFS-or-IIS
1433/tcp	open	ms-sql-s
2010/tcp	open	search
2301/tcp	open	compaqdiag
5010/tcp	open	telepathstart
5800/tcp	open	vnc-http
5900/tcp	open	vnc

Tabla 3.29 Puertos abiertos de red del servidor Dalí Enterprise

En la Tabla 3.29 se observan los puertos abiertos para el IP 192.168.14.16, de los cuales se destaca el puerto 80 para administración vía Web, y los puertos 5800 y 5900 que permiten la conexión remota al escritorio del equipo y el 5010 el cual es quien recibe los datos del servidor de voz, la aplicación de este puerto será descrita en la sección 3.2.6.3 que sigue a continuación.

### **3.2.6.3 Interconexión con el Servidor de Voz**

Finalmente con base en lo anterior se puede concluir que este servidor trabaja como cliente del sistema de VoIP, ya que es de aclarar que el Servidor de Voz es quien se encarga de controlar y registrar todos los sucesos que ocurren en el sistema; más sin embargo este no se encuentra diseñado para permitir el acceso de forma clara y ordenada a esta información por lo cual el Servidor de Tarificación cumple la labor de registrar los datos almacenarlos, clasificarlos y con base en esto generar informes, para realizar posteriores análisis.

Por lo cual es importante explicar la configuración que permite establecer esta interconexión. Como se mostró en la Tabla 3.29 este equipo cuenta con diversos servicios para cumplir con sus funciones los cuales habilitan puertos de red, entre ellos se encuentra el puerto 5010 el cual se considera un puerto de escucha y se encarga de recibir la información procedente del Servidor de Voz a través de la red.

El Servidor de Voz se encarga de enviar la información con un formato específico usando un servicio llamado CDR (*Call Detail Recording*) el cual se encarga de registrar, filtrar, organizar y enviar las estadísticas de llamadas a otro servidor a través de un nodo configurado, en este caso específico el software *Dalí Enterprise* que a pesar de no ser desarrollado por la compañía AVAYA tiene la capacidad de recibir, interpretar y analizar la información siempre y cuando se cumpla con unos parámetros de configuración que el software Dalí requiere.

Es por esto que en esta sección se verifica la configuración del Servidor de Voz orientado a mostrar la interconexión del sistema pues se considera importante en el proceso de documentación, por lo cual usando el comando `change system-parameters cdr` en CM se puede obtener la información mostrada en la figura a continuación.

```

change system-parameters cdr                                     Page 1 of 2
                                CDR SYSTEM PARAMETERS

Node Number (Local PBX ID): 1                                CDR Date Format: month/day
Primary Output Format: customized                            Primary Output Endpoint: CDR1
Secondary Output Format: _____
Use ISDN Layouts? n                                         Enable CDR Storage on Disk? n
Use Enhanced Formats? n                                     Condition Code 'T' For Redirected Calls? n
Use Legacy CDR Formats? y                                   Remove # From Called Number? n
Modified Circuit ID Display? n                               Intra-switch CDR? y
Record Outgoing Calls Only? n                               Outg Trk Call Splitting? y
Suppress CDR for Ineffective Call Attempts? y               Outg Attd Call Record? y
Disconnect Information in Place of FRL? n                   Interworking Feat-flag? n
Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n

Inc Trk Call Splitting? y                                   Inc Attd Call Record? y
Record Non-Call-Assoc TSC? n                               Call Record Handling Option: warning
Record Call-Assoc TSC? n                                   Digits to Record for Outgoing Calls: dialed
Privacy - Digits to Hide: 0                                CDR Account Code Length: 15
  
```

Figura 3.25 Comando `change system-parameters cdr` en CM 5.0

En la Figura 3.25 se pueden observar múltiples parámetros del formato de envío de información los cuales son tratados en detalle en la documentación de AVAYA [5] más sin embargo es importante resaltar la opción Primary Output Endpoint: CDR1 la cual se encarga de indicar hacia donde deben ir los datos registrados por el Servidor de Voz en este caso CDR1 la cual posteriormente es configurada y registrada usando el comando `change ip-services` como se muestra en la Figura 3.26.

```
change ip-services Page 1 of 3
```

IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
CDR1		CLAN1	0	DALI	5010
SAT	Y	CLAN1	5111	any	0

Figura 3.26 Comando chane ip-services en CM 5.0

En donde se define hacia donde se deben re-direccionarse los datos que llegan al servicio CDR1 como se puede observar en este caso, a través de la tarjeta CLAN1 al puerto 5010 del nodo llamado DALI el cual tiene configurada la dirección IP 192.168.14.16 como se puede observar en la Figura 3.7 de la sección 3.2.1.6

### 3.2.7 Descripción del servidor que presta el servicio de Intuity Audix



Figura 3.27 Foto Servidor S3210R que presta el servicio de Intuity AUDIX<sup>1</sup>.

El servicio AUDIX (*For the audio Information Exchange*) es prestado por el servidor AVAYA S3210R, el cual consiste en un sistema de mensajería centralizado e integrado al sistema de telefonía IP el cual permite el transporte de mensajes entre Fax, Voz IP y E-mail.

Tiene la capacidad de almacenar 500 horas de audio y hasta 1200 buzones de correo lo cual está dentro de las necesidades de la Universidad y se encuentra instalado bajo Linux RedHat sobre el cual se encuentra instalado el software AUDIX INTUITY LX Release ia2.0-11.2

Dentro de las funciones básicas se encuentran:

- Contestar varios teléfonos al mismo tiempo
- Almacenar los mensajes de voz en casillas personalizadas asociadas al número del usuario.
- Reenviar los mensajes hacia otras casillas
- Personalizar el mensaje de introducción
- Enviar mensajes a varios destinatarios a la vez
- Guardar mensajes para enviarlos en otro momento
- Notificar al destinatario mediante una llamada o correo electrónico que le ha llegado un mensaje a su casilla de voz
- Transferir llamados hacia otro número telefónico
- Reproducir diferentes mensajes de introducción a la casilla de acuerdo a quien se comunique
- Proveer seguridad y confidencialidad, ya que para acceder al mismo se debe introducir una clave, de manera que sólo el usuario pueda escuchar los mensajes

---

<sup>1</sup> Foto tomada con autorización de la DSI

- Dar a conocer la fecha y hora de los mensajes, y el número telefónico desde el que se recibe.

Este tipo de servidores de tipo modular fue integrado por AVAYA a partir del año 2003, con el objetivo de permitir escalabilidad y facilidad de integración del sistema, pues antes de esto, este servicio estaba integrado al servidor S8700 lo cual le restaba rendimiento.

A continuación se presentan las características de este equipo tanto de hardware como físicas y las condiciones ambientales de funcionamiento:

### 3.2.7.1 Características Técnicas y condiciones ambientales

El servidor cuenta con las siguientes características técnicas y condiciones ambientales de operación:

Parámetro	Descripción
Temperatura ambiente de operación	50°F to 95°F (10°C to 35°C)
Humedad (operativo)	20% al 80% (Sin condensación)
Tension de alimentación	100 a 132 VAC
Frecuencia Tension de entrada	60 Hz
Corriente alimentación	6 A at 100 VAC
Potencia	370 W at 120V AC input
BTUs por hora	1123
Microprocesador	Intel Celeron 2Ghz
Memoria	512 MB
Unidades (IDE)	40 GB 7200 RPM
	DVD-RW
	Disquete 1.44MB
Tarjeta de red	2 tarjetas de 4 líneas analógicas
	2 Puertos 100/1000Gb Ethernet
	Conector para teclado
	Conector para Mouse
	4 puertos USB
	Conector de video

Tabla 3.30 Rangos de operación y características técnicas básicas.

Además presenta las siguientes características físicas.

Equipo	Peso(Kg)	Dimensiones (Cm)	Unidades
S3210	18.3	17x43.3x52	1

Tabla 3.31 Características físicas servidor S3210R

### 3.2.7.2 Configuración de red Servidor

Este servidor solo cuenta con una única interface de red para prestar sus servicios al sistema de VoIP, la configuración puede observarse en la siguiente tabla:

Interfaz	IP	Descripción	Estado
Eth0	192.168.14.15	Interfaz de red conectada a red Institucional	Activa

Tabla 3.32 Configuración de red servidor S3210

Esta interfaz se encarga de brindar la conectividad del servidor con la red corporativa de la universidad y brindar los servicios descritos al inicio de este numeral en sincronismo con el Servidor de Voz.

Como se ha venido ejecutando para todas las interfaces que se encuentran conectadas a la red LAN institucional, se hace uso de la herramienta *nmap* y se ejecuta un escaneo de puertos para verificar los puertos abiertos del sistema para el IP 192.168.14.15 los resultados se muestran en la Tabla 3.33.

PUERTO	ESTADO	SERVICIO
22/tcp	open	SSH
23/tcp	open	telnet
25/tcp	open	smtp
80/tcp	open	http
110/tcp	open	pop3
111/tcp	open	rpcbind
143/tcp	open	imap
161/tcp	filtered	snmp
162/tcp	filtered	snmptrap
443/tcp	open	https

465/tcp	open	smtps
993/tcp	open	imaps
995/tcp	open	pop3s
5500/tcp	open	hotline

Tabla 3.33 Puertos abiertos del servidor usando escaneo de puertos desde otro servidor.

De la Tabla 3.33 se puede destacar que los servicios SSH, telnet, http, https son puertos disponibles para administración del sistema, los servicios pop3, imap, snmp, snmptrap, smtps, imaps, pop3s, son dedicados para prestar los servicios de mensajería unificada por medio de correo electrónico, y software de mensajería compatible.

### 3.2.7.3 Interconexión con el Servidor de Voz

El servidor AUDIX como se introdujo en la sección 3.2.1.6 requiere estar configurado en el Servidor de Voz con el objetivo que este re-direccione las llamadas a los respectivos buzones de voz del sistema. Un ejemplo de ese caso es cuando se llama a un usuario y este no contesta, o se realiza desde el teléfono una consulta de buzón de voz.

A continuación se presenta la configuración orientada a mostrar la interconexión entre estos dos servidores.

En el Servidor de Voz, se encuentra configurado un nodo de tipo AUDIX con el mismo nombre, con el objeto de sincronizar la base de datos del sistema de Mensajería referente a números de buzón de voz (extensiones) con el Servidor de Voz como, se observa en la figura a continuación.

```
display node-names audix
                                AUDIX NODE NAMES
Audix Names   IP Address
audix        192.168.14 .15
              . . .
```

Figura 3.28 Comando `display node-names audix`

Este nodo le indica al sistema que se cuenta con un equipo independiente dedicado al sistema de Mensajería Unificada, pero adicionalmente debe configurarse como una extensión física a la cual el sistema re-direccionará las llamadas, para lo cual el CM integra la opción *Hunt-group* la cual se encarga de administrar y permite la transferencia de llamadas de forma automática a la extensión configurada, en este caso el grupo 1900 conformado internamente por 8 extensiones adicionales o canales para conectarse con el sistema de mensajería. En la Figura 3.29 se muestra esta configuración.

```

change hunt-group 1                                     Page 1 of 60
                                     HUNT GROUP
Group Number: 1                                         ACD? n
Group Name: audix                                       Queue? y
Group Extension: 1900                                   Vector? n
Group Type: ucd-mia                                     Coverage Path: _____
TN: 1                                                   Night Service Destination: _____
COR: 1                                                  MM Early Answer? n
Security Code: _____                             Local Agent Preference? n
ISDN/SIP Caller Display: _____

Queue Limit: unlimited
Calls Warning Threshold: _____ Port: _____
Time Warning Threshold: _____ Port: _____

LWC Reception: none                                    AUDIX Name: audix
First Announcement Extension: _____               Delay (sec): __

Message Center: audix

Message Center AUDIX Name: audix
Primary? n
Calling Party Number to INTUITY AUDIX? n
  
```

Figura 3.29 Configuración hunt-group 1

De la cual se destacan los campos *Message center*, *AUDIX name* y *Message Center AUDIX Name*, los cuales indican la conexión con el nodo llamado AUDIX previamente configurado y apuntando al IP 192.168.14.15 como se observa en la Figura 3.28, lo que permite la interconexión de estos dos servidores tanto por el

grupo de extensiones 1900 (para el re-direccionamiento de llamadas), como por el nodo AUDIX (para la sincronización de la base de datos de estaciones).

## 4 EVALUACIÓN, ANÁLISIS DE CONEXIONES Y DE CONFIGURACIÓN

En el siguiente capítulo se realiza un análisis crítico de la instalación el sistema de ToIP, con objeto de proponer futuras modificaciones que pueden ser implementadas, con procedimientos que permiten mejorar el sistema de ToIP instalado actualmente. Este capítulo se divide en secciones de acuerdo a los equipos evaluados durante la práctica.

Al igual que todo el documento, este capítulo se centra principalmente en analizar los servidores de voz y *Gateways*, evaluando su sistema de configuración y conexiones, teniendo presente como principal objetivo mejorar el funcionamiento, la estabilidad y estudiando los actuales sistemas de contingencia instalados.

### 4.1 Servidores de Voz AVAYA S8730

Con respecto a los servidores de voz del sistema de ToIP, se encontró durante la práctica que cada servidor solo cuenta con un disco duro conectado al sistema lo cual imposibilita el uso de los beneficios de un sistema RAID<sup>1</sup>, el cual permitiría mayor integridad de la información, mayor tolerancia a fallos y mayor *throughput*. Los servidores S8730 soportan configuración RAID 1 el cual al ser implementado permitirá que ambos discos trabajen de forma independiente, cada uno como espejo del otro (quiere decir con duplicidad en la información), e incrementar la velocidad de lectura de datos en un factor cercano a dos, como también la seguridad de la información garantizando la estabilidad del sistema incluso si uno de los discos duros presenta una falla y permitiendo operaciones como realizar el cambio de un disco duro sin necesidad de apagar el sistema (Hot-Plug).

---

<sup>1</sup> Se refiere a conjunto redundante de discos independientes.

A pesar de que el sistema cuenta con un robusto sistema de duplicación a nivel de equipo completo (véase sección 3.2.1.5.1), cada servidor de manera independiente no cuenta con un sistema RAID de discos para garantizar total confiabilidad del sistema en caso de que un disco duro salga de servicio, esta característica podrá ser agregada en cualquier momento debido a que no hay que realizar mayor labor técnica para activarla. Los servidores S8730 instalados con *Communication Manager 5.0* reconocen cuando es instalado el segundo disco en la bahía 2 y automáticamente realiza la sincronización y activación del RAID en nivel 1, la cual es una gran ventaja que incluye AVAYA sobre equipos de la competencia. Ya que en los equipos servidores comunes esto no sucede, pues hay que volver a instalar todo el SO (Sistema Operativo) al realizar cambios en el sistema de arreglo de discos RAID debido a que hay pérdida total de información cuando esto sucede, lo cual imposibilita la activación de esta característica en un ambiente de producción.

## 4.2 Media Gateways G650

Durante esta práctica se observó que los Gateways en el sistema de VoIP no cuentan con ningún sistema de contingencia ante una falla lo cual representa un problema de confiabilidad en la prestación del servicio de telefonía. Según documentación consultada se encontró que existe un sistema de redundancia que ofrece mayor confiabilidad y es recomendado para este caso el cual se implementa usando una segunda red de control (CNB) conformada por un switch y un Gateway adicional; para el caso específico de la Universidad. Luego de la práctica se ha diseñado un esquema de la posible estructura de conexión y de nueva instalación.

En la

Figura 4.1 se observa el diseño de una nueva configuración de conexiones para el sistema de ToIP de la universidad, el cual ofrece una confiabilidad mucho más alta según documentación del 99.99% [9], pues incluye dos redes de control (CNA y

CNB) capaces de administrar el sistema de ToIP. Adicionalmente se integra un Gateway adicional con los mismos componentes que se encuentran instalados actualmente, para que realice la función de equipo espejo en caso de que cualquiera de los componentes del otro Gateway presente algún problema.

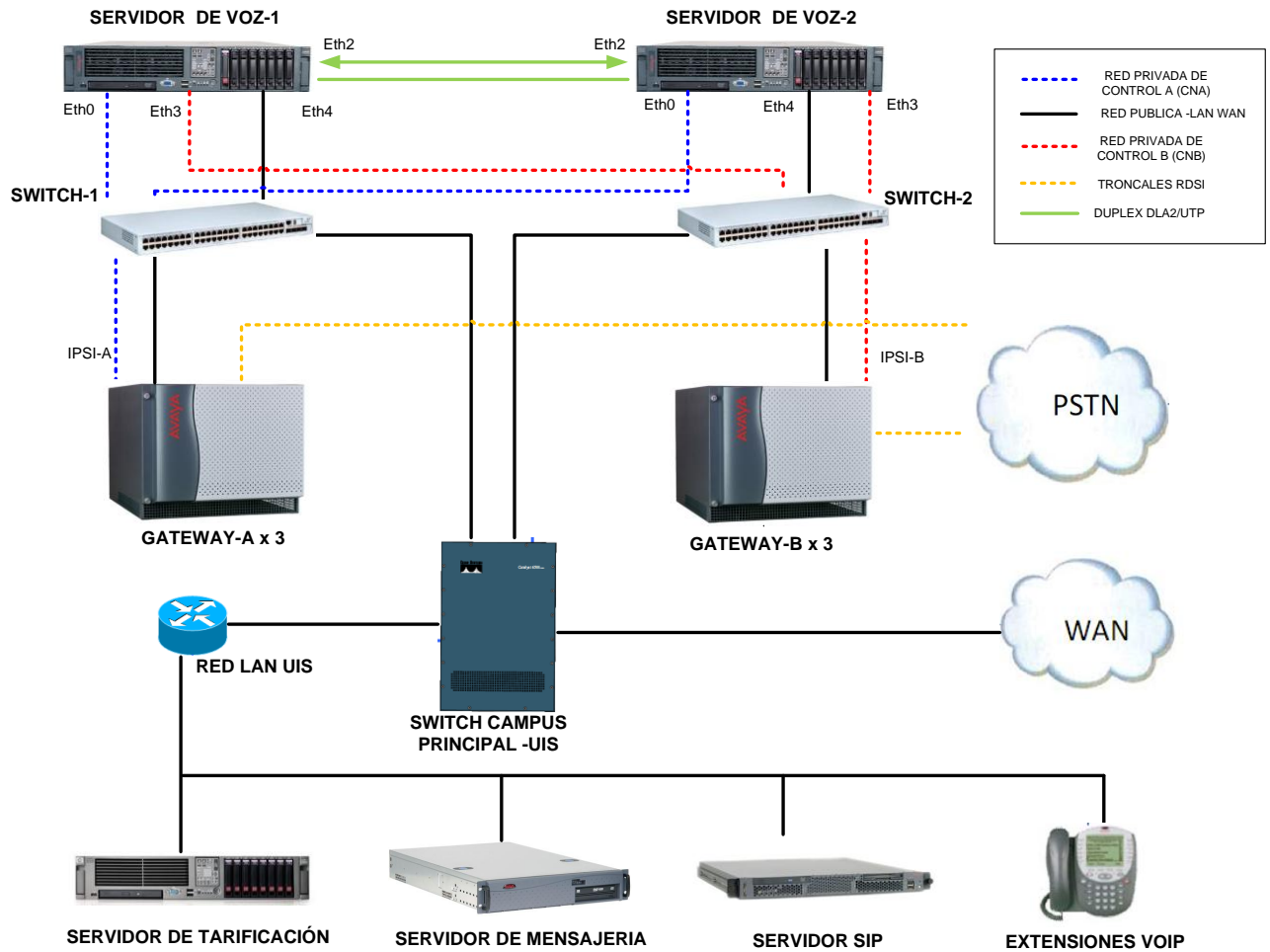


Figura 4.1 Propuesta de interconexión de servidores del sistema de ToIP para el campus UIS<sup>1</sup>.

<sup>1</sup> Figura diseñada por el autor con base en AVAYA Inc. Avaya S8700 Media Server IP Connect High Reliability Configuration using Avaya P333T and Extreme Summit 48si Switches for the Control Network. [PDF] s.l. : Avaya Solution and Interoperability Test Lab, 2004 Issue 1.0.

En la

Figura 4.1 se pueden observar varios cambios fundamentales en la configuración de las conexiones con respecto al sistema instalado actualmente y corresponden a lo siguiente:

- Dos redes de control CNA, CNB y duplicidad de Gateways.
- Redundancia de troncales digitales: Al existir dos *Gateways* existe la posibilidad de integrar troncales digitales de contingencia preferiblemente contratadas con una compañía de telecomunicaciones diferente y así brindar mayor robustez al sistema.
- Los servidores de tarificación, de mensajería y SIP ya no se encuentran conectados al Switch con los servidores S8730 y la red de control privada CNA como se observa en la Figura 3.3 del sistema instalado actualmente, pues el objetivo es garantizar la mayor confiabilidad al sistema de ToIP orientado al Servidor de Voz y a los Gateways los cuales son los equipos fundamentales para la prestación del servicio de ToIP, por lo cual estos servidores adicionales no hacen parte de este sistema de contingencia y serán conectados al sistema de ToIP por medio de un Switch independiente. Con objeto de brindar total independencia a las redes de control y a las conexiones de red administradas por los Switch-1 y Switch-2 y así evitar la dependencia de que estos servidores pierdan conectividad al encontrarse conectados a alguno de estos switch, y por algún motivo externo (daño, falla, pruebas) alguno de estos deba salir de servicio lo cual no afectaría el servicio básico de ToIP, por encontrarse en duplicación completa y si afectaría los servidores de servicios adicionales mencionados anteriormente. Con respecto a esto hay que aclarar que estos equipos deberán conectarse a un switch que debe ser configurado bajo los mismos parámetros de red a los usados cuando se encontraba conectado al switch de rack de VoIP, esto quiere decir que debe soportar Qos y los servidores

deben estar independizados de los otros equipos conectados al switch por medio del uso de una VLAN, (como se explico en el capitulo anterior) la cual corresponde a la subred 192.168.14.0/24, VLAN 114 esto con el objetivo de evitar trafico adicional en la red que afecten los tiempos de respuesta de estos servidores.

En la Tabla 4.1 se detalla la configuración de red propuesta de los servidores S8730 en ella se resaltan las diferencias con la Tabla 3.8 introducidos al activar y configurar la interfaz Eth3.

Interfaz	IP Servidor 1	IP Servidor 2	Descripción	Estado
Eth0	172.18.20.11	172.18.20.12	Interfaz de control CNA red privada	Activa
Eth0:0	172.18.20.10	Ninguna	Interfaz activa CNA	Activa
Eth1	192.11.13.6	192.11.13.6	Interfaz de Servicios	Inactiva
Eth2	192.11.13.13	192.11.13.14	conexión de duplicación de servidores	Activa
<b>Eth3</b>	<b>172.18.22.11</b>	<b>172.18.22.12</b>	<b>Interface de control CNB</b>	<b>Inactiva</b>
<b>Eth3:0</b>	<b>172.18.22.10</b>	<b>Ninguna</b>	<b>Interfaz activa CNB</b>	<b>Inactiva</b>
Eth4	192.168.14.11	192.168.14.12	Interfaz de conexión con LAN Institucional	Activa
Eth4:0	192.168.14.10	Ninguna	Interfaz activa LAN Institucional	Activa

Tabla 4.1 Configuración de interfaces de red Servidores S8730 con esquema de duplicación de alta disponibilidad propuesta.

De acuerdo a los descrito anteriormente se deben instalar 3 *Media Gateways* G650 y como el objetivo de este diseño es crear una red de control espejo que permita tomar el control del sistema de ToIP en caso de que algún equipo de la red de control A falle, deben incluirse todas las tarjetas y equipos que van anexos a los Media Gateways G650 descritos en la Tabla 3.12 y Tabla 3.13.

A continuación se enumeran las direcciones IP que deberán asignarse a las tarjetas que lo requieren para habilitar la red de control B.

TARJETA	IP GATEWAY-A	IP GATEWAY-B
IPSI-1	172.18.20.3	172.18.22.3
IPSI-2	172.18.20.4	172.18.22.4

IPSI-3	172.18.20.5	172.18.22.5
CLAN1	192.168.14.2	192.168.14.9
CLAN2	192.168.14.3	192.168.14.10
CLAN3	192.168.14.4	192.168.14.11
MEDPRO1	192.168.14.5	192.168.14.12
MEDPRO2	192.168.14.6	192.168.14.13
MEDPRO3	192.168.14.7	192.168.14.14
VAL1	192.168.14.8	192.168.14.15

Tabla 4.2 Direcciones IP red corporativa UIS tarjetas C-LAN, MEDPRO y VAL con sistema de alta confiabilidad.

Para activar esta nueva configuración en el servidor hay que realizar algunas modificaciones en su configuración las cuales consisten en habilitar las nuevas tarjetas IPSI en el sistema asignándoles la dirección IP mostrada en la Tabla 4.2, para esto hay que recordar que cada tarjeta IPSI cuenta con dos puertos Ethernet, uno de servicio con la IP 192.11.13.6/255.255.255.252, y otro conectado a la red de control el cual se configura desde la interfaz de servicios por medio del uso de un cable UTP cruzado conectado a un computador haciendo uso de telnet al IP 192.11.13.6 y escribiendo el comando `ipsilogin`. Luego de autenticado se debe definir el IP de la tarjeta IPSI haciendo uso de los siguientes comandos

```
set control interface 172.18.22.3 255.255.255.0
set control gateway 172.18.22.1
exit
```

Este proceso debe repetirse con cada una de las tarjetas IPSI cambiando la dirección IP de acuerdo a la Tabla 4.2 pues para el caso de la UIS cada red de control está conformada por 3 tarjetas IPSI.

Luego de esto debe configurarse el Servidor de Voz; hay que aclarar que AVAYA posee algunos criterios de licenciamiento para el cambio de conexiones del sistema que deben ser satisfechos para poder realizar la configuración, y luego se debe registrar la nueva red de control (CNB) a través de la interfaz de administración Web del Servidor de Voz S8730 realizando conexión a la URL

<https://192.11.13.6> usando un navegador desde un equipo conectado por medio de un cable UTP cruzado a la interfaz de servicios en el servidor 1. Luego de autenticado deben configurarse las interfaces de acuerdo a la Tabla 4.1 y tal como se muestra en la Figura 4.2 y en la Figura 4.3

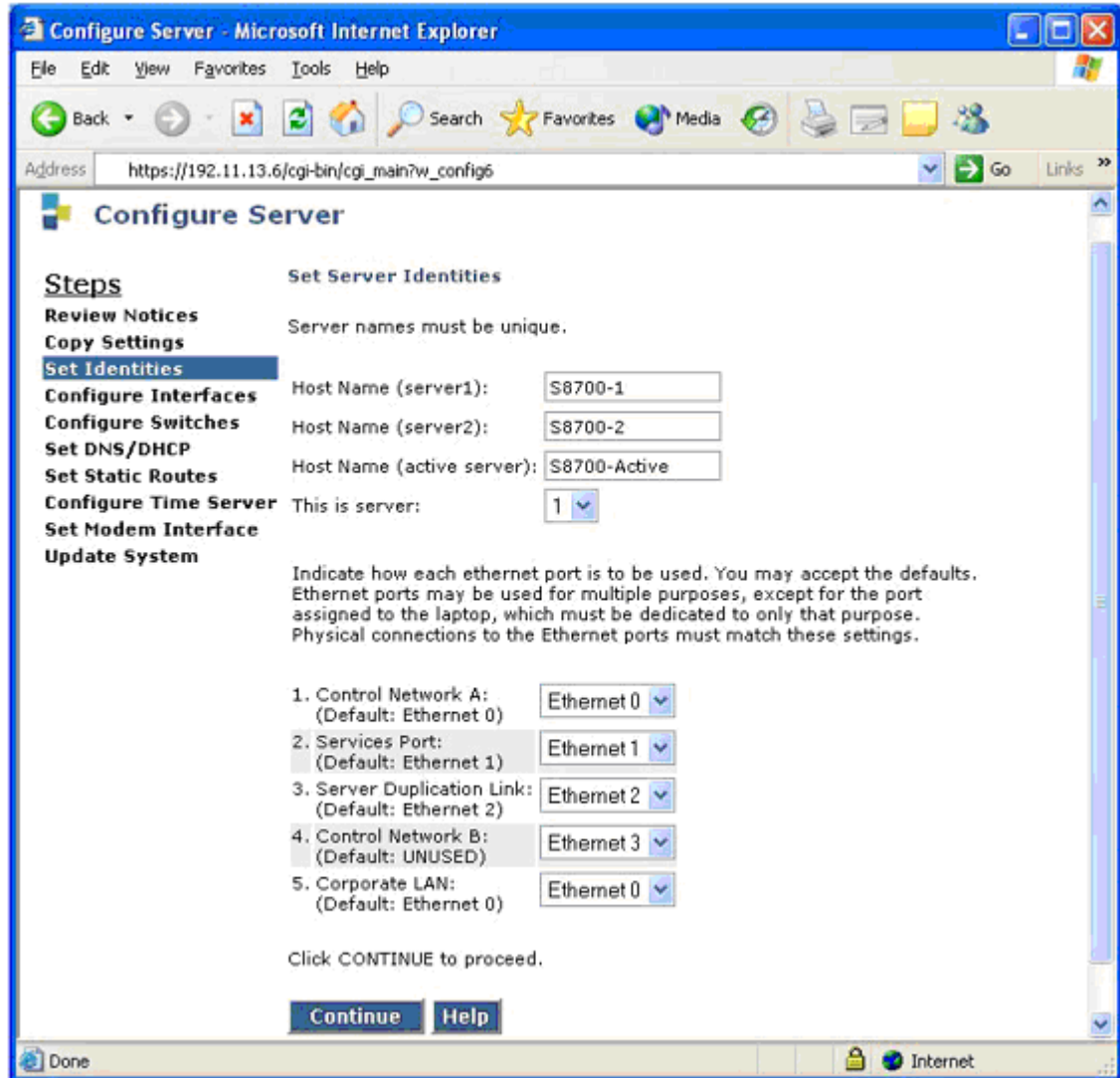


Figura 4.2 Configuración de Identidad AVAYA S8730.

Hay que tener presente que este procedimiento debe realizarse en el servidor 2. Para esto en el campo *This is Server*, luego de aplicar los cambios, se debe seleccionar el numero 2 y a continuación seleccionar las mismas opciones.

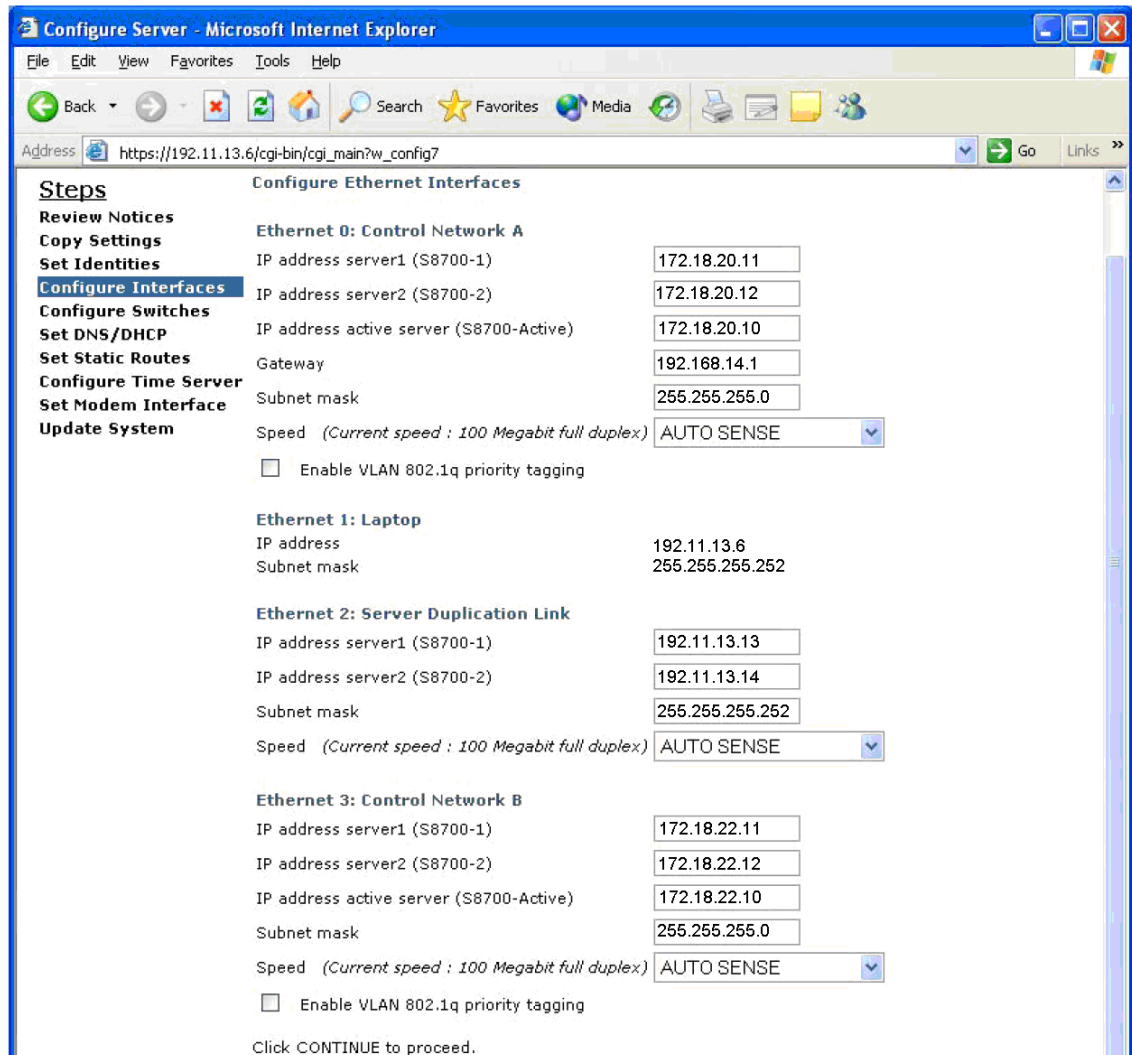


Figura 4.3 Configuración de Interfaces de red AVAYA S8730.

Además de la configuración de la nueva red de control, se debe actualizar la configuración del CM usando el SAT (*System Access Terminal*) para que el servidor reconozca las nuevas tarjetas IPSI, para esto es necesario acceder a la interfaz de administración del servidor usando el CM al IP 192.168.14.10 y luego de autenticarse, ingresar el comando `add cabinet #1` para agregar los nuevos *Media Gateway G650*, además es necesario decirle al sistema acerca de las

---

<sup>1</sup> # representa el numero del gabinete y el número de tarjeta IPSI.

nuevas tarjetas IPSI, para esto se usa la instrucción `add ipserver-interface #` en donde se definirá el IP y la configuración básica de las tarjetas con base en la Tabla 4.2, se deberá repetir el procedimiento con el numero 4,5 y 6 teniendo en cuenta que ya existen 3 gabinetes y 3 tarjetas IPSI configuradas, luego de agregadas al sistema podrán configurarse usando el comando `change ipserver-interface`.

Finalmente, debe activarse la duplicación de tarjetas IPSI usando el comando `change system-parameters duplication` en el cual solo debe seleccionarse la opción “y” a la pregunta *Enable Operation of IPSI Duplication?*.

El objetivo de esta sección es exponer una nueva configuración más robusta y estable luego de una evaluación completa del sistema de ToIP de la Universidad orientado al Servidor de Voz y *Gateway*. En este se exponen los procedimientos básicos para habilitar la duplicación de redes de control en los cuales están implicadas las tarjetas IPSI. Para los procedimientos de instalación usando *CM* de las demás tarjetas debe consultarse [6] donde se explica el procedimiento para cada una de ellas de forma detallada por lo cual no se considera parte de este trabajo.

Adicionalmente, para garantizar el correcto funcionamiento de este sistema debe habilitarse en la red de la universidad la posibilidad del uso de asignación de IP para los teléfonos por medio de DHCP <sup>1</sup> pues esto permite a los teléfonos cambiar y recibir su configuración de red del servidor de acuerdo a la disponibilidad de los diferentes dispositivos de red en caso de que alguna tarjeta falle el servidor automáticamente indicará a los teléfonos el cambio de configuración y ellos realizarán la conexión al siguiente servidor o tarjeta disponible, lo cual con la actual configuración no es posible debido a que la asignación de la configuración a los teléfonos es fija por lo cual si una tarjeta C-LAN saliera de servicio el teléfono

---

<sup>1</sup> *Dynamic Host Configuration Protocol*: protocolo que permite a los nodos de red obtener su configuración IP de forma automática.

no tiene la posibilidad de cambiar su configuración de forma automática y el sistema de redundancia propuesto no tendría utilidad práctica.

### **4.3 Servidor de protocolo SIP AVAYA S8500**

Continuando con la evaluación de las conexiones del sistema se encuentra que la redundancia del Servidor SIP es inexistente o hace falta mucho por mejorar, pues el único sistema encontrado instalado es la unidad virtual llamada Disco RAM descrita en la sección 3.2.4.1, por lo demás el equipo no cuenta con soporte de RAID en ningún nivel, ni ningún sistema de duplicación. Esto es crítico pues no se cuenta con ningún sistema físico de hardware que permita mantener la disponibilidad del servidor en caso de que alguno de sus componentes falle o exista pérdida de información y ante una falla de disco duro<sup>1</sup>, la única solución consiste en instalar el sistema operativo y restablecer una copia de seguridad lo cual implica tiempo apreciable en el cual el sistema se encontrará fuera de servicio y habrá pérdida de información teniendo en cuenta que no es posible realizar copias de seguridad en tiempo real.

### **4.4 Servidor de Tarificación y Mensajería Unificada.**

Para finalizar este análisis, durante la práctica y luego de registrar la configuración de hardware y conexiones de estos equipos, se puede afirmar que actualmente no cuentan con ningún sistema de redundancia.

Con respecto al Servidor de Tarificación Dalí existe cierta garantía pues corresponde a un servidor de gama alta, robusto y con componentes de larga duración, que incluye opciones de redundancia en cuanto a fuente de poder y discos duros que no fueron implementadas en el momento de la instalación pero

---

<sup>1</sup> Componente mecánico de poca vida útil con respecto a los circuitos impresos que conforman el servidor extraído de Bahareh Momken, PhD. *Avaya Communication Manager Software Based Platforms High Availability Solutions*. [PDF] s.l. : Avaya Inc., August 2009.

que aún existe la posibilidad de integrar para garantizar un funcionamiento más estable.

En cambio con respecto al Servidor de Mensajería es preocupante ya que los componentes que integran son propios de un equipo de uso personal los cuales no están diseñados para mantenerse funcionando por periodos largos de tiempo.

En este caso debido a que no es posible la instalación de algún sistema de contingencia por el tipo de hardware instalado, la recomendación es intentar crear copias de seguridad completas del sistema o incluso instalar un equipo con todo el software (servidor de duplicación espejo) y sincronizar los archivos cada cierto tiempo con el objetivo de tener una contingencia en el menor tiempo posible en caso de que el Servidor de Mensajería presente alguna falla.

## **5 PROPUESTA DE PROCEDIMIENTO PARA LA CONFIGURACIÓN E INSTALACIÓN DE EQUIPOS ACTIVOS ADICIONALES**

La universidad Industrial de Santander en sus procesos de estandarización y modernización de la red de datos seleccionó al Switch 3COM 4500G PoE el cual por relación calidad/precio/prestaciones es el que mejor se adapta a los requerimientos de la universidad. Estos switches soportan PoE (*Power over Ethernet*), VLANs (*Virtual Network*), QoS (*Quality of Service*), NDP (*Network Discovery Protocol*), entre otros protocolos además de estar preparados para soportar IPV6 (*Internet Protocol Version 6*) y de cumplir con los requisitos exigidos por el sistema de ToIP.

En el siguiente capítulo se presenta en forma de instructivo el procedimiento que debe seguirse para instalar uno de estos nuevos equipos en caso de que sea necesario, por crecimiento de la red, o por remplazo de un equipo averiado.

En la primera parte se describe el proceso que debe ser realizado para todos los switches previa instalación y se dividirá en algunos subprocesos que se realizarán

dependiendo del modo en que se vaya a instalar el switch. En la segunda parte se explica los cambios de configuración que deben realizarse en los servidores cuando un nuevo equipo activo es ingresado a la red LAN institucional.

Dentro de este capítulo no se explican los procedimientos para agregar nuevos teléfonos y activación de extensiones en el sistema, debido a que ya existen procedimientos establecidos y fueron materia de estudio de otro proyecto de grado [8].

## **5.1 Configuración de nuevos switches**

En esta sección se inicia describiendo los procesos básicos a realizarse en un Switch 3COM 4500G PoE que vaya a ingresar a la red de la Universidad a prestar los servicios de ToIP, luego se explica cómo interconectar varios switches en modo clúster.

### **5.1.1 Configuración básica**

Aquí se explican los procedimientos requeridos para configurar un switch 4500G PoE, con objeto de agrupar los procedimientos esta sección se ha dividido en 8 sub-secciones los cuales es recomendable que se ejecuten en orden pues muchos de ellos tienen dependencias previas, esto quiere decir por ejemplo que no es posible por ejemplo definir contraseña para el servicio de SSH si aún no se ha habilitado dicho servicio.

### 5.1.1.1 Primeros pasos

Primero que todo hay que saber que los Switches 3COM 4500G en la universidad se comportan como un dispositivo de Capa<sup>1</sup> 2<sup>2</sup> y son administrables y configurables a través de varios métodos entre los más importantes tenemos:

- Conectándose por medio del puerto de consola.
- Realizando una conexión a través de la red local usando el servicio de Telnet o SSH.
- Realizando una conexión a través de la red local usando un navegador web al puerto 80.

Además existen dos interfaces de usuario para establecer conexión con el switch 3COM usando una terminal Telnet AUX y VTY.

1. AUX: Se refiere a toda conexión realizada desde el puerto de consola solo soporta máximo 1 usuario.
2. VTY: Se refiere a toda conexión realizada a través de la red Ethernet soporta hasta 5 usuarios simultáneos.

Los procedimientos que se explican a continuación debe realizarse usando el puerto de consola.

Para realizar conexión a través del puerto de consola debe realizar lo siguiente:

- a. Conecte el puerto serial (RS232<sup>1</sup>) de su computador con el puerto de Consola del Switch como se muestra en la figura a continuación.

---

<sup>1</sup> Quiere decir que se comportan esencialmente como puentes multipuerto que usan micro-segmentación para incrementar el ancho de banda. Cisco Systems, Guía del primer año CCNA 1y 2 Tercera edición, Pearson Educación S.A Marid, 2004.

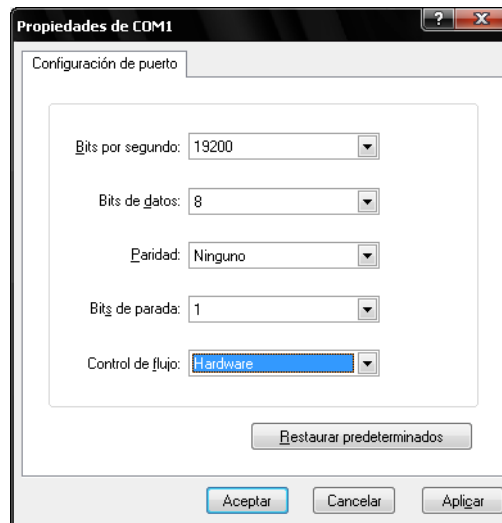
<sup>2</sup> Capa de enlace de datos en el modelo OSI (Open System Interconnection).



Figura 5.1 Diagrama de conexión usando el puerto de consola<sup>2</sup>.

- b. Ejecute un emulador de terminal desde su computador que permita realizar conexiones a través del puerto serie RS232, en Windows puede usar Hyperterminal. Cree una conexión al puerto serie con los siguientes parámetros:

Bits por segundo: 19200, Bits de datos: 8, Paridad: Ninguno, Bit de parada: 1, Control de Flujo: Hardware, como se muestra en la figura a continuación.



<sup>1</sup> Es una interfaz de comunicación serie que designa una norma para el intercambio de datos binarios entre dos equipos.

<sup>2</sup> Imagen dibujada con base en 3COM. 3Com® Switch 4500G Family Configuration Guide. February 2008. Part Number: 10014900 Rev. AC

Figura 5.2 Configuración de puerto Rs232 en Hyperterminal.

- c. Establezca conexión con el switch.

A partir de este momento debe visualizar la consola que permite la administración de los switches para poder dar inicio a la configuración.

#### 5.1.1.2 Habilitar servicio SSH

De forma predeterminada el Switch no trae activo el servicio de SSH para administración remota a través de Ethernet así que se debe activar.

- a. Para esto se crea una llave de acceso cuando el sistema pregunte debe hacerse de 1024 bits de seguridad para encriptar la conexión con el switch.

```
[3COM]rsa local-key-pair create
```

- b. Se habilita el servicio SSH.

```
[3COM]SSH server enable
```

- c. Se habilita el servicio SSH para las conexiones a través de VTY de la terminal 0 a la 4.

```
[3COM]user-interface vty 0 4  
[3COM -ui-vty0-4]authentication-mode scheme  
[3COM -ui-vty0-4]protocol inbound SSH  
[3COM -ui-vty0-4]quit
```

#### 5.1.1.3 Definir contraseña para SSH y Consola

Por estándar de la universidad el puerto de consola, y la terminal SSH debe estar protegido con contraseña, para crear una ejecute lo siguiente:

- a. Se ingresa a la configuración del sistema

```
[3COM]System-view
```

- b. Se define el modo de acceso a modificar, en este caso el de puerto consola.

```
[3COM]user-interface aux 0
```

- c. Activa el modo de autenticación por password.

```
[3COM-ui-aux0]authentication-mode password
```

- d. Define el password para conectarse a la consola de modo encriptado.

```
[3COM-ui-aux0]set authentication password cipher 123456
```

- e. Finaliza edición de AUX

```
[3COM-ui-aux0]quit
```

Para crear una contraseña para la consola usando el puerto SSH a través de Ethernet haga lo siguiente.

- f. Se define un usuario local llamado admin

```
[3COM]local-user admin
```

- g. Se define un password (Por seguridad no incluido en este documento.)

```
[3COM -luser-admin]password cipher 123456
```

```
[3COM -luser-admin]service-type SSH level 3
```

```
[3COM -luser-admin]quit
```

- h. Se define el tipo de autenticación para el usuario admin.

```
[3COM]SSH user admin authentication-type password
```

#### 5.1.1.4 Definir Fecha y hora, nombre del sistema, VLANs y servidor de log

A continuación se definen parámetros como nombre del sistema, la fecha y hora, se crean VLANs, se habilita un servidor de Log y otros parámetros básicos.

- a. La Universidad con respecto al nombre del switch establece que debe corresponder al nombre del edificio o según una tabla de nombres existente, seguido del número de switch teniendo en cuenta que el switch principal del Rack será el número 1 y así sucesivamente.

```
<3Com> system-view
```

```
[3COM]sysname nombre de edificio_numero
```

b. Aquí se define la fecha y hora del sistema:

```
<3Com> clock datetime 0:0:0 2001/01/01
```

c. Se habilita la conexión con un servidor de log.

```
[3COM -R1-VD5]info-center enable
```

d. Se selecciona el servidor con dirección IP 192.168.5.183 como servidor de estadísticas y de log.

```
[3COM]info-center loghost 192.168.5.183
```

e. Se crean las VLANs de acuerdo a los criterios definidos en el switch principal de la universidad Extreme Networks el cual es capa 3<sup>1</sup>. Al momento de la instalación hay que tener presente que actualmente en el sistema de ToIP existen 5 VLANs definidas para ser usadas por los servicios de ToIP las cuales son las siguientes:

VLAN	Descripción
14	VoIP01
15	VoIP02
16	VoIP03
17	VoIP04
120	VoIP05

Tabla 5.1 VLANs de Voz configuradas en campus de la Universidad.

La forma de establecer la configuración de cada una se muestra a continuación:

```
<3Com> system-view
[3Com] vlan 14
[3Com-vlan14] desc VoIP01
[3Com-vlan14] quit
```

---

<sup>1</sup> Capa de red, según la normalización OSI, es una capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts.

```
<3Com> system-view  
[3Com] vlan 15  
[3Com-vlan15] desc VoIP02  
[3Com-vlan15] quit
```

```
<3Com> system-view  
[3Com] vlan 16  
[3Com-vlan16] desc VoIP03  
[3Com-vlan16] quit
```

```
<3Com> system-view  
[3Com] vlan 17  
[3Com-vlan17] desc VoIP04  
[3Com-vlan17] quit
```

```
<3Com> system-view  
[3Com] vlan 120  
[3Com-vlan17] desc VoIP05  
[3Com-vlan17] quit
```

Aquí hay algo importante que recordar, y es que según la configuración del sistema, cada puerto del switch tendrá la capacidad de transportar tanto voz como datos de forma simultánea, ya que en la mayoría de los casos se encontrará un teléfono IP y un computador conectados al mismo punto de red. Es por esto que se ha determinado que cada puerto tenga configuradas dos VLANs, una destinada a voz y una destinada a datos con objeto de independizar la información y priorizar los datos de Voz de acuerdo a los parámetros de diseño.

Por lo cual existen otras VLANs validas en la universidad orientadas a datos las cuales son de conocimiento de la DSI de la UIS y no hacen parte de este trabajo.

### 5.1.1.5 Definir IP de administración a través de interface Ethernet y rutas de red.

Luego se debe definir el IP del Switch. La Universidad ha establecido la subred 192.168.5.0/24 para los switches de red del Campus Principal, es importante resaltar que de forma predeterminada todos los puertos del switch vienen configurados con la VLAN 1 la cual es la VLAN seleccionada por la DSI para realizar la administración de los equipos. A continuación el procedimiento:

- a. Se selecciona la interfaz a editar.

```
<3Com> system-view  
[3COM] interface Vlan-interface 1
```

- b. Se asigna la dirección IP donde XXX equivale al IP y 24 <sup>1</sup>

```
[3COM] ip address 192.168.5.XXX 24
```

- c. Finalmente se asigna una ruta estática al 192.168.5.1 teniendo en cuenta que este corresponde al IP del Switch Core de la Universidad, de la siguiente forma:

```
<3Com> system-view  
[3Com] ip route-static 0.0.0.0 0.0.0.0 192.168.5.1
```

### 5.1.1.6 Activación de QoS

Con el objetivo de que los datos de voz tengan prioridad sobre los datos, los Switches incorporan el protocolo QoS el cual permite priorizar el procesamiento de datos de voz de acuerdo a ciertos parámetros, a continuación se muestra como configurarlo.

- a. Se ingresa a la configuración del sistema

```
<3com> system-view
```

---

<sup>1</sup> Que equivale a 8bit x 3 octetos = 24 bit. En la red al IP 255.255.255.0

- b. Se define un tipo de tráfico en este caso llamado “Class\_Uis” en el cual se definen las propiedades.

```
[3com] traffic classifier Class_Uis
```

- c. Aquí se define la prioridad sobre el tráfico para “Class\_Uis”, la escala va de 0 a 7, para la Universidad se ha determinado en 6.

```
[3com-classifier_Class_UIS] if-match ip-precedence 6  
[3com-classifier_Class_UIS]quit
```

- d. Ahora hay que definir otro grupo llamado “behavior\_Uis”, en el cual se asignarán parámetros los cuales serán aplicados a los paquetes<sup>1</sup> que son clasificados como tipo “Class\_Uis”, los paquetes serán marcados usando el comando `remark dot1p6` que se basa en el protocolo 802.1p para priorizar el tráfico.

```
[3com]traffic behavior Behavior_Uis  
[3com-behavior_behavior_IUS]remark dot1p 6  
[3com-behavior_behavior_IUS]quit
```

- e. Ahora solo resta crear la política con los parámetros de selección y las acciones que se realizaran a dichos paquetes.

```
[3com] qos policy Policy_Uis  
[3com_qospolicy_Policy_UIS] classifier Class_Uis behavior  
Behavior_Uis  
[3com_qospolicy_Policy_UIS] quit
```

---

<sup>1</sup> un paquete de datos es una unidad fundamental de transporte de información y está generalmente compuesto de tres elementos: una cabecera, el área de datos, y la cola.

- f. Para terminar hay que seleccionar las diferentes interfaces y aplicarle las políticas creadas el anterior procedimiento que será repetido en la sección siguiente cuando se mostrará como configurar un puerto como híbrido.

```
[3com] interface GigabitEthernet 1/0/10  
[3com_ GigabitEthernet 1/0/10] qos apply policy Policy_Uis  
inbound
```

#### 5.1.1.7 Configuración de puertos como híbridos

Luego de los procedimientos anteriores a modo de recopilación, se presenta a continuación la configuración de un puerto híbrido que hará uso de telefonía IP y de un Computador conectado en el mismo puerto Ethernet de forma simultánea para lo cual se realiza o siguiente.

- a. Se selecciona la interfaz a modificar donde **xx** representa el número del puerto.

```
[3com] interface GigabitEthernetxx/xx/xx
```

- b. Se selecciona el tipo de puerto en este caso híbrido.

```
[3com] port link-type hybrid
```

- c. Se asignan las VLANs que manejará los datos marcados por el protocolo 802.1p, quiere decir la Vlan que manejara los datos de voz.

```
[3com] port hybrid vlan xx tagged
```

- d. Se definen las demás VLANs disponibles para ser usadas por el puerto en este caso las VLANs de datos.

```
[3com] port hybrid vlan x xx untagged
```

- e. Se selecciona una VLAN predeterminada (alguna de las VLANs de Datos definidas), y se definen algunos parámetros estándar.

```
[3com] port hybrid pvid vlan xx
```

```
[3com] broadcast-suppression pps 3000
```

```
[3com] undo jumboframe enable
```

- f. Se habilita el soporte de PoE para el puerto.

```
[3com] poe enable
```

```
[3com] stp edged-port enable
```

- g. Se aplica la política de QoS (creada en la sección anterior).

```
[3com] qos apply policy Policy_Uis inbound
```

- h. Finalmente, antes de tener que ejecutar este procedimiento en todos los puertos de forma independiente. Existe la posibilidad de copiar la configuración y replicarla en puertos requeridos para agilizar el proceso de configuración.

A continuación se presenta un ejemplo de este procedimiento:

```
[3Com] copy configuration source GigabitEthernet 1/0/5  
destination GigabitEthernet 1/0/6 to GigabitEthernet 1/0/20
```

En donde se muestra como copiar el perfil de configuración creado en el puerto 1/05 a los puertos desde el puerto 1/0/6 al 1/0/20.

#### 5.1.1.8 Configuración de puerto para enlace de fibra óptica

La mayoría de los racks de la Universidad se encuentran interconectados con el núcleo principal por medio de enlaces de fibra óptica, los switches 3COM 4500G incluyen un modulo de fibra óptica en el puerto 52 para los switches de 48 puertos y en el puerto 26 para los switches de 24 puertos, a continuación se presenta los parámetros que se deben configurar a estos puertos para establecer dicho enlace.

- a. Ingrese a la configuración del puerto 1/0/52

```
[3com] interface gigabitethernet1/0/52
```

- b. Cambie el tipo de puerto a tipo trunk y permita el acceso a todas las VLANs disponibles.

```
[3com -GigabitEthernet1/0/52]port link-type trunk  
[3com -GigabitEthernet1/0/52]port trunk permit vlan all
```

- c. Se deshabilita la auto-negociación de velocidad de transferencia, fijando los siguientes valores:

```
[3com -GigabitEthernet1/0/52] speed 1000  
[3com -GigabitEthernet1/0/52] duplex Full 1000
```

### 5.1.2 Configuración conexión entre switches de tipo clúster<sup>1</sup>

A continuación, se presentan los procedimientos que se deben realizar para configurar un clúster de switches, el cual consiste en enlazar 2 o más switches permitiendo que todos puedan ser administrados y se comporten en la red como uno solo, además de garantizar en el enlace el cumplimiento de los requerimientos del sistema de ToIP. Esto es útil cuando el requerimiento de puertos es superior a la capacidad del switch instalado.

En la Figura 5.3 se describe la configuración a realizar.

---

<sup>1</sup> Clúster: tecnología propietaria de 3COM que permite apilar hasta 32 switches y proporciona una conectividad de LAN segura y flexible, así como funcionalidades avanzadas optimizadas para voz tales como VLAN automática de voz y QoS, Extraído de [http://www.3com.com/prod/es\\_la\\_amer/detail.jsp?tab=features&sku=3CR17761-91](http://www.3com.com/prod/es_la_amer/detail.jsp?tab=features&sku=3CR17761-91)

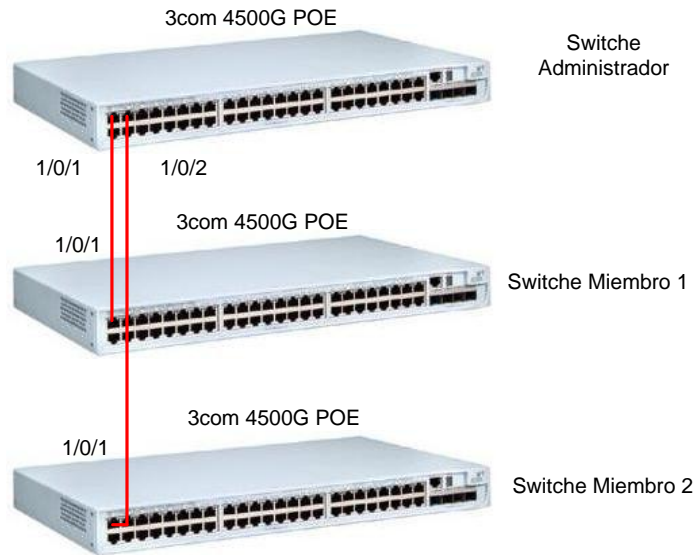


Figura 5.3 Configuración de Switches en Clúster un administrador y dos miembros.

El siguiente procedimiento se elabora para el caso en que se desee crear un clúster de 3 switches donde exista un switch administrador y dos switches miembros, como se muestra en la Figura 5.3, pero podrá ser modificado de acuerdo a los requerimientos. El proceso se inicia en los switches miembros y finalmente se ejecuta en el switch administrador.

#### 5.1.2.1 Procedimiento para configurar los Switches miembros

En el siguiente procedimiento, se muestran los pasos de configuración que deben ser ejecutados para formar el clúster correctamente, primero que todo se activa el protocolo NDP (*Network Discovery Protocol*) y NTDP (*Network Topology Information Collection*) a nivel de dispositivo y en el puerto que va a hacer parte del clúster en este caso el Ethernet 1/0/1, luego se cambia el tipo de puerto a tipo *Trunk*, y finalmente se habilitan todas las VLANs creadas con anterioridad para este puerto.

Para el primer miembro:

- a. Se ingresa a la configuración

```
< 3com _2> system-view
```

**b. Se habilita a nivel de dispositivo protocolo NDP**

```
[3com _2] ndp enable
```

**c. Se habilita a nivel de interface Ethernet protocolo NDP**

```
[3com _2] interface Ethernet 1/0/1
```

```
[3com _2-Ethernet1/0/1] ndp enable
```

```
[3com _2-Ethernet1/0/1] quit
```

**d. Se habilita NTDP a nivel global y en la interface Ethernet 1/0/1**

```
[3com _2] ntdp enable
```

```
[3com _2] interface Ethernet 1/0/1
```

```
[3com _2-Ethernet1/0/1] ntdp enable
```

```
[3com _2-Ethernet1/0/1] quit
```

**e. Se habilita la función de clúster.**

```
[3com _2] cluster enable
```

**f. Se configura el tipo de puerto como *Trunk* y se asignan todas las VLANs como activas, para garantizar la conectividad.**

```
[3com _2] interface Ethernet 1/0/1
```

```
[3com _2-Ethernet1/0/1] port trunk permit vlan all
```

```
[3com _2-Ethernet1/0/1] port link-type trunk
```

```
[3com _2-Ethernet1/0/1] quit
```

**g. Ahora para el segundo miembro se realiza el mismo procedimiento:**

**Habilitar NDP.**

```
< 3com _3> system-view
```

```
[3com _3] ndp enable
```

```
[3com _3] interface Ethernet 1/0/1
```

```
[3com _3-Ethernet1/0/1] ndp enable
```

```
[3com _3-Ethernet1/0/1] quit
```

Habilitar NTDP.

```
[3com _3] ntdp enable
[3com _3] interface Ethernet 1/0/1
[3com _3-Ethernet1/0/1] ntdp enable
[3com _3-Ethernet1/0/1] quit
```

Habilitar la función de clúster.

```
[3com _3] cluster enable
```

Se configura el tipo de puerto como Trunk y se asignan todas las vlans como activas, para garantizar la conectividad.

```
[3com _3] interface Ethernet 1/0/1
[3com _3-Ethernet1/0/1] port trunk permit vlan all
[3com _3-Ethernet1/0/1] port link-type trunk
[3com _3-Ethernet1/0/1] quit
```

#### 5.1.2.2 Procedimiento para configurar el Switch administrador del clúster.

A continuación se presenta la configuración que debe realizarse en el Switch administrador del clúster. El procedimiento es similar al de los switches miembros, inicialmente se habilitan los protocolos de NDP y NTDP y se establecen los puertos involucrados como tipo *Trunk*, la diferencia radica en que para el switch administrador se crea el clúster que administrará el conjunto de switches, además en él se configuran tantos puertos como switches el clúster tenga, en este caso se realizará la configuración de un clúster con dos miembros correspondientes a los puertos Ethernet 1/0/1 y Ethernet 1/0/2.

- a. Se configura el tipo de puerto como Trunk y se asignan todas las VLANs como activas, para garantizar la conectividad.

```
[3com _1] interface Ethernet 1/0/1
[3com _1-Ethernet1/0/1] port trunk permit vlan all
```

```
[3com _1-Ethernet1/0/1] port link-type trunk
[3com _1-Ethernet1/0/1] quit
[3com _1] interface Ethernet 1/0/2
[3com _1-Ethernet1/0/1] port trunk permit vlan all
[3com _1-Ethernet1/0/1] port link-type trunk
[3com _1-Ethernet1/0/1] quit
```

**b. Habilitar NDP.**

```
< 3com _1> system-view
[3com _1] ntdp enable
```

**c. Habilitar NDP en la interface Ethernet 1/0/1.**

```
[3com _1] interface Ethernet 1/0/1
[3com _1-Ethernet1/0/1] ndp enable
[3com _1-Ethernet1/0/1] quit
```

**d. Habilitar NDP en la interface Ethernet 1/0/2.**

```
[3com _1] interface Ethernet 1/0/2
[3com _1-Ethernet1/0/2] ndp enable
[3com _1-Ethernet1/0/2] quit
```

**e. Se definen parámetros para NDP**

**Tiempo de espera para descubrimiento 200 segundos.**

```
[3com _1] ndp timer aging 200
```

**Intervalo entre envío de paquetes a 70 segundos.**

```
[3com _1] ndp timer hello 70
```

**Habilitar NTDP a nivel de dispositivo y en interface Ethernet 1/0/1 y 1/0/2.**

```
[3com _1] ntdp enable
[3com _1] interface Ethernet 1/0/1
[3com _1-Ethernet1/0/1] ntdp enable
```

```
[3com _1-Ethernet1/0/1] quit  
[3com _1] interface Ethernet 1/0/2  
[3com _1-Ethernet1/0/2] ntdp enable  
[3com _1-Ethernet1/0/2] quit
```

- f. Se selecciona la topología de clúster a crear en este caso conformada por dos dispositivos miembros.

```
[3com _1] ntdp hop 2
```

- g. Se establece un tiempo de 150 ms de espera para un dispositivo miembro, para reenviar la solicitud de conformación de la topología.

```
[3com _1] ntdp timer hop-delay 150
```

- h. Se establece un tiempo de 15 ms de espera para un puerto de un dispositivo miembro, para reenviar la solicitud de conformación de la topología.

```
[3com _1] ntdp timer port-delay 15
```

- i. Se define el intervalo de tiempo entre el cual se conforma la topología de clúster.

```
[3com _1] ntdp timer 3
```

- j. Se habilita la función de clúster, en este momento se asume que todos los demás dispositivos terminaron su configuración se encuentran encendidos y conectados a los respectivos puertos configurados y mostrados en la Figura 5.3.

```
[3com _1] cluster enable
```

- k. Se ingresa a la configuración del cluster

```
[3com _1] cluster  
[3com _1-cluster]
```

- l. A continuación, se define el rango de direcciones disponibles para el clúster en este caso el IP 172.16.0.1 con máscara de subred 255.255.255.248 lo que equivale a 6 direcciones IP empezando por 172.16.0.1

```
[3com _1-cluster] ip-pool 172.16.0.1 255.255.255.248
```

- m. Luego de asignada la configuración, se crea el clúster con un nombre.

```
[3com _1-cluster] build nombre
```

- n. Luego de creado el clúster, se deben agregar los miembros para esto debe conocerse la MAC address del dispositivo miembro.

```
[stack_0. IngIndustrial_1-cluster] add-member 1 mac-address  
xxxx-xxxx-xxxx
```

```
[stack_0. 3com _1-cluster] add-member 2 mac-address xxxx-  
xxxx-xxxx
```

- o. Se define un parámetro de espera de 100 segundos para el clúster para recibir respuesta de los switches miembros.

```
[stack_0. 3com _1-cluster] holdtime 100
```

- p. Se selecciona un intervalo de 10 segundos para monitoreo de los miembros del clúster.

```
[stack_0. 3com _1-cluster] timer 10
```

## 5.2 Cambios en la configuración de los servidores para nuevos switches.

Una de las grandes ventajas de nuevo sistema de ToIP es que no se requiere realizar cambios en la configuración de los servidores cuando la red de datos presenta modificaciones pues lo único que hay que garantizar es la conectividad cumpliendo los parámetros de calidad para que el sistema funcione correctamente, a crecimiento futuro las únicas modificaciones que se deben realizar en los servidores de Voz se refieren al licenciamiento de estaciones dado que la universidad adquirió un determinado número de licencias para instalación

de teléfonos IP este licenciamiento a futuro deberá ser ampliado para permitir el crecimiento del sistema así como también quizás la creación de nuevas VLANs de voz las cuales deberán ser registradas en el Switch Core de la Universidad.

## 6 CONCLUSIONES Y RECOMENDACIONES

- Durante la elaboración de este trabajo se documentaron los principales parámetros de configuración de los servidores involucrados en los servicios de ToIP, de una forma clara y detallada. Mostrando al lector un panorama que le permitiera entender el funcionamiento del sistema y la función que cada equipo cumple dentro del sistema de ToIP, con el objetivo principal de permitir su administración, pues uno de los principales requisitos para tomar el control completo de un sistema es conocerlo de la mejor forma. con lo cual hasta el momento la Universidad Industrial de Santander no contaba.
- Se mostró de forma detallada la configuración de conexiones físicas actuales como son la configuración del switch, conexiones de red de los servidores, tarjetas de *Media Gateways* y se presentó una propuesta de conexiones incluyendo especificaciones de nuevos equipos con objeto de incrementar la confiabilidad del sistema, con base en el estudio realizado durante la elaboración de este proyecto.
- Se realizó un estudio de los sistemas de redundancia instalados y se resaltaron las falencias detectadas, además de la descripción de los procedimientos para la implementación de posibles soluciones, según la documentación estudiada durante este trabajo.
- Con este documento, se considera que se dieron por cumplidos los objetivos planteados, dejando muy claro que durante la fase de práctica y recolección de datos, se encontró extensa información de procedimientos y manuales para CM 5.0. Lo que permitió centrar el capítulo 3 de este trabajo en documentar la configuración del sistema en el área de hardware,

conexiones de red y configuración de software, teniendo en cuenta los principales parámetros de instalación de los servidores, como también mostrar información, que quizás no se encuentra plasmada de forma detallada en la documentación existente, y que se considera es de gran relevancia a la hora de asumir la administración de un sistema de esta magnitud. Para que posteriormente este documento pueda ser utilizado conjuntamente con los procedimientos diseñados por el fabricante en la configuración del sistema.

- Adicionalmente en este trabajo se realizó una investigación con la división de servicios de información para la elaboración de procedimientos que permitan configurar equipos de red próximos a ingresar a la red de la Universidad, con base en los estándares establecidos para el sistema.

## **7 RECOMENDACIONES TECNICAS**

- Durante la práctica se observó que inicialmente el sistema de ToIP integraba el uso de DHCP, para auto-asignar la configuración IP de los teléfonos, pero debido a problemas de compatibilidad con la red de datos de la Universidad (Actualmente, la cual no soporta DHCP), este debió ser desactivado y los teléfonos IP configurados manualmente. Luego del estudio realizado durante este proyecto se recomienda configurar DHCP a nivel de todo el campus en la red de datos, para eliminar la incompatibilidad y poder habilitar DHCP para el sistema de voz, pues esto garantizaría una administración más robusta. Dado que permitiría asignar los recursos de direccionamiento desde un punto central, hacer balance de carga de forma automática, implementar sistemas de contingencia más confiables (Ver sección 4.2) y evitar tener que reconfigurar cada uno de los teléfonos IP, en caso de realizar algún cambio en el sistema.

- Las actuales copias de seguridad de todos los servidores se realizan manualmente. En un entorno como es el de la Universidad Industrial de Santander este tipo de operaciones deben encontrarse automatizadas con el objetivo primordial de: garantizar la ejecución de estas tareas, mejorar la seguridad de la manipulación de la información y utilizar los recursos humanos de forma más eficiente. Teniendo en cuenta que todos los servidores cuentan con sistemas configurables y de ejecución automática para la ejecución de estos procesos [10].
- Actualmente, los Switches 3COM 4500 que se encuentran apilados en los diferentes centros de cableados de la Universidad, usan una tecnología propietaria de 3COM llamada Clúster para centralizar la administración. La cual cierra la posibilidad de usar switches de otras referencias pues solo está disponible para 4 de 3COM (Switch 4200G, 4500G y switches Series 5500 y 5500G), por lo cual se recomienda migrar el sistema de interconexión entre switches (Apilamiento) a un sistema de *stacking* estándar que permita el crecimiento y sostenibilidad de la red en el futuro.
- Se recomienda la instalación en los servidores S8730 de un segundo disco duro, con objeto de habilitar el sistema RAID nivel 1 y así aumentar el rendimiento y la confiabilidad del almacenamiento de la información.

## 8 BIBLIOGRAFÍA

1. **Guzmán, Paola.** *Análisis de la gestión de los dispositivos administrables en la red de datos institucional.* Universidad Industrial de Santander - E3T. Bucaramanga : Tesis de Maestría, 2005.
2. **Wikipedia, Colaboradores de.** Wikipedia. [En línea] Wikimedia, 2010. [Citado el: 10 de Junio de 2010.] Consulta de VLAN, QoS, PoE, VoIP, SIP, ToIP, H323,

Gateway, Gatekeeper, AVAYA, Rack, U, SAS, SCSSI, RAID, IDE, Paquete de red, Switch, Router, Audix, Stacking, Modelo OSI. [www.wikipedia.org](http://www.wikipedia.org).

3. **Gonzales, Gustavo y Vásquez, Javier.** *Sistema de Contact Center Basado en Telefonía IP*. Universidad Industrial de Santander - E3T. Bucaramanga : Tesis de Especialización en Telecomunicaciones, 2001.

4. **UIS.** *Modernización de la Infraestructura de Telecomunicaciones de la Universidad Industrial de Santander*. Bucaramanga : División de Mantenimiento Tecnológico - División de Servicios de Información, 2008.

5. **Avaya Inc.** *Administrator Guide for Avaya Communication Manager*. [PDF] January 2008, Release 5.0. 03-300509.

6. —. *Administration for Network Connectivity for Avaya Communication Manager*. [PDF] January 2008 Issue13. 555-233-504.

7. —. *Installing, Administering, Maintaining, and Troubleshooting SIP Enablement Services*. [PDF] January 2008. 03-600768.

8. **Morales, Lilian y Pinzón, Juan.** *Supervisión y documentación de la implementación de la red de telefonía IP en la Universidad Industrial de Santander*. Universidad Industrial de Santander -E3T. Bucaramanga : s.n., 2009.

9. **Bahareh Momken, PhD.** *Avaya Communication Manager Software Based Platforms High Availability Solutions*. [PDF] s.l. : Avaya Inc., August 2009.

10. **Alvarez Bauza, Christian.** *Análisis y Mejoramiento del Funcionamiento de un Centro de Llamadas (Call Center)*. Universidad de las Américas Puebla - Centro Interactivo de Recursos de Información y Aprendizaje. 2009.

11. **Avaya Inc.** *Avaya Communication Manager Descripción Técnica*. [En línea] 2008. [www.seguridad-a1.com/xesControl/pdfs/CommunicationManager.pdf](http://www.seguridad-a1.com/xesControl/pdfs/CommunicationManager.pdf).

12. —. *Descripción general de Avaya Communication Manager*. [PDF] Noviembre 2003 3a edición. 555-233-767SPL.

13. —. *Quick Start for Hardware Installation Avaya S8700-Series Servers*. [PDF] January 2008 Issue 8. 555-245-703.
14. —. *Security and Avaya Communication Manager Media Servers*. [PDF] Summer 2005 Issue 3.0.
15. —. *Avaya S8700 Media Server IP Connect High Reliability Configuration using Avaya P333T and Extreme Summit 48si Switches for the Control Network*. [PDF] s.l. : Avaya Solution and Interoperability Test Lab, 2004 Issue 1.0.
16. —. *Installing and Configuring the Avaya S8700-Series Server Release 5.2*. [PDF] May 2009 Issue 8. 03-300145.
17. **Alzate, John**. *Modernización tecnológica de la infraestructura de telecomunicaciones de la universidad industrial de santander diseño*. Bucaramanga : Assenda S.A, 2008.
18. **Avaya Inc**. *Application Notes for Configuring Avaya Communication Manager, Avaya Modular Messaging or Avaya INTUITY™ AUDIX® LX to Support IPC Information Systems Alliance MX using QSIG*. [PDF] s.l. : Avaya Solution & Interoperability Test Lab, 2009. Vol. 1.
19. **Sims, Jamie**. Jaymzworld. [En línea] Technical Manager, Avaya Inc. [Citado el: 6 de 5 de 2010.] [http://jaymzworld.com/wiki/Server\\_ports\\_and\\_IP\\_addresses](http://jaymzworld.com/wiki/Server_ports_and_IP_addresses).
20. **Comunicaciones World**. *Telefonía en red redes convergentes de voz y datos aplicaciones*. s.l. : IDG, 2002.
21. **3Com Corp**. *3Com® Switch 4500G Family Command Reference Guide*. February 2008. Part Number: 10014901 Rev. AB.
22. —. *3Com® Switch 4500G Family Configuration Guide*. February 2008. Part Number: 10014900 Rev. AC.
23. **Avaya Inc**. *Centralized Integrated Management for Avaya Communication Manager and Intuity AUDIX 770 Messaging using Avaya Multi-Site Administration*

and the Avaya Integrated Management Database. [En línea] 2006. [Citado el: 10 de Marzo de 2010.]

24. —. *Intuity Audix LX Release 1.1-5.8*. 2006.

25. —. *IP Telephony Deployment Guide*. [PDF] s.l. : Avaya Application Solutions:, February 2010. 555-245-600.

26. —. *Job Aid: Server and CSS Separation—Avaya S8700 Series Media Servers*. [PDF] June 2005 Issue 4. 555-245-766.

27. —. *Job Aids for Field Replacement Units (FRUs) for the Avaya S8700 Series Servers*. [PDF] May 2009 Issue 5. 03-300530.

28. —. *Maintenance Commands for Avaya Communication Manager, Media Gateways and Servers*. [PDF] January 2008. 03-300431.

29. —. *Product Brief, Avaya Intuity Audix LX Multimedia Server*. [PDF] 2007.